Cybersecurity Essentials /Information Assurance
(Instructor: Saqib Hakak)

Total marks = 25

This project focuses on applying the MITRE ATT&CK framework to real-world malware behavior using public threat intelligence sources. The primary goal is to analyze malware samples through VirusTotal's public API, extract behavioral indicators (such as command execution, file operations, and network activity), and systematically map these behaviors to MITRE ATT&CK techniques.

Students will work with known malware sample hashes available from public threat intelligence feeds and **will not execute or download any malware**. The analysis will rely on **cloud-based sandbox reports from VirusTotal**, making the project safe and suitable for you all without access to a dedicated security lab.

Project Objectives

- Collect and analyze behavioral data for a curated set of malware samples using the VirusTotal public API.
- Map observed malware behaviors to the MITRE ATT&CK framework techniques.
- Identify trends and patterns of adversary techniques across different malware families.
- Visualize mapped techniques with ATT&CK Navigator or similar tools.
- Document methodology, results, and recommendations in a technical report.

Project tips:

- Collect **at least 50 malware sample hashes** representing **3–5 malware families** (e.g., Emotet, TrickBot, AgentTesla). For Grad students (75+ and more than 5 families).
- Use publicly available malware hashes from sources such as MalwareBazaar, Malpedia, or ANY.RUN.
- Retrieve behavioral data (sandbox reports, network, process, and file activity) for these samples using VirusTotal API.
- Map observed behaviors to ATT&CK techniques.
- Produce visualizations of mapping results.

NOTE:

- This project does not require you to download or execute any malware.
- Do not use paid version for VirusTotal API features
- No Live dynamic analysis or malware development required.
- **Do not copy or use malware sample collected by other group.**

Tools and Technologies

Tools	Purpose
Python (requests, pandas)	API scripting, data processing
ATT&CK Navigator	Visualizing mapped techniques
Excel / Google Sheets	Data storage and initial analysis
Matplotlib / Plotly	Optional visualization of trends

UG and Grad student project difference chart

Area	Undergraduates	Graduates
Sample Size	Minimum 50 samples from 3-5 malware families	75+ samples from 5+ families
Mapping	Manual mapping of key behaviors	Develop or use scripts/tools to assist or automate mapping
Data analysis	Use simple charts like pie chart etc	Used advanced techniques such as Jaccard similarity, clustering etc.
Literature Review	Brief overview of MITRE ATT&CK and VirusTotal	Deeper literature survey including related threat intelligence research

Example (Data analysis):

Malware Family	Techniques Used
F1	T1, T2, T3
F2	T1, T2
F3	T1, T3

Deliverables: The deliverables for this project will include:

- **Report Length:** Maximum **10-15 pages** (including figures, tables, and references).
- **Font & Format:** Times New Roman, 12pt, single-column, 1.5-line spacing, standard margins
- **Final Project**

Grading Rubric (Total: 25 Points)

Category	Points	Criteria Summary
Introduction	3	Clear objectives and background explained
Methodology	5	Detailed and clear description of sample collection, API use, mapping process
Results	5	Well-organized data presentation, relevant charts/tables, insights
Discussion & Recommendations	4	Critical analysis, limitations, practical suggestions
Report Quality & Formatting	2	Clear writing, structure, grammar, and formatting
References	1	Proper citation of all sources used
Oral Presentation	5	Clarity, confidence, content coverage, time management, visual aids quality