Anatomy and Mechanism of DOS attack

Ms. Neha. D. Mistri[1], Dr. Nilesh. K. Modi[2]

[1]Research Scholar, Karpagam University, Coimbatore.
[1]Assistant Professor, S.V. Institute. Of Computer Studies,
S. V. Campus, B/h. Railway station, Kadi - 382 715. Gujarat - India

[2]Professor & Head of the Department, S V Institute of Computer Studies, S V Campus,
Kadi – 382 715, Gujarat, India

***ABSTRACT*— A revolution came into the world of computer and communication with the advent of Internet. Internet has become increasingly important to current society. The frequency and sophistication of Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) on the Internet are rapidly increasing. Attacks that are seen every day on the Internet include direct attacks, remote controlled attacks, reflective attacks, worms, and viruses. This paper will try to explain about Denial of Service attack and its classification. This paper will try to explain what DDoS is, and how it can be prevented or mitigated. DDoS happens due to lack of security awareness, application, or skill on the part of the network/server owners or administrators. This paper covers these attacks and discusses techniques to prevent attacks. It also explain various types of tool of DOS attack.**

Keywords: Denial of Service attack, Prevention, attack

I. INTRODUCTION

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular website into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site. An attacker can use spam email messages to launch a similar attack on your email account. Whether you have an email account supplied by your employer or one available through a free service such as Yahoo or Hotmail, you are assigned a specific quota, which limits the amount of data you can have in your account at any given time. By sending many, or large, email messages to the account, an attacker can consume your quota, preventing you from receiving legitimate messages.

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack. Denial-of-service attacks can essentially disable your computer or your network. Depending on the nature of your enterprise, this can effectively disable your organization. Some denial-of-service attacks can be executed with limited resources against a large, sophisticated site. This type of attack is sometimes called an "asymmetric attack." For example, an attacker with an old PC and a slow modem may be able to disable much faster and more sophisticated machines or networks.

II. DEFINING DOS ATTACK:

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer or network resource unavailable to its intended users. Denial of Service attacks basically means denying valid Internet and Network users from using the services of the target network or server. It basically means, launching an attack that will temporarily make the service offered by the network unusable by legitimate users.

III. CLASSIFICATION OF DENIAL OF SERVICE ATTACK:

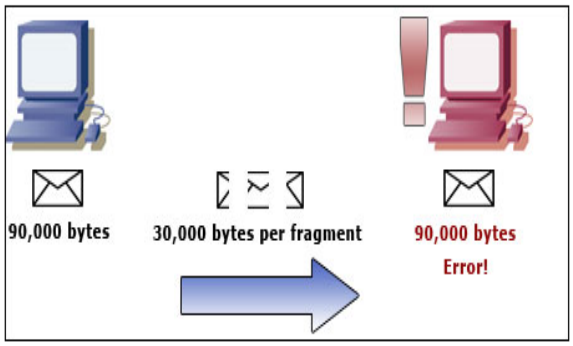
A denial of service (DoS) attack is an attack that clogs up so much memory on the target system that it cannot serve its users, or it causes the target system to crash, reboot, or otherwise deny services to legitimate users. There are several different kinds of dos attacks as discussed below:

1. Ping of Death: The ping of death attack sends oversized ICMP datagram's (encapsulated in IP packets) to the victim. The Ping command makes use of the ICMP echo request and echo reply messages and it's commonly used to determine whether the remote host is alive. The most basic of attacks is the ping flood attack. It relies on the ICMP echo command, more popularly known as ping. In legitimate situations the ping command is used by network administrators to test connectivity between two computers. In the ping flood attack,

it is used to flood large amounts of data packets to the victim's computer in an attempt to overload it.

```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Z>ping 127.0.0.1 -n 5 -l 65500

Pinging 127.0.0.1 with 65500 bytes of data:

Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Z>_
```

In a ping of death attack, however, ping causes the remote system to hang, reboot or crash. To do so the attacker uses, the ping command in conjunction with -l argument (used to specify the size of the packet sent) to ping the target system that exceeds the maximum bytes allowed by TCP/IP (65,536). Example: c:/>ping -l 65540 hostname Fortunately, nearly all operating systems these days are not vulnerable to the ping of death attack.



[Figure-1: Ping of death attack]

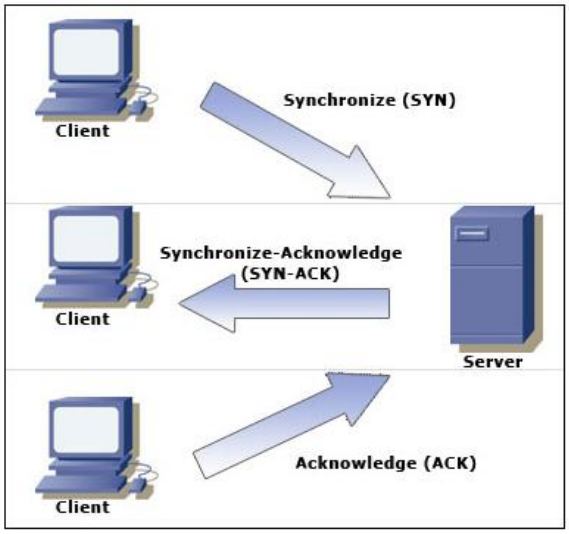
2. Teardrop Attack: Whenever data is sent over the internet, it is broken into fragments at the source system and reassembled at the destination system. For example you need to send 3,000 bytes of data from one system to another. Rather than sending the entire chunk in a single packet, the data is broken down into smaller packets as given below:

* Packet 1 will carry bytes 1-1000.
* Packet 2 will carry bytes 1001-2000.
* Packet 3 will carry bytes 2001-3000.

In teardrop attack, however, the data packets sent to the target computer contains bytes that overlap with each other. (bytes 1-1500) (bytes 1001-2000) (bytes 1500-2500) When the target system receives such a series of packets, it can not reassemble the data and therefore will crash, hang, or reboot.

Old Linux systems, Windows NT/95 are vulnerable.

3. SYN - Flood Attack: In SYN flooding attack, several SYN packets are sent to the target host, all with an invalid source IP address. When the target system receives these SYN packets, it tries to respond to each one with a SYN/ACK packet but as all the source IP addresses are invalid the target system goes into wait state for ACK message to receive from source. Eventually, due to large number of connection requests, the target systems' memory is consumed. In order to actually affect the target system, a large number of SYN packets with invalid IP addresses must be sent.

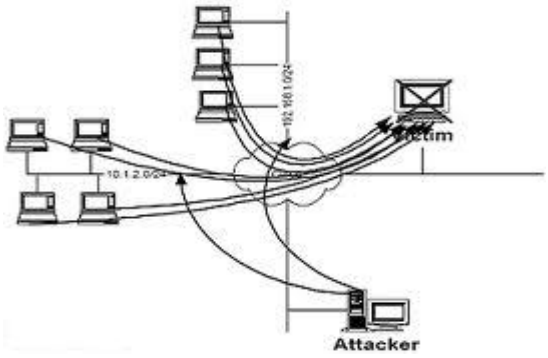


[Figure-2: SYN- flood attack]

4. Land Attack: A land attack is similar to SYN attack, the only difference being that instead of including an invalid IP address, the SYN packet includes the IP address of the target system itself. As a result an infinite loop is created within the target system, which ultimately hangs and crashes. Windows NT before Service Pack 4 are vulnerable to this attack.

5. Smurf Attack: There are 3 players in the smurf attack–the attacker, the intermediary (which can also be a victim) and the victim. In most scenarios the attacker spoofs the IP source address as the IP of the intended victim to the intermediary network broadcast address. Every host on the intermediary network replies, flooding the victim and the intermediary network with network traffic.

Result: Performance may be degraded such that the victim, the victim and intermediary networks become congested and unusable, i.e. clogging the network and preventing legitimate users from obtaining network services.

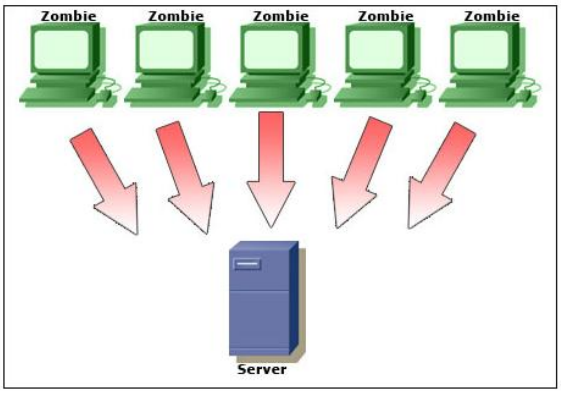


[Figure-3: Smurf Attack]

6. UDP - Flood Attack: Two UDP services: echo (which echos back any character received) and chargen (which generates character) were used in the past for network testing and are enabled by default on most systems. These services can be used to launch a DOS by connecting the chargen to echo ports on the same or another machine and generating large amounts of network traffic.

IV. DISTRIBUTED DENIAL OF SERVICE ATTACK:

A distributed denial of service attack, or DDoS, is much like the ping flood method, only multiple computers are being used. In this instance, the computers that are being used may or may not be aware of the fact that they are attacking a website or network. Trojans and viruses commonly give the hacker control of a computer, and thus, the ability to use them for attack. In this case the victim computers are called zombies.



[Figure-4 : Distributed Denial of service attack]

DDoS Prevention options:

1. Hire a security company to assess and repair the damage
2. Buy an intrusion detection system (IDS)

V. DISTRIBUTED DENIAL OF SERVICE ATTACK TOOLS:

There are a variety of different distributed DOS attack tools on the Internet that allow attackers to execute attacks on the target system.

1. Tribal Flood Network (TFN)
2. Trin00
3. Stacheldraht
4. Shaft
5. Mstream

1. TFN: The Tribal Flood Network (TFN) is a distributed DOS attack that allows an attacker to carry out a variety of DOS attacks including TCP floods, SYN floods and UDP floods on the target system. Each complete TFN network is made up of two parts:

- **TFN client program**
- **TFN daemon program**

Both the above parts of the TFN network can actually be modified to suit individual attack scenarios. This allows an attacker to fully customize the TFN tool based upon the target system's filtering mechanisms and countermeasures. A distributed DOS attack is executed using TFN in the following manner:

ATTACKER ⟶ CLIENTS ⟶ DAEMONS

1. Each attacker controls one or more TFN clients running on remote compromised or infected systems. An attacker can remotely communicate with the TFN client through a variety of different communication channels like telnet, TCP, UDP or ICMP remote shells etc. It is important to note that an attacker does not require a password to communicate with the TFN client.
2. Each TFN client in turn controls several different TFN daemons. These daemons are designed to together execute coordinated attacks on the target system. A TFN client communicates with all its respective TFN daemons by disguising the messages/commands in ICMP Echo reply packets. Such a strategy ensures that very few countermeasures can be employed to detect and block the malicious TFN traffic.

2. Trim00: Trin00 is a distributed DOS attack tool that allows an attacker to execute UDP flood attacks on the target system. Each Trin00 network is made up of the following parts:

- **Trin00 master**
- **Trin00 daemon**

It is indeed quite possible for a Trin00 network to have multiple levels of masters as well. The working of a Trin00 network is:

ATTACKER ⟶ MASTER ⟶ DAEMONS

1. Each attacker controls a number of Trin00 master systems. Attackers communicate with their respective masters through the TCP protocol. Unlike the TFN network, Trin00 master

systems are password protected, and unless the correct password is entered, the connection is refused.

2. Each master system in turn controls a number of daemon systems through the UDP protocol. All the daemon systems are configured to together execute coordinated attacks on the target system. All communication from the attackers to the master systems and finally to the daemon systems takes place on fixed pre-defined port numbers. An attacker can hence remotely use the master and daemon systems together to execute an attack on the target system.

3. Stacheldraht: This distributed DOS attack tool is probably one of the most evolved and advanced DOS tools available. It combines the best features of both TFN and Trin00.
Each stacheldraht network is made up of the two parts:

- Stacheldraht Master part (handler)
- Stacheldraht Daemon part (agent)

The stacheldraht distributed DOS tool was created with the primary aim of improving upon the shortcomings in the already existing tools like TFN and Trin00.

ATTACKER → MASTERS → DAEMONS

1. Each attacker controls a large number of handler systems, which are also known as master systems. The problem with the TFN and Trin00 networks was that all communication was carried out in plaintext, and could thus easily be sniffed and recorded by a malicious user. Stacheldraht solves this problem by using symmetric key encryption to encrypt all communications that occur between the attackers and handler systems.

2. Each master system controls a number of daemon systems or agents. All communications between the handlers and agents occur with the help of the ICMP and TCP protocols. It provides the attacker with the ability to upgrade the agents on demand.

4. Shaft: Shaft is yet another popular distributed DOS tool that has been modeled on the Trin00 network.

- Shaft Master part (handler)
- Shaft Daemon part (agent)

5. Mstream: Mstream is yet another distributed DOS attack tool that allows attackers to execute attacks on the target system. When compared to other attack tools, Mstream is not very favorable.

VI. CONCLUSION

The DoS and DDoS attacks in combination with malicious codes implantations are easily launched but difficult to completely stop. These attacks are an annoyance at a minimum, or can be seriously damaging if a critical system is the primary victim. This paper explains different types of Denial of service attack as well as how to prevent it. Explanations of this all tools are in this paper. A revolution came into the world of computer and communication with the advent of Internet. Internet has become increasingly important to current society. The frequency and sophistication of Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) on the Internet are rapidly increasing.

REFERENCES

[1].http://learn-networking.com/network-security/how-to-prevent-denial-of-service-attacks
[2].www.cybersecurity.my/data/content_files/13/72.pdf
[3].http://palms.ee.princeton.edu/.../DDoS%20Final%20PDCS%20Paper.pdf
[4].www.cs.virginia.edu/~adw5p/pubs/handbook04-dos-preprint.pdf
[5].Textbook: An Ethical hacking guide to corporate security by ankit fadia.