

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

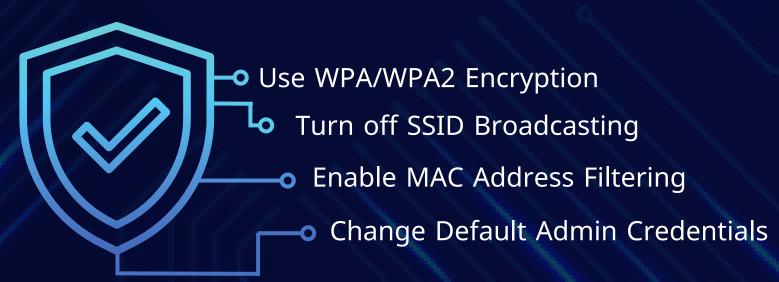
Weak and predictable passwords lead to log-in credential Vulnerability.

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]



Prepared by:

Maryam AlBugaey Sara AlSubaie Fatima Abujaid Lulwah Aldow

Lulwah Aldowihi Juri Alaqeel

RESOURCES

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



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.

SETTING UP MADWIFI-NG

airmon-ng start (wifi name)

•···· COMMANDS

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>



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.

TO SEE ALL OPTIONS ON THE HELP MENU

sudo wifite –h

• COMMANDS

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