Denial of Service – The Smurf Attack

Farhan Sajjad

School of Computer Science
University of Windsor
401 Sunset Avenue
Windsor Ontario, N9B 3P4, Canada
sajjadf@uwindsor.ca

Abstract – **Smurf Attack is a type of network-level Denial of Service (DoS) Attack by overwhelming the victim machine with Internet Control Message Protocol (ICMP) echo replies from computers in the same broadcast network by sending forged ICMP echo request to an IP broadcast address using the IP address of the victim machine, making computers in the same network reply to the requests, flooding the victim machine with ICMP echo replies. In this document it is discussed how such an attack could be engineered and detected using freely available tools in the Internet.**

Keywords – **Smurf Attack, Denial of Service Attack, ICMP, ICMP Echo Request, ICMP Flood, Nemesis.**

1 – INTRODUCTION

According to Wikipedia, the Smurf Attack is "a way of generating significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages." [1]. In this technique, the engineer of the attack forges ICMP echo request packets with the IP address of the victim as the source address and broadcasts the request on the network, making the computers in the network to send replies to the ICMP echo requests. Of course, in a multi-access broadcast network, the number of replies could be overwhelming as hundreds of computer may listen to the broadcast. Essentially, forging of the ICMP packet is a trivial task for a programmer as any network packet is a stream of binary data in a specified format described by the standards of the network protocol. Interestingly, the attack is named after the original C file "smurf.c" [2] which contained the source code to create such an attack but with time and the advancement of computing, now we do not even need to write our own programs to craft these packets as there as various tools freely available on the Internet capable of performing this task.

2 – BACKGROUNDS

A. *ICMP and ICMP Echo*

The ICMP "is one of the core protocols of the Internet Protocol Suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached." [3]. Typically, the ICMP packets are generated or sent in case the IP datagrams errors or diagnostic and routing purposes, and the echo request is "an ICMP message whose data is expected to be received back in an echo reply ("ping") containing the exact data received in the request message." [4].

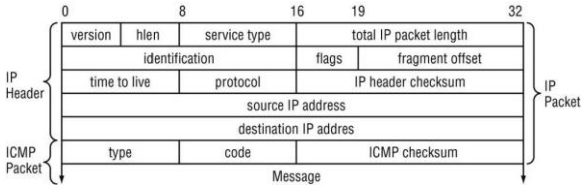

Figure 1 – The ICMP Header [5].

B. *No IP Directed-Broadcast*

"A broadcast, in particular, is a simple message that is sent to all clients on a local area network." [6]. 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 1s.

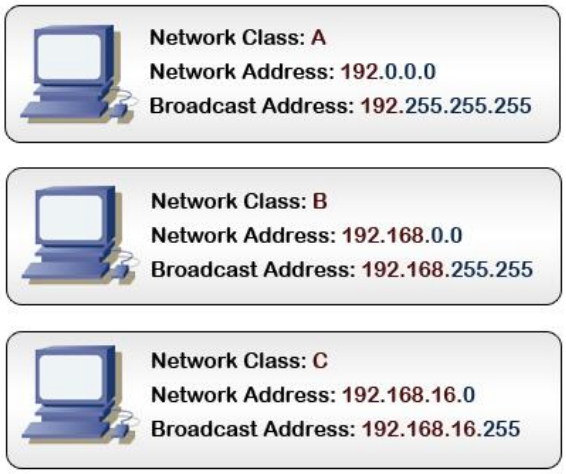

Figure 2 –Broadcast Address without Subnets [6]

In a network with subnets, the process is like this:

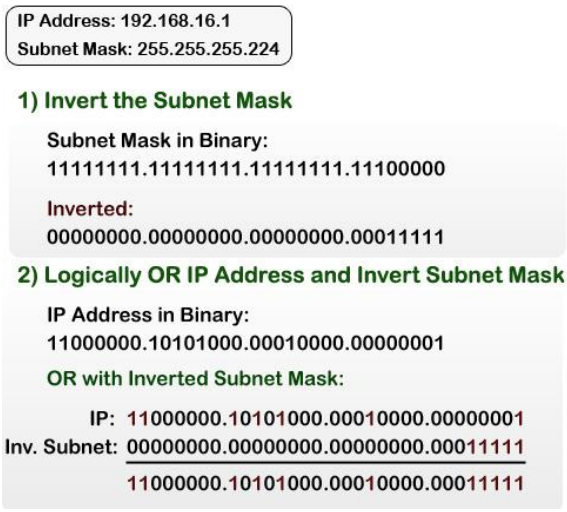

Figure 3 – Broadcast Address with Subnets [6]

So when a no IP directed-broadcast is made for a certain broadcast address range, all computers in the broadcast zone get the broadcasted message.

C. 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 [7]:

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."
5. "Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately."

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.

D. Nemesis

For our task of crafting the ICMP packets, we will use "Nemesis" which is a command-line network packet crafting and injection utility. It can natively craft and inject ARP, DNS, ETHERNET, ICMP, IGMP, IP, RIP, TCP and UDP packets. Using the IP and the Ethernet injection modes that it supports, almost any custom packet can be crafted and injected. It is freely available for download and usage [8].

The command parameters for crafting and sending an ICMP packet with Nemesis are [9]:

```
-i <ICMP type>
  -c <ICMP code>
  -s <ICMP sequence number>
  -m <IP address mask for ICMP address
mask>
  -G <Preferred gateway IP address for
ICMP redirect>
  -e <ICMP ID>
  -P <Payload file>
  -q <ICMP injection mode>
     -qE echo, -qM mask, -qU unreach, -
qX time exceeded,
     -qR redirect, -qT timestamp
```

Since the ICMP Header is wrapped using the IP Header, these are the IP parameters required for crafting ICMP packets as well [9]:

```
  -S <Source IP address>
  -D <Destination IP address>
  -I <IP ID>
  -T <IP TTL>
  -t <IP TOS>
  -F <IP fragmentation options>
     -F[D],[M],[R],[offset]
  -O <IP options file>
```

E. Wireshark

Wireshark is a GUI based network protocol analyzer that inspects incoming network packets

and finds out if there is any kind of anomaly in them. It runs on all major platforms and is a highly regarded tool among network and security experts because of its ability to deeply inspect hundreds of kinds of protocols. It will be run in our victim machine to track the ICMP Echo replies. Wireshark is also freely available for download and usage [10].

3 – Description of the Attack

A Smurf attack is a technique by which the attacker can generate a reasonably small amount of network traffic in form of spoofed ICMP Echo request packets and consequently cause a virtual outburst of traffic at the victim machine and network. The method used is as follows:

1. The attacker sends out, via no IP directed-broadcast, ICMP Echo request packets with the source IP address forged to be that of the victim of the intended Smurf attack.
2. All of the hosts which are on the broadcast segment of the network each pick up a copy of the ICMP Echo request, and sends an ICMP Echo reply back to what they think is the source of the request. If many hosts are on the LAN, the amplification factor can be considerably high.

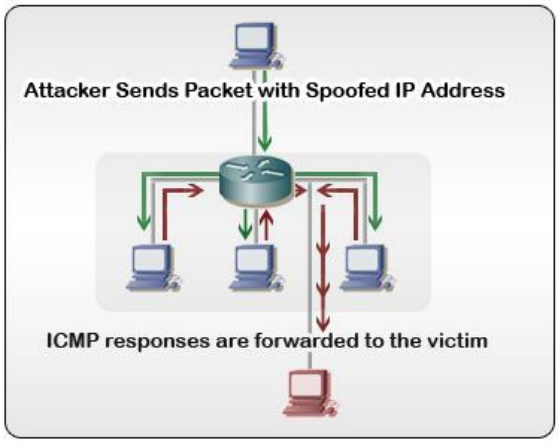

Figure 5 – A Smurf Attack [11]

It is to be noted that the attacker can use large packets (i.e. maximum allowed or highest possible MTU) to increase the effectiveness of the attack.

With the Smurf attack, not only can the attacker cause problems for the victim by making it inaccessible by overwhelming it with ICMP Echo replies, the flood of traffic because of these ICMP Echo requests can in fact be so great that it can create a network congestion in the network segment of the victim machine.

6 – Preventing Smurf Attacks

According to Wikipedia, the prevention of Smurf attacks is two-folds [1]:

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. Until 1999, standards required routers to forward such packets by default, but in that year, the standard was changed to require the default to be not to forward."

In addition to these two simple solutions, Craig A. Huegen's article on prevention of Smurf attack is highly revered [12].

5 – The Experiment

The experiment will be carried out by broadcasting of spoofed ICMP Echo packets from an attacking machine with the aid of Nemesis and the machine that will be attacked will have Wireshark running to detect the attack. Any computer connected to the broadcast network segment will become an active participant of the experiment by simply responding to the ICMP Echo requests.

A. The Testing Environment

The testing environment consists of:

1. A 32-bit Windows based victim machine that will be attacked with spoofed ICMP packets. It will be running Wireshark to detect any such attack.
2. A 32-bit Linux Ubuntu machine (hosted on a virtual machine) that will be the attacker, spoofing ICMP packets using Nemesis.
3. At least three 32-Bit Linux Ubuntu machines (also hosted on virtual machines) which will be participating as the computers residing in the broadcast network.
4. The attacker, the participating machines that simply replies to the ICMP Echo requests and the victim resides on a routed network, connected by a router.

B. The Testing Parameters

The experiments will be conducted with a number of parameters that would demonstrate how effective the detection system is, and how the number of computers participating in the reply process and ICMP Echo request generation rate affect the effectiveness of the attack. The initially planned variables are:

1. ICMP Echo request Packets spoofed at various rates. (At least 10 different rates.)
2. Increasing and decreasing the number of machines in the broadcast segment which replies to the ICMP Echo requests.
3. Loading the victim machine with processing task to see if packets are dropped at higher loads.

6 – SUMMARY

In this document, the idea of engineering a Smurf attack, detection and prevention of such attacks is discussed very briefly. The tools and testing environment proposed is preliminary and are subject to change if need be. In my future work, the construction, implementation and execution of the experiment will be performed and the results will be published.

REFERENCES

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

[2] smurf.c, [Online document] Available: http://personal.telefonica.terra.es/web/alexb/e/smurf.c

[3] The Internet Control Message Protocol, from Wikipedia: http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

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

[5] The ICMP Header. [Online document] Available: http://blog.csdn.net/xuhx/archive/2008/04/16/2297266.aspx

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

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

[8] Nemesis Packet Injection Tool Suite. [Online document] Available: http://nemesis.sourceforge.net/

[9] Manpage of NEMESIS-ICMP. [Online document] Available: http://nemesis.sourceforge.net/manpages/nemesis-icmp.1.html

[10] Wireshark. [Online document] Available: http://www.wireshark.org/

[11] Securing Cisco Routers with No IP Directed-Broadcast. [Online document] Available: http://learn-networking.com/network-security/securing-cisco-routers-with-no-ip-directed-broadcast

[12] Craig A. Hugen, The latest in denial of service attacks: "Smurfing". Description and information to minimize effects. [Online document] Available: http://www.pentics.net/denial-of-service/white-papers/smurf.cgi