Data Analytics and Artificial Intelligence
Vol: 3(7), 2023
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/daai/

A Study of Dos Attacks

N. Priyanka
Adhiyamaan college to engineering (autonomous), Hosur, Tamilnadu,india
*Corresponding Author Email: priyankanagesh212@gmail.com

Abstract: *Denial of service (DoS) attacks have become a major threat to current computer networks. To have a better understanding on DoS attacks, this article provides an overview on existing DoS attacks and major defense technologies in the Internet and wireless networks. In particular, we describe network based and host based DoS attack techniques to illustrate attack principles. DoS attacks are classified according to their major attack characteristics. Current counterattack technologies are also reviewed, including major defense products in deployment and representative defense approaches in research*
Keywords: *Denial of Service, Distributed Denial of Service, Internet Security, Wireless Security, Scanner.*

1. INTRODUCTION

A denial-of-service (DoS) attack is a security threat that occurs when an attacker makes it impossible for legitimate users to access computer systems, network, services or other information technology (IT) resources. Attackers in these types of attacks typically flood web servers, systems or networks with traffic that overwhelms the victim's resources and makes it difficult or impossible for anyone else to access them. Restarting a system will usually fix an attack that crashes a server, but flooding attacks are more difficult to recover from. Recovering from a distributed DoS (Dodos) attack in which attack traffic comes from a large number of sources is even more difficult. DoS and Dodos attacks often take advantage of vulnerabilities in networking protocols and how they handle network traffic. For example, an attacker might overwhelm the service by transmitting many packets to a vulnerable network service from different Internet Protocol (IP) addresses.

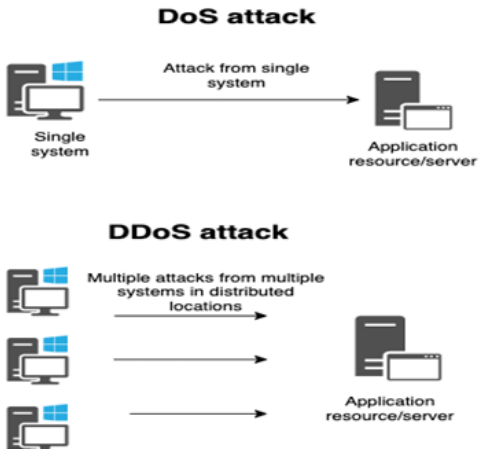

FIGURE 1. DDOS attack

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: □ attempts to "flood" a network, thereby preventing legitimate network traffic. Attempt to disrupt a server by sending more requests than it can possibly handle, thereby preventing access to a service. □ attempts to prevent a particular individual from accessing a service. Attempts to

disrupt service to a specific system or person.A DoS attack can be perpetrated in a number of ways. There are three basic types of attack: consumption of computational resources, such as bandwidth, disk space, or CPU time. Disruption of configuration information, such as routing information. disruption of physical network components. unusually slow network performance (opening files or accessing web sites) unavailability of a particular web site inability to access any web site dramatic increase in the number of spam emails received

2. TYPES OF DOS ATTACKS

3.1. Application layer : These attacks generate fake traffic to internet application servers, especially domain name system (DNS) servers or Hypertext Transfer Protocol (HTTP) servers. Some application layer DoS attacks flood the target servers with network data; others target the victim's application server or protocol, looking for vulnerabilities.

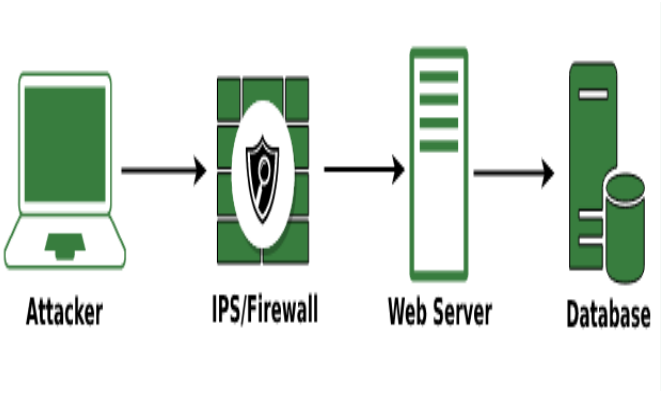

FIGURE 2. Application layer

3.2. Buffer overflow: This type of attack is one that sends more traffic to a network resource than it was designed to handle.

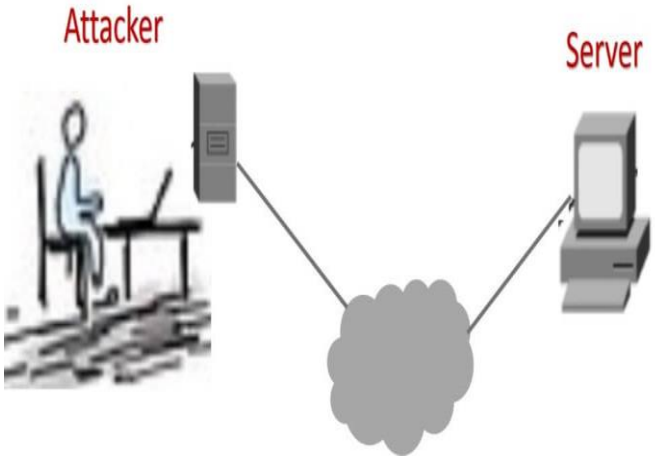

FIGURE 3. Buffer overflow

3.3. DNS amplification: In a DNS DoS attack, the attacker generates DNS requests that appear to have originated from an IP address in the targeted network and sends them to misconfigured DNS servers managed by third parties. The amplification occurs as the intermediate DNS servers respond to the fake DNS requests. The responses from intermediate DNS servers to the requests may contain more data than ordinary DNS responses, which requires more resources to process. This can result in legitimate users being denied access to the service.

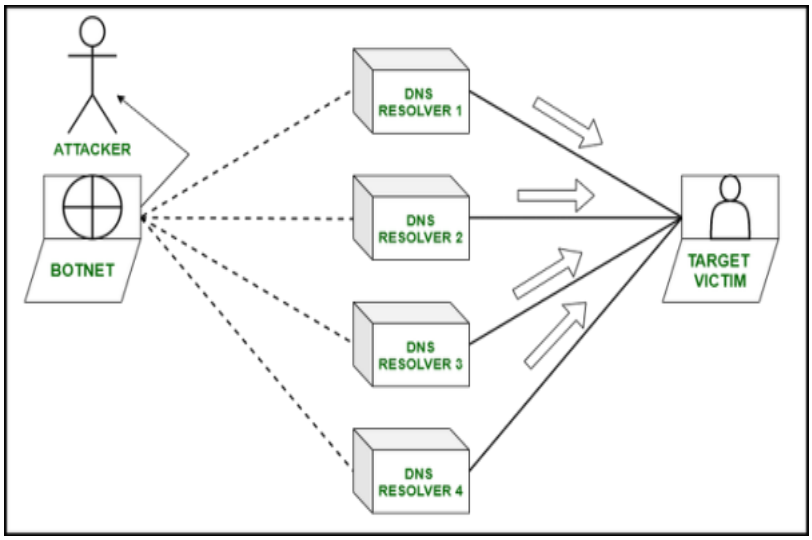

FIGURE 4. DNS amplification

3.4. Ping of death: These attacks abuse the ping protocol by sending request messages with oversized payloads, causing the target systems to become overwhelmed, to stop responding to legitimate requests for service and to possibly crash the victim's systems.

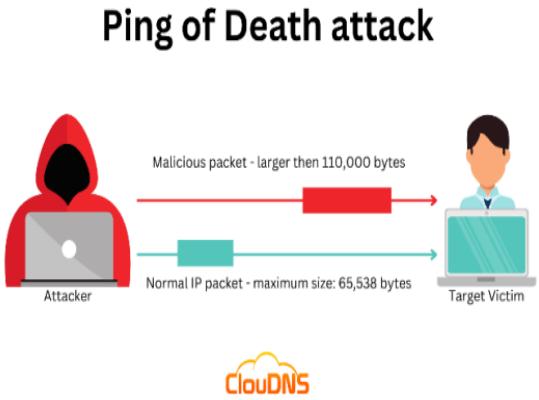

FIGURE 5. Ping of death

3.5. State exhaustion: These attacks -- also known as *Transmission Control Protocol (TCP) attacks* -- occur when an attacker targets the state tables held in firewalls, routers and other network devices and fills them with attack data. When these devices incorporate stateful inspection of network circuits, attackers may be able to fill the state tables by opening more TCP circuits than the victim's system can handle at once, preventing legitimate users from accessing the network resource.

FIGURE 6. State exhaustion

3.6. ***SYN flood:*** The attacker sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and eat the server resources. A legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

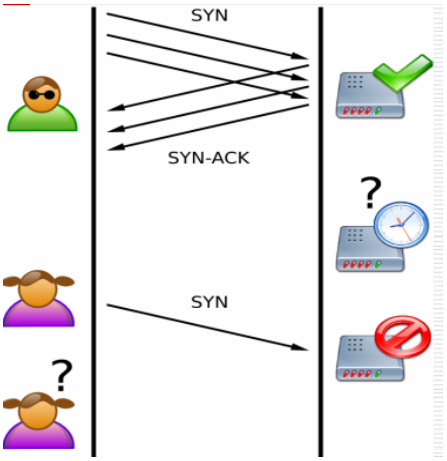

FIGURE 7. SYN flood

3.7. Teardrop: These attacks exploit flaws like how older operating systems (OSes) handled fragmented IP packets. The IP specification enables packet fragmentation when the packets are too large to be handled by intermediary routers, and it requires packet fragments to specify fragment offsets. In teardrop attacks, the fragment offsets are set to overlap each other. Hosts running affected OSes are then unable to reassemble the fragments, and the attack can crash the system.

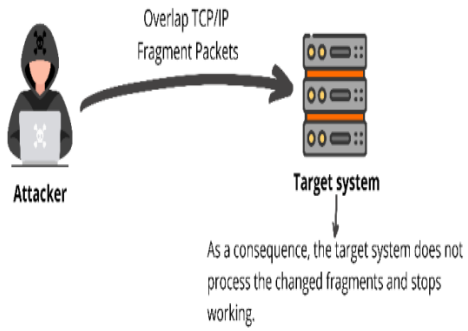

FIGURE 8. Teardrop

3.8. Volumetric: These DoS attacks use all the bandwidth available to reach network resources. To do this, attackers must direct a high volume of network traffic at the victim's systems. Volumetric DoS attacks flood a victim's devices with network packets using UDP or Internet Control Message Protocol (ICMP). These protocols require relatively little overhead to generate large volumes of traffic, while, at the same time, the victim's network devices are overwhelmed with network packets, trying to process the incoming malicious datagram's.

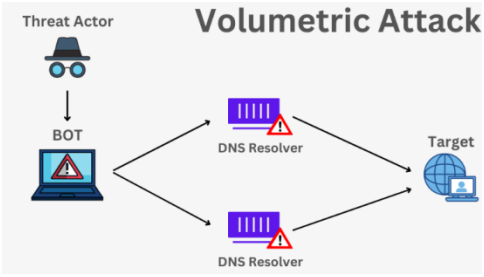

FIGURE 9. Volumetric Attack

TCP Three Way Handshake: When a computer wants to make a TCP/IP connection (the most common internet connection) to another computer, usually a server, an exchange of TCP/SYN and TCP/ACK packets of information occur. The computer requesting the connection, usually the client's or user's computer, sends a TCP/SYN packet w hitch asks the server if it can connect. If the server will allow connections, it sends a TCP/SYN-ACK packet back to the client to say "Yes, you may connect" and reserves a space for the connection, waiting for the client to respond with a TCP/ACK packet detailing the specifics of its connection.

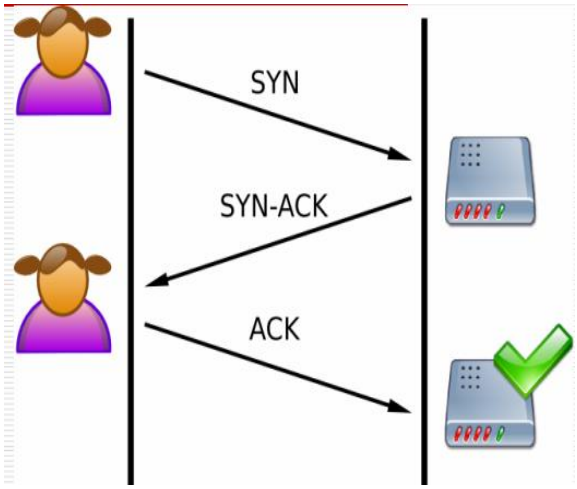

FIGURE 10. TCP Three Way Handshake

A normal connection between a user and a server. The three-way handshake is correctly performed.

4. DENIAL OF SERVICE ATTACK MECHANISM

Denial of Service attack is the major threat to the networks, computers and communications systems today .They have negatively affected services to organizations, individual users, critical Internet infrastructures etc., over the past decade or so .DoS Attack (including Dodos)is a malicious attempt to disrupt, degrade or prevent the availability of an Information resource to the legitimate users. The resources here are disk space, CPU time, the network b9andwidth, memory and other structures like static memory or memory buffers. DoS attacks are intentional almost all of the times but sometimes unintentional human errors during the designing process or programming, can lead to DoS attacks. The DoS attack that completely prevents the availability of a resource is called as the Destructive DoS attack. While as if the attack is only successful in bringing down the performance of the resource, it's called as a Degrading (non-destructive) DoS attack. A DoS attack can be executed from single sour9ce or from multiple sources either as a logic attack or as a flooding attack. A Logic DoS attack is based on exploiting vulnerability or a security hole in the target system. For example in the Internet Protocol (IP) packet, the Pay Load data size can be modified which may crash an operating system, due to a fault in the OS software. A common DoS attack scenario in which an Attacker (attack machine) sends large number of malicious packets to the Victim computer. Because of this attack the legitimate clients

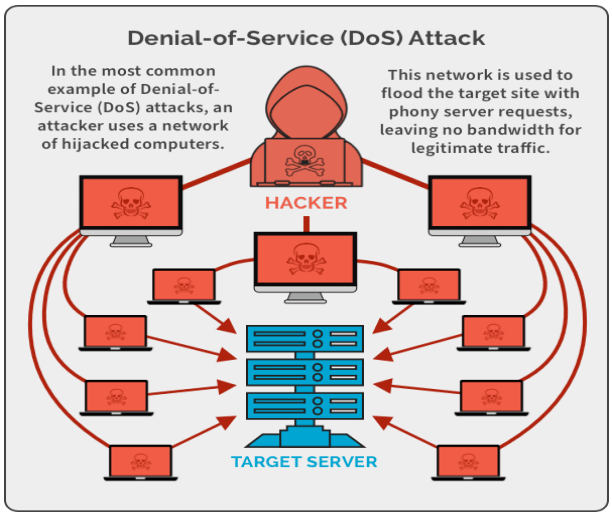

FIGURE 11. Denial of Service attack

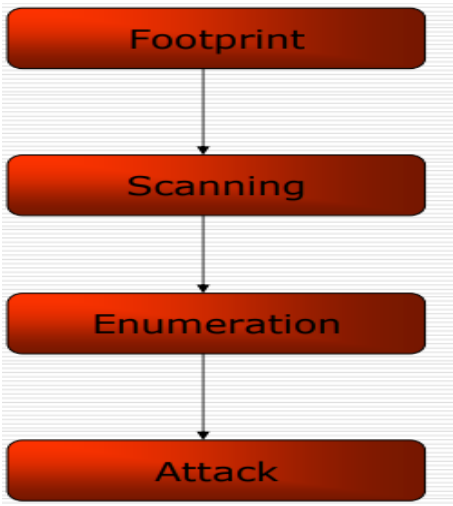

FIGURE 12. Hack Step

5. HOW CAN DENIAL-OF-SERVICE ATTACKS BE PREVENTED

Preventing a DoS attack can be challenging, but there are several effective techniques: Network segmentation - Segmenting networks into smaller, more manageable pieces, can limit the impact of a DoS attack. This can be done by creating VLANs, and firewalls can limit the spread of an attack. The optimal solution is zero trust micro segmentation. Adding device-level and device-cloaking firewalling, external to the operating system remains the most reliable form of DoS protection. Load balancing - Distributing traffic across multiple servers, a DoS attack can be prevented from overwhelming a single server or resource. Load balancing can be achieved using hardware or software solutions. IP blocking - Blocking traffic from known or suspected malicious sources can prevent DoS traffic from reaching its target. Rate limiting - Limiting the rate of traffic to reach a server or resource can prevent a DoS attack from overwhelming it. Content Delivery Networks (CDNs) - Distributing website content across multiple locations makes it more difficult for an attack to bring down an entire site.

6. DOS MITIGATION: WHAT TO DO DURING AN ATTACK

If a DoS attack is underway, there are several steps that can be taken to mitigate its impact: Traffic filtering can eliminate known or suspected malicious sources. Blackhole routing involves redirecting all traffic to a null route, effectively dropping all incoming traffic. This can be an effective way to mitigate a DoS attack, but it can also impact legitimate traffic. Scrubbing services identify and filter out malicious traffic, allowing legitimate traffic to reach its destination.

7. DOS PROTECTION: CHOOSING THE RIGHT SOLUTION

Approaches to DoS protection on the market today: Cloud-based services, On-premise hardware, Hybrid (combines cloud and on-premise), Asset cloaking (each asset is undiscoverable and inaccessible, with asset-specific firewalls running outside the operating system, blocking malicious packets from reaching or leaving the device),These tools offer a range of protection and mitigation capabilities, from basic IP blocking to advanced traffic filtering and scrubbing.

Vendor name	Product Name	Method	Open Source
Cloudflare	DoS Protection	Cloud-based	No
F5 Networks	Silverline	Cloud-based	No
Imperva	Incapsula	Cloud-based	No
Byos	Secure Edge	AssetCloaking	No
Fortinet	FortiDoS	On-premise	No
A10 Networks	Thunder TPS	On-premise	No
Snort	Snort	On-premise	Yes
NGINX	NGINX Plus	Hybrid	Yes
Radware	DefensePro	Hybrid	No
Arbor Networks	Peakflow	Hybrid	No

FIGURE 13. Dos Protection

8. CONCLUSION

A denial of service attack prevents legitimate users from accessing a device, service, or network. The disruption can have serious consequences for users and businesses alike and include loss of revenue, reputation, and sensitive data. DoS attacks come in many forms, including buffer overflows and flooding, with the attack having a single source. You may also encounter distributed denial of service attacks. These are similar to DoS attacks, but they come from multiple IPs, which makes them harder to detect and stop. The good news is there are ways to prevent DoS attacks. Some are simpler, like using a firewall and educating users about what DoS attacks look like. Others are more complex and involve using load balancing techniques, intrusion detection and prevention systems, encryption, and pen testing. Keep your systems secure against DoS and Dodos attacks with Gcore's Dodos. It can keep your services, apps, and websites safe, and has over 1 Tbps total filtering capacity. Connect with one of our experts to learn more.

REFERENCES

[1]. Aad, I., Hubbub, J.P., and Knightly, E. (2004). Denial of service resilience in ad hoc networks. Proceedings of ACM Modicum. ACM Press, New York. 2. Algieri, H., Smits, M., and Pons A. (2003). IP Trace back using header compression. Computers & Security, Vol. 22(2), pp. 136-151.
[2]. Carl, G., Resides, G., Brooks, R.R., and Rai, S.: 'Denial-of-service attack-detection techniques', IEEE Internet computing, 2006, 10, (1), pp. 82-89. [2] Tan, Z., Jading, A., He, X., Nanda, P., and Liu, R.P.: 'A system for denial-of-service attack detection based on multivariate correlation analysis', IEEE transactions on parallel and distributed systems, 2013, 25, (2), pp. 447-456
[3]. AWS Shield Managed Dodos protection. https://aws.amazon. com/shield/, November 2018.
[4]. Azure Dodos Protection Standard overview. https: //docs.microsoft.com/end-us/azure/virtual-network/ dodos-protection-overview, November 2018.
[5]. Consensus Health: Bandwidth Scanner Status. https:// consensus-health.torproject.org/#bwauthstatus, November 2018.
[6]. Meek. https://trac.torproject.org/projects/tor/wiki/ doc/meek, November 2018.