AICyberInnovate Spectrum Magazine

Safeguarding Against DoS and DDoS Attacks in Modern Networks

KUKUTLA TEJONATH REDDY,
International Center for AI and Cyber Security Research and Innovations (CCRI),
Asia University, Taiwan, tejonath45@gmail.com

ABSTRACT

DoS/DDoS attacks are the most common and frequent attack on networks. DoS will stand for Denial of Service and DDoS will stand for Distributed Denial of Service. In DoS attack, the attacker aims to show the user computer or network or website unavailable to use by over network traffic flooding illegitimate requests or data on the computer or network or website. DDoS is a more advanced form of attack than DoS attack in which the attack will launch from multiple compromised systems. DDoS attacks are harder to trace and mitigate. In this article we will discuss Dos and DDoS attack, mechanism of DoS and DDoS attack and some prevention from DoS and DDoS attack.

KEYWORDS: Vulnerabilities, DoS, DDoS, Botnets, Firewalls, Traffic filtering

I. INTRODUCTION

In this continuing evolving digital world, cybersecurity plays a major role. These days the internet is growing rapidly, cybercriminals are increasing day by day. They all are committing crimes on the internet rather than in the real world. In this digital world there is an attack called DoS in which an attacker will send multiple network traffic flooding requests on a user computer or network or website. This is a very common attack these days. When a DoS attack is launched from multiple compromised systems it is called Distributed Denial of Service (DDoS) attack. This includes overloading the target systems with traffic and taking advantage of software and network protocols vulnerabilities. On other hand they will take advantage of massive networks of infected devices to create some botnets that will increase their impact. These attacks will not only interrupt the services they also put the companies and organization in risk by stealing financial data and sensitive information. There are some of the prevention mechanisms also for protecting our data from attackers like firewalls, intrusion detection systems. In this article we will discuss about what is DoS and DDoS, what is the mechanism of these attacks, Evolving Strategies and Trends and prevention for DoS and DDoS attack

A. What is a DoS attack?

The attacker will send the network traffic flooding to a target server or network by making the server or network unable to respond to valid requests; this is called a Denial of Service (DoS) attack. Attacker will perform this attack by taking advantage of vulnerabilities on target system and utilizing its resources, like bandwidth, power, or memory

Fig.no:1 (DoS Attack)

B. What is a DDoS attack?

In this attack the attacker will use multiple sources instead of one source which includes a network of victim machines under the direction of an attacker. These attacks have more potential of overloading the network traffic to the target system. In this process the detection and mitigation are more difficult compared to DoS attack

C. How DoS and DDoS Attacks Works?

Mechanism of DoS attack: DoS attack usually will take advantage of vulnerabilities in software and network protocols. TCP/IP attacks which will take advantage of vulnerabilities in the TCP/IP protocol family, and HTTP flood attacks in which HTTP request flooding hits web servers. TCP/IP attack and HTTP flooding attacks are the common types of DoS attacks.

Mechanism of DDoS attack: Attackers usually involve compromised systems that have been infected with malware. The attacker will command the compromised systems to send the number of network traffic requests to the target server. Which is referred to as a botnet. By commanding the botnet to take over the target system. DDoS attacks are harder to prevent.

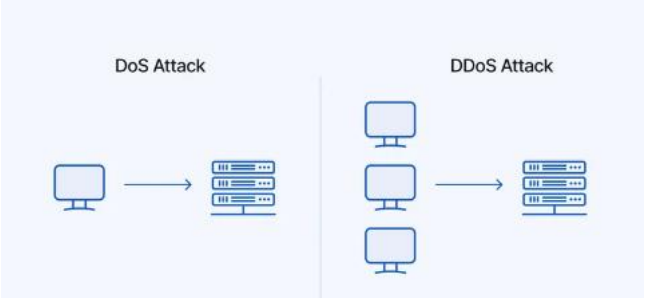

Fig.no:2 (how Dos and DDoS attack works)

III. RELATED WORKS

DDoS attack is divided into three categories: Volumetric, protocol and application layer. Volumetric attacks will consume the bandwidth of the target, Protocol attacks will exploit the weaknesses of the network protocol and application layer attacks will target specific services or applications running on the target machine [1].

DoS and DDoS attacks are divided into four categories: bandwidth depletion, resource depletion, semantic and amplification. In bandwidth depletion the attacker will flood the target with huge scale of traffic, resource depletion attacks will consume the CPU, memory, or disk space of the target, semantic attacks will exploit the vulnerabilities of the target, and amplification attacks will use third party servers to amplify the attack traffic [2].

“DDoS Attack Detection and Mitigation: Techniques and Challenges” In this paper we can analyze the challenges and limitations of DDoS mitigation techniques like firewalls, intrusion detection systems, traffic filtering and rate limiting

“Botnet-based DDoS Attack Detection using Flow-Based Features"

Focused on the detection of DDoS attacks orchestrated through botnets, this paper, published in the Journal of Computer Security, presents a novel approach based on flow-based features. By analyzing network flows, the research aims to identify patterns indicative of botnet-driven DDoS attacks. The study explores the effectiveness of flow-based features in distinguishing between legitimate and malicious traffic, offering valuable insights for improving DDoS detection systems.

Evolving Strategies and Trends:

IoT Based Attacks: Attackers will develop a botnet by taking advantage of IoT devices. In IoT based DDoS attacks smart devices like cameras and routers will compromise and they will turn into botnet nodes. These attacks will have high potential to generate traffic, they will make mitigation difficult.

Application Layer Attacks: Modern DDoS attacks usually concentrate on weakness to attack within particular apps or services, compared with normal volumetric attacks. Attacks on the application layer will target the application interface by flooding it with what appear to be trustworthy requests. Since the traffic flooding requests are legitimate these attacks are more difficult to detect.

Mobile Devices and 5G Networks: Nowadays mobile networks have become faster and safe because of 5G technology. Although it has advantages for authorized users, it will also allow attackers to use more powerful DDoS attacks with mobile devices. Due to the movable and dynamic nature of the sources, these attacks became harder to identify.

Machine Learning-Powered Attacks: Machine learning algorithms are used by cybercriminals to improve their attack plans. This will help for continuous monitoring and modification of attack patterns by these algorithms makes it challenging for standard security measures

IV. Preventions

The good news is that with the right security measures we can secure our data or information from DoS and DDoS attack.

Preventions:

Implement Firewalls and Intrusion Detection Systems (IDS/IPS): Firewalls will filter the malicious traffic and IDS/IPS will detect and block if any suspicious activities take place in real-time.

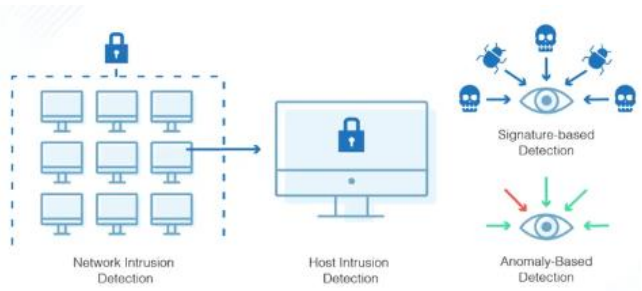

Fig.no: 3 (IDS working)

Implement CAPTCHA and Challenge-Response Tests: Using CAPTCHA and other challenge-response mechanisms we can distinguish human users and bots, by this we can identify the automated attacks.

Anomaly Detection: Using anomaly detection tools, we can identify unusual patterns and behavior in the traffic without allowing for quick response to potential attacks.

Rate Limiting and Throttling: By implementing rate limiting mechanisms we can restrict the number of requests from a single source that too in a specific time frame. By this method we can prevent an attacker from sending too many requests.

Mitigation:

DDoS Mitigation Services: Using Specific DDoS mitigation service, we can detect and filter the malicious traffic. DDoS mitigation service is a combination of traffic analysis, rate limiting and other techniques.

Cloud-Based DDoS Protection: By using Cloud-based DDoS protection services it will absorb and mitigate the large-scale attacks without reaching network infrastructure

Traffic Filtering: Using traffic filtering techniques, we can identify and block traffic based on some specific characteristics like IP addresses or protocols associated with known attack patterns.

Incident Response Plan: We need to have a well-defined incident response plan in place. This needs to identify, mitigate and recover from DoS and DDoS attacks.

Regular Training: We need to educate employees and network administrators about the latest threats

and best ways to prevent and responding from the DoS and DDoS attacks[8-10]

V. CONCLUSIONS

Cybersecurity is essential in this ever-expanding digital world, where the internet is the backbone of the global connection. Threats like DoS and DDoS exist for intercepting the connections. These attacks will harm the networks and websites and make them unreachable by flooding the network traffic requests on target systems. In this article we have discussed these topics.

VI. References

[1] Douligeris, Christos & Mitrokotsa, Aikaterini. (2004). DDOS Attacks and Defense Mechanisms: a Classification. 190 - 193. 10.1109/ISSPIT.2003.1341092.

[2] Tripathi, Nikhil & Mehtre, Babu. (2013). DoS and DDoS Attacks: Impact, Analysis and Countermeasures. 1-6.

[3] Mirkovic, Jelena & Reiher, Peter. (2004). A taxonomy of DDoS attack and DDoS Defense mechanisms. ACM SIGCOMM Computer Communication Review. 34. 10.1145/997150.997156.

[4] I. Sumantra and S. Indira Gandhi, "DDoS attack Detection and Mitigation in Software Defined Networks," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2020, pp. 1-5, doi: 10.1109/ICSCAN49426.2020.9262408.

[5] Yihunie, F., Abdelfattah, E., & Odeh, A. (2018, May 4). Analysis of ping of death DoS and DDoS attacks. *Proceedings from IEEE Long Island Systems, Applications and Technology Conference,* Farmingdale, NY. Doi: 10.1109/LISAT.2018.8378010

[6] Nezhad, S.M., Nazari, M., & Gharavol, E.A. (2016). A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks. *IEEE Communications Letters, 20*, 700-703.

[7] O. Ali and P. Cotae, "Towards DoS/DDoS Attack Detection Using Artificial Neural Networks," 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2018, pp. 229-234, doi: 10.1109/UEMCON.2018.8796637.

[8]Wang, H., et. al, C. (2020). Visual saliency guided complex image retrieval. Pattern Recognition Letters, 130, 64-72.

[9]Al-Qerem, A., et al. (2020). IoT transaction processing through cooperative concurrency control on fog–cloud computing environment. Soft Computing, 24(8), 5695-5711.

[10]Gupta, B. B., & Quamara, M. (2020). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience, 32(21), e4946.