

Subject Incharge: Prof. Sarala Mary Page No._

A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Semester: VI	Subject: CSS		Academic Year: 2028 - 2024
Phishing	11.	Phanny	1.0
		of	0 6
> In Phishing, au			
deceived into visi	ting a		
Malicions websil	1 0	in the adds	ess bar of the user is redirected
opening an attack	ment	browser, th	e ducheila
, 0		1- a Paudu	Lei
	11 A		IL ONTITE
It largets to	attack ->	1+ bo.	of largel the loners to attack.
one person at a	time.	gerver, ou	lomers to attack.
Domain Name Se			ena block of a
Domain Name Se	ever is a plan	ninent buin	alphabetic
Domain Name Se Internet It's dev	cloped as a sy	petern lo es	- accord mabeiles
no international	addresses, allow	oing werd !	hackers will
and exchange e	mails In DNI	s attacks,	hacker & will
and exchange	" source while	ch contains.	the domain name
There are different	The series of T	DNIS Attack	the domain names
(1) Derial of		1 .P. (DI	(200
(2) Distribut	ed Denial of	Service Co	Ne cache possoning
(2) DNS Sb	ooting Calso k	enous os FR	ons cache possoning
(4) Reflectio	n Attack.	E	. 1
(4) 14 15	Amplification	Attack	

Department of CSE-Data Science | APSIT

PARSHWANATH CHARITABLE TRUST'S



Subject Incharge: Prof. Sarala Mary Page No._

A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Subject : ____ C&S Academic Year: 2023 - 2024 Distributed Denial of Service (DDOS) It uses multiple systems to generale attacks The eyelem wed for DDOS are valnerable system Attacker inetalle his program on those machines to launch an attack. Attacker will gain access and launch the program Such affeded systems are known as tombies Zombies are entirely controlled by attacker.
(eg) Many broadband systems will be selected by the attacker to cause attack on a particular company. A small number of system handlers control the zombies. Attacker sends a single command to a handler, which then automatically forwards it all agents under its control. Once the agent software is uploaded to a newly compromised system, it can contact one or more handlers to automatically notify them of its availability Allacker. 1 -> Handlers (Botnet)] otgent Tombies.

Department of CSE-Data Science | APSIT

large

PARSHWANATH CHARITABLE TRUST'S



A.P. SHAH INSTITUTE OF TECHNOLOGY

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



Semester: VL	Subject : CSS		Academic Year: 2028- 2024
(4) Reflection Allack		4	I ID address
dHacker spoofs the J	Paddress with	vanous of	nii of heldi on
and ping the Victim	to shuldown	the server	
11			
	ing request to		
2222	ping request to sing reply gou to	2.5.5	
	request	2.2.2.2	
	reply		7
44.4.4	J	V	culum 5.5.5.5
AHacker	acquest 04.	, ,	
speed to	reply		
3.2.2,4.4.4.4			
33333			
→ The packets are r	effected leator	y system	Ip address.
- Attacker will use to - Attacker will choose	he intermediate	itan euste	In with higher
A !! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !	1116 1101	9 (1	remuct.
		my sena	request.
· lelen has paster	4 77 -		
There is no evidence	of an attacker	. Aal	1 010 15 one.
T. Non my sust	og entrice los	oks like	regitimale bid
There is no evidence The specific (or) system The specified address	directs of	all packel	is to the desired
The spoofed add	res are	directed	to the intermedia-
The specified addressed and res	pontes		
long			
, a J			
Subject Incharge: Prof. Sarala Many	Page No. 2	Department of	CSE-Data Science APSIT

PARSHWANATH CHARITABLE TRUST'S



A.P. SHAH INSTITUTE OF TECHNOLOGY

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



Subject : _ C&S Academic Year: 2028 202 4 Amplification Allack DNS Amplification Allack. How does the normal DNS work? What is 101010 example com: Do you know www.example.com Resolve to IP address DNS User 2.2.2.2 www.example.com bow.example.com 2.2.2.2 User DNS DNS Server. What an attacker will do? He will spoof the IP address to victims IP address. He will send request to all the subdomains of the website Subdomains Example com Subdemain? example com DNS quiny to get nample con subdemains example com Subdomaina example com DNS Rerver Since the IP address is spoofed, all reply goes to the [JP address] victim server. Subdomain 1: Subdomain 1. example. com [192.84.48.47] Domain: example.com Subclomain 2: Subclomain a. example.com [192.34.48.46] Subclomain 8: 8ubdomains example com [192.84.48.45] Subdomain 4: subdomain 4. example.com [192.34.48.44] Subject Incharge: Prof. Sarala Mary Page No. Department of CSE-Data Science | APSIT



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Semester: VI Subject: (SS Academic Year: 2028-2014
all records of server 1923 34 4 Bas) (05 2 Leaftimali
Attacker 80 urce ID= 1.2.3.4 25 1/2 1/2 1/2 1/2 Vser
(Spoof Ipaddress)
to 1.2.3.4 (3Mbps)
records of example com Server 192.34.48.43 193.34.48.45 193.34.48.45 193.34.48.45 193.34.48.49
Attacker Sooth Traddress to
(Spoots I Paddress to
(Speats Traddress to 1.2.3.4) DNS 1934 1934
DNS query to get all Server. records of example com with source IP 1.2.3 4 Attacker
(Spoots the IPaddress
to 1.2.8.4)
For the attacker to send the query it takes 3Mbps whereas
the victim to receive the reply packets its require 300 Mbps
from each system. This is how it amplifies the entire
1 1 1 1 1 1 1 1 1 1 1 1
Connect the serves, then it cannot access it.
Subject Incharge: Prof. Sarala Mary Page No. 5 Department of CSE-Data Science APSIT