ATTACK DEFENSE

by PentesterAcademy

Name	Impersonating Client Detection
URL	https://www.attackdefense.com/challengedetails?cid=1145
Type	WiFi Pentesting: Traffic Analysis

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

A WiFi traffic capture is provided in the lab. We are told that one of the devices in the capture is using MAC cloning i.e. that device is impersonating another device which is also present in the vicinity.

Objective: Analyze the traffic using Wireshark and find the MAC address of the client which is being impersonated?

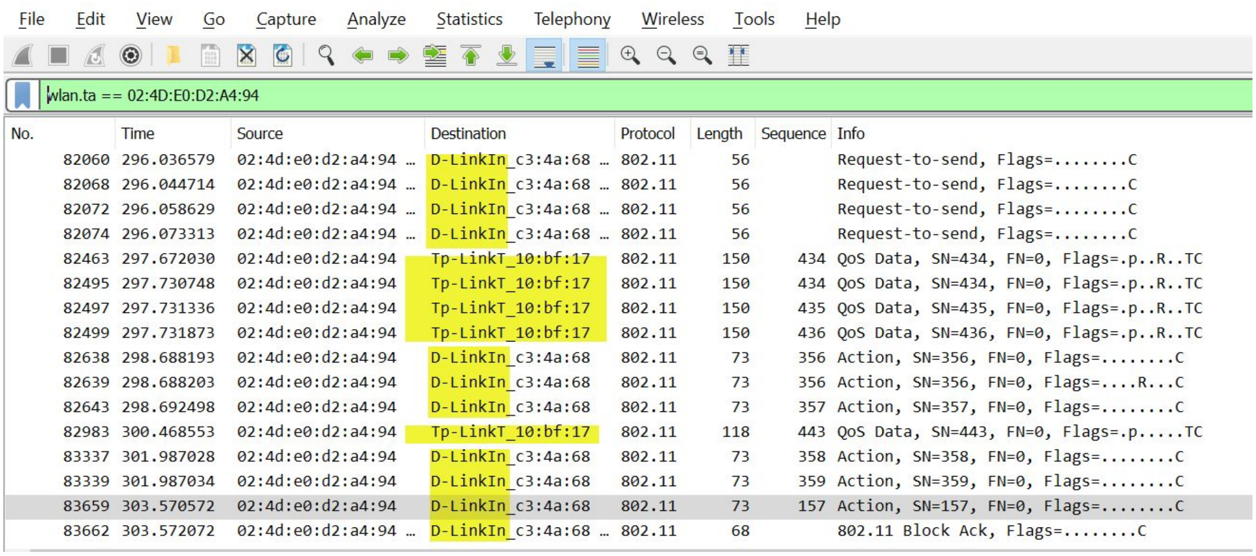
A. 02:4D:E0:D2:A4:94

Solution:

All clients need to be checked one by one for the anomalies.

When we filter the traffic for client 02:4D:E0:D2:A4:94, it is evident that the same MAC is associated with two BSSIDs at the same time which is not possible. So, it is a clear case of client MAC impersonation.

Filter: wlan.ta == 02:4D:E0:D2:A4:94

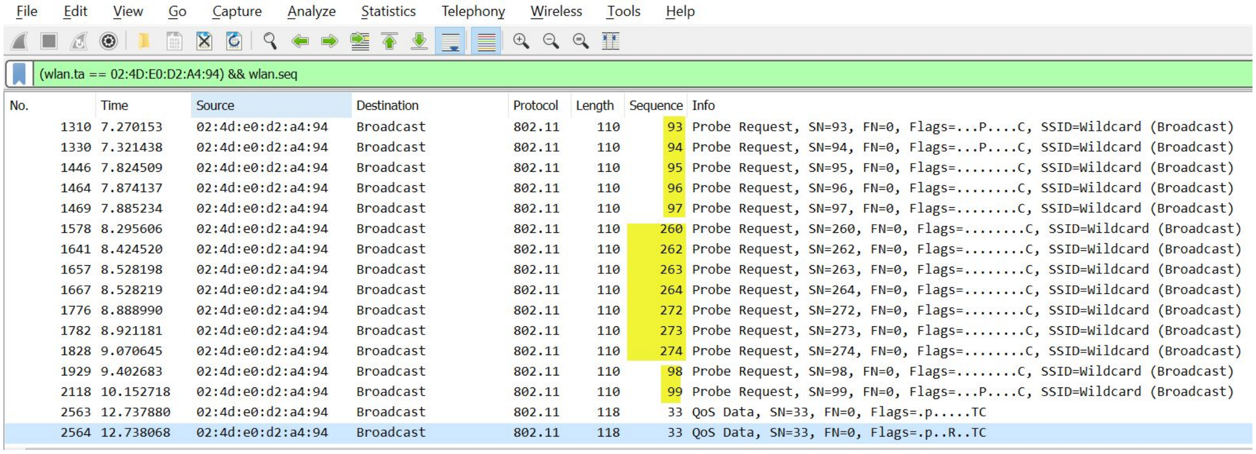


```
wlan.ta == 02:4D:E0:D2:A4:94

No.      Time        Source               Destination           Protocol  Length  Sequence  Info
   82060 296.036579  02:4d:e0:d2:a4:94 …  D-LinkIn_c3:4a:68 …   802.11     56             Request-to-send, Flags=........C
   82068 296.044714  02:4d:e0:d2:a4:94 …  D-LinkIn_c3:4a:68 …   802.11     56             Request-to-send, Flags=........C
   82072 296.058629  02:4d:e0:d2:a4:94 …  D-LinkIn_c3:4a:68 …   802.11     56             Request-to-send, Flags=........C
   82074 296.073313  02:4d:e0:d2:a4:94 …  D-LinkIn_c3:4a:68 …   802.11     56             Request-to-send, Flags=........C
   82463 297.672030  02:4d:e0:d2:a4:94    Tp-LinkT_10:bf:17     802.11    150       434   QoS Data, SN=434, FN=0, Flags=.p..R..TC
   82495 297.730748  02:4d:e0:d2:a4:94    Tp-LinkT_10:bf:17     802.11    150       434   QoS Data, SN=434, FN=0, Flags=.p..R..TC
   82497 297.731336  02:4d:e0:d2:a4:94    Tp-LinkT_10:bf:17     802.11    150       435   QoS Data, SN=435, FN=0, Flags=.p..R..TC
   82499 297.731873  02:4d:e0:d2:a4:94    Tp-LinkT_10:bf:17     802.11    150       436   QoS Data, SN=436, FN=0, Flags=.p..R..TC
   82638 298.688193  02:4d:e0:d2:a4:94    D-LinkIn_c3:4a:68     802.11     73       356   Action, SN=356, FN=0, Flags=........C
   82639 298.688203  02:4d:e0:d2:a4:94    D-LinkIn_c3:4a:68     802.11     73       356   Action, SN=356, FN=0, Flags=....R...C
   82643 298.692498  02:4d:e0:d2:a4:94    D-LinkIn_c3:4a:68     802.11     73       357   Action, SN=357, FN=0, Flags=........C
   82983 300.468553  02:4d:e0:d2:a4:94    Tp-LinkT_10:bf:17     802.11    118       443   QoS Data, SN=443, FN=0, Flags=.p.....TC
   83337 301.987028  02:4d:e0:d2:a4:94    D-LinkIn_c3:4a:68     802.11     73       358   Action, SN=358, FN=0, Flags=........C
   83339 301.987034  02:4d:e0:d2:a4:94    D-LinkIn_c3:4a:68     802.11     73       359   Action, SN=359, FN=0, Flags=........C
   83659 303.570572  02:4d:e0:d2:a4:94    D-LinkIn_c3:4a:68     802.11     73       157   Action, SN=157, FN=0, Flags=........C
   83662 303.572072  02:4d:e0:d2:a4:94 …  D-LinkIn_c3:4a:68 …   802.11     68             802.11 Block Ack, Flags=........C
```

Also apply the sequence number field filter to look sequence number based anomalies.

Filter: (wlan.ta == 02:4D:E0:D2:A4:94) && wlan.seq



```
(wlan.ta == 02:4D:E0:D2:A4:94) && wlan.seq

No.      Time       Source             Destination  Protocol  Length  Sequence  Info
    1310 7.270153   02:4d:e0:d2:a4:94  Broadcast    802.11    110        93  Probe Request, SN=93, FN=0, Flags=...P....C, SSID=Wildcard (Broadcast)
    1330 7.321438   02:4d:e0:d2:a4:94  Broadcast    802.11    110        94  Probe Request, SN=94, FN=0, Flags=...P....C, SSID=Wildcard (Broadcast)
    1446 7.824509   02:4d:e0:d2:a4:94  Broadcast    802.11    110        95  Probe Request, SN=95, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    1464 7.874137   02:4d:e0:d2:a4:94  Broadcast    802.11    110        96  Probe Request, SN=96, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    1469 7.885234   02:4d:e0:d2:a4:94  Broadcast    802.11    110        97  Probe Request, SN=97, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    1578 8.295606   02:4d:e0:d2:a4:94  Broadcast    802.11    110       260  Probe Request, SN=260, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    1641 8.424520   02:4d:e0:d2:a4:94  Broadcast    802.11    110       262  Probe Request, SN=262, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    1657 8.528198   02:4d:e0:d2:a4:94  Broadcast    802.11    110       263  Probe Request, SN=263, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    1667 8.528219   02:4d:e0:d2:a4:94  Broadcast    802.11    110       264  Probe Request, SN=264, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    1776 8.888990   02:4d:e0:d2:a4:94  Broadcast    802.11    110       272  Probe Request, SN=272, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    1782 8.921181   02:4d:e0:d2:a4:94  Broadcast    802.11    110       273  Probe Request, SN=273, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    1828 9.070645   02:4d:e0:d2:a4:94  Broadcast    802.11    110       274  Probe Request, SN=274, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    1929 9.402683   02:4d:e0:d2:a4:94  Broadcast    802.11    110        98  Probe Request, SN=98, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    2118 10.152718  02:4d:e0:d2:a4:94  Broadcast    802.11    110        99  Probe Request, SN=99, FN=0, Flags=...P....C, SSID=Wildcard (Broadcast)
    2563 12.737880  02:4d:e0:d2:a4:94  Broadcast    802.11    118        33  QoS Data, SN=33, FN=0, Flags=.p.....TC
    2564 12.738068  02:4d:e0:d2:a4:94  Broadcast    802.11    118        33  QoS Data, SN=33, FN=0, Flags=.p..R..TC
```

We can observe two different sequences in probe requests.

References:

1. Wireshark (https://www.wireshark.org/)
2. Pentester Academy WiFi course (https://www.pentesteracademy.com/course?id=9)