Lab 1: Understanding Man-in-the-Middle Attacks using WiFi Pineapple

Objective: Students will learn the basics of wireless auditing and gain an understanding of the tools available to conduct MITM pen-testing using the Wi-Fi Pineapple (WP).

Step 1: Connecting Wi-Fi Pineapple to host computer

WP will be connected to lab computer (preferably) running Kali Linux using the USB-C cable supplied with the kit.

Note: New WP devices by default do not have any firmware installed. Latest firmware from Hak5 will be installed by the tutor before teaching term so that the devices are ready for teaching.

Fig. 1 Typical connection setup

Step 2: Exploring Wi-Fi Pineapple Interface

Once connected, students will connect to WP management dashboard via web-browser (e.g., 172.16.42.1:1471/) and explore the different interfaces available. Tutor will provide an overview of each interface during lab session.

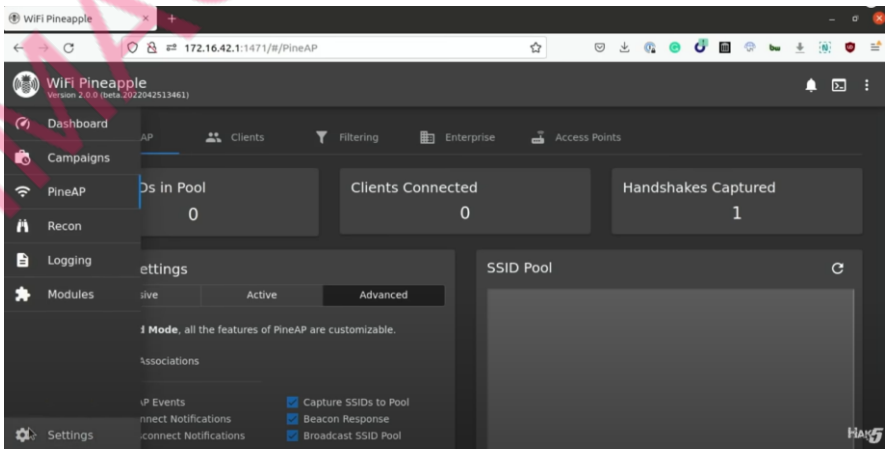


Fig. 2 WP management dashboard

Step 3: Exploring PineAP interface

Tutor will explain the specific use of each tab/tool in the PineAP interface (PineAP Wi-Fi, Clients, Filtering, Enterprise, Access Points). The dashboard shows the following information.,

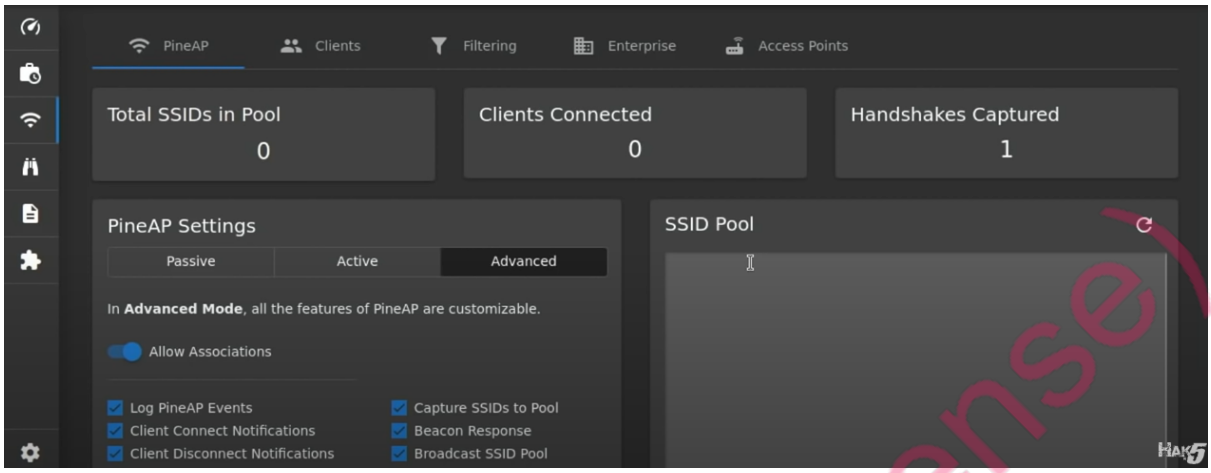


Fig. 3 WP Pine AP tools (tabs)

Total SSIDs in pool: showing list of networks that we will be using to emulate a list of connections we are trying to get our (victim) devices to connect to (list is available under SSID pool).

Connected Clients: if anyone authenticates to our rogue AP, we will see these devices here.

Wi-Fi Handshakes: the number of handshakes that have been captured either from reconnaissance interface or indirectly picked up from the PineAP.

Step 4: MITM (Karma) Attack Overview

Initial PC to AP connection: ***Blue team*** will connect their PCs to access points setup in the lab (AP1, AP2, AP3) using wireless routers (TP-Link Archer). Students will be able to connect to all three APs from their PCs to each AP iteratively without needing a password (open authentication). Once connected the SSID will be saved in each PCs *preferred network list (PNL).*

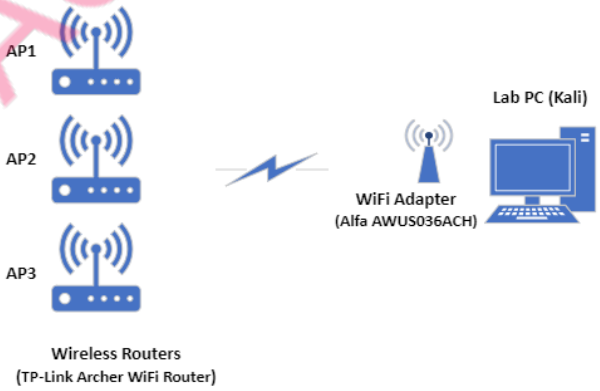


Fig. 4 Lab PC – AP1, AP2, AP3 Wi-Fi connection

MITM/Karma: *Red team* will initiate WiFi pineapple in passive mode (sniffer) to observe PC to AP connections of the blue team.

Passive scanner: does not antagonize devices and since it is only sniffing it is difficult to detect and will collect names of Access Points and display it in SSID pool (AP1, AP2, AP3).

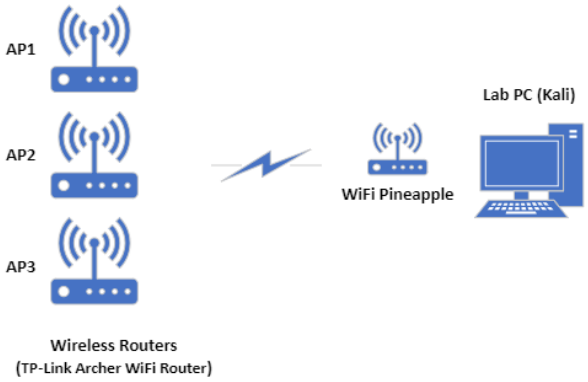


Fig. 5 Lab PC – Wi-Fi Pineapple AP connection monitoring

Other modes are **Active** and **Advanced**: *Active* provides the facility of using beacon responses and can also broadcast SSIDs from the previously sniffed SSID pool/list including AP1, AP2, AP3. Advanced is Active tab with customization available to toggle features on/off such as beacon responses and allow associations.

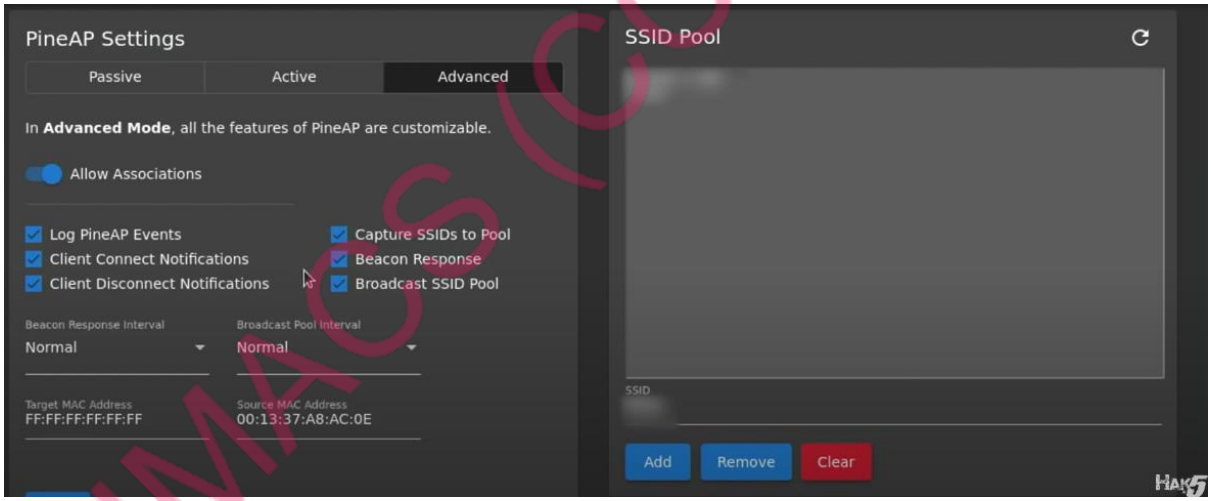


Fig. 6 PineAP settings (SSID pool populated by AP1, AP2, AP3)

Kicking off blue users from the AP: students will open the **Recon tab** and select the relevant client PC (or AP) and have the Wi-Fi pineapple send a de-authentication packet to kick-off user from the AP.

Blue PCs will disconnect from APs and attempt to reconnect, when re-connecting the devices will connect to rogue AP hosted by the Wi-Fi pineapple. This is possible due to the pineapple having three antennas, used to host AP, establish connection with victims and forward traffic to the real AP.

Once the task is complete, **red** and **blue** members will reverse roles and perform the same task again.

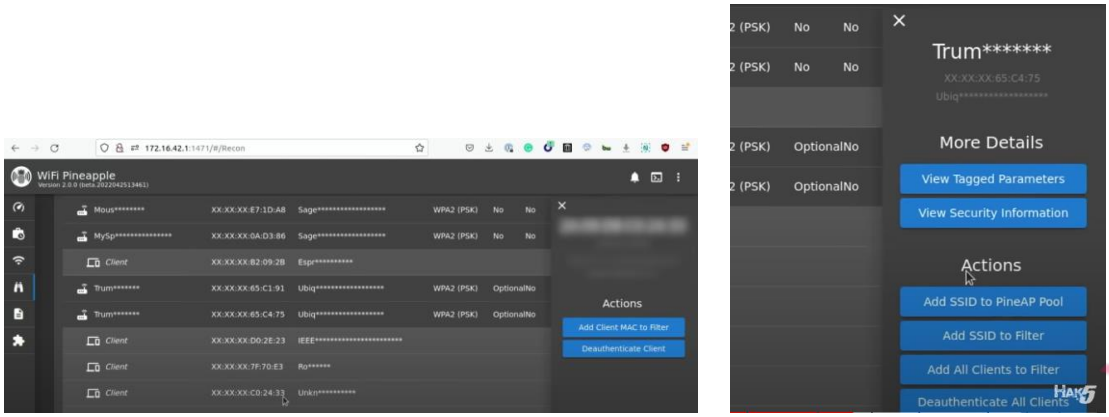


Fig. 7 De-authenticating single/all clients from AP1, AP2, AP3

Students will also be advised to research lists of commonly used AP names which do not require any authentication (Starbucks, Google AP, etc.) and how these can be manually added to the SSID pool in Wi-FI pineapple. This will help them appreciate that PNL history on mobile phones/any wireless device makes them highly vulnerable against wireless hacking, especially on open networks without password protection.

Summary:

1. Students will learn the basics of MITM attacks using WiFi pineapple,
2. Explore pineapple interfaces and understand the significance of using password authentication as well as
3. The importance of removing PNL from devices to mitigate against MITM (karma) attacks relying on previous connection history.
4. Using only password protected APs.

Demonstration Video: Hak5: Create Rogue Networks on the WiFi Pineapple (PineAP KARMA Attacks) https://www.youtube.com/watch?v=fOmDNn2aXXA

Lab 2: Wi-Fi Password Extraction using MITM Technique

Objective: Students will learn about SSID authentication using Wi-Fi pineapple devices and understand the vulnerabilities introduced due to weak AP password usage.

Step 1: Connecting Wi-Fi Pineapple to host computer

Same as lab 1.

Name of SSID and password previously used to connect to a network is stored in the NPL.

Step 2: Simple Password Extraction Overview (half-handshake attack)

Initial PC to AP connection: ***Blue team*** will connect their PCs to access points setup in the lab (AP1, AP2, AP3) using wireless routers (TP-Link Archer). Students will be able to connect to all three APs from their PCs to each AP iteratively using a very basic password which is commonly available in online password lists (e.g., password123). Once connected the SSID and password will be saved in each PCs *preferred network list (PNL).*

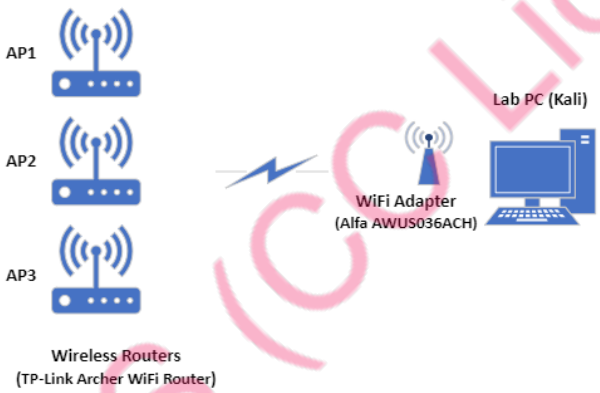


Fig. 1 Lab PC – AP1, AP2, AP3 Wi-Fi connection

Password extraction: ***Red team*** will initiate WiFi pineapple in passive mode (sniffer) to observe PC to AP connections of the blue team (Fig. 2).

On all Pineapple devices we have at least 2 WLAN interfaces -> wlan0 and wlan1. We can use tcpdump/Wireshark to analyse the traffic for all interfaces but to be more precise and correct we will only sniff packets on specific interface. In the following examples we will be using *wlan0.*

Interfaces on the devices can be simply verified as shown in Fig. 3 (ifconfig on Wifi Pineapple).

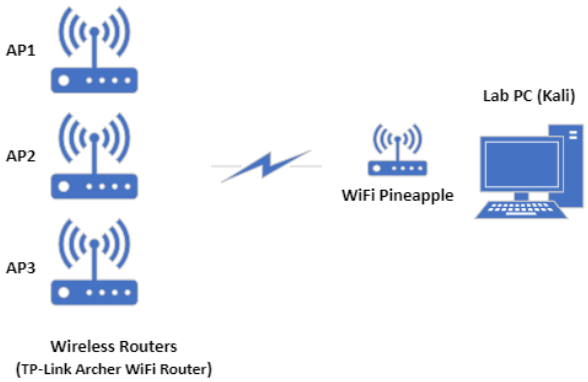


Fig. 2 Lab PC – Wi-Fi Pineapple AP connection monitoring

```
# get interface status (optional)
$ ssh -C4 root@172.16.42.1 "ifconfig"
wlan0     Link encap:Ethernet  HWaddr 00:13:37:A7:A3:3D
          inet6 addr: fe80::213:37ff:fea7:a33d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:334 errors:0 dropped:0 overruns:0 frame:0
          TX packets:479 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36864 (36.0 KiB)  TX bytes:58796 (57.4 KiB)

wlan1     Link encap:Ethernet  HWaddr 00:13:37:A7:A3:3E
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Fig. 3 Wi-Fi Pineapple interfaces

Normal device to Wi-Fi connection creates a four-way handshake. In this lab only two will be used to guess the password that **blue members** have used to connect to an AP.

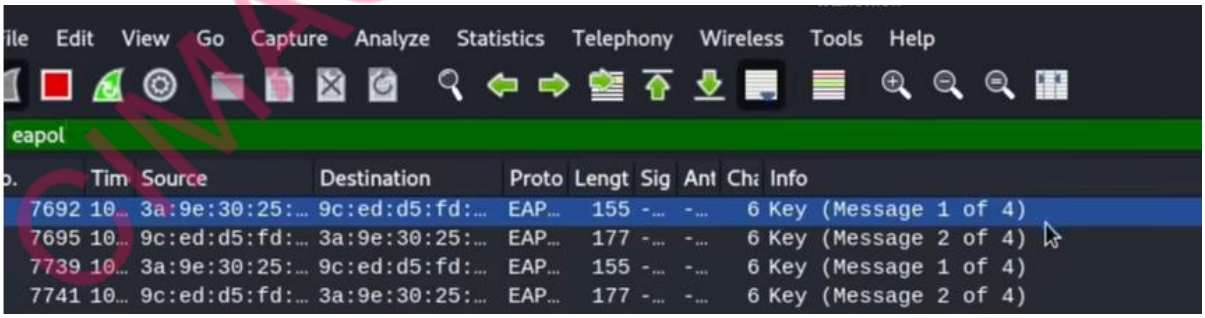


Fig. 4 Typical Wi-Fi Connection handshake

tcpdump examples will be executed directly on the Pineapple device, therefore **red team** will need to SSH into it from lab PC. The following tcpdump examples will help understand the basics. In case you need a deeper explanation about the commands use this free online service.

As disk space and hardware resources are not that high on Pineapple devices, local Wireshark on lab PC can be used and the traffic analysed more conveniently on the lab PC.

To start tcpdump and Wireshark only a single one-liner is needed.

```
# ssh into Pineapple
$ ssh -C4 root@172.16.42.1
```

```
# show DNS traffic
$ tcpdump -i wlan0 -nn -l udp port 53

# show HTTP User Agent and Hosts
$ tcpdump -i wlan0 -nn -l -A -s1500 | egrep -i 'User-Agent:|Host:'

# show HTTP requests and Hosts
$ tcpdump -i wlan0 -nn -l -s 0 -v | egrep -i "POST /|GET /|Host:"

# show e-mail recipients
$ tcpdump -i wlan0 -nn -l port 25 | egrep -i 'MAIL FROM\|RCPT TO'

# show FTP data
$ tcpdump -i wlan0 -nn -v port ftp or ftp-data

# show all passwords different protocols
$ tcpdump -i wlan0 port http or port ftp or port smtp or port imap or port pop3 or port telnet -l -A
```

```
# start tcpdump via SSH and Wireshark remote capture
$ ssh root@172.16.42.1 'tcpdump -i wlan0 -s0 -nn -w - not port 22' | /Applications/Wireshark.app/
```

Fig. 5 Wi-Fi pineapple SSH, tcpdump and Wireshark usage

Red team members will select individual networks in Wireshark using ***wlan.ta| wlan.da*** filters to select traffic stream between an individual PC (blue team) to the APs (AP1, AP2, AP3). Students will investigate different types of packets captured in the handshake at application, network and data link layer. Tutor will explain the working principle of each packet (Fig. 6).

After selecting the relevant stream, Wireshark filter will be updated to include **eapol** frame filter (e.g., eapol ||wlan.ta ==MAC address||wlan.da == MAC address). (Fig. 7)

Red team will now initiate disconnection of blue PC from the AP using Wi-Fi pineapple disconnection option (used in Lab 1).

The selected packet capture stream will be exported to local PC as a **.pcap file.**

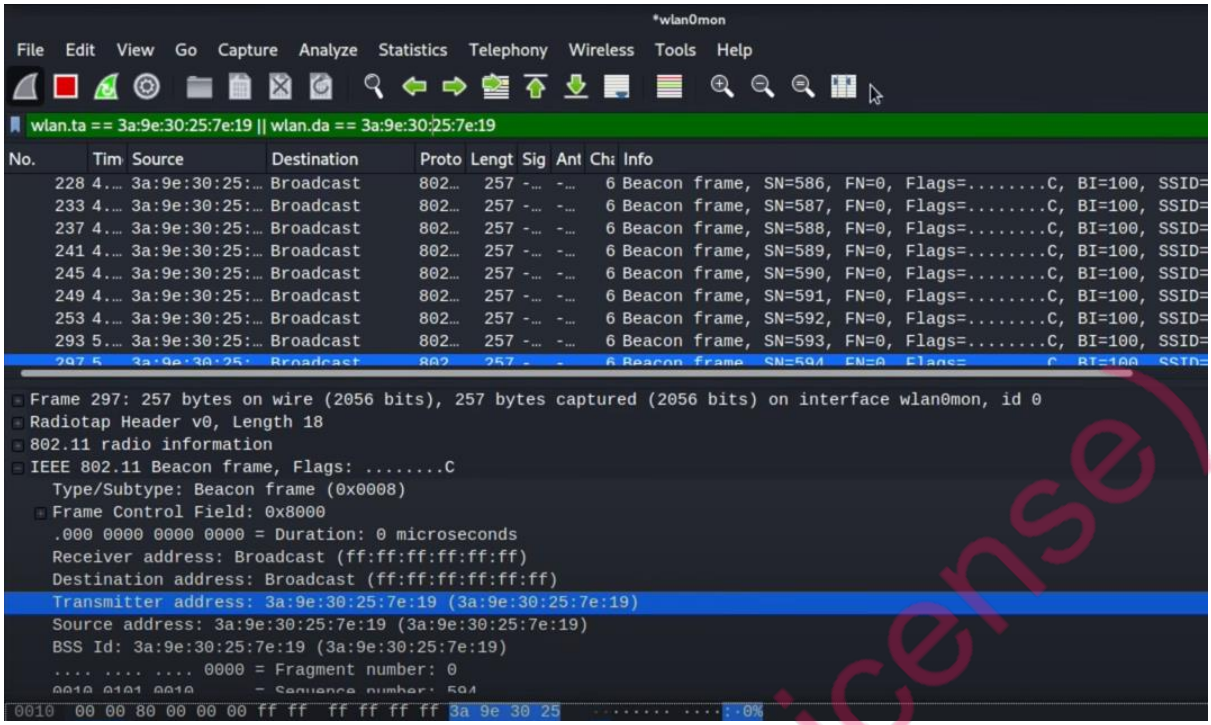


Fig. 6 Wireshark network stream filtering – Blue Team PC ←→ AP1||2||3

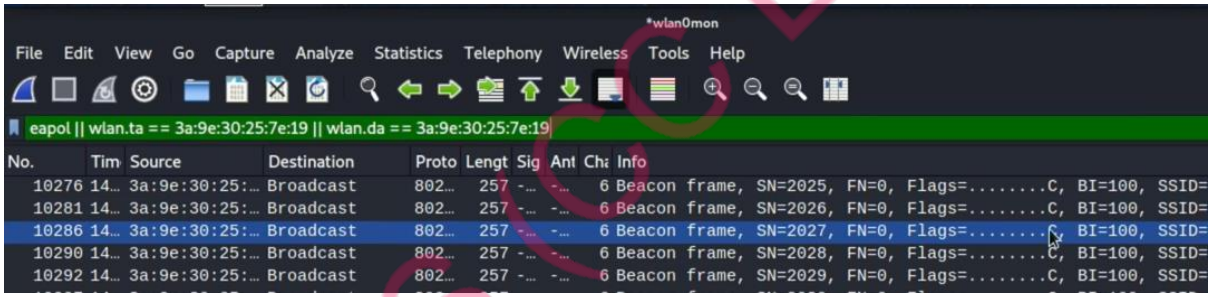


*Fig. 7 Wireshark with **eapol** filter*

Students will then use an online password list (e.g., rockyou.txt, etc,) and the packet capture file to guess the password using **aircrack-ng** tool (Fig. 8)

```
root@Macbook-Pro:~# aircrack-ng -w '/root/Desktop/rockyou.txt'  '/root/Desktop/halfhandshakehakbyte.pcap'
```

```
Terminal - root@Macbook-Pro: ~
File  Edit  View  Terminal  Tabs  Help

                          Aircrack-ng 1.6

      [00:00:01] 1546/10303727 keys tested (2608.90 k/s)

      Time left: 1 hour, 5 minutes, 48 seconds                  0.02%

                         KEY FOUND! [ password123 ]


      Master Key     : C2 CF 16 97 E8 24 3E 55 0E 41 D5 DD F3 48 DC ED
                       B9 DB 86 A6 D7 C0 2D 0D DE E2 0D 16 F6 03 65 5F

      Transient Key  : 58 07 80 0B 0E 6C 8E 5F 05 D3 3E D2 04 2D 36 60
                       98 81 E8 BF D5 78 6A 29 DA A4 B7 B0 F7 6A 7F EA
                       DA 24 3C F4 67 B3 0E A9 EB B9 0E 4F 13 C2 B5 BD
                       CD 9B E6 61 DA AC 69 CA 57 6A 8F FD D6 EE 14 00

      EAPOL HMAC     : 0C 40 86 BB B3 18 1F EB F1 4C D8 3B 24 38 BD B7


root@Macbook-Pro:~#
```

Fig. 8 Using aircrack-ng tool for password extraction from .pcap file

Once the task is complete, **red** and **blue** members will reverse roles and perform the same task again (tutor will update the password on APs using another commonly used password).

Students will also be advised to research lists of commonly used Wi-Fi passwords online and given an overview of Wigle.net which provides a readily available list of publicly found networks and serve as a resource for wireless auditing.

Summary:

1. Students will learn the basics of AP password extraction using WiFi pineapple,
2. Explore pineapple interfaces and understand the use of Wireshark, tcpdump and air-crack-ng,
3. Understand availability of commonly used online password lists, and wireless auditing resources such as wigle.net,
4. Vulnerability mitigation by employing best-practices (e.g., use of complex passwords) for wireless connections.

Demonstration Video: Hak5: Capture Wi-Fi Passwords with a Half-Handshake Attack
https://www.youtube.com/watch?v=5guDKTc6Hak

Note: To generate more exercises, small variations can be made to the lab 1 and lab 2. For example, making it a **time constrained exercise**, **allowing only limited members in each team access to WiFi pineapple** while the rest using only **Alfa Dual Band USB Adaptor** and **Kali tools** such as air-mon-ng to perform same tasks. This will help students understand the automation capability of basic wireless auditing campaigns provided by Wi-Fi pineapple devices.

However, the overall scope will be limited to the specifics discussed in lab 1 and 2.

Author: Dr. Taimur Bakhshi, 2023

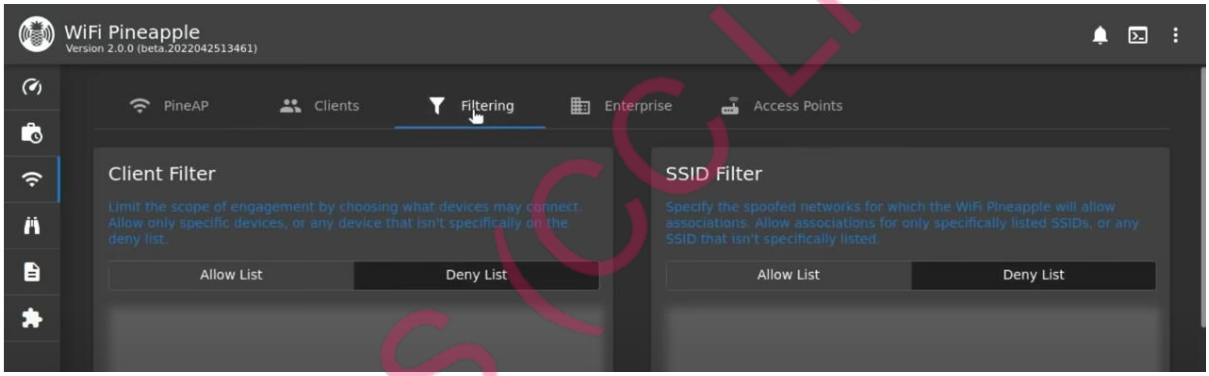
Potential Challenges

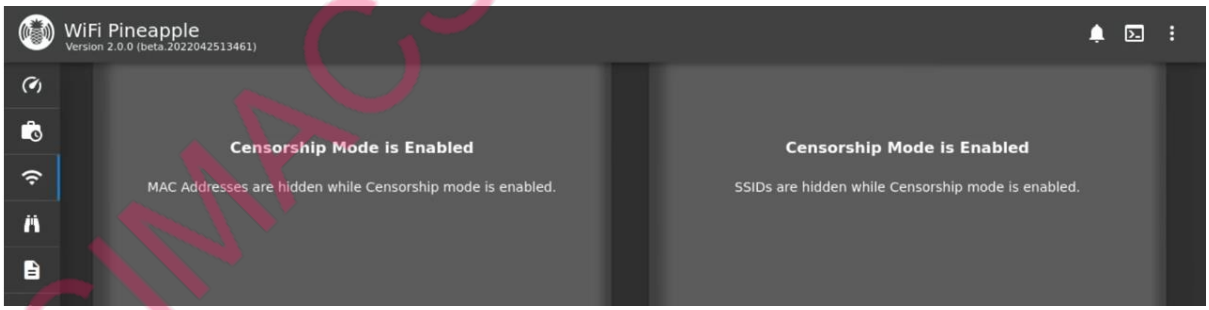
1) Eduroam or other LBU SSIDs

- If students connect to Eduroam or any other LBU SSID within pineapple range, they can use **the de-authentication option** in device to **remove legitimate users from these APs.**

Possible Workarounds

- MITM on Eduroam and LBU SSIDs may not be possible as Eduroam and LBU SSID are using strong password-based authentication.
- Students will only be given pineapple devices for the duration of the lab and device usage will be always monitored by tutor.
- Narrowing the scope of engagement: Filtering option in Wi-Fi pineapple provides the ability to disallow targeting specific devices/blocking out APs which are off-limit to us, and we do not want to pen-test. University Wi-Fi access points can be added to this list on each Wi-Fi AP and students made aware that they are not to change this list.





2) External Users connecting to open/unauthenticated APs (Lab 1)

- Users outside the lab and within pineapple/hosted AP wireless range may see open access points and if having any difficulty connecting to the university network may connect to these instead.
- During packet capture, packets from these (external) user devices may be captured and stored in .pcap file.

Possible Workarounds

- In each TP-Link Archer WiFi Router setting create an access-list allowing only MAC addresses of lab PC wireless cards (i.e., the Alfa AWUS036ACH USB adaptors). This will remove any connection attempt from external user devices to AP1, AP2 and AP3.