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

DOS ATTACKS DETECTION USING SNORT IN VIRTUALIZED ENVIRONMENT BY USING GNS3

Nurfatihah Yusharizal dan Abidah Haji Mat Taib
College of Computing, Informatics and Mathematics,
Universiti Teknologi MARA, Perlis Branch
2020489768@uitm.edu.my dan abidah@uitm.edu.my

ABSTRACT - This project focuses on the detection of Denial of Service (DoS) attacks using Snort, an open-source intrusion detection system, within a virtualized environment created using GNS3, a network simulation platform. The primary objective is to set up an isolated network that simulates DoS attacks on Linux and Windows hosts, allowing for the analysis of host behavior under these attacks. This is achieved by consuming a stream of request records from multiple servers using an Intrusion Detection System (IDS). The project also aims to demonstrate the network behavior under DoS attacks with and without security measures in place. Through the implementation of Snort, GNS3, and Wireshark, the project evaluates the effectiveness of these tools in detecting and mitigating DoS attacks, while also monitoring performance metrics such as connectivity tests, CPU usage of the victim, and throughput and packet drop rates. The outcomes of this project contribute to enhancing network security and provide valuable insights into the detection and evaluation of DoS attacks in a virtualized network environment.

Keywords: DoS attacks, Snort, GNS3, Wireshark, Virtualized environment

1. INTRODUCTION

This research aims to set up an isolated network using GNS3 to simulate DoS attacks on Linux and Windows hosts. The project involves analyzing the behavior of the hosts under DoS attacks by using an IDS and a stream of request records from multiple servers. It also includes analyzing host behavior with and without security measures, demonstrating network behavior, and monitoring performance during DoS attacks. The project scope includes the use of three PCs, implementation of Hping3, Snort, and Wireshark, and the deployment of a firewall for prevention. By enhancing the security of personal computers through the implementation of an IDS, this project contributes to the understanding and mitigation of DoS attacks in a virtualized network environment.

2. METHODOLOGY

An isolated network was set up using GNS3, and three PCs were configured to simulate various roles, including attacker and victims. The project utilized Hping3 as the attacking tool, Snort as the Intrusion Detection System (IDS), and Wireshark to analyze and monitor network behavior across different operating systems for Windows and Ubuntu. Furthermore, the deployment of a firewall for prevention was discussed. Consequently, the testbed was successfully established and is now ready for use.

3. RESULTS AND DISCUSSION

The experimental results can be divided into two scenarios. The first scenario evaluates the performance of the Snort IDS in Windows and Ubuntu operating systems during TCP DoS attack without any additional defense mechanisms. The second scenario evaluates the performance of the Snort IDS in Windows and Ubuntu operating systems during UDP DoS attack without any additional defense mechanisms. The third scenario assesses the performance of the Snort IDS in Windows and Ubuntu with the presence of a firewall as a defense mechanism. The Wireshark results show the captured network traffic before and during the DoS attacks. The performance analysis of Snort focuses on throughput and dropped packet rates for TCP and UDP flooding attacks, comparing the performance between Windows and Ubuntu. As shown in Figure 1, Snort performs better under a TCP DoS attack in Ubuntu compared to Windows, achieving a higher packet capture rate per second, and Ubuntu exhibits a smaller drop packet rate compared to Windows. On the other hand, as depicted in Figure 2, Snort performs better under a UDP DoS attack in Windows, exhibiting a higher packet capture rate per second, and a lower number of dropped packets compared to Ubuntu. The findings demonstrate the effectiveness of Snort in different operating systems.

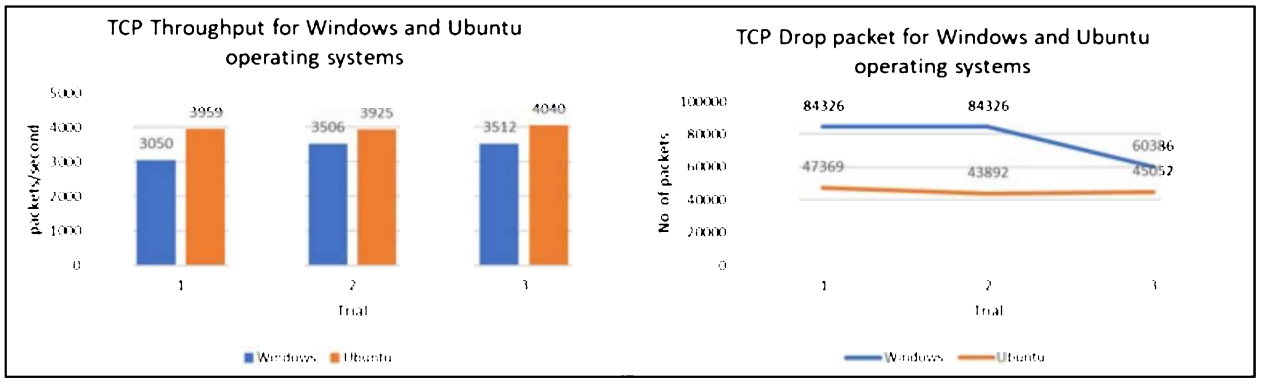

Figure 1. Throughput and Drop packet for TCP for both Windows and Ubuntu operating systems

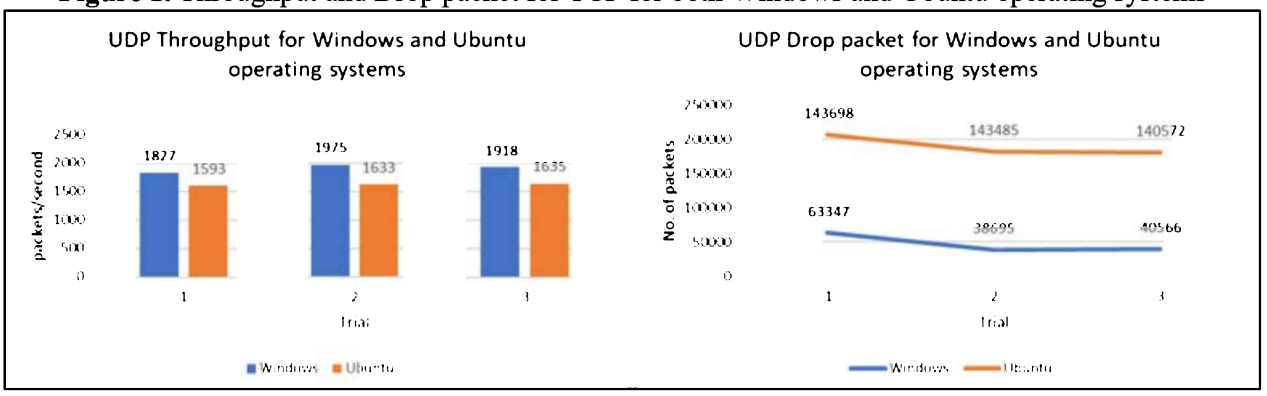

Figure 2. Throughput and Drop packet for UDP for both Windows and Ubuntu operating systems

In the third scenario, after implementing the firewall, no throughput and packets were dropped for Windows indicated that no attacks successfully penetrated the network. The packet drops and throughput for Ubuntu were lower, suggesting that the firewall successfully acted as a defense mechanism.

4. CONCLUSION

The conclusion section summarizes the key findings of the research. It reiterates the objective of the project to set up an isolated network for simulating DoS attacks and analyzing host behavior. The conclusion emphasizes the importance of implementing an IDS, analyzing network behavior, and monitoring performance during DoS attacks. The research contributes to the understanding and mitigation of DoS attacks in a virtualized network environment, ultimately enhancing network security.

REFERENCES

Adiwal, S., Rajendran, B., D., P. S., & Sudarsan, S. D. (2023). DNS Intrusion Detection (DID) — A SNORT-based solution to detect DNS Amplification and DNS Tunneling attacks. Franklin Open, 2, 100010. https://doi.org/10.1016/j.fraope.2023.100010

Alatawi, F. (2021). Defense mechanisms against Distributed Denial of Service attacks: Comparative Review. Journal of Information Security and Cybercrimes Research, 4(1), 81–94. https://doi.org/10.26735/lqez4186

Gupta, A., & Sharma, L. S. (2019). Mitigation of DoS and Port Scan Attacks Using Snort. International Journal of Computer Sciences and Engineering, 7(4), 248–258. https://doi.org/10.26438/ijcse/v7i4.248258