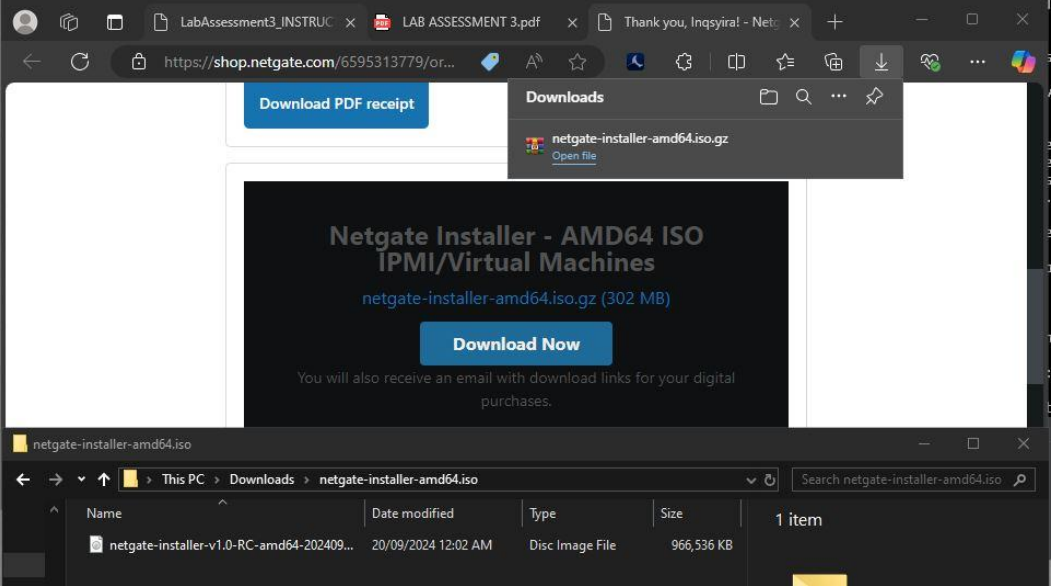


SNORT AND FIREWALL PROVISIONING

host address for LAN in the virtual box: 192.168.6.0

TOOL DETAILS	RESULTS
pfSense Installation (successful/Fail)	 A screenshot showing the successful download of the Netgate Installer for AMD64 ISO. The top part shows a web browser window at shop.netgate.com with a 'Download Now' button. Below it, a file explorer window shows the downloaded file 'netgate-installer-amd64.iso' in the Downloads folder, with a size of 966,536 KB.

Network Requirement Setup

```
Fadhilah_Inqsyira [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.6.20
Enter the end address of the IPv4 client address range: 192.168.6.250
Disabling IPv6 DHCPD...

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.6.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:

    http://192.168.6.1/

Press <ENTER> to continue.
```

```
Fadhilah_Inqsyira [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.6.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n
```

```
Fadhilah_Inqsyira [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

The IPv4 LAN address has been set to 192.168.6.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:

    http://192.168.6.1/

Press <ENTER> to continue.
KVM Guest - Netgate Device ID: 0bf49de7e9f2dfd6bb24

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.6.1/24

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:
```

Kali Linux Reboot (Successful/Fail)

```
inqsyirazamri@inq:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:27:41:0b:e4 txqueuelen 1000 (Ethernet)
    RX packets 10 bytes 1138 (1.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.6.22 netmask 255.255.255.0 broadcast 192.168.6.255
    inet6 fe80::a00:27ff:fe92:6a57 prefixlen 64 scopeid 0<link>
    ether 08:00:27:92:6a:57 txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 866 (866.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 3540 (3.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 206 bytes 12300 (12.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 206 bytes 12300 (12.0 KiB)
```

```
Fadhliah_Inqsyira [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20240304-1953
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
KVM Guest - Netgate Device ID: 0bf49de7e9f2dfd6bb24

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 192.168.6.1/24

0) Logout (SSH only) 9) pfTop
1) Reassign 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 (ssh)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM
8) Shell
```

Accessing pfSense GUI

Kali Linux VM [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

pfSense.home.arpa - Inte x

192.168.6.1/interfaces.php?if=lan

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.

Interfaces / LAN (em1)

General Configuration

Enable ☒ Enable interface

Description LAN

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xxxxxxxxxx

MTU

MSS

Speed and Duplex Default (no preference, typically autoselect)

Static IPv4 Configuration

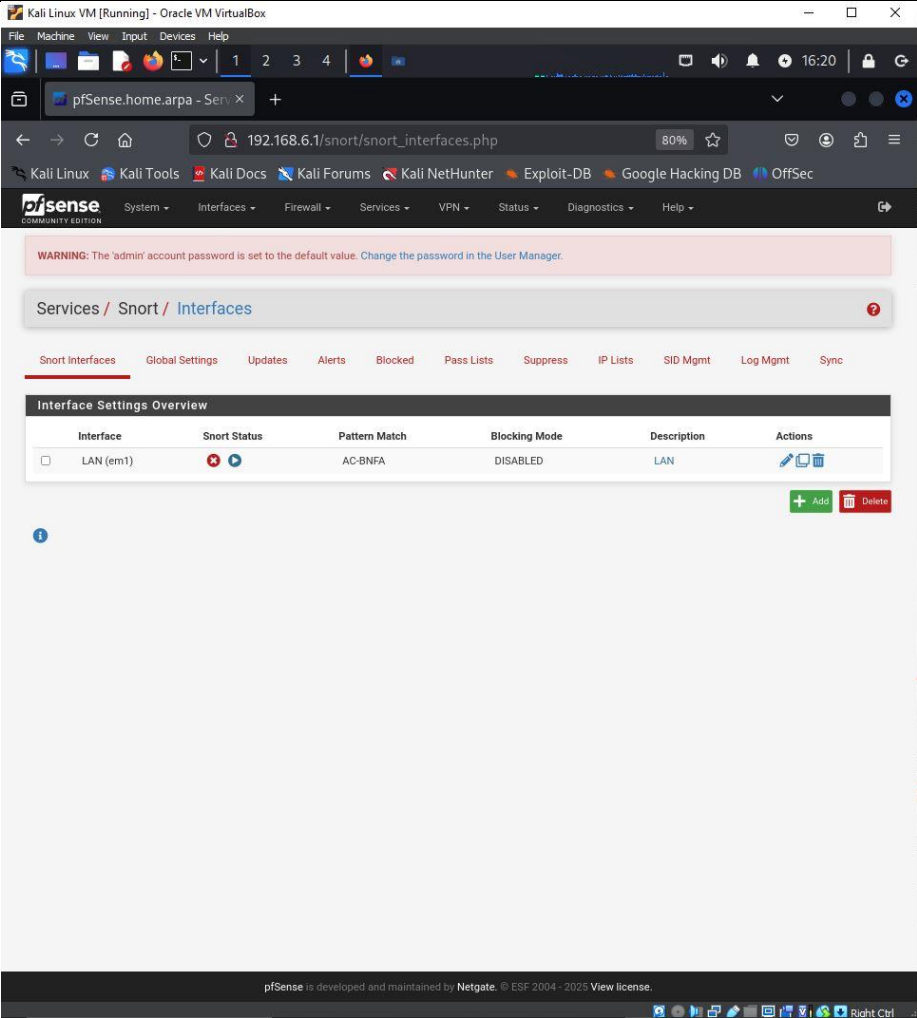
IPv4 Address 192.168.6.1 / 24

IPv4 Upstream gateway None + Add a new gateway

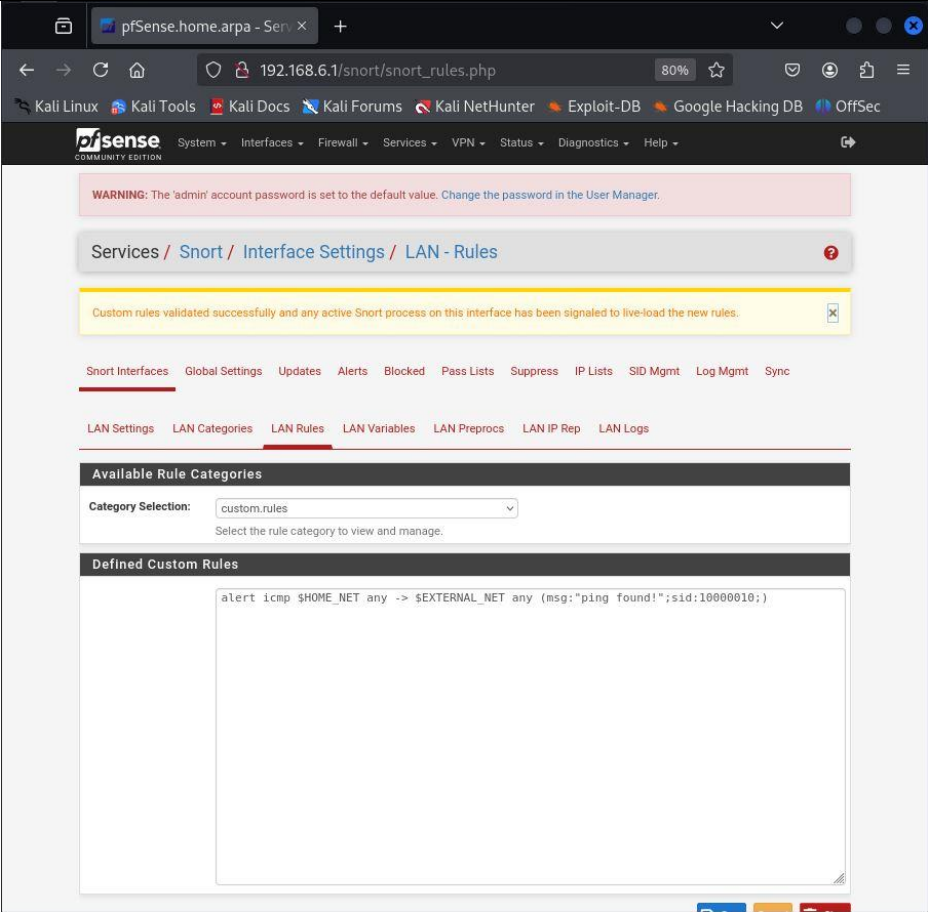
Reserved Networks

Block private networks

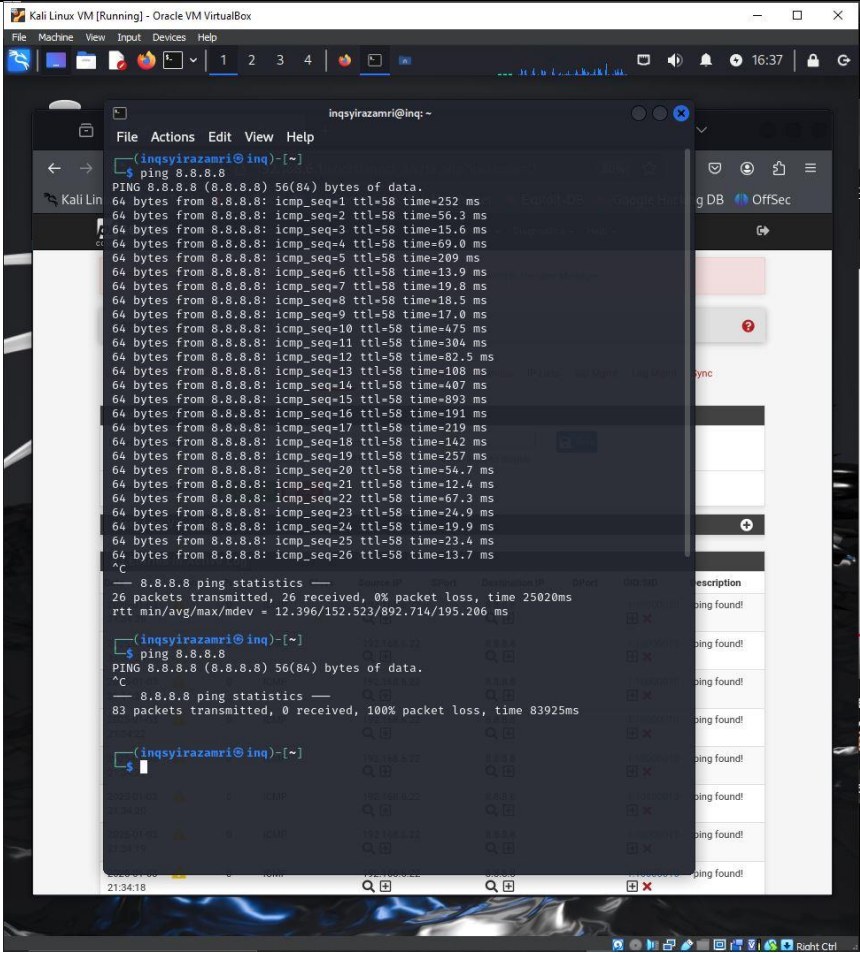
Interface Added
into pfSense



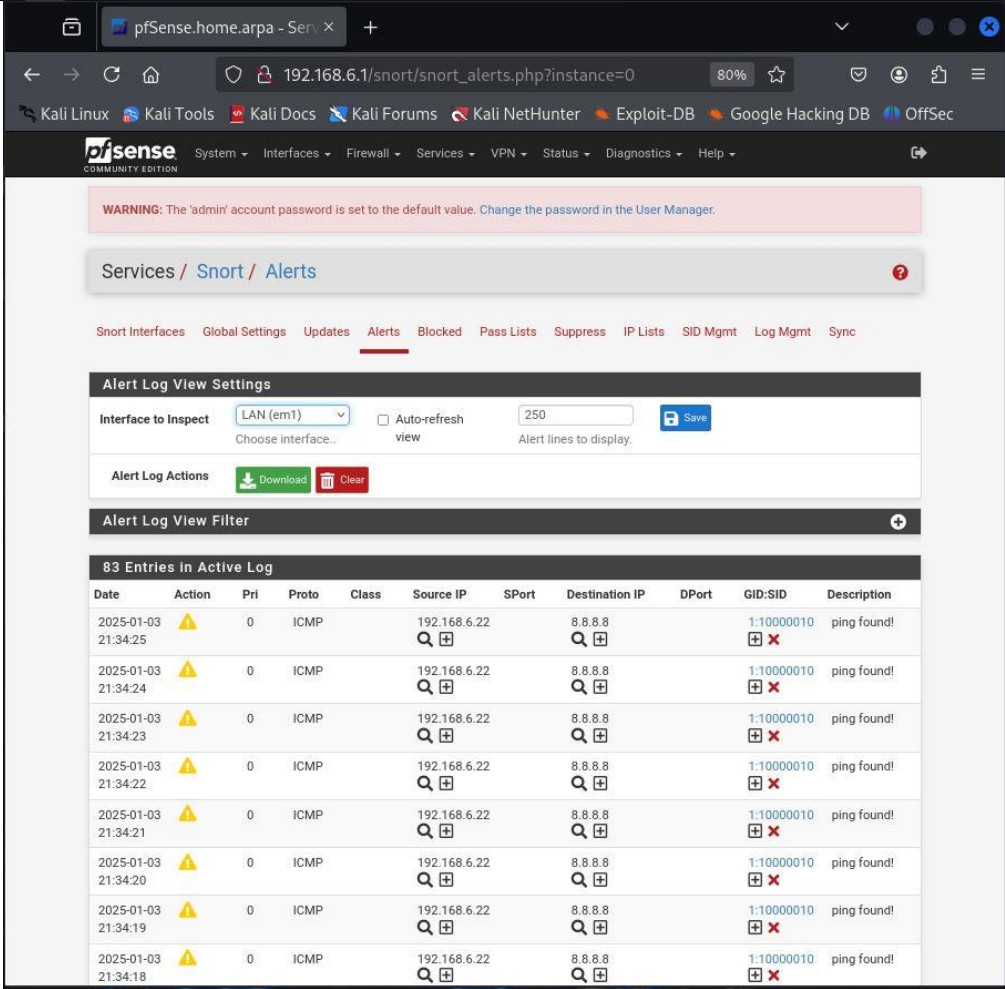
IDS Rules
Applied
(Successful/Fail)



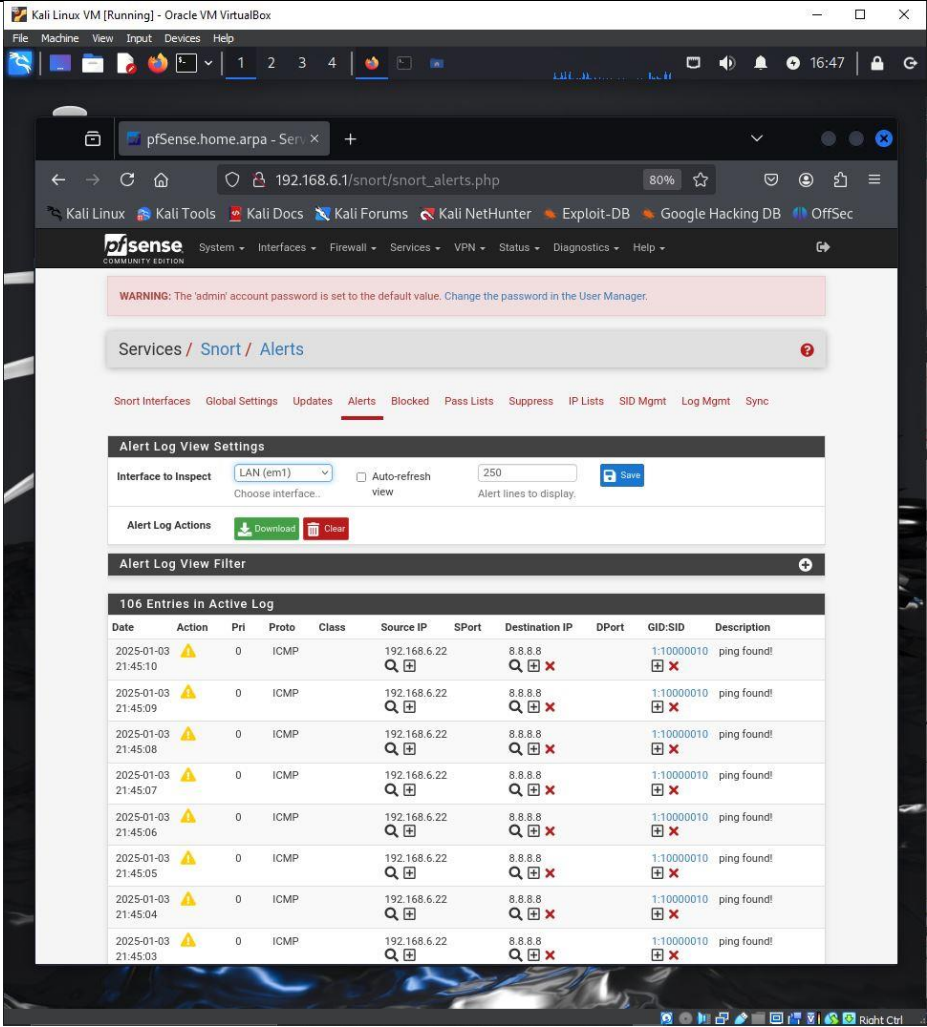
Host Triggered
in Kali Linux -
Ping 8.8.8.8
(Successful/Fail)



Alerts Showing
in the Snort
(Showing/Not
Showing)



Alerts showing for IPS Blocked Host in Snort (Showing/Not Showing)



IPS Blocked Host showing in the Blocked Section in Snort (Showing/Not Showing)

