THE UNIVERSITY OF ARIZONA
UA South

CYBV 479 Wireless Networking & Security

Secure WiFi Access Point Exercise

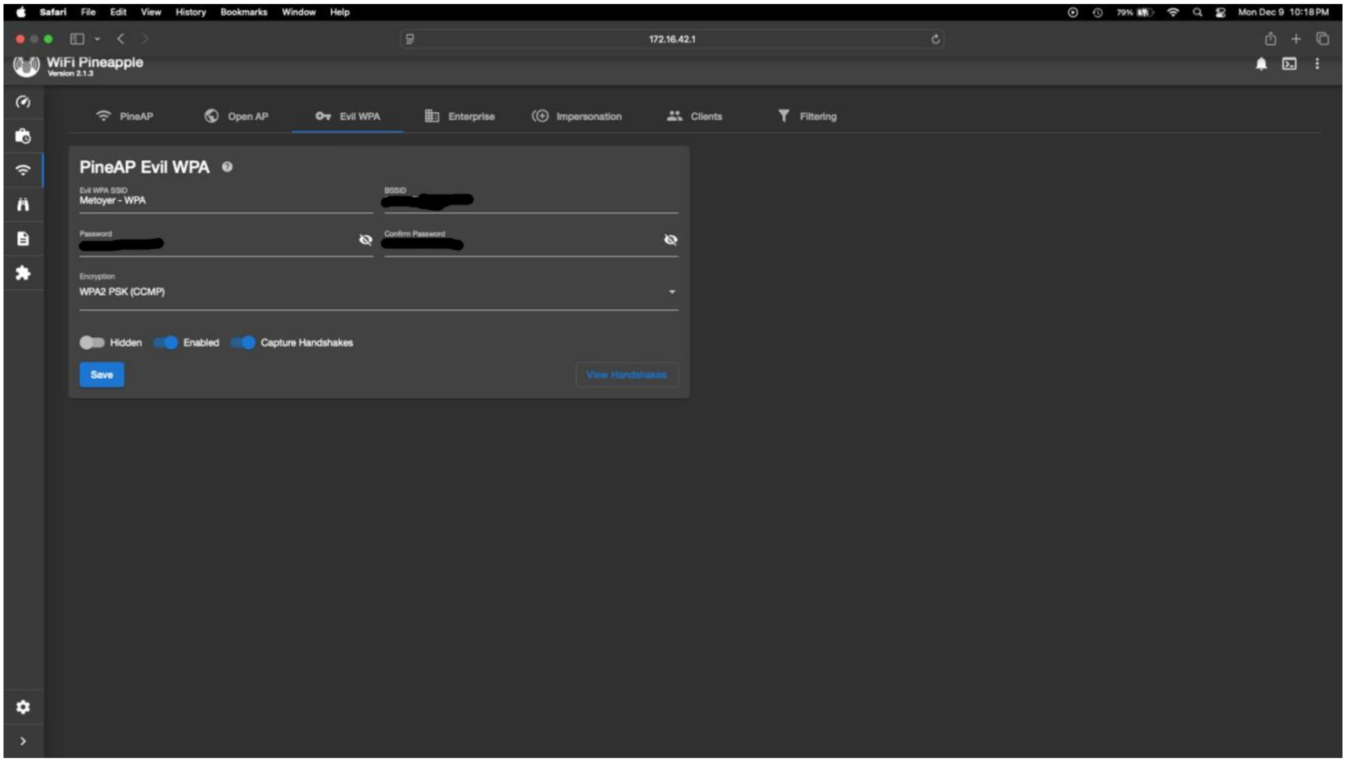
*****NOTE: THIS EXERCISE IS TO BE PERFORMED ON YOUR PERSONAL SYSTEMS ONLY! INTERACTING WITH 3RD PARTY'S SYSTEM COULD BE A VIOLATION OF LAW AND/OR UNIVERSITY OF ARIZONA'S POLICY WHICH WILL RESULT IN IMMEDIATE DISCIPLINARY ACTION.**

Exercise: Establish a secure WiFi Access Point that limits clients via both MAC address filtering and allowable associations to demonstrate a more secure AP implementation strategy.

Procedure:

1. Using your own computer system, connect to your WiFi Pineapple (*for this exercise, the WiFi Pineapple is representing the Secure Access Point).*

2. Configure your WiFi Pineapple to run as an Access Point with WPA2 security enabled. Provide a screenshot.



PineAP Evil WPA

Evil WPA SSID: Metoyer - WPA

BSSID: [redacted]

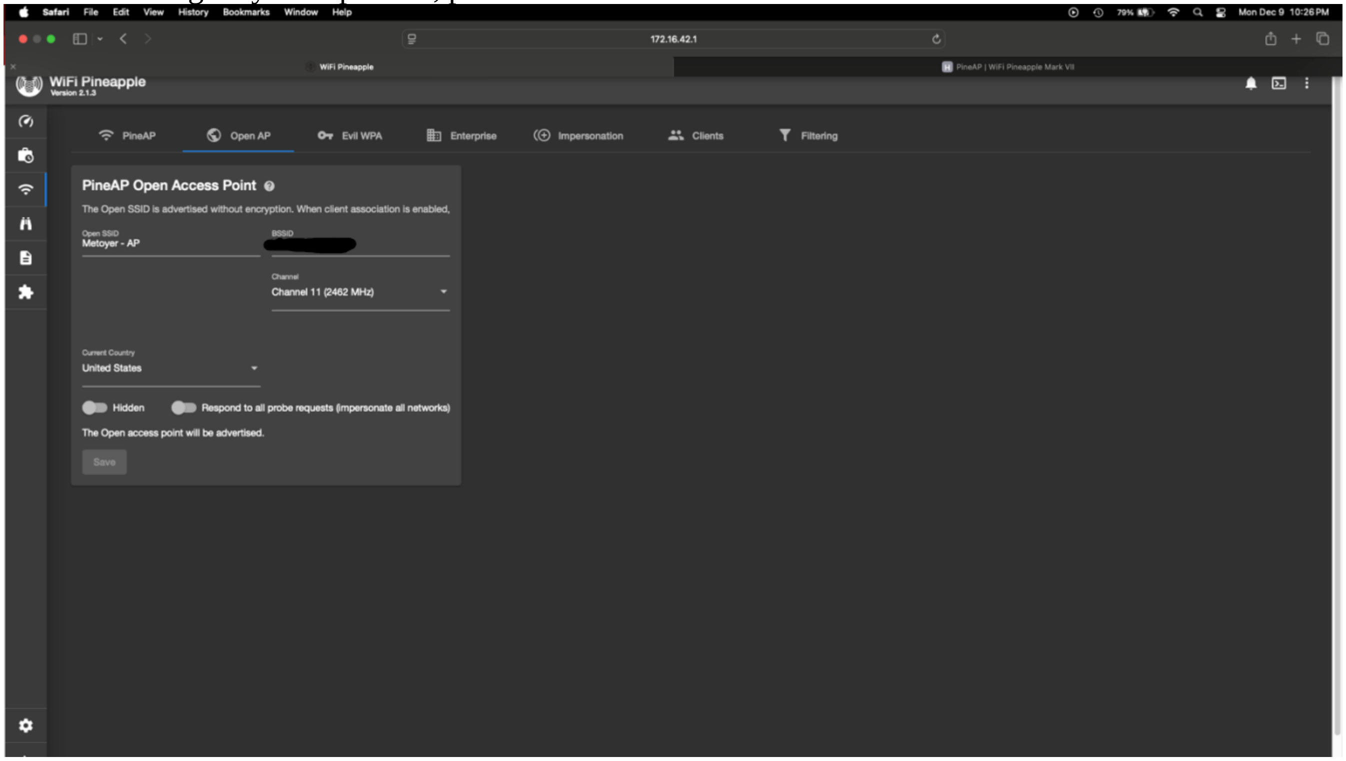
Password: [redacted]

Confirm Password: [redacted]

Encryption: WPA2 PSK (CCMP)

Hidden (off) Enabled (on) Capture Handshakes (on)

3. Configure your Open AP, provide a screenshot.



PineAP Open Access Point

The Open SSID is advertised without encryption. When client association is enabled,

Open SSID: Metoyer - AP

BSSID: [redacted]

Channel: Channel 11 (2462 MHz)

Current Country: United States

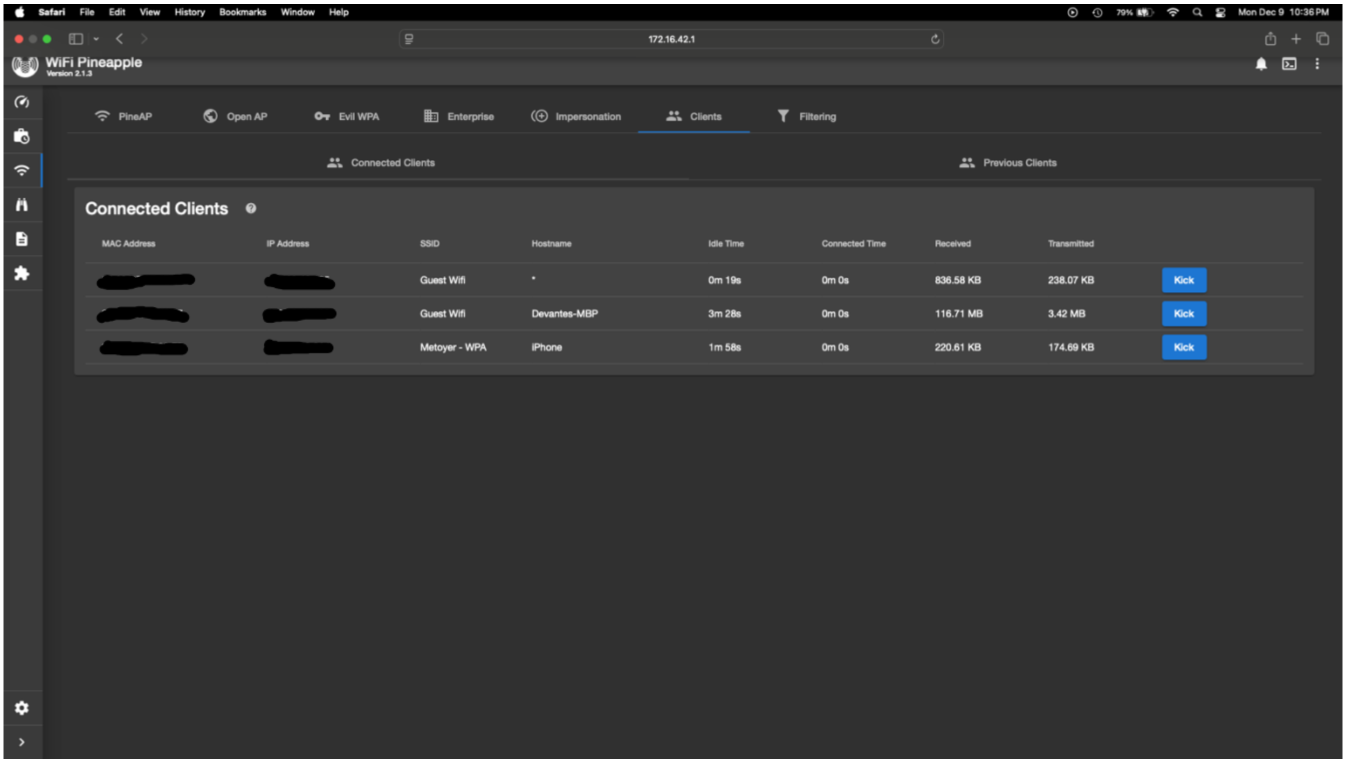
Hidden

Respond to all probe requests (impersonate all networks)

The Open access point will be advertised.

4. Using your personal phone or a second computer system, connect to the WiFi Pineapple as a client. Examine the WiFi Pineapple's client list and record the MAC address of your device then disconnect from the Pineapple's network.

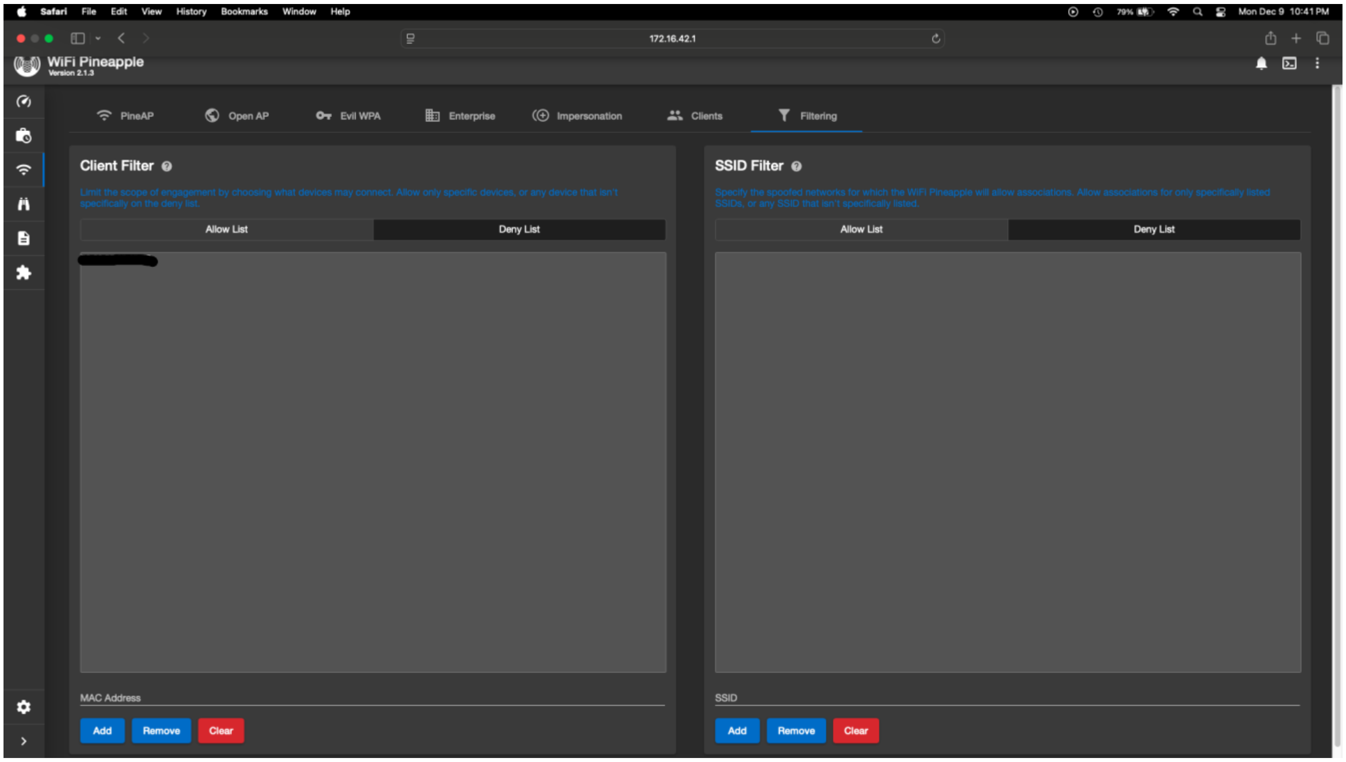
5. Take a screenshot of the clients.



Connected Clients

MAC Address	IP Address	SSID	Hostname	Idle Time	Connected Time	Received	Transmitted	
[redacted]	[redacted]	Guest Wifi	*	0m 19s	0m 0s	836.58 KB	238.07 KB	Kick
[redacted]	[redacted]	Guest Wifi	Devantes-MBP	3m 28s	0m 0s	116.71 MB	3.42 MB	Kick
[redacted]	[redacted]	Metoyer - WPA	iPhone	1m 58s	0m 0s	220.61 KB	174.69 KB	Kick

6. Using the Filters tab, filter by MAC address then add the MAC address you recorded for your personal device.



Client Filter

Limit the scope of engagement by choosing what devices may connect. Allow only specific devices, or any device that isn't specifically on the deny list.

[redacted]

MAC Address

SSID Filter

Specify the spoofed networks for which the WiFi Pineapple will allow associations. Allow associations for only specifically listed SSIDs, or any SSID that isn't specifically listed.

SSID

After attempting to reconnect my personal device to the WiFi Pineapple network, I found that I was unable to rejoin due to the presence of a MAC address filter. Despite this, my device automatically reverted to my home wireless network, allowing seamless access to the internet and successfully opening Google.com. Once I returned to the WiFi Pineapple's administrative interface and removed my device's MAC address from the deny list within the Filters tab, I attempted reconnection again and successfully rejoined—although the connection required manual initiation. This occurred because removing the entry from the deny list deactivated the previously enforced filter. Even without direct access to the AP's internal configuration, an attacker can still glean substantial information by simply listening passively. This includes details like the network's SSID, BSSID, operating channel, and implemented security protocols. Additionally, observing connected devices reveals behavioral patterns, such as connection frequency and timing. Leveraging this insight, an attacker might employ targeted denial-of-service attacks to disconnect specific devices, capturing authentication handshakes in the process, or establish rogue access points designed to deceive users into connecting unknowingly. Consequently, passive monitoring alone can provide sufficient information to disrupt network operations and lay the groundwork for more sophisticated, intrusive attacks.