NetSHIELD: Countermeasure Tool for Network Layer Attacks

Prachi Korgaonkar, Ashish Patil, Nilesh Khochare

Abstract—In TCP/IP Reference model, Network layer & Transport layer plays an important role in order to send any Information via network. So focus of attackers is to break all the security aspects of layer 3. The network has protocols like Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), Internet Protocol (IP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), etc. Each Protocol has its own vulnerability, which is exploited by an attacker. So mainly we are focusing on the attacks like DDoS (Distributed Denial of Service), Ping of Death, Teardrop, Smurf, Fraggle, TCP-SYN Flood attack. Here we are going to study, how actually attack is going to happen? What will be the effect of it? And what kind of Preventive measures needed?

Index Terms—Network-layer, DoS, Attacks, NetShield.

I. INTRODUCTION

Attacks on computer systems and networks can be grouped into two broad categories: attacks on specific software (such as an application or the operating system itself) and attacks on a specific protocol or service. Attacks on specific protocols or services are attempts to either take advantage of a specific feature of the protocol or service or to use the protocol or service in a manner for which it was not intended. In addition, the target of an attacker can be of two types: targets of opportunity where the attacker is attempting to find any machine that is susceptible to a specific vulnerability, and defined targets where the attacker wants to gain access to a very specific target and must attempt to find a vulnerability that exists in that target.

Denial-of-Service (DDoS) attacks can exploit a known vulnerability in a specific application or operating system, or they may attack features (or weaknesses) in specific protocols or services. In this form of attack, the attacker is attempting to deny authorized users access either to specific information or to the computer system or network itself.

A SYN flooding attack may be used to temporarily prevent service to a system in order to take advantage of a trusted relationship that exists between that system and another.

A LAND attack uses the TCP three-way handshake function. During such an attack, the attacker forces large amounts of TCP SYN packets with both the source address and destination address being the IP address of the target, causing the target to send SYN ACK messages to itself. After the target receives the SYN ACK messages, it sends ACK messages to itself and creates TCP connections, which will be kept until they time out. In this way, the attacker may deplete the resources of the target. Different operating systems respond differently to land attacks. For instance, UNIX hosts will crash down while Windows NT hosts will slow down.

A simple SMURF attack sends ICMP echo request messages with the destination address being a broadcast address on the target network. When all hosts on the target network reply to the requests, network congestion occurs. An advanced Smurf attack uses the address of a target host or network as the source address of the ICMP echo request messages, and keeps sending such ICMP echo request messages to the target, making the target crash down.

A FRAGGLE attack is similar to SMURF attack; we can say its cousin of SMURF. The only difference is FRAGGLE uses UDP packet for an attack instead of ICMP packets.

II. RELATED WORK

A. Network Layer Attacks

1) Denial of Service Attack

A Denial of Service attack is simply, like its name suggests, is a type of attack when the attacker prevents legitimate users of the service from accessing the service. A DoS attack may be engineered by using any of these five basic attack methodologies according to Wikipedia:

DoS attacks generally achieve their goal by sending large volumes of packets that occupy a significant proportion of the available bandwidth. Hence, DoS attacks are also called bandwidth attacks. The aim of a bandwidth attack is to consume critical resources in a network service. Possible target resources may include CPU capacity in a server, stack space in network protocol software, or Internet link capacity. By exhausting these critical resources, the attacker can prevent legitimate users from accessing the service. A crucial feature of bandwidth attacks is that their strength lies in the volume rather than the content of the attack traffic. This has two major implications:

- Attackers can send a variety of packets. The attack traffic can be made arbitrarily similar to legitimate traffic, which greatly complicates defense.
- The volume of traffic must be large enough to consume the target’s resources. The attacker usually has to control more than one computer to generate the attack traffic. Bandwidth attacks are therefore commonly DDoS attacks.

In others words one can describe a DOS attack, saying that a DOS attack is one in which you clog up so much memory...
on the target system that it cannot serve legitimate users. Or you send the target system data packets, which cannot be handled by it and thus causes it to either crash; reboot or more commonly deny services to legitimate users. There is several type of DOS attack, the most popular of which are as follows:

2) Smurf Attack

In a SMURF attack you can be affected in one of several ways:

- As a victim or target of the attack
- As a network which is abused to amplify the attack
- As a party harboring the instigator of the attack

SMURF and similar Denial-of-service (DoS) attacks can do serious damage to your network services, be it either as an individual end-user or as an entire institution in that your network or host can be inundated with unwanted and maliciously sent traffic.

Working: A SMURF attack (named after the program used to perform the attack) is a method by which an attacker can send a moderate amount of traffic and cause a virtual explosion of traffic at the intended target. The method used is as follows:

a) The attacker sends ICMP Echo Request packets where the source IP address has been forged to be that of the target of the attack.

b) The attacker sends these ICMP datagrams to addresses of remote LANs broadcast addresses, using so-called directed broadcast addresses. These datagrams are thus broadcast out on the LANs by the connected router.

c) All the hosts which are alive on the LAN each pick up a copy of the ICMP Echo Request datagram (as they should), and sends an ICMP Echo Reply datagram back to what they think is the source. If many hosts are alive on the LAN, the amplification factor can be considerably (100+ is not uncommon).

d) The attacker can use largish packets (typically up to ethernet maximum) to increase the effectiveness of the attack, and the faster network connection the attacker has, the more damage he can inflict on the target and the target's network.

Since the Smurf Attack is caused by flooding the network with spoofed traffic, we will be mostly dealing with the fifth type of attack, where the denial of service is caused by an overwhelmed victim, which runs out of resources in dealing with the torrent of ICMP echo replies.

Preventive measures: Check whether the destination address of a received ICMP echo request message is a subnet broadcast address or network address. If yes, drop or forward the packets and log the event, depending on the configuration.

3) Fraggle Attack:

A Fraggle attack is similar to a Smurf attack. The difference is that it uses UDP messages instead of ICMP messages. A Fraggle attacker sends to a subnet broadcast address large amounts of UDP packets with the source address being the target network address or target host address and the destination port number being 7 (Echo service) or 19 (Chargen service). All hosts in the subnet that are enabled with Echo or Chargen service will send reply messages to the target network or host, resulting in network congestion in the target network or crash of the target host.

Preventive measures: Check whether the destination port number of a received UDP packet is 7 or 19. If yes, drop or forward the packets and log the event, depending on the configuration.

4) Ping of Death attack:

The maximum allowable IP packet size is 65,535 bytes, including the packet header, which is typically 20 bytes long. An ICMP echo request is an IP packet with a pseudo header, which is 8 bytes long. Therefore, the maximum allowable size of the data area of an ICMP echo request is 65,507 bytes (65,535 - 8 = 65,507). However, many ping implementations allow the user to specify a packet size larger than 65,507 bytes. A grossly oversized ICMP packet can trigger a range of adverse system reactions such as denial of service (DoS), crashing, freezing, and rebooting.

Preventive measures: If the type of the packet is ping, then we need to check the size of the ICMP packet. If the size cross maximum limit then the packet need to be drooped.

5) Teardrop Attack:

The Teardrop attack exploits the vulnerability present in the reassembling of data packets. Whenever data is being sent over the Internet, it is broken down into smaller fragments at the source system and put together at the destination system.

Say you need to send 4000 bytes of data from one system to the other, then not all of the 4000 bytes is sent at one go. This entire chunk of data is first broken down into smaller parts and divided into a number of packets.

These packets have an OFFSET field in their TCP header part. This Offset field specifies from which byte to which byte does that particular data packet carries data or the range of data that it is carrying. This along with the sequence numbers helps the destination system to reassemble the data packets in the correct order. Now in this attack, a series of data packets are sent to the target system with overlapping Offset field values. As a result, the target system is not able to reassemble the packets and is forced to crash, hang or reboot.

6) SYN Flood Attack:

A SYN flood occurs when a host becomes so overwhelmed by SYN segments initiating uncompleteable connection requests that it can no longer process legitimate connection requests.

Two hosts establish a TCP connection with a triple exchange of TCP segments known as a three-way handshake: A sends a SYN segment to B; B responds with a SYN/ACK segment; and A responds with an ACK segment. A SYN flood attack inundates a site with SYN segments containing forged (“spoofed”) IP source addresses with nonexistent or unreachable addresses. B responds with SYN/ACK segments to these addresses and then waits for responding ACK segments. Because the SYN/ACK segments are sent to nonexistent or unreachable IP addresses, they never elicit responses and eventually time out.

7) Land Attack:

Combining a SYN attack with IP spoofing, a Land attack occurs when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address. The receiving system responds by sending the SYN-ACK packet to itself, creating an empty connection that lasts until the idle timeout value is reached. Flooding a system with such empty connections can overwhelm the system, causing DoS.

Preventive measures: Check the source address and destination address of each received IP packet. If the two addresses are the same or the source address is a loopback
address (127.0.0.1), drop or forward the packet and log the event, depending on the configuration.

B. Existing Network scanner

1) Snort:
   Snort is an Open Source and free Intrusion detection as well as Prevention systems. It does the real-time traffic analysis, it is designed in such a way that it can detect attacks. It does following:
   - Protocol analysis,
   - Content searching,
   - Content Matching.
   It performs respective action as specified by the user, as user will define rule set for the IDS. And accordingly Snort will take further action on Attack. It has 3 modes of operation,
   - Sniffer Mode
   - Packet logger Mode
   - Network Intrusion Detection System (NIDS) [11]

2) Nessus
   It’s a product by Tenable network Security which is a vulnerability and configuration assessment Product. Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerability that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

   Each computer has thousands of ports, all of which may or may not have services (i.e.: a server for a specific high-level protocol) listening on them. Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack. Nessus is called a “remote scanner” because it does not need to be installed on a computer for it to test that computer. Instead, you can install it on only one computer and test as many computers as you would like. [12]

3) Nmap:
   This tool is used to discover the hosts or services on the network, and create map of the network. Nmap not only discovers a host on the network but also figures out whether the host is Up or Down, which ports are open and close. It can determine the operating System of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a Firewall. [13]

4) Sguil
   This is also an Open Source tool. It captures session data, raw Packets, real-time events. It stores all alerts into the database. Main components of SGUIL are:
   - Server
   - Database server
   - Sensors
   - Clients
   On each sensor, full content data is captured by a Snort process running in packet-capture mode. Another Snort process runs as IDS in alert mode and SANCP collects session data. [14]

III. NETSHIELD: THE PROPOSED TOOL

The proposed approach to prevent Network layer attacks consist of various modules which is shown in figure 1 and aimed at (i) Monitoring the incoming and outgoing packets in the network (ii) Matching all the request packets and response packets with the stored rules, policies and the attack definitions present in database (iii) Block the malicious packets (iv) Alert the user regarding detected attack.

![Fig.1 Working of the Tool.](image)

Module I – User Interface Module
This module provides robust user interface through with user can interact with the NetShield tool. Through this module user can set or change the rule or the policies.

Module II – Database Module
This module provides the database which stores the rules and signatures of various attacks which is useful in detection and prevention of the attacks.

Module III – Detection Module
This module implement the algorithm to detect the various network layer attacks like DoS attacks, Smurf attacks, Fraggle attacks, Land attacks, SYN Flood attack, Teardrop attack, Ping of Death Attack.

Module IV – Prevention Module
This module implement the algorithm to prevent the various network layer attacks like DoS attacks, Smurf attacks, Fraggle attacks, Land attacks, SYN Flood attack, Teardrop attack, Ping of Death Attack.

IV. FUTURE SCOPE

This tool is a small step towards tackling the network related attacks. Some of the features of this tool are:

A. Statistics of the received, dropped packets, blocked IP Addresses, types of attacks, no. of attacks etc. can be shown.

B. The present system only prevents the known attacks. This can be extended by incorporating intelligence into it in order to gain knowledge by analyzing growing traffic.

C. Techniques to analyze the information in the LOG records which may help in efficient decision making.

V. CONCLUSION

Thus we have analyzed attacks on the network layer based on their Protocol vulnerabilities. In our paper we have presented problems and some preventive measures for network layer attacks. This could help to improve the security of network layer.
REFERENCES


[3] Li Xiaoming, V. Sejdini, H. Chowdhury, “Denial of Service (DoS) attack with UDP Flood”.


[9] SANS Institute InfoSec Reading Room, "802.11 Denial of service Attacks and Mitigation"


Prachi Korgaonkar is pursuing her BE in Computer Engineering, RMCET, Mumbai University. She is a member of ISTE.

Ashish Patil is pursuing his BE in Computer Engineering RMCET, Mumbai University. He is a member of ISTE.

Nilesh R. Khochare is an Asst. Professor in Department of Computer Engineering, RMCET, Mumbai University. He did his MTech (CSE) from VJTI, Mumbai in 2012. He published 5 papers in various International Journals and his area of interest is Networking and Security.