# Virtualized Apt Detection Framework Using Wazuh and Virus Total

Priyank Kumar Kartikey[1], Apoorv Khare[2]

[1,2] *Shri Ram Institute of Technology, Jabalpur, M.P.*

***Abstract*—Cybersecurity is a major concern in today's connected world. As digital technologies grow, they bring new opportunities but also more advanced threats. Cyber threats are evolving quickly, with attackers constantly improving their methods to find and exploit weaknesses, bypassing traditional security measures. To counter these challenges, organizations need to adopt proactive and integrated strategies to protect their digital assets and ensure smooth operations. This paper aims to develop and implement a thorough security framework within a virtual environment. By using virtual machines (VMs) with Ubuntu and Windows, and integrating advanced security tools like Wazuh , Virus Total, and Kali Linux, we simulate real-world cyber threats and improve our defensive capabilities. The main goal is to show how these integrated solutions can effectively detect, mitigate, and respond to various cyber threats, including Advanced Persistent Threats (APTs).***

***Index Terms*—** Virtual machine**, cybersecurity, Advanced persistent Threats.**

## I. INTRODUCTION

The method of identifying APT attacks was introduced based on a newly constructed APT attack dataset. APT attacks of the various attack types. Data that was gathered consisted of five types, i.e., normal, reconnaissance, initial compromise, lateral movement, and data exfiltration.[1].

The most important conclusions of the study and also highlights the importance of countering APTs in the current threat environment. It emphasizes the significance of proactive detection and sustained monitoring, and mitigation measures to improve the resilience of organizations to APTs [2,3].

According to the statistics by Kaspersky Lab, most of the attack attempts are known viruses with known signatures, then there is unknown malware, and only a small percentage of advanced malware. The presence of security solutions in companies is important in reducing any form of threats encountered by businesses [4,5,6].

One such issue is advanced persistent threats which are a cause of concern to businesses of both small and big sizes. These are very specific and high-tech attacks, which may be hard to identify and prevent and inflict severe damage on the network and systems of an organization [8].

In order to safeguard against APT attacks, companies should introduce an effective security framework, comprised of various current protection systems. This can involve traffic monitoring tools, EDR and XDR tools, routine penetration testing, and good access control. Through such measures, organizations will be able to better detect and react APT attacks, and will be able to minimize the chances of a successful attack [9,10,11,12].

The paper concludes that Convolutional Neural Networks (CNN) are the best tool to use to identify Advanced Persistent Threats (APTs) in cybersecurity [13,14] The paper highlights the necessity to keep researching and innovating to stay up to date with the changing cybersecurity threats.]

APTs pose a significant risk to large companies and states due to their stealthy nature and ability to cause extensive damage. By analyzing network traffic patterns and utilizing advanced artificial intelligence models, particularly in the data exfiltration stage, significant improvements in detection capabilities can be achieved, enhancing overall cybersecurity measures against APT attacks.[16]

Advanced Persistent Threats detection through Artificial Intelligence based Deep Packet Inspection Allard Dijk advanced persistent threats (APTs) are a major threat to large enterprises and states because they are stealthy and can inflict as much damage as possible. [17,18]

By analyzing network traffic patterns and utilizing advanced artificial intelligence models, particularly in the data exfiltration stage, significant improvements in detection capabilities can be achieved, enhancing overall cybersecurity measures against APT attacks.[19]

Current approaches to APT detection reveal the inadequacy of traditional methods, prompting the development of sophisticated, bottom-up and top-down strategies to enhance detection capabilities against advanced threats.[20].

## II. LITERATURE REVIEW

The motivation behind this project stems from the critical need to fortify organizational defenses against increasingly advanced cyber threats, especially the Advanced Persistent Threats (APTs). Contrary to traditional cyber attacks., APTs are stealthy and persistent, often designed to remain undetected within an organization's network for extended periods. This persistence allows attackers to conduct espionage, exfiltrate sensitive data, or disrupt operations without immediate detection.

i. Wazuh

Wazuh is an open-source security monitoring application that provides an extensive insight into the activities of the system and possible threats. It is designed to detect intrusions, monitor system integrity, and provide real-time security information. This platform integrates various security capabilities into a single solution, making it a powerful tool for organizations looking to enhance their cybersecurity posture. Wazuh combines log analysis, vulnerability detection, and incident response, providing a unified approach to threat management.

Wazuh is built on a flexible and scalable architecture that includes agents, the Wazuh manager, and the Elastic Stack (Elasticsearch, Logstash, and Kibana). Agents are deployed on monitored endpoints to collect security data, which is then processed by the Wazuh manager. The Elastic Stack stores and visualizes the collected data, offering powerful search and analytics capabilities.

This architecture allows Wazuh to process data in large quantities effectively, and is therefore appropriate both to small businesses and large enterprises.

ii. MISP

MISP (Malware Information Sharing Platform & Threat Sharing) is a free and open-source platform designed for the collection, sharing, storing, and distribution of cyber threat intelligence (CTI). Developed initially by the Belgian Defense and supported by the European Union, MISP has evolved to become a pivotal tool in the cybersecurity community. Its primary objective is to improve the detection, prevention, and response to cyber threats by enabling organizations to share detailed threat information effectively and securely. MISP's collaborative nature allows for enhanced situational awareness and collective defense against sophisticated cyber adversaries.

iii. APT

Advanced Persistent Threats (APTs) represent one of the most sophisticated and dangerous types of cyber-attacks facing organizations today. Unlike traditional cyber threats, APTs are characterized by their highly targeted, sustained, and stealthy nature. These attacks are typically carried out by well-funded and highly skilled adversaries, often with specific goals such as espionage, data theft, or sabotage. The persistence and advanced tactics used in APTs make them particularly challenging to detect and mitigate, necessitating robust and comprehensive security strategies.

APTs often involve a prolonged period of reconnaissance and intrusion, during which the attacker gains and maintains unauthorized access to a network. The ultimate objective is to exfiltrate sensitive data or disrupt operations over an extended period. Due to their complexity and the high level of expertise required to execute them, APTs are often associated with nation-states, organized crime groups, and other highly motivated threat actors.

## III. PROPOSED ALGORITHM

The project seeks to address this challenge by deploying a robust virtualized environment that replicates key components of a modern IT infrastructure. By integrating Wazuh, an open-source security monitoring platform, with Windows endpoints, the project aims to enhance visibility into system activities and promptly identify anomalous behaviors indicative of APT activity.

Furthermore, integrating VirusTotal into the monitoring ecosystem enables automated analysis of suspicious files and URLs, leveraging a vast repository of threat intelligence to bolster detection capabilities.

The scope of this project encompasses the following key objectives:

- Virtual Machine Setup: Configuration of Ubuntu and Windows VMs to establish a simulated network environment.
- Wazuh Integration: Installation and configuration of Wazuh agents on Windows VMs to monitor system logs, network traffic, and endpoint activities.
- VirusTotal Integration: Automation of file and URL submissions to VirusTotal for comprehensive malware analysis and threat intelligence gathering.
- Kali Linux Deployment: Utilization of Kali Linux as an attacking machine to simulate APT tactics and evaluate defensive capabilities.
- APT Detection Strategies: Implementation of specialized detection rules and methodologies within Wazuh to identify indicators of APT activities.

By focusing on these objectives, the project aims to demonstrate the effectiveness of integrated security solutions in mitigating APT risks and enhancing overall cybersecurity resilience within a controlled virtual environment

## VI. EXPERIMENTAL RESULTS AND DISCUSSION

The installation process began with setting up the Wazuh server on a virtual machine. This involved downloading the Wazuh repository, followed by the installation of the necessary packages. The configuration of the Wazuh manager was a crucial step, where we ensured that the server was optimally set up to handle the influx of data from various endpoints.


Fig 1: Wazuh Manager

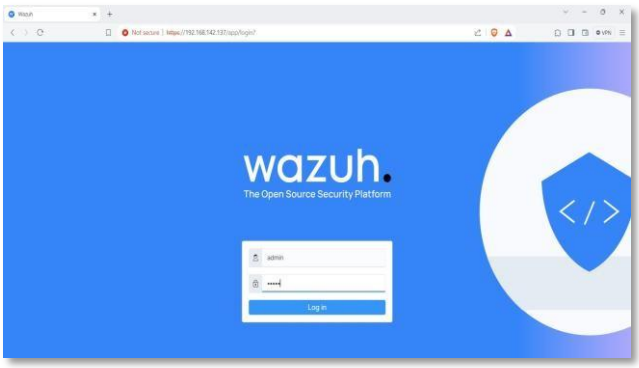



Fig 1.2: Wazuh login Dashboard

Ubuntu setup

We installed Wazuh agents on our Ubuntu machines to facilitate real-time data collection and monitoring. These agents are responsible for collecting log data, monitoring file integrity, and detecting any signs of intrusion.

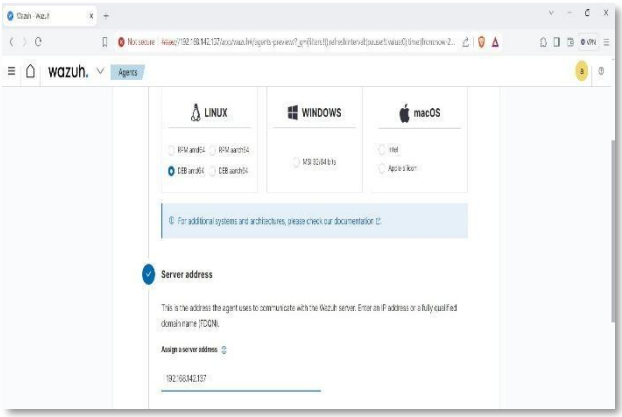
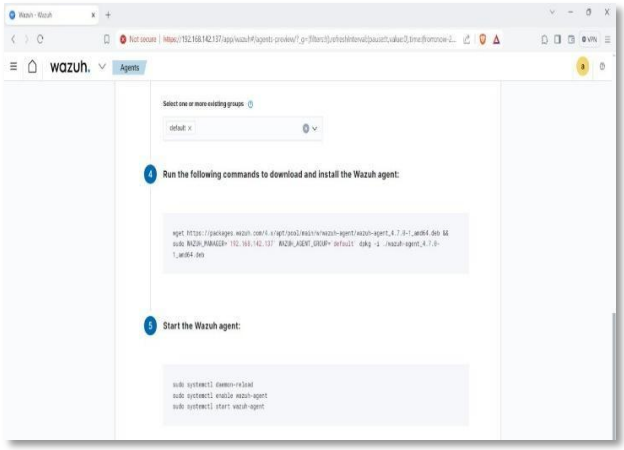



Fig 1.3: Wazuh Agent Deploy




Ossec.conf

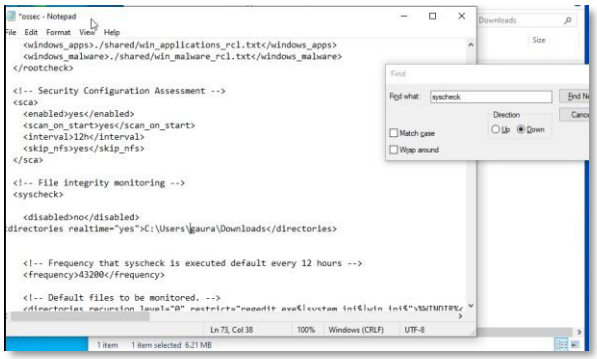
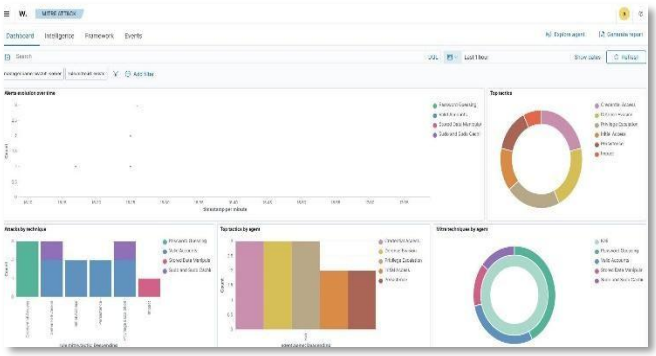
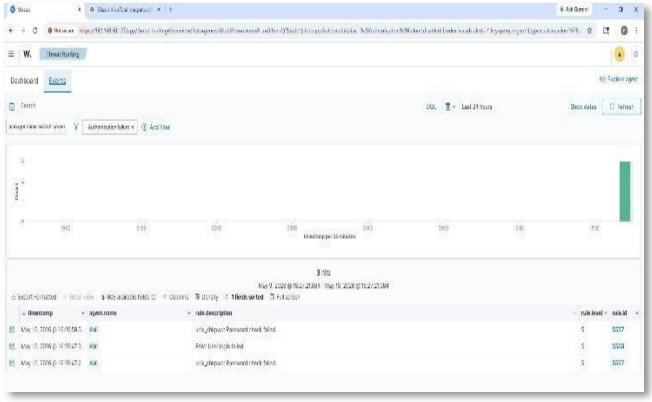



Fig 1.4: Virus Total Integration

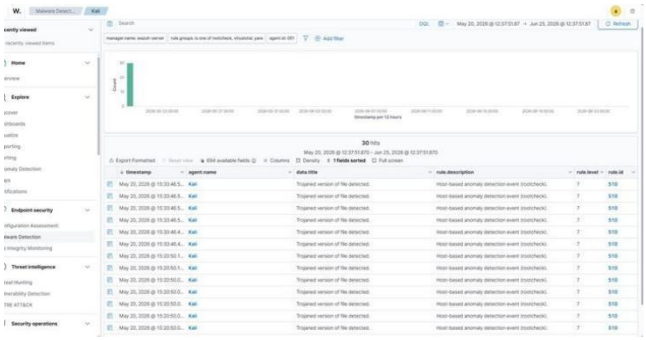
Throughout this paper, we have successfully integrated various infosec feeds, allowing for real- time monitoring and analysis of emerging threats. By aggregating data from multiple reputable sources, we created a centralized repository of threat intelligence that provides a holistic view of the current security landscape. This integration not only streamlines the process of threat detection but also enhances the accuracy and reliability of the information gathered.

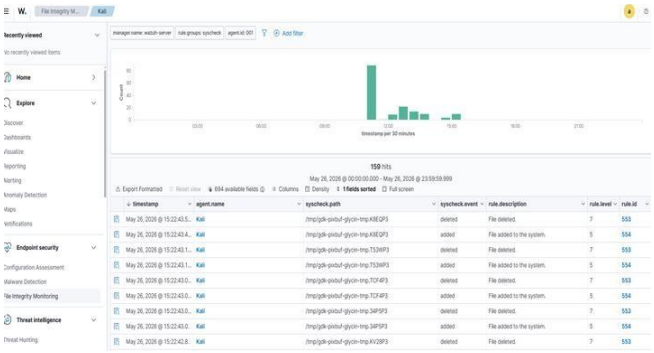




V. RESULT

**File automatically deleted:**





Threat Actor Analysis

A significant portion of our work involved identifying and analyzing threat actors. By leveraging advanced analytical tools and methodologies, we were able to profile these malicious entities, understand their motives, tactics, techniques, and procedures (TTPs), and predict potential future actions. This detailed analysis enables organizations to anticipate and defend against specific threats more effectively, thereby strengthening their overall security posture.

Leaked Databases Exploration

The exploration of leaked databases was another critical aspect of our paper by scrutinizing these databases, we identified patterns and trends in data breaches, which provided deeper insights into common vulnerabilities and exploitation techniques used by threat actors. This information is crucial for developing proactive measures to safeguard sensitive data and prevent future breaches.

V. CONCLUSION & FUTURE WORK

Throughout this paper, we have successfully integrated various infosec feeds, allowing for real- time monitoring and analysis of emerging threats. By aggregating data from multiple reputable sources, we created a centralized repository of threat intelligence that provides a holistic view of the current security landscape. This integration not only streamlines the process of threat detection but also enhances the accuracy and reliability of the information gathered.

Planned integration with MISP and the development of a Telegram scraper are pivotal steps in the evolution of our cybersecurity framework. These enhancements will provide us with deeper insights, more timely threat detection, and a greater ability to preemptively address potential security incidents. As we continue to innovate and expand our capabilities, we are committed to maintaining a robust defense against the ever-changing landscape of cyber threats.

## Acknowledgment

The authors would like to thank all those who are directly or indirectly involved, directed, and coordinated in this paper. Their valuable insights, guidance, and support have been active in forming this work.

REFERENCES

[1]. A NOVEL APPROACH FOR DETECTING ADVANCED PERSISTENT THREATS JAAFER AL-SARAIREH, ALA' MASARWEH

[2]. ADVANCED PERSISTENT THREATS (APTS): ANALYSIS, DETECTION, AND MITIGATION STRATEGIES HIDER ALI

[3]. ADVANCED PERSISTENT THREAT SECURITY: 5 MODERN STRATEGIES GILAD DAVID MAAYAN [4]. STRATEGIES FOR MITIGATING ADVANCED PERSISTENT THREATS (APTS) P.1 KASPERSKY IT ENCYCLOPEDIA

[5]. ADVANCED PERSISTENT THREAT DETECTION PERFORMANCE ANALYSIS BASED ON MACHINE LEARNING MODELSANIL KUMAR1, AMANDEEP NOLIYA2, RITU MAKANI3, PARDEEP KUMAR4, JAGSIR SINGH5

[6]. "ARE YOU BEING TARGETED BY AN ADVANCED PERSISTENT THREAT?". COMMAND FIVE PTY LTD. RETRIEVED 2011-03-31.

[7]. A NOVEL APPROACH FOR DETECTING ADVANCED PERSISTENT THREATS JAAFER AL-SARAIREH ⇑, ALA'

MASARWEH

[8]. ERIC M. HUTCHINS; MICHAEL J. CLOPPERTY; ROHAN M.AMIN. MCGRAW-HILL OSBORNE MEDIA. ISBN 978-0071772495.

[9]. "INTELLIGENCE-DRIVEN COMPUTER NETWORK DEFENSE INFORMED BY ANALYSIS OF ADVERSARY CAMPAIGNS AND

INTRUSION KILL CHAINS" (PDF). LOCKHEED MARTIN CORPORATION ABSTRACT. RETRIEVED MARCH 13, 2013.

[10]. "ASSESSING OUTBOUND TRAFFIC TO UNCOVER ADVANCED PERSISTENT THREAT" (PDF). SANS TECHNOLOGY INSTITUTE. RETRIEVED 2013-04-14.

[11]. "INTRODUCING FORRESTER'S CYBER THREAT INTELLIGENCE RESEARCH". FORRESTER RESEARCH. RETRIEVED 2014-04-14.

[12]. "ADVANCED PERSISTENT THREATS: LEARN THE ABCS OF APTS - PART A". SECUREWORKS. SECUREWORKS. RETRIEVED 23 JANUARY 2017.

[13]. OLAVSRUD, THOR. "TARGETED ATTACKS INCREASED, BECAME MORE DIVERSE IN 2011". PCWORLD. [14]. SEAN BODMER; DR. MAX KILGER; GREGORY CARPENTER; JADE JONES (2012). REVERSE DECEPTION: ORGANIZED CYBER THREAT COUNTER-EXPLOITATION.

[15]. "OUTMANEUVERING ADVANCED AND EVASIVE MALWARE THREATS". SECUREWORKS. SECUREWORKS INSIGHTS. RETRIEVED 24 FEBRUARY 2016.

[16]. "APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS". MANDIANT. 2013.

[17]RICHARD BEJTLICH. WHAT IS APT AND WHAT DOES IT WANT?
[18]HTTP://TAOSECURITY.BLOGSPOT.BE/2010/01/WHAT-IS-APT-AND-WHAT-DOES-IT-WANT.HTML, 2010.

[19] ISACA. ADVANCED PERSISTENT THREAT AWARENESS. 2013.

[20] KASPERSKY. THE ICEFOG APT: A TALE OF CLOAK AND THREE DAGGERS. 2013.

[21] FIREEYE LABS. FIREEYE ADVANCED THREAT REPORT 2013. 2014.

[22] MCAFEE LABS. PROTECTING YOUR CRITICAL ASSETS: LESSONS LEARNED FROM "OPERATION AURORA". 2010.

[23] MANDIANT. THE ADVANCED PERSISTENT THREAT. 2010.

[24] MANDIANT. APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNIT. 2013. [25]SYMANTEC. ADVANCED PERSISTENT THREATS: A SYMANTEC PERSPECTIVE. 2011.

[26] COLIN TANKARD. ADVANCED PERSISTENT THREATS AND HOW TO MONITOR AND DETER THEM. NETWORK SECURITY, 2011(8):16-19, 2011.

[27] GORDON THOMSON. APTS: A POORLY UNDERSTOOD CHALLENGE. NETWORK SECURITY, 2011(11):9-11, 2011.

[28] HTTP://WWW.MCAFEE.COM/US/RESOURCES/WHITE-PAPERS/WP-OPERATION-SHADY-RAT.PDF
[29] HTTP://WWW.NYTIMES.COM/2013/02/19/TECHNOLOGY/CHINAS-ARMY-IS-SEEN-AS-TIED-TO-HACKING- AGAINST-US.HTML?EMC=NA&_R=2&

[30] HTTPS://WWW.SECUREWORKS.COM/RESEARCH/ANALYSIS-OF-DHS-NCCIC-INDICATORS
[31] HTTPS://WWW.SCRIBD.COM/DOC/13731776/TRACKING-GHOSTNET-INVESTIGATING-A-CYBER- ESPIONAGE-NETWORK
[32]HTTP://WWW.NARTV.ORG/MIRROR/GHOSTNET.PDF

[33]HTTP://CDN0.VOXCDN.COM/ASSETS/4589853/CROWDSTRIKE-INTELLIGENCE-REPORT-PUTTER- PANDA.ORIGINAL.PDF.