MONITORING OF TRAFFIC OVER THE VICTIM UNDER TCP SYN FLOOD IN A LAN

Kanika[1], Renuka Goyal[2], Gurmeet Kaur[3]

[1]*M.Tech Scholar, Computer Science and Technology, Central University of Punjab, Punjab, India*
[2]*M.Tech Scholar, Computer Science and Technology, Central University of Punjab, Punjab, India*
[3]*M.Tech Scholar, Computer Science and Technology, Central University of Punjab, Punjab, India*

Abstract

Denial of service attack is a major threat in the network security. The purpose of Denial of service (DoS) attack is to disrupt the services offered by the victim. The most common type of DoS attack is flooding with the network traffic to waste the server's resoures.TCP SYN flood is a kind of DoS attacks that take advantage of three way handshake of TCP/IP protocol in order to disrupt Internet services. The paper explores what a Denial of Service is and how it functions. A Denial of Service demonstration has been shown with TCP SYN flood and the effects it has on the victim computer. The different parameters are analyzed on the victim system and compared with normal behavior of the network indicates the presence of attack.

Keywords: *Denial of Service attack, Spoofing, Network Security, TCP SYN*

----------***----------

1. INTRODUCTION

A denial-of-service attack is defined as preventing a system to deliver services from its normal behaviour. DoS attacker tries to prevent the legitimate user to access the services from the server. To perform the denial of service attack, the attacker consumes all resources of that system, thus preventing other users gaining access to those resources results Denial of Service. Denial of Service attacks is normally associated with computer networks to attack on the main server that deliver services to the computer network. DoS attacks mainly focus of on web servers such as banks, e-mail, and voicemail network.

1.1 Distributed Denial of service attack

The attack attempted by multiple people in a Distributed environment leads to Denial of Service attack. A malicious attacker uses a DDoS attack to make computer resources stop responding to legitimate users. The attacker does this by commanding hundreds of computers that are remotely controlled to flloa network traffic at the victim.

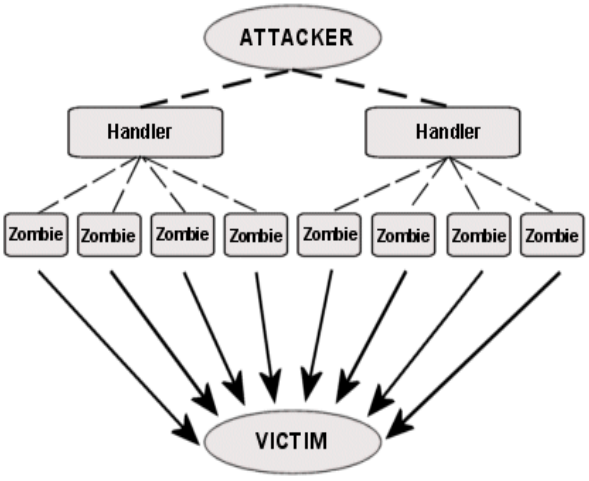

Fig 1 Architecture of DDoS attack

The victim becomes so busy with dealing request from these systems and not able respond legitimate users' requests. The systems that are involved as attacking agent known as Zombie and a large group of zombie computers is called a robot network, or botnet.

2. TCP DENIAL OF SERVICE

TCP/IP is a connection oriented networking protocol that starts with "handshaking" in client-server architecture. TCP provides reliable delivery of data. To establish a connection the client firstly sends a "SYN" packet to server.

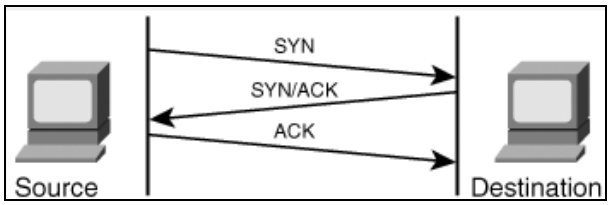

Fig 2 Three way handshake

Then the server replies with a "SYN/ACK" packet that signals the server is ready to accept the connection. Finally, the client sends a "ACK" packet to establish the connection. As the connection established in three steps, the procedure known as "Three Way Handshaking".

2.1 TCP SYN Flood

TCP connection is exploited to perform DoS attacks by TCP SYN flood. The attacker takes advantage of 3-way handshake in order to exhaust the resources. An attacker tries to overload the victim with so many TCP connection requests that it will not be able to respond to legitimate requests. The attacker sends too many TCP SYN packets to the victim.

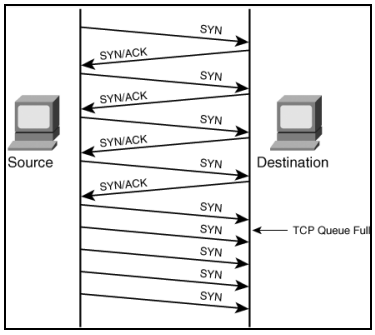

Fig 3 TCP SYN Flood

The victim allocates buffers for each new TCP connection and transmits a SYN-ACK in response to the connection request. The attacker does not respond to the SYN-ACK. In this way large number of half open connections are maintained on a victim server's queue and it get full. The queue of the server is limited, and legitimate client's request cannot be fulfil due to unavailability of the resources (space) in the queue.

2.2 IP Spoofing

IP spoofing is creation of IP packets with forged IP source addresses. IP spoofing is used in denial of service attack used for hiding the identity of the sender. In DoS attack, the attacker floods the packets with overwhelming amount of traffic and does not care about receiving back the IP packet's respose. IP spoofing uses randomized IP addresses to start the three way handshake. IP spoofing is difficult to filter as spoofed packets appears to be coming from a different address. The attacker can also use subnet spoofing, spoofs a random address within the address space of the sub network.

3. EXPERIMENT ARCHITECTURE

To conduct the experiment, a set up of four machines with LAN connectivity on the same network is created in the lab, one machine, acts as a source of the TCP SYN flood packets is used for attacking. The other machine, acts as a receiver of the TCP SYN packets is used as the victim. The attacking machine performs network sniffing to know the IP addresses available in the network.

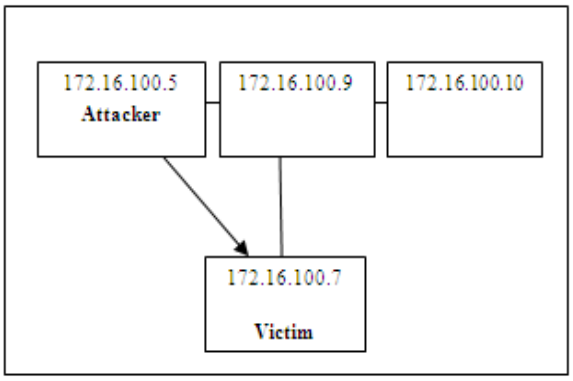

Fig 4 implementation architecture

There is two sections, first is performing denial of service attack on ubuntu host using Backtrack attacker machine. The second section shows the effect of TCP SYN flood on the victim.

4. TCP SYN FLOOD BY MALICIOUS ATTACKER

One machine in the network could be a malicious attacker and using ARP protocol it can come to know about the neighbouring IP addresses and MAC address of other machine linked in the network.

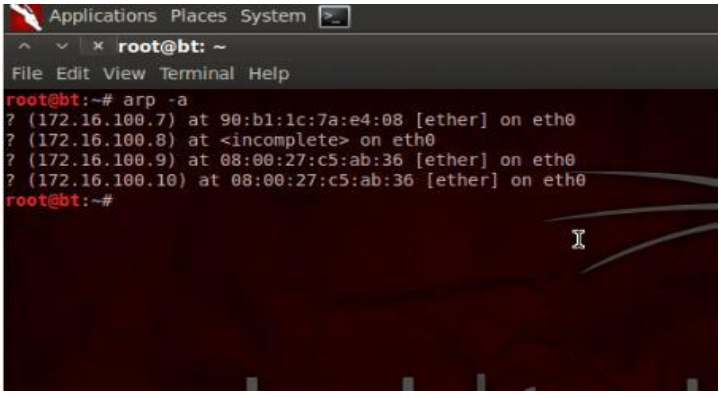

Fig 5 ARP command results

The 'arp' command lists and manipulate the local system ARP table. ‘arp –a’ list the entries currently in the arp table. The resulting list consists of the IP address, the MAC address and the Ethernet interface in the network.

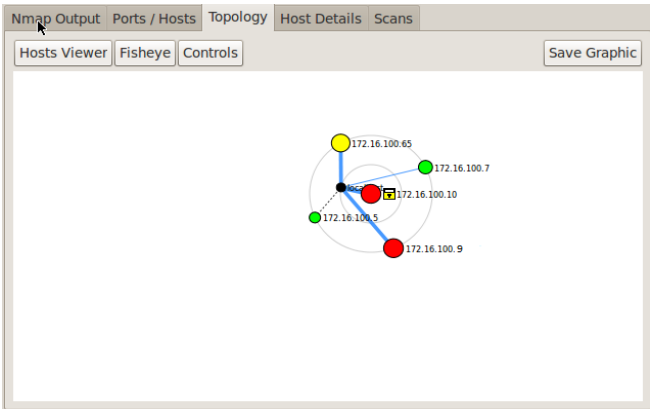

Fig 6 'NMAP' Scanning

Now the attacker machine has a list of MAC addresses and IP addresses available over the network. Using the ‘nmap’ tool the attacker performs the scan over the target Machine. As the figure shows it reports whether the host is up or down. The green symbol shows the host is currently up.

Now the attacker picks the IP address 172.16.100.7 to perform syn flood with spoofed IP addresses of other two machines available in the network.

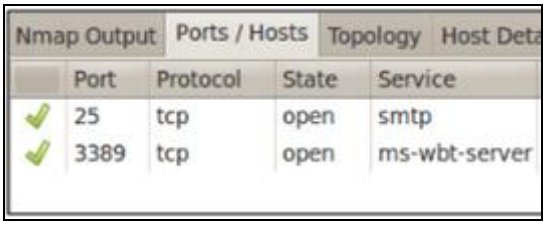

Fig 7 Open port scanning

Another option available for the attacker guest machine is to check for the open ports of the victim machine to perform the attack.

5. DETECTION OF TCP SYN FLOOD ATTACK

A variety of tools are employed in the research to measure the effect of TCP DDOS attack by a malicious machine. Wireshark, Bandwidth monitor, Netflow and IPtraf are few of the tools used to analyze the system under attack. Exclusive Netstat commands are also used for getting the results. The performance of the victim machine under attack is determined on the basis of network traffic, average number of SYN requests over the system, number of half opened connections, OS response time, round trip etc.

To detect the attack effect, the attacker Machine trying to communicate with the victim Machine. 20 seconds after communication, attacker starts sending attack traffic that lasts 40 seconds. The attacker virtual machine floods the victim at the maximum possible rate allowed by operating system.

5.1 Number of Packets Captured

Wireshark tool captures the SYN packets passing through the eth0 port .The Ethernet port was monitored during a TCP SYN flood attack; thousands of SYN requests were captured. Figure shows the malicious machine sending the SYN request to the host and don’t acknowledge them.

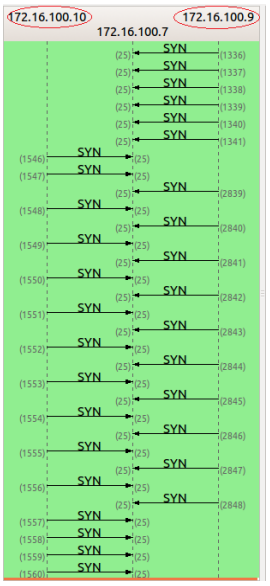

Fig 8 'Wireshark results'

The IO graph used to count the number of SYN requests and analysed with the previous captured traffic. At the time SYN flood the number of requests more than 6000 when compared to normal traffic that is about 5 to 10 packets per second.

5.2 Round Trip Time

The time taken by a packet to reach the destination and acknowledged back by the receiver is called the Round trip time (RTT). When a packet exceeds its RTT, the packet is considered to be lost and thus it is retransmitted in a TCP connection. Since retransmissions aggregates Denial of Service. It is evident that when there is no attack, there is no TCP traffic.

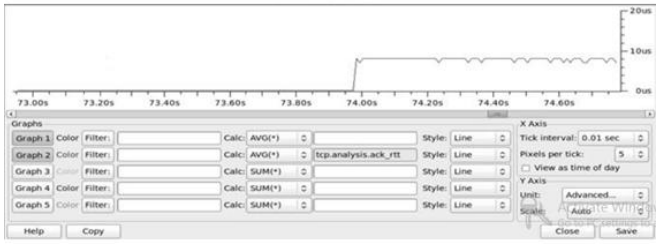

Fig 9 Round trip time for SYN packets

Thus the reading is close to zero when the attack is not live. When the attack is initiated, the RTT increases to up to 10 microseconds which stays almost constant till the end of the attack.

5.3 The Start and End Time of an Attack

The exact time when the attack starts is analyzed with the post processing of the TCP SYN packets.

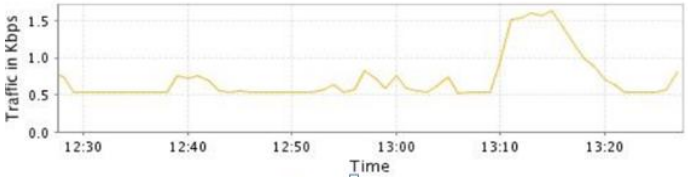

Fig 10 Time when the attack was active

NetFlow tool is used to analyze the network traffic over the victim. At the time of attack the network traffic increases abruptly compared to normal flow of data.

5.4 Number of Half Opened Connections

The command used to list the number of active SYN connections is *"netstat -an | grep" SYN_RCVD*"**.**

The number of awaiting SYN connection was 7015 during the attack which completely drained out the host operating system memory. The operating system was not able to hold all the pending SYN connections in its CPU memory space and eventually crashed. However, when the attack was stopped, the number of awaiting SYN connections dropped down to 6. The command "*netstat -s -t | more"*used to pull out the entire details of the existing, awaiting and pending connection requests. This command brings out the entire information about all the incoming and outgoing connections the system is currently handling.

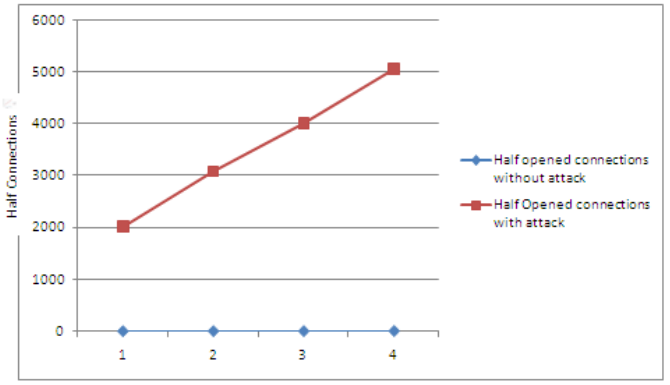

Fig 11 No. of half opened connections

The figure shows the results yielded with the command which gives the complete listing of all the connection status. When there is no attack in the system number of half open connections is very less that is 2 to 5. At the initial stages of SYN flood attack, the number of active connection showed about 2000 and then rose up to 5000 during the peak.

6. CONCLUSIONS

A denial of service attack is to prevent the legitimate user from gaining access to a certain resources or even complete failure of the server by sending too many requests. The TCP DDOS attack can be implemented by an attacker that may lead to damage to computer network. . Responding, defeating these attacks in a effective manner is the primary challenge of today's network security. The demonstration of a Denial of Service attack in this paper is a way to show how a Denial of Service attack can be implemented by the malicious attacker in a LAN and prepare the server to respond and defeat these attacks because if you are not prepared for the worst you will suffer when the worst happens.

To detect attack, Network Traffic is analyzed at the victim and the results showed that the arrival rates of normal TCP SYN packets and attacked SYN Flood attack varies with large difference. On the basis of daily network behavior a SYN Packet arrival rate is decided. At the victim side the attack is detected by considering different parameters. The future work is to block the attacking traffic by deciding the threshold values of these parameters by using intrusion detection systems and firewalls.

REFERENCES

[1]. C. Manusankar, et al., "Intrusion Detection System with Packet Filtering for IP Spoofing," The International Conference on Communication and Computational Intelligence, pp. 563-567, 2010.

[2]. D. Erhan, Anarim, et al., "Effect of DDoS attacks on traffic features," 21st Conference Signal Processing and Communications Applications, pp. 24-26 April 2013.

[3]. D. Nashat , X. Jiang, "Detecting syn flooding agents under any type of ip spoofing," in IEEE International Conference on e-Business Engineering, pp. 499-505, 2008.
[4]. Kavisankar , C. Chellapan ," A Mitigation model for TCP SYN flooding with IP Spoofing", IEEE-International Conference on Recent Trends in Information Technology, pp. 251-256, 2011.
[5]. L. Limwiwatkul, A. Rungsawang, "Distributed denial of service detection using TCP/IP header and traffic measurement analysis,", IEEE International Symposium on Communications and Information Technology, pp.26-29 Oct. 2004.
[6]. L. Rizzo, M. Landi, "Netmap: memory mapped access to network devices," In Proceedings of the ACM SIGCOMM, pp. 422-423, 2011.
[7]. Ma Miao, "Mitigating denial of service attacks with password puzzles," 2005.International Conference on Information Technology: Coding and Computing, vol.2, pp.621-626, 2005
[8]. Srinivas Shakkottai, et al., "The rtt distribution of tcp flows in the internet and its impact on tcp-based flow control," 2004.
[9]. Stopforth, Riaan "Techniques and countermeasures of TCP/IP OS fingerprinting on Linux Systems," Thesis, University of KwaZulu-Natal, Durban, 2007
[10]. T. Nakashima, T. Sueyoshi, "Performance Estimation of TCP under SYN Flood Attacks," First International Conference on Complex, Intelligent and Software Intensive Systems, pp.10-12 April 2007.
[11]. Wireshark http://www.wireshark.org/about.html, Accessed February 9, 2014
[12]. Z. Gao, et.al. , "Differentiating Malicious DDoS Attack Traffic from Normal TCP Flows by Proactive Tests,", IEEE Communications Letters, vol.10, pp.793,795, November 2006.
[13]. Zhuang Wei, et al., "TCP DDOS Attack Detection on the Host in the KVM Virtual Machine Environment," IEEE/ACIS 11th International Conference on Computer and Information Science (ICIS),pp.62-67, June 1 2012.