Task 5: Malware Types & Behavior Analysis (Basic)

Objective:
To understand different malware types and analyze their behavior using VirusTotal.

Malware Types:
- Virus – Attaches to files and spreads with user action
- Worm – Self-replicates and spreads automatically
- Trojan – Disguised as legitimate software
- Ransomware – Encrypts files and demands ransom

Tool Used:
VirusTotal (Free online malware analysis tool)

Analysis Process:
1. Search known malware hashes in VirusTotal
2. Observe detection ratios
3. Analyze behavior indicators
4. Review MITRE ATT&CK; techniques

Behavior Indicators:
- File modification
- Registry persistence
- Network communication
- Encryption activity

Malware Lifecycle:
Delivery → Execution → Persistence → Command & Control → Impact

Prevention Methods:
- Antivirus / EDR
- Email filtering
- Regular patching
- User awareness

Outcome:
Improved malware awareness and basic detection skills suitable for SOC L1 roles.