International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

EXESCAN - MALWARE DETECTOR FOR EXECUTABLE FILE

[1] NIJANTHAN.N, [2] AKASH.K, [3] KESHAVAN.T, [4] VINOTH KUMAR.M

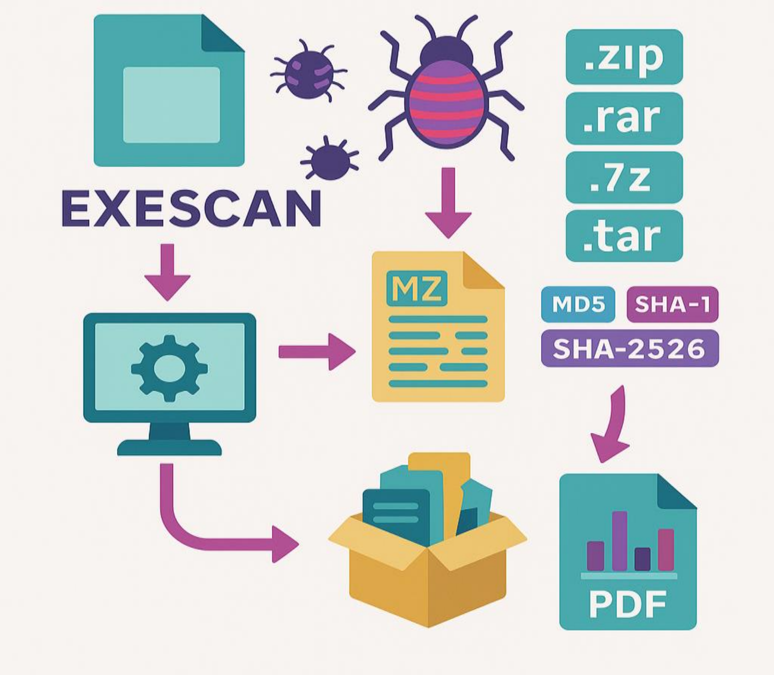
[1234] Paavai institution, India.

ABSTRACT :

EXESCAN is an advanced Python-based file scanning tool designed to analyze executable files and compressed archives for potential security threats. The pri mary objective of this project is to assist cybersecurity professionals and analysts in detecting malicious files by examining their metadata, structure, and digital signatures. EXESCAN supports a wide range of file formats including .exe , .zip , .rar , .7z , and .tar. It performs static analysis on executable files, extracting important attributes such as PE headers, import/export tables, and hash values (MD5, SHA-1, SHA-256) to identify anomalies. For archive files, it recursively extracts and scans the contents to ensure deep inspection. The tool also generates a detailed PDF report summarizing the analysis, making it suitable for documentation and forensic investigations. With its lightweight CLI interface and extensible architecture, EXESCAN is a valuable asset for malware analysts, incident responders, and cybersecurity researchers aiming to automate and enhance threat detection workflows. EXESCAN enhances threat detection by combining static analysis with multi-format archive scanning. Its automated reporting and extensibility make it ideal for security audits and forensic investigati ons.

1 INTRODUCTION

In the ever-evolving landscape of cybersecurity, detecting and analyzing malicious files is a critical aspect of protecting systems and data. With cyber threats becoming more sophisticated, there is a growing need for tools that can perform reliable static analysis and offer insights into potentially harmful executables and archived files. To address this challenge, we developed EXESCAN, a Python-based file scanning solution tailored for cybersecurity professionals, malware analysts, and digital forensics investigators. EXESCAN is capable of scanning a variety of file formats including executable files (`.exe`) and compressed archive formats such as `.zip`, `.rar`, `.7z`, and `.tar`.



The tool performs deep static analysis on executable files by inspecting PE (Portable Executable) headers, analyzing import/export functions, and generating cryptographic hashes (MD5, SHA1, SHA256) to help identify known threats. When dealing with archive files, EXESCAN automatically extracts and scans the contents recursively, ensuring that embedded threats do not go unnoticed. One of the standout features of EXESCAN is its ability to generate a detailed PDF report, summarizing metadata, scan results, and potential indicators of compromise (IOCs). This makes it extremely useful for documentation and reporting purposes in real-world security investigations. With its command-line interface, modular structure, and potential for integration with threat intelligence platforms, EXESCAN is a powerful tool for strengthening file-level threat analysis. EXESCAN aims to simplify the malware analysis process by providing actionable insights through automated scanning and reporting. Its modular design allows for future enhancements like YARA rule integration and VirusTotal API support.

2 OBJECTIVE

The primary objective of the EXESCAN project is to develop a comprehensive and efficient file scanning tool that aids in the detection and analysis of potentially malicious executable and archive files. In the current cybersecurity landscape, where threats are increasingly complex and often hidden within legitimatelooking files, EXESCAN aims to bridge the gap by providing security analysts, ethical hackers, and forensic investigators with an automated solution for file inspection and threat identification. EXESCAN is designed to perform static analysis on `.exe` files, extracting critical information such as PE (Portable Executable) headers, import/export functions, and generating unique hash values (MD5, SHA-1, SHA-256) for threat correlation. It also supports scanning of compressed archive formats including `.zip`, `.rar`, `.7z`, and `.tar`, by recursively extracting their contents and analyzing each file individually. An essential goal of EXESCAN is to simplify threat detection by offering a command-line interface that is lightweight, modular, and suitable for automation or integration into larger security operations.

Another key objective is the generation of detailed, well-structured PDF reports that summarize metadata, file structures, hash results, and any detected anomalies—providing documentation useful for audits, incident response, and forensic investigations. Furthermore, EXESCAN is built with extensibility in mind, making it adaptable for future enhancements such as integration with threat intelligence sources, YARA rule-based detection, and real-time file monitoring. Ultimately, the objective of EXESCAN is to provide a reliable, opensource tool that enhances file-level threat visibility and supports proactive cybersecurity defense strategies.

EXESCAN aims to provide a reliable file scanning solution for detecting malicious executable and archive files. It performs static analysis, metadata extraction, and generates detailed PDF reports. The tool enhances threat visibility and supports cybersecurity investigations with automation and extensibility. EXESCAN is designed to be lightweight, modular, and easily integrable into security workflows. EXESCAN is built to streamline filelevel threat detection through automated scanning and detailed reporting. Its modular design allows for easy expansion, making it adaptable for future security needs and integration with threat intelligence platforms.