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

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 if 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.

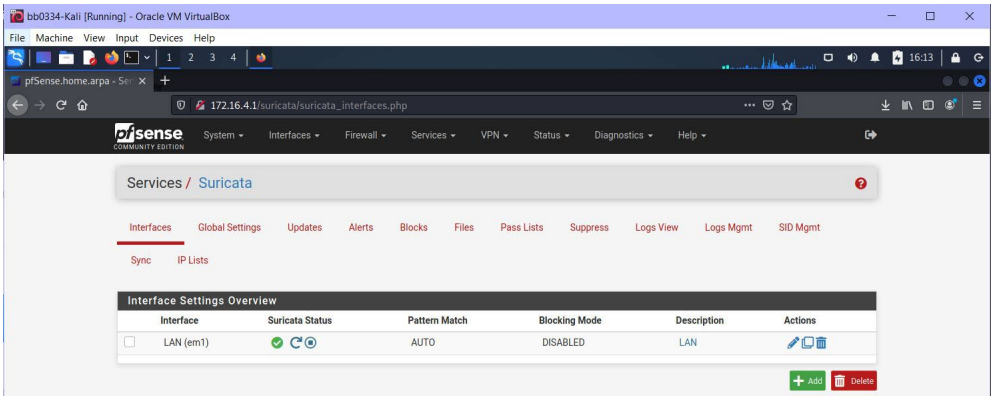
Observations

1. As per the first task, I ensured that all of the virtual machines were names 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” 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.

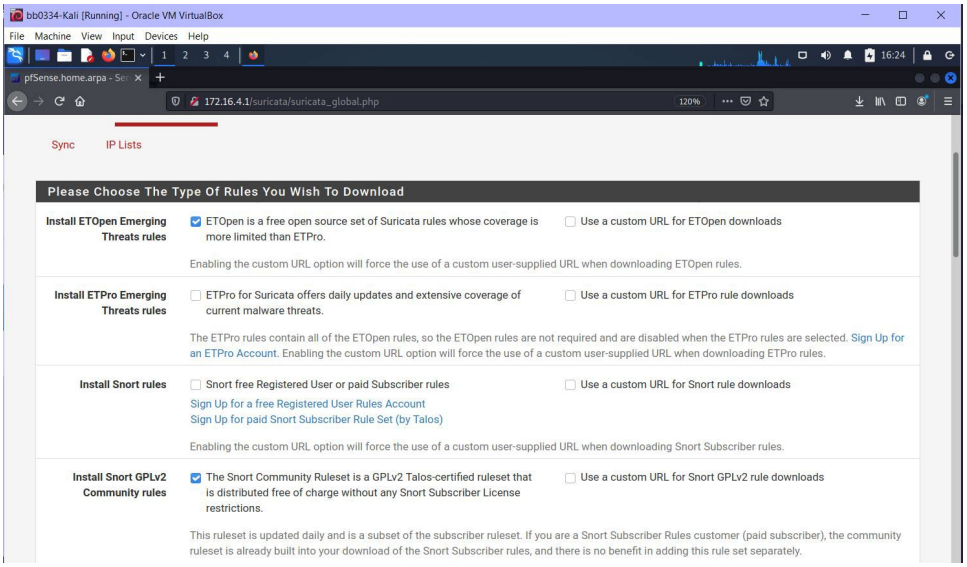
Screenshots

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

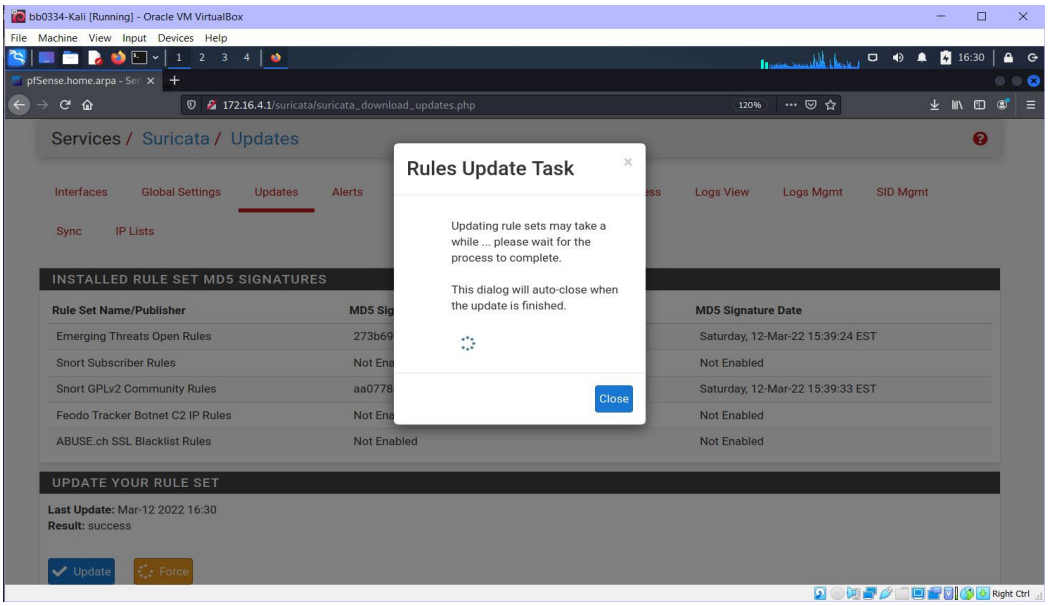
2. **Task #2** Suricata running.



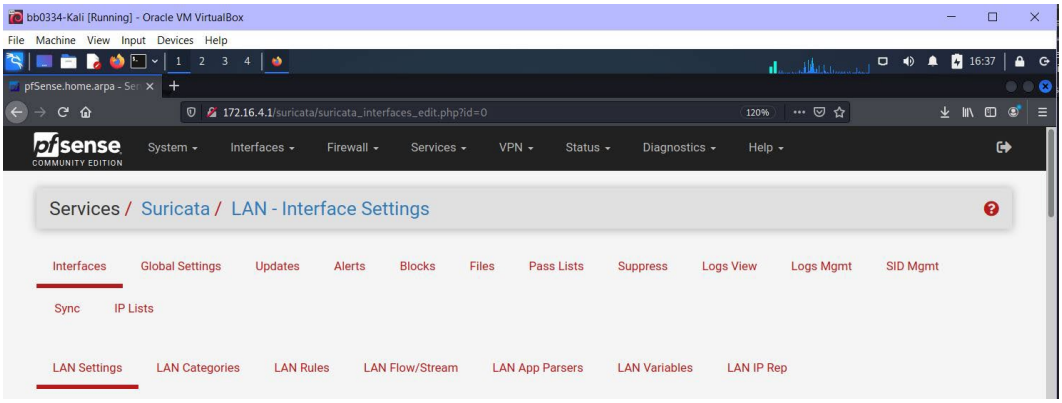
3. **Task #3** Ensuring that ETOpen Emerging Threat Rules and Install Snort GPLv2 Community Rules are selected.



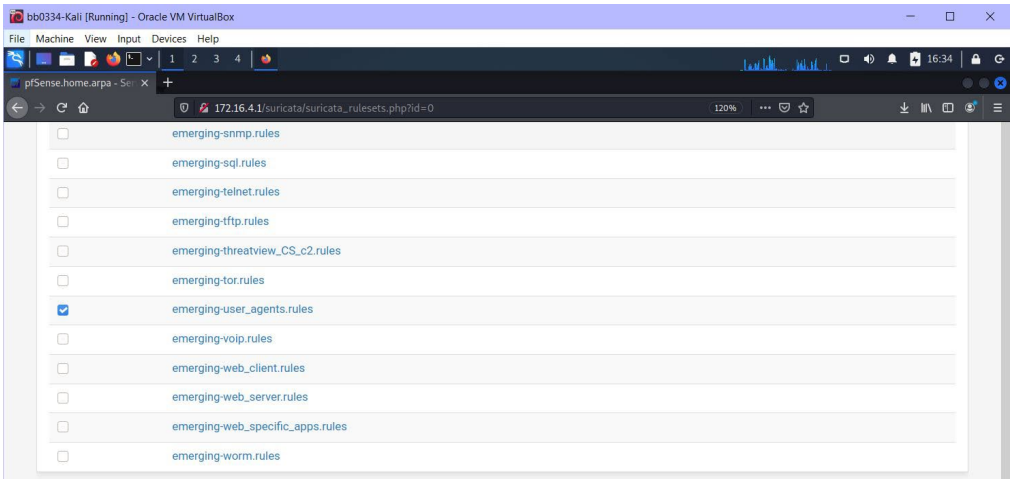
4. **Task #4** Forcing update for the ruleset.



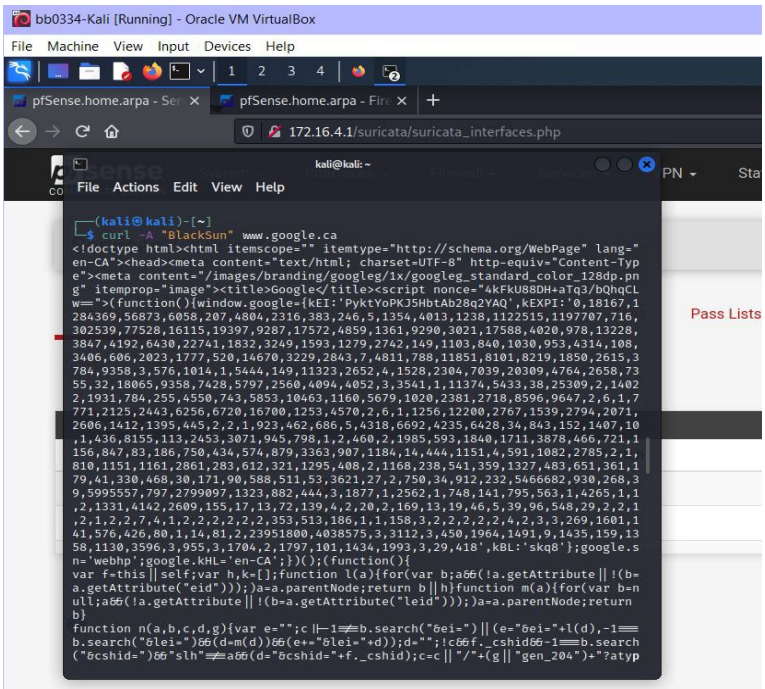
5. **Task #5** In Suricata LAN interface settings.



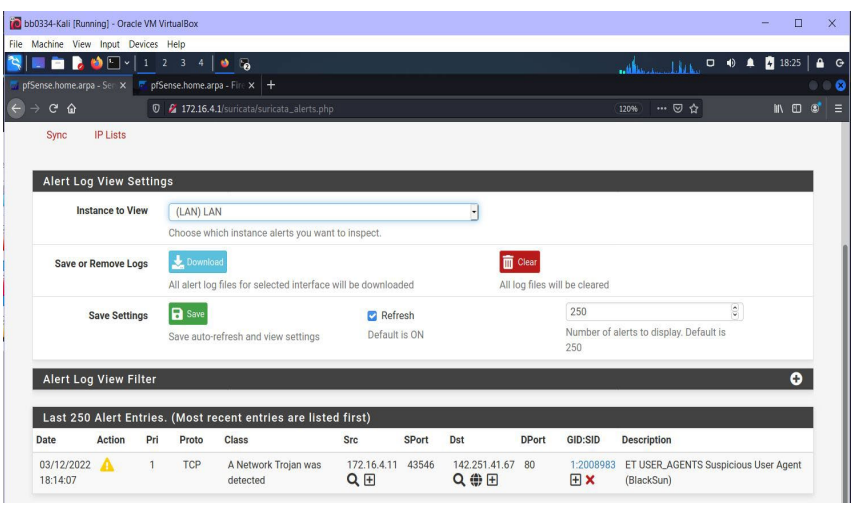
6. **Task #6** Enabling the “emerging-user_agents.rules”.



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



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

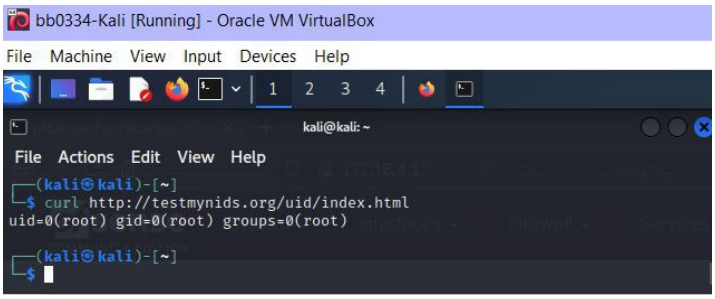


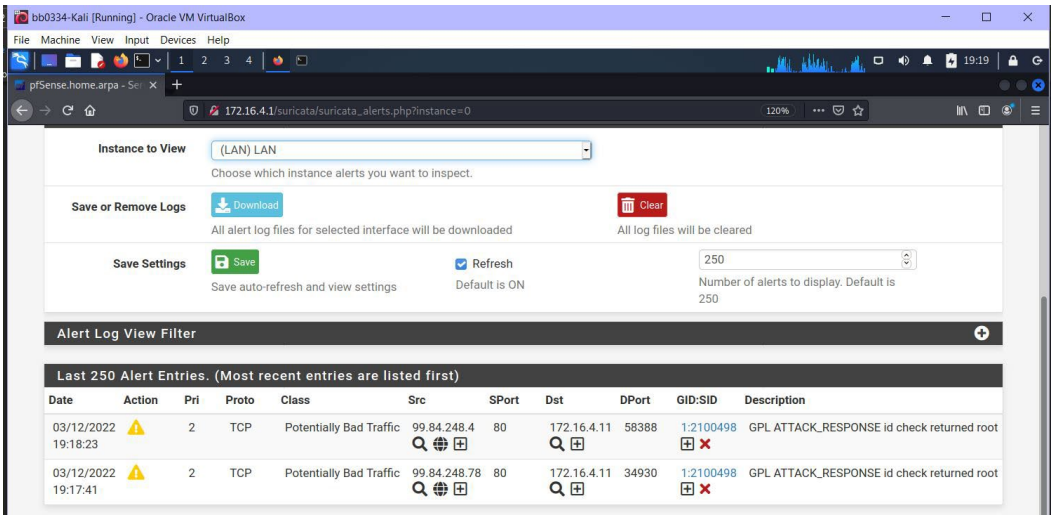
Reflection

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.





Lab 4 – Enumeration with NMap

Part 1

Description

For this lab (Enumeration with NMap), the purpose of the lab if 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

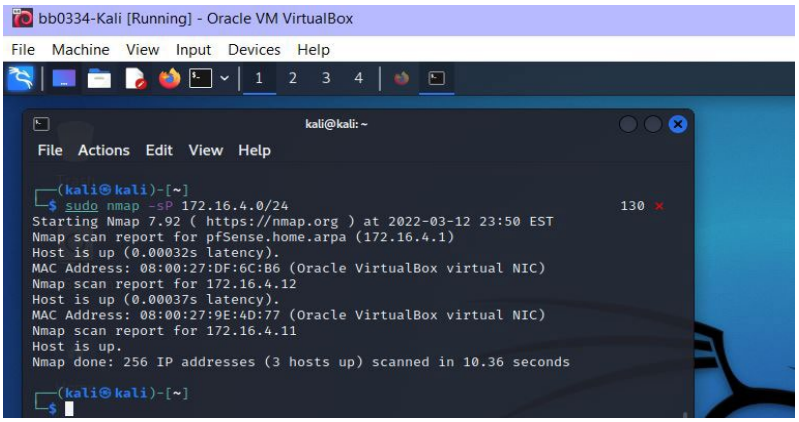
For this lab surrounding the Nmap and enumeration, the preparation that was done beforehand was following the various instructions, along with the lecture, on how to properly setup Metasploitable3 Linux and install its successfully. After following the instructions, I had Metasploitable3 installed, and 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

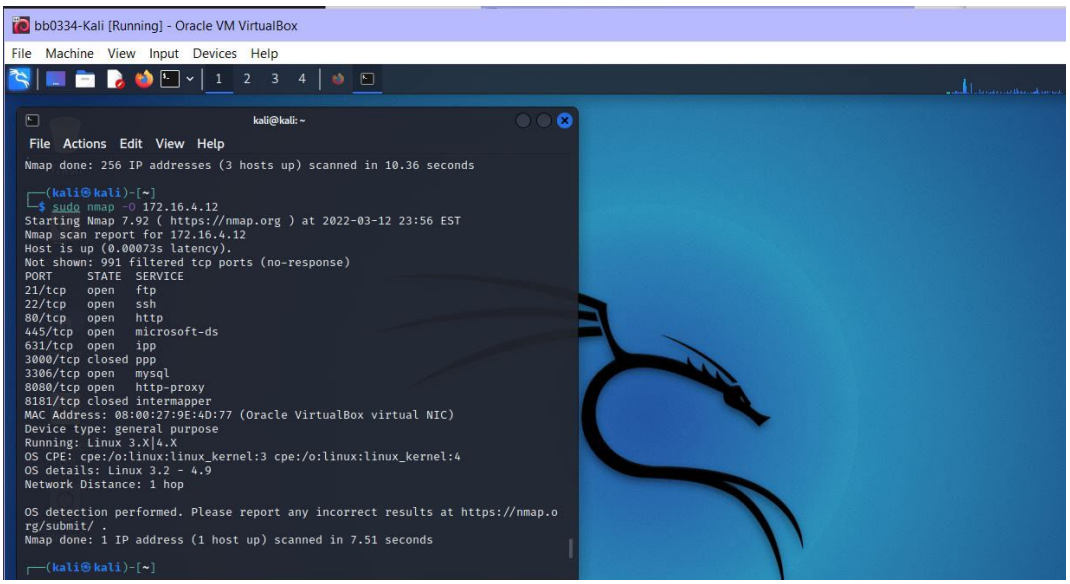
1. After installing and setting up metasploitable3, I followed the instructions for the first task to locate the metasploitable3 machine. The ping scan was run using "sudo nmap -sP 172.16.4.0/24" command. After running the command, I was able to see the ping scan of the network and determine hosts were 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 metaspoitable3 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

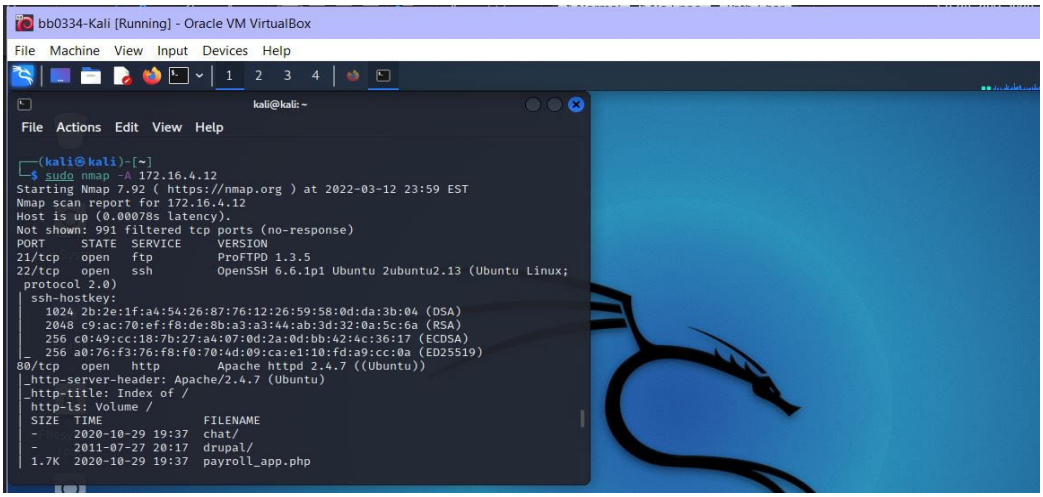
1. **Task #1** Ping scan of network.



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



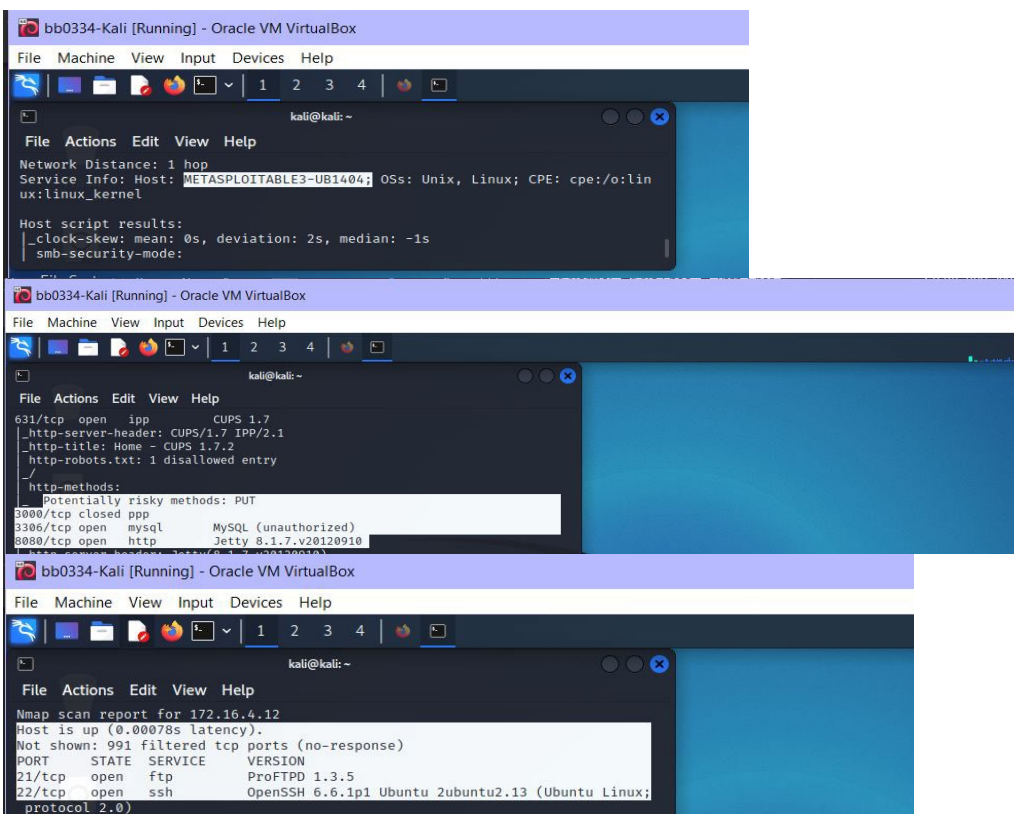
3. **Task #3** Thorough scan of metasploitable3.



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.



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

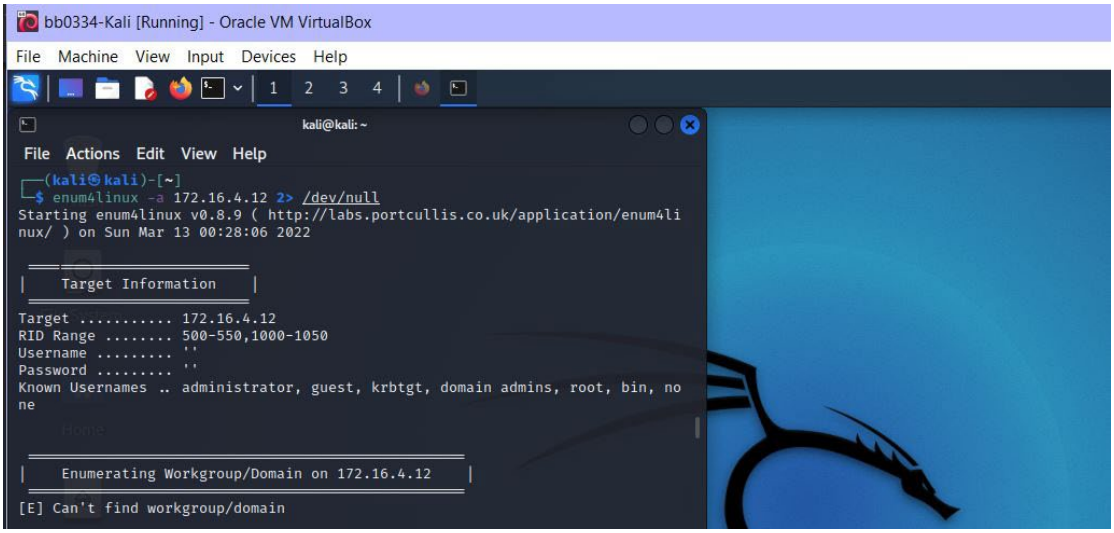
For this lab the preparation involved was relatively similar to Lab 5, as I just made sure that Metasploitable3 Linux was installed its successfully and correctly. I again tested to make sure that the metasploitable3 was accessible on the network, and I did this my running the machine, as well as the 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

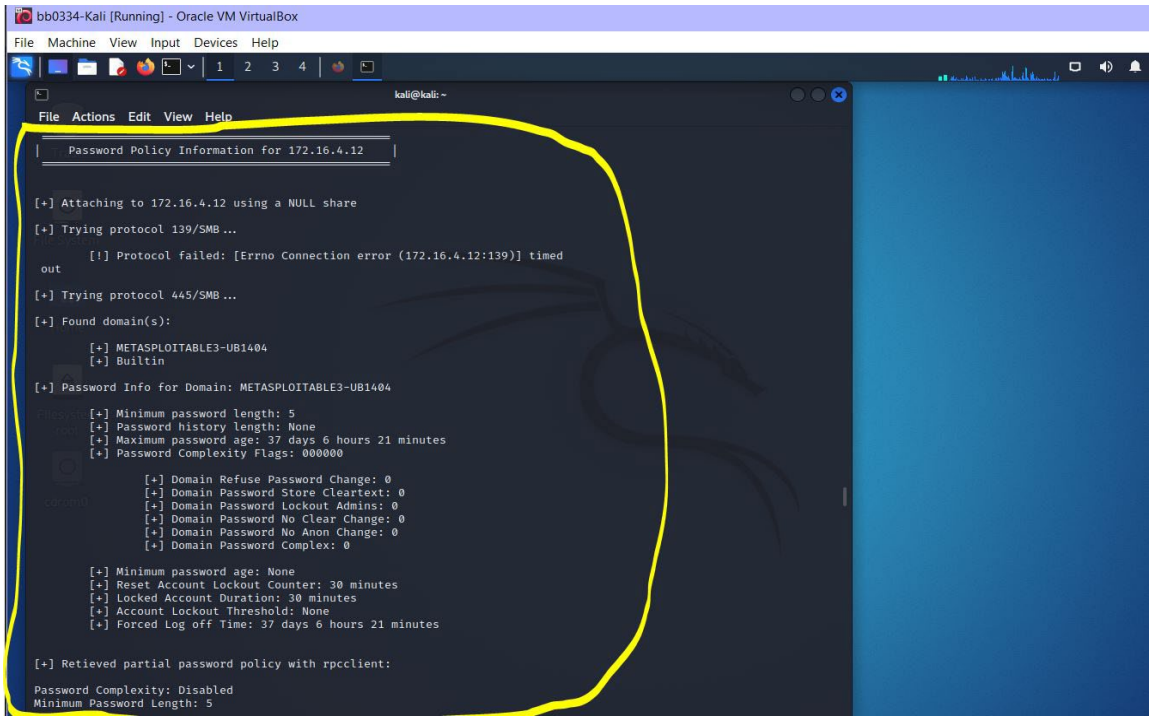
1. **Task #1** Running the “enum4linux -a 172.16.4.12 2> /dev/null” command.



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.



References

N/A