Security Term Project

Attack name: ICMP ping spoofing

Shashata Sawmya
Student Id. : 1505089

July 30, 2019

Department of Computer Science and Engineering
Bangladesh University of Engineering and
Technology (BUET)
Dhaka - 1000

Contents

1 Introduction

The Internet Protocol (IP) is used for host-to-host datagram service in a system of interconnected networks. Occasionally a gateway or destination host will communicate with a source host, for example, to report an error in datagram processing. For such purposes this protocol, the Internet Control Message Protocol (ICMP), is used. ICMP, uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and must be implemented by every IP module.

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software. Ping measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source.

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply. The program reports errors, packet loss, and a statistical summary of the results, typically including the minimum, maximum, the mean round-trip times, and standard deviation of the mean.

2 ICMP Ping Spoofing Attack Definition

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. In ICMP ping spoofing, a ping is sent with false source IP address which gets the reply from the server although it didn't send the original ICMP REQUEST packet.

3 Topology Diagram

The topology diagram of the attack consists of two PC. One for simulating the victim and another for simulating the Attacker. There will be a router which will route the request and reply packets to and from the server.

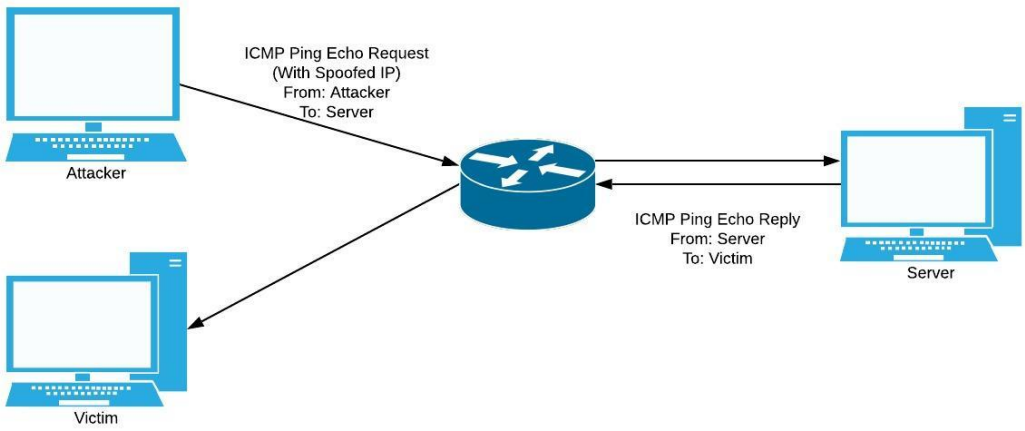

Figure 1: ICMP ping spoofing topology diagram

4 Timing Diagram of the Original Protocol

In original ICMP ping protocol, the initiating host sends an ICMP echo request packet, and awaits for an ICMP echo reply packet send from the other end point. If the reply is received, there are valid routes to and from the destination node (host), and the network layer of the OSI model is working properly.

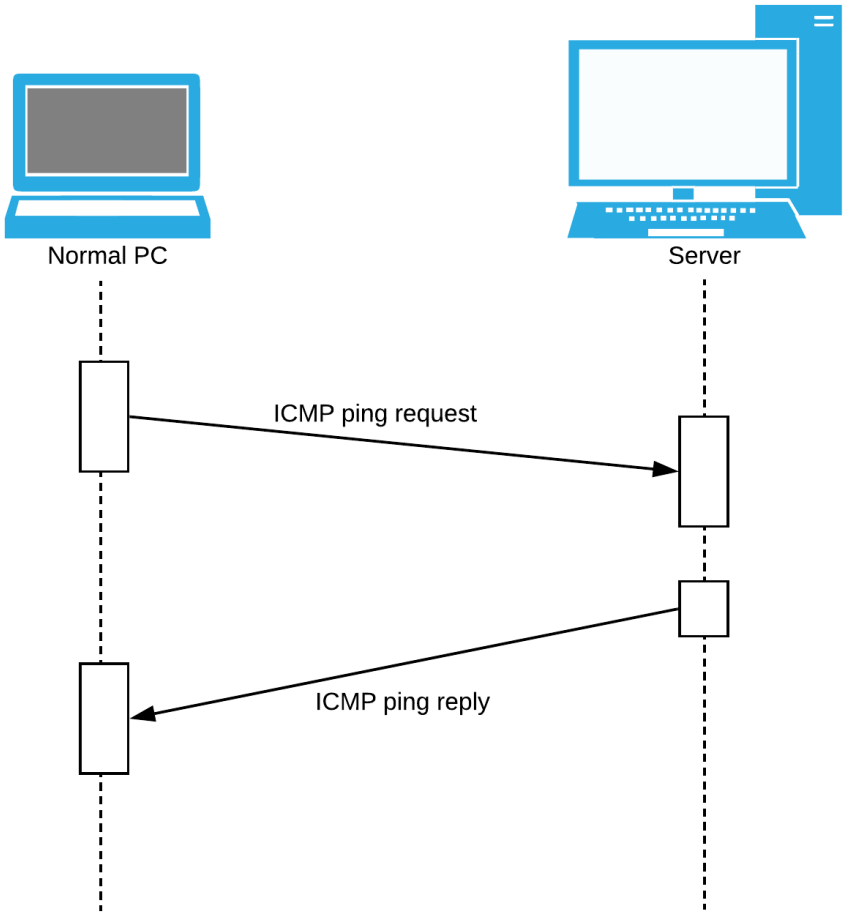

Figure 2: Timing Diagram of the Original Protocol

5 Timing Diagram of the Attack

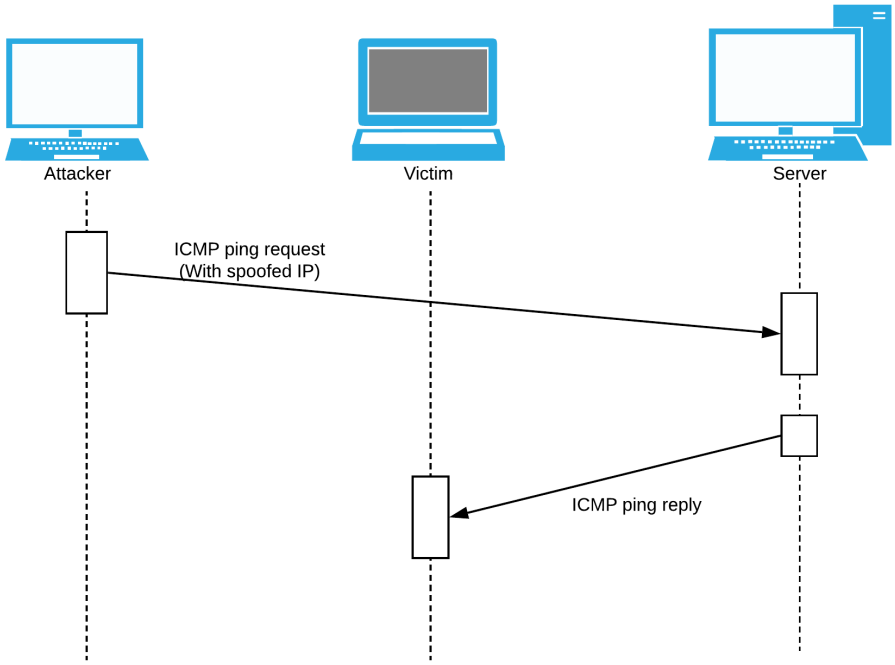

Figure 3: Timing Diagram of the Attack Protocol

6 Attack Strategy

- The server will have to listen to ICMP request packet and generate reply packet as soon as it get's the request.
- The spoofing mechanism will be implemented using socket programming by fraudulently setting the source IP to another IP other than our computer.
- We will implement the system of changing the payload of the ping request by manipulating the payload field of the Ipv4 Ip header.
- We will use wireshark and tcpdump C library to sniff the spoofed packets.
- We can use pcap to listen between two ports for the packets transferred and analyze the packets to get a destination port.

7 Some important C/C++ Libraries to be used

1. <sys/socket.h>
2. <netinet/ip.h>
3. <arpa/inet.h>
4. <netinet/ipicmp.h>

8 Packet/Frame Details

IP Datagram

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			

Figure 4: Ipv4 and ICMP header

The IP Datagram header's source IP address will be modified with the spoofed IP and the type of message in ICMP header will be always 0 or 8 for ping reply and ping request respectively. We can modify the

payload data field in the ICMP header to send unnecessary payload with the spoofed ping.

9 Justification

We will use wireshark and tcpdump C library for sniffing and analyzing the packets sent and recieved in the process. To successfully send a spoofed packet, we must use source IP within the range of our known IP addresses. We will sniff only icmp packets at both the ends for the justification of our attack.