Network Pentesting

Target

CSIS NETWORK

Tools used

- Airmon-ng
- Wireshark
- aireplay-ng
- ettercap
- ifconfig
- iw

Procedure

Analyzing network packets using wireshark

- first put wifi card into monitor mode - this allows the card to accept all network packets instead of just packets around it
- command → `airmon-ng check kill`(to kill all services using the card)
- command → `airmon-ng start wlo1`(to start monitor mode on interface wl0)
- Run Wireshark on interface wl0 and use the filter
- ⟶ `wlan.fc.type = 0`(This sets wireshark to only show management frames)
- results for network (CSIS_DIR) similar results gotten for other networks

```
Frame 131: 249 bytes on wire (1992 bits), 249 bytes captured (1992 bits) on interface wlo1, id 0
    Section number: 1
    Interface id: 0 (wlo1)
        Interface name: wlo1
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jun 13, 2023 14:15:39.965830408 WAT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1686662139.965830408 seconds
    [Time delta from previous captured frame: 0.012547048 seconds]
    [Time delta from previous displayed frame: 0.043210687 seconds]
    [Time since reference or first frame: 67.028319989 seconds]
    Frame Number: 131
    Frame Length: 249 bytes (1992 bits)
    Capture Length: 249 bytes (1992 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
```

```
    Present flags
        Present flags word: 0x0000482e
            .... .... .... .... .... .... .... ...0 = TSFT: Absent
            .... .... .... .... .... .... .... ..1. = Flags: Present
            .... .... .... .... .... .... .... .1.. = Rate: Present
            .... .... .... .... .... .... .... 1... = Channel: Present
            .... .... .... .... .... .... ...0 .... = FHSS: Absent
            .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
            .... .... .... .... .... .... .0.. .... = dBm Antenna Noise: Absent
            .... .... .... .... .... .... 0... .... = Lock Quality: Absent
            .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
            .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
            .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
            .... .... .... .... .... 1... .... .... = Antenna: Present
            .... .... .... .... ...0 .... .... .... = dB Antenna Signal: Absent
            .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
            .... .... .... .... .1.. .... .... .... = RX flags: Present
            .... .... .... .... 0... .... .... .... = TX flags: Absent
            .... .... .... ..0. .... .... .... .... = data retries: Absent
            .... .... .... .0.. .... .... .... .... = Channel+: Absent
            .... .... .... 0... .... .... .... .... = MCS information: Absent
            .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
            .... .... ..0. .... .... .... .... .... = VHT information: Absent
            .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
            .... .... 0... .... .... .... .... .... = HE information: Absent
            .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
            .... .0.. .... .... .... .... .... .... = 0 Length PSDU: Absent
            .... 0... .... .... .... .... .... .... = L-SIG: Absent
```

```
Flags: 0x10
    .... ...0 = CFP: False
    .... ..0. = Preamble: Long
    .... .0.. = WEP: False
    .... 0... = Fragmentation: False
    ...1 .... = FCS at end: True
    ..0. .... = Data Pad: False
    .0.. .... = Bad FCS: False
    0... .... = Short GI: False
  Data Rate: 2.0 Mb/s
  Channel frequency: 2457 [BG 10]
  Channel flags: 0x00a0, Complementary Cod
  Antenna signal: -46 dBm
  Antenna: 6
```

- From the Management Frames we can infer the following things
  - The routers use the IEEE 802.11 protocol
  - The network is transmitting at a Data Rate of 2.0mb/s
  - The signal strengthis about -46dm
  - WPA encryption instead of WEP is used(This is significantly better for security)

Attempting Deauthentication attack

- This attempts to deauthenticate all connected users by pretending to be the router and sending deauthentication packets to connected clients. This is done by spoofing the MAC address of the router
- First get the BSSID of the network using
  - command ⟶ `iw dev wlo1 link`
  - the BSSID is ==84:23:88:1E:CA:98 ==
- Set the channel of the wifi card to the channel of signal
  - command ⟶ sudo airmon start wlo1 8(8 here is used to put the wifi card on channel 8)
- Run deauthentication attack using aireplay-ng
  - command ⟶ `sudo aireplay-ng -0 20 -a 84:23:88:1e:ca:98 wlo1`

- The command executed succesfully and disconnected all nearby devices from the network

Vulnerability

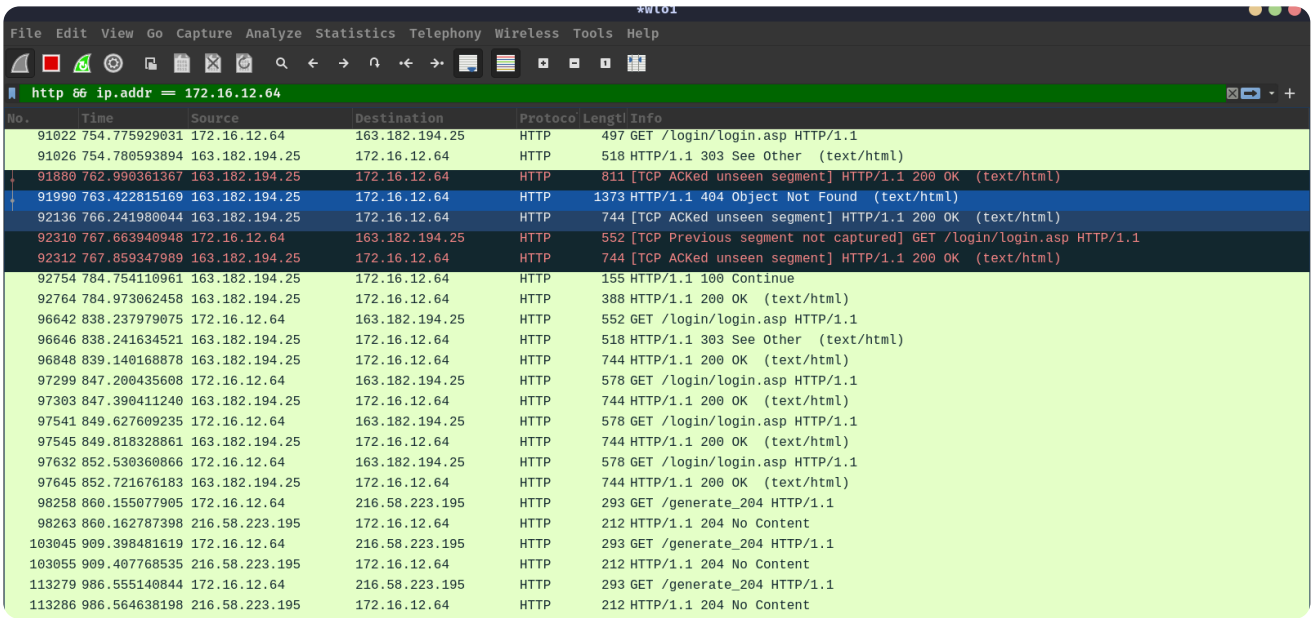
- The network was found to be vulnerable to Deauthentication attacks through MAC spoofing

Proposal

- We propose that MAC filtering be done for all requests on the network to filter out packets whose MAC addresses do not correlate with the manufacturer information

Attempting MITM attack through ARP poisioning

- This attempts to intercept traffic between the client and the router by spoofing ARP packets
- This is done using a tool called ettercap
- Wireshark is used to monitor victim traffic after spoofing



Vulnerability

- The network was found to be vulnerable to ARP poisoning attack
- This compromises the safety of information transmitted in plain text(unencrypted data) from the client over the network ie http requests

Proposal

- Use Packet filtering firewalls
- Use a static ARP entry on the client computers instead of dynamically resolving from