ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

A Review on IPS Techniques for DoS Attacks

Dr. K. Prabha1[#1], S. Sudha Sree[*2]

[#] *Department of Computer Science, Periyar University PG Extension Centre*
Dharmapuri - 636705, INDIA
[1]prabhaeac@gmail.com
[*] *Ph.D Research scholar, Department of Computer Science,*
Periyar University PG Extension Centre, Dharmapuri - 636705, INDIA
[2]sudhalishi@gmail.com

***Abstract*— Some of the most thrilling attacks done on networks to track, and requires very nominal effort on the attacker's part. Denial of Service (DoS) has the most destructive effects among the various online attacks which is hindering the security. The security experts are in tremendous pressure, to bring out effective defence solutions for the various attacks occurring recently. Variety of tools and coding are used to implement these destructive attacks. DoS attack has managed to exist in the internet for more than a decade as there is no steady solution to prevent this attack. The Intrusion prevention system is used as an extension of Intrusion detection system as a prevention technique for the DoS attacks. Network Intrusion Detection and Prevention system analyzes the packets coming and going through the interface. The paper provides the idea of various types of DoS attacks, detecting them and preventing them. There are many methods which are available to detect and resist the DoS attack. The detection and prevention techniques shown are effective for small network topologies and can also be extended to analogous large domains.**

***Keywords*— Put your keywords here, keywords are separated by comma.**

I. Introduction

Denial of Service is an attack which makes an information or data unavailable to its intended hosts. This attack can be carried out in various ways and various strategies are mentioned. The underlying aspect would be to congest victim's network and thus make it inaccessible by other client. There are many other ways of making service unavailable rather than just flooding it with abundant IP packets. The victim could also be attacked at various loopholes making it unstable which depends on the nature of the attack.

There are many manifestations of Denial of Service attacks but they ultimately have the same objective that is to deny or degrade users' ability to legitimately access network. DoS attacks are accomplished by draining the limited resources of network bandwidth by flooding with packets or exhausting host resources by consumption of CPU cycles, random memory, static memory or data structures .DoS attacks can generally be classified as either a Flood Attack or a Malformed Packet Attack and that where attacks originate simultaneously from several compromised sources that these can be classified as Distributed DoS attacks. An Intrusion Prevention System (IPS) is extension of Intrusion Detection System (IDS) which is the combination of Intrusion Detection System and Firewall.

An Intrusion Prevention System uses highly sophisticated and dedicated technology to provide increase levels of protection against DoS and Network Worm type attacks.

- Signature-based,
- Statistical anomaly-based,
- Firewalls
- Policy based and
- Honey pot based.

II. Overview of DoS Attacks

DoS attacks today have become a major threat to network security all over the world. They can be easily launched by anyone with the basic knowledge of network security. They don't require as much time and planning as some other attacks, in short they are cheap and efficient method of attacking networks. They can shutdown the company network by overflowing it with requests and thus affects availability of the network. With the help of easy to use network tools such as Trinoo, which can be easily downloaded of the internet any normal user can initiate an attack. DoS attacks usually works by exhausting the targeted network of bandwidth, TCP connections buffer, application/service buffer, CPU cycles, etc. DoS attacks use many users connected to a network known as zombies most of the time users are unaware of their computer is infected [8].

As a worst case, there are attacks that can cause permanent damage. These kinds of attacks are called the Permanent Denial of Service or Phlashing. Permanent Denial of Service attacks are mostly network based firmware updates and it aims to make the hardware inoperable. Firmware is the inbuilt code or program that is embedded on every electronic system for its proper functioning. When an attacker changes the

All Rights Reserved © 2016 IJARTET

firmware and replace it with a defective or corruptive code, the hardware could no longer be used.

III. Page Style

Classify the DoS Attacks, the information on which the classification was built was gathered from live and publicly available DDoS attack tools. On the basis of protocol DDoS can be further classified as Network/transport level and Application level DDoS attacks.

A. *Network/transport level DDoS attack:*

At this level, mostly TCP, UDP, ICMP, and DNS protocol packets are used to launch the attacks.

B. *Application level DDoS attack:*

These attacks generally consume less bandwidth and are stealthier in nature when compared to volumetric attacks. However, they can have a similar impact to service as they target specific characteristics of well-known applications such as HTTP, DNS, VoIP or Simple Mail Transfer Protocol (SMTP)[5]. These attacks focus on disrupting legitimate users services by exhausting the resources [5]. An application-level DDoS attack overloads an application server, such as by making excessive login, database lookup or search requests. Application attacks are harder to detect than other kinds of DDoS attacks. Since the connections are already established and the requests may appear to from legitimate users. However, once identified, these attacks can be stopped and back-traced to source more easily than any other types of DDoS attacks.

There are three general categories of attacks

1) Against users
2) Against hosts
   - •fork() bomb
   - •intentionally generate errors to fill logs, consuming disk space, crashing
   - •The power switch
3) Against networks
   - •UDP bombing
   - •TCP SYN flooding
   - •Ping of death
   - •Smurf attack

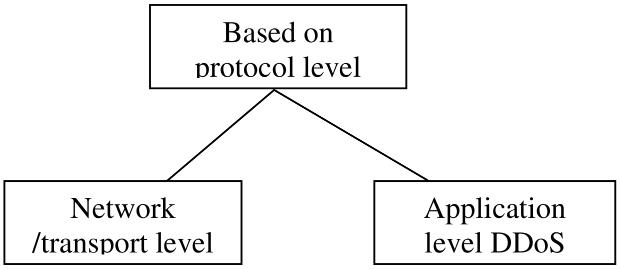


Fig.1 DDoS classification based on protocol level

There are several flavor of Denial of Service that could disrupt a normal service. The attacking methods are classified into two methods.

- First type would be to flood the network not leaving enough bandwidth for the legitimate packet which is termed as Flooding.
- The other method is to crash a hardware or software and make it inoperable. Web servers, routing devices, DNS look up servers are the common targets that could be crashed during an attack.

1) Ping of death: Ping of death is caused by an attacker sending a ping packet (normally 64 bytes), that is larger than the 65,535 bytes. Computer systems cannot handle an IP packet that is larger than the maximum IP packet size, and leads to crashing of computer systems. A packet of larger size can be sent if it is fragmented. When a receiving computer system reassembles the packet, a buffer overflow occurs, which leads computer to crash.

2) Ping of flood: Ping of flood is caused by an attacker over whelming the victim's network with ICMP Echo Request packets. This does not require extensive network knowledge as many ping utilities support this operation. Ping flood traffic consumes significant bandwidth on low to mid-speed networks bringing down a network to a crawl.

3) *Smurf Attack:* Smurf attach exploits the target by sending repeated ping request to broadcast address of the target network. The ping request packet often uses forged IP address which is the target site that is to receive the denial of service attack. The result will be lots of ping replies congesting the spoofed host. The network will not receive real traffic if the number of hosts replying to ping request is large.

4) SYN Floods: When establishing a session between TCP client and server, a hand-shake message exchange occurs between a server and client. A session setup packet contains a SYN field that identifies the sequence in the message exchange. An attacker may send a flood of connection request and do not respond to the replies, which leaves the request packets in the buffer so that legitimate connection request can't be accommodated.

5) Teardrop Attack: Teardrop attack exploits the network by sending IP fragment packets that are difficult to reassemble. A fragment packet first identifies an offset that can be used to assemble the entire packet so that the receiving system can reassemble them. In this attack, the attacker's IP puts an offset value in the subsequent fragments that confuses the receiving system thus making the system unable to handle that situation in turn leading to system crash.

6) Mail Bomb: This is the denied email service to the legitimate users when the unauthorized users send large number of email messages which has large attachments to a particular mail server thus filling up disk space.

7) CHARGEN and ECHO: enerally speaking, CHARGEN and ECHO type of attack is a kind of blind attack. There is no particular object from a hacker's point of view. The goal is to slow down a whole network. The idea behind this attack can be easily extended to other UDP services. If a poorly designed UDP server could not correctly deal with the abnormal incoming request, it is highly possible that a hacker could trigger infinite message exchanging between two innocent hosts.

IV. Classification of DoS Attacks

DoS attacks can be classified into five categories based on the attacked protocol level [5].

1) Network Device Level: Include attacks that might be caused either by taking advantage of bugs or weaknesses in software, or by trying to exhaust the hardware resources of network devices. One example of a network device exploit is the one that is caused by a buffer overrun error in the password checking routine.

2) OS level: DoS attacks take advantage of the ways operating systems implement protocols. One example of this category of DoS attacks is the Ping of Death attack [7]. In this attack, ICMP echo requests having total data sizes greater than the maximum IP standard size are sent to the targeted victim. This attack often has the effect of crashing the victim machine.

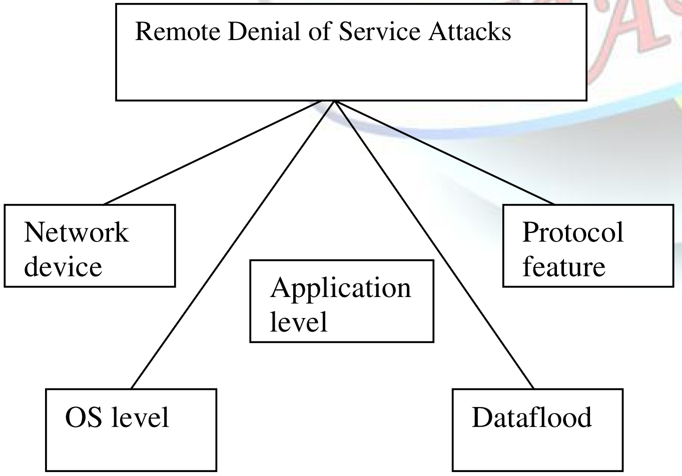


Fig.2 Classification of Remote Denial of Service attacks.

3) *Application-based attacks*: Try to settle a machine or a service out of order either by taking advantage of specific bugs in network applications that are running on the target host or by using such applications to drain the resources of their victim.

4) *Data flooding attacks*: An attacker attempts to use the bandwidth available to a network, host or device at its greatest extent, by sending massive quantities of data and so causing it to process extremely large amounts of data. An attacker could attempt to use up the available bandwidth of a network by simply bombarding the targeted victim with normal, but meaningless packets with spoofed source addresses. An example is flood pinging. Simple flooding is commonly seen in the form of DDoS attacks.

5) *Protocol features* :Take advantage of certain standard protocol features. For example several attacks exploit the fact that IP source addresses can be spoofed. Several types of DoS attacks have focused on DNS, and many of these involve attacking DNS cache on name servers.

V. DoS Attack Mechanism

Denial of service attacks can be further classified into many categories according to the style with which it is implemented.

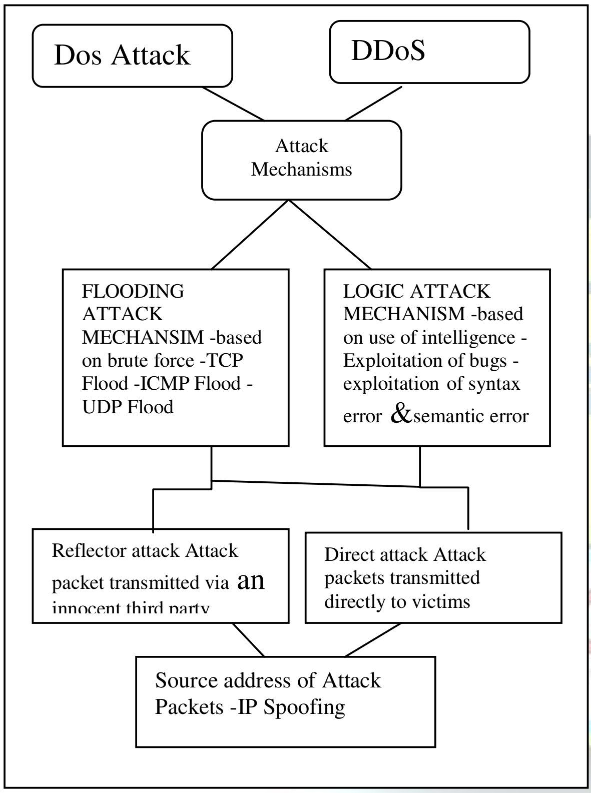
A. *Distributed Denial of service:*

The most stunning feature of the DDoS attack was that it appeared to emanate from multiple sources, not all of which were obviously directly owned or controlled by malicious parties. The first stage of this attack is to build its platform with many host systems that can work under remote commands. The attacker first scans the networks to hunt for vulnerable systems that are weak in security features. The compromised systems which are termed as zombies will be infected with relatively sophisticated software called as DDoS clients.

The programs used to remotely control compromised zombies have been termed bots (after robot) because they typically rely heavily on remote automation techniques borrowed from Internet Relay Chat (IRC) scripts of the same name. A group of zombies under the control of a single entity is called a zombie network or bot army. The controlling entity can directly bombard a target computer or network with a SYN flood or other DoS attack.

B. *Low Rate TCP Targeted DoS Attacks:*

The attacks called the Shrew attacks are carried out by exploiting the TCP timers. This attack uses a low rate burst designed to exploit TCP's retransmission timeout mechanism, throttles the bandwidth of a TCP flow in a stealthy manner. When there is congestion in TCP network, the congestion window is gradually reduced until the network is clear. Thus during congestion the sender's rate is reduced which apparently reduces the potential throughput. The TCP waits for the Retransmission Time out (RTO) to expire after which the data is sent again. When the congestion is more in the network, the RTO timer is doubled after which the packets are Retransmitted. Thus during a low rate attack, when packets are lost, TCP enters RTO. When an attacker is able to calculate this RTO time, the attacking packets are sent to create packet collision and loss thus pushing the TCP into waiting state.


Dos Attack
DDoS
Attack Mechanisms
FLOODING ATTACK MECHANSIM -based on brute force -TCP Flood -ICMP Flood -UDP Flood
LOGIC ATTACK MECHANISM -based on use of intelligence -Exploitation of bugs -exploitation of syntax error &semantic error
Reflector attack Attack packet transmitted via an innocent third party
Direct attack Attack packets transmitted directly to victims
Source address of Attack Packets -IP Spoofing

DoS attacks are a class of attacks initiated by individual or group of individuals exploiting aspects of the Internet Protocol to deny other users from legitimate access to systems and information. In the past DoS attacks has been associated to which were targeted at routers. If an attacker can force a router to stop forwarding packets, then all hosts behind the router are effectively disconnected. Recently though more forms of attacks are crafted to attack web servers, mail servers and other services. The book "Incident Response: Investigating Computer Crimes" provides a good description of DoS attacks which are Categorized in the following manner.

Destructive– Attacks which destroy the ability of the device to function, such as deleting or changing configuration information or power interruptions.

Resource consumption– Attacks which degrade the ability of the device to function, such as opening many simultaneous connections to the single device.

Bandwidth consumption– Attacks which attempt to overwhelm the bandwidth capacity of the network device. Network with small bandwidth may suffer from high bandwidth consumption instantaneously if it becomes target.

Response rate will depend on cooperation from service providers, for example in applying filters at upstream routers. DDoS on the other hand is a combination of DoS attacks staged or carried out in concert from various hosts to penalize the target host from further serving its function.

DDoS is term coined when the source of the attack is not coming from a single source, but multiple source. DDoS cannot be eliminated with merely filtering the source IPs since it is often launched from multiple points installed with agents.

Some known DDoS tools are Mstream, Trinoo, TFN2 K (Tribe Flood Network), Stacheldraht and Shaft. DDoS attack is an example of a bandwidth attack.

VII. Methods to Detect Types of DoS Attacks

To detect the attacks or malicious traffic on the network first step is to capture the packets. There are two modes present to capture the packet one is normal in that the packets intended to the system are only captured by the system. And other is promiscuous mode in which every packet which is going through the interface is captured by the system. So to monitor the network traffic the system has to be operated in promiscuous mode.

The overall architecture contains the following units.

1) *Packet Sniffer unit*: This unit captures the packet from the network interface either in promiscuous mode or in normal mode.
2) *Intrusion Detection or Pre processing engine*: In this unit it uses the different approaches to detect the attack depending on flow based analysis or protocol based analysis.
3) *Countermeasures*: The packet which contains the malicious code are identified or if any abnormal flow of packets is observed then the particular action is selected to avoid the intruder to enter in to the network.

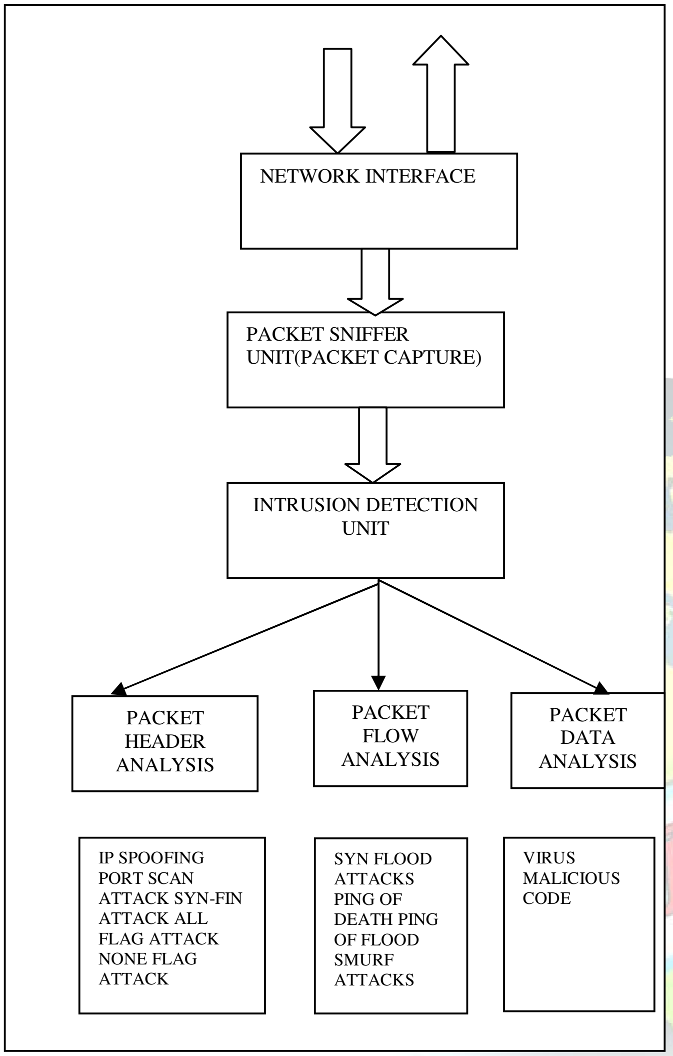

NETWORK INTERFACE
PACKET SNIFFER UNIT(PACKET CAPTURE)
INTRUSION DETECTION UNIT
PACKET HEADER ANALYSIS
PACKET FLOW ANALYSIS
PACKET DATA ANALYSIS
IP SPOOFING PORT SCAN ATTACK SYN-FIN ATTACK ALL FLAG ATTACK NONE FLAG ATTACK
SYN FLOOD ATTACKS PING OF DEATH PING OF FLOOD SMURF ATTACKS
VIRUS MALICIOUS CODE

Fig.4 . Architecture of DoS and DDoS

VIII. CONCLUSIONS

Distributed denial of service attacks is a complex and serious problem and consequently, numerous approaches have been proposed to counter them. It is important to recognize and understand trends in attack technology in order to effectively and appropriately evolve defense and response strategies. This paper gives adequate knowledge on various Denial of Service and DDoS attack mechanisms and also various types of DoS attacks in the network. It also suggests basic mitigation strategies that could be adopted in order to defend attacks. The DoS attacks are detected by analyzing of incoming packet and outgoing packets. The outline of various Intrusion detection and Intrusion prevention techniques are discussed. The methods to detect the DoS attacks in the network are discussed. The classifications described here are intended to think about the threats we face and the measures we can use to counter those threats.

REFERENCES

[1] Adrian Brindley,“Denial of Service attack and Emergence of ‘Intrusion prevention system’ ”, SANS institute Infosec Reading Room, Nov 1,2002.

[2] A. R. F. Hamedani, “Network Security Issues, Tools for Testing,” School of Information Science,Halmstad University, 2010.

[3] C. L. Schuba, I.V. Krsul, Makus G. Kuhn, E.H. Spafford, A. Sundaram, D. Zamboni,“Analysis of a Denial of Service Attack on TCP”, Purdue University, 1996.

[4] E. Earl Eiland, Scott C. Evans, T. Stephen Markham, Bruce Barnett, “Network Intrusion Detection: Using Mdlcompress For Deep Packet Inspection”,2008 IEEE.

[5] Hui Li, Dihua Liu , “Research on Intelligent Intrusion Prevention System Based on Snort”, 2010 Intern ational Conference on Computer, Mechatronics, Control and Electronic Engineering .

[6] M. A. Shibli, “MagicNET: Human Immune System & Network Security,” IJCSNS International.

[7] Journal of Computer Science and Network Security, Vol. .9 No.1, January 2009/

[8] *R. E. Mahan, “Introduction to Computer & Network Security,” Washington State University, 2000.*

[9] Shikha Goel , Sudesh Kumar , “An Improved Method of Detecting Spoofed Attack in Wireless LAN”, 2009 First International Conference on Networks & Communications 2009 IE.

[10] [10]R. C. Summers, Secure Computing – Threats and Safeguards, McGraw-Hill, 1997.

[11] Subramani Rao, Sridhar Rao, “Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis”, SANS institute Infosec Reading Room Sep 11,2011.

[12] Suchitha Patil, Dr.B.B. Meshram, “Network Intrusion Detection and Prevention Techniques”, International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012.

[13] Q. Gu, Peng Liu, “Denial of Service Attacks,” Texas State University, San Marcos.