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

Phishing Vs Pharming

Phishing	Pharming
→ In phishing, a user is deceived into visiting a malicious website or opening an attachment	→ In pharming, even when a user types an legitimate URL in the address bar of the browser, the user is redirected to a fraudulent website
→ It targets to attack one person at a time.	→ It poisons the entire DNS server, so it targets the entire customers to attack.

DNS Attack :

Domain Name Server is a prominent building block of a Internet. It's developed as a system to convert alphabetic names into IP addresses, allowing users to access websites and exchange emails. In DNS attacks, hackers will sometimes target the servers which contains the domain names. There are different types of DNS Attacks.

(1) Denial of Service (DOS).
(2) Distributed Denial of Service (DDOS).
(3) DNS Spoofing Also known as DNS cache poisoning. [Refer Pharming]
(4) Reflection Attack.
(5) Reflection Amplification Attack.

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

Distributed Denial of Service (DDOS)

It uses multiple systems to generate attacks.

The system used for DDOS are vulnerable system.

Attacker installs his program on those machines to launch an attack.

Attacker will gain access and launch the program.

Such affected systems are known as zombies.

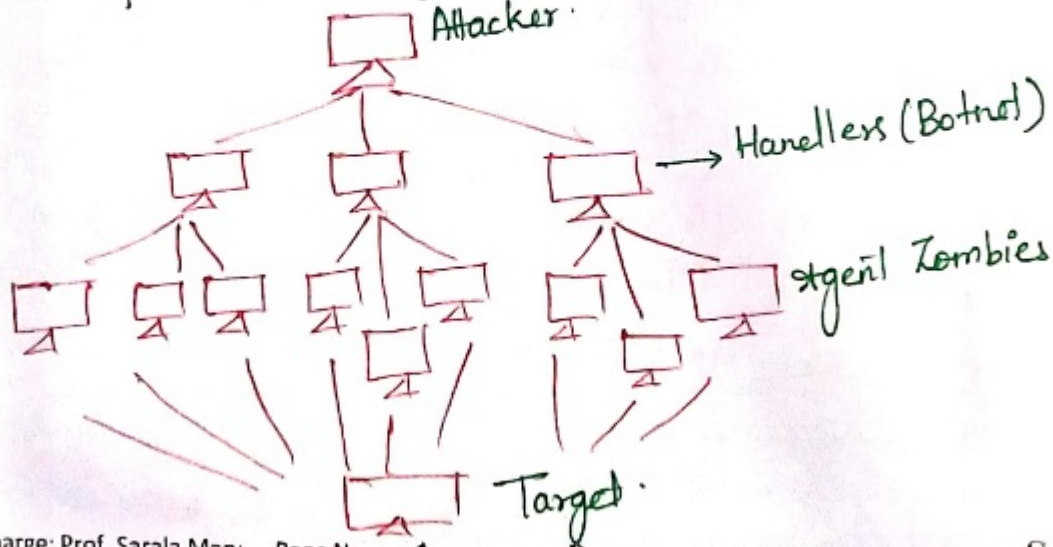
Zombies are entirely controlled by attacker.

(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.

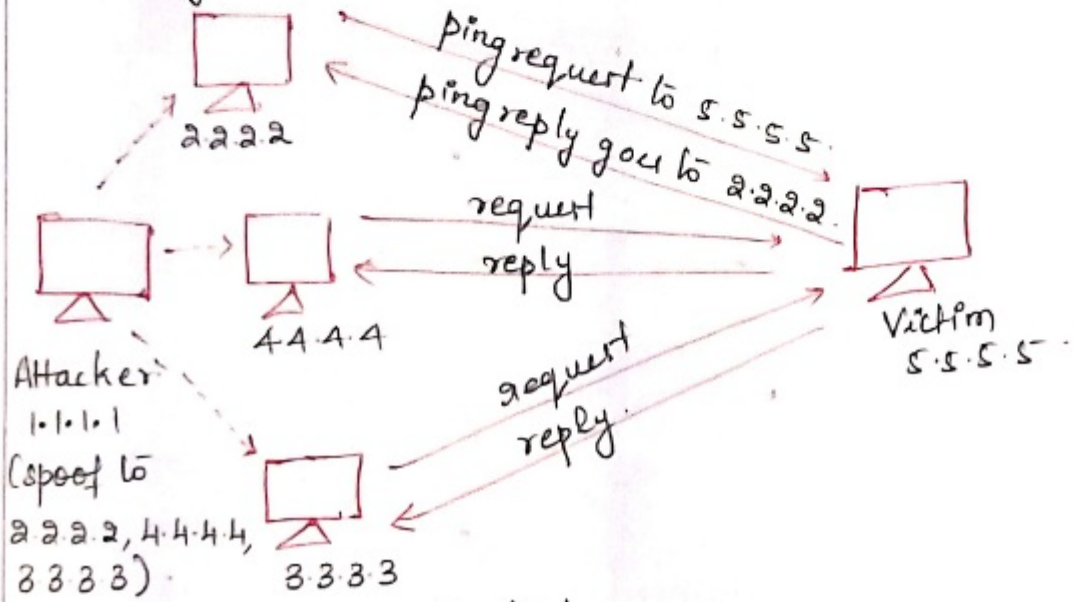
Once the agent software is uploaded to a newly compromised system, it can contact one or more handlers to automatically notify them of its availability



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

(4) Reflection Attack -

Attacker spoofs the IP address with various other IP address and ping the Victim to shutdown the server.

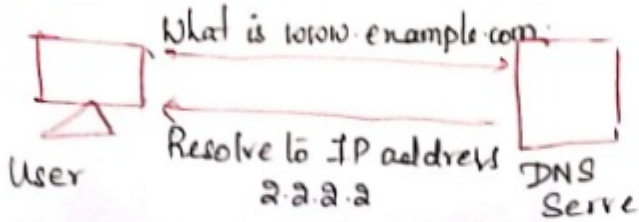


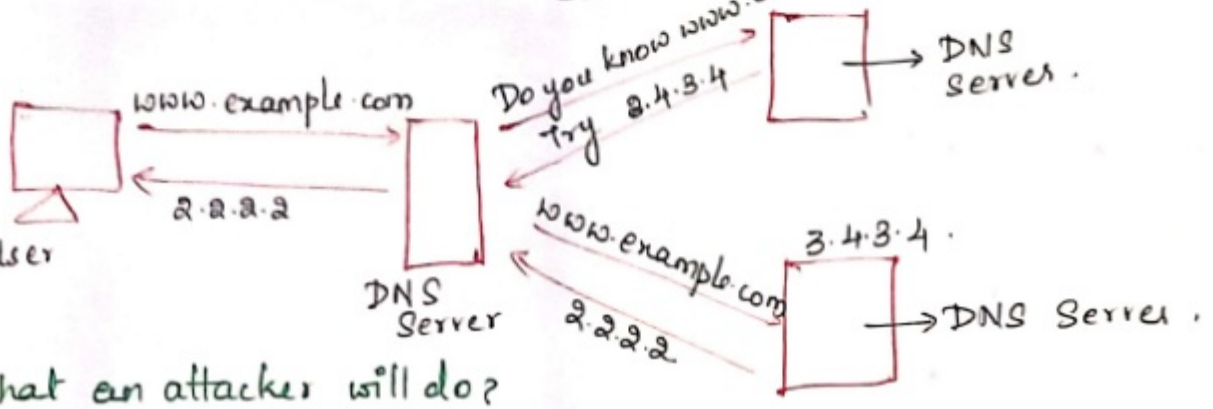
→ The packets are reflected
→ Attacker will use the intermediatory system IP address.
→ Attacker will choose the intermediatory system with higher bandwidth so that it can continuously send request.
→ Victim has to face heavy traffic.
→ There is no evidence of an attacker.
→ Traffic (or) syslog entries looks like legitimate one.
→ The spoofed address directs all packets to the desired targets and any responses are directed to the intermediatory

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

Amplification Attack: DNS Amplification Attack:

How does the normal DNS work?

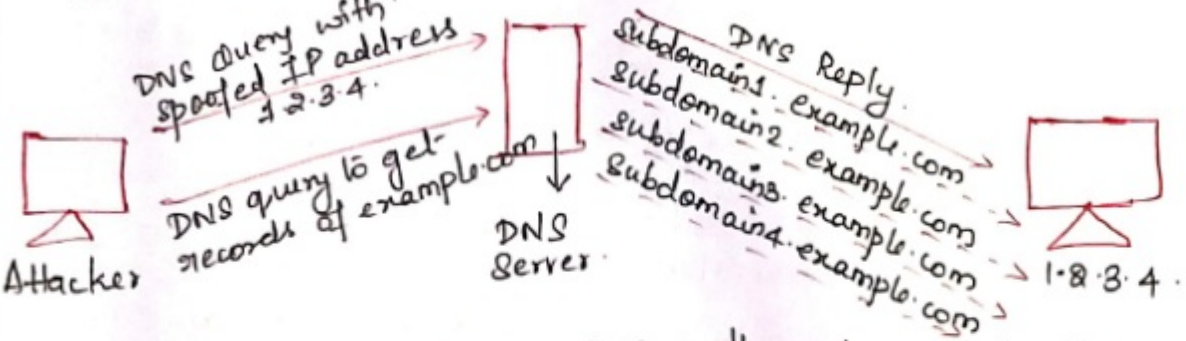




What an attacker will do?

He will spoof the IP address to victims IP address.

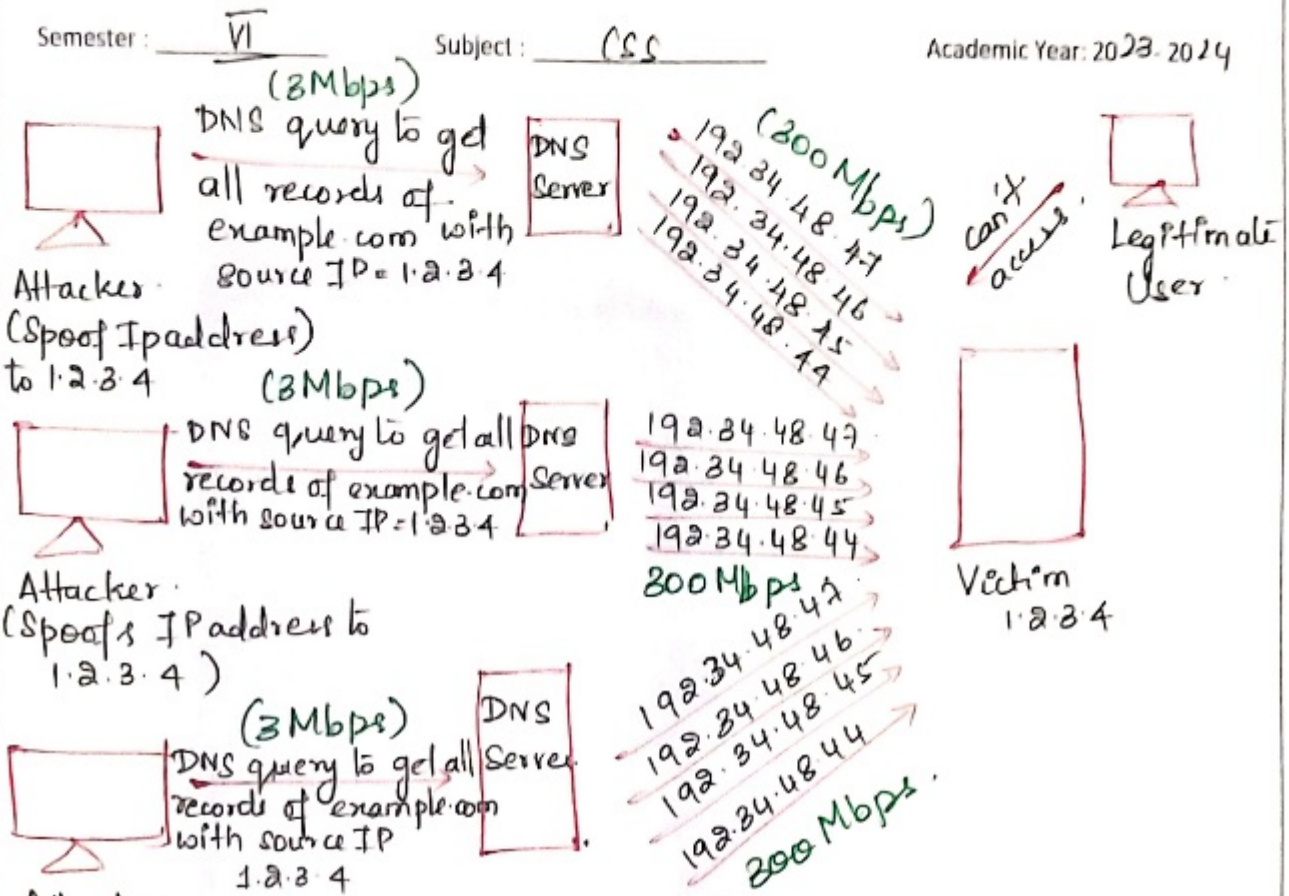
He will send request to all the subdomains of the website



Since the IP address is spoofed, all reply goes to the victim server.

		[IP address]
Domain :	example.com	
Subdomain 1 :	subdomain1.example.com	[192.34.48.47]
Subdomain 2 :	subdomain2.example.com	[192.34.48.46]
Subdomain 3 :	subdomain3.example.com	[192.34.48.45]
Subdomain 4 :	subdomain4.example.com	[192.34.48.44]

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



For the attacker to send the query it takes 3Mbps whereas the victim to receive the reply packets it's require 300Mbps from each system. This is how it amplifies the entire bandwidth (resources). When the legitimate user tries to connect the server, then it cannot access it.