Distributed Denial of Service attack Techniques and Defense Mechanisms

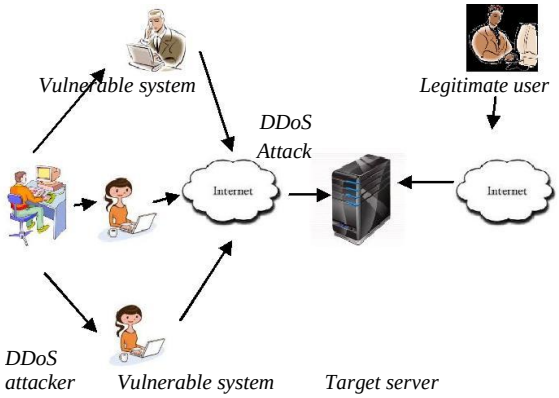
G. Nazia Sulthana[1], V.K. Sharma[2]
Research Scholar[1], Professor[2], Department of Computer Science and Engineering
Bhagwant University, Ajmer, India

Abstract: *A distributed denial of service (DDOS) is an attack which makes a computer system or network incapable of providing normal services. DDoS attacks are one of the oldest threats on the IT security landscape. They can be used to bring down Internet-facing business services and cause general havoc for any organization and its IT security staff. But despite having their roots in the past, DDoS attacks are still prevalent and devastating today, making the case to implement a dedicated mitigation solution to combat them stronger than it's ever been. The rigorous survey presented in this paper describes a platform for the study of methods of DDoS attacks and their defense mechanisms.*

Keywords:- *DDoS-Distributed Denial of Service, vulnerable systems, Traffic Detection, Bandwidth Exhaustion, Resource Exhaustion.*

I. INTRODUCTION

Distributed Denial of Service (DDoS) attacks are a type of attack launched by perpetrators so that Internet resources and services are unavailable to legitimate users. To set up a DDoS attack network, the perpetrators or the attackers gain accessibility of large number of systems in the internet by exploiting their software vulnerabilities. These vulnerable systems are then used to initiate an organized attack against one or more victim systems [1, 2].



Vulnerable system

Fig. 1: DDoS attack scenario

The scenario shows the DDoS attacker first selects the vulnerable systems which will be used to perform the attack [5]. Then DDoS attackers exploit the vulnerabilities of the selected systems and incorporate the attack code in such a way that the attack code can be sheltered from discovery and deactivation. After recruiting enough machines the attackers use the communication channels to activate the coordinate attack by sending a large number of requests through the network. The target server's network gets busy and then it will not respond to its genuine users and will not be able to provide services to the legitimate users.

II. LITERATURE REVIEW

A. *Why DDoS?*

The DDoS attackers perform the attacks for one or the other following reasons [3].

1) Profit: The one and easiest motivation is the aspiration to get profit from the targeted organization. The DDoS Attackers know that they can often extract money from an organization using the threat of a DDoS attack.
2) Hack: Hacking has become increasingly popular and DDoS attack actions are often performed by groups that want to damage organizations or individuals that disagree with their social, political or religious beliefs.
3) Dispute: DDoS attacks are used during disputes between one another. Online gamers often use short DDoS attacks to disturb their rivals.
4) Involuntary Outages: Unintended floods of traffic to a website can often have the same effect as that of DDoS. This may happen when a smaller organization is marked in a major part of news and users flock to their websites as a result.

B. *Outcomes of DDoS:*

1) Income Loss: Internet dependent Businesses and services are undoubtedly has the most to lose in case of a DDoS attack.
2) Production Loss: An organization's workforce

unavoidably experiences a nontrivial drop in production when business systems are down.

3) Impact and Cost: Any organization's period of downtime affects its bottom line. Often prolonged characteristic of DDoS attacks are damaging for organizations. When a DDoS attack is encountered the companies need to concern themselves with other important considerations along with the obvious financial implications [3].
4) Popularity Damage: Popularity damage is a significant DDoS attack consequence. After a DDoS attack customers lose confidence in the brand and think twice before shopping there in the future[3].

III. DDOS ATTACK TECHNIQUES

The DDoS attacks can be carried out by collapsing two major factors: bandwidth and network resource. Collapsing the bandwidth is usually termed as bandwidth exhaustion. This kind of attack is designed to burst the target network with useless traffic that avoids genuine traffic from reaching the target/victim system. Collapsing the network resources is usually termed as resource exhaustion. This kind of attack is designed to bind the resources of a target system, so that resources are unavailable to the genuine users furthermore.

The attacks on bandwidth exhaustion can be categorized further as shown below [1].

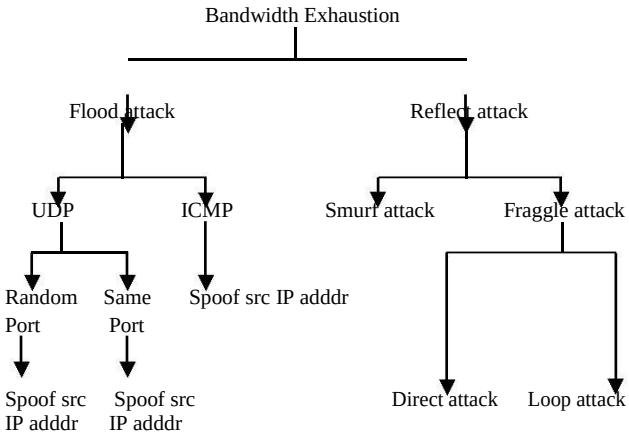


Fig. 2: Classification of bandwidth exhaustion attacks

- **Flood Attack:** In this type of attack, vulnerable systems burst the **target** system directly with IP traffic. The huge amounts of traffic exhaust the target systems network bandwidth so that other valid users are not able to access the service or experience severe slow down. In these attacks normally, ICMP echo request/reply and UDP packets are used [8].

ICMP echo request/reply: A flow of ICMP packets are passed to a target system's IP address which make the target system to reply and the combination of such traffic saturates the bandwidth of the target system's network connection. The source IP address may also be spoofed.

UDP floods: A flow of UDP packets are passed to the target system's IP address which causes the target system to process the incoming packets to determine which applications have requested data. If the target system is not running any applications on the specified port, then the target system will send back an ICMP packet to the sending system indicating a message "destination port unreachable" [8].

Often, the DDoS attacking tool spoofs the source IP address of the attacking packets. This aids to hide the identity of the vulnerable systems and it also ensures that return packets from the target system are not sent back to the vulnerable systems, but to another system with the spoofed address.

- **Reflect Attacks:** In a DDoS reflect attack, a sending system is allowed to specify a broadcast IP address as the destination address rather than a specific address which instructs the routers servicing the packets within the network to pass them to all the IP addresses within the range of broadcast address.

Smurf Attacks: In a DDoS Smurf attack, a network amplifier is sent packets with the return address spoofed to the target system's IP address by a DDoS attacker [14]. These packets request the network amplifier to generate an ICMP ECHO REPLY packet [9,10]. The amplifier sends the ICMP ECHO REQUEST packets to all of the systems within the broadcast address range and each of these systems will return an ICMP ECHO REPLY to the target system's IP address.

Fraggle Attacks: in a DDoS Fraggle attack the attacker sends UDP ECHO packets to a network amplifier. The UDP Fraggle packet will address the character generator [11] in the systems reached by the broadcast address to generate a character to send to the echo service in the target system, which will resend an echo packet back to the character generator and the process repeats.

The attacks on resource exhaustion can be categorized further as shown below [1].

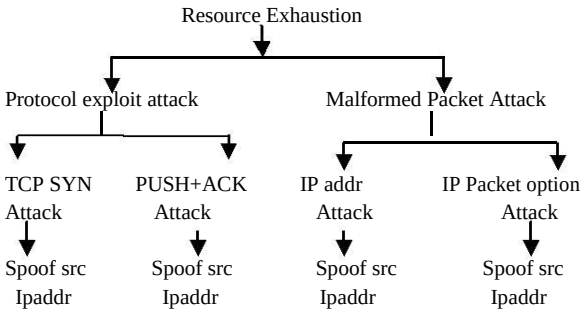


Fig 3: Classification of Resource Exhaustion Attacks

- **Protocol Exploit Attacks:** These type of attacks make use of loopholes in the communication protocol to perform the DDoS attacks.

TCP SYN Attack: in this TCP SYN attack the sender sends large amount of TCP SYN requests with spoofed source address to the receiver. If these half-open connection tie up resources on the server those resources may end up denying services to the valid user connection requests.

The PUSH + ACK Attack: In this attack the attacking agents send TCP packets to the target system with the PUSH and ACK bits set to one which instruct the target system to flush all data in the TCP buffer and to send an acknowledgement when done. If this process is repeated with multiple agents the receiving system cannot process large volume of incoming packets and it will crash.

- **Malformed Packet Attack:** This attack is referred as ping of death (POD) is a type of attack on a system that involves sending a malicious ping to a computer. The two types of malformed packet attacks are IP address attack and IP packet option attack.

IP address attack: In this attack the IP packet has both source and destination IP addresses as same to confuse the operating system of the target system and to crash it.

IP packet options attack: In this attack the optional fields within an IP packet are randomized and all quality of service bits are set to one so that additional processing time is used by target system to analyze the traffic. To bring down the processing capability of the target system this attack is multiplied using enough agents.

IV. DDOS ATTACK TOOLS

A number of common software characteristics are used as a DDoS attack tool. These characteristics include agents setup and activation, communication between attackers, handlers and agents and operating systems (OS) supported [3].

A. ***Agent setup and Activation:*** Attackers use either active or passive methods to install malicious code onto a vulnerable system.

Passive method: In Passive methods the vulnerable systems unknowingly causes the DDoS agent software to be installed by opening a corrupted file or visiting a bugged web-site.

Corrupt file: The target system becomes infected with the malicious code [14] when it tries to open corrupted file. The corrupt file is generated as a text file with the name of the binary executable code and a DDoS agent software embedded within it [17].

Bugged web-site: This is created with commands or code to catch a target system with the help of loophole found on web browsers [16]. The DDoS agent code is stealthily installed when the target system's web browser opens the web page.

Active method: In Active method first the attacker scans the network to find systems with known vulnerabilities. After identifying such systems, scripts are run to enter into the system and DDoS agent software is installed stealthily.

Trojan horse program: This is a vulnerable program [14] which appears to perform a useful function, actually contains hidden code that either executes malicious acts or provides a backdoor for unauthorized access to some privileged system function.

Buffer overflow: This is common software vulnerability. A buffer overflow is an attack that sends more data into the buffer than the size of the buffer. This causes the extra data to overwrite other information adjacent to the buffer in the memory stack, such as a procedure return address [15]. This can cause the computer to return from a procedure call to malicious code included in the data that overwrites the buffer. This malicious code can be used to start a program to provide access to the target system so that the attacker can install the DDoS Agent code.

B. Communication Network:

The DDoS attack agent, vulnerable system and target systems use ICMP, TCP, and/or UDP communication

protocols. In DDoS agent attacks encrypted communications might be used either between the target system/vulnerable system and/or between the vulnerable system-DDoS attack agents. In IRC-based DDoS attacks either a public, private, or secret channel might be used to communicate between the DDoS attack agents and the vulnerable systems. DDoS *agent activation* can be done in two ways. The DDoS attack agents may actively poll the vulnerable systems or IRC channel for instructions, or DDoS attack agents will wait for communication from either the vulnerable system or the IRC channel.

C. *Supported Operating Systems :*

DDoS attack tools are typically designed to be compatible with different operating systems (OS) such as Unix, Linux, Solaris, or Windows. The DDoS attack agent code is designed to support an OS of a server or workstation at either a corporate or ISP site.

V. DDOS DEFENSE MECHANISMS

A number of defense techniques exist to defend against the DDoS attack which can be broadly classified into preventive, defensive and post-active methods.

A. *Preventive methods:*

1) Prevent vulnerable systems: First the formation of DDoS attack network is to be prevented including vulnerable systems then DDoS attack agents are to be detected [13] and neutralized. The computing systems central software and hardware must provide protection against inclusion of DDoS agent code through buffer overflow violations [18]. The traffic patterns and communication protocols between vulnerable systems and target system or vulnerable systems and DDoS attack agents are studied to find network nodes that might be infected with DDoS attack code. Since there are far fewer DDoS handlers deployed than agents, shutting down a few handlers can render multiple agents useless thereby neutralizing a DDoS attack.
2) Security of systems: To prevent DDoS attacks the individual or network service providers should use rigid policies such as fragmenting the network into domain and applying token systems on security to be more secure so that the attackers find it difficult to capture vulnerable systems.
3) Identify legitimate user: Since DDoS attacks often use spoofed IP address there is a good probability that the source address of a valid user on a specific sub-network will not be used as the source address of DDoS attack packet. IP packet headers leaving a network are verified to see if they match certain criteria to be routed outside of the sub-network from which they originated Otherwise the packets will not be sent.

B. *Defensive Techniques:*

These are described in two phases: Detection and Mitigation. To enhance the security of the network or the server, the attack must have to be recognized and take further step to stop these attacks.

1) Detection can be done in two ways. Signature based detection and anomaly based detection.

   Signature based detection*:* In a network the entrance router or switch is provided with the pattern of incoming packets [19], such that fields like port number, identification number etc are checked in the incoming packets to detect the attack.

   Anomaly based detection: This method observes the normal behavior of the traffic and compares it with the incoming traffic to evaluate the difference to detect the DDoS attack.

2) Techniques for mitigation are divided into two categories: fault tolerance and Quality of Services.
   Fault tolerance can be maximized by duplicating its resources and diversifying its access points so that a network can continue to offer its services by other network link even after congesting one network link [7].
   Quality of service *(QoS)* assures ability of a network to deliver predictable output and service for certain type of application and traffic under attack situation.

C. *Post-active techniques:*

If traffic pattern data is stored during a DDoS attack, this data can be analyzed post-attack to look for specific characteristics within the attacking traffic. This characteristic data can be used for updating countermeasures to increase their efficiency and protection ability.

1) **Traceback**:

It is a technique for locating the agent machines

making the DDoS attacks. It helps a victim to identify the network paths traversed by attack traffic without requiring interactive operational support from internet Service Providers [6, 21]. Additionally, when the attacker sends vastly different types of attacking traffic, this method assists in providing the victim system with information that might help develop filters to block the attack.

2) Traffic Pattern Analysis:

If traffic pattern data is stored during a DDoS attack, this data can be analyzed post-attack to look for specific characteristics within the attacking traffic [22]. This characteristic data can be used for updating load balancing and throttling countermeasures [20] to increase their efficiency and protection ability. Additionally, DDoS attack traffic patterns can help network administrators develop new filtering techniques for preventing DDoS attack traffic from entering or leaving their networks.

3) Event Logs:

Network administrators can keep logs of the DDoS attack information in order to do a forensic analysis and to assist law enforcement in the event the attacker does severe financial damage. Using both Honeypots as well as other network equipment such as firewalls, packet sniffers, and server logs, providers can store all the events that occurred during the setup and execution of the attack. This will allow the network administrators to discover what type of DDoS attack (or combination of attacks) was used.

VI. CONCLUSION

DDoS attacks are quite advanced and use powerful methods to attack a network system to make it either unusable to the legitimate users or downgrade its performance. They are increasingly mounted by professional hacks in exchange for money and benefits. This paper gives a survey of various kinds of DDoS attacks techniques and methods to handle them. It helps to give a basic idea of the techniques to the researchers who want to get started his research work from network security.

REFERENCES

[1] Stephen M. Specht, Ruby B. Lee, "Distributed Denial of Service:Taxonomies of Attacks, Tools and Countermeasures," Electrical Engineering, Princeton University Princeton, NJ 08544.

[2] J. Mirkovic, P. Reiher, "A Taxonomy of DDoS Attack and DDoS defense Mechanisms", ACM SIGCOMM Computer Communications Review,Vol. 34, Issue 2, pp. 39-53, April 2004.

[3] "DDoS Protection: Keeping Your Business Safe" Cogeco Peer-1, http://www.cogecopeer1.com/wp-content/uploads/2016, Jan-2016.

[4] Manish Gupta, Gayathri Gopalakrishnan, and Raj Sharman, "Countermeasures against Distributed Denial of Service", 11th annual symposium on information assurance (Asia'16) June 8-9 2016 Albany, NY.

[5] Sakshi Kakkar, Dinesh Kumar, "A Survey on Distributed Denial of Services (DDOS)", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5(3), 2014.

[6] Yang Xiang, Ke Li, and Wanlei Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics", IEEE Transactions on Information Forensics and Security, Vol. 6, No. 2, June 2011.

[7] Ahmad Sanmorino, Setiadi Yazid, "DDoS Attack Detection Method and Mitigation Using Pattern of the Flow", International Conference of Information and Communication Technology (ICICT) 2013.

[8] Paul J.criscuolo, "Distributed Denial of Service Trinoo,Tribe Flood Network, Tribe Flood Network 2000,And Stachelrdaht CIAC-2319",Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev1., Lawrence Livermore National Laboratory,Feb 14,2000

[9] TFreak. "smurf.c", www.phreak.org. Oct 1997. www.phreak.org/archives/exploits/denial/smurf.c (6 May 2003).

[10] Federal Computer Incident Response Center (FedCIRC), "Defense Tactics for Distributed Denial of Service attacks".Washington, DC, 2000.

[11] TFreak,"fraggle.c"www.phreak.org/archives/exploits/denial/fraggle.c (6 May 2003).

[12] Martin, Michael J., "Router Expert: Smurf/Fraggle Attack Defense Using SACLS", Networking Tips and Newsletters, www.searchnetwork.techtarget.com. Oct 2002. http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci85
6112, 00.html (6 May 2003).

[13] "Nmap Stealth Port Scanner Introduction", Insecure.org. August 2002. http://www.insecure.org/nmap/. (8 Apr 2003).

[14] Colon E. Pelaez and John Bowles, "Computer Viruses",System Theory, 1991, Twenty-Third Southeastern Symposium,pp. 513-517, Mar 1999.

[15] CrispinCowan, Perry Wagle, Calton Pu, Steve Beattie, and Jonathan Walpole, "Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade", DARPA Information Survivability Conference and Exposition, 2000. Vol. 2 pp. 119-129, 2000.

[16] Microsoft "How to Write Active X Controls for Microsoft Windows CE2.1", Microsoft Corporation. Jun 1999. http://msdn.microsoft.com/library/default.asp?url=/library/enus/dnce21/html/activexce.asp. (5 Apr 2003).

[17] Dancho Danchev. "The Complete Windows Trojans Paper", BCVG Network Security. Oct 22, 2002. http://www.ebcvg.com/articles.php?id=91. (9 Apr 2003).

[18] Ruby B Lee, David Karig, Patrick McGregor and Zhijie Shi, "Enlisting Hardware Architecture to Thwart Malicious Code Injection", Proceedings of the International Conference on Security in Pervasive Computing (SPC-2003), LNCS 2802, pp.237-252, Springer Verlag, March 2003.

[19] Joao B. D. Cabrera, Lundy Lewis, Xinzhou Qin, Wenke Lee, Ravi K. Prasanth, B. Ravichandran, and Ramon K. Mehra, "Proactive Detection of Distributed Denial of Service AttacksUsing MIB Traffic Variables – A Feasibility Study", Integrated Network Management Proceedings, pp. 609-622, 2001.

[20] David K. Yau, John C. S. Lui, and Feng Liang, "Defending Against Distributed Denial of Service Attacks with Max-minFair Server-centric Router Throttles", Quality of Service, 2002Tenth IEEE International Workshop, pp. 35-44, 2002.

[21] Vern Paxon, "An Analysis of Using Reflectors for Distributed Denial of Service Attacks", ACM SIGCOMM Computer Communication Review, Vol. 31, Iss. 3, Jul 2001.

[22] Thomas E. Daniels and Eugene H. Spafford, "NetworkTraffic Tracking Systems: Folly in the Large?", Proceedings of the 2000 Workshop on New Security Paradigms, Feb. 2001.