Configuration Manual

MSc Research Project
Master of Science in Cyber Security

Niall Coughlan
Student ID: 21121214

School of Computing
National College of Ireland

Supervisor: Raza Ul Mustafa

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. …………Niall Coughlan……………………………………………………………………………

Student ID: ………………21121214…………………………………………………………………………..……

Programme: ……MSCCYBETOP……………………………… **Year:** ………2023……….

Module: …………Research Project……………………………………………………….………

Lecturer: …………Raza Ul Mustafa……………………………………………………………….………

Submission Due Date: ………18th September 2023…………………………………………………………….………

Project Title: ……Enhancing Public Wi-Fi Security Through Digital Certificate Authentication…………………………………………….………

Word Count: …………1059……………… **Page Count:** …………………7……………..……..………

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ………

Date: …………17/09/2023…………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Niall Coughla
Student ID: 21121214

1 Implementation

1.1 Devices/Software Required

The following devices and software were used during the implementation of the solution for this research project:

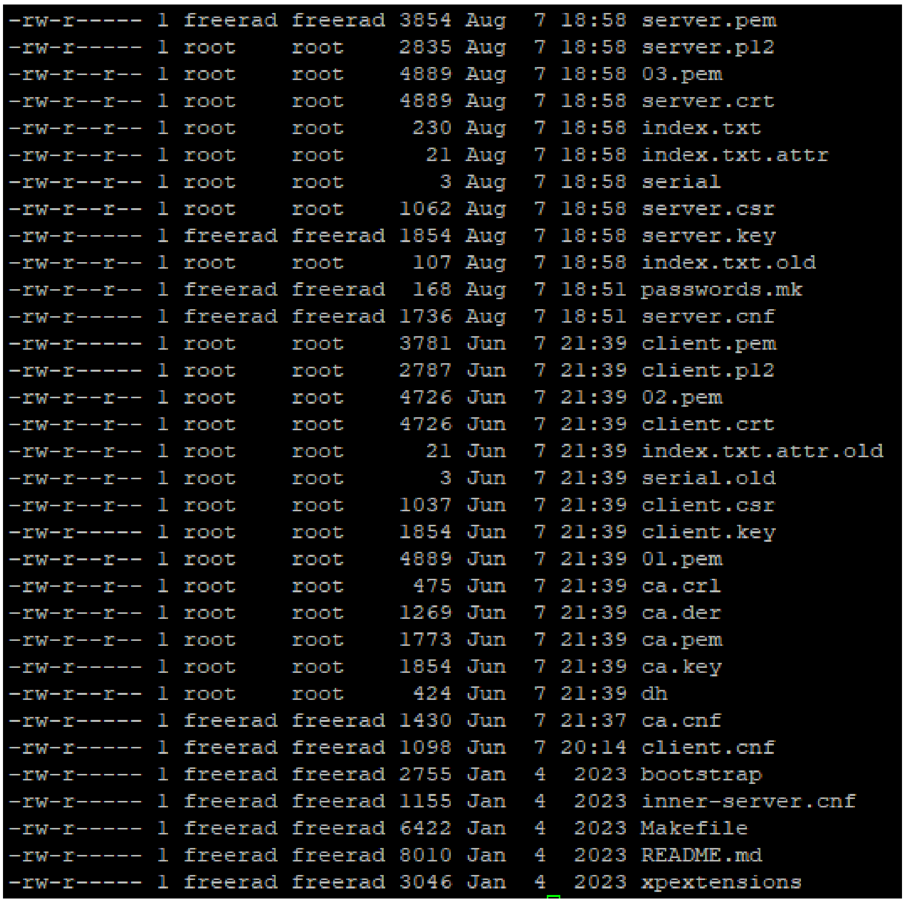
Name	Device	Required Software
RADIUS Server	Ubuntu 20.04 VM - 2 GB RAM - 2 vCPU - 20 GB disk space	- FreeRadius 3.0
Web Server	Windows 11 - 4 GB RAM - 4 CPU - 100 GB disk space	- Node.js 16.14.0 - WinRAR 6.22 - OpenSSL 1.1.1m - GitBash 2.35.1.windows.2
Access Point 1	Zyxel D2000 Modem	N/A
Access Point 2	Ubuntu 20.04 laptop with internet sharing capabilities - 2 GB RAM - 2 CPU - 20 GB disk space	- Hostapd 2.10 - Iptables 1.8.7 - UDHCPD 1.30.1

2 Configuration

Extract all files from zipped folder.

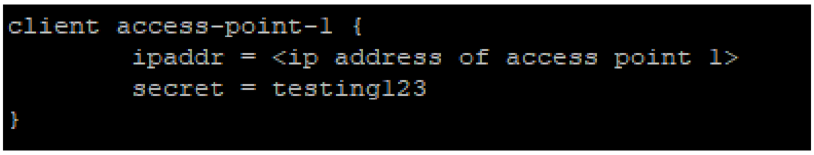
2.1 RADIUS Server

1. Deploy an Ubuntu 20.04 VM, ensuring it has network connectivity
2. Install FreeRadius 3.0 on the VM
3. With root access, navigate to the following folder:
   ```
   /etc/freeradius/3.0/certs
   ```
4. Copy the contents from the folder */certs* in the zipped folder, to this folder. Replace any files as required
5. Ensure that the permissions of the files have the owner set as **freerad** and **root, as below** (e.g., `chown freerad:freerad server.pem`*):*



```
-rw-r----- 1 freerad freerad 3854 Aug  7 18:58 server.pem
-rw-r----- 1 root    root    2835 Aug  7 18:58 server.p12
-rw-r--r-- 1 root    root    4889 Aug  7 18:58 03.pem
-rw-r--r-- 1 root    root    4889 Aug  7 18:58 server.crt
-rw-r--r-- 1 root    root     230 Aug  7 18:58 index.txt
-rw-r--r-- 1 root    root      21 Aug  7 18:58 index.txt.attr
-rw-r--r-- 1 root    root       3 Aug  7 18:58 serial
-rw-r--r-- 1 root    root    1062 Aug  7 18:58 server.csr
-rw-r----- 1 freerad freerad 1854 Aug  7 18:58 server.key
-rw-r--r-- 1 root    root     107 Aug  7 18:58 index.txt.old
-rw-r--r-- 1 freerad freerad  168 Aug  7 18:51 passwords.mk
-rw-r----- 1 freerad freerad 1736 Aug  7 18:51 server.cnf
-rw-r----- 1 root    root    3781 Jun  7 21:39 client.pem
-rw-r----- 1 root    root    2787 Jun  7 21:39 client.p12
-rw-r--r-- 1 root    root    4726 Jun  7 21:39 02.pem
-rw-r--r-- 1 root    root    4726 Jun  7 21:39 client.crt
-rw-r--r-- 1 root    root      21 Jun  7 21:39 index.txt.attr.old
-rw-r--r-- 1 root    root       3 Jun  7 21:39 serial.old
-rw-r--r-- 1 root    root    1037 Jun  7 21:39 client.csr
-rw-r----- 1 root    root    1854 Jun  7 21:39 client.key
-rw-r--r-- 1 root    root    4889 Jun  7 21:39 01.pem
-rw-r--r-- 1 root    root     475 Jun  7 21:39 ca.crl
-rw-r--r-- 1 root    root    1269 Jun  7 21:39 ca.der
-rw-r--r-- 1 root    root    1773 Jun  7 21:39 ca.pem
-rw-r----- 1 root    root    1854 Jun  7 21:39 ca.key
-rw-r--r-- 1 root    root     424 Jun  7 21:39 dh
-rw-r----- 1 freerad freerad 1430 Jun  7 21:37 ca.cnf
-rw-r----- 1 freerad freerad 1098 Jun  7 20:14 client.cnf
-rw-r----- 1 freerad freerad 2755 Jan  4  2023 bootstrap
-rw-r----- 1 freerad freerad 1155 Jan  4  2023 inner-server.cnf
-rw-r----- 1 freerad freerad 6422 Jan  4  2023 Makefile
-rw-r----- 1 freerad freerad 8010 Jan  4  2023 README.md
-rw-r----- 1 freerad freerad 3046 Jan  4  2023 xpextensions
```

6. Copy the file *eap* from the zipped folder, and replace the file at the following location, ensuring its permissions have the owner set to **freerad**:
   `/etc/freeradius/3.0/mods-available/eap`
7. Edit the following file:
   `/etc/freeradius/3.0/clients.conf`
8. Under the section **Define RADIUS clients**, add the following section to add **Access Point 1** as an authorized client for the RADIUS server:



```
client access-point-1 {
        ipaddr = <ip address of access point 1>
        secret = testing123
}
```

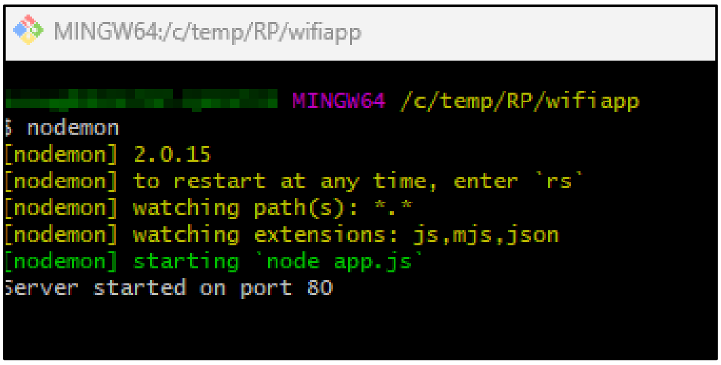
9. Restart FreeRadius to ensure changes take effect.

2.2 Web Server

1. Deploy Windows 11 machine (physical was used during implementation, but could be virtual)
2. Install required software
3. Copy all files from zipped folder to a directory on machine
4. Right-click the folder wifiapp, and select **Git Bash Here**. Type to following command to create a Node.js web project (press **Enter** to use the default values for each attribute when asked. Except for *entry point*, when *app.js* should be used:

```
1. npm init
```

5. Type the following commands to install required Node.js modules
   1. `npm install –save express pug path body-parser connect-flash express-session csurf cookie-parser node-cmd fs`
   2. `npm install -g bower`
   3. `bower install bootstrap`
   4. `bower install jquery`
6. Type the following command to start the web server:
   1. `nodemon`

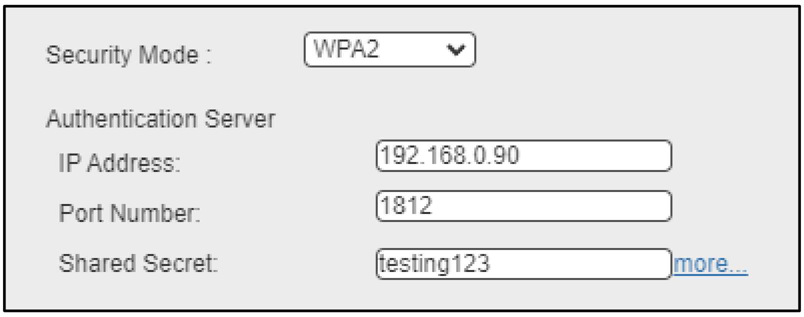


MINGW64:/c/temp/RP/wifiapp

```
[redacted] MINGW64 /c/temp/RP/wifiapp
$ nodemon
[nodemon] 2.0.15
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): *.*
[nodemon] watching extensions: js,mjs,json
[nodemon] starting `node app.js`
Server started on port 80
```

2.3 Access Point 1

1. Ensure the access point is connected to the same network as the RADIUS server
2. Configure the access point to use WPA encryption, and ensure the IP address is the same as for the RADIUS server:



Security Mode : WPA2

Authentication Server

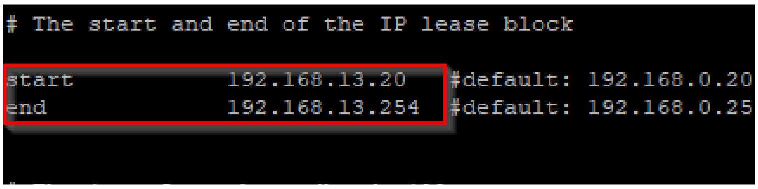
IP Address: 192.168.0.90

Port Number: 1812

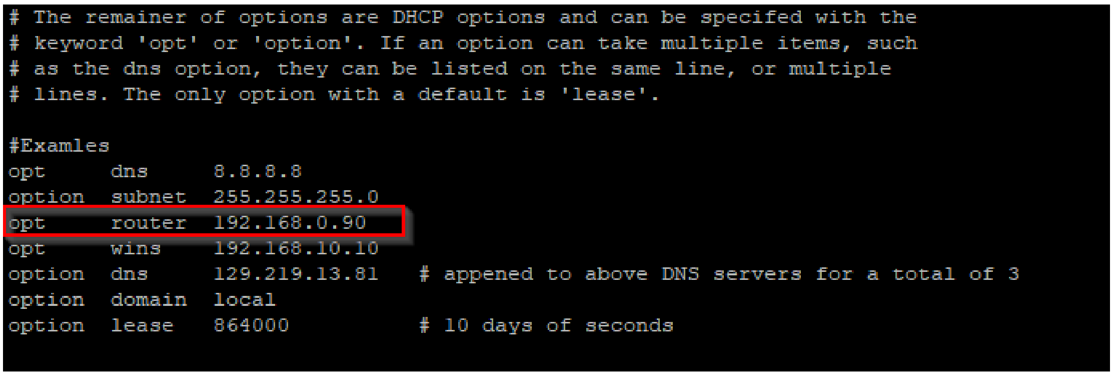
Shared Secret: testing123 more...

2.4 Access Point 2

1. Deploy Ubuntu machine to act as Access Point 2, install required software, and ensure it is connected to the same network as the Web server
2. Configure UDHCP to act as a DHCP server by editing the file at */etc/udhcpd.conf*, and adding the following configuration:



```
# The start and end of the IP lease block

start           192.168.13.20   #default: 192.168.0.20
end             192.168.13.254  #default: 192.168.0.25
```



```
# The remainer of options are DHCP options and can be specifed with the
# keyword 'opt' or 'option'. If an option can take multiple items, such
# as the dns option, they can be listed on the same line, or multiple
# lines. The only option with a default is 'lease'.

#Examles
opt     dns     8.8.8.8
option  subnet  255.255.255.0
opt     router  192.168.0.90
opt     wins    192.168.10.10
option  dns     129.219.13.81   # appened to above DNS servers for a total of 3
option  domain  local
option  lease   864000          # 10 days of seconds
```

Ensure the router address is the IP of the Ubuntu Access Point

3. Copy the file `hostapd_reg.conf` from the zipped folder to the Ubuntu Access Point, then run the following commands:

```
1. sudo iw phy phy0 interface add hotspot1 type __ap
2. sudo ifconfig hotspot1 192.168.13.2 up
3. sudo udhcpd -f
4. sudo hostapd <path to Hostapd conf
   file>/hostapd_reg.conf

*Run the following commands as root user*
5. echo "1" > /proc/sys/net/ipv4/ip_forward
6. iptables --table nat --append POSTROUTING --out-
interface wlp2s0 -j MASQUERADE
7. iptables -t nat -A PREROUTING -p tcp --dport 80 -
j DNAT --to-destination <IP address of Web
Server>:80
8. iptables -t nat -A PREROUTING -p tcp --dport 443
-j DNAT --to-destination <IP address of Web
Server>:80
```

Once this configuration has been setup, connect to RePro-WiFi-Registration, attempt to browse the internet, then following instructions to register and connect to RePro-WiFi using digital certificate authentication.

3 Evaluation

The following sections outline how to perform the evaluation methods used for assessing the security of Digital Certificate Authentication.

3.1 Devices/Software Required

Name	Device	Required Software
Attacking laptop	Linux Mint 21.1 laptop - 8 GB RAM - 4 vCPU - 10 GB disk space	- Aircrack-ng 1.6 (suite of tools which includes airmon-ng, Airodump-ng, and aireplay-ng) - Wireshark 3.6.2
Wireless Adapter	ASUS036NHA	- N/A

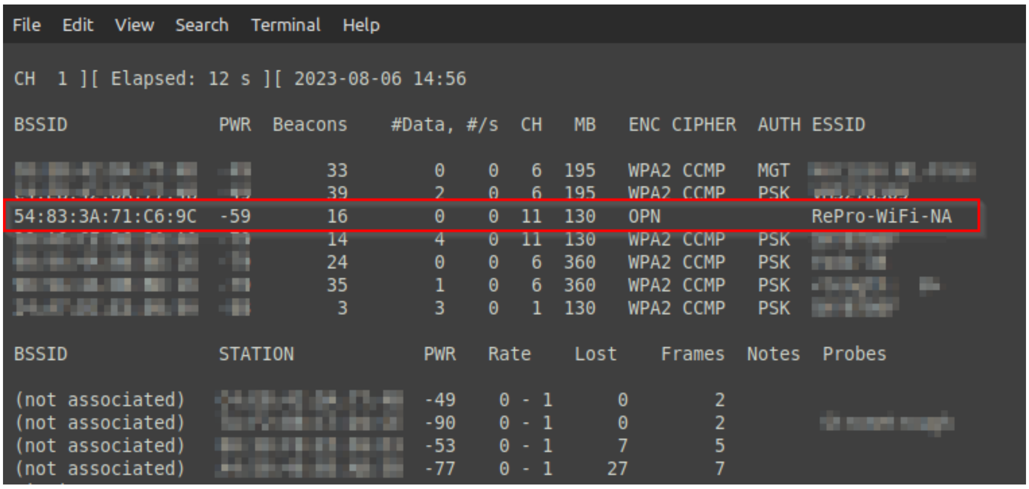
In addition to the wireless network configured above, configure 4 other wireless networks with the following security methods:

1. Unsecured (open Wi-Fi, no security method)
2. Captive Portal
3. WEP-PSK (any pre-shared key is suitable, as it is assumed the attacker will have access to it)
4. WPA2-PSK (any pre-shared key is suitable, as it is assumed the attacker will have access to it)

3.2 Testing

3.2.1 Network Eavesdropping

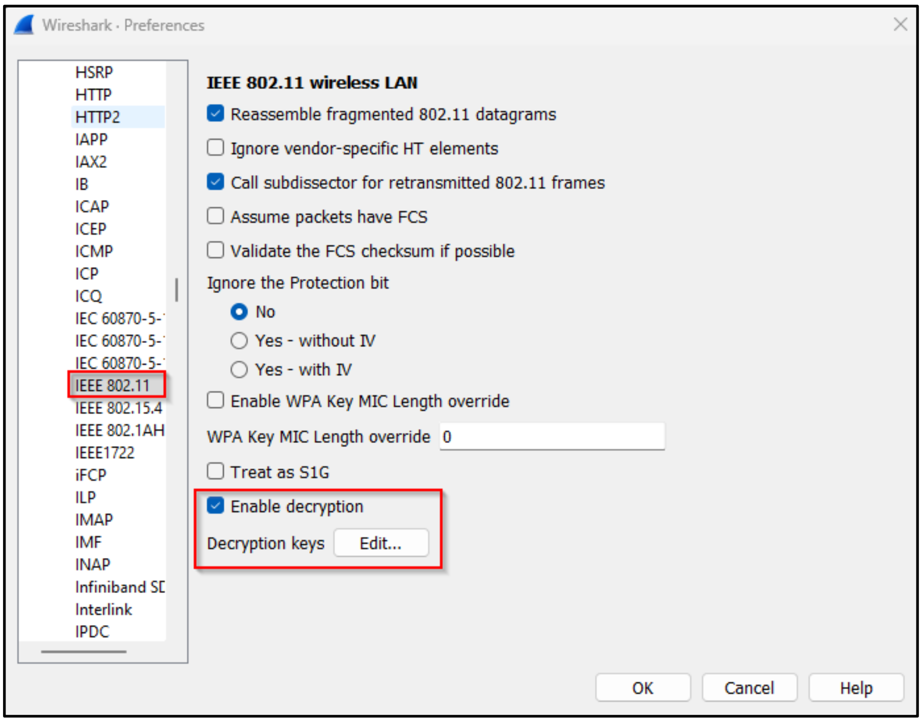
1. Configure the attacking laptop in monitoring mode, using Airmon-ng (some settings, such as interface names, may differ depending the device being used):
   1. `sudo airmon-ng check kill`
   2. `sudo airmon-ng start wlan0`
2. Run the following command to find the target network, identifying the **BSSID** and **Channel Number** of the network:
   1. `sudo airodump-ng wlan0mon`



```
CH  1 ][ Elapsed: 12 s ][ 2023-08-06 14:56

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

[redacted]                   33        0    0   6  195   WPA2 CCMP   MGT  [redacted]
[redacted]                   39        2    0   6  195   WPA2 CCMP   PSK  [redacted]
54:83:3A:71:C6:9C  -59       16        0    0  11  130   OPN              RePro-WiFi-NA
[redacted]                   14        4    0  11  130   WPA2 CCMP   PSK  [redacted]
[redacted]                   24        0    0   6  360   WPA2 CCMP   PSK  [redacted]
[redacted]                   35        1    0   6  360   WPA2 CCMP   PSK  [redacted]
[redacted]                    3        3    0   1  130   WPA2 CCMP   PSK  [redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   [redacted]         -49    0 - 1      0        2
(not associated)   [redacted]         -90    0 - 1      0        2          [redacted]
(not associated)   [redacted]         -53    0 - 1      7        5
(not associated)   [redacted]         -77    0 - 1     27        7
```

3. Start traffic capture using the following command:
   1. `sudo airodump-ng wlan0mon –bssid <BSSID> -c <Channel> -w capture`

4. Using Wireshark, open the traffic capture
   a. For WEP-PSK and WPA2-PSK protected networks, navigate to **Edit > Preferences > Protocols > 802.11n**
   b. Ensure **Enable Decryption** is selection, then select **Edit**



IEEE 802.11 wireless LAN

☑ Reassemble fragmented 802.11 datagrams

□ Ignore vendor-specific HT elements

☑ Call subdissector for retransmitted 802.11 frames

□ Assume packets have FCS

□ Validate the FCS checksum if possible

Ignore the Protection bit

● No

○ Yes - without IV

○ Yes - with IV

□ Enable WPA Key MIC Length override

WPA Key MIC Length override 0

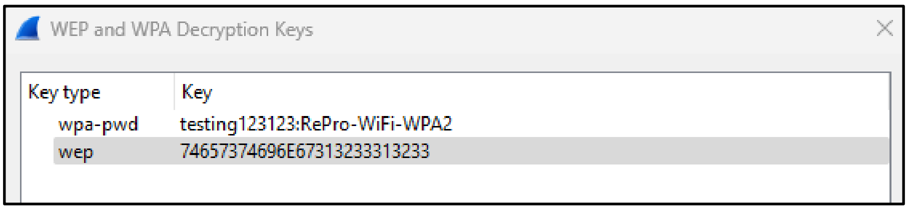
□ Treat as S1G

☑ Enable decryption

Decryption keys Edit...

c. Select the + symbol to add a new key

d. For WEP key, set **Key Type** to wep, then enter the PSK as hexadecimal. For WPA2 key, set **Key Type** to wpa-pwd, then enter as the format *<PSK>:<SSID>*



Key type	Key
wpa-pwd	testing123123:RePro-WiFi-WPA2
wep	74657374696E67313233313233

5. View captured traffic

3.2.2 2.2 Evil Twin

1. From the zipped folder, copy the folder **ET** to the attacking device
2. For each Hostapd configuration file, edit the SSID and PSK settings to match the SSID and PSK of the target network, as required
3. Repeat steps 1-6 from section 2.4 (Access Point 2 setup). However, use the Hostapd configuration file for the target network in step 4 (e.g., when replicating the WEP-PSK network, use the command `sudo hostapd <path to Hostapd conf file>/ET/hostapd_wep.conf`)
4. Force the target device off the target network by performing a deauthentication attack using Aireplay-ng:

```
1. sudo aireplay-ng --deauth 1000 -a <network BSSID> -c
   <Target MAC Address> wlan0
```

Network BSSID and Target MAC Address can be found during Eavesdropping attack, step 2 and 3.

5. Open Wireshark and begin capturing traffic on the hotspot1 interface to monitor traffic from target devices.