Basic Details of the Team and Problem Statement

PSID: KVH-008

Problem Statement Title: Malware Analysis Tool

Team Name: Hugs for Bugs

Team Leader Name: Anwarul Haque

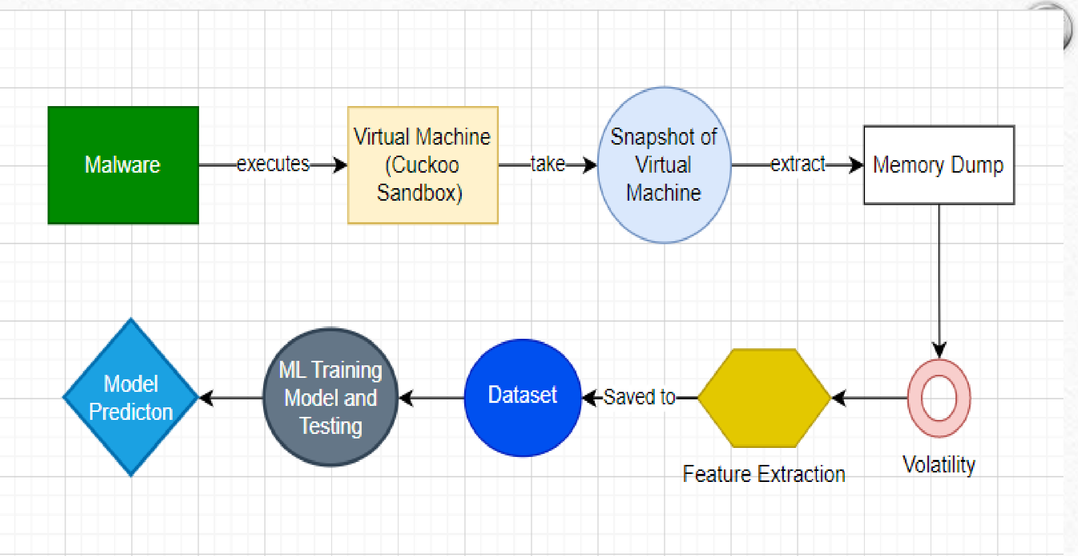
Institute Code (AISHE): C-6198

Institute Name: Techno International New Town

Idea/Approach Details

Describe your idea/Solution/Prototype here:

- The solution briefly describes a fileless malware detection method based on feature analysis using machine learning.
- Dynamic analysis of the malwares using a virtual machine (cuckoo sandbox) to capture the behavior patterns.
- Desired features are extracted using Volatility, a memory forensics tool.
- Memory forensics is an effective way to detect fileless malware which analyzes computer memory contents to identify and extract malicious activity.
- The resultant file is then trained and tested using ensemble ML methods to obtain best results on the performance metrices.
- Finally honeypots are used for collection of binary executables and labelling into the corresponding malware.



Architecture Diagram of our Approach

Describe your Technology stack here:

- Dynamic analysis of fileless malware
- Feature extraction methods
- Ensemble machine learning methods for classification of fileless malware and benign file.
- Language used – Python

Idea/Approach Details

Describe your Use Cases here:

- **Threat Hunting -** Fileless malware analysis can expose behavior and artifacts which directly effects the main memory of the system.
- **Incident Response -** The goal of the incident response (IR) team is to provide root cause analysis, determine impact and succeed in remediation and recovery.
- **Malware Research -** Academic or industry malware researchers perform malware analysis to gain an understanding of the latest techniques, exploits and tools used by adversaries.
- **Malware Detection -** By providing deep behavioral analysis, threats can be more effectively detected.

Describe your Dependencies / Show stopper here

- ➢ Virtual environment for dynamic analysis – **Cuckoo sandbox**
- ➢ Memory forensics for feature extraction – **Volatility**

Team Member Details

Sr. No.	Name of Team Member	Branch (Btech/Mtech/PhD etc):	Stream (ECE, CSE etc):	Year	Position in team (Team Leader, Front end Developer, Back end Developer, Full Stack, Data base management etc.)
1	Anwarul Haque	Btech	IT	Second	Team Leader
2	Faisal Shamim	Btech	IT	Second	Team Member
3	Aniruddha Mandal	Btech	IT	Second	Team Member
4	Tahseen Atique Ali	Btech	IT	Second	Team Member
5	MD Mujtaba	Btech	IT	Second	Team Member
6	Poushali Ghosh	Btech	IT	Second	Team Member

Team Mentor/s Details

Sr. No.	Name of Mentor	Category (Academic/Industry):	Expertise (AI/ML/Blockchain etc):	Domain Experience (in Years)
1	Anisha Mahato	Academic	ML	1