THE UNIVERSITY OF ARIZONA
UA South

CYBV 479 Wireless Networking & Security

WiFi Recon Exercise

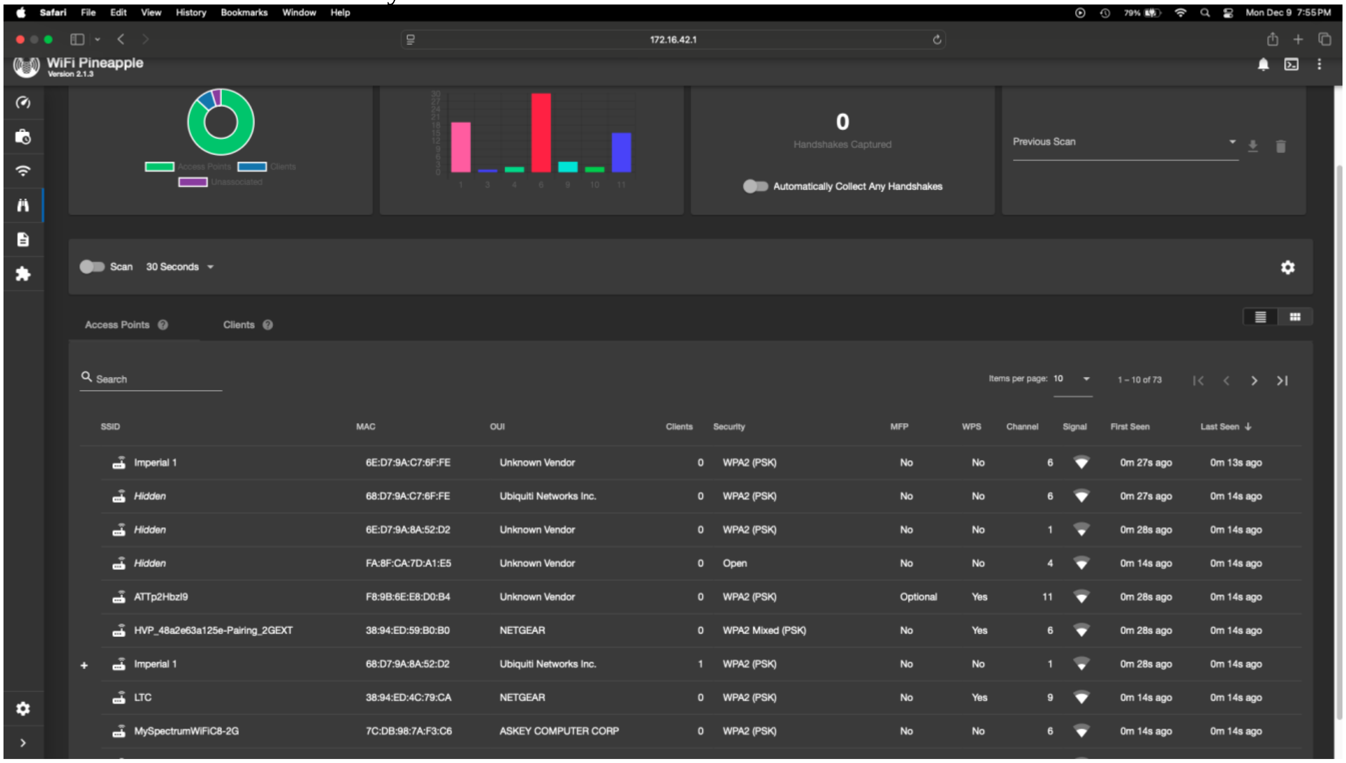
*****NOTE: THIS EXERCISE IS TO BE PERFORMED AS A PASSIVE SCANNING EXERCISE ONLY. ACTIVELY INTERACTING WITH ANY ACCESS POINTS OR CLIENTS COULD BE A VIOLATION OF LAW AND/OR UNIVERSITY OF ARIZONA'S POLICY WHICH WILL RESULT IN IMMEDIATE DISCIPLINARY ACTION.**

Exercise: Conduct a passive reconnaissance to identify Access Points (APs), their clients, and unassociated clients. Analyze these findings to determine WiFi network communications' security and data leakage implications. Before completing this assignment, make sure you watch the video provided. Failure could result in a 0 for this assignment.

Procedure:

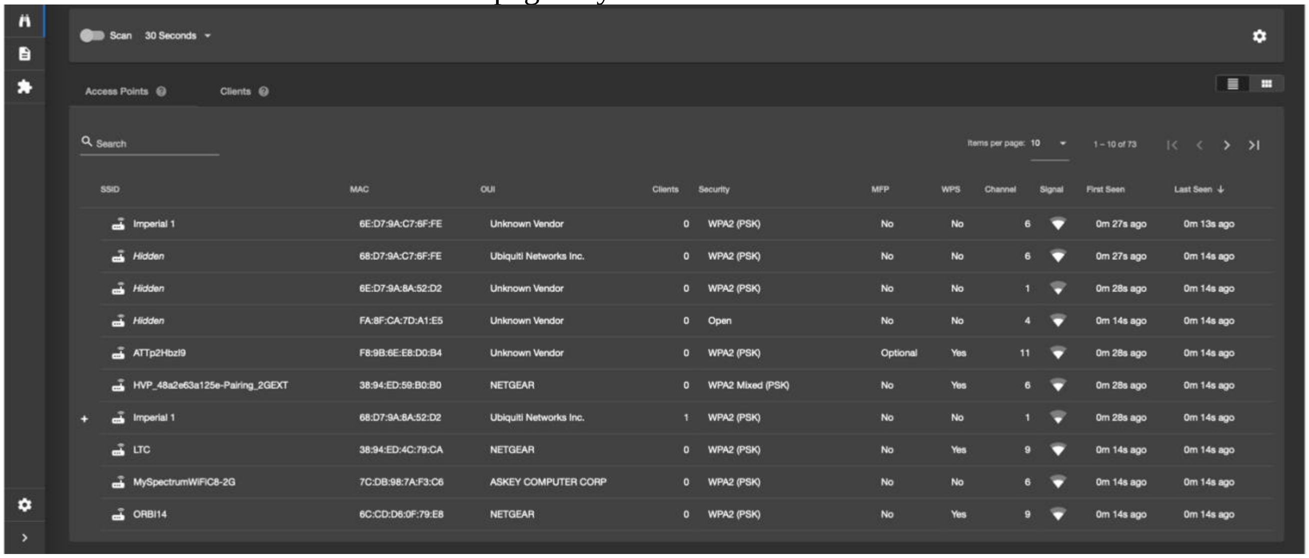
1. Take your WiFi Pineapple to a populated area where you will likely encounter WiFi access points. You will want to conduct your scan for approximately 10-15 minutes.

2. Take a screenshot of your recon information.



SSID	MAC	OUI	Clients	Security	MFP	WPS	Channel	Signal	First Seen	Last Seen ↓
Imperial 1	6E:D7:9A:C7:6F:FE	Unknown Vendor	0	WPA2 (PSK)	No	No	6	▼	0m 27s ago	0m 13s ago
Hidden	68:D7:9A:C7:6F:FE	Ubiquiti Networks Inc.	0	WPA2 (PSK)	No	No	6	▼	0m 27s ago	0m 14s ago
Hidden	6E:D7:9A:8A:52:D2	Unknown Vendor	0	WPA2 (PSK)	No	No	1	▼	0m 28s ago	0m 14s ago
Hidden	FA:8F:CA:7D:A1:E5	Unknown Vendor	0	Open	No	No	4	▼	0m 14s ago	0m 14s ago
ATTp2Hbzl9	F8:9B:6E:E8:D0:B4	Unknown Vendor	0	WPA2 (PSK)	Optional	Yes	11	▼	0m 28s ago	0m 14s ago
HVP_48a2e63a125e-Pairing_2GEXT	38:94:ED:59:B0:B0	NETGEAR	0	WPA2 Mixed (PSK)	No	Yes	6	▼	0m 28s ago	0m 14s ago
+ Imperial 1	68:D7:9A:8A:52:D2	Ubiquiti Networks Inc.	1	WPA2 (PSK)	No	No	1	▼	0m 28s ago	0m 14s ago
LTC	38:94:ED:4C:79:CA	NETGEAR	0	WPA2 (PSK)	No	Yes	9	▼	0m 14s ago	0m 14s ago
MySpectrumWiFiC8-2G	7C:DB:98:7A:F3:C6	ASKEY COMPUTER CORP	0	WPA2 (PSK)	No	No	6	▼	0m 14s ago	0m 14s ago

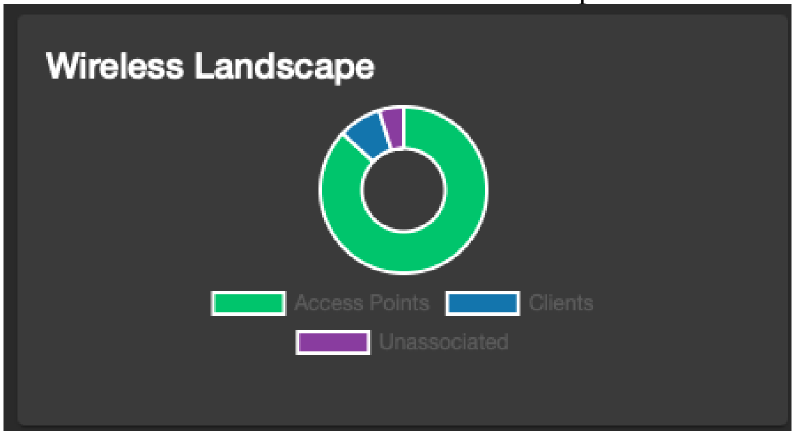
3. Take a screenshot of the first page of your search results.



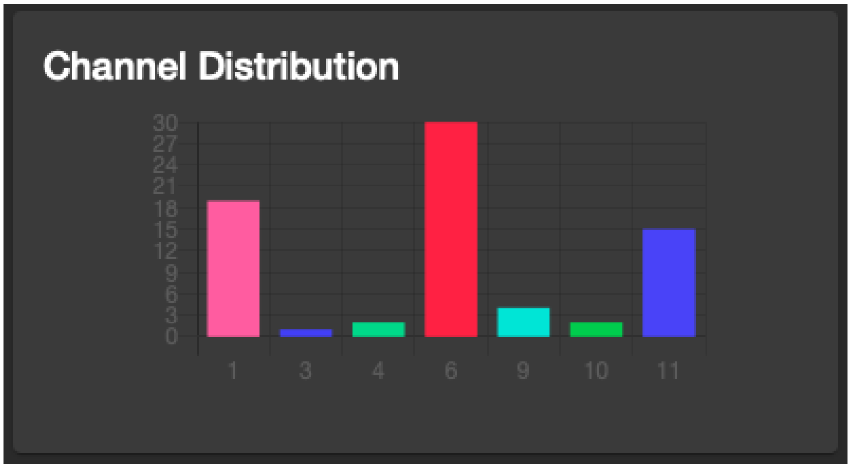
Items per page: 10 1 – 10 of 73

	SSID	MAC	OUI	Clients	Security	MFP	WPS	Channel	Signal	First Seen	Last Seen ↓
	Imperial 1	6E:D7:9A:C7:6F:FE	Unknown Vendor	0	WPA2 (PSK)	No	No	6	📶	0m 27s ago	0m 13s ago
	Hidden	68:D7:9A:C7:6F:FE	Ubiquiti Networks Inc.	0	WPA2 (PSK)	No	No	6	📶	0m 27s ago	0m 14s ago
	Hidden	6E:D7:9A:8A:52:D2	Unknown Vendor	0	WPA2 (PSK)	No	No	1	📶	0m 28s ago	0m 14s ago
	Hidden	FA:8F:CA:7D:A1:E5	Unknown Vendor	0	Open	No	No	4	📶	0m 14s ago	0m 14s ago
	ATTp2Hbzl9	F8:9B:6E:E8:D0:B4	Unknown Vendor	0	WPA2 (PSK)	Optional	Yes	11	📶	0m 28s ago	0m 14s ago
	HVP_48a2e63a125e-Pairing_2GEXT	38:94:ED:59:B0:B0	NETGEAR	0	WPA2 Mixed (PSK)	No	Yes	6	📶	0m 28s ago	0m 14s ago
+	Imperial 1	68:D7:9A:8A:52:D2	Ubiquiti Networks Inc.	1	WPA2 (PSK)	No	No	1	📶	0m 28s ago	0m 14s ago
	LTC	38:94:ED:4C:79:CA	NETGEAR	0	WPA2 (PSK)	No	Yes	9	📶	0m 14s ago	0m 14s ago
	MySpectrumWiFiC8-2G	7C:DB:98:7A:F3:C6	ASKEY COMPUTER CORP	0	WPA2 (PSK)	No	No	6	📶	0m 14s ago	0m 14s ago
	ORBI14	6C:CD:D6:0F:79:E8	NETGEAR	0	WPA2 (PSK)	No	Yes	9	📶	0m 14s ago	0m 14s ago

4. Take a screenshot of the wireless landscape.



5. Take a screenshot of the channel distribution.



6. Describe how this data would help an attacker set up a Rogue Access Point.

As we are already aware, the Hak5 Wifi Pineapple Mark VII is a penetration testing tool designed to provide detailed insight into the wireless environment. Using the Recon data we have gathered, displayed above, we can quietly piece together a comprehensive map of the surrounding wireless environment, pinpointing not just network names and their encryption methods, but also the channels they occupy, their relative signal strengths, and even the behavior of client devices searching for familiar connections. Armed with these insights, it becomes easier to select a less congested frequency, adopt a trusted SSID that users have previously connected to, and place a rogue access point in a prime location, ensuring that its signal appears stronger and more stable than any legitimate option. In turn, nearby devices often connect automatically (lured by what they perceive as a known, reliable network) allowing their unwitting traffic to pass under the attacker's watchful eye.

7. Describe how an attacker could use this data to target unassociated clients with the WiFi Pineapple's Allow Associations, Capture SSIDs to Pool, and Broadcast SSID Pool capability?

Using the WiFi Pineapple's Recon data, an attacker can identify nearby clients that are actively probing for previously known networks—these are often networks the clients have connected to in the past. By enabling the "Capture SSIDs to Pool" feature, the Pineapple will record those network names as soon as it detects a client's probe request. Once these SSIDs are captured, the attacker can then enable "Broadcast SSID Pool," causing the Pineapple to impersonate all those trusted network names simultaneously. Finally, with "Allow Associations" turned on, any unassociated client that automatically connects to previously trusted SSIDs will link up with the attacker's rogue access point instead. This effectively lures devices into joining what they perceive as familiar networks, granting the attacker visibility into their data traffic and the ability to carry out man-in-the-middle attacks.