Semester : VI Subject : CSS Academic Year: 2023-2024

DENIAL OF SERVICE ATTACK:

It is an action that prevents or impairs the authorized use of networks, s/ms or applications by exhausting resourses such as CPU, memory, bandwidth and diskspace.

Categories of resources that can be attacked:

- Network Bandwidth
- System Resources.

Network Bandwidth:

Attackers create a traffic directed at a target server by consuming the computer network bandwidth.

System Resources:

Rather than consuming bandwidth with large volumes of traffic, specific types of packets are sent that consume the limited resources available on the system.

(eg) Memory Table available in the system

This attack leads to system crash.

Types of DoS Attacks:

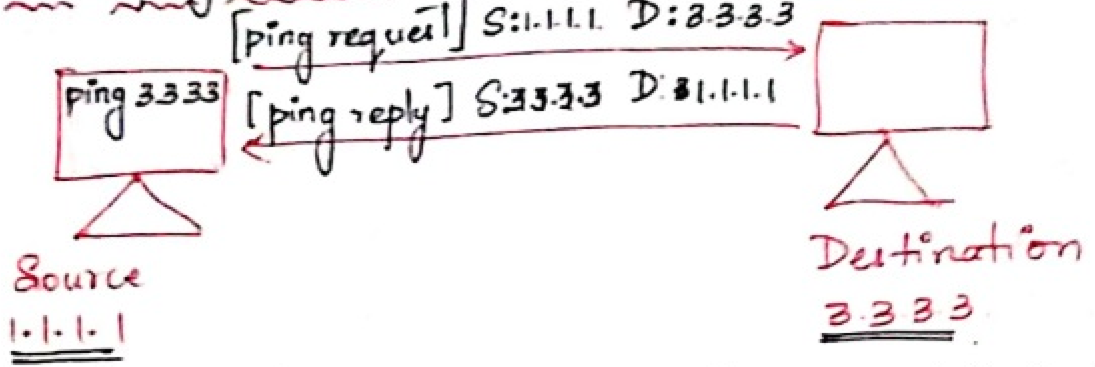
- ICMP Flood (or) Ping of Death.
- TCP SYN Flood

ICMP Flood (or) Ping of Death:

It aims to flood the network or the server with unwanted packets and overload the n/w capacity so that legitimate users cannot access the server.

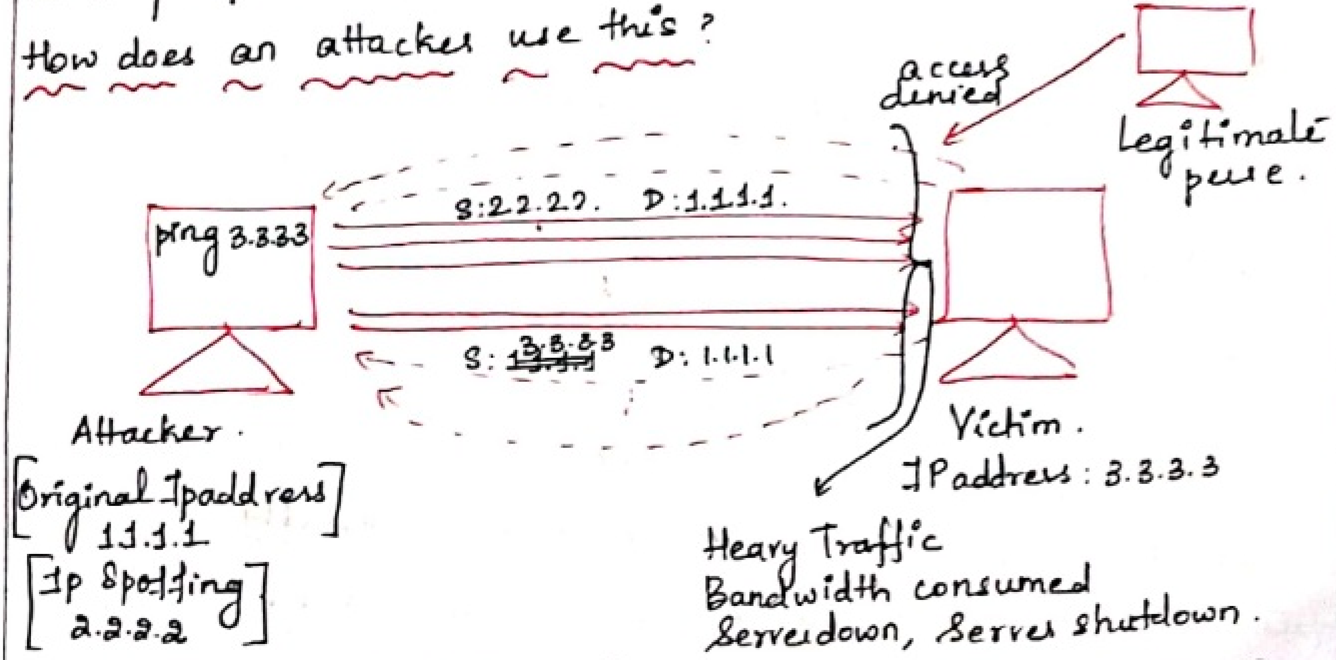
Semester: VI Subject: CSS Academic Year: 2023-2024

## How does ping command works?


[ping request] S:1.1.1.1. D:3.3.3.3
ping 3.3.33
[ping reply] S:3.3.3.3 D:1.1.1.1
Source
1.1.1.1
Destination
3.3.3.3

- Ping is essentially a combination of Internet Control Message Protocol (ICMP) echo requests and e response message.
- Each ping command transmits 2 ICMP packets
- When an administrator inputs a ping command on the command prompt, an echo request - a small data packet of upto 64 ~~packets~~ bytes - is sent to the target device or a specified IP address.

## How does an attacker use this?



Scanned with OKEN Scanner

* The very first thing attacker will do is to hide his identity by doing IPSpoofing → will change the IP address.

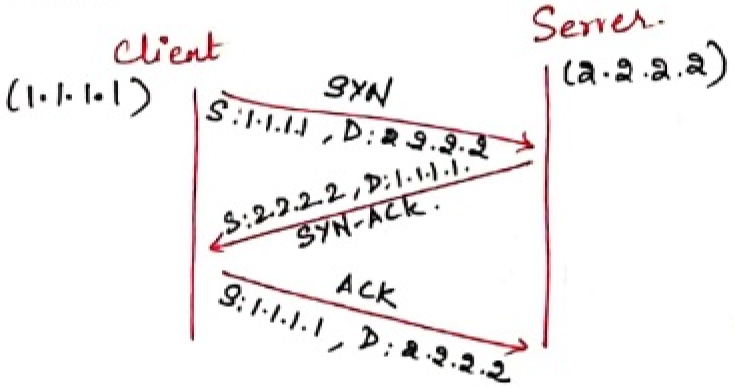
* Then the attacker attempts to overwhelm a targeted device with ICMP echo-request packets, causing the target to become inaccessible to normal traffic.

* The ICMP requires bandwidth on both the incoming messages (echo-request) and outgoing message (echo-reply). By doing this it exhausts the bandwidth.

* This leads to ping of death.

TCP SYN FLOOD:

Let us look into how the normal TCP protocol work.



The normal way of TCP communication is accomplished using 3 packets

* Client sends SYN packet to server.
* Server acknowledges client by sending SYN-ACK.
* Finally the client acknowledges by sending ACK packet to server. Once it is done the further communication continues.

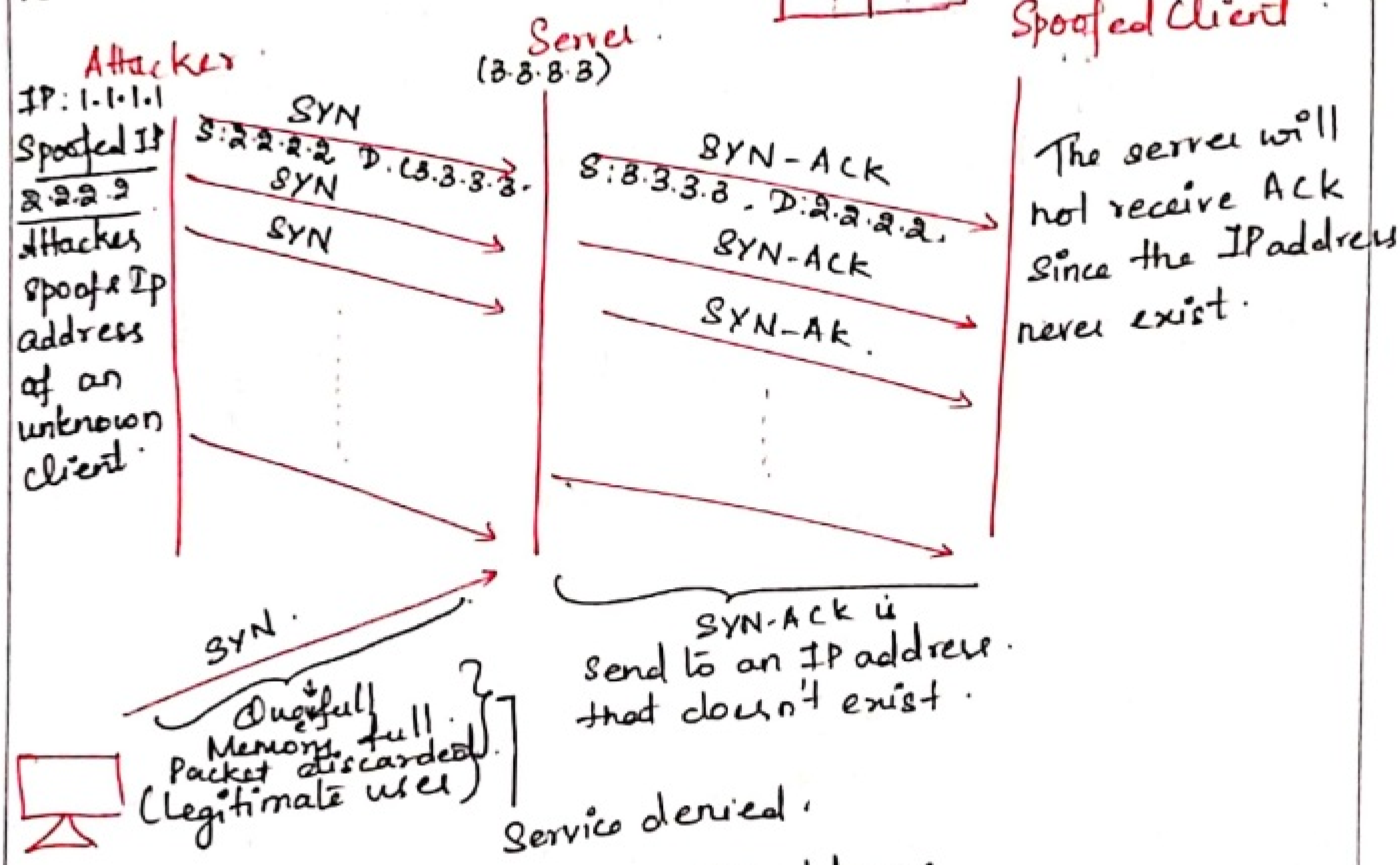
Scanned with OKEN Scanner

Everytime a new SYN packet enters the network, the packet information is stored in the memory table. Once the connection is closed the entry is deleted from the memory.

What does the attacker do.

| | |
|---|---|
| SYN | SYN-ACK |
| SYN | SYN-Ack |
| SYN | SYN-ACK |
| ⋮ | ⋮ |

queue full. It is waiting for ACK.



The Attacker spoofs the IP address
The Spoofed IP address is a non-existant client.
The Attacker sends the SYN packet to the victim.
The innocent victim will reply with SYN-ACK to the non-existant ~~ser~~ IP address. and simultaneously

it make entry of SYN packed in the memory table.

The victim (ie) the server is waiting to receive ACK. so that it can continue further communication, but it will not receive ACK, since it is an non-existance IP address.

Mean time if a legitimate user tries to connect to the server, he won't be able to connect because the queue is already full, memory capacity is full and the service is denied for the legitimate user. This is how the attacker floods the network using SYN packets which leads to DOS Attack.

Scanned with OKEN Scanner