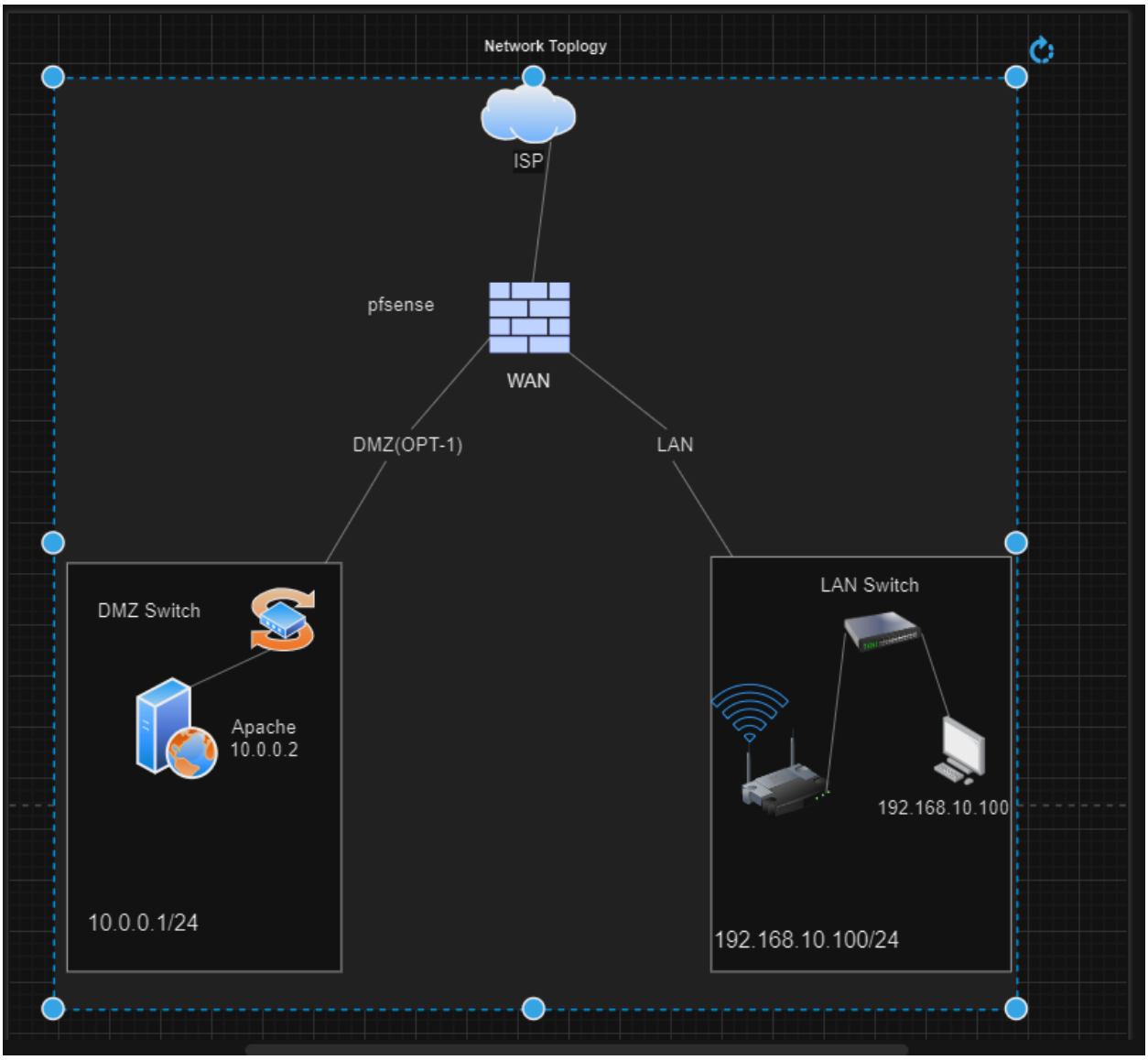
Name: Momenah Saif	**Roll No.:**21I-1909	**Section:**CY-T5

Assignment-2

Part 1:



The above topology shows how pfsense firewall works when we make LAN and DMZ using pfsense. The internet is connected to DMZ and LAN but between that connect pfsense is present that filters out any malicious traffic. The web server is connected to DMZ switch while computer and router is connected to LAN switch.

Part 2:

Installed pfsense and two Kali Linux Machines on Virtual box and set their network adapters:

- PFSENSE:

  Adapter 1: NAT (WAN was not working on Bridged)

  Adapter 2: Internal Network(Pfsense)

  Adapter 3: Bridged Network(Wireless)

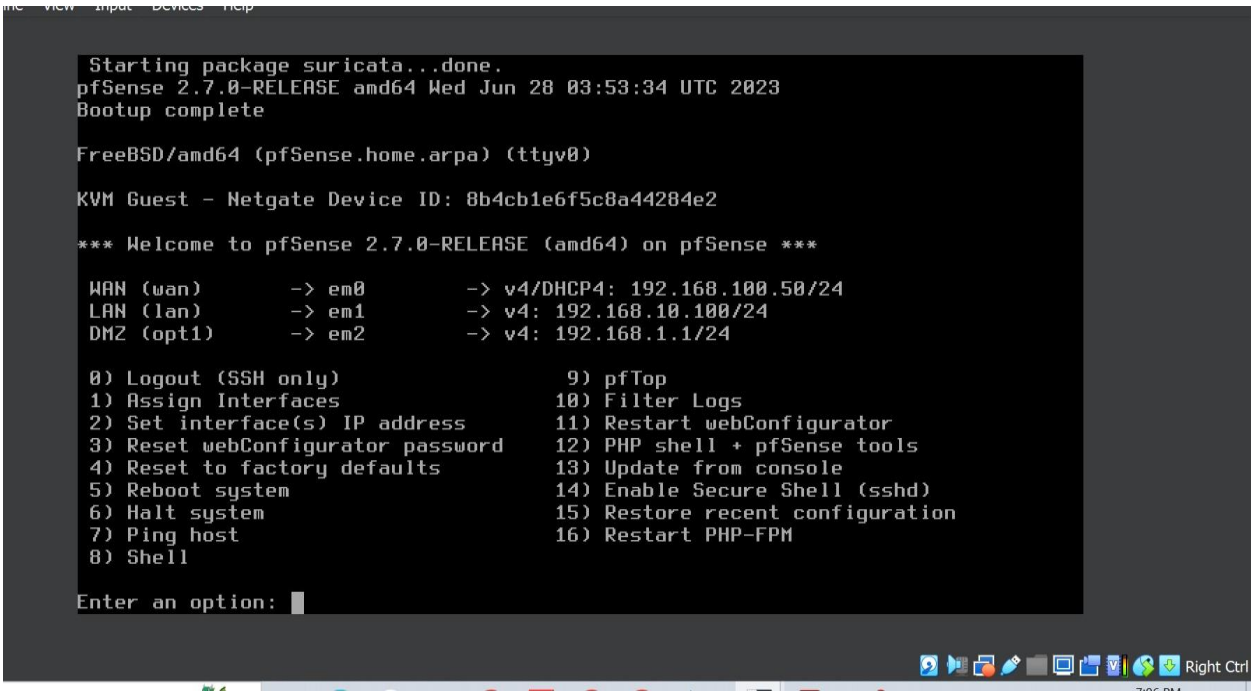
- Kali1:

  Adapter 1: Internal Network(Pfsense)

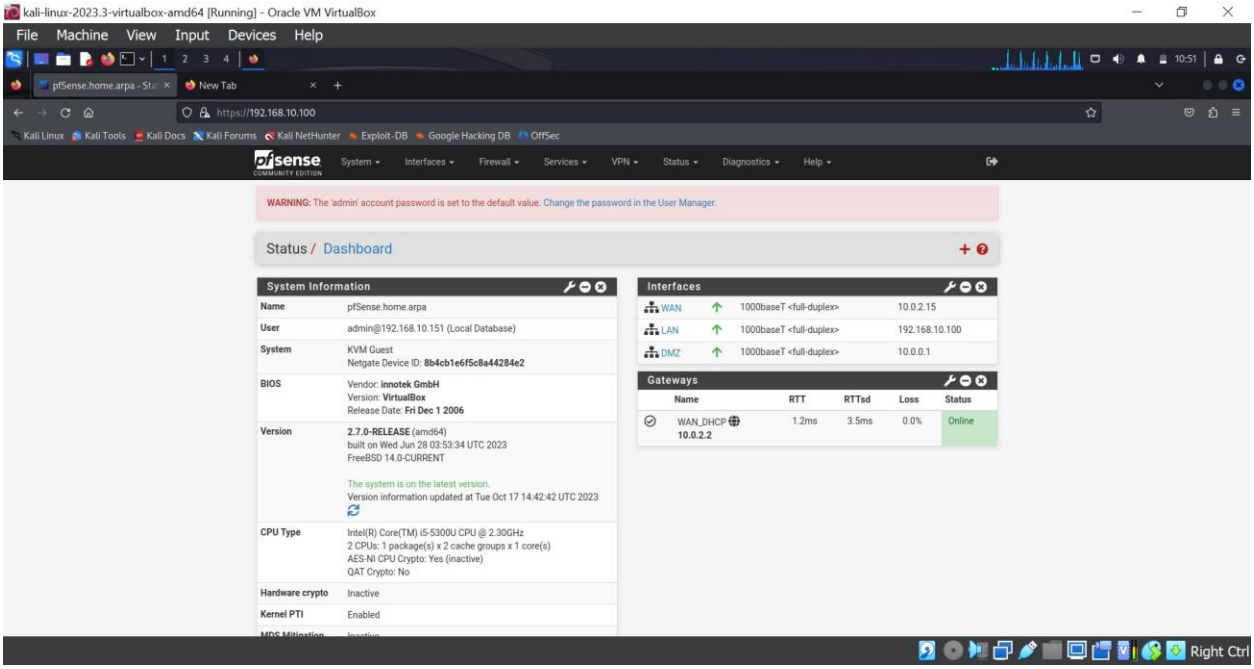
- Kali2(DMZ):

  Adapter 1: Internal Network(Pfsense)

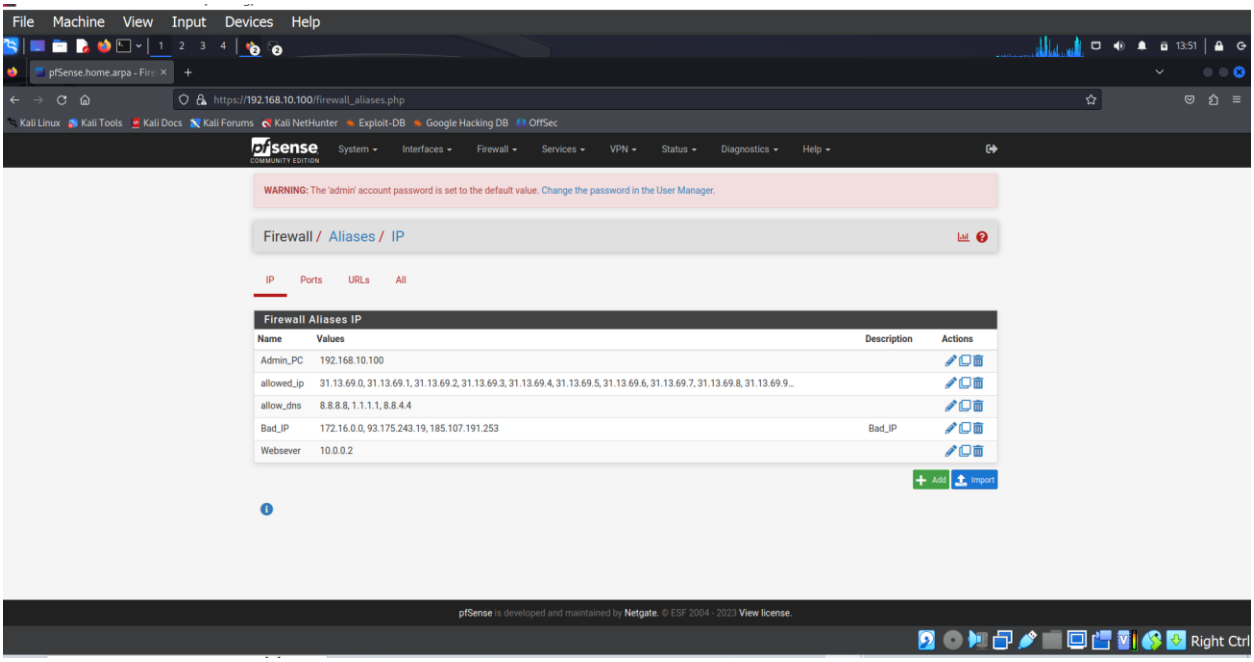
After installation and powering on pfsense (took screenshot after configuring DMZ so OPT1 is named as DMZ)



Opened pfsense LAN on Kali1 using LAN IP 192.168.10.100 that was set as static on pfsense (Had to change from 192.168.1.1 because it was not working due to IPV4(Ethernet) of my computer)

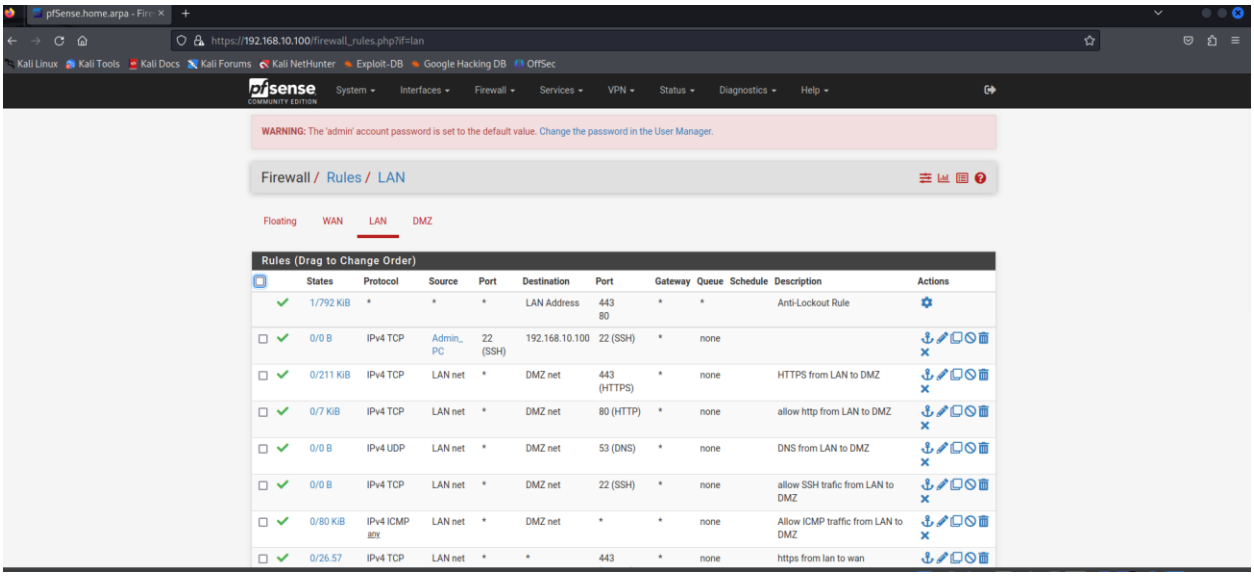


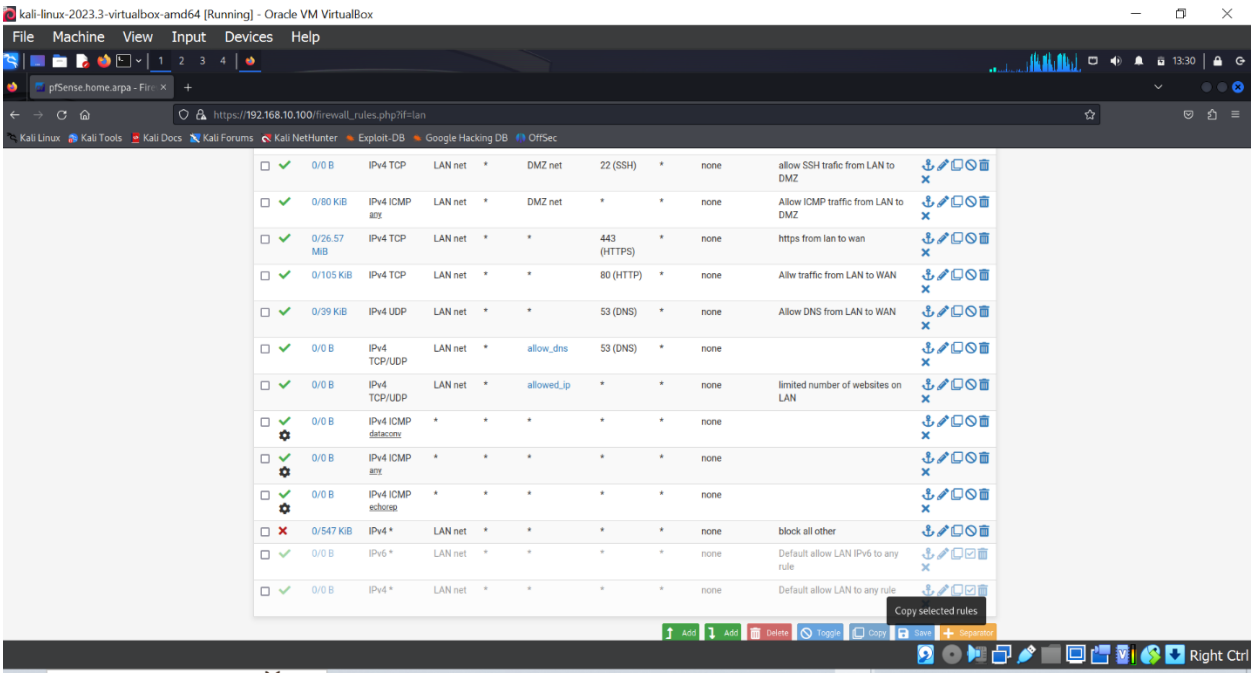
To set rules for firewall some Aliases was needed

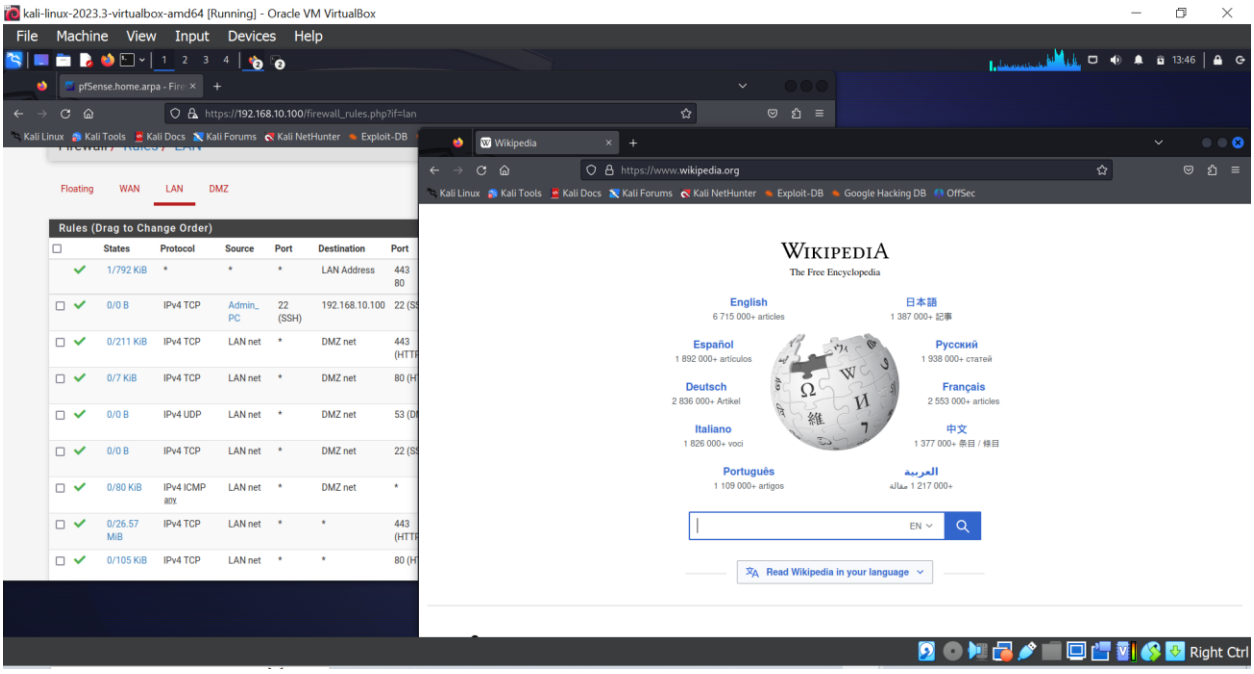


Set Firewall rules of LAN, WAN to access ports and IPs.

LAN:

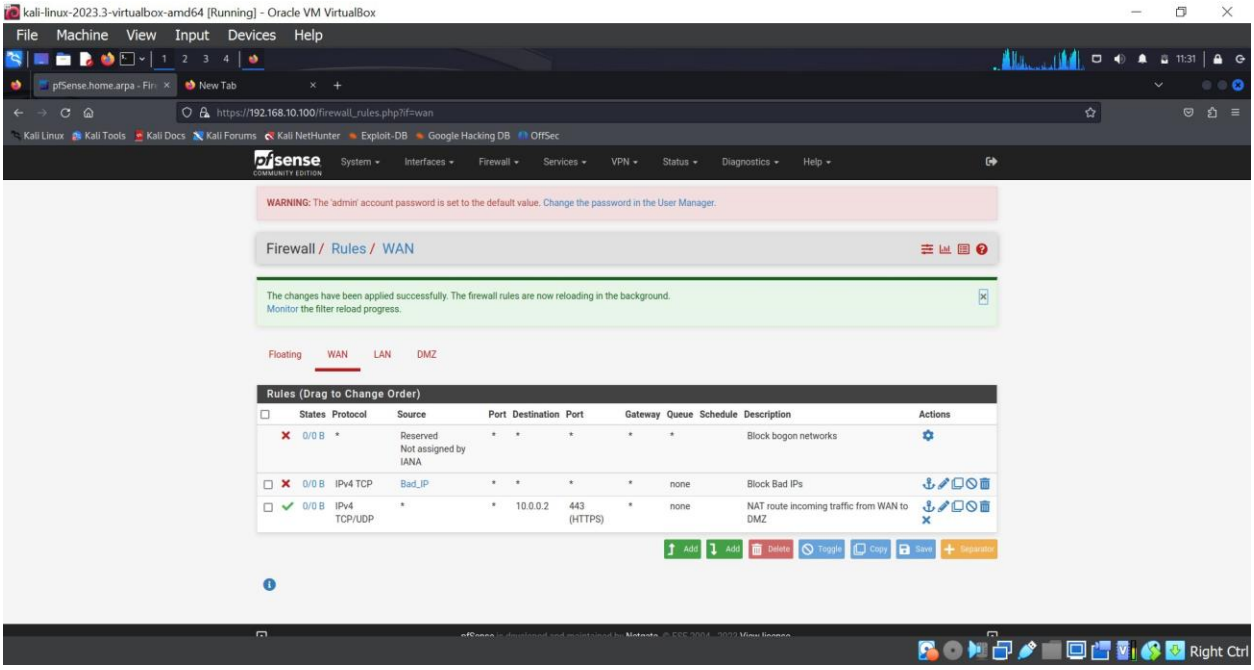




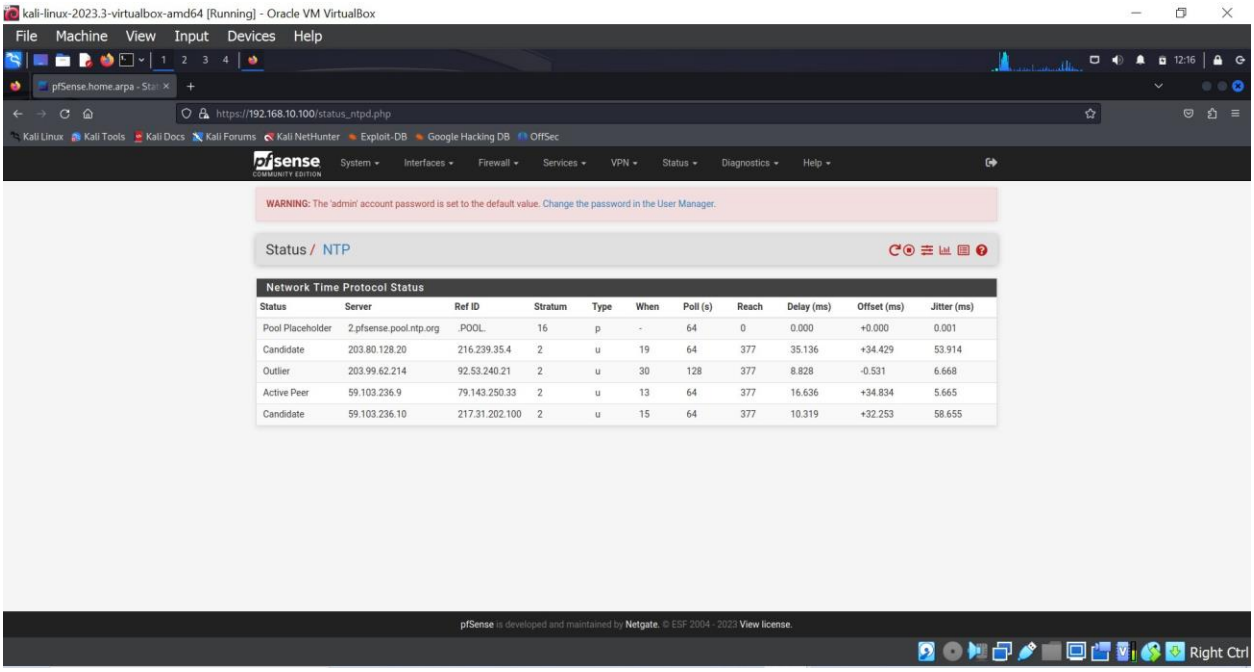


Internet can now be accessed, I opened Wikipedia

WAN:



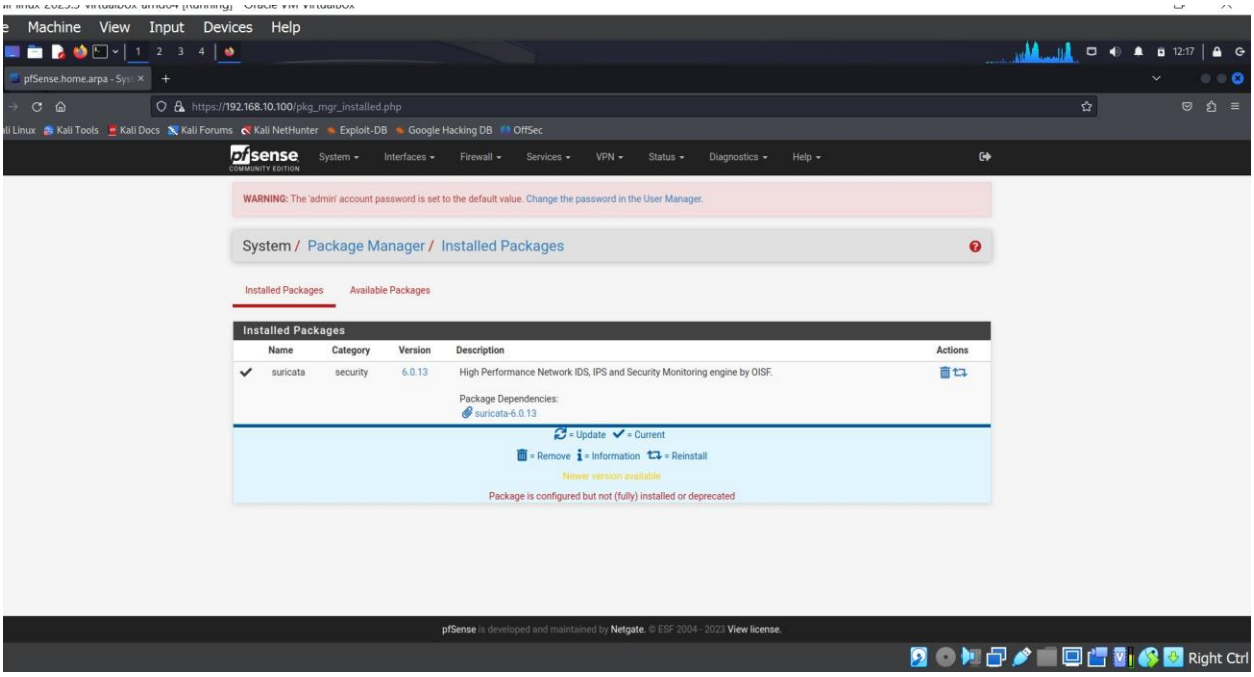
The NTP is also working.



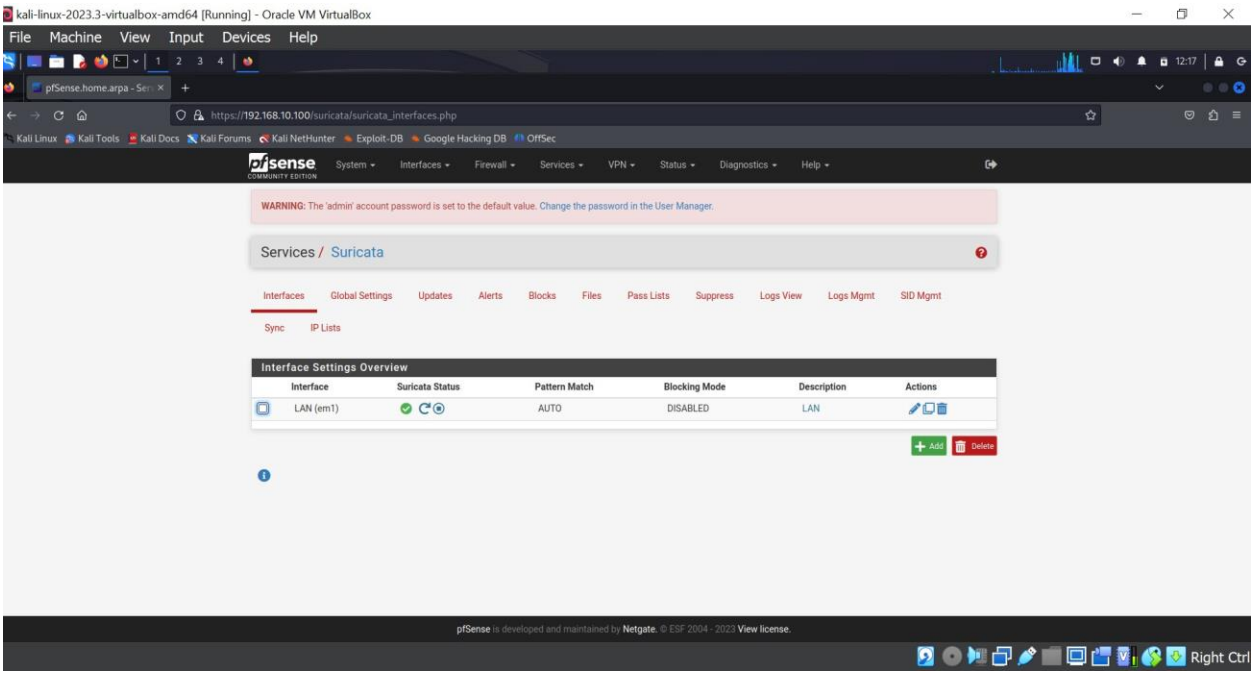
Status	Server	Ref ID	Stratum	Type	When	Poll (s)	Reach	Delay (ms)	Offset (ms)	Jitter (ms)
Pool Placeholder	2.pfsense.pool.ntp.org	.POOL.	16	p	-	64	0	0.000	+0.000	0.001
Candidate	203.80.128.20	216.239.35.4	2	u	19	64	377	35.136	+34.429	53.914
Outlier	203.99.62.214	92.53.240.21	2	u	30	128	377	8.828	-0.531	6.668
Active Peer	59.103.236.9	79.143.250.33	2	u	13	64	377	16.636	+34.834	5.665
Candidate	59.103.236.10	217.31.202.100	2	u	15	64	377	10.319	+32.253	58.655

Part 3:

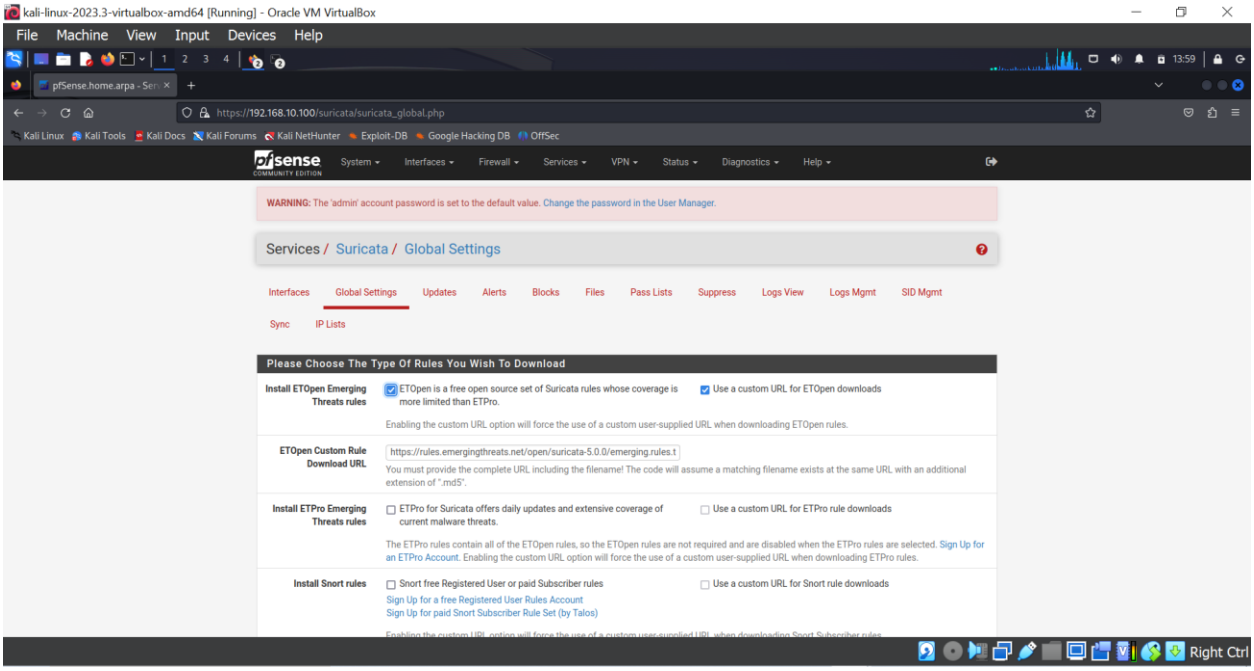
First went into Package Manager and installed Suricata.



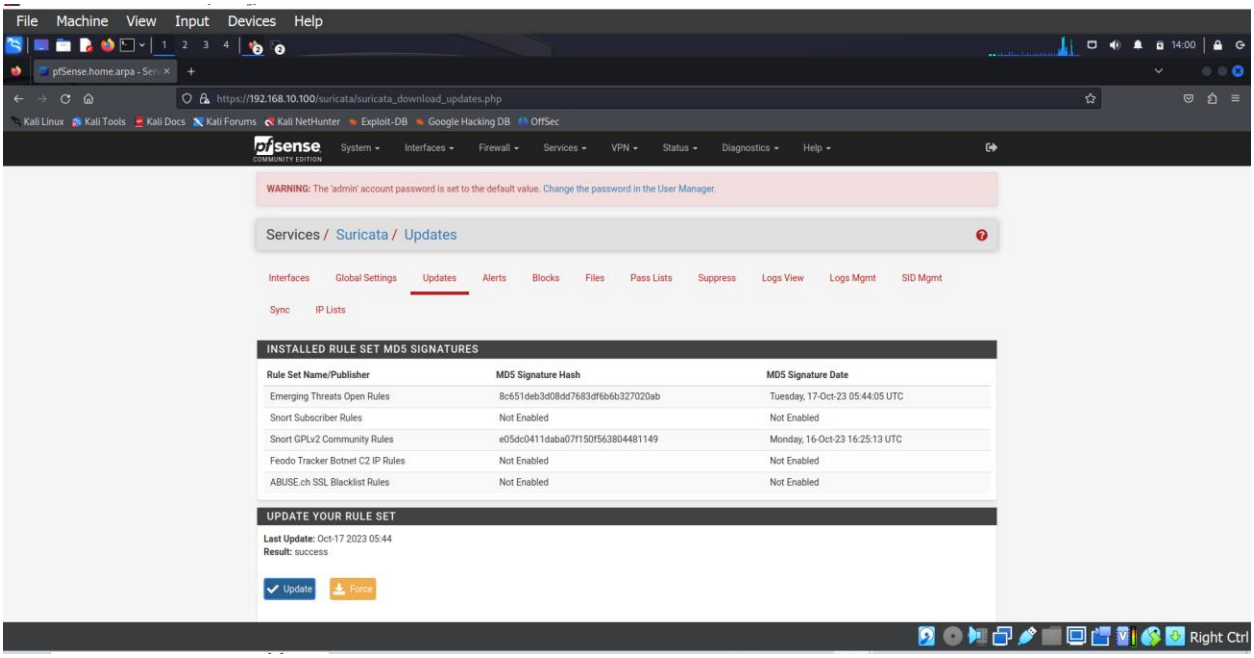
Went into Suricata interfaces in services and created a LAN interface through Add button.



Then went into global settings and selected options and added URL



Updated the rules

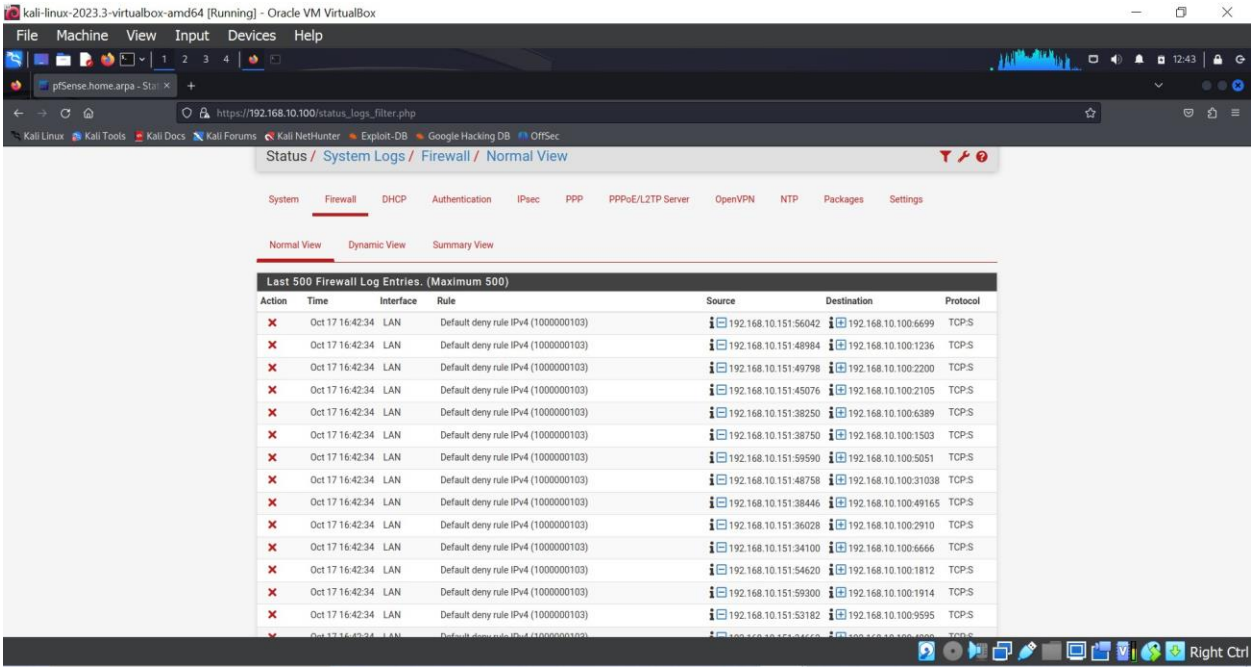


Went into LAN interface and edited it. Choose some made LAN Rules and added a Custom Rule regarding UDP. After that had to check Alerts but they were not coming so did

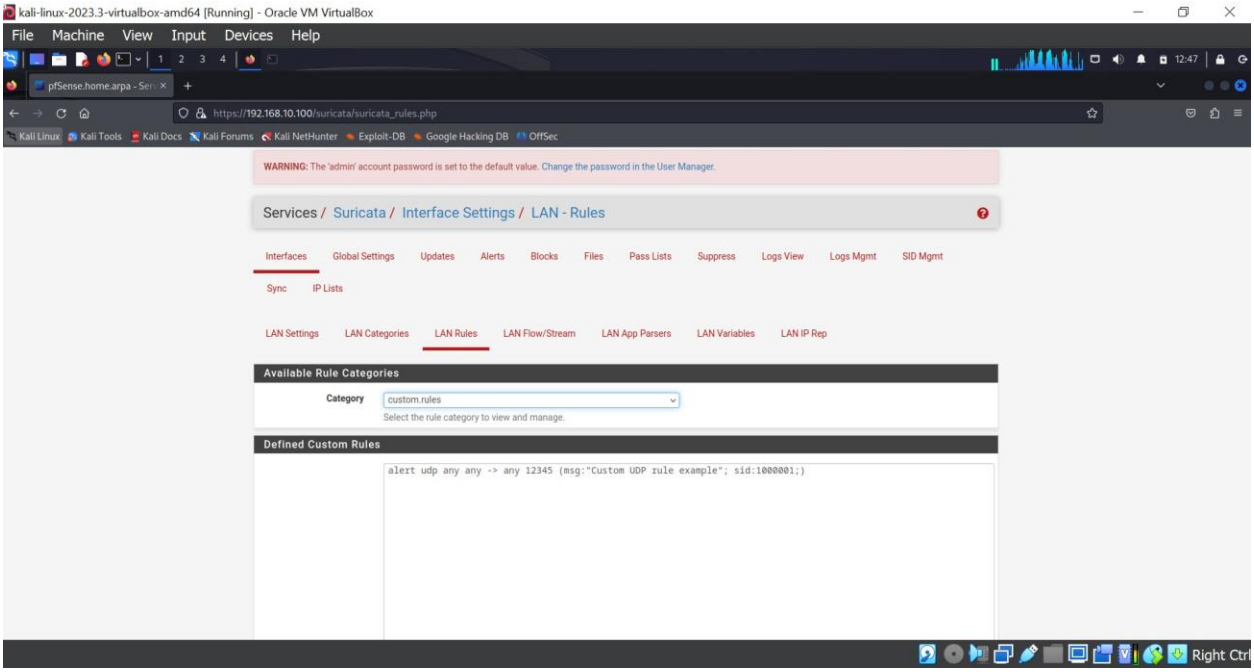
```
┌──(kali㉿kali1)-[~]
└─$ nmap -p- -A 192.168.10.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 13:44 EDT
Nmap scan report for 192.168.10.100
Host is up (0.0017s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
|_http-title: Did not follow redirect to https://192.168.10.100/
443/tcp open  ssl/http nginx
| ssl-cert: Subject: commonName=pfSense-651fa1dcbab6d/organizationName=pfSense webConfigurator Self-Signed Certificate
| Subject Alternative Name: DNS:pfSense-651fa1dcbab6d
| Not valid before: 2023-10-06T05:57:48
|_Not valid after:  2024-11-07T05:57:48
|_http-title: pfSense - Login
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|_  http/0.9

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.28 seconds

┌──(kali㉿kali1)-[~]
└─$
```

Check Suricata is working, send some packets through nmap and checked logs

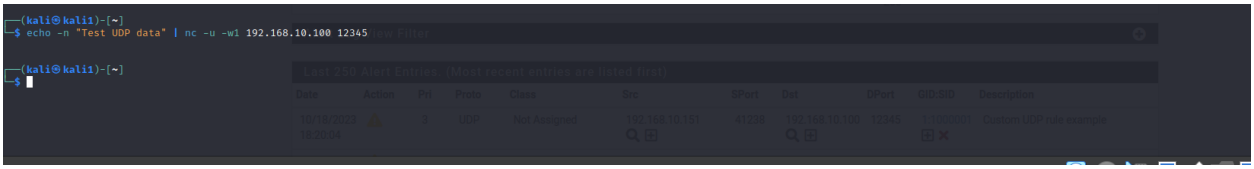
```
┌──(root㉿kali1)-[/home/kali/Desktop]
└─# nmap -sT -T4 -v 192.168.10.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-17 12:42 EDT
Initiating ARP Ping Scan at 12:42
Scanning 192.168.10.100 [1 port]
Completed ARP Ping Scan at 12:42, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:42
Completed Parallel DNS resolution of 1 host. at 12:42, 13.00s elapsed
Initiating Connect Scan at 12:42
Scanning 192.168.10.100 [1000 ports]
Discovered open port 443/tcp on 192.168.10.100
Discovered open port 80/tcp on 192.168.10.100
Completed Connect Scan at 12:42, 4.94s elapsed (1000 total ports)
Nmap scan report for 192.168.10.100
Host is up (0.0013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:95:29:A9 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 18.38 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

┌──(root㉿kali1)-[/home/kali/Desktop]
└─#
```



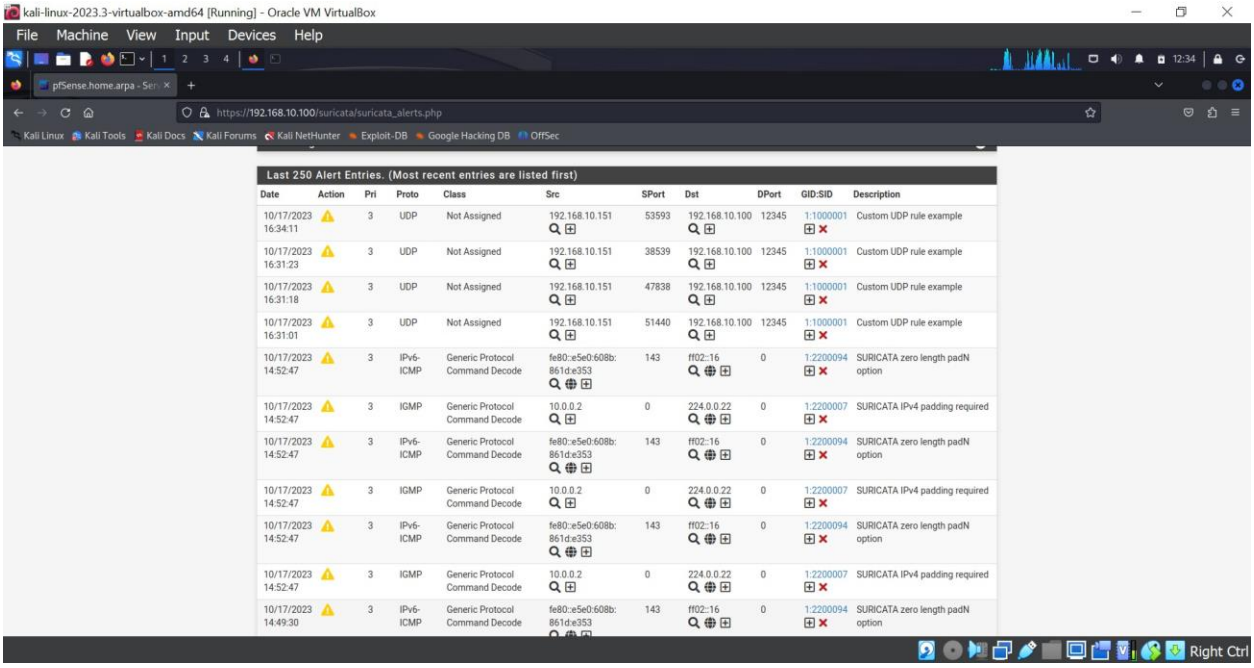
Made Custom rule



Generated test data for the custom rule and checked Alerts



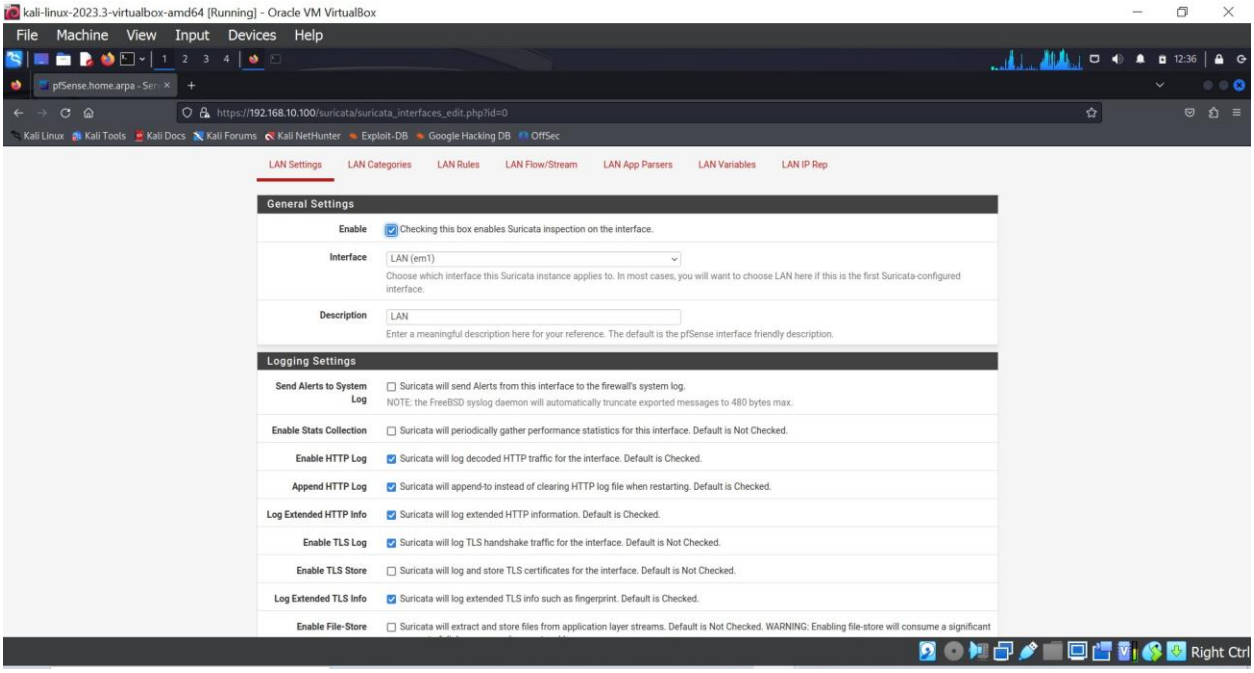
```
┌──(kali㉿kali1)-[~]
└─$ echo -n "Test UDP data" | nc -u -w1 192.168.10.100 12345

┌──(kali㉿kali1)-[~]
└─$ 
```



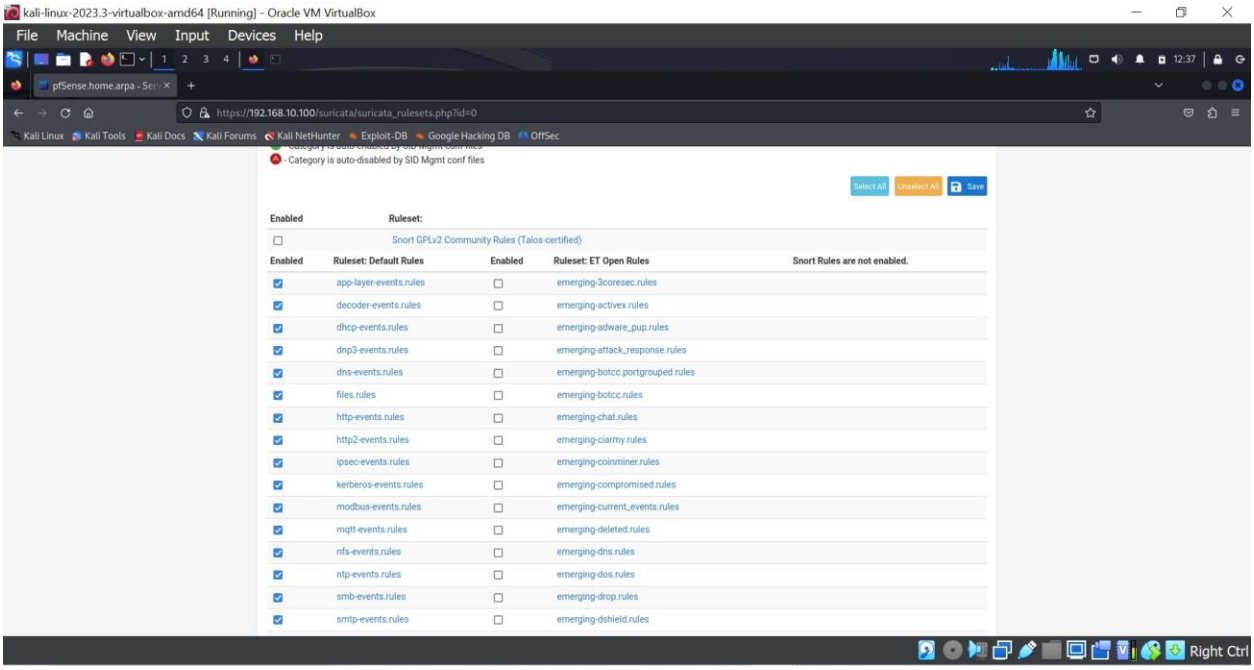
Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
10/17/2023 16:34:11	⚠	3	UDP	Not Assigned	192.168.10.151	53593	192.168.10.100	12345	1:1000001	Custom UDP rule example
10/17/2023 16:31:23	⚠	3	UDP	Not Assigned	192.168.10.151	38539	192.168.10.100	12345	1:1000001	Custom UDP rule example
10/17/2023 16:31:18	⚠	3	UDP	Not Assigned	192.168.10.151	47838	192.168.10.100	12345	1:1000001	Custom UDP rule example
10/17/2023 16:31:01	⚠	3	UDP	Not Assigned	192.168.10.151	51440	192.168.10.100	12345	1:1000001	Custom UDP rule example
10/17/2023 14:52:47	⚠	3	IPv6-ICMP	Generic Protocol Command Decode	fe80::e5e0:608b:861d:e353	143	ff02::16	0	1:2200094	SURICATA zero length padN option
10/17/2023 14:52:47	⚠	3	IGMP	Generic Protocol Command Decode	10.0.0.2	0	224.0.0.22	0	1:2200007	SURICATA IPv4 padding required
10/17/2023 14:52:47	⚠	3	IPv6-ICMP	Generic Protocol Command Decode	fe80::e5e0:608b:861d:e353	143	ff02::16	0	1:2200094	SURICATA zero length padN option
10/17/2023 14:52:47	⚠	3	IGMP	Generic Protocol Command Decode	10.0.0.2	0	224.0.0.22	0	1:2200007	SURICATA IPv4 padding required
10/17/2023 14:52:47	⚠	3	IPv6-ICMP	Generic Protocol Command Decode	fe80::e5e0:608b:861d:e353	143	ff02::16	0	1:2200094	SURICATA zero length padN option
10/17/2023 14:52:47	⚠	3	IGMP	Generic Protocol Command Decode	10.0.0.2	0	224.0.0.22	0	1:2200007	SURICATA IPv4 padding required
10/17/2023 14:49:30	⚠	3	IPv6-ICMP	Generic Protocol Command Decode	fe80::e5e0:608b:861d:e353	143	ff02::16	0	1:2200094	SURICATA zero length padN option

Changed in general settings allow Suricata IDS on this interface and enable all other logs related to HTTP.

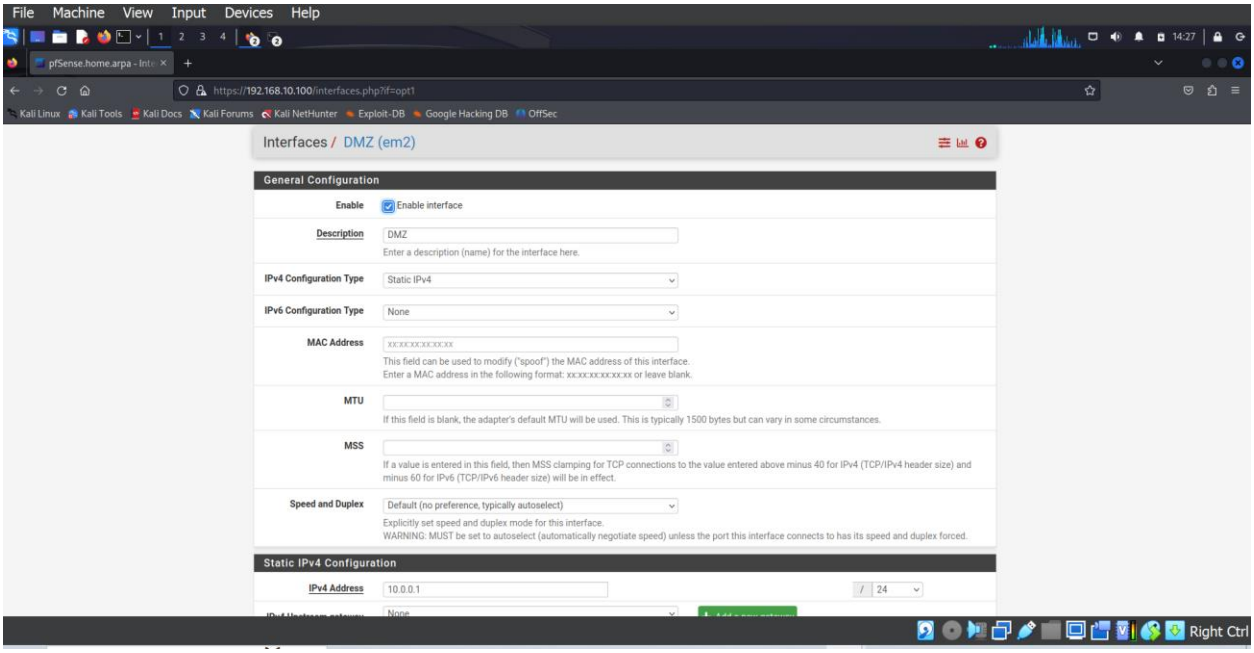


In the IDS selected the rulesets in which there are many rulesets and every set will give an alert on event occurring related to that ruleset.

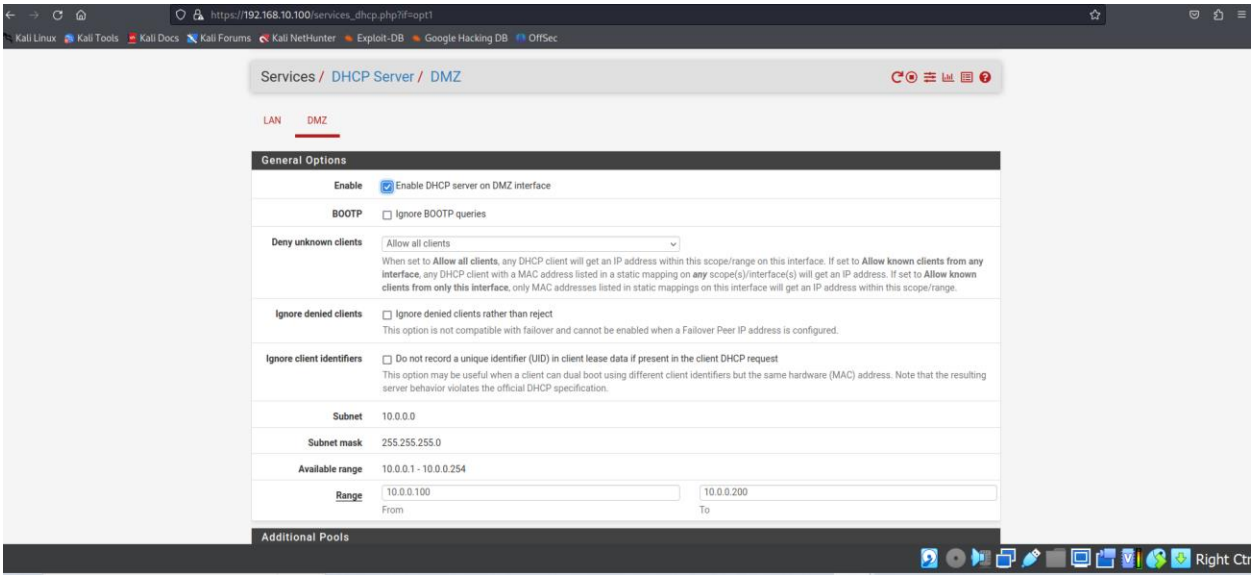


Part 4:

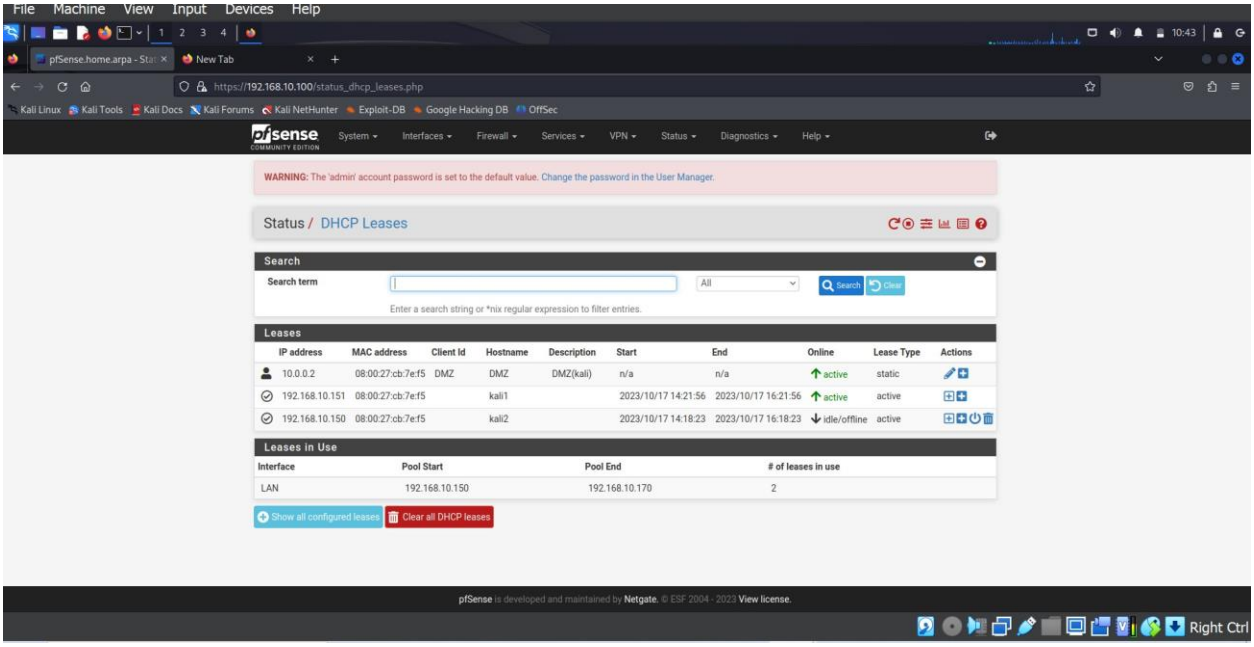
Changed OPT1 to DMZ and gave a range which is 10.0.0.1

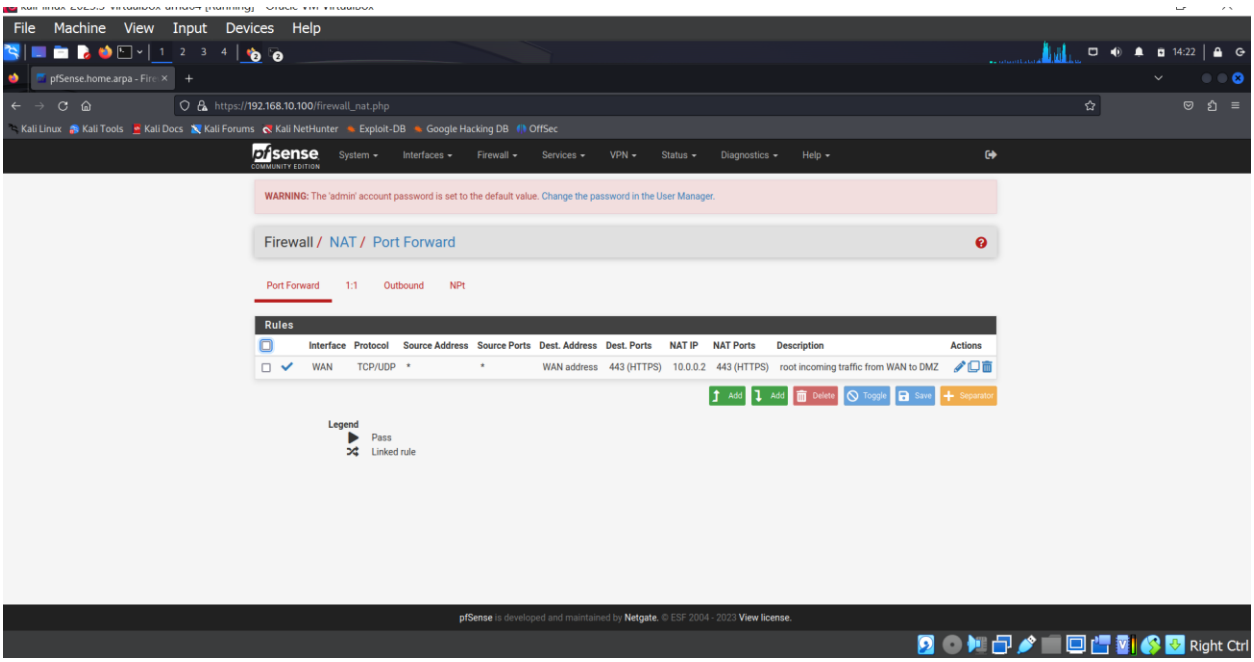


Set DHCP and made a DHCP Static Mapping of kali, made it DMZ by MAC and gave it an IP.

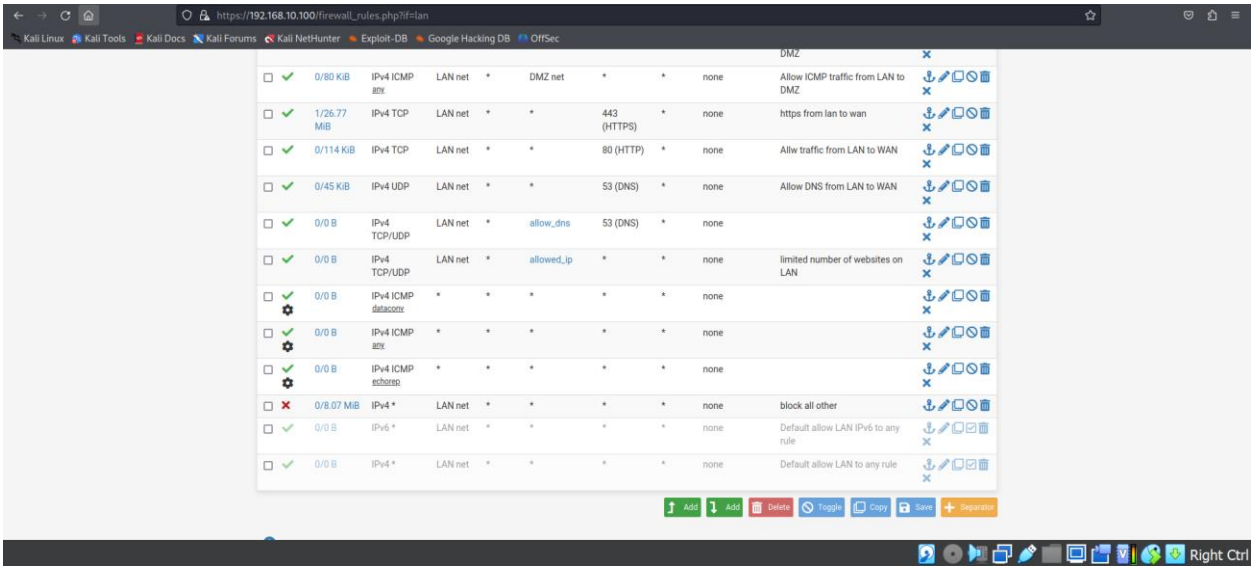


Shows in DHCP Leases



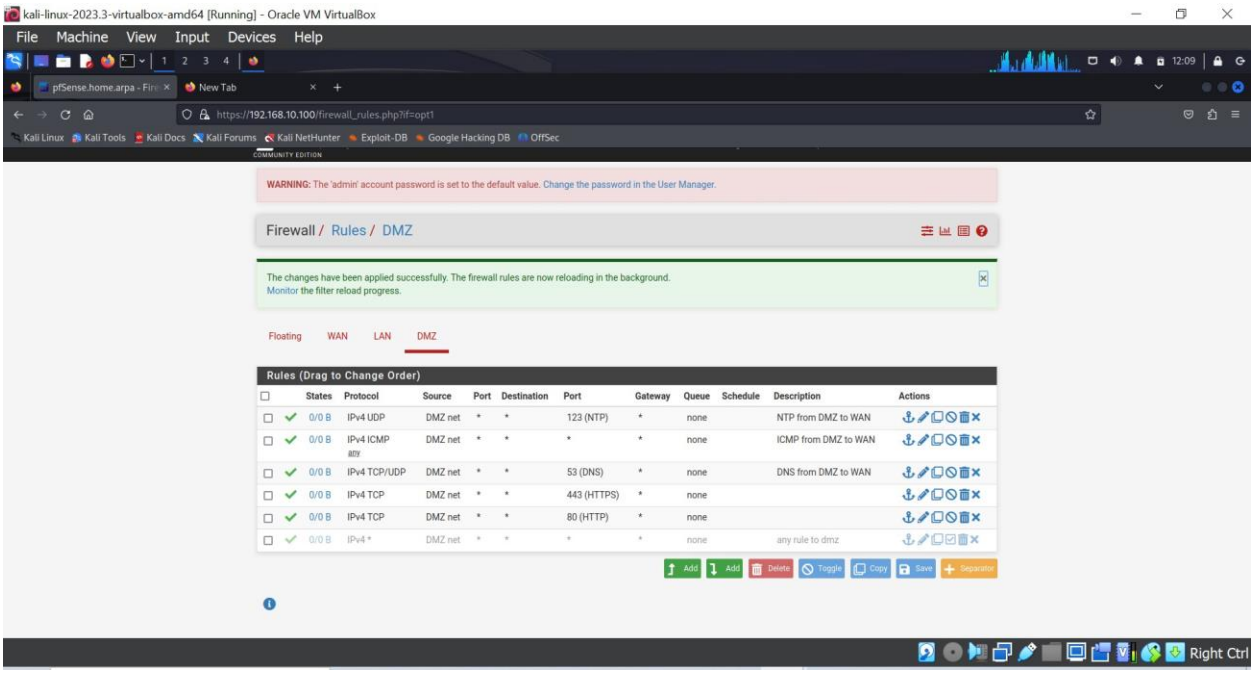


Made a NAT port forwarding rule in which WAN in using TCP/UDP to access the website. Now that website can be open through WAN anywhere using servers IP.

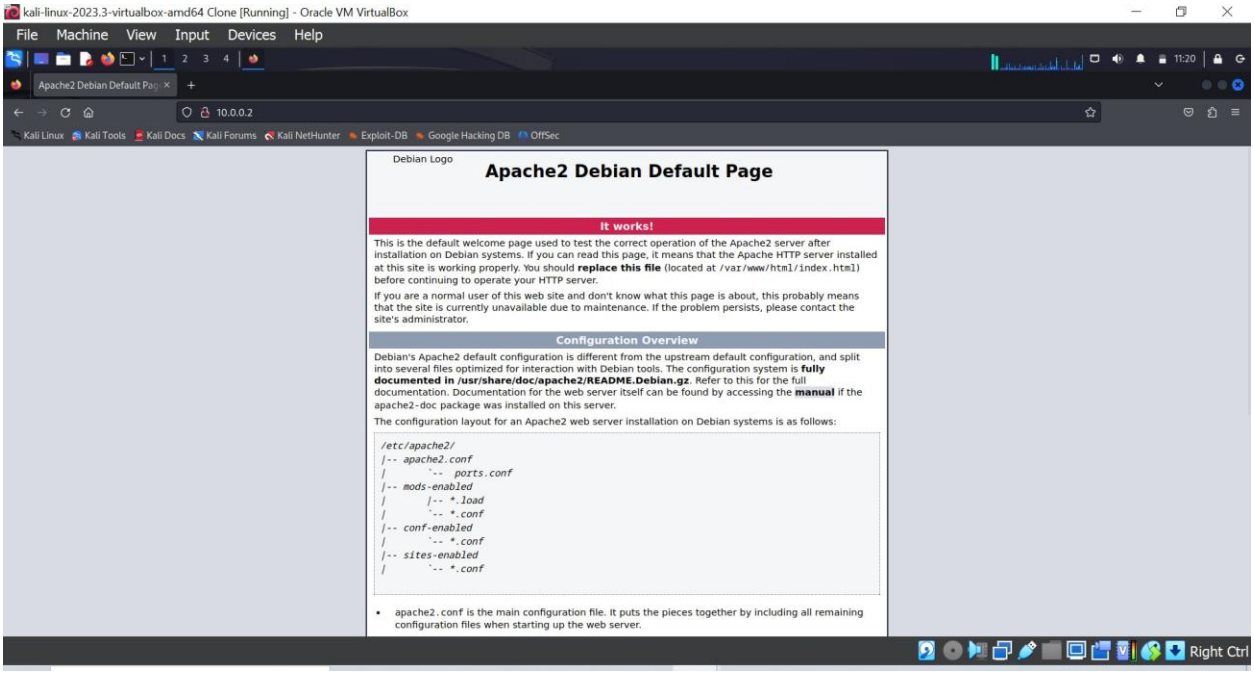


Added ICMP and Allowed Ip rules in LAN and changed Max states, Max scr nodes and Max scr states to 3.

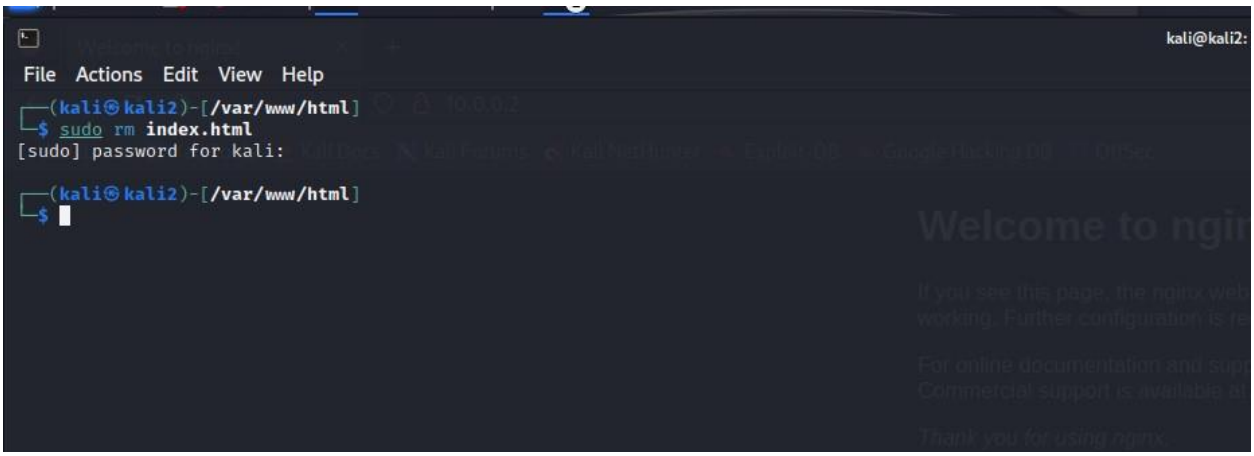
DMZ (OPT 1) firewall rules:



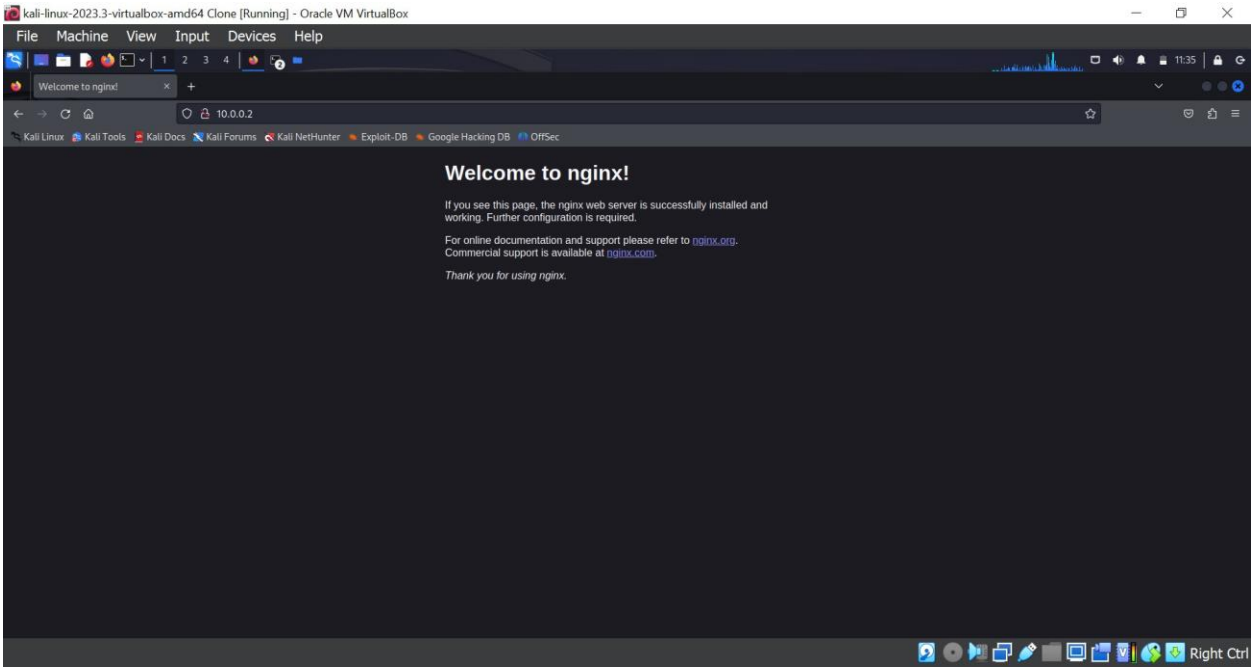
Apache server opened on DMZ(kali) FireFox with IP given which is 10.0.0.2



Installed nginx and disabled apache2. Started nginx and enabled it. Still the page of nginx didn't appear. Used the following command and deleted the default file index.html.



Refreshed the apache page



Problems Occurred:

1. A memory error occurred when installing pfsense iso file. Came on both VMware and Virtual box. Got a Virtual box image file from a friend in which memory settings were already selected.
2. After that added kali to Virtual box but the LAN page wouldn't open. Had to set IPv4 of my computer's Ethernet and gave static IP to LAN in the same range through option 2 on pfsense.
3. DHCP wouldn't work. Added IP of kali but in DHCP Leases no Leases in use showed. Had to set some DNS setting of Virtual box.
4. In Suricata installation, after installation the web page shows that it will restart in 20 seconds and timer starts. After every end of timer, the timer starts from 20 again. Solved the issue by using another Virtual Disk image with Suricata installed.
5. Configured DMZ and had to shut down pfsense. Next time opened pfsense the LAN web page won't open. Had to install pfsense on virtual box again.
6. After writing rules of LAN and WAN, the websites from internet couldn't be accessed. Changed DNS name server of kali and changed network settings from Bridged to NAT.
7. Tried to make second kali. Every time virtual machine would give error of same UUID. Clone was also rejected. Restarted Laptop, Clone option worked.
8. The hostname and MAC of both kali where same due to which DHCP and DMZ was creating problems. Changed both.
9. DMZ shows 10.0.0.2 IP as active and internet could be accessed but apache wouldn't open.
10. After Global Settings of Suricata, the update would go failed every time. Changed WAN to DHCP and then it started on show success in Update.
11. The MAC address of Kali and Cloned Kali was same due to which I couldn't access apache default page. Changed the MAC of Clone IP and also changed in DHCP server.