# CYBV 479 Wireless Networking & Security

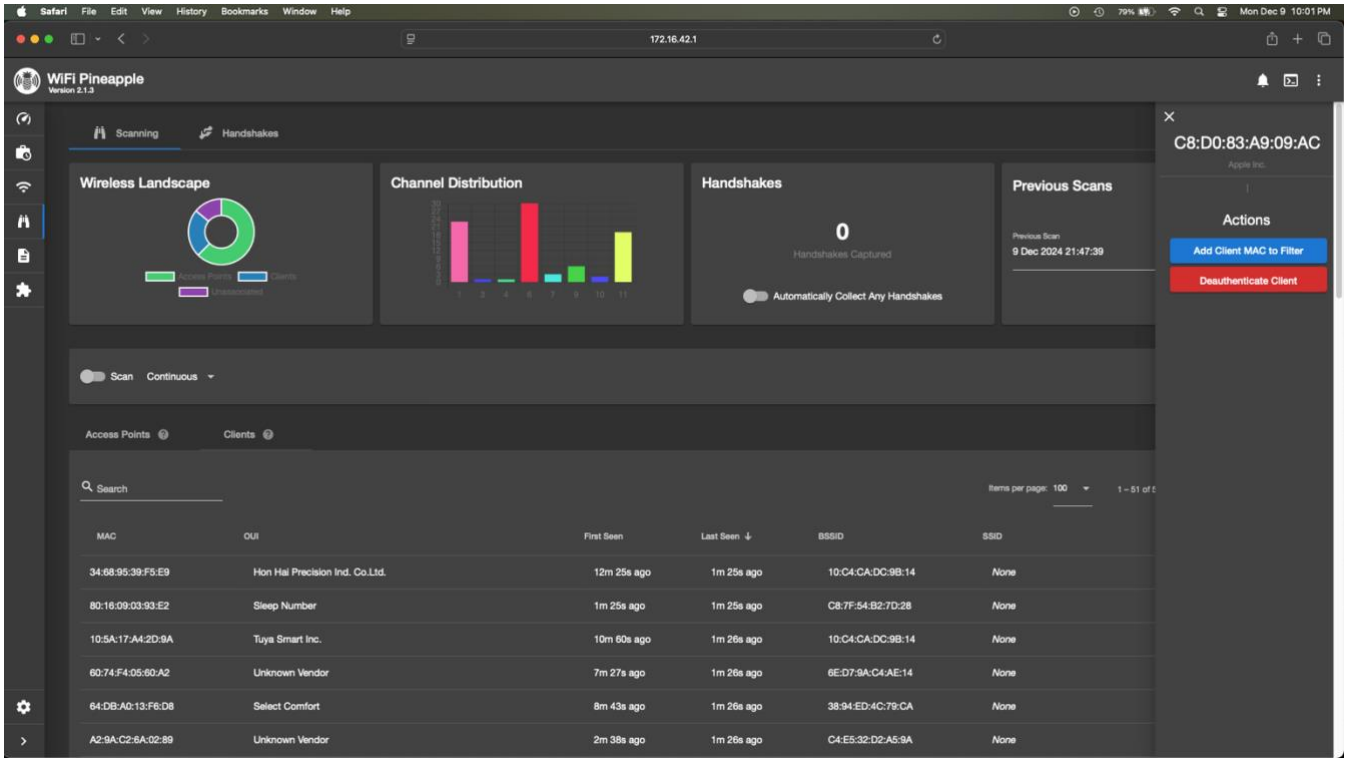
## WiFi DoS Exercise

*****NOTE: THIS EXERCISE IS TO BE PERFORMED ON YOUR PERSONAL NETWORK AND CLIENTS ONLY. ACTIVELY INTERACTING WITH ANY OTHER 3rd PARTY 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 Denial of Service exercise to identify how vulnerable Access Points (AP) and their clients are to remote interference. Analyze these findings to identify the security implications of WiFi network communications.

**Procedure:**

1. Set your WiFi Pineapple up in reconnaissance mode in your own home.
2. Using your computer, log into your WiFi Pineapple AP and select the Recon Tab.
3. Using your phone or a second personal computer, connect to your home WiFi network.
4. Configure your WiFi Pineapple to operate in continuous Recon mode.
    a. Select the "AP & Client scan" radio button
    b. Set scan to continuous
5. Take a screenshot of the DeAuth attack.




a. **What type of device is this?**

The device shown is my personal smartphone. In the provided video demonstration, the wireless landscape was displayed, and I replicated this approach. The device's Organizationally Unique Identifier (OUI) appears further down in the captured output.

6. **On your phone or your second computer, open a browser and attempt to navigate to www.google.com. Observe your phone's/second computer's browser and WiFi connection answer the following questions:**

    a. **Is your phone/second computer still connected to your home network?**

    Yes, my smartphone remains connected to my home wireless network..

    b. **Describe what effects the WiFi Pineapple DoS attack had on your phone/second computer and how it accomplished those effects?**

    During the WiFi Pineapple DoS attack, my smartphone experienced noticeably degraded performance and slower connectivity than usual. These symptoms indicate that the attack likely forced my device to repeatedly disconnect and reconnect to the network, causing instability and reduced responsiveness.

7. **Describe how an attacker could use type of attack to target both APs and clients?**

    Wireless management frames in standard Wi-Fi communications often remain unprotected, presenting a significant vulnerability that attackers can exploit. By crafting malicious frames disguised as legitimate management signals—from either the access point (AP) or client devices—an attacker can disrupt connectivity. For example, an attacker posing as the AP could send deceptive signals to forcefully disconnect all connected clients. Conversely, an attacker impersonating a legitimate client could send falsified messages, prompting the AP to terminate connections selectively. Since these forged management frames typically require no authentication, attackers can swiftly initiate a denial-of-service (DoS) scenario, effectively disabling network access for all devices within range without needing to compromise any passwords.

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