International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 10 | Oct -2017 www.irjet.net p-ISSN: 2395-0072

Denial of Service Attack Defense Techniques

Sheetal P.Desai[1], Priti R. Hadule[2], Prof. Arundhati A. Dudhgaonkar[3]

[1,2] Dept. of Master of Computer Application,MGM's Jnec college, Maharashtra, India
[3] Assistant Professor, Department of MCA, MGM's Jnec college, Maharashtra, India

---

Abstract - Denial of service attack(DOS attack)typically flood servers system or network with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them [1].It is the internet base attack, Denial-of-service attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer system ,devices or other network resources.[2]. In this paper goal is review on defense techniques
against denial of service attack .

***Key Words*: Denial of service attack, Defence techniques, Types of attack.**

1.INTRODUCTION

A denial-of-service (DOS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled

1.1 Symptoms:

- 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 (this type of DoS attack is considered an e-mail bomb).
- Disconnection of a wireless or wired internet connection long-term denial of access to the web or any internet server.

1.2 Types of denial of service attacks:

1. SYN flood

A SYN flood is a type of DOS attack in which an attacker sends a series of SYN requests to a target's system in an attempt to use vast amounts of server resources to make the system unresponsive to legitimate traffic.

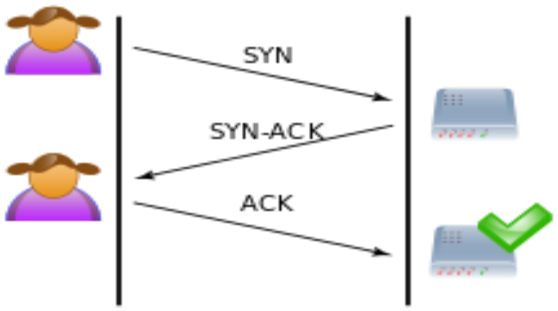


Fig 1.1 Normal SYN Flood

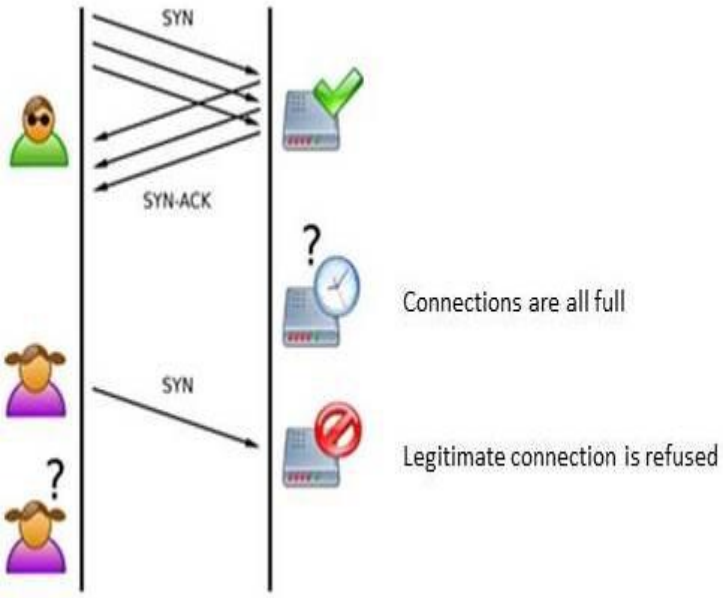


Fig1.2 SYN Flood

2. Teardrop attacks

A teardrop attack involves the hacker sending broken and disorganized IP fragments with overlapping, oversized payloads to the victims machine. The intention is to obviously crash operating systems and servers due to a bug in the way TCP/IP fragmentation is re-assembled. All operating systems many types of servers are vulnerable to this type of DOS attack, including Linux

3. Internet Control Message Protocol (ICMP) flood

Internet Control Message Protocol (ICMP) is a connectionless protocol used for IP operations, diagnostics, and errors. An ICMP Flood – the sending of an abnormally large number of ICMP packets of any type (especially network latency testing "ping" packets) – can overwhelm a target server that attempts to process every incoming ICMP request, and this can result in a denial-of-service condition for the target server.

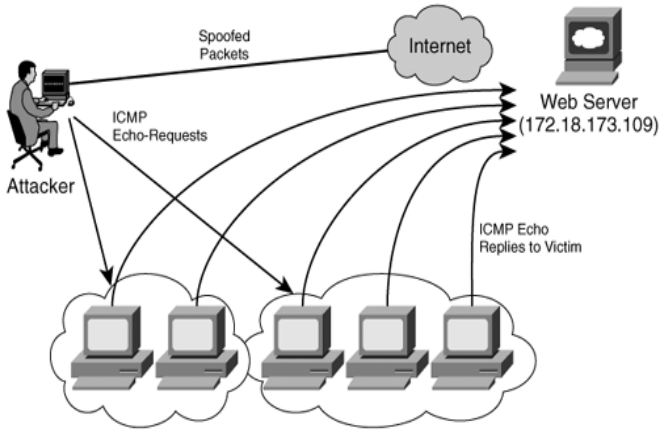
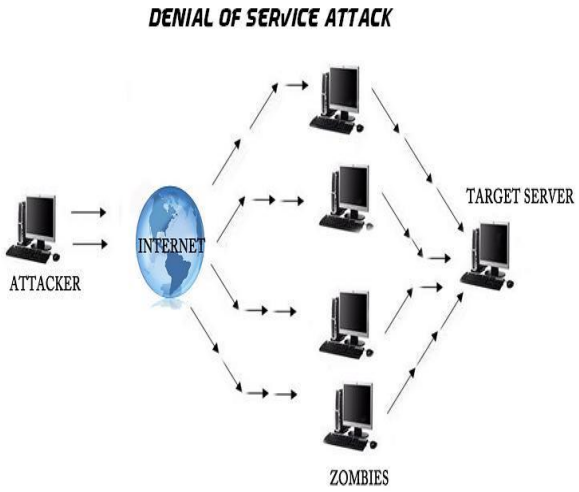


Fig1.3 Internet Control Message Protocol

4. Peer-to-peer attacks

A peer-to-peer (P2P) network is a distributed network in which individual nodes in the network (called "peers") act as both suppliers (seeds) and consumers (leeches) of resources, in contrast to the centralized client–server model where the client server or operating system nodes request access to resources provided by central servers.



5. Defense techniques in Dos attack:

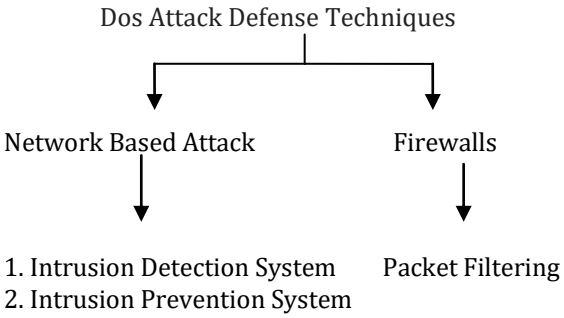


Fig 1.4 Defense Technologies in Dos Attack

6. Network Based Techniques:

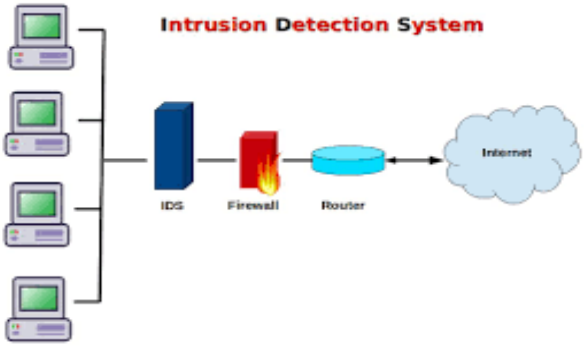
1. Intrusion Detection System (IDS):

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment(sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks

- Analysis of abnormal activity patterns
- Tracking user policy violations



2.Intrusion Prevention System (IPS):

Network intrusion prevention systems (IPS) monitor and analyze an organization's network traffic to identify malicious activity and -- optionally -- stop that activity by dropping and/or blocking associated network connections. IPS have been used for many years at key network locations, such as in close proximity to firewalls to identify a variety of network-based attacks that other security technologies are unable to detect. Intrusion prevention systems have since evolved to use a variety of more sophisticated detection techniques that allow them to understand the intricacies of application protocols and communications so they can detect application-based attacks, as well as attacks at other layers of the network stack.

Intrusion Prevention Functions Include:

- The intrusion prevention system (IPS) was designed to be deployed inline on the network close to be the perimeter and complement the work of network firewall
- The IPS must also detect and response accurately to eliminate false positives.

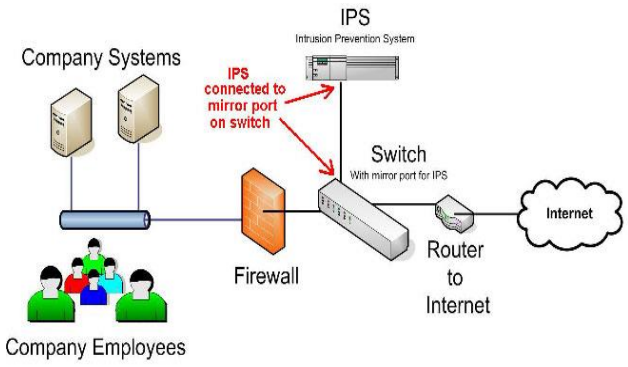


Fig: Intrusion prevention system

❖ Firewall Based Technique:

1.Packet Filtering Firewall:

On the internet, packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. The process is used in conjunction with packet managing and Network Address Translation (NAT).Packet filtering is often part of firewall program for protecting a local network from unwanted intrusion. Network layer firewall defines packet filtering rules sets, which provide highly efficient security mechanisms .packet filtering is also knows as static filtering.

Function of Packet Filtering Include:

A firewall filters the IP packet. the IP header of all the packet that enter or exit the network firewall are inspected. Firewall makes an explicit decision on each packet that enters as to whether to allow the packet or deny the packet.

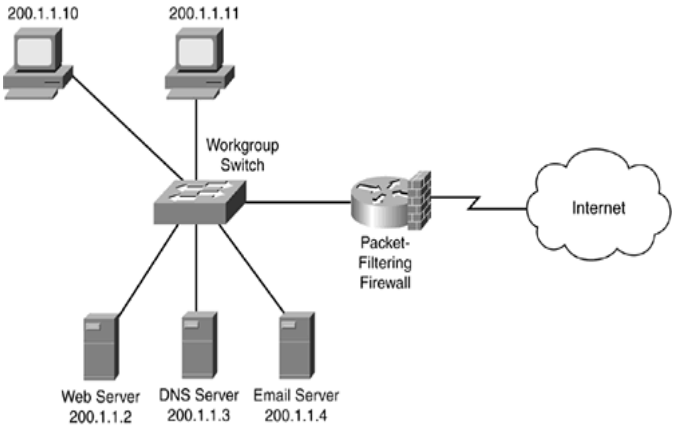


Fig: Packet Filtering

Related work:

In Denial of service attack there different techniques to defense the attack like Intrusion Detection System, Intrusion Prevention System, Packet Filtering then the comparison of Denial Of Service Attack defense techniques

Fig 1.5 Comparison of DOS Defense Technology

Defense techniques	Advantages	Disadvantages
Packet filtering	• Packet filters are generally faster than other firewall technologies because they	• Packet filtering firewalls can work only network layer . • Difficulty of

	perform fewer evolutions. • Cost of packet filtering technique is low. • Easy to install. • Makes security transparent to end users. It is high speed technique.	setting up packet filtering rules to the router. • Packet filter router are not very secure. • Packet filter cannot authenticate information coming from a specific user.
Intrusion Prevention System	• It is free to download and use technique. • The rules are easy to write in IPS technique. • IPS has good community support. • Intrusion prevention is highly flexible in terms of deployment.	• No GUI for rule manipulation in IPS. • It is slow in packet processing • It cannot detect signature slit over multiple TCP packet, which occurs when packet are configures in inline mode.
Intrusion Detection System	• Visibility :In IDS provide a clear view of what's going within your network . • Defense: IDS adds a layer of defense to your security profit, providing a useful backstop to some of your other security measures. • Response capability: Although they probably will be of limits' it is a valuable source of information .	• More maintained :unfortunately an IDS firewall virus scan or any other secure measures. • Staff requirements: properly managing an IDS requires experience staff. • IP packet can still faked: the information from an IP packet ready by an IDS but the network address can still be spoofed.

7. CONCLUSIONS

In this paper a review on denial of service attack, which types of attack in dos attack. different techniques or detecting and preventing DOS attack. We describe how attacks are conducted. Comparison between the defense techniques against the denial of service attack. which is the best technique to the defense of DOS attack, review on that techniques .which is useful avoid the DOS attack.

REFERENCES

1.Catherine Paquet "Network security using Cisco IDS IPS", Pearson Education

2. R. Zhong, and G. Yue DDoS detection system based on data mining." Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2-4 April, pp. 062–065. Academy Publisher. (2010)"

3. Anderson, T., Roscoe, T., and Wetherill, D. 2003. Preventing Internet denial-of-service with capabilities. In Proceedings of HotNets-II.

4.p.Hunter,distributed denial of services mitigation tools, network security5(2003),pp 12-14

5.H. Wang, C. Jin, and K.G. Shin, "Defense against Spoofed IP Traffic Using Hop-Count Filtering, in IEEE/ACM Trans. Networking, vol.15, no.1, 2007 pp.40-53.

6.CERT, "Denial of Service Attacks," June 4, 2001,[online] http://www.cert.org/tech tips/denial of service.html

BIOGRAPHIES

Sheetal Pralhad Desai
MCA TY
MGM' JNEC Aurangabad

Priti R. Hadule
MCA TY
MGM' JNEC Aurangabad

Prof. Arundhati A. Dudhgaonkar
Assistant Professor
MGM' JNEC Aurangabad
Master Of Computer Application