Research Exhibition in Mathematics and Computer Sciences (REMACS 6.0)/
ISBN: 978-629-97440-5-4

ANALYSIS OF ENTERPRISE NETWORK BY APPLYING MULTILAYER DEFENSE TOWARDS DOS ATTACK ON A SIMULATED NETWORK

Anis Afiqah Ahmad Fuzi, Abidah Haji Mat Taib and Hafizah Hajimia
College of Computing, Informatics and Mathematics,
Universiti Teknologi MARA, Perlis Branch
anisnsaa3@gmail.com, abidah@uitm.edu.my and hafizah.hajimia@uitm.edu.my

ABSTRACT- Due to the complexity of networking infrastructures, designing a corporate network security solution is a significant challenge. This study focuses on analyzing the efficiency of multilayer defense systems in reducing DoS assaults on corporate networks. The research was carried out by simulating a network environment with GNS3. The study intends to construct and install a simulated corporate network using GNS3, which closely resembles real-world network architecture. It then analyzes the enterprise network without having any defense configured and another one with multiple defenses deployed including firewalls, intrusion detection systems (IDS), and traffic shaping rules. Vital network performance parameters such as throughput, packet loss, and reaction time were continually monitored and analyzed throughout various assault scenarios to assess the impact of the defense measures on network operations. Finally, the findings were thoroughly examined in order to establish the efficacy of the multilayer defense mechanisms, allowing for a comparative comparison of their performance across various DoS assault scenarios.

Keywords: Enterprise Network, Multilayer Defense, GNS3, Network Performance, Snort

1. INTRODUCTION

The study aims to analyze the efficiency of the enterprise network under the DoS attack where multilayer defense were applied. The study also looked at the trade-offs between security measures and network performance parameters including throughput, latency, and resource utilization. This research is to examines the impact of various Denial of Service (DoS) attack scenarios on the enterprise network, taking into account different attack types which are SYN-Flood and ICMP Attack, traffic levels, and attack paths. GaO (2019) works on the research of the DoS attack using IDPS which shows that using only one defense is not enough in defending the network for a long time. This indicates that using more than one defense is necessary in order to tighten the security of the network. Therefore, in this study, applying the multilayer defense in the enterprise network towards DoS attack were analyzed.

2. METHODOLOGY

An experiment testbed was set up using GNS3((Wikipedia Contributors, 2022) to represent an enterprise network as shown figure 1. Three attack scenarios were conducted to represent the enterprise network under attacks without any defense, the enterprise network with one defense and the other one with more than one defense which will be measuring the packet drops, time and the throughput. The results gained from the simulation are then analyzed in order to measure the security performance.

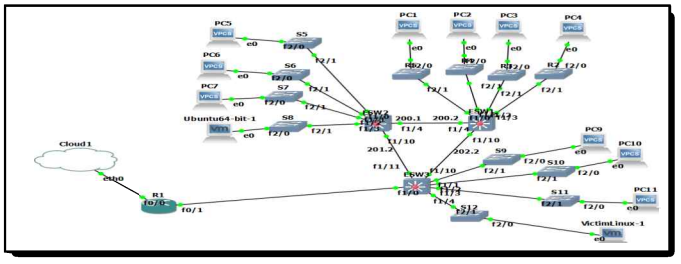

Figure 1. Enterprise Network

3. RESULTS AND DISCUSSION

The network performance is measured through the packet drop, throughput and traffic analyzation when the network was under ICMP and SYN-flooding attacks (see Figures 2 and 3). In Figure 2, the throughput shows the average numbered of 116 which indicates some traffics were still passed through, despite the network was under DoS attacks. It should be noted, however, that this figure is lower than the average throughput during normal network operation, suggesting a potential decline in network performance. Other than that, the average amount of packet drop during the assault was 162 which is quite a concern as it can result in delays, retransmissions, or complete loss of data, leading to disruptions in network communication. However, under the DoS assaults with the multilayer defense, there were no packet drops which means the defense was working out properly. Overall, the results of the analysis indicate that multilayer defense on the corporate network has optimal performance as the packet drops decreased, the CPU performs more efficiently and the throughput increases.

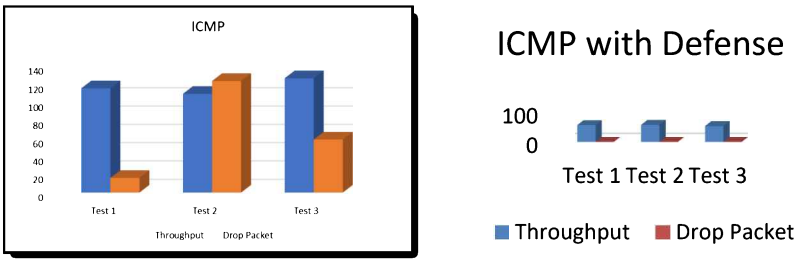

Figure 2. Analysis of Enterprise Network with and without defense (ICMP Attack)

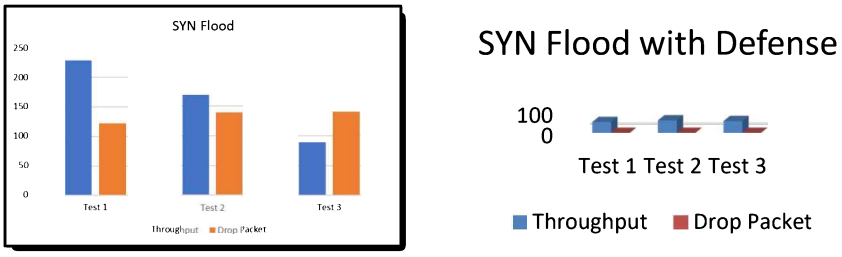

Figure 3. Analysis of Enterprise Network with and without defense (SYN-Flood Attack)

4. CONCLUSION

Enterprise network needs to tighten the security by applying multilayer defense as highlighted in this work. The network performance and reliability will be the key measures of keeping the corporate network on the highest level of performance. Besides, this study also demonstrates that enterprise network can utilize GNS3 to create an isolated network for analyzing the network under testing and also inhouse training of the network or security personnel.

REFERENCES

Gao, J., Chai, S., Zhang, B., & Xia, Y. (2019). Research about DoS Attack against ICPS. 19(7), 1542–1542. https://doi.org/10.3390/s19071542

Bogdan Korniyenko, Galata, L., & Lesya Ladieva. (2019). Research of Information Protection System of Corporate Network Based on GNS3. https://doi.org/10.1109/atit49449.2019.9030472

Wikipedia Contributors. (2022, September 29). Graphical Network Simulator-3. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Graphical_Network_Simulator-3