CSE-406

Project Design Report

Ping Of Death Attack

Ping Flood Attack

Prepared By

Muntaka Ibnath

1605106

Introduction

Ping

Ping refers to a program that helps to check whether the host computer is operating or not from a user's end. It sends a ICMP(Internet Control Message Protocol) echo request to a specified interface on the network and waits for a reply. It is also used for troubleshooting to test connectivity and determine response time.

Ping Of Death

Ping of death is a DoS attack. DoS refers to denial of service. In this attack, the attacker tries to freeze or crash the target machine by sending packets larger than the maximum size that is allowable. When the attacker sends such packets, the victim becomes unable to serve the users. It was a dangerous attack during the late nineties, but after that patches were available in the operating systems to defend this attack. Web sites started to block the ICMP ping messages at their firewalls and are now able to prevent these kinds of DoS attacks.

Ping Flood

Ping flood attack is also a DoS attack that is similar but more effective than Ping of death. The idea behind this attack is that the malicious computer triggers a program that tries to send a huge number of ping messages without waiting for the echo reply. After sending enough messages the link that connects the target computer gets overloaded and denies the normal users to provide services.

The two assumptions of general ping flooding scheme

1. The attacker has access to high capacity link
2. The target has lower capacity internet connection than the attacker

These assumptions make sure that the attacker is privileged enough to make the flooding. The attacking end hopes that the target will reply with echo messages so that both the incoming and outgoing bandwidth is consumed. If the target is slow enough, the attack can easily slow down it's CPU cycles and hamper it's services to the user significantly.

The reasons behind using ping packets instead of http GET requests or shell requests are that the ping packets are ICMP echo requests and are main contributors of the total internet traffic which reduces the possibility of suspicions from the victim end.

Topology

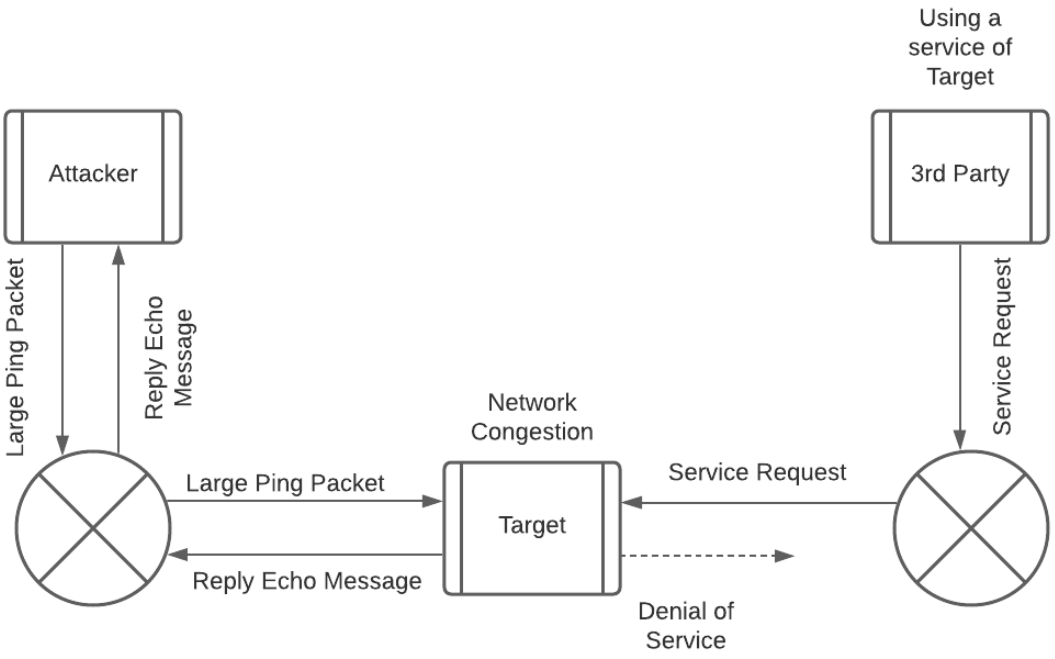

Figure: Ping Of Death

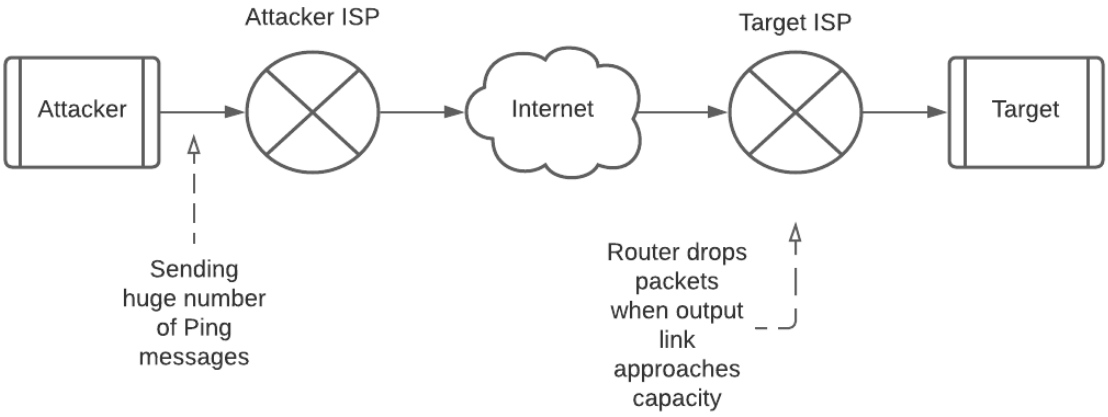

Figure: Ping Flood

Attack Strategies

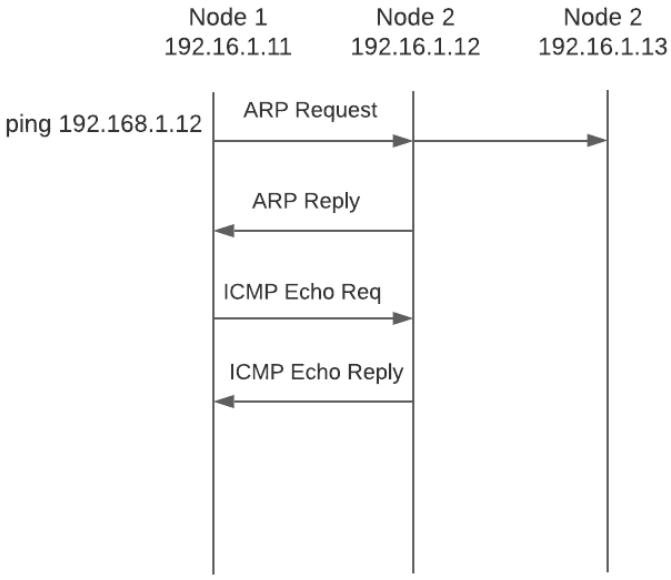

Figure: Normal Ping Exchange

Ping of Death

Design

To simulate a ping of death attack it is required to set up our own network because DoS attacks are illegal. Firstly, we'll have to set up our own LAN using the seedlabs virtual machine. IP4 ping packets are larger than most others and sometimes can be as large as the maximum allowable packet size of 65,535 bytes. When a malicious large packet is transmitted by the attacker, the large packet gets fragmented into smaller segments each having size less than the minimum size limit. So that while trying to combine the segments in the target machine, it experiences buffer overflow, which causes it to crash or freeze.

Timing Diagram

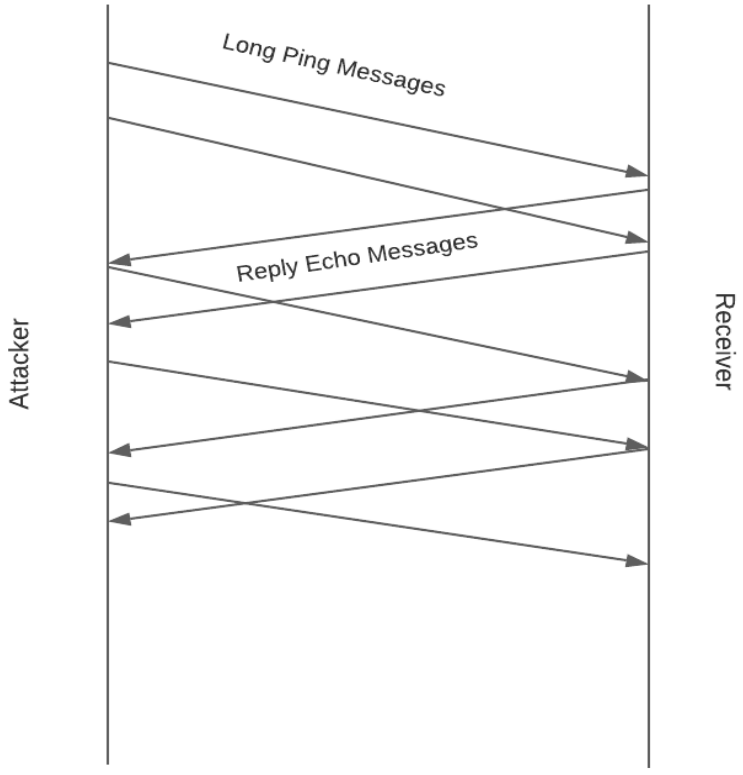

Figure: Timing diagram of Ping of Death

Ping Flood

Ping flood attacks can be hampered in several ways. For example, sometimes ISPs can block malicious machines attempting to send a lot of ICMP packets, targets may be able to identify such malicious requests, ICMP responses sent back to attackers which may affect their network network performance.

Timing Diagram

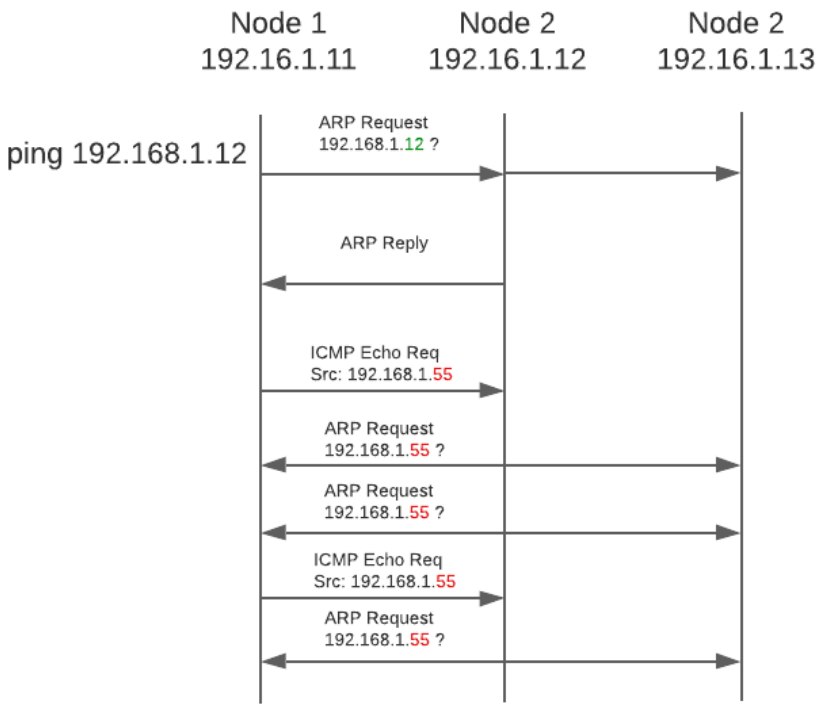

Figure: Ping Flood Attack using Source Address Spoofing

Schemes

1. **Source Address Spoofing:** The attacker sends ping with a fake or spoofed source address. Generally this is done by changing the source IP address on the outgoing ICMP packet headers.
2. **Reflector Attack:** This scheme is applied by bouncing messages off random unsuspecting normal hosts. The attacker uses the target's IP address as a

spoofed source address and sends protocol messages to multiple normal hosts. So the normal hosts start responding to the target.

3. **Broadcast:** The attacker broadcasts the ICMP echo request to all normal hosts using the target's IP address as a spoofed source address.
4. **Botnet:** This is a modern approach and in this one the attackers create a slave network and compromises other hosts to do their bidding.

Packet Details and Modification

In both ping of death and ping flood attacks, ICMP packets are manipulated. As ping of death is not much feasible in the current operating systems and websites, we'll mostly implement ping flood attack.

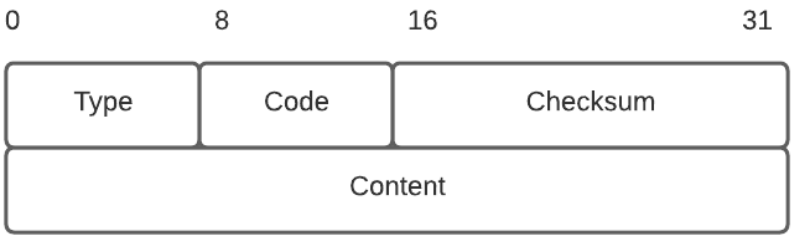

Figure: ICMP Packet Details

The outgoing ICMP packet headers need to be manipulated to simulate address spoofing. **iptables** is a packet filtering and firewall application on Linux. Using this the method of processing packets by the Linux kernel can be manipulated. Shell commands can be used to change the privilege in such a way that it will construct packets with fake source addresses.

Justification

Ping of death attack should make the target freeze in old versions of operating systems as it will be done in a controlled environment using LAN in a virtual machine. It will send a packet having a huge size and make the target over occupied. But due to firewalls in the modern operating systems, it may not be simulated perfectly.

On the other hand, ping flood attacks are hard to counter if a proper scheme is used. When the attacker and the hosts share the same LAN it gets harder. Sometimes, the attacker may use a large Botnet of zombies. The victim can't shut down ping to defend this attack as it is used by many other applications. By incorporating powerful flooding strategies we will be able to attack the target host successfully. As it's a distributed denial of service(DDoS) attack, traffic monitoring and blocking malicious traffic will not work either. In the schemes where ping flood uses other normal hosts, it gets tougher for the target to identify the attack as there remains the possibility of those normal hosts being authentic users requesting service.