Prevention and Mitigation of DDoS in Digital World

Anshika Tripathi
Student, Dept. of M.Sc I.T Part II, Model College, Dombivli, Mumbai, Maharashtra, India.

Abstract: *This era is completely dependent on the Internet which serves as a global information for all users. Therefore the availability of the internet is extremely important. Distributed denial-of-service is one of the most highlighted and most important attacks of today's cyber world. This paper mainly focuses on the DDoS attack which obstructs the network availability by overflowing the victim with high volume of illegal traffic usurping its bandwidth, over-burdening it to prevent valid traffic to get through. A distributed denial of service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting, freezing or suspending the services of its hosting server. A DDoS attack can occur from any device to anywhere at any time without knowing the users.*

Keywords: *Introduction, Types of Attack, Common DDoS Attack types, DDoS Attack works, Prevention from Attacks, Conclusion, Acknowledgement.*

1.1 Introduction:

The first-ever DoS attack occurred in 1974 courtesy of David Dennis-a 13-year-old student at University High School, located across the street from the Computer-Based Education Research Laboratory (CERL) at the University of Illinois Urbana-Champaign.

A DDoS attack is launched from numerous compromised devices, often distributed globally in what's mentioned as a botnet. It is different from other Denial of Service (DoS) attacks, in that it uses a one Internet connected device (single network connection) to flood a target with malicious traffic or malicious attempt. This modulation is the reason for the existence of these two, somewhat different, definitions.

1.2 Types of Attacks:

DoS and DDoS attacks can be divided into three types, here are types describe:

- **Volume Based Attacks:**
  The attack's goal is to soak the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).
  The common types of volumetric DDoS attack types are:
  UDP floods: These attacks allow a hacker to overwhelm ports on the target host with IP packets containing the stateless UDP protocol.

DNS amplification (or DNS reflection): This attack redirects high amounts of DNS requests to the target's IP address.

ICMP flood: This strategy uses ICMP false error requests to overload the network's bandwidth.

- **Protocol Attacks:**
  This type of attack consumes critical actual server resources or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps). The common types of protocol-based DDoS attacks are:

SYN floods: An attacker sends TCP requests with fake IP addresses to the target system. The target machine responds and waits for the sender to confirm the handshake. As the attacker never sends the response to complete the handshake, the incomplete processes eventually crash the server.

Smurf DDoS: A hacker uses malware to create a network packet attached to a false IP address (spoofing). The package contains an ICMP ping notification that asks the network to send back a reply. The hacker sends the responses back to the network IP address again, creating an infinite loop that eventually crashes the system.

- **Application Layer Attacks:**
  Includes low and slow attacks, GET/POST floods, attacks that target Apache, Windows or Open-BSD vulnerabilities and more, Composed of apparently legitimate and guilt-less requests, the goal of these attacks is to crash the web server, and the immensity is measured in Requests per second (Rps).

1.3 Common DDoS Attacks types:

Some of the most commonly used DDoS attack types include:

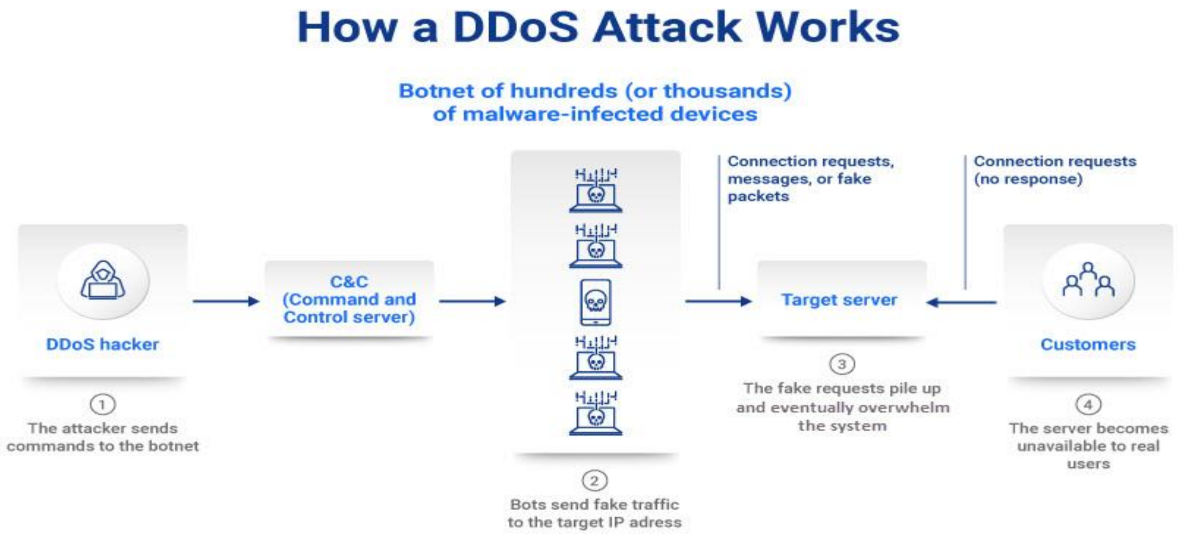
- **UDP Flood:**
  By definition, is any DDoS attack that floods a target with User Datagram protocol (UDP) packets. The goal of the attack is to flood unspecified ports on a remote host. This causes the host to check again and again for the application listening at port, and (when no application is found) reply with an ICMP ‘Destination Unreachable’ packet. This process saps host resources, which may ultimately cause inaccessibility.

- **ICMP (Ping) Flood:**
  Similar in theory to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without expecting replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often plan to respond with ICMP Echo Reply packets, leading to a big overall system slowdown.

- **SYN Flood:**
  A SYN flood DDoS attack exploits a known weakness within the TCP connection sequence (the "the-way handshake"), wherein a SYN request to initiate a TCP reference to a number must be answered by a SYN-ACK response from that host, then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either doesn't answer the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to attend for acknowledgement for every of the requests, binding resources until no new connections are often made, and ultimately leading to denial of service.

- **Ping of Death:**
  A ping of death (" POD") attack involves the hacker transferring multiple deformed or vicious tangs to a computer. The maximum packet length of an IP packet (including title) is bytes. Still, the Data Link Layer generally poses limits to the maximum frame size, for illustration 1500 bytes over an Ethernet network. In this case, a large IP packet is resolved across multiple IP packets (known as fractions), and the philanthropist host reassembles the IP fractions into the complete packet. In a Ping of Death script, following vicious manipulation of scrap content, the philanthropist ends up with an IP packet which is larger than bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for licit packets.

- **Slowloris:**
  Slowloris is a largely-targeted attack, enabling one web server to take down another server network, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by creating connections to the target server, but transferring only a partial request.


How a DDoS Attack Works
Botnet of hundreds (or thousands) of malware-infected devices
DDoS hacker
C&C (Command and Control server)
Connection requests, messages, or fake packets
Target server
Connection requests (no response)
Customers
1 The attacker sends commands to the botnet
2 Bots send fake traffic to the target IP adress
3 The fake requests pile up and eventually overwhelm the system
4 The server becomes unavailable to real users

Slowloris constantly sends further HTTP heads, but nowadays completes a request. The targeted server network keeps each of these false connections open. This ultimately overflows the maximum concurrent connection pool, and leads to denial of fresh connections from legitimate guests.

- **NTP Amplification:**

In NTP modification attacks, the perpetrator exploits publically accessible Network Time Protocol (NTP) waiters to overwhelm a targeted server with UDP business. The attack is defined as an modification assault because the query-to- response rate in similar scripts is anywhere between 120 and 1200 or further. This means that any hacker/attacker that obtains a list of open NTP projects (e.g., by a tool like Metasploit or data from the Open NTP Project) can fluently induce a ruinous high-bandwidth, high- volume DDoS attack.

1.4 DDoS Attacks works:

1.5 Motivation behind DDoS attacks

DDoS attacks are snappily getting the most current type of cyber trouble, growing fleetly in both number and volume according to recent request exploration. The trend is towards shorter attack duration, but bigger packet-per-alternate attack volume.

Attackers are primarily motivated by:

- Ideology – So called " hacktivists" use DDoS attacks as a means of targeting websites they differ with ideologically.
- Business feuds – Businesses can use DDoS attacks to strategically take down contender websites, e.g., to keep them from sharing in a significant event, similar to Cyber Monday.
- Boredom – Cyber defacers, a.k.a., "script- kiddies" use pre-written scripts to launch DDoS attacks. The perpetrators of these attacks are generally wearied, would- be hackers looking for an adrenaline rush.
- Extortion – Perpetrators use DDoS attacks, or the trouble of DDoS attacks as a means of exacting plutocrats from their targets.
- Cyber warfare – Government authorized DDoS attacks can be used to both cripple opposition websites and an adversary country's structure.

1.5 Prevention from Attack:

Create a DDoS Response Plan

Your security platoon should develop an incident response plan that ensures staff members respond instantly and effectively in case of a DDoS. This plan should cover :

- Clear, step-by- step instructions on how to reply to a DDoS attack.
- How to maintain business operations.
- Go-to staff members and crucial stakeholders.
- Escalation protocols.
- Team liabilities.
- A roster of all necessary tools.
- A list of charge-critical systems.

Ensure High Levels of Network Security

Network security is essential for stopping any DDoS attack attempt. You can calculate on the following types of network security to cover your business from DDoS attempts. Firewalls and intrusion discovery systems that act as business-scanning walls between networks.

Antivirus and anti-malware software that detects and removes contagions and malware. Endpoint security ensures network endpoints (desktops, laptops, mobile bias,etc.) don't become an entry point for vicious exertion.

Web security tools that remove web- grounded pitfalls, block abnormal business, and search for given attack autographs. Tools that help spoofing by checking if a business has a source address harmonious with the origin addresses. Network segmentation that separates systems into subnets with unique security controls and protocols.

Guarding from DDoS attacks also requires high situations of network structure security. Securing networking bias enables you to prepare your tackle (routers, cargo-balancers, Domain Name Systems (DNS),etc.) for business harpoons.

Look Out for the Warning Signs

If your security team can quickly identify the traits of a DDoS attack, you'll take timely action and mitigate the damage. Common signs of a DDoS are:

- Poor connectivity.
- Slow performance.
- High demand for one page or endpoint.
- Crashes.
- Unusual traffic coming from one or a little group of IP addresses.

A spike in traffic from users with a typical profile (system model, geolocation, application program version, etc.). Remember that not all DDoS attacks accompany high traffic. A low-volume attack with a quick duration often goes under the radar as a random event. However, these attacks are often a test or diversion for a more dangerous breach (e.g such as ransomware). Therefore, detecting a low-volume attack is as vital as discovering a full-blown DDoS.

Do Not Overlook the DDoS Threat

DDoS threats aren't only becoming more dangerous, but attacks also are increasing in number. Experts predict the typical number of annual DDoS attempts will rise to fifteen .4 million by 2023.

Leverage the Cloud to Prevent DDoS Attacks

While using on-prem hardware and software to counter the DDoS threat is significant , cloud-based mitigation doesn't have an equivalent capacity limitation. Cloud-based protection can scale and handle even a serious volumetric DDoS attack with ease.

Limit Network Broadcasting

Limiting(or, where possible, turning off) broadcast forwarding is effective thanks to disrupting a high- volume DDoS attempt. Where possible, you can also consider instructing workers to disable echo and chargen services.

Continuous Monitoring of Network Traffic

Using continuous monitoring (CM) to research traffic in real-time is a superb method of detecting DDoS activity. The benefits of CM are:

- Real-time record ensures you detect a DDoS attempt before the attack takes full swing.
- The team can establish a robust sense of typical network activity and traffic patterns. Once you recognize how everyday operations look, the team easily identifies odd activities.

- Around-the-clock monitoring ensures the detection of signs of an attack that happens outside of office hours and on weekends.

Have Server Redundancy

You should host servers at data centers and carrier hotel facilities in different regions to ensure you do not have any network congestion or single points of failure. You can also use a content delivery network (CDN) for a distributed network of proxy servers . Since DDoS attacks work by overloading a server, a CDN can share the load equally across several distributed network servers.

1.6 Conclusion:

The goal of a DDoS attack is to chop off users from a server or network resource by overwhelming it with requests for service. While an easy denial of service involves one "attack" computer and one victim, distributed denials of service believe armies of infected or "bot" computers ready to perform tasks simultaneously.

This "botnet" is made by a hacker who exploits a vulnerable system, turning it into a botmaster. The botmaster seeks out other vulnerable systems and infects them using malware — most frequently, a Trojan virus. When enough devices are infected the hacker orders them to attack; each system begins sending a flood of requests to the target server or network, overloading it to cause slowdowns or complete failure, in this way the loss and damage of data are seen in the victim system.

1.7 Acknowledgement

It gives me great pleasure to present my Research paper on “ Prevention and Mitigation of DDoS in the Digital World ”. I would like to express my sincere thanks to all the teachers who helped us throughout. I would like to acknowledge the help and guidance provided by our professors in all places during the presentation of this research paper.

We are also grateful to, Head of Department. This acknowledgement will remain incomplete if we do not mention a sense of gratitude towards our esteemed Principal who provided us with the necessary guidance, encouragement and all the facilities available to work on this project.

1.8 Reference:

❖ www.google.co.in

❖ www.wikipedia.co.in

❖ https://phoenixnap.com/blog/prevent-ddos-attacks

❖ https://www.imperva.com/learn/ddos/ddos-attacks/

❖ https://www.researchgate.net/publication/

❖ https://www.quora.com/