SIT327 - Network Forensics

DistinctionTask 2: WiFi Investigation

Overview

In this task we will examine a forensics investigation an attack against wifi. Download the included pcap of the wifi capture. We will use two tools to investigate the pcap, tcpdump and tshark. As discussed in class IVs are part of the WEP encrpytion algorithm. Let's see how many IV's were generated by the attacker. You may find the below helpful.

```
tshark -nn -r wlan.pcap -Y 'wlan.bssid==00:23:69:61:00:d0 and wlan.wep.iv' -T
    fields -e wlan.wep.iv
```

Pipe the output to a set of unix commands to count how many IVs we have. Do some research. Do you think this is should be enough IVs to attack WEP? Based on the result of your answer to the first question, research and use the the aircrackng tool to crack the WEP password. Use the password to decrypt the packets in the attached pcap. You may find the below helpful.

```
man aircrack-ng
```

Decrypt the packets. What type of packets are the vast majority of the packets that were sent by the attacker? Why might the attacker send this type of packet?

Report Submission:

- An answer to the number of IVs involved, and your opinion on if this is enough to attack the algorithm.
- A screenshot finding the WEP key and decrypting the data.
- Your analyis of the attack.