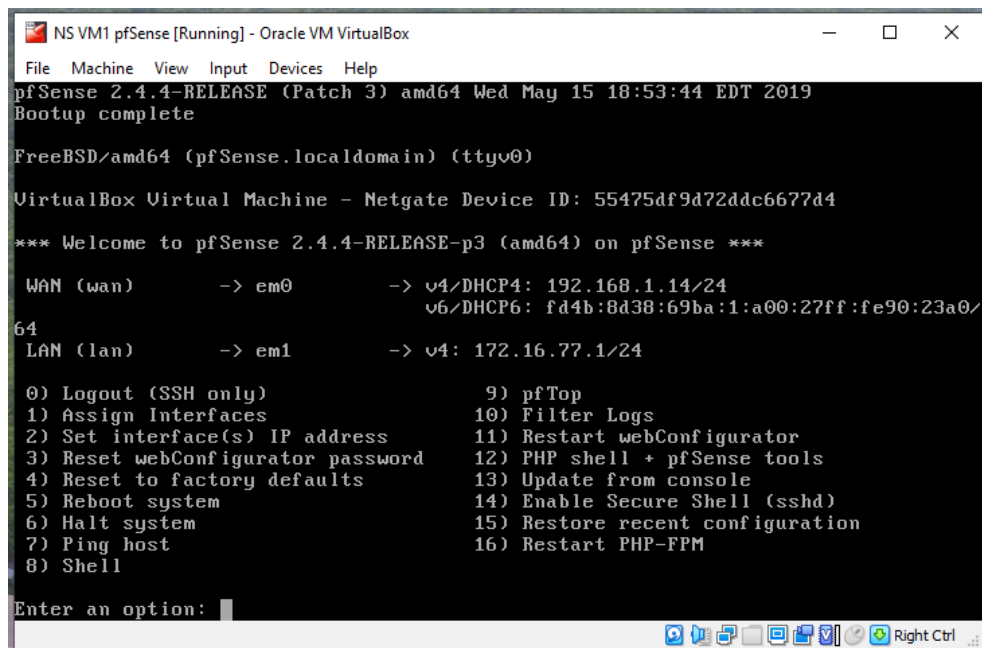
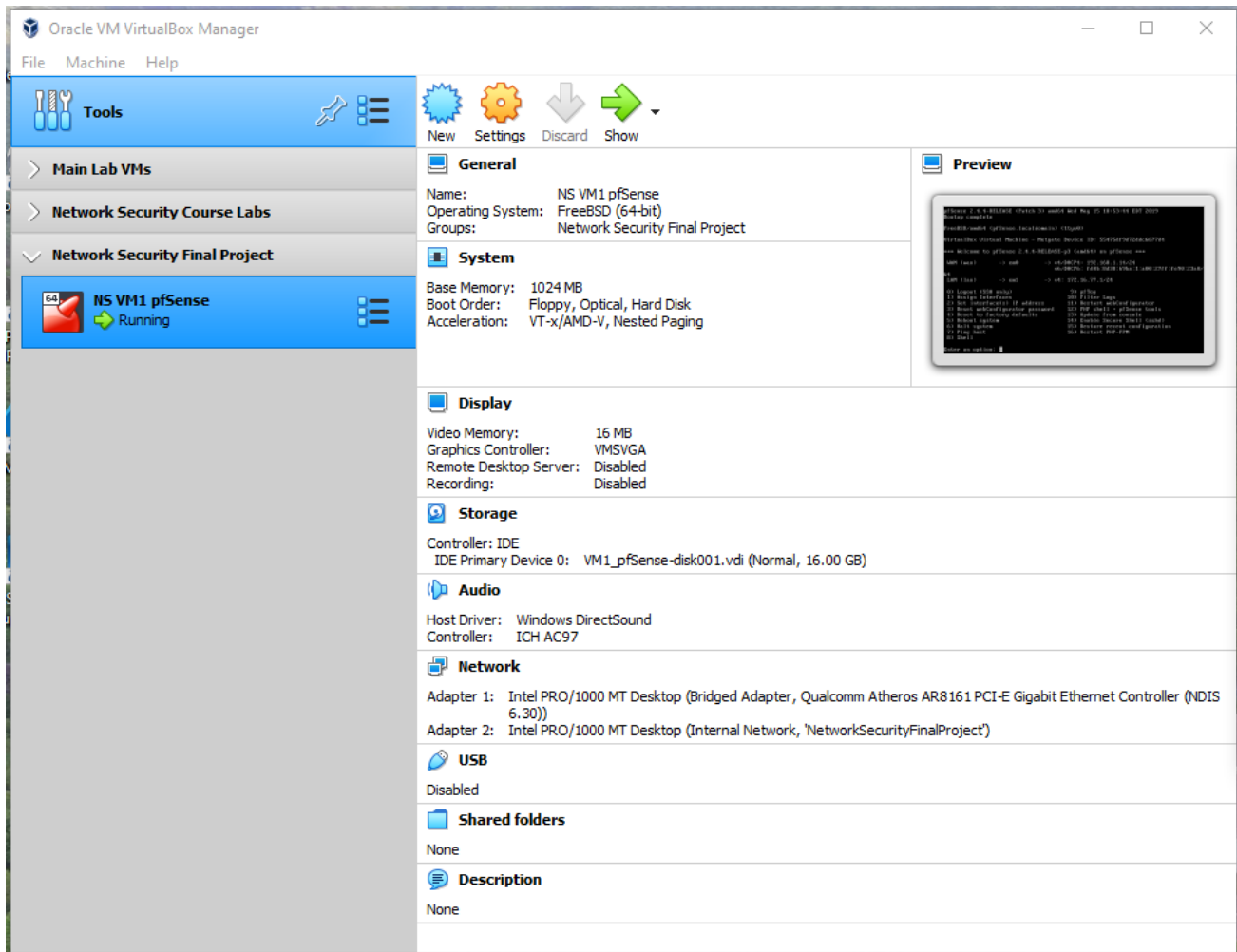


Project Background: Play the role of a Security Analyst to solve various challenges with a corporate environment's network security. (For example, users are still able to access some resources they should not be able to, and some inbound traffic that should be blocked is still allowed. Secure access for remote employees is also not set up.)

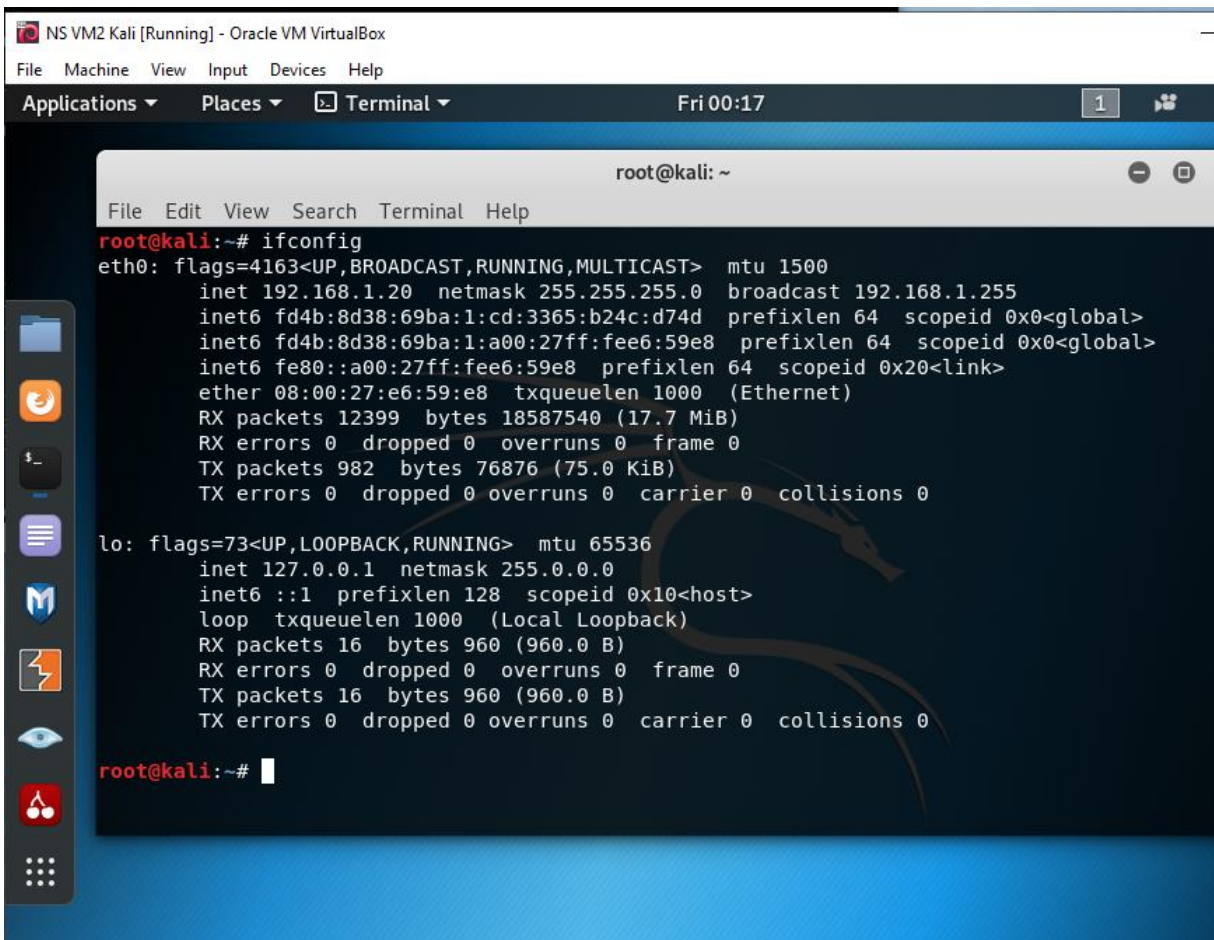
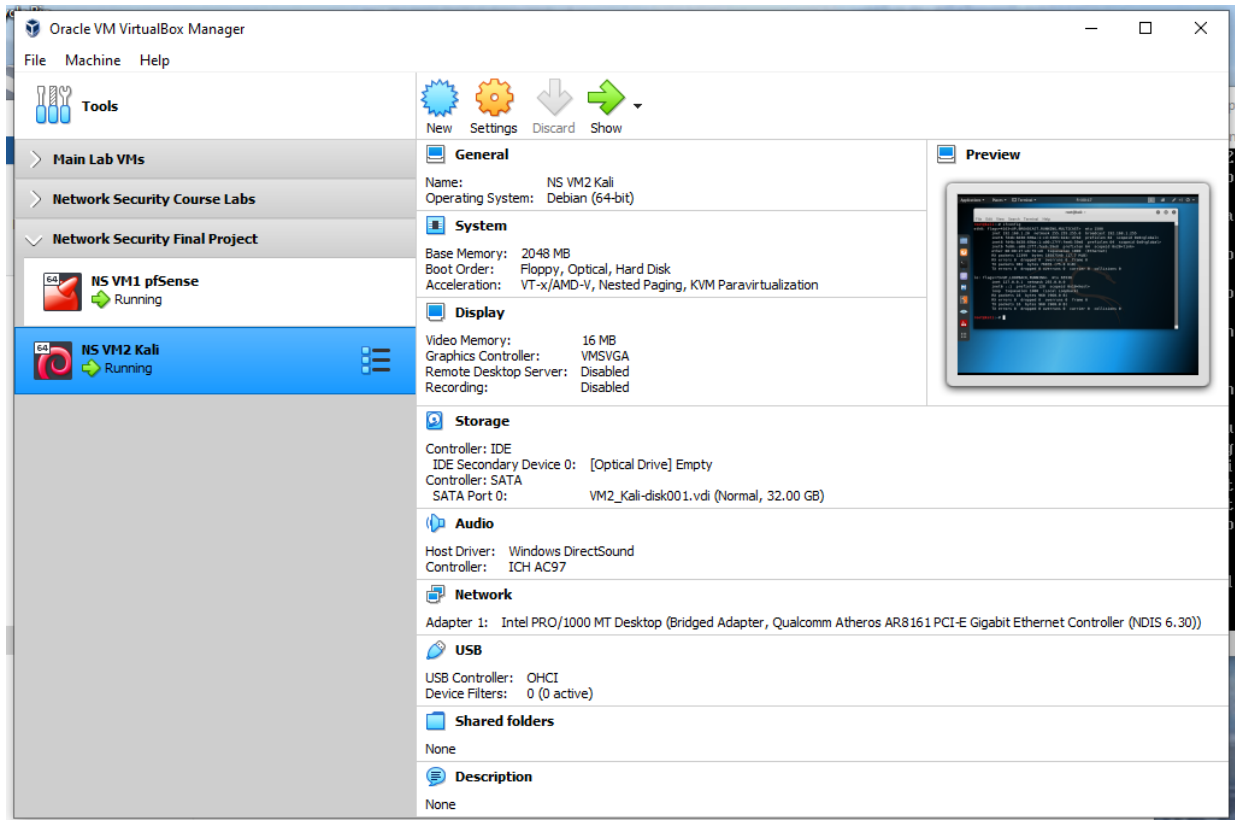
Virtual Environment Scenario and Setup:

- **Host System:** The physical host (running the hypervisor) and its network connection will be used to mimic the Internet for this project. It will act as an external agent to access certain resources within the virtualized corporate network.

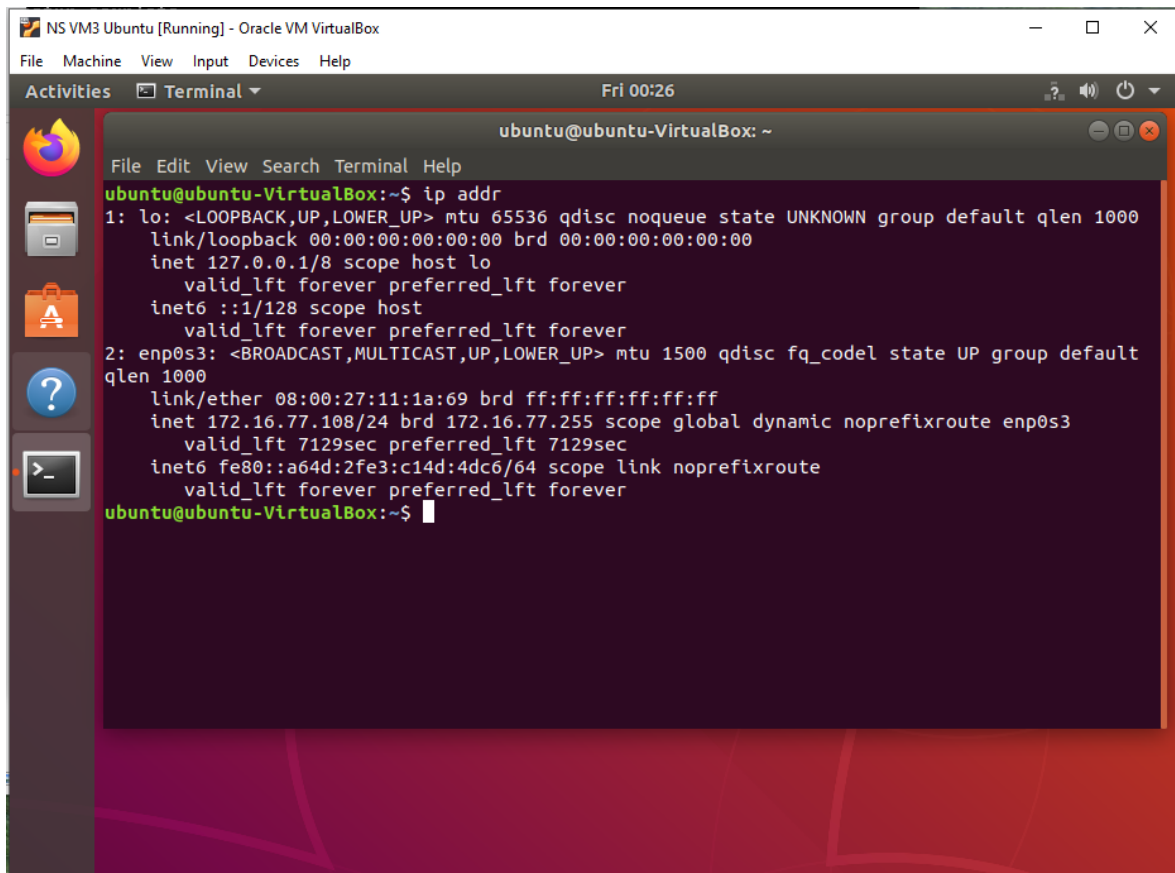
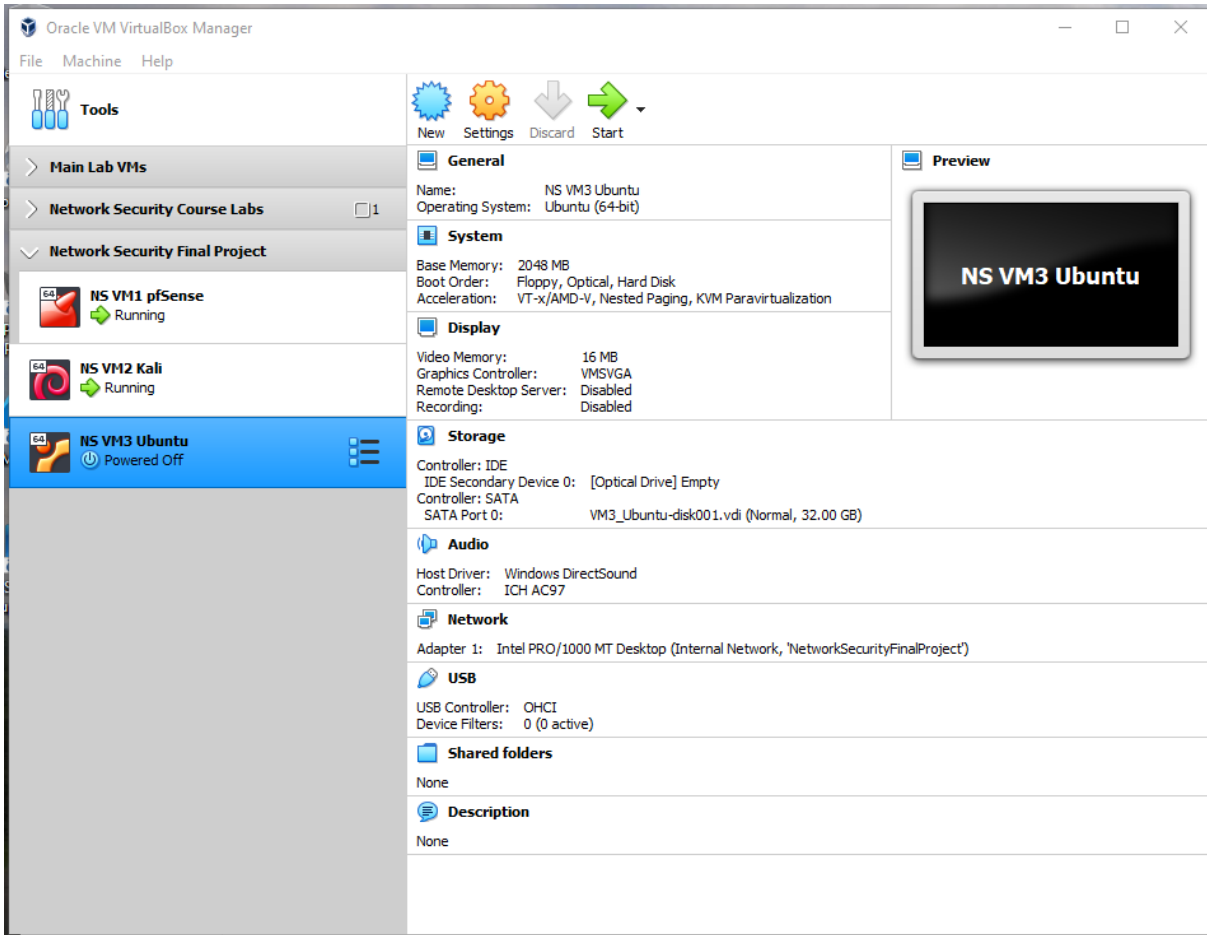
- **VM #1:** This virtual machine is a pfSense firewall. It separates the Internet from the internal scenario and works with NAT between the networks. The firewall is configured to get, on the WAN interface, an IP address from the same subnet as the physical host (DHCP client, bridged adapter in VirtualBox). For the LAN interface, pfSense acts as the DHCP server and the default gateway for the internal environment. pfSense also runs Suricata and OpenVPN for some tasks.



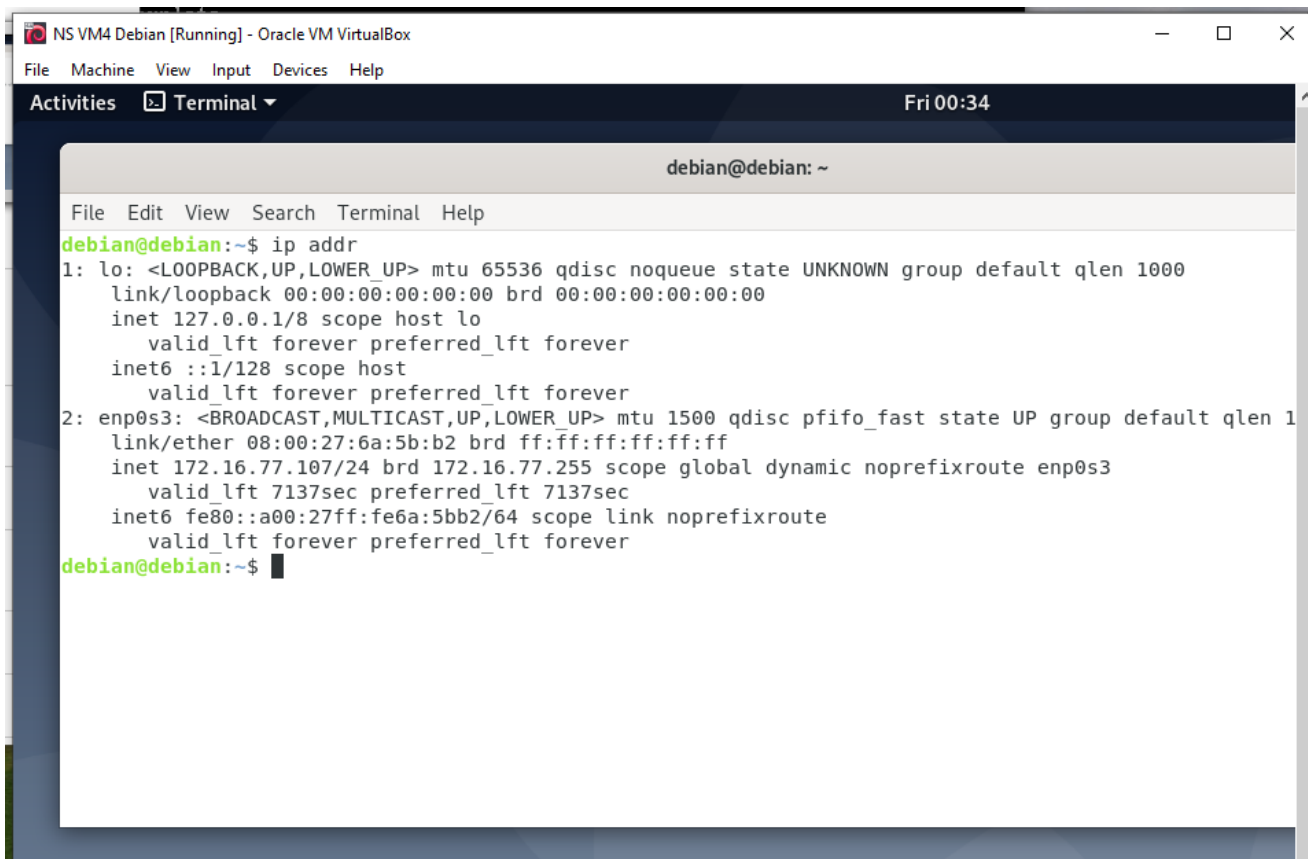
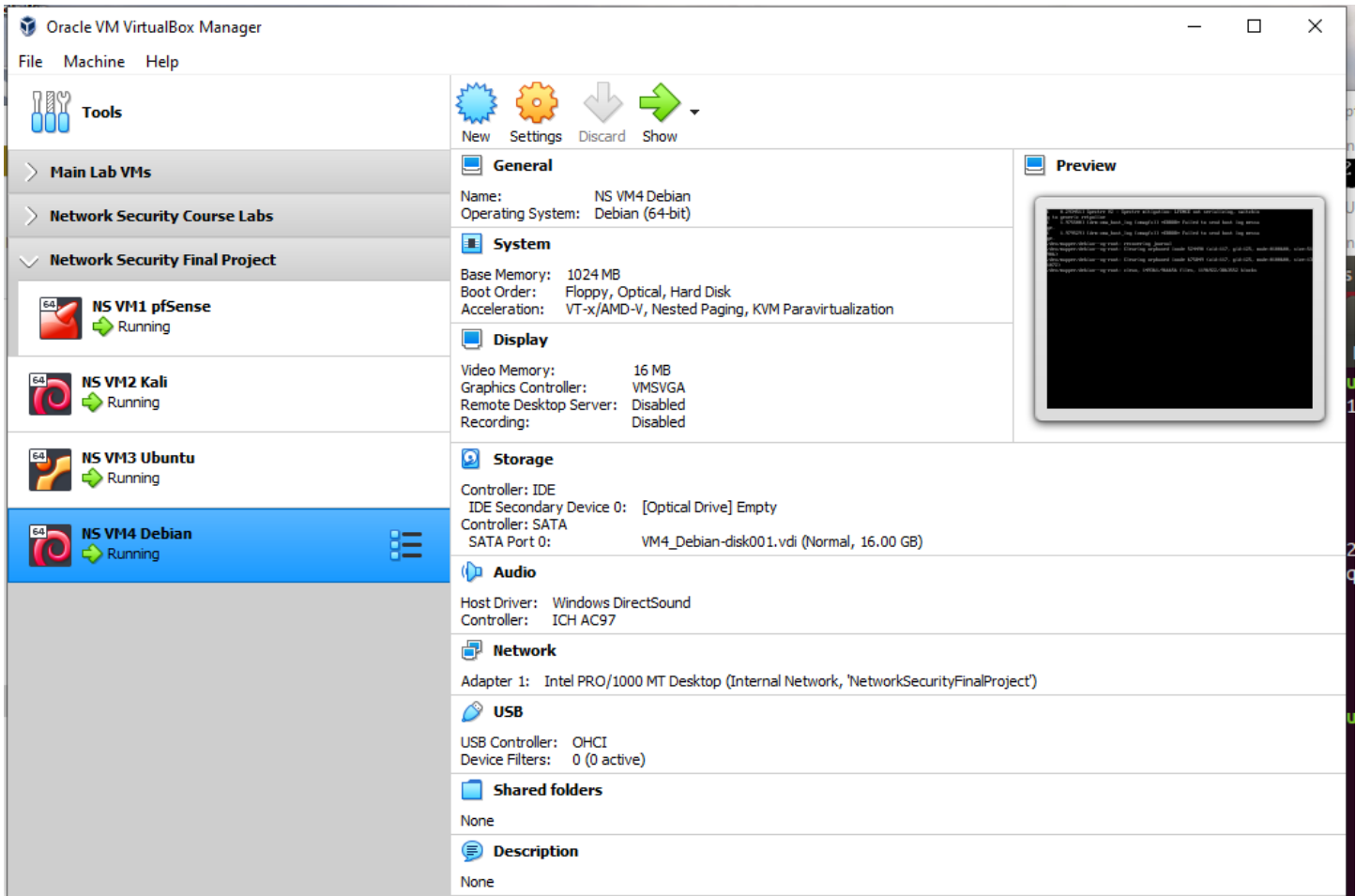
- **VM #2:** This virtual machine runs Kali Linux and will be used later in the project. It runs in bridged mode, meaning that it has an IP address on the same subnet as the physical host.



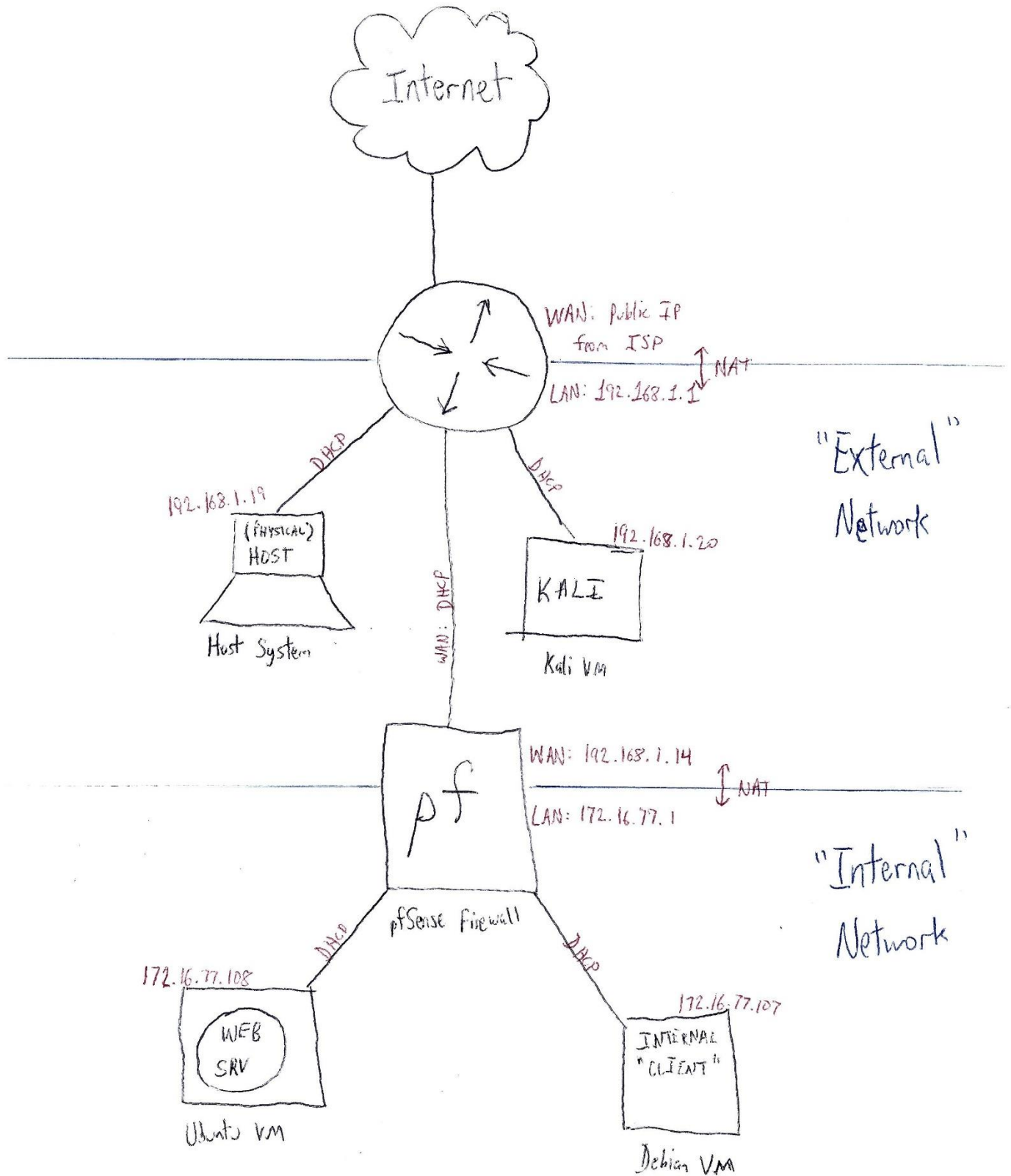
- **VM #3:** This virtual machine runs Ubuntu and represents servers in the corporate network. It hosts various services, including a web server that will simulate an internal web service for external access.



- **VM #4:** This virtual machine runs Debian and represents the internal network clients. It will be used for remote access tests, among other tasks, and is a DHCP client in the internal network.

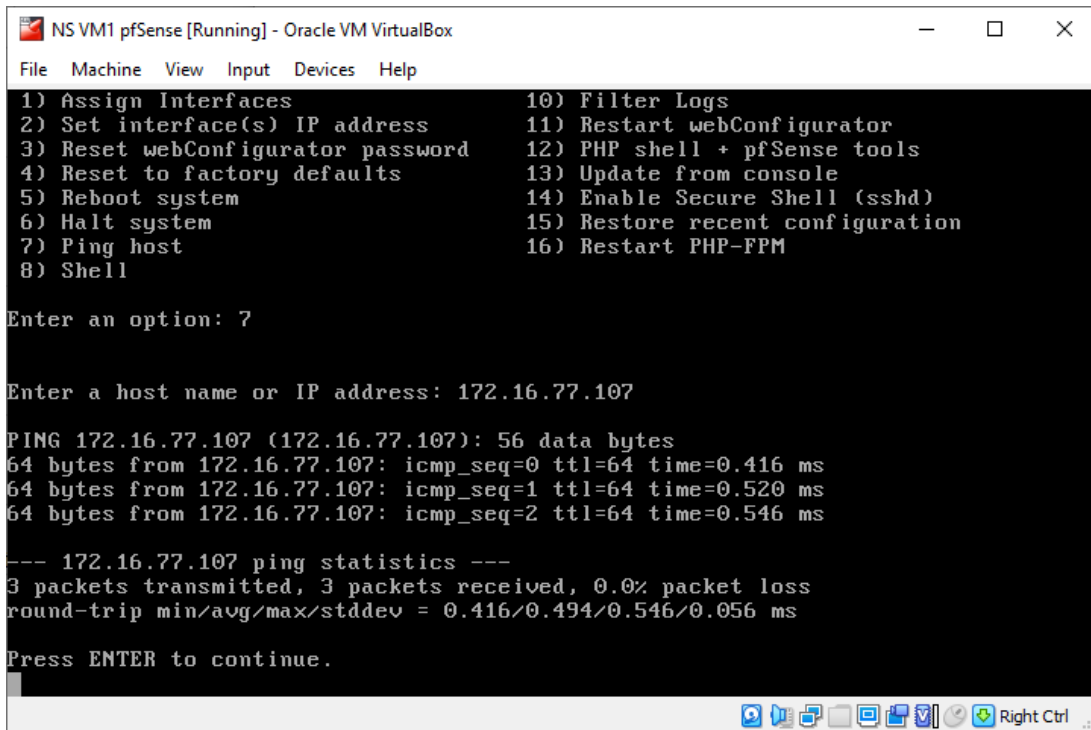


Network Diagram:



Scenario Validation:

1. IP addresses were verified to be correctly acquired/configured in the correct subnets, as shown in the above screenshots.
2. The pfSense machine was able to successfully ping another host on the internal subnet.



```
NS VM1 pfSense [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) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 7

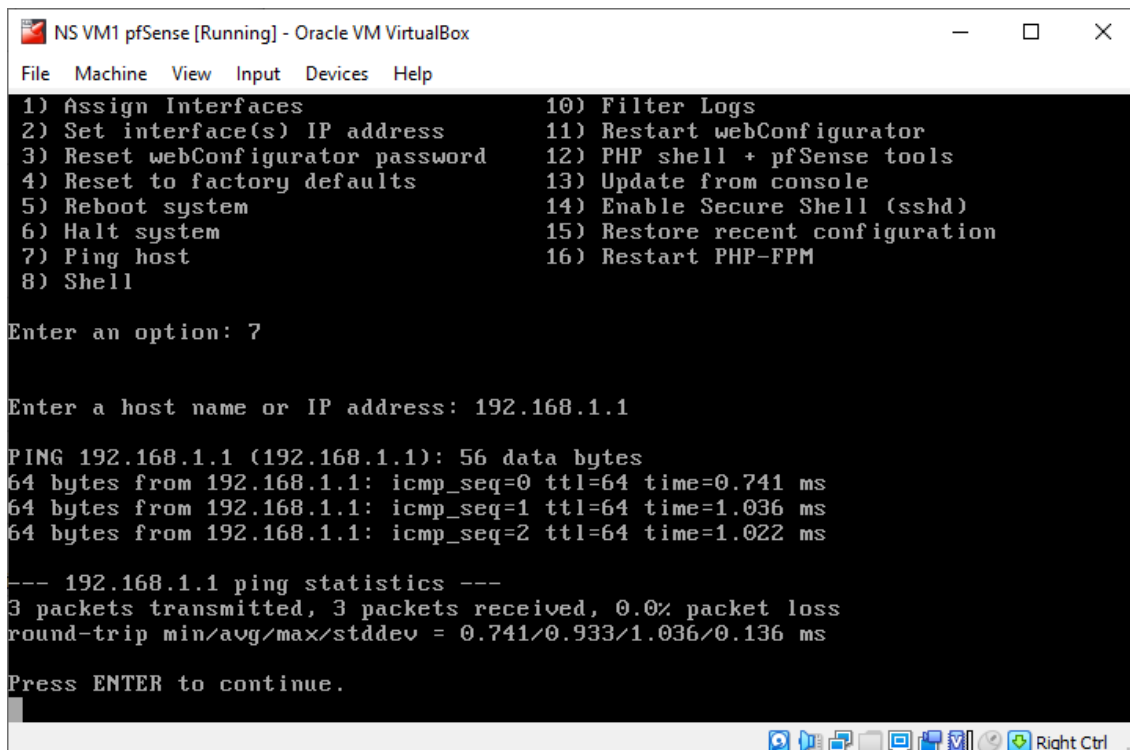
Enter a host name or IP address: 172.16.77.107

PING 172.16.77.107 (172.16.77.107): 56 data bytes
64 bytes from 172.16.77.107: icmp_seq=0 ttl=64 time=0.416 ms
64 bytes from 172.16.77.107: icmp_seq=1 ttl=64 time=0.520 ms
64 bytes from 172.16.77.107: icmp_seq=2 ttl=64 time=0.546 ms

--- 172.16.77.107 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.416/0.494/0.546/0.056 ms

Press ENTER to continue.
```

3. The pfSense machine was able to successfully ping another host on the external subnet.



```
NS VM1 pfSense [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) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 7

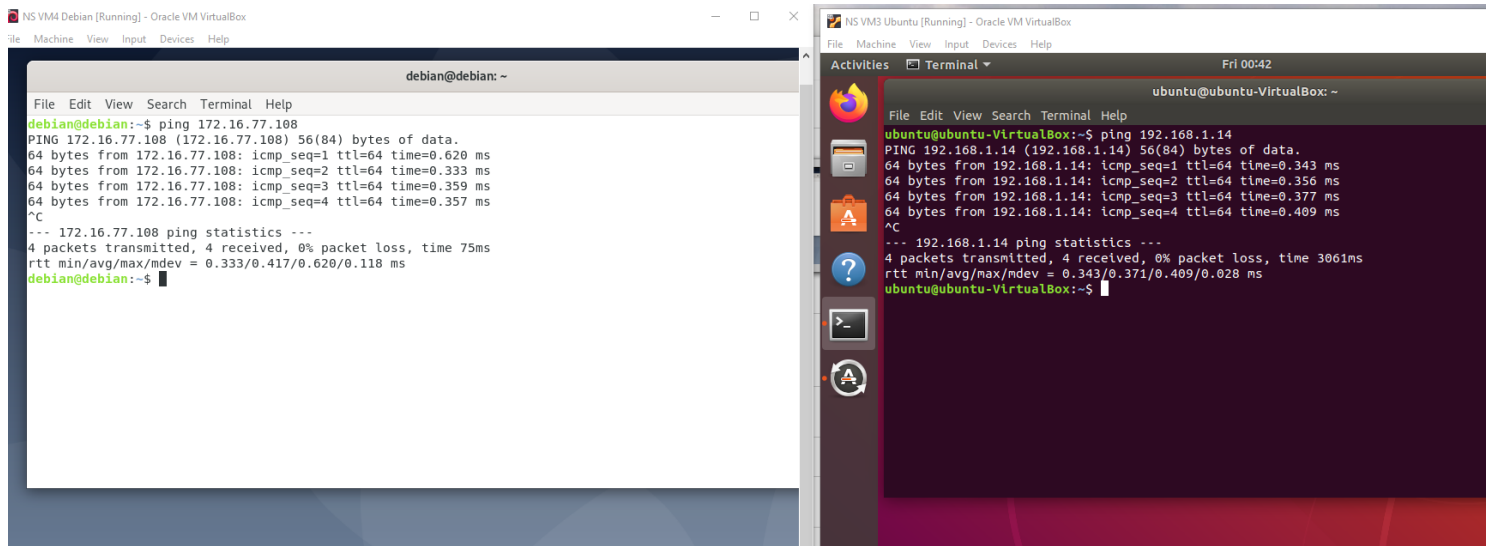
Enter a host name or IP address: 192.168.1.1

PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=0.741 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.036 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.022 ms

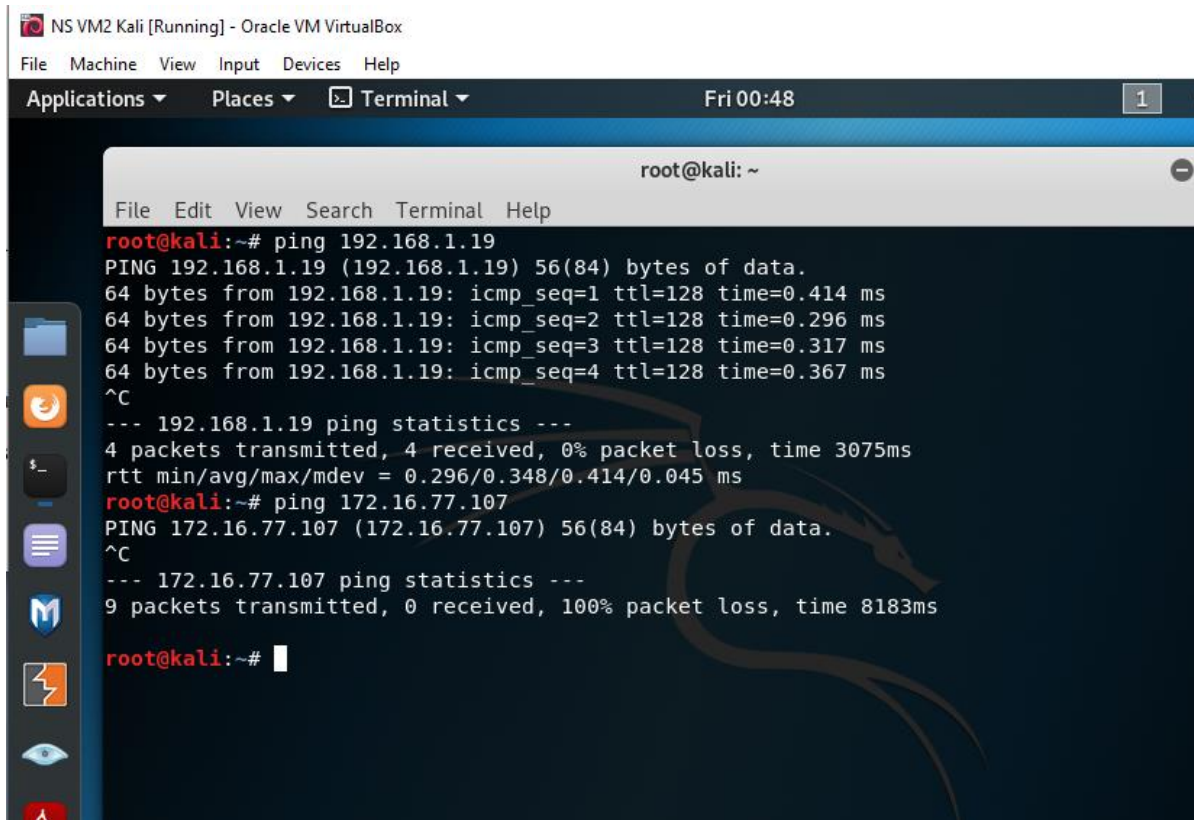
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.741/0.933/1.036/0.136 ms

Press ENTER to continue.
```

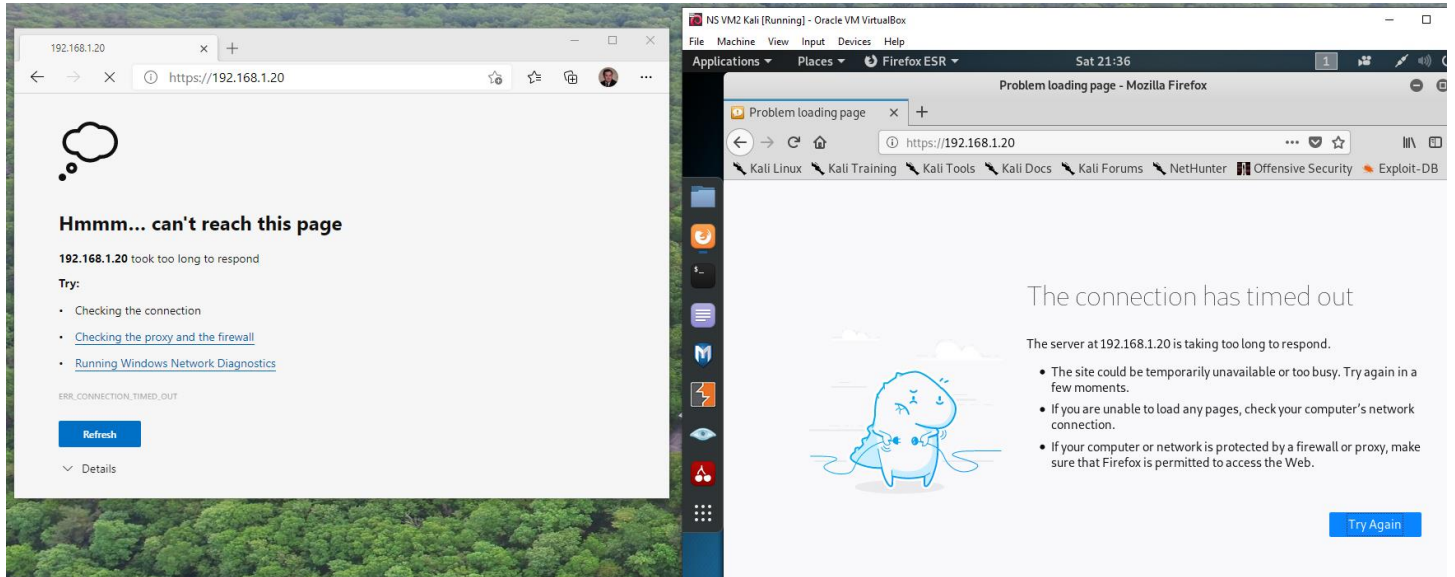

4. Any VM in the internal subnet can ping any other VM.



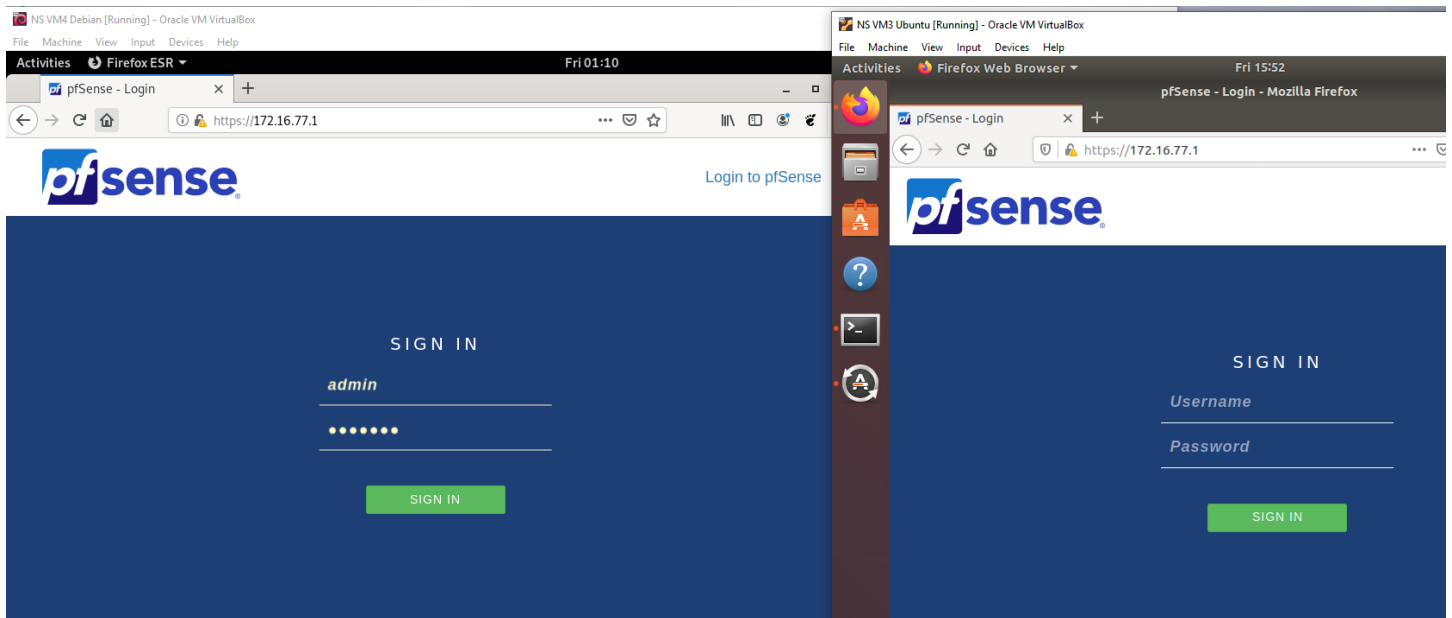
5. The Kali VM can ping the physical host but not the other VMs.



6. The pfSense management webpage cannot be accessed from the Kali VM and from the physical host (on the external network).

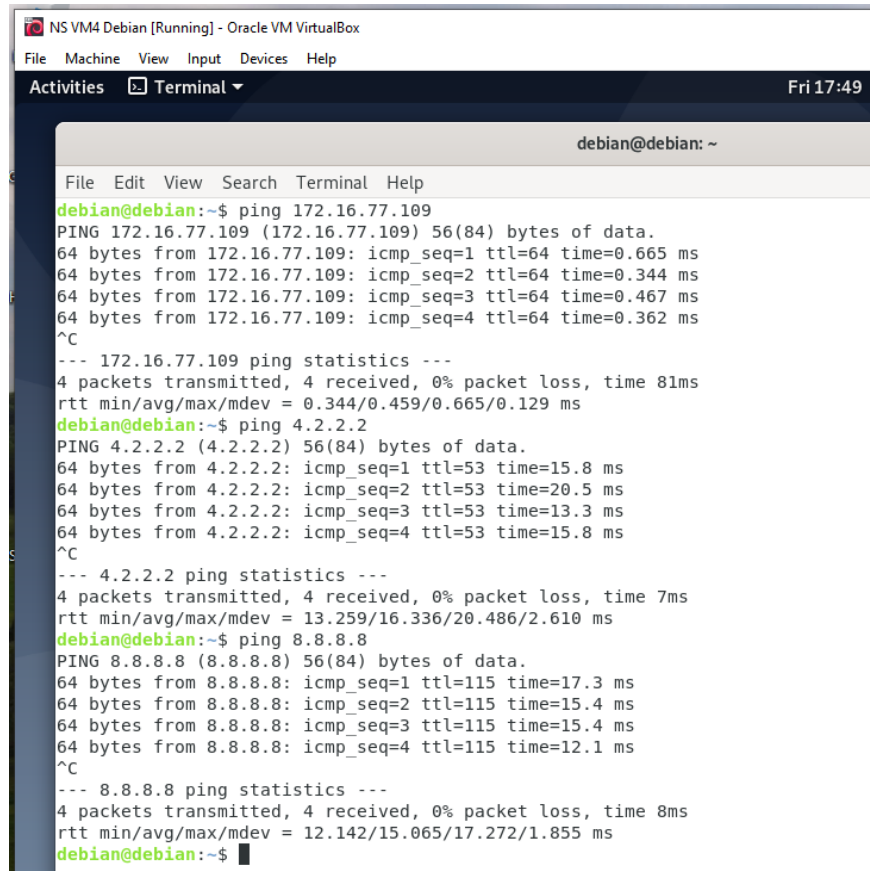


7. The pfSense management webpage can be opened from VMs on the internal subnet.



Project Task 1: Blocking Unwanted Traffic

- **Scenario:** Employees in the corporate / “internal” network can access online resources which they should not use (such as online games). Configure the firewall to block this unwanted traffic. For this scenario, the ICMP protocol will be used to represent the unwanted traffic.
1. From the Debian VM, it was verified that ICMP traffic is allowed to other internal VMs and to external addresses on the Internet (4.2.2.2 and 8.8.8.8 were tested). (Note: Systems were rebooted, so, from this point forward, the Ubuntu VM is now 172.16.77.109 and the Debian VM is now 172.16.77.110).



```
NS VM4 Debian [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Fri 17:49
debian@debian: ~
File Edit View Search Terminal Help
debian@debian:~$ ping 172.16.77.109
PING 172.16.77.109 (172.16.77.109) 56(84) bytes of data.
64 bytes from 172.16.77.109: icmp_seq=1 ttl=64 time=0.665 ms
64 bytes from 172.16.77.109: icmp_seq=2 ttl=64 time=0.344 ms
64 bytes from 172.16.77.109: icmp_seq=3 ttl=64 time=0.467 ms
64 bytes from 172.16.77.109: icmp_seq=4 ttl=64 time=0.362 ms
^C
--- 172.16.77.109 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 81ms
rtt min/avg/max/mdev = 0.344/0.459/0.665/0.129 ms
debian@debian:~$ ping 4.2.2.2
PING 4.2.2.2 (4.2.2.2) 56(84) bytes of data.
64 bytes from 4.2.2.2: icmp_seq=1 ttl=53 time=15.8 ms
64 bytes from 4.2.2.2: icmp_seq=2 ttl=53 time=20.5 ms
64 bytes from 4.2.2.2: icmp_seq=3 ttl=53 time=13.3 ms
64 bytes from 4.2.2.2: icmp_seq=4 ttl=53 time=15.8 ms
^C
--- 4.2.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 13.259/16.336/20.486/2.610 ms
debian@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=17.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=15.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=15.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=12.1 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 12.142/15.065/17.272/1.855 ms
debian@debian:~$
```

2. The WAN interface of pfSense was configured to allow traffic for private networks and loopback addresses.

The screenshot shows the pfSense web interface for configuring the WAN interface. The browser address bar shows `https://192.168.1.14/interfaces.php?if=wan`. The page contains several sections with checkboxes and dropdown menus:

- Use IPv4 connectivity as parent interface**: ☐ Request a IPv6 prefix/information through the IPv4 connectivity link
- Request only an IPv6 prefix**: ☐ Only request an IPv6 prefix, do not request an IPv6 address
- DHCPv6 Prefix Delegation size**: The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the ISP.
- Send IPv6 prefix hint**: ☐ Send an IPv6 prefix hint to indicate the desired prefix size for delegation
- Debug**: ☐ Start DHCP6 client in debug mode
- Do not wait for a RA**: ☐ Required by some ISPs, especially those not using PPPoE
- Do not allow PD/Address release**: ☐ dhcp6c will send a release to the ISP on exit, some ISPs then release the allocated address or prefix. This option prevents that signal ever being sent

Reserved Networks

- Block private networks and loopback addresses**: ☐ Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
- Block bogon networks**: ☒ Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

A **Save** button is located at the bottom of the configuration area.

3. A firewall rule was created within the pfSense LAN interface to block ICMP traffic for a specific destination, 8.8.8.8, and logging was enabled for packets that match the rule.

The screenshot shows the pfSense web interface for editing a firewall rule. The browser address bar shows `https://172.16.77.1/firewall_rules_edit.php?if=wan&after=-1`. The page is titled "Edit Firewall Rule" and contains the following configuration:

- Action**: Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
- Disabled**: ☐ Disable this rule Set this option to disable this rule without removing it from the list.
- Interface**: Choose the interface from which packets must come to match this rule.
- Address Family**: Select the Internet Protocol version this rule applies to.
- Protocol**: Choose which IP protocol this rule should match.
- ICMP Subtypes**: Alternate Host, Datagram conversion error, Echo reply For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

- Source**: ☐ Invert match. Source Address:

Destination

- Destination**: ☐ Invert match. Destination:

Extra Options

- Log**: ☒ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
- Description**: A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

- By pinging both WAN addresses again, it was verified that the firewall rule successfully blocks ICMP traffic to 8.8.8.8 only.

```
NS VM4 Debian [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal ▾
debian@debian: ~
File Edit View Search Terminal Help
debian@debian:~$ ping 4.2.2.2
PING 4.2.2.2 (4.2.2.2) 56(84) bytes of data.
64 bytes from 4.2.2.2: icmp_seq=1 ttl=53 time=15.9 ms
64 bytes from 4.2.2.2: icmp_seq=2 ttl=53 time=12.8 ms
64 bytes from 4.2.2.2: icmp_seq=3 ttl=53 time=12.8 ms
64 bytes from 4.2.2.2: icmp_seq=4 ttl=53 time=14.7 ms
^C
--- 4.2.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 10ms
rtt min/avg/max/mdev = 12.805/14.049/15.892/1.312 ms
debian@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 100ms

debian@debian:~$
```

- Evidence:** Since logging was enabled for the firewall rule, the pfSense firewall logs show that the rule was successfully configured and is blocking ICMP traffic to 8.8.8.8.

pfSense.localdomain - Status

https://172.16.77.1/status_logs_filter.php 80%

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / System Logs / Firewall / Normal View

System Firewall DHCP Captive Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings

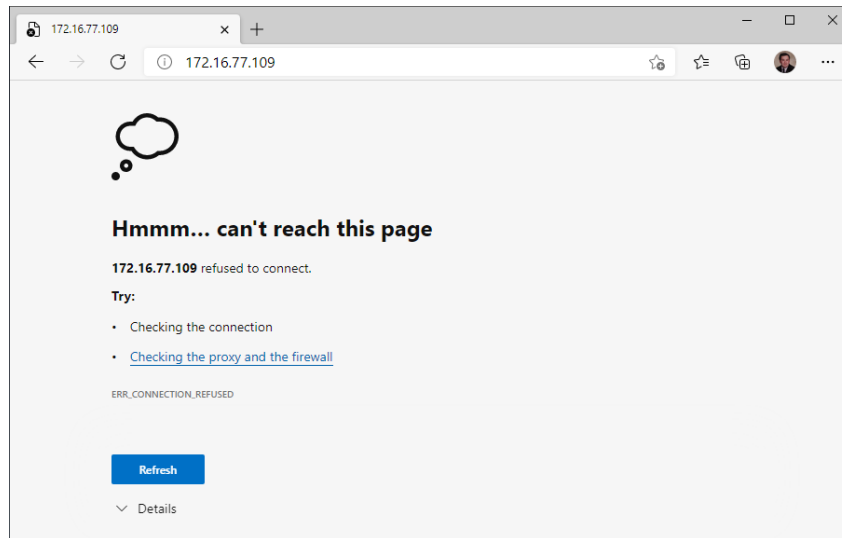
Normal View Dynamic View Summary View

Last 50 Firewall Log Entries. (Maximum 50)

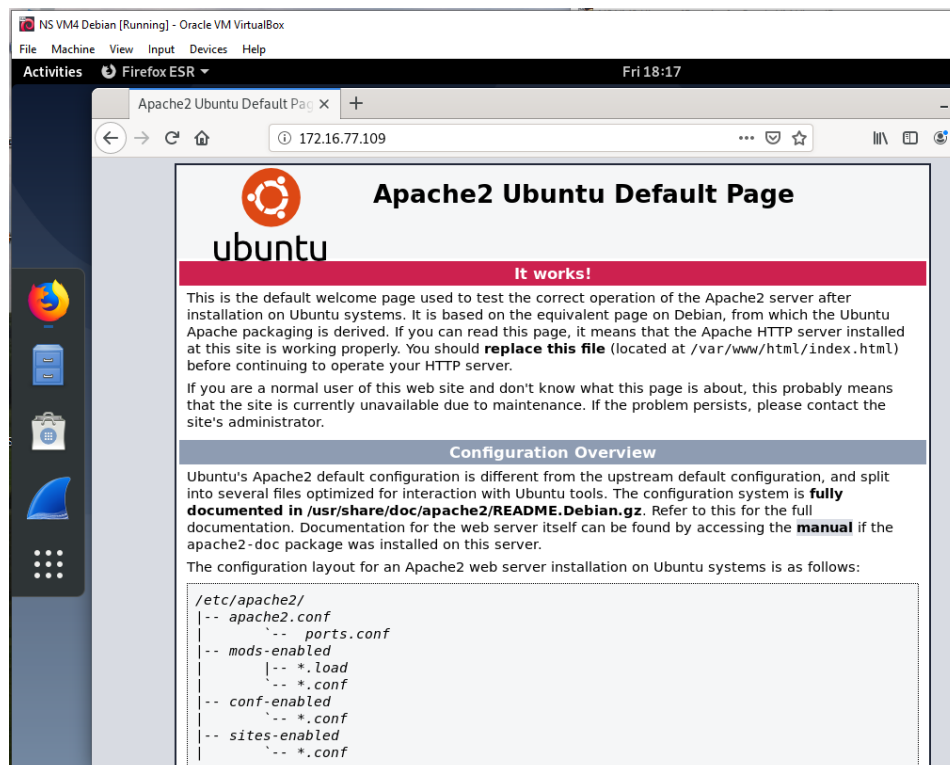
Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jan 29 23:00:39	LAN	Block ICMP to 8.8.8.8 (1611961110)	172.16.77.110	8.8.8.8	ICMP
✗	Jan 29 23:00:40	LAN	Block ICMP to 8.8.8.8 (1611961110)	172.16.77.110	8.8.8.8	ICMP
✗	Jan 29 23:00:41	LAN	Block ICMP to 8.8.8.8 (1611961110)	172.16.77.110	8.8.8.8	ICMP
✗	Jan 29 23:00:42	LAN	Block ICMP to 8.8.8.8 (1611961110)	172.16.77.110	8.8.8.8	ICMP
✗	Jan 29 23:00:43	LAN	Block ICMP to 8.8.8.8 (1611961110)	172.16.77.110	8.8.8.8	ICMP

Project Task 2: Quick Solution for Remote Access

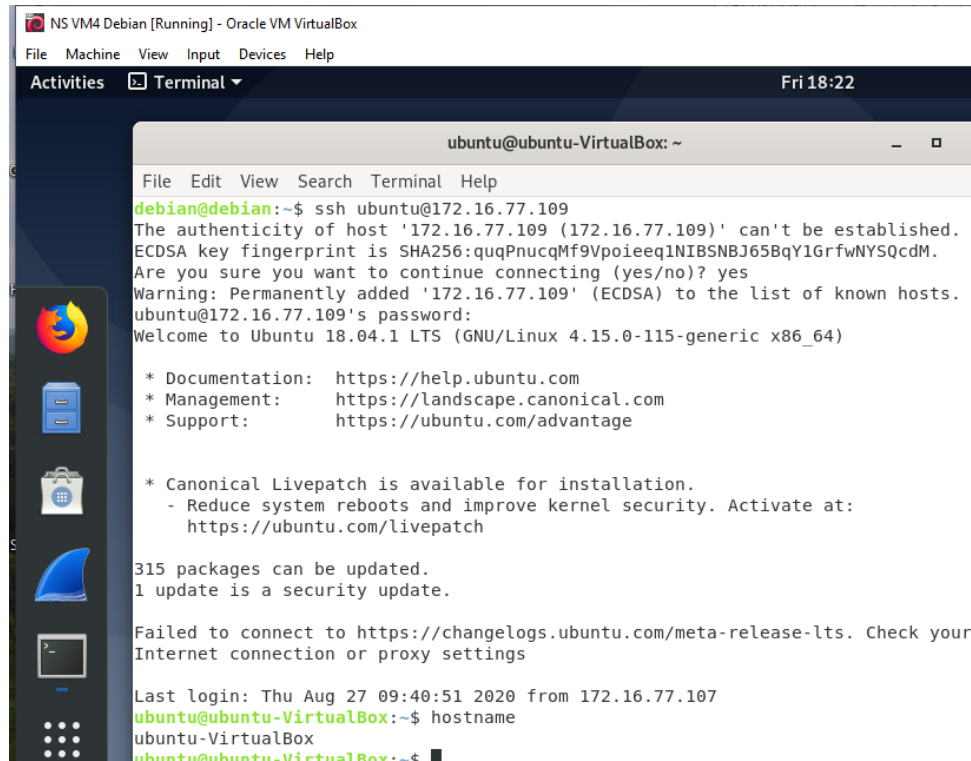
- **Scenario:** During the COVID-19 outbreak, some services needed to be performed remotely. An employee requires access to systems running on the web server at the HQ office and the ability to manage the web server that runs on the Ubuntu VM via SSH. The Warehouse Manager requested VPN access for the employees, but, while the firewall is not licensed and configured to work as needed, he wants the employees to have temporary access via other means. In this task, the web server and SSH service is to be made available for connection from remote networks by means other than a VPN.
1. The web server cannot be accessed from the host machine. This is because the Ubuntu VM (which hosts the web server) is on a different subnet that cannot be reached from the external network. (The internal machines are able to access the external network through NAT, but not vice-versa.)



2. The web server can be successfully accessed from the Debian VM (on the same internal network), verifying its functionality.



3. I can successfully access the Ubuntu VM's SSH service from the Debian VM, verifying its functionality.



```
NS VM4 Debian [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Fri 18:22

ubuntu@ubuntu-VirtualBox: ~
File Edit View Search Terminal Help

debian@debian:~$ ssh ubuntu@172.16.77.109
The authenticity of host '172.16.77.109 (172.16.77.109)' can't be established.
ECDSA key fingerprint is SHA256:quqPnucqMf9Vpoieeq1NIBSNBJ65BqY1GrfwNYSQcdM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.77.109' (ECDSA) to the list of known hosts.
ubuntu@172.16.77.109's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-115-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

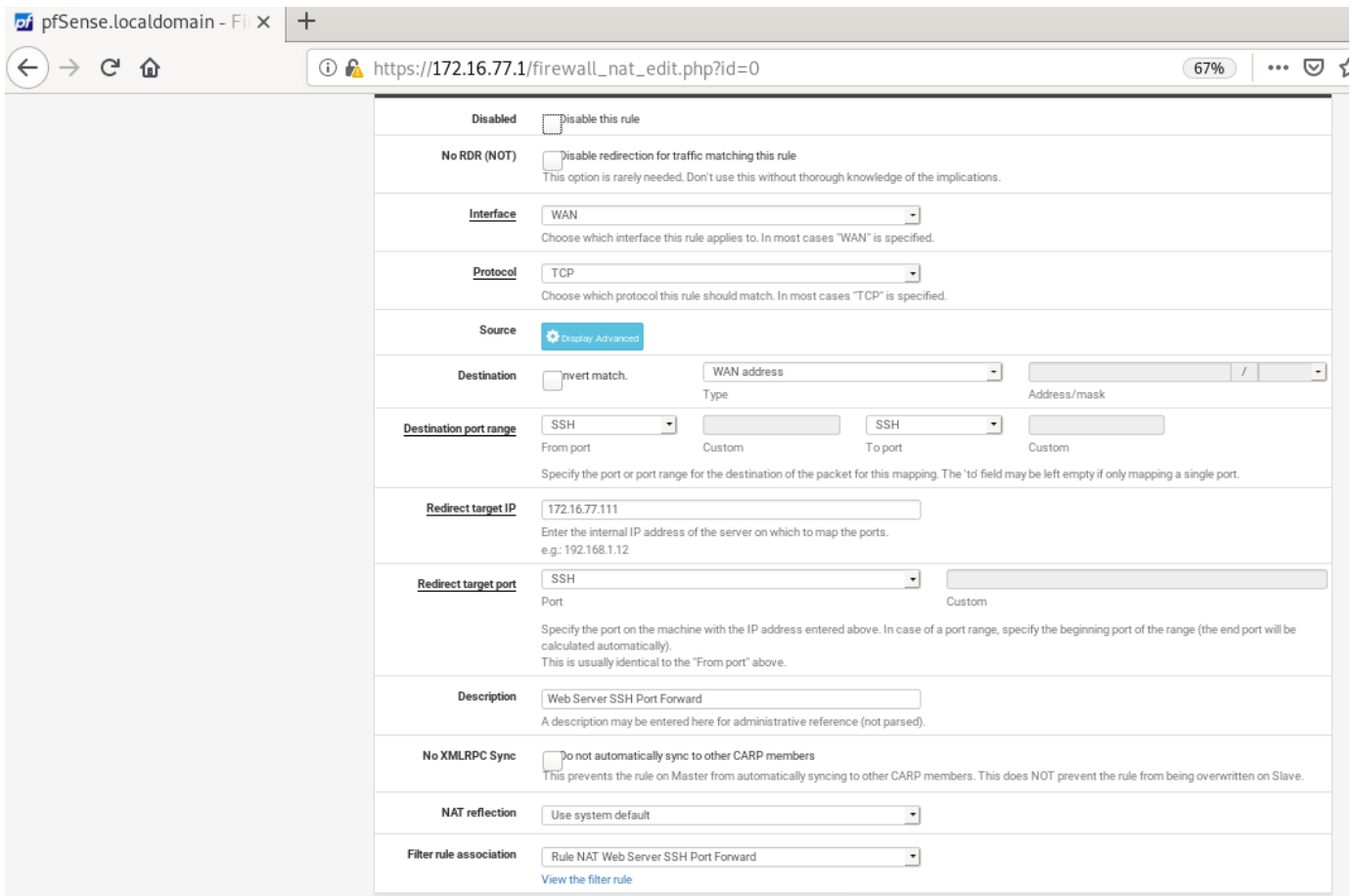
 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

315 packages can be updated.
1 update is a security update.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Thu Aug 27 09:40:51 2020 from 172.16.77.107
ubuntu@ubuntu-VirtualBox:~$ hostname
ubuntu-VirtualBox
ubuntu@ubuntu-VirtualBox:~$
```

4. Two NAT port forwarding rules were created in pfSense to translate the external requests to the web server. Firewall rules were automatically created on the WAN port to authorize this traffic. (Note: Systems were rebooted, so, from this point forward, the Ubuntu VM's IP address is now 172.16.77.111.)



pfSense.localdomain - Firewall

https://172.16.77.1/firewall_nat_edit.php?id=0

67%

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination ☐ Invert match. WAN address / Address/mask
Type Address/mask

Destination port range SSH From port Custom SSH To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP 172.16.77.111
Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12

Redirect target port SSH Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description Web Server SSH Port Forward
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync ☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Rule NAT Web Server SSH Port Forward
[View the filter rule](#)

Port Forward 1:1 Outbound NPt

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions	
<input type="checkbox"/>	✓	WAN	TCP	*	*	WAN address	22 (SSH)	172.16.77.111	22 (SSH)	Web Server SSH Port Forward	
<input type="checkbox"/>	✓	WAN	TCP	*	*	WAN address	80 (HTTP)	172.16.77.111	80 (HTTP)	Web Server HTTP Port Forward	

Firewall / Rules / WAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/16 KiB	IPv4 TCP	*	*	172.16.77.111	80 (HTTP)	*	none		NAT Web Server HTTP Port Forward	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	172.16.77.111	22 (SSH)	*	none		NAT Web Server SSH Port Forward	

- **Evidence:** Multiple systems on the external network (the physical host and the Kali VM) were able to successfully access both the web server and SSH service via the pfSense WAN address. (Note: Systems were rebooted, so, from this point forward, the pfSense WAN IP address is now 192.168.1.20.)

Apache2 Ubuntu Default Page: It works!

Warning: Permanently added '192.168.1.20' (ECDSA) to the list of known hosts.

ubuntu@192.168.1.20's password:

Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-115-generic x86_64)

* Documentation: <https://help.ubuntu.com>
 * Management: <https://landscape.canonical.com>
 * Support: <https://ubuntu.com/advantage>

Canonical Livepatch is available for installation.
 - Reduce system reboots and improve kernel security. Activate at: <https://ubuntu.com/livepatch>

315 packages can be updated.
 1 update is a security update.

New release '20.04.1 LTS' available.
 Run 'do-release-upgrade' to upgrade to it.

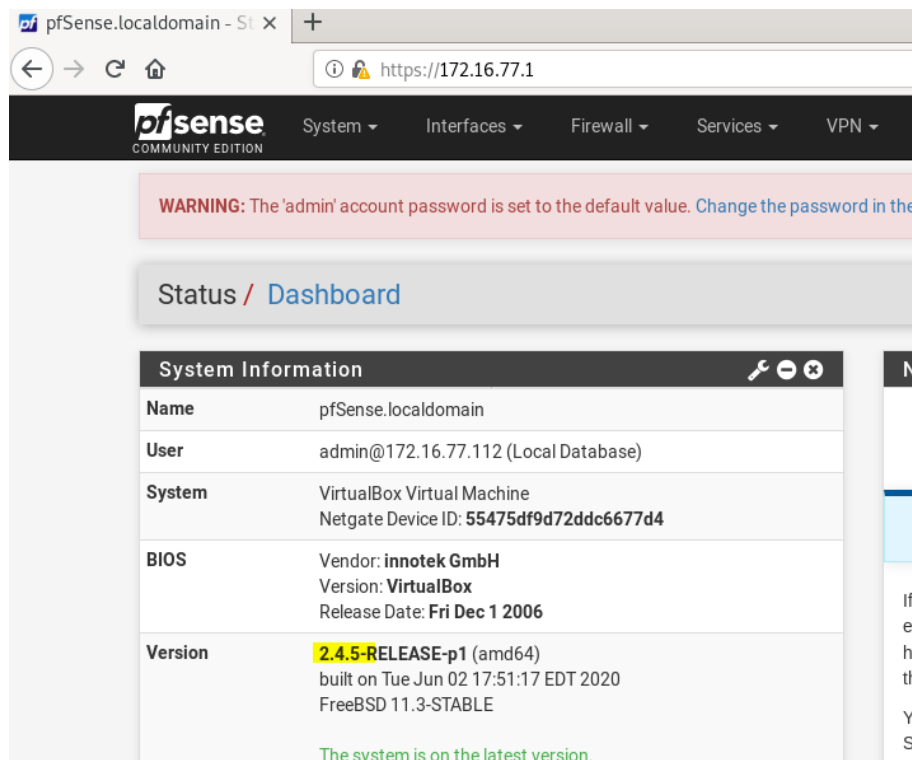
Last login: Sat Jan 30 17:34:18 2021 from 192.168.1.21

ubuntu@ubuntu-VirtualBox:~\$ hostname
 ubuntu-VirtualBox
 ubuntu@ubuntu-VirtualBox:~\$

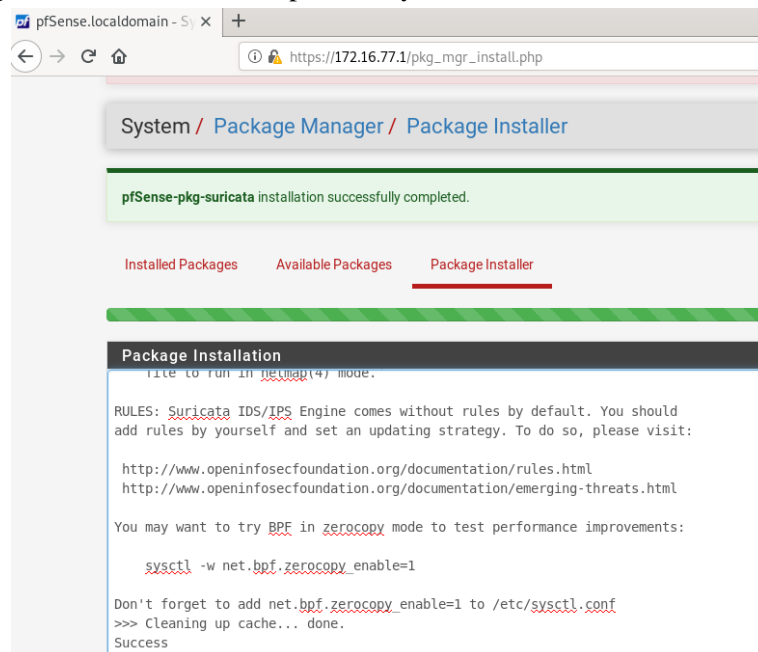
Project Task 3: The All-Seeing Eye

- **Scenario:** The CISO of the company decided to implement a detection and prevention system against potential known network attacks. It was requested to set up a mechanism capable of detecting DoS and brute-force attacks, and to verify that they function properly.

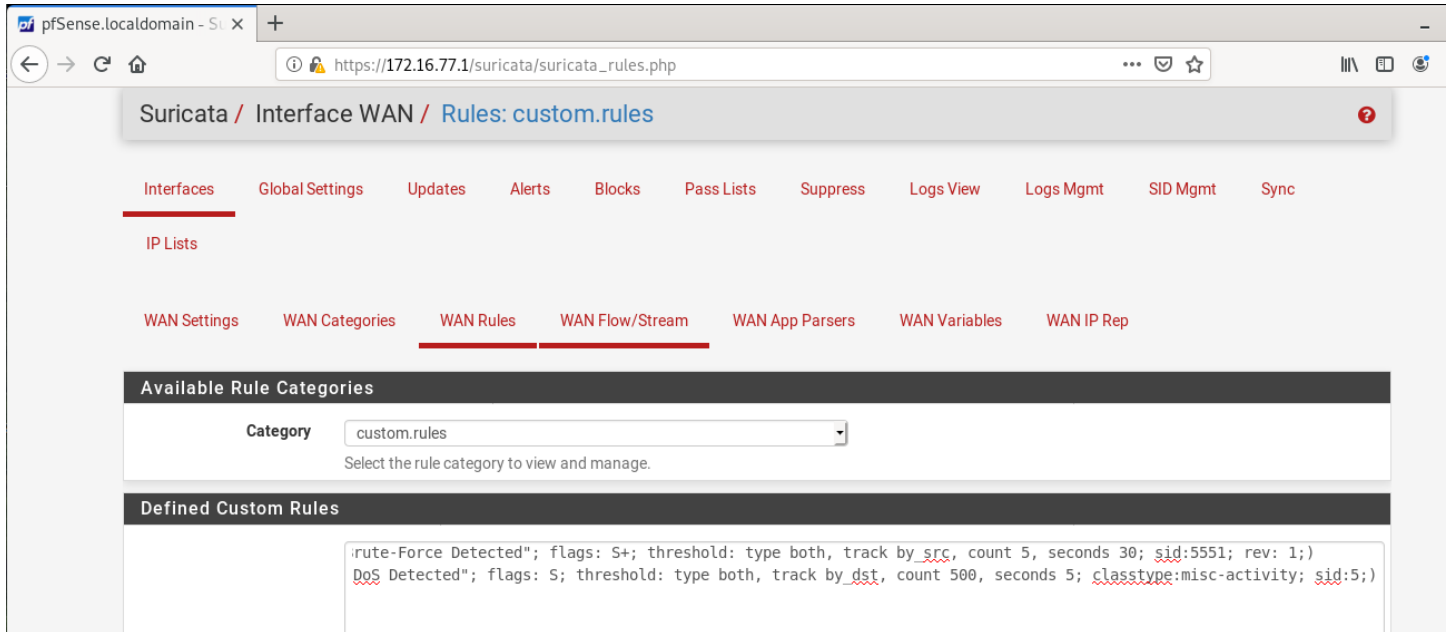
1. The Suricata IDS can be installed on top of pfSense to meet these requirements.
2. pfSense was updated to the latest version, 2.4.5, in order to support the most recent release of Suricata.



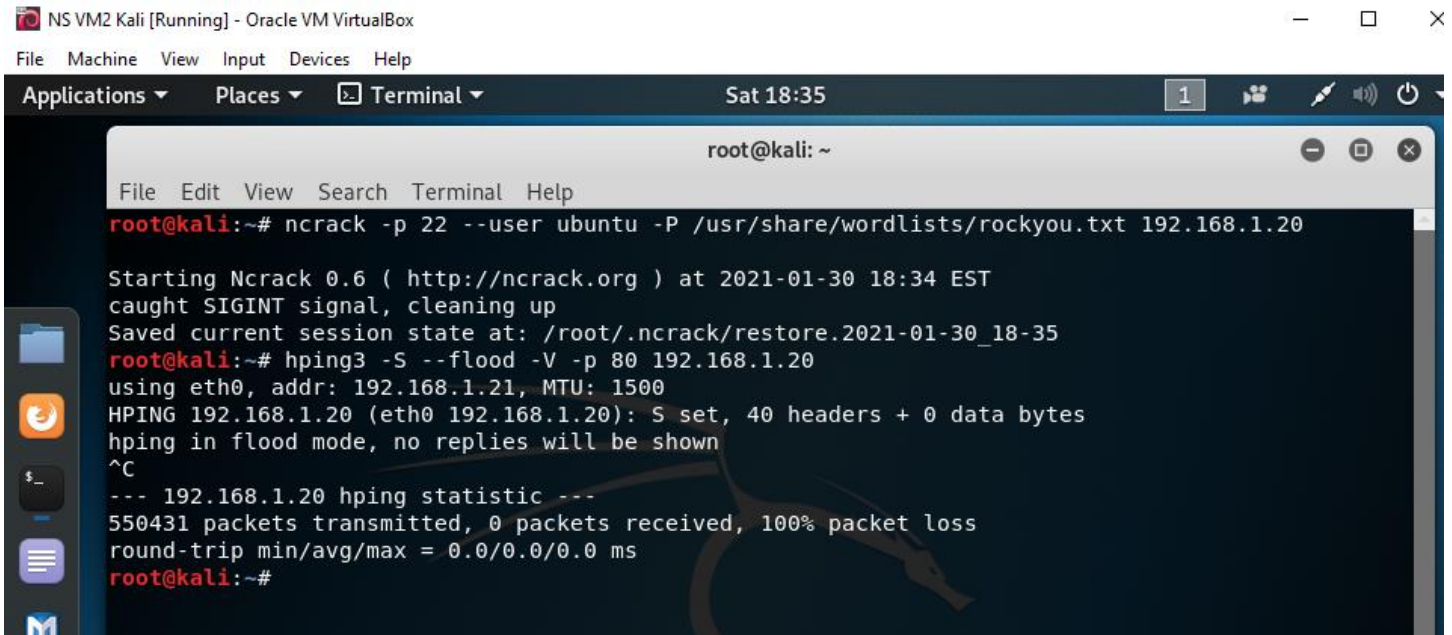
3. The Suricata package was installed onto the pfSense system.















4. Suricata was configured in pfSense to monitor the WAN interface, with custom rules to detect abnormal traffic. Rules applied were:
- ```
alert tcp any any -> any 22 (msg:"SSH Brute-Force Detected"; flags: S+; threshold: type both, track by_src, count 5, seconds 30; sid:5551; rev: 1;)
alert tcp any any -> any 80 (msg:"HTTP DoS Detected"; flags: S; threshold: type both, track by_dst, count 500, seconds 5; classtype:misc-activity; sid:5;)
```



5. An SSH brute-force attack and a HTTP DoS attack were executed, each for 30 seconds, from the Kali Linux machine.



6. **Evidence:** The Suricata alert entries within pfSense verify that everything works as expected and that the attacks were detected.

|                                                             |                                                                                   |   |     |               |                    |                 |        |                                                                                                                                                                         |                          |  |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------|---|-----|---------------|--------------------|-----------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--|
| pfSense.localdomain - Se x +                                |                                                                                   |   |     |               |                    |                 |        |                                                                                                                                                                         |                          |  |
| https://172.16.77.1/suricata/suricata_alerts.php?instance=0 |                                                                                   |   |     |               |                    |                 |        |                                                                                                                                                                         |                          |  |
| 01/30/2021 23:43:34                                         |  | 3 | TCP | Misc activity | 192.168.1.21 1539  | 192.168.1.20 80 | 1:5    |   | HTTP DoS Detected        |  |
| 01/30/2021 23:43:34                                         |  | 3 | TCP | Misc activity | 192.168.1.21 1539  | 192.168.1.20 80 | 1:5    |   | HTTP DoS Detected        |  |
| 01/30/2021 23:43:05                                         |  | 3 | TCP | Not Assigned  | 192.168.1.21 59594 | 192.168.1.20 22 | 1:5551 |   | SSH Brute-Force Detected |  |
| 01/30/2021 23:43:05                                         |  | 3 | TCP | Not Assigned  | 192.168.1.21 59594 | 192.168.1.20 22 | 1:5551 |   | SSH Brute-Force Detected |  |