ATTACK DEFENSE

by PentesterAcademy

Name	WPA Supplicant: WPA Enterprise
URL	https://www.attackdefense.com/challengedetails?cid=1284
Type	Wi-Fi Attack-Defense : AP-Client Basics

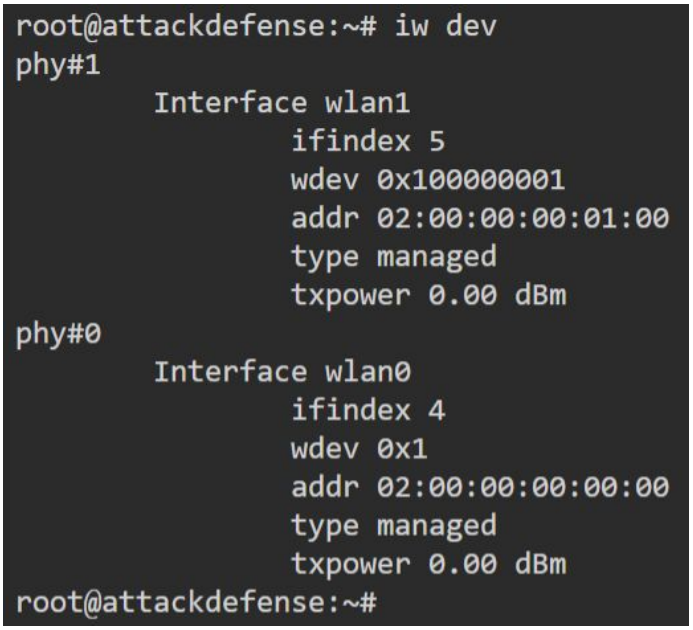
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Objective: Connect to SSID Corporate-A by using different EAP authentication methods using wpa_supplicant.

Solution:

Step 1: Check the list of available WiFi network interfaces on the machine

Command: iw dev.

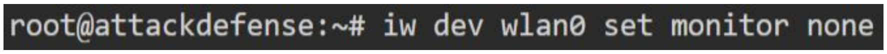


```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1
                addr 02:00:00:00:00:00
                type managed
                txpower 0.00 dBm
root@attackdefense:~#
```

Wlan0 and wlan1 interfaces are present on the machine.

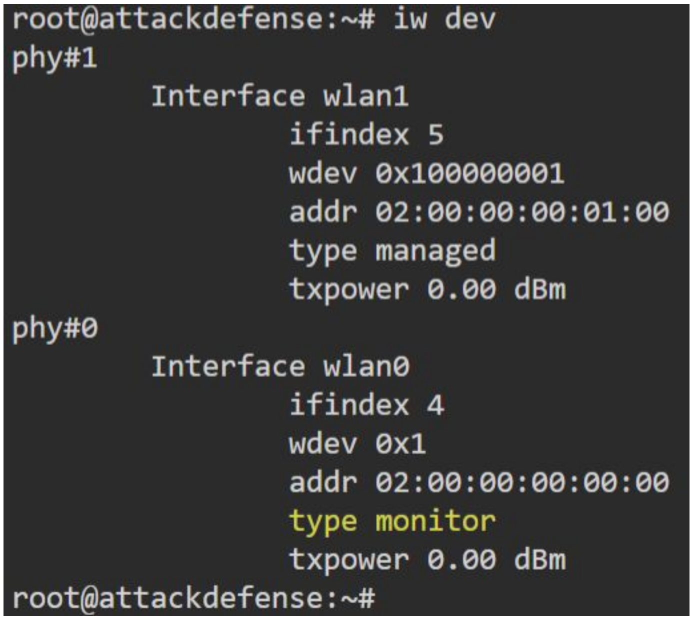
Step 2: Change interface wlan0 to monitor mode.

Command: iw dev wlan0 set monitor none



```
root@attackdefense:~# iw dev wlan0 set monitor none
```

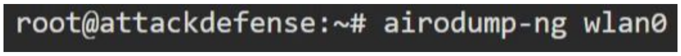
Verify the same using iw dev command.



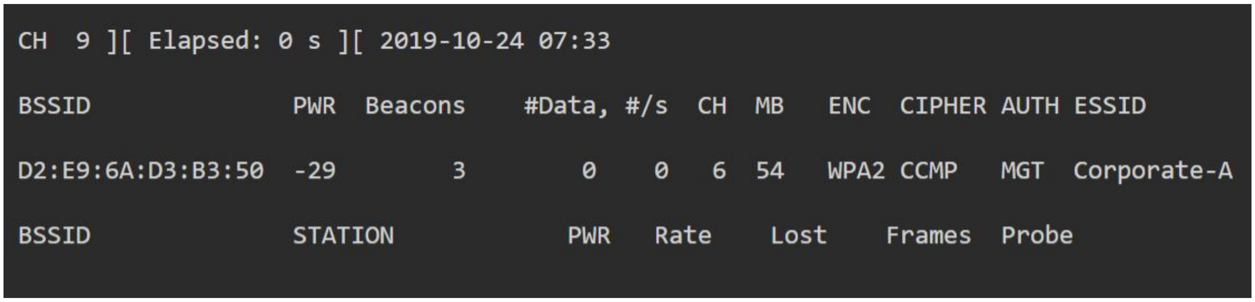
```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1
                addr 02:00:00:00:00:00
                type monitor
                txpower 0.00 dBm
root@attackdefense:~#
```

Step 3: Run airodump-ng on wlan0 interface to view all networks present in the vicinity on 2.4 (b/g) Ghz band.

Command: airodump-ng wlan0



```
root@attackdefense:~# airodump-ng wlan0
```



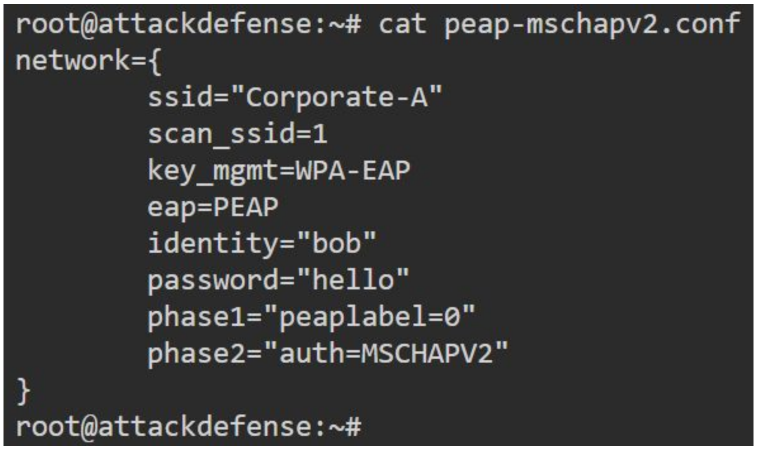
```
CH  9 ][ Elapsed: 0 s ][ 2019-10-24 07:33

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

D2:E9:6A:D3:B3:50  -29        3        0    0   6  54   WPA2 CCMP   MGT  Corporate-A

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

SSID “Corporate-A” is available.

Step 4: Create a wpa_supplicant configuration file for this network (the required information is given in challenge statement). Start with PEAP-MSCHAPv2 authentication.

WPA Supplicant Configuration

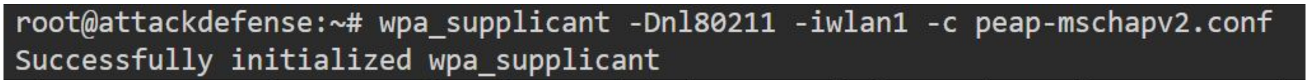
```
network={
        ssid="Corporate-A"
        scan_ssid=1
        key_mgmt=WPA-EAP
        eap=PEAP
        identity="bob"
        password="hello"
        phase1="peaplabel=0"
        phase2="auth=MSCHAPV2"
}
```



```
root@attackdefense:~# cat peap-mschapv2.conf
network={
        ssid="Corporate-A"
        scan_ssid=1
        key_mgmt=WPA-EAP
        eap=PEAP
        identity="bob"
        password="hello"
        phase1="peaplabel=0"
        phase2="auth=MSCHAPV2"
}
root@attackdefense:~#
```

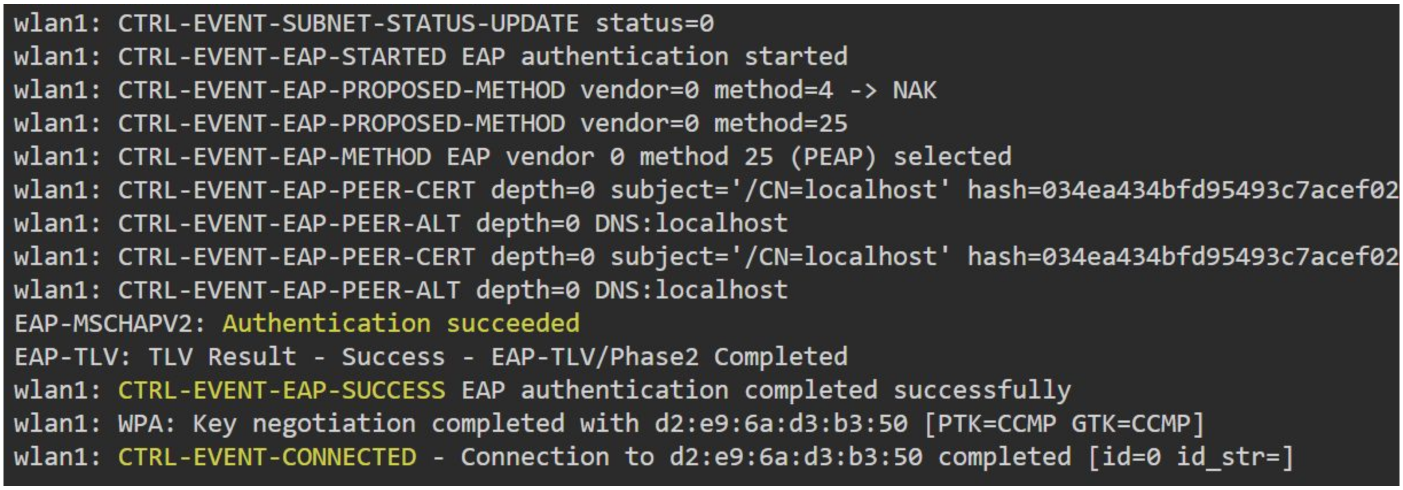
Step 5: Start wpa_supplicant

Command: wpa_supplicant -Dnl80211 -iwlan1 -c peap-mschapv2.conf



```
root@attackdefense:~# wpa_supplicant -Dnl80211 -iwlan1 -c peap-mschapv2.conf
Successfully initialized wpa_supplicant
```

Step 6: Wait for it to connect to WiFi network. As soon as it connects to the network, the logs will appear on the console.



```
wlan1: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
wlan1: CTRL-EVENT-EAP-STARTED EAP authentication started
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=4 -> NAK
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan1: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 25 (PEAP) selected
wlan1: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/CN=localhost' hash=034ea434bfd95493c7acef02
wlan1: CTRL-EVENT-EAP-PEER-ALT depth=0 DNS:localhost
wlan1: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/CN=localhost' hash=034ea434bfd95493c7acef02
wlan1: CTRL-EVENT-EAP-PEER-ALT depth=0 DNS:localhost
EAP-MSCHAPV2: Authentication succeeded
EAP-TLV: TLV Result - Success - EAP-TLV/Phase2 Completed
wlan1: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
wlan1: WPA: Key negotiation completed with d2:e9:6a:d3:b3:50 [PTK=CCMP GTK=CCMP]
wlan1: CTRL-EVENT-CONNECTED - Connection to d2:e9:6a:d3:b3:50 completed [id=0 id_str=]
```

From the logs, one can observe that the connection was successful.

Step 8: Similarly, other auth methods can be used by using suitable configurations.

PEAP-GTC WPA Supplicant Configuration

```
network={
        ssid="Corporate-A"
        scan_ssid=1
        key_mgmt=WPA-EAP
        eap=PEAP
        identity="bob"
        password="hello"
        phase1="peaplabel=0"
        phase2="auth=GTC"
}
```

TTLS-PAP WPA Supplicant Configuration

```
network={
        ssid="Corporate-A"
        scan_ssid=1
        key_mgmt=WPA-EAP
        eap=TTLS
        identity="bob"
        anonymous_identity="anon"
        password="hello"
        phase2="auth=PAP"
}
```

TTLS-CHAP WPA Supplicant Configuration

```
network={
        ssid="Corporate-A"
        scan_ssid=1
        key_mgmt=WPA-EAP
        eap=TTLS
        identity="bob"
        anonymous_identity="anon"
        password="hello"
        phase2="auth=CHAP"
}
```

TTLS-MSCHAPv2 WPA Supplicant Configuration

```
network={
        ssid="Corporate-A"
        scan_ssid=1
        key_mgmt=WPA-EAP
        eap=TTLS
        identity="bob"
        anonymous_identity="anon"
        password="hello"
        phase2="auth=MSCHAPV2"
}
```