Usman Ahmad

Danyal Bhatti

Alberto Munar

Professor Asma Paracha

SRT411 Digital Data Analysis

March 30th, 2022

Phase 2: Log Collection

Introduction

We have multiple goals for this phase of the project. They include identifying the logs we need to collect from our system built in phase 1. Create users and generate data from them that would be considered normal and malicious. Create logs from the generated traffic and analyze them.

Objective

To achieve our goals within this phase we will run scans and collect the data. We will use Logstash for the collection process. We will create traffic by pinging all the machines and scanning their ports to see what services are running. We will also scan the console looking for files and folders in each machine. We create and run queries using SQLmap on our MySQL server. Lastly, we will show normal traffic such as web browsing and ssh connection as well as malicious traffic through attacks.

Contents

Introduction 1

Objective 1

Information Gathering: 3

NMAP Scans: 3

Greenbone Scanning: 8

Pings 15

Snort: 16

Snort Configuration: 16

Snort Rules: 17

Attacks: 18

DDoS or DoS attack: 19

Snort event Logging for DoS attack: 20

SSH Logins and Brute Force Attacks: 21

Snort Logs and events triggered by SSH Brute force 21

SSH Connection: 22

Snort Pick up of ssh connection: 23

Deep Scan of M1 of each port service and details: 24

Snort collection of data: 24

Security Goals, Vulnerabilities and Threats 25

How Data Collection help you achieve your goal: 25

Explain Data Collection: 25

Data Collection: 26

Brute Force Attack: 26

DDoS Attack: 27

Nmap Scan: 28

Greenbone Scan Results: 29

Snort Files/Logs collected and sent to Kali 30

References 31

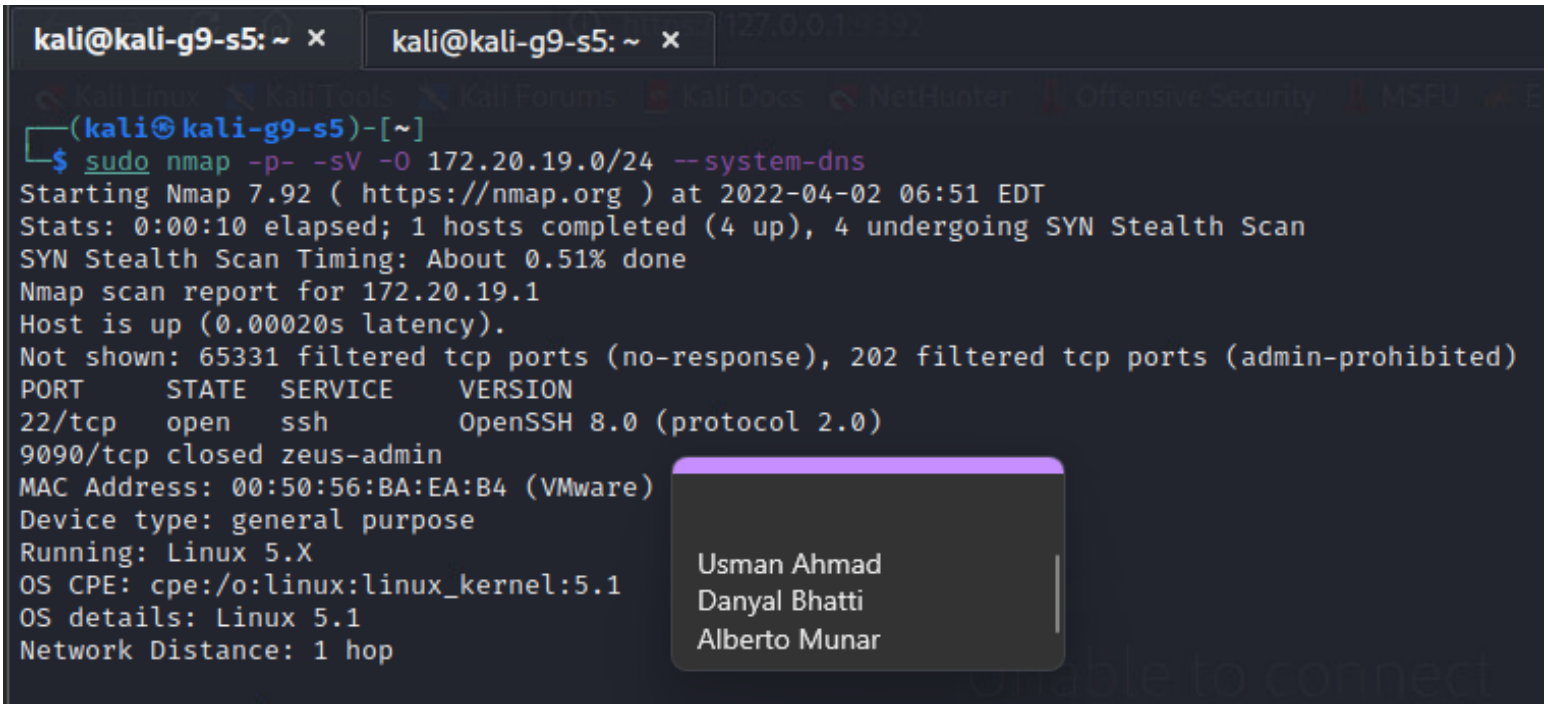
Information Gathering:

NMAP Scans:

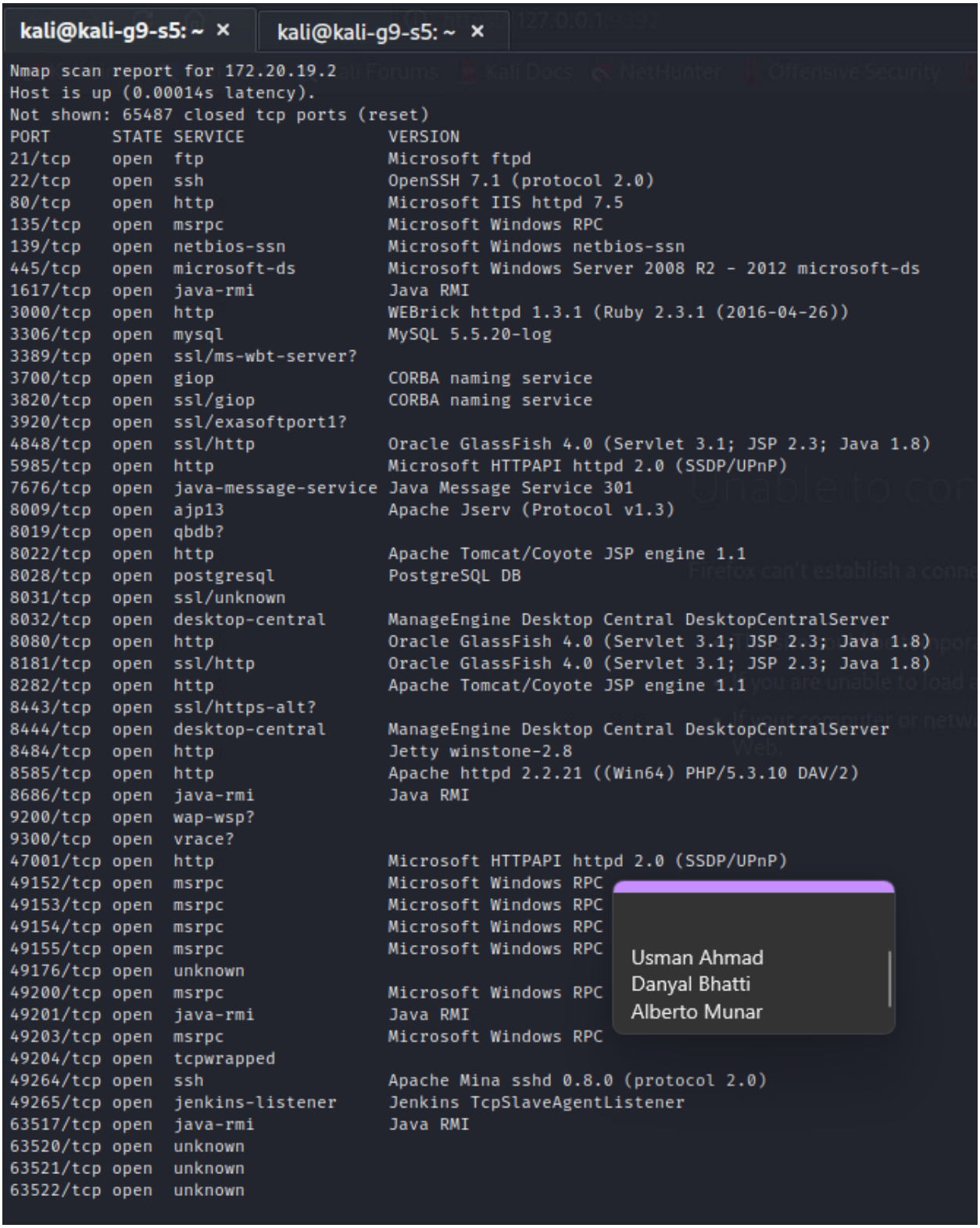
Nmap -p- -sV -O 172.20.19.0/24 --system-dns

172.20.19.1 M1

172.20.21.1 Attack Network



All the Open Ports:

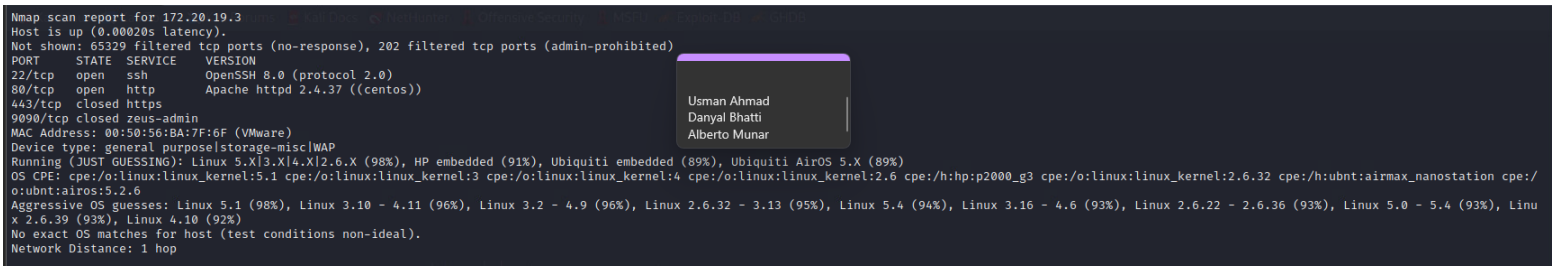


The following is the OS information and other details about the service types and the TCP fingerprint:

```
49176/tcp open  unknown
49200/tcp open  msrpc               Microsoft Windows RPC
49201/tcp open  java-rmi            Java RMI
49203/tcp open  msrpc               Microsoft Windows RPC
49204/tcp open  tcpwrapped
49264/tcp open  ssh                 Apache Mina sshd 0.8.0 (protocol 2.0)
49265/tcp open  jenkins-listener    Jenkins TcpSlaveAgentListener
63517/tcp open  java-rmi            Java RMI
63520/tcp open  unknown
63521/tcp open  unknown
63522/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9200-TCP:V=7.92%I=7%D=4/2%Time=62482BA6%P=x86_64-pc-linux-gnu%r(Get
SF:Request,18A,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20application/jso
SF:n;\x20charset=UTF-8\r\nContent-Length:\x20307\r\n\r\n{\r\n\x20\x20\"sta
SF:tus\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"Doorman\",\r\n\x20\x20
SF:\"version\"\x20:\x20{\r\n\x20\x20\x20\x20\"number\"\x20:\x20\"1\.1\.1\"
SF:,\r\n\x20\x20\x20\x20\"build_hash\"\x20:\x20\"f1585f096d3f3985e73456deb
SF:dc1a0745f512bbc\",\r\n\x20\x20\x20\x20\"build_timestamp\"\x20:\x20\"201
SF:4-04-16T14:27:12Z\",\r\n\x20\x20\x20\x20\"build_snapshot\"\x20:\x20fals
SF:e,\r\n\x20\x20\x20\x20\"lucene_version\"\x20:\x20\"4\.7\"\r\n\x20\x20},
SF:\r\n\x20\x20\"tagline\"\x20:\x20\"You\x20Know,\x20for\x20Search\"\r\n}\
SF:n")%r(HTTPOptions,4F,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20text/p
SF:lain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,
SF:4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20charset=U
SF:TF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,A9,"HTTP/1\.
SF:0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=U
SF:TF-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20found\x20for\x20u
SF:ri\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\x20and\x20method\x20\[G
SF:ET\]")%r(SIPOptions,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text
SF:/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
MAC Address: 00:50:56:BA:09:7B (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; Device: remote management; CPE: cpe:/o:microsoft:windows
```

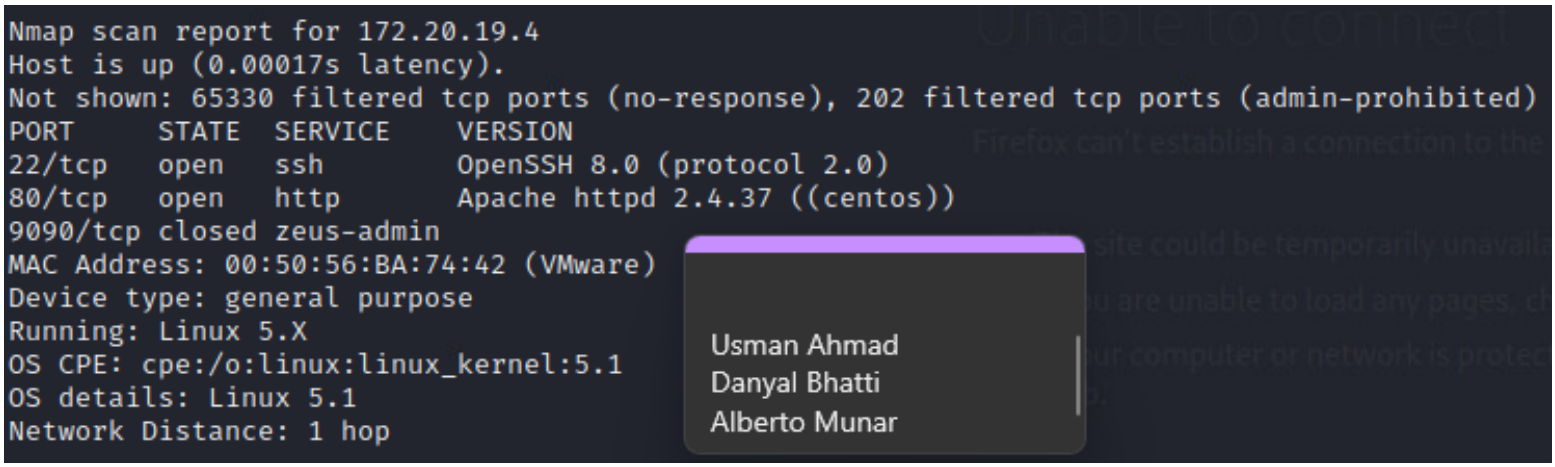
172.20.19.3 M3:

172.20.21.3 Attack Network



172.20.19.4 M4:

172.20.21.4 Attack Network



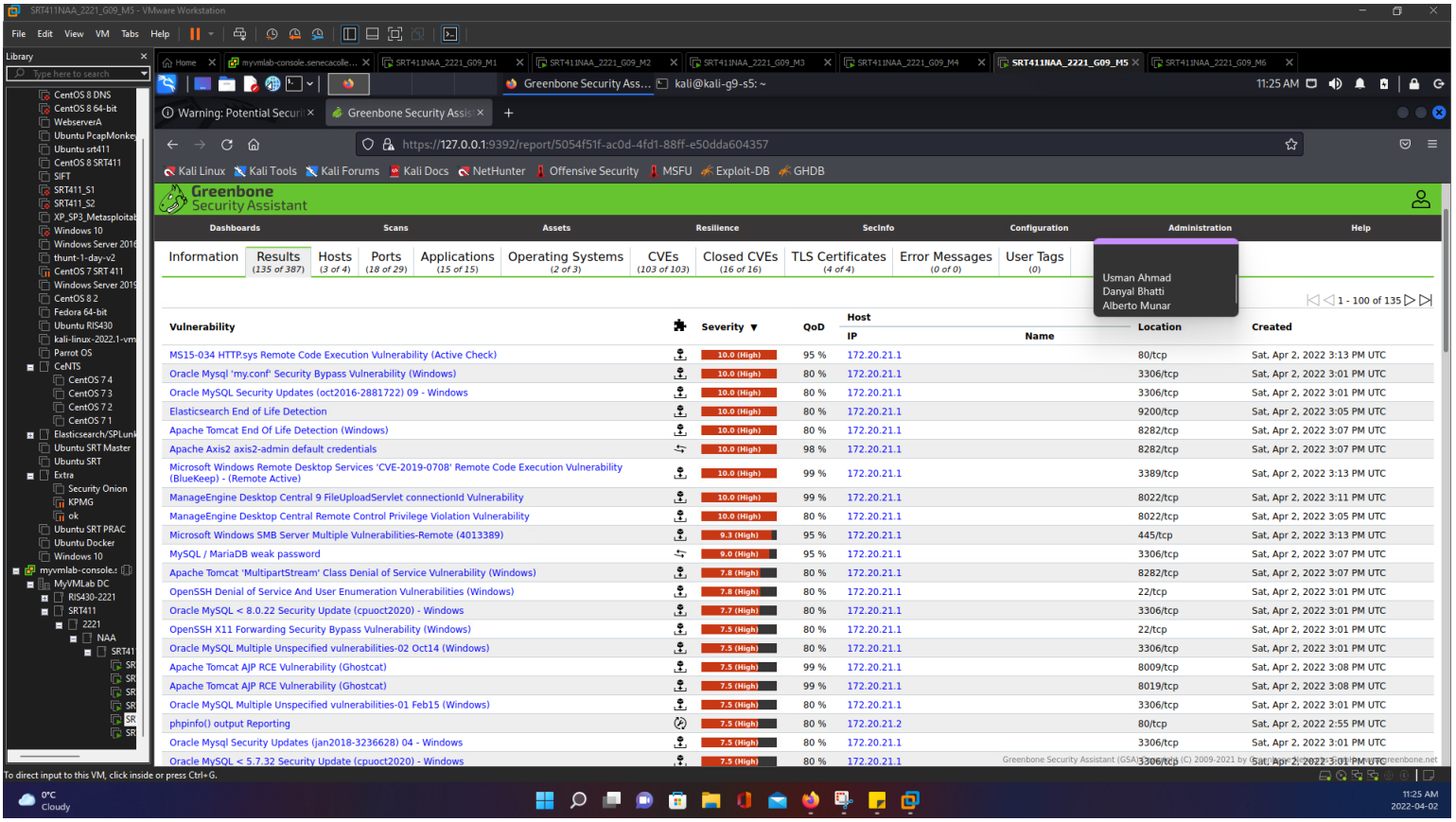
172.20.19.5 M5:

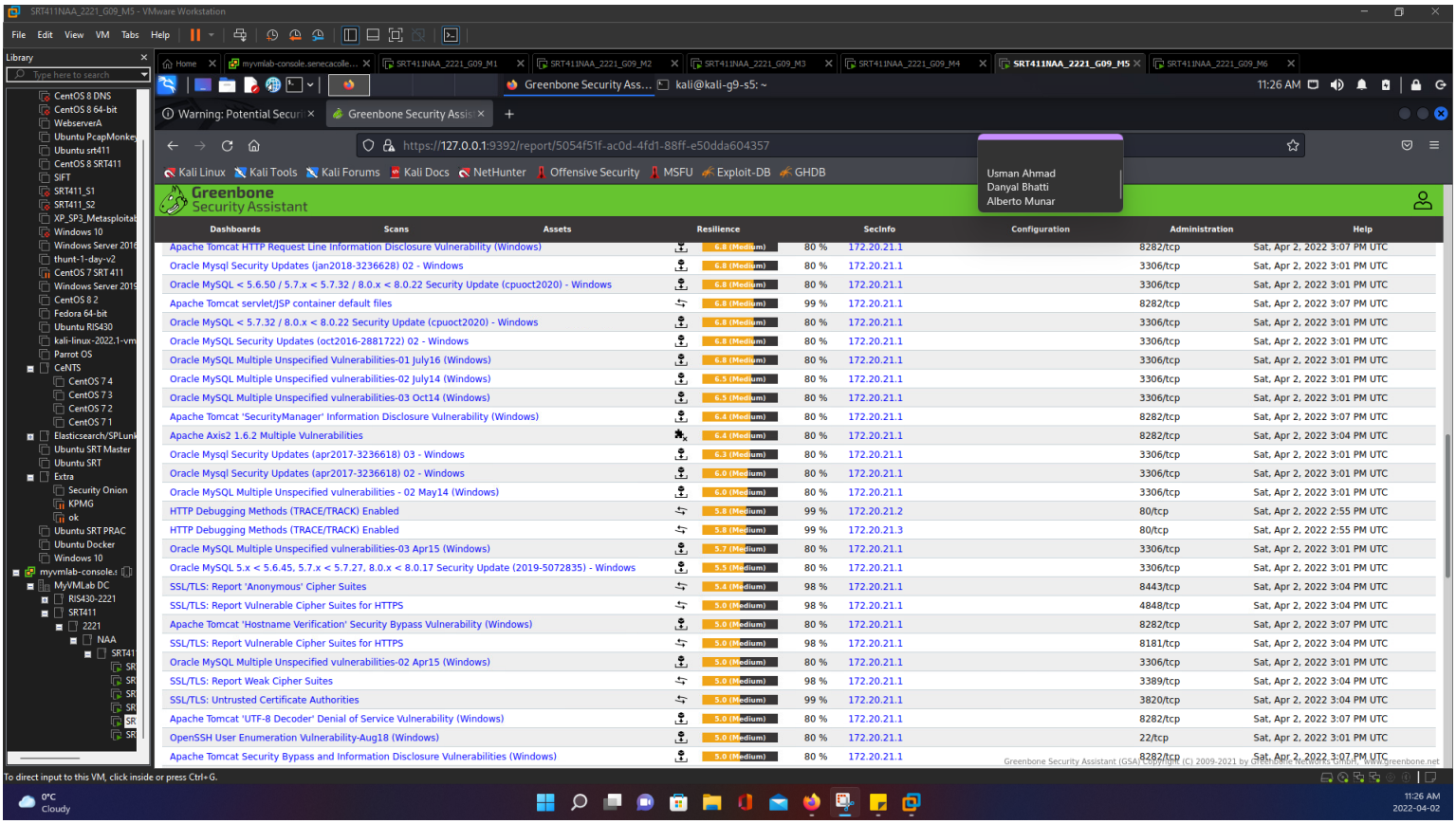
```
Nmap scan report for 172.20.19.5
Host is up (0.00014s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:50:56:BA:E5:66 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=4/2%OT=135%CT=1%CU=31928%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=62482D10%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=111%TI=I%CI=I%II=I%
OS:SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5
OS:B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
OS:ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=
OS:80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=
OS:A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=80%CD=Z)

Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

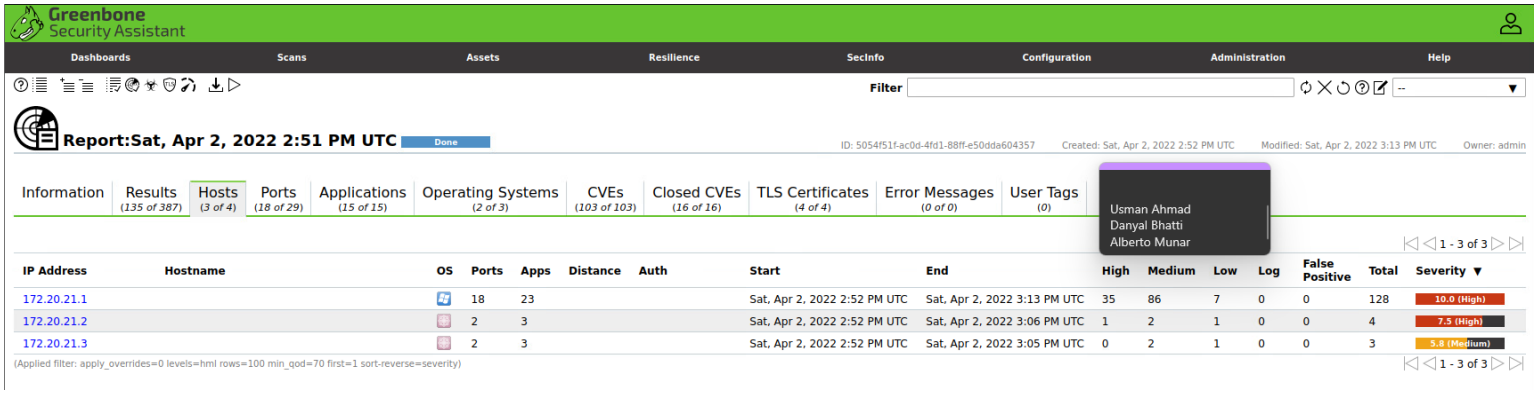
Greenbone Scanning:

The Screenshots below show the Vulnerabilities found over the systems on the network. These scans were performed on the Attack Network Interface. There were three Hosts detected.



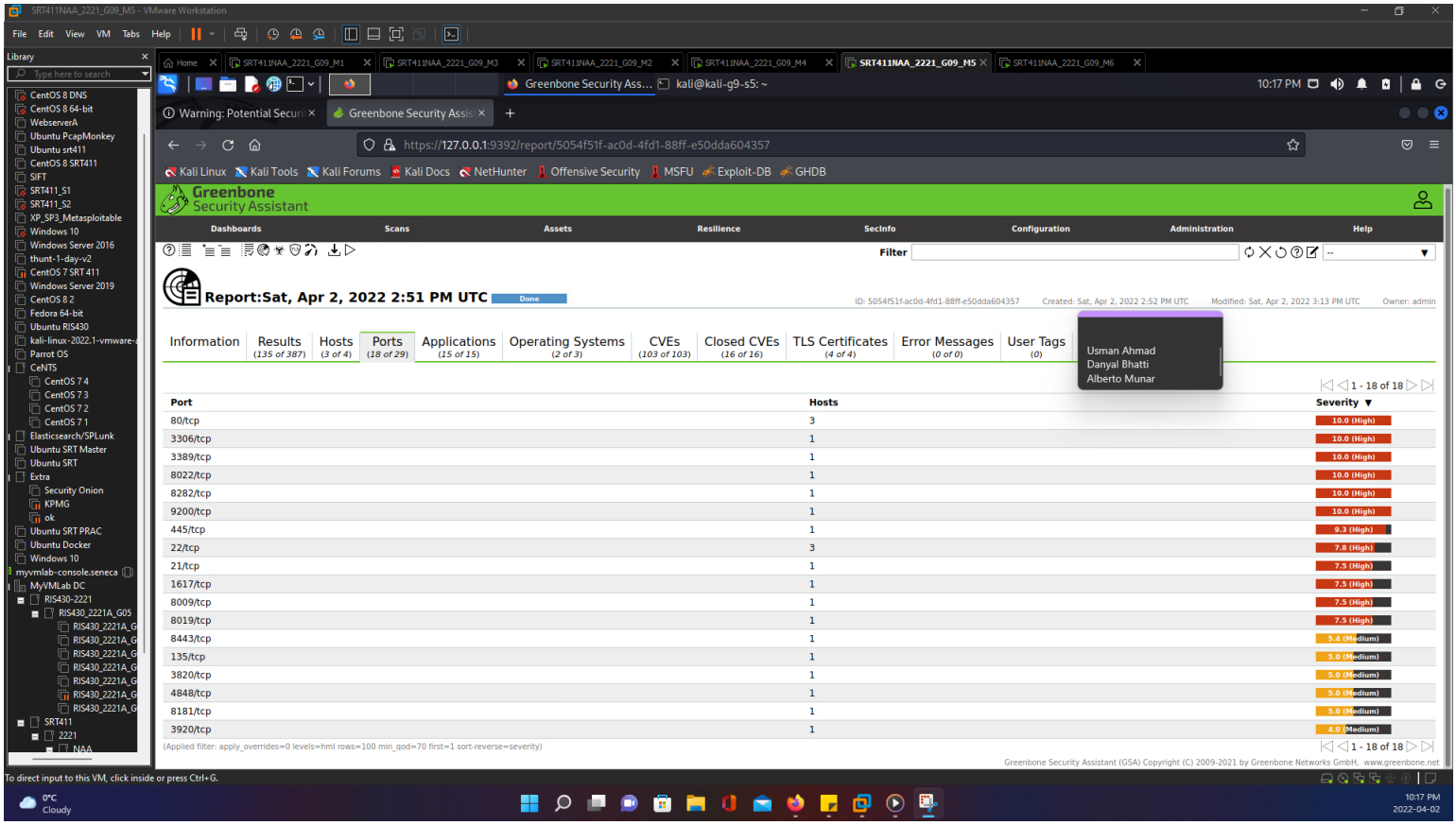


The following Hosts were

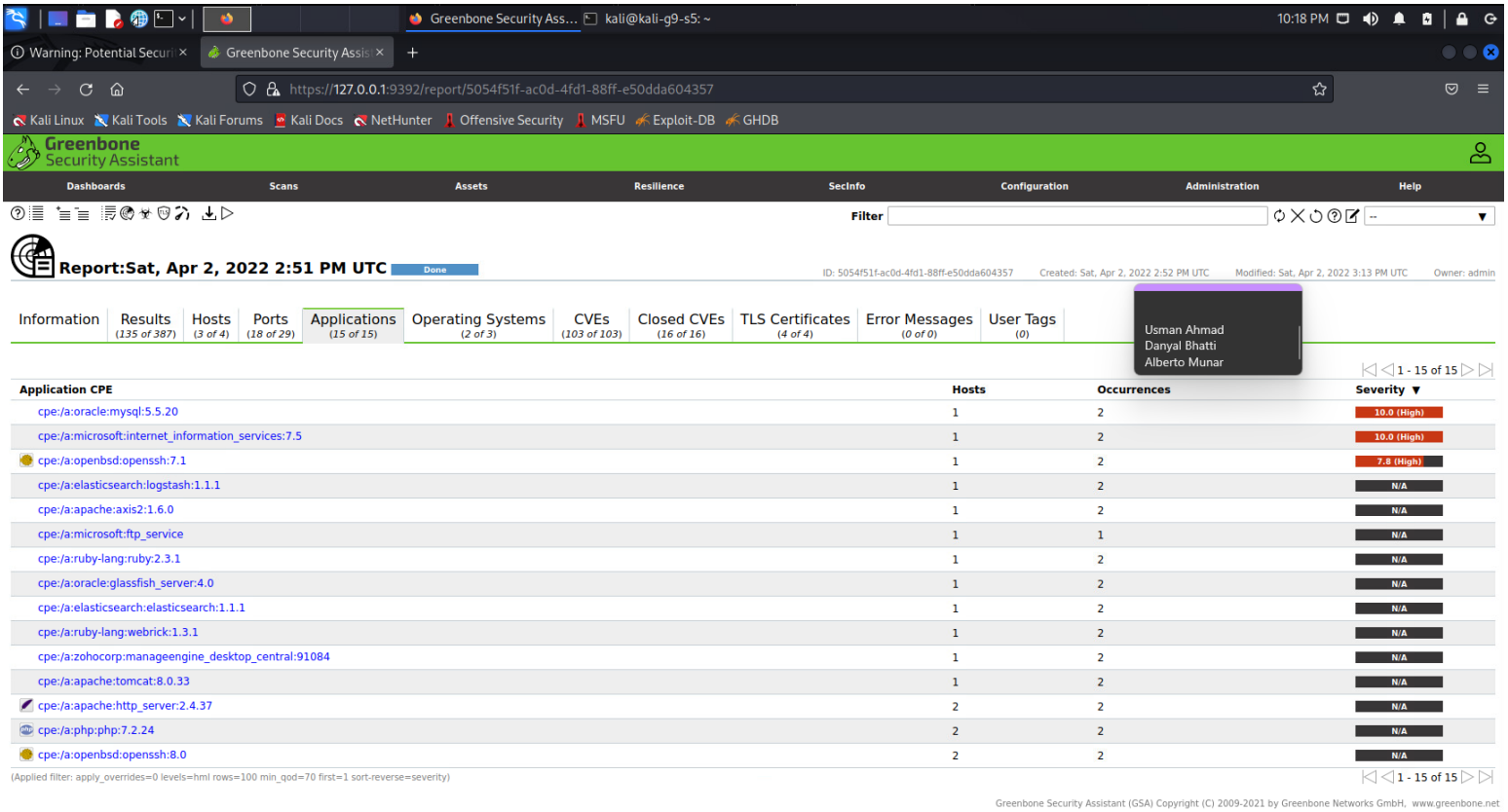


IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity
172.20.21.1			18	23			Sat, Apr 2, 2022 2:52 PM UTC	Sat, Apr 2, 2022 3:13 PM UTC	35	86	7	0	0	128	10.0 (High)
172.20.21.2			2	3			Sat, Apr 2, 2022 2:52 PM UTC	Sat, Apr 2, 2022 3:06 PM UTC	1	2	1	0	0	4	7.5 (High)
172.20.21.3			2	3			Sat, Apr 2, 2022 2:52 PM UTC	Sat, Apr 2, 2022 3:05 PM UTC	0	2	1	0	0	3	5.8 (Medium)

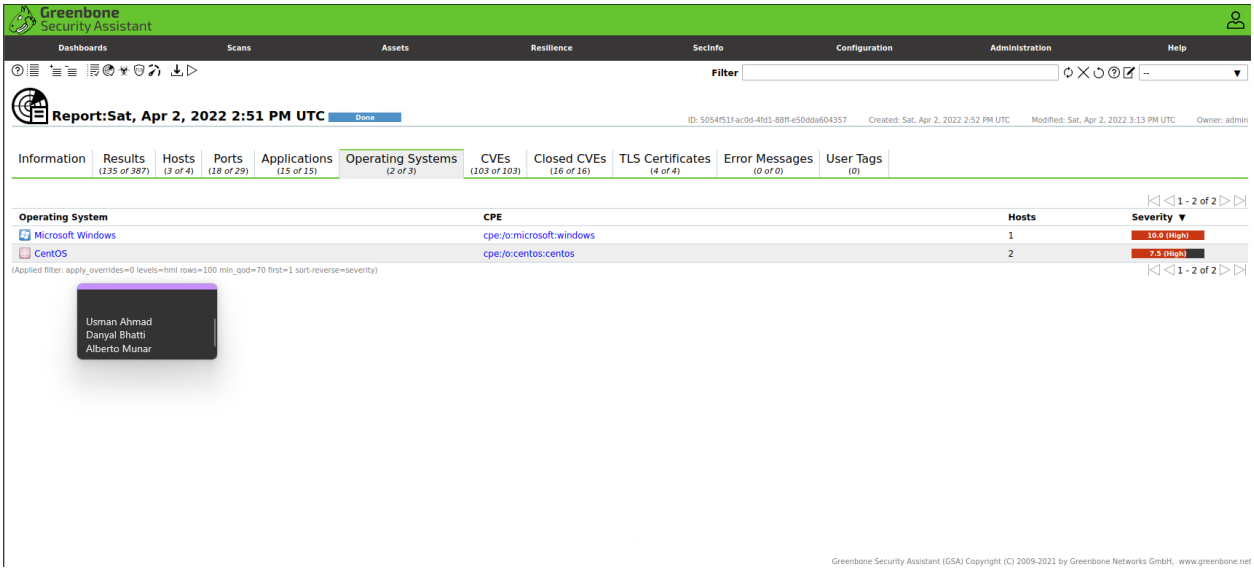
The Ports found from The Greenbone Scan:



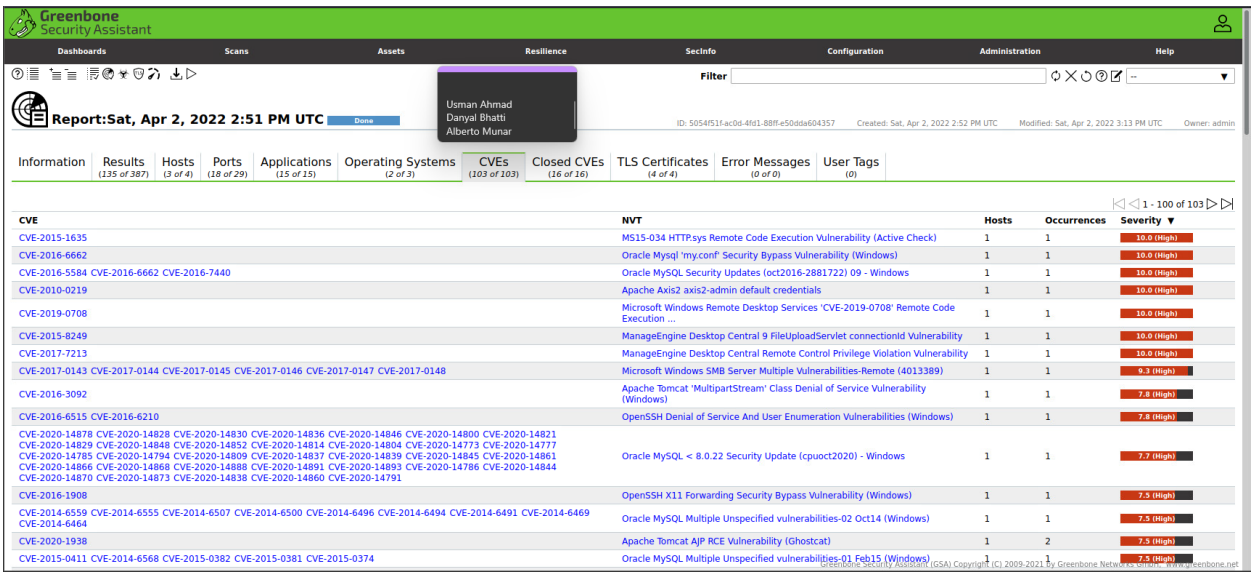
Applications:



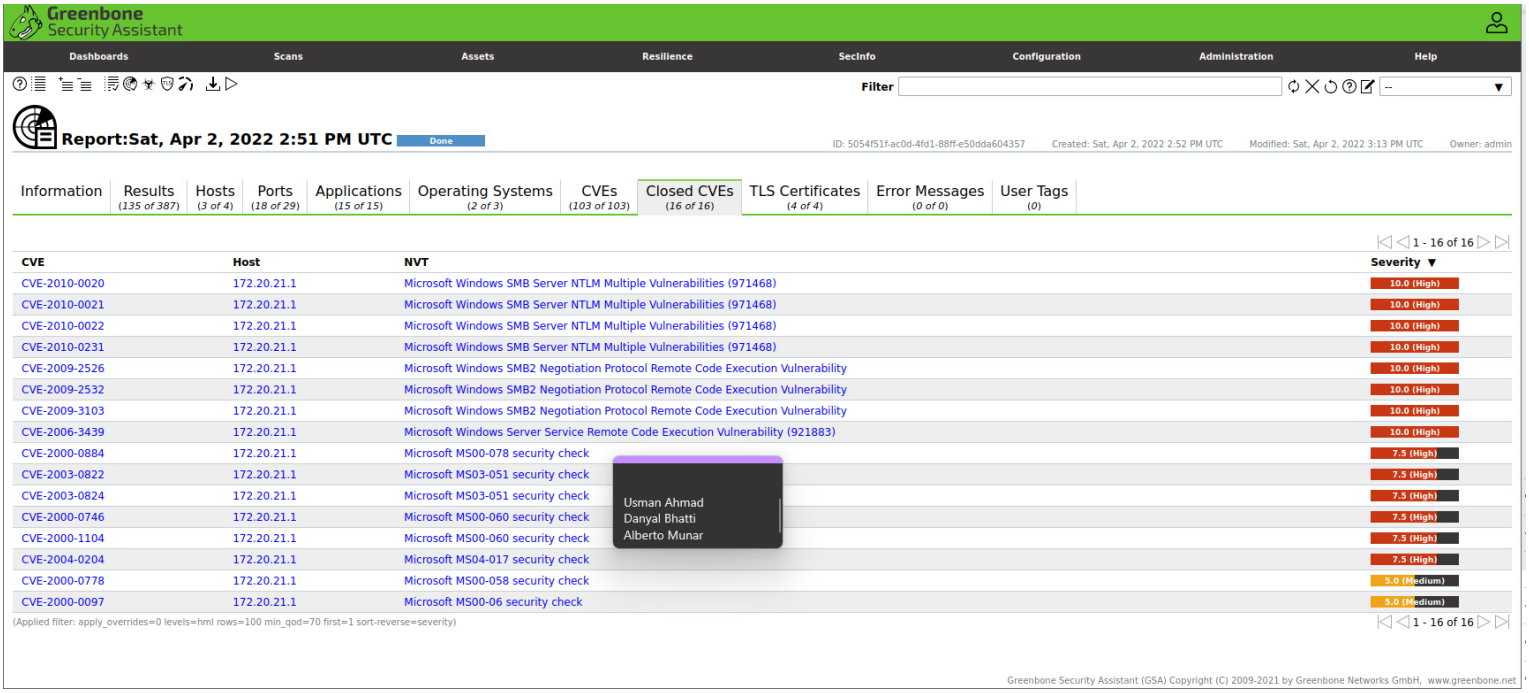
Operating Systems:



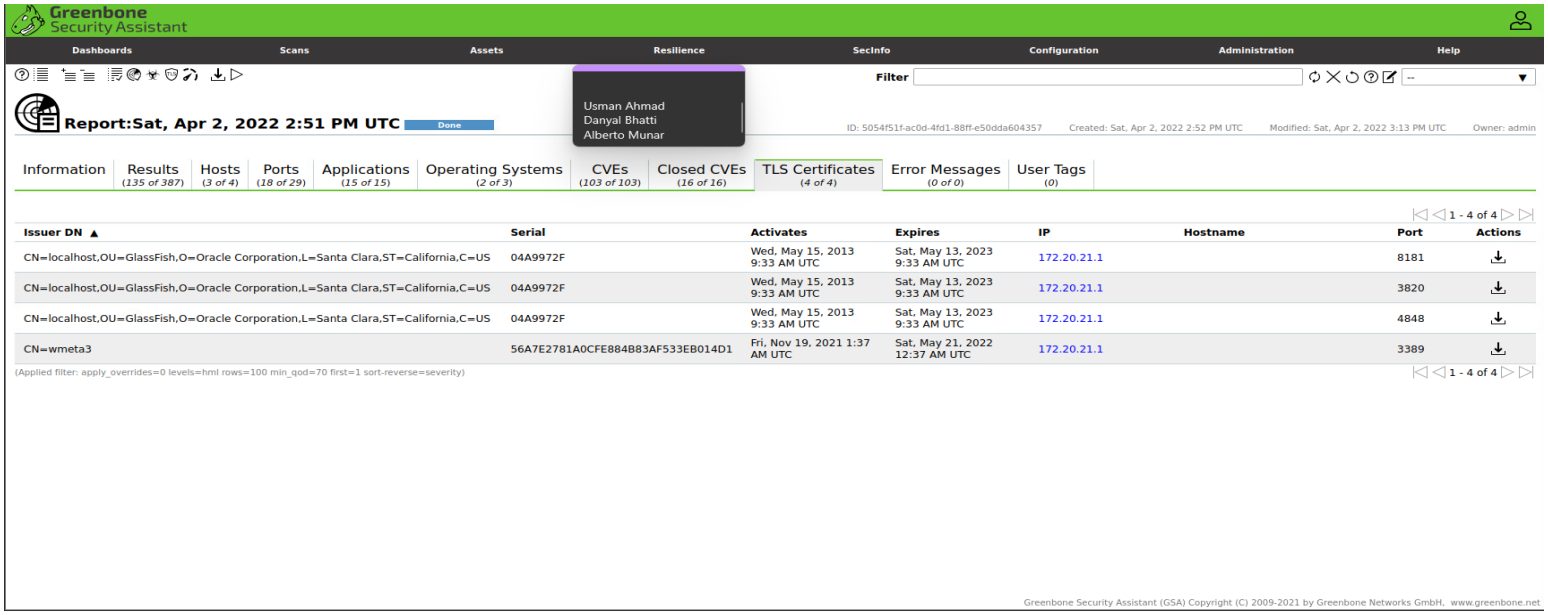
CVEs:



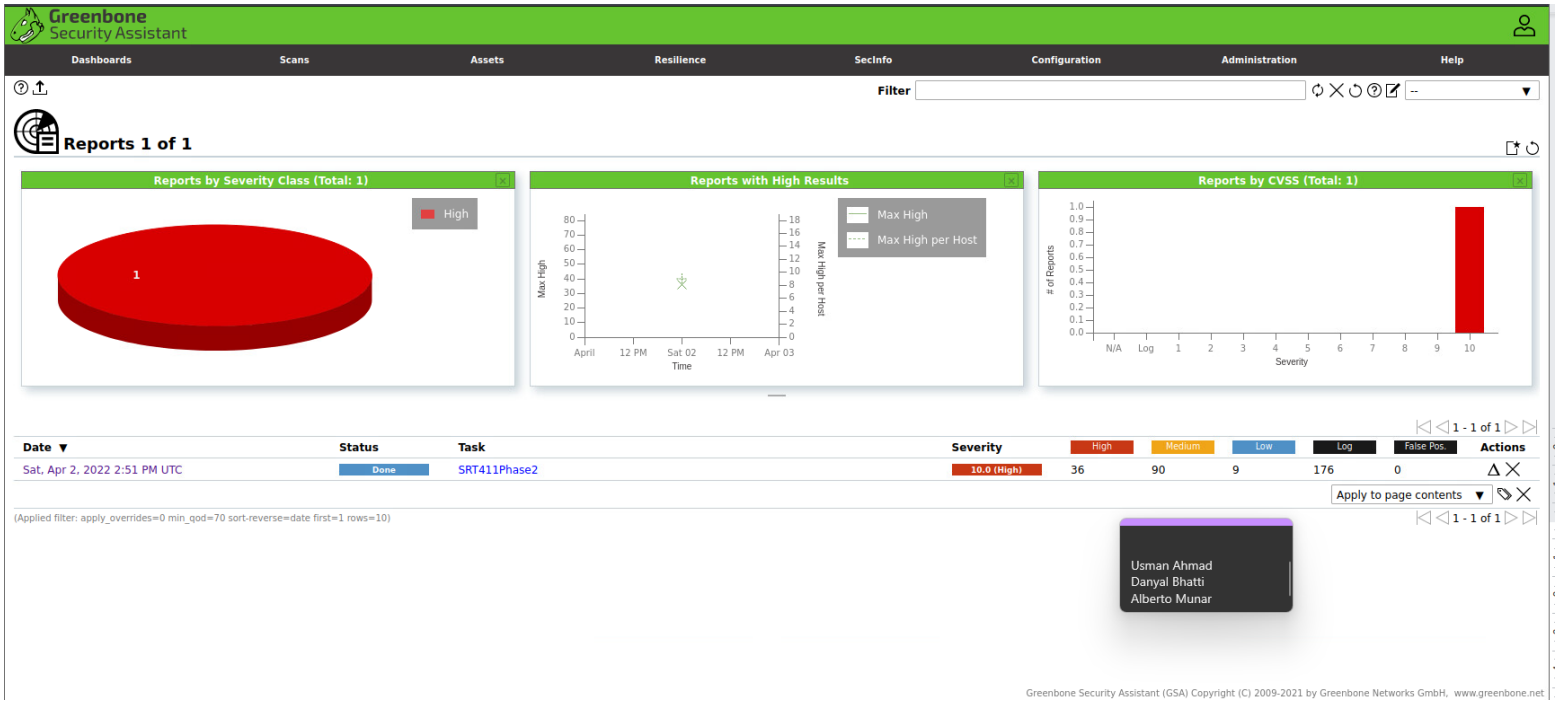
Closed CVE's:



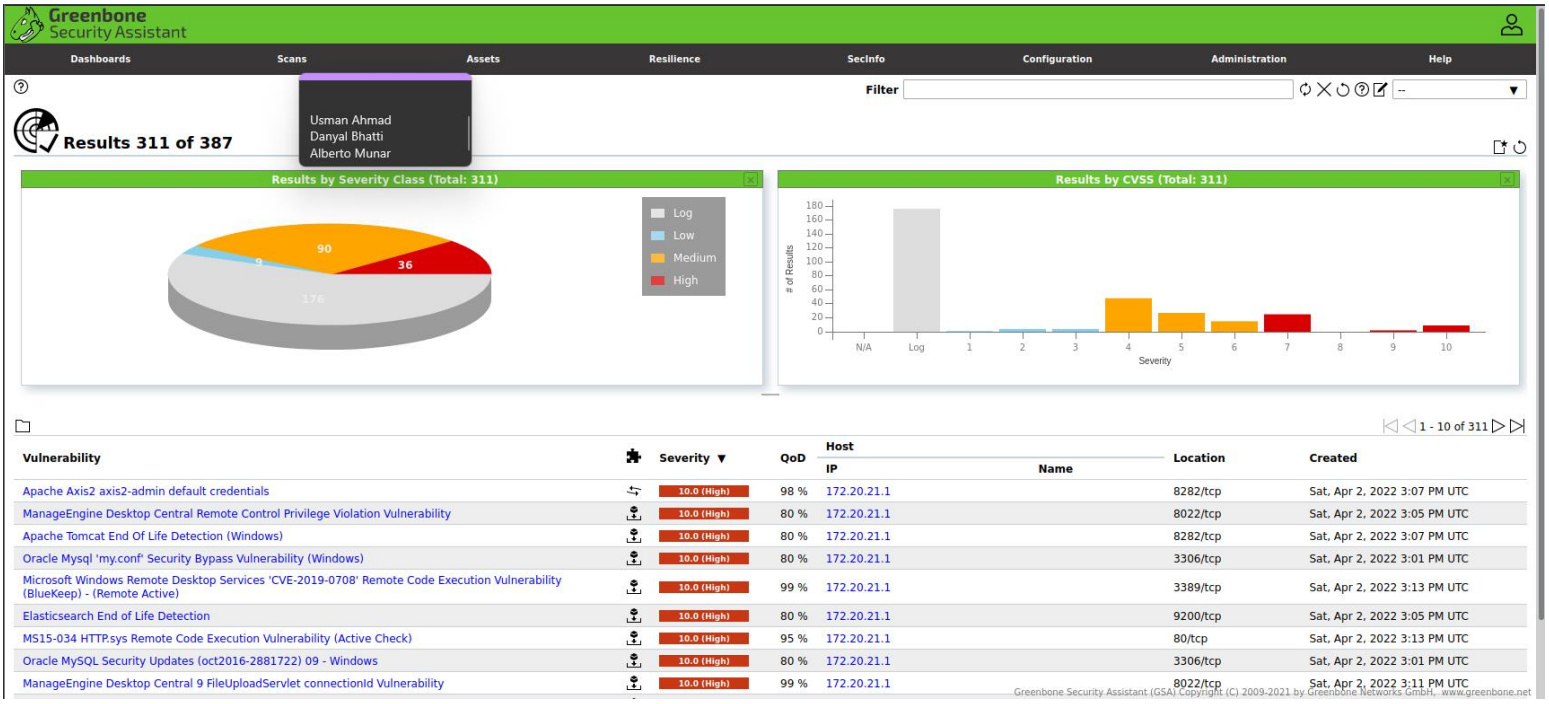
TLS Certificates:



The total Report for the scan of the Network:



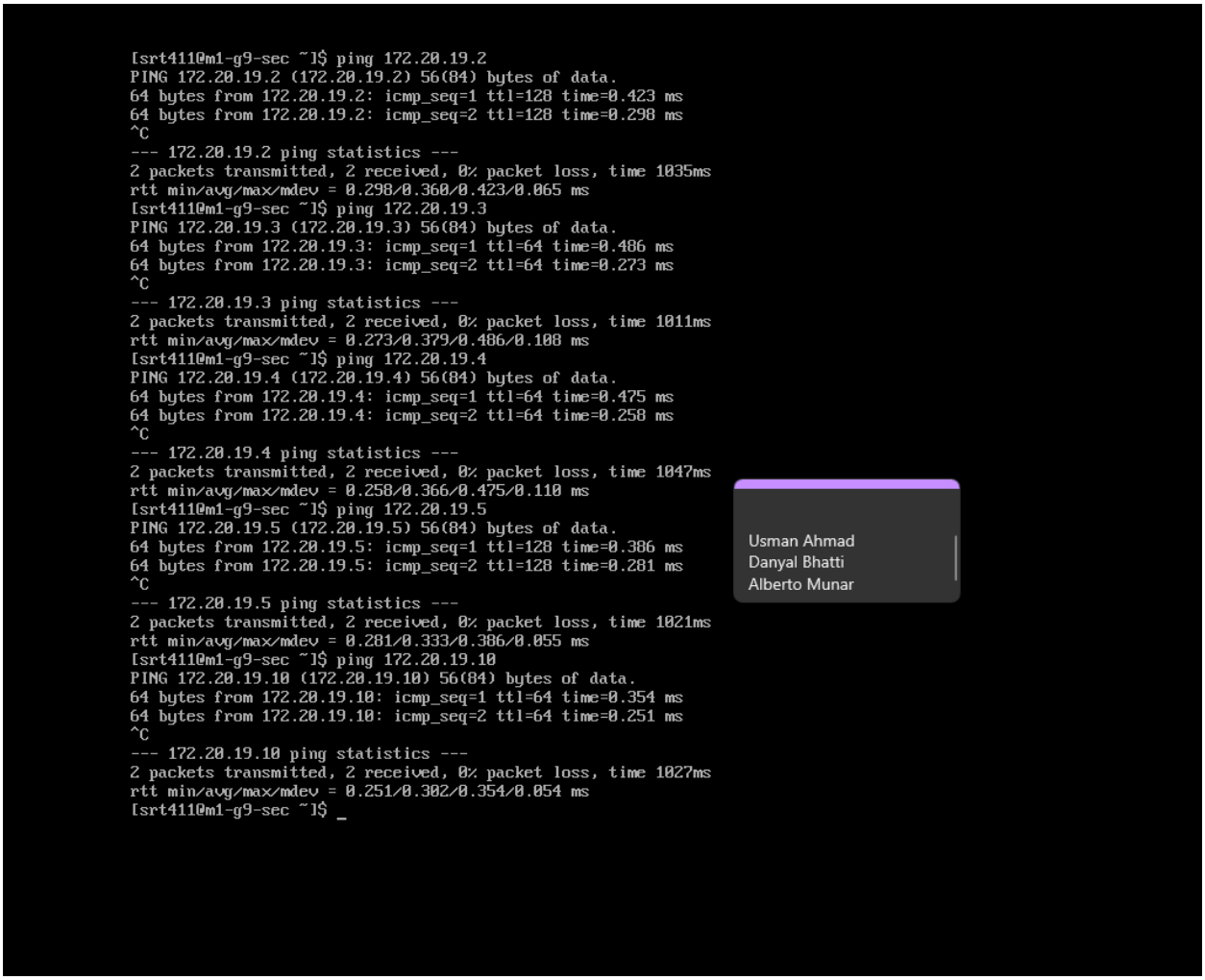
All The Vulnerabilities by class:



Pings

The above Screenshots are all the Vulnerabilities that were found on the systems that wer

Pinging All Machines:

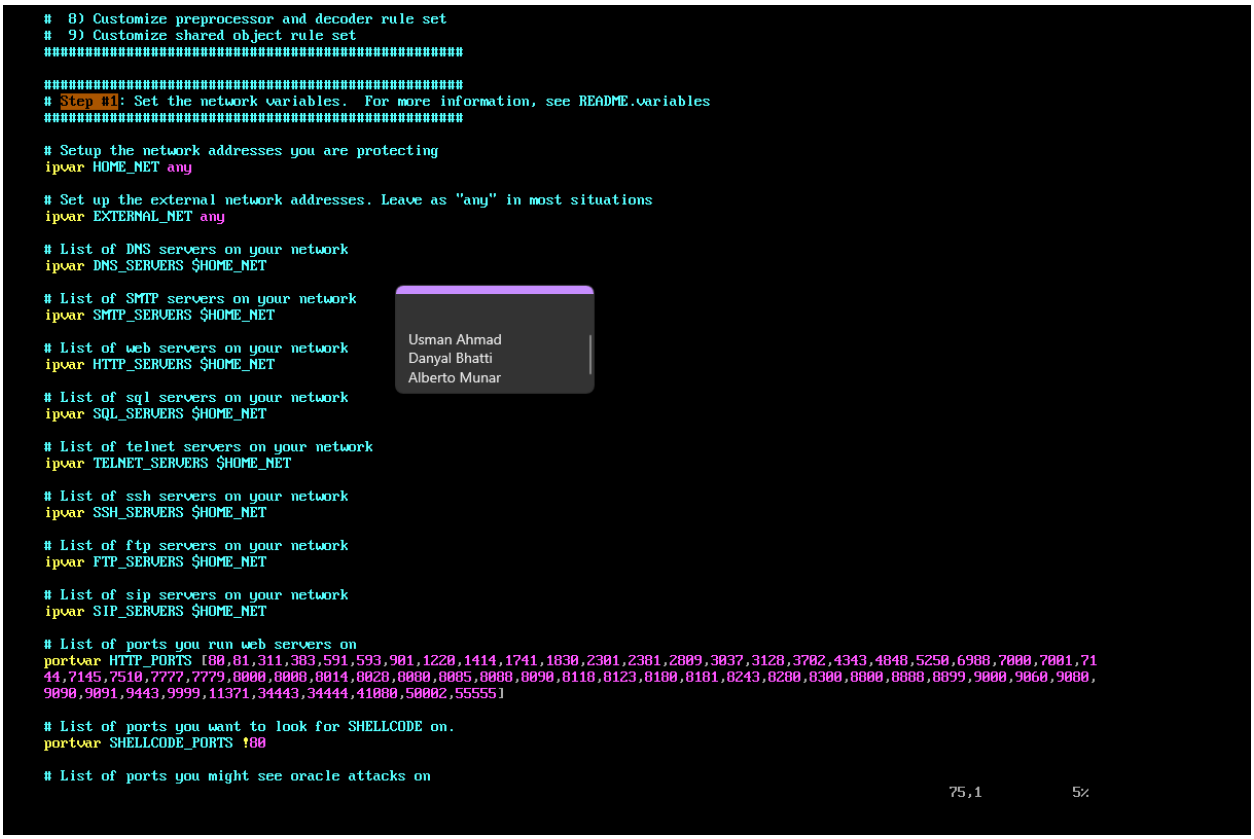


Snort:

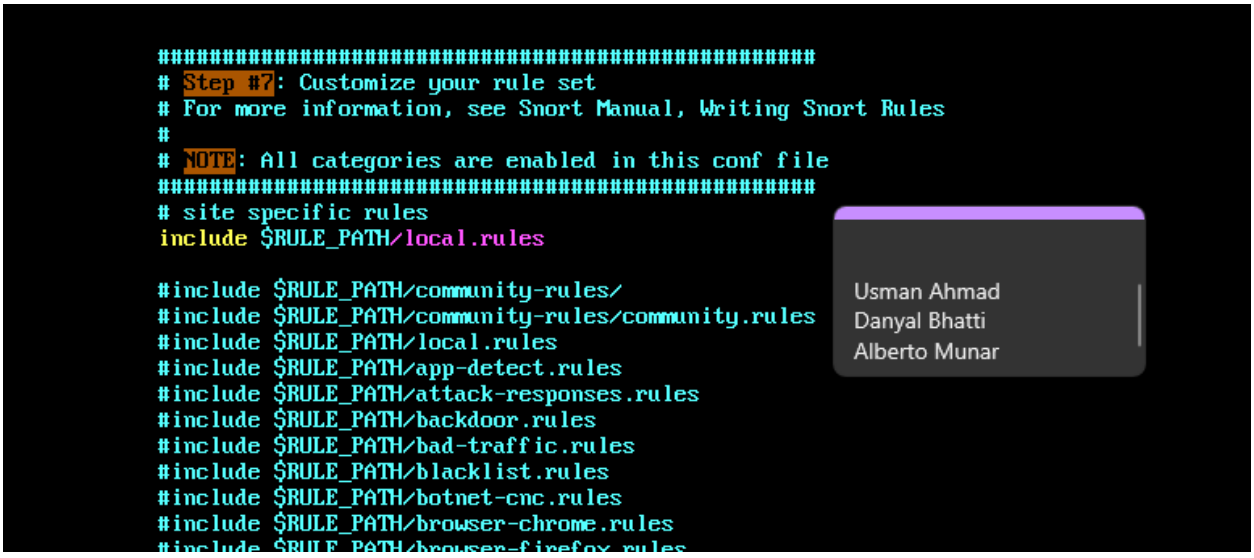
Snort Configuration:

The snort file can be configured with:

vim /etc/snort/snort.conf



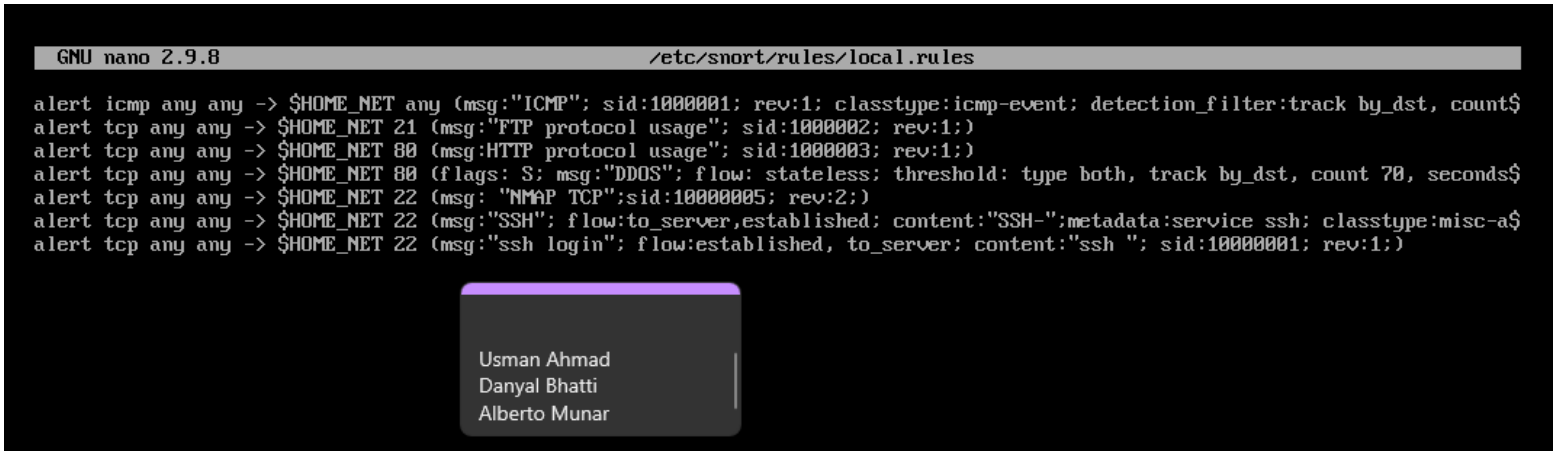
ipvar HOME_NET was set to any so that all the IPs on the network could be picked up.



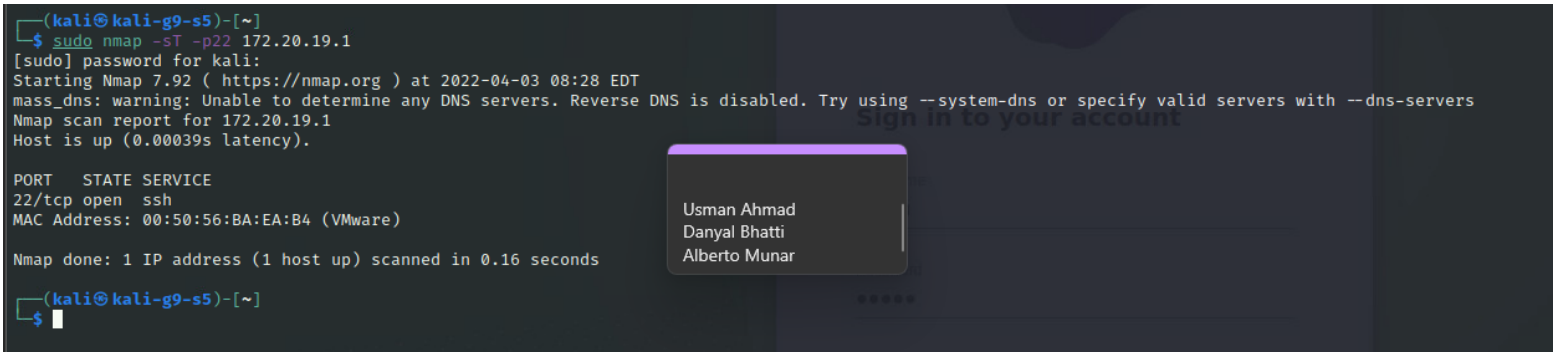
The site-specific rules were described in the local rules file.

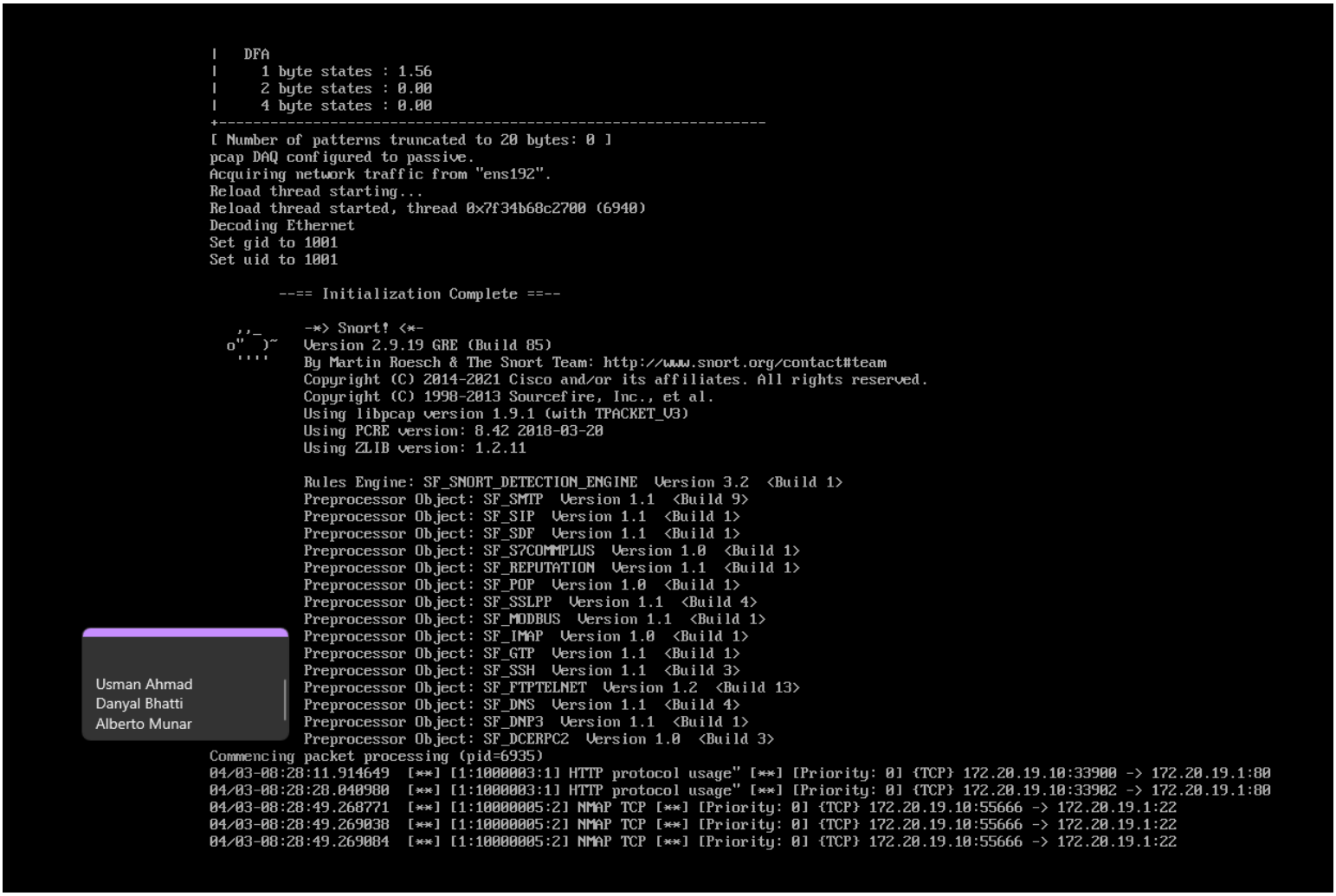
Snort Rules:

The following are the snort rules that we set up for collecting logs and traffic from all the interfaces.



nmap scan snort test:



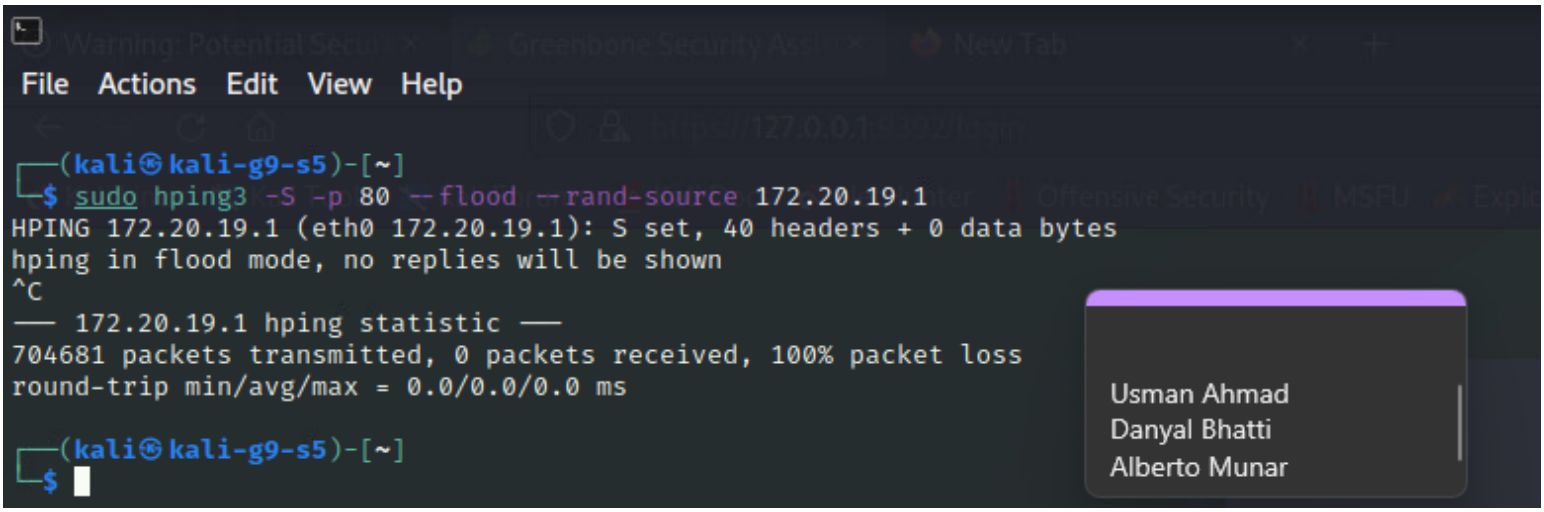


The image below shows the event or the activity that was collected by performing an nmap scan.

Attacks:

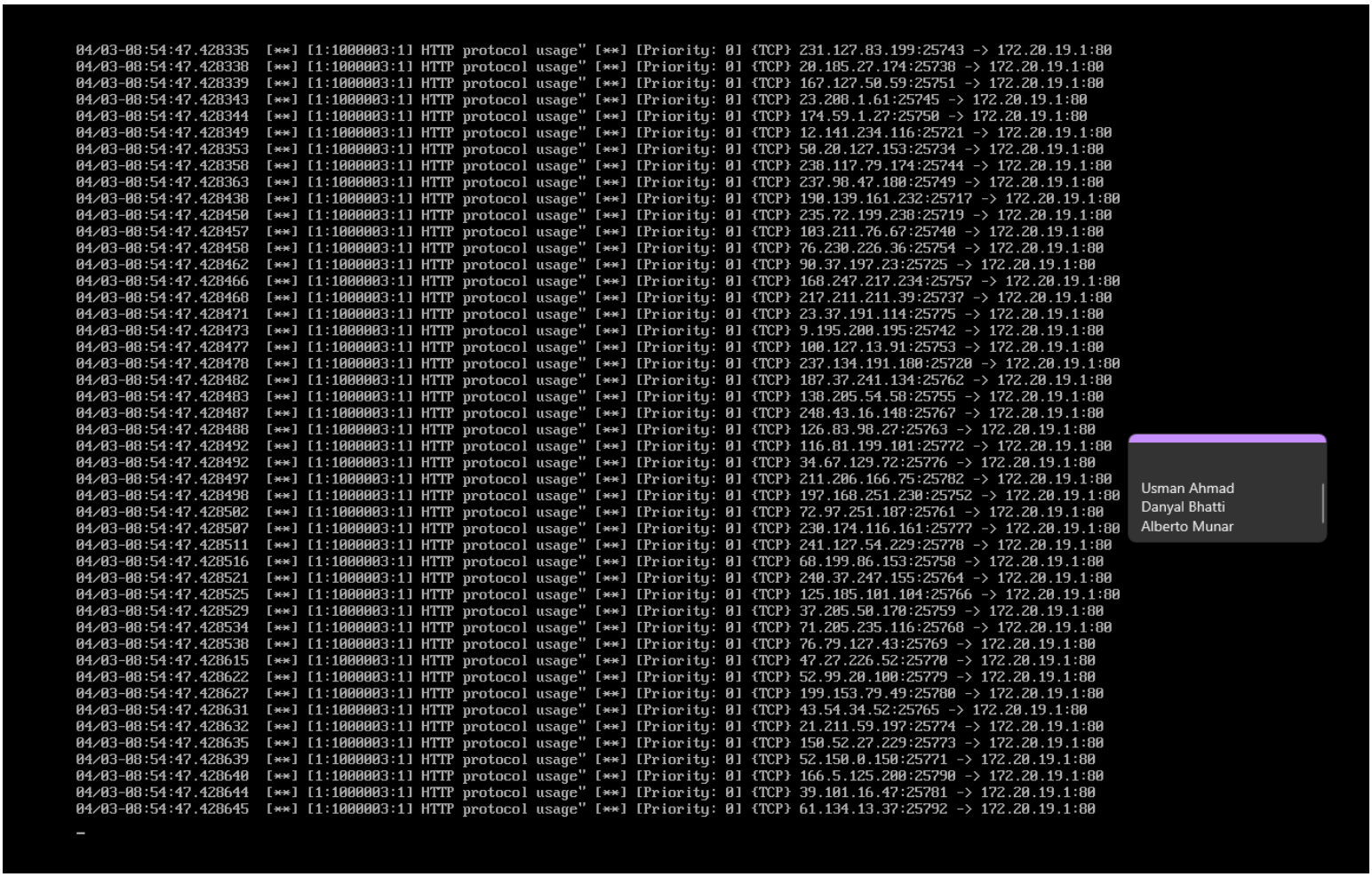
DDoS or DoS attack:

A tool called hping3 was used to flood a system with SYN packets:

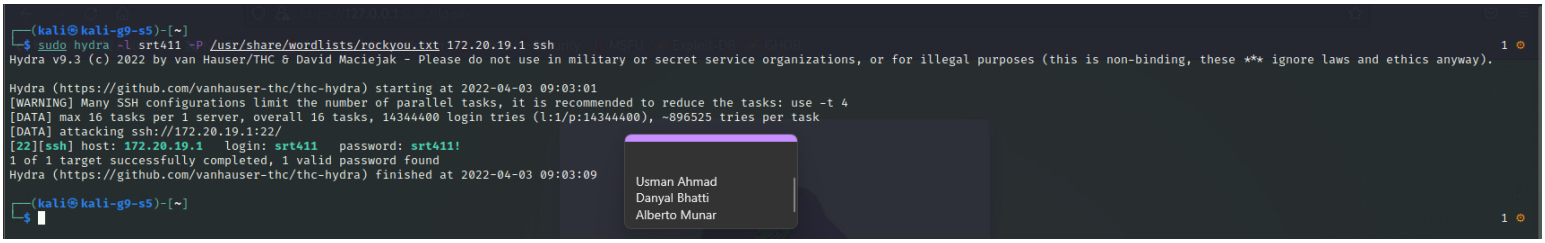


Hping is essentially flooding the target VM with SYN packets.

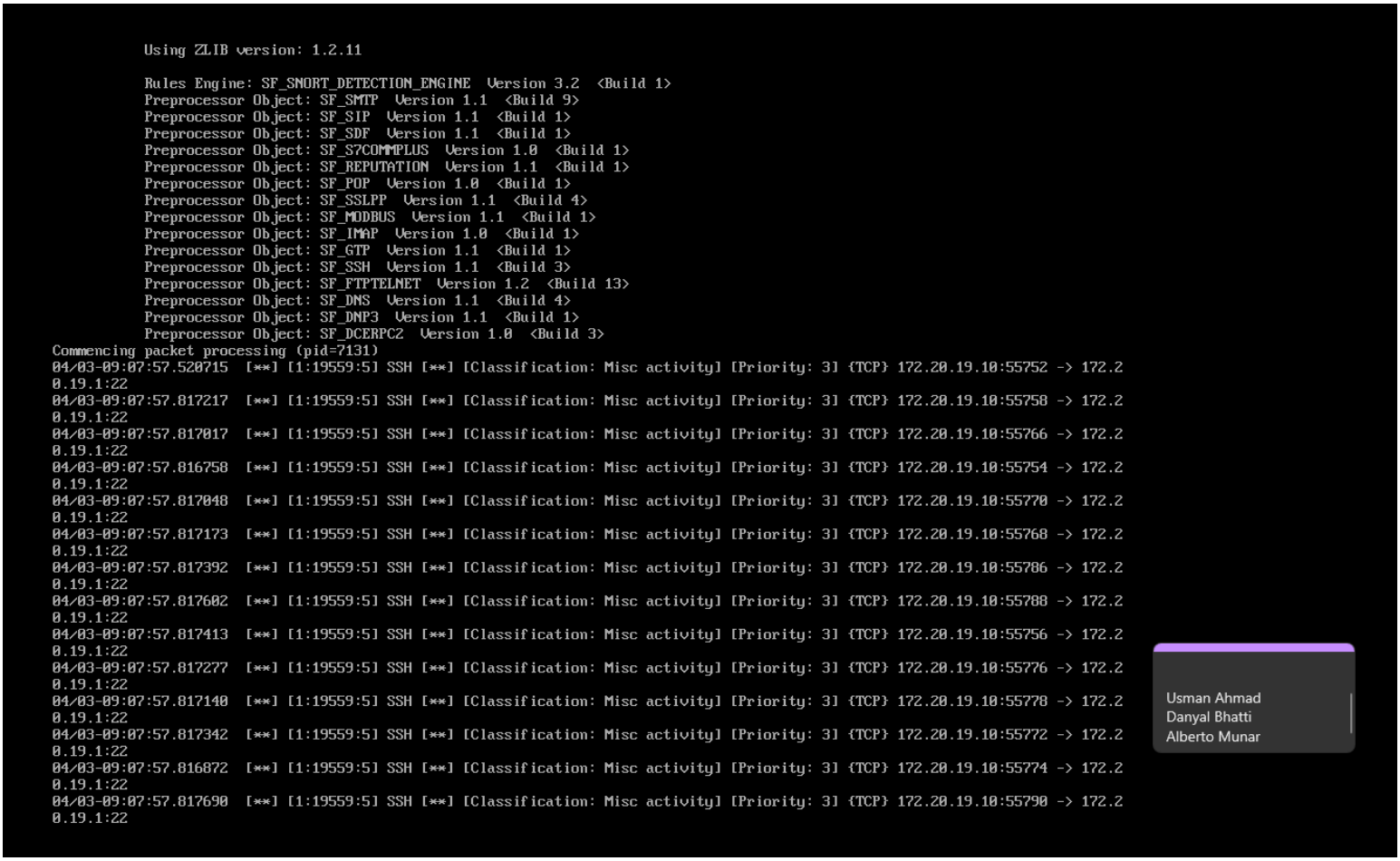
Snort event Logging for DoS attack:



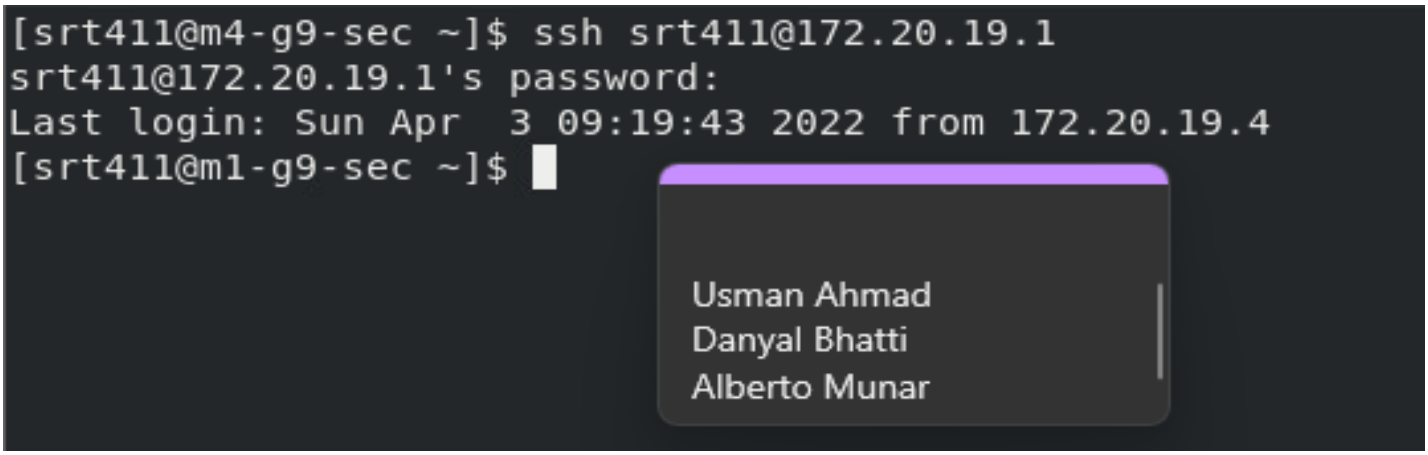
SSH Logins and Brute Force Attacks:



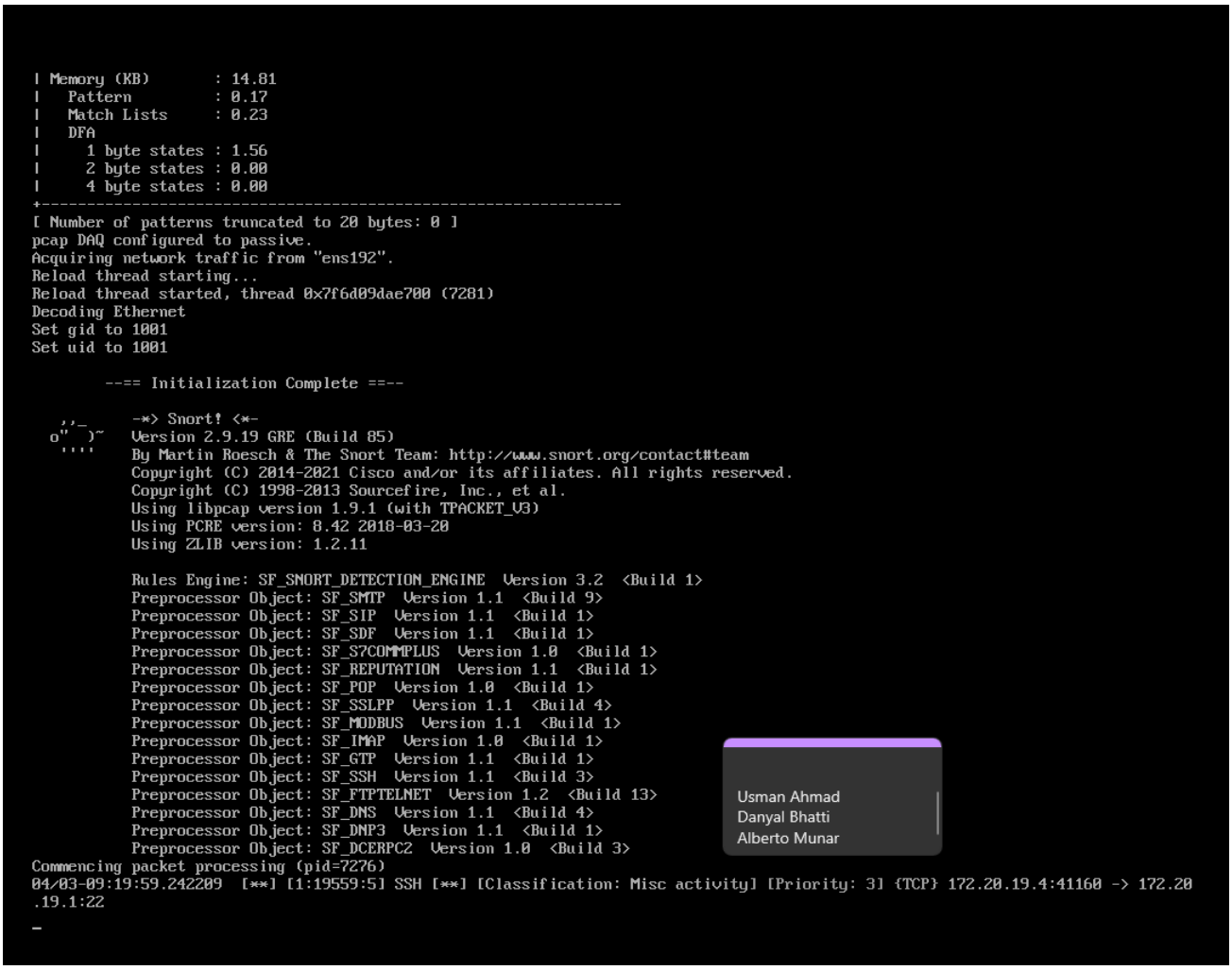
Snort Logs and events triggered by SSH Brute force



SSH Connection:



Snort Pick up of ssh connection:



Deep Scan of M1 of each port service and details:

```
┌──(kali㉿kali-g9-s5)-[~]
└─$ sudo nmap -p- -sV -O 172.20.19.1 --system-dns
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 10:10 EDT
Nmap scan report for 172.20.19.1
Host is up (0.00031s latency).
Not shown: 65386 filtered tcp ports (no-response), 147 filtered tcp ports (admin-prohibited)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 8.0 (protocol 2.0)
9090/tcp closed zeus-admin
MAC Address: 00:50:56:BA:EA:B4 (VMware)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.1
OS details: Linux 5.1
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 143.28 seconds

┌──(kali㉿kali-g9-s5)-[~]
└─$
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

Snort collection of data:

```
            Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
            Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
            Preprocessor Object: SF_POP  Version 1.0  <Build 1>
            Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
            Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
            Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
            Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
            Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
            Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
            Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
            Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
            Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=7997)
04/03-10:10:42.978877  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:35556 -> 172.20.19.1:22
04/03-10:10:42.979225  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:35556 -> 172.20.19.1:22
04/03-10:10:42.979257  [**] [1:1000002:1] FTP protocol usage [**] [Priority: 0] {TCP} 172.20.19.10:35556 -> 172.20.19.1:21
04/03-10:10:42.981463  [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 172.20.19.10:35556 -> 172.20.19.1:80
04/03-10:10:44.080405  [**] [1:1000003:1] HTTP protocol usage" [**] [Priority: 0] {TCP} 172.20.19.10:35558 -> 172.20.19.1:80
04/03-10:10:44.080499  [**] [1:1000002:1] FTP protocol usage [**] [Priority: 0] {TCP} 172.20.19.10:35558 -> 172.20.19.1:21
04/03-10:13:04.172587  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55794 -> 172.20.19.1:22
04/03-10:13:04.173029  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55794 -> 172.20.19.1:22
04/03-10:13:04.191453  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55794 -> 172.20.19.1:22
04/03-10:13:04.191970  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55794 -> 172.20.19.1:22
04/03-10:13:04.193683  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:55794 -> 172.20.19.1:22
04/03-10:13:04.292233  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45807 -> 172.20.19.1:22
04/03-10:13:04.292631  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45807 -> 172.20.19.1:22
04/03-10:13:04.392316  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45808 -> 172.20.19.1:22
04/03-10:13:04.392660  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45808 -> 172.20.19.1:22
04/03-10:13:04.492372  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45809 -> 172.20.19.1:22
04/03-10:13:04.492628  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45809 -> 172.20.19.1:22
04/03-10:13:04.592448  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45810 -> 172.20.19.1:22
04/03-10:13:04.592686  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45810 -> 172.20.19.1:22
04/03-10:13:04.692543  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45811 -> 172.20.19.1:22
04/03-10:13:04.692743  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45811 -> 172.20.19.1:22
04/03-10:13:04.792650  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45812 -> 172.20.19.1:22
04/03-10:13:04.792943  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45812 -> 172.20.19.1:22
04/03-10:13:04.892970  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45819 -> 172.20.19.1:22
04/03-10:13:04.893271  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45819 -> 172.20.19.1:22
04/03-10:13:04.918031  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45821 -> 172.20.19.1:22
04/03-10:13:04.943179  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45822 -> 172.20.19.1:22
04/03-10:13:04.968264  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45823 -> 172.20.19.1:22
04/03-10:13:05.095016  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45821 -> 172.20.19.1:22
04/03-10:13:05.120075  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45822 -> 172.20.19.1:22
04/03-10:13:05.195325  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45821 -> 172.20.19.1:22
04/03-10:13:05.220469  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45822 -> 172.20.19.1:22
04/03-10:13:05.295702  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45821 -> 172.20.19.1:22
04/03-10:13:05.320825  [**] [1:10000005:2] NMAP TCP [**] [Priority: 0] {TCP} 172.20.19.10:45822 -> 172.20.19.1:22
```

Usman Ahmad
Danyal Bhatti
Alberto Munar

Security Goals, Vulnerabilities and Threats

The goal is to protect the network infrastructure and always keep the resources accessible and effective as much as possible. Due to the vast number of resources, services and the design of the network and devices, it is not possible to eliminate threats. Due to the vast number of software programs and application services that are present regardless of how secure the network may be configured, there will be openings and vulnerabilities that can be exploited to get access to the network and perform kinds of attacks and malicious goals of adversaries. The goal is to keep track of the network activities and unusual activities that may take place, which can be found with snort and then further mitigate those issues by looking at demographics that could further help the businesses and other infrastructures.

How Data Collection help you achieve your goal:

Data Collection allows us to keep track and get the understanding of the events and activities that are taking place. These further help with, getting to know the unusual activities that are likely threats, track them down and protect the infrastructure by mitigating the threats

Explain Data Collection:

The collection of activities and events that take place in a network and collecting all that information and preserving or importing it in a readable format for visual or statistical analysis is basically data collection. For our case we sent the Snort Files to Kali from M1, we also collected packet captures in the form of CSV and the vulnerability report in CSV.

Data Collection:

Brute Force Attack:

The following screenshot shows the data imported in csv format.

No.	Time	Source	Destinatic	Protocol	Length	Info
1	0	172.20.19.	172.20.19.	TCP	74	55796 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2679135521 TSecr=0 WS=128
2	0.000476	172.20.19.	172.20.19.	TCP	74	22 > 55796 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2761570306 TSecr=2679135521 WS=128
3	0.000511	172.20.19.	172.20.19.	TCP	66	55796 > 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2679135521 TSecr=2761570306
4	0.000539	172.20.19.	172.20.19.	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.9.6)
5	0.000663	172.20.19.	172.20.19.	TCP	66	22 > 55796 [ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=2761570306 TSecr=2679135522
6	0.016011	172.20.19.	172.20.19.	SSHv2	87	Server: Protocol (SSH-2.0-OpenSSH_8.0)
7	0.016021	172.20.19.	172.20.19.	TCP	66	55796 > 22 [ACK] Seq=23 Ack=22 Win=64256 Len=0 TSval=2679135537 TSecr=2761570321
8	0.016216	172.20.19.	172.20.19.	SSHv2	1042	Client: Key Exchange Init
9	0.018577	172.20.19.	172.20.19.	SSHv2	1114	Server: Key Exchange Init
10	0.018596	172.20.19.	172.20.19.	TCP	66	55796 > 22 [ACK] Seq=999 Ack=1070 Win=64128 Len=0 TSval=2679135540 TSecr=2761570324
11	0.018772	172.20.19.	172.20.19.	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
12	0.025803	172.20.19.	172.20.19.	SSHv2	454	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=180)
13	0.025816	172.20.19.	172.20.19.	TCP	66	55796 > 22 [ACK] Seq=1047 Ack=1458 Win=64128 Len=0 TSval=2679135547 TSecr=2761570331
14	0.026026	172.20.19.	172.20.19.	SSHv2	82	Client: New Keys
15	0.06707	172.20.19.	172.20.19.	TCP	66	22 > 55796 [ACK] Seq=1458 Ack=1063 Win=30976 Len=0 TSval=2761570373 TSecr=2679135547
16	0.067086	172.20.19.	172.20.19.	SSHv2	118	Client: Encrypted packet (len=52)
17	0.067188	172.20.19.	172.20.19.	TCP	66	22 > 55796 [ACK] Seq=1458 Ack=1115 Win=30976 Len=0 TSval=2761570373 TSecr=2679135588
18	0.067261	172.20.19.	172.20.19.	SSHv2	118	Server: Encrypted packet (len=52)
19	0.067266	172.20.19.	172.20.19.	TCP	66	55796 > 22 [ACK] Seq=1115 Ack=1510 Win=64128 Len=0 TSval=2679135588 TSecr=2761570373
20	0.06735	172.20.19.	172.20.19.	SSHv2	134	Client: Encrypted packet (len=68)
21	0.074651	172.20.19.	172.20.19.	SSHv2	150	Server: Encrypted packet (len=84)
22	0.074733	172.20.19.	172.20.19.	SSHv2	118	Client: Encrypted packet (len=52)
23	0.074765	172.20.19.	172.20.19.	TCP	66	55796 > 22 [FIN, ACK] Seq=1235 Ack=1594 Win=64128 Len=0 TSval=2679135596 TSecr=2761570380
24	0.078086	172.20.19.	172.20.19.	TCP	66	22 > 55796 [FIN, ACK] Seq=1594 Ack=1236 Win=30976 Len=0 TSval=2761570384 TSecr=2679135596
25	0.078098	172.20.19.	172.20.19.	TCP	66	55796 > 22 [ACK] Seq=1236 Ack=1595 Win=64128 Len=0 TSval=2679135599 TSecr=2761570384
26	0.30867	172.20.19.	172.20.19.	TCP	74	55800 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2679135830 TSecr=0 WS=128
27	0.308704	172.20.19.	172.20.19.	TCP	74	55798 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2679135830 TSecr=0 WS=128
28	0.308969	172.20.19.	172.20.19.	TCP	74	22 > 55800 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2761570614 TSecr=2679135830 WS=128
29	0.308998	172.20.19.	172.20.19.	TCP	66	55800 > 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2679135830 TSecr=2761570614
30	0.309001	172.20.19.	172.20.19.	TCP	74	22 > 55798 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2761570614 TSecr=2679135830 WS=128
31	0.309016	172.20.19.	172.20.19.	TCP	66	55798 > 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2679135830 TSecr=2761570614
32	0.309044	172.20.19.	172.20.19.	TCP	74	55802 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2679135830 TSecr=0 WS=128
33	0.30905	172.20.19.	172.20.19.	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.9.6)
34	0.30909	172.20.19.	172.20.19.	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.9.6)
35	0.309098	172.20.19.	172.20.19.	TCP	74	55804 > 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2679135830 TSecr=0 WS=128

Usman Ahmad
Danyal Bhatti
Alberto Munar

DDoS Attack:

The following data was collected with DDoS attack:

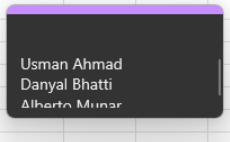
No.	Time	Source	Destinatic	Protocol	Length	Info
1	0	145.131.82	172.20.19.	TCP	54	1911 > 80 [SYN] Seq=0 Win=512 Len=0
2	5.47E-05	63.21.131.	172.20.19.	TCP	54	1912 > 80 [SYN] Seq=0 Win=512 Len=0
3	7.01E-05	137.238.18	172.20.19.	TCP	54	1913 > 80 [SYN] Seq=0 Win=512 Len=0
4	8.37E-05	239.213.23	172.20.19.	TCP	54	1914 > 80 [SYN] Seq=0 Win=512 Len=0
5	9.85E-05	92.188.92.	172.20.19.	TCP	54	1915 > 80 [SYN] Seq=0 Win=512 Len=0
6	0.000122	120.139.50	172.20.19.	TCP	54	1916 > 80 [SYN] Seq=0 Win=512 Len=0
7	0.000135	162.214.16	172.20.19.	TCP	54	1917 > 80 [SYN] Seq=0 Win=512 Len=0
8	0.000147	174.196.16	172.20.19.	TCP	54	1918 > 80 [SYN] Seq=0 Win=512 Len=0
9	0.00016	160.71.24.	172.20.19.	TCP	54	1919 > 80 [SYN] Seq=0 Win=512 Len=0
10	0.000172	88.57.213.	172.20.19.	TCP	54	1920 > 80 [SYN] Seq=0 Win=512 Len=0
11	0.000184	69.239.175	172.20.19.	TCP	54	1921 > 80 [SYN] Seq=0 Win=512 Len=0
12	0.000196	31.162.120	172.20.19.	TCP	54	1922 > 80 [SYN] Seq=0 Win=512 Len=0
13	0.000209	57.97.99.1	172.20.19.	TCP	54	1923 > 80 [SYN] Seq=0 Win=512 Len=0
14	0.000229	62.172.9.1	172.20.19.	TCP	54	1924 > 80 [SYN] Seq=0 Win=512 Len=0
15	0.000241	196.26.118	172.20.19.	TCP	54	1925 > 80 [SYN] Seq=0 Win=512 Len=0
16	0.000254	149.67.38.	172.20.19.	TCP	54	1926 > 80 [SYN] Seq=0 Win=512 Len=0
17	0.000266	122.175.20	172.20.19.	TCP	54	1927 > 80 [SYN] Seq=0 Win=512 Len=0
18	0.000287	117.32.224	172.20.19.	TCP	54	1928 > 80 [SYN] Seq=0 Win=512 Len=0
19	0.000301	245.188.73	172.20.19.	TCP	54	1929 > 80 [SYN] Seq=0 Win=512 Len=0
20	0.00032	38.62.191.	172.20.19.	TCP	54	1930 > 80 [SYN] Seq=0 Win=512 Len=0
21	0.00034	206.50.122	172.20.19.	TCP	54	1931 > 80 [SYN] Seq=0 Win=512 Len=0
22	0.000353	75.22.210.	172.20.19.	TCP	54	1932 > 80 [SYN] Seq=0 Win=512 Len=0
23	0.000366	149.182.22	172.20.19.	TCP	54	1933 > 80 [SYN] Seq=0 Win=512 Len=0
24	0.000378	9.64.112.1	172.20.19.	TCP	54	1934 > 80 [SYN] Seq=0 Win=512 Len=0
25	0.000384	15.57.14.1	172.20.19.	TCP	54	1935 > 80 [SYN] Seq=0 Win=512 Len=0
26	0.000397	160.148.11	172.20.19.	TCP	54	1936 > 80 [SYN] Seq=0 Win=512 Len=0
27	0.000409	19.203.46.	172.20.19.	TCP	54	1937 > 80 [SYN] Seq=0 Win=512 Len=0
28	0.000426	214.62.24.	172.20.19.	TCP	54	1938 > 80 [SYN] Seq=0 Win=512 Len=0
29	0.000439	147.73.49.	172.20.19.	TCP	54	1939 > 80 [SYN] Seq=0 Win=512 Len=0
30	0.000451	96.66.110.	172.20.19.	TCP	54	1940 > 80 [SYN] Seq=0 Win=512 Len=0
31	0.000464	68.94.66.1	172.20.19.	TCP	54	1941 > 80 [SYN] Seq=0 Win=512 Len=0
32	0.000476	168.72.106	172.20.19.	TCP	54	1942 > 80 [SYN] Seq=0 Win=512 Len=0
33	0.000495	63.81.159.	172.20.19.	TCP	54	1943 > 80 [SYN] Seq=0 Win=512 Len=0
34	0.000513	228.21.132	172.20.19.	TCP	54	1944 > 80 [SYN] Seq=0 Win=512 Len=0
35	0.000525	122.208.65	172.20.19.	TCP	54	1945 > 80 [SYN] Seq=0 Win=512 Len=0

Usman Ahmad
Danyal Bhatti
Alberto Munar

Nmap Scan:

The following Data was generated with Nmap scan:

No.	Time	Source	Destinatic	Protocol	Length	Info
1	0	VMware_	Broadcast	ARP	42	Who has 172.20.21.1? Tell 172.20.21.10
2	3.61E-05	VMware_	Broadcast	ARP	42	Who has 172.20.21.2? Tell 172.20.21.10
3	4.04E-05	VMware_	Broadcast	ARP	42	Who has 172.20.21.3? Tell 172.20.21.10
4	6.72E-05	VMware_	Broadcast	ARP	42	Who has 172.20.21.4? Tell 172.20.21.10
5	7.09E-05	VMware_	Broadcast	ARP	42	Who has 172.20.21.5? Tell 172.20.21.10
6	7.48E-05	VMware_	Broadcast	ARP	42	Who has 172.20.21.6? Tell 172.20.21.10
7	7.89E-05	VMware_	Broadcast	ARP	42	Who has 172.20.21.7? Tell 172.20.21.10
8	9.04E-05	VMware_	Broadcast	ARP	42	Who has 172.20.21.8? Tell 172.20.21.10
9	9.52E-05	VMware_	Broadcast	ARP	42	Who has 172.20.21.9? Tell 172.20.21.10
10	0.000101	VMware_	Broadcast	ARP	42	Who has 172.20.21.11? Tell 172.20.21.10
11	0.000223	VMware_	VMware_	ARP	60	172.20.21.1 is at 00:50:56:ba:a5:ce
12	0.000337	VMware_	VMware_	ARP	60	172.20.21.2 is at 00:50:56:ba:74:7f
13	0.000596	VMware_	VMware_	ARP	60	172.20.21.3 is at 00:50:56:ba:fc:be
14	0.018041	VMware_	Broadcast	ARP	42	Who has 172.20.21.14? Tell 172.20.21.10
15	0.018068	VMware_	Broadcast	ARP	42	Who has 172.20.21.15? Tell 172.20.21.10
16	0.018078	VMware_	Broadcast	ARP	42	Who has 172.20.21.16? Tell 172.20.21.10
17	0.018082	VMware_	Broadcast	ARP	42	Who has 172.20.21.17? Tell 172.20.21.10
18	0.018085	VMware_	Broadcast	ARP	42	Who has 172.20.21.18? Tell 172.20.21.10
19	0.018088	VMware_	Broadcast	ARP	42	Who has 172.20.21.19? Tell 172.20.21.10
20	0.100303	VMware_	Broadcast	ARP	42	Who has 172.20.21.22? Tell 172.20.21.10
21	0.100334	VMware_	Broadcast	ARP	42	Who has 172.20.21.23? Tell 172.20.21.10
22	0.100359	VMware_	Broadcast	ARP	42	Who has 172.20.21.24? Tell 172.20.21.10
23	0.100365	VMware_	Broadcast	ARP	42	Who has 172.20.21.25? Tell 172.20.21.10
24	0.10037	VMware_	Broadcast	ARP	42	Who has 172.20.21.26? Tell 172.20.21.10
25	0.100373	VMware_	Broadcast	ARP	42	Who has 172.20.21.27? Tell 172.20.21.10
26	0.100378	VMware_	Broadcast	ARP	42	Who has 172.20.21.28? Tell 172.20.21.10
27	0.118188	VMware_	Broadcast	ARP	42	Who has 172.20.21.31? Tell 172.20.21.10
28	0.11822	VMware_	Broadcast	ARP	42	Who has 172.20.21.32? Tell 172.20.21.10
29	0.11823	VMware_	Broadcast	ARP	42	Who has 172.20.21.33? Tell 172.20.21.10
30	0.118233	VMware_	Broadcast	ARP	42	Who has 172.20.21.34? Tell 172.20.21.10
31	0.118238	VMware_	Broadcast	ARP	42	Who has 172.20.21.35? Tell 172.20.21.10
32	0.118241	VMware_	Broadcast	ARP	42	Who has 172.20.21.36? Tell 172.20.21.10
33	0.200498	VMware_	Broadcast	ARP	42	Who has 172.20.21.39? Tell 172.20.21.10
34	0.200533	VMware_	Broadcast	ARP	42	Who has 172.20.21.40? Tell 172.20.21.10
35	0.200556	VMware_	Broadcast	ARP	42	Who has 172.20.21.41? Tell 172.20.21.10

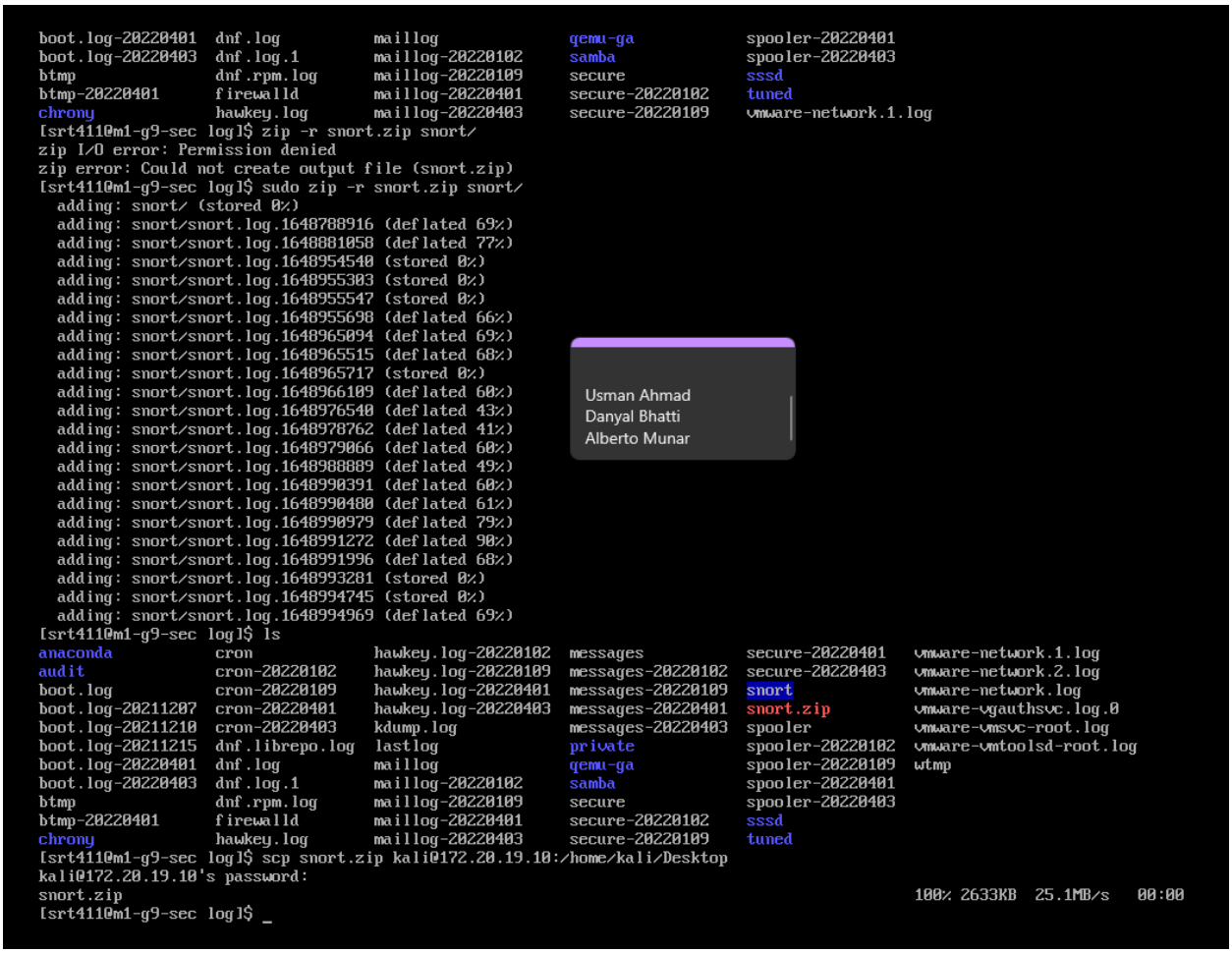


Greenbone Scan Results:

Data collected after Greenbone Scan:

IP	Hostname	Port	Port Protc	CVSS	Severity	Solution T	NVT Nam	Summary	Specific R	NVT OID	CVEs	Task ID	Task Nam	Timestam	Result ID	Impact	Solution	Affected S	Vulnerabi	Vulnerabi	Product D	BIDs	CERTs	Other References
172.20.21.1		80	tcp	10	High	VendorFi	MS15-034	This host	Vulnerabi	1.3.6.1.4.1	CVE-2015-	849145ac-	SRT411Ph	2022-04-0	76f18ef4-:	Successf	The vende	'-	Flaw	Send a	Product:		DFN-CERT-2015-0545,CB-K15/0527	
172.20.21.1		3306	tcp	10	High	VendorFi	Oracle My	This host	Installed	1.3.6.1.4.1	CVE-2016-	849145ac-	SRT411Ph	2022-04-0	bae1fb03-	Successf	Upgrade	Oracle	The flaw	Checks if	Product:	92912	DFN-CERT-2020-1473,DFN-CERT-2017-0138,DFN-CERT-2017-0060,D	
172.20.21.1		3306	tcp	10	High	VendorFi	Oracle My	This host	Installed	1.3.6.1.4.1	CVE-2016-	849145ac-	SRT411Ph	2022-04-0	c196cd43-	Successf	Apply the	Oracle	Multiple	Checks if	Product:		DFN-CERT-2020-1473,DFN-CERT-2017-0138,DFN-CERT-2017-0060,D	
172.20.21.1		9200	tcp	10	High	VendorFi	Elasticsea	The	The	1.3.6.1.4.1.25623.1.0.	849145ac-	SRT411Ph	2022-04-0	e06d8fc9-	cd52-420d-	Update Elasticsearch to a versi			Checks if					
172.20.21.1		8282	tcp	10	High	VendorFi	Apache Tc	The	The	1.3.6.1.4.1.25623.1.0.	849145ac-	SRT411Ph	2022-04-0	0e239ef7-	An end	Update the Apache Tomcat ver			Checks if					
172.20.21.1		8282	tcp	10	High	Mitigatior	Apache Ai	The	Vulnerabi	1.3.6.1.4.1	CVE-2010-	849145ac-	SRT411Ph	2022-04-0	3a4c9826-	This	Change the passwor	It was pos	Try to			44055		
172.20.21.1		3389	tcp	10	High	VendorFi	Microsoft	This host	By	1.3.6.1.4.1	CVE-2019-	849145ac-	SRT411Ph	2022-04-0	e9854c04-	Successf	The	'-	A remote	Sends a		108273	DFN-CERT-2019-0977,CB-K19/0415	
172.20.21.1		8022	tcp	10	High	VendorFi	ManageEr	ManageE	It was	1.3.6.1.4.1	CVE-2015-	849145ac-	SRT411Ph	2022-04-0	b24260b0-	Successf	Update to	ManageEngine Desk	Try to					
172.20.21.1		8022	tcp	10	High	VendorFi	ManageEr	Zoho	Installed	1.3.6.1.4.1	CVE-2017-	849145ac-	SRT411Ph	2022-04-0	88c2c850-db3b-4aa3		Upgrade t	ManageEngine Desk	Checks if					
172.20.21.1		445	tcp	9.3	High	VendorFi	Microsoft	This host	Vulnerabi	1.3.6.1.4.1	CVE-2017-	849145ac-	SRT411Ph	2022-04-0	940bf2a2-	Successf	The vende	'-	Multiple	Send the		########	DFN-CERT-2017-0448,CB-K17/0435	
172.20.21.1		3306	tcp	9	High	Mitigatior	MySQL / M	It was	It was	1.3.6.1.4.1.25623.1.0.	849145ac-	SRT411Ph	2022-04-0	afe70364-5d8e-4fc2-	Change the password as soon a						Product:			
172.20.21.1		8282	tcp	7.8	High	VendorFi	Apache Tc	This host	Installed	1.3.6.1.4.1	CVE-2016-	849145ac-	SRT411Ph	2022-04-0	78adb23e-	Successf	Upgrade	Apache	The flaw	Checks if		91453	DFN-CERT-2018-2554,DFN-CERT-2018-0729,DFN-CERT-2017-1821,D	
172.20.21.1		22	tcp	7.8	High	VendorFi	OpenSSH	This host	Installed	1.3.6.1.4.1	CVE-2016-	849145ac-	SRT411Ph	2022-04-0	3bda47eb	Successf	Upgrade t	OpenSSH	Multiple	Checks if	Product:	92212	DFN-CERT-2019-1408,DFN-CERT-2018-1828,DFN-CERT-2018-1070,D	
172.20.21.1		3306	tcp	7.7	High	VendorFi	Oracle My	Oracle My	Installed	1.3.6.1.4.1	CVE-2020-	849145ac-	SRT411Ph	2022-04-0	a14014ac-	b34c-48ed-	Update to	Oracle MySQL 8.0.21	Checks if	Product:		DFN-CERT-2020-2295,CB-K20/1017		
172.20.21.1		22	tcp	7.5	High	VendorFi	OpenSSH	This host	Installed	1.3.6.1.4.1	CVE-2016-	849145ac-	SRT411Ph	2022-04-0	c5d17c1a-	Successf	Upgrade t	OpenSSH	An access	Checks if	Product:	84427	DFN-CERT-2018-1828,DFN-CERT-2016-1574,DFN-CERT-2016-0754,D	
172.20.21.1		3306	tcp	7.5	High	VendorFi	Oracle My	This host	Vulnerabi	1.3.6.1.4.1	CVE-2014-	849145ac-	SRT411Ph	2022-04-0	a3f9190d-	Successf	Apply the	MySQL	Unspecifi	Checks if	Product:	########	DFN-CERT-2015-1604,DFN-CERT-2015-1016,DFN-CERT-2015-0593,D	
172.20.21.1		8009	tcp	7.5	High	VendorFi	Apache Tc	Apache	It was	1.3.6.1.4.1	CVE-2020-	849145ac-	SRT411Ph	2022-04-0	87604a64-53be-4eb6		Update	Apache	Apache	Sends a			DFN-CERT-2020-1508,DFN-CERT-2020-1413,DFN-CERT-2020-1276,D	
172.20.21.1		8019	tcp	7.5	High	VendorFi	Apache Tc	Apache	It was	1.3.6.1.4.1	CVE-2020-	849145ac-	SRT411Ph	2022-04-0	8522923f-ae35-403c-		Update	Apache	Apache	Sends a			DFN-CERT-2020-1508,DFN-CERT-2020-1413,DFN-CERT-2020-1276,D	
172.20.21.1		3306	tcp	7.5	High	VendorFi	Oracle My	This host	Installed	1.3.6.1.4.1	CVE-2015-	849145ac-	SRT411Ph	2022-04-0	76cf47ca-(	Successf	Apply the	Oracle	Unspecifi	Checks if	Product:	########	DFN-CERT-2015-1264,DFN-CERT-2015-1016,DFN-CERT-2015-0593,D	
172.20.21.2		80	tcp	7.5	High	Workarou	phpinfo()	Many	The	1.3.6.1.4.1.25623.1.0.	849145ac-	SRT411Ph	2022-04-0	1f32ef40-(	Some of	Delete the listed files or restric								
172.20.21.1		3306	tcp	7.5	High	VendorFi	Oracle My	This host	Installed	1.3.6.1.4.1	CVE-2018-	849145ac-	SRT411Ph	2022-04-0	0766e83e-	Successf	Apply the	Oracle	The flaw	Checks if	Product:		DFN-CERT-2019-1047,DFN-CERT-2018-1276,DFN-CERT-2018-1265,D	
172.20.21.1		3306	tcp	7.5	High	VendorFi	Oracle My	Oracle	Installed	1.3.6.1.4.1	CVE-2020-	849145ac-	SRT411Ph	2022-04-0	c5dd6fd8-03ae-4803-		Update to	Oracle MySQL 5.7.31	Checks if	Product:		DFN-CERT-2020-2295,CB-K20/1017		
172.20.21.1		1617	tcp	7.5	High	Mitigatior	Java JMX I	The Java	It was	1.3.6.1.4.1.25623.1.0.	849145ac-	SRT411Ph	2022-04-0	1fb8b2e6-19cd-438d	Enable				Sends					
172.20.21.1		22	tcp	7.5	High	VendorFi	OpenSSH	This host	Installed	1.3.6.1.4.1	CVE-2016-	849145ac-	SRT411Ph	2022-04-0	a990077d-	Successf	Upgrade t	OpenSSH	Multiple	Checks if	Product:	########	DFN-CERT-2019-1408,DFN-CERT-2018-2259,DFN-CERT-2018-2191,D	
172.20.21.1		8022	tcp	7.5	High	VendorFi	ZOHO Mar	This host	Vulnerab	1.3.6.1.4.1	CVE-2018-	849145ac-	SRT411Ph	2022-04-0	55790cf7-:	Successf	Upgrade	Zoho	Multiple	Send the				
172.20.21.1		3306	tcp	7.5	High	VendorFi	Oracle My	This host	Installed	1.3.6.1.4.1	CVE-2018-	849145ac-	SRT411Ph	2022-04-0	9d76fed1-	Successf	Apply the	Oracle	Multiple	Checks if	Product:		DFN-CERT-2020-1536,DFN-CERT-2019-1614,DFN-CERT-2019-1588,D	
172.20.21.1		9200	tcp	7.5	High	VendorFi	Elasticsea	This host	Installed	1.3.6.1.4.1	CVE-2015-	849145ac-	SRT411Ph	2022-04-0	d5eb463c-	Successf	Upgrade	Elasticse	The Flaw	Checks if		75935	DFN-CERT-2015-1160,CB-K15/1118	
172.20.21.1		8022	tcp	7.5	High	VendorFi	ManageEr	Zoho	Installed	1.3.6.1.4.1	CVE-2017-	849145ac-	SRT411Ph	2022-04-0	3adb6a08-50f6-4b17-		Upgrade t	ManageEngine Desk	Checks if					
172.20.21.1		21	tcp	7.5	High	Mitigatior	FTP Brute	It was	It was	1.3.6.1.4.1.25623.1.0.	849145ac-	SRT411Ph	2022-04-0	b9df8d7a-601c-4815-	Change the password as soon a				Reports					
172.20.21.1		22	tcp	7.5	High	Mitigatior	SSH Brute	It was	It was	1.3.6.1.4.1.25623.1.0.	849145ac-	SRT411Ph	2022-04-0	513cd5b4-54dc-4040-	Change the password as soon a				Reports					
172.20.21.1		21	tcp	7.5	High	Mitigatior	FTP Brute	It was	It was	1.3.6.1.4.1.25623.1.0.	849145ac-	SRT411Ph	2022-04-0	4ca6c11d-1cd4-4423-	Change the password as soon a				Reports					
172.20.21.1		22	tcp	7.5	High	Mitigatior	SSH Brute	It was	It was	1.3.6.1.4.1.25623.1.0.	849145ac-	SRT411Ph	2022-04-0	001eafd0-628e-49af-	Change the password as soon a				Reports					
172.20.21.1		3306	tcp	7.2	High	VendorFi	Oracle My	This host	Installed	1.3.6.1.4.1	CVE-2016-	849145ac-	SRT411Ph	2022-04-0	a740db4b-	Successf	Apply the	Oracle	Unspecifi	Checks if	Product:	########	DFN-CERT-2016-1192,DFN-CERT-2016-0994,DFN-CERT-2016-0845,D	
172.20.21.1		3306	tcp	7.2	High	VendorFi	Oracle My	This host	Installed	1.3.6.1.4.1	CVE-2015-	849145ac-	SRT411Ph	2022-04-0	464c5f30-(	Successf	Apply the	Oracle	Unspecifi	Checks if	Product:	########	DFN-CERT-2016-1192,DFN-CERT-2016-0845,DFN-CERT-2016-0532,D	
172.20.21.1		3306	tcp	7.2	High	VendorFi	Oracle My	This host	Installed	1.3.6.1.4.1.25623.1.0.	849145ac-	SRT411Ph	2022-04-0	56d8a4e6-	Successf	Upgrade t	Oracle	Multiple e	Checks if	Product:				

Snort Files/Logs collected and sent to Kali



References

Chandel, R., says:, K. O. S. T. I. A. N. T. Y. N., says:, R. C., says:, A. A., & says:, V. (2022, January 12). *How to detect NMAP scan using Snort*. Hacking Articles. Retrieved April 4, 2022, from https://www.hackingarticles.in/detect-nmap-scan-using-snort/

Essche, A. V. (n.d.). *Re: Rule for detecting SSH*. Snort: Re: Rule for detecting ssh. Retrieved April 4, 2022, from https://seclists.org/snort/2014/q2/482

How to use SQLMAP to test a website for SQL injection vulnerability. GeeksforGeeks. (2021, June 28). Retrieved April 4, 2022, from https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/

Hydra: Kali linux tools. Kali Linux. (2022, February 10). Retrieved April 4, 2022, from https://www.kali.org/tools/hydra/

Shah, N. A. (I. C. via S.-users. (n.d.). *Snort rule to detect HTTP post data*. Snort: snort rule to detect HTTP POST data. Retrieved April 4, 2022, from https://seclists.org/snort/2018/q1/317

sinxLoud. (2019, January 22). *How to install DVWA into your linux distribution*. Medium. Retrieved April 4, 2022, from https://medium.datadriveninvestor.com/setup-install-dvwa-into-your-linux-distribution-d76dc3b80357

staff, J. R., Ruostemaa, J., Staff, Janne Ruostemaa Editor-in-chief and Technical writer at UpCloud since 2015. Cloud enthusiast writing about server technology and software., Editor-in-chief and Technical writer at UpCloud since 2015. Cloud enthusiast writing about server technology and software., Says:, B., says:, J. R., Says:, M., says:, J., says:, M. siraj, Says:, A., says:, S. M. S., says:, C. J., Says:, M., says:, J., says:, M. M., says:, I., says:, K., says:, A. D., … says:, T. T. (2021, August 5). *How to install Snort on ubuntu*. UpCloud. Retrieved April 4, 2022, from https://upcloud.com/community/tutorials/install-snort-ubuntu/