**Project Title: Threat Management**

Team Name: **CYBER BOTS**

Team Members:

* **Vinta Grishitha - grishithavinta@gmail.com**
* **Hiranmayi Ch - hiranmayichilukuri@gmail.com**
* **Erroju Vaishnavi - vaishnavierroju@gmail.com**

College: **ACE Engineering College**

Tools Used: VMWare Workstation Pro , YARA, Kali Linux, Cutter,

Application: Wepage with VirusTotal API Integration

**Project Summary**:

Analyze various kinds of threats and malware.

**Problem Statement**:

- Detect the malware from all affected systems and understanding the different threat mechanisms and purpose using various tools.

**TABLE OF CONTENTS:**

|  |  |  |
| --- | --- | --- |
| S NO | NAME | PAGE |
| 1 | YARA | 2-4 |
| 2 | PHISHING – SPAM DETECTION | 5-6 |
| 3 | MALWARE ANALYSIS | 7- |
| 4 | Integration of VirusTotal tool using API | 35-40 |

**YARA TOOL:**

YARA, which stands for "Yet Another Recursive Acronym," is an open-source tool primarily used for malware research and detection. Developed by Virus Total’s Victor Alvarez, YARA allows security professionals to create descriptions of malware families based on textual or binary patterns. These descriptions, known as YARA rules, help identify and classify malware samples.

YARA serves multiple purposes in the cybersecurity domain:

1. **Pattern Matching**
2. **Malware Identification**
3. **Forensic Analysis**
4. **Threat Hunting**
5. **Signature-Based Detection**

**STEPS:**

1. **Update System Packages and Install YARA:**

Open a terminal in your Kali Linux VM and update the package list:

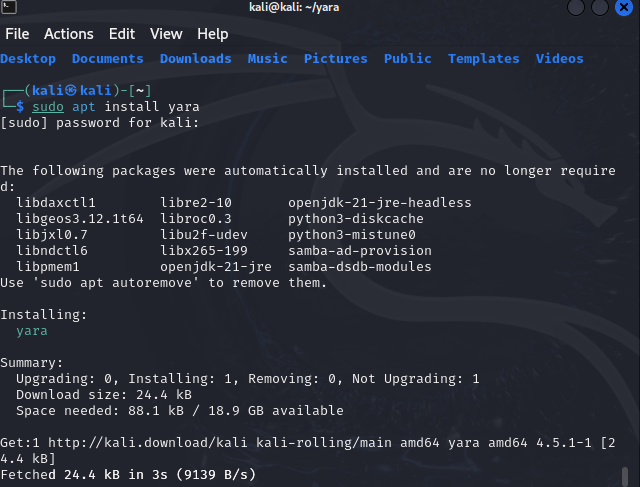
Update ensures your system has the latest package information and installs any available updates.

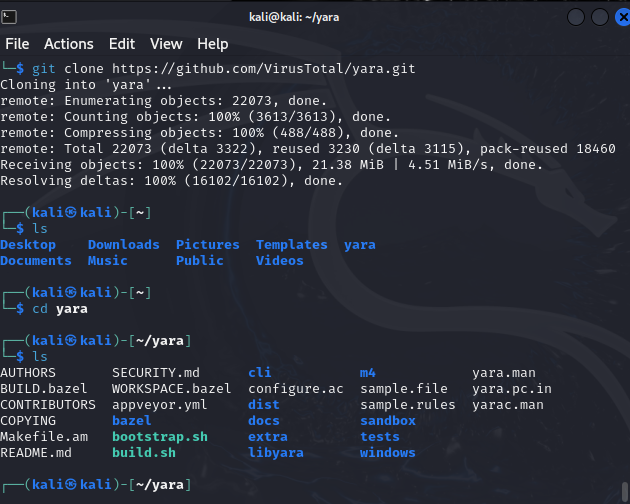
* + - * Install yara into your system using command

Sudo apt install yara

* + - * Ensure your system has the autoconf package, if not install it using the command sudo apt install autoconf.
      * Use the command pip install yara-python

1. **Clone Git repository.**
   * + - https://github.com/VirusTotal/yara.git

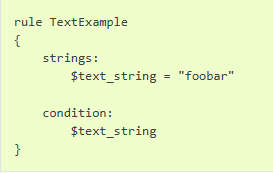


****

**YARA SYNTAX:**

rule <rule\_name>

{



// Optional metadata section

meta:

<metadata\_key> = "<metadata\_value>"

// Strings section with defined patterns

strings:

$<string\_identifier> = "<pattern>"

// Optional condition section

condition:

// Condition for when the rule should match

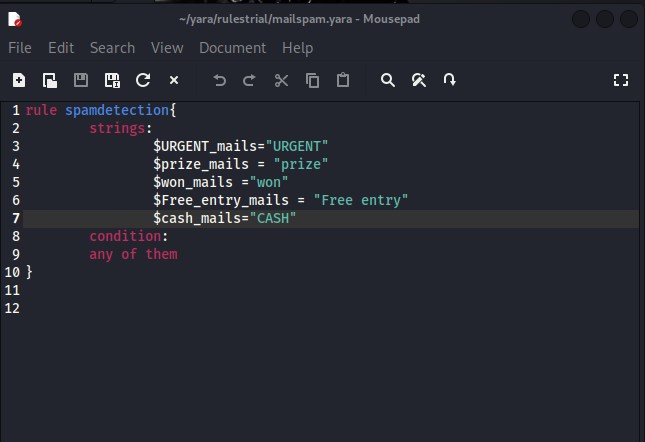
}

**Spam Detection:**

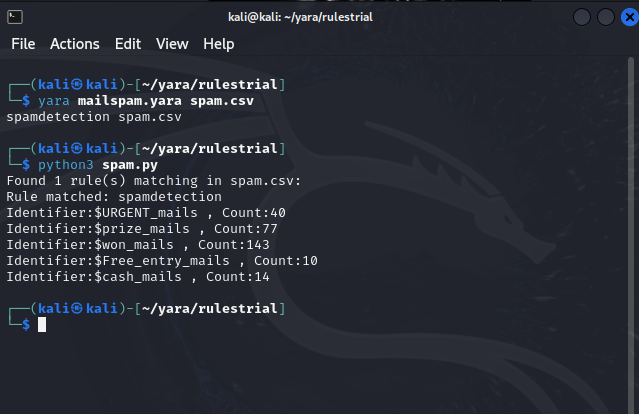
* + - * Download any spam dataset available on the internet
      * Write the yara rule
      * Apply the yara rule on the dataset , to find the spam mails

Mails with words like “URGENT”, “CASH”, “prize”, “won”, “lottery”, “free entry” ,”hiring”, “loan” ….. are ususally detected as spam mails.

PYTHON FILE:

****

OUTPUT :

****

**DOWNLOADING THE MALWARE:**

* From any git repository, safely download the malware samples.
* Ensure to download the samples only from the safe sites / GitHub repositories like Zoo Repository available on the internet.

https://github.com/ytisf/theZoo

* Make sure to download the files in an isolated environment like a VMware workstation.

**STEPS TO CHANGE THE NETWORK SETTINGS:**

* Go to VMware settings, and open the network settings.
* Change the network settings to HOST ONLY settings.

**VIRUSES WE USED FOR OUR PROJECTS:**

1. **Zeus Banking Trojan**
2. **No Mercy Virus**

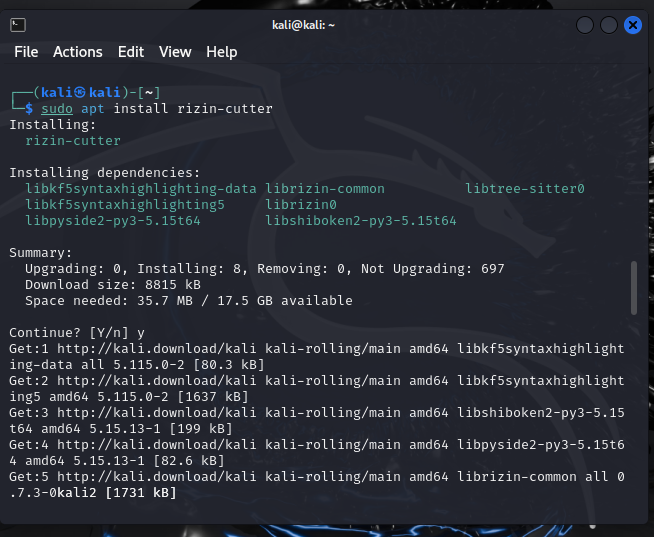
**CUTTER TOOL:**

Cutter is a powerful tool used for reverse engineering and analysing executable files and binaries. It is a graphical user interface (GUI) for the Rizin framework, which is an open-source reverse engineering toolkit designed to make the process of dissecting and understanding malware more efficient and accessible.

**Steps to use cutter:**

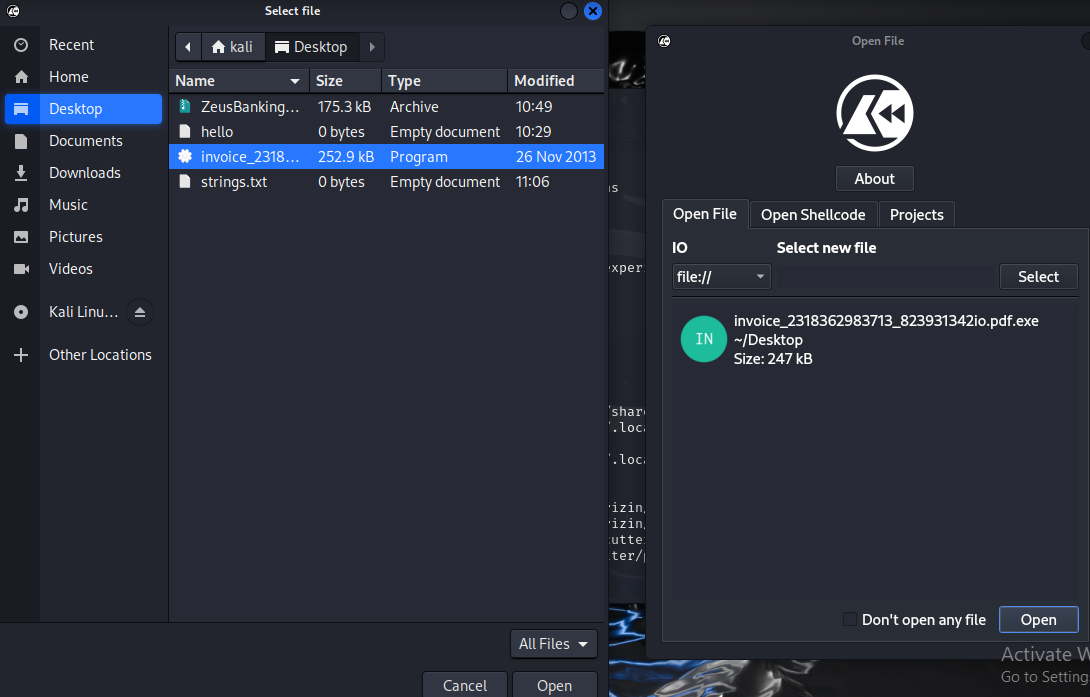
* Install the rizin-cutter in the kali linux using the command

Sudo apt install rizin-cutter

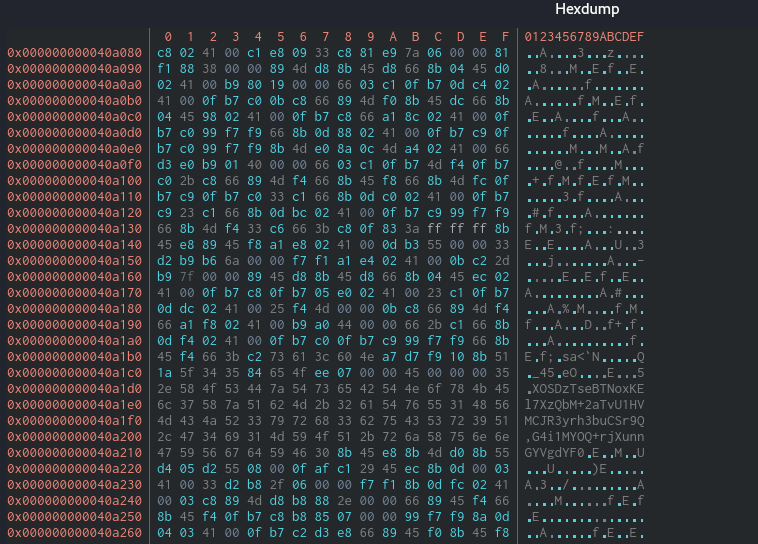


* Open the cutter using the command

cutter



* The below is the hex dump of the function.

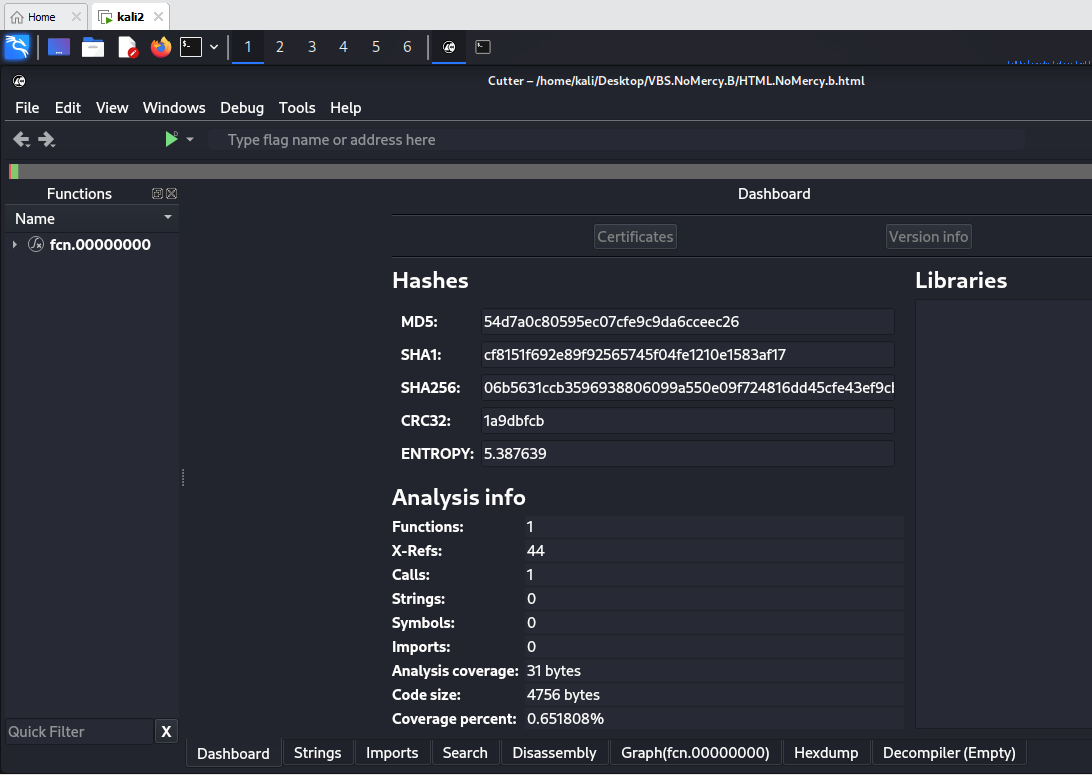


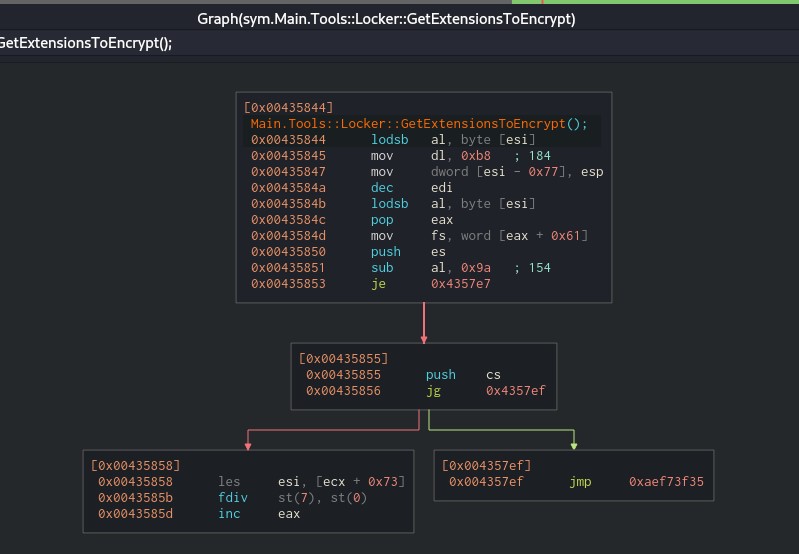
**NO MERCY VIRUS**

The No Mercy Virus was particularly harmful due to its aggressive nature and the significant damage it could inflict on infected systems.

The No Mercy Virus was known for its highly destructive payload. Once it infected a system, it often led to the deletion of critical files or entire directories. This resulted in loss of data and potentially rendered the system inoperable.

We will get the basic information such as the filename and details, hashes and analysis information using cutter.



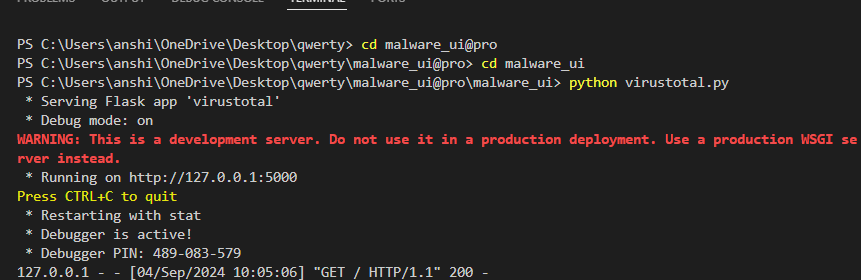


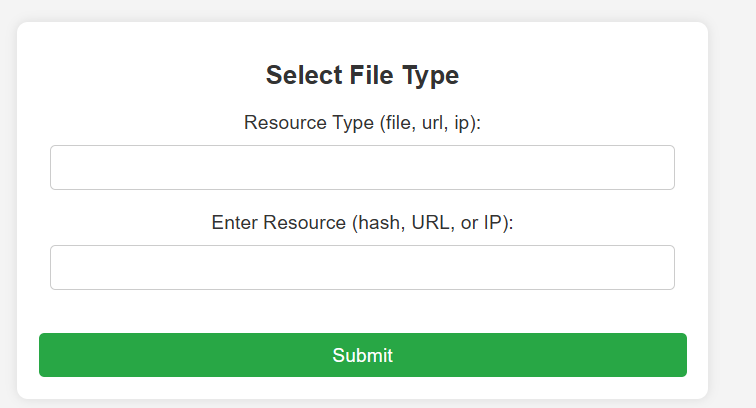
**CREATED A WEB APPLICATION WITH INTEGRATION OF VIRUSTOTAL API:**

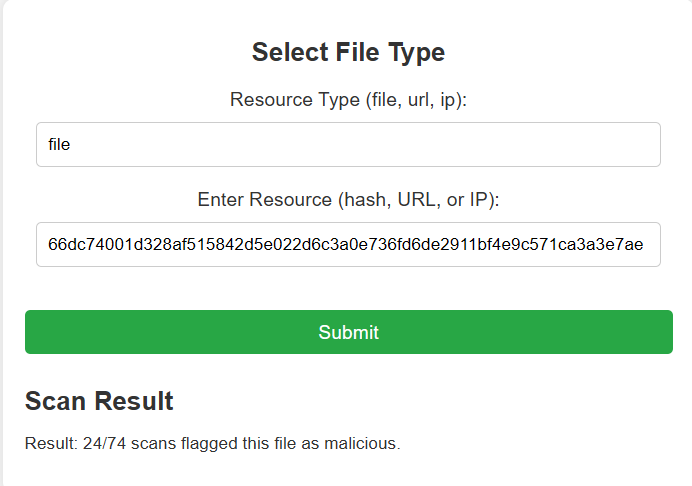
Advanced Malware Analysis Web Interface:

To streamline and modernize the detection of malicious content, we have engineered an advanced web interface that empowers users to evaluate the security status of URLs or hash values. Leveraging the VirusTotal API, this interface provides thorough, real-time analysis to determine the potential threat level of the provided inputs.

Technologies Employed: HTML, CSS, JAVASCRIPT

****



****

**Conclusion:**

Our cybersecurity initiative focused on developing a cutting-edge web-based tool for comprehensive malware analysis and threat detection. This tool allows users to input URLs or hash values for in-depth evaluation of potential risks. It leverages both VirusTotal API integration and YARA rules to enhance threat detection capabilities.