Task 5: Malware Types & Behaviour Analysis (Basic)

1. What is Malware?

Malware is any malicious software designed to damage, disrupt, steal data, or gain unauthorized access to systems.

Common Malware Types

Type	Description
Virus	Attaches to files and spreads when executed
Worm	Self-propagates across networks without user action
Trojan	Disguised as legitimate software
Ransomware	Encrypts files and demands payment
Spyware	Steals user data silently
Adware	Displays unwanted advertisements

---

3. Malware Lifecycle (Basic)

1. **Delivery** – Email, USB, malicious download
2. **Execution** – User runs file
3. **Persistence** – Startup registry / scheduled tasks
4. **Propagation** – Network or removable media
5. **Payload** – Data theft, encryption, damage
6. **Command & Control** – Attacker communication

---

4. How Malware Spreads

- Phishing emails
- Cracked / pirated software
- USB devices
- Exploit kits
- Weak passwords

- Unpatched systems

---

5. Prevention Methods

- Updated antivirus
- OS & software patching
- Disable macros
- Firewall & IDS
- User awareness training
- Least privilege access
- Regular backups

---

6. Malware Classification Report (Deliverable)

Sample Malware: WannaCry Ransomware

Category: Ransomware
Platform: Windows
Detection Ratio: High (Multiple AV engines)
Behaviour Observed:

- Encrypts user files
- Uses SMB vulnerability (EternalBlue)
- Drops ransom note
- Communicates with C2 servers

Impact:

- Data loss
- System downtime
- Financial damage

Prevention:

- Patch SMB vulnerability
- Disable SMBv1
- Use backups
- Network segmentation

- **NAME: NITIN G N**
- Submission: Task 5
- Date & Day: 22nd January, Thursday
- Internship: Elevate Labs

THANKYOU