ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (312-317), Month: October - December 2014, Available at: www.researchpublish.com

A Study of DOS & DDOS – Smurf Attack and Preventive Measures

[1]Sandeep, [2]Rajneet

***Abstract*: The term denial of service (DOS) refers to a form of attacking computer systems over a network. When this attack to be made at a large amount that is by using multiple computers, such an attack is called distributed denial of service (DDOS). The attack can be categorized as protocol based attacks, volume based attack and application layer attack. In this document it will be discuss Smurf attack (type of protocol based attack) that how it is undertaken by attacker and the techniques by which the user can protect its resources from this type of attack.**

***Keywords*: Denial of Service (DOS), Distributed Denial of Service (DDOS), Smurf Attack, ICMP, Echo Request, Broadcast, Spoofing, Ingress Filtering and Threshold value**.

I. INTRODUCTION

As it is very well known that the Internet is the life for almost all type of work done in daily routine now-a-days. Internet consists of hundreds of millions of computers distributed all around the world. Millions of people use the Internet daily, taking full advantage of the available services at both personal and professional levels.

But the connectivity or interconnectivity among computers on which the World Wide Web relies, however, renders its nodes an easy target for malicious users who attempt to exhaust their resources and launch Denial-of-Service (DoS) attacks against them.

The term *DOS refers* to a form of attacking computer system over a network. It is normally a malicious attempt to render a networked system unable but without permanently damaging it [1].

It is also possible that a lot of malicious hosts coordinate to flood the victim with an abundance of attack packets, so that the attack takes place simultaneously from multiple points. This type of attack is called a *Distributed DoS, or DDoS attack.*

The main purpose of the attackers to perform this attack is to effect the following are as [2]:

1. Consumption of computational resources, such as bandwidth, disk space, or processor time.
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.
4. Disruption of physical network components.

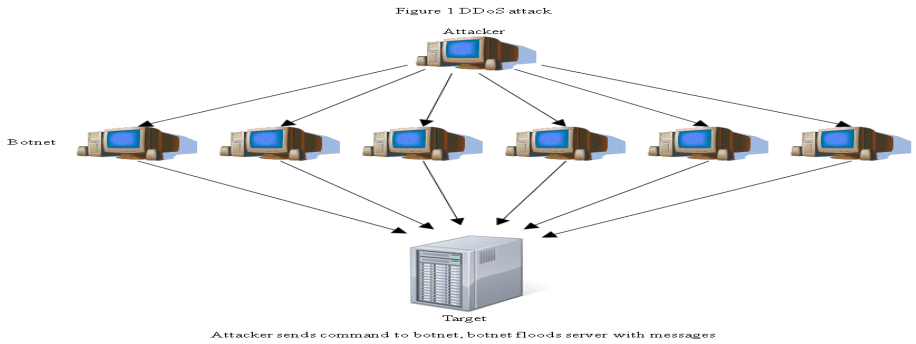


Figure 1: Shows the overview of DDOS [3]

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (312-317), Month: October - December 2014, Available at: www.researchpublish.com

II. DIFFERENCE BETWEEN DOS AND DDOS

It is important to differentiate between denial of service (DOS) and distributed denial of service (DDOS) attacks.

In a DOS attack, a single computer and a single internet connection is used to exhaust the victim resources by flooding a server with packets.

On the other hand DDOS attacks multiple computers and multiple internet connections are used which are distributed globally to make an attack. In this situation the victim will be flooded with the packets send from many hundreds and thousands of sources.

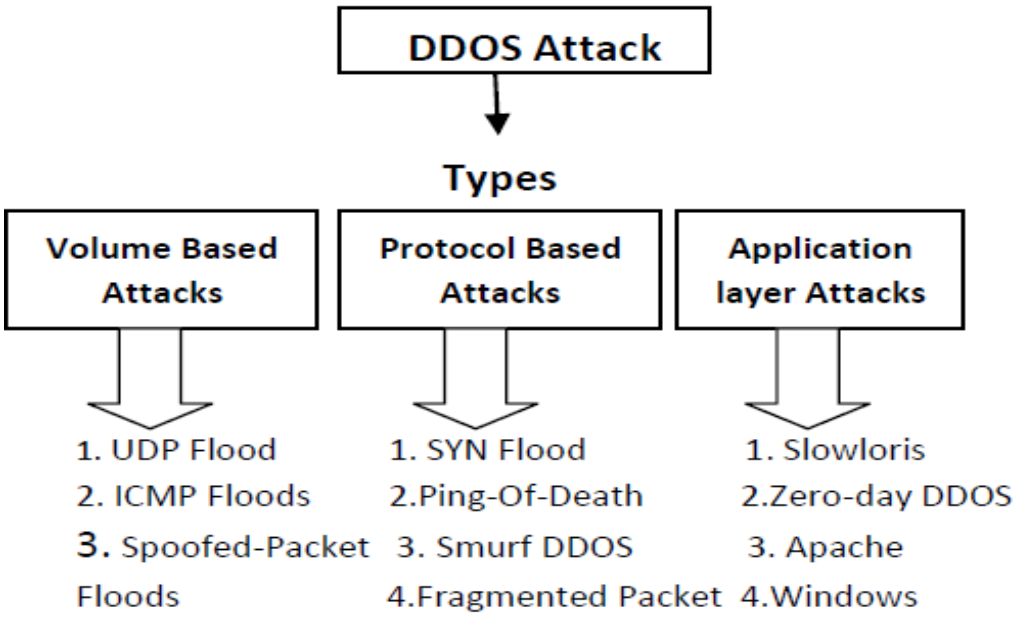
III. TYPES OF DDOS ATTACKS

DDoS attacks can be divided into three main categories:

1. ***Volume based attacks:-*** These include ICMP floods, UDP floods and other spoofed packet attacks. The main goal of the attacker is to consume the bandwidth of the victim's site. The magnitude of the attack is measured in bits per second (Bps).
2. ***Protocol based attacks***:- These include SYN floods, fragmented packet attacks, Ping of death, Smurf attack and more.

The main goal of the attacker is to consume actual server resources, such as firewall. The magnitude of the attack is measured in Packets per second.

3. ***Application layer based attack***:- These include attacks like Zero-day attack, Slowloris etc. the main goal of the attacker is to target the Apache, Windows or open BSD vulnerabilities and more.



Attack classification

There are two types of attacks:

1. Direct attack
2. Indirect/reflective attacks

Direct attack is those in which packets are send directly to the victim. On the other hand reflective attacks are those in which the packets are sending to the intermediate network and then they goes to the victim. The Smurf attack is example of reflective attack.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (312-317), Month: October - December 2014, Available at: www.researchpublish.com

IV. SMURF ATTACK

Some terms to be cleared before understanding Smurf Attack:-

ICMP: The ICMP is one of the core protocols of the Internet Protocols Suite. It is chiefly used by network computers operating systems to send error messages. For example that a requested service is not available or that a host or router could not be reached. [4]

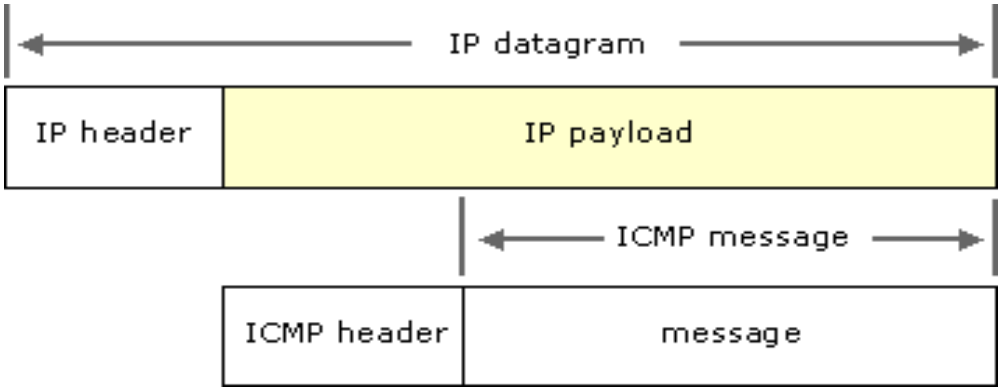


Figure 2: Shows ICMP components [5]

ICMP ECHO: The ICMP packets are generated or sent in case when the IP datagram generates errors or any diagnostic request occurs or for routing purposes. The Echo request is an ICMP massages whose data is expected to be received back in an echo reply (ping) containing the exact data received in the request message [6].

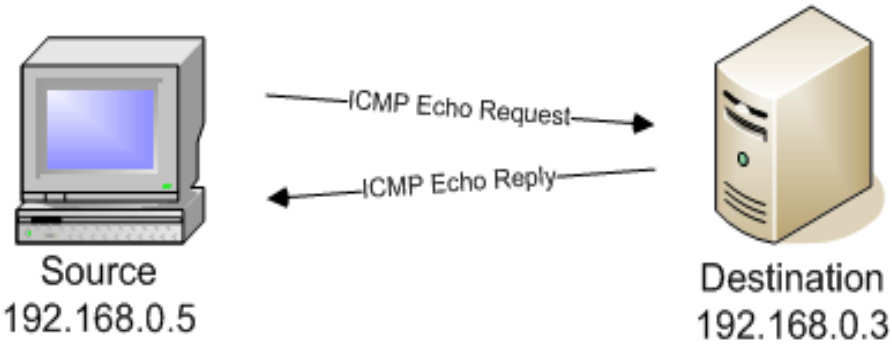


Figure 3: Shows the Echo Request [7]

BROADCAST: "A broadcast, in particular, is a simple message that is sent to all clients on a local area network." [8]. In an IP network, where there are no subnets, the broadcast address range is found by just setting the host bits of an IP address in the network to 1's.

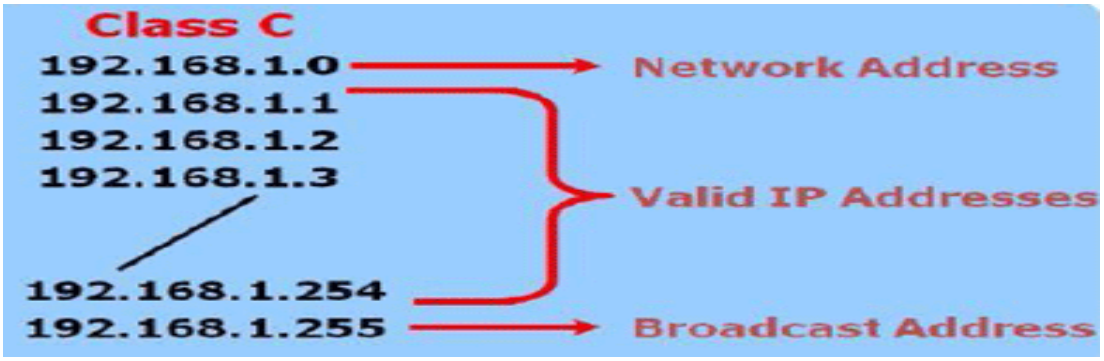


Figure 4: Shows Broadcast address for Class C [9]

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (312-317), Month: October - December 2014, Available at: www.researchpublish.com

SPOOFING: The word spoof means to trick or deceive .In IT world spoofing refers to tricking or deceiving other computer systems or computer users. This typically is done by hiding one's identity on the internet. It is done through e-mails or IP address etc. Here we are concern with the spoofing via IP address. IP spoofing is done by hiding computer IP address so that it becomes difficult to track the source of transmission. It is often used in DDOS attacks to overload a server. This may cause the server to either crash or become unresponsive to legitimate requests [10].

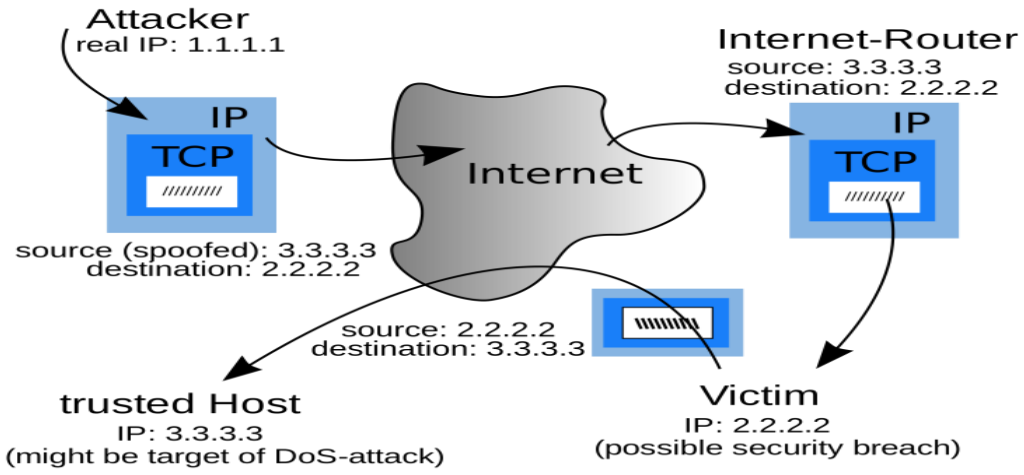


Figure 5: Shows IP Spoofing Technique (which is used for making Smurf attack)[11]

V. MEANING OF SMURF ATTACK

The Smurf attack is a way of generating significant computer network traffic on a victim network. This is type of denial-of-service attack that floods a target system via spoofed broadcast ping messages [12].

In other words we can say that, the Smurf attack is a distributed denial-of-service attack in which a large number of internet control message protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address [13].

Working of Smurf Attack:

Smurfing takes certain well known facts about internet protocols and internet control message protocols (ICMP) into account. ICMP is used by network administrator to exchange information about network state, and also be used to ping other nodes to determine their operational status. The nodes which are operational return an echo message in response to a ping message. The Smurf program builds a network packet that appears to originate from another address (this is known as spoofing and IP address). The packet contains an ICMP ping message that is addressed to an IP broadcast address, it means all the IP address in an given network.[14] The resulting echo responses to the ping message are directed towards the victim's IP address. Large number of pings and the resulting echoes can make the network unusable for real traffic [15].

Steps of Smurf attack

Step1: Victim IP address is to be identified by the attacker.

Step2: Intermediary site is to be identified by attacker which helps in amplifying attack.

Step3: Large amount of traffic will be sent by attacker to the broadcast address at particular intermediary sites.

Step4: These intermediaries will provide broadcast to all hosts which are there in a subnet.

Step5: Hosts will reply to network. [16]

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (312-317), Month: October - December 2014, Available at: www.researchpublish.com

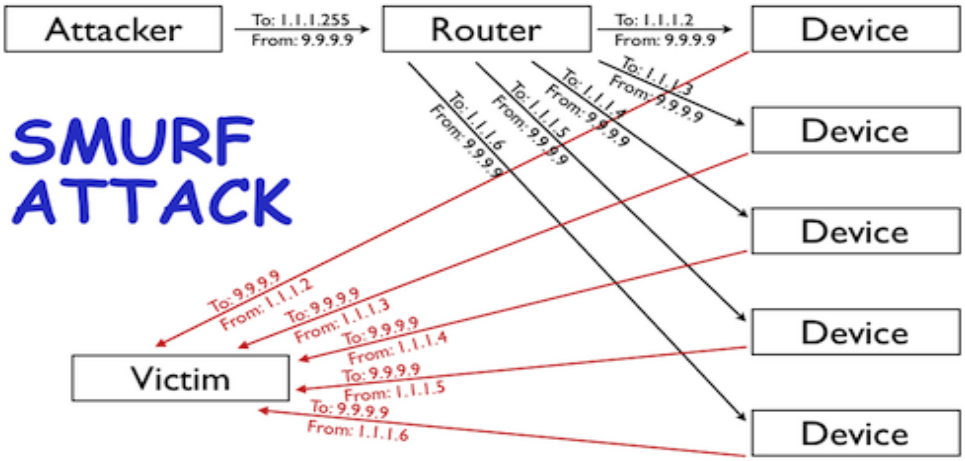


Figure 6: Shows the working of Smurf Attack [17]

VI. PREVENTIVE MEASURES

The protection against Smurf attack can be done by using following methods:

1. Configure individual hosts and routers not to respond to ping requests or broadcasts.
2. Configure routers not to forward packets directed to broadcast addresses [18].
3. To protect the device from Smurf attack use threshold method. According to this method, set the threshold values for ICMP packets. The router will drop the packets when the threshold values are exceeded. The syntax for setting the threshold value is: [19]

For example, to set threshold values for ICMP packets targeted at the router, enter the following command in

CONFIG mode: HP9300(config)# ip icmp burst-normal 5000 burst-max 10000 lockup 300

To set threshold values for ICMP packets received on interface 3/11:

HP9300(config)# int e 3/11

HP9300(config-if-e100-3/11)# ip icmp burst-normal 5000 burst-max 10000 lockup 300

***Syntax*:** ip icmp burst-normal <value> burst-max

<value> lockup <seconds>

The burst-normal value can be from 1 – 100000.

The burst-max value can be from 1 – 100000.

The lockup value can be from 1 – 10000.

The number of incoming ICMP packets per second are measured and compared to the threshold values as follows:

• If the number of ICMP packets exceeds the burst-normal value, the excess ICMP packets are dropped.

• If the number of ICMP packets exceeds the burst-max value, all ICMP packets are dropped for the number of seconds specified by the lockup value. When the lockup period expires, the packet counter is reset and measurement is restarted.

In the example above, if the number of ICMP packets received per second exceeds 5,000, the excess packets are dropped. If the number of ICMP packets received per second exceeds 10,000, the device drops all ICMP packets for the next 300 seconds (five minutes)[20].

4. Another solution is network ingress filtering, which rejects the attacking packets on the bases of the forged address.[21] This means on the bass of source address attacking packets are rejected, packets are to be filtered if packets are not coming from originating computer.

VII. CONCLUSION

DOS and DDOS attacks are done to effect the resources like bandwidth, server, disk space or processor time. This paper gives the information about the Smurf attack which is the protocol (ICMP) based DDOS attack undertaken by the attacker using IP Spoofing technique. The user can protect its devices from a smurf attack by using techniques like Ingress filtering and threshold values.

REFERENCES

[1] DoS - Denial of Service By Bradley Mitchell http://compnetworking.about.com/od /network security privacy /g/ denialofservice.htm

[2] Denial-of-services attack, from Wikipedia: http://en.wikipedia.org/wiki/Denial-of-service attack

[3] http://www.cse.wustl.edu/~jain/cse571-11/ftp/cyberwar/fig1.gif

[4] The Internet Control Message Protocol, from Wikipedia: http:// en.wikipedia.org /wiki/Internet _ Control _Message _Protocol

[5] https://www.google.co.in/search?q=ICMP&es_sm

[6] Ping, from Wikipedia: http://en.wikipedia.org/wiki/Ping

[7] http://www.networkuptime.com/nmap/images/PE_ping.gif

[8] How a Broadcast Address Works. [Online document] Available: http://learn-networking.com/network-design/how-a-broadcast-address-works

[9] https://www.google.co.in/search?q= bROADCAST+IP+CLASS&facrc

[10] http://www.techterms.com/definition/spoofing

[11] http://upload.wikimedia.org/wikipedia/commons/thumb/7/72/IP_spoofing_en.svg/2000pxIP_spoofing_en.svg.png

[12] Smurf attack, from Wikipedia: http://en.wikipedia.org/wiki/Smurf_attack

[13] http://en.wikipedia.org/wiki/Smurf attack

[14] http://seachsecurity.techtarget.com/definition/smurfing Posted by : Margaret Rouse WhatIs.com

[15] http://www.techopedia.com/definition/17294/smurf-attack

[16] Kavita Choudhary, Meenakshi, Shilpa (ITM University, Gurgoan, Haryana, India) "Smurf Attack: Attacks using ICMP" IJCST Vol.2, Issue 1, March 2011 (ISSN:2229-4333)

[17] http://blog.cloudflare.com/content/images/smurf_attack_diagram.png.scaled500.png

[18] Farhan Sajjad , school of computer science , university of Windsor, 401 Sunset Avenue Windsor Ontario, N9B 3P4, Canada, sajjad@uwindsor.ca "Denial of Service-The Smurf Attack".

[19] Brocade Turbolron 24X series configuration guide R08.0.00a Documentation@broad.com "Protecting against Denial of DeviceAttacks"www.brocade.com/downloads/documents/html_product_manuals/f1_08000a_TI_CFG/wwhelp.htm#context=fastlron_IT_config_Guide_08000a&file=F1_DoS_protection.35.2.html

[20] http://www.hp.com/rnd/support/manuals/pdf/release_06628_07110/Bk2_ApixB_DoS_Protection.pdf "Protecting Against Denial of Service Attacks"

[21] http://www.wegilant.com/what -is-a-smurf-attack/