ShibumiKat / **Portfolio_CyberSecurityMonashBootcamp** Private

generated from ShibumiKat/ShibumiKatTemplate

Code Issues Pull requests Actions Projects Security Insights Settings

master ▾ ···

Portfolio_CyberSecurityMonashBootcamp / 24-Final-Project / **Readme.md**

ShibumiKat Final Project Submitted

1 contributor

```
235 lines (164 sloc) | 9.9 KB
```

Unit 24: Final Project README

ITEM	DESCRIPTION
Name	Pieter Booysen
Date	30/05/2022
Title	Final Project Submission for Cyber Security Bootcamp

Unit Description

In this project, you will act as a security engineer supporting an organization's SOC infrastructure. The SOC analysts have noticed some discrepancies with alerting in the Kibana system and the manager has asked the security engineering team to investigate and confirm that newly created alerts are working.

If the alerts are working, you will then monitor live traffic on the wire to detect any abnormalities that aren't reflected in the alerting system. Then, you will report back your findings to the manager with appropriate analysis.

Deliverables

The following reports are submitted as a result of the investigation.

- Network Forensics Analysis Report

  Network Forensics: Use Wireshark to analyze live malicious traffic on the wire.

  You are working as a Security Engineer for X-CORP, supporting the SOC infrastructure. The SOC analysts have noticed some discrepancies with alerting in the Kibana system and the manager has asked the Security Engineering team to investigate.

  Yesterday, your team confirmed that newly created alerts are working. Today, you will monitor live traffic on the wire to detect any abnormalities that aren't reflected in the alerting system.

  You are to report back all your findings to both the SOC manager and the Engineering Manager with appropriate analysis.

  The Security team requested this analysis because they have evidence that people are misusing the network. Specifically, they've received tips about:

  - "Time thieves" spotted watching YouTube during work hours.
  - At least one Windows host infected with a virus.
  - Illegal downloads.

  A number of machines from foreign subnets are sending traffic to this network. Your task is to collect evidence confirming the Security team's intelligence.

- Red Team: Offensive Analysis Report

  Offensive Security: Assess a vulnerable VM and verify that the Kibana rules work as expected.

- Blue Team: Defensive Analysis Report

  Defensive Security: Implement alerts and thresholds

Lab Environment

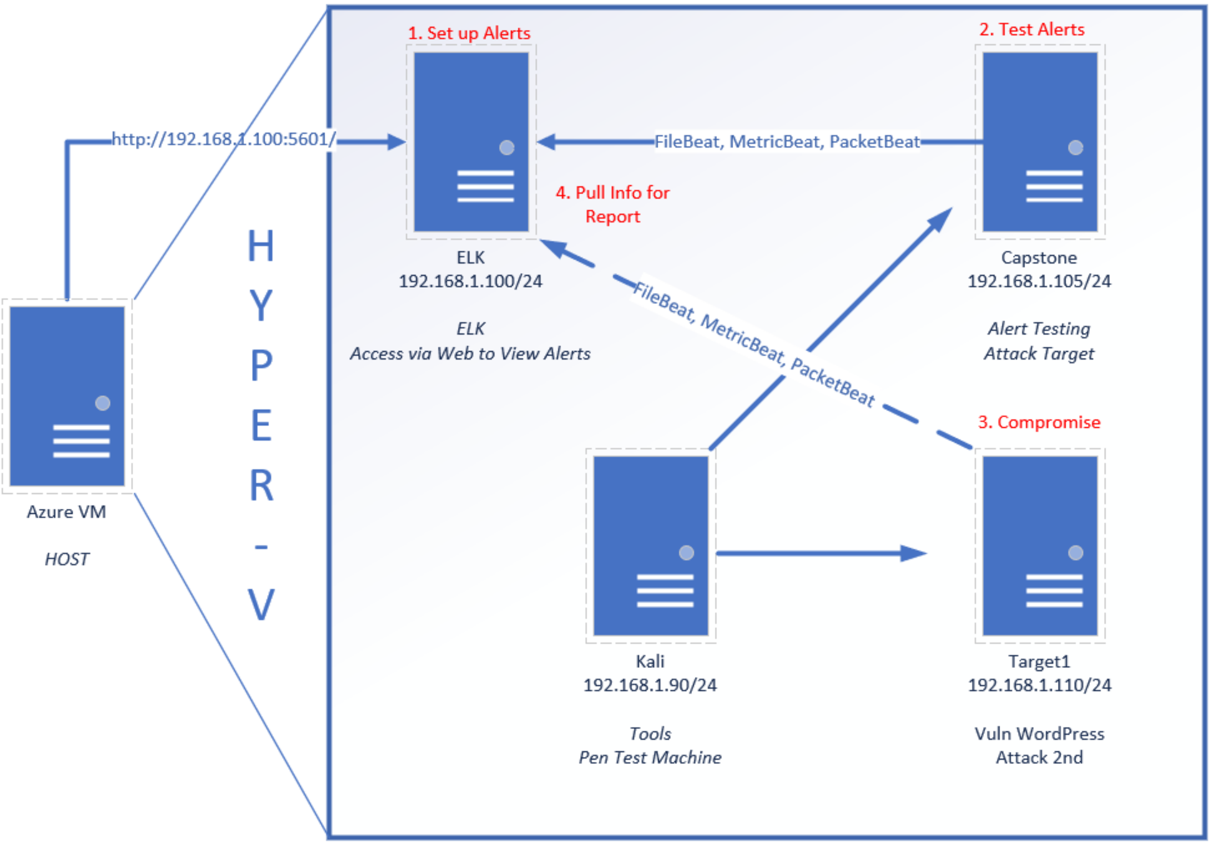
NOTE: PLEASE REFER TO THE OFFENSIVE OR DEFENSIVE ANALYSIS REPORTS FOR A MORE DETAILED NETWORK DIAGRAM

Web Vulns lab environment located in Windows Azure Lab Services. RDP into the **Windows RDP host machine** using the following credentials:

- Username: `azadmin`

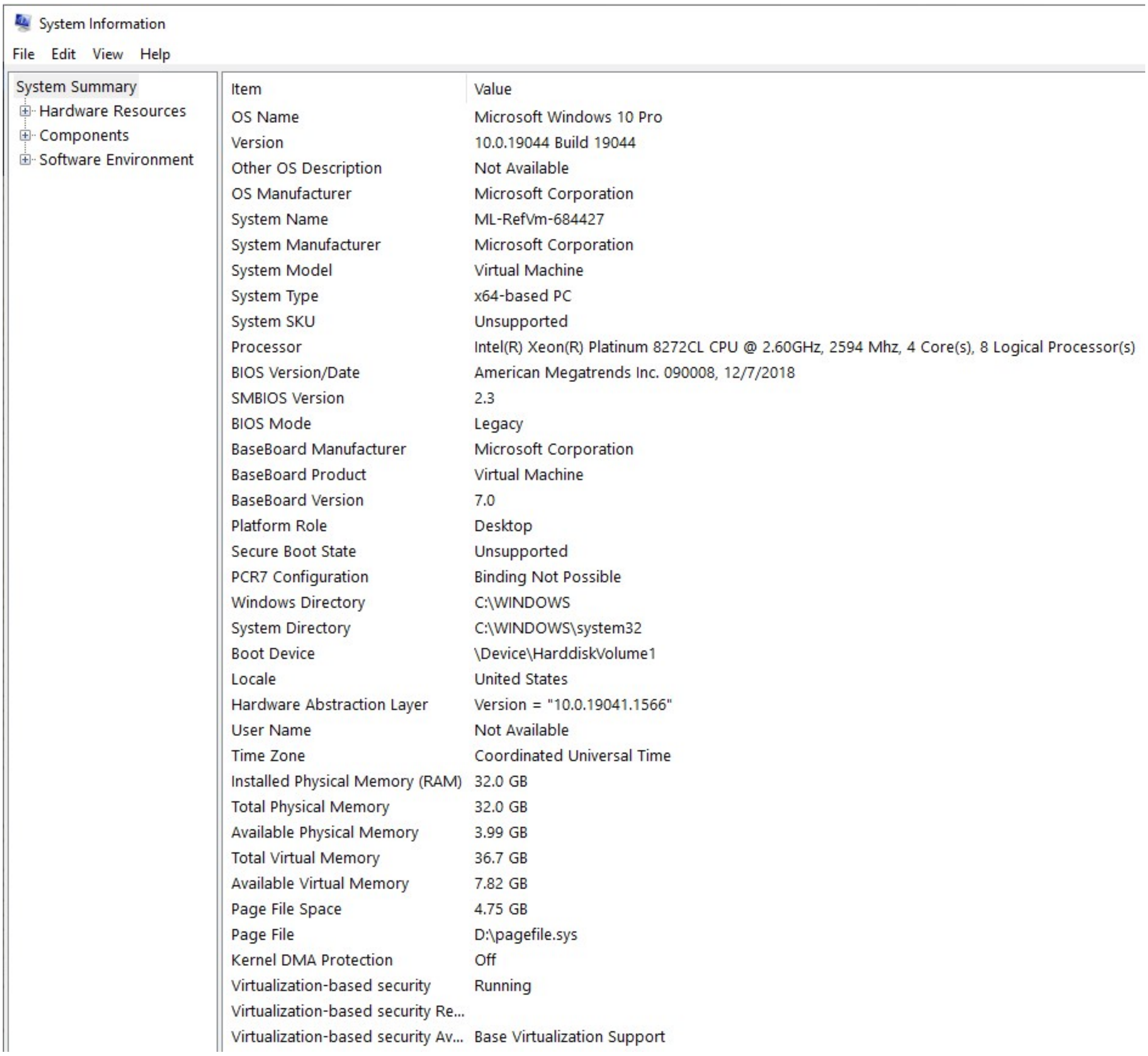
- Password: `p4ssw0rd*`

This is a diagram of the network and the machines that will be used in this lab:



Azure VM Host

Azure Host system information:



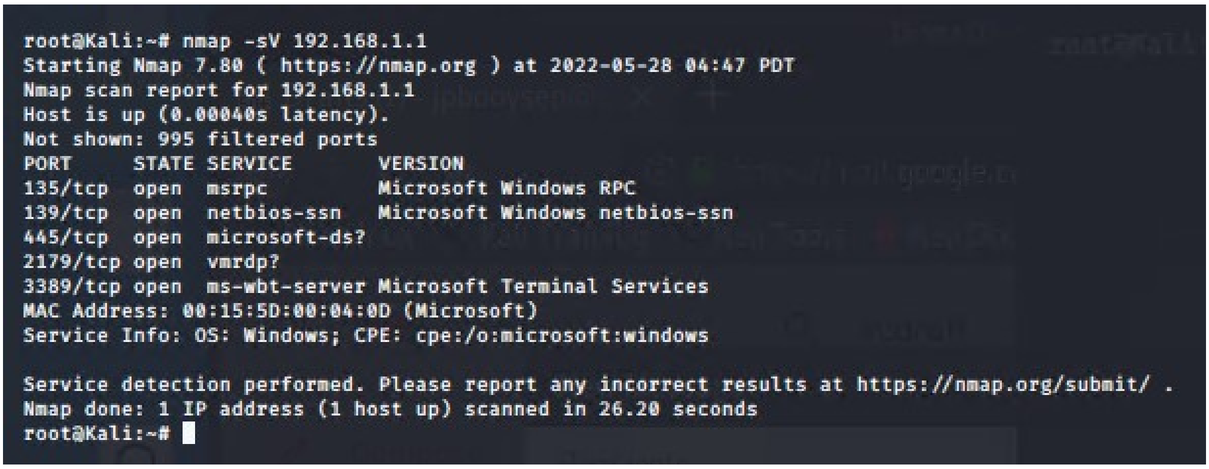
Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.19044 Build 19044
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	ML-RefVm-684427
System Manufacturer	Microsoft Corporation
System Model	Virtual Machine
System Type	x64-based PC
System SKU	Unsupported
Processor	Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz, 2594 Mhz, 4 Core(s), 8 Logical Processor(s)
BIOS Version/Date	American Megatrends Inc. 090008, 12/7/2018
SMBIOS Version	2.3
BIOS Mode	Legacy
BaseBoard Manufacturer	Microsoft Corporation
BaseBoard Product	Virtual Machine
BaseBoard Version	7.0
Platform Role	Desktop
Secure Boot State	Unsupported
PCR7 Configuration	Binding Not Possible
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "10.0.19041.1566"
User Name	Not Available
Time Zone	Coordinated Universal Time
Installed Physical Memory (RAM)	32.0 GB
Total Physical Memory	32.0 GB
Available Physical Memory	3.99 GB
Total Virtual Memory	36.7 GB
Available Virtual Memory	7.82 GB
Page File Space	4.75 GB
Page File	D:\pagefile.sys
Kernel DMA Protection	Off
Virtualization-based security	Running
Virtualization-based security Re...	
Virtualization-based security Av...	Base Virtualization Support

Key Network Information	Detail
Host Name . . . . :	ML-RefVm-684427
Ethernet adapter Ethernet 4:	
Description . . . . :	Microsoft Hyper-V Network Adapter #4
Physical Address. . . . . :	00-22-48-69-36-2E
Link-local IPv6 Address . . . . . :	fe80::4520:6fac:7ee:63a7%4(Preferred)
IPv4 Address. . . . . :	10.0.0.42(Preferred)
Subnet Mask . . . . :	255.255.240.0
Default Gateway . . . . :	10.0.0.1
DNS Servers . . . . :	168.63.129.16
Ethernet adapter vEthernet (NATSwitch):	

Key Network Information	Detail
Description . . . . :	Hyper-V Virtual Ethernet Adapter #2
Physical Address. . . . . :	00-15-5D-00-04-0D
Link-local IPv6 Address . . . . . :	fe80::90ca:742e:54ed:7bb7%13(Preferred)
IPv4 Address. . . . . :	192.168.1.1(Preferred)
Subnet Mask . . . . :	255.255.255.0
Ethernet adapter vEthernet (Default Switch):	
Description . . . . :	Hyper-V Virtual Ethernet Adapter
Physical Address. . . . . :	00-15-5D-DD-68-20
Link-local IPv6 Address . . . . . :	fe80::a96e:b358:4547:4917%14(Preferred)
IPv4 Address. . . . . :	172.17.16.1(Preferred)
Subnet Mask . . . . :	255.255.240.0

Service Information	Detail		
Command	nmap -sV 192.168.1.1		
PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
2179/tcp	open	vmrdp?	
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services

Service Information	Detail		
MAC Address:	00:15:5D:00:04:0D	(Microsoft)	
Service Info:	OS: Windows;	CPE: cpe:/o:microsoft:windows	



```
root@Kali:~# nmap -sV 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-28 04:47 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00040s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.20 seconds
root@Kali:~# 
```

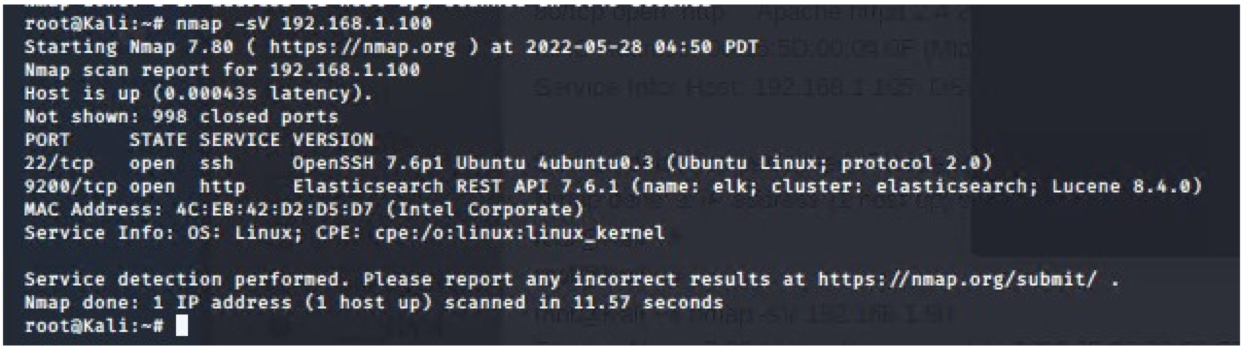
Open the Hyper-V Manager to access the nested machines:

ELK machine credentials: The same ELK setup that you created in Project 1. It holds the Kibana dashboards.

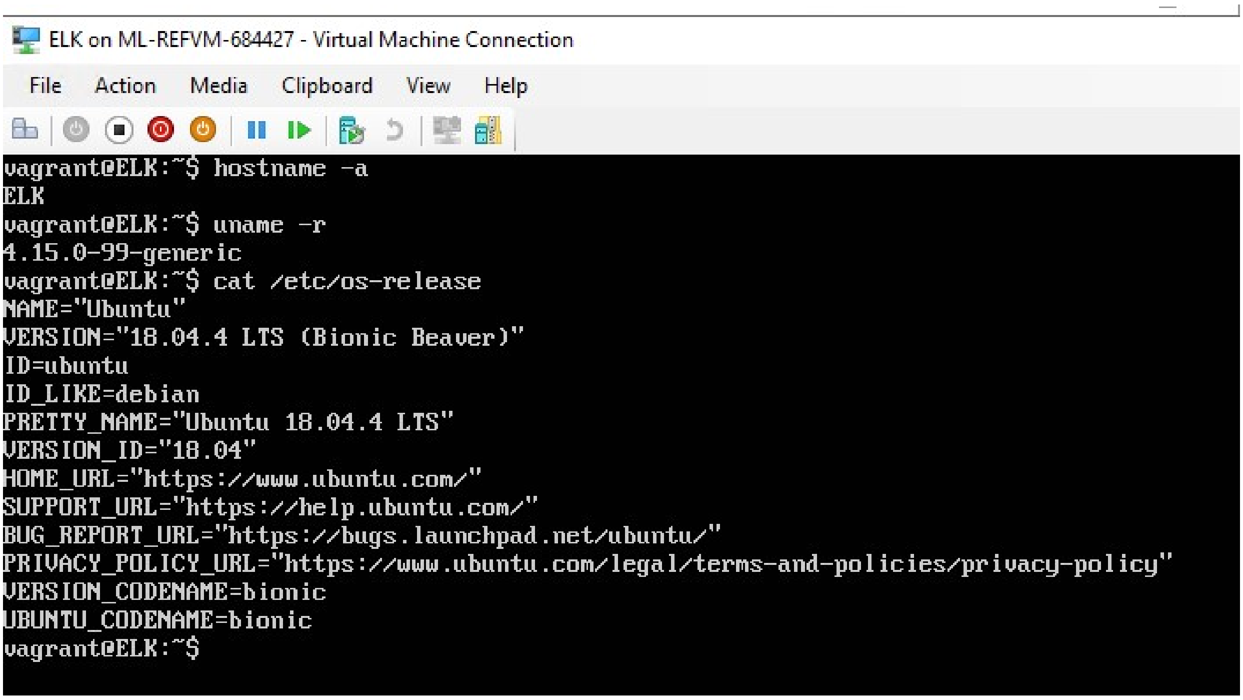
- Username: `vagrant`
- Password: `vagrant`
- IP Address: `192.168.1.100`

Service Information	Detail		
Command	nmap -sV 192.168.1.100		
PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

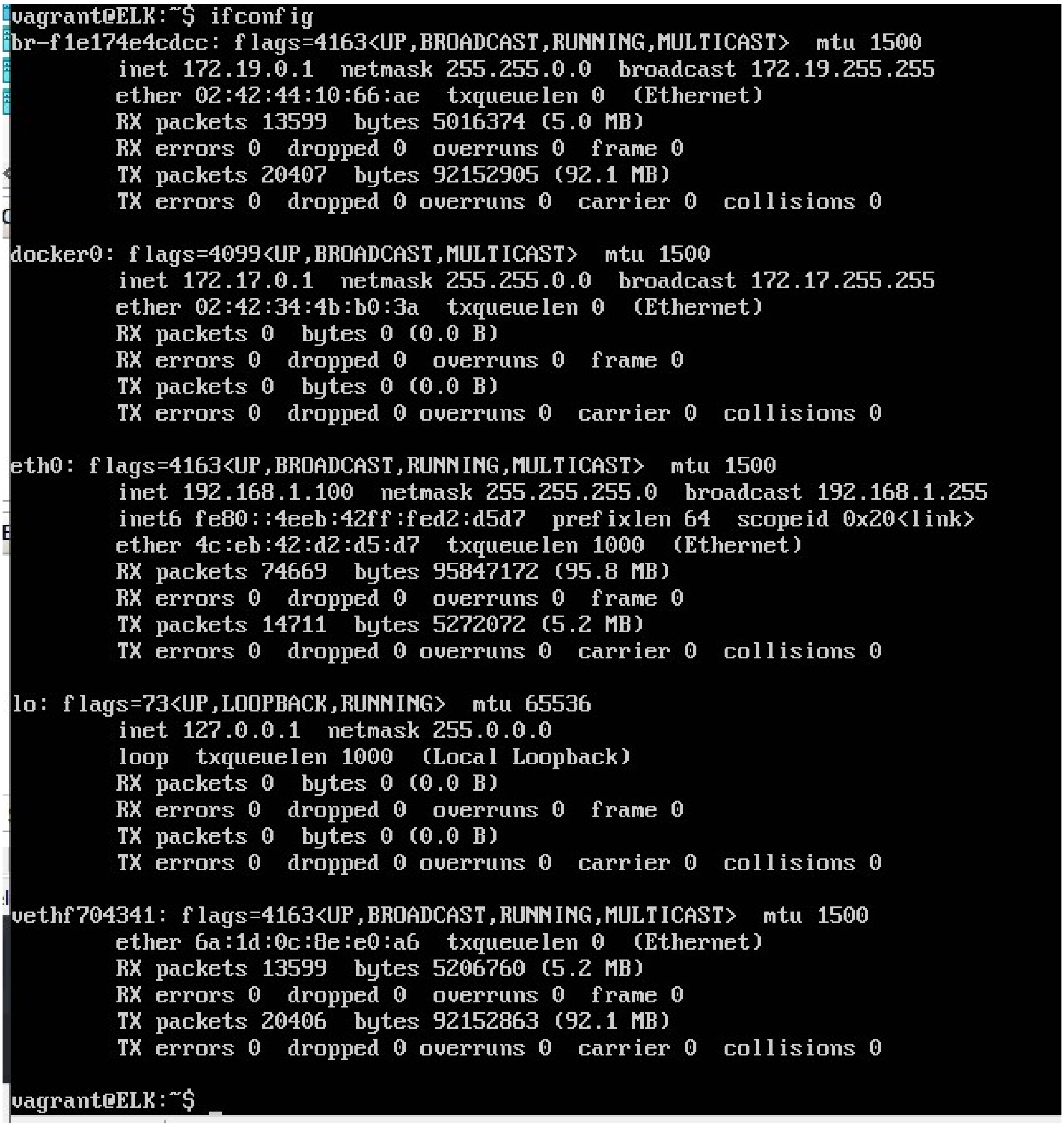
Service Information	Detail		
9200/tcp	open	http	Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address:	4C:EB:42:D2:D5:D7	(Intel Corporate)	
Service Info:	OS: Linux;	CPE: cpe:/o:linux:linux_kernel	



```
root@Kali:~# nmap -sV 192.168.1.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-28 04:50 PDT
Nmap scan report for 192.168.1.100
Host is up (0.00043s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.57 seconds
root@Kali:~# 
```



```
vagrant@ELK:~$ hostname -a
ELK
vagrant@ELK:~$ uname -r
4.15.0-99-generic
vagrant@ELK:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="18.04.4 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.4 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
vagrant@ELK:~$
```



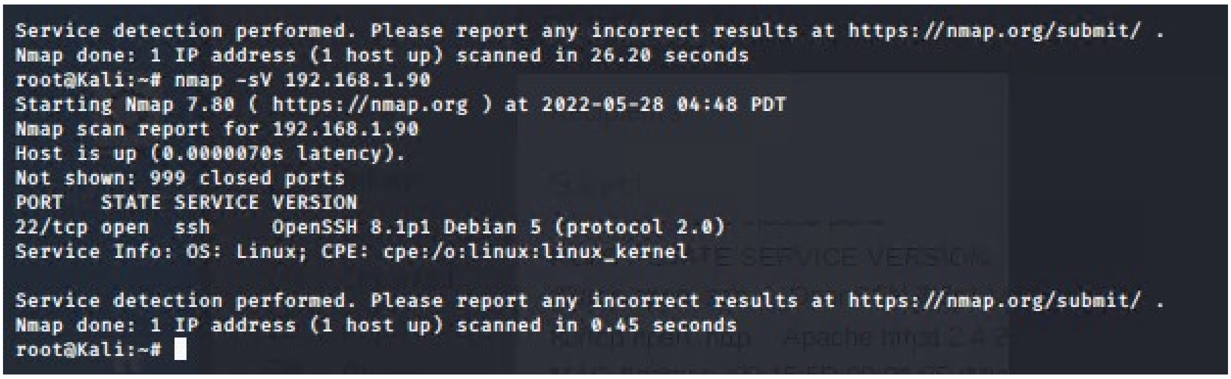
```
vagrant@ELK:~$ ifconfig
br-f1e174e4cdcc: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.19.0.1  netmask 255.255.0.0  broadcast 172.19.255.255
        ether 02:42:44:10:66:ae  txqueuelen 0  (Ethernet)
        RX packets 13599  bytes 5016374 (5.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20407  bytes 92152905 (92.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:34:4b:b0:3a  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::4eeb:42ff:fed2:d5d7  prefixlen 64  scopeid 0x20<link>
        ether 4c:eb:42:d2:d5:d7  txqueuelen 1000  (Ethernet)
        RX packets 74669  bytes 95847172 (95.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14711  bytes 5272072 (5.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vethf704341: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 6a:1d:0c:8e:e0:a6  txqueuelen 0  (Ethernet)
        RX packets 13599  bytes 5206760 (5.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20406  bytes 92152863 (92.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vagrant@ELK:~$ _
```

Kali: A standard Kali Linux machine for use in the penetration tests.

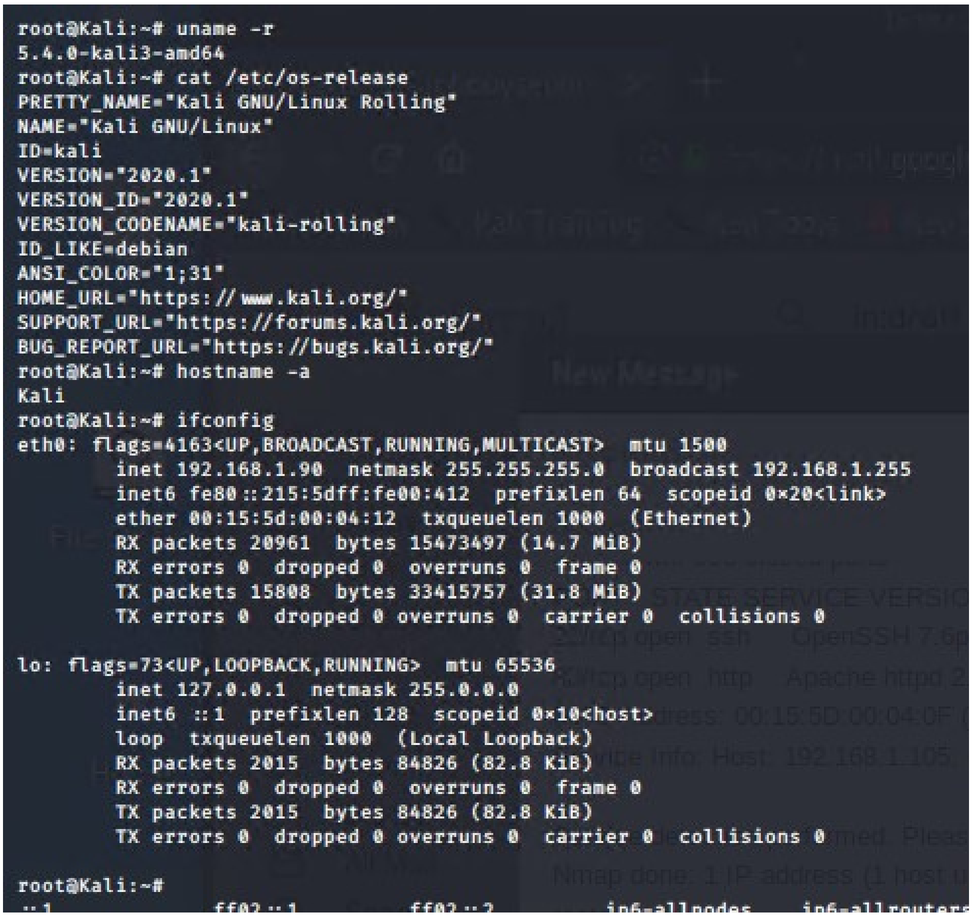
- Username: `root`
- Password: `toor`
- IP Address: `192.168.1.90`

Service Information	Detail		
Command	nmap -sV 192.168.1.90		
PORT	STATE	SERVICE	VERSION

Service Information	Detail		
22/tcp	open	ssh	OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info:	OS: Linux;	CPE: cpe:/o:linux:linux_kernel	



```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.20 seconds
root@Kali:~# nmap -sV 192.168.1.90
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-28 04:48 PDT
Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
root@Kali:~# █
```



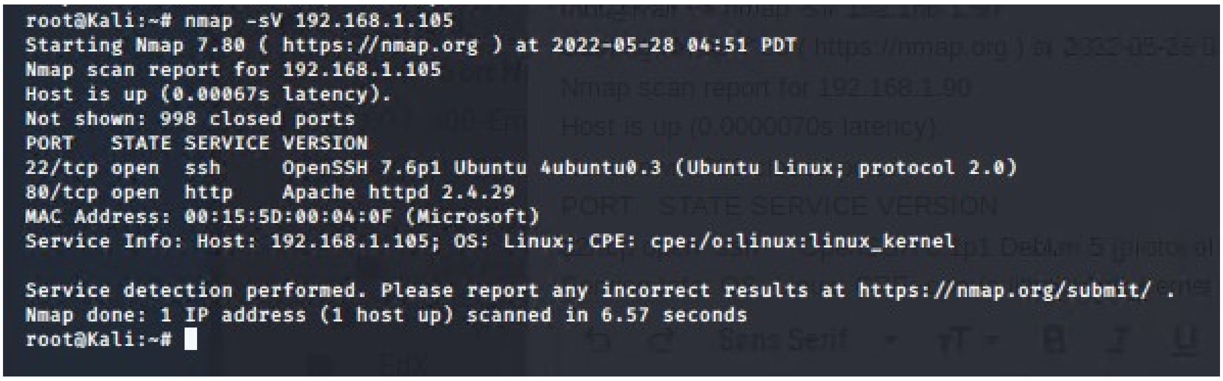
```
root@Kali:~# uname -r
5.4.0-kali3-amd64
root@Kali:~# cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2020.1"
VERSION_ID="2020.1"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
root@Kali:~# hostname -a
Kali
root@Kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.90  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:412  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
        RX packets 20961  bytes 15473497 (14.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15808  bytes 33415757 (31.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2015  bytes 84826 (82.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2015  bytes 84826 (82.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Kali:~#
::1            ff02::1          ff02::2          ip6-allnodes     ip6-allrouters
```

Capstone: Filebeat and Metricbeat are installed and will forward logs to the ELK machine.

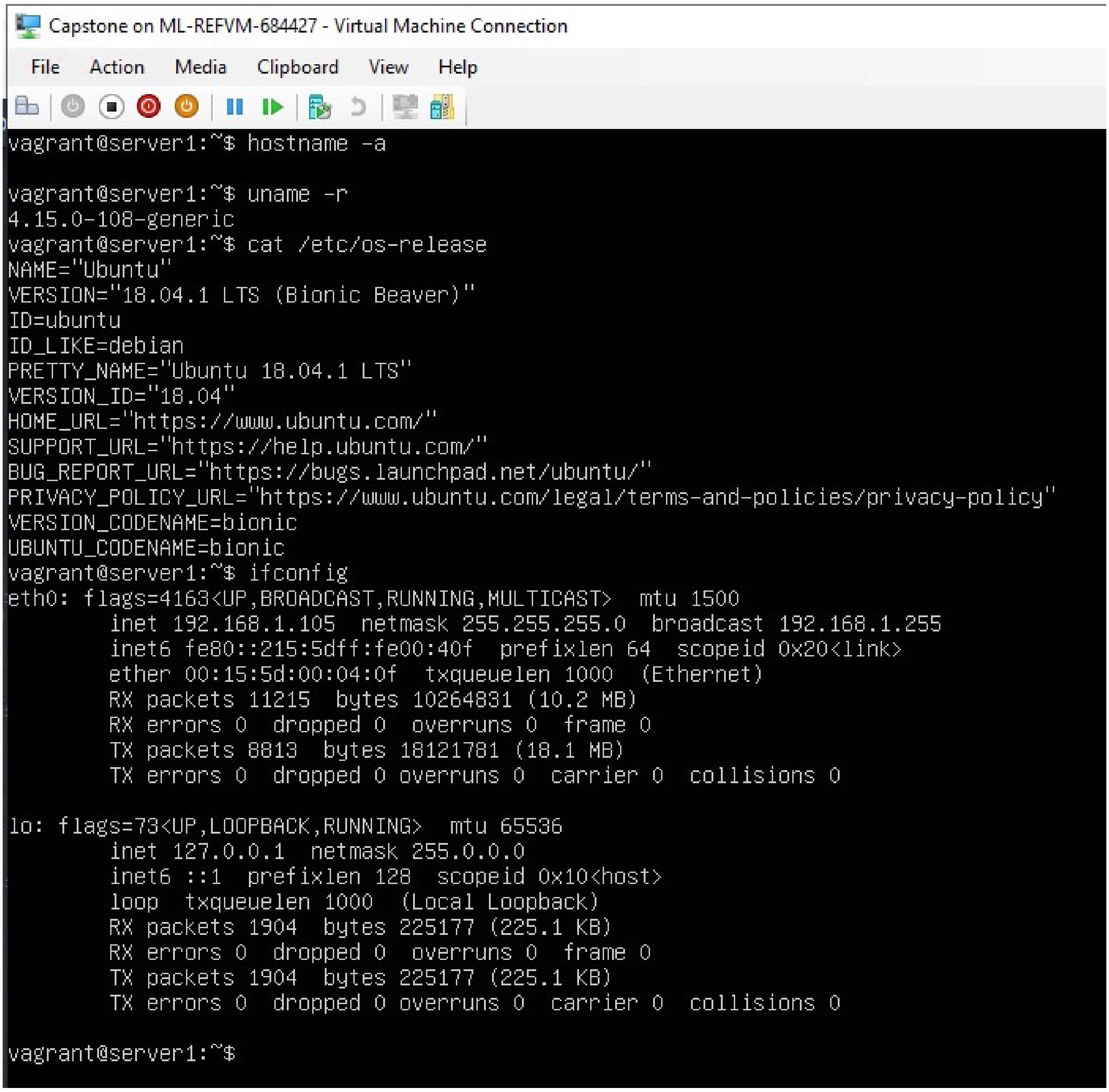
- IP Address: `192.168.1.105`

- Please note that this VM is in the network solely for the purpose of testing alerts.

Service Information	Detail		
Command	nmap -sV 192.168.1.105		
PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp	open	http	Apache httpd 2.4.29
MAC Address:	00:15:5D:00:04:0F	(Microsoft)	
Service Info:	Host: 192.168.1.105;	OS: Linux;	CPE: cpe:/o:linux:linux_kernel



```
root@Kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-28 04:51 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00067s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.57 seconds
root@Kali:~#
```


Capstone on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help

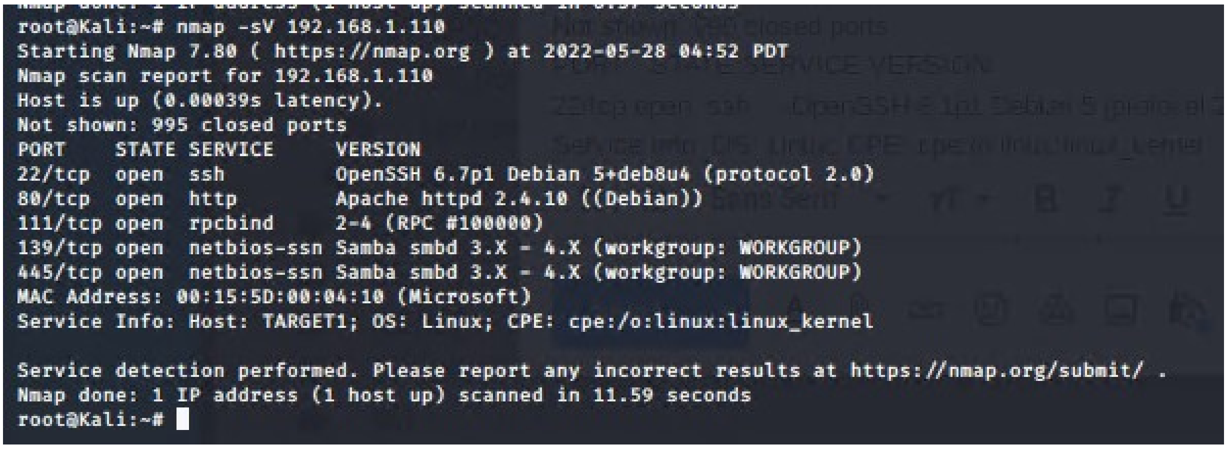
```
vagrant@server1:~$ hostname -a

vagrant@server1:~$ uname -r
4.15.0-108-generic
vagrant@server1:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="18.04.1 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.1 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
vagrant@server1:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.105  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:40f  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:0f  txqueuelen 1000  (Ethernet)
        RX packets 11215  bytes 10264831 (10.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8813  bytes 18121781 (18.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1904  bytes 225177 (225.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1904  bytes 225177 (225.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vagrant@server1:~$
```

Target 1: Exposes a vulnerable WordPress server.

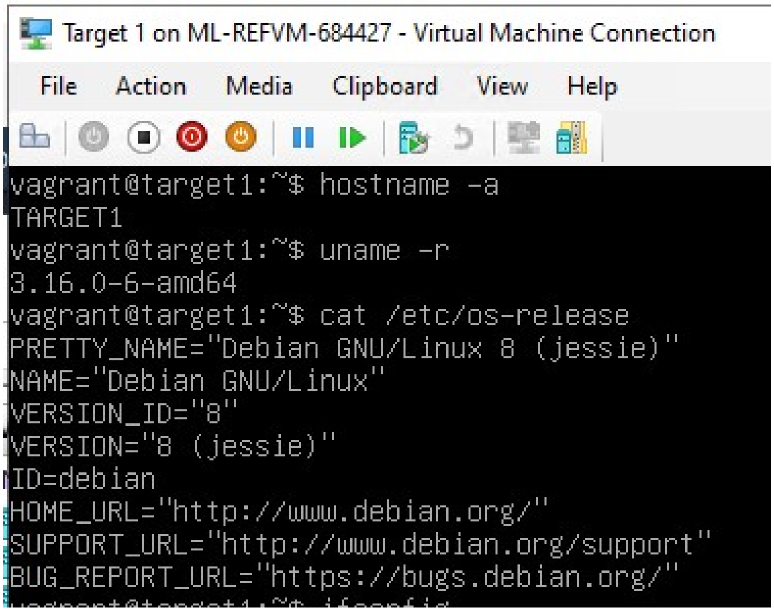
- IP Address: `192.168.1.110`

Service Information	Detail		
Command	nmap -sV 192.168.1.110		
PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp	open	http	Apache httpd 2.4.10 ((Debian))
111/tcp	open	rpcbind	2-4 (RPC #100000)

Service Information	Detail		
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address:	00:15:5D:00:04:10	(Microsoft)	
Service Info:	Host: TARGET1;	OS: Linux;	CPE: cpe:/o:linux:linux_kernel



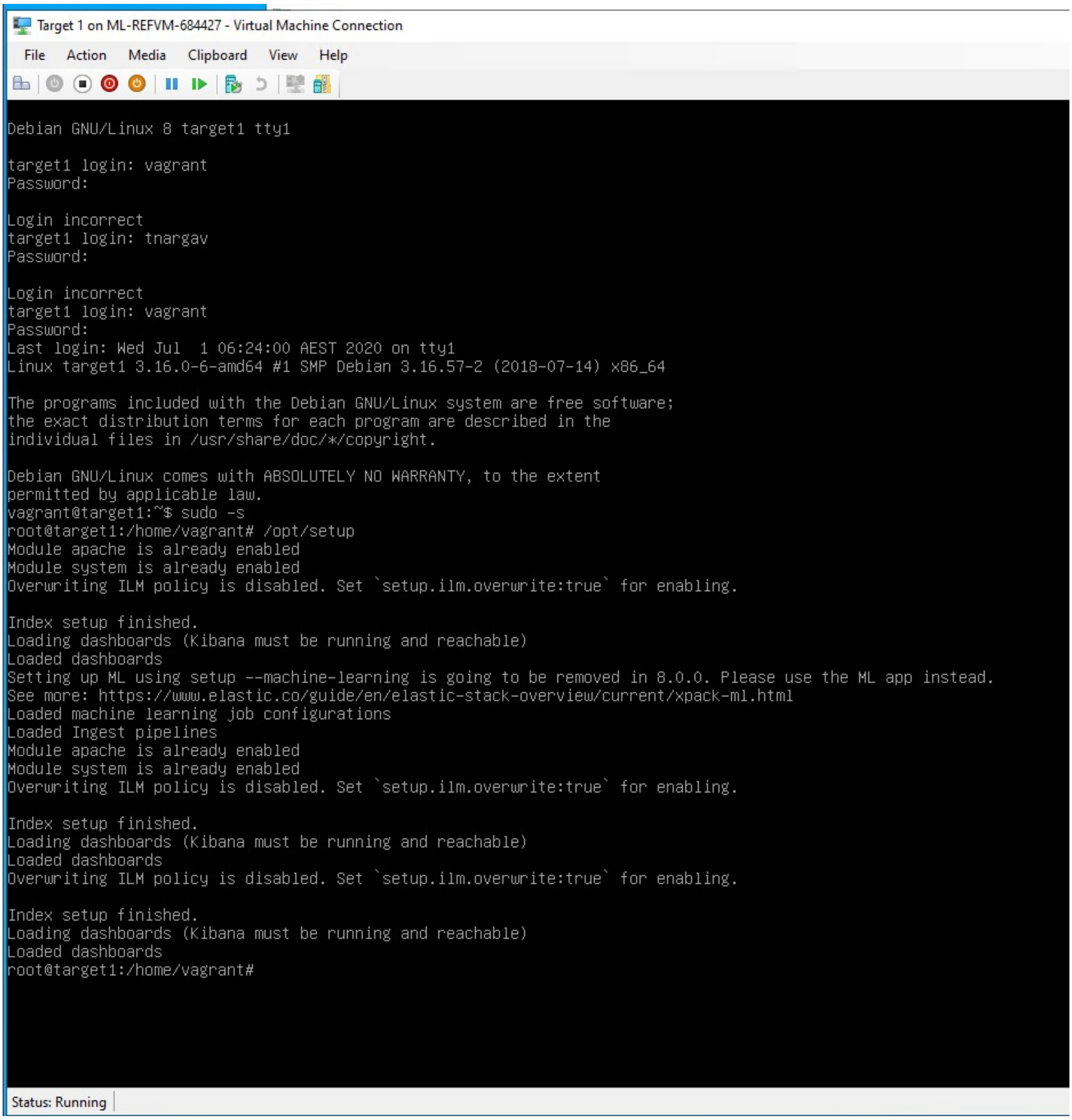
```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-28 04:52 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00039s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.59 seconds
root@Kali:~#
```



```
vagrant@target1:~$ hostname -a
TARGET1
vagrant@target1:~$ uname -r
3.16.0-6-amd64
vagrant@target1:~$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 8 (jessie)"
NAME="Debian GNU/Linux"
VERSION_ID="8"
VERSION="8 (jessie)"
ID=debian
HOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
vagrant@target1:~$ ifconfig
```

Setting up the Kibana requires a few commands:

- Escalate to root `sudo -s`
- Setup up Apache and Kibana (Filebeat, Metricbeat, and Packetbeat) and system dashboards with a provided script `/opt/setup`



Target 1 on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running

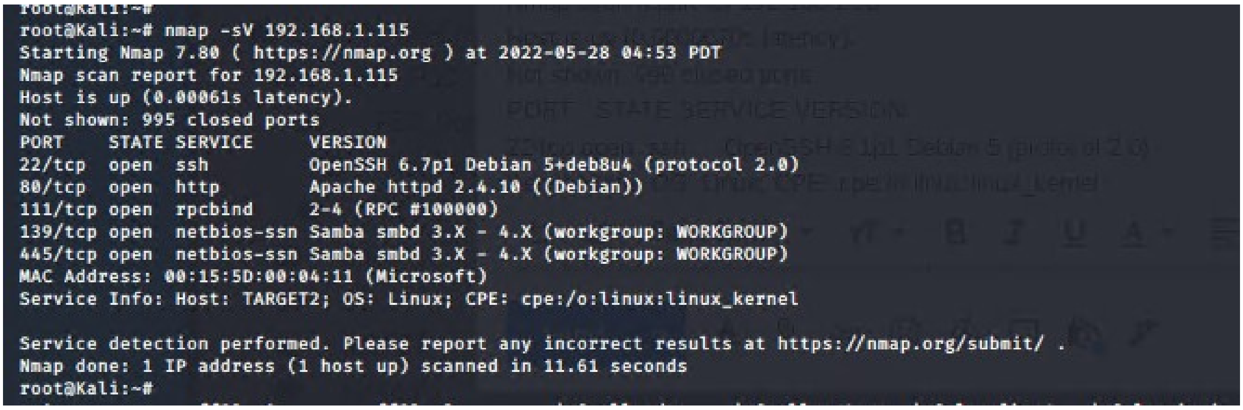
```
Debian GNU/Linux 8 target1 tty1

target1 login: vagrant
Password:

Login incorrect
target1 login: tnargav
Password:

Login incorrect
target1 login: vagrant
Password:
Last login: Wed Jul  1 06:24:00 AEST 2020 on tty1
Linux target1 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
vagrant@target1:~$ sudo -s
root@target1:/home/vagrant# /opt/setup
Module apache is already enabled
Module system is already enabled
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Setting up ML using setup --machine-learning is going to be removed in 8.0.0. Please use the ML app instead.
See more: https://www.elastic.co/guide/en/elastic-stack-overview/current/xpack-ml.html
Loaded machine learning job configurations
Loaded Ingest pipelines
Module apache is already enabled
Module system is already enabled
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
root@target1:/home/vagrant#
```

Target 2: A `bonus` target machine. A more difficult WordPress target. Sends logs to ELK.

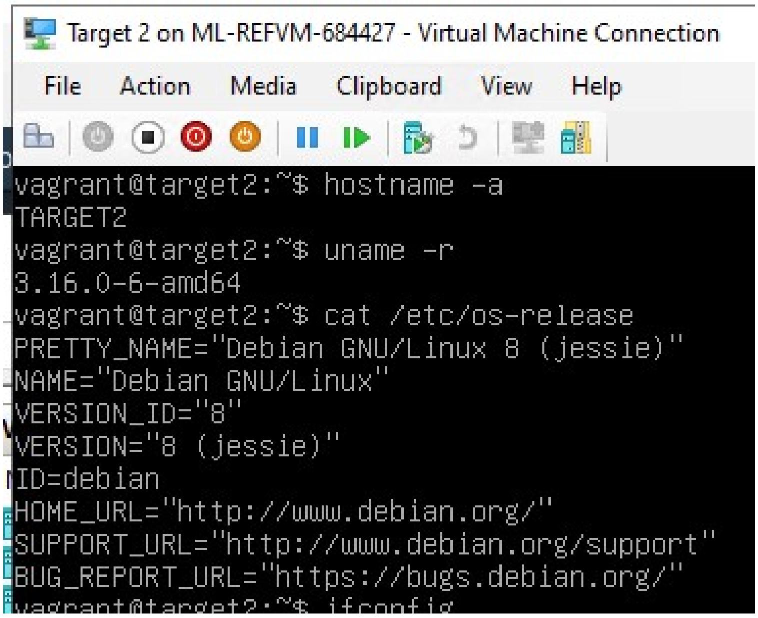
- IP Address: `192.168.1.115`

Service Information	Detail		
Command	nmap -sV 192.168.1.115		
PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)

Service Information	Detail		
80/tcp	open	http	Apache httpd 2.4.10 ((Debian))
111/tcp	open	rpcbind	2-4 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address:	00:15:5D:00:04:11	(Microsoft)	
Service Info:	Host: TARGET2;	OS: Linux;	CPE: cpe:/o:linux:linux_kernel



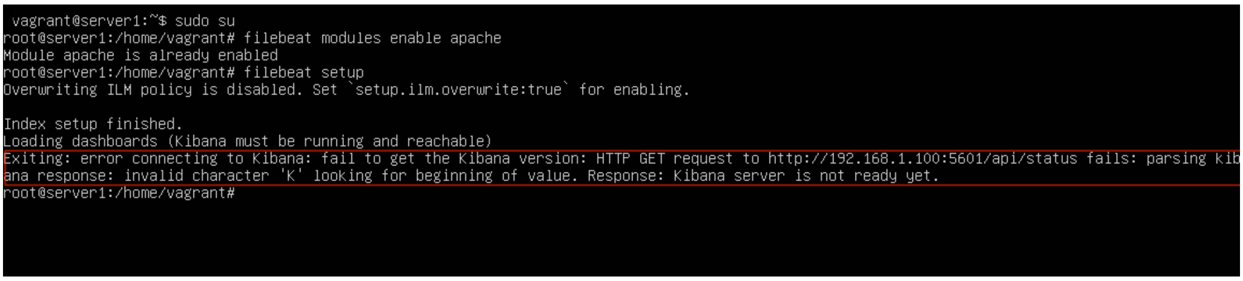
```
root@Kali:~#
root@Kali:~# nmap -sV 192.168.1.115
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-28 04:53 PDT
Nmap scan report for 192.168.1.115
Host is up (0.00061s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.61 seconds
root@Kali:~#
```



```
vagrant@target2:~$ hostname -a
TARGET2
vagrant@target2:~$ uname -r
3.16.0-6-amd64
vagrant@target2:~$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 8 (jessie)"
NAME="Debian GNU/Linux"
VERSION_ID="8"
VERSION="8 (jessie)"
ID=debian
HOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
vagrant@target2:~$ ifconfig
```

What to Be Aware Of during the setup process

It is common to encounter to experience the following issue:



```
 vagrant@server1:~$ sudo su
root@server1:/home/vagrant# filebeat modules enable apache
Module apache is already enabled
root@server1:/home/vagrant# filebeat setup
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Exiting: error connecting to Kibana: fail to get the Kibana version: HTTP GET request to http://192.168.1.100:5601/api/status fails: parsing kib
ana response: invalid character 'K' looking for beginning of value. Response: Kibana server is not ready yet.
root@server1:/home/vagrant#
```

- If students encounter this error, explain that Kibana needs time to finish setting up. They should wait five to ten minutes and then try again.

- If the issue is still not resolved, ask to students to log into the ELK machine using the machines credentials and run the following commands:

  - `sudo su` which will allow the student to become the root user.
  - `docker container ls` to find the name of the running docker container.
  - `docker container stop <container-name>` which will stop the docker container.
  - `docker container start <container-name>` which will start the docker container back up.

- When setting alerts in Kibana to send log messages, those messages will not show in Kibana without additional configuration. Instead, the status of alerts can be viewed from the 'Watcher' page where the alerts are created.

Additional Reading and Resources

These resources are provided as optional, recommended resources to supplement the concepts covered in this unit.

- SANS Pentesting Cheatsheet

Reference Sheets

Collection of useful reference sheets.

1. cURL Reference Sheet
2. HTTP Reference Sheet