SIT327 - Network Forensics

Pass Task 3: WiFi Forensics Analysis

Overview

In this exercise, we'll delve into a forensic examination of an attack on a WiFi network. You're required to download the provided pcap file that contains the captured WiFi data. We will utilize two analytical tools, tcpdump and tshark, to scrutinize the pcap file. In our upcoming class, we'll explore different types of WiFi frames, including the WiFi beacon frame, which will be our focus for this task.

Use tcpdump to identify a broadcast frame within the capture. Analyze this frame to ascertain the MAC address of the wireless access point and the SSID (Service Set Identifier) of the network.

```
tcpdump -nne -r wlan.pcap 'wlan[0] = 0x80'
```

Use tshark to confirm the MAC address by typing

```
tshark -nn -r wlan.pcap -Y '((wlan.fc.type_subtype == 0x08)) || wlan.fc.
    type_subtype == 0x05' -T fields -e wlan.bssid
```

Report Submission:

Submit a report containing:

- A screenshot running the commands
- An answer to what the MAC of the WAP, refrencing the data.
- An answer to what the SSID is, referencing the data.