Hybrid Intrusion Detection System and Network Infrastructure Vulnerability Mitigation using Active Response (XDR) Technique Wazuh and Suricata

Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Active Response (XDR) Wazuh dan Suricata

Hillman Akhyar Damanik[1)], Merry Anggraeni[2)]

Fakultas Teknologi Informasi Universitas Budi Luhur

Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, DKI Jakarta, Indonesia 1226012

hillmanakhyardamanik@gmail.com

Received: 23 September 2024 || Revised: 10 November 2024 || Accepted: 18 November 2024

Abstract – The complexity of cyber threats against the network infrastructure of companies, educational institutions, and government makes protecting network infrastructure a top priority. Router and server devices are highly vulnerable to various types of cyber threats, requiring comprehensive detection and response solutions. This research will implement an intrusion detection system by integrating SIEM technology and Wazuh XDR (Extended Detection and Response). This system analyzes index pattern data from Wazuh agent devices to detect and respond to attacks using the XDR active response firewall. The testing was conducted MikroTik RouterOS, Ubuntu Server 20.04 as Wazuh agent to test reconnaissance attacks, brute force and DoS attacks. The results of the research show Nmap and brute force attacks were successfully detected by Wazuh manager and blocked the attacker IP malicious through active response. Detection of brute force attacks showed an increase in traffic of up to 60 Kbps and CPU usage reached 100%, then decreased after the active response firewall was activated. Authentication failure reached 2198 times in the first hour of the brute force attack. CPU usage increased from 20% to 85% during the attack and decreased to 15% after the active response firewall was activated. DoS attacks, on MikroTik experienced an increase in CPU usage of up to 61% and memory of 67%. After activating the active response firewall, CPU usage decreased to 3%. Traffic on the MikroTik interface increased to 3.3 Mbps during the attack, then decreased to 1 Kbps after the firewall was activated.

Keywords: Router, Server, Wazuh XDR, Suricata, Firewall

Abstrak *– Kompleksitas ancaman siber pada infrastruktur jaringan perusahaan, institusi pendidikan, dan pemerintah menjadikan perlindungan infrastruktur jaringan sebagai prioritas utama. Berbagai perangkat router dan server sangat rentan terhadap berbagai jenis ancaman siber, sehingga memerlukan solusi deteksi dan respons yang komprehensif. Penelitian ini akan mengimplementasikan sistem deteksi intrusi dengan mengintegrasikan teknologi SIEM dan (Extended Detection and Response) XDR Wazuh. Sistem ini menganalisis data index pattern dari perangkat Wazuh agent untuk mendeteksi dan merespons serangan menggunakan firewall active response XDR. Pengujian dilakukan pada perangkat MikroTik Router, ubuntu server untuk menguji serangan reconnaissance attack, brute force dan DoS. Hasil penelitian menunjukkan serangan Nmap dan brute force berhasil dideteksi oleh Wazuh manager dan memblokir IP penyerang melalui active response. Pendeteksian serangan brute force menunjukkan peningkatan traffic hingga 60 Kbps dan penggunaan CPU mencapai 100%, kemudian terjadi penurunan setelah firewall active response diaktifkan. Authentication failure mencapai 2198 kali dalam satu jam pertama serangan brute force. Penggunaan CPU meningkat dari 20% hingga 85% selama serangan dan menurun menjadi 15% setelah firewall active response diaktifkan. Serangan DoS, pada MikroTik mengalami peningkatan penggunaan CPU hingga 89% dan memori 56.32%. Setelah aktivasi firewall active response, penggunaan CPU menurun menjadi 3%. Traffic pada interface MikroTik meningkat hingga 3.3 Mbps selama serangan, kemudian menurun menjadi 1 Kbps setelah firewall diaktifkan.*

Kata Kunci: *Router, Server, Wazuh XDR, Suricata, Firewall*

doi: 10.56873/jpkm.v9i2.5829

INTRODUCTION

The current network infrastructure devices, such as routers and servers, come in various forms and numbers, with device placements at nodes, edges, and endpoints being vital and crucial to the operational continuity of a company network (Damanik et al., 2023). Many companies have offices spread out and connect hundreds of devices, such as routers and servers, which are often insecure and possess different vulnerabilities caused by the rapid growth of information and networks (Damanik, 2022).

Research using Wazuh can provide guidance for organizations to consider integrating Wazuh into a company security infrastructure (Amami et al., 2024). The study concluded that the integration of Osquery with Wazuh can improve system monitoring and security through real-time threat detection, network activity monitoring, and anomaly detection. The study also offers a framework for customized anomaly detection and proactive response, which strengthens cyber defenses in keeping digital assets secure. These findings demonstrate the effectiveness of Osquery and Wazuh collaboration in quickly identifying and remediating vulnerabilities (Prasad et al., 2024). DDoS attacks cause congestion and disrupt server functions, significant improvement in Quality of Service (QoS) CPU reduced by 81.23%, from 78.3% to 14.7% (Praptodiyono et al., 2023). Monitoring and Classification dataset CICIDS2017 and CICDDOS2019 with results showing accuracies of 99.84% and 93% respectively, which are higher for detecting DDoS attacks (Fuhr et al., 2022). Medusa as a tool to test brute force attacks on servers. The results showed that Honeypot successfully prevented attackers from accessing the original server, as well as recording all attacker activity on the shadow server in the kippo activity log (Nursetyo et al., 2019). DDoS attacks are one of the biggest threats frequently occurring in government procurement services (Akbar et al., 2016). DDoS attacks remain a significant threat, particularly due to the increased connectivity of devices at the ISP edge router. This study identifies and analyzes DDoS activity using a honeynet based on packets captured and analyzed by a network protocol sniffer and signature-based attack analysis tools (Triantopoulou et al., 2019) As many as 4 million packets totaling 4 TB in size revealed MikroTik devices infected by DDoS attacks and malware (Ceron et al., 2020). Muwardi conducted an experiment creating a prototype security system, monitoring, and evaluating server security systems using Snort IDS for the security of server infrastructure connected to the network, to test brute force attacks (Helmiawan et al., 2021). The brute force attack pattern on the SSH port on router devices yielded the most exploited usernames and passwords by hackers (Subhan et al., 2023). HTTP flood attacks, IIS 10.0 server outperforms Apache2 in terms of efficiency and responsiveness. However, Apache2 shows better stability and responsiveness when subjected to SYN flood attacks. These results highlight the performance differences between the two servers in handling different types of DDoS attacks (Zebari et al., 2018). The study used Wazuh to detect defacement attacks in real-time with an average response time of 1.2 seconds and successfully isolated the network on AWS servers, but failed on GCP servers, indicating the need for further analysis on the platform (Kurniawan & Triayudi, 2024).Wazuh as monitoring and protection for IT assets through SIEM and XDR capabilities, is used to protect digital assets and improve organizational cybersecurity (Moiz et al., 2024).

Attack category clustering using the K-Means method and automatic mitigation through IPTables rules. The analysis shows that 64% of attacks are in the high category, with mitigation that reduces the CPU load on the vRouter to 28% and memory to 39%, and on the vFarm Server, the CPU load of each vServer is reduced to 43% and memory to 21% (Damanik & Anggraeni, 2024). The research conducted by Oktivasari only focused on web server services with IPTables mitigation techniques (Oktivasari et al., 2022).

In this research, compared to previous research, to overcome the complexity of cyber threats and attacks, a better approach is needed to improve cyber resilience that is more holistic and integrated with detection and active response systems. This research implements a hybrid approach, by combining Wazuh XDR Suricata and iptables techniques for detection systems and active responses to threats *reconnaissance attack, brute force dan DoS*. 1) Developing and building an effective security system for routers and servers to detect *reconnaissance attack, brute force dan DoS*. 2) Integrating Wazuh XDR and Suricata to implement a holistic intrusion detection system that responds to detected attacks. 3) Testing, evaluating, and mitigating types of attacks, including measuring CPU and memory resources.

RESEARCH METHOD

The approach used in this research involves the PPDIOO method (Prepare, Plan, Design, Implement, Operate, and Optimize) of the Cisco life cycle, as illustrated in Figure 1 as the research flow diagram. These research phases are designed to ensure that the intrusion detection system and attack mitigation on the network infrastructure of router and server devices can be implemented effectively.

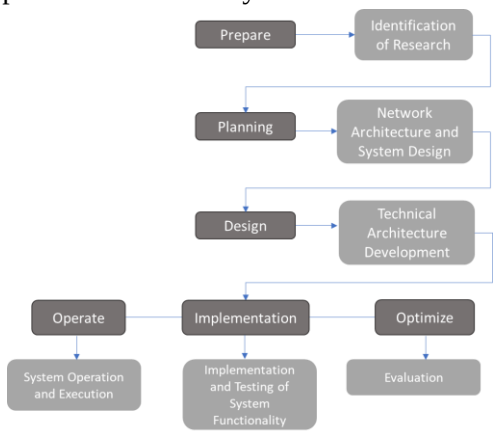

Figure 1 Research Approach Method

Prepare (Identification Research)

The prepare stage involves implementing, documenting, and researching developments in the research area to be applied. This research will be conducted from June to August 2024 on the network infrastructure of AJN Company. The network infrastructure requirements include a CCR1036-8G-2S router, an RB941 router, VMware and Proxmox hypervisor servers, and IDCloud vServer. The hardware and software will be used according to their roles: routers will function as internet gateways, Proxmox and VMware hypervisors will be used for the virtual environment as victims (agents), and the IDCloud vServer will be used for the Wazuh Manager. Testing will be conducted to ensure that each component of the infrastructure functions properly and meets expectations, including security testing to evaluate the effectiveness of the implemented hybrid intrusion detection and vulnerability mitigation solutions. Types of attacks are categorized into three types:

1) Reconnaissance attack the reconnaissance attack involves scanning to detect vulnerabilities in the ubuntu server 20.04.6 operating system where the Wazuh agent will be installed. The attack technique involves scanning the victim (Wazuh agent) using Nmap from kali linux to identify the services running on the target operating system.
2) Brute force attack aims to gain unauthorized credentials to the ubuntu server 20.04 operating system (Wazuh agent). Brute force attacks are included in this category, where the attacker tries various combinations of usernames and passwords to gain access, using the rockyou.txt wordlist. The technique used for attack emulation is Hydra on Parrot OS.
3) Denial of Service (DoS) Attack The DoS attack is modeled to make MikroTik RB941 (Wazuh agent) inaccessible by flooding the system with traffic, exploiting specific vulnerabilities to cause a crash. The technique used for attack emulation is Hping3.

Mitigation phase is carried out with the following three techniques Implementation of Integrating XDR solutions for rapid response to threats modeled from brute force attacks. Evaluation of the implementation involves measuring the performance of network interface traffic, CPU and memory resources usage will be compared before and after the attack.

Planning (Formulation Network Architecture and System Design)

Figure 2 shows the network topology architecture used in the research. The modeled topology consists of several main components, including devices and connectivity that work together to test and to monitor the modeled network infrastructure. The Internet gateway router connects the internal network with the public internet for interconnecting Wazuh agents and the Wazuh manager.

An attacker using Kali Linux OS, which includes tools like Hping3, Hydra (for brute force), and NMAP (network mapping), emulates attacks against the network. The attack targets (victims) are virtual operating systems installed on proxmox vms and MikroTik routers. Wazuh agents are installed on all vServers to monitor activity and send data to the Wazuh manager. The Wazuh manager, installed on a VPS server, collects and analysis data from each Wazuh agent, and a firewall framework is applied to the Wazuh manager to manage active responses to the modeled attacks. All attack and prevention datasets are monitored through the Wazuh dashboard, which provides a graphical interface for further analysis.

The entire system is monitored by a security operation center, which uses data from Wazuh manager

and dashboard to detect, analysis, and respond to security incidents in real-time.

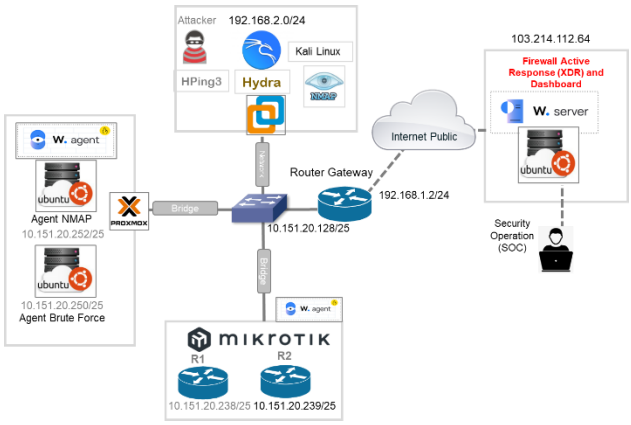

Figure 2 Designing Logical Topology Architecture in Network Infrastructure Environment with Wazuh manager

Table 1 details the components configured with specific IP addresses to ensure optimal communication based on the topology requirements, ensuring that each device can securely communicate through the designated gateway. The gateway router is allocated the IP address 192.168.1.2/24 to connect the modeled private network infrastructure to the internet. The Proxmox hypervisor and the hbuntu server VM (Wazuh agent) use the 10.151.20.0/25 subnet. Kali Linux (Hydra, Hping3, and Nmap), used for attack emulation and simulation, is allocated the 192.168.2.0/24 subnet to test the system response to attacker threats. There are two MikroTik routers acting as victim devices with IP addresses 10.151.20.238 and 10.151.20.239, aiming to test various attack scenarios and XDR of Wazuh 103.214.112.64/32.

Tabel 1 Component IP Address Devices vServer and Router

Devices	IP Address Prefix
Router Gateway	192.168.1.2/24
Proxmox Hypervisor	10.151.20.230/25
Active response (XDR) Wazuh	103.214.112.64/32
Kali Linux OS (Hydra, Hping3 and NMAP)	192.168.2.39/24
Ubuntu Server (Brute Force) (Victim)	10.151.20.250/25
Ubuntu Server (DoS) (Victim)	10.151.20.251/25
Ubuntu Server (NMAP) (Victim)	10.151.20.252/25
Router MikroTik (Victim)	10.151.20.238/25
Router MikroTik (Victim)	10.151.20.239/25

Design (Technical Architecture Development)

In this design phase, the primary focus is on designing the detailed architecture of the logical network topology and the technical configuration for system implementation. The design phase for system implementation involves drafting technical specifications and system architecture to be used for implementing intrusion detection and vulnerability mitigation solutions. This includes designing the configuring communication between components, node proxmox hypervisor Wazuh agent, node VMWare hypervisor attacker and node Wazuh agent. The configuration for the Wazuh agent node on the proxmox hypervisor VM is detailed in table 2. Below is the VM configuration for the Wazuh agent node, which is set up with ubuntu server.

Table 2 Node proxmox hypervisor Wazuh agent

	Node		
Name	**Wazuh Agent-1**	**Wazuh Agent-2**	**Wazuh Agent-3**
VM ID	120	121	122
Storage	Local-VM	Local-VM	Local-VM
SCSI Controller	VirtIO SCSI	VirtIO SCSI	VirtIO SCSI
Hard Disk	80 GB	80 GB	80 GB
CPU (Core)	6	6	6
Memory	8192	8192	8192
Bridge	VMBR1	VMBR1	VMBR1

The installation and configuration of the VMware hypervisor in this research are used to install and configure Kali Linux and execute attack techniques using Hydra, Hping3, and Network Mapper (NMAP). The Kali Linux configuration sets and allocates resources such as vCPU, memory, and hard disk (SCSI), and network interfaces. The Kali Linux 2023.1 ISO image was chosen as the installation media, providing the necessary built-in security tools for attack simulation. Hydra will be used to perform brute force attacks on network protocols, attempting various combinations of usernames and passwords from the rockyou.txt wordlist to test the system's resilience against brute force attacks. Secondly, Hping3 will be used on the Mikrotik RouterOS target to conduct denial-of-service (DoS) attacks. Testing with the Nmap tool will be carried out for network mapping and

scanning, as well as identifying services running on the Wazuh agent, to detect active devices and services.
The node configuration for the Wazuh agent is modeled by adding the Wazuh agent to the proxmox hypervisor for the buntu server 20.04 operating system, which has been installed according to table 4.

Tabel 4 Wazuh agent configuration on proxmox hypervisor

Hypervisor Node	FQDN	Agent Name	Groups
Agent-1	103.214.112.64	Agent_BF	Brute Force
Agent-2	103.214.112.64	Agent_Hping3	Slowloris
Agent-3	103.214.112.64	Agent_Nmap	Nmap

The configuration for attack mitigation is carried out using the Wazuh XDR active response, as shown in Figure 3. This firewall dynamically blocks rules to respond to attacker source IP address activity. The active response configuration modeled in this research is used to mitigate brute force attacks and Nmap scanning by utilizing Wazuh active response feature to automatically block the attacker's IP address. This active response configuration involves key components, including the Wazuh agent installed on the ubuntu server operating system and the Wazuh manager acting as the controller. Figure 3 illustrates the architecture of the Wazuh active response module, which works by automatically executing response scripts on the monitored endpoint (Wazuh agent) based on pre-configured index patterns (Wazuh alert.json and Wazuh archives.json) using rule-ID, level, or rule group. By implementing the active response module, the security operations center (SOC) team can automate response actions to events or incidents on network infrastructure devices.

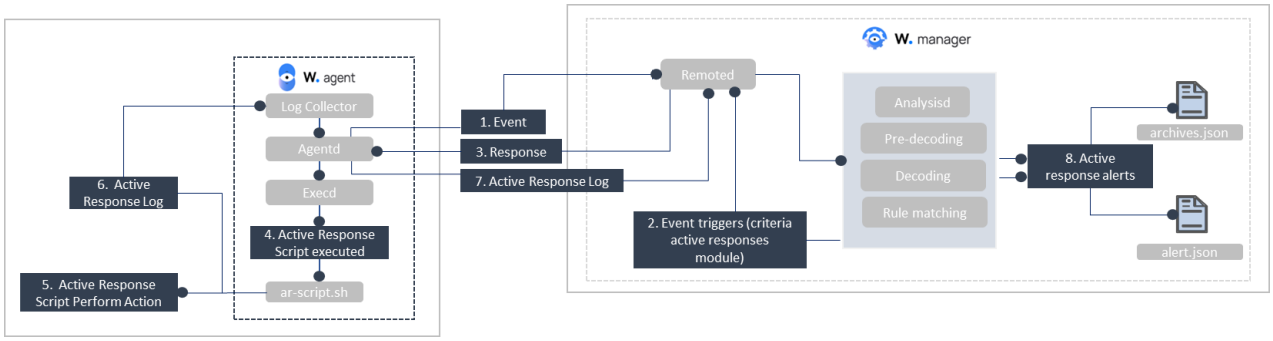

Figure 3 Configuration of Wazuh XDR Active Response module architecture

Using the Wazuh active response module, this configuration automates the firewall framework for brute force attacks. The firewall action policy involves blocking access from the attacker's IP with predetermined rules.

1. Event
   Monitoring Wazuh agent - when there is an event with attack detected on the monitored Wazuh agent, this event is logged by the log collector.
2. The event trigger criteria configured in the active response - the event is sent to the Wazuh manager for analysis. This event triggers a script configured in the active response module, such as a specific rule identifying the brute force, Nmap and Hping3 threat or attack type.
3. Response - on the Wazuh agent, once the event meets the criteria, the response is activated and sent back to the agent on the endpoint running the ubuntu server operating system
4. Execution of active response script (4 and 5) the Wazuh agent executes the previously configured scripts and active responses. This script is a firewall drop to block the attacker IP address.
5. Active response log – create on the Wazuh agent, a log of the active responses is created and recorded by the Wazuh agent. This log contains information about the actions taken in response to the event.
6. Active response log analysis - analysis will be performed on the Wazuh server for the active response logs and will be analyzed on the Wazuh server to ensure that the actions take were appropriate mitigating threats.
7. The Wazuh server will display alerts on the Wazuh dashboard based on the active responses taken and will store them in json files (archives.json and alerts.json). Each of these

alerts will provide the security team with information about the actions taken and the status of the endpoint on the Wazuh dashboard.

Implementation and Testing of System Functionality

The implementation phase of this research involves the installation, configuration, and creation of firewall scripts in the testing environment to ensure that the firewall system and active responses function as expected. This process includes the installation and configuration of hardware, the ubuntu server operating system, proxmox and VMware, and the active response framework using Python scripts. Testing will be conducted with real attack scenarios using tools in Kali Linux to assess reconnaissance attacks, access attacks, and DoS attacks. The researcher will measure the effectiveness of the system in detecting, responding to, and mitigating attacks on the firewall by monitoring the Wazuh dashboard. The results from this implementation phase will provide empirical data that can be used to evaluate the effectiveness and performance of the proposed solution in the research.

The Wazuh agent is implemented with Suricata for attack detection capabilities on the Wazuh agent. Suricata will function as an intrusion detection system to provide threat detection and Nmap scanning capabilities. By installing the Wazuh Agent on each ubuntu server, the agent can collect logs from Suricata and send them to the Wazuh manager for potential threat analysis. The implementation of XDR aims to detect threats in real-time using the Wazuh dashboard and mitigate threats on the network infrastructure. It plays a role in collecting, analyzing, and responding to Wazuh agents or services on operating systems and MikroTik router devices in real-time. This installation process will begin with the installation of the Wazuh indexer node, server, and dashboard on VPS public, which is responsible for receiving and processing logs from various Wazuh agents distributed and installed on endpoint devices (ubuntu server vServers and MikroTik routers). Wazuh manager working to maximize syslog and log archive capabilities for active responses XDR, an index pattern is used to analysis and store logs from Wazuh agents, including vServer and router. The storage created by the Wazuh manager contains alerts, log, and other data collected from Wazuh agent endpoints. The Wazuh index pattern to be implemented and configured includes log (archive.log and alert.log). The Wazuh-archive stores all events received by the Wazuh manager, allowing for the review of historical security incident data, trend analysis, and report. In figure 4 it is configuration `<alerts_log>yes</alerts_log>` will function to record all logs and alerts generated by Wazuh into alerts.log and archive.log files.

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>yes</logall_json>

  <remote>
    <connection>syslog</connection>
    <port>514</port>
    <protocol>udp</protocol>
    <allowed-ips>10.151.20.128/25</allowed-ips>
    <local_ip>103.214.112.64</local_ip>
  </remote>
```

Figure 4 Wazuh manager (ossec_config) configuration

These log files will be used to track and review alerts detected on the Wazuh server. `<logall_json>yes</logall_json>`: functions to enable logging of all log datasets. `<jsonout_output>yes</jsonout_output>` will be configured to be able to save all log results.
Connection refers to the type of connection used by syslog for the Wazuh agent to send logs to the Wazuh manager via the syslog protocol. Port is used for syslog connection using the default port 514 and is configured on the Wazuh agent for the syslog log sending process. Protocol will be used for the syslog connection with the UDP protocol for sending logs from the Wazuh agent to the Wazuh manager. Allowed-IPS is a subnet IP address with a permit accept rule to send log data to the Wazuh manager 10.151.20.128/25. Local_IP will specify the Wazuh manager IP address so that the Wazuh agent knows the destination for sending log data. Figure 5 is a configuration Wazuh agent for communication with the Wazuh manager. The configuration of the Wazuh agent for communication to the Wazuh manager involves configuration and parameter settings in the `ossec.conf` file.

```
<ossec_config>
  <client>
    <server>
      <address>103.214.112.64</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>ubuntu, ubuntu20, ubuntu20.04</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
    <enrollment>
      <enabled>yes</enabled>
      <agent_name>Agent_Brute_Force</agent_name>
      <authorization_pass_path>etc/authd.pass</authorization_pass_path>
    </enrollment>
  </client>
<ossec_config>
```

Figure 5 Wazuh agent (*ossec_config*) configuration

In the `<server>` section, the IP address is determined by the `<address>` tag, with a subnet of 103.214.112.64/32. Then for the port used for communication and connection between the Wazuh

agent and Wazuh manager is determined by the <port> tag, with a value of 1514. The protocol used for data transmission between the Wazuh agent and Wazuh manager is the TCP protocol, with the <protocol> tag. The configuration create on this Wazuh agent is to ensure that the Wazuh agent can send log data and receive commands from the Wazuh manager through the modeled network infrastructure communication. The agent node configuration for MikroTik routers is configured on logging to collect logs from routers and send them to Wazuh manager. The command line of R1 and R2 routers are configured as follows:

```
/system logging action
set 3 bsd-syslog=yes
remote=103.214.112.64 syslog-
severity=emergency
/system logging
set 0 action=remote
set 1 action=remote
set 2 action=remote
add action=remote topics=!debug
add action=remote topics=system
```

R1 and R2, will be configured for logging to send logs to Wazuh manager using the default port 514. This configuration created with a new rule adding a new rule to `system` and action to `remote`. This rule policy is configured to ensure that all log messages will be sent remotely to Wazuh manager. Wazuh manager also configured decoder for log format sent by router. This decoder will function to parse log messages from router device for log time data, log source, event type and other relevant data. The first step, create `mikrotik_decoders.xml` file in `/var/ossec/etc/decoders/` directory. This decoder file defines pattern to parse MikroTik log. Decoder (mikrotik) with <prematch> tag is configured to ensure router log can be processed, followed by several child decoder using regex pattern to receive log timestamp, user login, IP address, interface, and protocol. This configuration automatically Wazuh manager will extract log data from router, with rules to detect and respond to attacks. The active response Wazuh architecture modeling is a mechanism for mitigating attacks on Wazuh agent automatically, the technique used is firewall-drop Stateful Active Response. In Wazuh manager active response will be used to respond to emulated attacks from brute force, network mapping, and DoS. Attacks with brute force techniques, Wazuh manager will be configured to detect attacks on SSH protocol services. The implementation of attack emulation in this research, will be emulated with brute force attacks on Wazuh agents with active response scripts, by create rules to block (deny) the attacker IP address. When the rule specified with the name -`SSH brute force trying to get access to the system` is detected, the active response module will run a script to block the attacker IP address. Figure 6 is a snippet of the Stateful Active Response firewall-drop implementation script line.

Figure 6 Firewall-Drop Stateless Active Response Wazuh Manager

The stateful active response firewall-drop configuration above is part of the Wazuh configuration that is run on the Wazuh manager in the `/var/ossec/etc/ossec.conf` file. `<active-response>`: is the main part that defines the active response action. `<command>firewall-drop</command>`: will be configured to determine the script that will be adding the attacker IP `<location>local</location>`: determines the local value agent where the alerts event is detected. `<rules_id>5758</rules_id>`: determines the ID rule that will trigger the active response action on the Wazuh manager. `<timeout>180</timeout>`: determines the duration in seconds to perform the stateful active response action before being automatically canceled. The action that will be the firewall-drop to block the IP address for 180 seconds (3 minutes) and will automatically reactivate.

Figure 7 the script configured for firewall-drop will add the IP address to the firewall list. When the Wazuh manager system detects scanning activity from Nmap and DoS attacks through alerts generated from the Wazuh agent, the rules configured on the Wazuh manager will trigger firewall-drop. `<group`

`name="custom_active_response_rules"` will determine the group with the rules to trigger an active response based on the detected attack. `<field name="event_type">^alert$</field>`, will determine the rule if the type of events is an alert. `<match>Denial of Services (DoS) attack</match>` this rule will trigger when there is a message that matches "Denial of Services (DoS) attack". Nmap rules, the main component is `<rule id="100201" level="12">`, this rule will determine the allocation of ID 100201 and level 12, which indicates the severity level of the threat. `<fieldname="event_type">^alert$</field>` is a rule if the attack event that occurs is an alert.

```
<group name="custom_active_response_rules">
  <rule id="100200" level="12">
    <if_sid>86600</if_sid>
    <field name="event_type">^alert$</field>
    <match>Hping3 DoS attack</match>
    <description>Hping3 DoS attack has been detected.</description>
    <mitre>
      <id>T1498</id>
    </mitre>
  </rule>

  <rule id="100201" level="12">
    <if_sid>86600</if_sid>
    <field name="event_type">^alert$</field>
    <match>SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)</match>
    <description>Nmap Scripting Engine detected.</description>
    <mitre>
      <id>T1595</id>
    </mitre>
  </rule>
</group>
```

Figure 7 Firewall-Drop Stateless Active Response Wazuh Manager (Nmap and DoS)

Operate (Operation and Execution)

The operation phase test attack techniques with reconnaissance attacks (Nmap), access attacks (brute force), and DoS attacks.

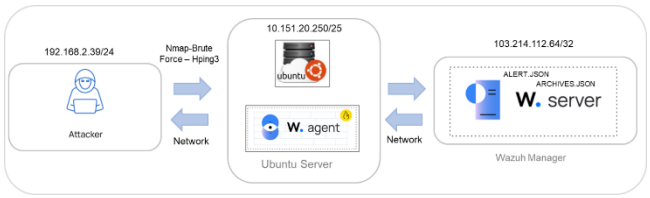

Figure 8 Attacker attack scenario towards Wazuh agent

Figure 8 scenario performed attack Nmap to the ubuntu server and router (Wazuh agent). In this scenario, the attacker uses the IP address subnet 192.168.2.39/24 to scan the system on the target network (Wazuh agent). The Wazuh agent is connected to the Wazuh manager. When the Wazuh agent detects an attack, the Wazuh agent will send log data and the Wazuh server in the archives.json and alert.json files will store and process the logs for analysis and display them on the Wazuh dashboard. Brute force attack activity was carried out from kali linux OS using hydra to try crack the SSH login password credentials on the IP address 10.151.20.252 using the username agent. on the wordlist rockyou.txt. Hydra processed trying as many combinations of username and password credentials wordlist rockyou.txt file. The attack process by running up to 4 tasks in parallel to speed up the process, hydra tries to find the correct password for the username "agent" on the Wazuh agent (ubuntu server).

Figure 9 Attack alerts detected on the Wazuh manager

Figure 9, shows on July 12, 2024, number of logs from the Wazuh agent showed scanning activity using Nmap. The log entry records the detection of Nmap scripting engine detected, this notification indicates the use of the Nmap scripting engine in the attack. Testing of brute force attacks with wordlist to the targeted Wazuh agent (10.151.21.252). Within a few minutes hydra had tried 87 password combinations from a total of 14,344,398 combinations. Figure 50 is monitoring on the Wazuh dashboard. The notification 180 authentication failure indicates that there were 180 failed authentication attack attempts on the Wazuh agent. This notification indicates that there were attempts at attacks and brute force attempts using wordlist, with unauthorized login attempts trying to access the Wazuh agent operating system using incorrect password credentials.

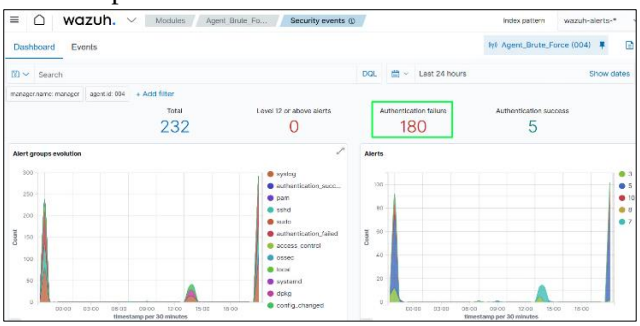

Figure 10 Failed authentication attempts from brute force attack

DoS attack testing on MikroTik RouterOS devices (Wazuh agent) aims to evaluate Wazuh ability to detect and respond to DoS attacks. In this test, hping3 is used

to perform DoS attacks from a virtual machine installed in VMware.

Figure 11 Denial of Service (DoS) attack statistics on Wazuh manager

Figure 11 is one of logs that shows an attempted syn flood attack from the attacker IP address 192.168.2.39 to target IP address 10.151.20.238 Wazuh agent on service port 80, which was detected by Wazuh as high traffic and an attempted syn flood attack. Figure 11 is result of DoS attack on Wazuh manager, by showing number of logs and statistics over a certain time and recording attack activity on router.

The attack statistics in the figure 11 graph show the number of hits per second received by the Wazuh manager during a certain time on july 30, 2024, between 20:29:30 and 20:30:00 as many as 8,867, and with a total of 299 hits per second. This number shows a spike in traffic caused by a DoS attack. The detailed attack log contains several log entries that show syn flood attacks and high traffic.

RESULTS AND DISCUSSION

The results of this research are the optimize phase, which focuses on increasing the effectiveness and efficiency of the security system of the network infrastructure that has been implemented. The steps taken include two main aspects, namely the configuration and evaluation of firewall optimization and active responses Wazuh XDR, and evaluation of the performance of network interface capacity resources, CPU and memory on server and router devices before and after an attack occurs.

Figure 12 shows the implementation of a network infrastructure security system using Wazuh XDR with active responses. The logs generated from this Nmap scanning, brute force and DoS activity will be sent from the Wazuh agent to the Wazuh server (103.214.112.64/32).

This log is sent through a router gateway that functions as a liaison between the internal network and the wazuhWazuh server located in the public cloud. WazuhWazuh server will receive the logs and perform analysis based on the configured rules and decoders. This analysis allows the wazuhWazuh server to detect suspicious activity patterns such as Nmap scanning, brute force attacks and DoS attacks. Based on the analysis results, the wazuhWazuh server detects Nmap scanning from the attacker IP address (192.168.2.39).

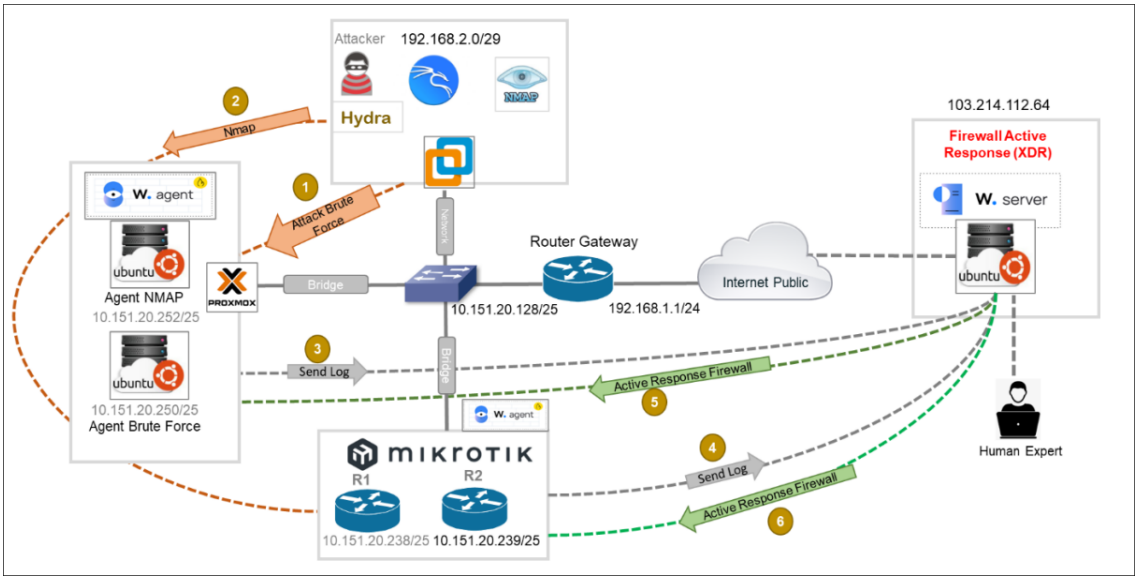

Figure 12 Firewall active responses Wazuh XDR optimize Topology

Figure 13 Wazuh manager performs its function as an intrusion detection system and XDR active response.

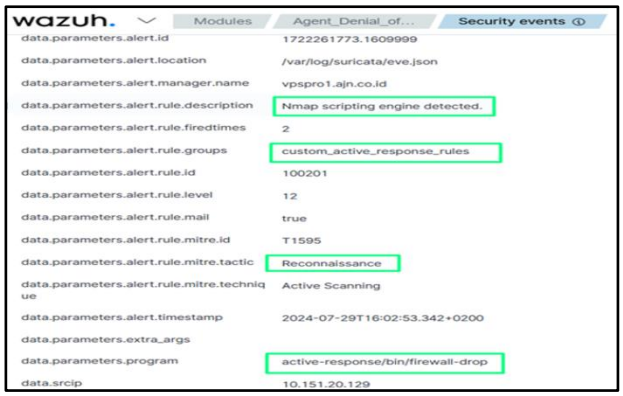

Figure 13 Nmap attack manager detection (Scanning)

Index pattern detection of Wazuh manager attacks successfully detects scanning activity on the Wazuh agent which is carried out using Nmap `data.parameters.alert.rule.description` : Nmap scripting engine detected. From value of `data.parameters.program` which shows the execution of the `active-response/firewall-drop` program. After detecting an attack, the Wazuh server will activate the configured active response module. In this case, the active response firewall is activated to block the attacker IP address that was scanned by Nmap.

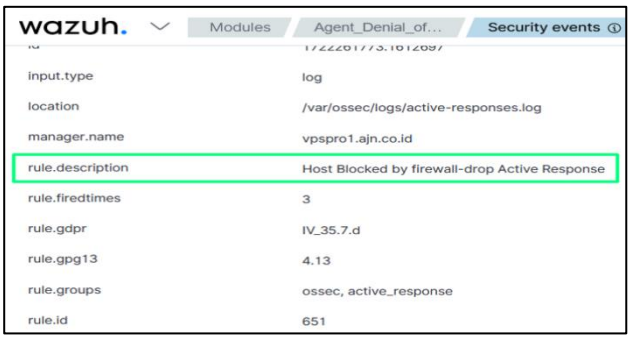

Figure 14 Active responses Wazuh attack (Nmap)

Figure 14 shows that the active responses successfully blocked the attack. This is indicated by the value of `rule.description = Host blocked by Firewall Active Response`.

SSH brute force attack emulation testing with active response, configured to block the attacker IP address. The main purpose of this configuration is to prevent brute force attacks on the active SSH service on the Wazuh agent device. The steps taken to detect attacks and execute Wazuh active responses are used with the following process steps:

1. Rule ID - response to be executed and run for every log event with ID 5758
2. Rule Group - response to executed and run for every event in the configured group
3. Level - response to executed and run for every event at low level to high level.

The active responses module is configured to run script blocking the attacker IP address when the rule 5758 - maximum authentication attempts exceeded occurs. The detection configuration the Wazuh agent to monitor SSH authentication, login access attempts when exceeding the maximum limit, with rule ID 5758, the Wazuh agent will send a log to the Wazuh server for analysis. Figure 15 show detection Wazuh server when receiving a log from the Wazuh agent by detecting rule 5758 will be triggered that a brute force attack has occurred on the SSH service.

Figure 15 Brute Force Attack Detection Results on Wazuh Manager (Dashboard)

Figure 16 shows a spike in traffic on Wazuh agent starting at 14:07. This increase in traffic is the number of bits received by the ens180 interface on the Wazuh agent. Before 14:07, traffic on the interface was relatively stable. However, after 14:07, there was a significant increase, reaching a peak of 60 Kbps.

This increase in traffic indicates that the brute force attack using the rockyou.txt wordlist began to put a significant load agent device interface, by sending large number of requests to the target server. Packets received is the number of packets received also increased, this increase in traffic is an authentication attempt sent by the attacker from the brute force attempt.

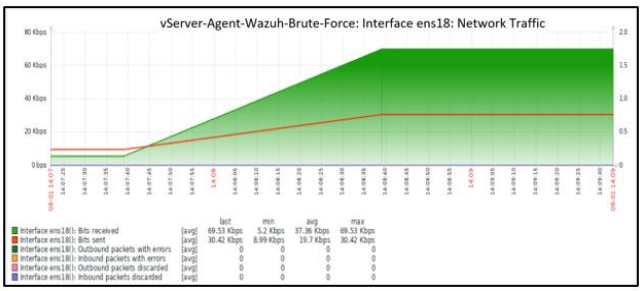

Figure 16 Increase in ens18 traffic on Wazuh agent from brute force attack

Figure 17, it can be seen context switches and interrupts per second on CPU jumps start to occur 14:07. Previously, CPU jumps value was normal level. However, after 14:07, this value increased, indicating that CPU jumps began to receive more requests and interrupts from running processes reach 20% to 85%. High context switches indicate that CPU jumps had to switch frequently between processes, this was caused by the high workload of the brute force attack.

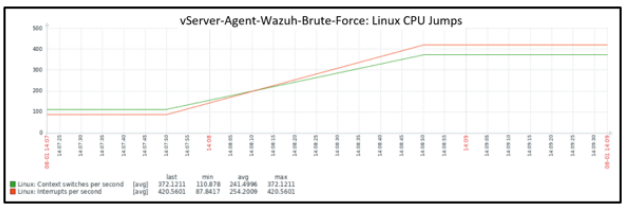

Figure 17 Increased CPU traffic jumps on the Wazuh agent from brute force attacks

Figure 18 number of authentication failures 2198, is authentication failure within 1 hour. The analysis results from Wazuh manager show a very massive brute force attack on Wazuh agent.

Figure 18 Authentication Failure Brute Force Attack (1 Hour)

Figure 19 concluded Wazuh manager successfully performs its function as an intrusion detection system and XDR active response, with a value in `data.parameters.alert.rule.description:` maximum authentication attempts exceeded, this can be seen in the `rule.description` value which shows the execution of the `Host Blocked by firewall-drop active response` program.

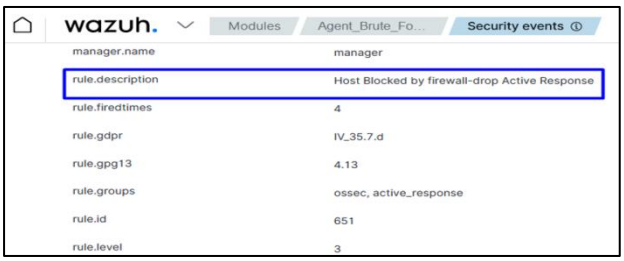

Figure 19 Active Response Firewall Results from Brute Force Attacks

Figure 20 after monitoring 2 hours, the number of authentication failures remains the same, which is 2198 (authentication failure), which indicates that there were no additional successful attacks from attackers penetrating the Wazuh agent.

Figure 20 Authentication Failure Brute Force Attack (2 Hour)

Figure 21 shows that after the active response firewall was activated, there was a decrease in traffic from 14:09. Before that time, the capacity of the ens18 interface showed a significant increase in traffic, reaching 60 Kbps. However, after 14:09, traffic on the ens18 interface decreased to 0-1 Kbps. This shows that the active response firewall successfully blocked the ongoing brute force attack.

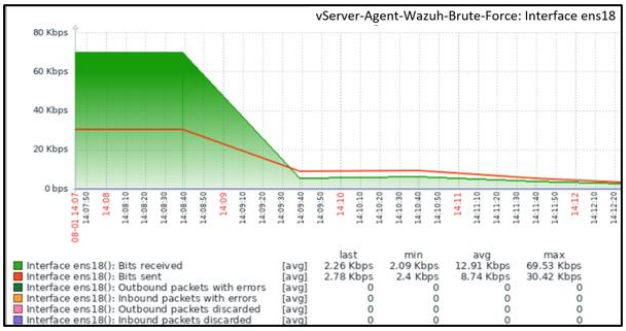

Figure 21 Reduction in network traffic usage traffic on the Wazuh agent

Figure 22 shows a decrease in CPU jumps context switches and interrupts per second, starting around 14:09. The CPU value drops back to a stable, lower level. This decrease in value indicates that after the active response firewall was enabled, the CPU jumps workload due to high interrupts and requests from brute force attacks was significantly reduced, and the CPU jumps returned to normal (reached 15% after active response firewall was activated).

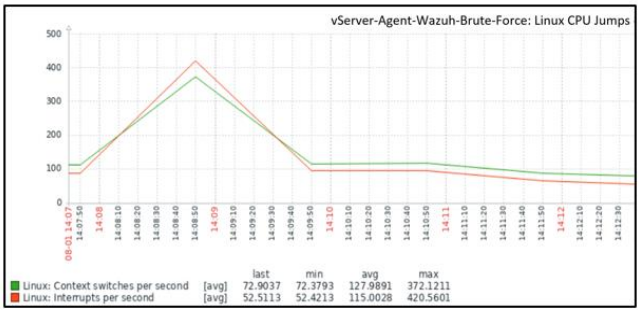

Figure 22 Reduction in CPU Usage Traffic on the Wazuh agent

Figure 23 Wazuh agent experiencing a significant DoS attack. There is an increase in resource capacity in a relatively short time. This spike is an activity that floods the Wazuh agent system with excessive requests, thus disrupting the normal performance of the system.

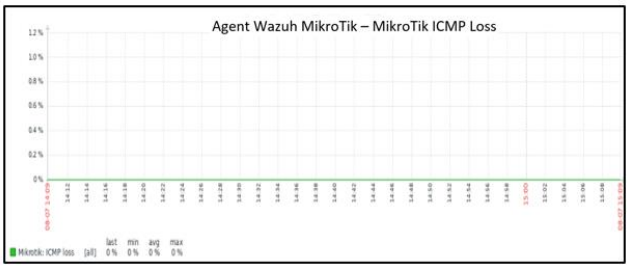

Figure 23 ICMP ping loss attack DoS

ICMP ping loss is seen spike significantly at 13:00, with ICMP ping loss reaching 100%. This ping loss indicates that during the DoS attack, the router was unable to respond to ICMP ping requests, indicating a complete loss of connectivity.

Figure 24 shows the result of ICMP ping response dropping to 0 at 13:00. This drop confirms the total loss of ICMP ping response, from this DoS attack can be seen that the router is unable to process ping requests due to the DoS attack.

Figure 24 ICMP ping loss attack DoS

Figure 25 shows router memory capacity usage is relatively low and normal before the attack at 13:00, there is a high spike in memory usage, reaching 67%. This spike indicates that the router memory is heavily burdened during the DoS attack, showing the router inability to handle network traffic.

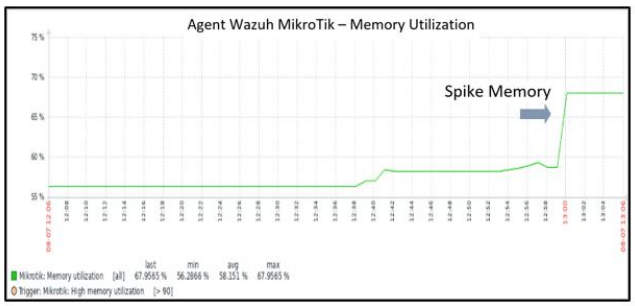

Figure 25 High Spike Memory Usage Attack DoS

Figure 26 shows router CPU capacity usage is relatively low and normal before the attack at 13:00, there is a high spike in CPU usage, reaching 67%. This spike indicates that the router CPU is heavily burdened during the DoS attack, showing the router's inability to handle network traffic.

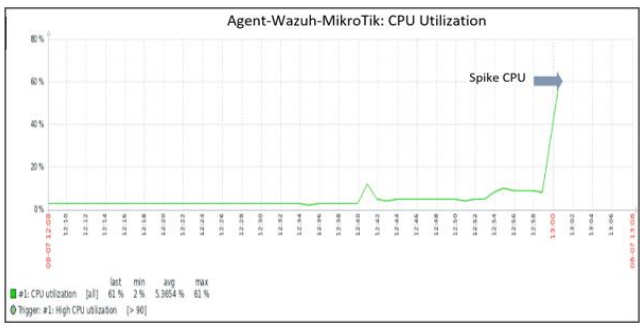

Figure 26 High Spike Memory Usage Attack DoS

After the active response firewall is activated, it can be seen in the graph that the CPU utilization on the Wazuh agent device has started to decrease, returning to a maximum normal usage of 3%. The increase in CPU utilization shows that the DoS attack caused a very high workload on CPU utilization, but from the activation of the Wazuh manager firewall active response managed

to reduce the load significantly, by blocking the attacker IP address.

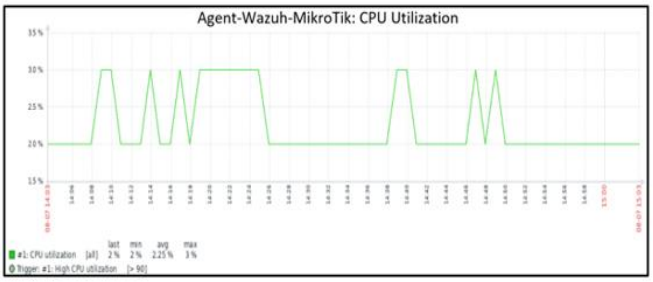

Figure 27 Reduction in CPU usage traffic on the Wazuh agent

In addition, the memory usage graph in figure 28 also shows normalization after Wazuh server active response was enable.

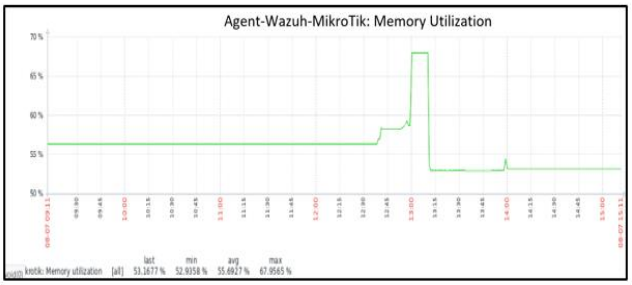

Figure 28 Reduction in memory usage traffic on the Wazuh agent

In addition, figure 29 ICMP ping and ICMP loss figure 30 usage graphs also show normal results after the Wazuh server's active response was activated, blocking the attacker IP address.

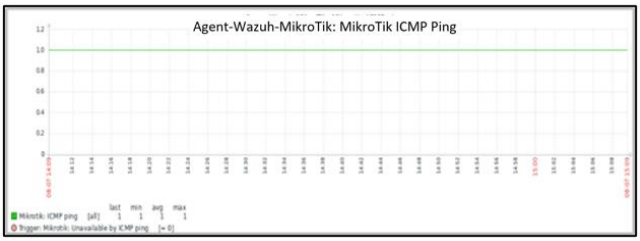

Figure 29 ICMP Ping normal status

Before the intervention, the DoS attack caused a significant increase in memory usage and caused ICMP packet loss decrease in ICMP ping. However, after the mitigation system was implemented, all these metrics returned to normal, indicating that the attack had been successfully resolved and the network was operating stable again.

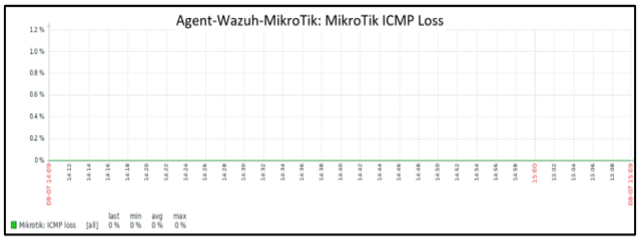

Figure 30 ICMP Ping Loss normal status

This mitigation proves the effectiveness of Wazuh XDR firewall implementation in maintaining network stability and security for router devices against DoS attacks. Overall, these results underscore the importance of having a responsive detection and mitigation system to ensure the continuity of network operations without significant disruption.

CONCLUSIONS

The implementation of intrusion detection and mitigation system from this research shows and produces that the techniques used on the router and server device infrastructure are very effective in detecting and mitigating various emulated attacks. The configured Wazuh manager successfully detected brute force attacks, DoS and Nmap scanning, and activated the active response firewall to block the attacks based on the attacker malicious IP address. In scanning using Nmap, Wazuh XDR was able to detect scanning activity and activate the active response firewall to block the attacker IP. During the brute force attack, a significant increase in CPU usage and network traffic was observed, but after the firewall was activated, CPU usage and network traffic returned to normal, indicating the effectiveness of the system in handling the attack. In the case of a DoS attack on MikroTik RouterOS, CPU and memory usage increased by users, but after the active response firewall was activated, CPU usage dropped back to normal status. Overall test results indicate and produce that the XDR active response firewall provides protection against various types of modeled attacks, reduces system workload, and ensures network stability. The implications of the research results with active and fast response on XDR, ensuring the stability and security of router and server devices, this system can help organizations in monitoring and managing attacks efficiently, reducing manual intervention and the risk of undetected attacks. Wazuh manager is effective in detecting and mitigating modeled attacks.

ACKNOWLEDGEMENTS

The author would like to thank DRPM Universitas Budi Luhur for the support and funding for research with Nomor: K/UBL/FTI/000/004/03/24.

REFERENCE

Akbar, S., Endroyono, & Wibawa, A. D. (2016). The impact analysis and mitigation of DDoS attack on local government electronic procurement service (LPSE). *2016 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, 405–410.

Amami, R., Charfeddine, M., & Masmoudi, S. (2024). Exploration of Open Source SIEM Tools and Deployment of an Appropriate Wazuh-Based Solution for Strengthening Cyberdefense. *2024 10th International Conference on Control, Decision and Information Technologies (CoDIT)*, 1–7.

Ceron, J. M., Scholten, C., Pras, A., & Santanna, J. (2020). MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification. *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, 1–9.

Damanik, H. A. (2022). Securing Data Network for Growing Business VPN Architectures Cellular Network Connectivity. *Acta Informatica Malaysia*, *6*(1), 01–06.

Damanik, H. A., & Anggraeni, M. (2024). Pola Pengelompokan dan Pencegahan Public Honeypot menggunakan Teknik K-Means dan Automation Shell-Script. *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, *12*(1), Article 1.

Damanik, H. A., Anggraeni, M., & Nusantari, F. A. A. (2023). *Konsep dan Penerapan Switching dan Routing Implementasi Jaringan Komputer Berbasis Cisco*. CV. Mega Press Nusantara.

Fuhr, J., Wang, F., & Tang, Y. (2022). MOCA: A Network Intrusion Monitoring and Classification System. *Journal of Cybersecurity and Privacy*, *2*(3), Article 3.

Helmiawan, M. A., Julian, E., Cahyan, Y., & Saeppani, A. (2021). Experimental Evaluation of Security Monitoring and Notification on Network Intrusion Detection System for Server Security. *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 1–6.

Kurniawan, C., & Triayudi, A. (2024). Reconstruction and Detection of Gambling Web Defacement Attack Using Wazuh and Velociraptor. *2024 International Conference on Information Technology Research and Innovation (ICITRI)*, 257–262.

Moiz, S., Majid, A., Basit, A., Ebrahim, M., Abro, A. A., & Naeem, M. (2024). Security and Threat Detection through Cloud-Based Wazuh Deployment. *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, 1–5.

Nursetyo, A., Ignatius Moses Setiadi, D. R., Rachmawanto, E. H., & Sari, C. A. (2019). Website and Network Security Techniques against Brute Force Attacks using Honeypot. *2019 Fourth International Conference on Informatics and Computing (ICIC)*, 1–6.

Oktivasari, P., Zain, A. R., Agustin, M., Kurniawan, A., Murad, F. arbi, & Anshor, M. fabian. (2022). Analysis of Effectiveness of Iptables on Web Server from Slowloris Attack. *2022 5th International Conference of Computer and Informatics Engineering (IC2IE)*, 215–219.

Praptodiyono, S., Firmansyah, T., Anwar, M. H., Wicaksana, C. A., Pramudyo, A. S., & Al-Allawee, A. (2023). Development of hybrid intrusion detection system based on Suricata with pfSense method for high reduction of DDoS attacks on IPv6 networks. *Eastern-European Journal of Enterprise Technologies*, *5*(9 (125)), Article 9 (125).

Prasad, M. D., Sindusha, M. S. N. V. R. S., Jahnavi, N., Ali, M. W., & Devi, S. A. (2024). Enabling Cybersecurity Defenses: Advanced Endpoint Detection, Data Breach Identification, and Anomaly Resolution. *2024 8th International Conference on Inventive Systems and Control (ICISC)*, 461–468.

Subhan, A., Kunang, Y. N., & Yadi, I. Z. (2023). Analyzing the Attack Pattern of Brute Force Attack on SSH Port. *2023 International Conference on Information Technology and Computing (ICITCOM)*, 67–72.

Triantopoulou, S., Papanikas, D., & Kotzanikolaou, P. (2019). An Experimental Analysis of Current DDoS attacks Based on a Provider Edge Router Honeynet. *2019 10th International Conference on Information, Intelligence, Systems and Applications (IISA)*, 1–5.

Zebari, R. R., Zeebaree, S. R. M., & Jacksi, K. (2018). Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers. *2018 International Conference on Advanced Science and Engineering (ICOASE)*, 156–161.