**Student Name:** **Coleton Sanheim**  **Weight: \_\_\_2.0\_\_\_\_\_%**

**Student ID:** **000862545**  **Marks: \_\_\_\_\_\_\_\_\_\_**

Lab 6: Firewalls

# Learning Outcomes

* Configure zone-based policy firewalls.
* Perform firewall configuration and policy testing.
* Verify firewall functionality.

# Purpose

In this lab, we focus on the installation of a firewall and the configuration of access rules to allow traffic through the firewall.

# Tools

* VM Firewall (pfSense)
* VM workstation x 2
  + Kali-nmap-hping3-OpenVAS
  + Ubuntu-Apache

# References

<https://doc.pfsense.org/index.php/Installing_pfSense#Prepare_Installation_Media>

<https://doc.pfsense.org/index.php/Category:PF>

# Topology

VM Web

Server

pfSense

Firewall

Kali VM

LANseg2

LANseg1

© 2017, Southern Alberta Institute of Technology

|  |  |  |
| --- | --- | --- |
| System | Network | IP Address |
| PFSense | Trusted Net  Untrusted Net | 192.168.1.1  172.16.4.1 |
| Kali | Untrusted | 172.16.4.98 |
| Ubuntu | Trusted | 192.168.1.2 |

# Setup

Before you begin the lab activities, perform the steps below to set up your computer.

1. Set up a Kali workstation in a VM using ISO with the following parameters:

* 1 CPU
* 1 GB of RAM
* 80 GB HDD
* Network Adapter: NAT, for Internet access
* Latest version of Wireshark with Winpcap

Reconfigure the network adapter:

* Change network adapter to LAN Segment 1 in the VM console
* Configure the IP address to: 172.16.4.98/24
* Configure the gateway to: 172.16.4.1

1. Set up an Ubuntu (Web) server in the VM using ISO with the following parameters, use previous if available

* 1 CPU
* 1 GB of RAM
* 80 GB HDD
* Network Adapter: NAT, for Internet access
  1. Install an Ubuntu web server by entering the following commands:
  + sudo apt install apache2
  + sudo apt install net-tools

Reconfigure the network adapter:

* Change network adapter to LANSeg 2 in the VM console

You may need to perform sudo ifconfig <interfacename> down

* Configure the IP address to: 192.168.1.2/24
* Configure the gateway/dns to: 192.168.1.1

You may need to perform sudo ifconfig <interfacename> down

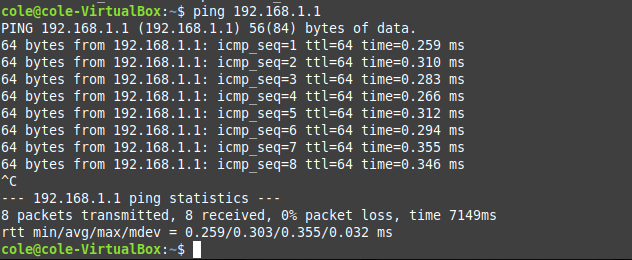
1. Set up pfSense, see pfSense setup document:

* Set up LANSeg2 – MAC:**0800275D9178** 192.168.1.1/24 (LAN) em1
* Set up LANSeg1 – MAC:**0800273560DB** 172.16.4.1/24 (WAN) em0

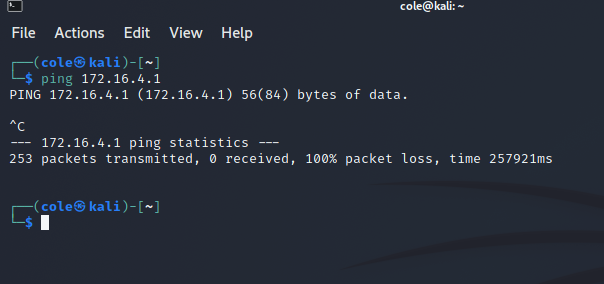
# Activities

## Verify connectivity to gateways

1. Verify that the Web VM can reach gateway 192.168.1.1.



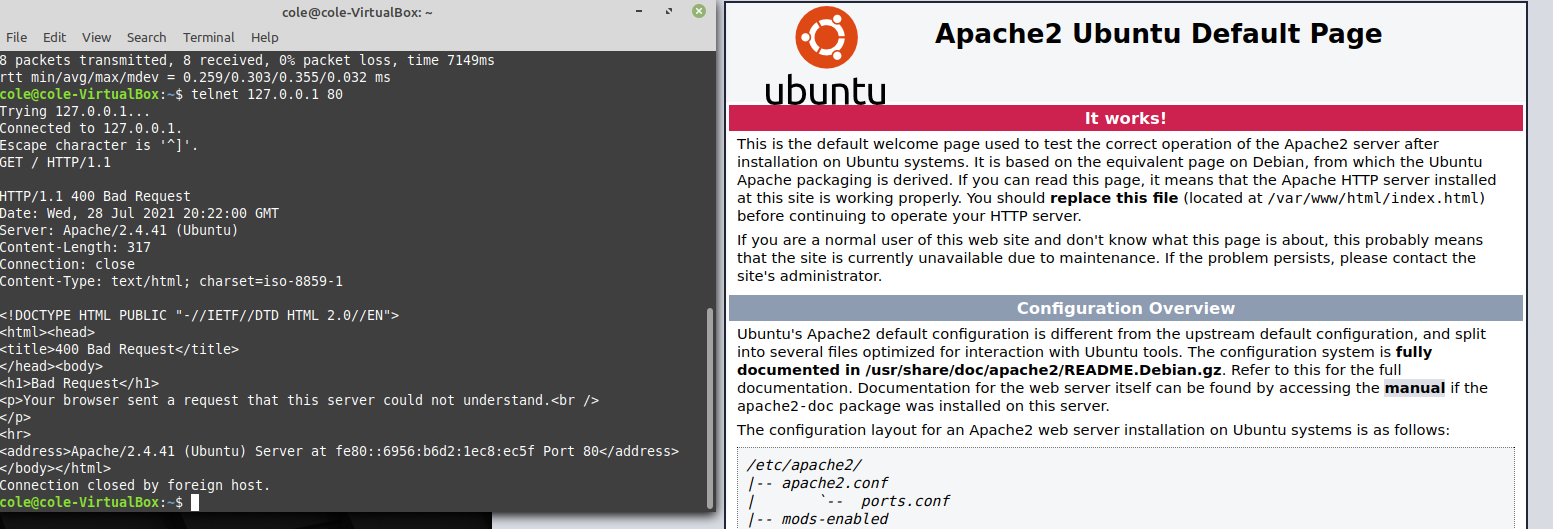
1. Verify the Kali VM can’t reach gateway 172.16.4.1.



## Verify that VM web server Apache2 is running

1. From the VM web server console, telnet to localhost (127.0.0.1) on port 80.
2. Type **GET /** HTTP/1.1 and press ENTER.

You should receive HTML code from the web server.



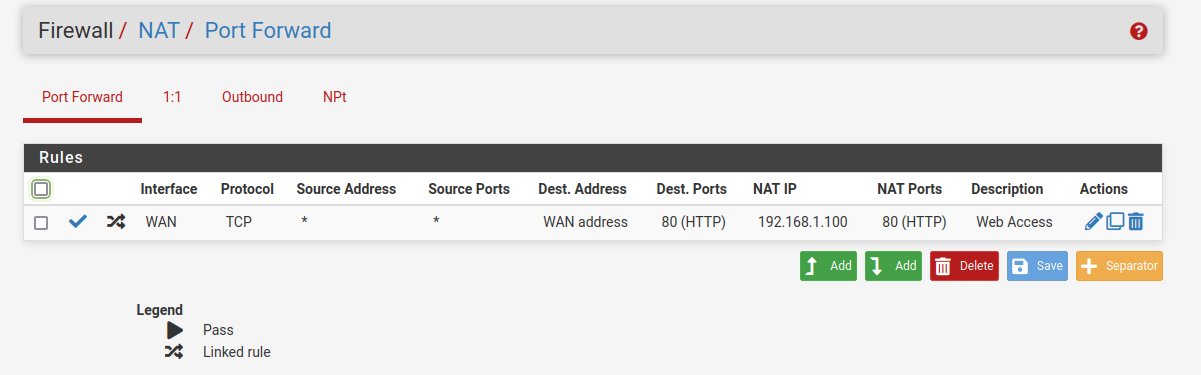
## Reboot pfSense Firewall

## Configure pfSense to permit port 80 access from the VM Web Server

1. Log into pfSense interface to configure firewall rules.

default username admin and password pfsense to login

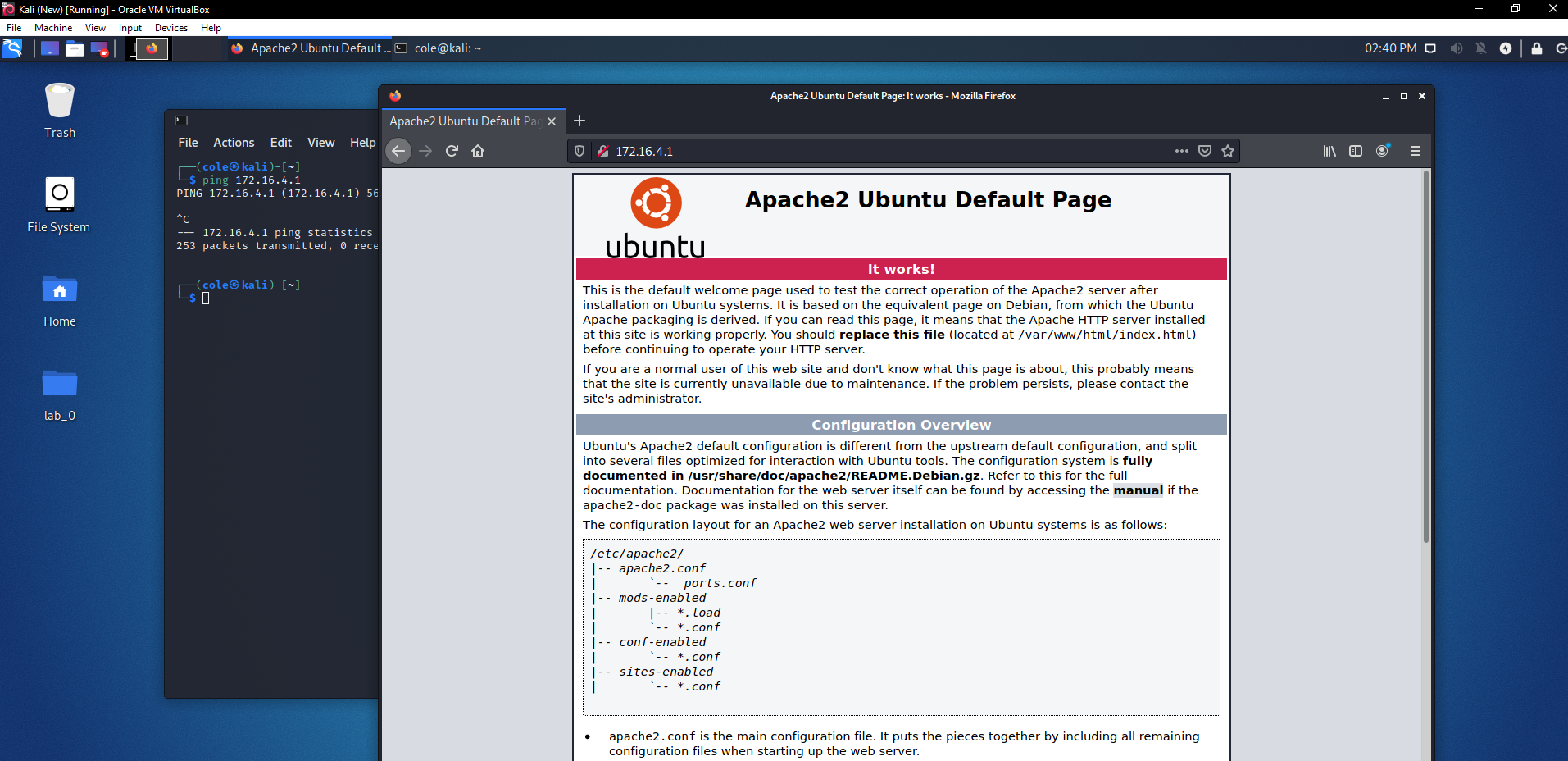
1. Under **firewall > NAT > Port Forward**, add a new rule to the OUTSIDE interface.
   1. Permit WAN Interface
   2. Protocol: TCP
   3. Destination WAN address
   4. Destination port range From: HTTP To: HTTP
   5. Redirect target IP: 192.168.1.2
   6. Redirect target port HTTP.
2. Change Firewall rules to ensure block is at the bottom
3. Click on Apply changes



## Verify VM workstation connectivity to the VM web server on port 80

1. From the Kali VM workstation, open a browser to [http://172.16.4.](http://172.16.4.2)1.

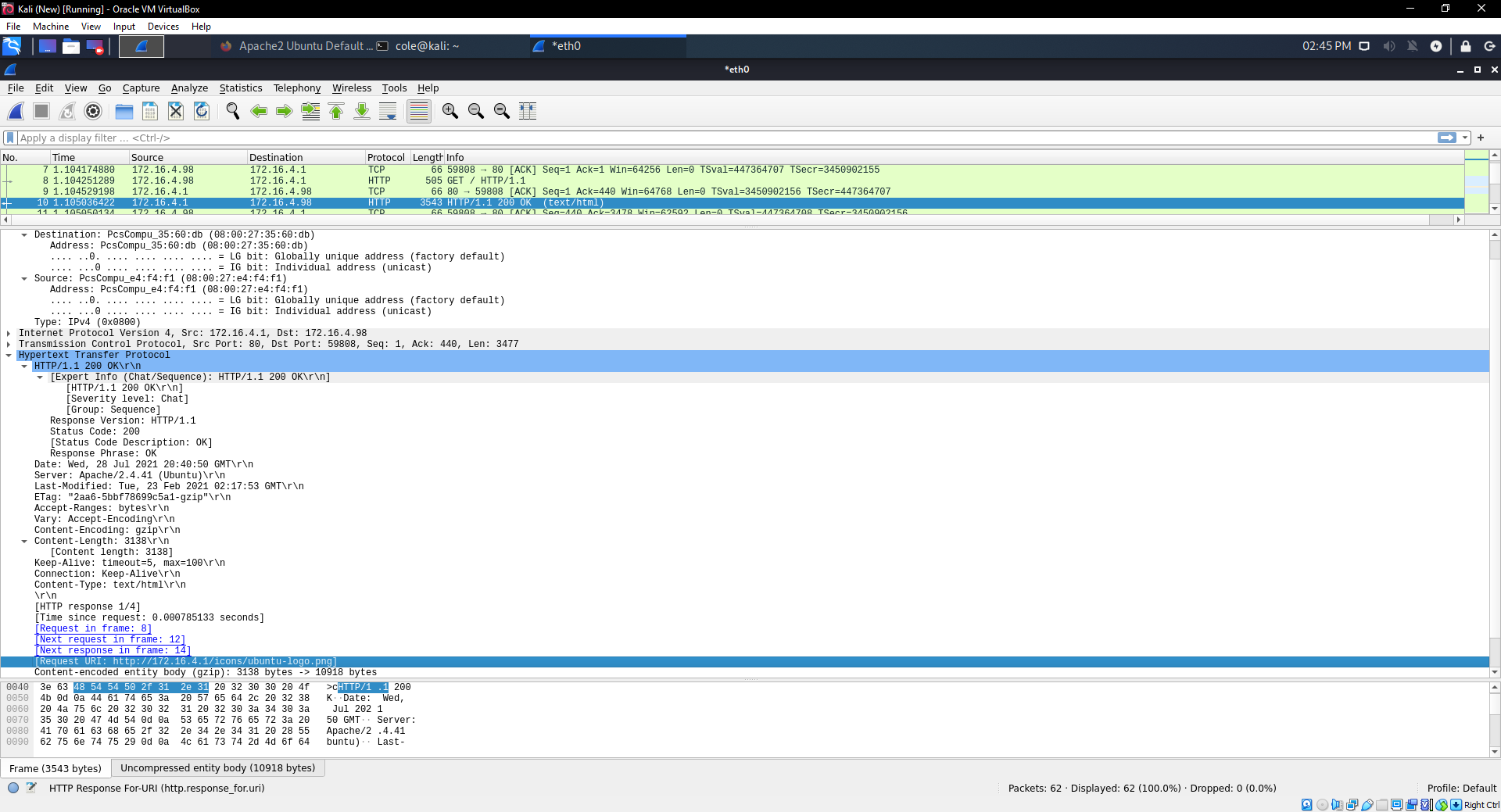
The Apache2 Ubuntu default page opens.



1. Demonstrate connections to the web server using Wireshark.

**Question:** What URIs are requested by the web browser?

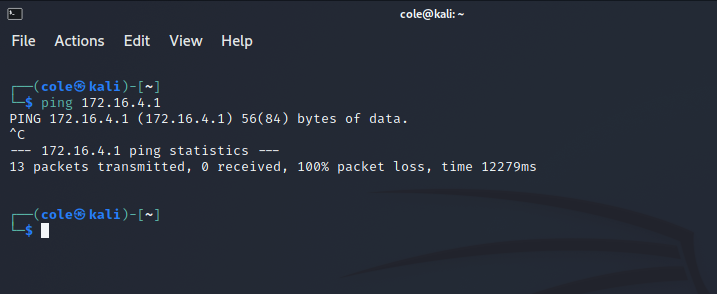
**Hint:** Wireshark, Apache log

****

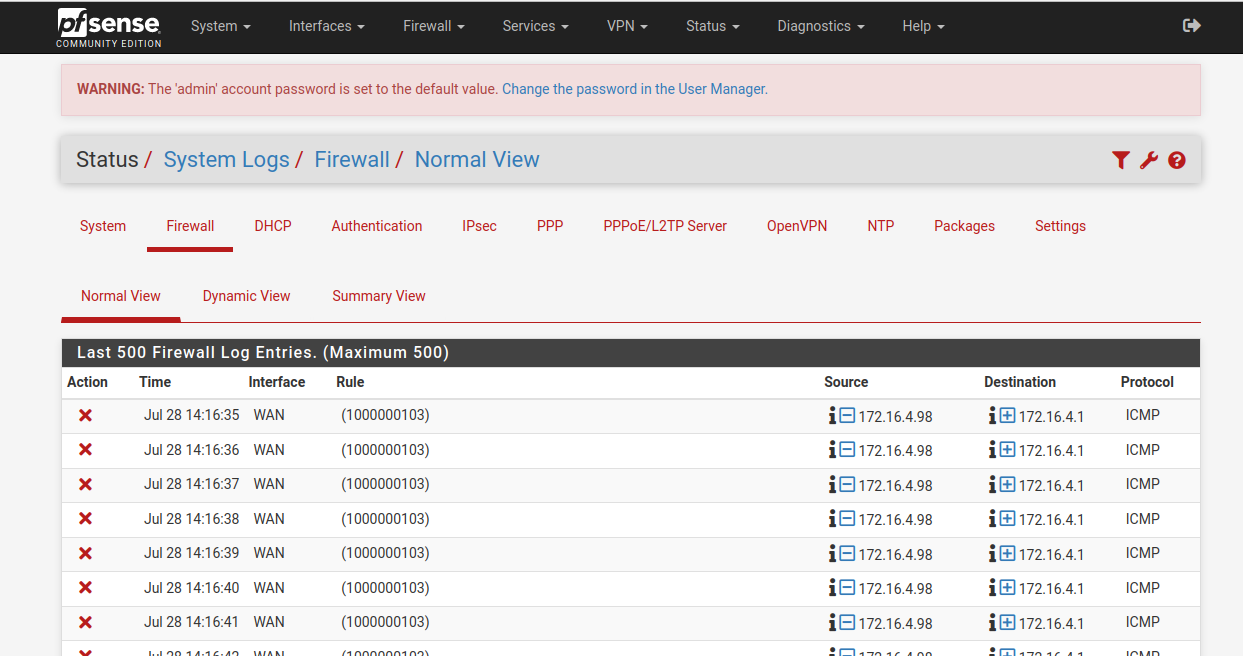
## Ping the web server

1. From VM workstation, ping the web server at 172.16.4.1.

Your ping should be blocked by the pfSense firewall.

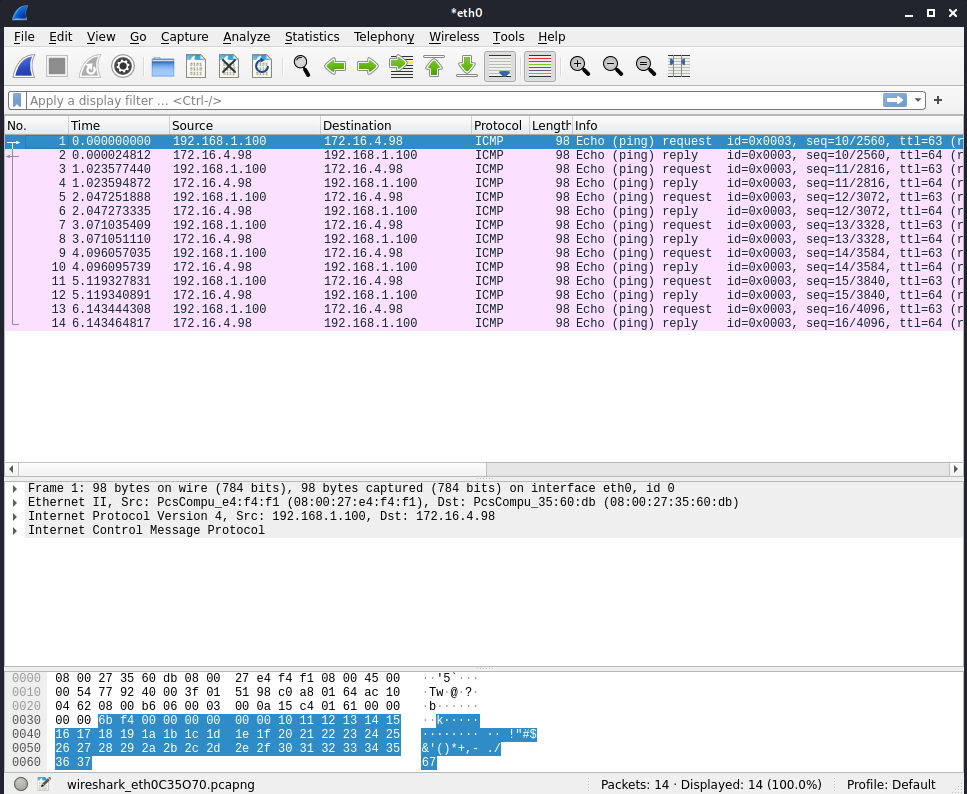


1. Demonstrate that the ping was denied by the firewall using firewall logs, pfSense tcpdump



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Demonstrate the ping sent by the VM web server using Wireshark.



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Instructor verified

1. Ask instructor to review setup and workings evidence: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Testing Activities

## Perform testing against the firewall from Kali

## Verify that the Web VM can reach gateway 192.168.1.1.

Suggested commands

nmap

-sS TCP Syn Scan

-sU UDP Scan

-p1-65535 ports 1-65535

-Pn Treat all hosts as online -- skip host discovery

-n Never do DNS resolution/Always resolve [default: sometimes]

-sV Probe open ports to determine service/version info

-T 3 Set timing template (higher is faster)

-v Increase verbosity level (use -vv or more for greater effect)

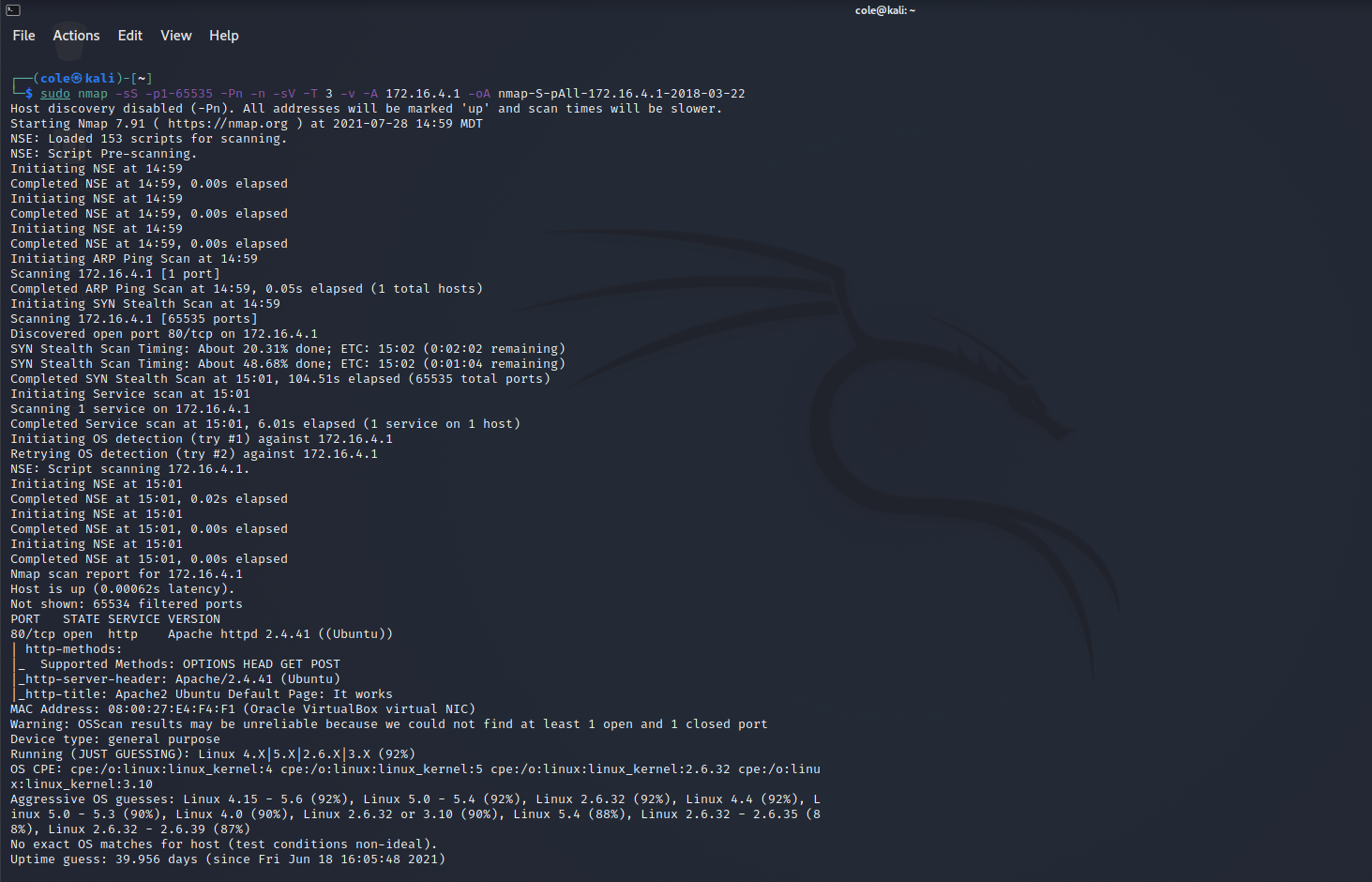
-A Enable OS detection, version detection, script scanning, and traceroute

-f; --mtu <val>: fragment packets (optionally w/given MTU)

-g/--source-port <portnum>: Use given port number

-oA <filename> Output in the three major formats at once

nmap -sS -p1-65535 -Pn -n -sV -T 3 -v -A 172.16.4.1 -oA nmap-S-pAll-172.16.4.1-2018-03-22

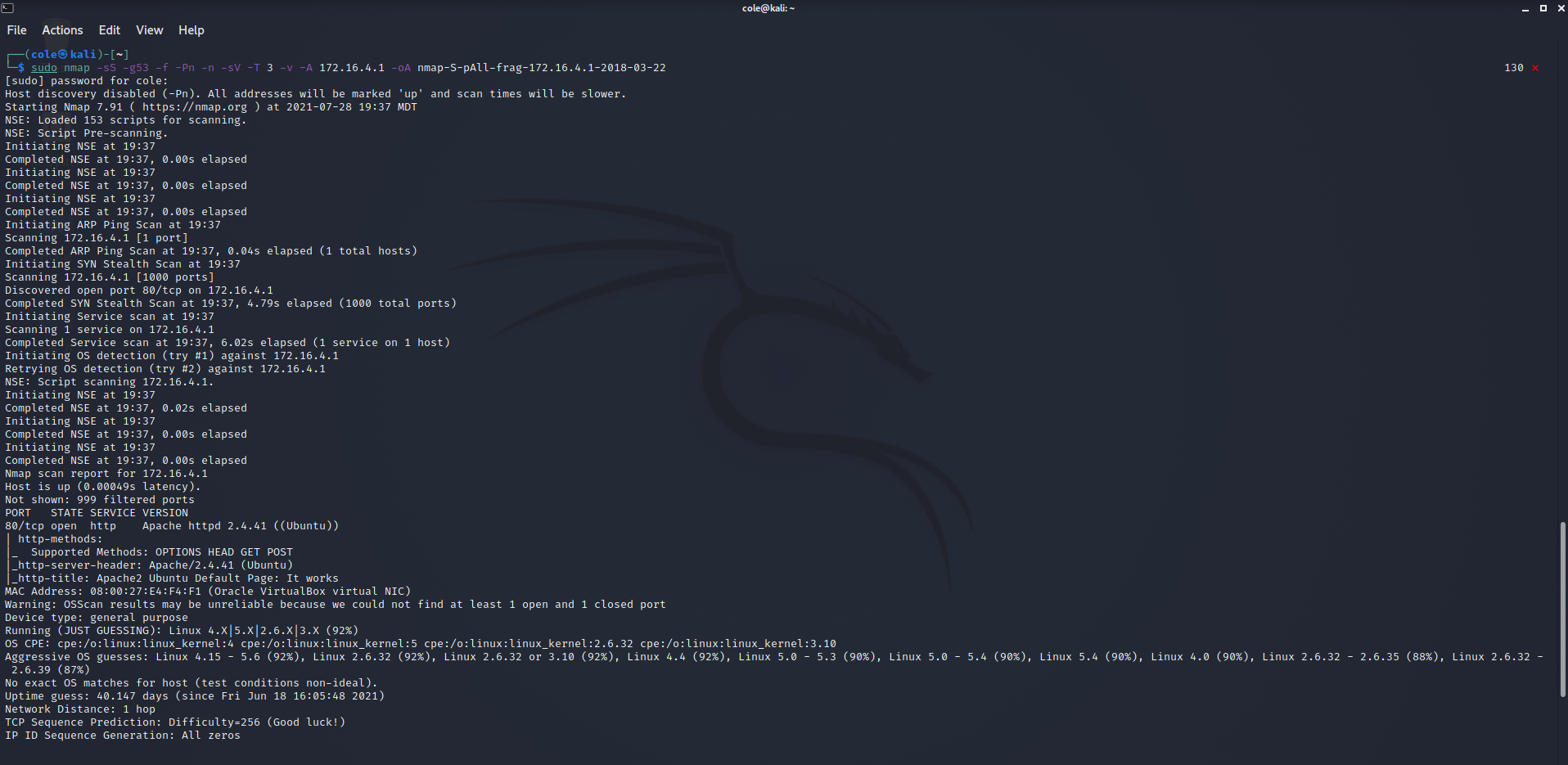


nmap -sU -p1-65535 -Pn -n -sV -T 3 -v -A 172.16.4.1 -oA nmap-U-pAll-172.16.4.1-2018-03-22



**So I ran this one for ~3 hours and it got 1.01% done, and with an estimated time of 90 hours I decided to not finish it, sorry.**

nmap -sS -g53 -p80 -f -Pn -n -sV -T 3 -v -A 172.16.4.1 -oA nmap-S-pAll-frag-172.16.4.1-2018-03-22



hping3

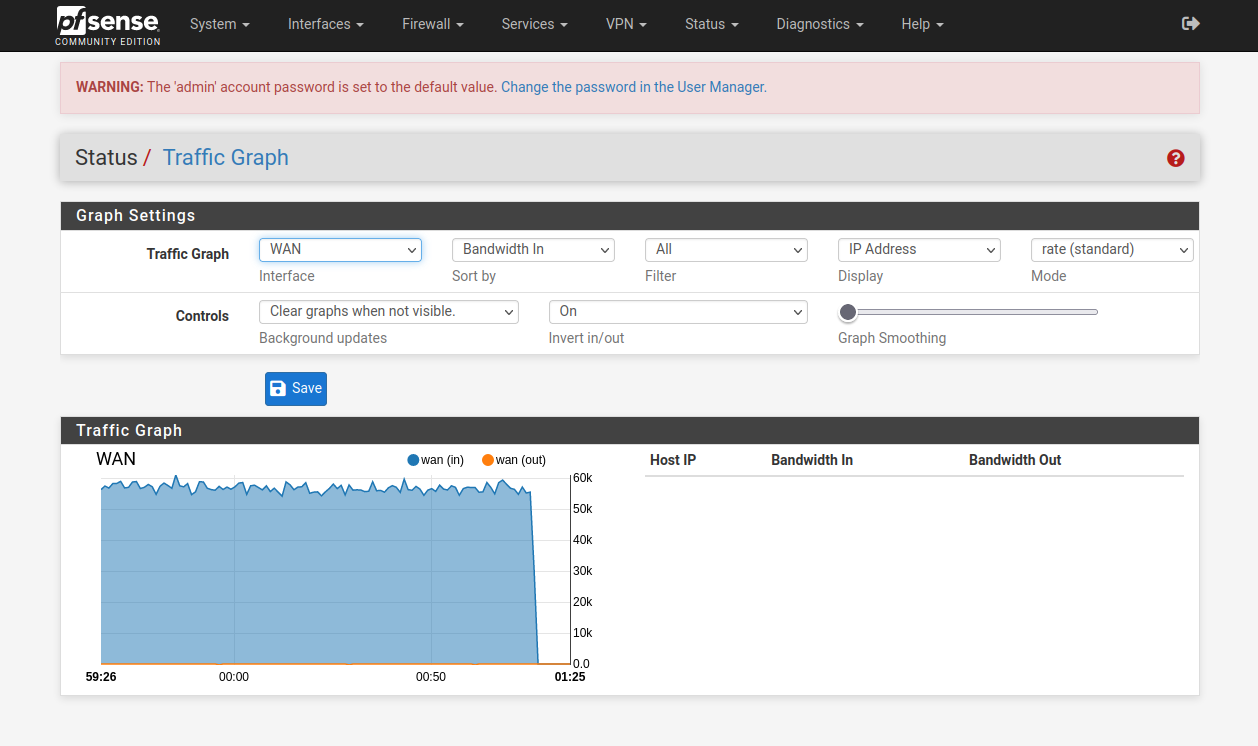
hping3 [destination host] [port] [number of packets to transmit] [verbose] [-S for SYN]

hping3 172.16.4.1 -p 22 -c 4 -V –S

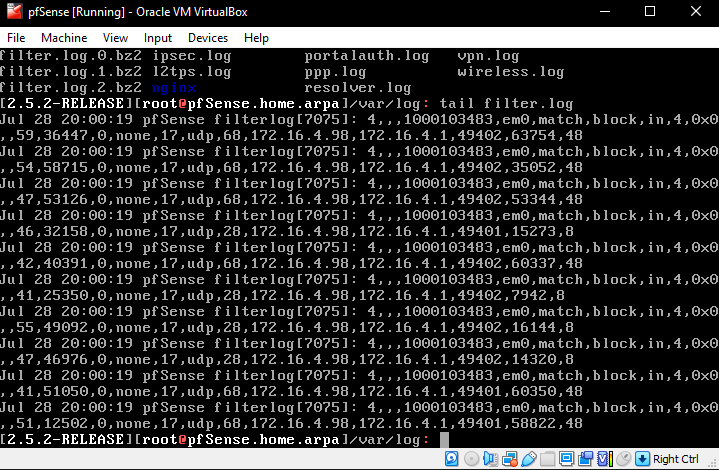
## Gather Evidence Using

Screenshots or files of above output:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Using Firewall Web GUI - Status> Traffic Graph



Using Firewall Command line interface - [admin@pfSense.localdomain]/var/log: clog -f filter.log



## Vulnerability Assessment

# Activities

1. Verify connectivity to gateways
2. Verify that the Kali VM can reach gateway 172.16.4.1
3. If browser didn’t pop up after install open with OpenVAS login screen, goto <https://127.0.0.1:9392/>
   1. Login with creds from the setup file possible 32 character
   2. Use OpenVAS browser goto Scans, use 172.16.4.1, output results

