International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 04 | Apr 2025 www.irjet.net p-ISSN: 2395-0072

Monitor and Mitigate Cyberattacks with SIEM

Sameer Pathan[1], Sumedh Vartak[2], Yash Zagade[3], Prof. Bhavesh Panchal[4]

[123]Department of Computer Engineering, Rajiv Gandhi Institute of Technology, Mumbai
[4]Assistant Professor, Department of Computer Engineering, Rajiv Gandhi Institute of Technology, Mumbai

---

ABSTRACT - ***As more and more common and sophisticated cyber-attacks happen, you should have a strong defence system in place to detect and respond to such threats in a quick manner. The project attempts to create a Security Operations Center (SOC) setup that is powered by a Security Information and Event Management (SIEM) system to monitor as well detect cyber threats in real time. Second, we built a simulated working environment with VirtualBox, and open-source tools like Wazuh, Suricata, ModSecurity and DVWA (Damn Vulnerable Web Application) were installed and configured. It includes functioning as the central SIEM to collect and analyze data from different sources and reveals suspicious activity. We had then simulated common attacks such as Denial of Service (DoS), file tampering and some web-based exploits, and observed how the system detects and react to them. This hands-on setup does more than show how different security layers work together, but how important it is to have real time monitoring, log analysis and automated response security for protecting systems from such modern cyber threats.***

Key Words: **Cybersecurity, Virtualized SOC, SIEM, Wazuh, Denial Of Service (DOS), File Integrity Monitoring (FIM), Suricata.**

1. INTRODUCTION

In today's cyber aware world, the cyber threats have reached new levels, and they are both frequent and sophisticated such that they could put lives and companies in grave danger. Attackers are always depriving new ways to exploit the system vulnerabilities, from simple phishing scams to complex network intrusions. The growing threat landscape makes a centralized system that allow monitoring, detecting, and responding to suspicious activities in real time is practically a must.

The idea of this project is to design and build a Security Operations Centre (SOC) utilizing the Security Information and Event Management (SIEM) approach to showcase the ways in the identification and mitigation of electronic threats. Wazuh is the heart of the system; it's a powerful open source SIEM tool capable of collecting and analysing logs from many sources to detect potential threats. In variational environment, Wazuh is deployed as the central brain of the security setup with all other components working as necessary functionality.

The Damn Vulnerable Web Application (DVWA) is used to simulate real world vulnerabilities. The deliberately insecure web application within the library allows the safe testing of common attack techniques, including SQL injection and Cross Site Scripting attacks. Host DVWA to the system so that it has something to monitor, and see live implications of attacks.

We also add ModSecurity, a Web Application Firewall, to the setup in order to help defend against web-based threats. ModSecurity will help to block malicious traffic coming in before it reaches DVWA with the OWASP Core Rule Set enabled. So, in turning to protect their users and their data, this is a strong first line of defence against attacks towards the web application.

Suricata is deployed on the network level as intrusion detection system (IDS). This Traffic monitoring helps detect abnormal pattern such as scan, DDoS attempts, unauthorized access attempts or any other on the network. It also has well developed deep packet inspection capabilities that allow it to be useful identifying threats early on in the attack chain.

Another important layer that we have added as part of Wazuh's built in sys-check feature is File Integrity Monitoring. It records any changes made to sensitive files or directories—particularly in the DVWA environment—and hence any unauthorized modifications can be captured straight away.

With the Active Response features of Wazuh set, finally, we can set certain Active Response features to take some action automatically in the event those threats are identified. Consider, for example, when Wazuh detects a brute force attack or a DoS pattern and it can temporarily block an attacker's IP address by updating the firewall rules to give the administrator time to investigate and react.

All together, these tools create a multi layered, lightweight security environment as a proof of concept for how a modern SOC can be build using open-source technologies. Such setup provides a clear and hands on understanding of activities to detect and counter cyber threats ranging from host to the whole network. By having this setup, one will have a hands-on idea about how to detect and mitigate cyber threats.

2. LITERATURE REVIEW

The paper [1] presents a cybersecurity solution in line with SIEM that detects and reacts to threats in real time. Suricata and Splunk are integrated into the system, and together with it, the monitoring of network traffic compliance with intrusion detection, and compliance with system events are enabled. Also, honeypots help to draw in, record and study malicious actions for earlier threat identification, and for a more overall view of security monitoring.

Unfortunately, the system has some drawbacks. Since the threat that it relies on is static detection rules which leads to threats that are simple or evolved it cannot catch sophisticated threats. Without machine learning, the system has no ability to change itself to deal with new attack patterns. Also, attackers may be able to bypass honeypots and the system can fight with encrypted traffic and complex obfuscation techniques. This limitation suggests the need for the future implementations to have more dynamic and adaptive characteristics.

The paper [2] gives an example of a practical approach to building an Security Operations Center (SOC), couple with Wazuh, and a suitable File Integrity Monitoring (FIM) system to protect your servers. The use case that is focused on is real-time analysis of the logs, alerting and visualization to detect security threats. This is done with ELK tools (Elasticsearch, Logstash, and Kibana), and with adding features for intrusion detection, vulnerability assessment, and active response, this is extended with the Wazuh system. FIM adds to this and helps monitor non authorized file changes which ensures the integrity of the data within the system. It can somehow solve the problem of identifying and reacting suspicious activity, but there are downsides.

It is important to note the complexity of setting this up and keeping it in good working order when team members are not technically savvy. In addition, scaling the system to the size of greater environments might result in performance troubles. Although powerful, Wazuh can also generate many false alerts at a high rate unless properly tuned. The second challenge is that most detection rules are hand created, thus slowing responses and not having any mechanism of automatic threat intelligence. Overall the paper lays a good groundwork for SOC deployment yet it also suggests points for improvement in terms of automation and scalability in cyberattack prevention.

The paper [3] discusses why it has become so important for SIEM systems to have become key instruments in defending modern digital environments against sophisticated cyber threats. This enables organizations to gather and analyze security data from different sources and then centralize its monitoring as well as threat detection supported by these systems. Despite the importance of traditional SIEMs, the paper notes several challenges of them. The problem is processing the 'masses' of log data they need to process, which can gum up performance and slow down threat detection. Often weighing in on the high side for false positives and on the low side for rapid threat pattern changes, SIEMs cannot keep up. They can also be integrated with complex IT systems, which further reduces their efficiency. Technologies such as machine learning and automation may improve their capabilities, but such incorporation of technologies brings with them new issues including the increased complexity of the system, need of skilled professionals, and more resources. The study highlights that SIEM tools need to remain as unwavering and as prime as ever if they want to stay relevant in the ever so progressive world, in terms of modern security needs and to detect and tackle attack trends in real time.

The paper [4] explains the detail Security Information and Event Management (SIEM) systems approach is provided: how SIEM systems collect, normalize and analyze security data in real time. It presents log management and event correlation as components that enhance the detection of threats early and support incident response, as a part of SIEM. The authors compare open-source and commercial SIEM tools regarding their functionality and implementation.

It should, however, be noted that there are several challenges mentioned with the paper. Usage of large volume data is often an Execution problem for SIEM systems and it causes Performance problems or a number of missed threats. In addition, they also produce false positives, as rule accuracy is lacking, and it needs to be set up and managed by skilled professionals. It has privacy concerns when we have to store sensitive security logs in a centralized system. While in cybersecurity, SIEM is absolutely necessary, the scalability, automation, and usability of it must improve.

3. METHODOLOGY

Objectives of the project are to simulate, monitor and respond to cyber-attacks by using an open-source Security Information and Event Management (SIEM) system in a virtualized setup. Based on the methodology we have developed this, is structured through a series of practical phases starting from creating a simulated environment, installing monitoring tools, carrying out attack simulations, and engaging in real time response to a threat.

First, an Oracle VirtualBox virtual lab was created via two Ubuntu based virtual machines (VMs), which is to say that these were virtual machines running Ubuntu. The SIEM Server was configured to be one machine with the ability to store, analysis and respond to each security events it collected. The second machine was the Target System that contained vulnerable applications and security tools. To network these machines, a host only adapter was used to bring them together in such a way as networked machines would be across an isolated network not to be interfered on by external factors.

Management of log collection and event correlation was performed by Wazuh Manager on the SIEM Server. Agents constantly provided data to Wazuh and, on occasion, they triggered alerts for suspicious actions. To handle data index and deliver real time visual insights, the ELK stack composed of Elasticsearch, Logstash, Kibana was added. Wazuh send's logs to Elasticsearch using Filebeat, which could then display security alerts through the Kibana interface.

Several critical components were deployed on our Target Machine in order to replicate a real-world attack surface on it. To simulate exploitable web vulnerabilities, Damn Vulnerable Web Application (DVWA) was installed. A Web Application Firewall (WAF) in the form of ModSecurity monitored and filtered the malicious HTTP traffic aimed at DVWA. Another IDS was also deployed to watch for strange network behaviour such as scanning through ports or denial of service attempts; this is Suricata. On this machine the Wazuh Agent also actively watched log files, file changes, and system processes, and sent such information to the Wazuh Agent which in turn transmitted it to the Wazuh Manager for central analysis.

Once virtual SOC environment was deployed and connected, various cyberattacks were simulated on the target machine (192.168.56.102) to check whether it can detect and response the monitored cybersecurity events. They performed a stealth network scan (i.e. a test of what the traffic looks like from an outside host against the target VM using Nmap) with Suricata running on the target VM as an OpenFlow AON agent able to inspect live traffic in real time. During this, a SlowLoris Denial-of-Service (DoS) attack was performed against the DVWA web application to evaluate how the system behaves towards application layer threats and how ModSecurity is capable to identify and log abnormal HTTP behaviour. Further, I enabled Wazuh's File Integrity Monitoring (FIM) capabilities to monitor unauthorized changes in critical directories, /var/www/html/DVWA being one of them, and to alert as soon as someone tries to intervene tampering them. The Wazuh Agent on the target system generates all alerts that are transmitted to the Wazuh Manager on the SIEM Server (192.168.56.10) and visualized through Kibana dashboards in real time for the incident analysis and rapid response.

On the SIEM Server the Active Response feature of Wazuh was activated for extending protection features of the system. Specific threat signatures, repetitive DoS traffic or vulnerability scans would now be countered by having predefined firewall rules running to block offending IP addresses with this. The results from these two examples proved that such an automation can reduce dramatically the time between detection and response with a proactive SIEM setup.

Overall, this methodology showcases the practical implementation of an open-source SOC environment capable of real-time cyber threat monitoring and response. The project demonstrates a low cost to deploy strategy to secure networked systems against increasingly moving cyber threats via integration of tools such as Wazuh, Suricata, ModSecurity, the ELK stack.

4. SYSTEM ARCHITECTURE

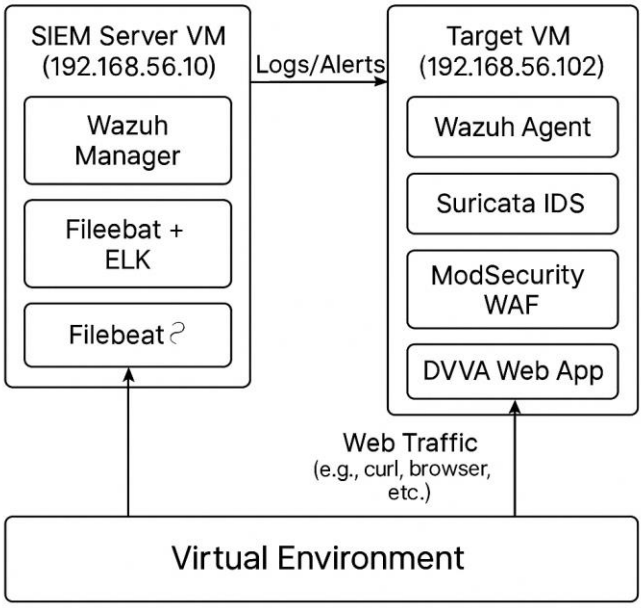

Figure 1: System Architecture

A virtualized lab is created to build the architecture of the proposed system in a simulation, similar to a real-world network environment. The setup is comprised of two Ubuntu based virtual machines: one is the Security Information and Event Manager (SIEM) server and the other is a target machine with vulnerable endpoint and where the attack will take place. But, from both VMs, a host only network is used that connects them and utilizes an isolated communication for controlled testing and analysis, without internet interference.

The central node where the security related data is aggregated, processed, and visualized with an IP of 192.168.56.10. It runs the Wazuh Manager that will collect logs coming from Wazuh agents, will analyze them following pre-configured rules to identify any possible threats. These logs are forwarded to the ELK stack using filebeat forwarding them to Elasticsearch, Logstash, and Kibana. Log data is indexed and stored on Elasticsearch, Logstash processes the log data and filters out alerts and activities, while Kibana gives the user an easy-to-use dashboard to immediately see the alerts and activities in real time.

However, the target machine with IP 192.168.56.102 is configured in order to run components to simulate the type of a typical web facing server. Among them evolve Damn Vulnerable Web Application (commonly referred to as DVWA), a testbed to assess common web-based

vulnerabilities. ModSecurity is installed as a Web Application Firewall (WAF) to protect the web application for incoming HTTP requests and blocks malicious payload. Also, Suricata is installed as a Network Intrusion Detection System (NIDS) and it will monitor traffic patterns and where they may find a suspicious behavior such as port scans or denial of service attacks.

To monitor the local system, the Wazuh Agent installed on the target VM is crucial. It messages each time a file is changed, a process started, and the console is written to. According to File Integrity Monitoring (FIM), it is configured to follow any unapproved modification in critical folders like the DVWA folder (/var/www/html/DVWA). It also gives you an immediate alert if someone is attempting to tamper or intrude.

The Suricata, ModSecurity and the Wazuh Agent all push their alerts to the SIEM server where Wazuh runs the data and provides actionable insight. These alerts are visualized with Kibana dashboards to detect the real time threats. The Wazuh Active Response module is configured to respond automatically to some alert conditions, for instance to block IP's involved in bad activity

At the same time, this architecture describes how a virtual setup with a few open-source tools can be efficiently integrated together and form a lightweight Security Operations Center (SOC). The system can support such continuous monitoring, threat detection, and automated response and is appropriate for cybersecurity training, experimentation and in small scale enterprise environments.

5. EXPERIMENTAL RESULTS

A couple of cyberattack scenarios were run in a controlled virtual environment to evaluate the effectiveness of the deployed SIEM setup. This configuration consisted of a SIEM Server (192.168.56.10) with Wazuh Manager connected to the ELK stack and a Target Machine (192.168.56.102) with DVWA, ModSecurity, Suricata and Wazuh Agent. Real time monitoring was accomplished through Kibana dashboard with respect to security events and alerts.

5.1 Detection of Web Attacks

In order to simulate a web-based attack, a command injection was attempted by crafting and attempting to use a curl request for the DVWA application that was hosted on the Target Machine. When the malicious request actually executed, ModSecurity, which is acting as the Web Application Firewall (WAF), intercepted an blocked the malicious request, returning a 403 Forbidden response. Thealog entry that contains the information relevant in the Apache log was first captured by the Wazuh Agent, integrated with the web server, then forwarded to the Wazuh Manager, where it generated an alert. The Kibana dashboard had started showing this alert along with source IP address, nature of the request and timestamp as they have been displayed on it.

Figure 2: Simulation of XSS attack

Observation: The result of this test are given below and verified that the system was able to block in real time any suspicious web traffic to vulnerable web applications, with strong protection for vulnerable web applications.

Figure 3: Blocking a command injection attack

5.2 File Integrity Monitoring

For the evaluation of the File Integrity Monitoring's effectiveness, it was intentional to modify a file in the /var/www/html/DVWA directory. When this path was altered, the Wazuh Agent, which was configured to monitor it, immediately started monitoring it. This generated a corresponding alert which was sent to the Wazuh Manager and eventually displayed in the Kibana dashboard. It included the precise file path, the type of change, file hashes potentially before and after the change.

Observation: This experiment validated the system's immediate capability to detect and report unauthorized changes to files to provide forensic analysis support, with assurance of the integrity of sensitive web application files.

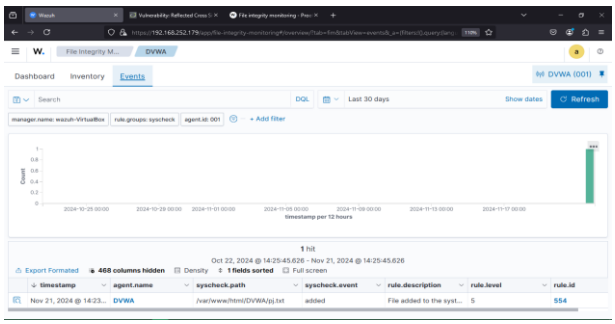

Figure 4: File integrity alert triggered by the addition of new file

5.3 Detect and Mitigate Dos Attack

To evaluate the ability of the present SIEM infrastructure to detect and mitigate against the DoS attack launched, the DVWA web server was targets with a Slowloris Denial Of Service (DoS) attack. The purpose of this is to create numerous incomplete HTTP requests to the server so it can keep the connections open and waste the server's resources. Suricata as an intrusion detection system was able to find the abnormal traffic pattern accurately and Wazuh observed system level anomalies accurately. When it detected the unknown IP address, the Wazuh Active Response module was triggered to automatically execute a firewall dropscript with a specified duration on the attacker's IP address.

Observation: It was demonstrated the robustness and efficiency of automatically defending in a single SIEM environment the system successfully neutralized the threat in real time without any manual intervention.

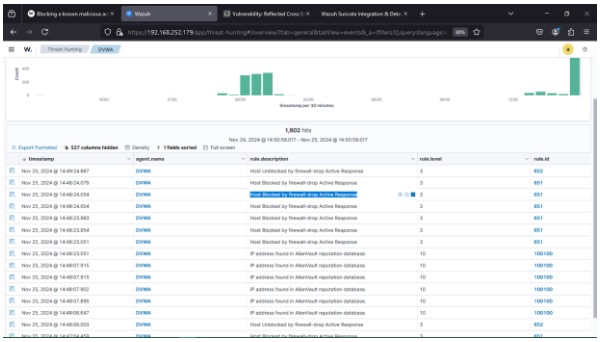

Figure 5: Detection and active response to Dos attack

6. CONCLUSIONS

It was practical deployment of Security Information and Event Management (SIEM) system in controlled virtual environment as a cyber threat monitoring & reacting system. The system successfully detected and mitigated different kinds of attacks, such as denial of service, malicious web requests, as well as unauthorized file changes by integrating some open-source tools, Wazuh, Suricata, ModSecurity, and File Integrity Monitoring (FIM).

Having proved the capability not only to identify suspicious activity but also to take automated response actions such as blocking malicious IP addresses, the system relieved the need for continual manual intervention. By utilizing these tools, all security events on the infrastructure could be visible in real time and analyzed very nicely with one tool, the Kibana dashboard.

This project demonstrates, in general, how a lightweight, inexpensive, and customizable SIEM system can be deployed on virtual machines with free tools. For academic labs or small organizations, it gives good base for building a proactive defense mechanism. Future may include enlarging the attack surface or even integrating cloud services or even implementation of machine learning to be more IoT ideas of catching more clever threats.

ACKNOWLEDGEMENT

The authors express their sincere gratitude to Prof. Bhavesh Panchal for his invaluable guidance and support throughout this research project.

REFERENCES

[1] Z. S. Younus and M. Alanezi, "Detect and Mitigate Cyberattacks Using SIEM," 2023 16th International Conference on Developments in eSystems Engineering (DeSE), Istanbul, Turkiye, 2023, pp. 510-515, doi: 10.1109/DeSE60595.2023.10469387.

[2] N. Akshai Sankar and K. A. Fasila, "Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring," 2023 9th International Conference on Smart Computing and Communications (ICSCC), Kochi, Kerala, India, 2023, pp. 350-354, doi: 10.1109/ICSCC59169.2023.10334992.

[3] M. Cinque, D. Cotroneo and A. Pecchia, "Challenges and Directions in Security Information and Event Management (SIEM)," 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Memphis, TN, USA, 2018, pp. 95-99, doi: 10.1109/ISSREW.2018.00-24.

[4] I. Bachane, Y. I. K. Adsi and H. C. Adsi, "Real time monitoring of security events for forensic purposes in Cloud environments using SIEM," 2016 Third International Conference on Systems of Collaboration (SysCo), Casablanca, Morocco, 2016, pp. 1-3, doi: 10.1109/SYSCO.2016.7831327.