Utilizing Game Console as an OSSEC Platform to Detect and Respond to Cyber Attacks

Ramiati[1], Ratna Dewi[2], Rikki Vitria[3], Ideva Gaputra[4], Harfebi Fryonanda[5]
{ramiati@pnp.ac.id[1], ratnadewi@pnp.ac.id [2], rikkivitria@pnp.ac.id[3]
,ideva@pnp.ac.id[4],harfebi@pnp.ac.id[5]}

Politeknik Negeri Padang, contact address[12345]

Abstract. This research explores the potential of the Sony PlayStation 4 (PS4) varian Slim, which has been converted into a web server, as an efficient platform for Open Source Security Information and Event Management (OSSEC) in detecting and responding to cyber-attacks. In the era of information technology that continues to develop, cyber-attacks are increasingly complex and threaten data and infrastructure security. Therefore, developing methods and tools that can identify threats and provide a rapid response is very important. The PS4 Slim was chosen as the research platform because of its low power consumption, potential to reduce operational costs in the long term, and ability to run OSSEC and act as a web server. In scenario testing, including penetration testing with Metasploit, Nmap, and SQL injection testing using Sqlmap, this game console successfully detected attacks and provided an efficient response. This research provides insight into the potential for sustainable use of existing resources for network security monitoring in the face of increasingly sophisticated cyber attacks.

Keywords: ossec, PS4, SQL Injection, HIDS, NMap.

1 Introduction

The rapid growth of information and communications technology (ICT) has brought tremendous benefits, but it has also introduced new threats in the form of increasingly sophisticated and destructive cyber attacks. Organizations and individuals are often targets[2] of cyberattacks that can threaten data security, infrastructure, and privacy. Therefore, developing methods and tools to detect, prevent, and respond to cyber attacks is necessary [3].

Open Source Security Information and Event Management (OSSEC) is a credible open-source solution for Host-Based Intrusion Detection Systems (HIDS), which functions to identify potential attacks or intrusions into systems and networks [4]. OSSEC works by detecting suspicious behavior patterns or unusual signs of attacks[5]. One of the main challenges in implementing OSSEC is determining an efficient and effective platform supporting security monitoring tasks.

In recent years, entertainment devices such as game consoles have become increasingly connected to internet networks[6]. Modern game consoles have impressive computing capabilities and can be converted into web servers, which allows their use for other purposes, including network security monitoring. One game console of interest for this research is the Sony PlayStation 4 (PS4) Slim, known for being power efficient and having sufficient processor and RAM capabilities to run security monitoring applications.

ABEC 2023, September 21, Bengkalis, Indonesia

DOI 10.4108/eai.21-9-2023.2342969

This research explores the potential of a PS4 Slim converted into a web server as a platform for efficient OSSEC. PS4 Slim with web server has low power consumption, which can reduce operating costs in the long run. The PS4 Slim, as a security monitoring tool, utilizes existing resources more sustainably.
By utilizing a PS4 Slim converted into a web server as an OSSEC platform, this research will also investigate the effectiveness and efficiency of game consoles in identifying and responding to cyber-attacks. The results of this research can provide valuable insight into how to integrate entertainment devices that have been converted into web servers with increasingly complex network security..

2 Research Methods

In designing the scenario that will be implemented, it can be seen in **Fig.1** .

Fig. 1. Skenario Host-Based Intrusion Detection System (HIDS)

This research on HIDS was carried out in several stages, starting with creating scenarios and attack patterns in research methodology, such as the flowchart in Figure 2. Reports regarding intrusion detection can be accessed via remote SSH on the command line interface (CLI) with the command tail –f /var/ossec/logs/alerts/alerts.log. With log activity reporting, administrators can see activity in real time. Administrators will be presented with complete information regarding detected incidents. Particular information for analyzing incidents is based on the rules classification (level) in OSSEC, which displays text and includes all activity log results.

Identification The problem with the methodology is how the PS4 Slim device can run Linux Operating System and OSSEC application. Literature study taken on basis research where the Linux operating system previously ran on public computers and will run on the PS4 Slim console. Preparation for Software Installation, namely the Operating System Fedora 32 has been customized to run on the PS4 Slim console.

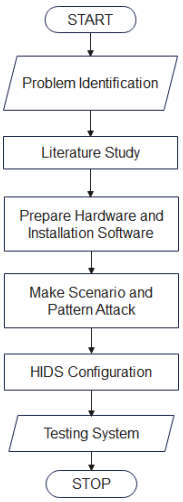

Fig. 2. Reseach Method

Then the package will be detected by comparing existing rules. If identified as an intrusion, it will be carried out Recording which will later produce a warning in real time or in the form of digital documents. See Figure 3.

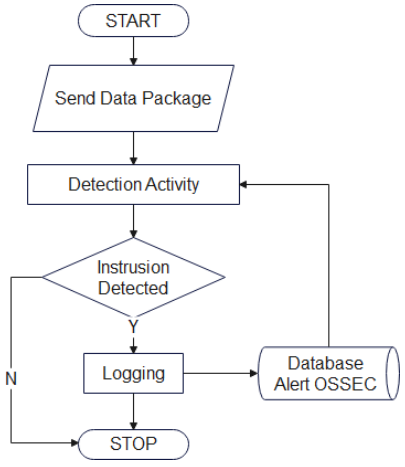

Fig. 3. Scenario System Intrusion Detection

Based on predefined classification rules, OSSEC will analyze data packets sent from the Raspberry Pi3 device attack. It is ignored if the packet is not detected as an intrusion or attack. However, when the package is detected as an intrusion, it will be recorded in the log file or database. After being recorded and stored in the OSSEC alert database.

3 Result and Discussion

3.1 Login Access Testing Scenario using SSH

Attempting access via the Secure Shell (SSH) protocol, one of the main entrances to servers and network systems. This testing covers various aspects, including attempted authentication attempts using username and password combinations that may be weak or vulnerable authentication methods[7].

During this test scenario, researchers will log any suspicious access attempts, noting the source IP address, time and date of access, and the outcome of the authentication attempt, whether successful or failed. In addition, this research will also examine system activity logs and identify potential security gaps that attackers can exploit to access the system. The results of this test scenario will provide an in-depth understanding of the system's security vulnerabilities against attacks via SSH and help in designing the necessary security measures to protect the system from unauthorized access..

3.2 Testing Scenarios Using Nmap

In this scenario, researchers will use the Nmap network scanning tool to scan the network and system infrastructure. Nmap is a valuable tool for identifying open ports, running services, and network configuration[8], allowing researchers to view network infrastructure from an attacker's perspective[9].

During this test scenario, researchers will log Nmap scan results, including open ports[10], running services, and essential information about the network, such as IP addresses and configuration[11]. The main goal of this testing is to identify potential security vulnerabilities[11] that may exist in the network infrastructure and to test the effectiveness of the monitoring system (such as OSSEC) in detecting and responding to suspicious network scans. The results of these scenarios will provide valuable insight into the strengths and vulnerabilities of the network and system infrastructure used in this research.

3.3 Testing Scenarios Using Sqlmap

In this scenario, researchers will use the Sqlmap penetration testing tool to search for and exploit potential SQL Injection vulnerabilities in the targeted web application or system[12][13]. SQL Injection attacks are one of the most common cyber attacks and can be damaging because they can provide illegal access to database systems [13].

During this test scenario, researchers will record the results of a successful attack, including information found in databases that may include sensitive data. Additionally, researchers will identify necessary steps to protect applications or systems from future SQL Injection attacks. The results of these scenarios will provide a deep understanding of the security vulnerabilities in the web applications or systems used in this research, as well as provide a basis for taking proactive actions to improve the security of the applications and underlying data.

3.4 System response to Login Access Testing using SSH

```
** Alert 1694758141.3212: - syslog,sshd,authentication_failed,
2023 Sep 15 13:09:01 localhost->/var/log/secure
Rule: 5716 (level 5) -> 'SSHD authentication failed.'
Src IP: 192.168.88.161
User: ITmania
Sep 15 13:09:00 localhost sshd[5937]: Failed password for ITmania from 192.168.88.161 port 14591 ssh2

** Alert 1694758145.3517: - syslog,sshd,authentication_success,
2023 Sep 15 13:09:05 localhost->/var/log/secure
Rule: 5715 (level 3) -> 'SSHD authentication success.'
Src IP: 192.168.88.161
User: ITmania
Sep 15 13:09:03 localhost sshd[5937]: Accepted password for ITmania from 192.168.88.161 port 14591 ssh2
```

Fig. 4. System Respons Using SSH

The first OSSEC alert (authentication_failed) indicates a failed SSH authentication attempt occurred on the system. The associated log message indicates that user "ITmania" attempted to log in with an incorrect password from IP address "192.168.88.161" on port 14591 with SSH2 protocol. The rule used in this alert has a severe level of 5, indicating high importance, and aims to detect failed SSH authentication attempts. This alert is an initial warning of suspicious or potential authentication attempts from unknown sources.

The second OSSEC alert (authentication_success) records successful SSH authentication by user "ITmania" from the same IP address, "192.168.88.161." Although this was a successful authentication, the associated rule has a severe level of 3, indicating moderate importance. This helps in monitoring and logging significant authentication activities in the system. The combination of these two alerts makes monitoring suspicious and successful SSH authentications possible, which is vital for keeping systems and networks secure from potential threats.

3.5 System Response to the Use of Nmap

```
** Alert 1694758207.4665: - apache,access_denied,
2023 Sep 15 13:10:07 localhost->/var/log/httpd/error_log
Rule: 30306 (level 5) -> 'Attempt to access forbidden directory index.'
Src IP: 192.168.88.161
Src Port: 14611
[Fri Sep 15 13:10:06.972545 2023] [autoindex:error] [pid 855:tid 1002] [client 192.168.88.161:14611]
AH01276: Cannot serve directory /var/www/html/: No matching DirectoryIndex (index.html,index.php)
found, and server-generated directory index forbidden by Options directive
```

Fig. 5. System Respons Using Nmap

This alert indicates that there has been a denial of access to the Apache HTTP Server service, which is recorded in the Apache error log file. The rule used in this alert has a severe level of 5 and aims to detect failed access attempts to prohibited index directories. The log message that triggers this alert explains that there was an attempt to access the directory "/var/www/html/" that does not have a suitable index file, such as "index.html" or "index.php," and the server has denied access because the Options directive prohibits Server-generated directory indexes. This information helps identify and troubleshoot problems related to unauthorized access or improper server configuration.

```
** Alert 1694758207.5158: - web,accesslog,
2023 Sep 15 13:10:07 localhost->/var/log/httpd/access_log
Rule: 31101 (level 5) -> 'Web server 400 error code.'
Src IP: 192.168.88.161
192.168.88.161 - - [15/Sep/2023:13:10:06 +0700] "GET / HTTP/1.1" 403 5564 "-" "Mozilla/5.0 (Windows NT
10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0"
```

Fig. 6. Alert Indicated http services

The OSSEC alert with a unique identification number 1694758207.5158 occurred on September 15, 2023, at 13:10:07 and is related to an Apache HTTP Server access log recorded in the access_log file. The rule used in this alert has a severe level of 5 and aims to detect error code 400 from the web server. The log message that triggered this alert indicates that the IP address "192.168.88.161" attempted to access the home page ("/") with the "GET" method, but the server returned status code 403, indicating access denied. This could represent an unauthorized access attempt or a problem in the web request that needs to be investigated further in the context of your web server's security.

```
** Alert 1694758217.5498: mail  - syslog,errors,
2023 Sep 15 13:10:17 localhost->/var/log/secure
Rule: 1002 (level 2) -> 'Unknown problem somewhere in the system.'
Sep 15 13:10:16 localhost phpMyAdmin[808]: user denied: test (empty-denied) from 192.168.88.161
```

Fig.7. Alert Indicated Nothing Get Vulnerability

The OSSEC alert with a unique identification number 1694758217.5498 occurred on September 15, 2023, at 13:10:17 and is associated with a log message logged in a secure file. The rules used in this alert have a severe level of 2 and aim to detect unknown problems in the system. The log message that triggers this alert is "user denied: test (empty-denied) from 192.168.88.161," which indicates that there was a denied access attempt by user "test" from the IP address "192.168.88.161" to PHPMyAdmin. This error refers to an authentication or permissions issue within PHPMyAdmin, which requires further investigation to understand the source of the problem. This alert also notes that there is an unknown issue in the system simultaneously, which also needs to be investigated.

```
** Alert 1694784897.3333214: - web,accesslog,attack,
2023 Sep 15 20:34:57 localhost->/var/log/httpd/access_log
Rule: 31104 (level 6) -> 'Common web attack.'
Src IP: 192.168.88.59
192.168.88.59 - - [15/Sep/2023:20:34:55 +0700] "GET /CFIDE/administrator/enter.cfm?locale=..\\..\\..
\\..\\..\\..\\..\\..\\CFusionMX\\lib\\password.properties%00en HTTP/1.1" 404 196 "-" "Mozilla/5.0
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

Fig.8. Alert Indicated Vurnerability SQL Injection

The OSSEC alert with a unique identification number 1694784897.3333214 occurred on September 15, 2023, at 20:34:57 and is associated with a log message logged in the access_log file of the Apache HTTP web server service. The rules used in this alert have a severity level of 6 and aim to detect common attacks on web services. The log message that triggers this alert indicates that there was a suspicious attack attempt from the IP address "192.168.88.59" trying to access a suspicious URL, trying to reach the "password.properties" file in an unauthorized directory, indicating a potential security flaw attempt in the system. Additionally, information

about the user agent used in the attack indicates that it resulted from the Nmap Scripting Engine scanning tool. These alerts help detect and deal with suspicious attacks on web services and provide insight into the potential pursuit of system vulnerabilities.

```
** Alert 1694784899.3339169: - apache,access_denied,
2023 Sep 15 20:34:59 localhost->/var/log/httpd/error_log
Rule: 30306 (level 5) -> 'Attempt to access forbidden directory index.'
Src IP: 192.168.88.59
Src Port: 50648
[Fri Sep 15 20:34:59.091816 2023] [autoindex:error] [pid 22145:tid 22186] [client 192.168.88.59:50648]
AH01276: Cannot serve directory /var/www/html/: No matching DirectoryIndex (index.html,index.php)
found, and server-generated directory index forbidden by Options directive
```

Fig.9. Alert Indicated Access Denied Nothing Index

The OSSEC alert with a unique identification number 1694784899.3339169 occurred on September 15, 2023, at 20:34:59 and is associated with a log message logged in the error_log file of the Apache HTTP web server service. The rule used in this alert has a severe level of 5 and aims to detect access attempts to access prohibited directory indexes. The log message that triggers this alert indicates that the IP address "192.168.88.59" attempted to access the directory "/var/www/html/" with source port 50648. However, the server returned status code 403, indicating denied access. The log message also explains that the server cannot serve the request because there is no appropriate directory index file (for example, "index.html" or "index.php"), and the Options directive prohibits the directory index generated by the server. This indicates an unauthorized access attempt or a problem in the request that needs to be investigated further in the context of your web server's security. This information is helpful for monitoring and troubleshooting problems related to unauthorized access or incorrect server configuration.

3.6 System response to using Sqlmap

```
** Alert 1694784903.3802666: - web,accesslog,
2023 Sep 15 20:35:03 localhost->/var/log/httpd/access_log
Rule: 31101 (level 5) -> 'Web server 400 error code.'
Src IP: 192.168.88.59
192.168.88.59 - - [15/Sep/2023:20:35:03 +0700] "HEAD /phpMyAdmin-2.7.0/ HTTP/1.1" 404 - "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

Fig.10. Alert Indicated Access Log SQL Injection

The OSSEC alert with a unique identification number 1694784903.3802666 occurred on September 15, 2023, at 20:35:03 and corresponded to a log message logged in the access_log file of the Apache HTTP web server service. The rule used in this alert has a severe level of 5 and aims to detect error code 400 from the web server. The log message that triggers this alert indicates that there was an attempt to send a "HEAD" request to the URL "/phpMyAdmin-2.7.0/" from the IP address "192.168.88.59." The server returns a 404 status code, indicating that the requested page was not found.

The log message also notes that the user agent used in the request is "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)," indicating that this is the result of the Nmap Scripting Engine scanning tool. This alert records suspicious access attempts to a specific URL and the server's response to the request. This can indicate scanning attempts or exploration of potential vulnerabilities on the web server, and these alerts help in detecting and identifying suspicious activity on the web server service.

```
** Alert 1694784905.3804812: - apache,access_denied,
2023 Sep 15 20:35:05 localhost->/var/log/httpd/error_log
Rule: 30306 (level 5) -> 'Attempt to access forbidden directory index.'
Src IP: 192.168.88.59
Src Port: 51126
[Fri Sep 15 20:35:04.217581 2023] [autoindex:error] [pid 849:tid 972] [client 192.168.88.59:51126]
AH01276: Cannot serve directory /var/www/html/: No matching DirectoryIndex (index.html,index.php)
found, and server-generated directory index forbidden by Options directive

** Alert 1694784905.3805305: - apache,access_denied,
2023 Sep 15 20:35:05 localhost->/var/log/httpd/error_log
Rule: 30305 (level 5) -> 'Attempt to access forbidden file or directory.'
Src IP: 192.168.88.59
Src Port: 51126
[Fri Sep 15 20:35:04.223607 2023] [authz_core:error] [pid 849:tid 972] [client 192.168.88.59:51126]
AH01630: client denied by server configuration: /var/www/html/.htaccess
```

Fig.11. Multiple Alert Indicated Access Index SQL Injection

The OSSEC alert with a unique identification number 1694784905.3804812 occurred on September 15, 2023, at 20:35:05 and corresponded to a log message logged in the error_log file of the Apache HTTP web server service. The rule used in this alert has a severe level of 5 and aims to detect access attempts to access prohibited directory indexes. The log message that triggers this alert indicates that the IP address "192.168.88.59" attempted to access the directory "/var/www/html/" with source port 51126. However, the server returned status code 403, indicating that access was denied.

The log message also explains that the server cannot serve the request because there is no appropriate directory index file (for example, "index.html" or "index.php"), and the Options directive prohibits the directory index generated by the server. This indicates an unauthorized access attempt or a problem in the request that needs to be investigated further in the context of your web server's security. This information is helpful for monitoring and troubleshooting problems related to unauthorized access or incorrect server configuration.

4 Conclusion

This research explores the potential of using the Sony PlayStation 4 (PS4) Slim, which has been converted into a web server, as an efficient platform for Open Source Security Information and Event Management (OSSEC) in detecting and responding to cyber-attacks. PS4 Slim was chosen as the platform due to its low power consumption, which can reduce operational costs in the long term, and its ability to run OSSEC and function as a web server.

In this research, testing scenarios, including penetration testing using Metasploit, testing with Nmap, and SQL injection testing using Sqlmap, have been carried out. The test results show the PS4 Slim's ability to integrate OSSEC as an efficient Intrusion Detection System (IDS). PS4 Slim successfully detected cyberattacks, including suspicious access attempts and network scans by tools such as Nmap.

PS4 Slim also provides efficient responses to attacks, including notifications and appropriate actions. Using PS4 Slim as an OSSEC platform contributes to sustainable and energy-efficient use of resources in network security monitoring.

In the context of increasingly complex cybersecurity, this research provides valuable insight into the potential use of entertainment devices converted into web servers as efficient and effective security monitoring tools. The results of this research can be used as a basis for

developing more innovative approaches to maintaining system and network security in the future.

Acknowledgements

Financial support for this study was provided by Politeknik Negeri Padang and I am deeply appreciative of their commitment to advancing scientific knowledge. Lastly, I want to acknowledge the unwavering support of my family and friends. Their belief in me sustained me throughout this journey.

References

[1] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, Jan. 2021, doi: 10.1002/ett.4150.

[2] A. O. Alzahrani and M. J. F. Alenazi, "Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks," *Futur. Internet*, vol. 13, no. 5, p. 111, Apr. 2021, doi: 10.3390/fi13050111.

[3] S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *J. Big Data*, vol. 7, no. 1, p. 105, Dec. 2020, doi: 10.1186/s40537-020-00379-6.

[4] D. Teixeira, L. Assunção, T. Pereira, S. Malta, and P. Pinto, "OSSEC IDS Extension to Improve Log Analysis and Override False Positive or Negative Detections," *J. Sens. Actuator Networks*, vol. 8, no. 3, p. 46, Sep. 2019, doi: 10.3390/jsan8030046.

[5] Ronal Hadi, Y. Yuliana, and H. A. Mooduto, "Deteksi Ancaman Keamanan Pada Server dan Jaringan Menggunakan OSSEC," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 3, no. 1, pp. 8–15, 2022, doi: 10.30630/jitsi.3.1.58.

[6] Y. Reynaldo, A. Triayudi, and S. Ningsih, "Analisis Faktor yang Mempengaruhi Gamers PC dan Konsol Beralih ke Game Mobile menggunakan Metode K-Means Clustering," *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 6, no. 1, pp. 42–48, Jan. 2022, doi: 10.35870/jtik.v6i1.383.

[7] M. D. Hossain, H. Ochiai, F. Doudou, and Y. Kadobayashi, "SSH and FTP brute-force Attacks Detection in Computer Networks: LSTM and Machine Learning Approaches," in *2020 5th International Conference on Computer and Communication Systems (ICCCS)*, IEEE, May 2020, pp. 491–497. doi: 10.1109/ICCCS49078.2020.9118459.

[8] D. Essaadi, J. Laassiri, and S. Hanaoui, "Using NMAP for Data Collection in Cloud Platform," 2020, pp. 507–517. doi: 10.1007/978-3-030-36674-2_51.

[9] F. Mohammed, N. A. A. Rahman, Y. Yusof, and J. Juremi, "Automated Nmap Toolkit," in *2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC)*, IEEE, Nov. 2022, pp. 1–7. doi: 10.1109/ASSIC55218.2022.10088375.

[10] M. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, and Ata-ur-rehman, "Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool," in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, IEEE, Jan. 2019, pp. 1–6. doi:

10.1109/ICOMET.2019.8673520.
[11] G. Bagyalakshmi *et al.*, “Network Vulnerability Analysis on Brain Signal/Image Databases Using Nmap and Wireshark Tools,” *IEEE Access*, vol. 6, pp. 57144–57151, 2018, doi: 10.1109/ACCESS.2018.2872775.
[12] E. Crespo-Martinez, “Análisis de vulnerabilidades con SQLMAP aplicada a entornos APEX 5,” *Ingenius*, no. 25, pp. 104–113, Dec. 2020, doi: 10.17163/ings.n25.2021.10.
[13] O. Ojagbule, H. Wimmer, and R. J. Haddad, “Vulnerability Analysis of Content Management Systems to SQL Injection Using SQLMAP,” in *SoutheastCon 2018*, IEEE, Apr. 2018, pp. 1–7. doi: 10.1109/SECON.2018.8479130.