# **What is Phishing?**

**Phishing** is a type of cyber attack where attackers attempt to deceive individuals into providing sensitive information such as usernames, passwords, credit card numbers, or other personal details. This is typically achieved through deceptive emails, websites, or messages that appear to come from legitimate sources. Phishing is a form of social engineering and is one of the most common threats in the cybersecurity landscape.

**Types of Phishing Attacks**

1. **Email Phishing**

Attackers send fraudulent emails that appear to come from a reputable source, such as a bank or a well-known company. The email usually contains a link to a fake website where victims are prompted to enter their personal information.

1. **Spear Phishing**

A more targeted form of phishing, spear phishing involves personalized messages sent to a specific individual or organization. Attackers often research their targets to make the emails appear more credible and relevant.

1. **Whaling**

Whaling is a type of phishing aimed at high-profile targets within an organization, such as executives or senior management. The messages are crafted to look like legitimate communication from trusted sources, often related to business operations or executive matters.

1. **Clone Phishing**

In clone phishing, attackers create a nearly identical copy of a legitimate email that the victim has previously received. They replace any links or attachments with malicious ones and resend the email, often claiming it as an updated version.

1. **Vishing (Voice Phishing)**

Vishing involves phone calls where attackers impersonate legitimate entities, such as banks or government agencies, to trick victims into providing personal information or transferring money.

1. **Smishing (SMS Phishing)**

Smishing uses text messages to lure victims into clicking on malicious links or revealing personal information. The messages often appear to come from legitimate sources, such as service providers or financial institutions.

1. **Angler Phishing**

Angler phishing targets users on social media platforms. Attackers create fake accounts that mimic real customer service profiles and lure victims into sharing personal information by responding to fake customer service inquiries or promotions.

1. **Malware-Based Phishing**

Attackers send emails or messages that contain malicious attachments or links. When the victim clicks on the attachment or link, malware is installed on their device, allowing attackers to steal information or take control of the system.

1. **Search Engine Phishing**

Attackers create fake websites that appear in search engine results. These sites are designed to look like legitimate businesses or services. When users visit these sites, they are prompted to enter personal information, which is then stolen by the attackers.

1. **Pop-Up Phishing**

Attackers use pop-up windows that appear while users are browsing the web. These pop-ups often mimic legitimate messages from the operating system or a trusted application, tricking users into entering their credentials.

1. **Website Forgery**

Attackers create fake websites that mimic legitimate ones, often using URLs that are very similar to the real site's URL. These websites are designed to steal login credentials and other sensitive information when users enter their details.

1. **Pharming**

Pharming redirects users from legitimate websites to fraudulent ones without their knowledge. This is often done by exploiting vulnerabilities in DNS (Domain Name System) servers or using malware to change the DNS settings on a victim's computer.

1. **Man-in-the-Middle (MitM) Phishing**

In MitM phishing, attackers intercept the communication between the victim and a legitimate service. This can be done through techniques such as Wi-Fi eavesdropping or malware. The attacker can then steal credentials or manipulate the communication to extract sensitive information.

1. **Session Hijacking**

Attackers steal session tokens, which are unique identifiers for a user's session on a website. With these tokens, attackers can impersonate the victim and gain unauthorized access to their account without needing to know their password.

# **Examples and Impact**

**Email Phishing Example**

An email appears to come from a popular online payment service, claiming there is an issue with the user's account. The email includes a link to a fake login page designed to steal the user's credentials.

**Spear Phishing Example**

An attacker sends an email to a company's HR manager, appearing to come from the CEO, requesting sensitive employee information or a wire transfer.

**Vishing Example**

A victim receives a phone call from someone claiming to be from their bank, asking them to verify their account details to resolve an urgent issue.

**Preventive Measures**

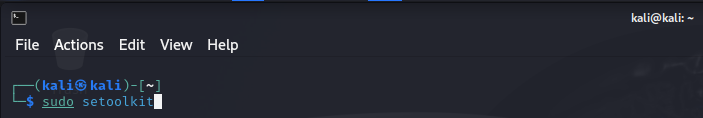
* **Education and Awareness**: Regular training for individuals and employees about recognizing and avoiding phishing attempts.
* **Email Filtering**: Using advanced email filtering solutions to detect and block phishing emails.
* **Two-Factor Authentication (2FA)**: Implementing 2FA to add an extra layer of security to accounts.
* **Secure Browsing**: Encouraging the use of secure, trusted websites and verifying URLs before entering personal information.
* **Anti-Phishing Tools**: Utilizing browser extensions and security software that can detect and warn about phishing attempts.

Phishing remains a significant threat, but by understanding the different types and implementing robust security measures, individuals and organizations can reduce their risk of falling victim to these attacks.

# **ASSIGNMENT OF MAKING A PDF EXPLOIT IN KALI Linux:**

Here is the way of making a exploit of a pdf:

**STEP 1: Type this………**



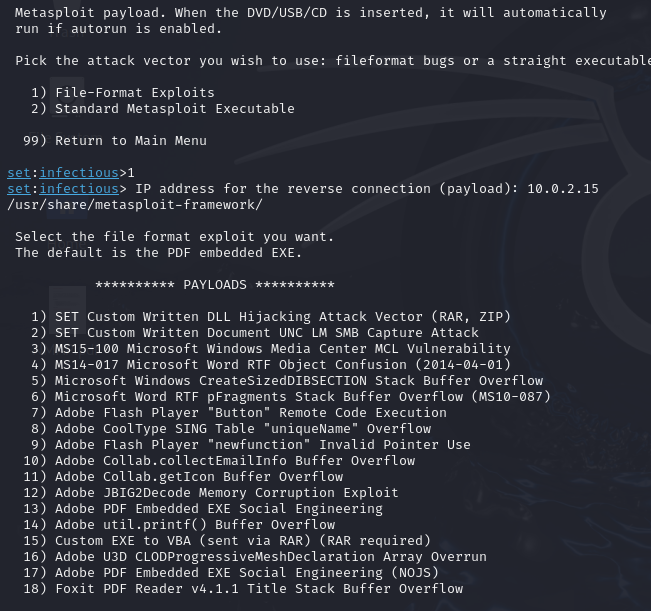
**STEP 2: Select the first option………….**

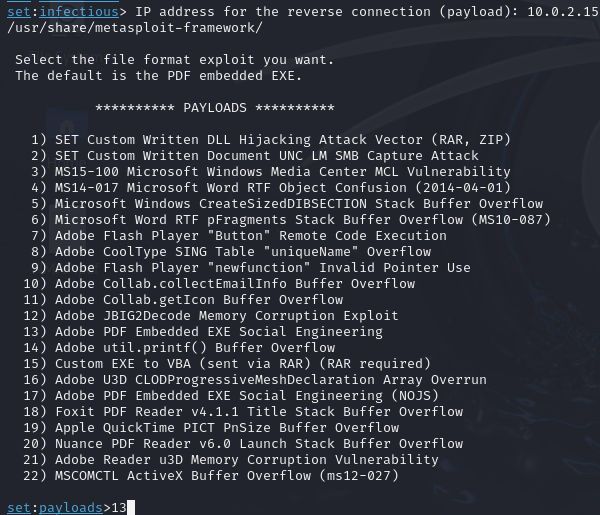


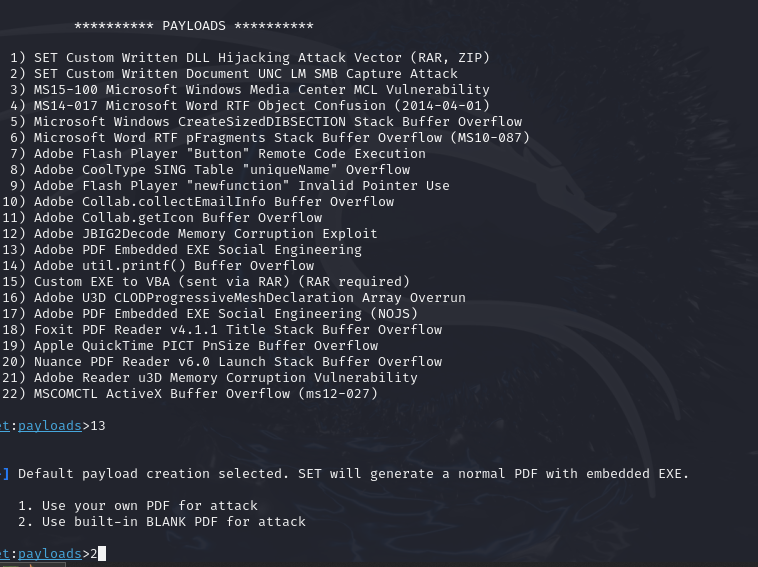
**STEP 3: Select the the 3th option**



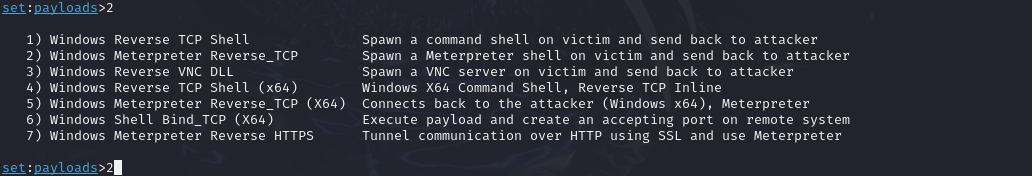
**STEP 4: Select the 1st option and then put your IP address for the reverse connection (payload)**



**STEP 5: Select the 13th option**

**STEP 6: here I’m selecting the 2nd option ……………..**

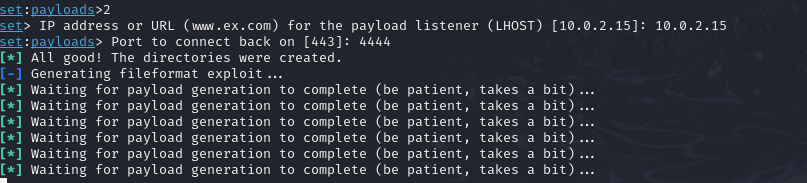
**STEP 7: here select the 2nd option……….**



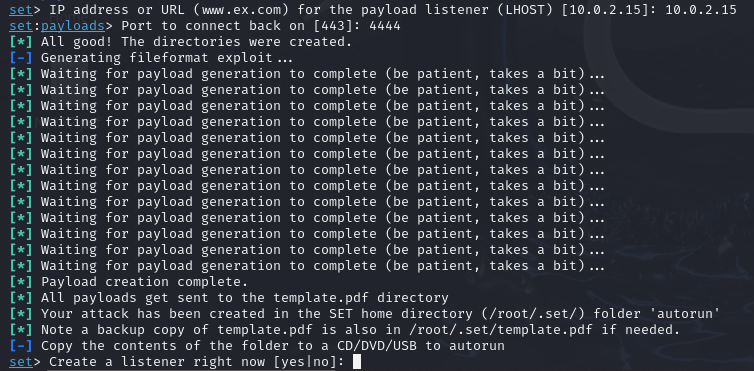
**STEP 8: Put the IP address for the payload listener and the port number……**

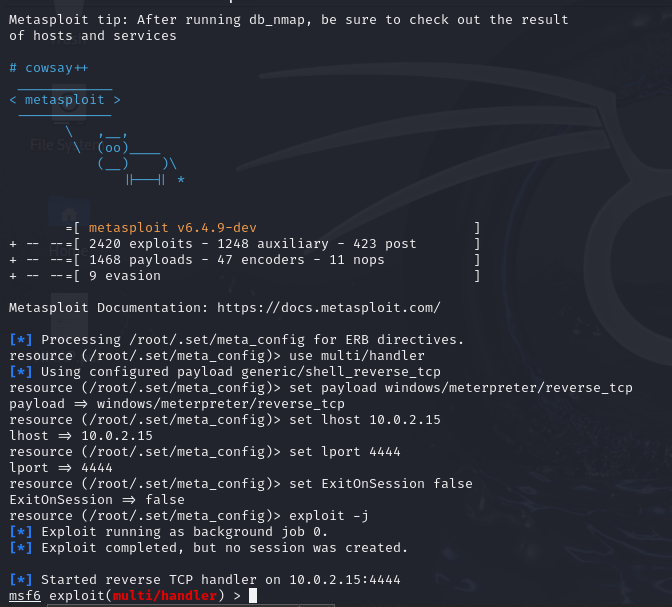
****

**Now its generating**

****

**STEP 9: Type “yes”………….it will start the metaexploit framework**

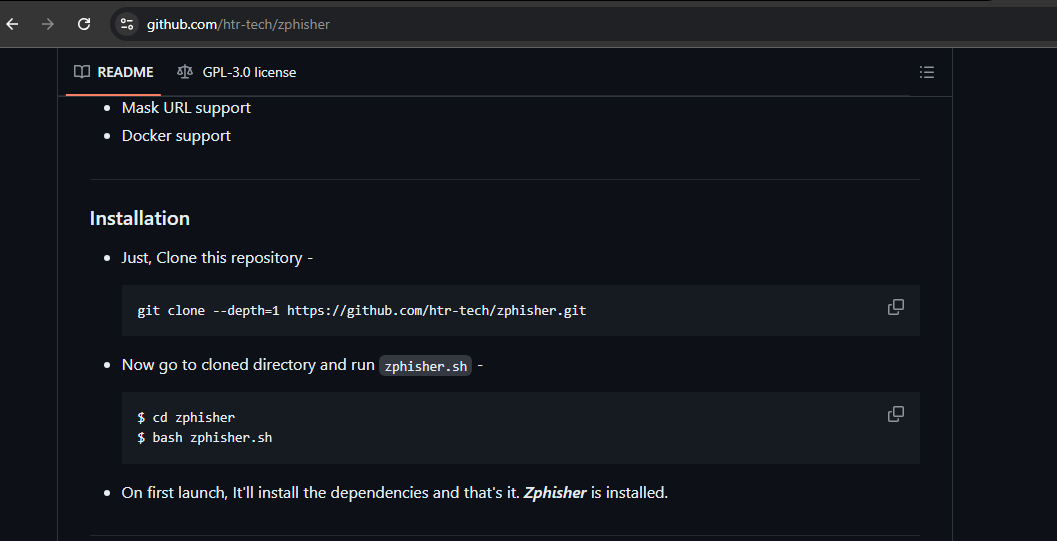


****

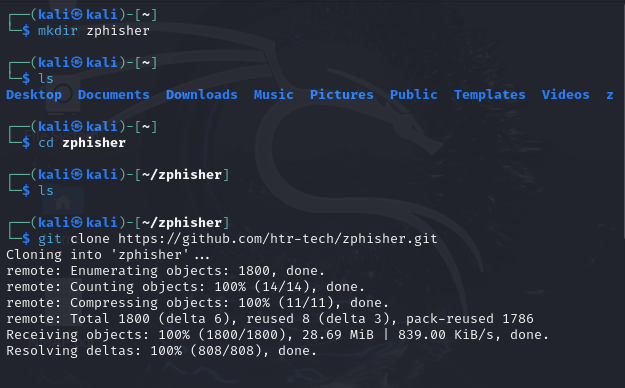
**Now the file has been created at “root/.set/meta\_config”**

# **Installation Process of the Zphisher:**

**STEP 1: Goto this page and follow the instruction as mentioned**

****

**STEP 2: Make a folder on Desktop named “zphisher”………and goto in that folder ….now paste the link to clone the file of the zphisher through the github link**

****

**STEP 3: Run the “zphisher.sh” file you will get this………**

****

**I’m going to select the 2nd option…. Now I’m selecting the 1st option….**

****

**Now I’m selecting the 2nd option**

****

**Now I’m selecting “n”**

****

**I’m selecting “n” again….**

****

**Now it has created me links ………….**

****