Journal of Applied Engineering and Technological Science
Vol xx(x) 201x : xx-xx

IMPLEMENTATION OF IDS (INTRUSION DETECTION SYSTEM) DI DIRECTORATE INNOVATION AND BUSINESS INCUBATOR USING PORTSENTRY

Rahmat Novrianda Dasmen[1], Apriyani Abdul[2], Rasmila[3]
Computer Engineering,Vocational Faculty, University Bina Darma [1,2]
rahmatnovrianda@binadarma.ac.id[1],abdulapriyani717@gmail.com[2],rasmila@binadarma.ac.id[3]

**Coresponding Author*

ABSTRACT
At the Directorate of Innovation and Business Incubators (DIIB) in website security and storage for storing important data or files. DIIB does not yet have an identification system to detect attacks from outside. Therefore, the DIIB system is vulnerable to attacks and suspicious activity, one of which is in the form of website pages that suddenly change when opened, as well as the appearance of annoying advertisements and changes to the overall appearance of the website. So with the above problems the researchers tried to find a solution, namely "Implementing an IDS (Intrusion Detection System) Using Portsentry". For its implementation, researchers used the Action Research Method as a reference in testing the existence of attacks and suspicious activity on the DIIB Website and Storage as well as testing the success of using portsentry as a system that blocks attacks. From this research it is known that portsentry works very well where in its detection it directly blocks and detects attacks or suspicious activity.

Keywords: Intrusion Detection System,Portsentry, DIIB, Serangan,website

1. Introduction

The Directorate of Innovation and Business Incubator (DIIB) is a unit that has a website and storage as a place to store important data or files, but at DIIB the website does not yet have an identification system for suspicious activity or attacks from outside. Therefore, the absence of an identification system at DIIB cannot detect attacks from outside or suspicious activity. One of the attacks that occurred was a website page that suddenly changed when opened, as well as the appearance of annoying advertisements that changed the appearance of the website as a whole (Anif et al., 2015).

Because of the problems above, researchers are trying to find a solution by implementing an Intrusion Detection System (IDS) as a system that monitors network traffic to detect suspicious activity or unauthorized access using Portsentry. The first thing that must be done in implementing IDS is to install Ubuntu first before using Portsentry as a tool used to avoid various scanning activities and detect port scanning and actively respond to attacks from outside. After IDS successfully run using Portsentry and suspicious activity is found, the system will provide a report in the form of a warning. In this case, Portsentry will actively block the hacker's IP or server automatically. The aim is to ensure that the DIIB website is safe from access by unauthorized parties (Fauzi et al., 2023a)

In addition to being available for various Unix platforms, such as Linux, OpenBSD, and FreeBSD, PortSentry version 2.0 offers many capabilities for detecting scans on a variety of Unix machines. Version 1.1 supports PortSentry classic detection mode, which is no longer used in version 2.0. To run PortSentry 2.0, the libpcap library is required, which is usually available in RPM format and can be installed on Unix. installed automatically if using Linux Mandrake. And here the researcher chose to use Portsentry from the Ubuntu Linux OS because it is easier to run (Muh Mashuri Mustofa, 2013) Portsentry is an Intrusion Detection System (IDS) that is created by installing Ubuntu first and configuring Portsentry after successful installation. The advantage of using Portsentry as the main feature in detecting and responding to external attacks is that Portsentry can detect various attacks scanning, Reacts to external port scan attacks by stopping attacks from scanners and systems in real time, reporting all threats and breaches, and

remembering the attacker's IP address in case of an accidental port scan attack. And portsentry is designed to be easy to configure and free from maintenance (Ulfa et al.2012).

Based on the description above regarding website security issues and storage as data storage and important files in the Directorate of Innovation and Business Incubator (DIIB) unit, especially web servers which are often accessed carelessly, such as website infiltration.Security of storage data stored via the web. For this reason, researchers apply IDS using Portsentry to monitor attacks or suspicious activities. Therefore, the researcher took the title "Implementation of IDS (Intrusion Detection System) in the Directorate of Innovation and Business Incubator Using Portsentry"

2. Literature Review

a. Laptop Asus E410MA

This laptop is used as an Ubuntu server running PortSentry which works to detect and also block attacks or suspicious activity through network ports.

b. Asus AMD 3 3200U laptop with radeon vega mobile Gfx 2.60 GHz.

This laptop was used as a test attack in which the attack was a Ping death attack, which is a type of attack on a computer system.

C. Portsentry

Portsentry is an IDS designed to detect and actively respond to suspicious activities or external attacks carried out by irresponsible people. Where, if a suspicious attack is detected, the Portsentry IDS will immediately block the IP that is considered suspicious. The image above is what Portsentry will look like if the tool is successfully installed.

3. Research Methods

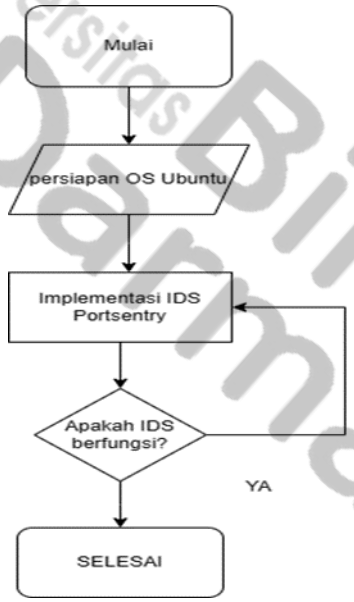
In this research, researchers used the Action Research method which is a method that explains, describes a problem context or situation together with an intervention process aimed at development. The Action Research method is a research design, covering things that the researcher will do starting from making a diagnosis to final analysis, data which is then concluded and suggestions are given.

Ping 1.1 research Methods Penelitian *Action Research* (Novrianda, Rasmila.2019)

A. Diagnosis

At this stage, the research will carry out a diagnosis regarding problems on the website and storage through the security network at the Directorate of Innovation and Business Incubators (DIIB). The more technology develops, the more attacks or suspicious activities occur from irresponsible parties, causing websites to sometimes experience sudden errors, even storage.

Storage of important data files was also attacked. To prevent another attack, researchers are trying to find a solution by making IDS a security system that is able to detect and provide reports in the form of warnings assisted by tools as a tool to block and scan the attacker's IP address or forcibly blacklist it. Apart from that, the advantage of the function of portsentry is that when it detects a scan, the system will automatically disappear from the attacker's presence so that the attacker cannot do anything, portsentry always remembers the attacker's IP address and if there is a suspicious port scanning attack call, portentry will react automatically. direct. as storage of important data files was also attacked. To prevent another attack, researchers are trying to find a solution by making IDS a security system that is able to detect and provide reports in the form of warnings assisted by tools as a tool to block and scan the attacker's IP address or forcibly blacklist it. Apart from that, the advantage of the function of portsentry is that when it detects a scan, the system will automatically disappear from the attacker's presence so that the attacker cannot do anything, portsentry always remembers the attacker's IP address and if there is a suspicious port scanning attack call, portentry will react automatically. direct.



`Figure 2. 11 Flowchart of testing techniques

Based on the flowchart above, the following is an explanation of each stage in planning the implementation of IDS using Portsentry:

The first preparation to be able to implement IDS on a server is by installing Ubuntu OS version 20.04 on a virtual box. Ubuntu is a Linux OS based on Debian and distributed as software (Open Source), a software that is easy to use for users. any user.The second preparation to do is to implement Portsentry by installing it first in Virtual Box. Portsentry is an IDS-based tool that works as a detector of attacks or activities that are considered disturbing and suspicious. For this reason, configuring portsentry can block attacks and suspicious activity on frequently accessed websites. The implementation of IDS Portsentry functions quite well in blocking and detecting attacks from outside. where UDP, which is an internet protocol that functions to send messages to other computers on a network without initial communication, can be blocked by Portsentry.
IDS Portsentry actively detects the DIIB Website from attacks or suspicious activity where there are annoying advertisements and pages that change suddenly. Portsentry has succeeded in detecting attacks or activities via the IP Address that you want to detect and monitor for attacks Portsentry also works very well if an attack is discovered, directl IDS Portsentry will forcibly block the attacker's IP on the blacklist so that the attacker is unable to access the website again

Table 2.10 Table of detected attacks

NO	Jenis Serangan	Keterangan
1	PING OF DEATH	Penyerang
2	NMAP	Pendeteksi

The table above shows that there are two attacks that were successfully blocked by IDS Portsentry, namely Ping of Death and Nmap which can be effectively blocked and detected attacks or suspicious activity using IDS. Ping of death is an attack on a system that uses a ping in the form of a denial of service (DoS) or malicious freeze to the computer. Nmap is a network scanning that works to find hosts and services by sending packets and
analyzing the response (Maryati & Information, n.d.).

4. Results and Discussions

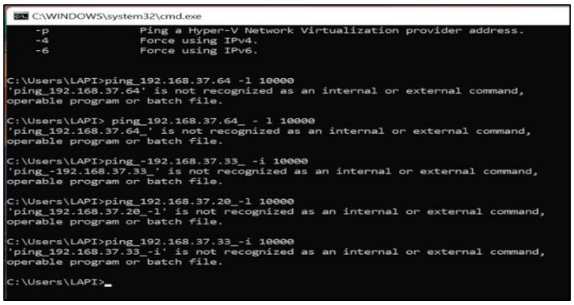
Results and Discussion is a section that contains all scientific findings obtained as research data. This section is expected to provide a scientific explanation that can logically explain the reason for obtaining those results that are clearly described, complete, detailed, integrated, systematic, and continuous.

The discussion of the research results obtained can be presented in the form of theoretical description, both qualitatively and quantitatively. In practice, this section can be used to compare the results of the research obtained in the current research on the results of the research reported by previous researchers referred to in this study. Scientifically, the results of research obtained in the study may be new findings or improvements, affirmations, or rejection of a scientific phenomenon from previous researchers.

5. Conclusion

Ping of Death Attack Test Results

At this stage it is based on researchwhich was carried out by researchers in testing a ping of death attack on the Website IP, by entering a data packet of 1000 bytes on the server 192.168.37.64. Testing this system produces portsentry detection which identifies scanning instructions for attacks or external activity. Ping death attacks only on the basis of testing the IP address that you want to attack via Windowns cmd



.

Figure 3.7. Ping Attack Configuration
of Death

To detect whether or not there are attacks or suspicious activities from the Directorate of Innovation and Business Incubation (DIIB) website, it is necessary to check the IP address, where to find out the IP, researchers must enter the domain hostname on the Nslookup.id IP address search site. Test results from portsentry and NMAP where there was an attack that was successfully detected so, in this case the researchers blocked and prevented the attack from accessing and created the IP of the attacker who was trying to carry out suspicious activity on the blacklist of the web server. So this made the attacker unable to access anything . In the first test, Portsentry succeeded in detecting the attack well and performed better. In
The second test portsentry experienced an error due to the laptop system suddenly losing its network. In the third trial, try to reconfigure by repeating the commands. In the fourth trial, portsentry was successfully detected, but for the web server-based one it could not be done and continued to experience errors even though the IP, gateway and Nermask had been repeatedly entered. Therefore, researchers are trying again to carry out trials to achieve this success until researchers are able and successful in getting better results in preventing and blocking these attacks so that they are more effective and no unnecessary access is detected. Portsentry IDS will actively block the attacker's access point so that the attack can be prevented. Portsentry is a type of host-only IDS or commonly known as HIDS. Portsentry cannot monitor all ports on the target system because it only monitors ports that are directly connected to the Internet. The iptables configuration that can be done is to make all data point to the client as the target and the target IP address will be directed to the server via a port or gateway (transparent proxy) before routing. So that it can be monitored to reduce incidents. attacks attempt to exploit system or common DNATs in iptables rules. In this research, Portsentry and nmap succeeded in detecting attacks and activity via iptables where when scanning was carried out an attack was detected which resulted in Portsentry being active and automatically blocking the attack. The implementation of this IDS aims to overcome various problems related to

Discussion

Based on the test results using the learning method, it will explain the recap of the results of the tests that have been carried out where the results of the tests are stated in the form of a description. The following are the results of the tests that have been carried out.
In the first test, the researchers succeeded in running Portsentry by testing attacks on the DIIB website and storage where in the attack Portsentry blocked attacks and activities directly. It has been proven that portsentry is able to detect attacks or unauthorized access via the IP Address that has been obtained. Forcibly portsentry will immediately blacklist IPs that have unauthorized access, making it impossible for attackers to do anything.
In the second test using Nmap scanning all ports detected by Porsentry the IP address will be entered into the host.deny file where TCP Wrapper based on the host deny file will block iptabless, making it impossible for attackers to communicate with the website server. Successfully protects by blocking attacks and suspicious activity from attacks trying to access and detecting attackk or suspicious activity. The Ping Death attack test which was carried out 3 times can be carried out via CMD Windows on the Asus Radeon laptop. In this first experiment, the researcher succeeded in detecting the attack carried out by Ping of Death. The second attempt, Portsentry was unable to detect the attack due to an error. The third attempt was Portsentry. successfully detected and blocked it. The attacks planned to attack the DIIB website are as follows:
It can be seen that there are two attacks that have been successfully blocked by Portsentry and can be detected in the form of warning reports so that the IP can be protected from attacks or suspicious activity. So with this DIIB can have an identification system that can protect the Website and Storage from attacks or suspicious activity so that access that is deemed suspicious can be immediately blocked

References

[1] Anif, M., Hws, S., & Huri, D. (2015). Implementation of the Intrusion Detection System (IDS) with the Port Scanning Detection method on Computer Networks at the Semarang State Polytechnic. In TELE JOURNAL (Vol. 13).
[2] Asmah Akhriana, & Andi Irmayana. (2019). 296434-web-app-net-attack-type-detector-9bb3e03e.
[3] Fauzi, R., Muhyidin, Y., & Singasatia, D. (2023a). Computer Network Security System Based on Intrusion Detection System (IDS) Techniques to Detect Distributed Denial of Service (DDOS) Attacks. In Journal of Computer Science & Informatics (J-SAKTI (Vol. 7, Issue 1).
[4] Fauzi, R., Muhyidin, Y., & Singasatia, D. (2023b). Computer Network Security System Based on Intrusion Detection System (IDS) Techniques to Detect Distributed Denial of Service (DDOS) Attacks. In Journal of Computer Science & Informatics (J-SAKTI (Vol. 7, Issue 1).
[5] Firdaus, B. P., & Informatics, T. (2020). Implementation of Network Security Intrusion Detection/Prevention System Using Pfsense I Made Suartana.
[6] Ilham, K. F., Alwi, E. I., & Fattah, F. (2023). Implementation and Analysis of Network Security Snort Using Intrusion Detection System in UDP Flood Attacks. In Informatics Journal (Vol. 8, Issue 1).
[7] Maryati, Y., & Information, T. (2023). Computer Network Security Analysis with the Application of Firewall Technology and Intrusion Detection System (IDS) (Vol. 3, Issue 5).
[8] Muh Mashuri Mustofa, E. A. (2013). 211211-implementation-of-honeypot-and-i-security-system.
[9] Ulfa, M., University, D., Darma, B., Jenderal, J., Yani, A., & 12, N. (2012). Implementation of an Intrusion Detection System (IDS) …… (Maria Ulfa).
[11] Utami, E., & Information, T. (2023). Computer Network Security Analysis Using Intrusion Detection System (IDS) Techniques in Corporate Environments (Vol. 3, Issue 6).963
[12] Wijaya, B., & Pratama, A. (2020). Intrusion Detection on Servers Using the Snort-Based Intrusion Detection System (IDS) Method. Information Systems and Computers), 09, 97–101. https://doi.org/10.32736/sisfokom.v9.i1.770