Task 7 :Static Malware Analysis

Objective: Analyze a suspicious binary or script file without executing it.

Tools : strings, hexdump, Ghidra, VirusTotal

Deliverables: Report showing analysis results, suspicious indicators, hash values

Hints/Mini Guide:

Use strings to extract readable content. Check imports or encoded payloads.

Outcome:Learn how malware hides in files and how analysts detect it.

Interview Questions:

1.What is malware analysis?
2.What is static vs dynamic analysis?
3.How can you identify malicious strings in a file?
4.What does VirusTotal do?
5.What are file hashes used for?
6.What is reverse engineering?
7.What are IOCs (Indicators of Compromise)?
8.What is Ghidra and how is it used?
9.How can you tell if a file is obfuscated?
10.What is the danger of opening unknown files?

Key Concepts:Malware Analysis, Static Inspection, Reverse Engineering, File Signatures

🌟 Task Submission Guidelines

🕙 Time Window:

You've got a 12-hour window—from 10:00 AM to 10:00 PM—to give your best. It's your time to shine. But remember, once the clock hits 10:00 PM, submissions close.

🔍 Self-Research Allowed:

You're not alone—but we believe in your ability to explore and grow. Feel free to use Google, YouTube, or any learning resource. Learning how to learn is your biggest strength.

🛠️ Debug Yourself:

Mistakes? Perfect. That's how real learning happens. Try solving issues on your own—it'll build your confidence and sharpen your problem-solving skills for the future.

💸 No Paid Tools:

We value learning over luxury. If any task points to a paid tool, skip it. Don't spend a single rupee. Just search for free, open-source options—we promise, it's part of the real-world hustle.

📁 GitHub Submission:

For each task, start fresh. Create a new GitHub repo.

Upload everything you used—your code, dataset, screenshots (if any), and a short README.md. That README is your story—tell us what you built, why, and how.

📩 Submission:

When you're done and proud of what you've built, drop your GitHub repo link through the submission form. Let your work speak for you.