Smurf Attacks: Attacks using ICMP

[1]Kavita Choudhary , [2]Meenakshi, [3]Shilpa
[1,2,3]ITM University, Gurgaon, Haryana, India

Abstract
IP Address Spoofing attacks are used to take control over computer by unauthorized means, whereby the attacker sends messages to a computer with fake IP address indicating that the message is coming from trusted host. In IP Address Spoofing attack through ICMP , attackers use incorrect source IP addresses in attack packets (spoofed IP packets) to hide identity from victim, it also reduce the risk of trace-back and avoid detection. In this paper, we investigate the methods adopted in order to perform attacks through Internet Control Message Protocol (ICMP) messages, also known as Smurf Attack. We present the comparative analysis of the various solutions of Smurf Attack.

Keywords
ICMP, Smurf Attack, IPTables, Ingress Filteing, IP Address.

I. Introduction

In IP address spoofing Internet Protocol[1,2,5] packets are created with forged source IP address. The main aim of spoofing is for hiding sender identity. In this attacker unauthorizingly access computer or network showing as if malicious message came from trusted machine by spoofing that machine address. This spoofing can be used in denial of service attack where victim flows with large traffic but attacker has no problem if responses come from attack packets and spoofed address packets are required for these attacks.

Smurf attack[2-4] overflows network traffic which is a kind of denial of service attack where with the help of spoofed broadcast ping messages flooding of target system is done. Generally smurf is used by attackers so that attack part cannot be operated. Smurfing can make use of Internet Protocol (IP) and Internet Control Message Protocol (ICMP). Basically network nodes and their administrators use ICMP for exchanging information regarding state of network. ICMP ping other nodes to check whether they are operating or not. A node which is operating basically sends an echo message when we send any ping message. Fig.1 will explain the working of smurf attacks.

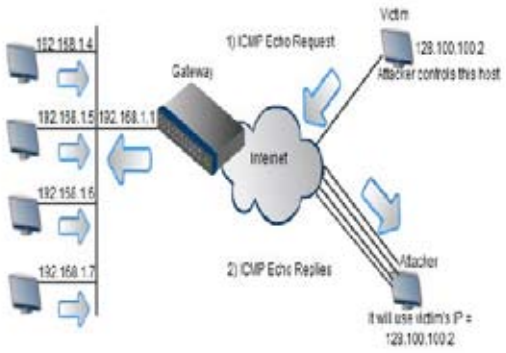

Fig.1: Smurf Attack

Smurf program forms a network packet seems to originate from another address that means spoofing an IP address. The packet basically has ICMP ping message addressing the IP broadcast address that means all IP addresses are within a gi.ven network. When ping messages will be sent responses come back to victim address. Due to flooding of no of pings and echoes inside a network it may cause hurdles for real traffic to pass through.

A. ICMP echo attacks

Whenever attacker sends an ICMP[3] echoes to no of hosts in a given subnet reply will come back showing which hosts are alive.When spoofed ICMP echo requests are sent to no of subnets victim will receive ICMP echo replies through every machine.

B. ICMP Redirect Attacks

ICMP redirect messages route traffic on particular route or particular host which is not a router actually. This is really simple as we just need to send spoofed ICMP message as if coming from a host gateway.Fig.2(a) and 2(b) will depict the process.

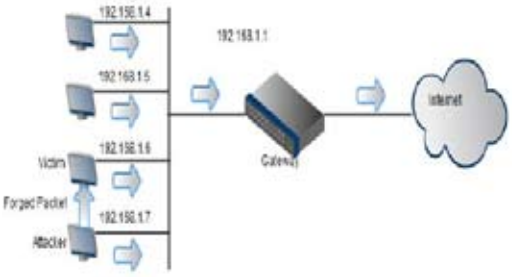

Fig.2(a): ICMP Redirect Attack

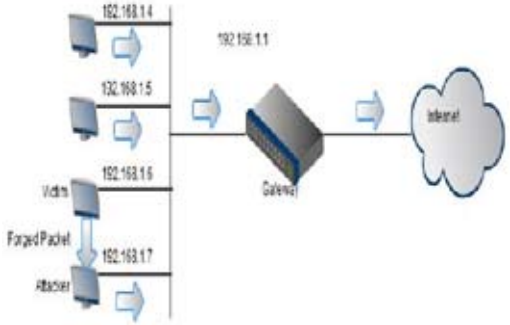

Fig. 2(b): ICMP Redirect Attack

C. ICMP Destination unreachable attacks

Gateways use ICMP Destination unreachable message to define datagram is not delivered. This can used even to cut some of the nodes in a network. It is also denial of service attack.Fig.3 shows the destination unreachable attack.

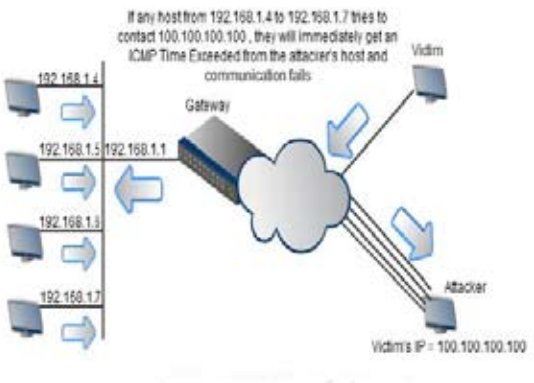

Fig.3: ICMP Destination Unreachable Attack

II. Steps defining 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.

III. Analysis for solutions of Smurf Attack

1. Filtering should be done at network's edge where customer are connected or at network's edge which are connected to upstream providers for fighting with spoofed packets coming from downstream networks or from upstream networks.
2. At each and every network router IP broadcast addressing is to be disabled but this is rarely used.
3. Ingress Filtering[2]: On the basis of source address attacking packets are rejected, packets are to be filtered if packets are not coming from originating computer.
4. Packet Filtering: Router connecting one of the network to other is known as border router. One way of checking threat due to IP Spoofing is to inspect packets during their arrival or departure in a network asking for invalid source addresses. If such kind of filtering is performed on all the routers then IP address spoofing will get reduced.
In Linux Filtering will be activated by using following:
Echo2>/proc/sys/net/ipv4/conf/*/rp_filter
5.Iptables: They are used for filtering inbound ICMP messages, as it is one of the solution for attack.

```
iptables -A IN_ICMP -p icmp –icmp-type echo-request -s $ sip -j ACCEPT
iptables -A IN_ICMP -p icmp –icmp-type echo-reply -s $ sip -j ACCEPT
iptables -A IN_ICMP -p icmp –icmp-type destination-unreachable -j ACCEPT
iptables -A IN_ICMP -p icmp –icmp-type source-quench -j ACCEPT
iptables -A IN_ICMP -p icmp –icmp-type time-exceeded -j ACCEPT
iptables -A IN_ICMP -p icmp –icmp-type parameter-problem -j ACCEPT
```

IV. Conclusion

If filtering is done at edge of the network then load on the network will increase. This method is not much efficient.It its very difficult if we need to disable IP broadcast address at each and every network router even though this is one of the solution for smurf attack.For Ingress filtering network should have information regarding which IP address it is connected to in network where it can send which is not possible always. So for a network having single connection through Internet cannot know whether packet is spoofed or not.For Packet filtering if a spoofed IP address lies within valid address range then it helps in attacking .As source IP address is within valid range then it would be easier to trace packets.Linux Iptables basically avoid IP spoofing and bad address attacks. With the help of ICMP we can overcome IP spoofing using these Linux Iptables. Fig.4 shows how smurf attack takes place and how to overcome by these attacks.

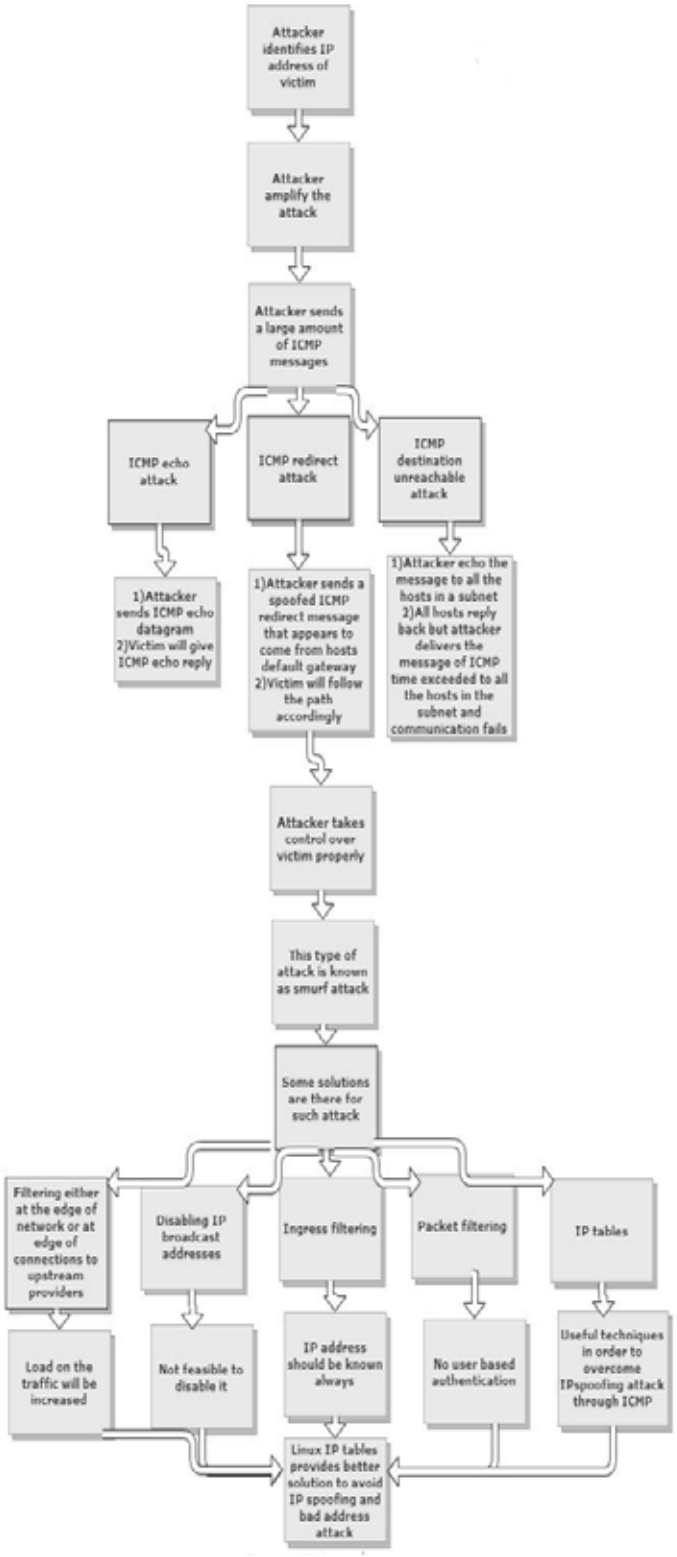

Fig.4: Analysis of Smurf Attack

References

[1] Zhenhai Duan, Xin Yuan, Jaideep Chandrashekar, "Controlling IP Spoofing Through Inter-Domain Packet Filters", IEEE INFOCOM, 2006
[2] Abhrajit Ghosh, Larry Wong, Giovanni Di Crescenzo, Rajesh Talpade, "InFilter: Predictive Ingress Filtering to Detect Spoofed IP Traffic", Proc. of the 25th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'05) 1545-0678/05 , 2005 IEEE
[3] Sanjeev Kumar, "Smurf-based Distributed Denial of Service (DDoS), Attack Amplification in Internet", Second

International Conference on Internet Monitoring and Protection (ICIMP 2007) 0-7695-2911-9/07 2007 IEEE
[4] Gholam Reza Zargar, Peyman.Kabiri, "Identification of Effective Network Features to Detect Smurf Attacks", 978-1-4244-5187-6/09/2009 IEEE
[5] [Online] Available : www.wikipedia.org

Kavita Choudhary completed her B.E. in Computer Science and Engineering from JECRC, Jaipur, India with Honours in 2005 and M.Tech (IT) from Guru Gobind Singh Indraprastha University, Delhi, India in 2010. Presently, she is working as Assistant Professor in ITM University, Gurgaon, India. She has five years of experience in teaching. She has published and presented many papers in national and international conferences. Her research area is Analysis of Effort Estimation using Genetic Algorithm.