

Department of Computer Science and Engineering Data Science



	an an
Semester:	Academic Year: 2028- 2028
It is an action that prevents or is use of nelworks, s/ms or applications	width and diskupace
Network Bandwidth	
Network Bandwidth: Attacker create a traffic directed by consuming the computer network Stelem Resources:	at a larget server
242	/1
Rather than consuming bands traffic, specific types of packets	are sent that

consume - the limited resources available (
leg) Memory Table available in the system
This attack leads to system crash.

Types of Dos Attacks: * JCMP Flood cos) Ping of Death.

* TCP SYN Flood

JCMP 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 legitimale users cannot access the server. Subject Incharge: Prof. Sarala Mary Page No. 1 Department of CSE-Data Science | APSIT



Department of Computer Science and Engineering Data Science



Academic Year: 2028-2024 How does ping command works? ping requeil S:1.1.1. D: 8.3.3.3 [ping reply] S:33.33 D:31.1.1.1 Destination Source 3333 1.1.1. * Ping is essentially a combination of Internet Control Message Prolocol LILMP) echo requesti and eresponse message. * Each ping command tearemile & ICMP packets * When an administrator inputs a ping command on the command prompt, an echo request - a small date packet of uplo 64 packets bytes - is sent to the larget device or a specified IP address. How does an attacker use this? Legitimale S: 13.3.63 D: 1.1.1.1 Victim . Attacker. JPaddres: 3.3.3.3 Original Ipaddress Heary Traffic Tip Sportling Bardwidth consumed Serverdown, Server shutdown. Department of CSE-Data Science | APSIT Subject Incharge: Prof. Sarala Mary Page No. 2

PARSHWANATH CHARTABLE TRUST'S



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science**



		30
Semester: VI	Subject :CSS	Academic Year: 20 26- 2024

* The very first thing attacker will do is to hide his identity by doing JPSpoofing -> will alonge the JP address.

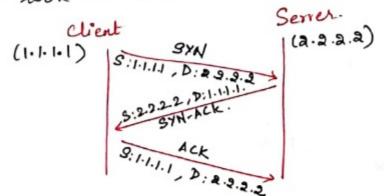
* Then the attacker attempts to overwhelm a targeted device with ICMP echo-requert packets, causing

the larget to become inaccusible to normal fraffic. * The JCMP requires bandwidth on both the incoming messages (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 TLP protocol work.



The normal way of TCP communication is accomplished using spackets

* Client sends SYN packet to server. * Server acknowledges client by sending SYN-ACK.

* Finally the dient acknowledges by sending Ack packet- to server. Once it is done the further

communication continues.

Subject Incharge: Prof. Sarala Mary Page No. 3

Department of CSE-Data Science | APSIT



Department of Computer Science and Engineering Data Science



Semester: VI Subject: CSS Academic Year: 2023- 20.24		
Everytime a new SYN packet externs the network,		
the packet information is stored in the memory table.		
the packet byormic closed the entry is deteled		
on the connection as		
in the control of the		
What does Ack.		
Correl.		
2 11) 5:50		
Affactus SYN Syn-Ack Since the IPaddress		
spoofs Ip		
address never 2000		
at an		
whenown dient		
CU DU		
3		
Dial ACK W		
34 N Send to an IP address.		
Questall 11. 17 that doesn't exist.		
Memory full		
(legitimate well)		
Syn-Ack is Send to an IP address. Memory full Packet discarded (legitimale uses) Service derived.		
The Attacker spoods the IP address The Attacker spoods the IP address a non-existant client.		
The more line is a non-existent cited		
The spoofed IP address is avail backed to the		
The Attacker speads the IP address is a non-existent client. The Speaded IP address is a non-existent client. The Attacker sends the SYN packed to the The Attacker sends the SYN packed to the		
victim. The innocent victim will neply with SYN-ACK		
victim in heard state		
The innocent Victory The address and elimultaneously Subject Incharge: Prof. Sarala Many Page No. A. December of Control of Contro		
to the non-existant ter -11 and		
Subject Incharge: Prof. Sarala Mary Page No. 4 Department of CSE-Data Science APSIT		



Department of Computer Science and Engineering **Data Science**



Semester: VI	Subject :	Academic Year: 20 28- 20-24
it make entry	of eval packet in	

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

Mean time if a legitimate uses 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 deniced for the legitimate user. This is how the attacker floods the network using SYN packels which leads to Dos Attack.

