Hello Everyone! In this video you will learn about cyber threats, vulnerabilities and attacks.

Before understanding cyber-attacks, we should know about threats and vulnerabilities, which play an important role for the attackers to choose your machine or network as an attack target. Threats are circumstances or events that can possibly harm a computer by destroying it, disclosing the information stored on the system, harmfully modifying data, or making the system unavailable. E.g. your computer may have a malware attack, is a threat.

On the other hand, vulnerabilities are weakness in an information system or its components that could be exploited. Using an older version of TLS certificate for the security of your website is a vulnerability.

A cyber-attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. They aim to disable, disrupt, destroy or control computer systems or to modify, block, delete, manipulate or steal the data held within these systems.

Let's understand the complete process, an attacker follows to reach to your machines and attack them for stealing information. This is called cyber kill chain.

The “cyber kill chain” is a sequence of 7 steps used by an attacker to successfully infiltrate a network and exfiltrate data. Each step demonstrates a specific goal along the attacker’s path.

Let’s understand the steps, one by one.

First step is Reconnaissance. In this stage, the attacker chooses their target and conduct an in-depth research of it, to identify the vulnerabilities that can be exploited.

Second step is Weaponization where, the intruder creates a **malware weapon** like a virus, worm or preparing a phishing website etc. in order to exploit the vulnerabilities of the target.

After weaponization, third step is Delivery when the weapon is transmitted to the target. The intruder / attacker can employ different methods like USB drives, e-mail attachments and websites for this purpose.

After delivering the weapon, Exploitation takes place. Here, the malware starts the action. The program code of the malware is triggered to exploit the target’s vulnerability/vulnerabilities.

In Installation step, the malware installs an access point, known as the backdoor for the intruder / attacker

After installation, the attacker gets command and Control of the target machine: The malware gives the intruder / attacker access in the network/system. After getting the command of the system, the attacker finally takes action to fulfil its purpose, such as **encryption** for ransom, **data exfiltration** or even **data destruction**.

Let’s discuss some common cyber-attacks. Phishing is the most common attacks, which can target any individual, who is not alert. It can be implemented using malicious links included in emails, social media sites etc.

Another attack is Identity threat, in which the identity of an individual may be stolen to commit frauds such as bank related frauds. This is achieved by stealing your personal identification details like adhar number, PAN card number, password etc.

Man in the Middle attack allows an attacker to steal the information being flown from one user to another. This can be implemented inside the local network or the Internet using various free tools and techniques.

Similarly, Password stealing allows the attacker to unauthorizedly steal the password of the users and Denial of service attack aims to make the resources of information unavailable to the user.

Each user should get alerted for any of the mentioned attacks

Let’s discuss these cyber-attacks one by one.

Phishing refers to the practice of creating fake emails or SMS that appear to come from someone you trust, such as: Bank, Credit Card Company, Popular Websites

The email/SMS will ask you to click on the malicious links (included in the email) and then re-direct you to a website that looks just like the real website, but with the purpose of information stealing, allowing cybercriminals to steal your identity and possibly making fraudulent purchases with your money. The phishing activities must be reported to the system administration, as and when encountered.

In Identity theft a person’s personal or financial information is stolen and used. It could be that person's name, credit card information, Social Security number, or medical insurance details.

Password cracking or stealing is the process of obtaining the correct password to an account in an unauthorized way. The password can be stolen using the credential stuffing method in which attackers use lists of compromised user credentials to breach into a system or use a **key logger** software or hardware capable of recording input from a computer keyboard and intercepting keystrokes without the user's knowledge. It can also be done using a dictionary attack method of breaking into a password-protected computer, network, or other IT resource by systematically entering every word in a dictionary as a password. Social engineering is the art of manipulating, influencing, or deceiving you in order to gain control over your computer system. The hacker might use the phone, email, snail mail or direct contact to gain illegal access. A Password Spraying Attack is also a type of brute force attack where a malicious actor attempts the same password on many accounts before moving on to another one and repeating the process. This is effective because many users use simple, predictable passwords, such as "password123."

A DOS or denial of service attack in which a computer sends a massive amount of traffic to a victim's computer and shuts it down. A Dos attack is an online attack that is used to make the website unavailable for its users when done on a website. In DDoS attacks i.e. distributed denial of service, dos attacks are executed from many different locations using many systems.

A man-in-the-middle attack (MITM attack) is a cyber-attack where an attacker relays and possibly alters communication between two parties who believe they are communicating directly. This allows the attacker to relay communication, listen in, and even modify what each party is saying.

Thank You.