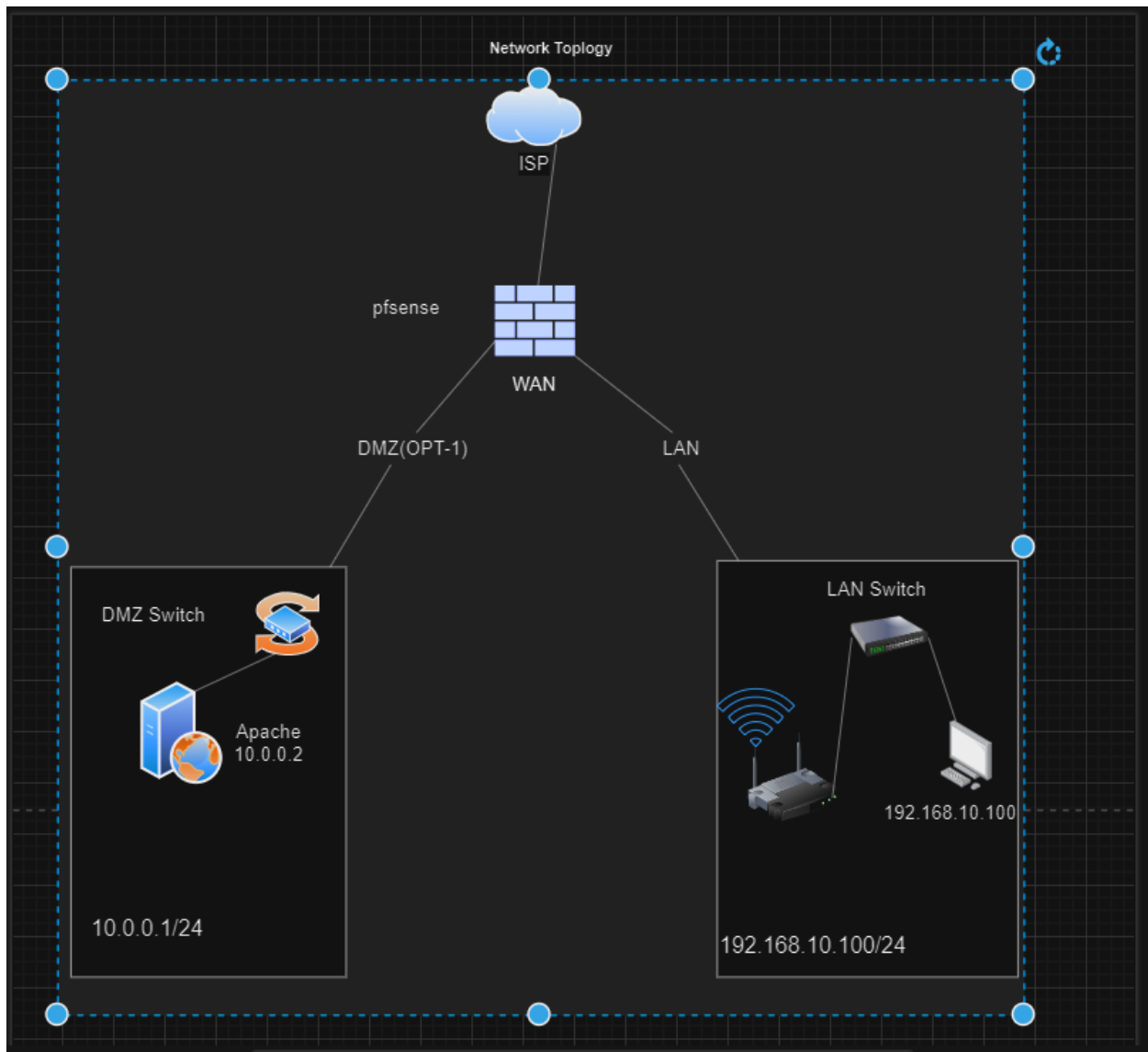


Assignment-2

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)

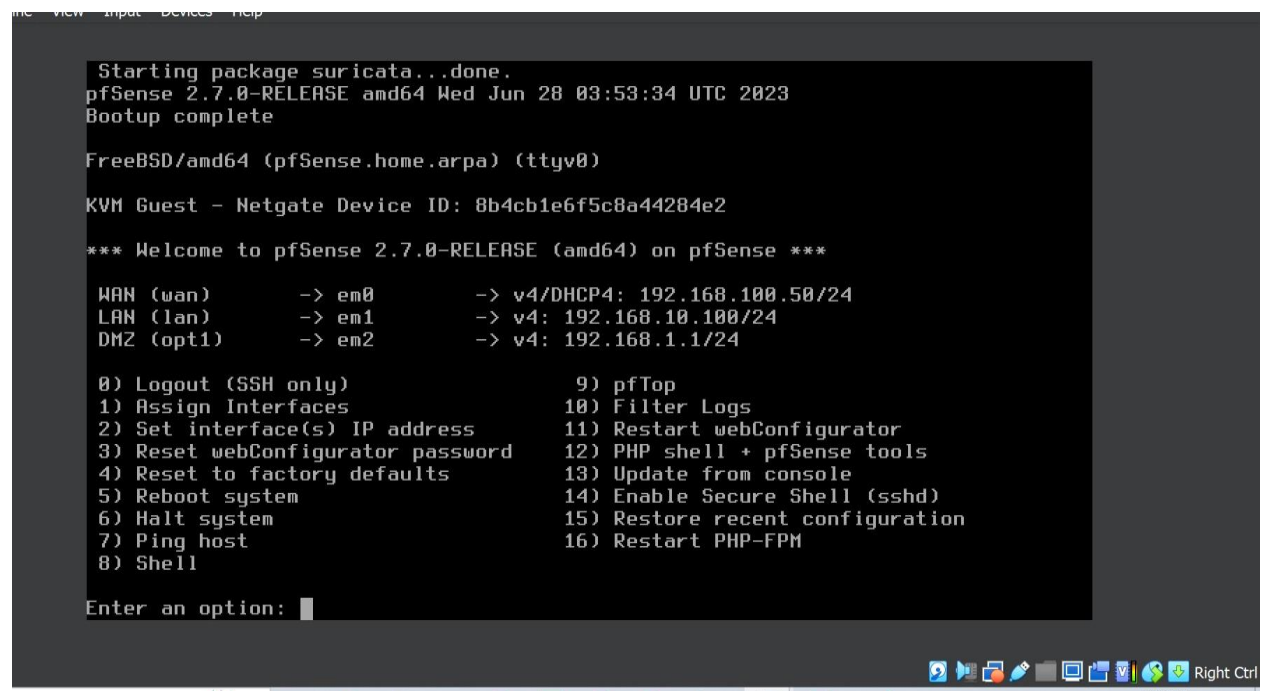
- Kali1:

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)



```
Starting package suricata...done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
KVM Guest - Netgate Device ID: 8b4cb1e6f5c8a44284e2

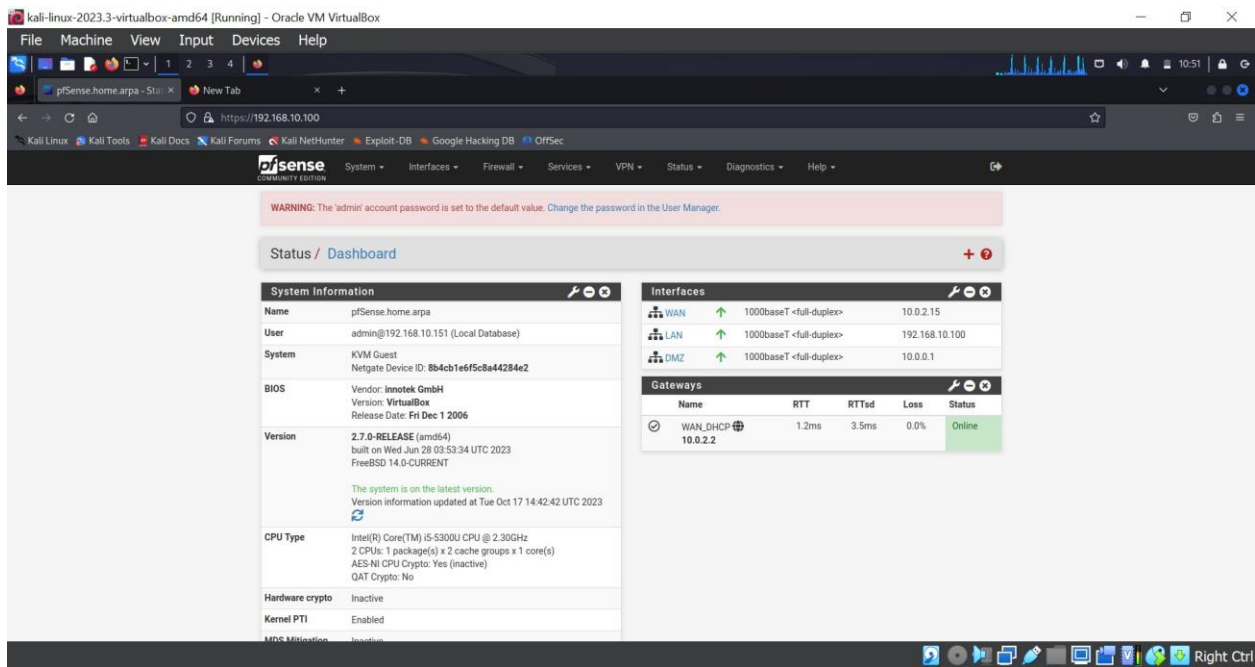
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.100.50/24
LAN (lan)      -> em1      -> v4: 192.168.10.100/24
DMZ (opt1)     -> em2      -> v4: 192.168.1.1/24

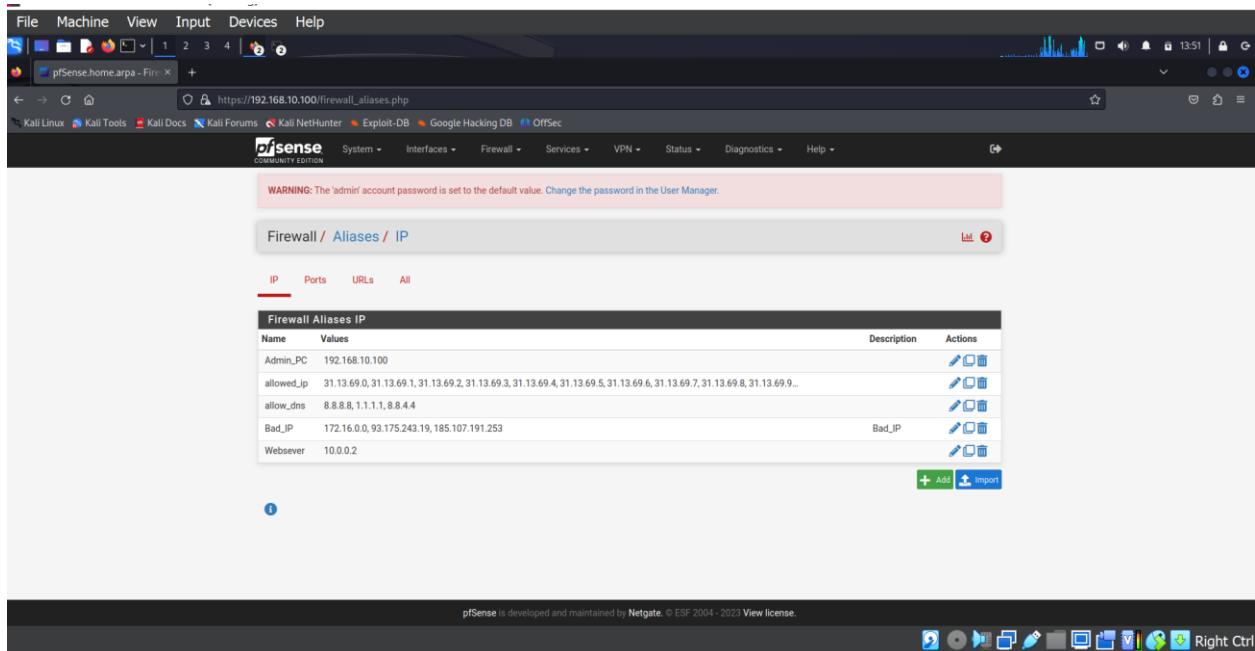
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

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:

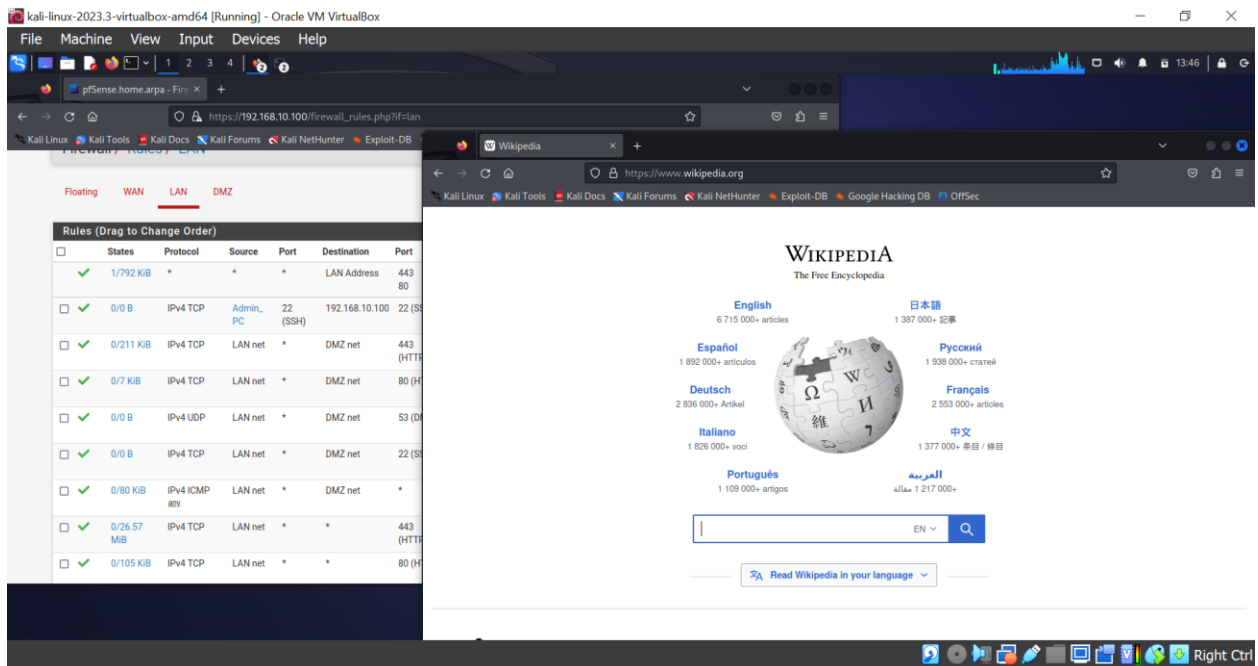
The screenshot shows the pfSense web interface for the LAN firewall rules. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Firewall / Rules / LAN" breadcrumb is visible. The "Rules (Drag to Change Order)" table lists the following rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1/792 KIB	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	[Settings]
0/0 B	IPv4 TCP	Admin PC	22 (SSH)	192.168.10.100	22 (SSH)	*	none	*		[Down] [Up] [Edit] [Delete]
0/211 KIB	IPv4 TCP	LAN net	*	DMZ net	443 (HTTPS)	*	none	*	HTTPS from LAN to DMZ	[Down] [Up] [Edit] [Delete]
0/7 KIB	IPv4 TCP	LAN net	*	DMZ net	80 (HTTP)	*	none	*	allow http from LAN to DMZ	[Down] [Up] [Edit] [Delete]
0/0 B	IPv4 UDP	LAN net	*	DMZ net	53 (DNS)	*	none	*	DNS from LAN to DMZ	[Down] [Up] [Edit] [Delete]
0/0 B	IPv4 TCP	LAN net	*	DMZ net	22 (SSH)	*	none	*	allow SSH traffic from LAN to DMZ	[Down] [Up] [Edit] [Delete]
0/80 KIB	IPv4 ICMP	LAN net	*	DMZ net	*	*	none	*	Allow ICMP traffic from LAN to DMZ	[Down] [Up] [Edit] [Delete]
0/26.57	IPv4 TCP	LAN net	*	*	443	*	none	*	https from lan to wan	[Down] [Up] [Edit] [Delete]

This screenshot shows the same pfSense Firewall Rules for the LAN interface, but with a "Copy selected rules" button at the bottom right of the table. The rules listed are:

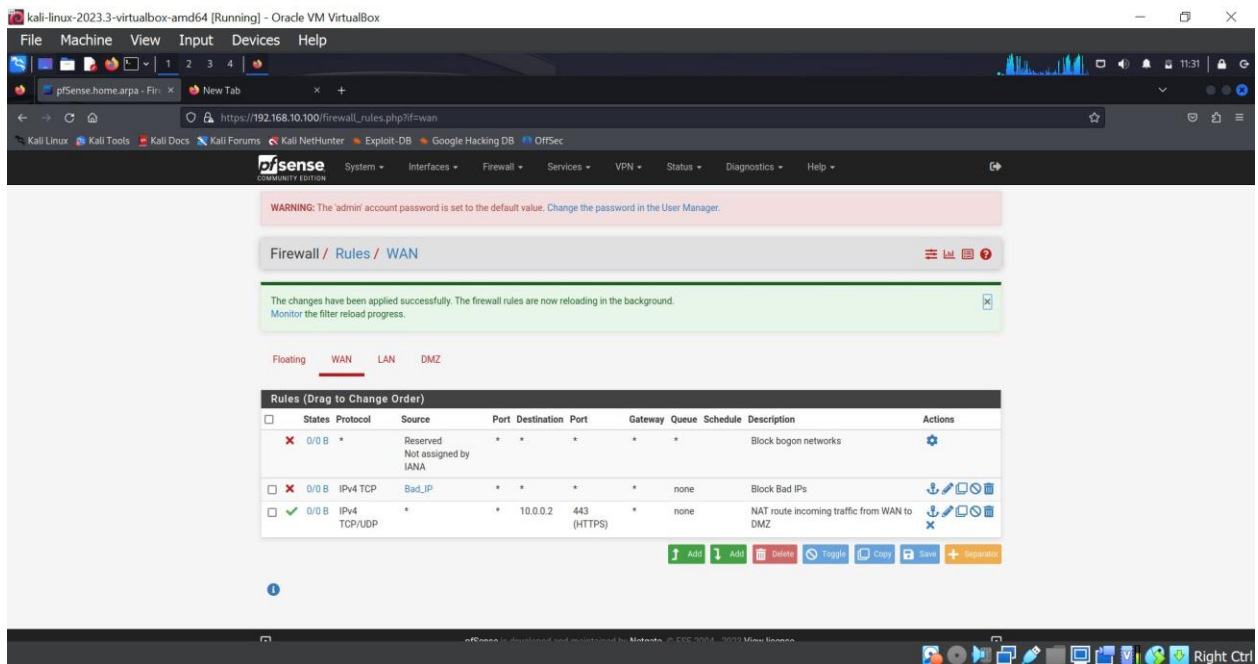
0/0 B	IPv4 TCP	LAN net	*	DMZ net	22 (SSH)	*	none	*	allow SSH traffic from LAN to DMZ	[Down] [Up] [Edit] [Delete]
0/80 KIB	IPv4 ICMP	LAN net	*	DMZ net	*	*	none	*	Allow ICMP traffic from LAN to DMZ	[Down] [Up] [Edit] [Delete]
0/26.57 MIB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none	*	https from lan to wan	[Down] [Up] [Edit] [Delete]
0/105 KIB	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none	*	Allow traffic from LAN to WAN	[Down] [Up] [Edit] [Delete]
0/29 KIB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none	*	Allow DNS from LAN to WAN	[Down] [Up] [Edit] [Delete]
0/0 B	IPv4 TCP/UDP	LAN net	*	allow_dns	53 (DNS)	*	none	*		[Down] [Up] [Edit] [Delete]
0/0 B	IPv4 TCP/UDP	LAN net	*	allowed_ip	*	*	none	*	limited number of websites on LAN	[Down] [Up] [Edit] [Delete]
0/0 B	IPv4 ICMP	datacom	*	*	*	*	none	*		[Down] [Up] [Edit] [Delete]
0/0 B	IPv4 ICMP	net	*	*	*	*	none	*		[Down] [Up] [Edit] [Delete]
0/0 B	IPv4 ICMP	school	*	*	*	*	none	*		[Down] [Up] [Edit] [Delete]
0/547 KIB	IPv4 *	LAN net	*	*	*	*	none	*	block all other	[Down] [Up] [Edit] [Delete]
0/0 B	IPv6 *	LAN net	*	*	*	*	none	*	Default allow LAN IPv6 to any rule	[Down] [Up] [Edit] [Delete]
0/0 B	IPv4 *	LAN net	*	*	*	*	none	*	Default allow LAN to any rule	[Down] [Up] [Edit] [Delete]

Copy selected rules

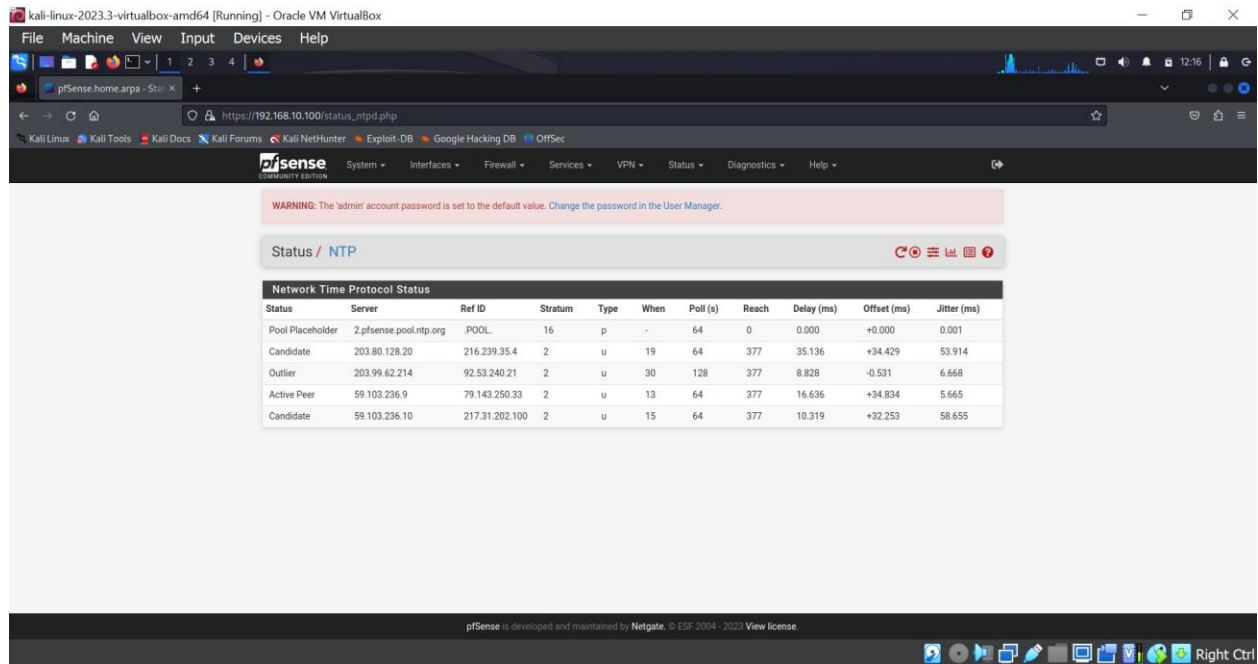


Internet can now be accessed, I opened Wikipedia

WAN:



The NTP is also working.



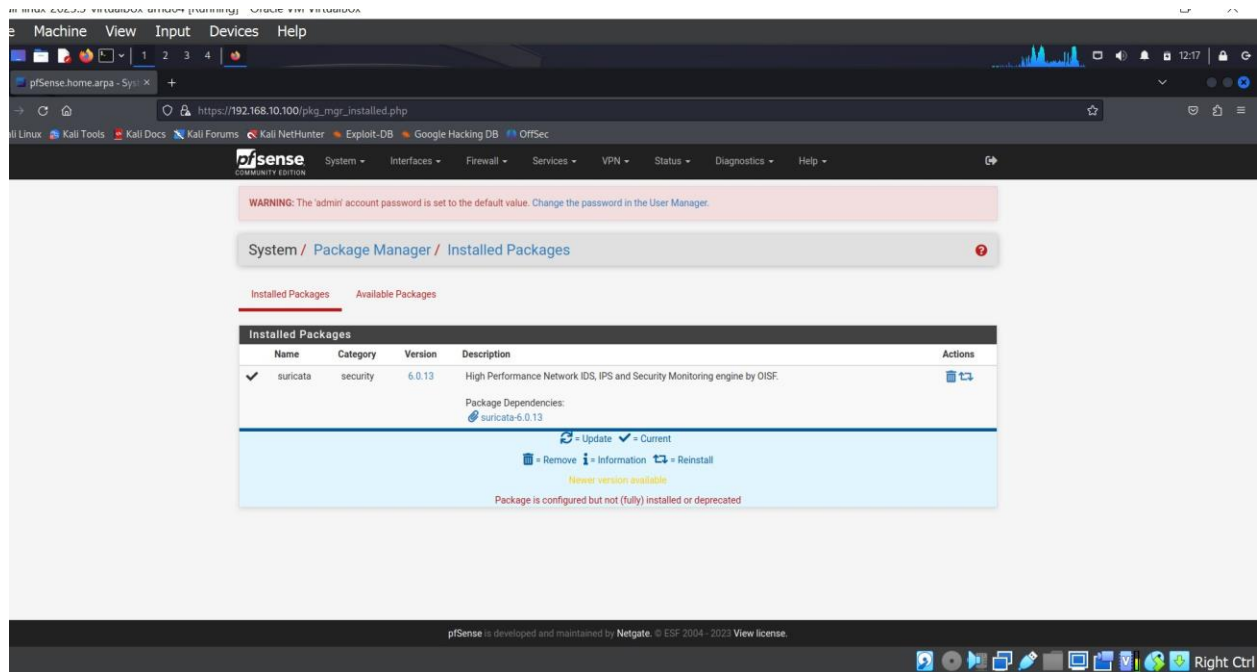
The screenshot shows a web browser window displaying the pfSense web interface. The browser's address bar shows the URL `https://192.168.10.100/status_ntpd.php`. The pfSense interface has a top navigation bar with menus for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Status / NTP" page is displayed, featuring a table titled "Network Time Protocol Status".

Status	Server	Ref ID	Stratum	Type	When	Poll (s)	Reach	Delay (ms)	Offset (ms)	Jitter (ms)
Pool Placeholder	2.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

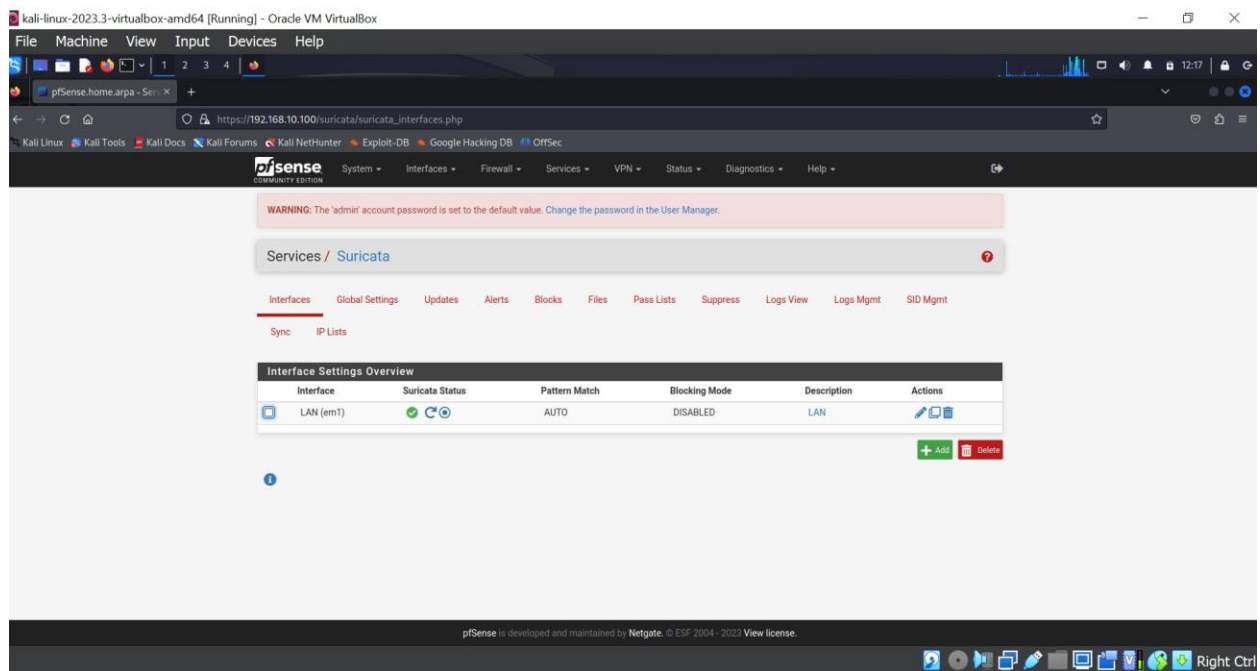
At the bottom of the interface, a footer note states: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license." The bottom of the browser window shows a taskbar with various icons and the text "Right Ctrl".

Part 3:

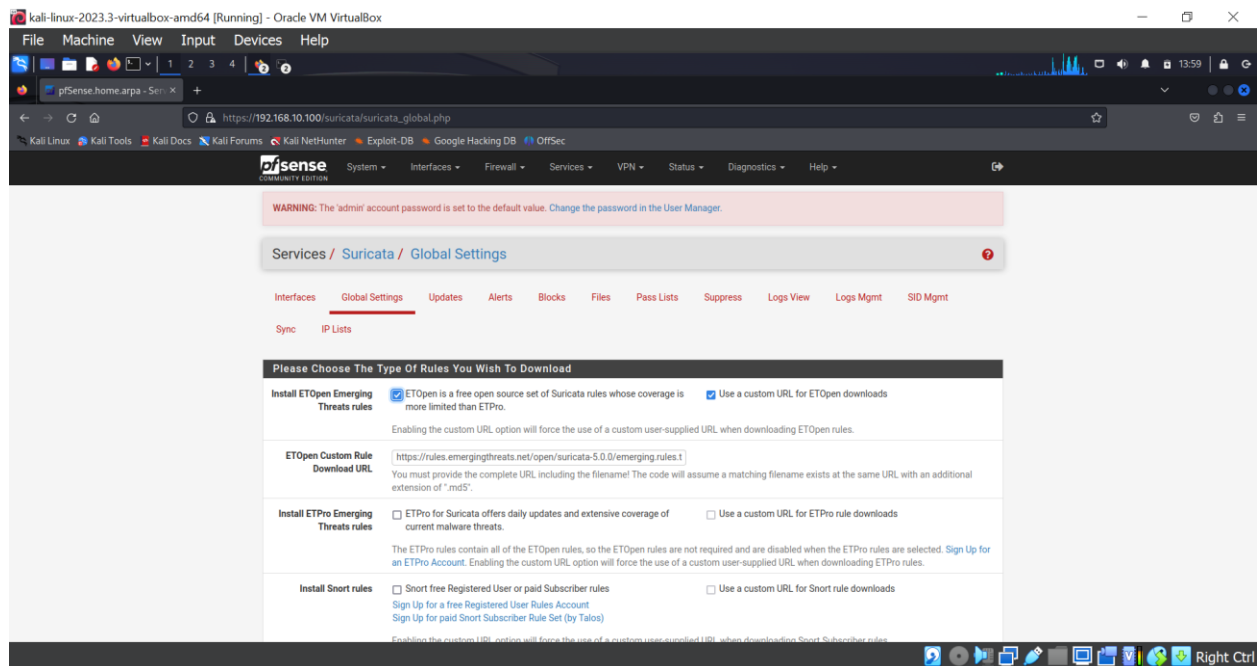
First went into Package Manager and installed Suricata.



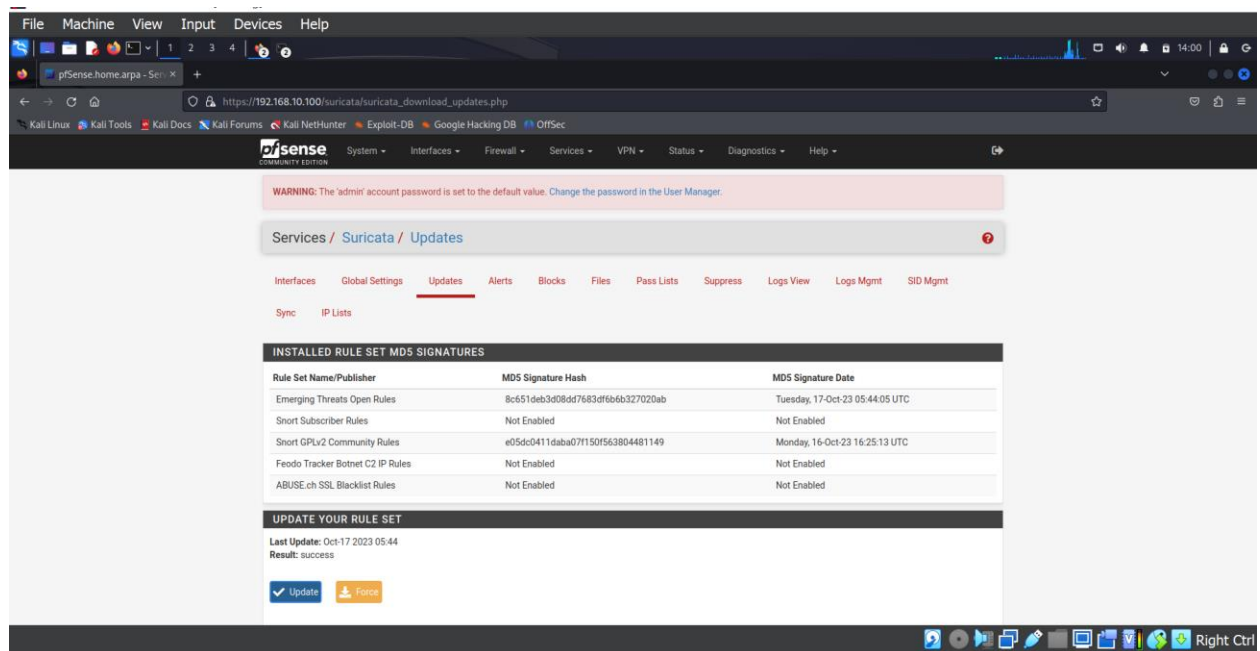
Went into Suricata interfaces in services and created a LAN interface through Add button.



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@kali)-[~]
$ 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/uricata/updates
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
```

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

```
(root@kali)-[/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)
```

kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

pfSense.home.arpa - Sta

https://192.168.10.100/status_logs_filter.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Status / System Logs / Firewall / Normal View

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:56042	192.168.10.100:6699	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:48984	192.168.10.100:1236	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:49798	192.168.10.100:2200	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:45076	192.168.10.100:2105	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:38250	192.168.10.100:6389	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:38750	192.168.10.100:1503	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:59590	192.168.10.100:5051	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:48758	192.168.10.100:31038	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:38446	192.168.10.100:49165	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:36028	192.168.10.100:2910	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:34100	192.168.10.100:6666	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:54620	192.168.10.100:1812	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:59300	192.168.10.100:1914	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:53182	192.168.10.100:9595	TCP-S
✗	Oct 17 16:42:34	LAN	Default deny rule IPv4 (1000000103)	192.168.10.151:53162	192.168.10.100:9000	TCP-S

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Right Ctrl

Made Custom rule

kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

pfSense.home.arpa - Ser

https://192.168.10.100/suricata/suricata_rules.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Suricata / Interface Settings / LAN - Rules

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt

Sync IP Lists

LAN Settings LAN Categories LAN Rules LAN Flow/Stream LAN App Parsers LAN Variables LAN IP Rep

Available Rule Categories

Category: custom_rules
Select the rule category to view and manage.

Defined Custom Rules

```
alert udp any any -> any 12345 (msg:"Custom UDP rule example"; sid:1000001;)
```

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Right Ctrl

Generated test data for the custom rule and checked Alerts

The screenshot shows a Kali Linux terminal window at the top and a web browser window below it. The terminal window displays the command `echo -n "Test UDP data" | nc -u -w1 192.168.10.100 12345` and the resulting alert data. The web browser window shows the URL `https://192.168.10.100/suricata/suricata_alerts.php` and a table of the last 250 alert entries.

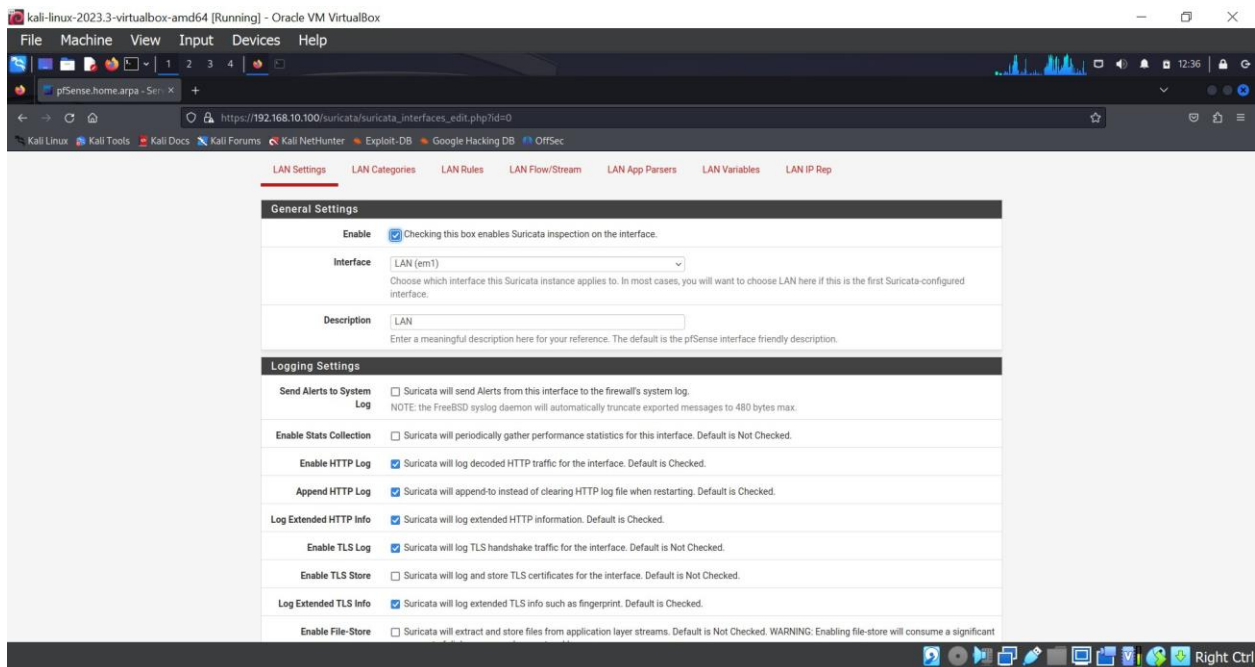
Terminal Output:

```
(kali@kali)~$ echo -n "Test UDP data" | nc -u -w1 192.168.10.100 12345
(kali@kali)~$
```

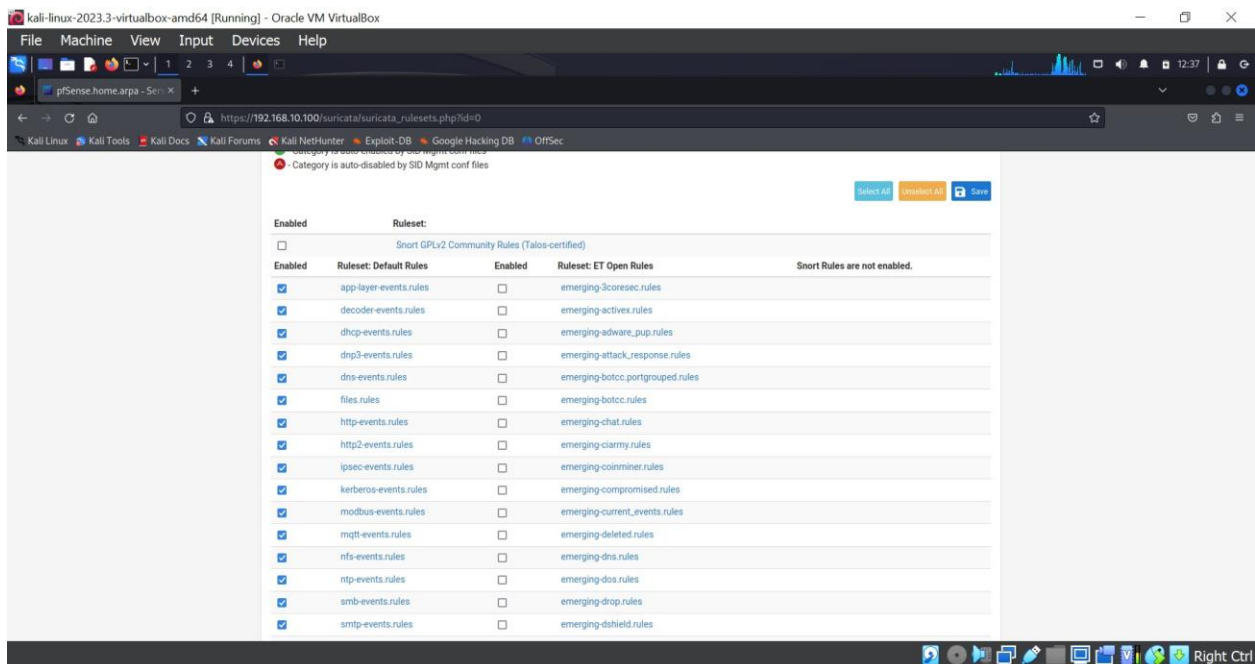
Alert Data Table:

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	OID-SID	Description
10/17/2023 16:34:11	Alert	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	Alert	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	Alert	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	Alert	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	Alert	3	IPv6-ICMP	Generic Protocol Command Decode	fe80::e5e0:608b:861d:e353	143	:::ffff::16	0	1:22000094	SURICATA zero length padN option
10/17/2023 14:52:47	Alert	3	ICMP	Generic Protocol Command Decode	10.0.0.2	0	224.0.0.22	0	1:22000007	SURICATA IPv4 padding required
10/17/2023 14:52:47	Alert	3	IPv6-ICMP	Generic Protocol Command Decode	fe80::e5e0:608b:861d:e353	143	:::ffff::16	0	1:22000094	SURICATA zero length padN option
10/17/2023 14:52:47	Alert	3	ICMP	Generic Protocol Command Decode	10.0.0.2	0	224.0.0.22	0	1:22000007	SURICATA IPv4 padding required
10/17/2023 14:52:47	Alert	3	IPv6-ICMP	Generic Protocol Command Decode	fe80::e5e0:608b:861d:e353	143	:::ffff::16	0	1:22000094	SURICATA zero length padN option
10/17/2023 14:52:47	Alert	3	ICMP	Generic Protocol Command Decode	10.0.0.2	0	224.0.0.22	0	1:22000007	SURICATA IPv4 padding required
10/17/2023 14:49:30	Alert	3	IPv6-ICMP	Generic Protocol Command Decode	fe80::e5e0:608b:861d:e353	143	:::ffff::16	0	1:22000094	SURICATA zero length padN option

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

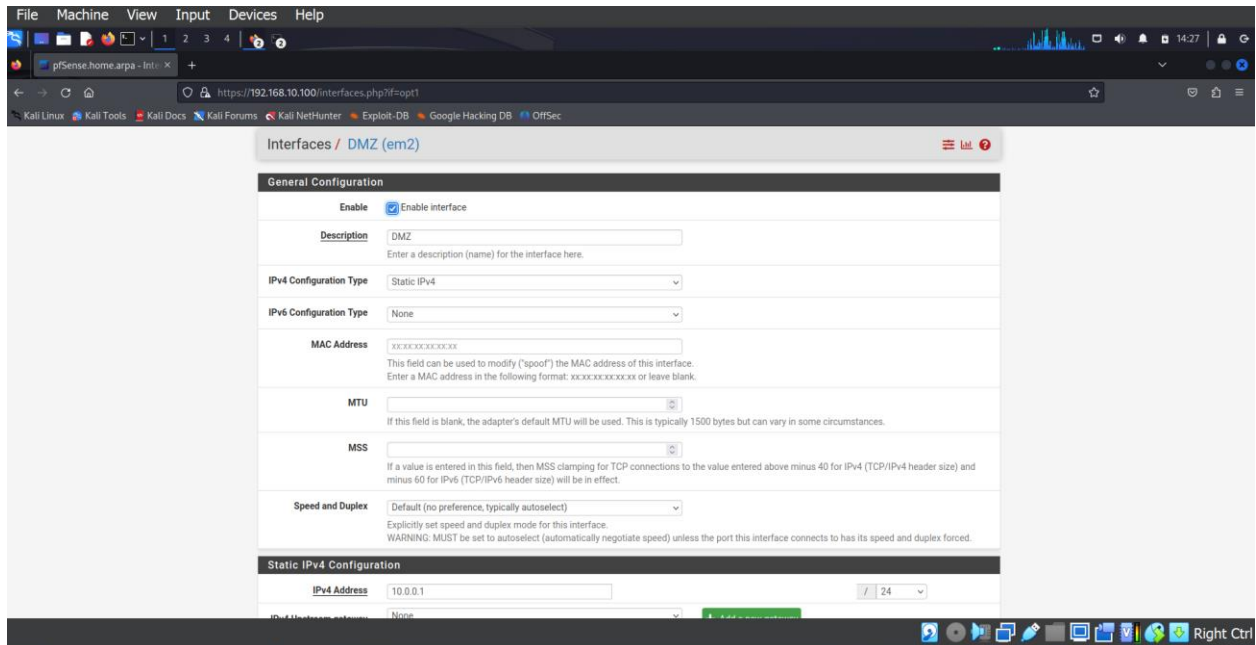


In the IDS selected the rulesets in which there are many rulesets and every set will give an alert on event occurring related to that ruleset.

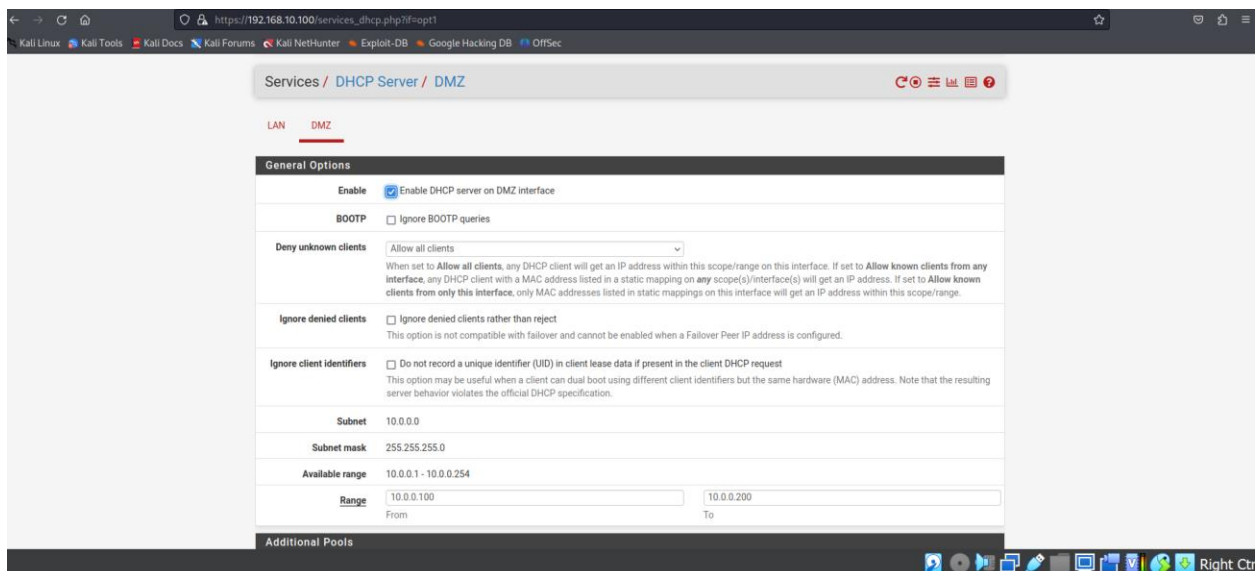


Part 4:

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

File Machine View Input Devices Help

1 2 3 4

pfSense.home.arpa - Sta... New Tab

https://192.168.10.100/status_dhcp_leases.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfSense Community Edition

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / DHCP Leases

Search

Search term All

Enter a search string or *nix regular expression to filter entries.

Leases

IP address	MAC address	Client id	Hostname	Description	Start	End	Online	Lease Type	Actions
10.0.0.2	08:00:27:cb:7e:f5	DMZ	DMZ	DMZ(kali)	n/a	n/a	active	static	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
192.168.10.151	08:00:27:cb:7e:f5	kali1			2023/10/17 14:21:56	2023/10/17 16:21:56	active	active	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
192.168.10.150	08:00:27:cb:7e:f5	kali2			2023/10/17 14:18:23	2023/10/17 16:18:23	idle/offline	active	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Leases in Use

Interface	Pool Start	Pool End	# of leases in use
LAN	192.168.10.150	192.168.10.170	2

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

Right Ctrl

File Machine View Input Devices Help

1 2 3 4

pfSense.home.arpa - Fir... New Tab

https://192.168.10.100/firewall_nat.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfSense Community Edition

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NAT

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	443 (HTTPS)	10.0.0.2	443 (HTTPS)	root incoming traffic from WAN to DMZ	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Legend

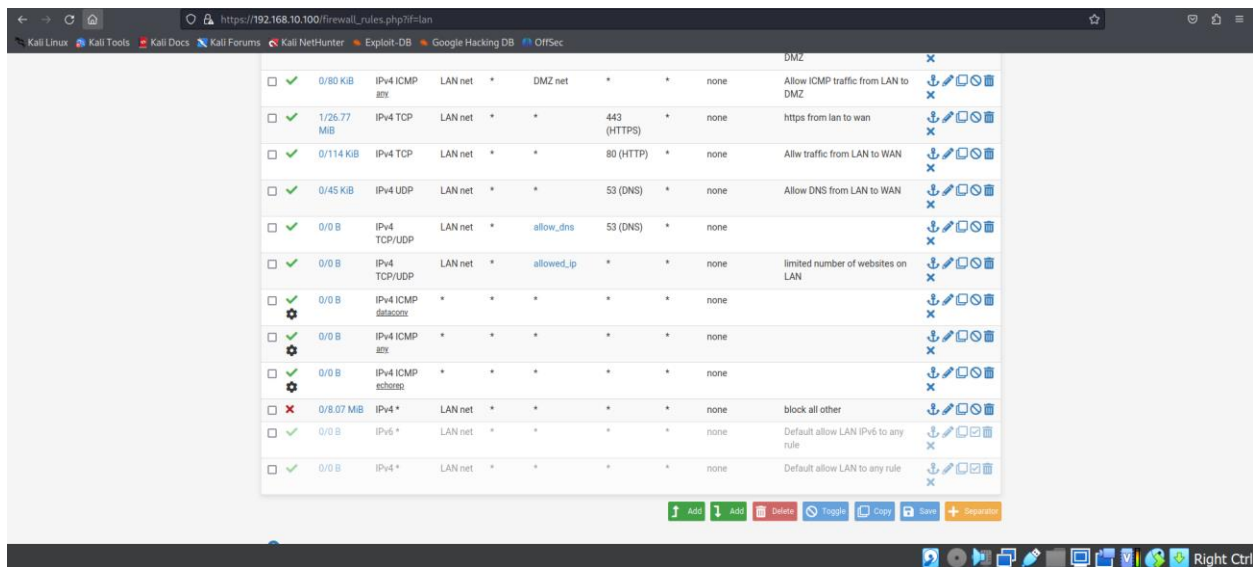
Pass

Linked rule

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

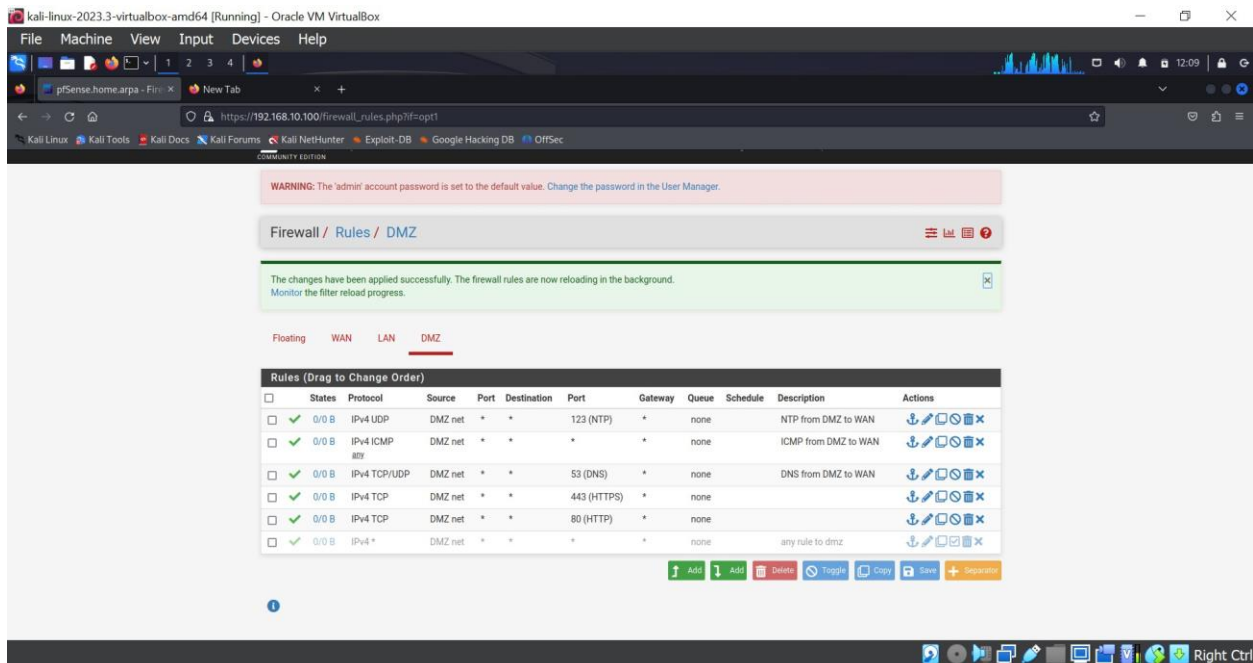
Right Ctrl

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

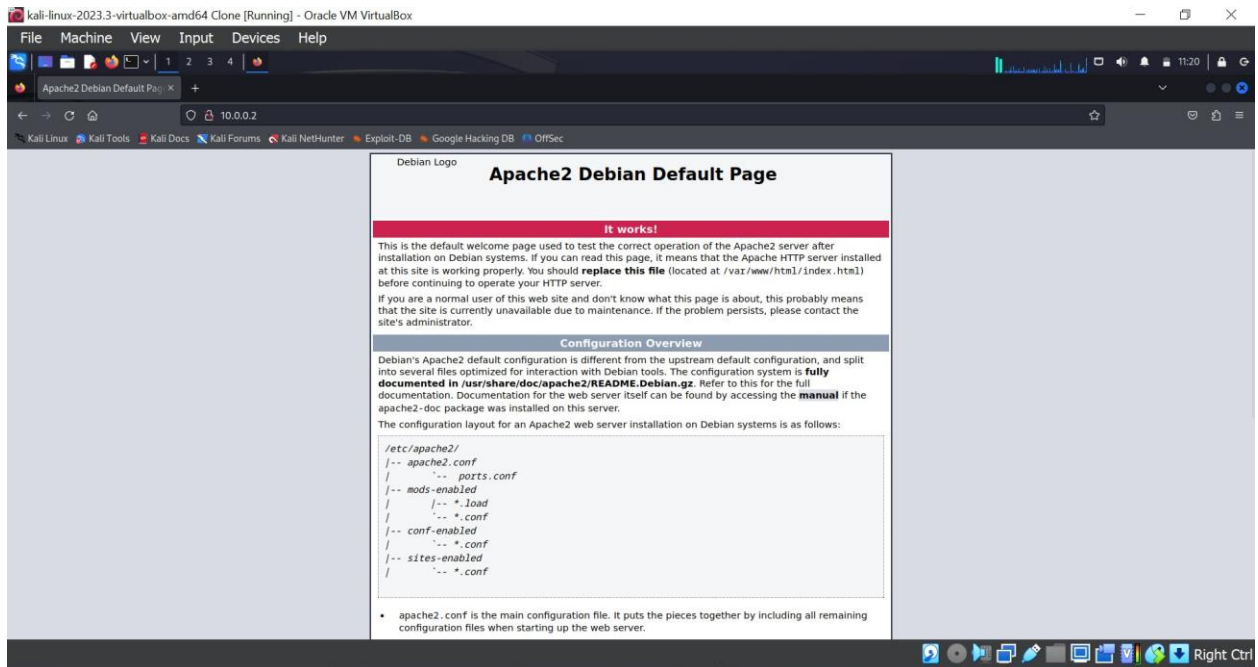


Added ICMP and Allowed Ip rules in LAN and changed Max states, Max scr nodes and Max scr states to 3.

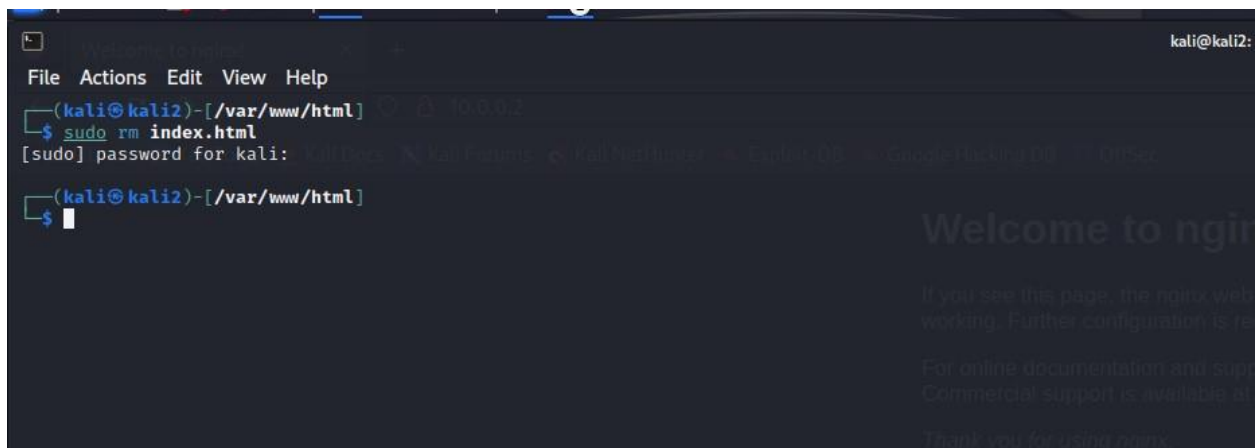
DMZ (OPT 1) firewall rules:



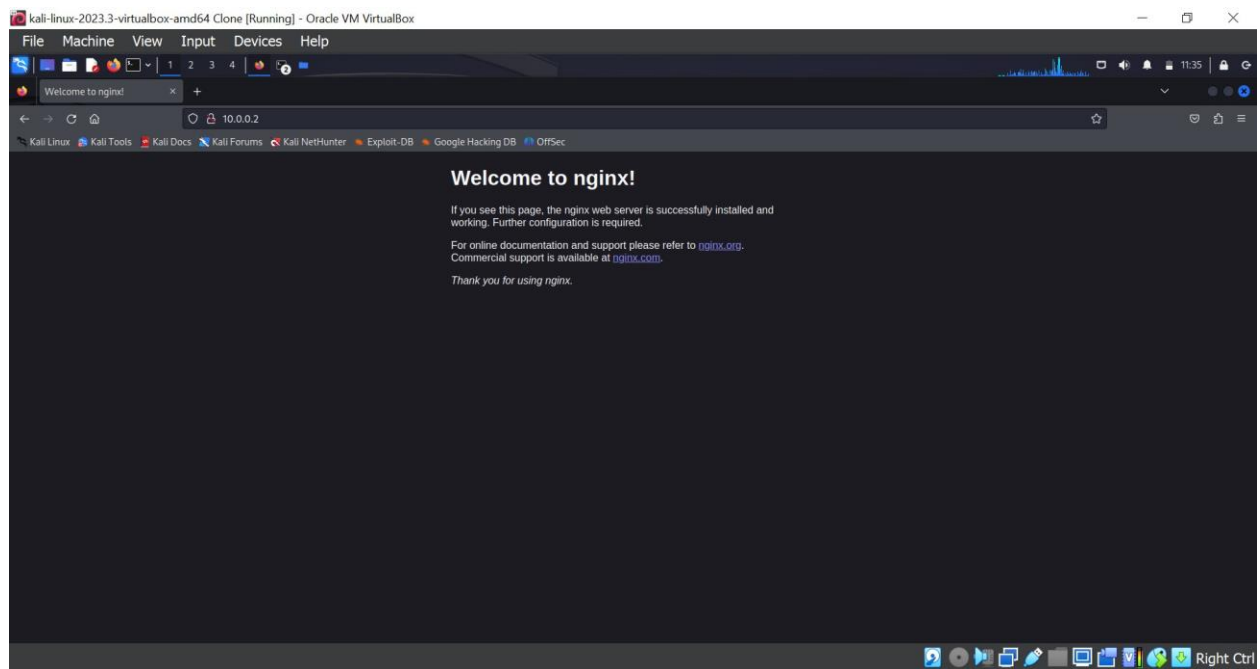
Apache server opened on DMZ(kali) FireFox with IP given which is 10.0.0.2



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 were 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.