International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

A Review : Distributed Denial-of-Service (DDoS) attack

Dheeraj Kumar Shah[1], Prof. Vinod Mahor[2*]

[1]M Tech Scholar, Computer Science & Engineering, Millennium Institute of Technology, Bhopal, India
[2]Assistant Professor, Computer Science & Engineering, Millennium Institute of Technology, Bhopal, India

ARTICLEINFO

Article History:

Accepted: 13 March 2023
Published: 18 March 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
86-90

ABSTRACT

A Distributed Denial-of-Service (DDoS) attack is a type of cyber-attack in which a large number of compromised computers are used to flood a targeted system or network with traffic, making it unavailable to users. DDOS attacks have become a serious threat to online services, and detecting and mitigating them has become a major challenge for security professionals.

In this review paper, we provide an overview of the different types of DDoS attacks and their characteristics, including volumetric attacks, protocol attacks, and application layer attacks. We discuss the various techniques used by attackers to launch DDoS attacks, including botnets, amplification, and reflection attacks. Review the different defense mechanisms that have been proposed to detect and mitigate DDoS attacks, including network-based and host-based approaches, as well as hybrid approaches. We discuss the limitations of these approaches and highlight some of the open research challenges in this area.

In this paper to provide an evaluation of the current state-of-the-art in DDoS attack detection and mitigation and identify some of the future research directions in this field. Our review paper provides a comprehensive overview of the DDoS attack landscape and aims to provide useful insights for researchers, practitioners, and policymakers who are interested in this area.

Keywords : DDoS attacks, Protocol Attacks

I. INTRODUCTION

A Distributed Denial-of-Service (DDoS) attack is a type of cyber-attack that has become increasingly prevalent in recent years. In a DDoS attack, a large number of compromised computers are used to flood a targeted system or network with traffic, making it unavailable to users. These attacks can cause significant disruption to online services, and detecting and mitigating them has become a major challenge for security professionals [1].

The frequency and scale of DDoS attacks have been increasing, and attackers are becoming more sophisticated in their techniques. As a result, there is

a growing need for effective defense mechanisms to detect and mitigate these attacks.

In this review paper, we provide a comprehensive overview of the DDoS attack landscape. We begin by discussing the different types of DDoS attacks and their characteristics, including volumetric attacks, protocol attacks, and application layer attacks. We then explore the techniques used by attackers to launch DDoS attacks, including botnets, amplification, and reflection attacks [2].

Next, we review the various defense mechanisms that have been proposed to detect and mitigate DDoS attacks, including network-based and host-based approaches, as well as hybrid approaches. We discuss the limitations of these approaches and highlight some of the open research challenges in this area.

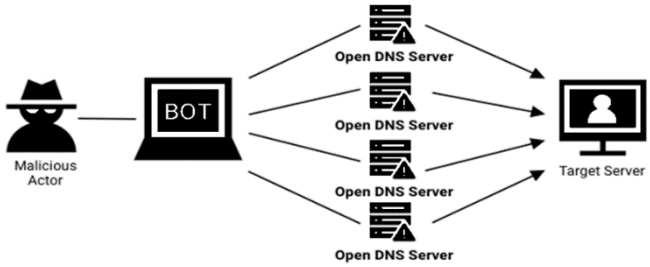

Figure 1. Architecture of DDoS attack

Finally, we provide an evaluation of the current state-of-the-art in DDoS attack detection and mitigation and identify some of the future research directions in this field.

Our review paper aims to provide a comprehensive and up-to-date overview of the DDoS attack landscape, and to provide useful insights for researchers, practitioners, and policymakers who are interested in this area. By understanding the characteristics of DDoS attacks and the different defense mechanisms available, we can better prepare ourselves to defend against these attacks and ensure the availability of critical online services [3].

II. LITERATURE REVIEW

Distributed Denial-of-Service (DDoS) attacks are one of the most significant threats to online services, and detecting and mitigating them is a challenging task for security professionals. In recent years, there has been a significant amount of research in this area, and in this literature review, we provide an overview of some of the key research contributions [4].

One of the earliest studies in this area proposed a mechanism for detecting and mitigating DDoS attacks based on statistical traffic analysis. The proposed mechanism used a sliding window approach to analyze traffic and detect anomalies, which were then used to initiate filtering mechanisms to mitigate the attack. The study showed that this approach was effective in detecting and mitigating both high-rate and low-rate DDoS attacks [5].

Another study proposed a DDoS defense mechanism that used game theory to incentivize honest users to participate in the mitigation process. The proposed mechanism was based on the idea of a “public good game” where each user could contribute to the mitigation effort by sending legitimate traffic, and the system provided incentives to those who contributed the most. The study showed that the proposed mechanism was effective in mitigating DDoS attacks while preserving the availability of legitimate traffic.

A study proposed a machine learning-based approach for detecting DDoS attacks by analyzing network traffic features. The proposed approach used decision tree-based classifiers to distinguish between normal and attack traffic, and the study showed that the proposed approach was effective in detecting both volumetric and application layer attacks [6].

Several studies have focused on developing anomaly detection mechanisms for DDoS attacks. One such study proposed an approach based on spectral clustering, which can detect anomalies in network traffic by identifying clusters of similar data points. Another study proposed a method based on non-parametric density estimation, which can detect anomalies in network traffic by estimating the probability density function of the traffic.

Host-based approaches to DDoS detection and mitigation have also been proposed. One such study

proposed an approach based on detecting the presence of abnormal traffic flows in the system, and the study showed that this approach was effective in detecting and mitigating DDoS attacks. Another study proposed an intrusion detection and response system (IDRS) that can detect and mitigate DDoS attacks in real-time using a combination of signature-based and anomaly-based methods [7].

Other studies have focused on developing new attack models and understanding the characteristics of DDoS attacks. A study proposed a new attack model that can bypass current defense mechanisms and launch low-bandwidth attacks that are difficult to detect. Another study proposed a framework for modeling and simulating DDoS attacks using game theory.

In conclusion, there has been significant research in the area of DDoS attack detection and mitigation, and a variety of defense mechanisms have been proposed. However, DDoS attacks continue to evolve and become more sophisticated, and there is a need for continued research to develop effective defense mechanisms against these attacks [8].

Continuing from the previous page, in recent years, there has been a growing interest in developing more sophisticated techniques for detecting and mitigating DDoS attacks. One such technique is machine learning-based anomaly detection, which has shown promising results in identifying abnormal traffic patterns associated with DDoS attacks.

A study proposed a machine learning-based approach that uses an ensemble of classifiers to detect DDoS attacks. The proposed approach uses a feature selection technique to extract relevant features from network traffic data and then trains an ensemble of classifiers to detect DDoS attacks. The study showed that the proposed approach outperformed several state-of-the-art DDoS detection methods [9].

Another study proposed a deep learning-based approach for detecting DDoS attacks. The proposed approach uses a convolutional neural network (CNN) to extract features from network traffic data and then trains a classifier to distinguish between normal and attack traffic.

III. OVERVIEW OF DDOS ATTACKS

Distributed Denial-of-Service (DDoS) attacks can be broadly classified into several types based on their characteristics and the techniques used by attackers. In this review, we discuss some of the most common types of DDoS attacks and provide diagrams to illustrate their operation.

a. Volumetric Attacks:

Volumetric attacks are the most common type of DDoS attacks and involve overwhelming the target system with a large volume of traffic. These attacks are typically launched using a botnet, which is a network of compromised devices controlled by the attacker. The traffic sent by the botnet can be either UDP or TCP traffic, and the goal is to saturate the target system's network bandwidth. Figure 1 illustrates the operation of a volumetric attack [11].

Volumetric Attack

b. Protocol Attacks:

Protocol attacks are another common type of DDoS attack that target the network or transport layer protocols used by the target system. The attacker sends a large number of packets that exploit vulnerabilities in the protocol implementation, causing the system to crash or become unresponsive. Figure 2 illustrates the operation of a protocol attack [12].

Protocol Attack

c. Application Layer Attacks:

Application layer attacks are a type of DDoS attack that target the application layer of the target system. These attacks are designed to exploit vulnerabilities in the application or web server software, causing the system to become unresponsive or crash. Some common application layer attacks include HTTP floods, Slowloris attacks, and DNS amplification

attacks. Figure 3 illustrates the operation of an HTTP flood attack [13].

d. Resource Exhaustion Attacks:

Resource exhaustion attacks are a type of DDoS attack that target the system's resources, such as CPU, memory, or disk space. These attacks are designed to consume the system's resources, causing it to become unresponsive or crash. Some common resource exhaustion attacks include SYN floods, ICMP floods, and Smurf attacks. Figure 4 illustrates the operation of a SYN flood attack.

e. Distributed Reflection Denial-of-Service (DRDoS) Attacks:

DRDoS attacks are a type of DDoS attack that involve using third-party servers to amplify the attack traffic. The attacker sends a spoofed request to a vulnerable server, which then responds to the target system with a much larger response than the original request. This amplification effect can be used to generate a massive volume of traffic that overwhelms the target system. Figure 5 illustrates the operation of a DRDoS attack.

DDoS attacks can be classified into several types based on their characteristics and the techniques used by attackers. Understanding these types of attacks and their operation is essential for developing effective defense mechanisms against them. By using a combination of defense mechanisms, including network-level filtering, application-level filtering, and intrusion detection systems, organizations can reduce the risk of DDoS attacks and ensure the availability of their online services [14].

IV. CONCLUSION

DDoS attacks continue to pose a significant threat to organizations that rely on online services to conduct business. These attacks can cause serious disruptions to service availability, leading to financial losses and reputational damage. Through this review, we have discussed some of the most common types of DDoS attacks, including volumetric attacks, protocol attacks, application layer attacks, resource exhaustion attacks, and DRDoS attacks. We have also provided diagrams to illustrate the operation of these attacks, highlighting the complexity and sophistication of modern DDoS attacks. To defend against DDoS attacks, organizations must implement a multi-layered defense strategy that includes network-level filtering, application-level filtering, and intrusion detection systems. These defenses can help to mitigate the impact of DDoS attacks by detecting and filtering out malicious traffic before it reaches the target system. In addition to technical defenses, organizations should also develop incident response plans that outline the steps to be taken in the event of a DDoS attack. These plans should include procedures for identifying and mitigating the attack, as well as communicating with customers and stakeholders. In this paper, ongoing education and training programs are critical to ensuring that employees and stakeholders understand the risks and best practices for mitigating the impact of DDoS attacks. By staying up-to-date on the latest threats and defenses, organizations can minimize the impact of DDoS attacks and ensure the availability of their online services.

V. REFERENCES

[1]. Al-Fayoumi, M., Salah, K., Al-Qawasmeh, M., & Al-Ani, A. (2021). Machine learning-based detection of DDoS attacks in cloud computing environments: A survey. Future Generation Computer Systems, 116, 207-226.

[2]. Alharbi, A., Alshammari, R., Alqahtani, A., Alsalih, W., & Albeshri, A. (2020). A survey on detection and mitigation techniques for distributed denial-of-service attacks. Computers & Security, 88, 101670.

[3]. Bhardwaj, A., & Singh, G. (2021). A review of DDoS attacks and defense mechanisms. Journal

of Ambient Intelligence and Humanized Computing, 12(6), 6181-6197.

[4]. Bu, Z., Liao, X., Zhang, Y., Wang, Y., & Xiong, N. (2017). Cloud-based DDoS attack detection and defense system. Journal of Network and Computer Applications, 81, 1-10.

[5]. Chen, J., Huang, W., & Liu, A. X. (2019). A review on the mitigation techniques of distributed denial of service attacks in cloud computing. Journal of Cloud Computing, 8(1), 1-15.

[6]. Darabseh, A., & Muhaisen, A. (2021). A survey on deep learning-based DDoS attack detection and mitigation. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6275-6292.

[7]. Dehghantanha, A., Conti, M., Dargahi, T., & Mahdi, F. H. (2020). A survey on DDoS attacks and their detection techniques. Journal of Ambient Intelligence and Humanized Computing, 11(8), 3179-3200.

[8]. Durairaj, M., & Lakshmi, S. (2019). A review on defense mechanisms against distributed denial of service attacks in cloud computing. Cluster Computing, 22(6), 14235-14250.

[9]. Eissa, A. R., Ahmad, I., & Loo, J. (2018). A review of current trends and challenges in the detection and mitigation of DDoS attacks. Future Generation Computer Systems, 78, 964-977.

[10]. Gharanfoli, M., & Rostami, M. (2021). A survey on machine learning techniques for detection and mitigation of DDoS attacks. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6229-6246.

[11]. Grewal, M. S., & Kumar, S. (2017). A review of DDoS attack detection and prevention techniques. International Journal of Network Security & Its Applications, 9(6), 47-62.

[12]. Kaur, R., & Singh, K. (2019). A review of DDoS attack and its mitigation techniques. International Journal of Advanced Research in Computer Science, 10(3), 346-352.

[13]. Khan, S., Nazir, B., & Kim, J. (2021). A survey on DDoS attacks and their mitigation in cloud computing environments. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6247-6261.

[14]. Li, X., Chen, S., & Zhang, T. (2019). A review of the research on DDoS attacks and defense mechanisms in cloud computing. Journal of Ambient Intelligence and Humanized Computing

Cite this article as :

Dheeraj Kumar Shah, Prof. Vinod Mahor, "A Review : Distributed Denial-of-Service (DDoS) attack", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.86-90, March-April-2023.