IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Distributed Denial of Service: Mitigation Solution and Techniques of Attack

Somaskandan[1], Agnes Sharon A[2] , Jayalakshmi S[3],Lydia P.S[4]
somaskandanm@gmail.com[1],agnes25anto@gmail.com[2],jayajaiu26@gmail.com[3],lydiaps42457@gmail.com[4]
Department of Information Technology,Panimalar Engineering college.

Abstract -A Distributed Denial of Service (DDoS) attack involves flooding a server with malicious traffic in order to make it unavailable. In the recent past, DDoS attacks have become the most tedious and inconvenient issue. The number and size of attacks has grown in recent years, from a few megabytes to hundreds of terabytes. It is difficult to detect these attacks effectively due to differences in attack patterns or new types of attacks. We devise new techniques for causing DDoS attacks and mitigation in this paper, which are shown to perform significantly better than existing techniques. We also classify DDoS attack techniques, as well as the techniques used to detect them, in order to provide a comprehensive overview of the problem
We also compare our attack module to a few other tools on the market.

Keywords: Distributed Denial of Service; Ping flooding; TCP SYN flooding; TCP RST attack; UDP flooding; HTTP GET flooding; Rate detection; Port checking; SYN thresholding; RST thresholding.

I. INTRODUCTION

One of the most dangerous security dangers is a denial of service (DoS) attack.
It's a way of denying service to the people who are supposed to use it. The severity of this attack is determined by the size of the l oss and the length of the attack.
DDoS attacks, which cause widespread harm, could be added to DoS attacks.
This attack can be carried out in a variety of ways, and the methodologies are detailed in this paper. The overburdening of the vict im's network, the exhaustion of resources, and hence the inaccessibility of the network to other clients would be the underlying as pect.
There are numerous assaults such as Man-in-the-Middle, Session Hijacking, Cross-Site Scripting, Spamming, and so on, but the Denial-of-Service attack is the most serious. This remark is backed up by a huge number of incidents. In a single afternoon, the websites of the US Department of Justice, the US Copyright Office, the FBI, and the MPAA were all taken down[10]. Over 5,635 persons utilized a basic tool called a Low Orbit Ion Cannon in these attacks. Even though China has one of the most effective filtering systems in the world, a DDoS attack brought down a portion of the Chinese internet in 2013. Another programme, Lizard Stresser, was used to bring down Xbox and PlayStation's online gaming systems[10][11]. In 2013, the spamhaus.org website was subjected to a 300 Gbps attack[11]. A 17-year-old Londoner admitted to carrying out the attack, demonstrating how simple it is to disrupt the internet using DdoS[11].
Furthermore, leveraging the flaws in internet protocols can be used to make services i-naccessible in a variety of ways. Any layer of the OSI or the TCP/IP protocol stack can be used in a DDoS assault.

II. DOS (FLOODING) ATTACK CLASSIFICATION

A.DDoS Flooding Attacks at the Network/transport level

TCP, UDP, ICMP, and DNS are among the internet protocols used in these assaults.
This is further divided into four categories:

A.i Flooding Assaults [1]

An attacker delivers a significant volume of irrelevant data to a network's bandwidth using a faked source IP address (e.g., UDP flood, ICMP flood, DNS flood, VoIP Flood and etc.).

A.ii Protocol Exploitation Flooding Attacks[1]

By exploiting certain features and vulnerabilities in the victim's protocol, the attacker consumes an excessive amount of the vict im's resources.
(For example, a TCP SYN assault)

A. iii Reflection-based flooding attacks[3]

When the attacker sends forged requests (e.g., ICMP echo requests) to the reflector instead of direct requests to the victim, t he victim's resources are depleted.

A. iv. Amplification-based flooding assaults[3]

For each message they receive, attackers generate big or several messages in order to magnify the flow towards the target, whic-h exploits the services.

B. Application-level DDoS flooding assaults: These attacks cause legitimate users' services to be disrupted by draining server res ources (such as sockets, CPU, RAM, disk/database bandwidth, and I/O capacity).
DDoS assaults at the application level typically require less bandwidth.

B.i Flooding Attacks Based On Reflection/Amplification[3]

This is akin to a network/transport level attack.
The DNS amplification attack, for example, uses both reflection and amplification techniques.

B.ii. HTTP Flooding Assaults[1]

This category includes four types of attacks:
Session flooding attacks, request flooding attacks, asymmetric attacks, and sluggish request/response assaults are all examples of asymmetric attacks.

DDoS attacks come in a variety of forms.
Only the most important are listed.

III IMPORTANT DOS ATTACK TOOLS

A . Hping[8]

hping is a TCP/IP packet assembler/analyzer with a command-line interfac-e. This utility can be used for firewall testing, adva nced port scanning, network testin-g utilising various protocols, and so on.

B. RUDY (R-U-Dead-Yet)

This submits large content using long-form components via HTTP requests.
This dynamic utility creates a user-friendly environment by merely using the targeted system's URL.

C. High Orbit Ion Cannon DDoS Tool[3]

This one features a graphical user interface.
HTTP queries are sent to the victim's server on a regular basis.
This programme can manage up to 256 sessions at the same time.

D. The LOIC (Low-Orbit Ion Cannon)[3][4]

By making HTTP requests at an extremely rapid pace, this attack tool causes the victim's system to fail. The master attacker's big gest flaw is that it has no hidden identity because it doesn't spoof handlers and agents' IP addresses.

E. Hyenae

This is a very flexible network packet generator that is used to check for network security vulnerabilities.

IV SCOPE AND CLASSIFICATION OF DDOS DEFENSE

When a DDoS attack is detected, the best solution is to manually resolve the issue by disconnecting the victim from the network. DDoS flooding attacks waste a lot of resources (bandwidth, processing time, etc.) not only at the target but also on the paths leadi ng to the target machine; as a result, the purpose of a DDoS defence system should be to detect them as quickly as feasible.
ADDoS flooding assault is comparable to
The tip of the funnel is formed by an attack that begins at the dispersed area (i.e. sourc-es)[1].
The victim is at the narrow end of a funnel that collects all assault flows.
As a result, detecting a DDoS flooding assault on the targeted machine is easier (destination). The problem with detecting an attac k at the source is that it's difficult for an individual source network to identify an assault unless it's a high-volume attack.
There is always a tradeoff between detection accuracy and distance from the source, as well as the mitigating method used[1].
Traffic Anomaly Detection, Behaviour Anomaly Detection, and Pattern Matching Detection are the three detection methodologies available.

V.NETWORK SETUP

In this configuration, there are three different sorts of machines. One will play the role of the victim (PC-1), the other will play the role of the attacker (PC-2), and the third will play the role of the legitimate client (PC-3) (PC-3). All of the PCs are runni ng Linux (Kali Linux OS [5]) and are connected to a NETGEAR router's Wi-Fi access point.

VI. IMPLEMENTATION

Python was chosen as the programming language for the attack and defensive module[6].

A. The Assault Module

The attack module includes a packet generator that generates IP headers based o-n the attacker's attack type. Inputs such as t he type of attack, source and destination information, speed, spoofing, and randomization parameters are entered through a PyQt4 -based GUI[7].

The following are the sorts of assaults used in this paper.

A.1.TCP SYN Flooding

This attack is designed to consume server CPU memory. In this assault, the attacker floods the system with DataTip SYN requests should be used to consume a big portion of the target's bandwidth. Server resources and, as a result, the link between them is disrupted. The intended and authentic customers When a customer wants to start a business, A sequence of messages are sent

through a TCP connection to a server. Traded. The procedure for creating a connection is referred to as Handshaking in three directions. In a SYN flood attack, the attacker sends out a large number of messages in a short period of time. Sends several SYN messages to the target's various ports Often, the source IP address is spoofing. The computer server, despite not being aware of the attack, he reacts to each attempt with a SYN-Each open port sends an ACK packet assuming it's a genuine SYN packet. The attacker either does not deliver the required ACK or does not receive it if the IP address is faked.SYN-ACK. In any case, the sufferer will have to wait. For a long time, it has not received acknowledgement of its SYN-ACK packet. The server does not shut down at this period. Connection by sending a RST packet before the connection time-out. As a result, the connection remains open. Prior to making the link When the current SYN packet expires, a new one will be sent. As a result There are a lot of half-open connections. It is for this reason that "Half -open" attacks are another name for SYN flood attacks. As the server's resources are depleted, service to the client will eventually cease. Clients who are legitimate will be rejected, and the server may even be shut down or crash

A.2 TCP RST Attack

A TCP reset attack involves resetting internet connections. A third party can monitor the connection between two machines. It is possible to use a computer and a faked packet with the TCP RST flag set. Messages can be sent to one or both endpoints. In the faked packet, the headers It needs to say that it came from an endpoint. This is the heading. Comprises the IP addresses of the monitoring computers as well as their port numbers If the TCP packets are tampered with, It is easy to effectively break any TCP connection can be kept track of

A.3 User Datagram Protocol (UDP) Flooding

The User Datagram Protocol (UDP) is a protocol that allows you to send and receive data over the Internet. Protocol that does not require a connection. The UDP is launching a flood attack. Sending a big number of UDP packets to a number of different ports the unfortunate. As a result, the target will: Determine whether any application is listening on that port; Check to see if such an application exists; Return an ICMP Destination as a response. Packet is unreachable. As a result, when a high number of such UDPs are present, the victim will get packages and will respond by sending a large number of ICMP packets, eventually rendering it unreachable other customers

A.4. Ping Flooding

A ping flood is a simple denial of service attack. An ICMP echo attack is a type of service attack in which the attacker sends a sequence of ICMP echo packets. Request packets to the victim (ping) The victim's response will be Echo reply packets from ICMP. This assault eats both incoming and outgoing data. Both outgoing and incoming bandwidth In the event that the victim If the machine is slow enough, the legitimate user may have a negative experience. There is a big latency.

A.5. HTTP GET Request Flooding

HTTP flood is a sort of DDoS assault in which the attacker attacks a web server by flooding it with HTTP GET requests.

B .Defense Module

The defensive module consists of an IP packet parser that decodes each field in an IP header, a DDoS detector programme that detects a DDoS attack using several methods that will be discussed later in this section, and lastly a mitigation programme that uses iptables for packet filtering. It shows the Source IP address, the Protocol used by the packet, the packet size, the Source and Destination Ports if they are accessible, the Traffic Status (Normal or DDoS), the Source IP Status (Connected or Blocked), and the Rate at which the Source is sending the packets.

Traffic anomaly detection and pattern matching are the detection methods used. They are:

B.1. Rate Detection

The rate of traffic from each source IP address is calculated in this section. If the rate exceeds the threshold, packets (packet types vary depending on protocol) from that IP address are dropped without being processed. TCP SYN flood, UDP flood, HTTP GET flood, and Ping flood assaults are all mitigated using this strategy.

B.2. Port Checking

The packets' source and destination ports from each source IP address are checked here. UDP packets from that IP address are dropped without being processed if the originating IP uses more than a specified number of source and/or destination ports. This technique is used to protect against UDP flood attacks.

B.3. SYN Thresholding

The number of SYN and ACK packets received from each source IP is calculated in this section. TCP SYN packets from that IP address are dropped without being processed if the difference between SYN and ACK packets is greater than the threshold. TCP SYN flood attacks are mitigated using this strategy.

B.4. RST Thresholding

RST packets from that source are deleted if the number of RST packets received for a successful TCP three-way handshake exceeds a threshold.TCP RST flood attacks are mitigated using this strategy.

C. Algorithm

The assault and defence modules' algorithms are displayed.The source code for attack and defense module can be found at .

C.1. Attack Module Algorithm

Step 1: Accept inputs via the attack tool's graphical user interface.
Step 2: When the 'Lock' button is pressed, the IP header fields are initialised.
Step 3: Jump to the appropriate attack programme depending on the type of attack selected.

Step 4: Create an assault packet.
Step 5: The assault packet should be sent.
Step 6: If the 'Stop' button is hit, proceed to Step 7; otherwise, proceed to Step 4 with a delay or without a delay, depending on the rate selected.
Step 7: Stop sending attack packets and show the Summary instead.

C.2. Defense Module Algorithm

Step 1: Accept a packet that has arrived. Break if the IP address is trusted. Otherwise, proceed to Step 2.
Step 2: Parse the packet and save the necessary fields in their appropriate variables.
Step 3: To detect any anomaly, use the detection procedures outlined above.
Step 4: If the packet is genuine, proceed to Step 6; otherwise, proceed to Step 5.
Step 5: Drop the packet without processing it any further.
Block the IP address.
Step 6: If the detection has been halted, proceed to Step 7; otherwise, return to Step 1.
Step 7: Put an end to the detection

Each IP address is assigned a Trust Score by the defensive module.
If the value is high enough, the IP address is regarded trustworthy and whitelisted.After each time period specified in the configuration file, the whitelisting and blacklisting process is repeated.The configuration file contains all of the necessary information for detecting any irregularities. The defence module keeps track of all incidences in a log file and displays a live record.It also saves all of the received packets to a pcap file.

VII. RESULTS AND ANALYSIS

A. ATTACK RESULTS AND ANALYSIS

A.1. Ping Flooding

The round trip delay for ping packets provided by the legitimate client will rise as the attack progresses, and when the victim's CPU and/or bandwidth reaches its maximum, the client will receive a Destination unreachable message.The percentage packet loss is used to assess performance.

The attack module's performance improves as the packet loss increases.

A.2. TCP SYN Flooding

When we start the attack, we send SYN + ACK packets to the target for every SYN packet.

A.3. TCP RST Attack

We need to intercept all traffic to and from the target in order for our attack to operate. ettercap has successfully executed a Man-In-The-Middle (MITM) attack.Ettercap[9] is a complete man-in-the-middle attack package. It can sniff live connections, filter content on the fly, and perform a variety of other activities. To achieve an MITM, ARP poisoning is used.

Ettercap command to start an MITM – 'ettercap -T -M ARP

Every time a connection is attempted, this attack resets the connection. The client was unable to view the webpage housed on the victim's computer.

A.4. UDP Flooding

The victim's bandwidth uses during the attack, as well as performance comparisons with hping3 and hyenae.Number of packets sent per second is used for comparison (size of the packets being equal).

A.5. HTTP GET Flooding

An HTTP GET request is sent after a three-way handshake has established a connection. This is done repeatedly in order to overwhelm the victim with requests.

B. DEFENSE RESULTS AND ANALYSIS

B.1. Ping Flooding

Incoming and outgoing traffic bandwidth at the target before and after mitigation of the attack. Once the victim recognises the assault, it stops delivering ICMP echo reply packets by simply dropping the requests as they arrive.

B.2. TCP SYN Flooding

Outgoing bandwidth is reduced to zero once an assault is detected. This is because once the victim realises it is under assault, it begins dropping all SYN packets. For HTTP GET flooding, a similar result can be obtained. The attacker is unable to send a GET request without the three
way handshake.

B.3. TCP RST Attack

The detector is used by both the client and the destination machines to drop the RST packets provided to them by the man in the middle.

B.4. UDP Flooding

Because UDP is a connectionless protocol, the best the detector can do is delete UDP packets from the same source IP address with various destination Ports without delivering ICMP Port Unreachable warnings.

VIII. CONCLUSION AND FUTURE SCOPE

A .CONCLUSION

This article provides sufficient information to carry out Denial of Service attacks. It discusses numerous DDoS assault tactics and attack tools, as well as how to build a DoS attack tool from the ground up. It also recommends basic mitigation measures and how to put them into action in order to fight against the attacks.

This study demonstrates the network's damaging impacts that can be created by intermediate programming and networking abilities, as well as the need of having such knowledge to limit those effects.

FUTURE SCOPE

The attack and mitigation mechanisms described in this paper are only the beginning; more techniques are required. To harden the network's strength and security, advanced ways for mitigating such assaults employing machine learning techniques must also be introduced.

When IPv6 is used, more problems develop. Optional headers in IPv6 include the Routing header, Encapsulation Security Payload Header, Authentication header, and Mobility header.
Although IPv6 delivers improved security through authentication, encryption, and encapsulation mechanisms, it also introduces significant challenges.

When compared to IPv4, IPv6 is estimated to allow for 80 percent more powerful DoS attacks. As a result, future effort should concentrate on IPv6 security, which can be extended to MANETs.

REFERENCES

[1]S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,"
in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046- 2069, Fourth Quarter

[2]S. S. Kolahi, A. A. Alghalbi, A. F. Alotaibi, S. S. Ahmed and D. Lad, "Performance comparison of defense mechanisms against TCP SYN flood DDoS attack," 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, pp. 143-147.

[3]B. Nagpal, P. Sharma, N. Chauhan and A. Panesar, "DDoS tools: Classification, analysis and comparison," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, pp. 342-346.

[4]Mahadev, V. Kumar and K. Kumar, "Classification of DDoS attack tools and its handling techniques and strategy at application layer," 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall), Bareilly, pp. 1- 6.

[5] Kali Linux Operating System - Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and networksecurity assessments. [Online]. Available : https://www.kali.org/

[6] Python programming language. [Online] Available: https://www.python.org/
[7] Python bindings for Qt application framework. [Online]. Available: https://riverbankcomputing.com/software/pyqt/intro
[8] Hping security testing tool. [Online]. Available: http://hping.org/
[9] Ettercap Man-In-The-Middle-Attack tool. [Online]. Available: http://ettercap.github.io/ettercap
[10] Spamhaus attack. [Online]. https://blog.cloudflare.com/the-ddos-that-

almost-broke-the-internet/

[11] Xbox Live and Sony PlayStation attack. [Online]. https://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/P

[12]M. Sumithra and Dr. S. Malathi, "3D Densealex NET Model with Back Propagation for Brain Tumor Segmentation", International Journal OfCurent Research and Review, Vol. 13, Issue 12, 2021.

[13]M. Sumithra and Dr. S. Malathi, "Segmentation Of Different Modalitites Using Fuzzy K-Means And Wavelet ROI", International Journal Of Scientific & Technology Research, Vol. 8, Issue 11, pp. 996-1002, November 2019.

[14]B.Buvaneswari and Dr.T. Kalpalatha Reddy,"EEG signal classification using soft computing techniques for brain disease diagnosis",Journal of International Pharmaceutical Research ,ISSN : 1674-0440,Vol.46,No.1,Pp.525-528,2019.

[15]Sharanyaa, S., P. N. Renjith, and K. Ramesh. "An Exploration on Feature Extraction and Classification Techniques for Dysphonic Speech Disorder in Parkinson's Disease." In *Inventive Communication and Computational Technologies*, pp. 33-48. Springer, Singapore, 2022.

[16]K. Sridharan , and Dr. M. Chitra "Web Based Agent And Assertion Passive Grading For Information Retervial", ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 16, September 2015 pp:7043-7048

[17]Sharanyaa, S., S. Lavanya, M. R. Chandhini, R. Bharathi, and K. Madhulekha. "Hybrid Machine Learning Techniques for Heart Disease Prediction." *International Journal of Advanced Engineering Research and Science* 7, no. 3 (2020).