Text

Description automatically generated

**Activity based**

**Project Report on**

**IT DATA SECURITY**

**Project Module - I**

**Submitted to Vishwakarma University, Pune**

**Under the Initiative of**

**Contemporary Curriculum, Pedagogy, and Practice (C2P2)**

**By**

**Name:- Prathamesh P Chawande**

**SRN No : 202101152**

**Roll No : 49**

**Div : C**

**Third Year Engineering**

**Faculty In charge:- prof. Suhas Chavan**

**Date Of Project 1:- 27/03/2024**

**Department of Computer Engineering**

**Faculty of Science and Technology**

**Academic Year**

**2023-2024 Term-II**

**IT DATA SECURITY : Project I**

**Project Name : Whale Phishing Attacks**

**INTRODUCTION:-**

This presentation will provide a deep dive into the world of whale phishing and strategies to prevent it.

Whale phishing is a targeted form of phishing that aims at high- proﬁle individuals within an organization. Attackers use sophisticated techniques to deceive and manipulate these individuals. Understanding the tactics and impact is crucial for prevention.

Whale phishing often involves spear phishing , where attackers customize emails to appear legitimate, and social engineering, manipulating emotions to elicit desired actions. Awareness of these tactics is essential for defence.

**METHODOLOGY:-**

**Whale phishing attacks, targeting high-value individuals within organizations, follow a structured methodology for successful execution. Here's a concise summary:**

**1.Target Identification and Research:** Identify and gather information about high-value targets within the organization.

**2.Profile Building:** Develop detailed profiles of targets to personalize phishing messages effectively.

**3.Message Crafting:** Create convincing phishing emails tailored to the targets' roles and interests.

**4**.**Spoofing and Impersonation:** Spoof email addresses and impersonate trusted sources to enhance credibility.

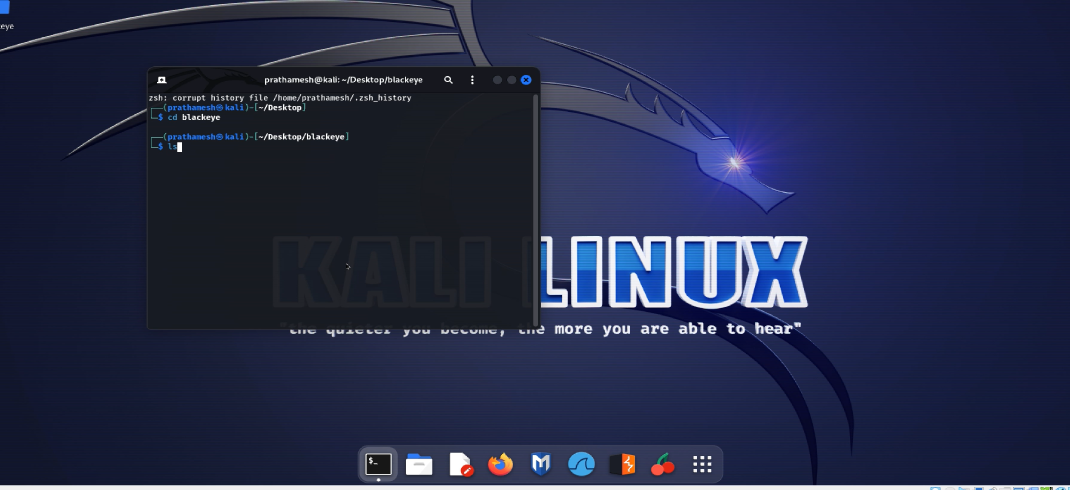
**5.Delivery and Distribution:** Send phishing emails using various methods and strategically schedule delivery.

**6.Monitoring and Follow-Up:** Monitor responses and follow up with additional attempts as needed to increase success rates.

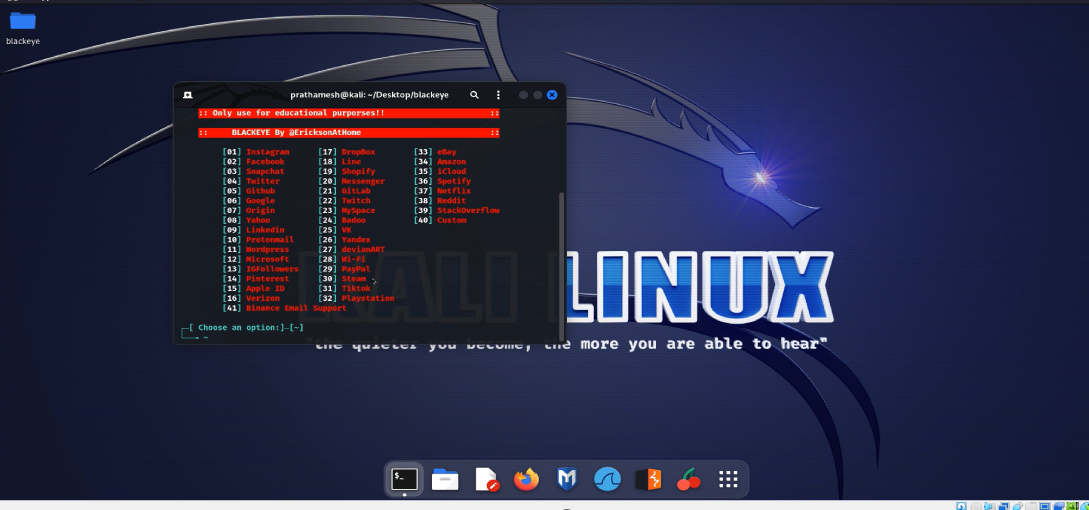
**7. Post-Attack Analysis:** Analyse outcomes to refine future attacks and improve security measures.

**Steps involve in the attacks are give below:-**

**STEP-1**: we have a blackeye tool which we have to open in kali linux which have all the fake fishing website.



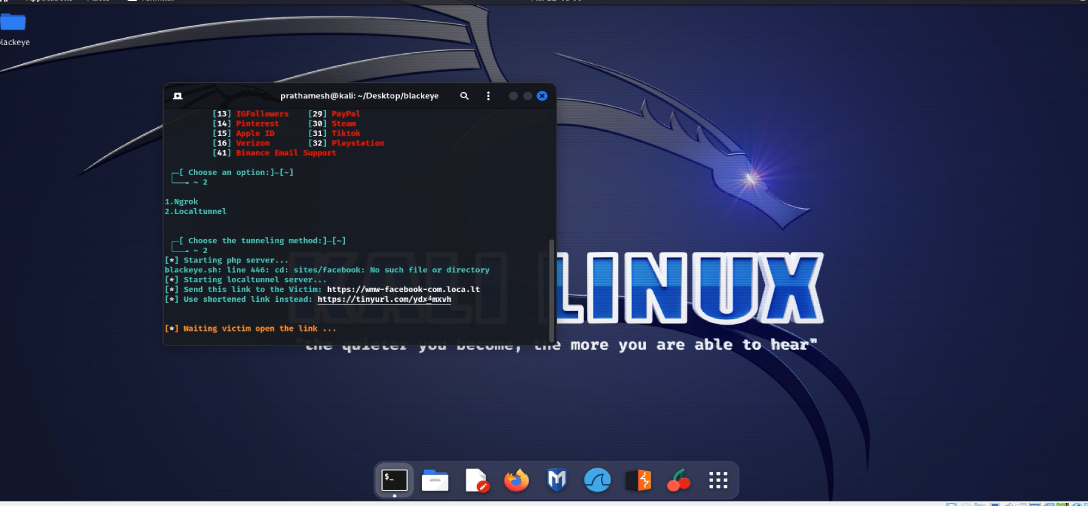
**STEP-2:** we can see all the available websites we have.



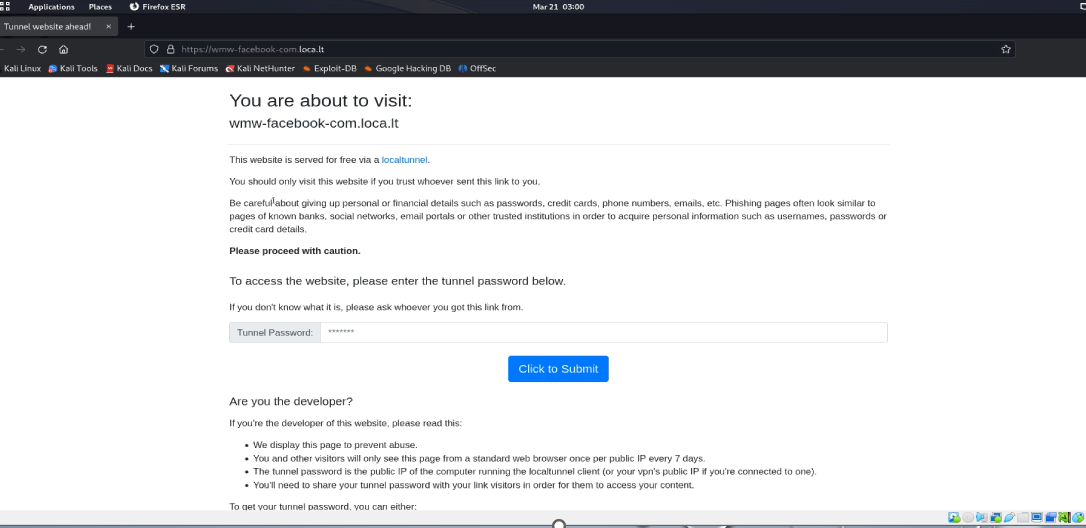
**STEP-3**: we can select the method we want to select.



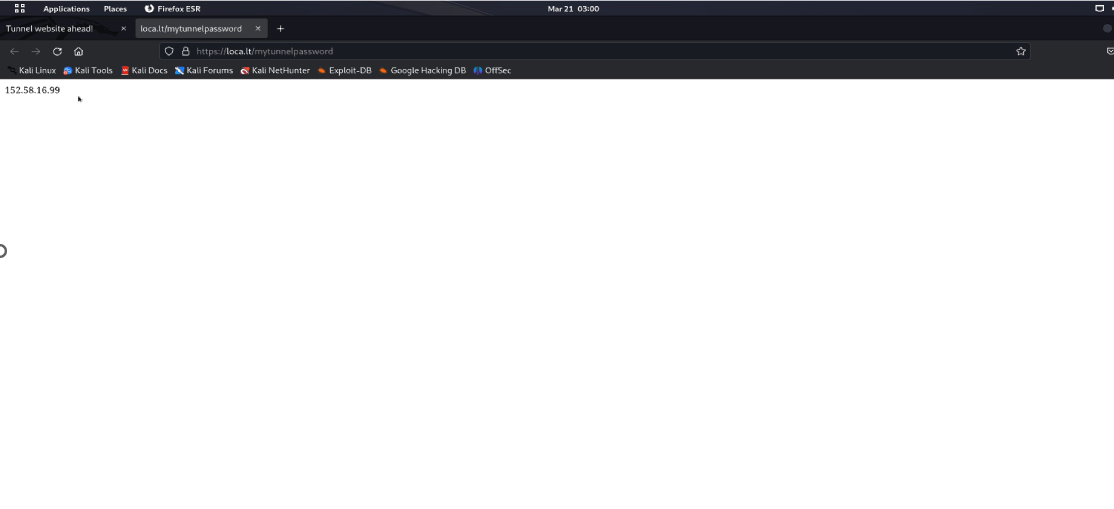
**STEP-4**: as soon as we select the method it start the server start and gives us the line we need to send to sender for access its login id and password.



**Step-5 :** we can see the page as open and we need to put password to access it.



**Step-6** **:** as we got the password put the password and you can access others id and password.



**Preventive Measures:-**

* To prevent whale phishing, use strong email security checks to make sure emails are really from who they claim to be from. Also, teach your team, especially top executives, about the dangers of phishing so they can spot suspicious emails and avoid falling for them.
* Utilizing advanced systems, encryption technologies, and behavioural analytics can signiﬁcantly enhance an organization's against whale phishing. Investing in technology is critical for it.
* Use email security tools to confirm if emails are real and from trusted sources. Train employees to recognize and avoid phishing attempts.

**Conclusion:-**

In conclusion, understanding the nuances of whale phishing and implementing a multi-faceted approach to prevention, detection , and response are essential for safeguarding organizations against this pervasive threat.