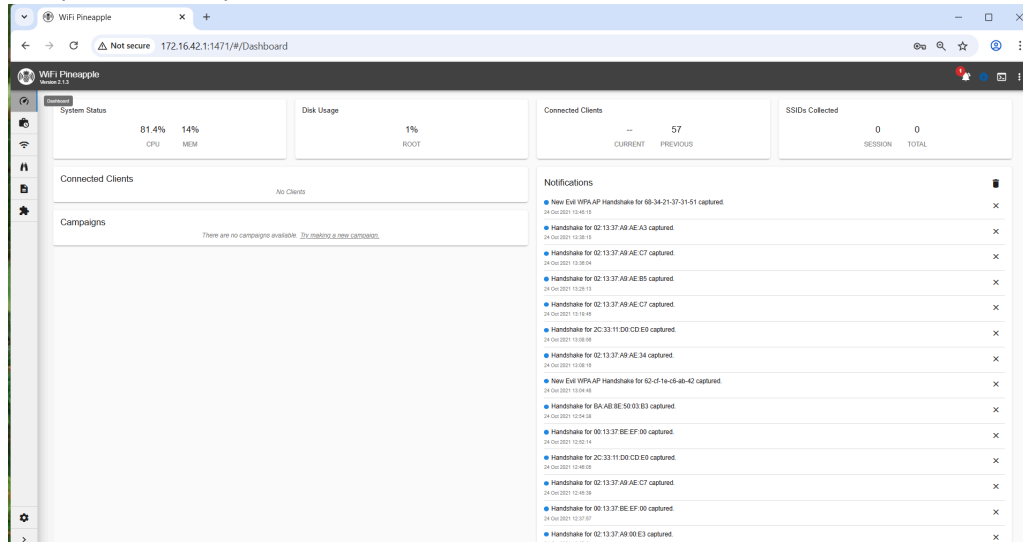


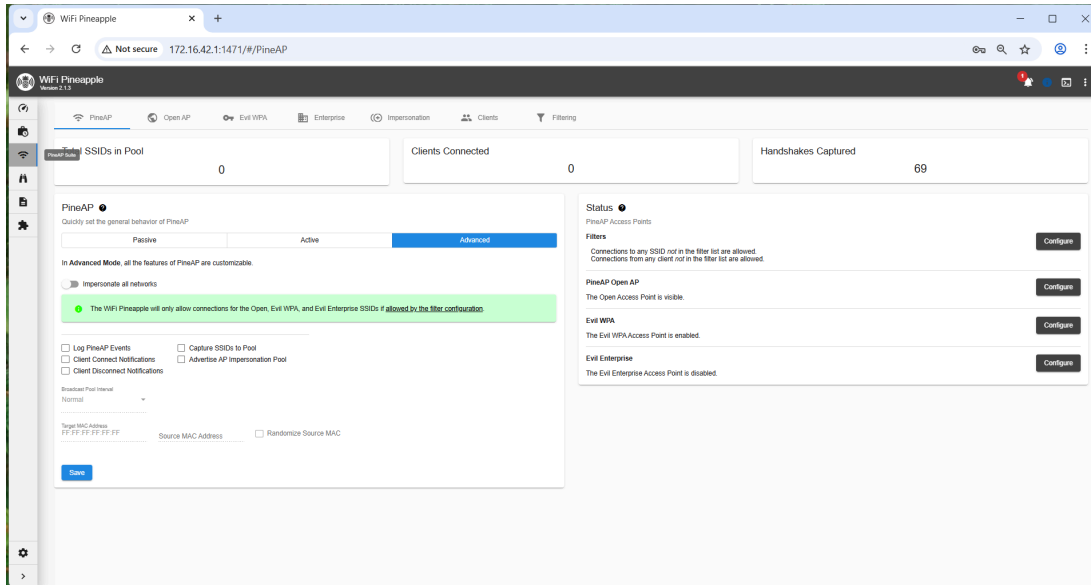
Lab 5 | CSE 3140 | Abdul Chowdhury (unable to communicate with partner asked TA said to work by myself) | amc20031 | ssh -L 127.0.0.1:8000:10.13.4.8:80 cse@10.13.6.41

Q1 (Dashboard):



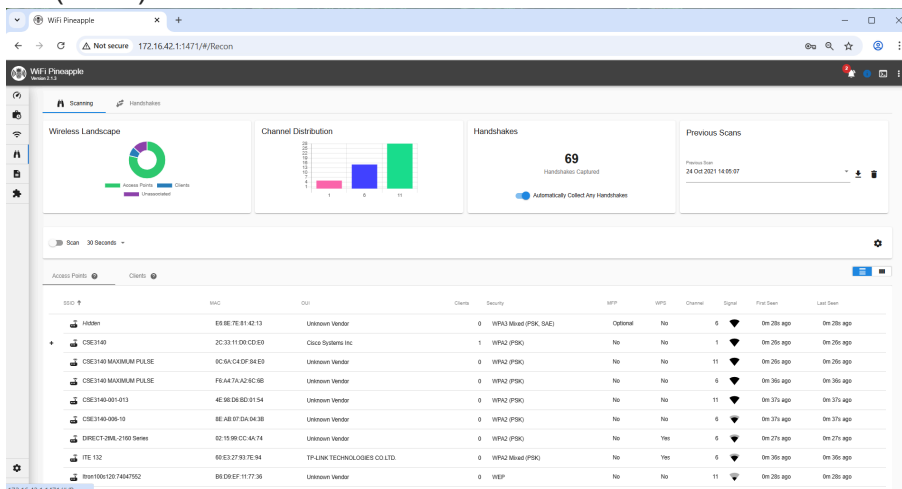
Above is the dashboard where we can view information about the system

- Top row shows **System Status**: which displays current CPU and RAM percentages
- **Disk Usage**: Displays current disk percentage
- **Connected Clients**: Displays every client (MAC address and IP address) that is currently and previously connected when the client is connected to the non-management server.
- **SSIDs collected**: Displays all SSIDs collected since the pineapple was booted
- **Campaigns**: Displays list of all current campaigns which includes status, types and names
- **Wireless landscape**: General overview of statistics on the recon scan that is done
- **Notification system**: Notifies user when there is a change or update in the system



Above is the Wifi Administration Console which is similar to the dashboard. The top 3 boxes are the number of SSIDS found from clients, number of handshakes captured, and number of clients connected. Handshakes can change and are captured when a client joins or refreshes the network. The PineAP section allows us various ways for how the system is able to scan, some ways are impersonating access points and controlling access with filters. My interface name was wlan2, and a WLAN is a network, for instance wifi is an example of WLAN.

Q2 (Scan).



Above is the recon dashboard of the pineapple.

- **Scanning in the Wireless Landscape:** Displays pie chart containing APs, clients, and unassociated clients
- **Channel Distributions:** Displays channel frequencies picked up by Pineapple's antennas

- Handshakes tab:

WiFi Pineapple

Not secure 172.16.42.1:1471/#/Recon/handshakes

WiFi Pineapple
Version 2.1.0

Scanning Handshakes

Captured WPA Handshakes

ESSID	Client	Source	Type	Detected	Message 1	Message 2	Message 3	Message 4	Decom Frame	
EB C8 26 97 D0 09	EVLTVNM22000	Ext WPA2 Twin	Evilvm Hashcat	4h 56m ago	?	?	?	?	?	
10 91 D1 06 D0 F8	EVLTVNM22000	Ext WPA2 Twin	Evilvm Hashcat	4h 27m ago	?	?	?	?	?	
9C FC EB CF 55 76	EVLTVNM22000	Ext WPA2 Twin	Evilvm Hashcat	4h 7m ago	?	?	?	?	?	
9C EF AF D7 28 18	EVLTVNM22000	Ext WPA2 Twin	Evilvm Hashcat	4h 18m ago	?	?	?	?	?	
9C FC EB CF 53 AE	EVLTVNM22000	Ext WPA2 Twin	Evilvm Hashcat	2h 34m ago	?	?	?	?	?	
9C FC EB CF 55 76	EVLTVNM PCAP	Ext WPA2 Twin	Evilvm PCAP	4h 7m ago	?	?	?	?	?	
AE A5 56 2E C1 A2	9C FC EB CF 55 39	Recon	Full Hashcat	5h 8m ago	✓	✓	✓	✓	✓	
DE DF 38 F4 68 76	84 FD D1 54 EA B5	Recon	Partial PCAP	5h 17h ago	✗	✓	✓	✓	✓	
00 13 37 BE EF 90	9C FC EB D3 1A 21	Recon	Full PCAP	1h 36m ago	✓	✓	✗	✗	✓	
84 FD D1 54 EA B5	EVLTVNM PCAP	Ext WPA2 Twin	Evilvm PCAP	5h 8m ago	?	?	?	?	?	
82 4B A9 71 73 01	CC 2F 71 25 FD 91	Recon	Partial PCAP	4h 2m ago	✓	✓	✗	✗	✓	
EB CA 60 9C 14 BF	EVLTVNM22000	Ext WPA2 Twin	Evilvm Hashcat	2h 14m ago	?	?	?	?	?	
02 13 37 A9 AE 7C	C8 BE 06 4A C8 AA	Recon	Partial Hashcat	5h 37m ago	✓	✓	✗	✓	✓	
02 13 37 A9 AE 7C	68 24 28 3E 1B C5	Recon	Partial PCAP	1h 37m ago	✓	✓	✓	✓	✓	
9C EF AF D6 9C 3F	EVLTVNM22000	Ext WPA2 Twin	Evilvm Hashcat	7h 8m ago	?	?	?	?	?	
38 F9 D3 E4 F8 24	EVLTVNM22000	Ext WPA2 Twin	Evilvm Hashcat	3h 7m ago	?	?	?	?	?	
172.16.42.1:1471/#/Recon/	EVLTVNM22000	Ext WPA2 Twin	Evilvm Hashcat	5h 8m ago	?	?	?	?	?	

The handshakes tab shows details for every handshake the system has gotten, particularly the SSID, client, source, type, and time it took for handshake to be captured. It also shows various different statistics that show the strength and validity of connection created.

Q3:

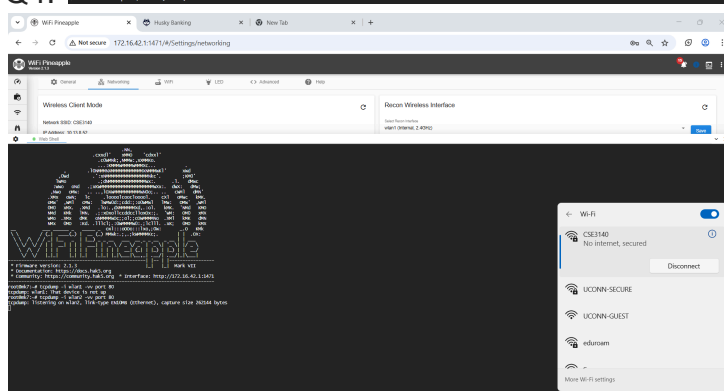
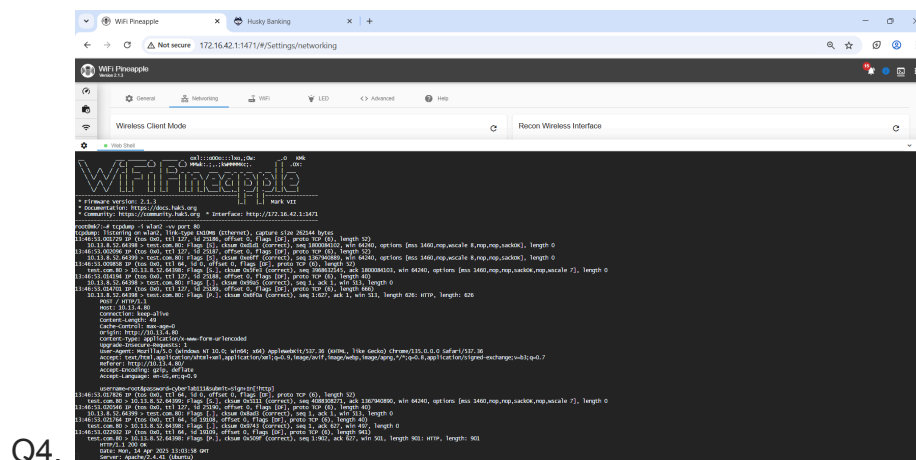
This was the access point created by the personal hotspot on my iphone

The SSID tab notifies user of the name of network, MAC tab shows the identifier assigned to Network interface controller, OUI shows vendor of network adapter (When that information is accessible), clients tab show the amount of clients that are connected to the network, Security shows type of security each network uses, and MFP is extra security system displays if the network has it

- I was able to find an access point through my hotspot, and I could see clients on the specific access point, especially when the left side of the access point was accessed. Information about client connection to the access point was also displayed and the network is using WPA2(PSK) security.

Below we can also see the handshakes that were captured in our vulnerable network

Access Points		Clients				
MAC	OUI	First Seen	Last Seen	BSSID	SSID	Channel
0C:EF:AF:D7:28:EE	IEEE Registration Authority	1m 59s ago	0m 2s ago	2C:33:11:D0:CD:E9	None	None
22:F8:5A:9F:7A:DA	Unknown Vendor	0m 2s ago	0m 2s ago	C8:28:E5:BA:0E:E3	None	None
9C:FC:E8:CF:63:AE	Intel Corporate	1m 45s ago	0m 3s ago	00:13:37:A9:AE:52	None	None
9C:FC:E8:D3:19:A9	Intel Corporate	0m 3s ago	0m 3s ago	None	None	None
EA:38:A9:10:91:9B	Unknown Vendor	0m 3s ago	0m 3s ago	90:E9:5E:FA:85:53	None	None
C4:35:D9:96:49:86	Unknown Vendor	0m 4s ago	0m 4s ago	None	None	None
E2:D8:24:D8:EF:9E	Unknown Vendor	0m 4s ago	0m 4s ago	84:5A:3E:FF:8B:43	None	None
E8:67:75:F9:5D	Unknown Vendor	0m 4s ago	0m 4s ago	None	None	None
EA:AB:60:EA:D4:8B	Unknown Vendor	0m 4s ago	0m 4s ago	A0:93:51:A3:30:63	None	None
0C:EF:AF:D6:9C:3F	IEEE Registration Authority	2m 2s ago	0m 5s ago	2C:33:11:D0:CD:E9	None	None



When connected to an unsecured network, traffic is able to be seen because it is unencrypted. Traffic that appeared came from a lab laptop, and when connected to a protected network however no traffic was able to be seen because of security and encryption. Information is more accessible on unsecured networks vs. secured networks.

Q5.

The image displays a Kali Linux terminal window and a web browser window. The terminal window shows the output of the `tcpdump` command, capturing network traffic on the `wlan2` interface. The output shows several packets, including a GET request to `http://172.16.42.1:1471` and a response from the server. The browser window shows the `WiFi Pineapple` interface, which displays a list of detected wireless networks. The list includes networks such as `UConnBusWifi1705`, `open-004-03`, `secure-004-03`, `eduroam`, `UCONN-GUEST`, and `eduroam`. The interface also shows details for each network, including the SSID, MAC address, OUI, Clients, Security, MFP, WPS, Channel, Signal, First Seen, and Last Seen.

```
* Firmware Version: 2.1.3
* Documentation: https://docs.hak5.org
* Community: https://community.hak5.org * Interface: http://172.16.42.1:1471

root@kali:~# tcpdump -i wlan2 -vv port 80
tcpdump: listening on wlan2, link-type EN10MB (Ethernet), capture size 262144 bytes
07:05:05.216791 IP (tos 0x0, ttl 127, id 45232, offset 0, flags [DF], proto TCP (6), length 52)
    10.13.8.90.57427 > 10.13.4.80.80: Flags [S], cksum 0x5303 (correct), seq 3318962657, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
07:05:05.216953 IP (tos 0x0, ttl 127, id 45233, offset 0, flags [DF], proto TCP (6), length 52)
    10.13.8.90.57428 > 10.13.4.80.80: Flags [S], cksum 0x77d5 (correct), seq 2129689585, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
07:05:05.220217 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    10.13.4.80.80 > 10.13.8.90.57427: Flags [S], cksum 0x3741 (correct), seq 3258285646, ack 2129689586, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
07:05:05.220474 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    10.13.4.80.80 > 10.13.8.90.57427: Flags [S], cksum 0x3741 (correct), seq 3258285646, ack 2129689586, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
07:05:05.222458 IP (tos 0x0, ttl 127, id 45234, offset 0, flags [DF], proto TCP (6), length 40)
    10.13.8.90.57428 > 10.13.4.80.80: Flags [F], cksum 0x7103 (correct), seq 1, ack 1, win 513, length 0
07:05:05.222670 IP (tos 0x0, ttl 127, id 45235, offset 0, flags [DF], proto TCP (6), length 40)
    10.13.8.90.57427 > 10.13.4.80.80: Flags [F], cksum 0x53b9 (correct), seq 1, ack 1, win 513, length 0
07:05:05.222974 IP (tos 0x0, ttl 127, id 45236, offset 0, flags [DF], proto TCP (6), length 405)
    10.13.8.90.57428 > 10.13.4.80.80: Flags [P-], cksum 0x6cb9 (correct), seq 1:426, ack 1, win 513, length 425: HTTP, length: 425
    GET / HTTP/1.1
    Host: 10.13.4.80
    Connection: keep-alive
    Upgrade-Insecure-Requests: 1
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
    Accept-Encoding: gzip, deflate
    Accept-Language: en-US,en;q=0.9
07:05:05.225239 IP (tos 0x0, ttl 64, id 54082, offset 0, flags [DF], proto TCP (6), length 40)
    10.13.4.80.80 > 10.13.8.90.57428: Flags [F], cksum 0x6f68 (correct), seq 1, ack 426, win 499, length 0
07:05:05.228630 IP (tos 0x0, ttl 64, id 54083, offset 0, flags [DF], proto TCP (6), length 905)
    10.13.4.80.80 > 10.13.8.90.57428: Flags [P-], cksum 0xb2bd1 (correct), seq 1:866, ack 426, win 501, length 865: HTTP, length: 865
    HTTP/1.1 200 OK
```

SSID	MAC	OUI	Clients	Security	MFP	WPS	Channel	Signal	First Seen	Last Seen
UConnBusWifi1705	28 C2 DD 72 E2 AB	AzureWave Technology Inc.	0	WPA2 (PSK)	No	No	1	1m 11s ago	1m 11s ago	
open-004-03	00 13 37 A9 01 19	Orient Power Home Network Ltd	0	Open	No	No	11	14m 51s ago	2m 48s ago	
secure-004-03	02 13 37 A9 01 19	Unknown Vendor	0	WPA2 (PSK)	No	No	11	14m 51s ago	2m 48s ago	
eduroam	38 90 A5 D9 08 41	Cisco Systems Inc	0	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	11	19m 10s ago	3m 3s ago	
UCONN-GUEST	14 84 73 35 FC 52	Unknown Vendor	0	Open	No	No	11	19m 50s ago	3m 27s ago	
eduroam	08 96 AD C2 46 21	Cisco Systems Inc	0	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	1	17m 20s ago	4m 28s ago	

When TCPDUMP was ran off the secure networks no traffic was shown in the terminal due to the secure network preventing Pineapple from seeing data about IP addresses connected, connecting to protected networks is useful in order to protect privacy such as activity and information.

Q6.

The screenshot shows the WiFi Pineapple web interface. The 'Access Points' tab is active, displaying a table of detected wireless networks. The table includes columns for MAC, OUI, First Seen, Last Seen, BSSID, SSID, and Channel. The 'Clients' tab is also visible, showing a table of detected clients with columns for SSID, MAC, OUI, Clients, Security, MFP, WPS, Channel, Signal, First Seen, and Last Seen.

MAC	OUI	First Seen	Last Seen	BSSID	SSID	Channel
9C:FC:E8:D3:1A:30	Intel Corporate	4h 55m ago	4h 55m ago	00:13:37:A9:AE:B5	None	None
DA:0F:D0:8B:37:10	Unknown Vendor	2m 39s ago	2m 39s ago	00:25:00:FF:94:73	None	None
EE:14:55:09:86:3D	Unknown Vendor	2m 38s ago	2m 38s ago	00:25:00:FF:94:73	None	None
E8:C8:29:58:85:90	Unknown Vendor	8h 17m ago	8h 17m ago	00:6B:F1:35:C7:83	None	None
9C:FC:E8:D3:1D:D2	Intel Corporate	5h 2m ago	5h 2m ago	02:13:37:A7:FF:72	None	None
84:FD:D1:59:F8:62	Intel Corporate	8h 35m ago	8h 35m ago	02:13:37:A9:00:9B	None	None
68:34:21:38:19:22	Unknown Vendor	3h 45m ago	3h 45m ago	02:13:37:A9:00:E3	None	None
9C:FC:E8:D3:19:72	Intel Corporate	1m 13s ago	1m 13s ago	02:13:37:A9:01:1F	None	None
84:FD:D1:55:12:02	Intel Corporate	3h 19m ago	3h 19m ago	02:13:37:A9:AE:88	None	None
EA:91:DA:D7:F1:C1	Unknown Vendor	2m 17s ago	2m 17s ago	14:84:73:31:CE:63	None	None

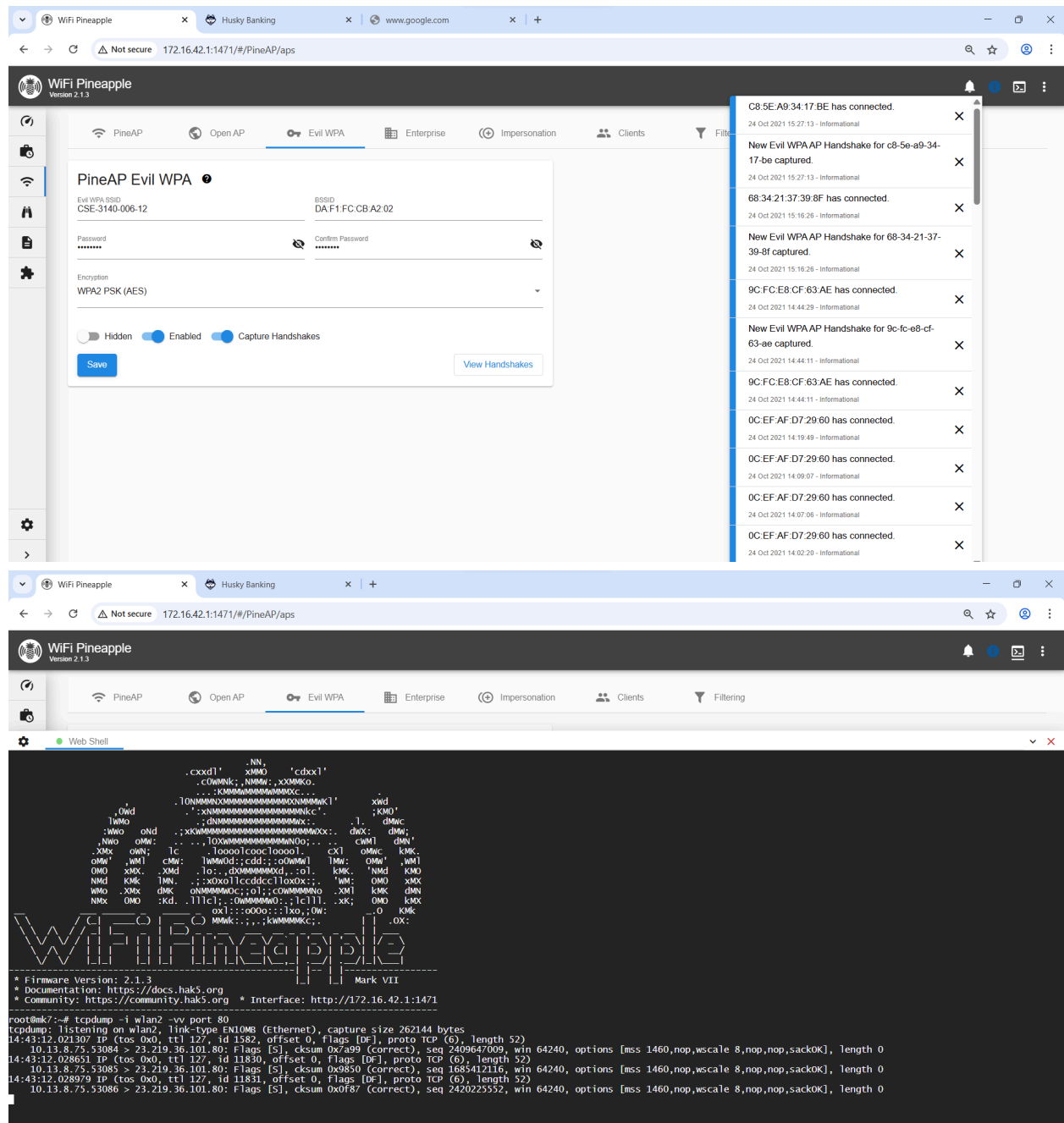
SSID	MAC	OUI	Clients	Security	MFP	WPS	Channel	Signal	First Seen	Last Seen
Survey	00:6B:F1:35:C7:80	Cisco Systems Inc	0	WPA3 (SAE)	Required	No	11	0m 29s ago	0m 29s ago	
Survey	14:84:73:35:FC:50	Unknown Vendor	0	WPA3 (SAE)	Required	No	11	0m 29s ago	0m 29s ago	
UCONN-GUEST	00:6B:F1:35:C7:82	Cisco Systems Inc	0	Open	No	No	11	0m 29s ago	0m 29s ago	
UCONN-GUEST	A0:93:51:A3:2B:52	Cisco Systems Inc	0	Open	No	No	6	0m 29s ago	0m 29s ago	
UCONN-SECURE	F8:0B:CB:B2:02:E3	Cisco Systems Inc	0	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	6	0m 36s ago	0m 36s ago	
secure-006-07	02:13:37:A9:AE:C7	Unknown Vendor	0	WPA2 (PSK)	No	No	11	0m 36s ago	0m 36s ago	
Survey	08:96:AD:C2:46:20	Cisco Systems Inc	0	WPA3 (SAE)	Required	No	1	0m 37s ago	0m 37s ago	
UCONN-SECURE	90:E9:5E:FA:85:53	Unknown Vendor	1	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	1	0m 37s ago	0m 37s ago	
UCONN-SECURE	A0:93:51:A3:2C:A3	Cisco Systems Inc	0	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	1	0m 37s ago	0m 37s ago	
UCONN-SECURE	C8:28:E5:B5:7B:43	Unknown Vendor	0	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	1	0m 37s ago	0m 37s ago	
eduroam	08:96:AD:C2:46:21	Cisco Systems Inc	0	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	1	0m 37s ago	0m 37s ago	
eduroam	58:8B:1C:6C:7D:81	Unknown Vendor	0	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	1	0m 37s ago	0m 37s ago	
open-006-07	00:13:37:A9:AE:C7	Orient Power Home Network Ltd.	0	Open	No	No	11	0m 37s ago	0m 37s ago	
CSE3140-006-0	9E:42:A5:D8:05:4E	Unknown Vendor	0	WPA2 (PSK)	No	No	6	0m 45s ago	0m 45s ago	

The wireless networks visible are UCONN-GUEST, UCONN-SECURE, eduroam, Survey and other networks created by other students in classroom.

UCONN SECURE and UCONN GUEST came up at various different times but each time UCONN SECURE was listed it had different values in MAC, while other columns were the same amongst secure and guest.

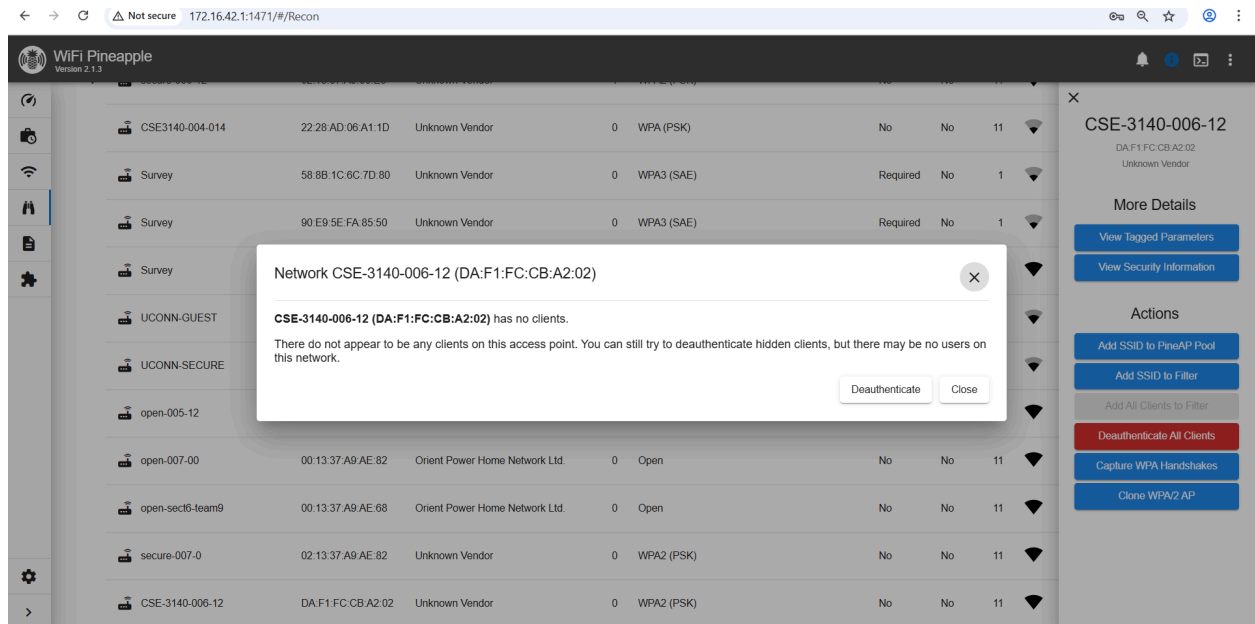
Open, WEP, WPA2(PSK) (CSE 3140 NETWORK) and WPA2(802 1x Enterprise, 802 1x Enterprise FT) were used for UCONN-secure networks were the different values listed.

Q7.



I Did this on the lab computer unable to screen record but recorded through screenshots I was able to connect and then I went to the terminal typed in the root number and was able to connect to the IP Address.

Q8. For Q8 I record through my phone and screenshots as this was done through lab computer



WiFi Pineapple interface showing a list of detected networks and a detailed view of the 'secure-006-12' network.

Network Name	BSSID	Vendor	Mode	Auth	Sec	Ch	Signal
UCONN-GUEST	F8:0B:CB:B2:02:E2	Cisco Systems Inc	0	Open	No	No	6
CSE-3140-006-12	DA:F1:FC:CB:A2:02	Unknown Vendor	0	WPA2 (PSK)	No	No	11
Survey	C8:28:E5:B5:7B:40	Unknown Vendor	0	WPA3 (SAE)	Required	No	1
UCONN-SECURE	4C:77:6D:EB:FC:83	Cisco Systems Inc	0	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	11
eduroam	4C:77:6D:EB:FC:81	Cisco Systems Inc	0	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	11
passio_FC87	00:1A:DD:78:F8:84	PeWave Ltd	0	WPA2 (PSK)	No	No	2
UCONN-GUEST	00:6B:F1:35:C7:82	Cisco Systems Inc	0	Open	No	No	11
DIRECT-HP M203 LaserJet	AA:6B:AD:A0:AC:F9	Unknown Vendor	0	WPA2 (PSK)	No	Yes	6
UCONN-GUEST	38:90:A5:D9:08:42	Cisco Systems Inc	1	Open	No	No	11
UCONN-SECURE	90:E9:5E:FA:85:53	Unknown Vendor	1	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	1
eduroam	58:8B:1C:6C:7D:81	Unknown Vendor	0	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	1
open-1.3	00:13:37:A9:AE:34	Orient Power Home Network Ltd.	0	Open	No	No	2
LABTEST-ATH-PATRONS-LAB	A0:B4:39:86:88:C2	Cisco Systems Inc	0	WPA3 (SAE)	Required	No	1
UCONN-GUEST	90:E9:5E:FA:85:52	Unknown Vendor	0	Open	No	No	1
UCONN-SECURE	A0:93:51:A3:2C:A3	Cisco Systems Inc	5	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	1

secure-006-12
02:13:37:A9:00:E3
Unknown Vendor

More Details

View Tagged Parameters

View Security Information

Actions

Add SSID to PineAP Pool

Add SSID to Filter

Add All Clients to Filter

Deauthenticate All Clients

Capture WPA Handshakes

Clone WPA2 AP

Captured WPA Handshakes												
BSSID	Client	Source	Type	Captured	Message 1	Message 2	Message 3	Message 4	Beacon Frame			
02:13:37:A9:AE:67	9C:FC:E8:CF:46:E4	Recon	Full PCAP	4h 24m ago	✓	✓	✓	✓	✓			
02:13:37:A9:AE:C7	9C:FC:E8:CF:55:30	Recon	Full PCAP	4h 28m ago	✓	✓	✓	✓	✓			
5E:B1:16:6F:67:F0	EVILTWIN 22000	Evil WPA/2 Twin	Eviltwin Hashcat	5h 48m ago	?	?	?	?	?			
9C:FC:E8:CF:63:AE	EVILTWIN 22000	Evil WPA/2 Twin	Eviltwin Hashcat	1h 16m ago	?	?	?	?	?			
CA:25:65:2B:BD:BB	EVILTWIN 22000	Evil WPA/2 Twin	Eviltwin Hashcat	7h 31m ago	?	?	?	?	?			
00:13:37:BE:EF:00	9C:FC:E8:CF:55:76	Recon	Partial Hashcat	4h 30m ago	✓	✓	✓	✓	✓			
02:13:37:A9:00:E3	9C:FC:E8:CF:55:30	Recon	Full Hashcat	9h 27m ago	✓	✓	✓	✓	✓			
02:13:37:A9:01:31	84:FD:D1:54:E4:85	Recon	Full Hashcat	10h 42m ago	✓	✓	✓	✓	✓			
02:13:37:A9:AE:82	84:FD:D1:59:FA:2E	Recon	Partial PCAP	6h 2m ago	✓	✓	✗	✓	✓			
24:EE:9A:D9:D0:3C	EVILTWIN 22000	Evil WPA/2 Twin	Eviltwin Hashcat	7h 51m ago	?	?	?	?	?			
4A:CA:8D:7D:E5:52	EVILTWIN PCAP	Evil WPA/2 Twin	Eviltwin PCAP	7h 42m ago	?	?	?	?	?			

I was able to observe that one the d'authentification happened traffic was able to be seen through the secure network even through encryption.

Q9. Pineapple's DNS records were configured for rerouting towards bank.com to the VM static ip address and was done by editing /etc/host files with entries. But despite DNS being successful, the Pineapple device failed to forward these connections to test machines leaving me unable to finish this part entirely.