ICMP Smurf Attack

Student Id: 1505095

July 2019

1 Introduction

1.1 Smurf attack

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”. In this technique, the attacker 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.

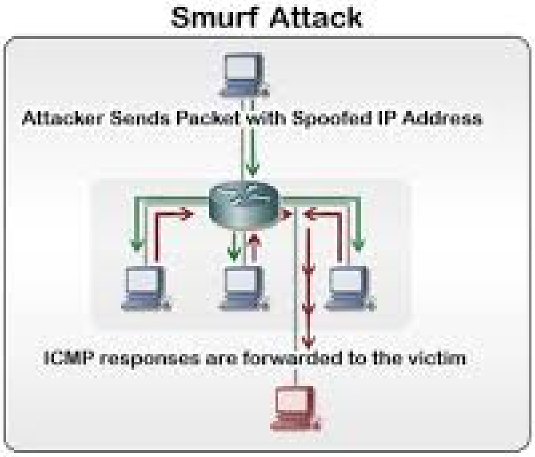
Smurf Attack
Attacker Sends Packet with Spoofed IP Address
ICMP responses are forwarded to the victim

Figure 1: A smurf attack

Testing topology

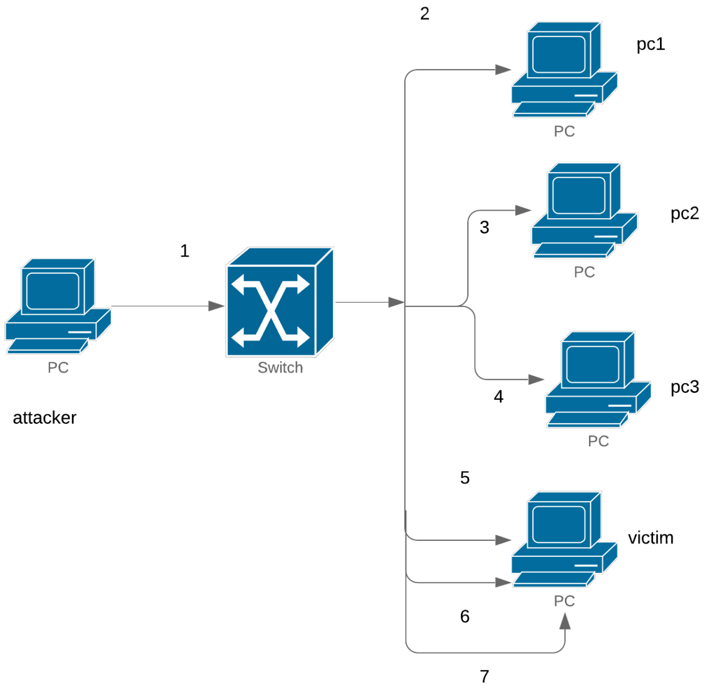

Figure 2: A smurf attack testing topology

1.2 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”. 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.”

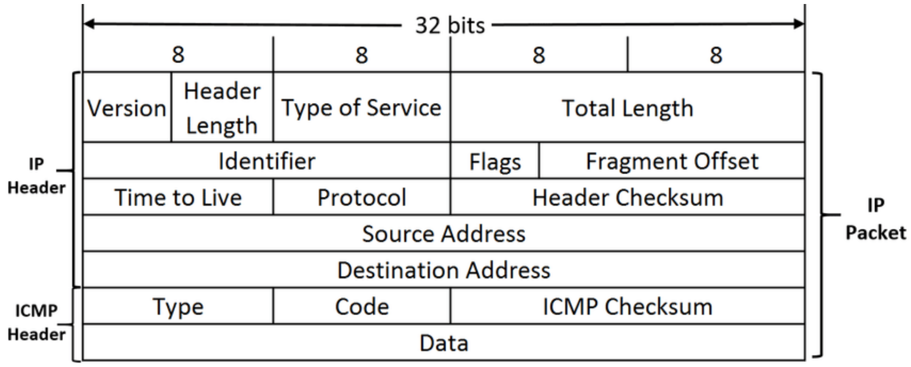

Figure 3: ICMP header

2 Timing and attack strategies

2.1 Timing diagram of ICMP

ICMP is commonly used by network tools such as ping or traceroute. **PC1** wants to test whether it can reach **PC2** over the network. **PC1** will start the ping utility that will send ICMP Echo Request packets to **PC2**. If **PC2** is reachable, it will respond with ICMP Echo Reply packets. If **PC1** receives no response from **PC2**, there might be a problem on the network.

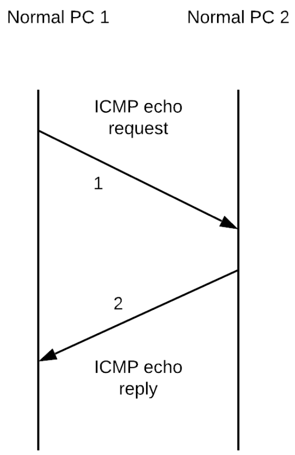

Figure 4: Internet Control Message Protocol

2.2 Attack timing diagram

For smurf attack, attacker send ICMP echo request with spoofed source IP of the victim to router of the IP broadcast network. The reflectors in that network send the ICMP echo reply to the source IP address of the victim; thus flooding the target system.

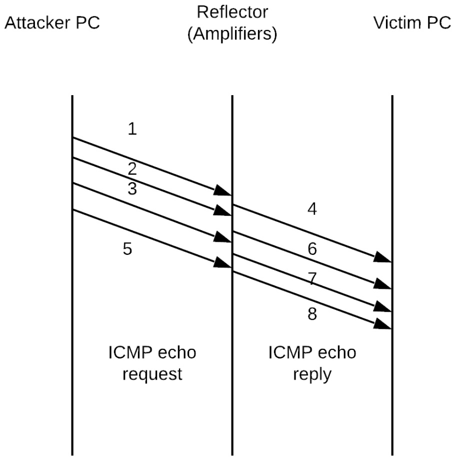

Figure 5: ICMP Smurf attack

2.3 Attack strategies

For initiating a "smurf attack", the attacker program has a list of broadcast addresses which it stores into an array, and sends a spoofed icmp echo request to each of those addresses in series and starts again. The result is a devastating attack upon the spoofed ip with, depending on the amount of broadcast addresses used, many, many computers responding to the echo request.

Generally smurf is used by attackers so that attack part cannot be operated. Smurfing can make use of IP and 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.

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 given 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.

2.3.1 Steps defining Smurf Attack

- Victim IP address is to be identified by the attacker.
- Intermediary site (a broadcast address) is to be identified by attacker which helps in amplifying attack.
- Large amount of traffic will be sent by attacker to the broadcast address at particular intermediary sites.
- These intermediaries will provide broadcast to all hosts which are there in a subnet.
- Hosts will reply to network.

3 Frame details and modifications in header

For ICMP Smurf attack, attacker does not need to modify IP and ICMP header. Attacker only need to set the victim's IP address in the "source address" field of the IP header.

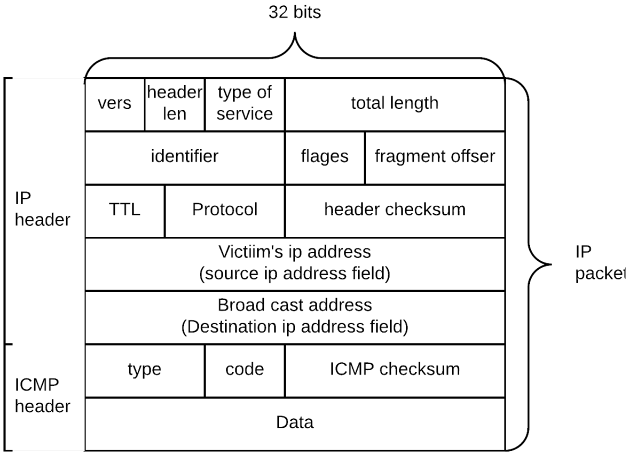

Figure 6: ICMP Smurf attack

4 Justification

Above design will work because the attacker has identified the IP address of the victim. Attacker then uses other PCs in the network to amplify the attack by sending a large amount of ICMP messages. ICMP echo reply is redirected to source address of the victim. Attacker sends a spoofed ICMP redirect message that appears to come from hosts default gateway. Victim reflectors will follow the path accordingly flooding the victim system causing link congestion Endpoint resource exhaustion.