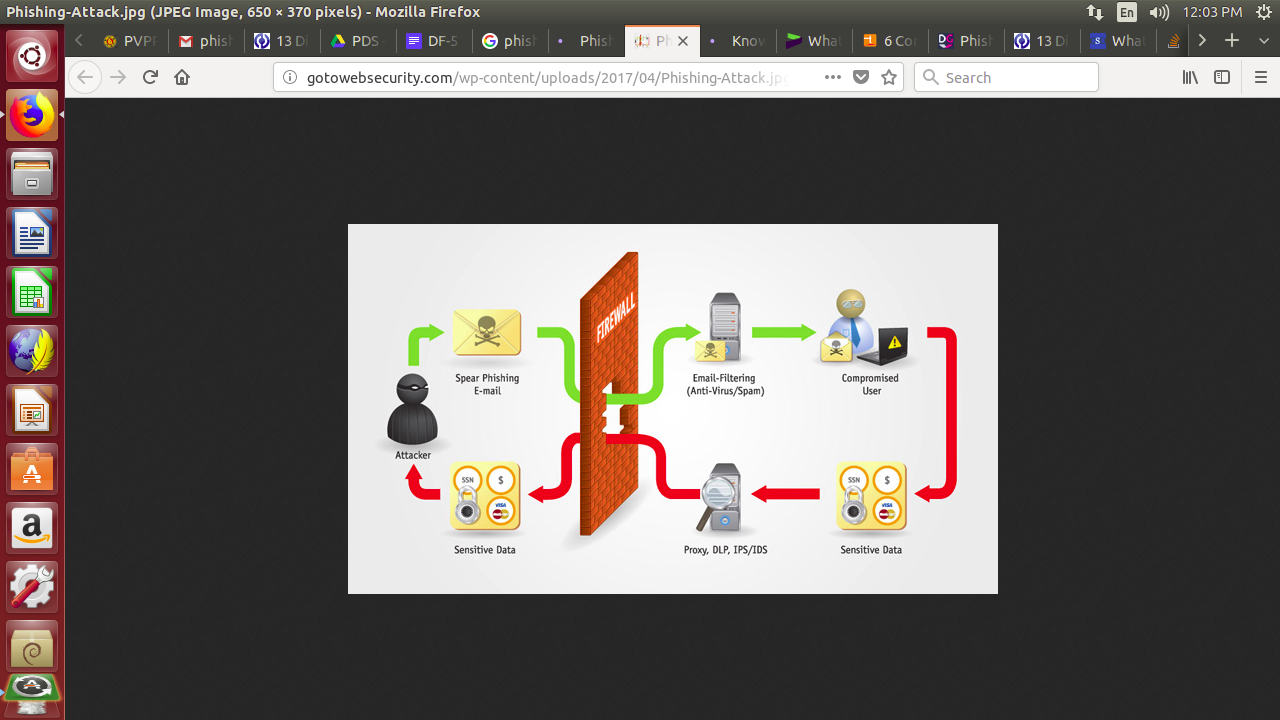
Experiment No:11

**Aim:** To implement Phishing Attack.

**Theory:**

**Phishing Attack**

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identity theft.



**Types of Phishing Attacks:**

* **Deceptive Phishing.** The term "phishing" originally referred to account theft using instant messaging but the most common broadcast method today is a deceptive email message. Messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams are broadcast to a wide group of recipients with the hope that the unwary will respond by clicking a link to or signing onto a bogus site where their confidential information can be collected.
* **Malware-Based Phishing** refers to scams that involve running malicious software on users' PCs. Malware can be introduced as an email attachment, as a downloadable file from a web site, or by exploiting known security vulnerabilities--a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.
* **Keyloggers and Screen Loggers** are particular varieties of malware that track keyboard input and send relevant information to the hacker via the Internet. They can embed themselves into users' browsers as small utility programs known as helper objects that run automatically when the browser is started as well as into system files as device drivers or screen monitors.
* **Session Hijacking** describes an attack where users' activities are monitored until they sign in to a target account or transaction and establish their bona fide credentials. At that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge.
* **Web Trojans** pop up invisibly when users are attempting to log in. They collect the user's credentials locally and transmit them to the phisher.
* **Hosts File Poisoning.** When a user types a URL to visit a website it must first be translated into an IP address before it's transmitted over the Internet. The majority of SMB users' PCs running a Microsoft Windows operating system first look up these "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. By "poisoning" the hosts file, hackers have a bogus address transmitted,taking the user unwittingly to a fake "look alike" website where their information can be stolen.
* **System Reconfiguration Attacks** modify settings on a user's PC for malicious purposes. For example: URLs in a favorites file might be modified to direct users to look alike websites. For example: a bank website URL may be changed from "bankofabc.com" to "bancofabc.com".
* **Data Theft.** Unsecured PCs often contain subsets of sensitive information stored elsewhere on secured servers. Certainly PCs are used to access such servers and can be more easily compromised. Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

## **Phishing protection**

* Two-factor authentication (2FA) is the most effective method for countering phishing attacks, as it adds an extra verification layer when logging in to sensitive applications.
* In addition to using 2FA, organizations should enforce strict password management policies. For example, employees should be required to frequently change their passwords and to not be allowed to reuse password for multiple applications.
* Educational campaigns can also help diminish the threat of phishing attacks by enforcing secure practices, such as not clicking on external email links.

**So How to Prevent ?**

* **Anti-malware:** Popular anti-virus/anti-malware solutions
* **Web Filters:** Determining what websites users can access using a risk-based approach
* **Data Loss Prevention(DLP) :** Protecting data in transit, at rest, and in use
* **Anti-phishing software:** Containerization solutions for downloads from malicious emails and websites
* **Using HTTPS for transactions:** Checking the padlock icon to ensure secure transactions
* **Spam Filters:** Many email clients can detect potential spam (many being phishing attacks) and separate out those emails
* **Patch Management:** Ensuring systems are patched and up-to-date can mitigate many vulnerabilities targeted by phishing campaigns

**Conclusion:** Thus, we have successfully studied Phishing Attack.