Day 156

Topic: Malware Analysis

Objective: To analyze malicious software safely to understand its behavior.

Theoretical Concepts:
We defined types of malware: Virus, Worm, Trojan, Ransomware, Rootkit. We discussed Static Analysis (looking at code/strings) vs. Dynamic Analysis (running it in a sandbox).

Practical Work:
We uploaded file hashes to **VirusTotal** to see detection rates. We used *strings* command on a suspect executable to look for hardcoded IP addresses or domains. We observed the behavior of a sample malware in a disconnected VM, noting registry changes.

Tools Used: VirusTotal, Metasploit (for generation).

Outcome: Basic skills in identifying and analyzing suspicious files.