

Module 2 - Wireshark & Cybersecurity Ethics

Cybersecurity Ethics

Before continuing on our Cyber Lions journey, we believe it is important to accustom yourself to the ethical aspects as they are related to cybersecurity. Below we have included a short video as well as a web link that will help familiarize you with all the different topics.

[Cyber Ethics in a Real World - YouTube Video](#)

[Cybersecurity Ethics - Article](#)

Wireshark

Thankfully, Wireshark is already included in the base version of Kali Linux, meaning we won't have to worry about any installation or setup on your Raspberry Pis. As long as you have followed all the previous modules correctly, this module should be pretty straightforward, and hopefully, you won't run into any issues. However, if you are running into issues, here is the documentation:


[Module 1- OS Setup and Networking](#)

This module will be broken up into two pieces, the first section will demonstrate a basic ping command and showcase Internet Control Message Protocol (ICMP). There won't be much to see, as there will only be pinging packets, which is why we have included the second half which involves contacting and making a virtual handshake with an Apache HTTP server.

Basic Ping Walkthrough

1. Start up Kali Linux on your Raspberry Pis

- a. By now, you should be familiar with how to login to Kali Linux on your Raspberry Pi, but if you have forgotten the credentials, the ones we recommended you use are:
 - i. Username: kali
 - ii. Password: kali

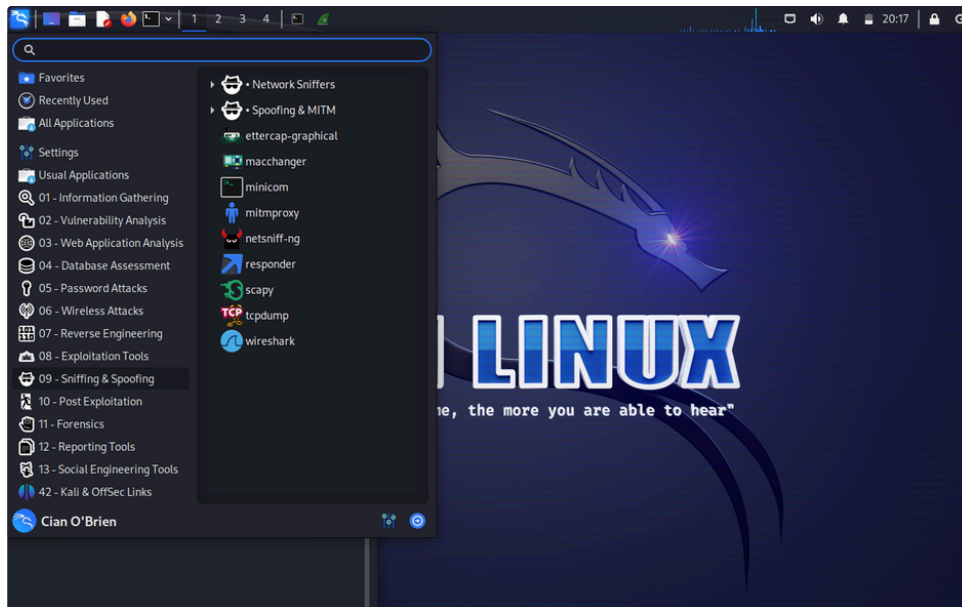
 Make sure to follow the rest of this module from the Raspberry Pi **NOT** set up to run the Apache server. We want to interact with the server so you should use the "regular" Raspberry Pi to access it.

2. Configure the Network of your Raspberry Pis

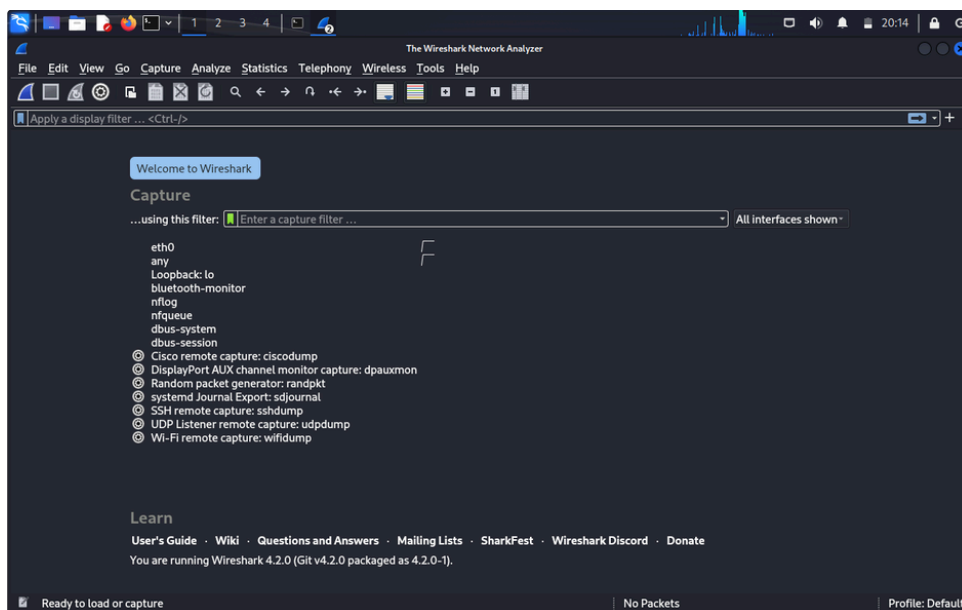
- a. Use the same command that we used in the last module to set static IPv4 addresses on both your Raspberry Pis so that they can communicate correctly.
 - i.

```
1 sudo ifconfig eth0 xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx
```
 - b. We recommend setting the IP addresses as follows:
 - i. Regular Raspberry Pi - 192.168.56.2
 - ii. Apache Raspberry Pi - 192.168.56.3
-

3. Click on the Kali Linux Icon in the Top Left, Go Down to "Sniffing and Spoofing"

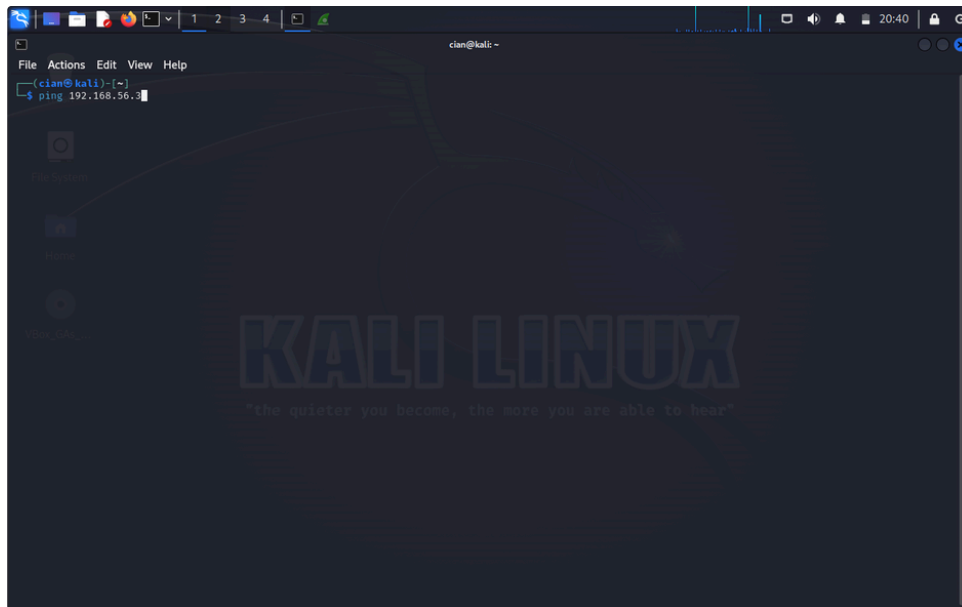


3. Open Wireshark



- a. Once you have opened Wireshark, you will see a search bar that allows you to filter all the networking packets on the network.
 - i. You can filter by **IP address**, **Protocol Type**, as well as **Port**
- b. Because you are interacting with Wireshark on a closed LAN (Local Area Network), there will not be much to see at the start, but we'll get there.

4. Ping the Apache Raspberry Pi from the Terminal of the "Regular" Raspberry Pi



1 ping 192.168.56.3

- a. Ensure the Wireshark window is open and that you are capturing packets (*blue fin symbol on the top left*) before pinging the other Raspberry Pi. It may look different from student to student, but after pinging, you should see the ICMP protocols roll in as the RP's constantly ping one another until you "Ctrl + C" to halt the pings.
- b. Look through everything. Do you notice anything that surprises you?

Apache Server Walkthrough

1. Start up the Apache Web Server on the Raspberry Pi Labeled "Apache"

- a. The Raspberry Pi should already be configured to host the HTTP server, and all you need to do is run the following command from the terminal:

i. 1 sudo systemctl start apache2

- ii. However, if you are running into any issues or your Raspberry Pi has yet to be configured, then we have provided additional documentation below to troubleshoot or help you set up.

iii.

- b. Test that your web server is running by checking it's status:

i. 1 sudo systemctl status apache2

- c. If everything is working correctly, then you should see a return that states the server is **active(running)** like so:

```
(cian@kali)-[~]
└─$ sudo systemctl start apache2


(cian@kali)-[~]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Tue 2024-03-19 12:38:08 PDT; 10s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 4639 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 4655 (apache2)
    Tasks: 6 (limit: 2260)
   Memory: 18.3M
      CPU: 132ms
   CGroup: /system.slice/apache2.service
           └─4655 /usr/sbin/apache2 -k start
             └─4658 /usr/sbin/apache2 -k start
               └─4659 /usr/sbin/apache2 -k start
                 └─4660 /usr/sbin/apache2 -k start
                   └─4661 /usr/sbin/apache2 -k start
                     └─4662 /usr/sbin/apache2 -k start

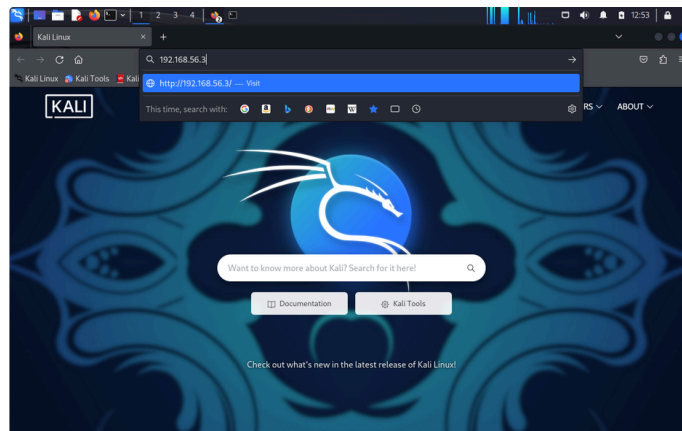
Mar 19 12:38:08 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Mar 19 12:38:08 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Now that we know the server is up and running, we can interact with it from our “regular” Raspberry Pi, and by running Wireshark at the same time, we will be able to see all of the packets that create a connection between the two Raspberry Pis you are using.

2. Open Firefox and Input the Apache Raspberry Pi IP Address

- a. By doing this on your regular Raspberry Pi, you will be making HTTP requests to the Apache Raspberry Pi as it loads up the web server.

 Make sure to have Wireshark open while doing this step, and ensure that you are capturing packets. Otherwise you won't see anything.



Congratulations, you have officially completed Module 2. After looking over the packets you caught from accessing the web server, is there anything that surprises you? Compare it to the packets you caught when just pinging, notice any differences? Was there anything you did expect to happen that didn't? Or vice versa?

As you are most likely in the networking class and learning about the connectional handshakes that computers make from one to another, we would highly recommend trying Wireshark on your own laptop connected to the internet. This will allow you to see all the different steps that occur as your laptop connects to the internet and surfs the web, introduce you to different protocols, and show you all the OSI layers they appear at.
