Unit-1
Introduction to Cyber Security

- Concept of Cyber Security
- Cyber Crimes
- Types of Attacks in cyber
- Hacker Techniques

Introduction/ (Why cyber security is important?)

- We live in a digital era which understands that our private information is more vulnerable than ever before.
- We all live in a world which is networked together, from internet banking to government infrastructure, where data is stored on computers and other devices.
- A portion of that data can be sensitive information that can be intellectual property, financial data, personal information,
- An unauthorized access or exposure to that data could have negative consequences.
- Cyber-attack is now an international concern.
- And cybercrime is a global problem that's been dominating the news cycle.
- It poses a threat to individual security and an even bigger threat to large international companies, banks, and governments.
- Hacks and other security attacks could endanger the global economy and sensitive data is transmitted across networks and to other devices frequently.
- As the volume of cyber-attacks grows, companies and organizations, need to take steps to protect their sensitive business and personal information.
- And cybersecurity describes to protect that information and the systems used to process or store it.

Cyber:

- Merriam Webster defines cyber as:
  : of, relating to, or involving computers or computer networks (such as the Internet).
- "Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age.
- The word "cyber" denotes a relationship with information technology (IT), i.e., computers. (It can relate to all aspects of computing, including storing data, protecting data, accessing data, processing data, transmitting data, and linking data.)
- The common words related with cyber are Cyber-attack, Cyber Crime, Cyber Space, Cyber Security etc.

Cyber Security:

- Cyber Security is the process of detecting and preventing any unauthorized use of our laptop/computer.
- It involves the process of safeguarding against hacker from using our personal or office-based computer resources with malicious intent or for their own gains, or even for gaining any access to them accidentally.
- Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyber-attacks.
- It is made up of two words one is cyber and other is security. Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.
- It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access. It may also be referred to as information technology security.
- A strong cybersecurity strategy can provide a good security against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data.

Ethics:

- Ethics is a system of moral principles.
- Ethics is concerned with what is good for individuals and society and is also described as moral philosophy.
- Ethics is the discipline concerned with what is morally good and bad and morally right and wrong.

Professional Ethics:

- Professional ethics are principles that govern the behavior of a person or group in a business environment.
- Like values, professional ethics provide rules on how a person should act towards other people and institutions in such an environment.

Cyber Crimes

- Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network.
- It is criminal activity that either targets or uses a computer, a computer network or a networked device.
- In this, computer is the object of the crime or is used as a tool to commit an offense.
- The illegal activities such as committing fraud, harassment, abuse, stealing identities and intellectual property, or violating privacy etc. are the example of cyber-crime.
- Cybercrime may threaten a person, company or a nation's security and financial health.
- A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device.
- Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.
- Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money.
- Cybercrime can also be carried out by individuals or organizations.
- Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others might be novice hackers.
- Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

Types of cyber-crime:

Hacking

- It is an illegal practice by which a hacker breaches the computer's security system of someone for personal interest.

Unwarranted mass-surveillance

- Mass surveillance means surveillance of a substantial fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.

Child grooming

- It is the practice of establishing an emotional connection with a child especially for the purpose of child-trafficking and child prostitution.

Copyright infringement

- If someone infringes someone's protected copyright without permission and publishes that with his own name, is known as copyright infringement.

Money laundering

- Illegal possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legitimate business. In other words, it is the practice of transforming illegitimately earned money into the legitimate financial system.

Cyber-extortion

- When a hacker hacks someone's email server, or computer system and demands money to reinstate the system, it is known as cyber-extortion.

Cyber-terrorism

- Normally, when someone hacks government's security system or intimidates government or such a big organization to advance his political or social objectives by invading the security system through computer networks, it is known as cyber-terrorism.

Online Scams

- These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

Types of attacks in Cyber/ Hacker Techniques

The most common types of attacks are given below:

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
2. Man-in-the-middle (MitM) attack
3. Phishing and spear phishing attacks
4. Drive-by attack
5. SQL injection attack
6. Cross-site scripting (XSS) attack
7. Malware attack
8. Ransomware attack
9. Brute Force attack
10. Session Hijacking
11. DNS Spoofing
12. Dictionary attack

1. **Denial-of-service (DoS) and distributed denial-of-service (DDoS) attack**
   It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash.

2. **Man-in-the-middle (MitM) attack**
   A MitM attack occurs when a hacker inserts itself between the communications of a client and a server.

3. **Phishing attacks**
   Phishing attack is the practice of sending emails, web pages or links that appear to be from trusted sources which attempts to steal sensitive information like user login credentials and credit card number etc.

4. **Drive-by attack**
   Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages.

5. **SQL injection attack**
   SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server.

6. **Cross-site scripting (XSS) attack**
   XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application. Specifically, the attacker injects a payload with malicious JavaScript into a website's database.

7. **Malware attack**
   Malicious software is an unwanted software that is installed in our system without our knowledge. The software is injected with malicious code and after installing it can send data to the attacker or damage our system.

8. **Ransomware attack**
   With ransomware, the victim's system is held hostage until they agree to pay a ransom to the attacker. After the payment has been sent, the attacker then provides instructions regarding how the target can regain control of their computer. The name "ransomware" is appropriate because the malware demands a ransom from the victim.

9. **Brute Force attack**
   It is a type of attack which uses a trial-and-error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number.

10. **Session Hijacking**
    It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

11. **DNS Spoofing**
    Domain Name System (DNS) poisoning and spoofing are types of cyberattack that exploit DNS server vulnerabilities to divert traffic away from legitimate servers towards fake ones.

12. **Dictionary attack**
    This type of attack stored the list of a commonly used password and validated them to get original password.