Cyber Security Introduction

Cyber Crime

- Cyber crimes are, as the name implies, crimes committed using computers, phones or the internet.

- Some types of cyber crime include:
    - Illegal interception of data.
    - System interferences.
    - Copyrights infringements.
    - Sale of illegal items.

Cyber Security

- Cyber security is the body of technologies, processes and practices involved in protecting individuals and organizations from cyber crime.

- It is designed to protect integrity of networks, computers, programs and data from attack, damage or unauthorized access.

Kill Chain, Zero-day attack, ransomware, alert fatigue and Man-in the middle attack are just a few examples of common cyber attacks.

Cyber Security Principles

There are five key principles in cyber security:

- Confidentiality
- Integrity
- Availability
- Accountability
- Auditability

Cyber Security Principle Definitions

- **Confidentiality:**
  - A set of rules that limits access or place restrictions on certain type of information.
- **Integrity:**
  - Assurance that the information is trustworthy and accurate.
- **Availability:**
  - The guarantee of reliable access to the information by authorized people.

Cyber Security Principle Definitions

- **Accountability:**
  - Is an assurance that an individual or an organization will be evaluated on their performance or behaviour related to something for which they are responsible.

- **Auditability:**
  - A security audit is a systematic evaluation of the security of a company’s information system by measuring how well it conforms to a set of established criteria.

Cyber Threats

Cyber Threat

- A Cyber threat is any malicious act that attempts to gain access to a computer network without authorization or permission from the owners.

- It refers to the wide range of malicious activities that can damage or disrupt a computer system, a network or the information it contain.

- Most common cyber threats: Social Engineered Trojans, Unpatched Software, Phishing, Network worms, etc.

Sources of Cyber Threats

- Cyber threats can come from a wide variety of sources, some notable examples include:
  - National governments.
  - Terrorists.
  - Industrial secret agents.
  - Rogue employees.
  - Hackers.
  - Business competitors.
  - Organization insiders.

Anyone with a motive and the needed technology can create cyber threats.

Cyber Threat Classifications

- Threats can be classified by multiple criteria:
  - Attacker's Resources
  - Attacker's Organization
  - Attacker's Funding

- On basis of these criteria, threats are of 3 types:
  - Unstructured Threats
  - Structured Threats
  - Highly Structured threats

Unstructured Cyber Threats

- **Resources:** Individual or small group.
- **Organization:** Little or no organization.
- **Funding:** Negligible.
- **Attack:** Easy to detect and make use of freely available cyberattack tool.
- Exploitation based on documented vulnerabilities.

Structured Cyber Threats

- **Resources:** Well trained individual or group.
- **Organization:** Well planned.
- **Funding:** Available.
- **Attack:** Against particular individual or organizations.
- Exploitation based on information Gathering.

Highly Structured Cyber Threats

- Extensive organization, resources and planning over time.

- Attack: Long term attack on particular machine or data.

- Exploitation with multiple methods:
    - Technical, social and insider help.

Cyber Security Threat Index Level

- Cyber threats are evaluated daily by the CTU (counter threat unit) and associated with an threat index level.

- The threat index levels are:
    - Level 1: Guarded.
    - Level 2: Elevated.
    - Level 3: High.
    - Level 4:Critical.

HACKSTUDENT

MOHAWK COLLEGE

Cyber Attacks

Types of Cyber Attacks

- Advanced Persistent Threat (APT):
    - A network attack in which an unauthorized person gains access to network and stays there undetected for a long period of time.
- Backdoor:
    - Method of bypassing normal authentication and gaining access in OS or application.

Types of Cyber Attacks Continued

- Buffer Overflow:
    - An exploit that takes advantage of the program that is waiting for a user’s input.

- Man-in-the-middle Attack
    - This attack intercepts and relays messages between two parties who are communicating directly with each other.

Types of Cyber Attacks Continued

- Cross-Site Scripting (XSS):
    - A code injection attack that allows an attacker to execute malicious JavaScript in another user’s browser.

- Denial of Service Attack:
    - Any attack where the attackers attempt to prevent the authorized users from accessing the service.

Types of Cyber Attacks Continued

- SQL injection:
  - A very common exploited web application vulnerability that allows malicious hacker to steal and alter data in website's database.

- Zero-day exploit:
  - A vulnerability in a system or device that has been disclosed but is not yet patched.

Impacts of Cyber Attacks

- A successful cyber attack can cause major damage to organizations or systems, as well as to business reputation and consumer trust.

- Some potential results include:
    - Financial loss.
    - Reputational damage.
    - Legal consequences.

HACKSTUDENT

MOHAWK COLLEGE

Malicious Code

Types of Malicious Code

- Virus:
  - Malicious software program, when it is executed, it replicates itself by modifying other computer programs and inserting its own code.

- Network Worm:
  - Standalone malware which replicates itself in order to spread to other computers.

Types of Malicious Code Continued

- Trojan Horse:
    - A program that claims to free your computer from viruses but instead introduces viruses onto your system.
- Botnet:
    - Used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allow the attacker access to the device and its connection.

Types of Malicious Code Continued

- Keylogger:
  - A type of surveillance technology used to monitor and record each keystroke typed on specific computer's keyboard.

- Rootkit:
  - Collection of tools or programs that enable administrator-level access to computer or computer network.

Types of Malicious Code Continued

- Spyware:
    - Software that is hidden from the user in order to gather information about internet interaction, keystrokes, passwords, and other valuable data.

- Adware:
    - Designed to display advertisements on your computer and redirect your search requests to advertising websites to collect marketing data about you.

Types of Malicious Code Continued

- Ransomware:
  - Malware that prevents or limits users from accessing their system, either by locking the system’s screen or by locking the user’s files unless a ransom is paid.

Vulnerabilities

What is a Vulnerability?

- A cyber-security term that refers to a flaw in a system that can leave it open to attack.

- Vulnerability is the composition of three elements:
  1. A flaw in system.
  2. Access of attacker to that flaw.
  3. Capability of attacker to exploit the flaw.

Classification of Vulnerabilities

- Vulnerabilities are classified according to the asset:
  - Hardware.
  - Software.
  - Network.
  - Personal.
  - Physical site.
  - Organizational.

Causes

- Some of the vulnerability in the system occur due to:
  - Missing patches.
  - Cleartext credentials.
  - Using unencrypted channels.
  - RF Emanation.