Chapter-#01

Cyber Security

Classification of Cyber Crime

- **What is Cyber Crime?**
- Cybercrime is defined as an unlawful action against any person using a computer, its systems, and its online or offline applications. It occurs when information technology is used to commit or cover an offense. However, the act is only considered Cybercrime if it is intentional and not accidental.
- Cybercrime can cause direct harm or indirect harm to whoever the victim is.
- However, the largest threat of cybercrime is on the financial security of an individual as well as the government. Cybercrime causes loss of billions of USD every year.
- **Types of Cybercrime.**
- Let us now discuss the major types of cybercrime –
- **Email Bombing/Denial of Service Attack:**
- Email bombing is a form of cyber crime consisting of sending huge volumes of email to an address in order to overflow the mailbox or overwhelm the server where the email address is hosted. This results in the server crashing there by disrupting the website or web portal and its online functioning.

Types of Cybercrime

- An email bomb is an attack against an email inbox or server designed to overwhelm an inbox or inhibit the server's normal function, rendering it unresponsive, preventing email communications, degrading network performance, or causing downtime. The intensity of an email bomb can range from an inconvenience to a complete denial of service. Typically, these attacks persist for hours or until the targeted inbox or server implements a mitigation tactic to filter or block the attacking traffic. Such attacks can be carried out intentionally or unintentionally by a single actor, group of actors, or a botnet. There are five common email bomb techniques:
- **i): Mass mailing** – intentionally or unintentionally sending large quantities of random email traffic to targeted email addresses. This attack is often achieved using a botnet or malicious script, such as by the automated filling out of online forms with the target email inserted as the requesting/return address.
- **ii):List linking** – signing targeted email addresses up for numerous email subscriptions, which indirectly flood the email addresses with subscribed content. Many subscription services do not ask for verification, but if they do these emails can be used as the attack emails. This type of attack is difficult to prevent because the traffic originates from multiple legitimate sources.

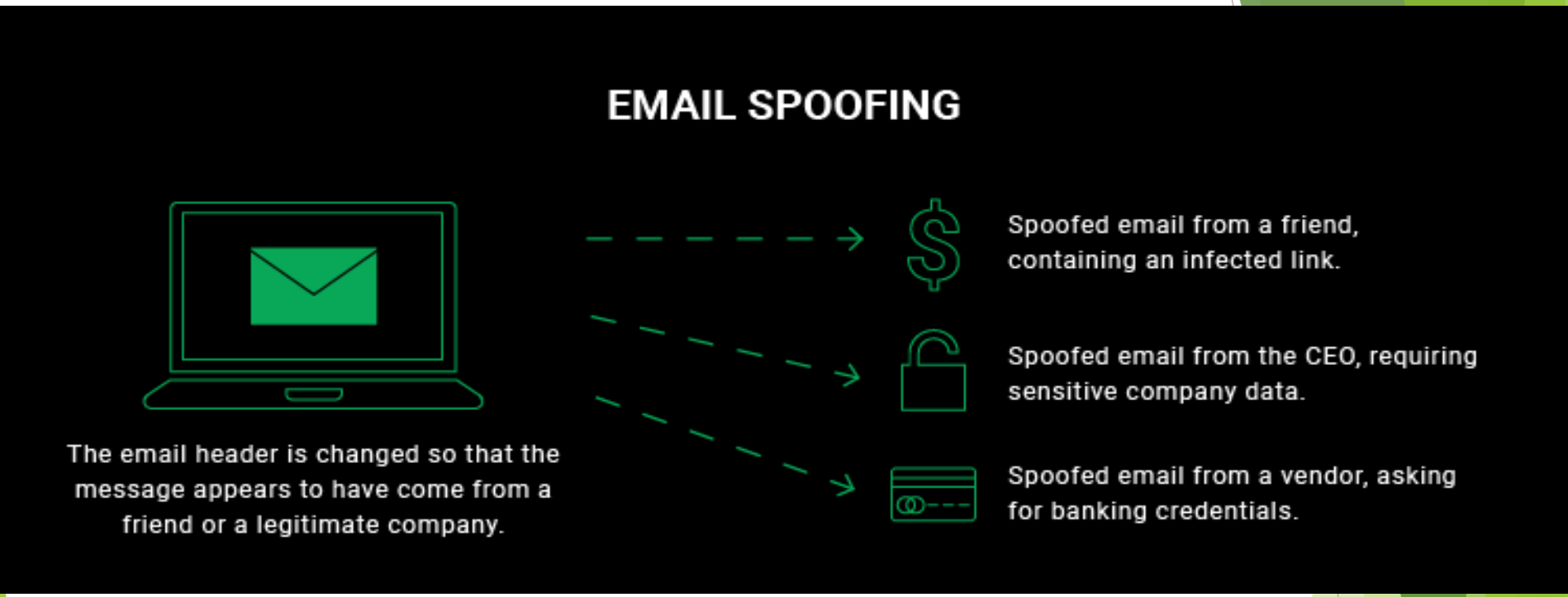
Types of Cybercrime

- **iii):ZIP bomb** – sending very large compressed archive files to an email address, which when decompressed, consume available server resources to damage performance.
- **Iv):Attachment** – sending multiple emails with large attachments designed to overload the storage space on a server and cause the server to stop responding.
- **V):Reply-all** – responding "Reply All" to large dissemination lists instead of just to the original sender. This inundates inboxes with a cascade of emails, which are compounded by automated replies, such as out-of-office messages. These are often accidental in nature. This can also occur when a malicious actor spoofs an email address and the automatic replies are directed toward the spoofed address.

2:Email Spoofing:

- mail spoofing is the act of sending emails with **a forged sender address**. It tricks the recipient into thinking that someone they know or trust sent them the email. Usually, it's a tool of a phishing attack, designed to take over your online accounts, send malware, or steal funds.
- Spoofed email messages are easy to make and easy to detect. However, more malicious and targeted varieties can cause significant problems and pose a huge security threat.

Types of Cyber crime



- Email spoofing is possible due to the way email systems are designed. Outgoing messages are assigned a sender address by the client application; outgoing email servers have no way to tell whether the sender address is legitimate or spoofed.
- Recipient servers and antimalware software can help detect and filter spoofed messages. Unfortunately, not every email service has security protocols in place. Still, users can review email headers packaged with every message to determine whether the sender address is forged.

Types of Cyber crime

3:Web-jacking

- This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even change the information on the site. This may be done for fulfilling political objectives or for money. E.g. recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also web jacked. Another case of web jacking is that of the 'gold fish' case. In this case the site was hacked and the information pertaining to gold fish was changed.
- Illegally seeking control of a website by taking over a domain is known as **Web Jacking**. In web jacking attack method hackers compromises with the domain name system (DNS) that resolves website URL to IP address but the actual website is never touched. Web jacking attack method is another type of social engineering phishing attack where an attacker create a fake web page of victim website and send it to the victim and when a victim click on that link, a message display on the browser "the site abc.com has move on another address, click here to go to the new location" and if a victim does click on the link, he/she will redirect on the fake website page where an attacker can ask for any sensitive data such as credit card number, username, password etc.

Types of Cyber crime

- Web jacking attack method is one kind of trap which is spread by the attacker to steal the sensitive data of any people, and those people got trapped who are not aware about cyber security. **Web Jacking Attack Method:**
- The first step of web jacking attack method is to create a fake page of victim website for example www.anywebsite.com/login.php.
- The second step is to host it either on your local computer or shared hosting.
- The third step is to send the link of a fake page to the victim.
- The fourth step victim will open the link and enter their details and submit.
- Last step, you will get all the details submitted by victim.
- **How to be safe from web jacking attack method !**
- First of all do not enter sensitive data in any link sent to you.
- Check the URL. Just because the address looks Ok, don't assume this is a legitimate site. Read company name carefully, is it right or wrong.
- check that there is http protocol or https, if http then do not enter your data.
- If you are not sure, site is real or fake, enter a wrong username and password.
- Use a browser with anti phishing detection.

Types of Cyber crime

- **4: Salami Attack**
- A salami attack is a type of cybercrime that involves the theft of small amounts of money from a large number of accounts, often over a long period of time. It is named after the method of slicing thin slices of salami, as the thief is able to steal small amounts of money from many accounts without being noticed. These attacks can be difficult to detect and can have serious consequences for individuals and organizations. In this article, we will discuss what a salami attack is, how it works, and what you can do to protect yourself from these types of attacks.
- **What is Salami Attack?**
- A salami attack is a form of financial fraud that involves the theft of small amounts of money from a large number of accounts. The goal of this type of attack is to steal small amounts of money from each account over a long period of time, in order to avoid detection. The thief is able to do this by manipulating financial transactions in a way that is difficult to detect.
- **How to Protect Yourself from a Salami Attack**
- **i:Use Unique Passwords**
- **ii:Enable Two-Factor Authentication (2FA)**
- **iii:Use Up-to-Date Software**

Types of Cyber crime

- iv: Avoid Unknown Links
- V: Keep an Eye on All Your Accounts
- Vi: Beware of Phishing

5: Software Piracy

- Software piracy is the act of illegally using, copying, modifying, distributing, sharing, or selling computer software protected by copyright laws. A software pirate is anyone who intentionally or unintentionally commits these illegal acts.
- You don’t have to be a hacker to become a software pirate. It’s enough to use illegal software or copy and share legal software without the author’s consent.
- Software piracy is the illegal copying, distributing, sharing, selling or use of software, whether intentional or not. Software piracy examples include activities such as an end-user installing a single-use license on multiple computers, a holidaymaker buying a pirated copy of a piece of software in the Far East or the mass distribution of illegally obtained software.
- **What is pirated software?**
- Any software you did not pay for or see online for free that's normally not free is considered **pirated software**. For example, Adobe Photoshop is a popular commercial image editor that must be paid for to use.

Types of Cyber crime

- **6: Password Sniffing**
- Password sniffing is a type of network attack in which an attacker intercepts data packets that include passwords. The attacker then uses a password-cracking program to obtain the actual passwords from the intercepted data.
- Password sniffing can be used to obtain passwords for any type of account, including email, social media, and financial accounts. It is one of the most common types of attacks on both home and business networks.
- **Password Sniffing** is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic. This often happens on public WiFi networks where it is relatively easy to spy on weak or unencrypted traffic.
- **What Is a Sniffing Attack?**
- Sniffing attacks are a type of network attack in which an attacker intercepts data packets as they travel across a network. Sniffing attacks can steal sensitive information, such as passwords and credit card numbers, or eavesdrop on communications. Sniffing attacks are possible because most networks use shared media, such as Ethernet cables or wireless networks. This means that every computer can see all data packets sent across the network on the network. Using a packet sniffer, an attacker can see all the data passing through the network, including any unencrypted passwords or other sensitive information.

Types of Cyber crime

- **Types of Sniffing**
- i: Web Password Sniffing
- ii: LAN Sniffing
- iii: Protocol Sniffing
- iv: ARP Sniffing
- **7:online fraud**
- The term cybercrime refers to a variety of crimes carried out online, using the internet through computers, laptops, tablets, internet-enabled televisions, games consoles and smart phones. Cyber-enacted crimes can only be committed on the internet – stealing confidential information that's stored online, for example. Other crimes which are carried out online, but could be committed without the use of the internet, such as sexual grooming, stalking or harassment, bullying, and financial or romance fraud, are called cyber-enabled crimes.
- Internet fraud involves using online services and software with access to the internet to defraud or take advantage of victims. The term "internet fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing, and other hacking activities designed to scam people out of money.

Types of Cyber crime

- **8:Identity Theft**
- Identity thieves usually **obtain personal information** such as passwords, ID numbers, credit card numbers or social security numbers, and misuse them to **act fraudulently** in the victim's name. These sensitive details can be used for various **illegal purposes** including applying for loans, making online purchases, or accessing victim's medical and financial data.
- **Identity Theft** also called Identity Fraud is a crime that is being committed by a huge number nowadays. Identity theft happens when someone steals your personal information to commit fraud. This theft is committed in many ways by gathering personal information such as transactional information of another person to make transactions.
- **Types of Identity Thefts:**
- There are various amount of threats but some common ones are :
- **i: Criminal Identity Theft**
- **ii: Driver's license ID Identity Theft**
- **iii: Senior Identity Theft**
- **iv: Medical Identity Theft**

Types of Cyber crime

- **V: Tax Identity Theft**
- **Vi: Social Security Identity Theft**
- **Vii: Synthetic Identity Theft**
- **Viii: Financial Identity Theft**

9:Forgery

- Offences of computer forgery and counterfeiting have become rampant as it is very easy to counterfeit a document like birth certificate and use the same to perpetuate any crime. The authenticity of electronic documents hence needs to be safeguarded by making forgery with the help of computers abs explicit offence punishable by law. When a perpetrator alters documents stored in computerized form, the crime committed may be forgery. In this instance, computer systems are the target of criminal activity.
- Computers, however, can also be used as instruments with which to commit forgery. A new generation of fraudulent alteration or counterfeiting emerged when computerized color laser copiers became available. These copiers are capable of high-resolution copying, modification of documents, and even the creation of false documents without benefit of an original, and they produce documents whose quality is indistinguishable from that of authentic documents except by an expert.

Types of Cyber crime

- **10: Cyber Terrorism**
- Cyber terrorism involves the same techniques as traditional cyber attacks. Cyber terrorists can use DDoS attacks, various forms of malware, social engineering strategies, phishing campaigns and more to reach their targets.
- *"Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."*
- The main difference between cybercrime and cyber terrorism lies in the objective of the attack. Cybercriminals are predominantly out to make money, while cyber terrorists may have a range of motives and will often seek to have a destructive impact, particularly on critical infrastructure.
- Cyber terrorists also want to have maximum impact with the greatest stealth. Green gard (2010) identified a range of cyber attack methods that can be deployed by cyber terrorists, including "vandalism, spreading propaganda, gathering classified data, using distributed denial-of-service attacks to shut down systems, destroying equipment, attacking critical infrastructure, and planting malicious software."