REPORT

Attack Wifi

Group Member:

Zyad AL-Bshry 443006946

Faris AL-Lahibi 443003119

What is Attack Wifi?

Attack Wi-Fi networks:

Wi-Fi networks are vulnerable to various types of attacks aimed at compromising the security and integrity of the network. These attacks can lead to unauthorized access, data theft, or disruption of network services. WiFi attack is a topic that has received significant attention in recent years. Kali Linux, a popular operating system for penetration testing and ethical attacks, offers a set of tools and techniques that can be used to evaluate the security of wireless networks. However, it is important to note that hacking into someone else's WiFi network without permission is illegal and unethical.

some common types of attacks on Wi-Fi networks:

1- **Evil Twin Attack**
2- **Man-in-the-Middle (MitM) Attack**
3- **Denial-of-Service (DoS) Attack**
4- **KRACK Attack**

The tools we used to attack:

1- Kali Linux

Introduction

Kali Linux is an advanced penetration testing Linux distribution that is widely used for penetration testing, ethical hacking, and network security assessments
. It is a Debian-based operating system that comes with a large number of pre-installed tools essential for security professionals, ethical hackers, and cybersecurity researchers.

Features and benefits:

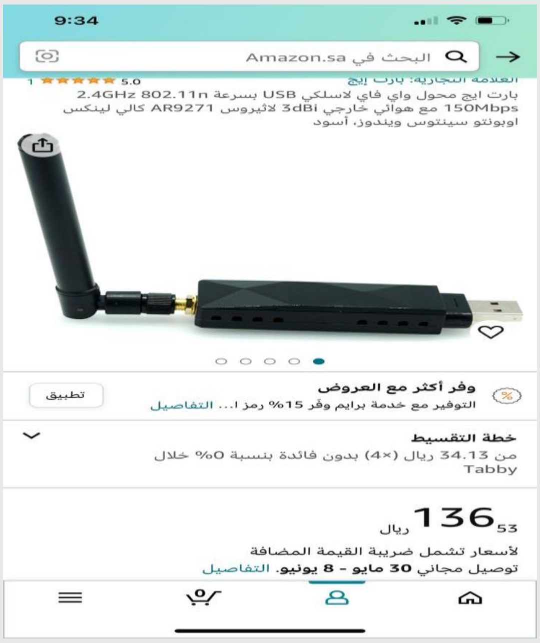
-Optimized for Penetration Testing: Kali Linux is optimized to reduce the amount of work required to set up and configure penetration testing tools. This allows professionals to quickly get started on their security assessments.

-Kali Linux can be installed on various platforms, including mobile devices, containers, ARM devices, cloud providers, the Windows subsystem of Linux, pre-built virtual machines, and more.

Note: that Kali Linux should only be used for legal and ethical purposes, and it is strictly prohibited to use it for any malicious activities.

2- USB wireless wifi adapter

Key Features It is a powerful tool that offers a wide range of features specially designed for WiFi penetration testing and ethical hacking.



9:34

البحث في Amazon.sa

العلامة التجارية: بارت إيج

5.0 1

بارت ايج محول واي فاي لاسلكي USB بسرعة 2.4GHz 802.11n
150Mbps مع هوائي خارجي 3dBi لاثيروس AR9271 كالي لينكس
اوبونتو سينتوس ويندوز، أسود

وفر أكثر مع العروض

التوفير مع خدمة برايم وفّر 15% رمز ا... التفاصيل

تطبيق

خطة التقسيط

من 34.13 ريال (4×) بدون فائدة بنسبة 0% خلال
Tabby

136 53 ريال

لأسعار تشمل ضريبة القيمة المضافة

توصيل مجاني 30 مايو - 8 يونيو. التفاصيل

STEPS FOR ATTACK:

1- **Airmon-ng:**is a tool in Kali Linux that allows users to put their wireless network interface cards into monitor mode, enabling them to capture network packets without connecting or authenticating with an access point. It is part of the Aircrack-ng suite, used for auditing and testing wireless network security, and is useful for tasks such as network analysis, penetration testing, and security auditing.

2- **Airodump-ng:** is used to analyze network traffic, identify connected devices, and obtain basic information such as encryption keys and handshakes required to breach network security.

Features and Usage

Here are some key features and usage instructions for Airodump-ng:

Packet Capture: Airodump-ng allows you to capture raw 802.11 frames from wireless networks.

Channel Selection: You can make Airodump-ng capture on specific channels or bands using command-line options such as `--channel` or `--band`.

3- **Aireplay-ng:** is a tool in the Aircrack-ng suite that is used for injecting and replaying network frames. It is primarily used for generating traffic on wireless networks and performing specific attacks to test network security.

Features and Usage:

Deauthentication Attacks: Aireplay-ng can be used to perform deauthentication attacks on wireless clients, forcing them to disconnect from the network and potentially capturing handshake data.

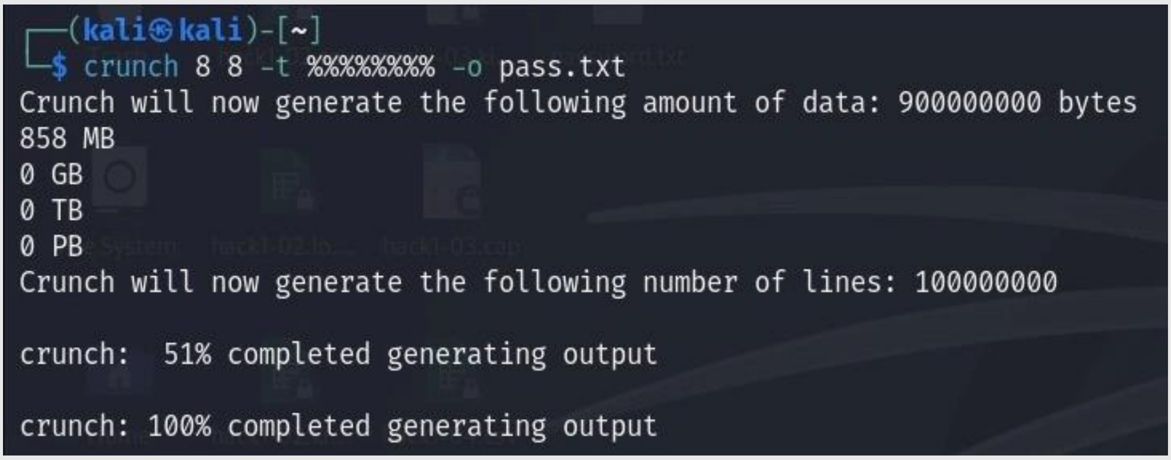
Fake Authentication: Aireplay-ng supports fake authentication attacks, where it authenticates to a network access point to create and capture new IVs.

4- **Aircrack-ng :**is a comprehensive suite of tools used for assessing the security of WiFi networks. It focuses on various aspects of WiFi security, including packet sniffing, network detection, and cracking encryption keys for WEP and WPA/WPA2-PSK networks.
-These tools, along with others in the suite, are primarily command-line based and are available for Linux, Windows, macOS, FreeBSD, OpenBSD, NetBSD, Solaris, and eComStation 2.

It's important to note that Aircrack-ng is a powerful tool that should only be used for ethical purposes, such as network auditing and security testing. Unauthorized use of these tools is illegal and unethical

5- **Crunch:** is a powerful wordlist generation tool that comes pre-installed with Kali Linux. It is commonly used in WiFi attacks to create custom wordlists for password cracking. By generating wordlists with different combinations of characters, Crunch increases the chances of finding the correct password or passphrase for a target WiFi network.

EXAMPLE

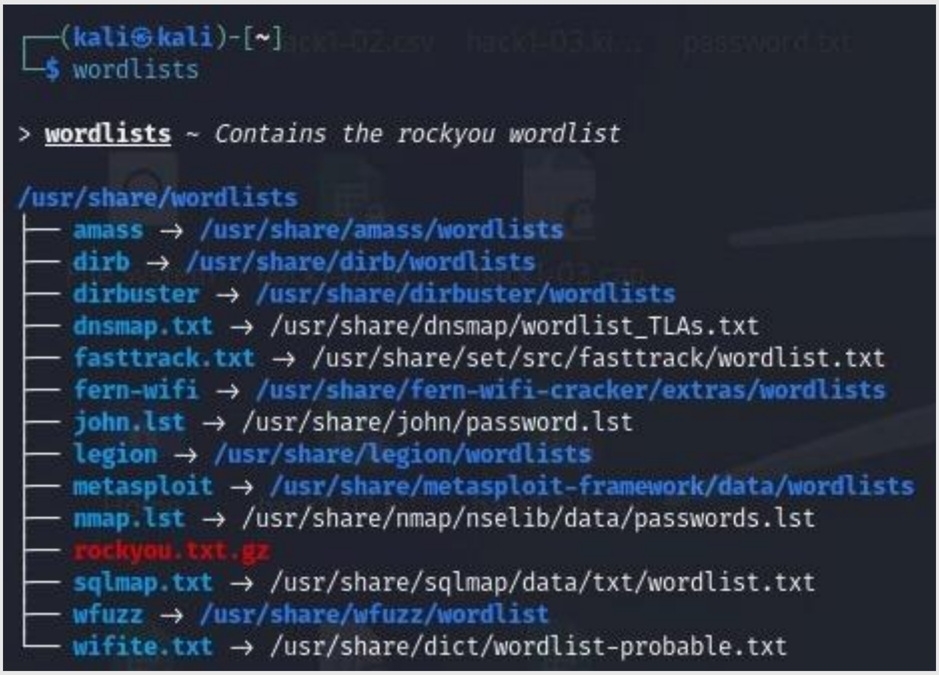


```
┌──(kali㉿kali)-[~]
└─$ crunch 8 8 -t %%%%%%%% -o pass.txt
Crunch will now generate the following amount of data: 900000000 bytes
858 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000000

crunch:  51% completed generating output

crunch: 100% completed generating output
```

We have two ways to create symbol lists:

1- **Wordlist** A wordlist is a collection of words, phrases, or passwords that are used in dictionary attacks to guess or crack passwords. These wordlists contain commonly used passwords, dictionary words, and variations of words that are likely to be used as passwords. Wordlists are an essential tool in Wi-Fi attacks as they allow attackers to automate the process of guessing passwords by trying different combinations from the wordlist.

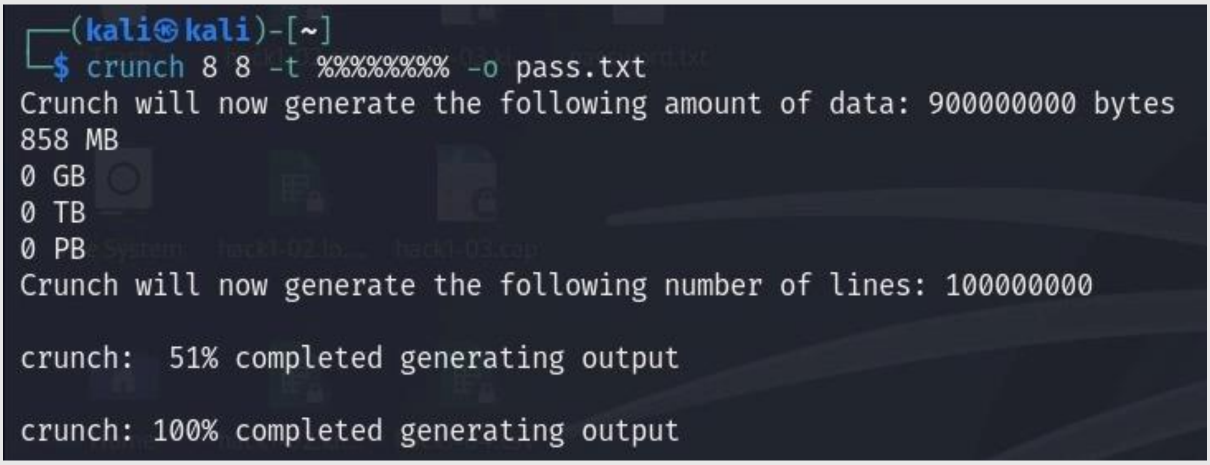
EXAMPL



```
┌──(kali㉿kali)-[~]
└─$ wordlists

> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists
├── amass → /usr/share/amass/wordlists
├── dirb → /usr/share/dirb/wordlists
├── dirbuster → /usr/share/dirbuster/wordlists
├── dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
├── john.lst → /usr/share/john/password.lst
├── legion → /usr/share/legion/wordlists
├── metasploit → /usr/share/metasploit-framework/data/wordlists
├── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
├── rockyou.txt.gz
├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt
```

2- **Crunch:** is a powerful wordlist generation tool that comes pre-installed with Kali Linux. It is commonly used in WiFi attacks to create custom wordlists for password cracking. By generating wordlists with different combinations of characters, Crunch increases the chances of finding the correct password or passphrase for a target WiFi network.

EXAMPL



```
┌──(kali㉿kali)-[~]
└─$ crunch 8 8 -t %%%%%%%% -o pass.txt
Crunch will now generate the following amount of data: 900000000 bytes
858 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000000

crunch:  51% completed generating output

crunch: 100% completed generating output
```

CONCLUSION

In conclusion, wifi hacking is a serious and illegal act that can have severe consequences. Whether for personal gain or malicious intent, unauthorized access to someone else's wifi network is a violation of privacy and can lead to theft of sensitive information. It is important for individuals and businesses to take steps to secure their networks and protect themselves from potential attacks. By using strong passwords, keeping software updated, and being cautious of suspicious activity, we can help prevent wifi hacking incidents and maintain a safer online environment. Remember, respect others' privacy and always seek permission before attempting to access any wifi network.