**SAPIENCE EDU CONNECT INTERNSHIP**

(**Cyber Security**)

**NAME :** KATAKAM LIKITH KUMAR

**REPORT DATE :**

**EMAIL :** [likithkumarkatakam811@gmail.com](mailto:likithkumarkatakam811@gmail.com)

**Week 4**  : Perform Phishing using Zphisher.

* Task 1:

**Objective** : To understand and analyze social engineering attack vectors, evaluate the effectiveness of phishing techniques, and assess the security awareness of users.

**Introduction :**

Phishing is one of the most prevalent cyber threats, leveraging social engineering techniques to deceive individuals into revealing sensitive information such as login credentials, financial details, or personal data. Attackers use various methods, including fake websites, emails, and messages, to trick users into believing they are interacting with a legitimate source.

Zphisher is an open-source phishing tool that automates the creation of fake login pages to demonstrate how attackers exploit human vulnerabilities. By simulating phishing attacks in a controlled environment, cybersecurity professionals and ethical hackers can analyze attack techniques, assess security awareness, and develop effective countermeasures.

**Software and Hardware requirements :**

Software :

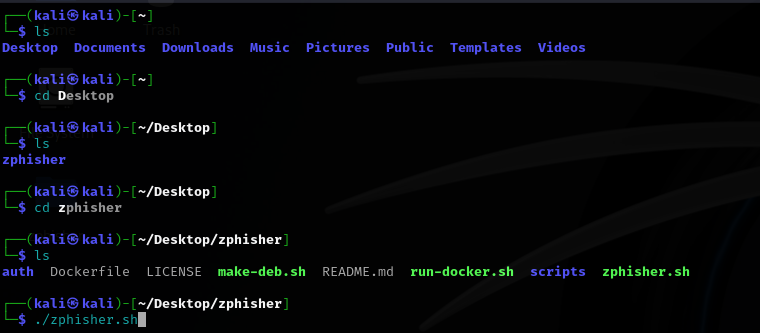
* Oracle virtual Box or VMware software
* Kali Linux
* Zphisher

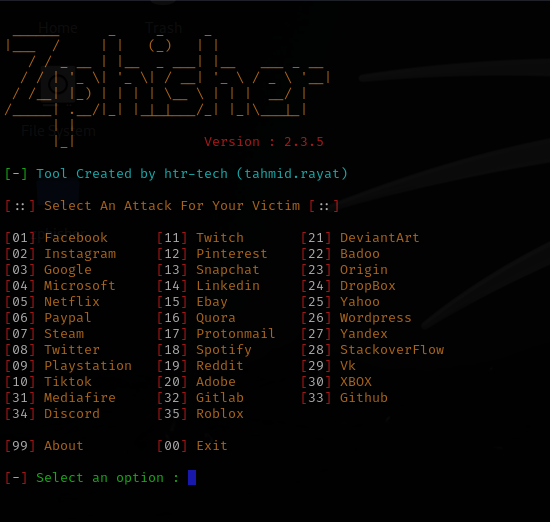
Hardware :

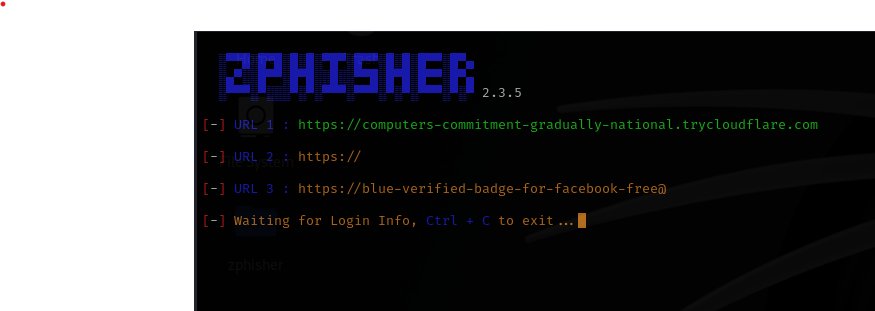
* Computer or Laptop with Internet connectivity

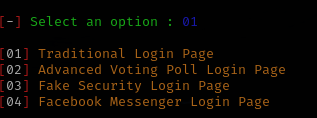
**Methodology**

1. **Setup Environment** – Install dependencies and clone Zphisher on a Linux-based system.
2. **Configure & Execute** – Run Zphisher, choose a phishing template, and select an attack vector (e.g., Ngrok, Cloudflare).
3. **Deploy Simulation** – Generate a phishing URL and distribute it ethically in a controlled test.
4. **Data Collection** – Monitor captured credentials (if any) and analyze user responses.
5. **Awareness & Mitigation** – Educate users, implement MFA, and enhance phishing detection.
6. **Reporting** – Document findings, identify security gaps, and provide recommendations.

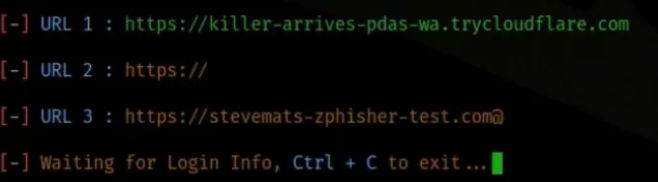
Output :











**Conclusion:**

ZPhisher is a powerful and effective phishing tool that leverages social engineering techniques to simulate popular login pages and steal sensitive information from unsuspecting users. While it serves as a useful tool for penetration testing and understanding security vulnerabilities, it should be used responsibly and ethically. Unauthorized use of ZPhisher or any phishing tool for malicious purposes is illegal and unethical, and can have serious consequences. To protect against phishing attacks, it is essential to implement strong cybersecurity measures, educate users about common phishing tactics, and promote safe online practices. Always remember that cybersecurity is a shared responsibility, and ethical hacking should always aim to improve and enhance digital security for all.

**Task 2 :**

**Objectives :**

**Identify Vulnerabilities** – Scan the target using Nmap to detect vsftpd 2.3.4.

**Exploit the System –** Use Metasploit to exploit the backdoor and gain access.

**Establish Persistence** – Maintain access via new user creation, SSH, or a reverse shell.

**Introduction :**

The exploitation of the vsftpd 2.3.4 vulnerability in a Metasploitable 2 machine using Nmap and Metasploit. The vsftpd 2.3.4 service contains a backdoor that allows remote unauthorized access. to identify the vulnerability, exploit it, establish persistence, and document the entire process. This highlights the risks of outdated software and emphasizes the importance of regular security assessments and patching.

**Methodology :**

**Reconnaissance –** Use Nmap to scan for open ports and detect vsftpd 2.3.4.

**Exploitation –** Use Metasploit to exploit the backdoor and gain unauthorized access.

**Post-Exploitation –** Establish persistence by:

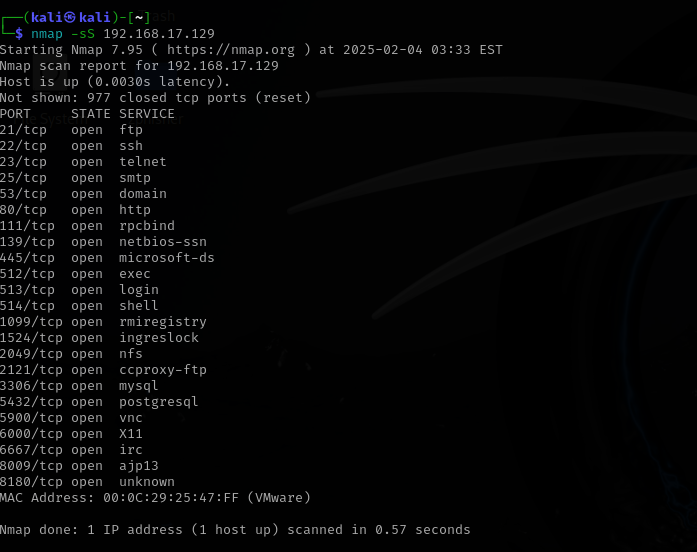
Creating a new user with admin privileges.

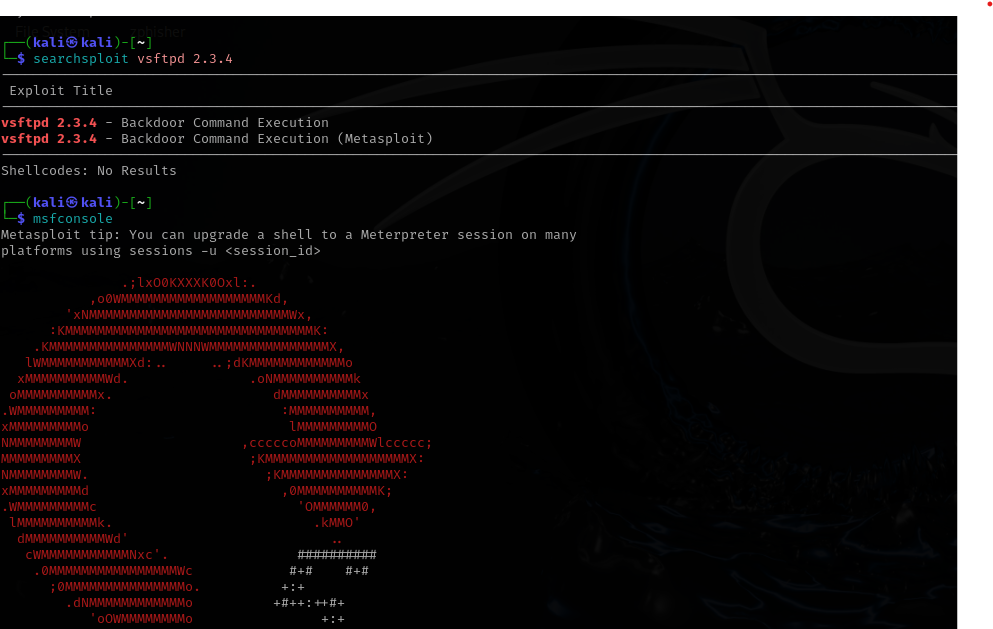
Enabling SSH for remote access.

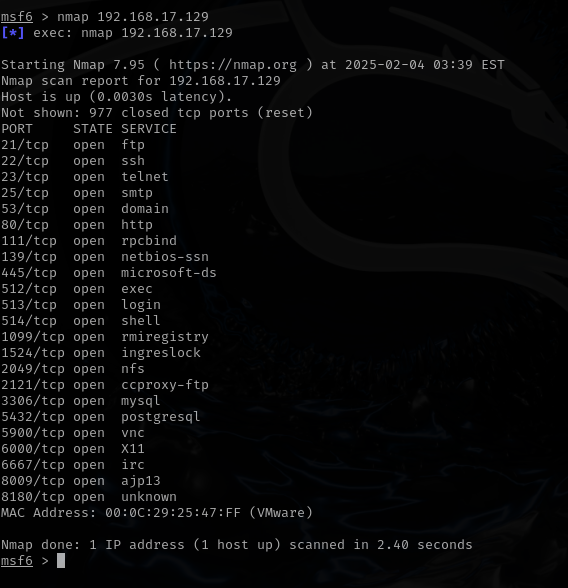
Setting up a reverse shell for re-entry.

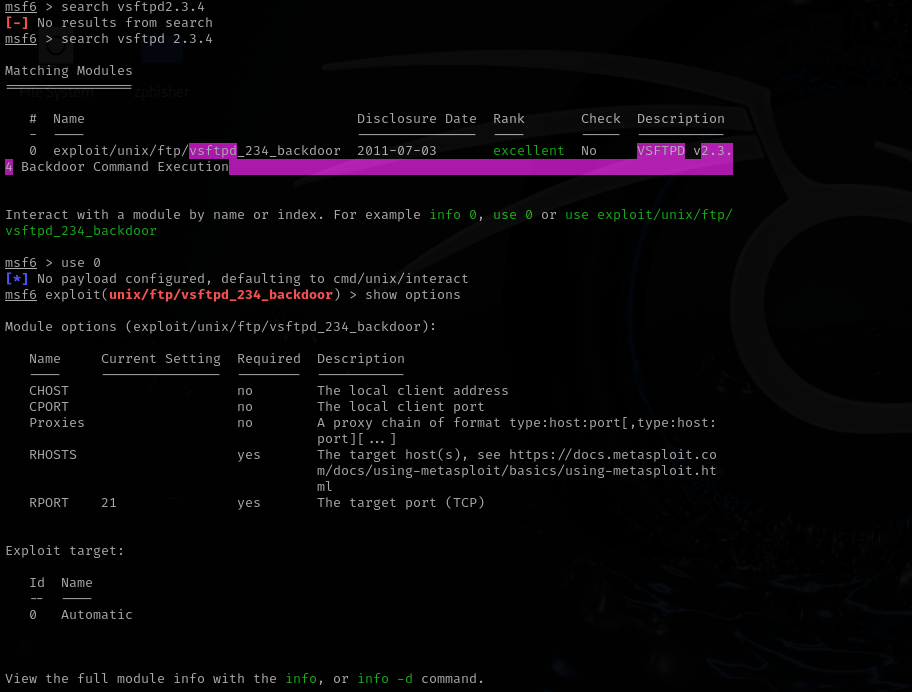
**Documentation & Analysis** – Record steps, outputs, and screenshots, and suggest mitigation strategies.

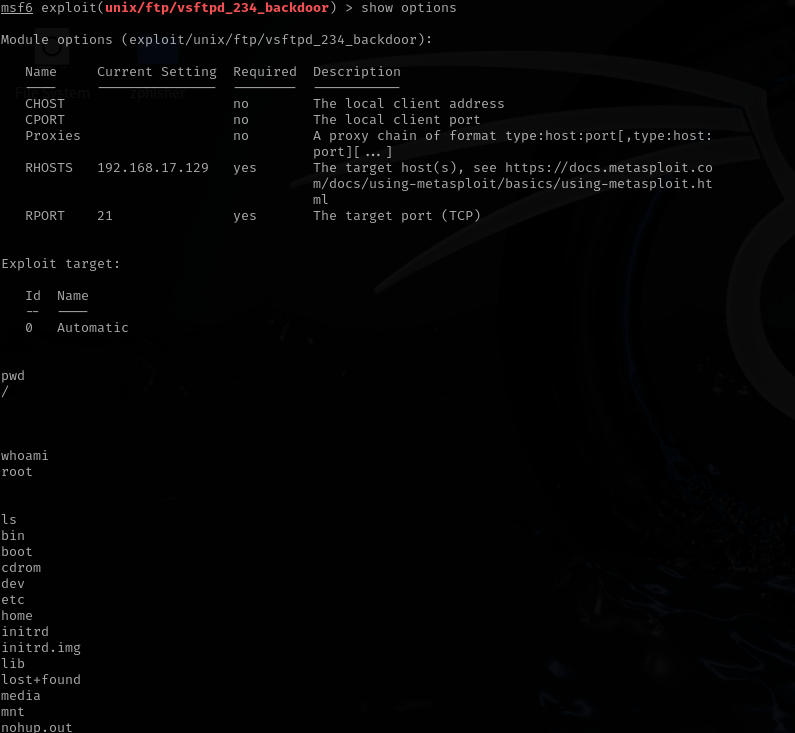
Output :

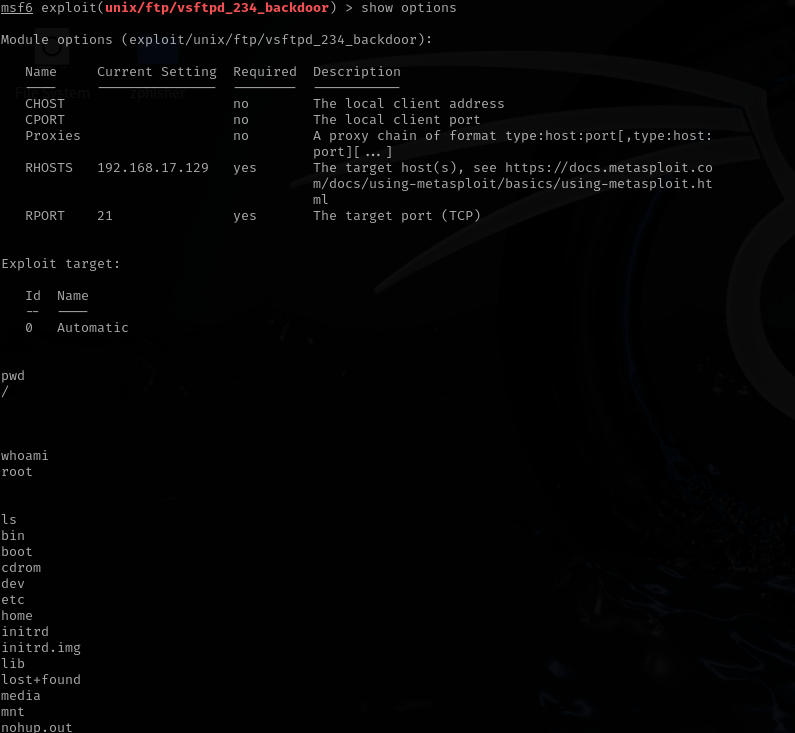


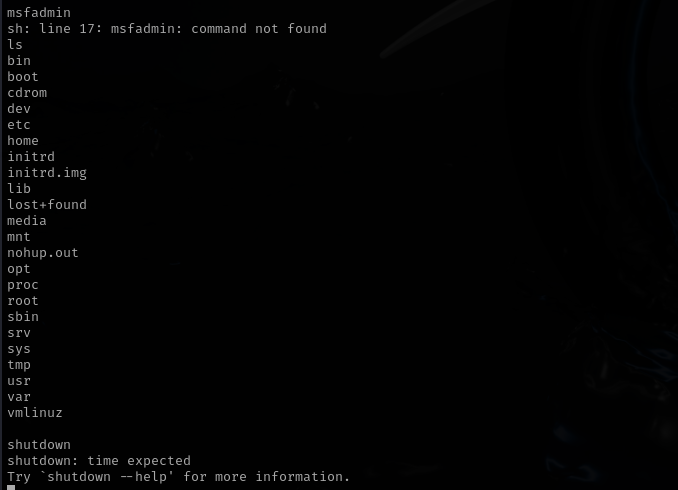












**Conclusion :**

The exploitation of the vsftpd 2.3.4 vulnerability in Metasploitable 2 using Nmap and Metasploit. By successfully gaining unauthorized access and establishing persistence, we highlighted the risks associated with outdated software. The findings emphasize the importance of regular security assessments, patch management, and system hardening to prevent such attacks.