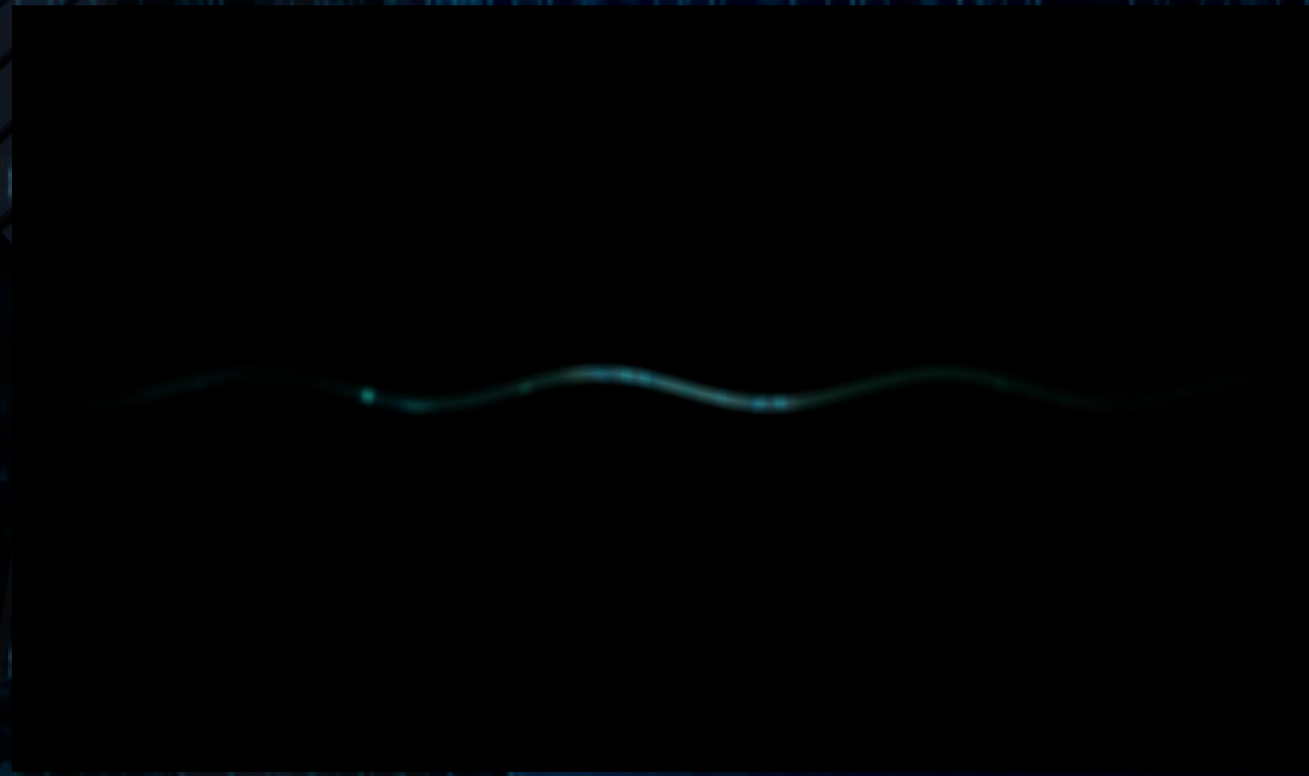

Ĥ@¢K!πG/¢R@CK!NG
PRESENTED BY
SIGMA BOYS

TEAM

Gangajit Singar
Papu Chaudhary
Pratik Shrestha
Ritik Yadav
Sunil Rai



AGENDA OF TODAY

- What is Hacking/Cracking?
- Difference between hacking and cracking
- Objective of Hacking
- Hacking as a cyber crime/cyber security.
- Types of hackers
- Why do hacker hacks?
- Need of Programming knowledge to become hacker?
- Generally used programming language for hacking.
- Tools/software used by Hackers.
- Operating Systems of Hackers.
- Mode of hacking attacks
- Types of Hacking attack
  - Spoofing
  - Session Hijacking
  - DOS Attack
  - Password Attack
  - Phishing Attack
  - Cookies Theft
  - SQL injection Attack
- Conclusion
- Extra Gyan (If time Favours)

WHAT IS HACKING & CRACKING?

A hacking is expolring methods for breaching defenses and exploiting weaknesses in a computer system or network

Cracking is a technique used to breach computer software or an entire computer security system, and with malicious intent.

DIFFERENCE BETWEEN HACKING AND CRACKING

Hacking

- A hacking is expolring methods for breaching defenses and exploiting weaknesses in a computer system or network
- May Constructive

Cracking

- Cracking is a technique used to breach computer software or an entire computer security system, and with malicious intent
- Mostly Destructive

OBJECTIVE OF HACKING

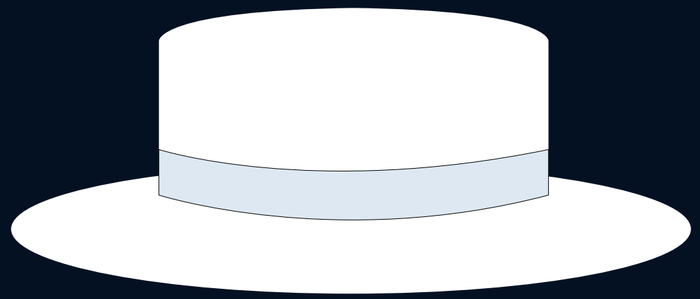
Cyber Securities

Protecting the System /data
Making the System Secure

Cyber Crimes

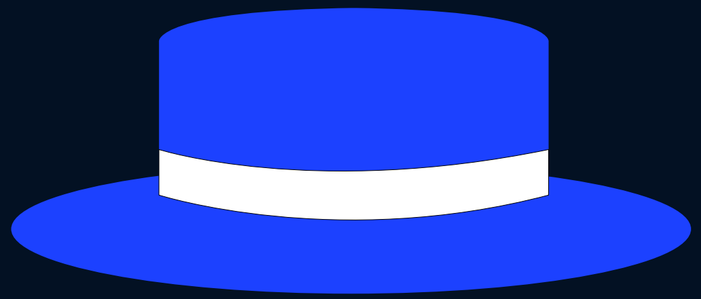
Destruction of data /system.

TYPES OF HACKERS



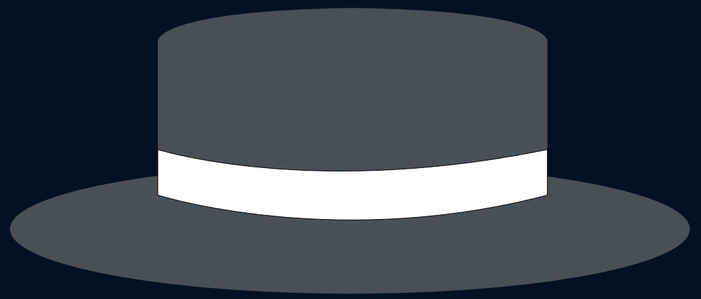
White Hat
Authorized Hackers

Help businesses prevent cybersecurity attacks



Blue Hat
Authorized Software Hackers

To identify vulnerabilities in new organizational software before it's released



Black Hat
Criminal Hackers

To get profit from data breaches

WHY DO HACKERS HACKS?

- Steal/Leak Information
- Vulnerability Scanning
- Just for fun
- Show off
- Curosity
- Theft for financial gain
- Revenge, boredom, challenge etc

DO WE NEED NEED TO KNOW PROGRAMMING TO BECOME HACKER?

No/Yes

Learning programming is not that compulsory for hacking, Hackers don't need to learn programing. Anyway, learning programming can help hackers to make more customized tools, understand the developers and become more compitative.

GENERALLY USED PROGRAMMING LANGUAGE USED FOR HACKING

Python

Python is a general-purpose programming language and used extensively for exploit writing in the field of hacking. It plays a vital role in writing hacking scripts, exploits, and malicious programs.

PHP

: Hypertext Preprocessor or PHP is a server-side programming language used to build websites. Understanding PHP will help hackers understand web hacking techniques better.

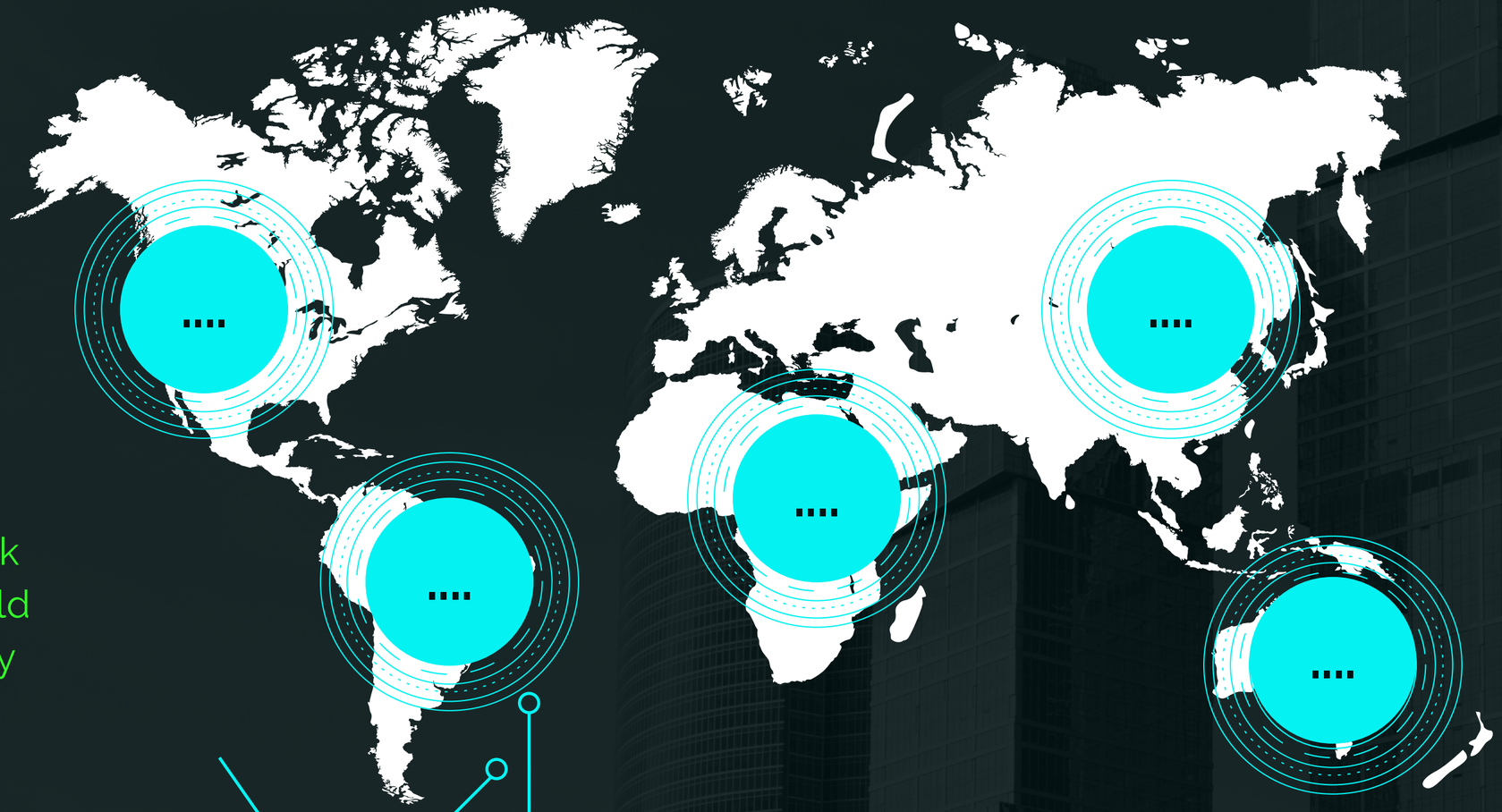
Javascript

Currently, JavaScript is one of the best programming languages for hacking web applications. Understanding JavaScript allows hackers to discover vulnerabilities and carry web exploitation since most of the applications on the web use JavaScript or its libraries.

Shell

Using a shell script is most useful for repetitive tasks that may be time consuming to execute by typing one line at a time.

Interesting Website:



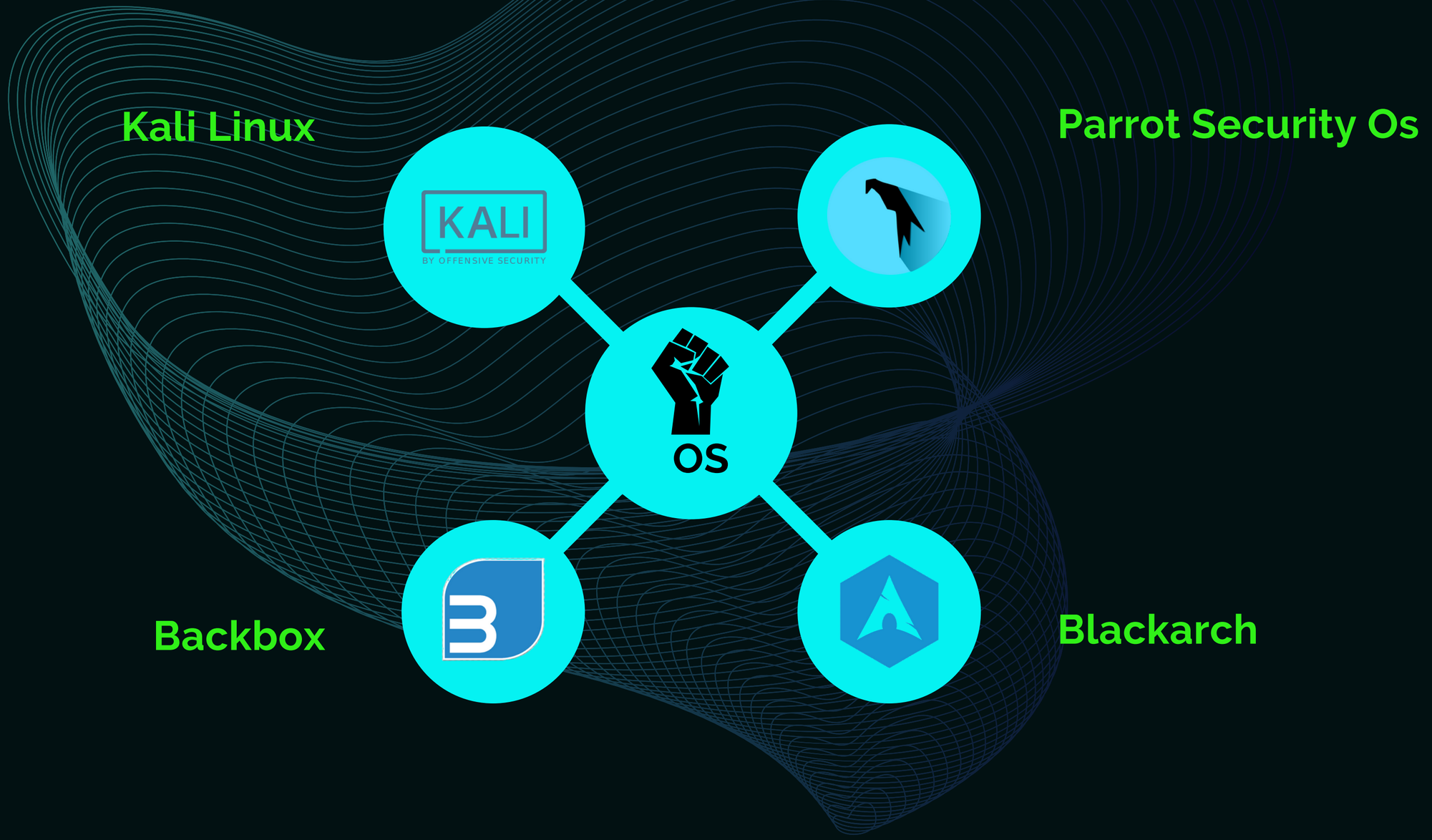
You can see live hacking attack going in different parts of World with the help of one of the very trusted website by Kaspersky.

View hacking Maps

MODE OF HACKING

- Over LAN
- Over the Internet
- Locally
- Offline
- Theft etc.

OPERATING SYSTEM USED FOR HACKING



CONCEPT OF ENCRYPTION AND DECRYPTION

#thisISMyP@$$Word

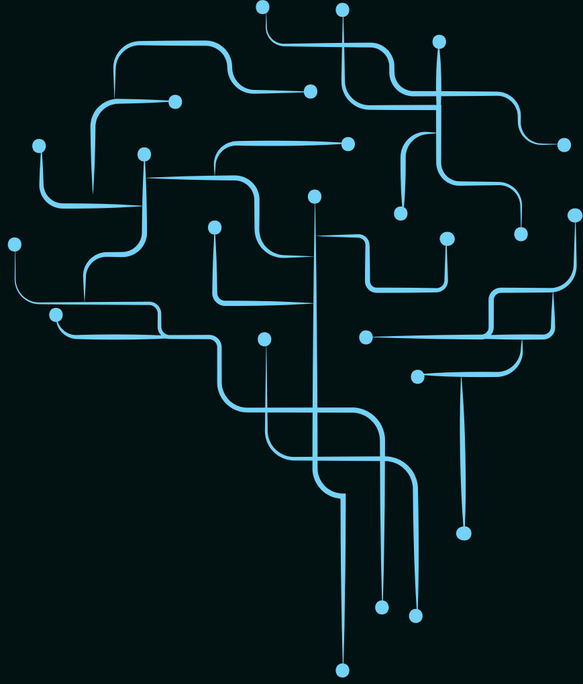
Encryption
Type: DES

1WXpgt517$j8MtQKbC
3FmHPcGl1EDaW1

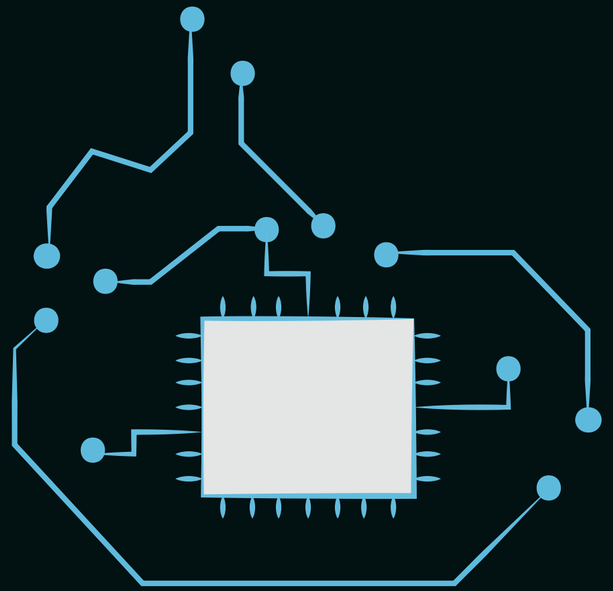
Encryption is the process by which a readable message is converted to an unreadable form to prevent unauthorized parties from reading it.

Decryption is a process that transforms encrypted information into its original form.

TYPES OF HACKING



- Spoofing
- Session Hijacking
- DOS/DDOS Attack
- Password Attack
- Phishing Attack
- Cookies Theft
- SQL injection Attack
- Keylogging etc.



SPOOFING

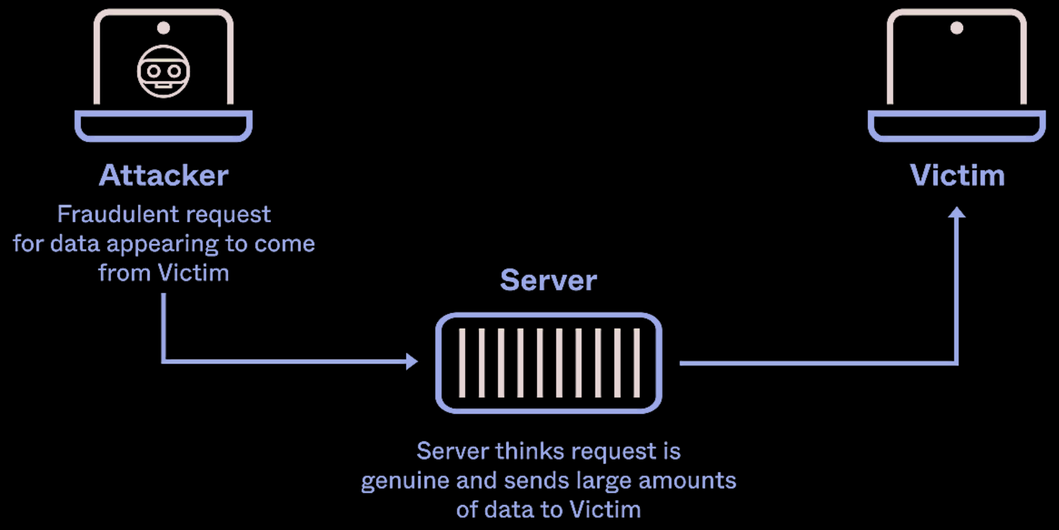
Spoofing is a specific type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity.

Types of Spoofing :

- IP Spoofing
- Web Spoofing
- Email Spoofing
- Call Spoofing etc.

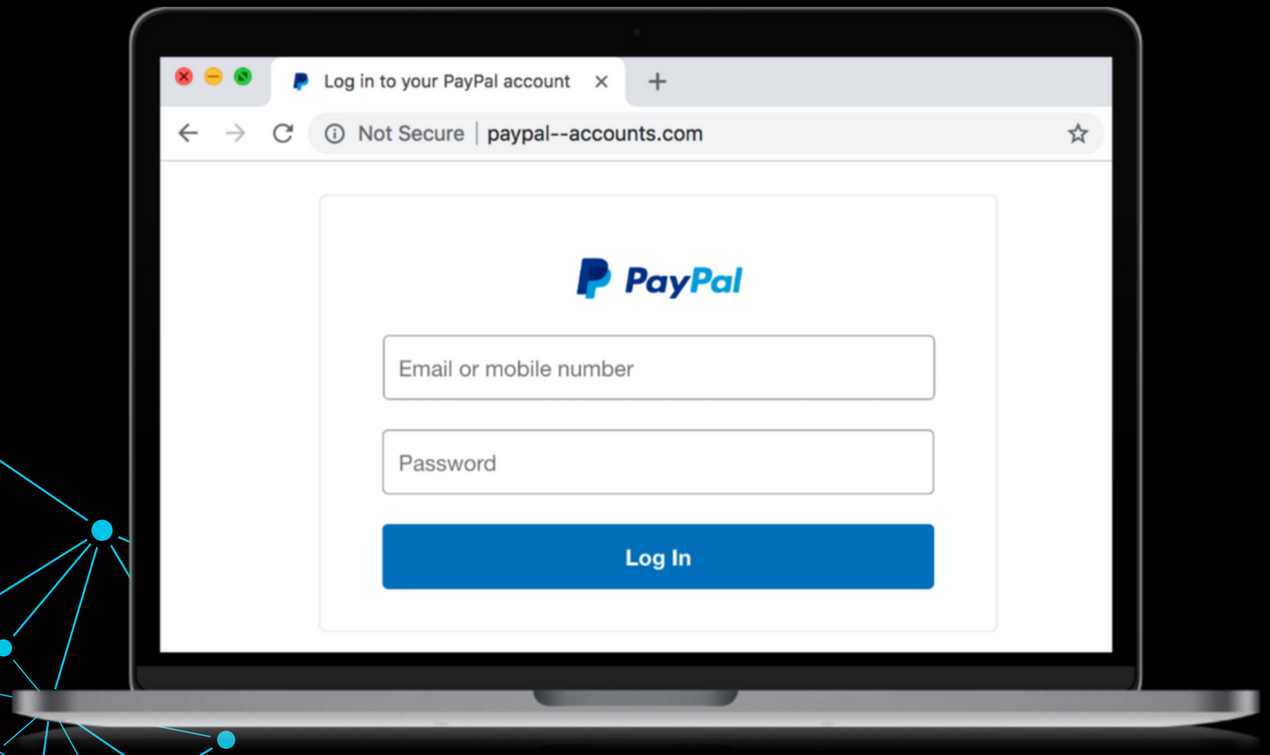
IP SPOOFING

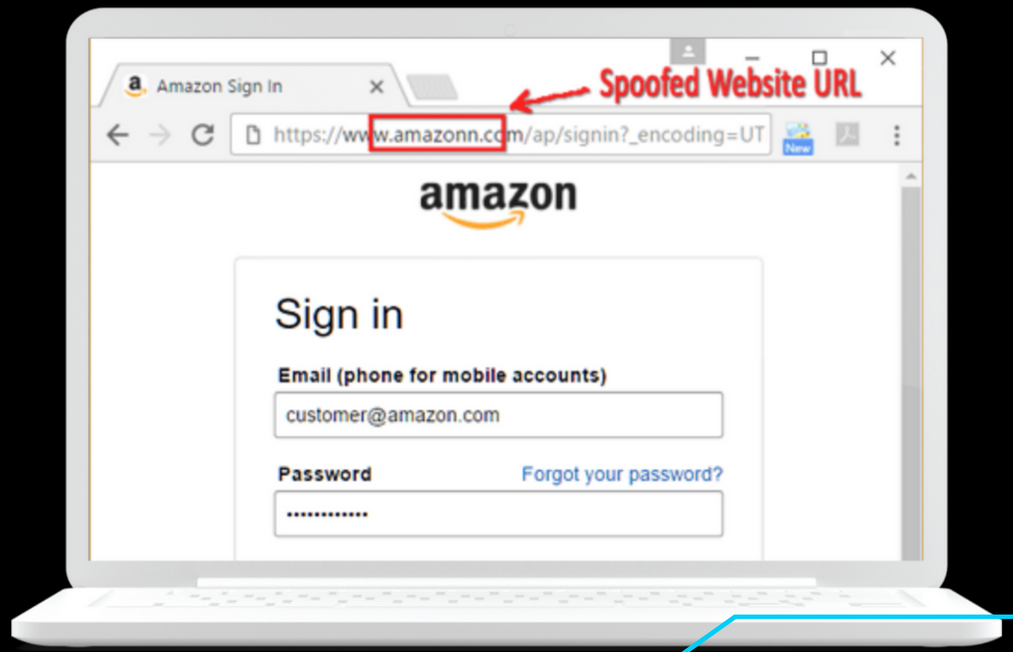
IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.



WEB SPOOFING

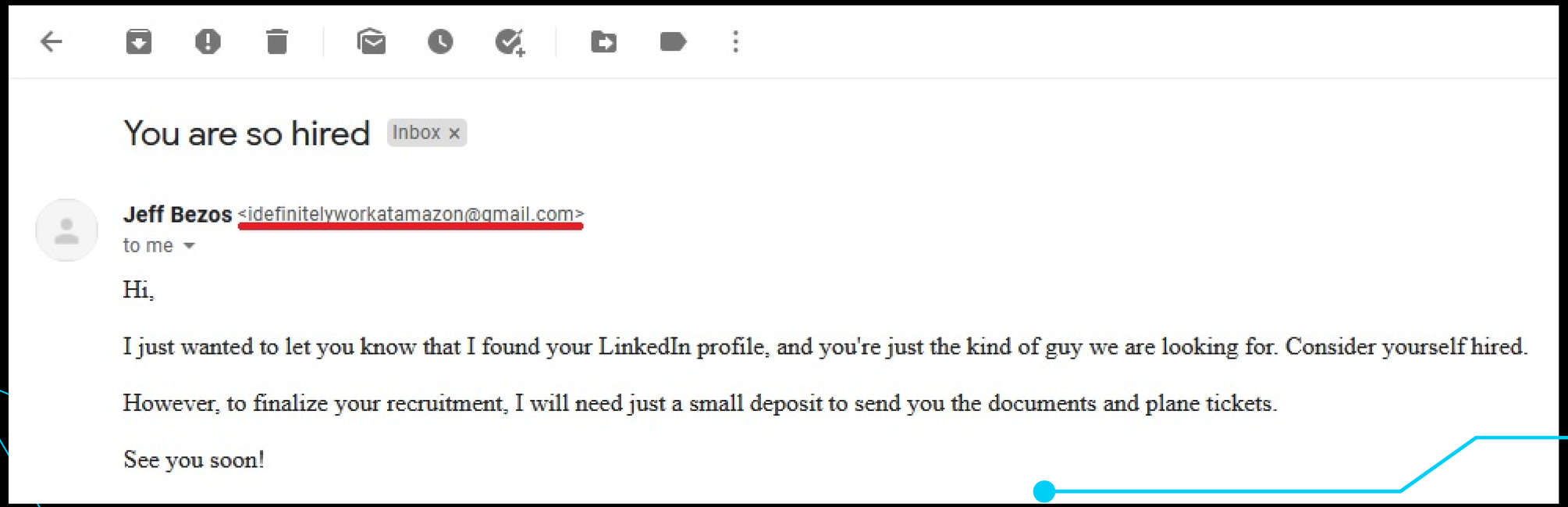
Website spoofing is the creation of a replica of a trusted site with the intention of misleading visitors to a phishing site. Legitimate logos, fonts, colors and functionality are used to make the spoofed site look realistic.





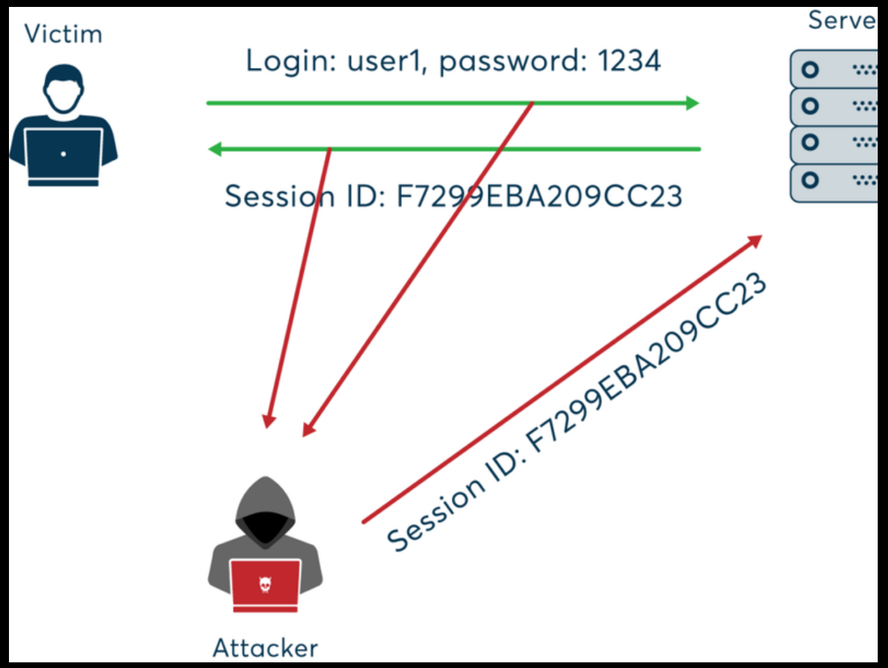
EMAIL SPOOFING

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust.



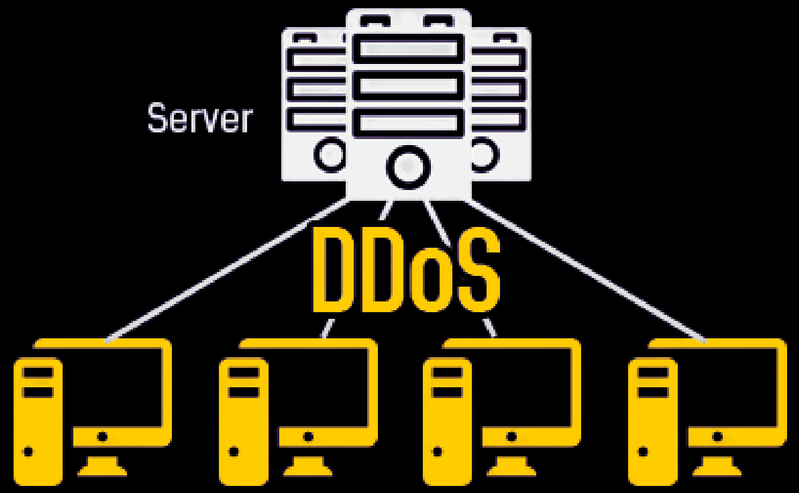
SESSION HIJACKING

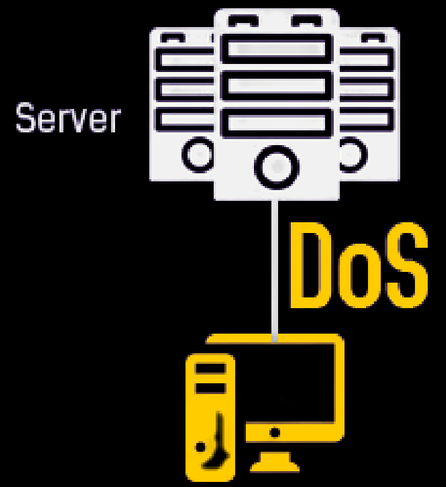
Session hijacking, also known as TCP session hijacking, is a method of taking over a web user session by surreptitiously obtaining the session ID and masquerading as the authorized user.



DOS/DDOS ATTACK

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.





PASSWORD ATTACK

A password attack refers to any of the various methods used to maliciously authenticate into password-protected accounts. These attacks are typically facilitated through the use of software that expedites cracking or guessing passwords.

Types of Password Attack :

- Dictionary Attack
- Bruteforce attack
- Hybrid

DICTIONARY ATTACK

A dictionary attack is a method of breaking into a password-protected computer, network or other IT resource by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

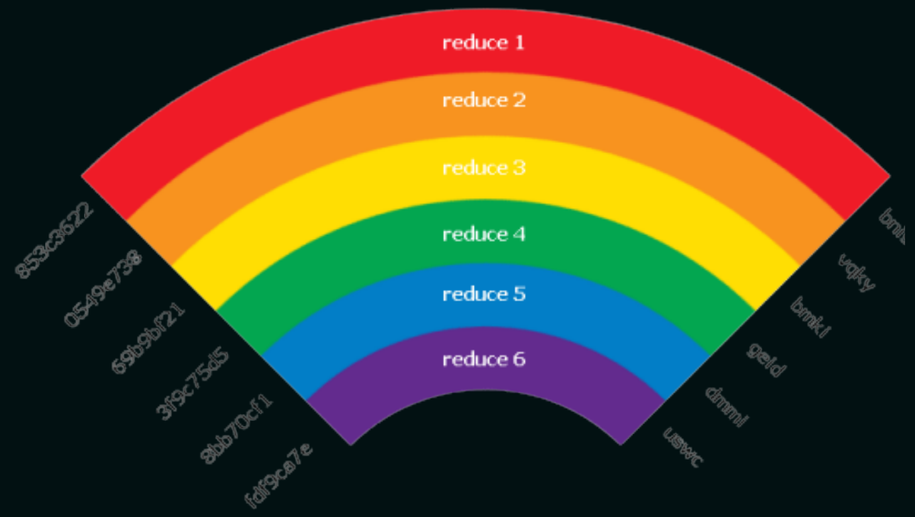
BRUTEFORCE ATTACK

A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered. The longer the password, the more combinations that will need to be tested.

HYBRID ATTACK

A common method utilized by users to change passwords is to add a number or symbol to the end. A hybrid attack works like a dictionary attack, but adds simple numbers or symbols to the password attempt.

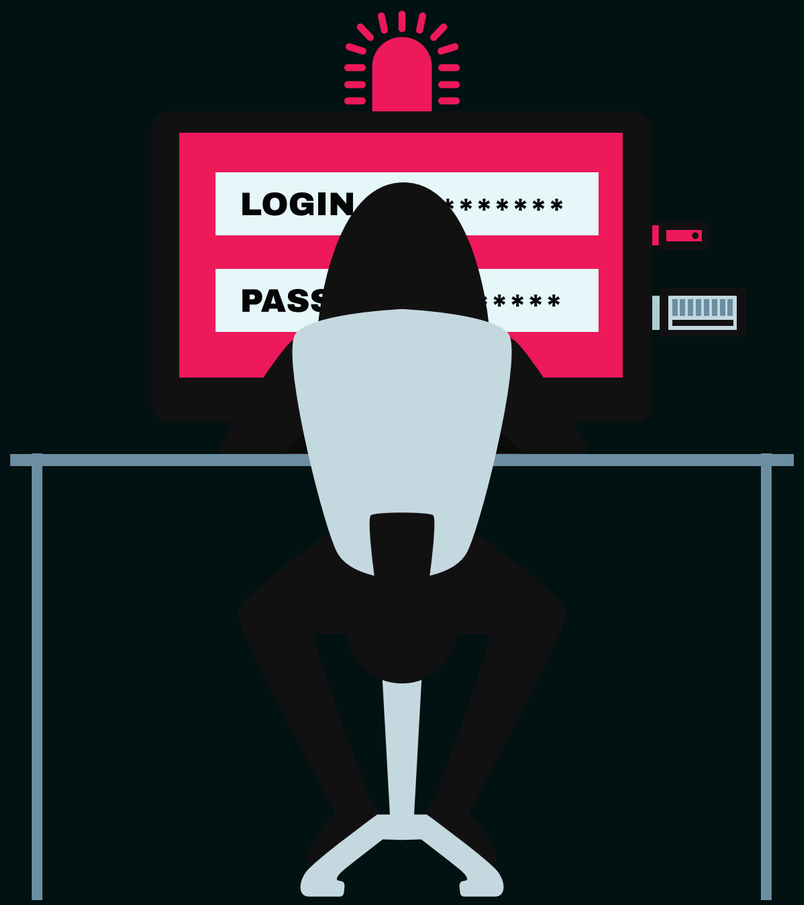
RAINBOW TABLE ATTACK



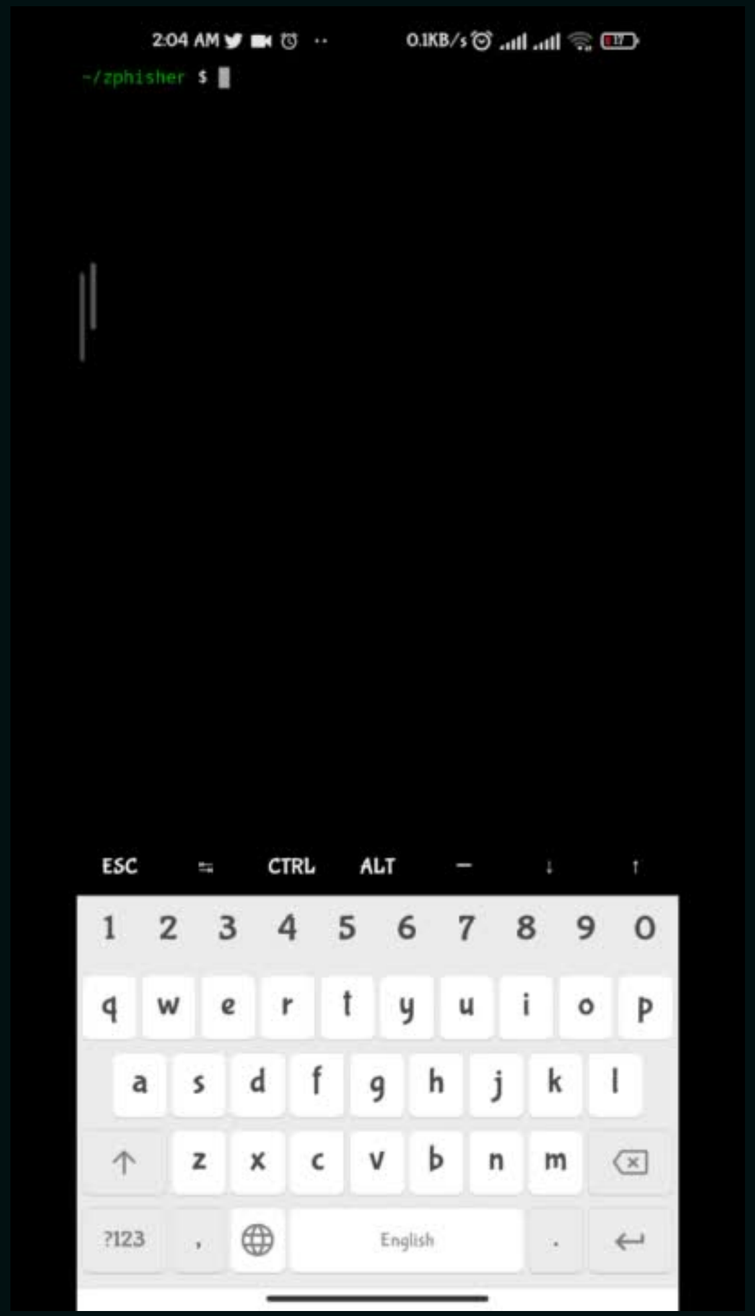
A rainbow table attack is a password cracking method that uses a special table (a “rainbow table”) to crack the password hashes in a database. Applications don’t store passwords in plaintext, but instead encrypt passwords using hashes. After the user enters their password to login, it is converted to hashes, and the result is compared with the stored hashes on the server to look for a match. If they match, the user is authenticated and able to login to the application.

PHISHING ATTACK

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.




Phishing Attack

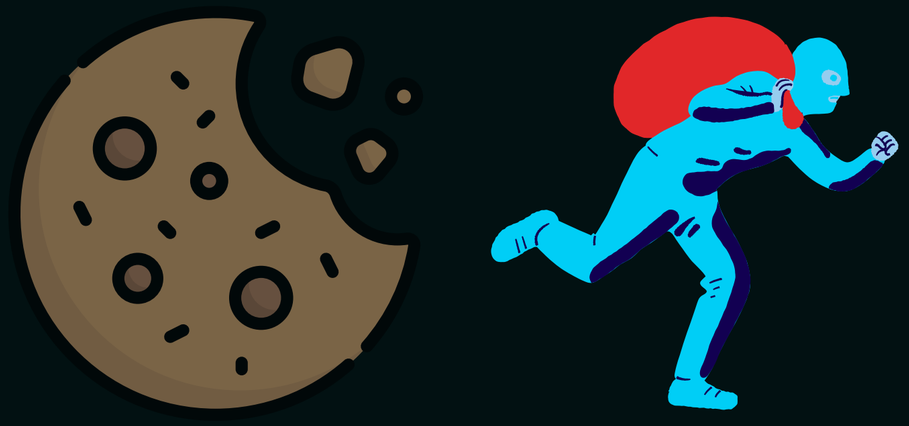


PHISHING ATTACK

App name : Termux
Hacking Tool name: Zphisher
Device : Android

Command Used:
Git clone <repo link> --- This Command fetches tool/repo from github
cd zphisher --- Moved to zphisher folder
bash zphisher.sh --- To open and perform operation with zphisher.sh file
No. to choose the platform --- For selection of phishing Site
No. choose the page type --- To get types of page of selected website
No. host the Website with --- To host the Website from local machine to internet
you will get two link for phishing attack. send link to the targeted person and convince him open the link and fill the login credintials.
If he login to our phishing website. tada...
His/her will be will be hacked.

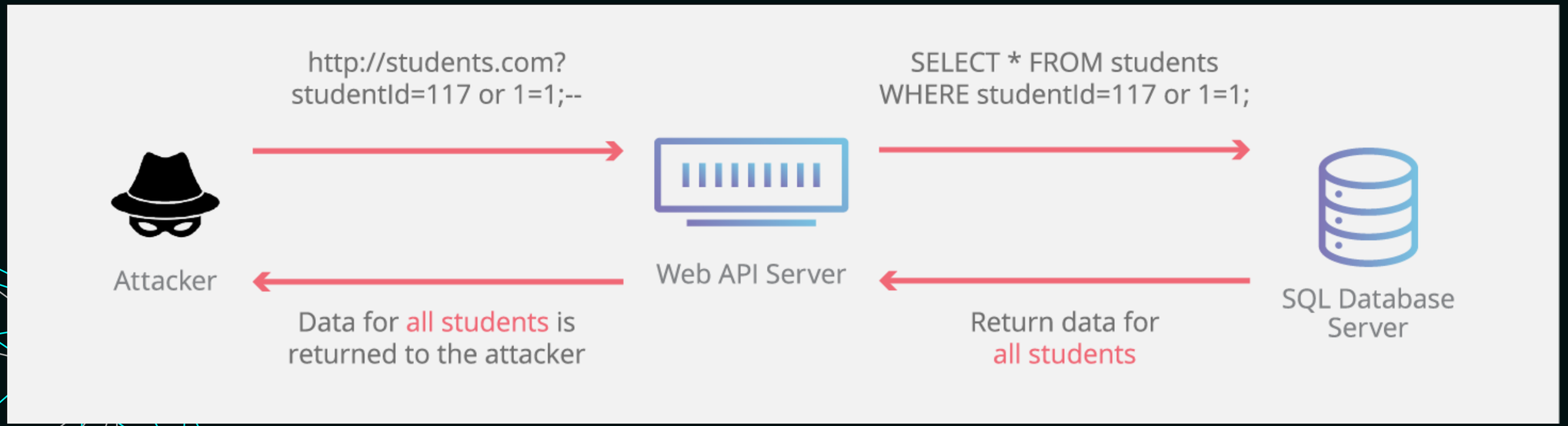
COOKIES THEFT



Cookie theft, also known as the “pass-the-cookie attack,” is a session hijacking tactic that gives an attacker access to user accounts which have stored session cookies in the browser. It occurs when hackers steal the victim's session ID and spoof the person's cookie over the same network.

SQL INJECTION ATTACK

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access.



TOP TOOLS RELATED TO HACKING

Metasploit

Wireshark

Nikto

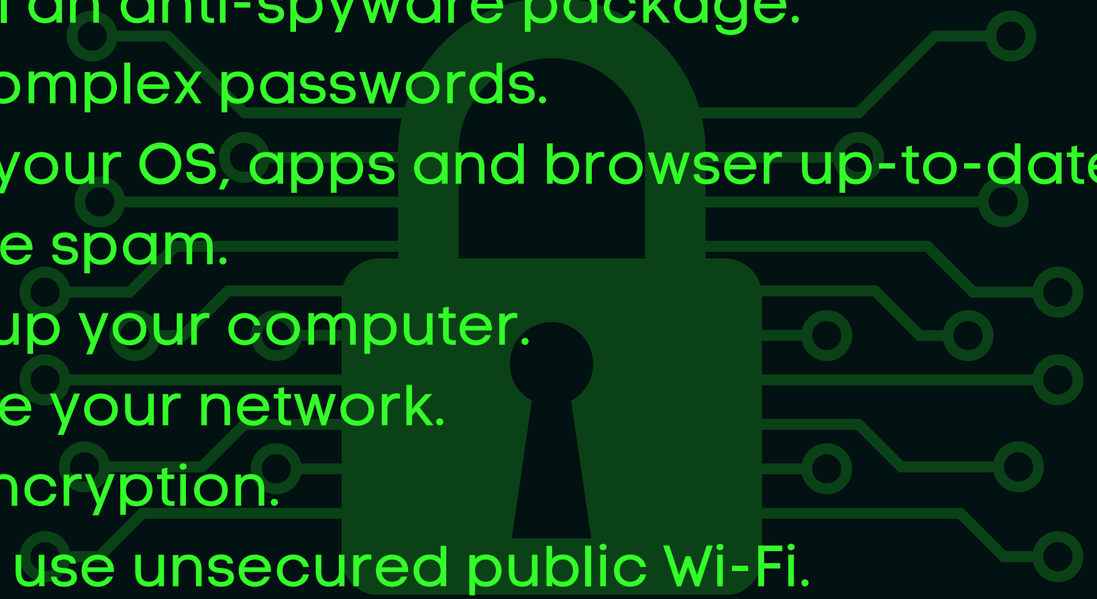
Nmap

Acunetix

TERMINOLOGY

Backdoor
Malware
Ransomware
Reverse Shell
Tor Network
Carding
Payload
Spyware
Shell
Zero-Day Attack

WAYS TO REMAIN SECURE AND AVOID BEING HACKED



1. Use a firewall.
2. Install antivirus software.
3. Install an anti-spyware package.
4. Use complex passwords.
5. Keep your OS, apps and browser up-to-date.
6. Ignore spam.
7. Back up your computer.
8. Secure your network.
9. Use encryption.
10. Don't use unsecured public Wi-Fi.
11. Turn off Bluetooth.
12. Clear your browsing history.
13. Be Unpridictable

What is Cyber Security?

Cyber Security study programmes teach you how to protect computer operating systems, networks, and data from cyber attacks. You'll learn how to monitor systems and mitigate threats when they happen. This is an oversimplification of IT security degrees' curricula. Each module will have a certain focus, but the overall goal is to help you develop the computing skills needed to prevent attacks and protect people's data and privacy.

•

CAREERS IN HACKING

What's the duration of Cyber Security degrees?

- Bachelor's degrees in Cyber Security take 3 or 4 years in most countries.
- Master's courses in Cyber Security take between 1-2 years to complete.
- PhD programmes in Cyber Security last 3-5 years. Some only take 1 or 2 years, but they are less common.

Printf("Thank You");