



# LAB BOOK PORTFOLIO #2

## Advanced Computer Security

Date: 2022-03-12

Lab Book Portfolio #2 | Advanced Computer Security | Course Code: INFO2231

Sunraj Sharma  
Sunraj751@gmail.com

## Table of Contents

Table of Contents .....	1
Lab 3 - PFSense and Intrusion Prevention and Detection .....	2
Part 1 .....	2
Description.....	2
Preparation .....	2
Observations .....	2
Screenshots.....	3
Reflection.....	5
Lab 4 – Enumeration with NMap.....	7
Part 1 .....	7
Description.....	7
Preparation .....	7
Observations .....	7
Screenshots.....	7
Reflection.....	9
Lab 5 – Enumeration with enum4linux.....	10
Part 1 .....	10
Description.....	10
Preparation .....	10
Observations .....	10
Screenshots.....	10
Reflection.....	11
References .....	11

## Lab 3 - PFSense and Intrusion Prevention and Detection

### Part 1

#### Description

For this lab (PFSense and Intrusion Prevention and Detection), the purpose of the lab is to use the Suricata intrusion detection and prevention tool, explore the tool, and ensure that it is properly installed on PFSense. This lab will set up and enable a ruleset for the Suricata tool and explore triggering it.

#### Preparation

For this lab surrounding the Suricata tool, the preparation that was done for the lab was following the lecture and instructions on how to properly setup and install the Suricata intrusion detection and prevention tool on PFSense, and ensure that PFSense in general is in working order and that there were no issues beforehand regarding either of those things before attempting to begin the lab.

#### Observations

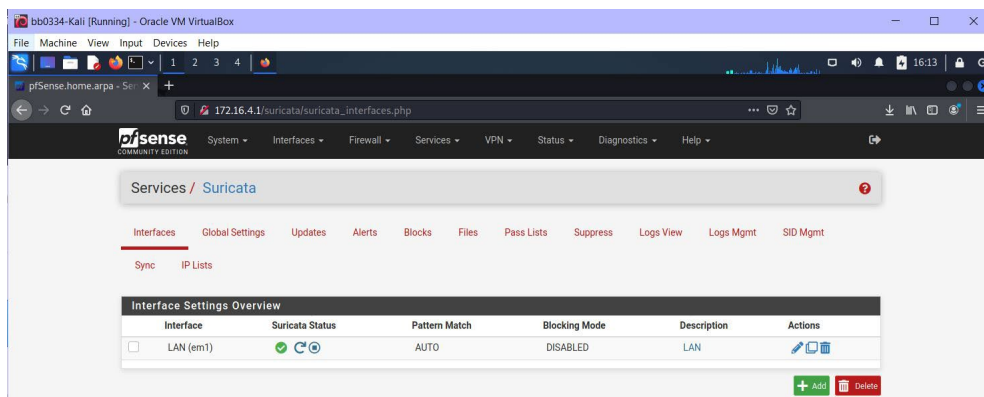
1. As per the first task, I ensured that all of the virtual machines were named correctly with the given naming convention (mine being bb0334 followed by the VM name).
2. I went into PFSense home on Kali Linux and ensured that the setup for Suricata was properly setup. I then pressed the play button to start running the configured Suricata device under the "interfaces" section as described in task 2. It started running after that was complete.
3. Went into the "Suricata -> Global Settings" section and checked if both the required rules (ETOpen Emerging Threat rules and Install Snort GPLv2 Community rules) were selected. They were already selected.
4. Went into the "Suricata -> Updates" section and pressed the "force" button to force update for the ruleset.
5. Went into the LAN interface settings -> LAN Categories and enabled the specified rule in task 6. Saved the changes made to the rules.
6. Ran the command "curl -A 'BlackSun' [www.google.ca](http://www.google.ca)" from the terminal. When the command was ran, lots of information was printed onto the terminal, but I am not exactly sure what it all represents.
7. Went into the Suricata -> Alerts section and checked if an alert was present. At first there wasn't an alert, but after checking the configurations and running the command a couple more times and cloning the Suricata instance then running the cloned version, the alert did appear in the alerts section.

## Screenshots

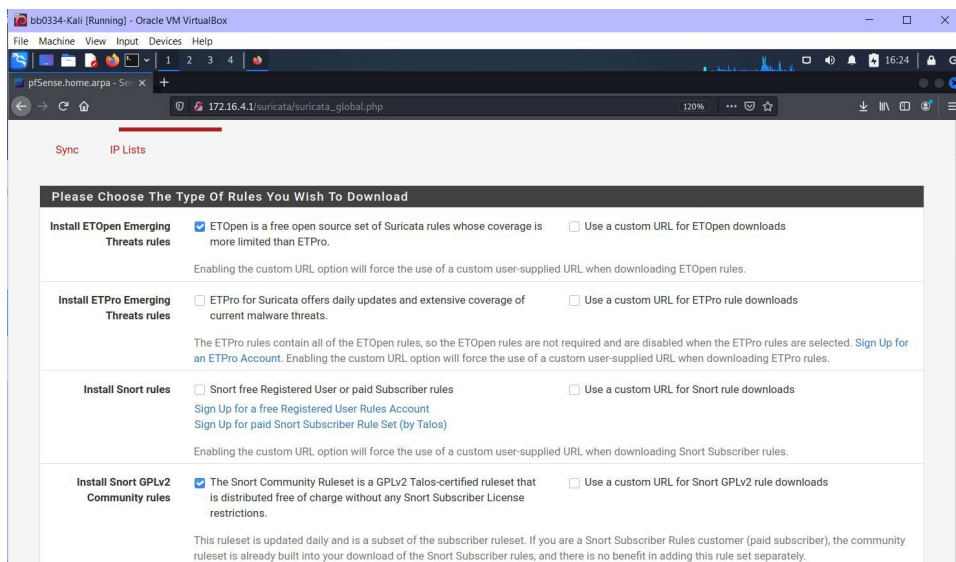
1. **Task #1** Ensuring virtual machines are named correctly.



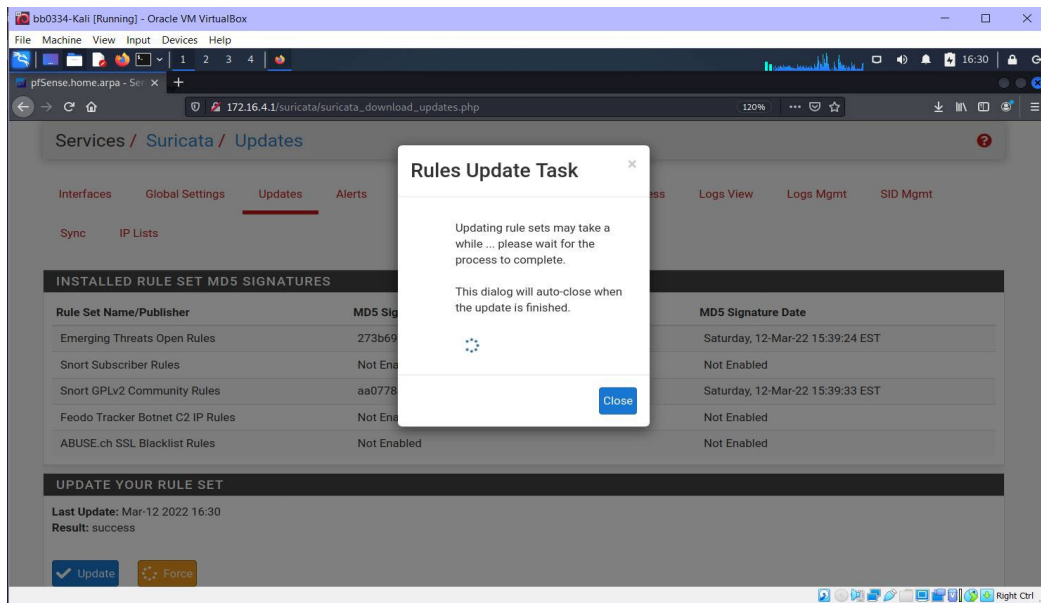
2. **Task #2** Suricata running.



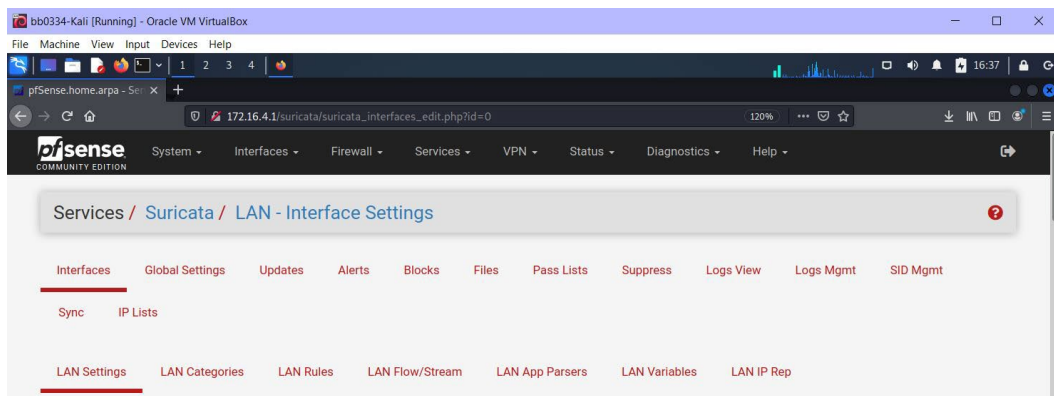
3. **Task #3** Ensuring that ETOpen Emerging Threat Rules and Install Snort GPLv2 Community Rules are selected.



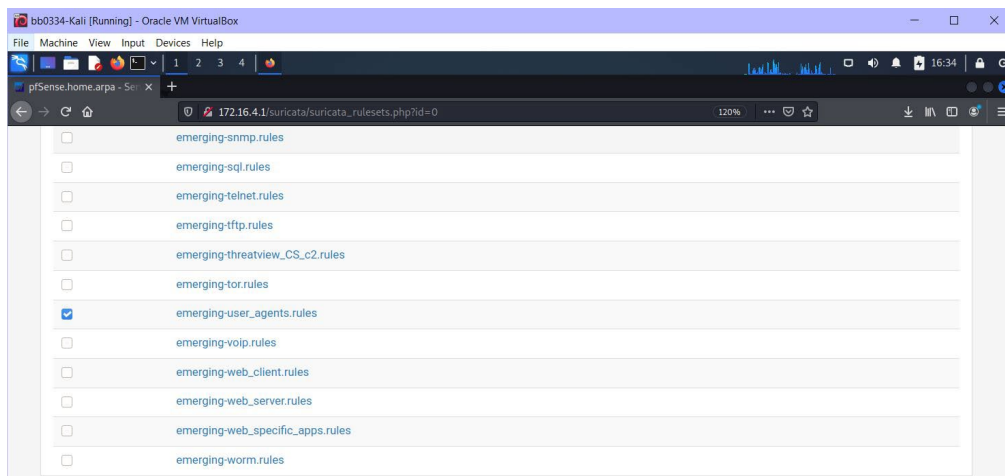
4. **Task #4** Forcing update for the ruleset.



##### 5. Task #5 In Suricata LAN interface settings.



##### 6. Task #6 Enabling the "emerging-user\_agents.rules".



## 7. Task #7 Running the `curl -A "BlackSun" www.google.ca` command.

```

(kali@kali)-[~]
$ curl -A "BlackSun" www.google.ca
<doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="
en-CA"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Typ
e"><meta content="/images/branding/google/1x/google_standard_color_128dp.pn
g" itemprop="image"><title>Google</title><script nonce="4kFKU88DH-aTq3/bQhql
w">(function(){window.google={kEI:'PykYvPKJ5HbtAb28q2YAAQ',kEXP1:'0,18167,1
284369,56873,6058,207,4804,2316,383,246,5,1354,4013,1238,1122515,1197707,716,
302539,77528,16115,19397,9287,17572,4859,1361,9290,3021,17588,4020,978,13228,
3847,4192,6430,22741,1832,3249,1593,1279,2742,149,1103,840,1030,953,4314,108,
3406,606,2023,1777,520,14670,3229,2843,7,4811,788,11851,8101,8219,1850,2615,3
784,9358,3,576,1014,1,5444,149,11323,2652,4,1528,2304,7039,20309,4764,2658,73
55,32,19065,0358,7428,5797,2500,4094,4052,3,3541,1,11374,5433,38,25309,2,1402
2,1931,784,255,4550,743,5853,10463,1160,5679,1020,2381,2718,8596,9647,2,6,1,7
771,2125,2443,6256,6720,16700,1253,4570,2,6,1,1256,12200,2767,1539,2794,2071,
2606,1412,1395,445,2,2,1,923,462,686,5,4318,6692,4235,6428,34,843,152,1407,10
,1,436,8155,113,2453,3071,945,798,1,2,460,2,1985,593,1840,1711,3878,466,721,1
156,847,83,186,750,434,574,879,3363,907,1184,14,444,1151,4,591,1082,2785,2,1,
810,1151,1161,2861,283,612,321,1295,408,2,1168,238,541,359,1327,483,651,361,1
79,41,310,468,30,171,900,588,511,53,3621,27,2,750,34,912,232,3466682,930,268,3
9,5995557,797,2799897,1323,882,444,3,1877,1,2562,1,748,141,795,563,1,4265,1,1
,2,1331,4142,2609,155,17,13,72,139,4,2,20,2,169,13,19,46,5,39,96,548,29,2,2,1
,2,1,2,2,7,4,1,2,2,2,2,2,353,513,186,1,1,158,3,2,2,2,2,2,4,2,3,269,1601,1
41,576,426,80,1,14,81,2,23951800,4038575,3,3112,3,450,1964,1491,9,1435,159,13
58,1130,3596,3,955,3,1704,2,1797,101,1434,1993,3,29,418',kBL:'skq8'};google.s
n="webhp";google.kHL="en-CA");})();(function(){
var f=this||self;var h,k=[];function l(a){for(var b;a&&!(a.getAttribute||!(b=
a.getAttribute("eid"))));a=a.parentNode;return b||function m(a){for(var b=n
ull;a&&!(a.getAttribute||!(b=a.getAttribute("leid"))));a=a.parentNode;return
b}
function n(a,b,c,d,g){var e="";c||=1===b.search("6ei=")||(e="6ei="+l(d),-1===
b.search("6ei=")?66(d=m(d))66(e+"6ei="+d)):d="";!c66f._cshid66-1===b.search
("6cshid=")?66("6cshid="+f._cshid):c=c||"/"+(g||"gen_204")+?atyp

```

## 8. Task #8 Checking if an alert is visible.

Alert Log View Settings

Instance to View: (LAN) LAN

Save or Remove Logs: Download, Clear

Save Settings: Save, Refresh

Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
03/12/2022 18:14:07	⚠	1	TCP	A Network Trojan was detected	172.16.4.11	43546	142.251.41.67	80	1:2008983	ET USER_AGENTS Suspicious User Agent (BlackSun)

## Reflection

- 1) While attempting this lab there were a handful of issues I did run into. I was stuck a on a problem relating to running the Suricata instance. It seemed that every time I tried to

start it, the wheel would spin and shut off again. After reading the suricata log, It stated that there was something going on with the .pid file and to delete it, but oddly enough I could not find the .pid file, or the suricata log file in the /var/log/suricata/ directory, or the var/run/ directories. They somehow did not even exist. I managed to fix the issue by cloning the suricata instance and running the cloned version.

- 2) In order to check for user agents with another rule besides emerging-user\_agents.rules, I decided to enable the rule emerging-attack\_response.rules since when clicking on the rule various “user agent” could be found inside of the code, so the assumption was that this rule would as well target user agents. I tested the emerging-attack\_response rule by running the command `curl http://testmynids.org/uid/index.html` . The screenshots show the command being ran twice, and the two alerts that show up.

```

bb0334-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
(kali@kali)~$

```

Instance to View: (LAN) LAN  
Choose which instance alerts you want to inspect.

Save or Remove Logs: Download Clear  
All alert log files for selected interface will be downloaded All log files will be cleared

Save Settings: Save Refresh  
Save auto-refresh and view settings Default is ON

Number of alerts to display. Default is 250

Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID/SID	Description
03/12/2022 19:18:23	Warning	2	TCP	Potentially Bad Traffic	99.84.248.4	80	172.16.4.11	58388	1:2100498	GPL ATTACK_RESPONSE id check returned root
03/12/2022 19:17:41	Warning	2	TCP	Potentially Bad Traffic	99.84.248.78	80	172.16.4.11	34930	1:2100498	GPL ATTACK_RESPONSE id check returned root

## Lab 4 – Enumeration with NMap

### Part 1

#### Description

For this lab (Enumeration with NMap), the purpose of the lab is to use the enumerating system information. This is done by using Nmap in the console using Linux. This lab will use NMap in order to get the IP address of the metasploitable3, among other things using NMap.

#### Preparation

For this lab surrounding the Nmap and enumeration, the preparation that was done beforehand was following the various instructions, along with the lecture, on how to properly setup Metasploitable3 Linux and install it successfully. After following the instructions, I had Metasploitable3 installed, and Metasploitable 3 was accessible on the lab network. This is what was needed to be finished before attempting the lab, as per the “preparation” section of the lab 4 document.

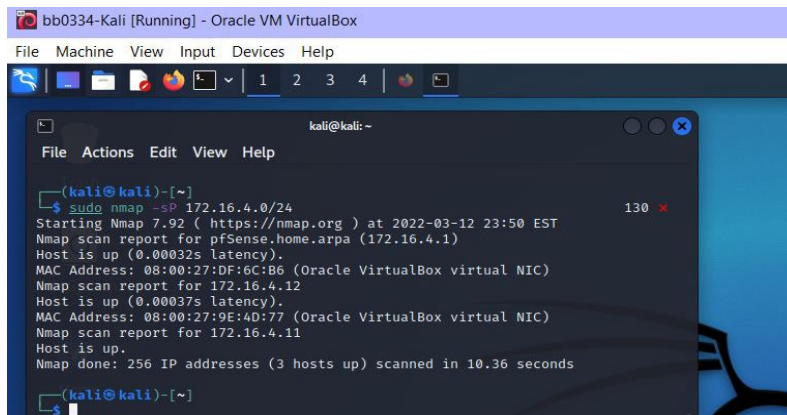
#### Observations

1. After installing and setting up metasploitable3, I followed the instructions for the first task to locate the metasploitable3 machine. The ping scan was run using “sudo nmap -sP 172.16.4.0/24” command. After running the command, I was able to see the ping scan of the network and determine hosts were online. Metasploitable3 was 172.16.4.12.
2. After running the previous command, I was able to see that status of which machines were online, I then targeted 172.16.4.12, since that was the IP on the metasploitable3 machine. After running sudo nmap -O 172.16.4.12, I was able to see information on the machine, such as the OS type.
3. For the third task, I ran the sudo nmap -A 172.16.4.12, with the IP being the IP of the metasploitable3 machine. After the command was ran, I was able to see a thorough scan of the machine, and see various details about the metasploitable3 using Nmap. I could see information such as the port, state, service, version, among other interesting things in relation to the metasploitable3 machine.

#### Screenshots

1. **Task #1** Ping scan of network.





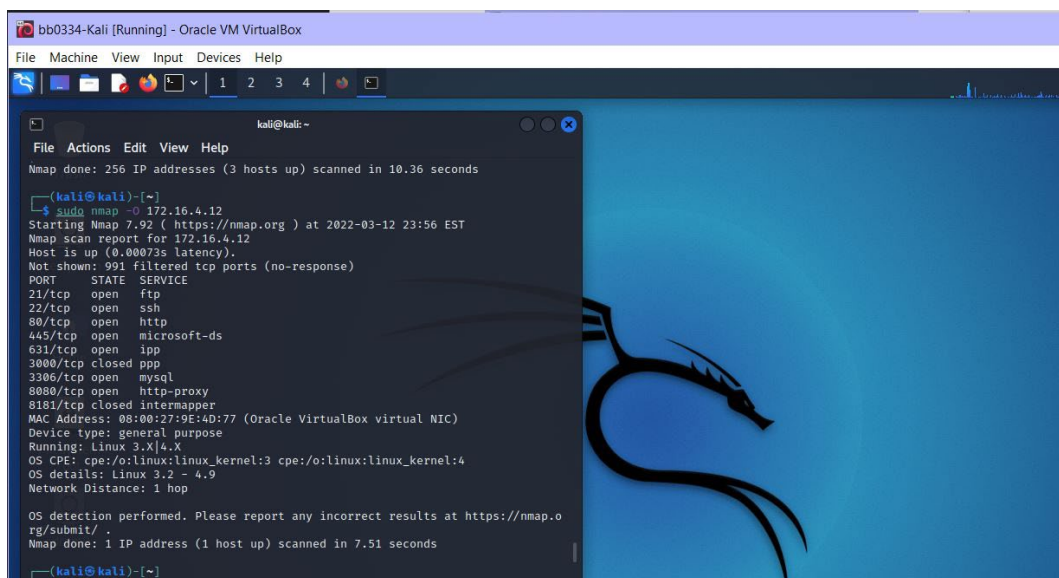
```
bb0334-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo nmap -sP 172.16.4.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-12 23:50 EST
Nmap scan report for pfSense.home.arpa (172.16.4.1)
Host is up (0.00032s latency).
MAC Address: 08:00:27:DF:6C:B6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 172.16.4.12
Host is up (0.00037s latency).
MAC Address: 08:00:27:9E:4D:77 (Oracle VirtualBox virtual NIC)
Nmap scan report for 172.16.4.11
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 10.36 seconds

(kali@kali)-[~]
```

## 2. Task #2 Directly targeting machines online for scan. (Metasploitable3)



```
bb0334-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

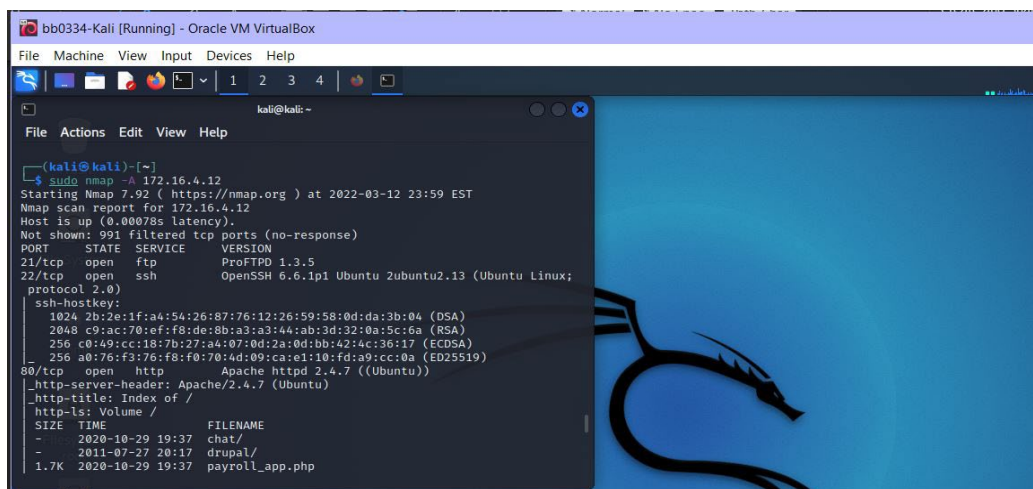
Nmap done: 256 IP addresses (3 hosts up) scanned in 10.36 seconds

(kali@kali)-[~]
$ sudo nmap -O 172.16.4.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-12 23:56 EST
Nmap scan report for 172.16.4.12
Host is up (0.00073s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp    open  microsoft-ds
631/tcp    open  ipp
3000/tcp   closed ppp
3306/tcp   open  mysql
8080/tcp   open  http-proxy
8181/tcp   closed intermapper
MAC Address: 08:00:27:9E:4D:77 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 7.51 seconds

(kali@kali)-[~]
```

## 3. Task #3 Thorough scan of metasploitable3.



```
bb0334-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

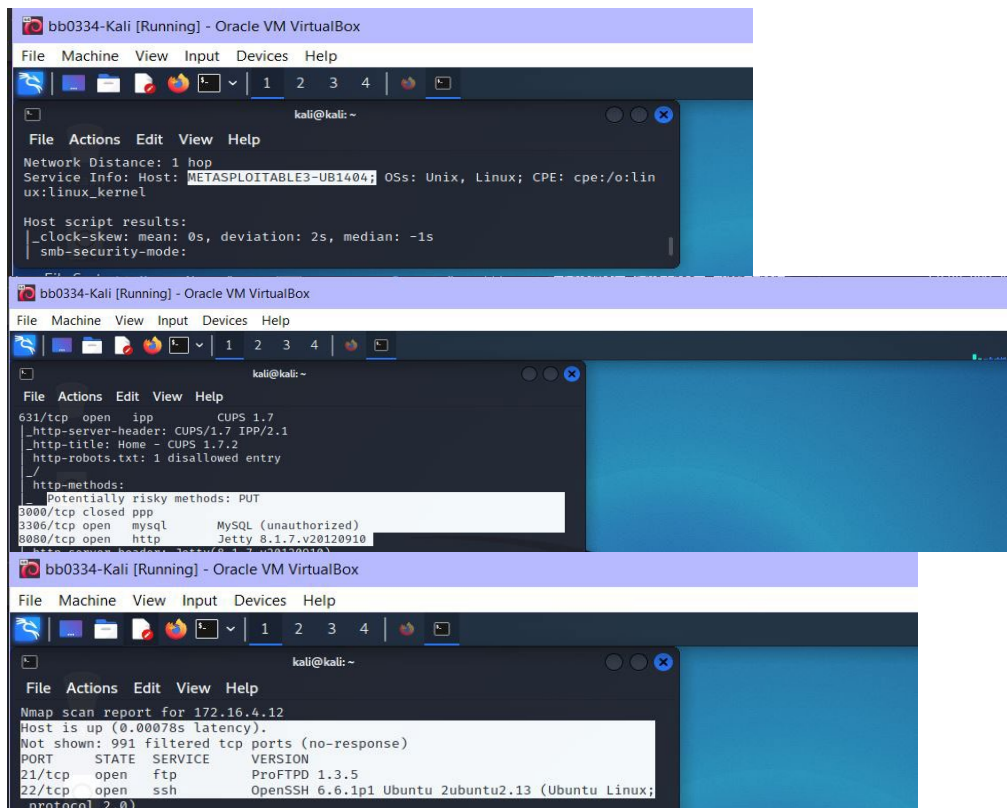
(kali@kali)-[~]
$ sudo nmap -A 172.16.4.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-12 23:59 EST
Nmap scan report for 172.16.4.12
Host is up (0.00078s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
_ftp-server-header: Apache/2.4.7 (Ubuntu)
_ftp-title: Index of /
_ftp-ls: Volume /
SIZE      TIME
- 2020-10-29 19:37 chat/
- 2011-07-27 20:17 drupal/
1.7K 2020-10-29 19:37 payroll_app.php

ssh-hostkey:
1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:9c:6a (RSA)
256 c0:a9:cc:c8:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)

_ftp-ls: Volume /
SIZE      TIME
- 2020-10-29 19:37 chat/
- 2011-07-27 20:17 drupal/
1.7K 2020-10-29 19:37 payroll_app.php
```

## Reflection

- 1) During this lab, I ran into some issues regarding the installation. Although on a technical level the problem wasn't too hard, It took an incredibly long time to install metasploitable3, probably hours in total due to my poor internet speeds. Eventually it did install, but not on the drive I wanted it to, as it defaulted to install on my C drive even though I had everything installed and running off of my E drive. Eventually the install worked out. This lab had some pretty interesting information regarding the abilities of NMap, and the multitude of information you can find on machines.
- 2) There was a lot of information found about the metasploitable3 system. I could see information such as the port, version, service, state, latency, network distance, service info, among other things. I found it interesting that you could find the entire name of the machine, in this case it being METASPLOITABLE3-UB1404. I now know that the latency of the metasploiteable3 is 0.00078s, that the service ftp was using version ProFTPD 1.3.5, and that the device type was general purpose. It would be nice to explore more about the "Potentially risky methods" section, since It seems to list MySQL and Jetty, which I'm not familiar with what jetty is.



```
bb0334-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
Network Distance: 1 hop
Service Info: Host: METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:lin
ux:linux_kernel

Host script results:
  _clock-skew: mean: 0s, deviation: 2s, median: -1s
  _smb-security-mode:

bb0334-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
631/tcp open ipp CUPS 1.7
  _http-server-header: CUPS/1.7 IPP/2.1
  _http-title: None - CUPS 1.7.2
  _http-robots.txt: 1 disallowed entry
  _http-methods:
    Potentially risky methods: PUT
3000/tcp closed ppp
3306/tcp open mysql MySQL (unauthorized)
8080/tcp open http Jetty 8.1.7.v20120910
  _http-server-header: Jetty/8.1.7.v20120910

bb0334-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
Nmap scan report for 172.16.4.12
Host is up (0.00078s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    ProFTPD 1.3.5
22/tcp    open  ssh    OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol 2.0)
```

## Lab 5 – Enumeration with enum4linux

### Part 1

#### Description

For this lab (Enumeration with enum4linux), the purpose of the lab was to use the enum4linux tool against the metasploitable3 machine, and explore the type of information that the enum4linux tool can provide about machines. This lab showcases the types of information pulled from enum4linux and asks questions to regard to how the information given can be used to exploit different types of vulnerabilities.

#### Preparation

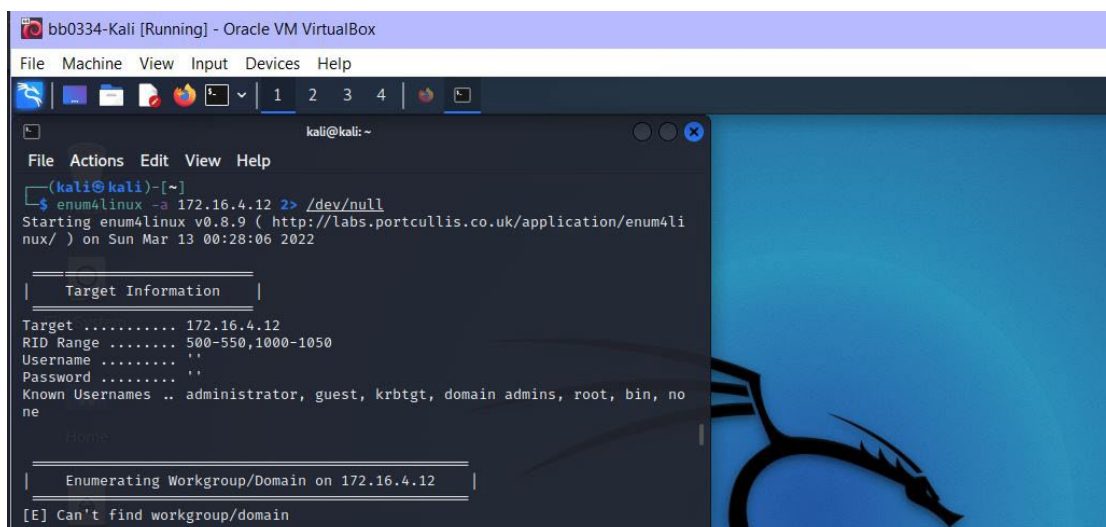
For this lab the preparation involved was relatively similar to Lab 5, as I just made sure that Metasploitable3 Linux was installed its successfully and correctly. I again tested to make sure that the metasploitable3 was accessible on the network, and I did this my running the machine, as well as the kali linux machine and running the sudo nmap -sP 172.16.4.0/24 command to make sure I could see it on the network, which I could.

#### Observations

1. By using enum4linux, I ran the command stated in the first task, “enum4linux -a 172.16.4.12 2> /dev/null”. After running this command, I was able to get “target information”, enumerating workgroup, nbtstat information, session check, domain SID, Os Information, Users, share enumeration, password policy information, groups, users via RID cycling, and printer information. There was a multitude of information given about the metasploitable3 machine I was running when using this command.

#### Screenshots

1. **Task #1** Running the “enum4linux -a 172.16.4.12 2> /dev/null” command.



The screenshot shows a Kali Linux terminal window titled "bb0334-Kali [Running] - Oracle VM VirtualBox". The terminal displays the command `enum4linux -a 172.16.4.12 2> /dev/null` and its output. The output includes a header "Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Mar 13 00:28:06 2022", followed by a section titled "Target Information" with details for target 172.16.4.12, including RID range, username, password, and known usernames. Below this, it shows "Enumerating Workgroup/Domain on 172.16.4.12" and ends with "[E] Can't find workgroup/domain".

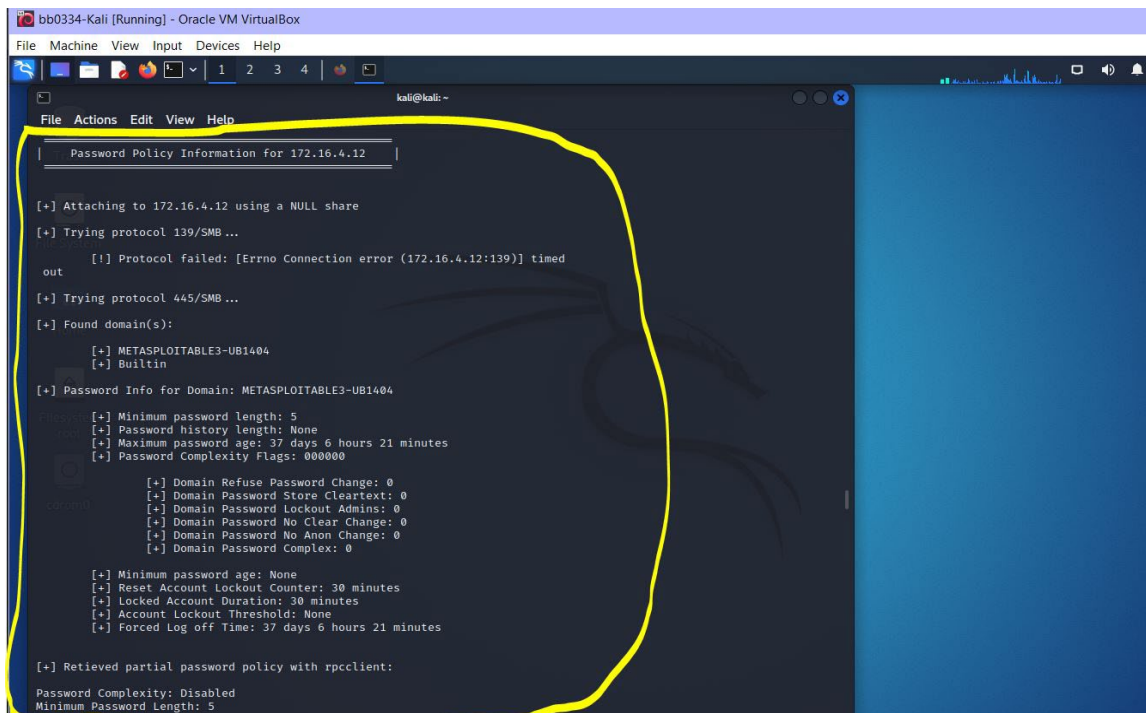
```
bb0334-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ enum4linux -a 172.16.4.12 2> /dev/null
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Mar 13 00:28:06 2022

+-----+
| Target Information |
+-----+
Target ..... 172.16.4.12
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, no
ne

+-----+
| Enumerating Workgroup/Domain on 172.16.4.12 |
+-----+
[E] Can't find workgroup/domain
```

## Reflection

- 1) Since this lab only required one task, I did not personally run into any issues doing, or preparing for this lab. I had no issues running the command itself either, and seemed to give all of the appropriate information it should give out when the command did execute. I think from this lab it gave valuable information regarding the kind of things that can be visible to others with your system, as the command that was run showcased a multitude of heavy information regarding the system that most people would not want others to see on their personal machines.
- 2) I think other information that was reported by the enum4linux tool in relation to the metasploitable3 machine that could be helpful in the future when looking into possible methods of exploiting a vulnerability, would possibly be the section regarding passwords, in particular, the "Password policy information for 172.16.4.12" heading. This portion showcases some really critical information regarding the metasploitable3 machine, and displays things such as password complexity, the minimum password length, the maximum password age, among other information. This data could be used to exploit a vulnerability in regard to the machine's password.



```
bb0334-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
Password Policy Information for 172.16.4.12

[+] Attaching to 172.16.4.12 using a NULL share
[+] Trying protocol 139/SMB...
[!] Protocol failed: [Errno Connection error (172.16.4.12:139)] timed out
[+] Trying protocol 445/SMB...
[+] Found domain(s):
[+] METASPLOITABLE3-UBI404
[+] Built-in
[+] Password Info for Domain: METASPLOITABLE3-UBI404
[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: 37 days 6 hours 21 minutes
[+] Password Complexity Flags: 000000
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: 37 days 6 hours 21 minutes
[+] Retrieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 5
```

## References

N/A