Practical No. 1

Aim: Introduction of Cyber Security and List of Cyber Security Attack.

1. Introduction

Cyber security are techniques generally set forth in published materials that attempt to safeguard the cyber environment of a user or organization. It manages the set of techniques used to save the integrity of networks, programs and data from unauthorized access. It refers to the body of technologies, processes, and it may also be referred to as information technology security. The field is of growing importance due to increasing reliance on computer systems, including smart phones, televisions and the various tiny devices that constitute the Internet of Things. Keywords: IT security, Internet of things (IOT)

The internet has made the world smaller in many ways but it has also opened us up to influences that have never before been so varied and so challenging. As fast as security grew, the hacking world grew faster. There are two ways of looking at the issue of cyber security. One is that the companies that provide cloud computing do that and only that so these companies will be extremely well secured with the latest in cutting edge encryption technology.

2. What is Cyber Security?

It's being protected by internet-connected systems, including hardware, software and data, from cyber-attacks. In a computing context, security comprises cyber security and physical security both are used by enterprises to safe against unauthorized access to data centre and other computerized systems. The security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security.

3. Why do we need Cyber Security?

The range of operations of cyber security involves protecting information and systems from major cyber threats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people.

Some of the common threats are:

1. Cyber terrorism
    - It is the innovative use of information technology by terrorist groups to further their political agenda. It took the form of attacks on networks, computer systems and telecommunication infrastructures.
2. Cyber spionage
    - It is the practice of using information technology to obtain secret information without permission from its owners or holders. It is the most often used to gain strategic, economic, military advantage, and is conducted using cracking techniques and malware.
3. Cyber warfare
    - It involves nation-states using information technology to go through something other nations networks to cause damage. In the U.S. and many other people live in a society, cyber warfare has been acknowledged as the fifth domain of warfare.
    - Cyber warfare attacks are primarily executed by hackers who are well-trained in use of benefit the quality of details computer networks, and operate under the favourable and support of nation-states.
    - Rather than closing a targets key networks, a cyber-warfare attack may force to put into a situation into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.

4. Who are Cyber Criminals?

It involves such activities as child printed sexual organs or activity; credit card fraud; cyber stalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright, software licensing and trademark safe to protect; overriding encryption to make illegal copies; software piracy and stealing another"s identity to perform criminal acts. Cybercriminals are those who conduct such acts.

They can be categorized into three groups that reflect their motivation.

Type 1: Cybercriminals – hungry for recognition:

i. Hobby hackers;

ii. IT professionals (social engineering is one of the biggest threat);
iii. Politically motivated hackers;
iv. Terrorist organizations.

Type 2: Cybercriminals – not interested in recognition:

i. Psychological prevents;
ii. Financially motivated hackers (corporate espionage);
iii. State – sponsored hacking (national espionage, sabotage); \
iv. Organized criminals.

Type 3: Cybercriminals – the insiders:

i. former employees seeking revenge;
ii. Competing companies using employees to gain economic advantage through damage and/or theft.

5. Types of Cyber Security Threats:

The use of keeping up with new technologies, security trends and threat intelligence is a challenging their task. However, it should be in order to protect information and other assets from cyber threats, which take many forms.

- **Ransom ware** is a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them.
- **Malware** is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.
- **Social engineering** is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.
- **Phishing** is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information.

Conclusion: We have studied the basics of cyber security and types of cyber-attacks.