TRAINING DAY 21 REPORT:

- ## Introduction to Malware

Definition:

Malware (short for **Malicious Software**) is any software intentionally developed to cause **damage** to a computer system, server, client, or network.

Objective of Malware:

1. Steal sensitive data
2. Spy on user activity
3. Damage files or systems
4. Control victim's system (remotely)
5. Spread to other systems

Common Types:

- Virus
- Worms
- Trojan
- Spyware
- Ransomware
- Adware
- Rootkits

- ## Computer Virus

What is a Virus?

A **virus** is a type of malware that **attaches itself to a legitimate program or file**, replicates, and spreads from one file/system to another **when triggered by user action**.

Key Characteristics:

- Needs **host program** to function

- Activated when user **executes** infected program

- Can **replicate and spread**

Effects:

1. Slows down system

2. Corrupts or deletes files

3. Alters boot sector

4. Can spread via USB, email, or infected websites

- ## Computer Worms

Definition:

A **worm** is a self-replicating malware that **spreads automatically through networks** without needing a host file or user action.

Key Traits:

- Does **not require user intervention**

- Exploits network vulnerabilities

- Causes network congestion and system overload

Impact:

1. Slows network performance

2. Creates backdoors for other malware

3. Consumes bandwidth and storage

- ## Computer Worms – Recognize and Remove Worms from Computer

Symptoms of Worm Infection:

- Unexpected system slowdowns

- Pop-ups or unusual programs running
- Excessive bandwidth usage
- New or duplicate files appearing

- **How to Remove Worms:**

1. Disconnect from network immediately

2. Use **updated antivirus or antimalware** software

3. Perform **full system scan**

4. Manually remove suspicious startup entries

5. Update all software to patch vulnerabilities

6. Use tools like Malwarebytes, Kaspersky Virus Removal Tool, Norton Power Eraser

- **Virus vs Worms**

Feature	Virus	Worm
Needs Host?	Yes	No
Spread Mechanism	Attached to files/programs	Via networks
User Action Needed?	Yes (needs execution)	No (self-replicates automatically)
Payload	May corrupt/ delete files	Often used to open backdoors
Speed of Spread	Slower	Faster

- # Trojan

What is a Trojan?

A **Trojan Horse** is malware disguised as **legitimate software**. It tricks users into installing it, and once inside, it can:

- Steal personal data

- Give **remote access** to attackers

- Log keystrokes

- Disable firewalls

Examples:

- Fake antivirus software

- Game cracks

- Pirated software installers

Protection:

- Avoid downloading unknown software

- Use real-time antivirus monitoring

- # Spyware

What is Spyware?

Spyware secretly gathers information from a user's device **without consent**, such as:

- Browsing habits

- Keylogging (keystrokes)

- Login credentials

- Screenshots or webcam data

Impact:

1. Breach of privacy

2. Identity theft

3. System slowdown

- ## Spyware Software Products

Examples of Notorious Spyware Tools:

1. FinFisher – Government-grade surveillance tool

2. CoolWebSearch – Hijacks search engines

3. Keyloggers – Record every keystroke (hardware or software-based)

4. Spytech SpyAgent – Logs keystrokes, screenshots, chats

5. FlexiSPY / mSpy – Commercial spy tools used to monitor devices

Anti-Spyware Tools:

- Malwarebytes Anti-Malware

- Windows Defender

- SUPERAntiSpyware

- Spybot Search & Destroy