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

PHISHING AND PHARMING TECHNIQUES

* Phishing is a method that hackers use to obtain your personal information
* They send you an email that is made to look just like a legitimate email in an effort to get you to click on a harmful link or attachment
* Phishers can also deceive you by sending you texts (SMiShing), voicemails (Vishing), or even faxes (Phasing), all in an efforts to obtain access to your private information.

How to safeguard yourself from phishing attacks.

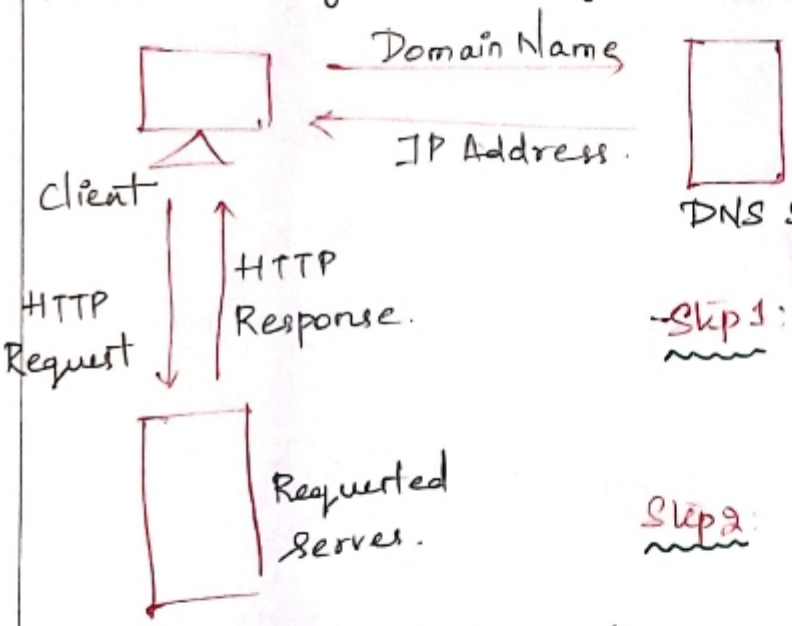
* Ensure that your antivirus software and operating system are up to date
* Hover over links in emails and on websites to verify the destination.
* Try putting in the website address rather than following a link from an email message.
* Always be aware of sensational subject lines and phrasing, such as "Much Act Now!" or contain spelling and grammar issues.
* If an email just seems suspect, it's better to delete it.

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

PHARMING :-

Pharming is a technique using which attackers redirect traffic from a legitimate website to a fraudulent website with the purpose of spreading malware or stealing sensitive data from the victims.

The normal way of working of DNS Server?

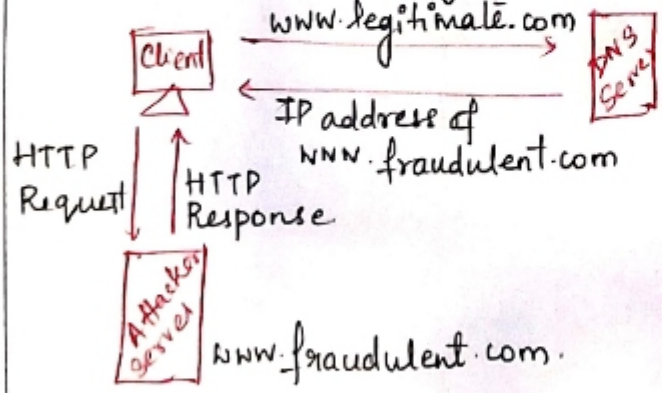


Step 1: When client types the domain name ~~ipaddress~~, the DNS Server resolves it into IPaddress.

Step 2: Then it is connected to the Requested server.

What does the attacker do?

The attacker actually poisons the DNS server.



Step 1: Attacker types the domain name — www.legitimate.com.

Step 2: Since the DNS server is poisoned by attacker, it will give the IP address of www.fraudulent.com.

Step 3: The client is connected to attacker website, and his credentials is taken by the attacker.

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.