INTRODUCTION TO ETHICAL HACKING

- Ethical hacking means the act of locating weaknesses and vulnerabilities of computer or any information system by duplicating the intention and actions of malicious hackers.

- Companies that work online are at a greater risk of hacking.

- The primary goal of ethical hacking is to identify and solve vulnerabilities in a system before they can be exploited by malicious hackers.

- Ethical hackers have to compromise their computer systems.

For hacking to be considered ethical, the hacker must obey the following rules:

1. Expressed (often written) permission to explore the network.
2. You respect the individuals or company's privacy.
3. You close out your work, not leaving anything open for you or someone else to exploit at a later time.
4. You let the software developer or hardware manufacturer know of any security vulnerabilities you locate in their software or hardware, if not already known by the company.

Need for ethical hacking:

- In the past, companies seemed to operate under the mind-set that 'locking the doors' was the best way to protect their systems.

- But with changing technology and techniques, they realised this is not enough.

- Ethical hacking offers an objective analysis of an organisations' information security posture

- Hackers must scan for weaknesses, test entry points, prioritize targets, and develop a plan that best suits their organization.

Scope and Limitations of Ethical Hacking:

. Ethical hackers must know the penalties for unauthorized system hacking.
. Hacking activities require legal permission through a signed document from the target organization before initiating a network-penetration test.

. should use their skills wisely, understanding the results of misuse.
. The depth and breadth of testing are determined by the client's needs and concerns.

The ethical hacker must follow certain rules to ensure that all ethical and moral obligations are met.

- Gain authorisation from the client and have a signed contract giving the ethical hacker permission to perform the test.
- Maintain and follow a Non-Disclosure Agreement (NDA) with the client in the case of confidential information disclosed during the test.
- Maintain confidentiality when performing the test. Information gathered may contain sensitive information. No information about the test or company confidential data should ever be disclosed to a third party.

Skills required to be an Ethical Hacker

Diverse set of skills is required to understand and secure computer systems, networks, and data.

1. Basic Computer Skills:
   1. Understanding the fundamentals of how computers function.
   2. Proficiency in using the command line in Windows and configuring networking parameters.
   3. Familiarity with MS Office programs, spreadsheets, email, database management, social media, and web applications.
2. Networking Skills:
   1. Knowledge of computer networks and how devices (hosts) communicate.
   2. Ability to identify and handle threats within a network.

3. Linux Skills:

- Familiarity with the Linux operating system, which is commonly used by hackers.

4. Wireshark: Wireshark is a tool that helps you inspect and analyze the traffic on a computer network. It's like a detective tool for computer networks.

- Imagine the data that travels between your computer and the internet is like a series of letters being sent and received. Wireshark lets you open and read those letters to understand what's happening on the network.

(MUST BE ABLE TO READ AND CAPTURE DATA PACKETS)

- **5. Programming Skills: Programming Skills are another most crucial skill to become an ethical hacker. Python, PHP, Java, ruby, C, C++, and JavaScript etc**

- **6. Virtualization: It means the making of the virtual version of something like operating system, server, and storage device or network resources. It helps in testing the hack that is going to take place before making your hack go live. It also helps to check and revise the hacks before making it go live**

- **7. Database : how data is preserved, how data is accessed.**

- **8. Web Applications: you use on the Internet through your Web Browser.**
- **web applications have also become a prime target of the hackers**
- **You must understand the functioning of web applications and the databases backing them**

- 9. Cryptography: is the practice and study of techniques used to secure communication and protect information from unauthorized access. It involves the use of mathematical algorithms to transform information (plain text) into an unreadable format (cipher text) and back again. The primary goal of cryptography is to ensure the confidentiality, integrity, and authenticity of data.

What are the three main types of hackers?

- Hackers fall into three general categories: black hat hackers, white hat hackers, and gray hat hackers.

- Although hackers are often related with exploiting vulnerabilities to gain unauthorized access to computers, systems, or networks, not all hacking is malicious or illegal.

- In its purest sense, hacking is simply the using computer skills to solve a particular problem.

- There are many different types of hackers, and a lot of hacking activities are beneficial, because they solve programming weaknesses that help developers improve software products

Black hat hackers

- **Black hat hackers are cybercriminals that illegally crack systems with malicious intent. Seeking to gain unauthorized access to computer systems**

- **Once a black hat hacker finds security vulnerability, they try to exploit it, often by implanting a virus or other type of malware such as a trojan.**

- **Ransomware attacks are a common tactic used by malicious hackers to demand money.**

White hat hackers

White hat hackers are ethical security hackers who identify and fix vulnerabilities.

Hacking into systems with the permission of the organizations

white hat hackers try to uncover system weaknesses in order to fix them and help strengthen a system’s overall security.

Many cyber security leaders started out as white hat hackers, but the vital role played by ethical hacking is still widely misunderstood

Gray hat hackers

Gray hat hackers are not necessarily bad like black hat hackers, but they still enter computer systems without permission.

However, instead of causing harm, they find and reveal weaknesses in the system.

When they discover new vulnerabilities, they tell the owner about it instead of exploiting it fully.

However, sometimes they may ask for money to share all the details about what they found.

What’s the difference between white, black, and gray hat hackers?

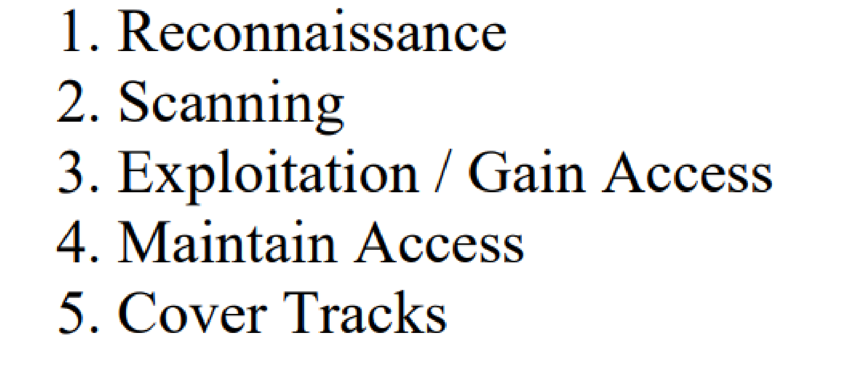
- **The main difference between white, black, and gray hat hackers is the motivation or intent that each type of hacker has when they break into computer systems.**

- **White hat hackers find cyber security weaknesses to help organizations develop stronger security.**

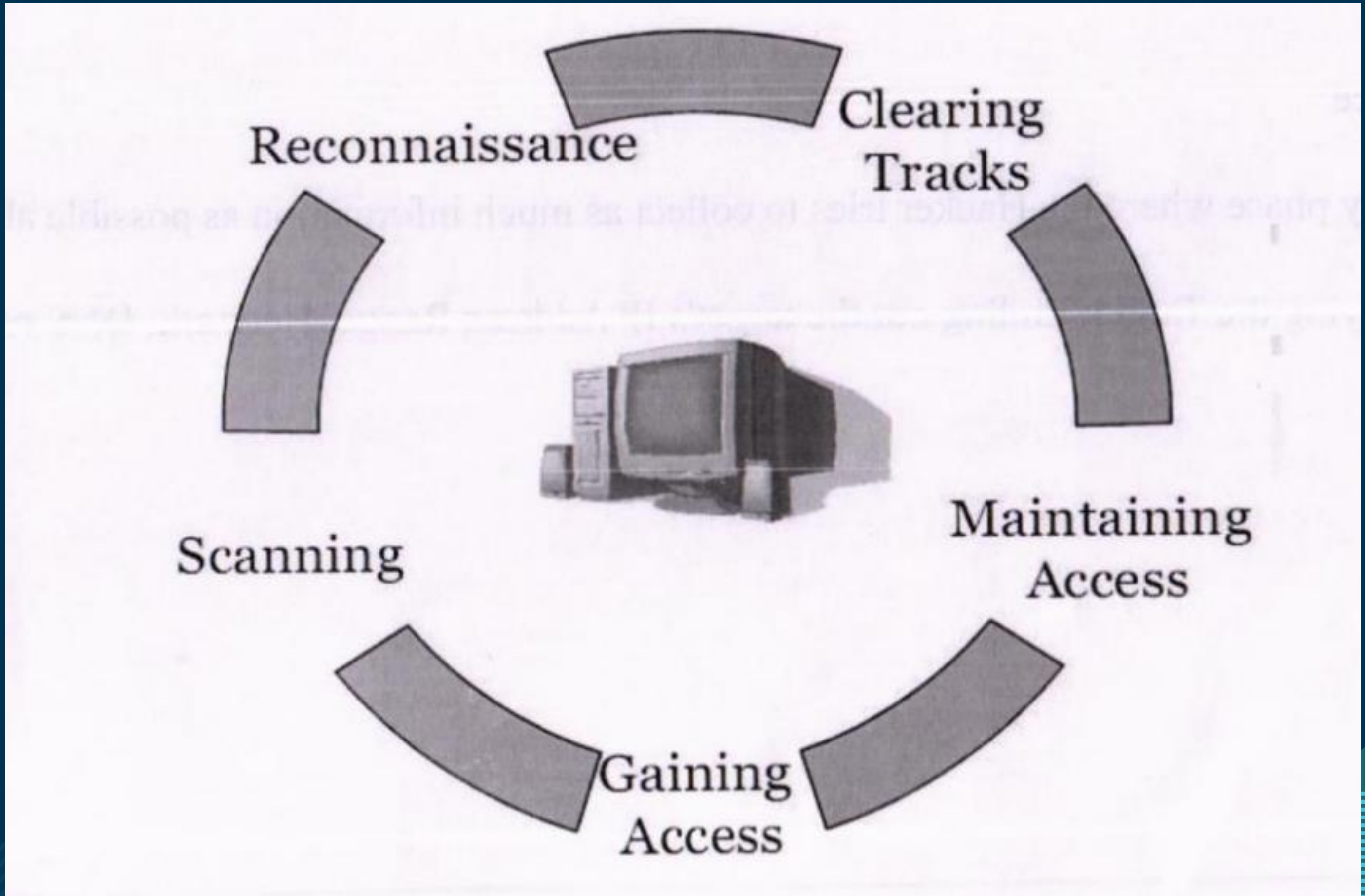
- **black hat hackers are motivated by malicious intent.**

- **Gray hat hackers operate in between — they’re not malicious, but they’re not always ethical either.**

The five phases of Hacking are as follow:



1. Reconnaissance
2. Scanning
3. Exploitation / Gain Access
4. Maintain Access
5. Cover Tracks



1. **Reconnaissance:** **This is the primary phase where the Hacker tries to collect as much information as possible about the target system.**

(INFORMATION GATHERING)

It includes identifying the Target, finding out the target's IP Address Range, Network. – wireshark, Maltego, Nslookup, Nikto, Burp Suite.

SOME INFORMATIONS INCLUDE –

✓ DOMAIN NAME

✓ IP ADDRESS

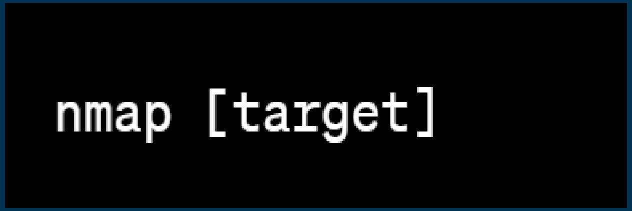
✓ EMPLOYEE INFORMATION

✓ PHONE NUMBER

✓ EMAIL ADDRESS

2. Scanning: It involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may use during the scanning phase can include **port scanners, network mappers and vulnerability scanners.**

Nmap, or Network Mapper - It is designed to explore and map networks, identify open ports, find hosts, and discover various services running on the network.



```
nmap [target]
```

- **3. Exploitation/ Gaining Access: After scanning, the hacker designs the blueprint of the network of the target with the help of data collection during Phase I and Phase 2.**
- **This is the phase where the real hacking takes place.**
- **Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access.**

Blueprint Design:

- **Think of the blueprint as a map showing all the important details of the network, like where data is stored and how everything is connected.**
- **Often, Exploitation targets an application or operating system vulnerability.**

4. Maintaining:

Once a hacker has gained access, they want to keep that access for future exploitation and attacks.

Sometimes, hackers harden the system from other hackers by securing their access with rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks.

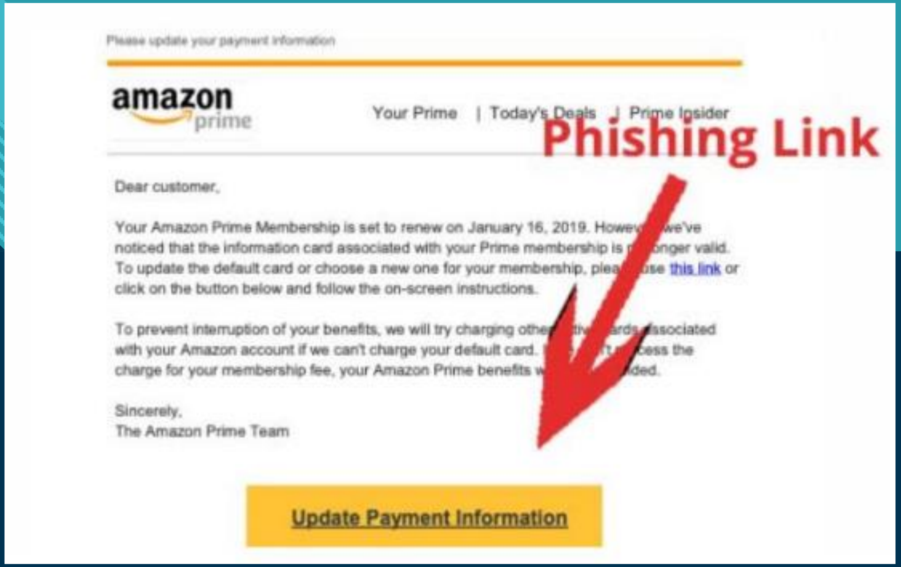
5. Covering Tracks:

Hackers try to remove all traces of the attack. Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking or to avoid legal action.

Hacking techniques:

PHISHING

- What is Phishing? Phishing is a common trick used by hackers to fool you into giving away your personal information.
- It often happens through emails or text messages that look like they're from trusted sources.
- How Does it Work? Imagine getting a message that seems to be from a familiar company (like Amazon or Netflix) or even a friend.
- The goal is to make you click on a link



Please update your payment information

Dear customer,

Your Amazon Prime Membership is set to renew on January 16, 2019. However, we've noticed that the information card associated with your Prime membership is no longer valid. To update the default card or choose a new one for your membership, please use this link or click on the button below and follow the on-screen instructions.

To prevent interruption of your benefits, we will try charging other active cards associated with your Amazon account if we can't charge your default card. If we can't process the charge for your membership fee, your Amazon Prime benefits w [illegible] ded.

Sincerely,
The Amazon Prime Team

Phishing Link

Typically they will:

□ Inform you that someone has been trying to log into your website and you should update your credentials
□ Claim that there’s a problem with your account or your payment information
□ Ask you to confirm some personal information

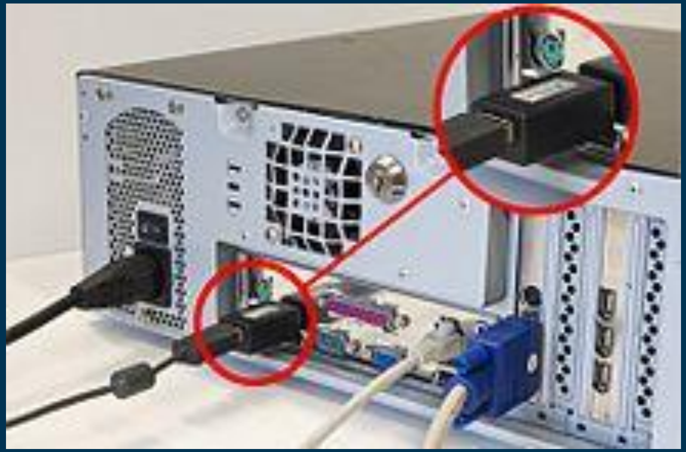
□ Offer you free stuff
□ Even messages appearing to be from friends can be dangerous if they contain suspicious links.

What is a Keylogger?

- A keylogger, also known as a keystroke logger or keyboard capture, is a form of surveillance technology.
- It records every key you press on your computer or device.

Types of Keyloggers:

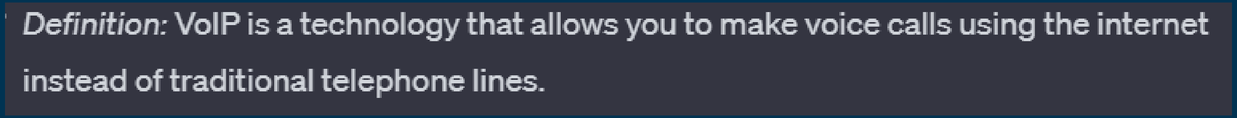
- 1. Hardware Keyloggers: A tiny device connected between your keyboard and computer.
- It appears as a regular part of your computer cables or connectors.
- *Use:* Lets someone spy on your typing without you knowing.
- 2. Software Keyloggers:
- Software that can record your keystrokes.
- *How it gets in:* Can be intentionally downloaded in your hard drive or sneak in with other harmful software.
- *Operation:* Works in the background, secretly recording what you type.



Eavesdropping:

- Eavesdropping is like someone secretly listening to your private conversations.
- Talking on the phone or sending messages, thinking it's private, but there is someone in middle listening to your conversation or messes with your data without you knowing.

- **Types of Eavesdropping:**
- There are two main types - Passive and Active.
- **Passive Eavesdropping:** Imagine someone silently listening to your digital conversations.
- When you're talking over the internet using VoIP (Voice over Internet Protocol).



Definition: VoIP is a technology that allows you to make voice calls using the internet instead of traditional telephone lines.

- **Active Eavesdropping:**
- Picture a hacker pretending to be a website where you share personal data.
- hackers imitate websites where online users can share personal data and information.
- An attacker using a sniffing program gathers the data of its target.
- MITM attack or man-in-the-middle attack is an example of an active eavesdropping attack.
- The data is captured, modified and sent to other devices

Penetration Test:

- A penetration test is a simulated cyber-attack carried out by testers or ethical hackers to find vulnerabilities in a system, website, mobile application, or network.
- Basically, a penetration test is a method of hacking into a system before cybercriminals get into it and exploit it.
- This way, the pen tester finds weaknesses in the system beforehand, makes a report, and sends it to the blue team to fix and patch.
- Blue Team" refers to a group of individuals or cybersecurity professionals within an organization who are responsible for defending against security threats and ensuring the overall security posture
- "Red Team," which conducts offensive security operations such as penetration testing.
- PENETRATION TESTING - It is a proactive and offensive security operation.

Different stages of Penetration testing

- **1. Planning and Reconnaissance:** The first stage involves: □ Defining the scope and goals of a test,
- including systems to be addressed and the testing methods to be used.
- □ Gathering INFORMATION (e.g., network and domain names) to better understand how a target works and WHAT ARE ITS vulnerabilities.

- **2. Scanning:** The next step is to understand how the target application will respond to various intrusion attempts.
- This is typically done using:
- □ Static analysis –Testing an application’s code to predict the way it behaves while running. Static analysis involves examining the code and structure of a software application without actually executing it.
- □ Dynamic analysis – Dynamic analysis involves observing how a software application behaves while it's running or in action.
- Provides a real-time view into how the application performs during execution. It helps uncover issues that might only become apparent when the application is running.

- **3. Gaining Access: t**he main goal at this stage is to test the security of a system by trying to break into it using various techniques.
- Testers conduct web application attacks, such as SQL injection. These are way to get into a system without proper authorization.
- The aim is to understand the extent of damage that could occur if a real attacker exploits these vulnerabilities. It helps organizations identify and fix weaknesses in their systems before actual attackers can take advantage of them.
- **4. Maintaining Access:** The idea is to see if an attacker, once inside, can remain undetected and maintain access for an extended period.
- **Duration:** The testers try to stay within the system for an extended period, imitating the actions of a persistent attacker. This could involve periodic checks to see if they can still access the system without being noticed.

- **5. Analysis:** After the penetration test is complete, the results are thoroughly examined and analyzed.
- **Purpose:** The analysis provides valuable insights for the organization. It helps them understand the weaknesses in their systems. and how long an attacker might go unnoticed if they exploit these vulnerabilities.

Black Box, White box , Gray Box Testing

- White Box Testing: Also known as glass box, or clear box testing.
- Testers have full access to the internal workings of the software. They can see the source code, architecture, and logic of the software.
- Goal: Make sure the inside of the software is built correctly.
- How: Look at the code, understand how it works, and test every part to catch any mistakes.
- Black Box Testing: Testers have no knowledge of the internal workings of the software. They interact with the software from an external perspective, like a regular user. It's similar to using a device without knowing how it's made.
- Goal: Check if the software does what it's supposed to do, without caring about how it's made inside.
- Give inputs, see what comes out
- Focus: Testing the software from the outside, like a user would, without looking at the code.
- Gray Box Testing: Testers have partial access to the internal structure. They can see some parts of the source code but not everything.
- Goal: Mix a bit of both. Check how the software works inside a little, but also test it from the outside like a user.
- Aims to find defects and vulnerabilities by considering both the internal logic and the external functionality.

Reverse engineering

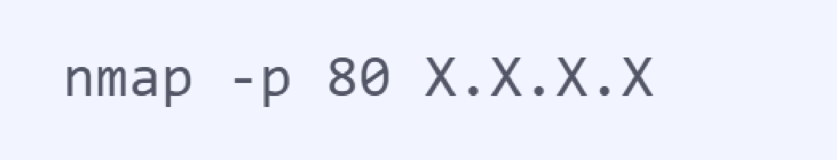
- **Reverse engineering refers to the duplication of another producer's product following a thorough examination of its construction or how it was built.**
- **It involves looking at a product made by someone else and trying to create a similar one.**
- **Once you understand how the an application works, you might want to make it even better or create a similar application with some improvements.**
- **People might use reverse engineering to understand how software or hardware functions, improve it, or create something similar.**

Vulnerability assessment. Explain its types

- A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures.
- Vulnerability assessments also provide an organization with the necessary knowledge, awareness and risk backgrounds to understand and react to each threats in their organization.
- A vulnerability assessment process is meant to identify threats and the risks they contain and fix it.
- They typically involve the use of automated testing tools, such as network security scanners.

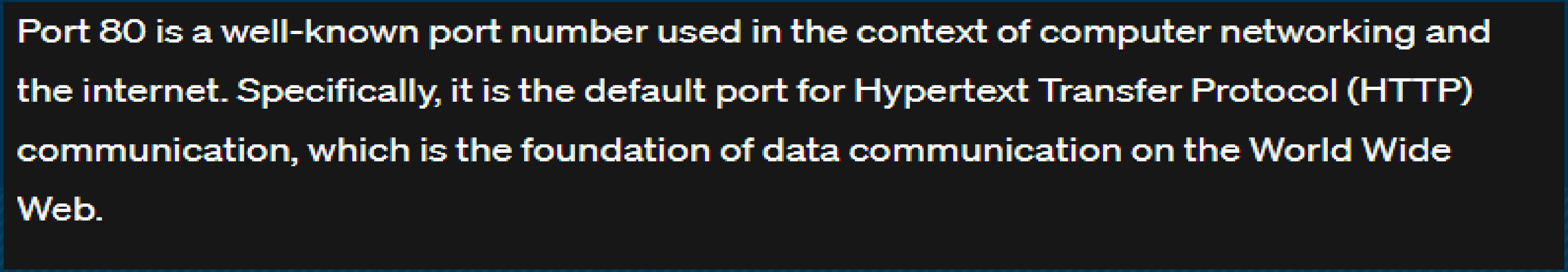
- Nmap can be used to discover hosts on a network, it could be used for port scanning, provide info about services running on that port.
- Nmap can determine versions of services running on one port, so version vulnerabitlities could be solved.

- To launch a default scan, the bare minimum you need is a target. A target can be an IP address, a hostname, or a network range.
- Nmap is pretty easy to use if you're familiar with command-line interfaces. As it’s already installed on most Linux/Unix-based distributions, you just have to execute the ‘nmap’ command from any terminal, and that’s it.
- One of the most basic Nmap commands for a scan is the nmap port scan command:



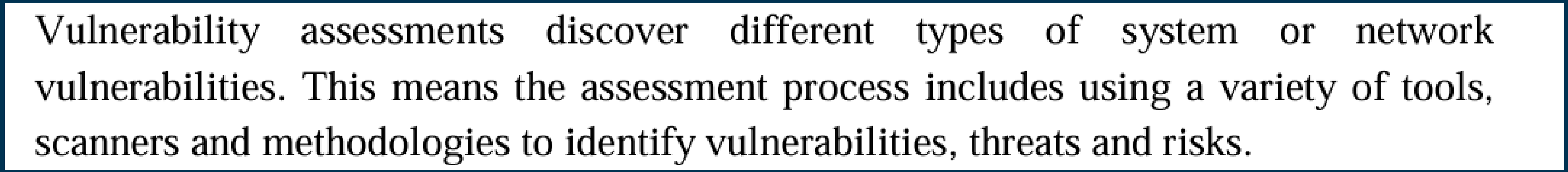
```
nmap -p 80 X.X.X.X
```

Can scan web servers, web application



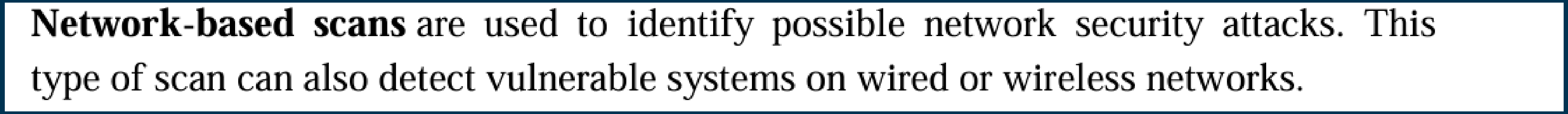
Port 80 is a well-known port number used in the context of computer networking and the internet. Specifically, it is the default port for Hypertext Transfer Protocol (HTTP) communication, which is the foundation of data communication on the World Wide Web.

- **In computer networking, a port refers to a communication endpoint used by software applications to exchange data.**
- **Think of it as a virtual gate that allows different programs on a computer to connect and communicate with each other or with programs on other devices over a network.**
- Types of vulnerability assessments:



Vulnerability assessments discover different types of system or network vulnerabilities. This means the assessment process includes using a variety of tools, scanners and methodologies to identify vulnerabilities, threats and risks.

- Different types of vulnerability assessment scans includes:



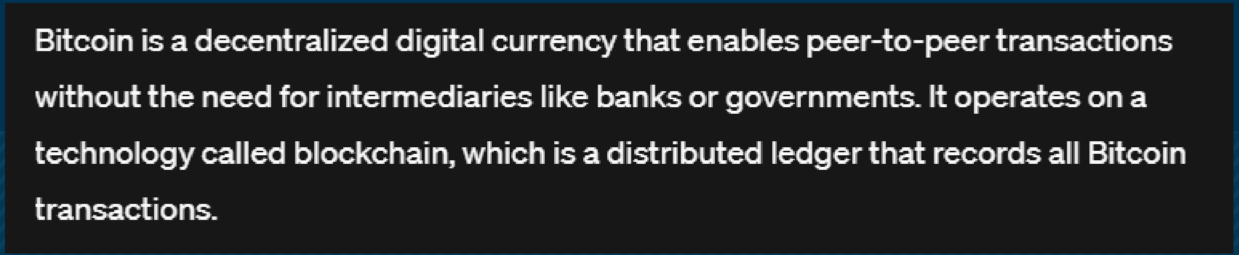
Network-based scans are used to identify possible network security attacks. This type of scan can also detect vulnerable systems on wired or wireless networks.

- Host-based scans are used to locate and identify vulnerabilities in servers, workstations or other network hosts. This type of scan usually examines ports and services
- Wireless network scans of an organization's Wi-Fi networks usually focus on points of attack in the wireless network infrastructure.
- Application scans test websites to detect known software vulnerabilities and incorrect configurations in network or web applications.
- Database scans can identify weak points in a database to prevent malicious attacks, such as SQL injection attacks.

Hacking Terminologies:

Ransomware

- Ransomware is a type of malicious software (malware) designed to encrypt files on a victim's computer or network, rendering them inaccessible, and then demand payment (typically in cryptocurrency like Bitcoin) in exchange for providing the decryption key to unlock the files.



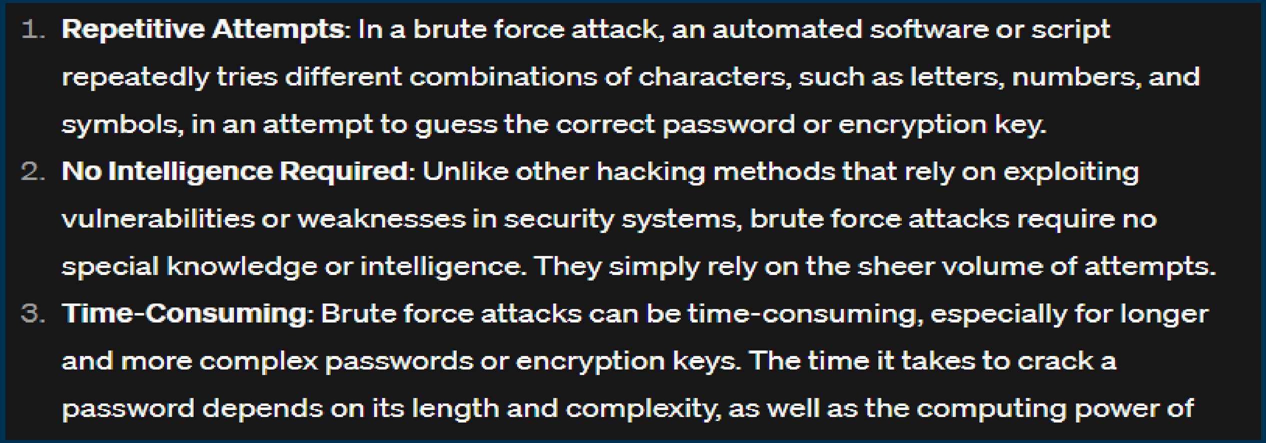
Bitcoin is a decentralized digital currency that enables peer-to-peer transactions without the need for intermediaries like banks or governments. It operates on a technology called blockchain, which is a distributed ledger that records all Bitcoin transactions.

Social engineering

- Social engineering is like a trick that hackers play to get what they want. Instead of using fancy computer skills to break into systems, they use clever tactics to manipulate people into giving them access or sensitive information.
- Tricking Trust
- Creating Urgency

Brute Force Attack

- A Brute Force Attack is a straightforward and systematic hacking method used to crack passwords or encryption keys by trying every possible combination until the correct one is found.
- It's like trying every key until you find the right key to unlock the door.



1. **Repetitive Attempts**: In a brute force attack, an automated software or script repeatedly tries different combinations of characters, such as letters, numbers, and symbols, in an attempt to guess the correct password or encryption key.
2. **No Intelligence Required**: Unlike other hacking methods that rely on exploiting vulnerabilities or weaknesses in security systems, brute force attacks require no special knowledge or intelligence. They simply rely on the sheer volume of attempts.
3. **Time-Consuming**: Brute force attacks can be time-consuming, especially for longer and more complex passwords or encryption keys. The time it takes to crack a password depends on its length and complexity, as well as the computing power of

DDoS attack

- In a DDoS attack, hackers flood a website or online service with so much traffic that it becomes overwhelmed and can't handle all the requests.
- Faces downtime or crashes.
- **Block Access**: By overwhelming the website's servers or network with fake requests, the attackers effectively block legitimate users from accessing the website or service.
- Even though the website's servers are still running, they're so busy dealing with the fake traffic that they can't respond to genuine requests