

**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 (AP), their clients and unassociated clients. Analyze these findings to identify the security and data leakage implications of WiFi network communications.

**Procedure:**

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

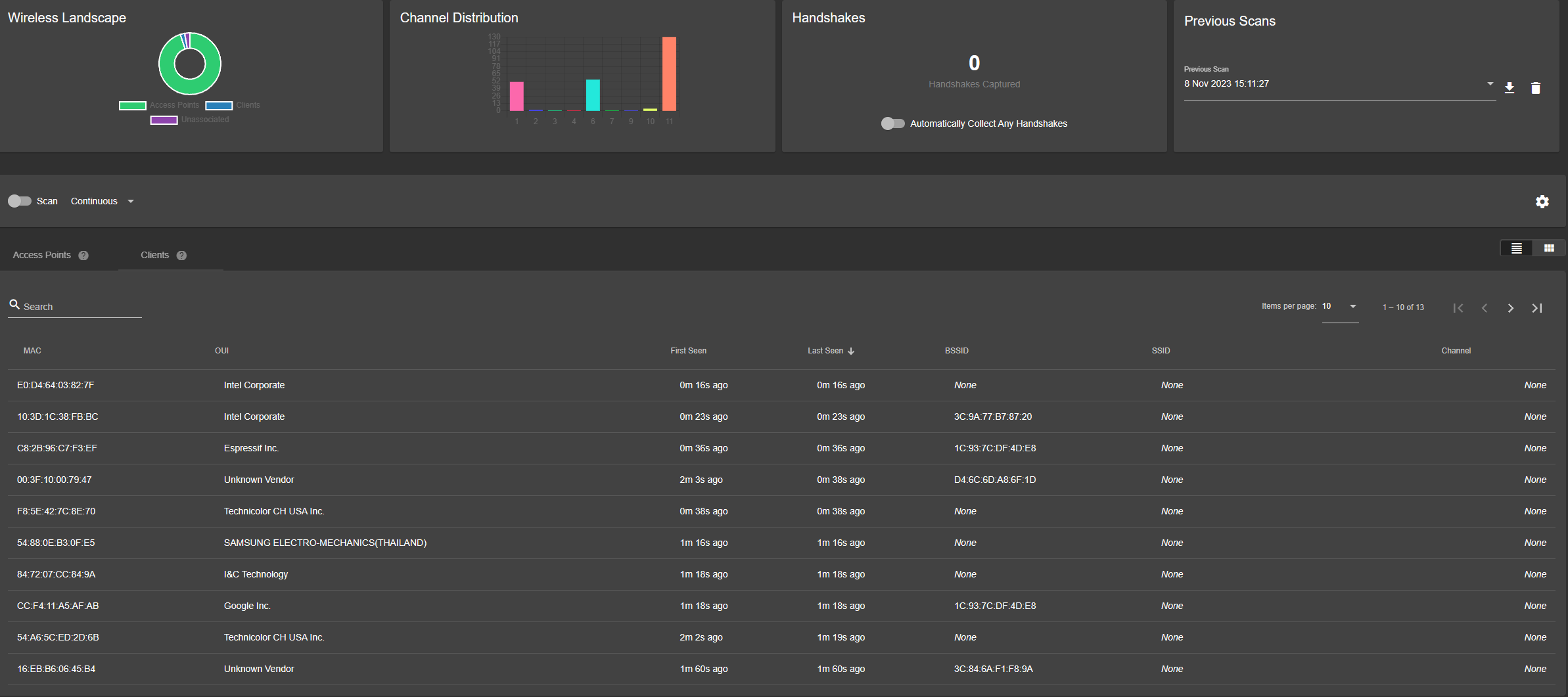
1. Log into your WiFi Pineapple AP and select the Recon Tab

1. Configure your WiFi Pineapple to operate in continuous Recon mode.
   1. Select the “AP & Client scan” radio button
   2. Set the scan interval to 30 seconds
   3. Select the “continuous box” to enable continuous scanning.

1. Take a screen grab of the Scan results on your WiFi Pineapple web interface so you can conduct off line analysis of your recon data capture. Turn the screen grab in with this report.

A screenshot of a computer

Description automatically generated



1. Analyze the “Scan Results” data and answer the following questions:

* 1. How many Access Points were detected?

248 Access Points were detected.

* 1. How many APs had associated clients?

6 APs had associated clients.

* 1. What channels were the Access Points using?

1 , 2 , 3, 4, 6, 7, 9, 10, 11

These were the channels being used through 248 AP’s.

* 1. How many APs were employing security and how many were Open?

246 APs were employing security while 2 had Open security.

* 1. What type of security was being used by each AP employing security?

A mix of: WPA2 (802.1X Enterprise), WPA2 Mixed (802.1X Enterprise), WPA2 (PSK)

f. How many Unassociated clients were detected?

7 unassociated clients were detected.

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

From the data I’ve collected, it allows an Attacker to:

* Identify target APs with active clients for spoofing.
* Helps an attacker set up a Rogue AP on prime channels to blend in or stand out.
* Attackers can mimic open/less secure APs to lure unsuspecting clients/targets.
* An attacker can exploit security protocol vulnerabilities.
* Attackers can mimic familiar networks and attract clients.

This of course with various other plugins/tools can cause unauthorized data interception and plenty of other malicious activities by tricking clients into connecting to an attacker’s Rogue AP.

1. 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?

An attacker can follow these steps or similar steps to target unassociated clients with WiFi Pineapple:

1. **Allow Associations:** An attacker can enable this feature on the Pineapple to accept connections from client devices that are looking to join networks.
2. **Capturing SSID’s to Pool:** Utilizing the data from unassociated clients which are most likely probing for known networks to capture and add these SSID’s to the Pineapple’s SSID list.
3. **Broadcasting SSID Pool:** Pineapple can broadcast out the captured SSID’s and trick unassociated clients into thinking they managed to find a trusted network they’re used to connecting to.

In order words this is a form of a Honeypot attack that is meant to lure unassociated clients into connecting with the attackers Pineapple, duping them into thinking the network is safe and familiar which would allow the attacker to carry out all sorts of data interception, credential harvests and possibly programs for malicious intent.

\* A WiFi Pineapple Primer can be found at: https://www.youtube.com/watch?v=eHnQwTCKe2o