|| Volume 2|| Issue 5|| 2017 || ISSN (Online) 2456-0774 INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

Towards Structured Understanding of DDoS Attacks: A Hierarchical Classification of Threats and Mitigation Techniques

Pradeep Kundlik Deshmukh

Associate Professor, Department of Computer Engineering,

Government College of Engineering, Awasari - Kh, Pune, Maharashtra, India pkdeshmukh9@gmail.com

---

Abstract: Denial of Service (DoS) attacks represent a significant danger and one of the most persistent security concerns in contemporary Internet infrastructure. DDoS attacks can be profoundly destructive, often occurring with minimal or no advance notice. A DDoS attack can rapidly incapacitate the processing and communication capacities of its target within a brief timeframe. The severity of the issue has necessitated the adoption of several defence methods to counter these attacks. Integrated systems, including web servers, database servers, and cloud computing servers, have been jeopardised by network adversaries. Managing a DDoS attack is tricky because it is hard to tell what traffic is legal and what is malicious especially when the traffic is caused by different scattered sources with different rates. As such, distributed denial-of-service (DDoS) attacks are better prevented proactively than addressed reactively. In this work, we present a hierarchical taxonomy of the tools used in the DDoS attack and a taxonomy of defense mechanisms used to alleviate such threats. The main goal is to structure both the attack and defense strategy systematically, and to enhance knowledge of the problem and remedy of the DDoS environment.

Keywords: *DDoS Attack, DDoS Tools, Taxonomy, Threats and Mitigation Techniques, Defense Mechanism*

I. INTRODUCTION

The DDoS attacks have turned out to represent a significant fright among the users of internet-based systems. These attacks are comparatively simple to execute and highly successful in incapacitating online resources and services. A DoS attack can be described as an attempt to deny a legitimate user entry to a network resource, including a web site, web service or computer system. A DDoS attack builds on this notion but organizes various systems which have been compromised to point at one system or network at a time thus increasing the effect. The targeted services are said to be primary victims whereas the affected machines are said to be secondary victims. Massive growth of the web has made DDoS attacks a significant concern in data center environments that have multiple servers in place. DDoS attack creates a large amount of packets sent by various sources, quickly exhausting the processing and communication resources of the target. The issue of network security is getting more intricate as the contemporary enterprise networks are constantly changing in line with the growing and dynamic structure of the Internet. The security risks to computer networks have increasingly become complex, more organized, and hard to detect every year. Such attacks are mostly aimed at overloading the target system and making it incapable of normal operation. A DDoS attack can be defined as an intentional effort towards stopping the legitimate users of a service. This may be by different means such as flooding a network to hinder normal traffic flow, (2) interrupting communications between systems to deny access to services, (3) denying access to specific users and (4) disrupting services to specific systems or individuals. The subsequent sections of the study will be organised as follows: Section 3 will present a discussion on the taxonomy of DDoS. Section 4 will delineate the taxonomy of defensive mechanisms. The document will be completed in section 5, where the references will be incorporated.

II.LITERATURE SURVEY

To develop a proper defence against DDoS attacks, it is important to understand every aspect of the attack and the defence in place. DDoS attacks and associated defence have been proposed to use various classifications.

Reference [1] delineates two primary categories of DDoS assaults based on the vulnerabilities they exploit: bandwidth depletion attacks and resource depletion attacks. Bandwidth depletion attacks aim to inundate the target network with excessive traffic, so obstructing the legal data flow to the target system. Resource depletion attacks, by contrast, are aimed at depleting the computational resources of the target (CPU, memory, connection bandwidth, etc.), which eventually causes the target to fail to respond to legitimate service requests.

In study [2], the researchers provide a range of criteria used to categorize DDoS attacks, which are the level of automation, vulnerabilities exploited, dynamics of the rate of attack, and the total impact.

In the same manner, study [3] addresses major issues like the automation level, attack network structure, vulnerability exploitation, impact of DDoS attacks and classifications according to the dynamics of attack intensity.

In paper [4], DDoS attacks are categorised into congestion-based, anomaly-based, and source-based approaches. The suggested countermeasures are categorised into destination network filtering and source network filtering strategies.

In [5], the authors present a taxonomy of denial-of-service (DoS) attacks categorised by factors including target type (e.g., firewall,

web server, router), resource consumption (e.g., network bandwidth, TCP/IP stack), and exploited vulnerabilities (e.g., software defects or system overload). This classification effectively captures the operational phase of the attack.

In [7], a methodology is presented for categorising DoS attacks based on attributes such as packet header information, transient ramp-up behaviour, and sophisticated techniques like spectral analysis.

TAXONOMY OF DISTRIBUTED DENIAL OF SERVICE ATTACKS

DDoS attacks occur in various forms, making it crucial to understand their classified characteristics in order to develop effective defense strategies. This study examines various attack kinds and categorises them accordingly. These characteristics are then incorporated into a structured taxonomy of DDoS attacks. The factors include degree of automation, exploited vulnerabilities, dynamics of attack rates, impact, communication mechanisms, scanning strategies, propagation mechanisms, relationship of packet contents with victim services, and rate of change mechanisms; these will be elaborated upon in depth subsequently.

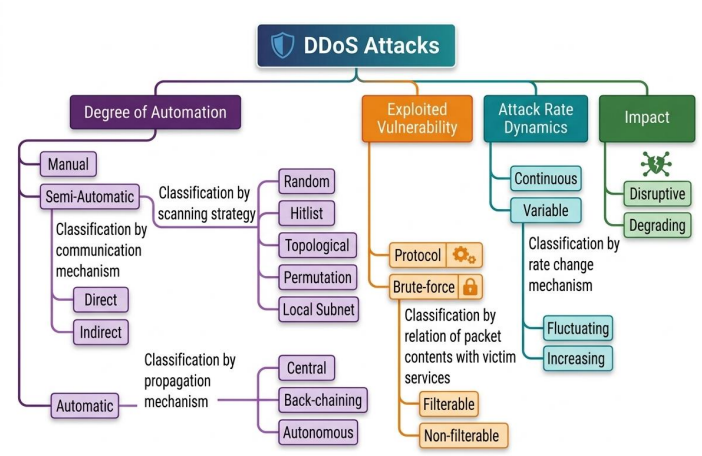

Fig.1 DDoS attacks Classification

A. *Classification By Degree Of Automation:*

Manual: The attacker first searched the remote workstations and identified vulnerabilities, then compromised the workstations, installed the malicious code, and further carried out the attack.

Semi-Automatic: An assailant generally use automated scripts to probe and infiltrate target systems, subsequently installing malicious software on them. Compromised computers are organised into a network where handler machines coordinate the assault by establishing parameters such as the attack type and the victim's address, and directing agent machines to initiate the transmission of malicious traffic. Interaction among components may occur either directly or indirectly. In direct communication, agents and handlers are predetermined to recognise each other, sometimes by embedding the handler's IP address into the attack code executed on the agents. Conversely, indirect communication utilises intermediary channels like Internet Relay Chat (IRC), enabling attackers to remotely manipulate agents. In such instances, pinpointing a solitary compromised agent may yield only restricted information, such as the IRC server and channel utilised, rather than the comprehensive attack network.

Automatic: Automated DDoS attacks simplify the execution process because real-time communication between the agent systems and the attacker is not necessary. When that occurs, the attack parameters, including the start time, attack type, duration and target address are hard-coded and stored in the attack script, allowing agents to execute the attack on their own.

B. *Classification By Exploited Vulnerability*

Bandwidth depletion: Under this category, the attacker floods the targeted network with data that is not requested. Flood amplification and flood methods are methods that have been tested and proven in this area. The process of a flood attack is produced by zombies that create an overload of traffic to a target system; therefore, filling the network bandwidth of a victim system with IP traffic. In these attacks, the system compromised can undergo reduced performance, system crashes, or a massive congestion of the network hence denying the legitimate users access to services. Attacks based on floods are usually implemented with such protocols as TCP, UDP, ICMP, and DNS.An amplification attack is a type of attack where a hacker or compromised systems send requests to a broadcast IP address, causing multiple devices in the network to respond at the same time to the target system. This significantly increases the volume of traffic directed towards the sufferer. Smurf and Fraggle attacks exemplify similar attacks.

Resource depletion: In such an attack, the attacker transmits packets, which take advantage of the vulnerabilities in the network protocols or which are poorly formed, which causes excessive utilization of the network resources and renders them inaccessible to legitimate users. Protocol exploit attacks use the particularities or poorly designed implementation of protocols to waste the resources of the victim. Popular ones are TCP SYN floods and PUSH+ACK attacks.

On the other hand, malformed packet attacks consist of transmitting poorly formatted or invalid packets to the target system in a bid to make it instable or crash. This may be packets that contain invalid IP address format or altered fields like the IP header OPTIONS field.

C. *Classification By Attack Rate Dynamic*

Continuous: When the initiation directive is received the agent machines will generate assault packets with maximum intensity. The discovery in this attack is very easy.

Variable: Variable-rate attacks can be designed to operate more discreetly by modulating their intensity, hence complicating detection and response efforts. These attacks dynamically alter their behaviour with time instead of having a fixed attack rate. The strategy usually involves two curves, which are growing and oscillating attack rates. In ascending attacks, the intensity is built

up gradually and gradually it washes the victim out and it takes time to note down the degradation as it gets carried out. In fluctuating attacks, the rate varies based on the target's activity, intermittently reducing or increasing traffic to remain less noticeable and bypass defensive systems.

D. Classification By Impact

Disruptive: In this category, the attack aims to completely disrupt or saturate the available network bandwidth, effectively cutting off all communication. Due to its highly disruptive and overwhelming nature, it is often referred to as a chaotic attack.

Degrading: A DDoS attack that leads to partial bandwidth use is termed a degrading attack. Detection is problematic because to the steady diminution of permissible bandwidth.

E. Classification By Scanning Strategy

Random: In random scanning, each hacked host autonomously queries random IP addresses throughout the address space. This approach can generate a significant amount of traffic, as multiple infected systems may target the same addresses simultaneously. An illustrative instance of this strategy is the Code Red (CRv2) worm, which utilised random scanning to disseminate swiftly among networks [12].

Hitlist*:* In hit-list scanning, a compromised device uses a predefined list of target IP addresses supplied from an external source. After identifying a vulnerable system, the device splits the original list, retaining one portion and transferring the other to the newly infected machine. This approach enables rapid propagation while minimizing overlap and collisions during the scanning process.

Topological: Topological scanning employs data from the breached host to detect further targets. All email worms utilise this strategy.

Permutation: In permutation scanning, all compromised systems utilise a shared pseudorandom sequence of the IP address space, with each IP address corresponding to a distinct index in the series. Each infected machine begins scanning from the position associated with its own IP address. If it encounters another infected machine, it selects a new random beginning point in the permutation, so reducing wasteful scanning and enhancing transmission efficiency.

Local Subnet*:* Local subnet scanning can be incorporated into any of the aforementioned methods to prioritise the detection of targets within the same subnet as the compromised host.

F. Classification By Propagation Strategy Base

Central: This is the framework for storing the attack code on a centralised server or a network of servers. Upon infiltration of the agent system, the code is subsequently retrieved from the central repository via a file transfer protocol [9].

Back-chaining*:* This process involves downloading the exploit code used to crack the system to the machine. The compromised machine thereafter serves as the source for the next phase of dissemination. The Ramen worm employed this approach. [10].

Autonomous*:* The method obviates the existence of an independent file transfer step and instead injects the instructions to be executed by the attack into the target system during exploitation. A specific instance of this method is a Warhol worm that adopted a comparable rapid propagation scheme. [11].

G. Classification By Relation Of Packet Contents With Victim Services

Filterable: Filterable attacks entail the exploitation of spoofed or non-critical traffic that is not essential to the normal running of the target and therefore filterable traffic can be identified and blocked more simply through firewalls or filtering tools. Examples would be UDP flood attacks or ICMP request floods to a web server, with the malicious traffic usually able to be filtered without incurring much effect on legitimate services.

Non-filterable: Non-filterable attacks are those involving traffic that seemingly contains legitimate traffic but can target vital services of the victim system. Consequently, it becomes hard to filter such packets, because any block on them would result in blocking of the legitimate users. Examples are common (HTTP request floods on web servers and DNS request floods on name servers) where it is hard to differentiate between malicious and legitimate traffic.

H. Classification Technique

The classification of Distributed Denial-of-Service (DDoS) attacks has been widely explored using both traditional analytical methods and machine learning-based techniques. In the work by S. M. Mousavi and M. St-Hilaire [15] the authors propose an early detection mechanism for DDoS attacks in Software Defined Networking (SDN) environments by analyzing traffic flow characteristics such as packet rate, flow duration, and entropy. Their approach emphasizes dynamic traffic classification, where abnormal patterns are distinguished from legitimate traffic using statistical thresholds and real-time monitoring, enabling rapid mitigation at the controller level. Similarly, Johnson and De [16] present a classifier-based detection framework that leverages supervised machine learning algorithms to categorize network traffic into normal and attack classes. Their study evaluates multiple classifiers, demonstrating that feature-based classification—using attributes like packet size, inter-arrival time, and protocol type—can significantly improve detection accuracy. Together, these studies highlight that modern DDoS classification techniques increasingly rely on hybrid approaches combining statistical analysis and machine learning models, facilitating more precise differentiation between benign and malicious traffic while supporting proactive defense mechanisms.

DDOS TOOLS

A plethora of attack tools, commonly termed "stressors," are readily accessible on the internet. Although several technologies fulfil legitimate functions—such as enabling security researchers and network managers to perform stress testing on their own systems—they may also be exploited for nefarious actions. Certain tools are designed to target specific layers of the protocol stack, whereas others support multiple attack vectors, enabling a broader range of attack strategies.

Attack tools can be broadly characterized into several groups [6]:

A. Low and slow attack tools

As the designation suggests, these assault tools utilise minimal data and function at a sluggish pace. Engineered to transmit minimal data over numerous connections to prolong the accessibility of ports on a designated server, these programs persist in using server resources until the targeted server can no longer sustain more connections. Surprisingly, low and sluggish attacks can often be effective even without utilising a distributed system such as a botnet, sometimes carried out by a single machine.

B. Application layer attack tools

These technologies largely focus on Layer 7 (Application Layer) of the OSI model, where internet-based interactions, such as HTTP requests, transpire. In these assaults, a nefarious entity can initiate an HTTP flood by transmitting a substantial volume of HTTP GET and POST requests to a targeted system. Since this traffic closely resembles legitimate user activity, it becomes difficult to distinguish between genuine and malicious requests, making detection and mitigation more challenging.

C. Protocol and transport layer attack tools

At the lower layers of the protocol stack, such tools utilise protocols like UDP to produce substantial traffic directed at a target server, as evidenced in UDP flood assaults. Though one source might not do much, they are normally performed as DDoS attacks where the attackers have multiple systems which are compromised to run the attack in parallel to increase its magnitude and performance.

A few commonly used tools include [8]:

i) Low Orbit Ion Cannon (LOIC)

LOIC (Low Orbit Ion Cannon) is a free-source program that was initially meant to stress test the network. It allows users to create traffic based on TCP, UDP, and HTTP protocols with an easy to use interface. Because of its popularity, browser versions were subsequently created which enabled it to be run directly out of web environments.

It operates by flooding a specific webserver with numerous requests in effect making the networks connection to a computer a water-gush of unwanted traffic. Nevertheless, it is typically not possible to produce enough simultaneous TCP, UDP or HTTP requests on one machine to saturate a server. Consequently, this kind of traffic is usually screened away and the proper user requests get to be processed without much interruption.

ii) High Orbit Ion Cannon (HOIC)

HOIC was created as an advanced successor of the LOIC with enhanced flexibility and customization. It mostly takes advantage of the HTTP protocol to execute more advanced and harder to detect attacks. HOIC permits an unauthenticated internet enemy to carry out DDoS) attacks by flooding the intended systems with enormous amounts of HTTP GET and POST traffic.

The tool can create up to 256 threads of attacks and it creates a continuous flow of traffic which can cripple normal operations in the servers and cause other legitimate requests to be queued. Moreover, HOIC also embraces the use of obfuscation and customization which complicates the ability of the conventional security controls and firewalls to detect and mitigate these attacks with a high degree of accuracy.

iii) Slowloris

Slowloris is an application utilized to execute a low and slow attack on a specified server, in addition to being a lethargic primate. Slowloris is astute in that it inflicts damage without significant resource use. It operates by creating many connections with the designated web server and sustaining them over an extended duration. It does this through constant transmission of partial HTTP requests none of which is ever finished. The servers that are hacked create more connections awaiting completion of each attack request. The simple, but advanced design of this attack requires the minimum bandwidth to carry out and only affects the target server web server with an insignificant effect on other services and ports.

iv) TOR's Hammer

ToR's Hammer was engineered to operate over the ToR network to obscure the attack and restrict mitigating efforts. This method is problematic since the ToR network is often sluggish, restricting the packet transmission rate and diminishing the tool's efficacy.

v) THC-SSL-DoS

This DDoS weapon, incorporated into Kali, distinguishes itself from typical DoS programs as it does not require much bandwidth and can be operated from a single system. It exploits vulnerabilities in SSL to disable the server. It is available for download at THC; however, if you are utilising Kali, it is already included.

vi) Pyloris

PyLoris is defined as a server testing utility. It can be utilised to execute denial-of-service assaults on a service. This utility can employ SOCKS proxies and SSL connections to execute a DOS attack on a server. It may include many protocols, such as HTTP, FTP, SMTP, IMAP, and Telnet. The latest version of the program includes an elegant and user-friendly graphical user interface. This tool directly targets the service, distinguishing it from conventional DOS attack tools.

vii) HULK (Http Unbearable Load King)

HULK is a powerful Denial of Service attack program that produces distinct requests for each created request to obscure traffic at a web server. This program utilises various ways to circumvent recognition by established attack patterns.

viii) R.U.D.Y (R-U-Dead-Yet)

R.U.D.Y. (R-U-Dead-Yet) is a "low-and-slow" attack tool designed to execute denial-of-service attacks through a simple, user-friendly interface. Rather of inundating a server with excessive traffic, it systematically depletes server resources by initiating several HTTP POST requests and maintaining those connections over an extended duration. This technique targets web forms on a website to exhaust server resources. After identifying available forms, R.U.D.Y. sends seemingly legitimate HTTP POST requests with an abnormally large *Content-Length* header. It then transmits the data at an extremely slow rate—often one byte at a time—forcing the server to maintain open connections and allocate resources for each request. In the long run, this slow drainage of resources may cause the exhaustion of resources and greatly affect the performance of the server because it will be unable to deliver legitimate user requests efficiently.

ix) XOIC

XOIC is a potent instrument capable of executing DOS attacks. It executes a Denial of Service assault on any server employing a designated IP address, user-defined port, and user-defined protocol. According to the developers of XOIC, it is superior in several aspects to LOIC. Similar to LOIC, it has a user-friendly graphic interface, which enables beginners to simply use this tool to attack various websites or servers.

x) GoldenEye

GoldenEye is a popular security testing tool. This device can cripple web servers of victims.

III.CONCLUSION

Distributed Denial-of-Service (DDoS) attacks continue to pose a critical threat to modern network infrastructures due to their distributed nature, dynamic behavior, and ability to mimic legitimate traffic. This survey highlights the importance of systematically classifying both attack mechanisms and defense strategies to better understand the evolving DDoS landscape. By organizing attacks based on factors such as degree of automation, exploited vulnerabilities, rate dynamics, and impact, a structured framework is established that aids in effective analysis and mitigation. Furthermore, the study emphasizes that proactive detection—achieved through continuous monitoring and analysis of network traffic patterns—is essential for identifying anomalies and distinguishing malicious activities from legitimate ones. The integration of statistical analysis, machine learning techniques, and intelligent traffic classification plays a vital role in enhancing detection accuracy and response time. Overall, a comprehensive taxonomy combined with advanced detection techniques significantly strengthens the capability to prevent and mitigate DDoS attacks in contemporary network environments.

IV.REFERENCES

[1] S. Specht, M. and R. B. Lee., Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures. Proceedings of the 17th International Conference on Parallel and Distributed.

[2] J. Mirkovic, J. Martin, et al., A Taxonomy of DDoS Attacks and DDoS Defence Mechanisms, Computer Science Department, University of California, 2002.

[3] U. Tariq, M. Hang, and et al., A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques., ADMA LNAI 4093, 2006 pp.1025 1036.

[4] L. Chen, T. Longstaff, K. Carley, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, Computers and Security, 2004.

[5] F. Kargl, J. Maier and M. Weber, Protecting web servers from distributed denial of service attacks, In Proceedings of 10th International World Wide Web Conference, 2001. Computing Systems, 2004, pp.543-550

[6] http://thehackerstuff.com/2017/08/07/top10-powerfull-ddos-tools-linux-windows/

[7] A. Hussain, J. Heidemann, C. Papadopoulos, A Framework for Classifying Denial of Service Attacks, ACM, 2003, pp.99-110

[8] https://www.cloudflare.com/learning/ddos/ddos-attack-tools/how-to-ddos/

[9] CERT Coordination Center, erkms and li0n worms, http://www.cert.org/incident_notes/IN- 2001- 03.html

[10] CERT Coordination Center, Ramen worm, http://www.cert.org/incident_notes/IN-2001-01. Html

[11] N. Weaver, Warhol Worm; http://www.cs. berkeley.edu/~nweaver/ warhol.html

[12] D. Moore, The spread of the code red worm (crv2), http://www.caida.org/analysis/security/codered/coderedv2_ analysis.xml.

[13] R. Stone. "CenterTrack: An IP Overlay Network for Tracking DoS Floods," In Proceedings of 9th USENIX Security Symposium, August 2000.

[14] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP Traceback," IEEE Infocom 2001.

[15] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 2015, pp. 77-81, doi: 10.1109/ICCNC.2015.7069319.

[16] kh, Johnson & De, Tanmay. (2015). An Approach of DDOS Attack Detection Using Classifiers. 10.1007/978-81-322-2550-8_41.