DOS Attack Scanner and Defender

Syed Ali Haider - 19754, Syed Meeran Tajalli - 19726

December,2023

Network Security Project Phase 01

December 2023

Supervisor: Dr. Faisal Iradat

Abstract

Denial of Service (DOS) attacks pose a significant threat to the availability and stability of network services. This report introduces a comprehensive DOS attack scanner and defender system designed to identify and mitigate such attacks. The scanner employs advanced techniques to detect anomalous traffic patterns indicative of DOS attacks, while the defender utilizes proactive measures to thwart and minimize the impact of such malicious activities. The project aims to enhance network security by providing a robust solution against DOS threats. Key features, methodologies, and experimental results are discussed, showcasing the effectiveness of the proposed scanner and defender in real-world scenarios.

1 Introduction

In recent years, the frequency and sophistication of DOS attacks have increased, posing a severe risk to the uninterrupted operation of network services. To address this growing concern, our project focuses on the development of a DOS attack scanner and defender system. By simulating local DOS attacks and analyzing the data using Wireshark, we aim to enhance our understanding of attack patterns and develop effective countermeasures.

2 Methodology

Our methodology involves creating controlled DOS attack scenarios within a local network environment. We utilize Wireshark to capture and analyze network traffic during these simulated attacks. The DOS attack scanner employs machine learning algorithms and heuristic analysis to identify abnormal patterns in the traffic, distinguishing between legitimate and malicious requests. The defender, on the other hand, responds to detected attacks by implementing various mitigation strategies, such as IP filtering, rate limiting, and traffic redirection.

3 Experimental Results

Preliminary experiments demonstrate the effectiveness of our DOS attack scanner and defender. Wireshark logs reveal the detection of anomalous traffic spikes corresponding to the simulated DOS attacks. The defender successfully mitigates the impact by dynamically adapting its defense mechanisms based on the characteristics of the attack. Our system shows promise in providing real-time protection against DOS threats in local network environments.

4 Training Model

In the development of our DOS attack scanner, we employed the Random Forest algorithm as our primary machine learning model. Random Forest is a robust and versatile ensemble learning technique that combines the predictions of multiple decision trees to enhance accuracy and reduce overfitting. The model was trained on a diverse dataset comprising both normal and simulated DOS attack traffic patterns. The utilization of Random Forest contributes to the effectiveness of our scanner in discerning subtle anomalies within network traffic.

5 Packet Transfer Mechanism

The packet transfer process during DOS attack simulations involves the use of Wireshark, a widely adopted network protocol analyzer. Wireshark captures packets traversing the local network during both normal and attack scenarios. The captured data is then subjected to detailed analysis, allowing us to identify patterns and anomalies indicative of a DOS attack. By studying packet-level information, we gain insights into the tactics employed by attackers and can subsequently refine our detection algorithms.

6 Wireshark Log Analysis

The effectiveness of our DOS attack scanner heavily relies on the analysis of Wireshark logs. During the experimental phase, we meticulously examined the logs to identify patterns associated with both legitimate and malicious traffic. Notable findings include the detection of sudden spikes in packet count, unusual traffic patterns, and distinctive signatures characteristic of DOS attacks. Wireshark's comprehensive log data facilitated the training of our machine learning model and informed the development of heuristic rules for real-time attack detection.

7 Defender Mechanisms

In response to identified DOS attacks, the defender component of our system implements a multi-faceted approach to mitigate their impact. IP filtering is employed to block traffic from suspicious sources, rate limiting helps control the influx of requests, and traffic redirection ensures that legitimate traffic is prioritized. These mitigation strategies are dynamically adjusted based on the characteristics of the ongoing attack, allowing for a flexible and adaptive defense mechanism.

8 Real-World Scenario Simulations

To validate the practical efficacy of our DOS attack scanner and defender, we conducted simulations in diverse real-world scenarios. These scenarios included variations in network size, traffic volume, and attack types. The results consistently demonstrated the system's ability to adapt and effectively defend against a range of DOS attacks, showcasing its relevance and reliability in different network environments.

9 Future Enhancements

While our current system exhibits promising results, ongoing efforts will focus on refining the Random Forest model, expanding the dataset to include a wider array of attack scenarios, and further optimizing the defender's response mechanisms. Additionally, integration with emerging threat intelligence sources and continuous monitoring will be explored to ensure the system remains resilient against evolving DOS attack tactics.

10 Conclusion

In conclusion, the development of a robust DOS attack scanner and defender is crucial for safeguarding network infrastructure. By leveraging Wireshark for data collection and analysis, we have gained valuable insights into the dynamics of DOS attacks within a controlled environment. The experimental results underscore the efficacy of our system in detecting and mitigating such threats. Future work will focus on refining the algorithms, expanding the scope of attack scenarios, and further validating the system's performance in diverse network settings.

11 Objective

Clearly state the objectives of the project, including the development of a DOS attack scanner and defender.

12 Methodology

Outline the steps and methodology used in the project. This may include:

- Setting up a local network for testing.
- Conducting DOS attacks on the local network.
- Capturing network traffic data using Wireshark.
- Preprocessing and analyzing the captured data.
- Developing a machine learning model for anomaly detection.
- Implementing the defense mechanism (detector) based on the trained model.