Cybersecurity Module- Week 3: Cybersecurity Threats and Attacks

Objective:

- Identify major types of cyber attacks.
- Understand how attacks occur and their consequences.
- Learn basic prevention and mitigation techniques.

Introduction

Cyber attacks are deliberate attempts to compromise systems, steal data, or cause harm. Understanding threats helps individuals and organizations prepare defenses.

Key Concept:

Threats target people, devices, networks, or applications.

Prevention is a combination of technology, processes, and education.

Cybersecurity Threats

1. Malware
2. Phishing & Social Engineering
3. Denial of Service (DoS)
4. Password Attacks
5. Insider Threats

1. Malware

Definition: Software designed to disrupt, damage, or gain unauthorized access to systems.

Types of Malware:

Type	Description	Example	Prevention
Virus	Attaches to files; spreads	Macro virus	Antivirus, updates
Worm	Self-replicates across networks	Conficker worm	Firewalls, patches
Trojan	Appears legitimate but harmful	Fake software installer	Antivirus, verify sources
Ransomware	Locks files until ransom paid	WannaCry	Backups, anti-malware

Example Scenario:

Juan downloads a free game from an untrusted site. The installer contains ransomware that encrypts his files.

2. Phishing and Social Engineering

Definition: Tricking individuals into revealing sensitive information.

Techniques:

Fake emails, messages, or websites

Phone calls impersonating authorities

Psychological manipulation

Example:

Maria receives a “bank alert” email requesting her login info. She clicks the link and enters credentials—her account is compromised.

Prevention:

Verify sender identity

Do not click suspicious links

Enable two-factor authentication (2FA)

3. Denial of Service (DoS) and Distributed DoS (DDoS) Attacks

Definition: Overloads systems to make them unavailable to users.

Difference:

DoS: Single source attack

DDoS: Multiple sources coordinate attack

Example Scenario:

An e-commerce website crashes during a DDoS attack, preventing customers from making purchases.

Prevention:

Traffic monitoring

Firewalls

Load balancing

4. Password Attacks

Definition: Attempts to gain unauthorized access to accounts through password cracking.

Types:

Brute Force: Trying every possible combination

Dictionary Attack: Using common words or passwords

Credential Stuffing: Reusing leaked passwords

Prevention:

Use strong, unique passwords

Enable MFA

Avoid reusing passwords

Example Scenario:

Hacker uses a leaked password database to access multiple accounts of the same user.

5. Insider Threats

Definition: Employees or insiders intentionally or accidentally causing harm to systems or data.

Examples:

Sharing sensitive files with unauthorized parties

Accidentally clicking phishing links

Sabotaging systems

Prevention:

Access control policies

Employee training

Monitoring and auditing

Case Study

Scenario:

A company suffers a malware attack after an employee opens a phishing email. Customer data is stolen, website downtime occurs, and financial loss is significant.

Analysis:

Threats involved: Phishing, malware

Prevention measures: Employee awareness, antivirus, email filtering, data backup

Discussion Questions:

1. Which threats were present in this scenario?
2. How could multi-layered security have prevented it?
3. What immediate steps should the company take after the attack?

Summary

- Cybersecurity threats include malware, phishing, DoS attacks, password attacks, and insider threats.
- Attacks can target individuals, networks, applications, and organizations.
- Prevention requires technology, user education, and policies.
- Understanding attacks is essential for mitigation and preparation.

Homework

1. Research 2 recent cyber attacks in the news. For each, identify:

Type of threat

Target and consequences

Prevention measures

2. Create a diagram of the top 5 cyber threats with prevention tips for each.
3. Write a paragraph on how human error can contribute to cyber attacks.