Identification and Prevention of Smurf Attack using Packet capture Analysis

Chaudhari Nivrutti Janardhan1, Dr.Shailesh Kumar2, Dr. Mangesh D. Salunke3

1 Department of Computer Engineering, Research Scholar, Shri JJT University, Rajasthan

2 Department of Computer Engineering, Associate Professor, Shri JJT University, Rajasthan

3 Department of Computer Engineering, Asst. Professor, JSPM NTC, Pune

Abstract- Among the several internet attacks that on security, denial of service (DoS) has the most damaging impact type of attack .DoS attacks pose a significant threat to the Internet. The Smurf assault is a type of DoS attack. The Smurf Attack is caused by faked traffic flooding the network. The Smurf attack exploits IP protocol flaws by sending ping packets to a large number of network hosts on the internet in order to generate reply packets, resulting in network traffic congestion and system breakdown. Smurf attack initially determined the attack host and then utilizes two steps further: first, it uses the network host address as the source address, creating a large number of ICMP response packets. The packets are then sent out with the Broadcast address, and they are returned to the network assault.

Keywords- ICMP, Smurf Attack, IP Address, Dos, DDoS, IDS

I INTRODUCTION

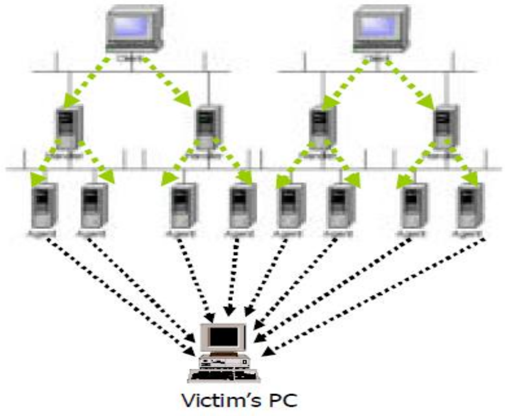

Fig. DDoS Attack

Denial of service (DoS) attacks has become a major threat to current computer networks. To have a better understanding on DoS attacks, this article provides an overview on existing DoS attacks and major defense technologies in the Internet and wireless networks. DoS attacks on the Internet often defeat the target by draining its resources, which can include anything related to network computing and service performance, such as link bandwidth, T CP connection buffers, application/service buffers, CPU cycles, and so on. Individual attackers can also exploit vulnerabilities, get access to target systems, and then disrupt services. Because it is difficult for attackers to overwhelm a target's resource from a single computer, many recent DoS attacks have been launched through a large number of distributed assaulting hosts on the Internet. These are known as distributed denial of service (DDoS) assaults.

II LITERATURE REVIEW

Gholam Reza Zargar el.et in this paper author describes a method for detecting the Smurf attack that is based on TCP/IP fundamental features and employs PCA for dimension reduction and feature analysis. As a result of the provided results, it is possible to conclude that employing PCA for dimension reduction can minimize calculation time in intrusion detection while maintaining detection accuracy [1].

Shankar Kumar el.et DDoS attacks are going unabated. Instead, the attackers are expanding the size and frequency of their attacks across multiple dimensions. The researchers will identify the root cause of any new threat or attack that happens in the world, as well as preventative measures. According to the current study, the basic problem with being unable to block new DDoS attacks is a lack of support among various network nodes. This is due to the Internet (networks of networks) preventing widespread worldwide collaborative deployment [2]

Raja Azrina author represented that the DoS and DDoS attacks, when combined with malicious code implantations, are simple to launch yet difficult to stop fully. Because of the structure of TCP/IP and sometimes missed programming flaws, the present Internet remains vulnerable to many types of DoS and DDoS attacks [3].

Kutub Thakur according to author study, numerous defence mechanisms were formed in the complexly expanding DDoS attacks, however in the present world, all defence systems are designed with diverse detection approaches and mitigation algorithms. Even if the DoS attacks are handled in many ways, not all the defense mechanisms match best for all forms of DDoS attacks. In these instances, TCP-SYN has been recognized as the effective strategy for mitigating and blocking DDoS attacks [4].

III. SMURF ATTACK

A Smurf attack is a type of distributed denial-of-service (DDoS) attack in which an attacker attempts to flood a server with Internet Control Message Protocol (ICMP) packets. By sending queries to one or more computer networks using the falsified IP address of the targeted device, the computer networks respond to the targeted server, potentially multiplying the initial attack flow and rendering the target unreachable. This attack vector is widely regarded as a closed vulnerability and is no longer used.

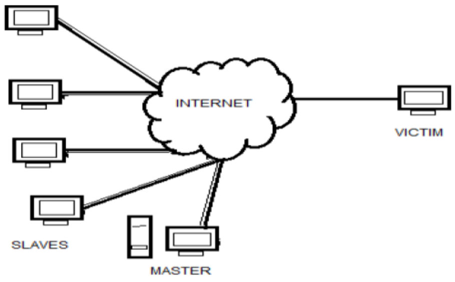

fig. Smurf attack

Steps of Smurf attack

Step 1: The attacker must determine the victim's IP address.

Step 2: The attacker must identify the intermediary site, which will aid in amplifying the attack.

Step 3: The attacker will send a large amount of traffic to the broadcast address at specific

Intermediary sites.

Step 4: These intermediaries will send broadcast messages to all hosts in a subnet.

Step 5: hosts will respond to network requests.

Types of smurf attack

Basic attack

A basic smurf attack happens when the attacker sends an endless number of ICMP request packets to the victim network. Packets contain a source address that is set to the network's broadcast address, prompting every device on the network that receives the request to respond. This generates a large quantity of traffic, which eventually brings the system down.

Advanced smurf attack

An advanced smurf attack begins with a basic attack. However, echo requests can be configured to react to additional third-party victims. This enables attackers to target several victims at the same time, allowing them to slow down larger networks and target greater groups of victims and broader portions of the web.

IV ATTACK IDENTIFICATION METHOD

Packet Sniffing

The technique comprises two major phases: data collecting and identification and analysis of an attacker's traits. To determine the behavior of assaults, two nodes are employed, one serving as an attacker machine and another as a victim with a tool installed to capture all network traffic entering the network environment.

Data collection

The programme includes filters, color-coding, and other capabilities that allow users to analyse network traffic and explore individual packets. Furthermore, this application provides a simple method for network identification, load, frequency, and delay between specific hops. The most prevalent packets on the network system are likely to be TCP, UDP, and ICMP.Using a packet sniffer, the data collection phase will capture all packets from an attacker, such as UDP and TCP traffic floods. The user recognises pattern assaults' activity after capturing UDP, HTTP, and TCP packets [5].

Attacking Scheme

It may carry out different forms of attacks on the target system: one machine is used as an attacker to flood malicious packets to the server machine, which has a tool for monitoring and recording all traffic in real-time.

V CONCLUSION

Sniffing is a technique used to capture and analyse pattern attacks (DoS) by sniffing all incoming network data such as TCP, UDP, and HTTP packets supplied by attackers to the targeted server. After gathering patterns, the user identifies packets and comprehends attacker behavior by comparing them to routine data communication. Based on the packet header and contents, an attacker can be recognized. To identify malicious traffic based on its behaviour, the receiver first establishes where the incoming packet belongs by analyzing by its source IP address, source port number, destination IP address, destination port number.

VI REFERENCES

[1] Gholam Reza Zargar, Peyman.kabiri"Identification of Effective Network Features to Detect Smurf Attacks" 978-1-4244-5187-6/09/$26.00 ©2009 IEEE.

[2] Shankar Kumar, Dr. Nandeshwar Pd Singh, Dr. Narendra Kumar "Literature Review of Distributed Denial of Service (DDoS) Attacks, its Detection Techniques and Prevention Mechanisms" ISSN: 2321-9653Volume 10 Issue IX Sep 2022.

[3] Raja Azrina Raja Othman Understanding the Various Types of Denial of Service Attack © SANS Institute 2000 – 2002.

[4] Kutub Thakur "Analysis of Denial of Services (DOS) Attacks and Prevention Techniques" IJERTV4IS070164 ISSN: 2278-0181 Vol. 4 Issue 07, July-2015 172

[5] Kagiraneza Alexis Fidele, Suryono, Wahyul Amien Syafei " Denial of Service (DoS) attack identification and analyse using sniffing technique in the network environment" https://doi.org/10.1051/e3sconf/202020215003 *ICENIS 2020.*