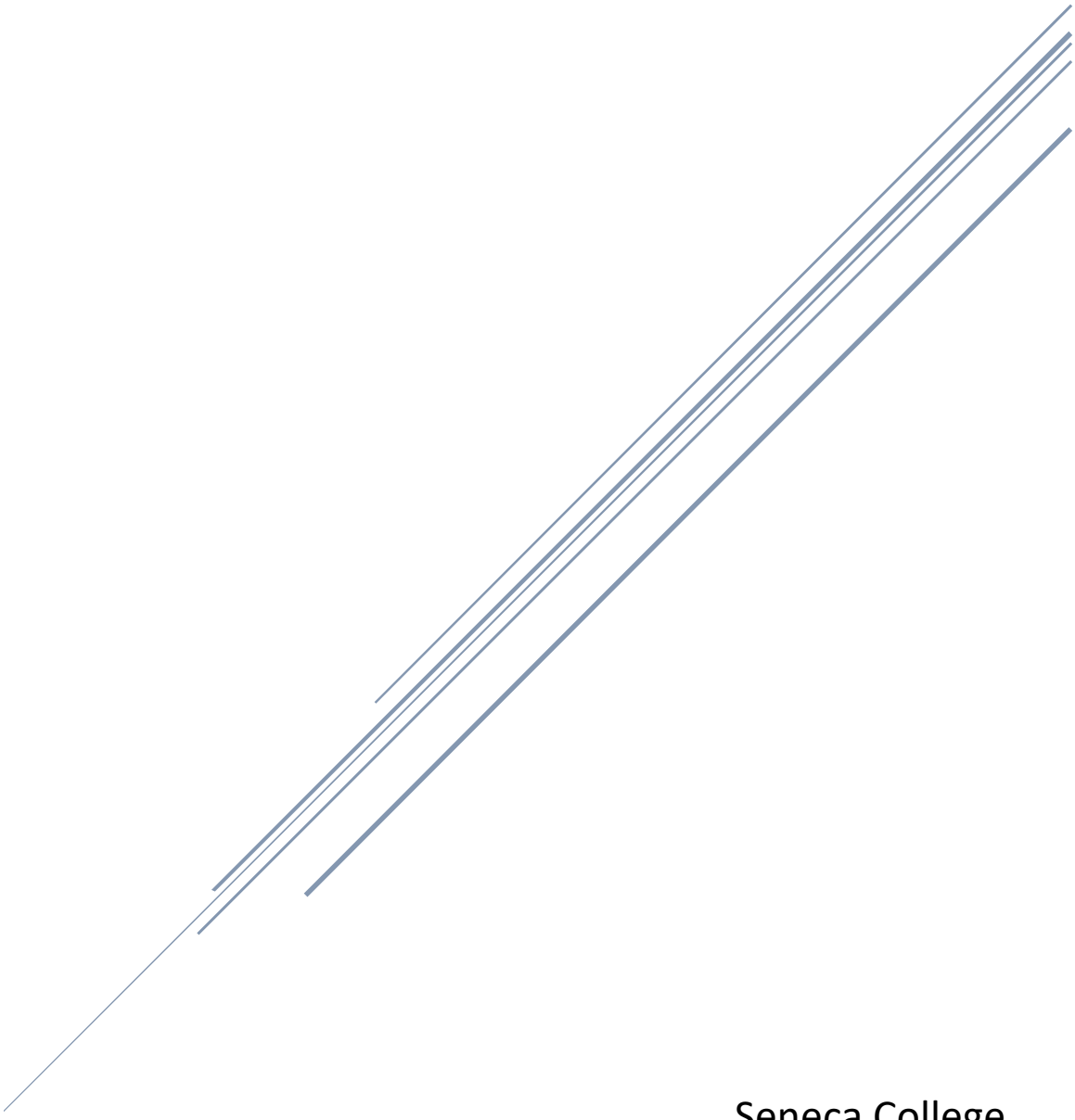
SRT 411 PROJECT PHASE 2

Using Snort to collect all the necessary logs



Seneca College

Group Members Associated with Configuring Project Phase 1

Professor Asma Paracha

Members

Ali Abdulkarim: 150706166

Murad Okasa: 108741208

Buwaneka Hettiarachchi: 104376165

College: Seneca College

Table of Contents

Introduction

This Phase focuses on the collection of the various logs within our system Environment. This is a continuation of the 1st phase of the Project, where our group requires to identify and collect the various different logs. We, then collect the logs to generate data from, data can be both malicious and normal traffic, data should be collected using snort, and later we need to analyze the collected data.

NMAP scans of the Attack Network

We started this phase by first scanning an Nmap scan on the Network, in this scenario, we were scanning the Attack network (172.20.21.0/24). This is the network where we will be able to discover the open ports in all the necessary machines such as the Matasploitable2 machine, Centos Machine 3 and 4, and the Kali Linux machine.

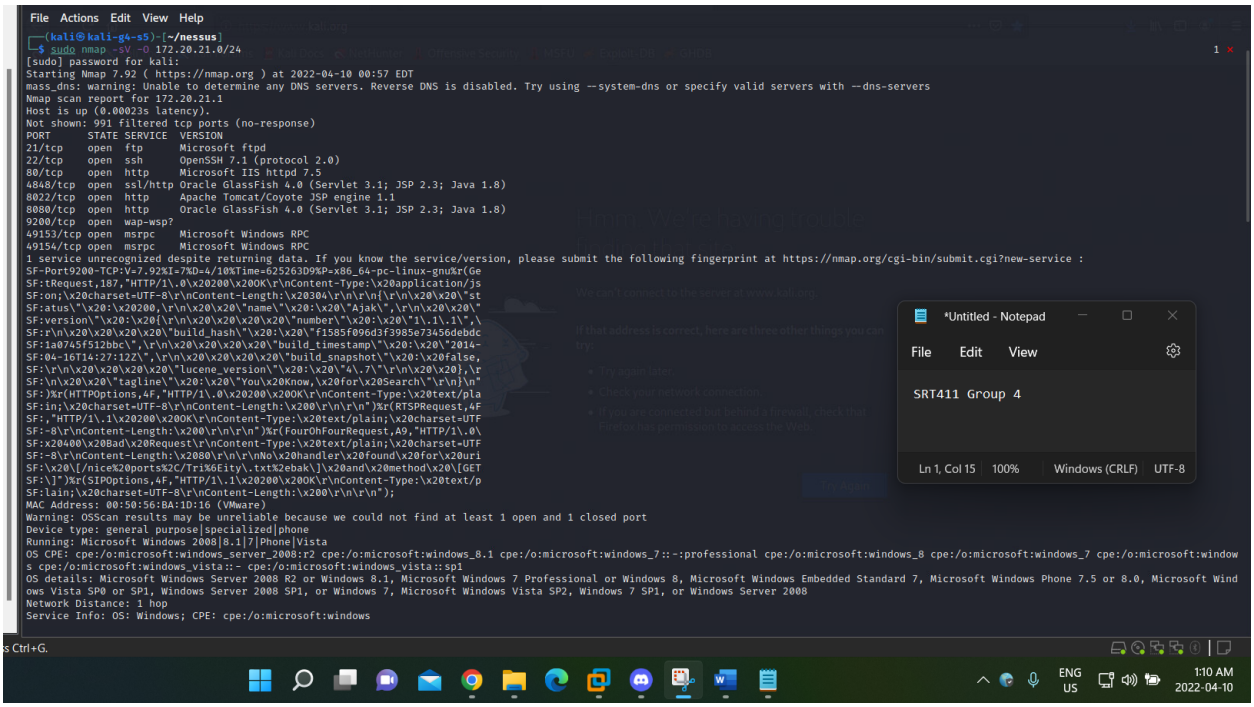


Figure 1: Nmap Scan of the open ports on Metasploitable 2 machine

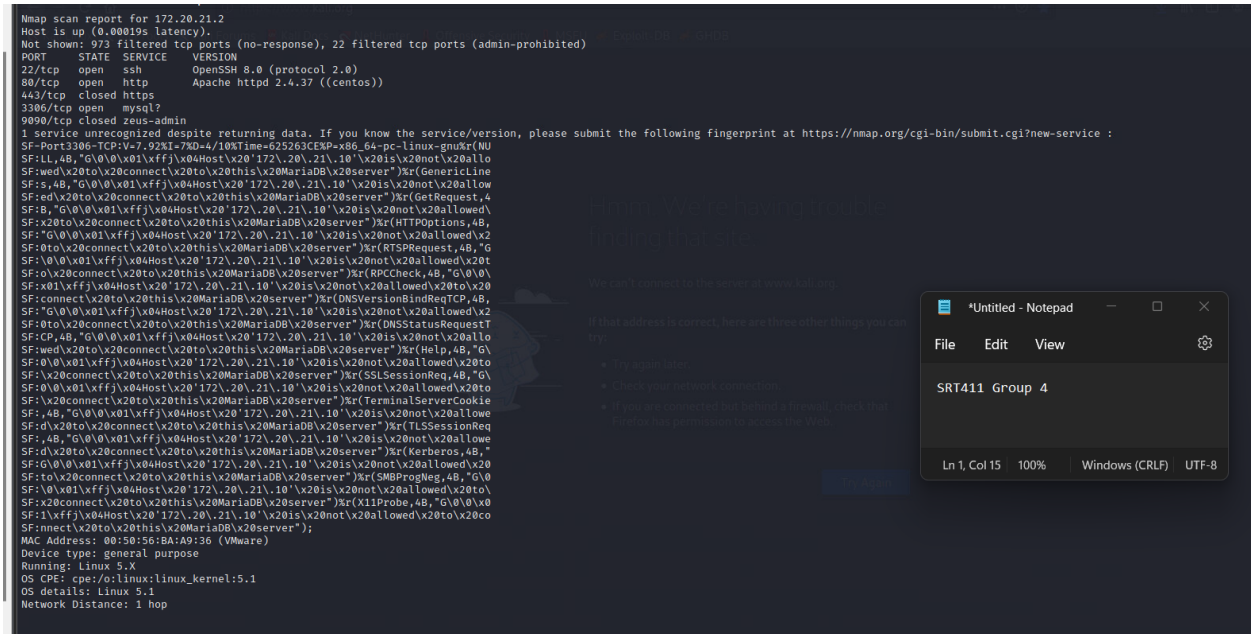


Figure 2: Nmap Open Port scan on the Centos Machine 3

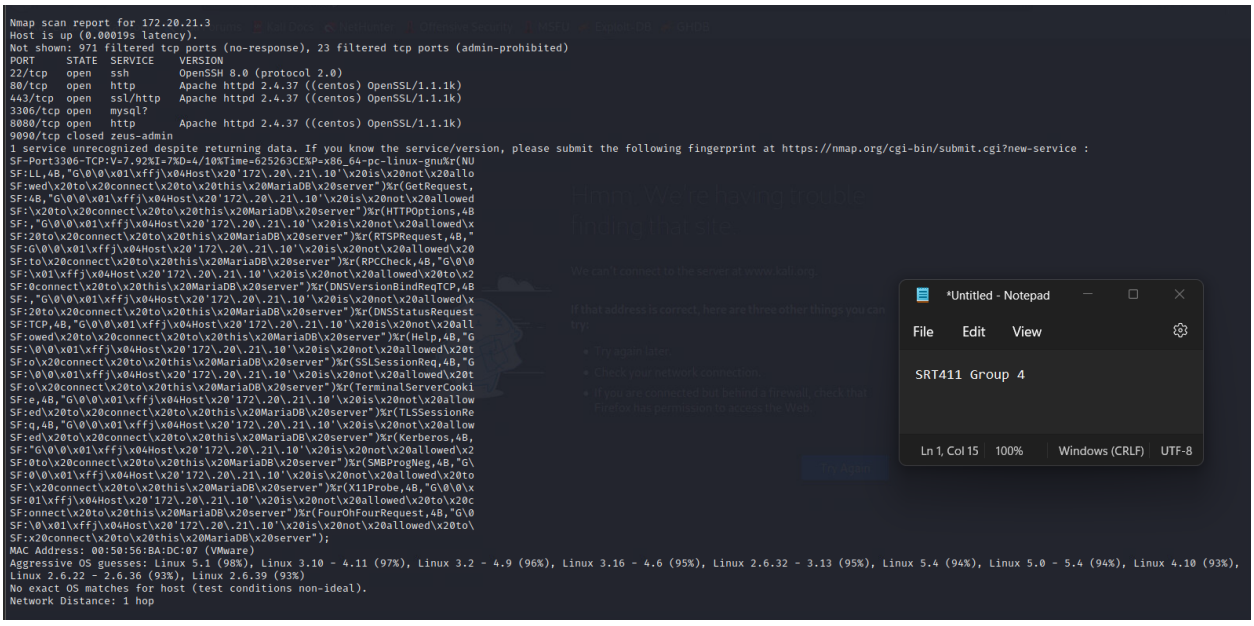


Figure 3: Nmap Open Port Scans on the Centos Machine 4

Figure 4: Showing the Open ports in the Kali Linux Machine

Machine Connectivity

The following images show that the machines can successfully ping all the other machines present within the Network. We need to ensure that all the packets are working fine in order to perform the scans.

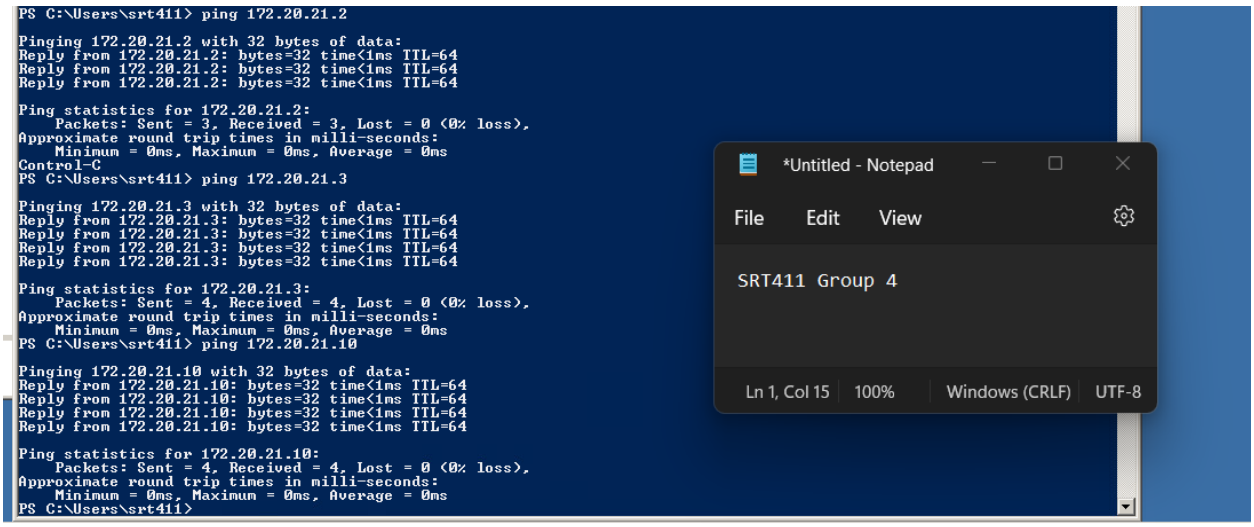


Figure 5: Machine 2 showing connectivity to the machines present in the attack network

Greenbone OpenVAS network scan

The Greenbone OpenVAS is used to detect the vulnerabilities that are present within the scanned machines and give out a rating on how severe each vulnerability that is present within its environment with a vulnerability scale. In this scenario, the IP addresses that I am focusing on are 172.20.21.1, 172.20.21.2, 172.20.21.3.

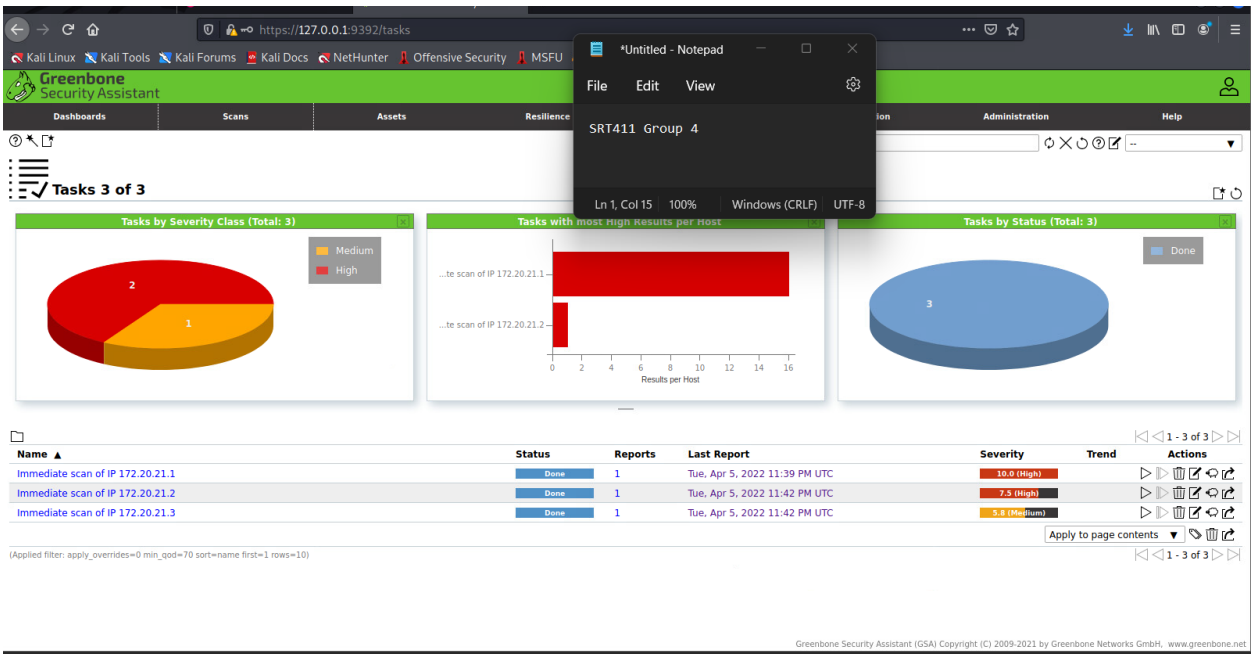


Figure 6: Vulnerability scan on each machine and how malicious each machine is

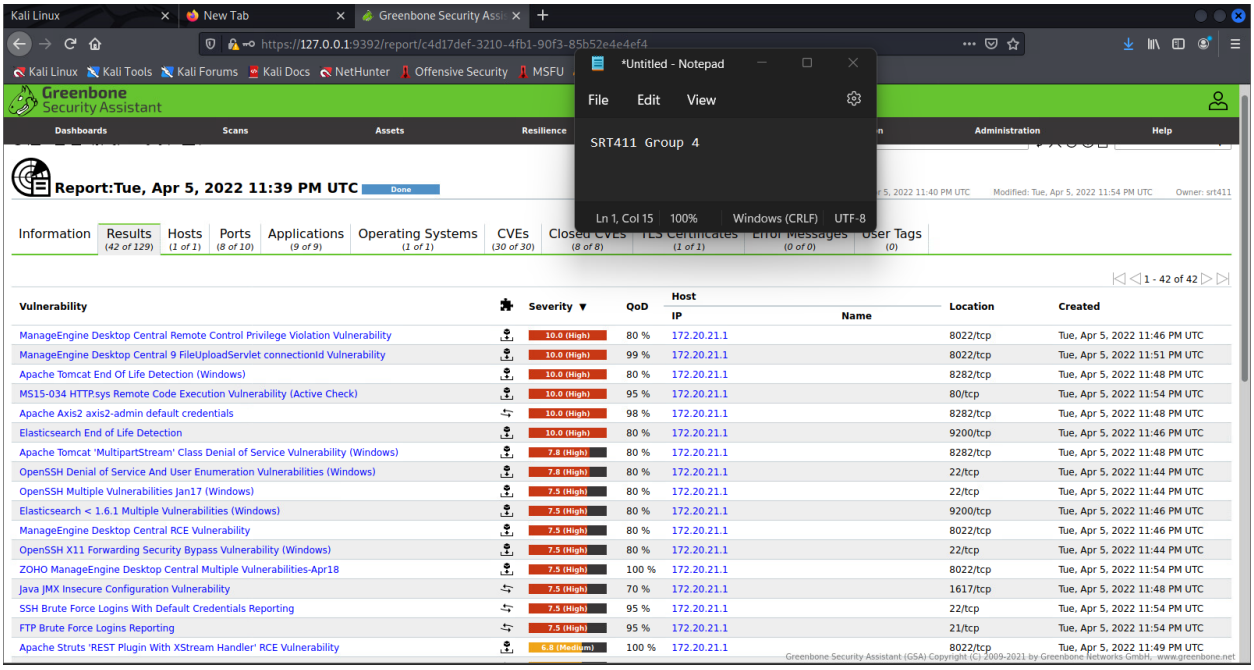


Figure 7: Vulnerabilities that are present in the IP address 172.20.21.1

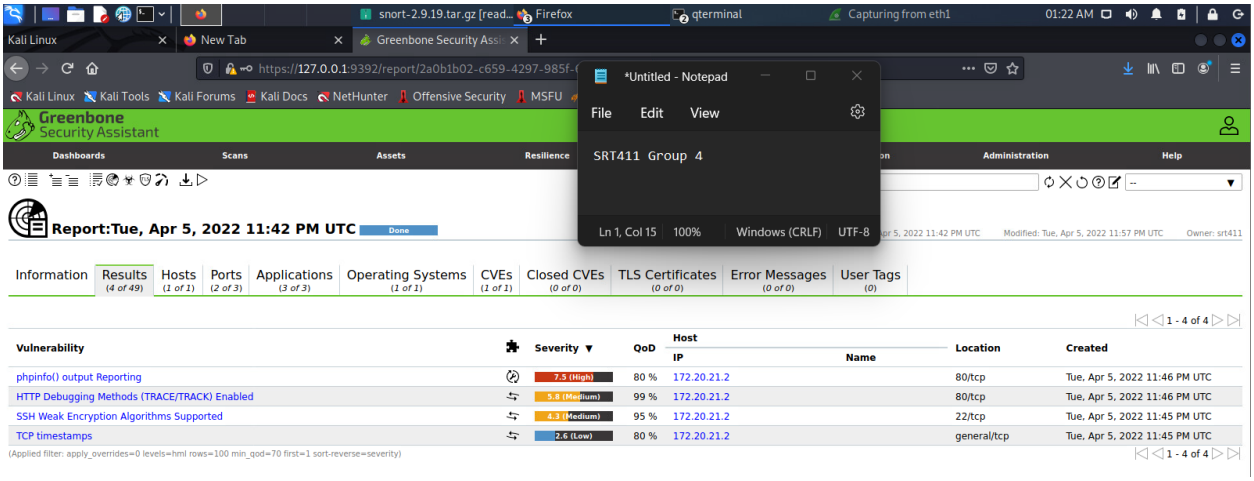


Figure 8: Vulnerabilities that are present in the IP address 172.20.21.2

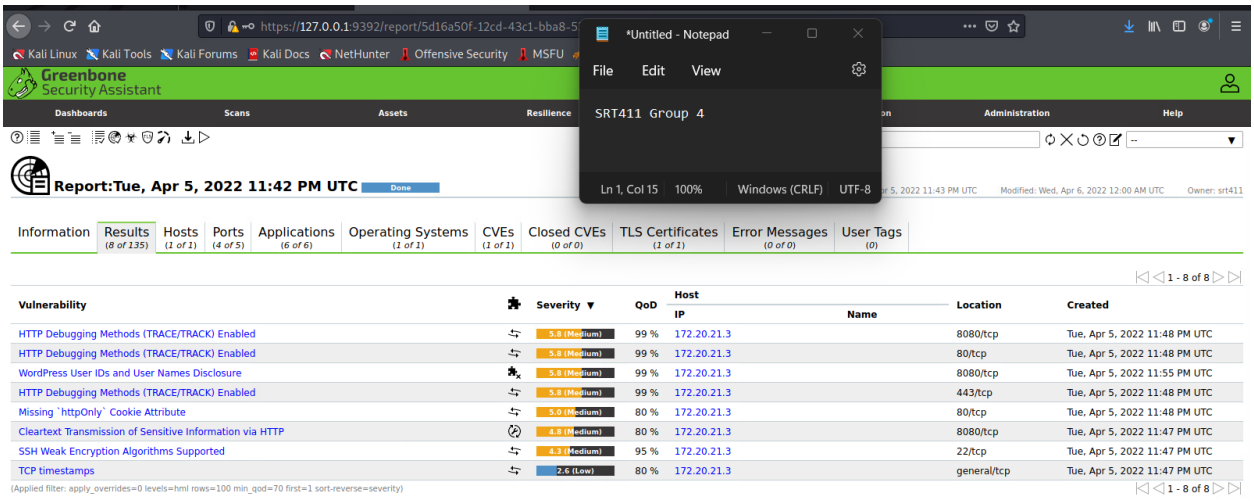


Figure 9: Vulnerability scan report on the IP address 172.20.21.3

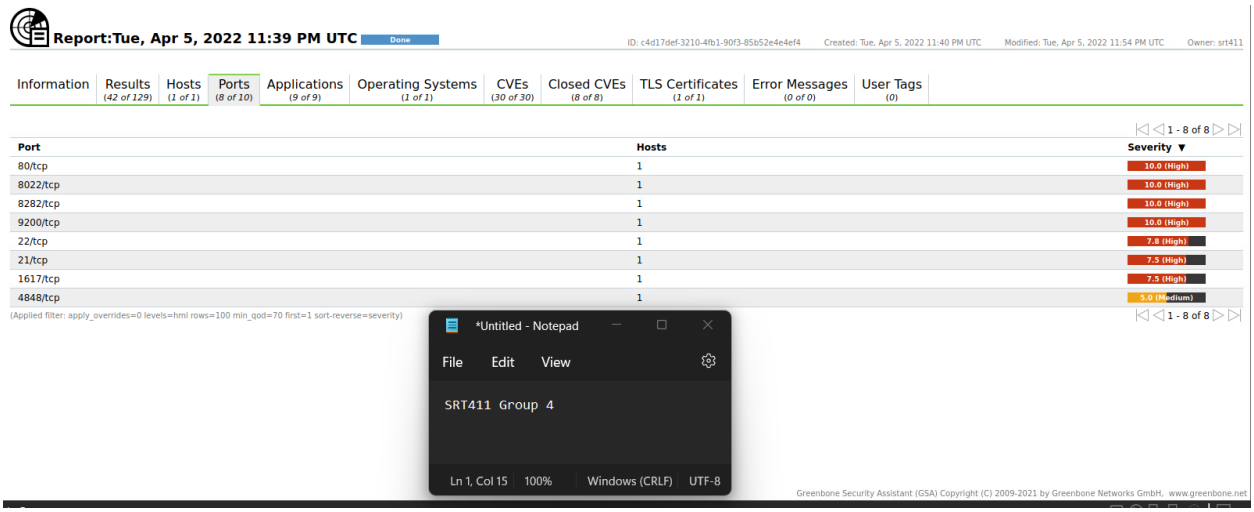


Figure 10: Information on the Open ports of the first machine

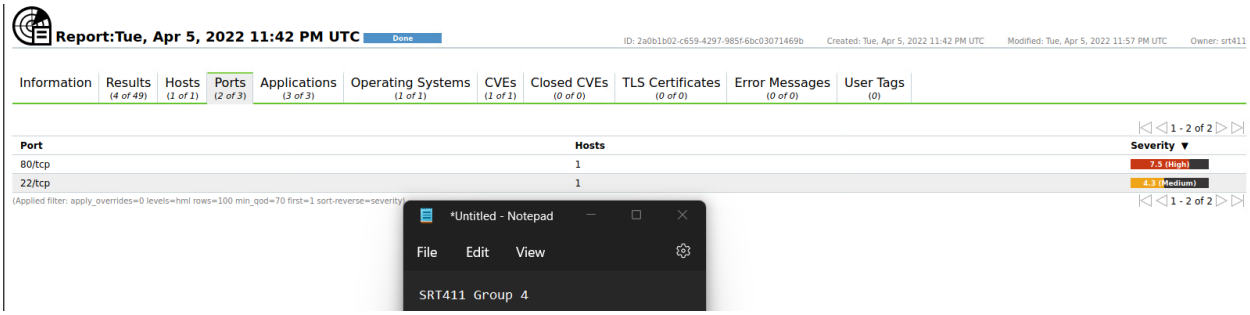


Figure 11: Open ports for the second machine

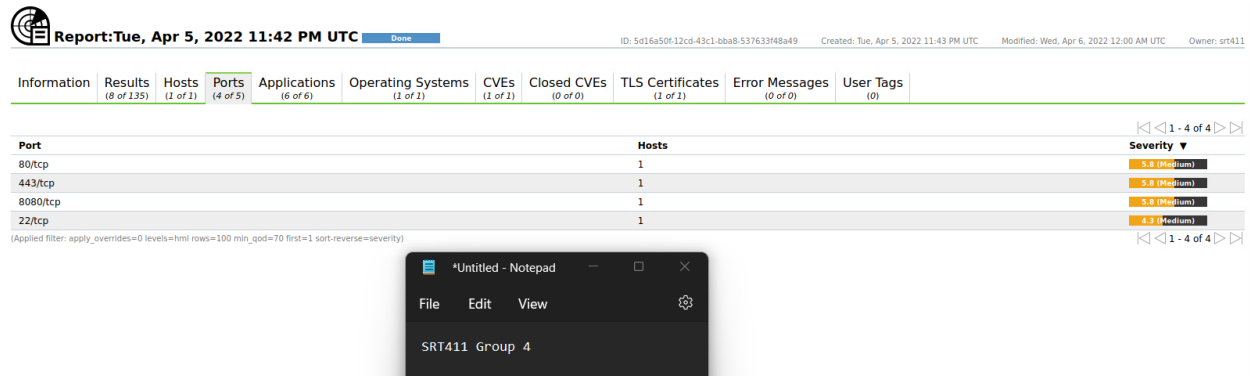


Figure 12: Open ports for the third machine

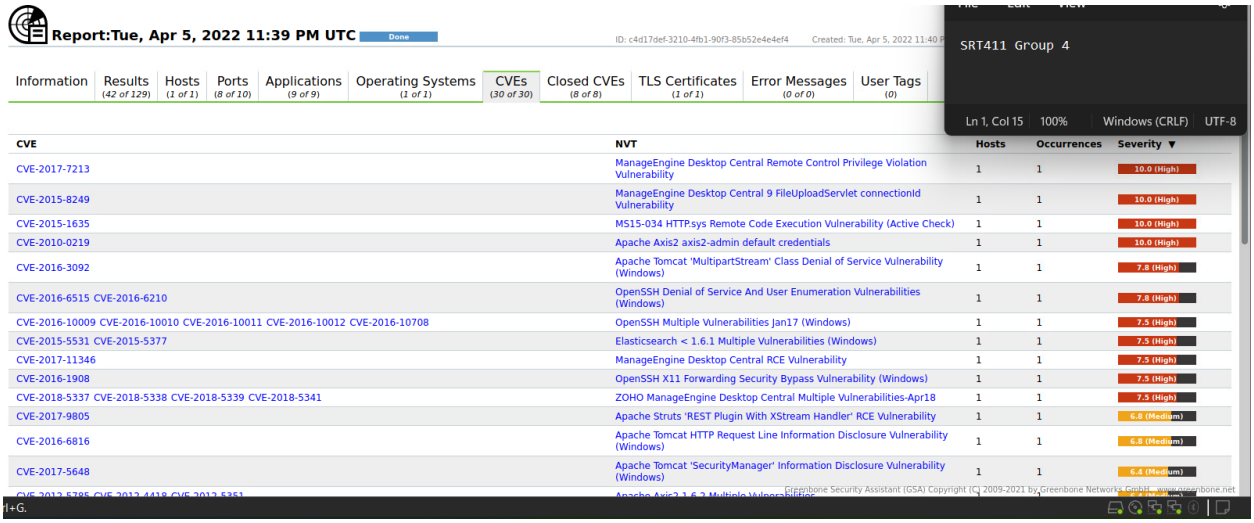


Figure 13: The available CVEs in machine 1

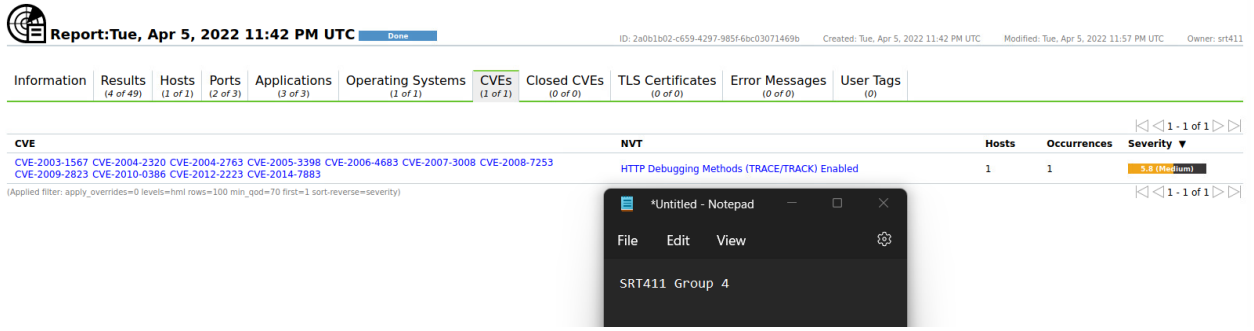


Figure 14: Available CVEs for machine 2

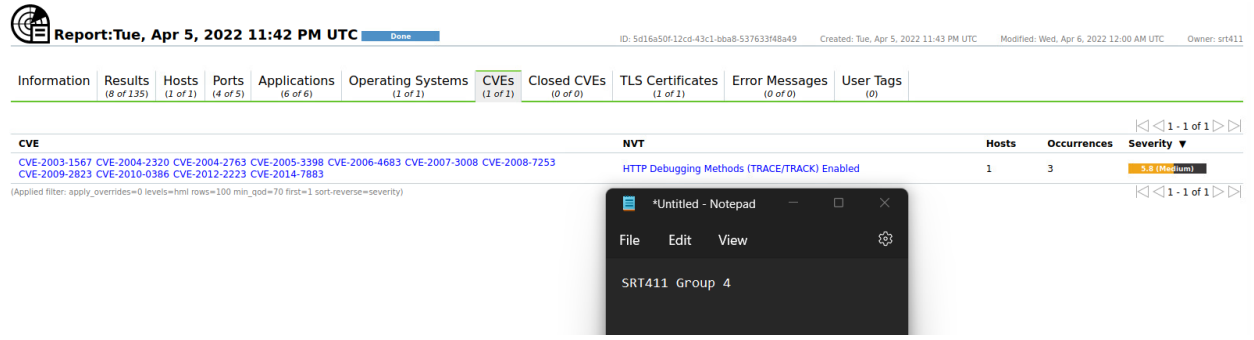


Figure 15: Available CVEs for machine 3

Snort

Snort is an open-source tool that is used for purposes such as Intrusion detection and other activities such as log collection and log generation. Our main goal within this phase is to collect the logs using snort, for snort to successfully collect the logs, we need to create specific rules and these rules are used to detect the certain activities that are present in the environment.

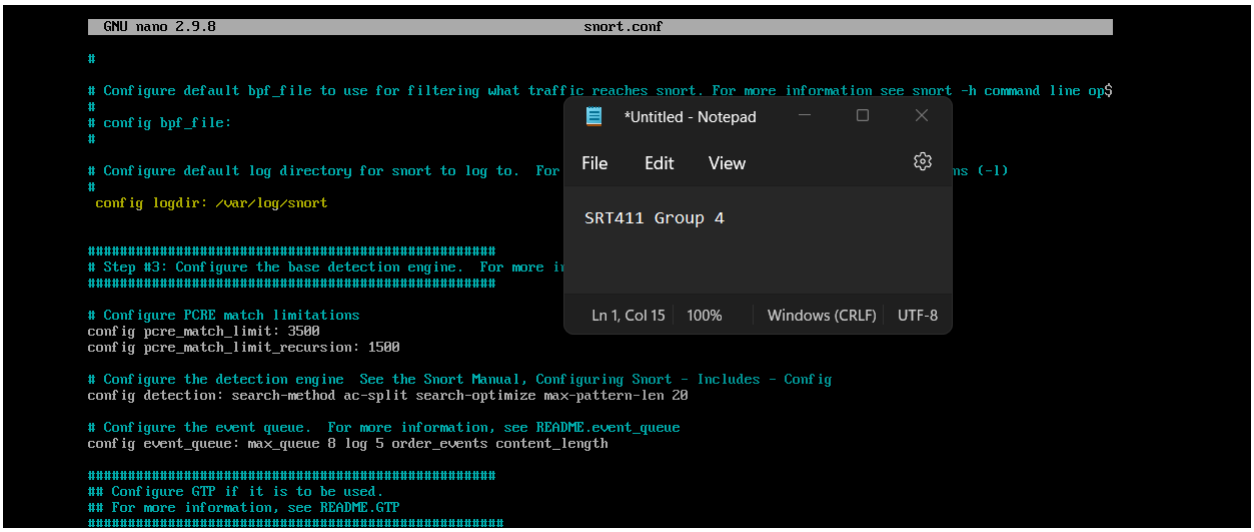


Figure 16: Editing the Snort configuration to add details regarding log directory

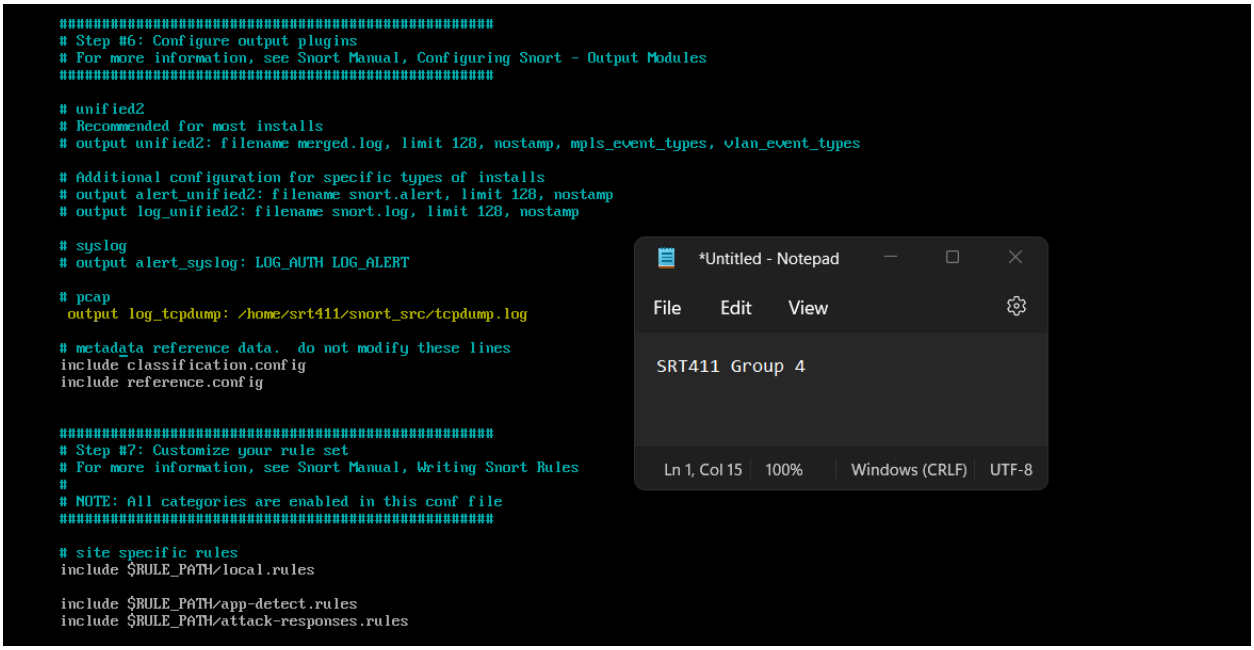


Figure 17: Output for log file for the PCAP files being collected

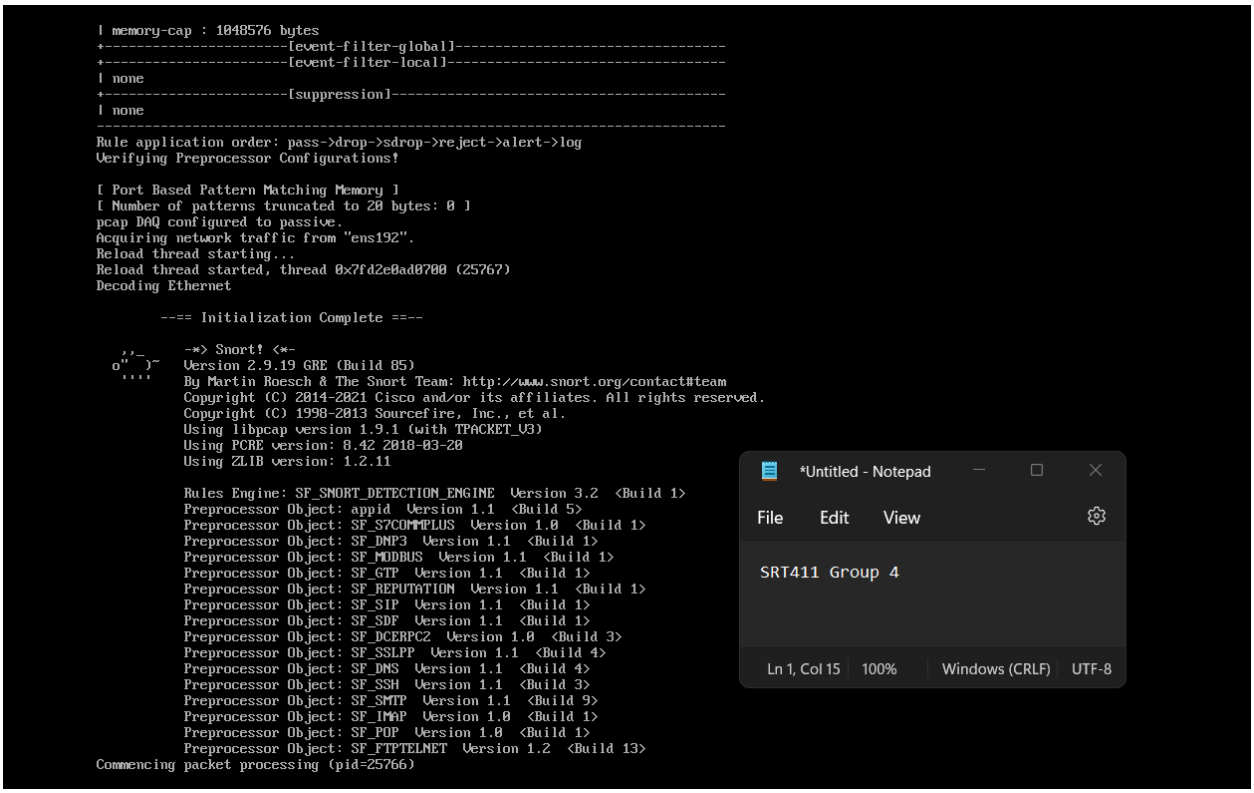


Figure 18: Using the snort configure command to ensure whether snort is running without issues

Generated Snort Rulesets

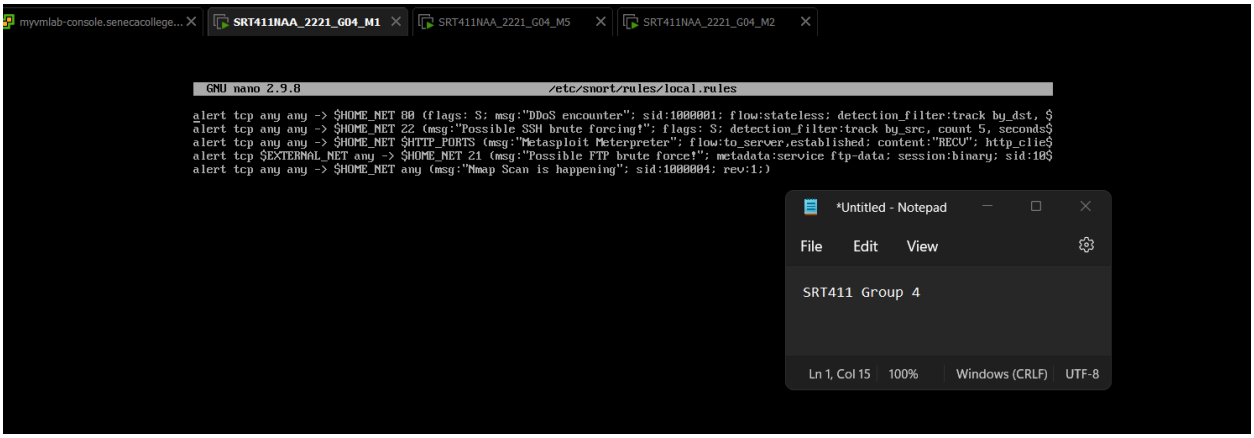


Figure 19: Rules that we generated to collect the logs

Attacks

In this process, we are working on four different log collections within our home network, two attacks are going to be related to brute force attacks where one attack is performed as a ssh attack while the other is performed as an ftp attack. The reason why we performed two separate attacks is to see if snort is able to differentiate the brute force attacks. Then, we performed a

DDoS attack using hping and finally we performed a rule that would generate alerts when we perform Nmap remote scans in the network.

Brute force (ssh)

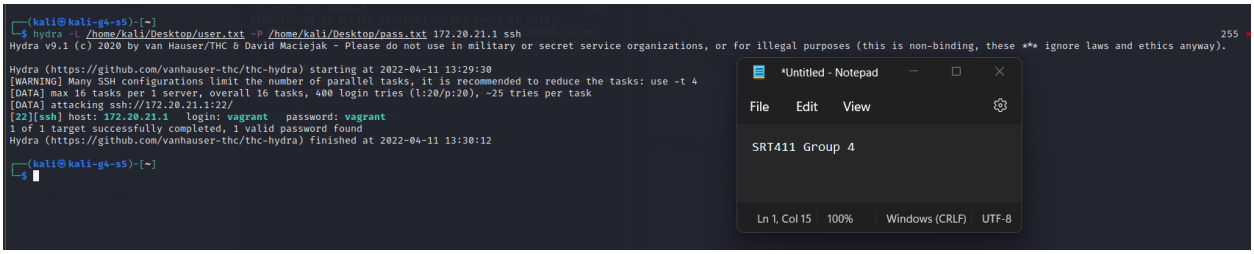


Figure 20: Performing a brute force attack using Hydra to attack Metasploitable 2 machine

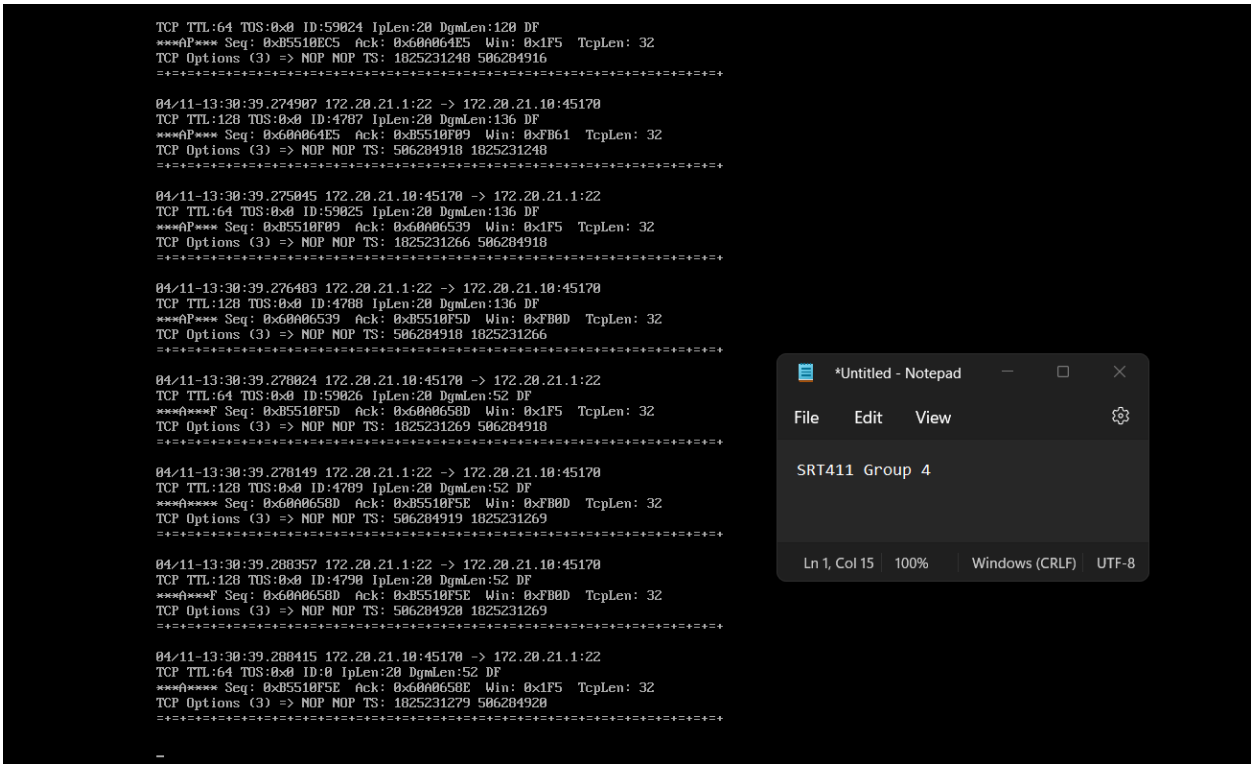


Figure 21:Snort Collecting the logs of the attack

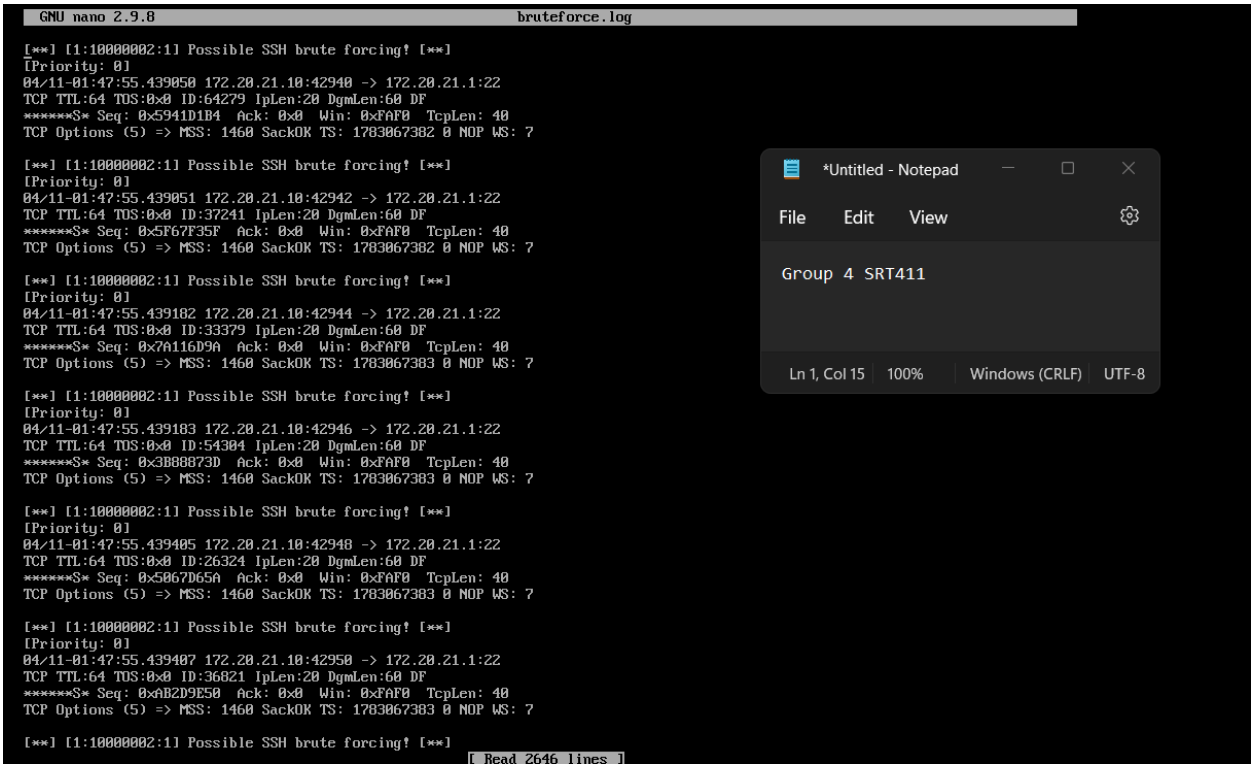


Figure 22: Alerts showing the SID and the generated alert log

Brute force (FTP)

Figure 23: Created the FTP Brute force session on the Metasploitable 2 machine

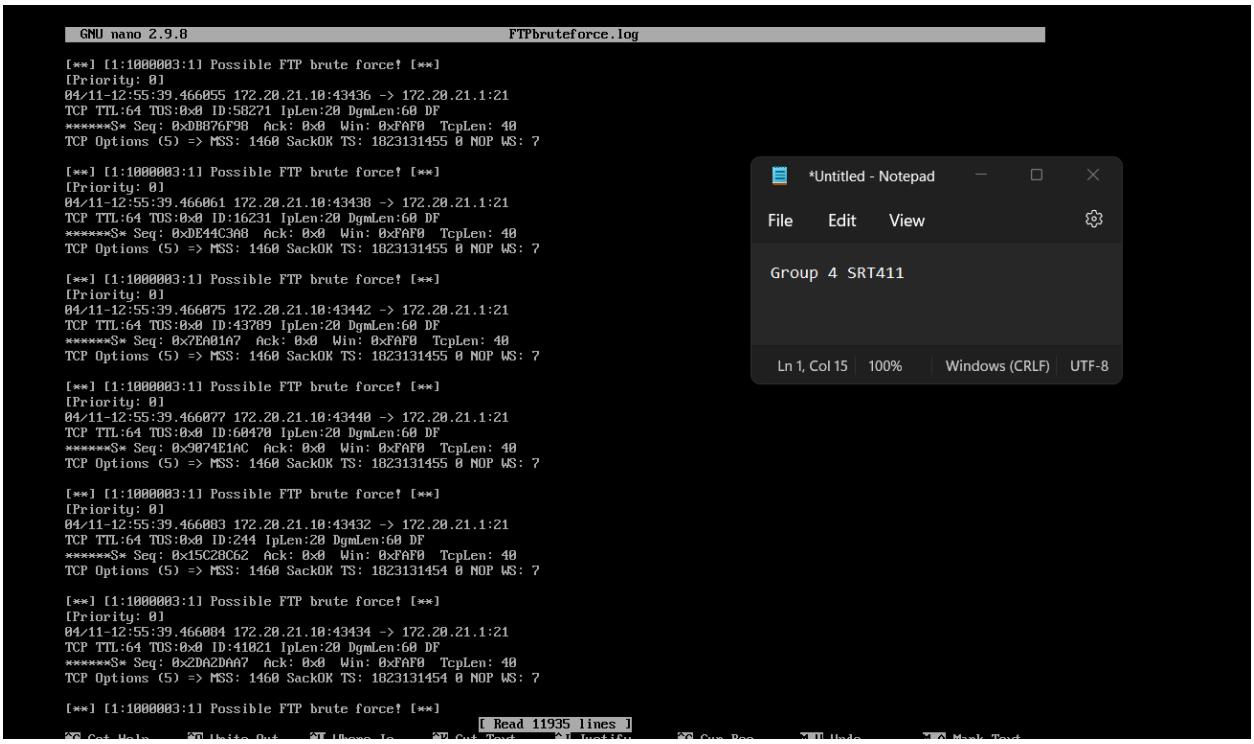


Figure 24: Generated Alerts from the FTP Brute force session

DDoS Session

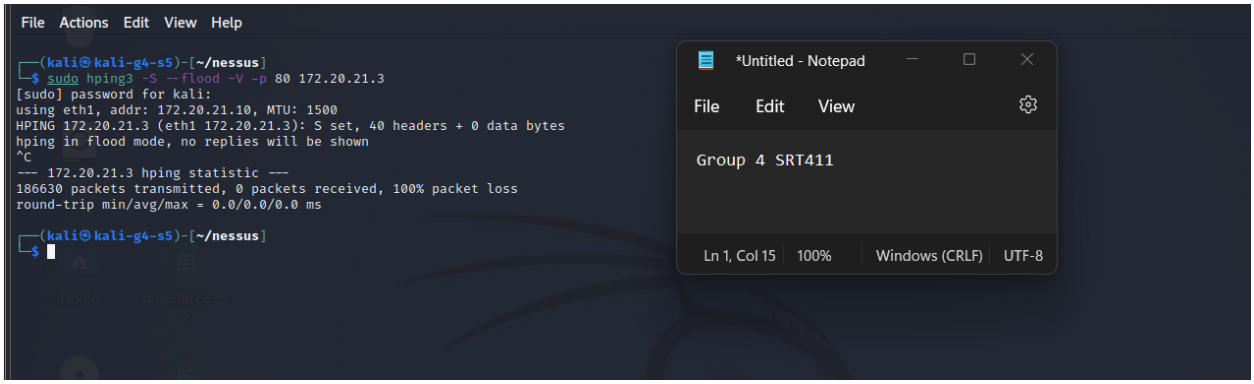


Figure 25: Performing an hping DDoS attack on Machine 4

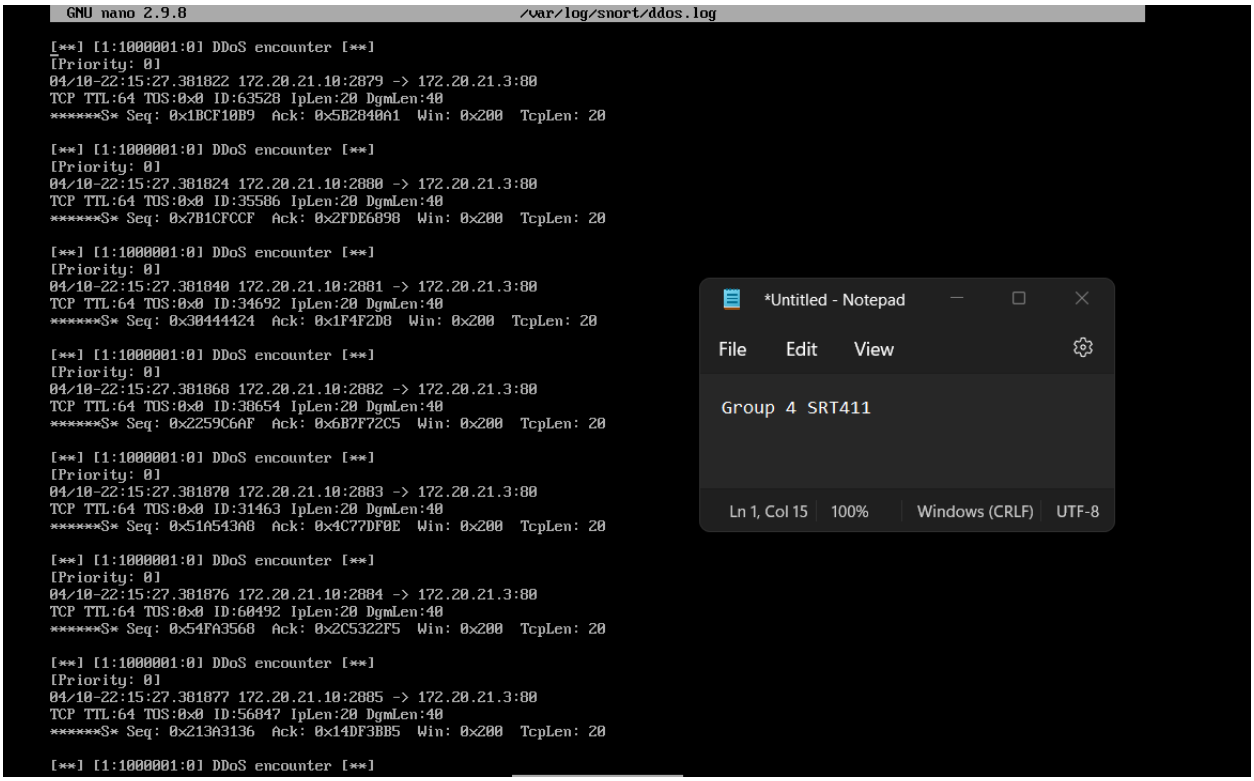


Figure 26: The Generated Logs of the DDoS attack

Any Nmap Scan

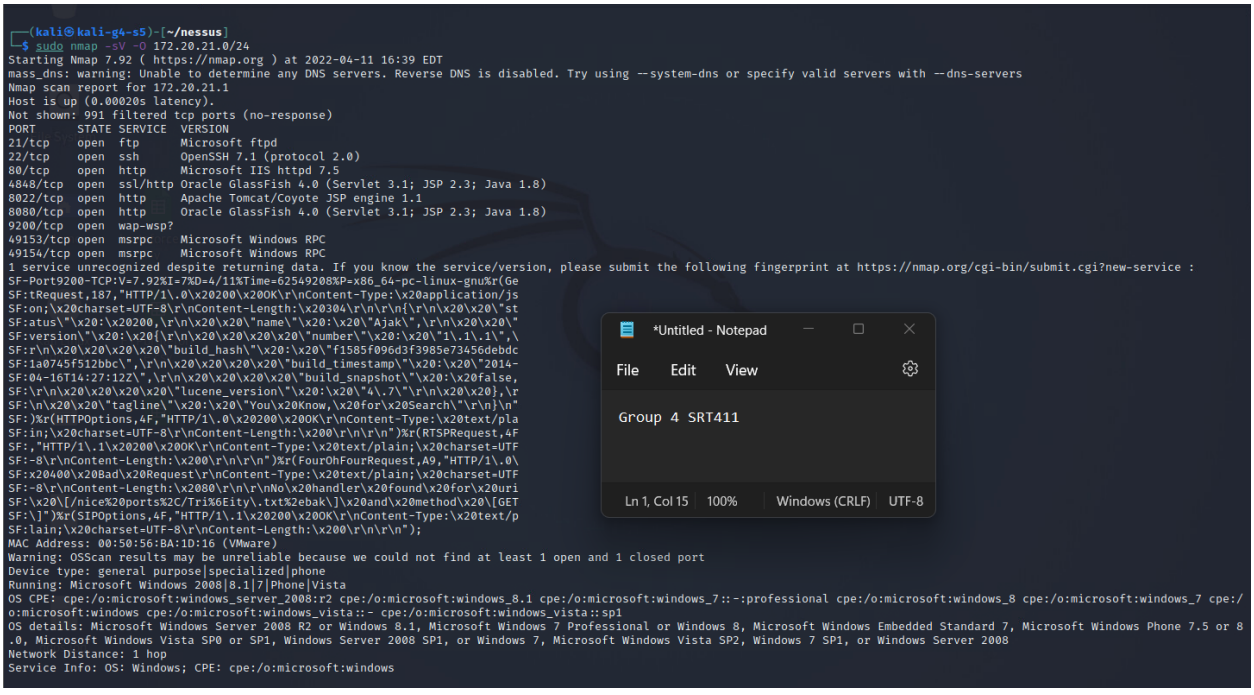


Figure 27: Performing an Nmap Scan on the Network

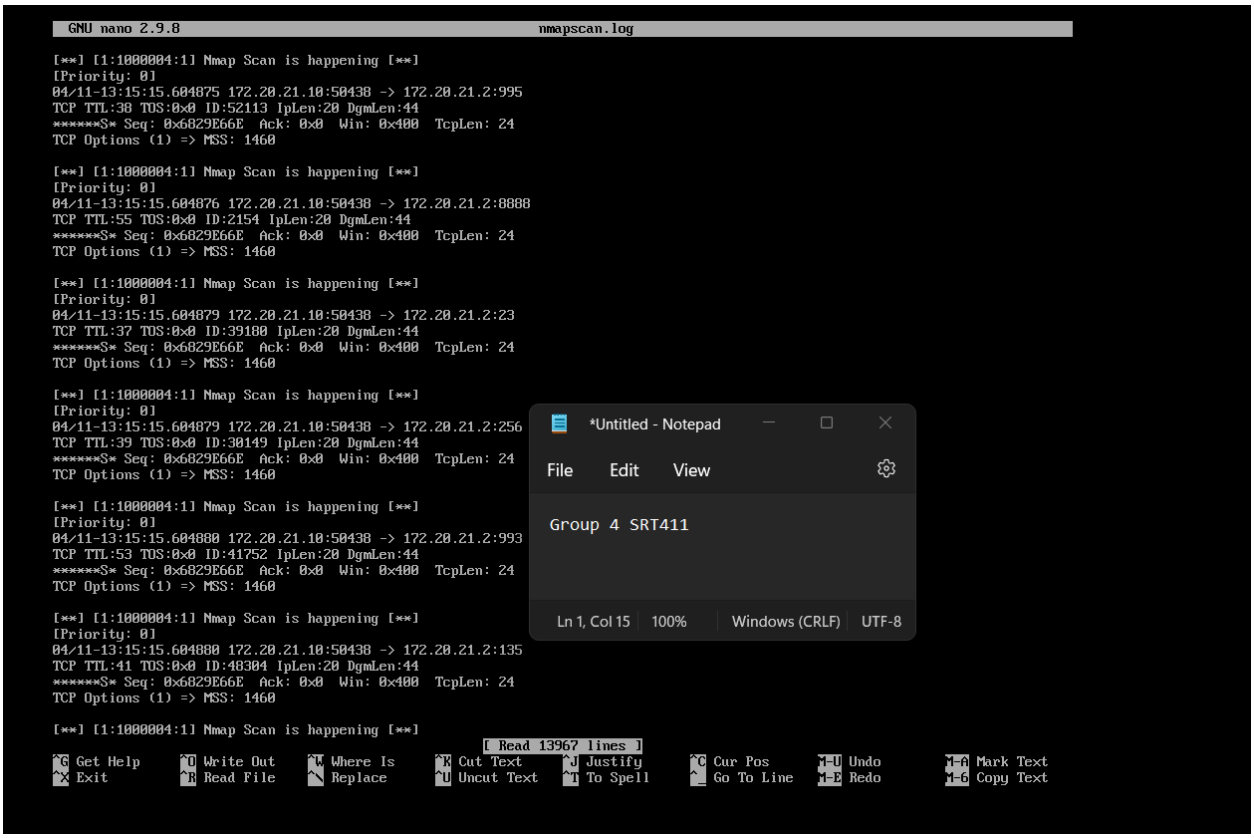


Figure 28: Performed the log collection for the Nmap scans

The Security Goal on this Log collection

The main Security Goal in this Log collection is to identify the importance of an intrusion detection system within a network. This is important mainly because we would not be able to identify any attacks happening within the network and that is the main functionality of snort. Snort detects these suspicious activity present within the Environment through the use of rules that we generated to detect these activities. By collecting the logs of the alerts, we are able to discover the extent of the suspicious activities present.

Vulnerabilities and Threats

Most of the Vulnerabilities and threats found within the Home Lab environment was the improper use of software and having many programs that ahs either exceeded its end of life, which makes them a prime target for attackers to exploit and reach machines. Other Threats where the lack of strong password generation, within the home environment, we were able to discover that most of the machines have week authentication segments which result in the exploitation of them through the use of attacks such as Brute-Force attacks.

How the collected Data would help me reach the goal

The collected Data will have a significant amount for us to reach the target, mainly because we were able to generate CSV files that will be used as logs to generate them in a Visualization platform, mainly for the purpose of understanding the main visualization of the logs collected. So, we can look into the activity and then track down any suspicious behaviours within the collected logs.

The Collected Data and Data Cleaning Techniques

The Collected data will be generated into CSV files, and they will be sent to a new location so that they can be easily Collected to visualize through the use of ELK. In terms of Data Cleaning techniques, we will look into columns with unusual information that might be unreadable, we would not include them into the log collection.

Collected CSV files

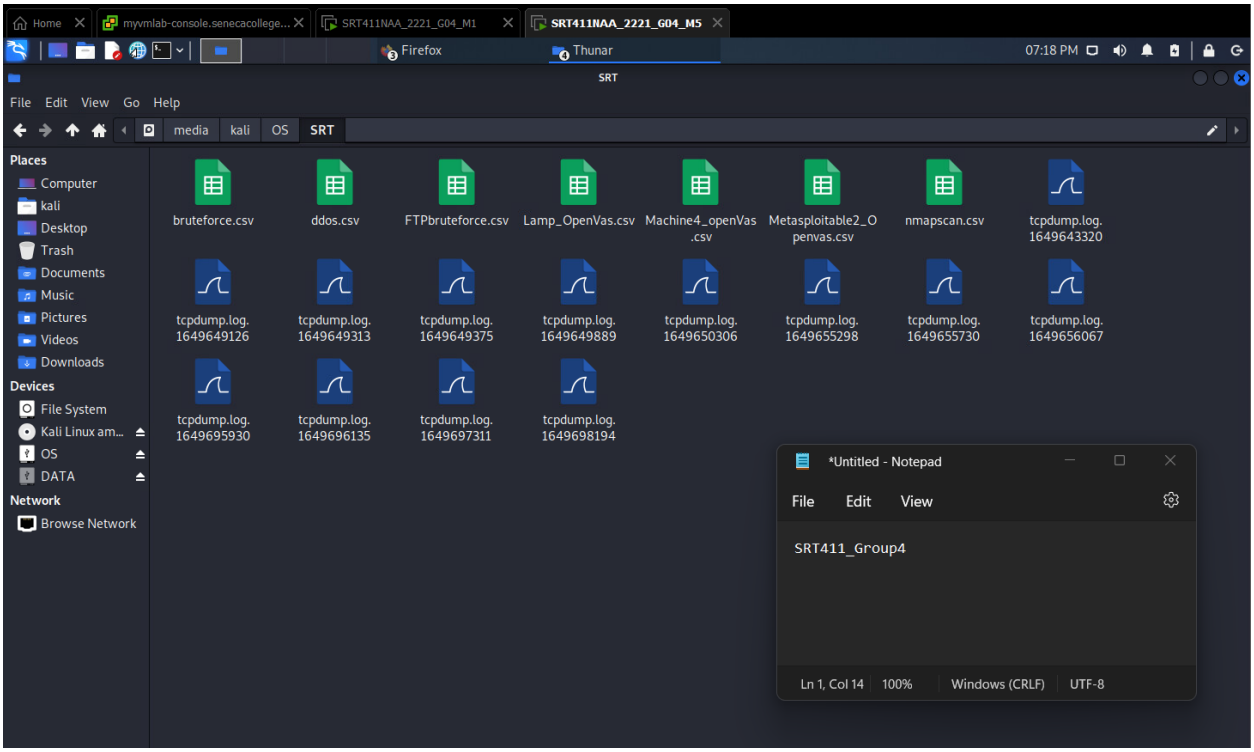
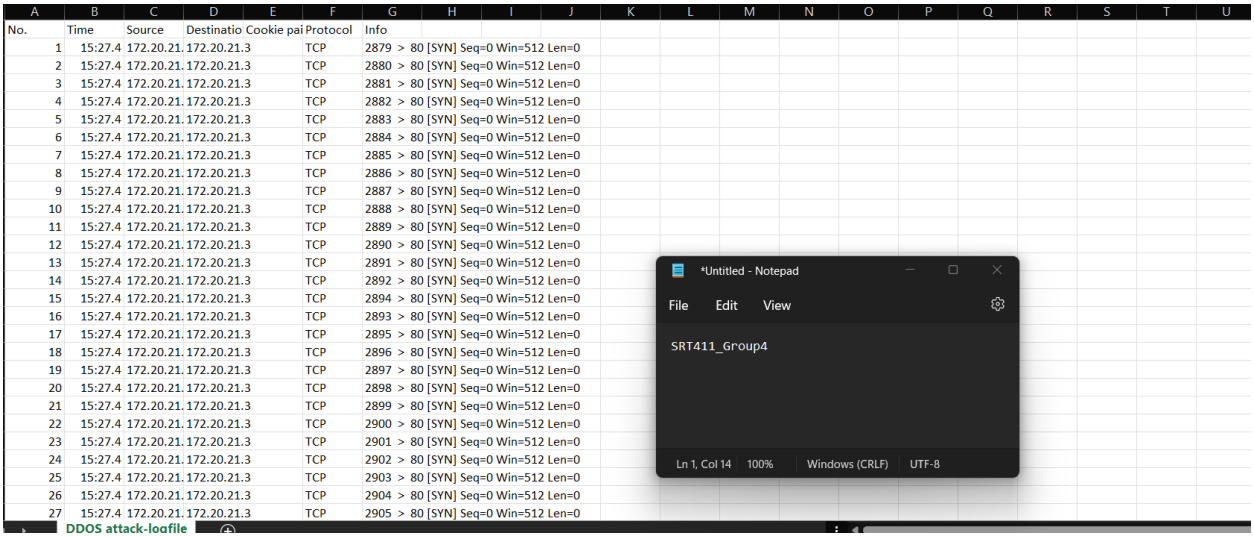


Figure 29: All the generated Alerts, OpenVAS CVEs, and the Snort Log files are generated

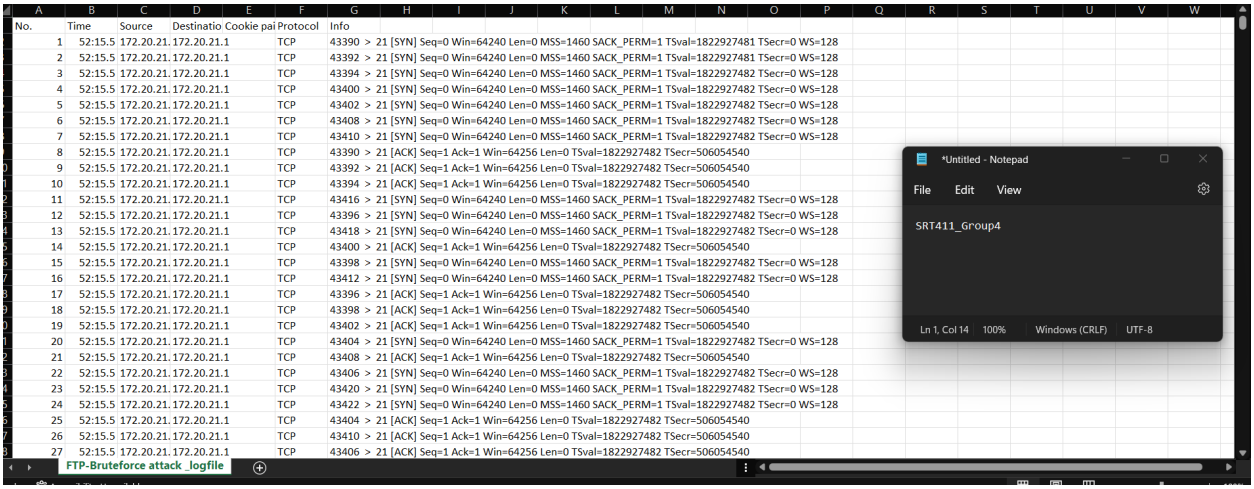
DDoS Attack CSV



No.	Time	Source	Destinatio	Cookie pai	Protocol	Info
1	15:27.4	172.20.21.	172.20.21.3		TCP	2879 > 80 [SYN] Seq=0 Win=512 Len=0
2	15:27.4	172.20.21.	172.20.21.3		TCP	2880 > 80 [SYN] Seq=0 Win=512 Len=0
3	15:27.4	172.20.21.	172.20.21.3		TCP	2881 > 80 [SYN] Seq=0 Win=512 Len=0
4	15:27.4	172.20.21.	172.20.21.3		TCP	2882 > 80 [SYN] Seq=0 Win=512 Len=0
5	15:27.4	172.20.21.	172.20.21.3		TCP	2883 > 80 [SYN] Seq=0 Win=512 Len=0
6	15:27.4	172.20.21.	172.20.21.3		TCP	2884 > 80 [SYN] Seq=0 Win=512 Len=0
7	15:27.4	172.20.21.	172.20.21.3		TCP	2885 > 80 [SYN] Seq=0 Win=512 Len=0
8	15:27.4	172.20.21.	172.20.21.3		TCP	2886 > 80 [SYN] Seq=0 Win=512 Len=0
9	15:27.4	172.20.21.	172.20.21.3		TCP	2887 > 80 [SYN] Seq=0 Win=512 Len=0
10	15:27.4	172.20.21.	172.20.21.3		TCP	2888 > 80 [SYN] Seq=0 Win=512 Len=0
11	15:27.4	172.20.21.	172.20.21.3		TCP	2889 > 80 [SYN] Seq=0 Win=512 Len=0
12	15:27.4	172.20.21.	172.20.21.3		TCP	2890 > 80 [SYN] Seq=0 Win=512 Len=0
13	15:27.4	172.20.21.	172.20.21.3		TCP	2891 > 80 [SYN] Seq=0 Win=512 Len=0
14	15:27.4	172.20.21.	172.20.21.3		TCP	2892 > 80 [SYN] Seq=0 Win=512 Len=0
15	15:27.4	172.20.21.	172.20.21.3		TCP	2894 > 80 [SYN] Seq=0 Win=512 Len=0
16	15:27.4	172.20.21.	172.20.21.3		TCP	2893 > 80 [SYN] Seq=0 Win=512 Len=0
17	15:27.4	172.20.21.	172.20.21.3		TCP	2895 > 80 [SYN] Seq=0 Win=512 Len=0
18	15:27.4	172.20.21.	172.20.21.3		TCP	2896 > 80 [SYN] Seq=0 Win=512 Len=0
19	15:27.4	172.20.21.	172.20.21.3		TCP	2897 > 80 [SYN] Seq=0 Win=512 Len=0
20	15:27.4	172.20.21.	172.20.21.3		TCP	2898 > 80 [SYN] Seq=0 Win=512 Len=0
21	15:27.4	172.20.21.	172.20.21.3		TCP	2899 > 80 [SYN] Seq=0 Win=512 Len=0
22	15:27.4	172.20.21.	172.20.21.3		TCP	2900 > 80 [SYN] Seq=0 Win=512 Len=0
23	15:27.4	172.20.21.	172.20.21.3		TCP	2901 > 80 [SYN] Seq=0 Win=512 Len=0
24	15:27.4	172.20.21.	172.20.21.3		TCP	2902 > 80 [SYN] Seq=0 Win=512 Len=0
25	15:27.4	172.20.21.	172.20.21.3		TCP	2903 > 80 [SYN] Seq=0 Win=512 Len=0
26	15:27.4	172.20.21.	172.20.21.3		TCP	2904 > 80 [SYN] Seq=0 Win=512 Len=0
27	15:27.4	172.20.21.	172.20.21.3		TCP	2905 > 80 [SYN] Seq=0 Win=512 Len=0

Figure 30: DDoS CSV

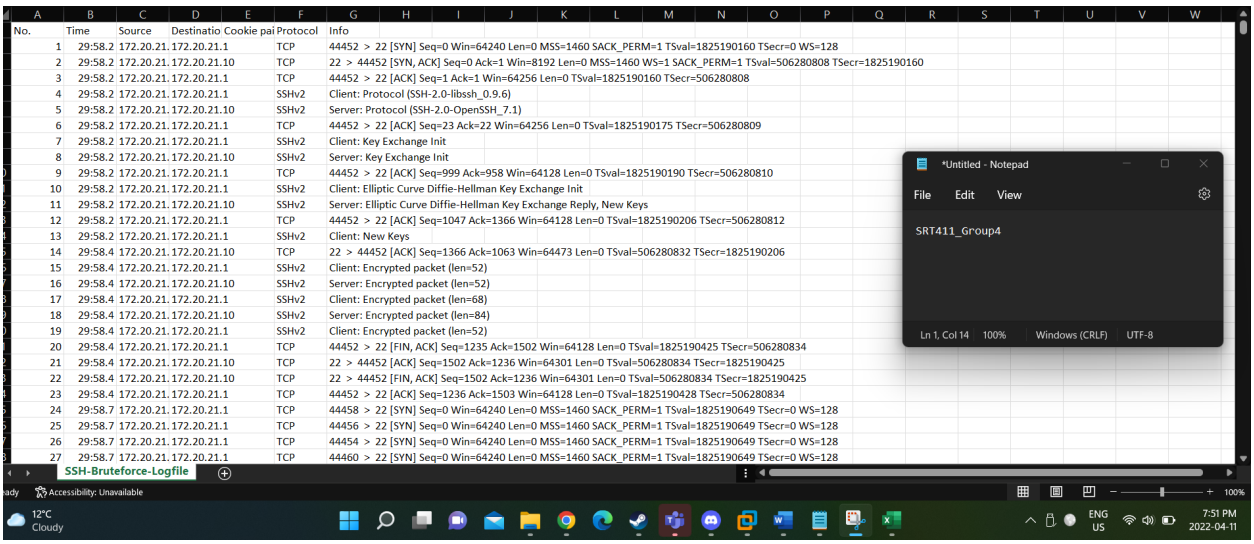
FTP Brute force



No.	Time	Source	Destinatio	Cookie pai	Protocol	Info
1	52:15.5	172.20.21.	172.20.21.1		TCP	43390 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927481 TSecr=0 WS=128
2	52:15.5	172.20.21.	172.20.21.1		TCP	43392 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927481 TSecr=0 WS=128
3	52:15.5	172.20.21.	172.20.21.1		TCP	43394 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
4	52:15.5	172.20.21.	172.20.21.1		TCP	43400 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
5	52:15.5	172.20.21.	172.20.21.1		TCP	43402 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
6	52:15.5	172.20.21.	172.20.21.1		TCP	43408 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
7	52:15.5	172.20.21.	172.20.21.1		TCP	43410 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
8	52:15.5	172.20.21.	172.20.21.1		TCP	43390 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540
9	52:15.5	172.20.21.	172.20.21.1		TCP	43392 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540
10	52:15.5	172.20.21.	172.20.21.1		TCP	43394 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540
11	52:15.5	172.20.21.	172.20.21.1		TCP	43416 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
12	52:15.5	172.20.21.	172.20.21.1		TCP	43396 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
13	52:15.5	172.20.21.	172.20.21.1		TCP	43418 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
14	52:15.5	172.20.21.	172.20.21.1		TCP	43400 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540
15	52:15.5	172.20.21.	172.20.21.1		TCP	43398 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
16	52:15.5	172.20.21.	172.20.21.1		TCP	43412 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
17	52:15.5	172.20.21.	172.20.21.1		TCP	43396 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540
18	52:15.5	172.20.21.	172.20.21.1		TCP	43398 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540
19	52:15.5	172.20.21.	172.20.21.1		TCP	43402 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540
20	52:15.5	172.20.21.	172.20.21.1		TCP	43404 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
21	52:15.5	172.20.21.	172.20.21.1		TCP	43408 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540
22	52:15.5	172.20.21.	172.20.21.1		TCP	43406 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
23	52:15.5	172.20.21.	172.20.21.1		TCP	43420 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
24	52:15.5	172.20.21.	172.20.21.1		TCP	43422 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1822927482 TSecr=0 WS=128
25	52:15.5	172.20.21.	172.20.21.1		TCP	43404 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540
26	52:15.5	172.20.21.	172.20.21.1		TCP	43410 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540
27	52:15.5	172.20.21.	172.20.21.1		TCP	43406 > 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1822927482 TSecr=506054540

Figure 31: FTP Brute-Force Attack

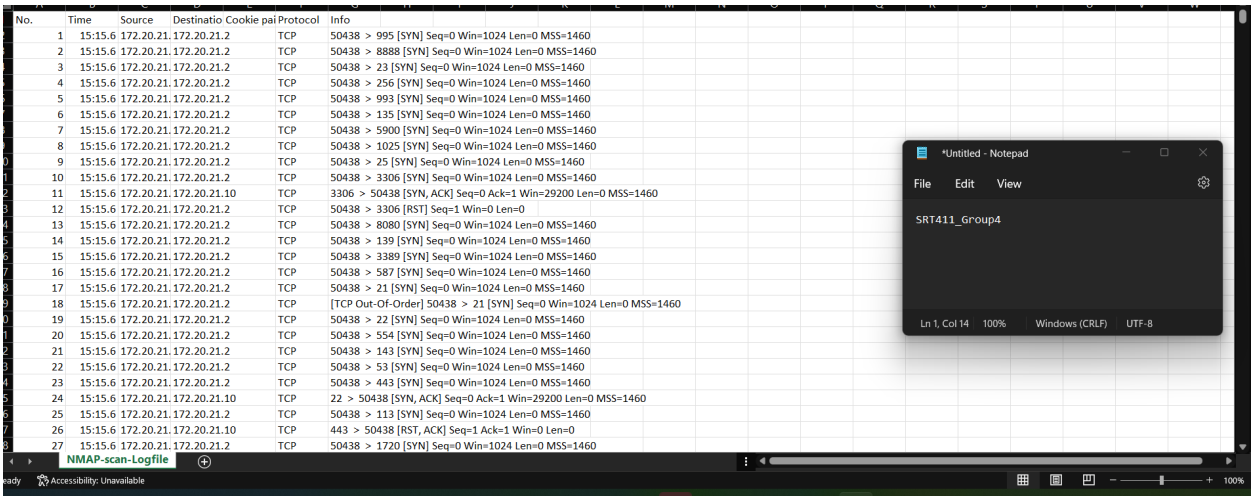
SSH Brute force Attack



No.	Time	Source	Destinatio	Cookie pai	Protocol	Info
1	29:58.2	172.20.21.	172.20.21.1		TCP	44452 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1825190160 TSecr=0 WS=128
2	29:58.2	172.20.21.	172.20.21.10		TCP	22 > 44452 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1 TSval=506280808 TSecr=1825190160
3	29:58.2	172.20.21.	172.20.21.1		TCP	44452 > 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1825190160 TSecr=506280808
4	29:58.2	172.20.21.	172.20.21.1		SSHv2	Client: Protocol (SSH-2.0-libssh_0.9.6)
5	29:58.2	172.20.21.	172.20.21.10		SSHv2	Server: Protocol (SSH-2.0-OpenSSH_7.1)
6	29:58.2	172.20.21.	172.20.21.1		TCP	44452 > 22 [ACK] Seq=23 Ack=22 Win=64256 Len=0 TSval=1825190175 TSecr=506280809
7	29:58.2	172.20.21.	172.20.21.1		SSHv2	Client: Key Exchange Init
8	29:58.2	172.20.21.	172.20.21.10		SSHv2	Server: Key Exchange Init
9	29:58.2	172.20.21.	172.20.21.1		TCP	44452 > 22 [ACK] Seq=999 Ack=958 Win=64128 Len=0 TSval=1825190190 TSecr=506280810
10	29:58.2	172.20.21.	172.20.21.1		SSHv2	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
11	29:58.2	172.20.21.	172.20.21.10		SSHv2	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
12	29:58.2	172.20.21.	172.20.21.1		TCP	44452 > 22 [ACK] Seq=1047 Ack=1366 Win=64128 Len=0 TSval=1825190206 TSecr=506280812
13	29:58.2	172.20.21.	172.20.21.1		SSHv2	Client: New Keys
14	29:58.4	172.20.21.	172.20.21.10		TCP	22 > 44452 [ACK] Seq=1366 Ack=1063 Win=64473 Len=0 TSval=506280832 TSecr=1825190206
15	29:58.4	172.20.21.	172.20.21.1		SSHv2	Client: Encrypted packet (len=52)
16	29:58.4	172.20.21.	172.20.21.10		SSHv2	Server: Encrypted packet (len=52)
17	29:58.4	172.20.21.	172.20.21.1		SSHv2	Client: Encrypted packet (len=68)
18	29:58.4	172.20.21.	172.20.21.10		SSHv2	Server: Encrypted packet (len=84)
19	29:58.4	172.20.21.	172.20.21.1		SSHv2	Client: Encrypted packet (len=52)
20	29:58.4	172.20.21.	172.20.21.1		TCP	44452 > 22 [FIN, ACK] Seq=1235 Ack=1502 Win=64128 Len=0 TSval=1825190425 TSecr=506280834
21	29:58.4	172.20.21.	172.20.21.10		TCP	22 > 44452 [ACK] Seq=1502 Ack=1236 Win=64301 Len=0 TSval=506280834 TSecr=1825190425
22	29:58.4	172.20.21.	172.20.21.10		TCP	22 > 44452 [FIN, ACK] Seq=1502 Ack=1236 Win=64301 Len=0 TSval=506280834 TSecr=1825190425
23	29:58.4	172.20.21.	172.20.21.1		TCP	44452 > 22 [ACK] Seq=1236 Ack=1503 Win=64128 Len=0 TSval=1825190428 TSecr=506280834
24	29:58.7	172.20.21.	172.20.21.1		TCP	44458 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1825190649 TSecr=0 WS=128
25	29:58.7	172.20.21.	172.20.21.1		TCP	44456 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1825190649 TSecr=0 WS=128
26	29:58.7	172.20.21.	172.20.21.1		TCP	44454 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1825190649 TSecr=0 WS=128
27	29:58.7	172.20.21.	172.20.21.1		TCP	44460 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1825190649 TSecr=0 WS=128

Figure 32: SSH-Brute Force attack

NMAP scan



No.	Time	Source	Destinatio	Cookie pai	Protocol	Info
1	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	15:15.6	172.20.21.	172.20.21.10		TCP	3306 > 50438 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 3306 [RST] Seq=1 Win=0 Len=0
13	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	15:15.6	172.20.21.	172.20.21.2		TCP	[TCP Out-Of-Order] 50438 > 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	15:15.6	172.20.21.	172.20.21.10		TCP	22 > 50438 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
25	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	15:15.6	172.20.21.	172.20.21.10		TCP	443 > 50438 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	15:15.6	172.20.21.	172.20.21.2		TCP	50438 > 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Figure 33: NMAP Scan

References

https://upcloud.com/community/tutorials/installing-snort-on-centos/

https://www.rapid7.com/blog/post/2016/12/09/understanding-and-configuring-snort-rules/#:~:text=Usually%2C%20Snort%20rules%20were%20written,large%20and%20difficult%20to%20understand.

https://www.researchgate.net/publication/338660054_DETECTING_DDoS_ATTACK_USING_Snort

https://www.clearos.com/clearfoundation/social/community/solved-snort-rule-for-ftp-brute-force