Emilie Dionisio
Cybersecurity Phase 1 Final Project
2022-12-16

For my cybersecurity phase 1 project, I used four host machines and installed virtual machines on them. I connected them by adding another router to my private network, resulting in a double NAT configuration. The Cybersecurity Lab is on a different subnet and it's using a Class B IP address of 172.17.17.0/24, whereas my home network is using Class C IP address of 192.168.4.0/24. Therefore, they are both on their own subnet.

You might have asked why I used four host machines for this project. First, I have old PCs that are just lying around in my computer room, and I want to put them to use. Plus, I don't want to use my everyday computer for my lab. Second, I realized that if I'm going to work in the cloud or as a Network Admin/Security Specialist, I need to be able to understand the basic networking concepts of connecting host machines and virtual machines and having them all communicate with each other and be on the same subnet. And last but not least, I assume that in the real world environment, some of the servers are not located in the same premise or building, so my thinking is, "How will I connect the hosts and virtual machines so that they are on the same subnet even though they are physically apart?"

Here's how I setup my Lab:

There are three host machines with Ubuntu Servers (with Suricata and Splunk), Kali, PfSense (with Snort), and Ubuntu Desktop installed, and the last host machine is my target or weak machine with Metasploitable VM and Windows 7 VM installed. Each host and virtual machine has two IP addresses, one for bridge mode and one for host only mode.

For my network adapters, I used Bridge mode for the 172.17.17.0/24 network and Host Only for the 192.168.56.0/24 network. By using bridge mode, all hosts and virtual machines can communicate to one another, and the host mode can establish its own private network between the host and virtual machine. Each host and virtual machine has two adapters.

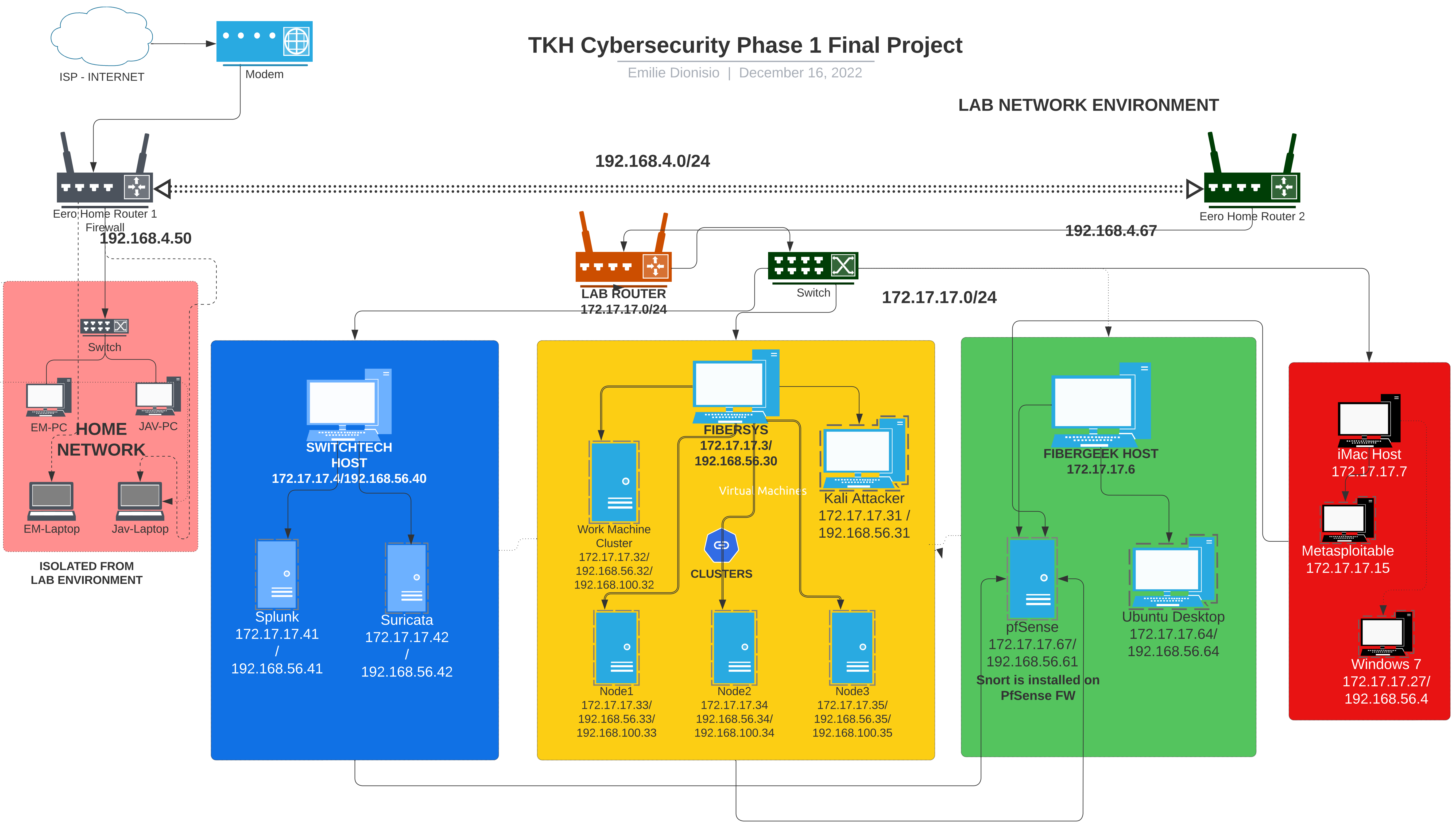
With the exception of the local cluster node virtual machines, I provisioned all of my nodes to use the same network configurations (bridge and host only). For the three nodes, I added a third adapter, provisioned them on Fibersys Host, and took screen photos that are displayed in the Fibersys Host portion. The setup is almost similar, but I've just added another adapter to allow for isolation of the three nodes to a single sub-network.

My analogy for using the Bridge and Host only mode is like the WAN (Bridge) and LAN (Host Only). I configured it this way so that I can easily use SSH on different host machines to connect to my virtual machines without having to go to the physical machine. In addition, I installed a VNC server on each of my host machines so that I can simply remote in using my main desktop, which is not part of the Lab network. The reason why I built this small network infrastructure was to demonstrate what I had learned and to be creative about it.

SWITCHTECH **172.17.17.4/192.168.56.40**	**FIBERSYS** **(172.17.17.3/192.168.56.30)**	**FIBERGEEK** **172.17.17.6/192.168.56.60**	**iMac - Metasploitable** **172.17.17.7/192.168.56.70**
Splunk on Ubuntu Server - 172.17.17.41/192.168.56.41	Kali - Control (Attacker) - 172.17.17.31/192.168.56.31	pFSense FW with Snort installed 172.17.17.67/192.168.56.61	Metasploitable 172.17.17.15
Suricata on Ubuntu Server 172.17.17.42/192.168.56.42	Workmachine.cluster.local - 172.17.17.32/192.168.56.32/192.168.100.32	Ubuntu Desktop to configure pFSense on the browser 172.17.17.64/192.168.56.64	Windows 7 172.17.17.27/192.168.56.4

TKH Cybersecurity Phase 1 Final Project

Emilie Dionisio | December 16, 2022



Emilie Dionisio

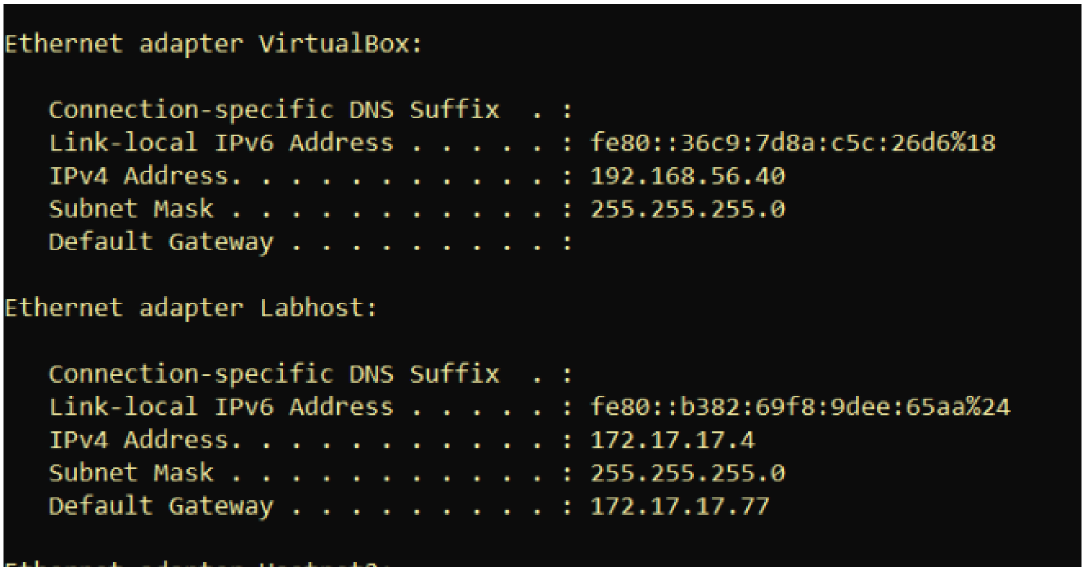
Cybersecurity Phase 1 Final Project

2022-12-16

Putty - installed on the host machine	node1.cluster.local - 172.17.17.33/192.168.56.33/192.168.100.33	Putty - installed on the host machine	Putty - installed on the host machine
	node2.cluster.local - 172.17.17.34/192.168.56.34/192.168.100.34		
	node3.cluster.local - 172.17.17.35/192.168.56.35/192.168.100.35		
	Putty - installed on the host machine		

Here are the screenshots and links to videos for each Host Machine: (Note: I uploaded my videos on one of my google drives and shared it without using credentials so you can just click the link and it's not loading the TKH google drive.)

SWITCHTECH HOST

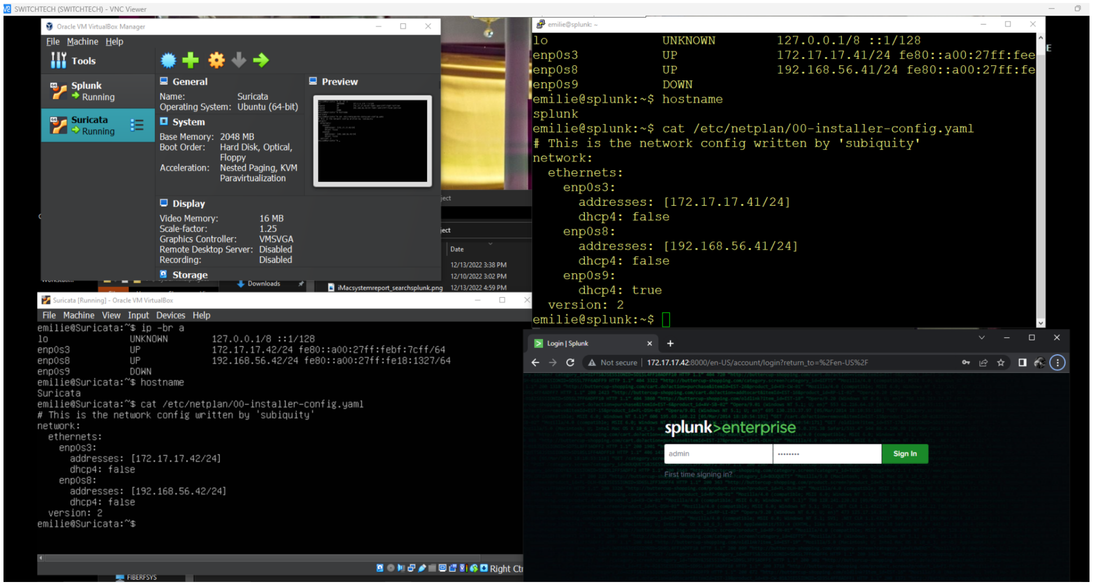


```
Ethernet adapter VirtualBox:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::36c9:7d8a:c5c:26d6%18
   IPv4 Address. . . . . . . . . . . : 192.168.56.40
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Labhost:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b382:69f8:9dee:65aa%24
   IPv4 Address. . . . . . . . . . . : 172.17.17.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.17.17.77
```

Emilie Dionisio

Cybersecurity Phase 1 Final Project

2022-12-16



Name: Suricata
Operating System: Ubuntu (64-bit)

Base Memory: 2048 MB
Boot Order: Hard Disk, Optical, Floppy
Acceleration: Nested Paging, KVM Paravirtualization

Video Memory: 16 MB
Scale-factor: 1.25
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

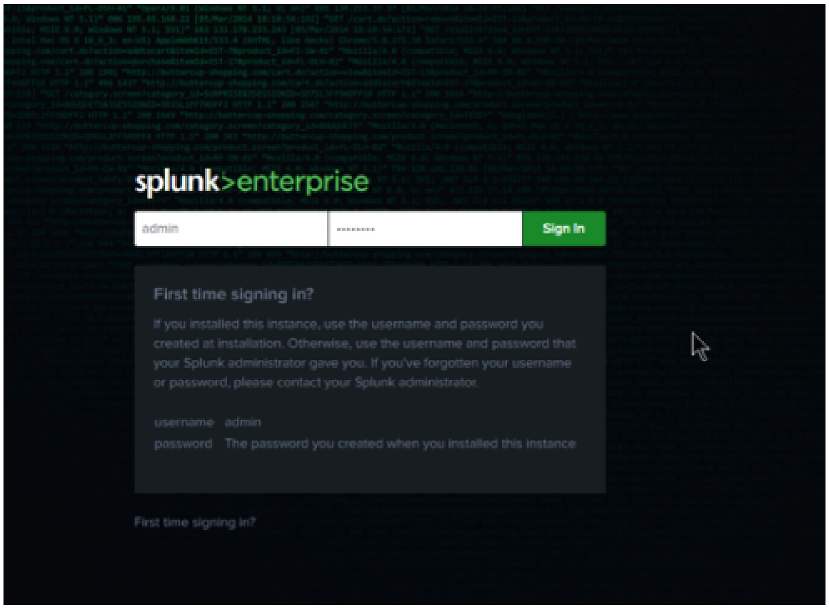
12/13/2022 3:38 PM
12/10/2022 3:02 PM
iMacsystemreport_searchsplunk.png 12/13/2022 4:59 PM

```
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             172.17.17.41/24 fe80::a00:27ff:fee
enp0s8           UP             192.168.56.41/24 fe80::a00:27ff:fe
enp0s9           DOWN
emilie@splunk:~$ hostname
splunk
emilie@splunk:~$ cat /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses: [172.17.17.41/24]
      dhcp4: false
    enp0s8:
      addresses: [192.168.56.41/24]
      dhcp4: false
    enp0s9:
      dhcp4: true
  version: 2
emilie@splunk:~$
```

```
emilie@Suricata:~$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             172.17.17.42/24 fe80::a00:27ff:febf:7cff/64
enp0s8           UP             192.168.56.42/24 fe80::a00:27ff:fe18:1327/64
enp0s9           DOWN
emilie@Suricata:~$ hostname
Suricata
emilie@Suricata:~$ cat /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses: [172.17.17.42/24]
      dhcp4: false
    enp0s8:
      addresses: [192.168.56.42/24]
      dhcp4: false
  version: 2
emilie@Suricata:~$
```

172.17.17.42:8000/en-US/account/login?return_to=%2Fen-US%2F

Splunk Screenshots:



First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

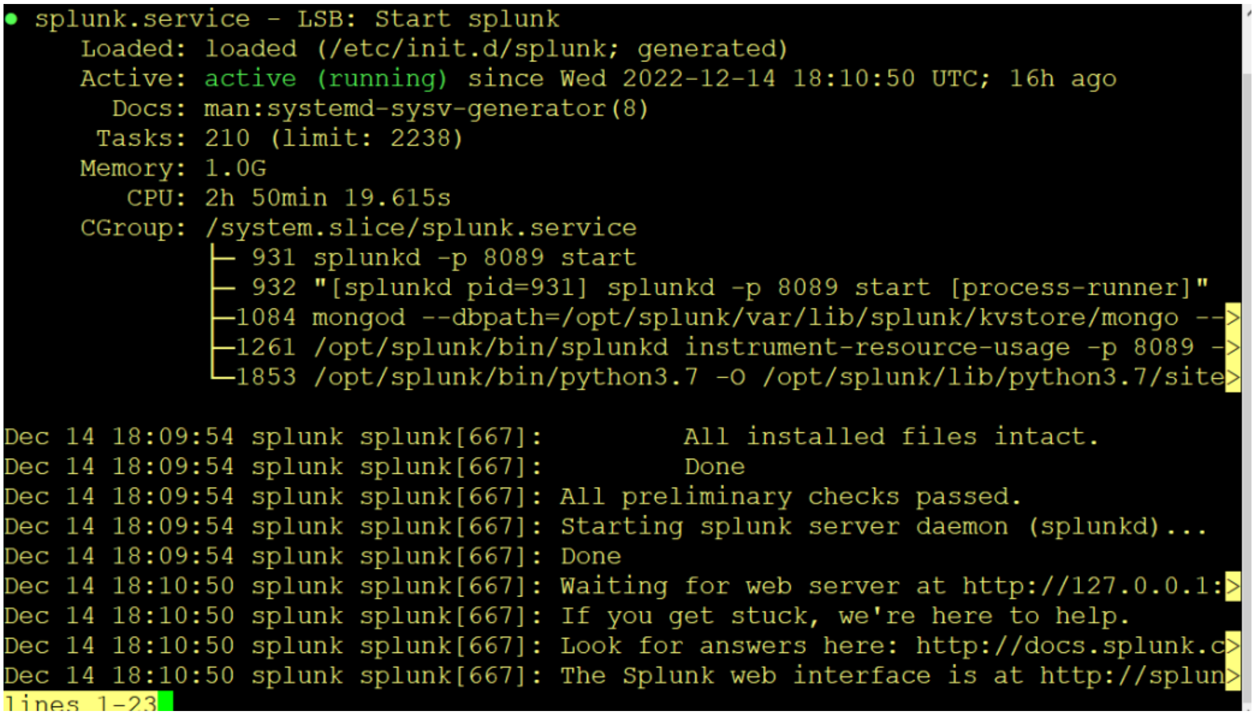
First time signing in?

Emilie Dionisio

Cybersecurity Phase 1 Final Project

2022-12-16

Splunk: Photo below shows that Splunk is active and running in the background.

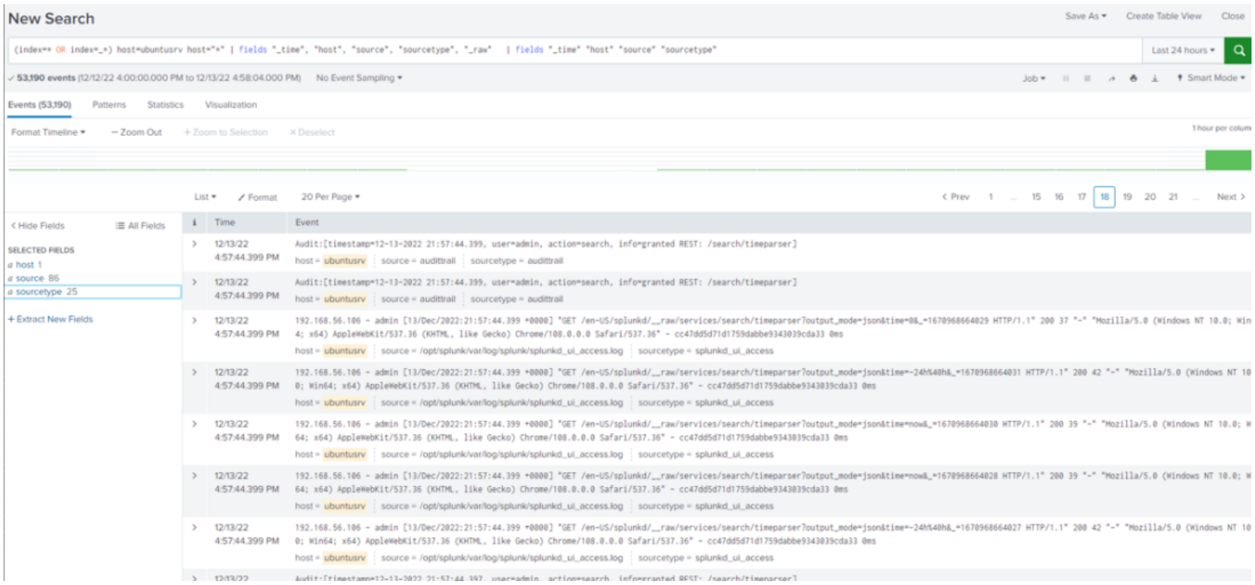


```
● splunk.service - LSB: Start splunk
     Loaded: loaded (/etc/init.d/splunk; generated)
     Active: active (running) since Wed 2022-12-14 18:10:50 UTC; 16h ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 210 (limit: 2238)
     Memory: 1.0G
        CPU: 2h 50min 19.615s
     CGroup: /system.slice/splunk.service
             ├─ 931 splunkd -p 8089 start
             ├─ 932 "[splunkd pid=931] splunkd -p 8089 start [process-runner]"
             ├─1084 mongod --dbpath=/opt/splunk/var/lib/splunk/kvstore/mongo -->
             ├─1261 /opt/splunk/bin/splunkd instrument-resource-usage -p 8089 ->
             └─1853 /opt/splunk/bin/python3.7 -O /opt/splunk/lib/python3.7/site>

Dec 14 18:09:54 splunk splunk[667]:         All installed files intact.
Dec 14 18:09:54 splunk splunk[667]:         Done
Dec 14 18:09:54 splunk splunk[667]: All preliminary checks passed.
Dec 14 18:09:54 splunk splunk[667]: Starting splunk server daemon (splunkd)...
Dec 14 18:09:54 splunk splunk[667]: Done
Dec 14 18:10:50 splunk splunk[667]: Waiting for web server at http://127.0.0.1:>
Dec 14 18:10:50 splunk splunk[667]: If you get stuck, we're here to help.
Dec 14 18:10:50 splunk splunk[667]: Look for answers here: http://docs.splunk.c>
Dec 14 18:10:50 splunk splunk[667]: The Splunk web interface is at http://splun>
lines 1-23
```

I was able to upload my own data from my host machine. I uploaded both iMac system logs and also Windows system logs.

Here's a sample of the actual system log from my old iMac machine. I was able to pull the system log from my iMac by going to the Apple icon on the top left, clicked on About, clicked on System Report once it's previewed, clicked on File then save as a text and uploaded on Splunk and created a report shown below:

Splunk Report:



```
(index=* OR index=_*) host=ubuntusrv host="*" | fields "_time", "host", "source", "sourcetype", "_raw"   | fields "_time" "host" "source" "sourcetype"
```

✓ 53,190 events (12/12/22 4:00:00.000 PM to 12/13/22 4:58:04.000 PM)   No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 86
- a sourcetype 25

i	Time	Event
›	12/13/22 4:57:44.399 PM	Audit:[timestamp=12-13-2022 21:57:44.399, user=admin, action=search, info=granted REST: /search/timeparser] host = ubuntusrv | source = audittrail | sourcetype = audittrail
›	12/13/22 4:57:44.399 PM	Audit:[timestamp=12-13-2022 21:57:44.399, user=admin, action=search, info=granted REST: /search/timeparser] host = ubuntusrv | source = audittrail | sourcetype = audittrail
›	12/13/22 4:57:44.399 PM	192.168.56.106 - admin [13/Dec/2022:21:57:44.399 +0000] "GET /en-US/splunkd/__raw/services/search/timeparser?output_mode=json&time=0&_=1670968664029 HTTP/1.1" 200 37 "-" "Mozilla/5.0 (Windows NT 10.0; Win 4; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36" - cc47dd5d71d1759dabbe9343039cda33 0ms host = ubuntusrv | source = /opt/splunk/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access
›	12/13/22 4:57:44.399 PM	192.168.56.106 - admin [13/Dec/2022:21:57:44.399 +0000] "GET /en-US/splunkd/__raw/services/search/timeparser?output_mode=json&time=-24h%40h&_=1670968664031 HTTP/1.1" 200 42 "-" "Mozilla/5.0 (Windows NT 10 0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36" - cc47dd5d71d1759dabbe9343039cda33 0ms host = ubuntusrv | source = /opt/splunk/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access
›	12/13/22 4:57:44.399 PM	192.168.56.106 - admin [13/Dec/2022:21:57:44.399 +0000] "GET /en-US/splunkd/__raw/services/search/timeparser?output_mode=json&time=now&_=1670968664030 HTTP/1.1" 200 39 "-" "Mozilla/5.0 (Windows NT 10.0; W 64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36" - cc47dd5d71d1759dabbe9343039cda33 0ms host = ubuntusrv | source = /opt/splunk/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access
›	12/13/22 4:57:44.399 PM	192.168.56.106 - admin [13/Dec/2022:21:57:44.399 +0000] "GET /en-US/splunkd/__raw/services/search/timeparser?output_mode=json&time=now&_=1670968664028 HTTP/1.1" 200 39 "-" "Mozilla/5.0 (Windows NT 10.0; W 64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36" - cc47dd5d71d1759dabbe9343039cda33 0ms host = ubuntusrv | source = /opt/splunk/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access
›	12/13/22 4:57:44.399 PM	192.168.56.106 - admin [13/Dec/2022:21:57:44.399 +0000] "GET /en-US/splunkd/__raw/services/search/timeparser?output_mode=json&time=-24h%40h&_=1670968664027 HTTP/1.1" 200 42 "-" "Mozilla/5.0 (Windows NT 10 0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36" - cc47dd5d71d1759dabbe9343039cda33 0ms host = ubuntusrv | source = /opt/splunk/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access
›	12/13/22	Audit:[timestamp=12-13-2022 21:57:44.397, user=admin, action=search, info=granted REST: /search/timeparser]

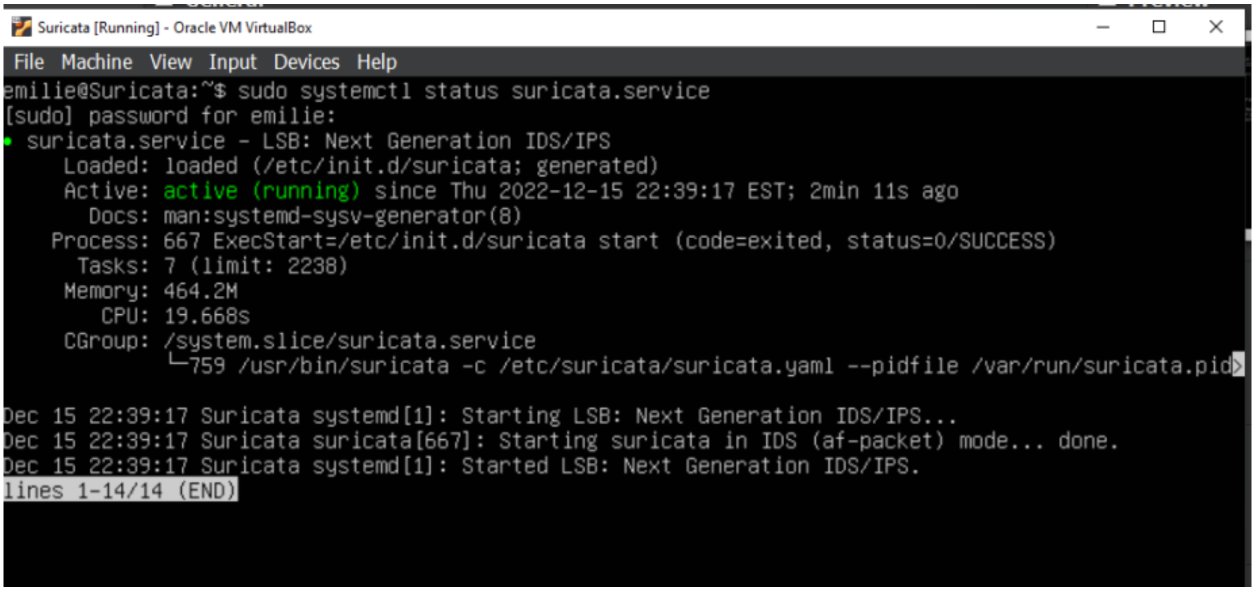
Suricata Screenshots:

Photo below shows that Suricata is active and running in the background.

Emilie Dionisio

Cybersecurity Phase 1 Final Project

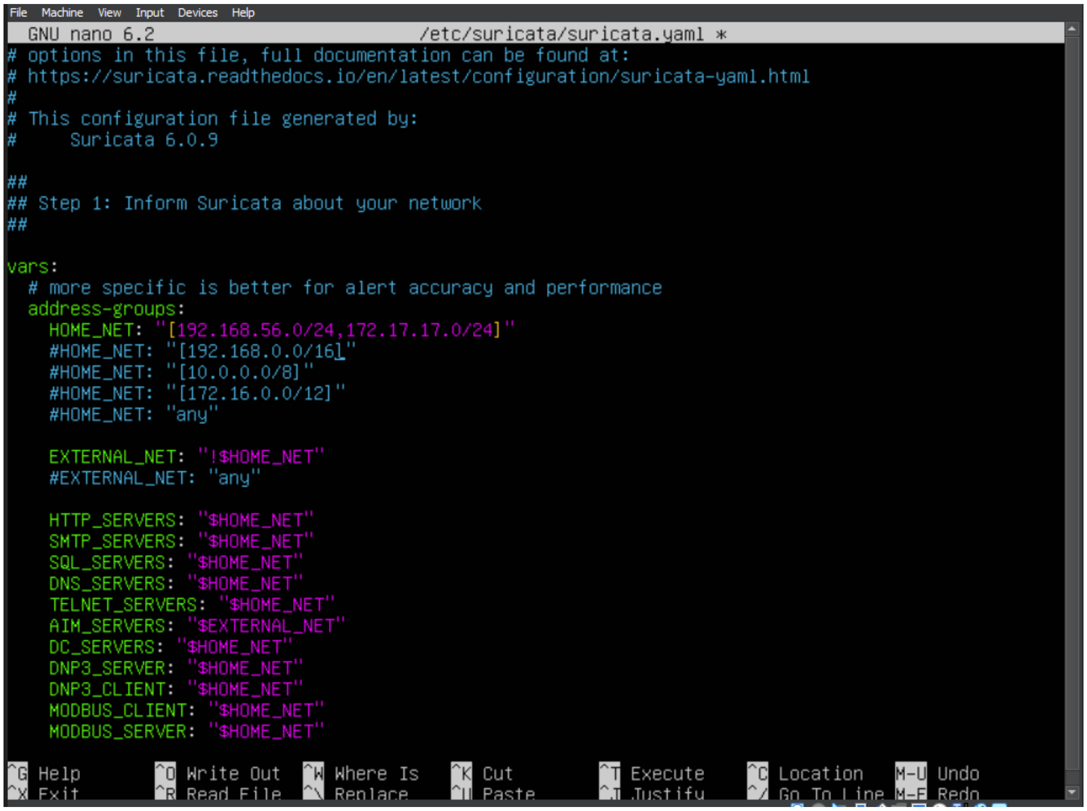
2022-12-16



Suricata [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
emilie@Suricata:~$ sudo systemctl status suricata.service
[sudo] password for emilie:
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (running) since Thu 2022-12-15 22:39:17 EST; 2min 11s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 667 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
      Tasks: 7 (limit: 2238)
     Memory: 464.2M
        CPU: 19.668s
     CGroup: /system.slice/suricata.service
             └─759 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid>

Dec 15 22:39:17 Suricata systemd[1]: Starting LSB: Next Generation IDS/IPS...
Dec 15 22:39:17 Suricata suricata[667]: Starting suricata in IDS (af-packet) mode... done.
Dec 15 22:39:17 Suricata systemd[1]: Started LSB: Next Generation IDS/IPS.
lines 1-14/14 (END)
```

Suricata yaml file.



```
  GNU nano 6.2                    /etc/suricata/suricata.yaml *
# options in this file, full documentation can be found at:
# https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html
#
# This configuration file generated by:
#     Suricata 6.0.9

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.56.0/24,172.17.17.0/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```

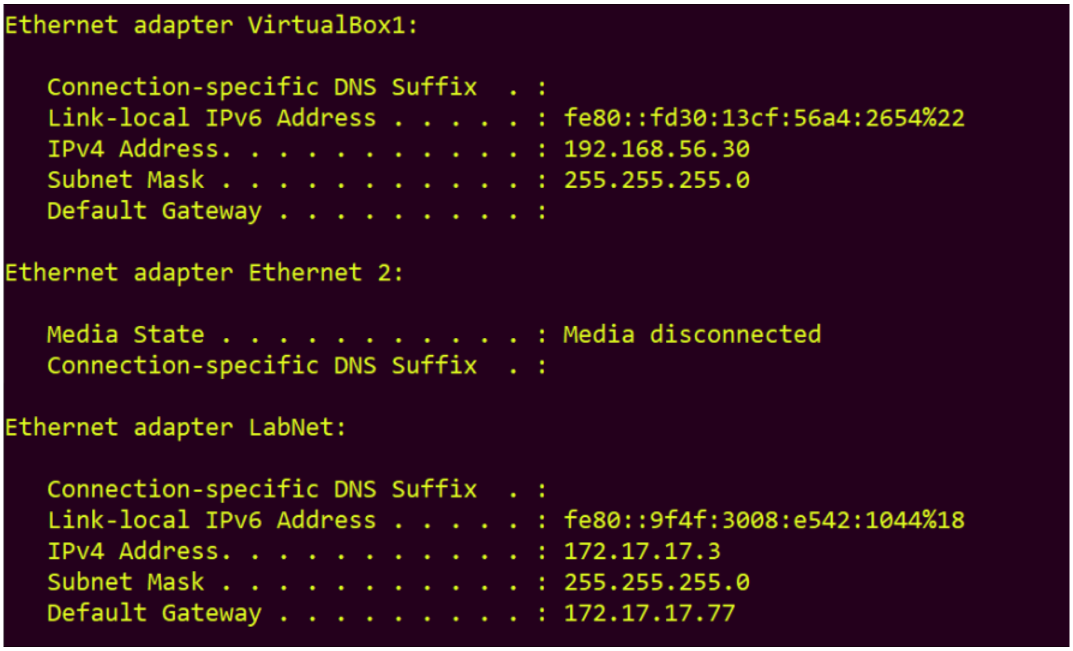
Installation video of Suricata: https://drive.google.com/file/d/1nC9ekdICy42Ujc5ZBItAZUdzuv6c5J-4/view

Emilie Dionisio

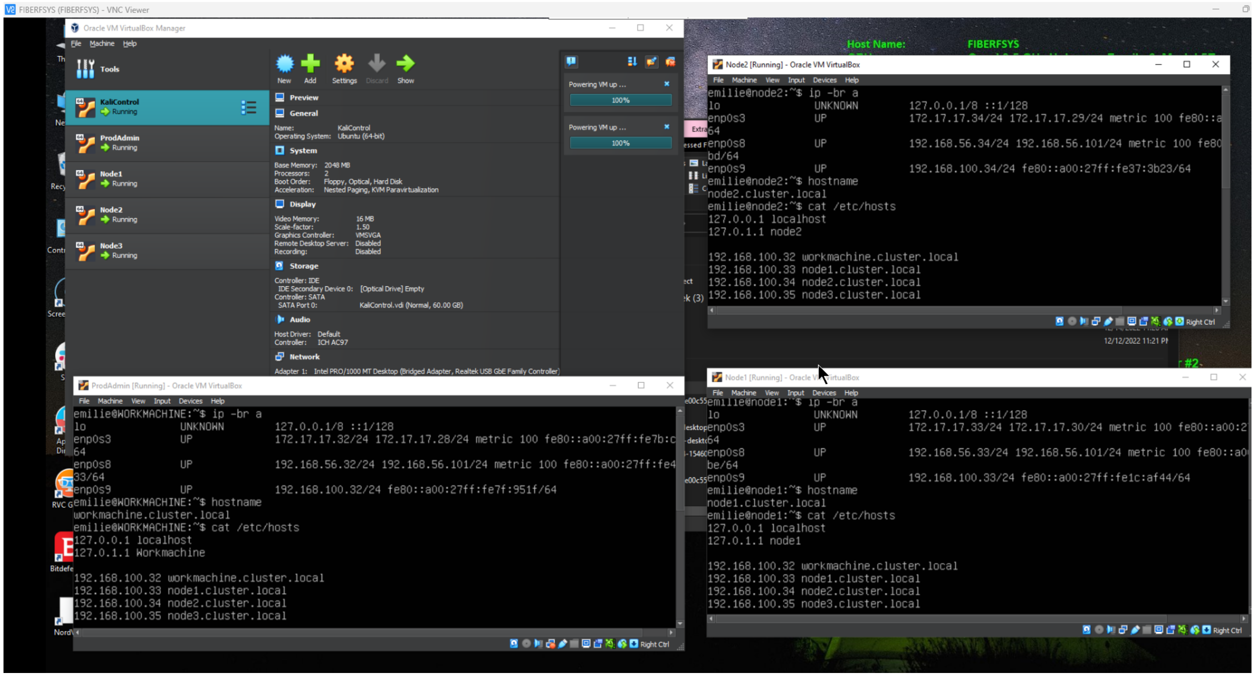
Cybersecurity Phase 1 Final Project

2022-12-16

FIBERSYS HOST



```
Ethernet adapter VirtualBox1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fd30:13cf:56a4:2654%22
   IPv4 Address. . . . . . . . . . . : 192.168.56.30
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter LabNet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9f4f:3008:e542:1044%18
   IPv4 Address. . . . . . . . . . . : 172.17.17.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.17.17.77
```



Preview

General
Name: KaliControl
Operating System: Ubuntu (64-bit)

System
Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Scale-factor: 1.50
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: KaliControl.vdi (Normal, 60.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Realtek USB GbE Family Controller)

Node2 [Running] - Oracle VM VirtualBox

```
emilie@node2:~$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             172.17.17.34/24 172.17.17.29/24 metric 100 fe80::a
64
enp0s8           UP             192.168.56.34/24 192.168.56.101/24 metric 100 fe80
bd/64
enp0s9           UP             192.168.100.34/24 fe80::a00:27ff:fe37:3b23/64
emilie@node2:~$ hostname
node2.cluster.local
emilie@node2:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 node2

192.168.100.32 workmachine.cluster.local
192.168.100.33 node1.cluster.local
192.168.100.34 node2.cluster.local
192.168.100.35 node3.cluster.local
```

ProdAdmin [Running] - Oracle VM VirtualBox

```
emilie@WORKMACHINE:~$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             172.17.17.32/24 172.17.17.28/24 metric 100 fe80::a00:27ff:fe7b:c
64
enp0s8           UP             192.168.56.32/24 192.168.56.101/24 metric 100 fe80::a00:27ff:fe4
33/64
enp0s9           UP             192.168.100.32/24 fe80::a00:27ff:fe7f:951f/64
emilie@WORKMACHINE:~$ hostname
workmachine.cluster.local
emilie@WORKMACHINE:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 Workmachine

192.168.100.32 workmachine.cluster.local
192.168.100.33 node1.cluster.local
192.168.100.34 node2.cluster.local
192.168.100.35 node3.cluster.local
```

Node1 [Running] - Oracle VM VirtualBox

```
emilie@node1:~$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             172.17.17.33/24 172.17.17.30/24 metric 100 fe80::a00:2
64
enp0s8           UP             192.168.56.33/24 192.168.56.101/24 metric 100 fe80::a0
be/64
enp0s9           UP             192.168.100.33/24 fe80::a00:27ff:fe1c:af44/64
emilie@node1:~$ hostname
node1.cluster.local
emilie@node1:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 node1

192.168.100.32 workmachine.cluster.local
192.168.100.33 node1.cluster.local
192.168.100.34 node2.cluster.local
192.168.100.35 node3.cluster.local
```

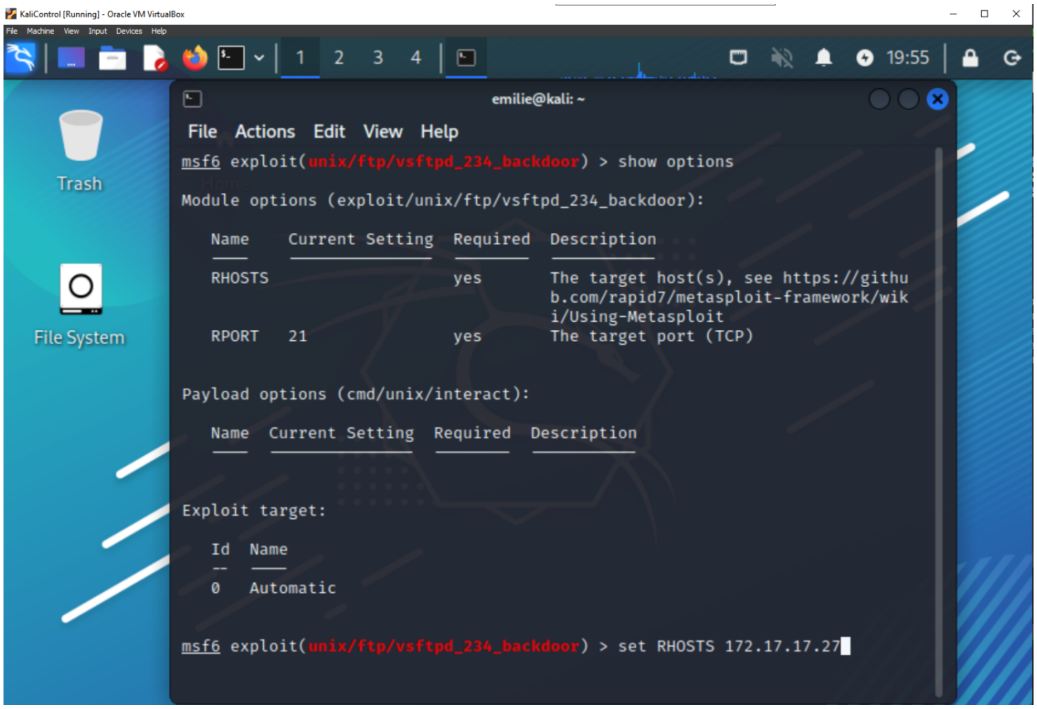
Here's a link to show how to setup a node and how to ssh to a node:
https://drive.google.com/file/d/1x9UKimzzfPiHtiRg3UQZBjGWiAXwbRfo/view?usp=share_link

I was able to exploit the Metasploitable and Windows 7 virtual machines that are installed on iMac Host from my Kali Linux virtual machine that is installed on Fibersys host.

Emilie Dionisio

Cybersecurity Phase 1 Final Project

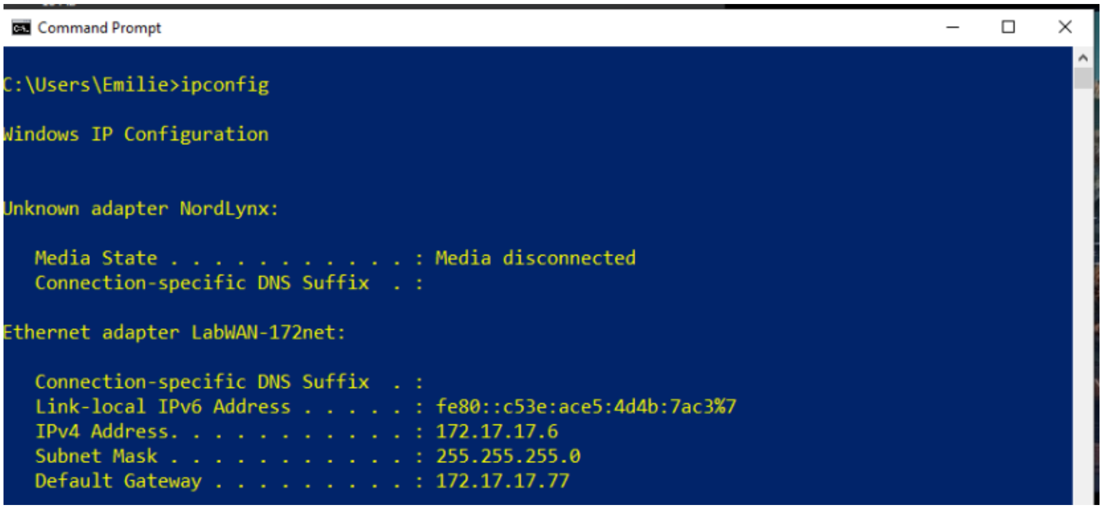
2022-12-16


KaliControl [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:55
Trash
File System
emilie@kali: ~
File Actions Edit View Help

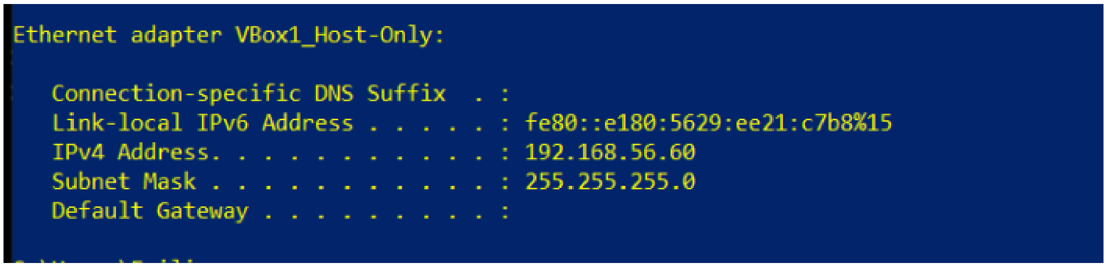
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://githu
                                      b.com/rapid7/metasploit-framework/wik
                                      i/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.17.27
```

FIBERGEEK HOST:

Screenshots of my host machine with WAN (Bridge) and LAN (Host only)



```
C:\Users\Emilie>ipconfig

Windows IP Configuration


Unknown adapter NordLynx:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter LabWAN-172net:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c53e:ace5:4d4b:7ac3%7
   IPv4 Address. . . . . . . . . . . : 172.17.17.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.17.17.77
```

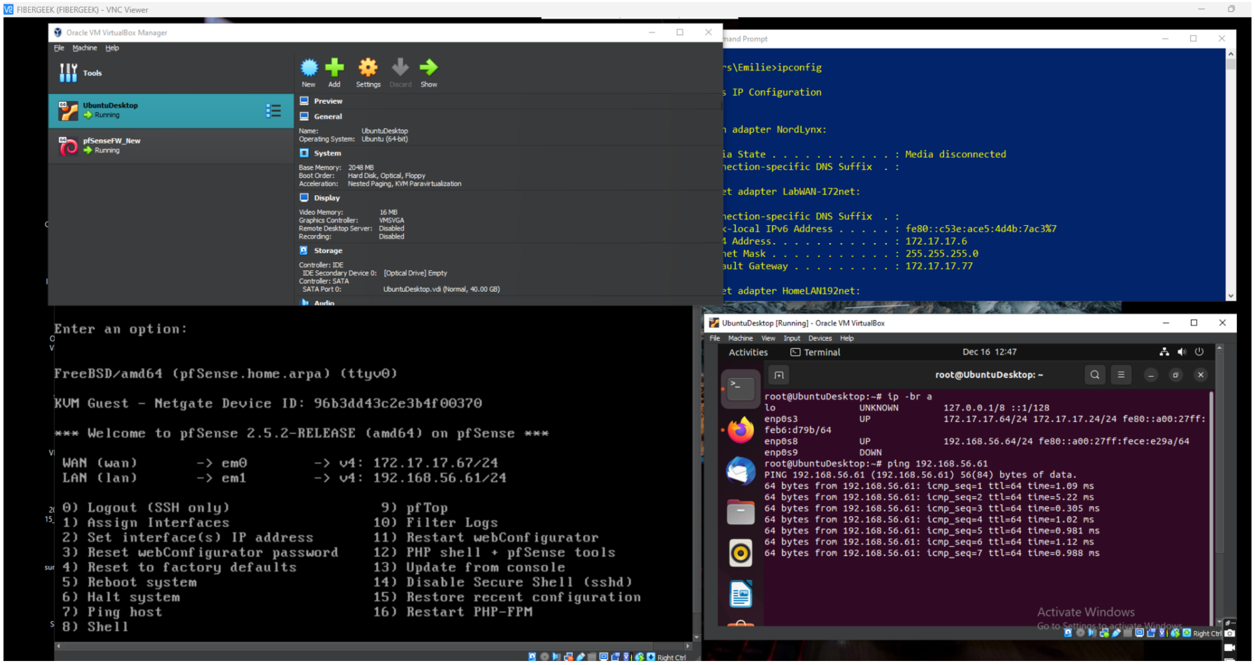


```
Ethernet adapter VBox1_Host-Only:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e180:5629:ee21:c7b8%15
   IPv4 Address. . . . . . . . . . . : 192.168.56.60
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Emilie Dionisio

Cybersecurity Phase 1 Final Project

2022-12-16


FIBERGEEK (FIBERGEEK) - VNC Viewer
Oracle VM VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Show
UbuntuDesktop
Running
pfSenseFW_New
Running
Preview
General
System
Display
Storage
Audio
mand Prompt
UbuntuDesktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Dec 16 12:47
root@UbuntuDesktop: ~
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

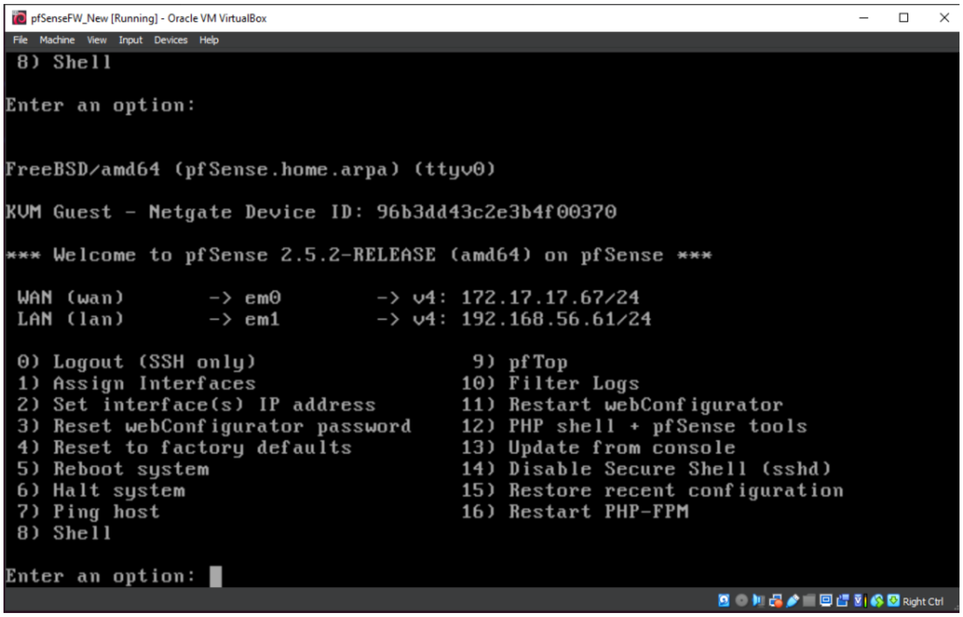
```
Name:               UbuntuDesktop
Operating System:   Ubuntu (64-bit)

Base Memory:    2048 MB
Boot Order:     Hard Disk, Optical, Floppy
Acceleration:   Nested Paging, KVM Paravirtualization

Video Memory:            16 MB
Graphics Controller:     VMSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled

Controller: IDE
 IDE Secondary Device 0:   [Optical Drive] Empty
Controller: SATA
 SATA Port 0:              UbuntuDesktop.vdi (Normal, 40.00 GB)
```

```
rs\Emilie>ipconfig

s IP Configuration


n adapter NordLynx:

ia State . . . . . . . . . . . : Media disconnected
nection-specific DNS Suffix  . :

et adapter LabWAN-172net:

nection-specific DNS Suffix  . :
k-local IPv6 Address . . . . . : fe80::c53e:ace5:4d4b:7ac3%7
4 Address. . . . . . . . . . . : 172.17.17.6
net Mask . . . . . . . . . . . : 255.255.255.0
ault Gateway . . . . . . . . . : 172.17.17.77

et adapter HomeLAN192net:
```

```
Enter an option:

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

KVM Guest - Netgate Device ID: 96b3dd43c2e3b4f00370

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 172.17.17.67/24
 LAN (lan)       -> em1        -> v4: 192.168.56.61/24

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

```
root@UbuntuDesktop:~# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             172.17.17.64/24 172.17.17.24/24 fe80::a00:27ff:
feb6:d79b/64
enp0s8           UP             192.168.56.64/24 fe80::a00:27ff:fece:e29a/64
enp0s9           DOWN
root@UbuntuDesktop:~# ping 192.168.56.61
PING 192.168.56.61 (192.168.56.61) 56(84) bytes of data.
64 bytes from 192.168.56.61: icmp_seq=1 ttl=64 time=1.09 ms
64 bytes from 192.168.56.61: icmp_seq=2 ttl=64 time=5.22 ms
64 bytes from 192.168.56.61: icmp_seq=3 ttl=64 time=0.305 ms
64 bytes from 192.168.56.61: icmp_seq=4 ttl=64 time=1.02 ms
64 bytes from 192.168.56.61: icmp_seq=5 ttl=64 time=0.981 ms
64 bytes from 192.168.56.61: icmp_seq=6 ttl=64 time=1.12 ms
64 bytes from 192.168.56.61: icmp_seq=7 ttl=64 time=0.988 ms
```

PfSense Screenshots:


pfSenseFW_New [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
 8) Shell

Enter an option:


FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

KVM Guest - Netgate Device ID: 96b3dd43c2e3b4f00370

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 172.17.17.67/24
 LAN (lan)       -> em1        -> v4: 192.168.56.61/24

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

Enter an option: █
```

This is how I changed the WAN and LAN IP Addresses for PfSense:
https://drive.google.com/file/d/170pLqkc3o9RoSeaya3dLUpF0soFauYIe/view?usp=share_link

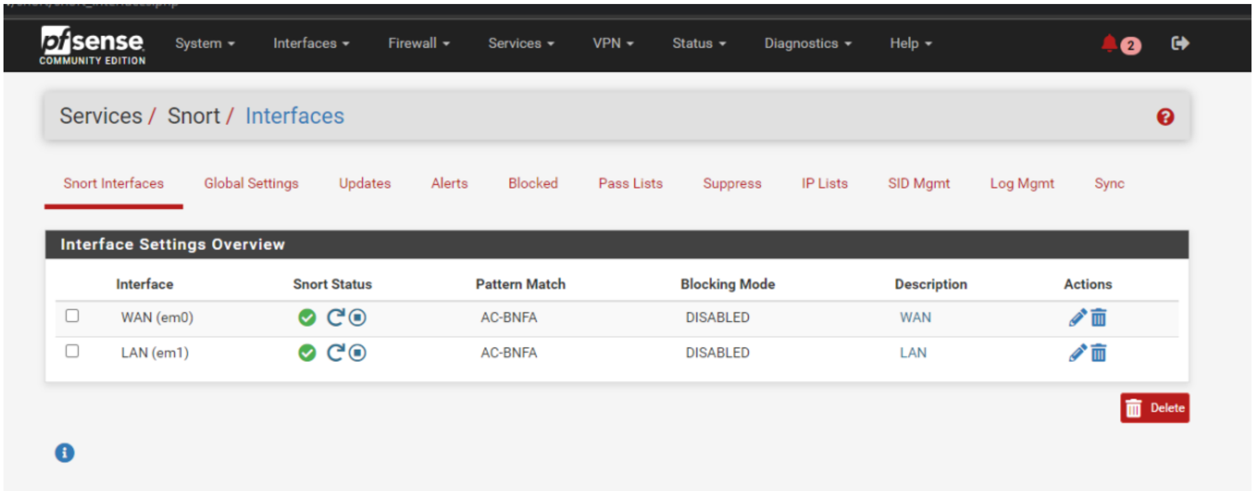
Link to successful installation of PfSense and I was able to login to the Web Interface of PfSense:
https://drive.google.com/file/d/15cephiaGUA5vjKiG0tmroYyfE3VBIoyj/view?usp=share_link

Emilie Dionisio

Cybersecurity Phase 1 Final Project

2022-12-16

I added Snort in PfSense:



Services / Snort / Interfaces

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

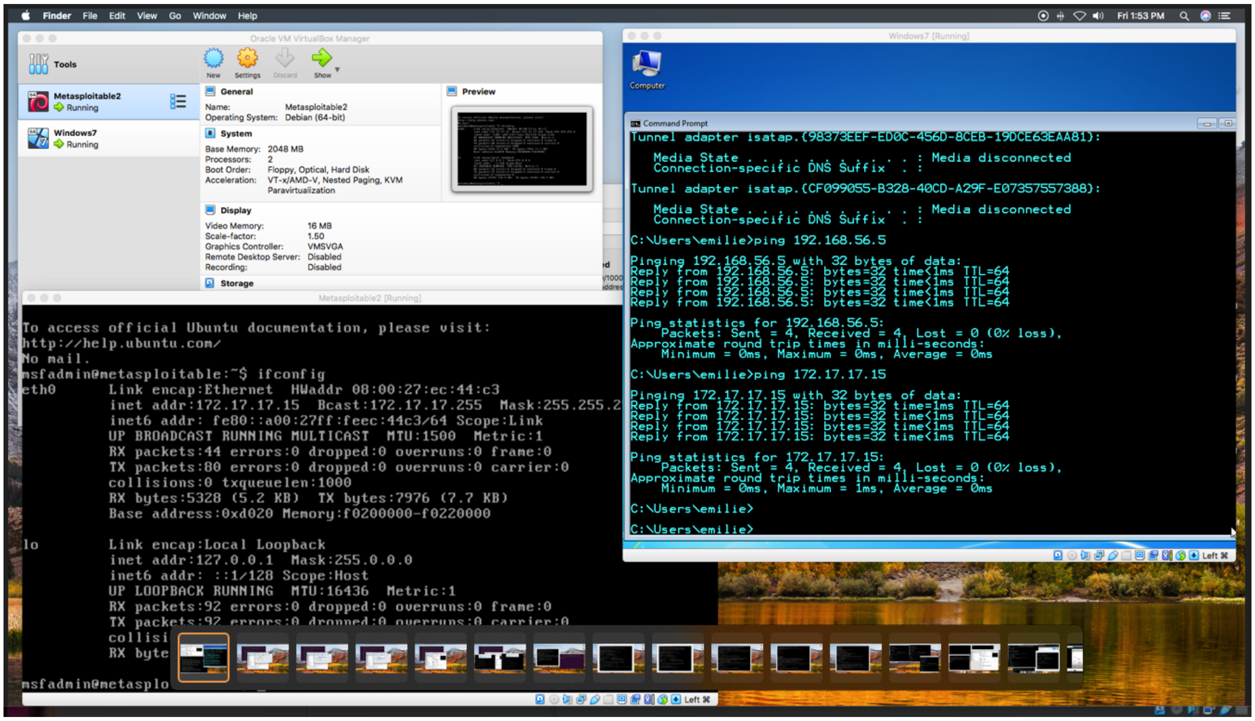
Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	WAN (em0)	✓	AC-BNFA	DISABLED	WAN	
□	LAN (em1)	✓	AC-BNFA	DISABLED	LAN	

Video on how I added Snort in PfSense:
https://drive.google.com/file/d/1Lmbs9nktJWvfoZOFmsN3FGsvJPnOkhuA/view?usp=share_link

iMac (Metasploitable/Weak Virtual Machine)

Photo shown below is the iMac weak machine with Metasploitable and Windows 7 installed.



Name: Metasploitable2
Operating System: Debian (64-bit)

Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Video Memory: 16 MB
Scale-factor: 1.50
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ec:44:c3
          inet addr:172.17.17.15  Bcast:172.17.17.255  Mask:255.255.2
          inet6 addr: fe80::a00:27ff:feec:44c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5328 (5.2 KB)  TX bytes:7976 (7.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisi
          RX byte

msfadmin@metasplo
```

```
Tunnel adapter isatap.{98373EEF-ED0C-456D-8CEB-19DCE63EAA81}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{CF099055-B328-40CD-A29F-E07357557388}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\emilie>ping 192.168.56.5

Pinging 192.168.56.5 with 32 bytes of data:
Reply from 192.168.56.5: bytes=32 time<1ms TTL=64
Reply from 192.168.56.5: bytes=32 time<1ms TTL=64
Reply from 192.168.56.5: bytes=32 time<1ms TTL=64
Reply from 192.168.56.5: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\emilie>ping 172.17.17.15

Pinging 172.17.17.15 with 32 bytes of data:
Reply from 172.17.17.15: bytes=32 time=1ms TTL=64
Reply from 172.17.17.15: bytes=32 time<1ms TTL=64
Reply from 172.17.17.15: bytes=32 time<1ms TTL=64
Reply from 172.17.17.15: bytes=32 time<1ms TTL=64

Ping statistics for 172.17.17.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\emilie>

C:\Users\emilie>
```

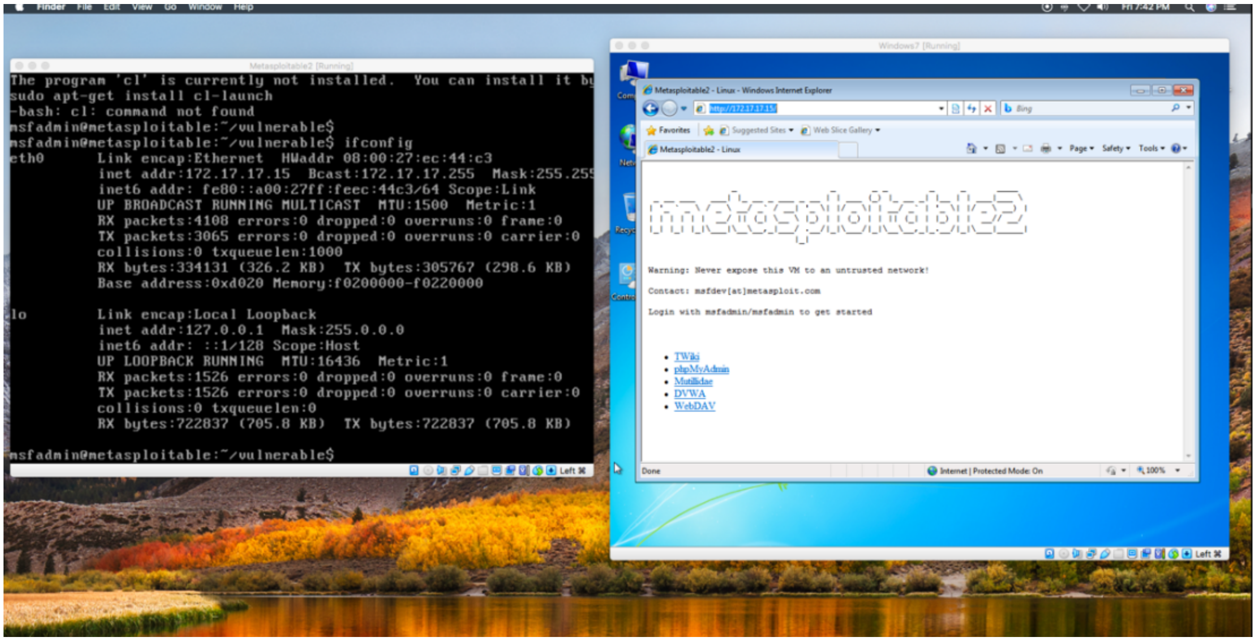
Here's a link to view that I was able to exploit the Metasploitable VM and Windows 7:
https://drive.google.com/file/d/1t3qNYQZ-IuBjMzpbteaQPpm2i656-Ccz/view?usp=share_link

Emilie Dionisio

Cybersecurity Phase 1 Final Project

2022-12-16

Metasploitable VM



Finder File Edit View Go Window Help
Fri 7:42 PM
Metasploitable2 [Running]
Windows7 [Running]
Left ⌘

```
The program 'cl' is currently not installed.  You can install it by
sudo apt-get install cl-launch
-bash: cl: command not found
msfadmin@metasploitable:~/vulnerable$
msfadmin@metasploitable:~/vulnerable$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ec:44:c3
          inet addr:172.17.17.15  Bcast:172.17.17.255  Mask:255.255
          inet6 addr: fe80::a00:27ff:feec:44c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3065 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:334131 (326.2 KB)  TX bytes:305767 (298.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1526 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1526 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:722837 (705.8 KB)  TX bytes:722837 (705.8 KB)

msfadmin@metasploitable:~/vulnerable$
```

```
metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Information about network adapters (I will not discuss the other adapter settings because I didn't use it for this lab).

Bridge mode means that the VM will be on the same subnet as the host machine or physical machine. For example, the additional router I added to my private network for my Cybersecurity Lab has a range of IP addresses of 172.17.17.0/24. If I create a new VM and choose bridge mode for adapter 1 while using DHCP, the first IP address assigned to that VM instance will be 172.17.17.2, which is the same IP range as my router.

Host-only mode establishes a private virtual network between the host machine and that specific VM machine and only permits network operations. This configuration works well if I want my virtual machine to communicate directly with my host computer using SSH.

Nat-Network (local-cluster-nat) means that nodes are exclusively connected to each other only. Nodes cannot access the internet and Internet cannot access the nodes.

I used the following Operating Systems for this Lab:

Ubuntu Server is an operating system that is exactly the same as Ubuntu Desktop but it doesn't include a GUI or a lot of the pre-packaged junk that **Ubuntu Desktop** does. As a result, there are major increases in performance since the operating system doesn't have to process having a GUI open at the same time as running servers. Ubuntu Server is basically like having the terminal window of Ubuntu in full screen mode, but you cannot close the terminal window and it is the interface used to interact with the operating system.

Kali Linux is a Debian-based open-source Linux system designed for a variety of information security tasks such as penetration testing, security research, computer forensics, and reverse engineering. I use Kali to exploit the Metasploitable and Windows 7 virtual machines.

Emilie Dionisio

Cybersecurity Phase 1 Final Project

2022-12-16

Windows 7 is a Microsoft Windows operating system. I only used this for penetration testing to exploit it from Kali.

Metasploitable virtual machine is a deliberately vulnerable version of Ubuntu Linux that is used to test security tools and demonstrate common vulnerabilities.

I was able to do a simple penetration testing from the Kali Control VM to my iMac Metasploitable VM. I did a demo video included on this project: https://drive.google.com/file/d/1t3qNYQZ-IuBjMzpbteaQPpm2i656-Ccz/view?usp=share_link. First, I installed Metasploitable 2 on a virtual box on my iMac and I was able to scan it from my KaliControl virtual box on my Windows machine. I ran this command: nmap -sV -O 172.17.17.15 and it showed me which port is available and accessible then I was to get in and view the directories and folders.

Applications I installed for this Lab:

Splunk is a real-time analytics-driven SIEM tool that collects, analyzes, and correlates large amounts of network and other machine data. Splunk, which is managed through a web browser, provides security teams with the relevant and actionable intelligence they need to respond to threats more effectively and maintain an airtight security posture at scale.

What can Splunk do?

Monitoring of Security

Splunk continuously monitors all network resources and activity 24 hours a day, seven days a week in order to detect anomalous behavior before it poses a serious threat to the organization. Security teams can get a detailed, data-driven view of the network's performance, health, and vulnerabilities at any time by using the information Splunk provides. Splunk automatically alerts the appropriate parties with complete contextual information detailing the threat when malicious or high-risk activity is detected.

- Automated event notification
- Automated event log collection for all devices, applications, and user activity
- Data-rich, graphical user dashboards
- Correlation parameters that are predefined and customizable
- Collect critical data to ensure audit readiness.

Detection of Advanced Threats

Splunk can detect and contextualize active threats or anomalous behavior in real-time by intelligently monitoring infrastructure, applications, users, and other network resources across environments. Splunk cross-correlates event logs to uncover indicators of compromise or malicious relationships, allowing security teams to engage with potential threats immediately before significant network damage occurs.

- Visibility and analytics across the entire network
- Threat classification that is intelligent
- Correlation of event logs across devices and environments
- To identify advanced threats, use the kill chain methodology.
- To detect behavioral and/or statistical anomalies, use user behavior analytics (UBA).

Emilie Dionisio

Cybersecurity Phase 1 Final Project

2022-12-16

Response to an Incident

When a threat is detected, security teams can respond more quickly and confidently than with legacy SIEM technology. Splunk's Adaptive Response Framework contextualizes event data across environments and automates response workflows, allowing analysts to quickly confirm, prioritize, and engage threats with the necessary information.

- Event notifications with threat prioritization
- Pull relevant threat information across devices and environments automatically.
- Automation of response workflow
- Dashboards with a lot of data and graphics

Forensic Investigations

Each day, Splunk monitors and logs massive data sets of security information gathered from a variety of network sources. This wealth of data can be used by security teams to conduct thorough forensic investigations into the origins of a breach or to validate emerging threats in order to gain a better understanding of the effectiveness of their security efforts (and make improvements accordingly).

- Automatic alert triage to identify high-priority incidents
- Data can be searched across devices, users, applications, time frames, and so on.
- Visualizations and reports that are customizable
- Capability to create event and activity sequences

What is Suricata?

Suricata is an open-source detection engine that may serve as both an intrusion detection system (IDS) and an intrusion prevention system (IPS). To identify and stop threats, the system employs a rule set and a signature language. Suricata is an excellent tool to have for intrusion detection. A geographic breakdown of the traffic entering and leaving your network can be created using the data generated by Suricata.

Suricata is an externally built rule set-based ID/PS engine that uses rules to monitor network traffic and notify the system administrator when suspicious activities take place. Suricata has unified output functionality and pluggable library options to accept calls from other applications. It is made to interact with current network security components.

What is Snort?

Snort is an open source network intrusion detection system created by Martin Roesch, the founder and former CTO of Sourcefire. Snort is now developed and maintained by Cisco. Snort is a packet sniffer that monitors network traffic, closely inspecting each packet for a dangerous payload or suspicious anomalies.

Snort employs a set of rules that aid in the definition of harmful network behavior, searches for packets that meet these criteria, and alerts users. In order to intercept these packets, Snort is installed inline.

Snort's most significant advantage is its ability to detect and prevent network security threats. Snort provides an early warning system that prevents malicious attacks from spreading throughout the network and causing additional damage. It assesses computer resources and reports any anomalies or anomalous tendencies. It detects known signatures and attack signatures and alerts administrators to unknown risks. Snort can help keep the problem from spreading until administrators can address it.

Emilie Dionisio

Cybersecurity Phase 1 Final Project

2022-12-16

The pfSense software is a free, open-source customized distribution of FreeBSD designed for use as a firewall and router. In addition to being a powerful, flexible firewall and routing platform, it includes a long list of related features and a package system that allows further expansion without adding bloat and potential security vulnerabilities to the base distribution.

Here are some examples of list of packages that can be added to pfSense:

- Snort
- Suricata
- OpenVPN
- Nmap package
- AWS VPC Wizard
- pfBlockerNG

Resources:

Splunk: https://www.bitsioinc.com/install-splunk-ubuntu/
https://www.youtube.com/watch?v=EIagVwiJj60&t=2s

Suricata: https://suricata.io/documentation/ - download within Ubuntu Server or pfSense
Installation: https://suricata.readthedocs.io/en/latest/install.html - documentation
https://suricata.readthedocs.io/en/latest/quickstart.html

Video Installations: It’s included on PfSense video.
https://www.youtube.com/watch?v=UXKbh0jPPpg

Snort
https://www.snort.org - download within Ubuntu Server
Video Installations: https://www.youtube.com/watch?v=U6xMp-MIEfA

PfSense
https://www.pfsense.org
https://www.youtube.com/watch?v=Vm98ofYp05g

Video Installations:
https://www.youtube.com/watch?v=q4z_oDYIqUA
https://www.youtube.com/watch?v=TvQfD5oUN5o
https://www.youtube.com/watch?v=Vm98ofYp05g

Metasploitable
https://sourceforge.net/projects/metasploitable/
Video Installations:
https://www.youtube.com/watch?v=qSPT-YlIZAc
https://www.youtube.com/watch?v=errn34YrEjM

Kali
https://www.kali.org/docs/installation/hard-disk-install/

Ubuntu
https://ubuntu.com/download/desktop

Emilie Dionisio
Cybersecurity Phase 1 Final Project
2022-12-16

Summary:

Here's the list of the things that I experienced when creating the Cybersecurity Lab:

- **Difficulties:**
  - Because of the dependencies required to install Snort, I encountered some difficulties. Also, when I was updating the Ubuntu Server for Snort, there was a server issue that prevented me from connecting properly to the server, so I had to keep looking for ways to download the necessary dependencies for Snort but had no luck, so I simply installed and added a snort package in PfSense and I was able to add Snort.
  - When I first attempted to install Splunk, I ran into some problems. I had three different YouTube resources that I followed until the last video that Mr. G provided. I installed it successfully, but I also tried the link Ariana provided and reinstalled Splunk on another host machine, which only took about 10-15 minutes. That's why I mentioned it in class.
  - The majority of the issues that everyone, including myself, ran through involved the cluster's network adapter setup and communication between the host and virtual machines. When I connected the virtual machines to my network using various host computers, I finally understood. I made the decision to use Bridge and Host Only mode throughout so that each host and virtual machine have two IP Addresses and can communicate with one another except for establishing the clusters within the Nat-Network. I added a third adapter with that configuration and used Nat-Network and it finally worked for me.
  - The primary issue I encountered was time management, which I admit and am willing to change my mindset about it. I believe I took on too many responsibilities in my personal life and did not manage them well. I know what I need to work on now and am willing to change it.

- **Things that I discovered while creating the Lab:**
  - Network Adapters can be changed while virtual machines are running but will not be able to add adapters.
  - Virtual Box has a recorder within the virtual machine so when it's enabled, it's easy to go back to the previous settings. This is a good tool for troubleshooting the network settings and other things.
  - I was able to change the WAN and LAN IPs in PfSense by going to the console and following the steps.
  - Metasploitable virtual machine's IP Address can be previewed on a web interface by typing the IP Address of it.