# ELEVATE LABS (CYBER SECURITY INTERNSHIP)

# Task 5: Malware Types & Behavior Analysis (Basic)

## 1. Different Types of Malware

Malware is harmful software created to damage systems or steal data.
A **virus** attaches to files and spreads when the file is executed.
A **worm** spreads automatically through networks without user action.
A **trojan** appears as a genuine program but performs malicious actions secretly.
**Ransomware** encrypts files and demands payment to restore access.

## 2. Uploading Malware Hashes to VirusTotal

Known malware samples are analyzed using **VirusTotal**.
Instead of uploading actual malware files, their **hash values** are submitted.
This method is safe and avoids infecting the system.

## 3. Analyzing Detection Reports

The detection report shows how many antivirus engines identify the file as malicious.
It also displays malware names, categories, and threat levels.
More detections usually mean the malware is widely known.

## 4. Observing Malware Behavior Indicators

Malware behavior can be identified through system activity.
Common indicators include slow performance, unknown processes, file changes, and unusual network connections.
These signs help detect malware even before damage occurs.

## 5. Understanding the Malware Lifecycle

The malware lifecycle starts with creation by an attacker.
It is then delivered to the victim and executed.
After execution, it maintains persistence and communicates with the attacker.
Finally, it performs harmful actions like data theft or system damage.

## 6. How Malware Spreads

Malware spreads through email attachments, phishing links, infected websites, and USB devices.
It can also spread through network vulnerabilities and untrusted software downloads.
User interaction often plays a major role.

## 7. Malware Prevention Methods

Malware can be prevented by using antivirus software and firewalls.
Systems should be updated regularly.
Users should avoid suspicious emails and downloads.
Security awareness is an important prevention method.

## 8. Summary of Findings

Malware exists in many forms and spreads through multiple methods.
Detection tools help identify known threats safely.
Understanding malware behavior and lifecycle improves security awareness.
Following basic security practices reduces the risk of infection.