Implementation of Web Server Security Against Denial of Service (DoS) Attacks

Mohammad Idhom¹, Ronggo Alit², Akhmad Fauzi³

¹,² Department of Informatics Engineering, University of Pembangunan Nasional “Veteran” Jawa Timur, Jalan Raya Rungkut Madya, Surabaya, Indonesia
³ Department Management, Faculty of Economics and University of Pembangunan Nasional “Veteran”

¹ idhom@upnjatim.ac.id
² ronggo.if@upnjatim.ac.id
³ akhmadfauzi@upnjatim.ac.id

Abstract. Denial of Service (DoS) is one of the top cyber-attacks that grows exponentially attacking every company, agency, and organization with a percentage of 43%. This type of attack has the most damage to business operations and affects globally. By flooding the bandwidth or resources of a machine or system, attackers deny it so that legitimate users cannot access the service. The objectives of this study are: 1. Creating a security system on a web server against Denial of Service (DoS) attacks that are applied to containerization architecture. 2. Implementation of load balancing methods for securing the web server from Denial of Service (DoS) attacks. 3. Implementing the deployment process and monitoring the web server in the containerization architecture. The results of comparisons and testing of services carried out with denial of service attacks prove that the memory load used by a web server with containerization architecture is less than that of conventional web servers. Testing was also carried out on hardware performance, namely CPU. Conventional web servers are heavier by up to touching 0.00015% compared to web servers with the highest containerization architecture, only touching 0.00010%.

Keywords: network security, DoS attack, web server, containerization

1. Introduction

Web servers are becoming an important part of today's internet infrastructure. Most of the web server architectures in use today, aim to improve web server performance by using only a single backend web server. The problem that arises is how a single backend web server is able to handle large spikes in data requests. That is why building a reliable and highly available web server infrastructure is so important. A single web server is not sufficient to support high traffic web applications so one should consider using web server clustering to increase the reliability and availability of web servers [1]. Denial of Service (DoS) is one of the top cyber attacks that grows exponentially attacking every company, agency, and organization with a percentage of 43%. This type of attack has the most damage to business operations and affects globally. By flooding the bandwidth or resources of a machine or system, the attacker denies it so that legitimate users cannot access the service [2]. Prevention that can be done to prevent Denial of Service (DoS) attacks is to build a network and server
architecture that implements the method of distributing data flows and resources at the nodes so that there is no downtime on the server, which can be done by implementing a data distribution system on the nodes [3]. The data distribution system is Load balancing. Load Balancing functions to reassign all loads to different nodes of the collaborative system to make resource utilization more effective and to increase more efficient job response times, while eliminating a condition where multiple nodes experience overload. loaded while others are under loaded. By applying this technique, all access loads can be applied to all nodes equally [4]. There is another problem, namely when implementing there are usually problems where the system is run and tested on too many physical servers then if there is damage it will cause cost losses, troubleshooting that is too complicated, use of too much power, and device requirements. more physical [5]. Based on this efficiency, containerization or container architecture is adopted to implement the development of network and system architectures. This technology is not a new technology, because many companies and IT organizations have adopted it. [6]. Containerization is a virtualization technology that has advantages over virtual machines: it boots faster, has less performance overhead, and uses fewer resources. By utilizing this technology for collaborative deployment of web applications and web servers, it is possible to run the system without having to spend a lot of money in procuring physical components and can better facilitate the process of building, testing, low-level system maintenance, and server consolidation. Based on the explanation above, the writer takes the title of the thesis "Web Server Security System with Containerization Architecture Against Denial Of Service Attacks" with the intention of building a security system on a web server against Denial of Service (DoS) attacks, with the security method used, namely Load Balancing with implementation. using a containerization or container architecture.

2. Literature Review

This study there will be several definitions that can be used as a data dictionary in the implementation of Web Server Security Against Denial of Service (Dos) attacks.

2.1 Denial of Service (DoS)
A denial of service (DoS) attack is a type of cyber attack in which a malicious actor aims to make a computer or other device unavailable to the intended user by interfering with the normal functioning of the device. DoS attacks typically function by inundating targeted machines with requests until normal traffic cannot be processed, resulting in denial of service for additional users. A DoS attack is characterized by using one computer to launch the attack[7]

2.2 Web Server
A web server is the computer that runs websites. A web server is a computer program that distributes web pages when a request is made. The basic purpose of a web server is to store, process and deliver web pages to users. Communication between this is carried out using the Hypertext Transfer Protocol (HTTP) [8]. The Web Server has a role in processing various data requested by the web browser and then results or answers in the form of documents, videos, photos, or various file forms. other. The web server can function as both hardware and software, that is, if it is hardware, the web server will play a role in storing data in various forms including JavaScript, CSS, HTML, images, documents, photos and videos. Another thing, if the web server functions as software, it will play a role in managing and processing all request activities that are received and read on browser pages.

2.3 Containerization
Containerization itself is an approach where running multiple instances (containers) on the same Operating System (OS), where the containers will have a shared kernel. Similar to a VM, where on one host OS can run various other applications isolated from the host. The main difference between virtualization and containerization is that virtualization turns on the OS inside the OS, so that in terms of resources and performance it will be heavier than containerization which isolates each application into a virtual environment with the host's shared kernel. But that doesn't mean virtualization is a bad technology, in fact the two technologies serve slightly different purposes. If you want to have an
environment that is very isolated from each other, you should use a VM. If you don't need 100% isolation then containerization can be a consideration[9]

2.4 Docker
Docker is a container-based service that excels in development, delivery, and can run anywhere. The main idea of Docker is so that developers can easily build applications, store them in containers and finally can be distributed and used everywhere. By leveraging the Docker methodology for delivering, testing and deploying code, developers can significantly reduce the delay between writing code and running it in production. Docker is licensed under the Apache 2.0 open source license. In Docker, the concept of designing and implementing load balancing uses the least connection and round robin algorithms in Docker to analyze server performance against client connections. [10][11]

3. Methodology
The research design is in the form of a framework design that will be carried out during the research period of the final project. This design is a basic guideline for creating a web server security system with a containerization architecture against denial of service attacks

Design In this final project research, the author will explain the design and flow design of a web server security system using containerization architecture against denial of service attacks. The network topology used to build a web server security system is as follows: The topology design is used to build a security system, the topology has a flow where the attacker or attacker sends Denial of Service attacks through the cloud network to the server then passes the load balancer whose job is to share the incoming data load to 2 servers or nodes so as not to overload. The two servers or nodes are connected using the docker swarm, while the load balancer with the nodes is linked in the docker containerization. After the topology is formed, the container design in the load balancer can be designed, the load balancer architectural design will be used as follows:
Figure 3. Container architecture in a Load Balancer

Figure 4. Containerization architecture nodes

Containerization Architecture Figure 4 Containerization architecture is created on a web server which consists of several containers with different functions, from deployment, monitoring, to notification. The architectural design is as follows: The notification system here is useful for sending reports or warnings in the event of an attack that threatens the stability of the server. Notifications sent via email are sent by alert manager which is obtained from the operating system and container matrix processing.

| Table 1. Denial of Service Test Parameters |
|-------------------------------------------|
| Jenis Denial of Service | Parameter | Number of packages | Duration of the Attack |
|-------------------------|-----------|--------------------|-----------------------|
| UDP Flood               | UDP       | 80000              | 1 Minute              |
| DDOS                    | SYN       | 100000             | 1 Minute              |
| ICMP Flood              | ICMP      | 50000              | 1 Minute              |

Table 1 shows the attack to be used for testing, the attack is divided into 3, namely the UDP Flood which sends 80000 packets, DDOS which sends 100 000 SYN packets, and the ICMP Flood which sends 50000 packets, all carried out within 1 minute.

4. Results and Discussions
This stage will explain the results of creating a web server security system with a containerization architecture, the system created is tested using 3 types of attacks, namely UDP Flood, ICMP Flood and DDOS (Distributed Denial of Service). This type of attack attacks by sending syn packets up to 100 000 packets within 1 minute which is used to test system services that include the CPU and memory.
In this section, graphical analysis is carried out related to the results of previous tests, here is a comparison of the results of using conventional web server architectures and using containerization architectures.

1. **Memory Usage**
   In this section, we compare memory usage between conventional web server systems and containerization.

   ![Figure 7. Conventional web server memory load](image1)
   ![Figure 8. Web server load containerization](image2)

   It can be seen in comparison to Figure 4 that memory usage is higher to reach 24 Mib due to memory load when access is not shared with other servers, in contrast to Figure 5, memory usage tends to be more stable only up to 19 Mib.

2. **Processor load**
   This section analyzes the load processed by the processor between conventional web server systems and containerization.

   ![Figure 9. Processor web server conventional](image3)
   ![Figure 10. Processor web server containerization](image4)

   It can be seen that the comparison between Figure 8 and Figure 9 shows that the load increase in conventional web server processors is higher and the jump looks more drastic than a web server with a more stable containerization architecture.

3. **Notification sent via email.**
   After seeing the comparison graph between a conventional web server and a web server with a containerization architecture, then we will see the success of the attack notification sent via email.
5. Conclusion

Conclusions that can be drawn from research related to the Implementation of Web Server Security Against Denial of Service (Dos) Attacks The results of comparisons and testing of services carried out with denial of service attacks prove that the memory load used by a web server with containerization architecture is less than that of conventional web servers. Testing was also carried out on hardware performance, namely CPU. Conventional web servers are heavier by up to touching 0.00015% compared to web servers with the highest containerization architecture, only touching 0.00010%. The processor load also proves that the processor load on conventional web servers is heavier than web servers with containerization architecture.

6. References
[1] Moniruzzaman, A. B. (2014). A High Availability Clusters Model Combined with Load Balancing and Shared Storage Technologies for Web Servers. International Journal of Grid Distribution Computing.
[2] Sanders, J. (2019, July 24). 83% have experienced a DDoS attack in the past two years, survey finds. Retrieved from Techrepublic: https://www.techrepublic.com/article/83-have-experienced-a-ddos-attack-in-the-past-two-years-survey-finds/
[3] Kaur, S., & Sharma, T. (2018). Efficient load balancing using improved central load balancing technique. 2018 2nd International Conference on Inventive Systems and Control (ICISC).
[4] Anselmi, J. (2020). Combining Size-Based Load Balancing with Round-Robin for Scalable Low Latency. IEEE Transactions on Parallel and Distributed Systems.
[5] Wang, S., Zhu, L., & Cheng, M. (2019). Docker-based Web Server Instructional System. 2019 IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS).
[6] Evans, A. (2018, December 19). What is Containerization and why is it important for your business? Retrieved from Hexnode: https://www.hexnode.com/blogs/what-is-containerization-and-why-is-it-important-for-your-business/
[7] Chelladhurai, J., Chelliah, P. R., & Kumar, S. A. (2016). Securing Docker Containers from Denial of Service (DoS) Attacks. 2016 IEEE International Conference on Services Computing (SCC).
[8] Kresna, I., & Rosmansyah, Y. (2018). Web Server Farm Design Using Personal Computer (PC) Desktop. 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE).
[9] Pathiratna, P., Ayesha, V., Imihira, W., & Wasala, W. (2017). Security testing as a service with docker containerization. 2017 Seventeenth International Conference on Advances in ICT for Emerging Regions (ICTer).
[10] Docker Documentation Team. (2018). Retrieved from Docs Docker Documentation: https://docs.docker.com/
[11] Afis, D. S., Data, M., & Yahya, W. (2019). Load Balancing Server Web Berdasarkan Jumlah Koneksi Klien Pada Docker Swarm. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer.