

HACKING WI-FI NETWORK

OBJECTIVE

The objective of this report to showcase the method of hacking using Offensive hacking tools present in Kali Linux operating system.

Wi-Fi is a family of wireless network protocols based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access, allowing nearby digital devices to exchange data by radio waves.

A “WiFi hack” is any technique used to gain unauthorized access to a WiFi network. Typically, this is done by exploiting security flaws or vulnerabilities, allowing the attacker to steal confidential information or disrupt the network's normal operations.

TOOLS

The tool that are required in this report are :

1. Fern Wi-Fi cracker
2. wifite
3. Kismet

METHODOLOGY

The steps involved in this report are:

1. Open kali Linux
2. Open Fern Wi-Fi cracker
3. Connect to Alpha adapter
4. Give the target IP address
5. Finally, after successful connection the password is displayed.

PROOF OF CONCEPT

```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Kali-Linux-2021.4a-vmwar... X

kali@kali:~$

[+] Scanning, Found 23 target(s), 10 client(s), Ctrl-C when ready
NUM ESSID CH ENCR POWER WPS? CLIENT
1 Rodas Note 8 6 WPA-P 7200 no
2 DIRECT-gpmcivamhmsv 11 WPA-P 6800 yes
3 Adm1 1 WPA-P 6800 no 1
4 Reinfosec_4g 11 WPA-P 5700 yes 7
5 DIRECT-89-HP Ink Tank ... 11 WPA-P 5600 yes 1
6 SPM98055_2_4G 13 WPA-P 3900 no
7 (E6:DA:DF:C6:F9:39) 13 WPA-P 3800 no
8 RMDLR 11 WPA-P 7400 yes 1
9 (FE:7A:5B:57:64:1A) 11 WPA-P 2400 yes
10 BlueSapling_SM_2_4GHz 18 WPA-P 2300 yes
11 Airtel_smba_3448 8 WPA-P 2300 no
12 (E2:68:F9:A1:12:39) 8 WPA-P 2300 no
13 SSID_24 6 WPA-P 2300 yes
14 OnePlus Nord 2T 5G 8 WPA-P 2300 no
15 OnePlus Nord 11 WPA-P 1900 no
16 (5E:42:8E:12:7F:67) 7 WPA-P 1900 no
17 Rakhsh 2 WPA-P 1700 yes 1
18 Asus ROG 1 WPA-P 1700 no 1
19 Perfomant 18 WPA-P 1500 no
20 Charliu 3 WPA-P 1200 no
21 SifySMC3_1947080803 8 WPA-P 1400 yes
22 (C2:86:C3:E4:57:98) 2 WPA-P 1000 no
23 All WPA-P 0 yes

[+] Scanning, Found 73 target(s), 17 client(s), Ctrl-C when ready
NUM ESSID CH ENCR POWER WPS? CLIENT
1 DIRECT-gpmcivamhmsv 11 WPA-P 6800 yes
2 Adm1 1 WPA-P 6800 no 1
3 DIRECT-89-HP Ink Tank ... 11 WPA-P 5600 yes 1
4 Reinfosec_4g 11 WPA-P 5700 yes 8
5 SPM98055_2_4G 13 WPA-P 3900 no
6 (E6:DA:DF:C6:F9:39) 13 WPA-P 3800 no
7 (FE:7A:5B:57:64:1A) 11 WPA-P 2400 yes
8 RMDLR 11 WPA-P 7400 yes 1
9 Airtel_smba_3448 8 WPA-P 2300 yes 1
10 Rakhsh 2 WPA-P 1700 yes 1
11 BlueSapling_SM_2_4GHz 18 WPA-P 2300 yes
12 (E2:68:F9:A1:12:39) 8 WPA-P 2300 no
13 SSID_24 6 WPA-P 2300 yes
14 Rodas Note 8 6 WPA-P 7200 no
15 OnePlus Nord 2T 5G 8 WPA-P 2300 no
16 OnePlus Nord 11 WPA-P 1900 no
17 (5E:42:8E:12:7F:67) 7 WPA-P 1900 no
18 SifySMC3_1947080803 8 WPA-P 1400 yes
19 Perfomant 18 WPA-P 1500 no
20 Asus ROG 1 WPA-P 1700 no 1
21 Charliu 3 WPA-P 1200 no
22 (C2:86:C3:E4:57:98) 2 WPA-P 1000 no
23 All WPA-P 0 yes

[+] select target(s) (1-23) separated by commas, dashes or all: 14

[+] Starting attacks against 2A:61:34:A3:CB:13 (Rodas Note 8)
[+] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcapngtool
[+] Rodas Note 8 (14) WPA handshake capture: Listening. (Clients: Rakhsh, timeout:300s)

84
```

```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Kali Linux 2021.4a vmwar... X

kali@kali:~$

[+] Scanning, Found 19 target(s), 9 client(s), Ctrl-C when ready
NUM ESSID CH ENCR POWER WPS? CLIENT
1 DIRECT-gpmcivamhmsv 11 WPA-P 6800 yes
2 DIRECT-89-HP Ink Tank ... 11 WPA-P 5600 yes
3 Adm1 1 WPA-P 6800 no 1
4 Reinfosec_4g 11 WPA-P 5700 yes 7
5 SPM98055_2_4G 13 WPA-P 3900 no
6 (E6:DA:DF:C6:F9:39) 13 WPA-P 3800 no
7 RMDLR 11 WPA-P 7400 yes 1
8 (FE:7A:5B:57:64:1A) 11 WPA-P 2400 yes
9 BlueSapling_SM_2_4GHz 18 WPA-P 2300 yes
10 Airtel_smba_3448 8 WPA-P 2300 no
11 (E2:68:F9:A1:12:39) 8 WPA-P 2300 no
12 SSID_24 6 WPA-P 2300 yes
13 Rakhsh 2 WPA-P 1700 yes 1
14 Charliu 3 WPA-P 1200 no
15 (E6:DA:DF:C6:F9:39) 13 WPA-P 3800 no
16 OnePlus Nord 2T 5G 8 WPA-P 2300 no
17 OnePlus Nord 11 WPA-P 1900 no
18 (5E:42:8E:12:7F:67) 7 WPA-P 1900 no
19 Perfomant 18 WPA-P 1500 no
20 Asus ROG 1 WPA-P 1700 no 1
21 Charliu 3 WPA-P 1200 no
22 (C2:86:C3:E4:57:98) 2 WPA-P 1000 no
23 All WPA-P 0 yes

[+] Scanning, Found 15 target(s), 9 client(s), Ctrl-C when ready
NUM ESSID CH ENCR POWER WPS? CLIENT
1 DIRECT-gpmcivamhmsv 11 WPA-P 6800 yes
2 DIRECT-89-HP Ink Tank ... 11 WPA-P 5600 yes
3 Adm1 1 WPA-P 6800 no 1
4 Reinfosec_4g 11 WPA-P 5700 yes 7
5 SPM98055_2_4G 13 WPA-P 3900 no
6 (E6:DA:DF:C6:F9:39) 13 WPA-P 3800 no
7 RMDLR 11 WPA-P 7400 yes 1
8 (FE:7A:5B:57:64:1A) 11 WPA-P 2400 yes
9 BlueSapling_SM_2_4GHz 18 WPA-P 2300 yes
10 Airtel_smba_3448 8 WPA-P 2300 no
11 (E2:68:F9:A1:12:39) 8 WPA-P 2300 no
12 SSID_24 6 WPA-P 2300 yes
13 Rakhsh 2 WPA-P 1700 yes 1
14 Charliu 3 WPA-P 1200 no
15 (E6:DA:DF:C6:F9:39) 13 WPA-P 3800 no
16 OnePlus Nord 2T 5G 8 WPA-P 2300 no
17 OnePlus Nord 11 WPA-P 1900 no
18 (5E:42:8E:12:7F:67) 7 WPA-P 1900 no
19 Perfomant 18 WPA-P 1500 no
20 Asus ROG 1 WPA-P 1700 no 1
21 Charliu 3 WPA-P 1200 no
22 (C2:86:C3:E4:57:98) 2 WPA-P 1000 no
23 All WPA-P 0 yes

[+] select target(s) (1-23) separated by commas, dashes or all: 3

[+] Starting attacks against 30:09:8A:D1:60:02 (Reinfosec_4g)
[+] Reinfosec_4g (550) WPA handshake [-] Timeout after 300 seconds
[+] Reinfosec_4g (550) WPA NULL PIN: [m00] Sending EAPOL (Timeout:1)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

CONCLUSION

In conclusion, unauthorized hacking of Wi-Fi networks poses significant risks to individuals, organizations, and the broader digital ecosystem, emphasizing the critical importance of robust security measures, ethical behavior, and responsible online practices to safeguard against potential threats and breaches of privacy.