ASW-MSCAN

Malicious File Scanner (asw_mscan) – Built a Python-based malware scanner that generates file hashes and compares them against known malicious hash datasets (VirusShare). Packaged into an executable for cross-platform use.

Overview

"asw_mscan" is an educational malware detection tool that scans files and checks whether they match known malicious hashes from a dataset (e.g., VirusShare). If a match is found, the file is flagged as potentially malicious.

This project demonstrates how hash-based malware detection works, a foundational concept in cybersecurity.

Features

🔍 File scanning – Generate MD5/SHA256 hashes of files.

📂 Batch scanning – Scan all files in a directory.

⚡ Hash comparison – Check file hashes against a malicious hash dataset.

🖥️ CLI support – Run directly in the terminal.

📏 Educational use – Designed for learning and research, not real-world AV replacement.

Safety Note 🔒

This project is for educational purposes only. Do not use it on real systems without proper isolation (VMs, sandboxes).

Installation 📦

Option 1 – Run with Python

Clone the repository:

git clone https://github.com/ADITYAdoesit /asw_mscan.git cd asw_mscan

Run The Script:

python3 asw_mscan.py

Option 2 – Run as Executable

If you built the executable with PyInstaller:

./dist/asw_mscan

Usage

It is pretty simple to use. After execution of the script, inside the terminal you will be prompted to Enter your File, you will have to choose your sample for testing.

Then, choose a database of malicious Hashes that you want to compare and match.

Now the script will generate a hash of your sample malicious file and match it with the database and give you the result.

Future Improvements

Integrate YARA rules for pattern-based detection.

Add real-time scanning capability.

Matching with Databases available Over the Internet.

Provide GUI frontend for easier use.

Author: Aditya Somnath Waghmare

LinkedIn: Click Here

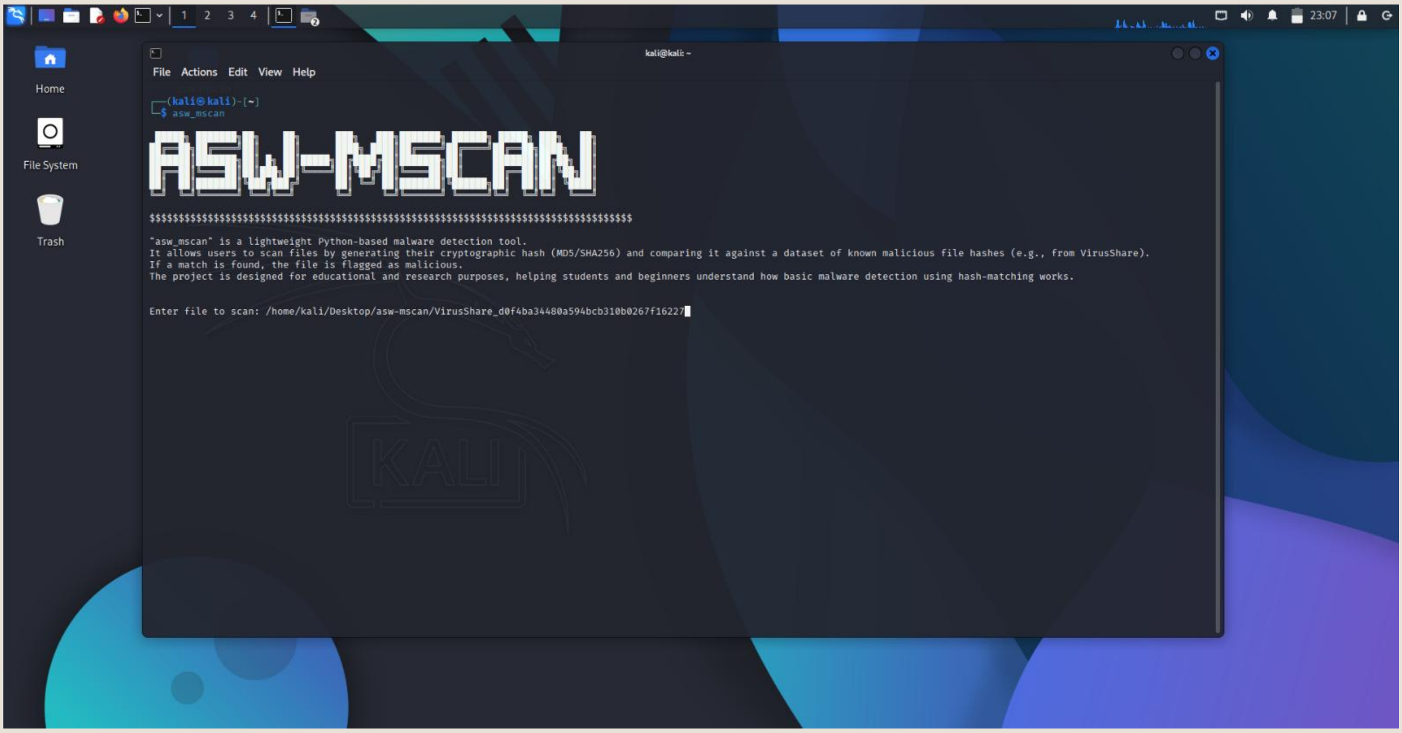
GitHub: Click Here

Website: Click Here

TryHackMe: Click Here

1) Start The “asw_mscan” Tool:

2)Enter The File You Want To Scan

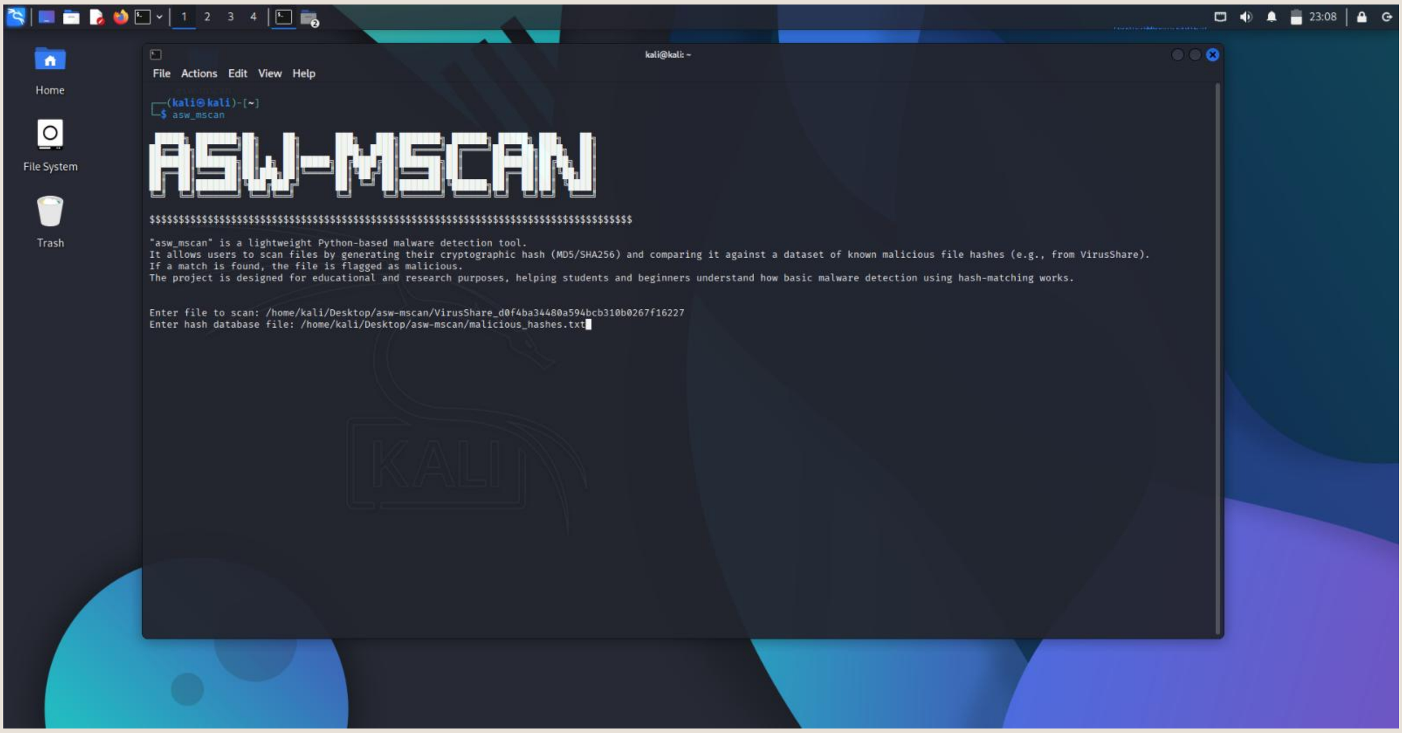


Firstly, we will scan a malicious file, when prompted by the Tool, enter the file path and its name.

This malicious sample was downloaded from VirusShare.com

Never execute these types of files on your device, make sure you handle them in a safe environment.

3)Enter The Database of Malicious Hashes:



After entering the file path and name of the malicious file, the tool will prompt you to enter the Database file which will have hashes of various malicious files. You have to provide the path and name of the dataset.

4)Press Enter To Run the Scanner And Get The Results

Now, after providing both the parameters, press Enter and let the tool analyze your file.

The tool will now generate a hash(MD5/SHA256) of your sample and match it with the database,

If match found, it will alert you that the file is Malicious! [Refer the image above].

5) Scanning Safe Samples

Now to check whether the tool is running perfectly, you can just create a sample file, it may be a simple text, pdf, img any sort of file.

By doing the same process mentioned above start the scanner and let it generate hash of your file and match it with database.

As we know the file we created was safe and had no malware in it, the scanner will label it as : Appears to be clean. [Refer the image below]

6)Result of a Safe file.