Reading material

1- Malware (Definition, Types of damage)

- **Definition**: Malware is software with malicious intent that compromises data integrity, availability, or user privacy.
- **Types of Damage**: Includes stealing information, corrupting/deleting files, and hijacking systems for further attacks.

2- Common Types of Malware

- **Viruses:** Attach to files and need user interaction to spread.
- **Worms:** Self-replicating malware that spreads through networks.
- **Trojans:** Disguised as useful software but have hidden malicious functions.
- **Ransomware:** Encrypts user data until a ransom is paid.
- **Spyware:** Tracks user activity for data theft.
- **Rootkits:** Gain unauthorized access and hide their presence.
- **Bootkits**

3- Malware Lifecycle and Infection Techniques

- **Virus Phases:** Dormant, Triggering, Propagation, Execution.
- **Infection Techniques:** Overwriting, Appending, Prepending, and cavity-based methods to evade detection.

4- Malware Obfuscation and Evasion Techniques

- **Obfuscation**: Methods like encryption, polymorphism, and stealth help malware evade detection.
- **Advanced Techniques**: Tunneling, armoring, and retro virus tactics bypass or disable security software

5- Malware Detection and Analysis

- **Static Analysis**: Inspects malware code without execution, using disassemblers and hex editors.
- **Dynamic Analysis**: Runs malware in a controlled environment (sandbox) to observe behavior.
- **Tools**: Wireshark, IDA Pro, and virtual machines are essential for analysis.

6- Prevention and Mitigation

- **Best Practices**: Regular updates, secure software, careful download habits, and strong passwords.
- **Incident Handling**: Preparation, identification, containment, eradication, and recovery.