JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PACKET SNIFFER WITH MALWARE DETECTION USING VIRUSTOTAL API

[1]Sheeba P. S., [2]Adnan Shaikh, [3]Inzamam Shaikh, [4]Maruf Shaikh, [5]Misbahuddin Shaikh,

[1]Associate Professor, [2-5]Undergraduate Student,
[1] Computer Engineering, [2-5] Computer Science & Engineering (IoT & CSBT)
[1]Lokmanya Tilak College of Engineering, Navi Mumbai, India

Abstract: With the rapid expansion of network-based systems and Internet-enabled devices, cybersecurity threats such as malware, ransomware, and unauthorized intrusions have increased significantly. Traditional packet sniffing tools provide detailed traffic analysis but lack automated mechanisms for identifying malicious activity in real time. This paper presents a packet sniffer integrated with malware detection using the VirusTotal threat intelligence platform. The proposed system captures live network packets, extracts critical packet attributes, and analyzes source IP addresses through the VirusTotal API to determine their malicious nature. A graphical user interface (GUI) is implemented to visualize real-time traffic and detection results, enhancing usability and accessibility. Experimental observations demonstrate that the system effectively detects malicious IP addresses and logs network activity for further analysis, making it a practical solution for proactive network security monitoring.

IndexTerms **- Packet Sniffing, Malware Detection, Network Security, VirusTotal API, Cybersecurity**

I. INTRODUCTION

Cybersecurity has become a critical area of focus in the digital era, where data breaches, ransomware attacks, and other cyber threats pose significant risks to individuals, organizations, and governments. Protecting sensitive information and maintaining the integrity of digital systems requires continuous advancements in threat detection and mitigation strategies. Network traffic monitoring is an essential component of these strategies, as it provides a window into the activities occurring within a system and helps identify unusual or malicious behavior. However, with the rapid increase in network traffic and the growing sophistication of cyberattacks, traditional monitoring tools often struggle to keep pace.

This work addresses these challenges by combining real-time packet sniffing with advanced malware detection capabilities. Packet sniffing enables the capture and analysis of live network traffic, providing detailed insights into data flow, including source and destination IP addresses, packet size, and protocols used. By integrating this capability with the VirusTotal API, a widely recognized threat intelligence service, the project enhances the ability to detect and analyze malicious activity in real time.

The tool is designed with usability and efficiency in mind, featuring an interactive graphical user interface (GUI) that simplifies the process of monitoring network traffic, identifying threats, and logging results for further analysis. The GUI not only displays live results but also provides detailed information about malicious packets, including reputation scores, malicious counts, and threat categories. This combination of technical depth and user-friendly design ensures that the tool is accessible to both seasoned cybersecurity professionals and network administrators with limited technical expertise.

By offering real-time monitoring, seamless malware detection, and actionable insights, the project serves as a robust and practical solution for modern cybersecurity challenges. Its ability to detect threats proactively and provide comprehensive analysis positions it as a valuable asset in the ongoing battle against cybercrime.

II. Literature Survey

The fields of packet sniffing and malware detection have been extensively studied in network security, leading to the development of tools and frameworks that address various aspects of threat detection. Tools like Wireshark have become industry standards for packet capture and analysis, offering detailed insights into network traffic. However, such tools lack built-in capabilities for real-time malware detection and rely on manual inspection to identify suspicious activity.

Several research studies have explored the integration of threat intelligence services, such as VirusTotal, into network monitoring systems. These efforts have demonstrated the potential for real-time analysis and detection of malicious activity by correlating network data with external intelligence databases. For example, systems that use APIs from threat intelligence services have shown success in identifying suspicious IPs, domains, or files in a timely manner.

Despite these advancements, existing implementations often fall short in usability and accessibility. Many tools require significant technical expertise to operate, limiting their adoption among non-specialist users. Additionally, some solutions focus on either packet capture or malware detection but do not provide a cohesive, integrated platform that combines these functionalities.

This work builds on prior research and tools by addressing these gaps. It integrates real-time packet sniffing with VirusTotal's threat intelligence API, allowing for automated detection of malicious IP addresses. Furthermore, the inclusion of an intuitive graphical user interface (GUI) enhances accessibility and usability, ensuring that even users with limited technical expertise can leverage the tool effectively. By offering detailed threat insights, such as malicious counts, reputations, and categories, the project sets itself apart as a comprehensive and user-friendly solution for network security monitoring.

The proposed system addresses these gaps by integrating packet sniffing, threat intelligence analysis, and GUI-based visualization into a single cohesive platform.

III. Comparison with Existing Implementations

Existing tools like Wireshark and Snort are widely used in the field of network monitoring and security. Wireshark excels in packet capture and deep packet analysis but lacks built-in capabilities for real-time malware detection or integration with threat intelligence databases such as VirusTotal. Users must manually inspect packets and cross-reference suspicious data with external resources, which can be time-consuming and prone to oversight.

Snort, on the other hand, is an intrusion detection and prevention system (IDS/IPS) that offers robust real-time monitoring capabilities. However, its configuration and use often require advanced technical expertise, and it does not natively integrate with services like VirusTotal to provide enriched threat intelligence data for malicious IP detection.

This project addresses these limitations by offering a unified solution that integrates real-time packet sniffing with automated malware detection using VirusTotal's API. Unlike Wireshark and Snort, this project includes an intuitive graphical user interface (GUI) that simplifies the monitoring process, making it accessible to both technical and non-technical users. It also enhances usability through features such as detailed threat insights, including packet size, reputation, and category information, which are absent in many traditional tools.

Additionally, the real-time detection and automated logging features in this project streamline network monitoring workflows, providing immediate feedback on potential threats. This comprehensive and user-friendly approach bridges the gap between packet analysis and actionable threat intelligence, making it a valuable alternative to existing solutions.

IV. Methodology

This project implements a systematic approach to detect malicious activity in network traffic by combining packet sniffing and threat intelligence analysis. The methodology involves the following key steps:

1. Packet Capture

The process begins by capturing live network packets using the Scapy library. Scapy enables real-time sniffing of packets from a specified network interface, ensuring that the tool collects all network traffic passing through the interface.

2. Data Extraction:

Once the packets are captured, relevant information such as source and destination IP addresses, packet size, and protocol type is extracted. These details are crucial for subsequent analysis and threat detection.

3. Threat Analysis:

The extracted IP addresses are queried against the VirusTotal API, which provides threat intelligence by cross-referencing the IP addresses with its database of known malicious records. The analysis includes identifying malicious activity, reputation scores, and associated threat categories for each IP address.

4. GUI Display:

A user-friendly graphical user interface (GUI) is developed using Tkinter. This interface displays real-time packet data along with the analysis results, making it easy for users to monitor suspicious activity. Malicious packets are highlighted for better visibility, and additional threat information is presented in an organized format.

5. Logging:

The tool includes functionality to save packet details and analysis results in CSV format. This feature allows users to maintain records for further investigation or compliance purposes, ensuring that all monitored activity is securely logged.

This methodology ensures a comprehensive, real-time, and user-friendly solution for detecting malicious network activities, combining advanced technical capabilities with intuitive usability.

V. RESULTS

Fig. 1

Fig. 1 displays the initial landing page of the application, built using Tkinter. It provides a user-friendly interface for starting the packet sniffing process, allowing users to specify the network interface and begin monitoring with a single click.

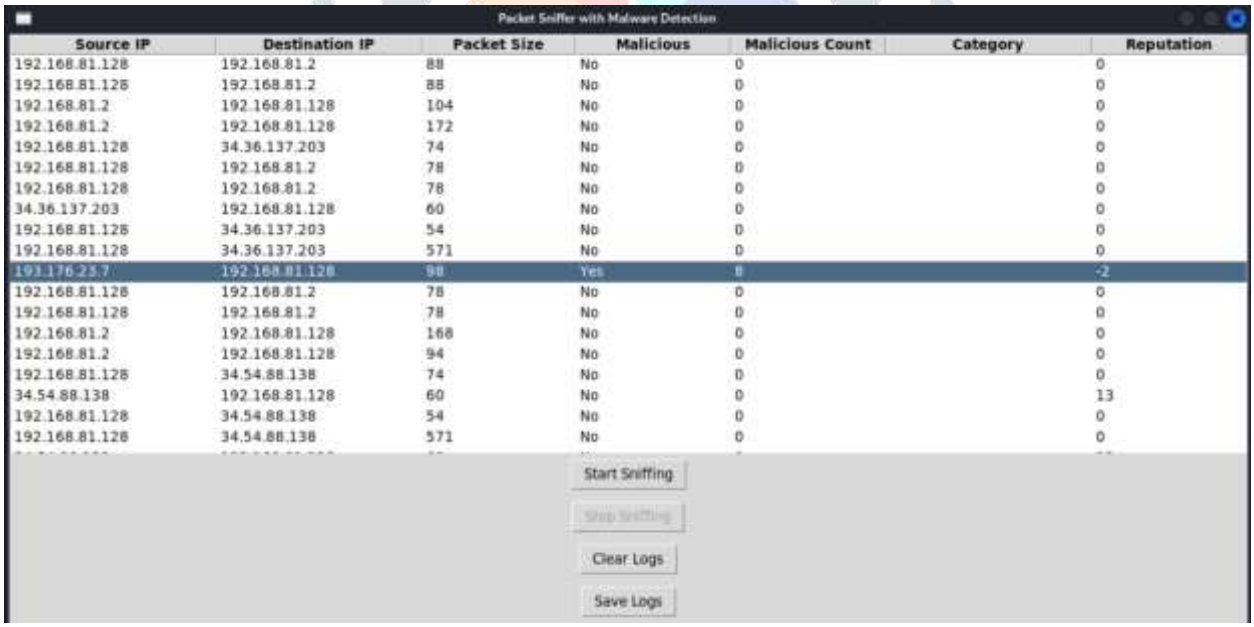

Fig. 2

Fig. 2 shows the GUI after packet sniffing has started. It dynamically displays captured packets along with their source and destination IP addresses, and indicates whether the source IP is flagged as malicious or clean based on VirusTotal's analysis.

Fig. 3 demonstrates the feature that allows users to save the captured packet data and VirusTotal results to a CSV file. With a simple button click, the application exports the session log, enabling further offline analysis and record-keeping.

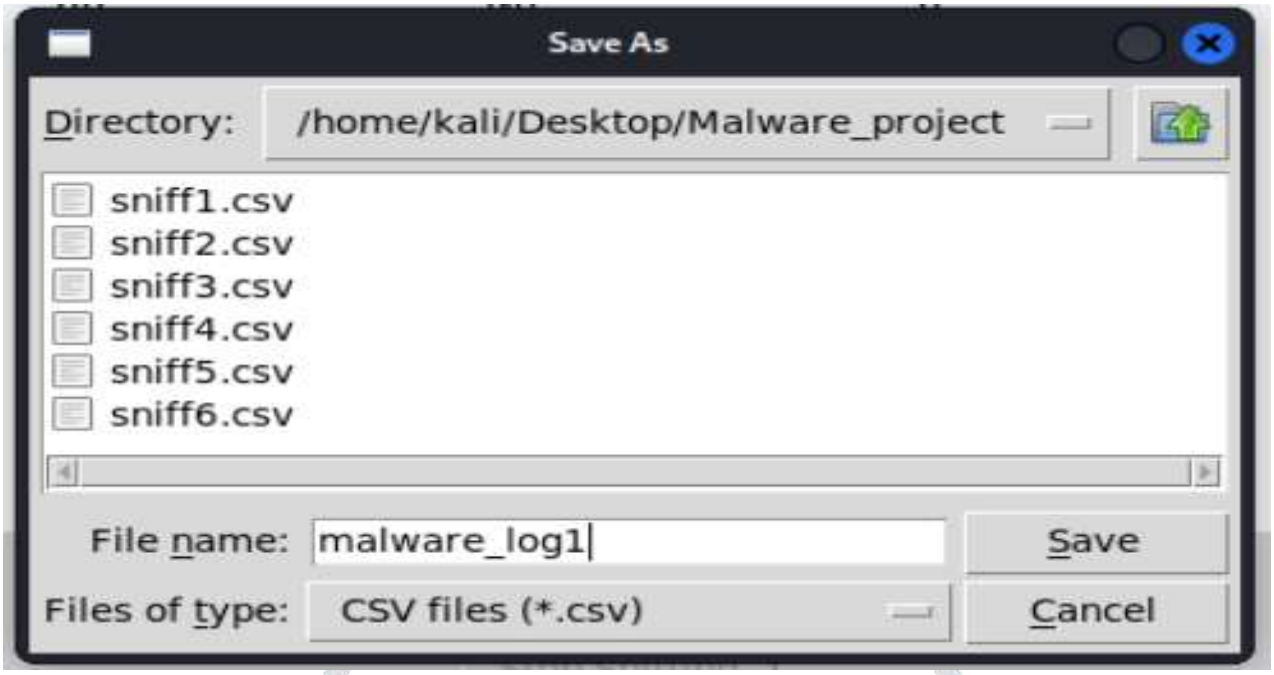

Fig. 3

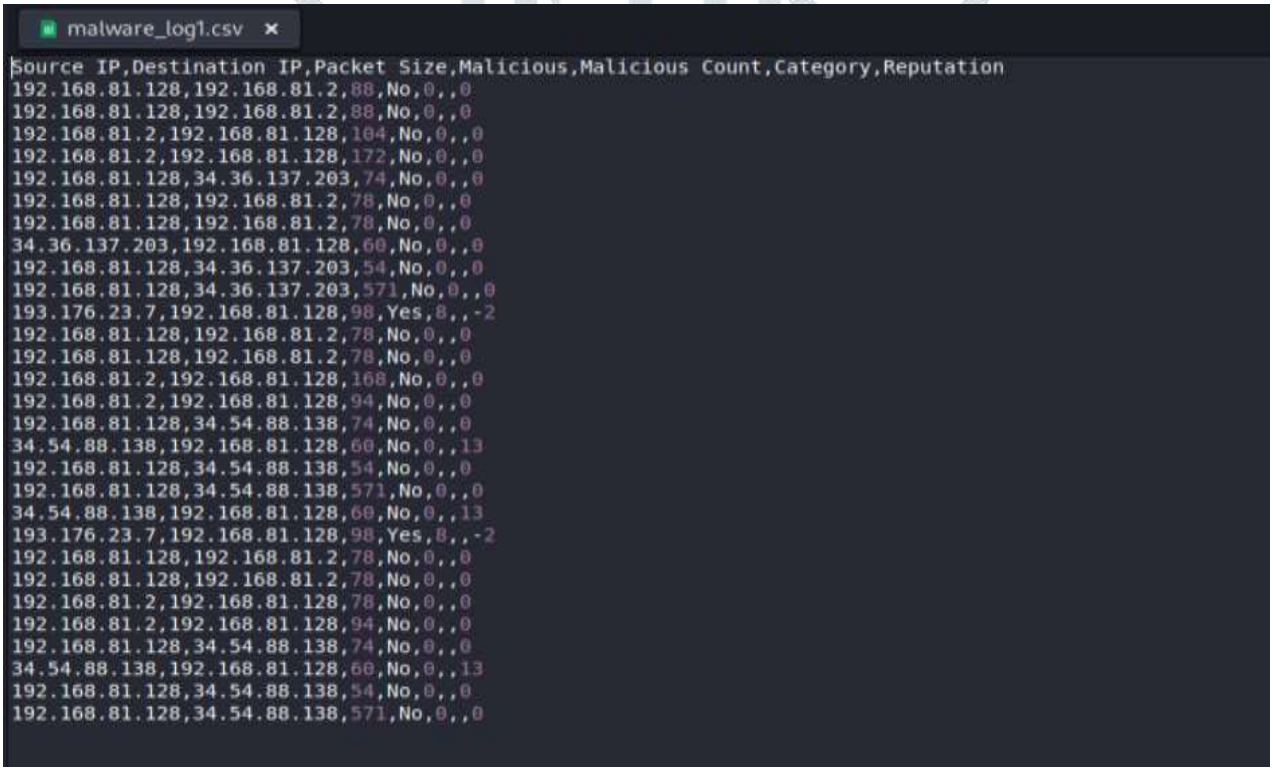

Fig. 4

Figure 4 showcases the generated CSV file containing the logged data. Each entry includes the timestamp, source IP, destination IP, and the VirusTotal status (malicious or clean), providing a structured and accessible format for later analysis or reporting.

VI. FUTURE SCOPE

The project "Malware Detection Using Sniffing Technique" has significant potential for future advancements, ensuring its relevance in dynamic cybersecurity environments.

1. Deep Packet Inspection (DPI):

Incorporating DPI would allow the tool to analyze packet payloads in addition to headers, enabling more detailed detection of malicious content, such as embedded malware or suspicious payload patterns.

2. Support for Additional Threat Intelligence APIs:

Expanding beyond VirusTotal, integrating other APIs like AlienVault OTX, IBM X-Force Exchange, or Cisco Talos could provide richer threat intelligence and improve the accuracy of malicious activity detection.

3. Enhanced Malware Detection Capabilities:
Future versions could detect malware based on behavior analysis, anomaly detection, or integration with machine learning algorithms, making the tool more robust against evolving threats.
4. Multi-Interface and Multi-Protocol Support:
Extending support for multiple network interfaces and protocols (e.g., IPv6, FTP, DNS) would broaden the tool's applicability across diverse network environments.
5. Cloud Integration and Remote Monitoring:
Adding cloud-based features for remote monitoring and storing logs in a secure, centralized location would enhance the tool's scalability and ease of access.
6. Customizable Alerts and Automation:
Developing automated responses (e.g., blocking IPs, notifying administrators) based on detected threats and allowing users to configure alerts for specific criteria would further streamline security operations.

VII. CONCLUSION

This project highlights the effective integration of packet sniffing and malware detection into a single, cohesive, and user-friendly tool. By leveraging the VirusTotal API for advanced threat intelligence, it enables real-time identification of potentially malicious network activity, offering a significant enhancement to traditional network monitoring tools. The intuitive graphical user interface (GUI) simplifies the complex task of network analysis, making it accessible even to those with limited technical expertise. This combination of real-time packet capture, automated malware detection, and easy-to-use interface provides a robust solution for organizations seeking to enhance their network security posture. By delivering actionable insights and comprehensive logging capabilities, the project demonstrates its practicality and effectiveness in real-world network security scenarios.

REFERENCES

[1] M. Roesch, “Snort – Lightweight Intrusion Detection for Networks,” *Proceedings of the 13th USENIX Security Symposium*, 1999.
[2] Wireshark Foundation, “Wireshark: Network Protocol Analyzer,” Available: https://www.wireshark.org
[3] P. Cabaj and D. Kotulski, “Network security analysis using packet sniffers,” *International Conference on Dependability of Computer Systems*, 2007.
[4] N. Ye and Y. Zhang, “Supervised clustering of HTTP traffic for malware detection,” *IEEE ISI*, 2015.
[5] A. Bagnall, “Crowdsourcing malware detection with VirusTotal,” SANS Institute, 2014.
[6] VirusTotal, “VirusTotal Online Malware Scanner,” Available: https://www.virustotal.com