جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
كلية علوم الحاسب وتقنية المعلومات
College of Computer Science and Information Technology

WIFI CRACKING PASSWORD

Wifi hacking is essentially cracking the security protocols in a wireless network, granting full access for the hacker to view, store, download, or abuse the wireless network. Usually, when someone hacks into a Wifi, they are able to observe the passwords and all the data that is being sent via the network.

THREATS [1]

PACKET SNIFFERS

A hacker can capture personal information such as credit card numbers and corporate email accounts by identifying, intercepting, and monitoring web traffic over unsecured Wi-Fi networks.

LOG-IN CREDENTIAL VULNERABILITY

Weak and predictable passwords lead to log-in credential Vulnerability.

NETWORK SNOOPING

Network snooping is an attack, which happens when a hacker uses malicious software on an unsecured wi-fi network to remotely monitor the activity on a third-party's laptop.

COUNTERMEASURE [2]

- Use WPA/WPA2 Encryption
- Turn off SSID Broadcasting
- Enable MAC Address Filtering
- Change Default Admin Credentials

FUNCTIONALITY

When you run the code, it will first display a list of WiFi networks near to you, and ask which one you want to crack the password for. Then you will insert a dictionary brute force file that will look for up to 400 passwords and will crack successfully.

SIMILAR TOOLS

1 AIRCRACK-NG [3]

Aircrack is a tool for WEP/WPA/WPA2 cracking. Aircrack-ng includes tools for capturing packets, de-authenticating connected clients, and generating traffic, as well as tools for brute force and dictionary attacks. It's in Kali Linux by default.

COMMANDS

SETTING UP MADWIFI-NG

```
airmon-ng start ‹wifi name›
```

START AIRODUMP-NG TO COLLECT AUTHENTICATION HANDSHAKE

```
sudo airodump-ng -c ‹channel number› --bssid ‹AP BSSID› ‹network interface›
-w ‹path for saved packets file›
```

USE AIREPLAY-NG TO DEAUTHENTICATE THE WIRELESS CLIENT

```
sudo aireplay-ng -a ‹BSSID of the AP› --deauth ‹time› ‹network interface›
```

RUN AIRCRACK-NG TO CRACK THE PRE-SHARED KEY

```
sudo aircrack-ng ‹captured file with .cap› -w ‹path to wordlist›
```

2 WIFITE [4]

Wifite is a Python script intended to make wireless security auditing simpler. It is made to function with the ParrotSec and Kali Linux distributions of Linux.

COMMANDS

TO SEE ALL OPTIONS ON THE HELP MENU

```
sudo wifite -h
```

USE MENTIONED WORDLIST FOR CRACKING HANDSHAKE FILE.

```
sudo wifite --dict /location/of/wordlist.txt
```

COMPARSION

AIRCRACK	WIFITE
is a complete suite of tools to access Wi-Fi network security	uses currently available wireless hacking tools
Aircrack output is simple	Wifite has a detailed output
Aircrack identified the password(key)	Identified the password, type of encryption, AP name, and saved the result to cracked.txt

Prepared by:
Maryam AlBugaey Sara AlSubaie
Fatima Abujaid Lulwah Aldowihi Juri Alaqeel

RESOURCES

[1] Western Governors University, "Risks of using public wi-fi networks for businesses," Western Governors University, 21-Dec-2021. [Online]. Available: https://www.wgu.edu/blog/7-dangers-public-wifi-businesses2112.html. [Accessed: 09-Feb-2023].
[2] D. Morelo, "Open-source framework for publishing content," NetSpot, 25-Jan-2023. [Online]. Available: https://www.netspotapp.com/blog/wifi-security/7-ways-to-stop-a-wifi-hacker.html. [Accessed: 09-Feb-2023].
[3] "Aircrack-ng," cracking_wpa [Aircrack-ng]. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=cracking_wpa. [Accessed: 09-Feb-2023].
[4] Svt, "(step by step) WIFITE - WIFI Hacking & Penetration Testing Tool," (Step by Step) WIFITE - WiFi Hacking & Penetration Testing Tool, 13-May-2022. [Online]. Available: https://www.hackershousenepal.com/2020/12/wifite-wifi-wireless-hacking-tutorial-pentest-guide.html. [Accessed: 09-Feb-2023].