कवच
KAVACH
2023
साइबर सुरक्षा हैकथॉन
Cybersecurity Hackathon

Basic Details of the Team and Problem Statement

PSID: KVH-010

Problem Statement Title: RAM dump collection tool

Team Name: Local-Host

Team Leader Name: Shashwat Gupta

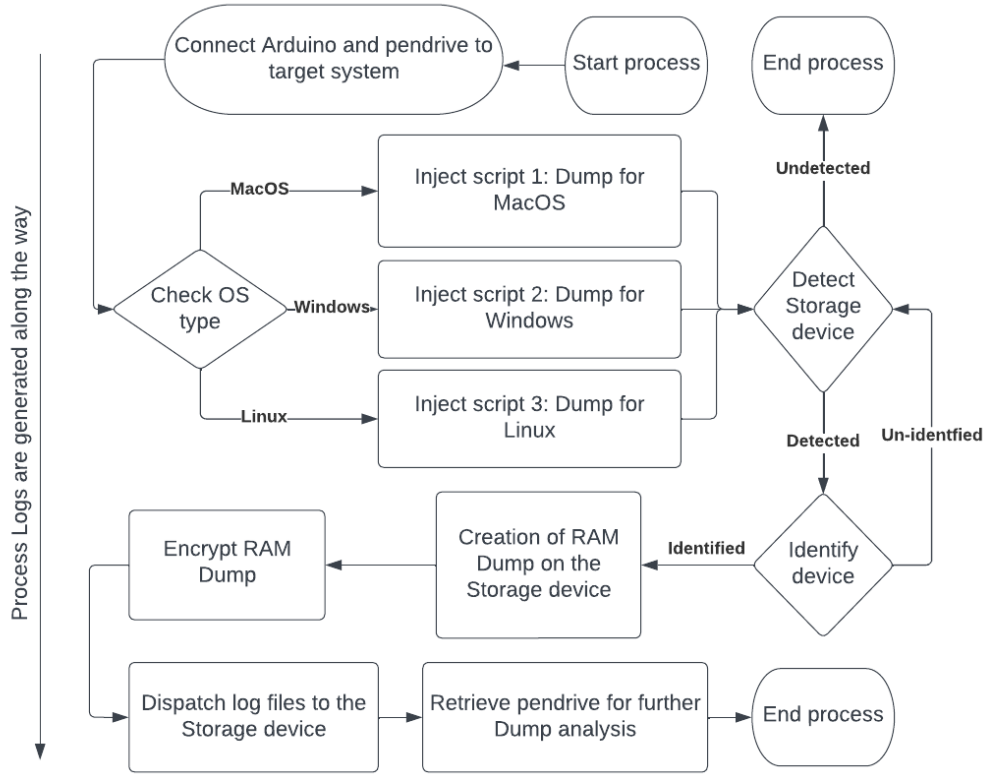
Institute Code (AISHE):

Institute Name: Amity University Lucknow Campus

Problem Statement Description: Design and develop a technological solution that can collect RAM Dump from any Windows, Linux or Mac based operating system. The solution may be in the form of an Auto-Executable/Lite Version that can be run/executed from any USB storage device without installation at the target computer system.

Idea/Approach Details

- Our solution can automatically detect the OS of the target system and generate the RAM Dump accordingly.
- We have created a **fully automated** pipeline which **does not require any human intervention.**
- There will be a controlling device (mobile/computer) linked to an Arduino using Wi-Fi functionality of Arduino where a UI will be displayed.
- This UI will enable the selection of specific processes for RAM dump collection or full system RAM dump collection. This feature will provide more targeted and efficient RAM dump collection, allowing for quicker analysis and investigation.
- The controlling device will also be used to ensure ethical usage of this device.
- Our solution ensures the security of the storage medium and target system by preventing file transfers other than the RAM dump and analyzing file signatures post-process.



PROCEDURE:

- Our solution involves intelligent usage of an Arduino's digital pins for OS detection and script injection making it **highly cost effective**.
- Based on the HIGH/LOW states of the digital pins, the OS-specific RAM Dump script gets executed.
- LED lights indicate the progress of the collection, and a final LED light indicates the completion of the RAM Dump transmission.
- The dump is then saved to a pen drive for analysis on another system.
- The dump is saved in encrypted and compressed format to prevent unauthorized access.
- Process logs are created along the way.
- In case of frozen system screen, a LED light will indicate the completion of RAM dump transmission.

Technology Stack:

- **Programming Languages** – C/C++
- **Bash scripting** - For creating bash scripts
- **Digital Forensic Tools –** such as: winpmem and avml for ramdump collection
- **Ducky Script –** For sending keystrokes to system

Idea/Approach Details

Version 2.0

- We will develop another version of the same device using an Arduino which has native DMA (Direct Memory Access) functionality, using which we can create RAM dump of any system without admin privileges.
- This will include all the features of the first version and can also access the RAM when the system is locked.
- **Unique use case:** Our device provides quick access to RAM in locked systems, saving time for government authorities to hack the system.

Use Cases

- **Forensic investigation:** Our solution can be used by forensic investigators to collect RAM Dump without human intervention, reducing the risk of data loss or alteration.
- **Malware Analysis:** RAM dump is used in malware analysis to identify the malicious activities and behavior of the malware while it is running in the memory of a compromised system.
- Our solution facilitates the collection of RAM dumps from systems where the screen has become unresponsive or frozen

Source Code: Gupta-Shashwat/localhost-KVH-010 (github.com)
Demo Video: localhost - Google Drive

Dependencies

- **Arduino :** Used for auto-executing scripts
- **Any USB Storage device :** for the purpose of storing necessary scripts, RAM Dump building software, and the resultant RAM Dump.
- **A to B-type USB connector :** For connecting Arduino to the target system.

Show stopper

- ✓ Automated and cost-effective solution for RAM Dump collection
- ✓ Collects RAM dump even from locked systems (version 2.0)
- ✓ LED lights for progress indication
- ✓ Process logs for forensic analysis
- ✓ Encrypted and Compressed RAM Dumps to prevent data breaches
- ✓ Controlling device can revoke access permissions upon unethical usage
- ✓ Can collect RAM Dump even in frozen systems
- ✓ Only allows transfer of RAM dump for added security, blocking all other file types.
- ✓ Reduces the risk of data loss or alteration
- ✓ Increases efficiency and accuracy of RAM Dump collection
- ✓ User-friendly and easy to use

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	Shashwat Gupta	B.Tech.	CSE	2	Team Leader
2	Naman Chawla	B.Tech.	CSE	2	System Administrator
3	Ashutosh Verma	B.Tech.	CSE	2	Core Developer
4	Kunal Mishra	B.Tech.	CSE	2	Hardware Engineer
5	Tanish Mishra	B.Tech.	CSE	1	DevOps Engineer
6	Anshika Gupta	B.Tech.	CSE	2	Researcher

Team Mentor/s Details

Sr. No.	Name of Mentor	Category (Academic/Industry):	Expertise (AI/ML/Blockchain etc):	Domain Experience (in Years)
1				
2				