EncryptEdge Labs

Cybersecurity Analyst Internship

Task Report

atalmamun@gmail.com

Task No: 10

Credit: Offensive Security

EncryptEdge Labs

Table of Contents

1.0 EncryptEdge Labs Internship Task Report **3**

1.1 Introduction 3

1.2 Objective 3

1.3 Requirements 4

2.0 Introduction to Social Engineering **5**

2.1 Understanding Social Engineering and Its Role in Red Teaming 5

2.2 Ethical Considerations in Social Engineering 5

3.0 Common Social Engineering Attacks **6**

4.0 Hands-on Exercises with HiddenEye **8**

4.1 Overview of the Tool Used 8

4.2 Setup and Installation Process 8

4.3 Phishing Simulation 9

4.4 Screenshots of the Simulation 10

4.5 Reflection on the Simulation 16

5.0 Lab Completion Screenshot **17**

5.1 Overview of the Lab 17

5.2 Lab Completion Screenshot 17

5.3 Reflection on the Lab 19

6.0 Reflection **20**

6.1 Personal Learning Experience 20

6.2 Challenges Encountered 20

6.3 Future Considerations in Red Teaming 21

6.4 Conclusion 21

1.0 EncryptEdge Labs Internship Task Report

1.1 Introduction

Social engineering is a technique used in cybersecurity that manipulates human behavior to gain unauthorized access to systems, networks, or confidential information. Unlike traditional hacking methods that rely on technical vulnerabilities, social engineering exploits psychological factors such as trust, curiosity, fear, or urgency. In red teaming exercises, social engineering plays a critical role by simulating real-world attacks that target the human element of security, often considered the weakest link. This task provided an opportunity to explore the principles of social engineering, understand various attack strategies, and experiment with phishing simulations using tools like SET (Social Engineering Toolkit) and HiddenEye.

1.2 Objective

The objective of this task is to gain a foundational understanding of social engineering and its relevance in cybersecurity. Key goals include:

- Defining social engineering and examining its role in red team operations.
- Identifying and simulating common social engineering attacks such as phishing, pretexting, and baiting.
- Gaining hands-on experience with phishing simulations using tools like SET and HiddenEye.
- Reflecting on the ethical considerations involved in using social engineering techniques responsibly and within legal boundaries.

1.3 Requirements

To complete this task, the following tools and platforms were required:

- **Social Engineering Toolkit (SET):** A powerful open-source framework used for simulating various types of social engineering attacks.
- **Phishing Simulation Platform – HiddenEye (or similar):** A tool used to create fake login pages and simulate phishing attacks.
- **TryHackMe – Phishing: HiddenEye Lab:** A guided hands-on lab designed to reinforce practical phishing techniques in a controlled environment.
- **Basic understanding of Linux command-line interface (CLI)** for executing commands during the simulation process.
- **Ethical mindset** to approach simulations responsibly, ensuring legal compliance and minimizing potential harm.

2.0 Introduction to Social Engineering

2.1 Understanding Social Engineering and Its Role in Red Teaming

Social engineering is a psychological manipulation technique used to deceive individuals into divulging confidential information or performing actions that compromise security. Rather than exploiting software vulnerabilities, social engineering exploits human vulnerabilities—such as trust, urgency, fear, or curiosity.

In the context of **red teaming**, social engineering is a vital tactic used to test an organization's security posture by simulating real-world attack scenarios. Red teamers often use social engineering techniques like phishing emails, phone-based scams (vishing), or impersonation (pretexting) to identify weaknesses in human behavior and awareness. These simulations help organizations understand how susceptible their employees are to manipulation and provide insights into improving security training and awareness.

Social engineering is commonly used in scenarios such as:

- Phishing campaigns targeting employees to gain login credentials.
- Impersonation tactics to gain physical access to restricted areas.
- Phone calls pretending to be IT support to extract sensitive information.

2.2 Ethical Considerations in Social Engineering

While social engineering is a powerful tool for assessing human-based security weaknesses, it must be approached with strict ethical standards to avoid harm and legal violations. Some of the key ethical considerations include:

- **Respect for Privacy:** Any simulation must avoid accessing or misusing personal data. Simulated attacks should be designed to mimic threats without intruding

into an individual's personal or private life.

- **Informed Consent:** Although realism is crucial, red team operations must operate under an agreement with the organization. All stakeholders, particularly leadership and legal teams, should be informed and consent to the simulation.

- **Minimizing Harm:** Social engineering simulations should not cause psychological distress, embarrassment, or career consequences for the employees involved. The aim is to educate, not punish.

- **Legal Compliance:** All simulations must adhere to legal frameworks. Unauthorized use of phishing tools or data collection outside the scope of agreed-upon simulations may result in legal consequences.

By combining realism with responsibility, social engineering exercises can be a valuable part of any security assessment strategy while maintaining professional and ethical integrity.

3.0 Common Social Engineering Attacks

Social engineering attacks take various forms, each targeting human psychology to bypass technical security controls. Understanding these attack types is crucial for recognizing and defending against them. The most common social engineering techniques include **phishing**, **pretexting**, and **baiting**.

3.1 Phishing

Phishing is one of the most widespread and effective social engineering attacks. In a phishing attack, an attacker typically sends fraudulent emails or messages that appear to be from a legitimate source—such as a bank, employer, or trusted service provider.

These messages often contain links to fake websites or malicious attachments designed to steal credentials or infect systems with malware.

Example:
A spoofed email from a company's IT department asking employees to reset their password using a provided link. The link leads to a fake login page that captures user credentials.

3.2 Pretexting

Pretexting involves creating a fabricated scenario to manipulate a victim into providing information or performing an action. The attacker often impersonates someone in a position of authority or trust, such as a colleague, manager, or support technician.

Example:
An attacker poses as a payroll administrator and calls an employee, claiming to need bank details for a "salary update," thereby tricking the employee into revealing sensitive financial information.

3.3 Baiting

Baiting relies on enticing a target with something appealing—such as free software, USB drives, or exclusive content—to lure them into compromising their system. The bait usually contains malware or leads the user to a malicious site.

Example:
A USB drive labeled "Confidential – Bonuses 2025" is left in the office parking lot. When an employee plugs it into their work computer out of curiosity, the device installs spyware.

4.0 Hands-on Exercises with HiddenEye

4.1 Overview of the Tool Used

I utilized **HiddenEye**, a phishing simulation tool designed for testing the effectiveness of phishing attacks by creating fake login pages for various online platforms. HiddenEye allows the user to simulate phishing attacks in a safe, controlled environment, helping understand how such attacks might be carried out in real-world scenarios. The tool provides a web interface to create fake login pages, such as those for popular platforms like Facebook, Instagram, and Google.

4.2 Setup and Installation Process

To set up HiddenEye, I followed these steps:

1. **Cloning the HiddenEye Repository:**
    - The HiddenEye tool was cloned from the official GitHub repository using the following command:
      `git clone https://github.com/DarkSecDevelopers/HiddenEye.git cd HiddenEye`
2. **Installing Dependencies:**
    - The dependencies listed in `requirements.txt` were installed using the following command:
      `pip3 install -r requirements.txt`
    - However, an issue arose due to the `pgrep` module not being found. After troubleshooting and removing the `pgrep` reference from the code, I was able to proceed with the installation.
3. **Running HiddenEye:**
    - After installation, I launched HiddenEye using the following command:
      `sudo python3 HiddenEye.py`

- This initiated the tool, and I was presented with a menu to select the phishing template.

4.3 Phishing Simulation

The phishing simulation was conducted using the **HiddenEye** tool, a popular framework used for simulating social engineering attacks such as phishing. The simulation aimed to create a fake Facebook login page to capture credentials when the target interacts with it. Below are the steps involved in the simulation:

1. **Tool Selection**: HiddenEye was executed in a Kali Linux environment. After launching the tool, I was prompted to select the phishing feature I wanted to use. I selected Facebook as the target platform for the phishing simulation.

2. **Feature Configuration**: After choosing Facebook as the target, I was asked to select additional features such as enabling a keylogger, using a fake Cloudflare protection page, and setting up data capture via email. For this simulation, I opted not to enable these additional features to focus on the core phishing attack.

3. **Server Configuration**: The tool then prompted me to select a server for hosting the phishing page. I chose **localhost** (option `00`), which allowed me to run the server on my local machine. The generated URL for the phishing page was http://127.0.0.1:4444, which could only be accessed from my local machine or other devices on the same network.

4. **URL Distribution**: Once the phishing page was up and running, I would typically distribute the URL to a target. Since I was performing the test in a controlled environment, I did not send the URL to a real target. Instead, I kept the URL to myself and monitored the tool's activity.

5. **Interaction Monitoring**: The tool waited for interactions from the target. If the phishing page were to be accessed by a victim, any submitted data (e.g., login

credentials) would be captured by HiddenEye and displayed in real-time.

By following this process, I simulated the creation of a phishing page, allowing me to understand how such attacks are performed and how tools like HiddenEye can be used in penetration testing and red teaming engagements.

4.4 Screenshots of the Simulation

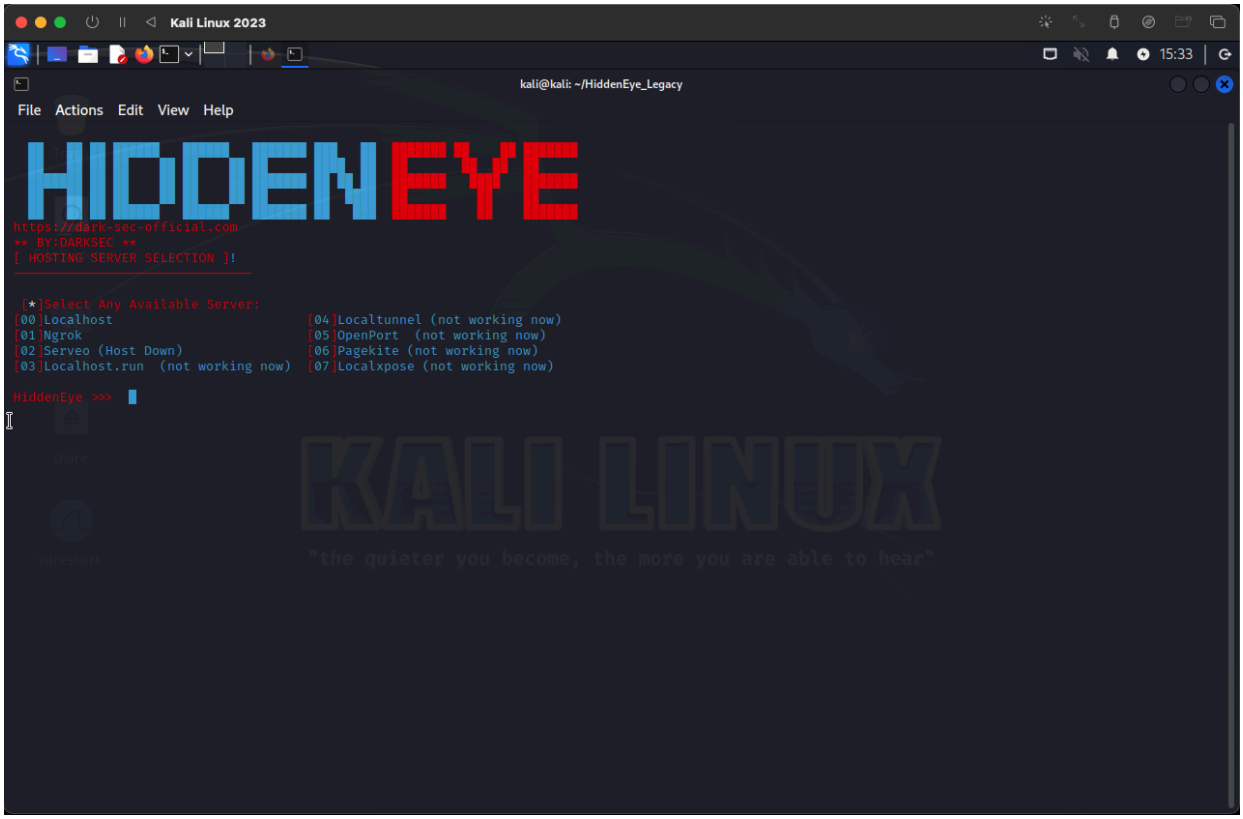
Below are the screenshots taken during the phishing simulation process:

1. **Step 1 - Phishing Feature Selection**: This screenshot shows the initial prompt where I selected **Facebook** as the target for the phishing attack.

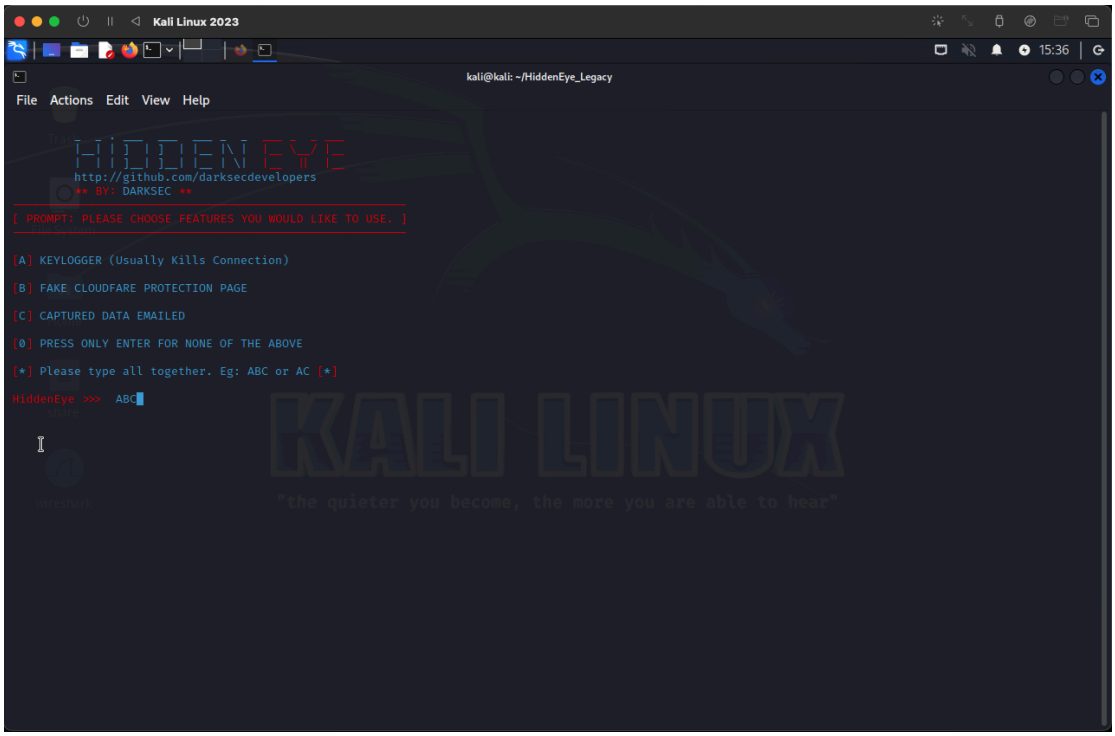
2. **Step 2 - Configuration of Additional Features**: In this step, I was prompted to select additional features like keylogging and fake protection pages. I chose not to enable any of these features for the simulation.

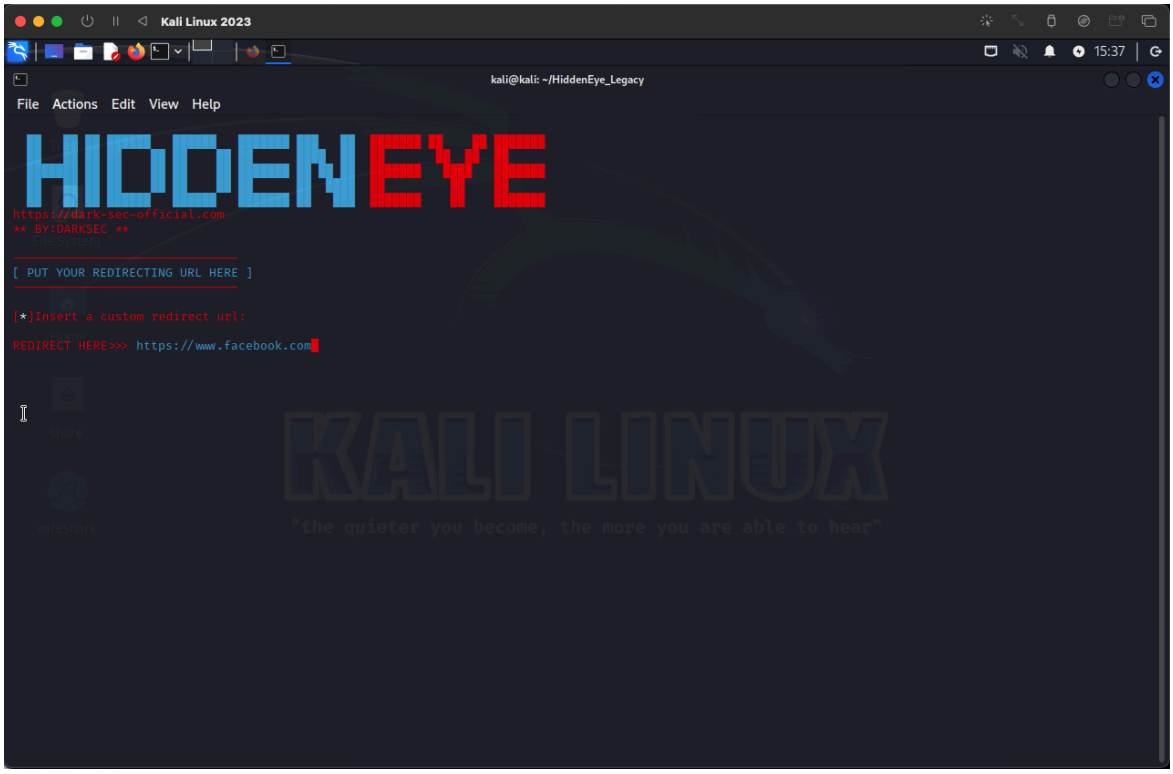
3. **Step 3 - Server Configuration**: This screenshot shows the prompt where I selected the **localhost** option to host the phishing page locally on my machine. The URL generated for the phishing page was **http://127.0.0.1:4444**.

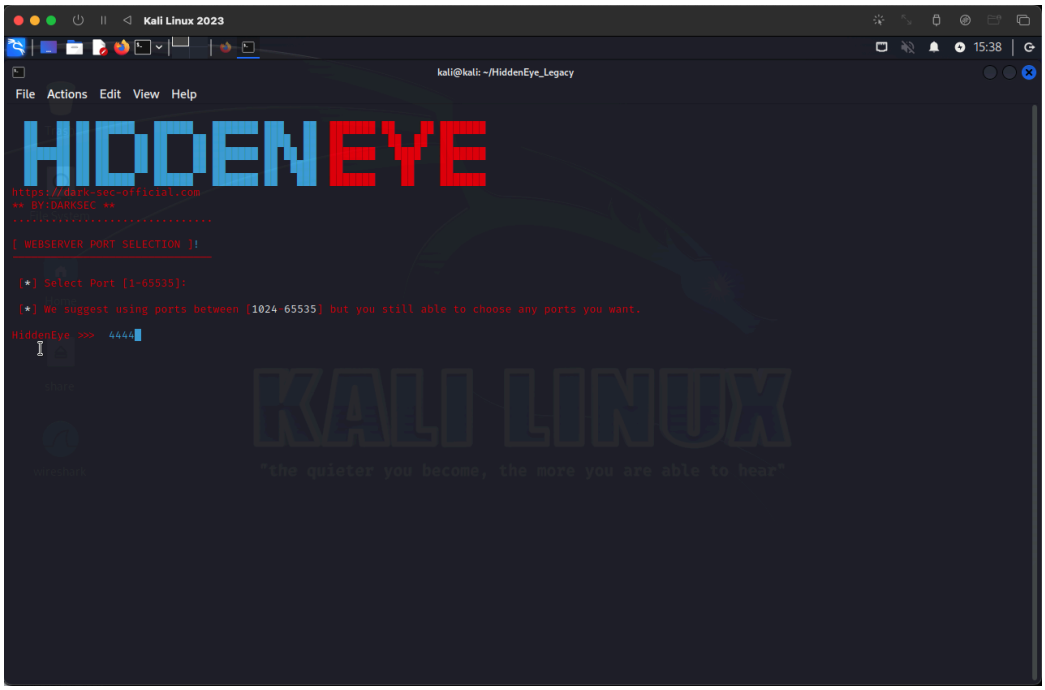
4. **Step 4 - Waiting for Target Interaction**: The tool displayed a waiting screen, indicating that it was ready to capture any interactions from the target. This is where the simulation would begin capturing data if a real victim interacted with the phishing page.

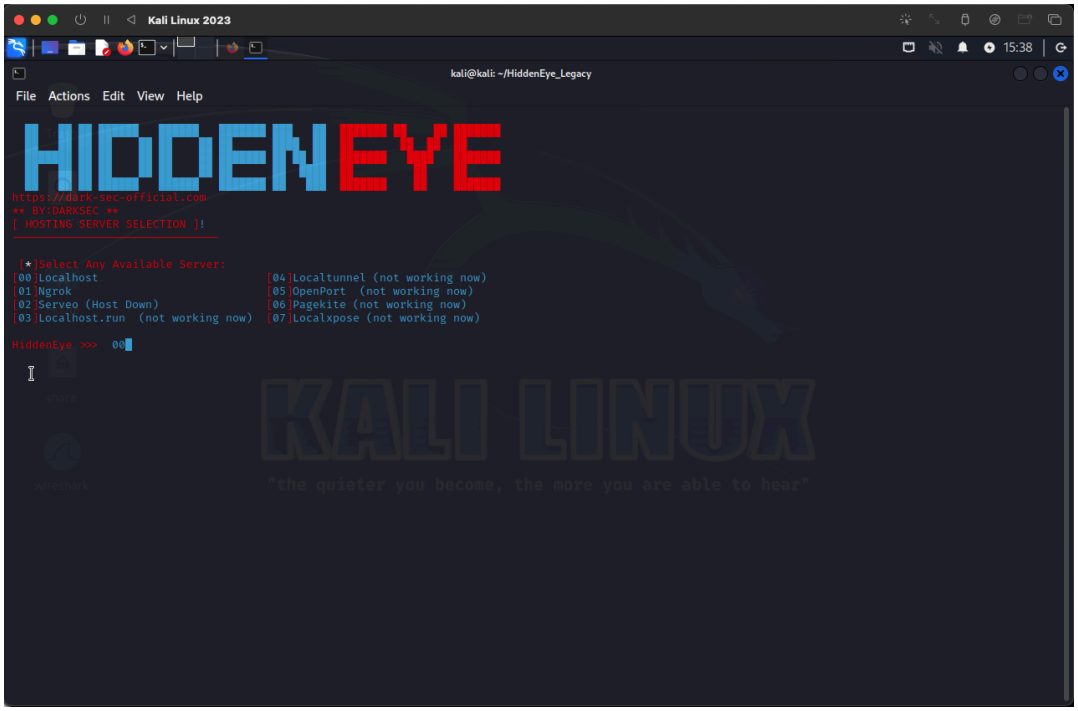

Kali Linux 2023
15:33
kali@kali: ~/HiddenEye_Legacy
File Actions Edit View Help
HIDDEN EYE
https://dark-sec-official.com
** BY:DARKSEC **
[HOSTING SERVER SELECTION]!
[★]Select Any Available Server:
[00]Localhost
[01]Ngrok
[02]Serveo (Host Down)
[03]Localhost.run (not working now)
[04]Localtunnel (not working now)
[05]OpenPort (not working now)
[06]Pagekite (not working now)
[07]Localxpose (not working now)
HiddenEye >>>
KALI LINUX
"the quieter you become, the more you are able to hear"

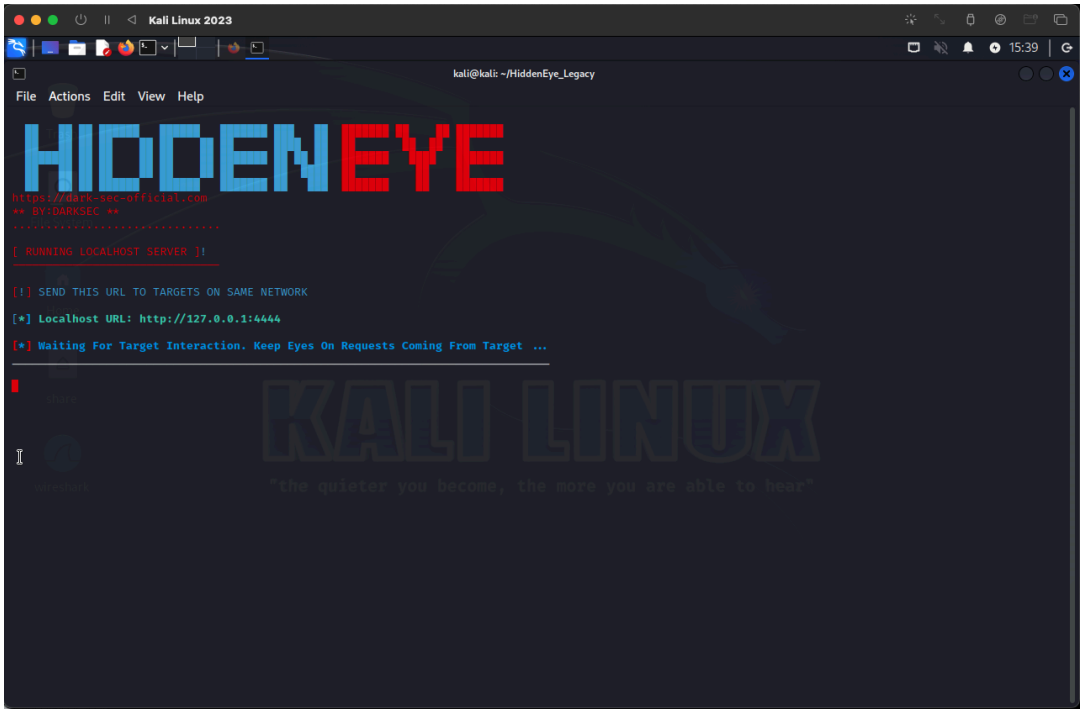

Kali Linux 2023
15:36
kali@kali: ~/HiddenEye_Legacy
File Actions Edit View Help
HIDDEN EYE
[v 1.0.0] BY:DARKSEC
[Modern Phishing Tool With Advanced Functionality]
[PHISHING-KEYLOGGER-INFORMATION COLLECTOR-ALL_IN_ONE_TOOL-SOCIALENGINEERING]
SELECT ANY ATTACK VECTOR:
PHISHING-MODULES:
[01] Facebook [13] Steam [25] Badoo [37] PlayStation
[02] Google [14] VK [26] CryptoCurrency [38] Xbox
[03] LinkedIn [15] iCloud [27] DevianArt [39] CUSTOM(1)
[04] GitHub [16] GitLab [28] DropBox [40] CUSTOM(2)
[05] StackOverflow [17] Netflix [29] eBay
[06] WordPress [18] Origin [30] MySpace
[07] Twitter [19] Pinterest [31] PayPal
[08] Instagram [20] ProtonMail [32] Shopify
[09] Snapchat [21] Spotify [33] Verizon
[10] Yahoo [22] Quora [34] Yandex
[11] Twitch [23] PornHub [35] Reddit
[12] Microsoft [24] Adobe [36] Subito.it
ADDITIONAL-TOOLS:
[0A] Get Target Location
HiddenEye >>> 01
Facebook IS LOADED ...
[*] SELECT ANY MODE ...
Operation mode:
[1] Standard Page Phishing
[2] Advanced Phishing-Poll Ranking Method(Poll_mode/login_with)
[3] Facebook Phishing- Fake Security issue(security_mode)
[4] Facebook Phishing-Messenger Credentials(messenger_mode)
HiddenEye >>> 1
"the quieter you become, the more you are able to hear"

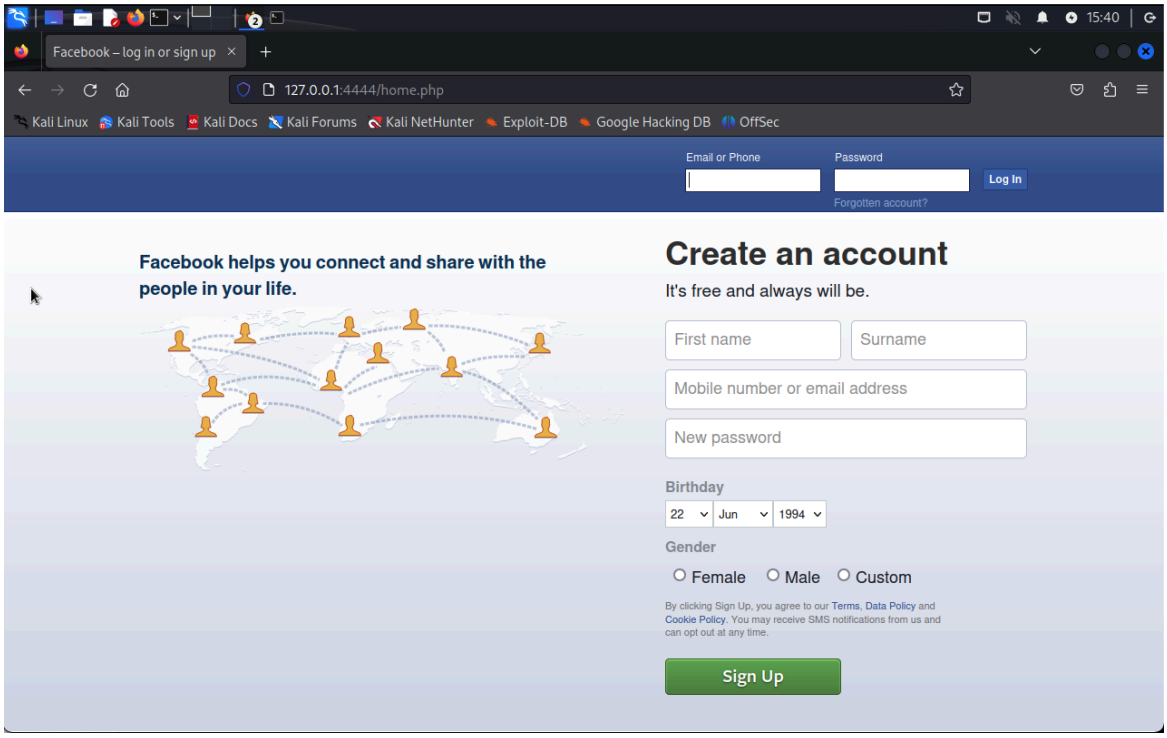

Kali Linux 2023
15:36
kali@kali: ~/HiddenEye_Legacy
File Actions Edit View Help
http://github.com/darksecdevelopers
** BY: DARKSEC **
[PROMPT: PLEASE CHOOSE FEATURES YOU WOULD LIKE TO USE.]
[A] KEYLOGGER (Usually Kills Connection)
[B] FAKE CLOUDFARE PROTECTION PAGE
[C] CAPTURED DATA EMAILED
[0] PRESS ONLY ENTER FOR NONE OF THE ABOVE
[*] Please type all together. Eg: ABC or AC [*]
HiddenEye >>> ABC
"the quieter you become, the more you are able to hear"

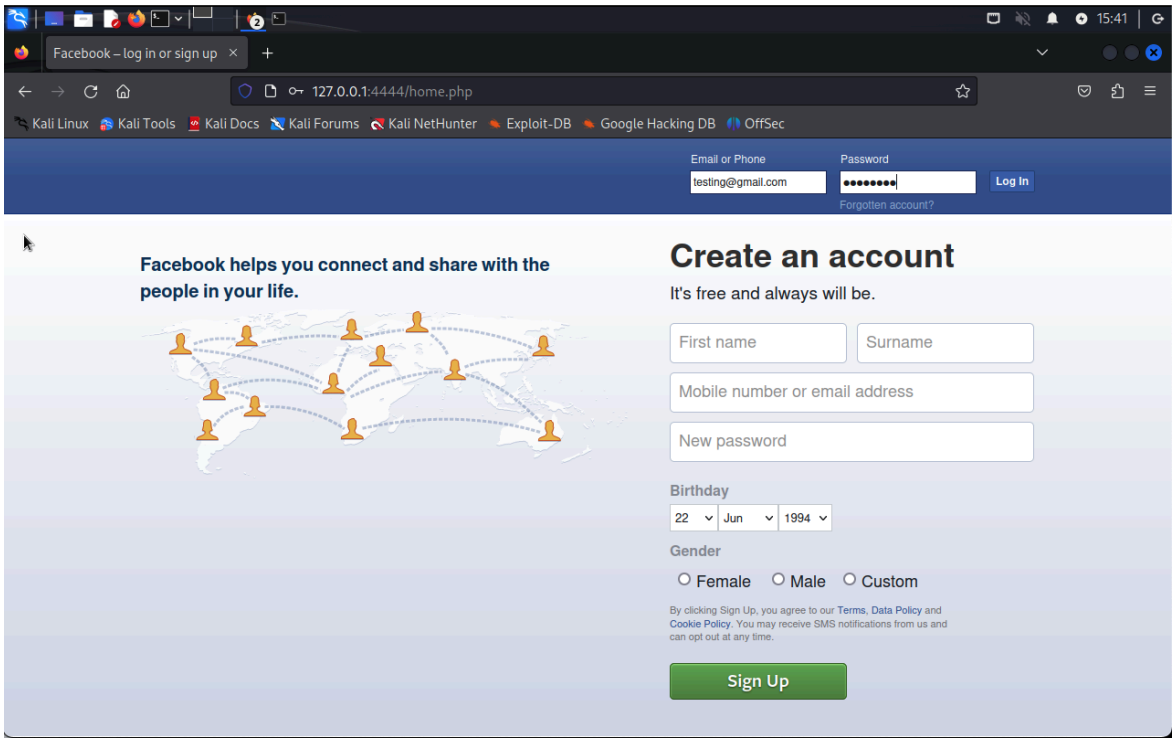

Kali Linux 2023
15:37
kali@kali: ~/HiddenEye_Legacy
File Actions Edit View Help
HIDDENEYE
https://dark-sec-official.com
** BY:DARKSEC **
[PUT YOUR REDIRECTING URL HERE]
[*]Insert a custom redirect url:
REDIRECT HERE>>> https://www.facebook.com
KALI LINUX
"the quieter you become, the more you are able to hear"

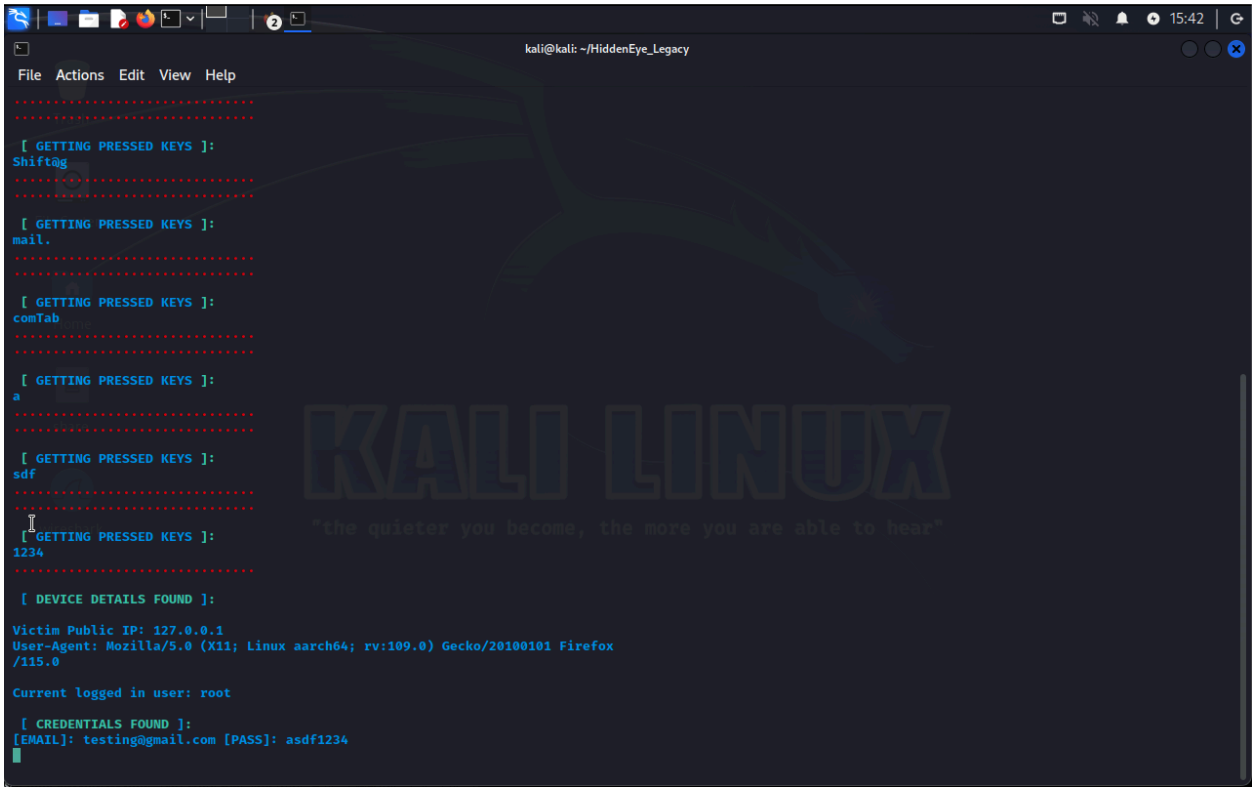

Kali Linux 2023
15:38
kali@kali: ~/HiddenEye_Legacy
File Actions Edit View Help
HIDDENEYE
https://dark-sec-official.com
** BY:DARKSEC **
[WEBSERVER PORT SELECTION]!
[*] Select Port [1-65535]:
[*] We suggest using ports between [1024-65535] but you still able to choose any ports you want.
HiddenEye >>> 4444
KALI LINUX
"the quieter you become, the more you are able to hear"

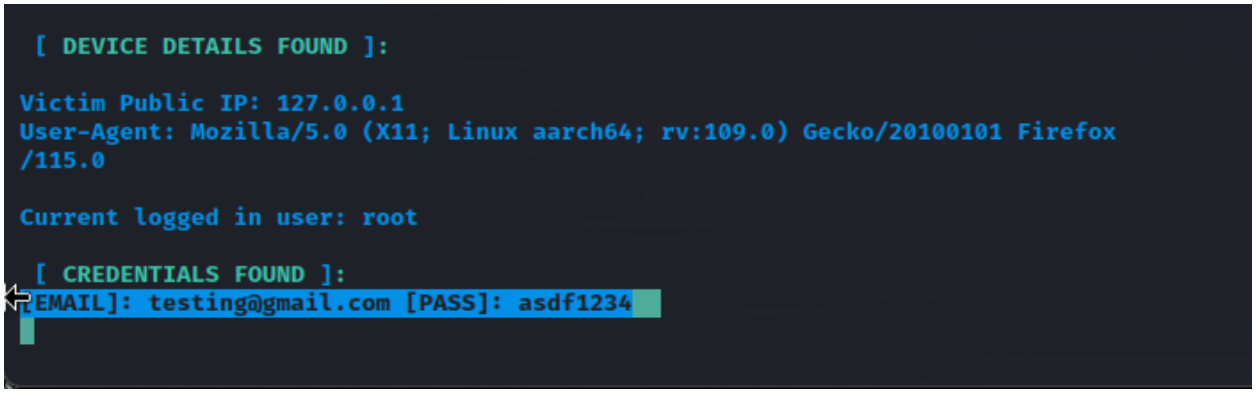

Kali Linux 2023
15:38
kali@kali: ~/HiddenEye_Legacy
File Actions Edit View Help
HIDDENEYE
https://dark-sec-official.com
** BY:DARKSEC **
[HOSTING SERVER SELECTION]!
[*]Select Any Available Server:
[00]Localhost
[01]Ngrok
[02]Serveo (Host Down)
[03]Localhost.run (not working now)
[04]Localtunnel (not working now)
[05]OpenPort (not working now)
[06]Pagekite (not working now)
[07]Localxpose (not working now)
HiddenEye >>> 00
KALI LINUX
"the quieter you become, the more you are able to hear"


Kali Linux 2023
15:39
kali@kali: ~/HiddenEye_Legacy
File Actions Edit View Help
HIDDENEYE
https://dark-sec-official.com
** BY:DARKSEC **
[RUNNING LOCALHOST SERVER]!
[!] SEND THIS URL TO TARGETS ON SAME NETWORK
[*] Localhost URL: http://127.0.0.1:4444
[*] Waiting For Target Interaction. Keep Eyes On Requests Coming From Target ...
KALI LINUX
"the quieter you become, the more you are able to hear"


15:40
Facebook – log in or sign up
127.0.0.1:4444/home.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Email or Phone
Password
Log In
Forgotten account?
Facebook helps you connect and share with the people in your life.
Create an account
It's free and always will be.
First name
Surname
Mobile number or email address
New password
Birthday
22 Jun 1994
Gender
Female Male Custom
By clicking Sign Up, you agree to our Terms, Data Policy and Cookie Policy. You may receive SMS notifications from us and can opt out at any time.
Sign Up


15:41
Facebook – log in or sign up
127.0.0.1:4444/home.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Email or Phone
testing@gmail.com
Password
Log In
Forgotten account?
Facebook helps you connect and share with the people in your life.
Create an account
It's free and always will be.
First name
Surname
Mobile number or email address
New password
Birthday
22 Jun 1994
Gender
Female Male Custom
By clicking Sign Up, you agree to our Terms, Data Policy and Cookie Policy. You may receive SMS notifications from us and can opt out at any time.
Sign Up





4.5 Reflection on the Simulation

Through this hands-on exercise, I gained practical experience with how phishing attacks are conducted and how tools like HiddenEye can be used to simulate such attacks. The process of creating a phishing page, deploying it, and capturing login credentials

provided a clear understanding of the steps involved in a phishing attack. The simulation also highlighted the effectiveness of phishing and the importance of implementing strong security practices, such as awareness training and multi-factor authentication, to protect against such attacks.

5.0 Lab Completion Screenshot

5.1 Overview of the Lab

As part of this task, I completed the **Phishing: HiddenEye** lab on TryHackMe, which provided practical experience in simulating phishing attacks using the HiddenEye tool. The lab aimed to familiarize me with phishing tactics, specifically using the HiddenEye tool to create and deploy phishing pages in a controlled and legal environment.

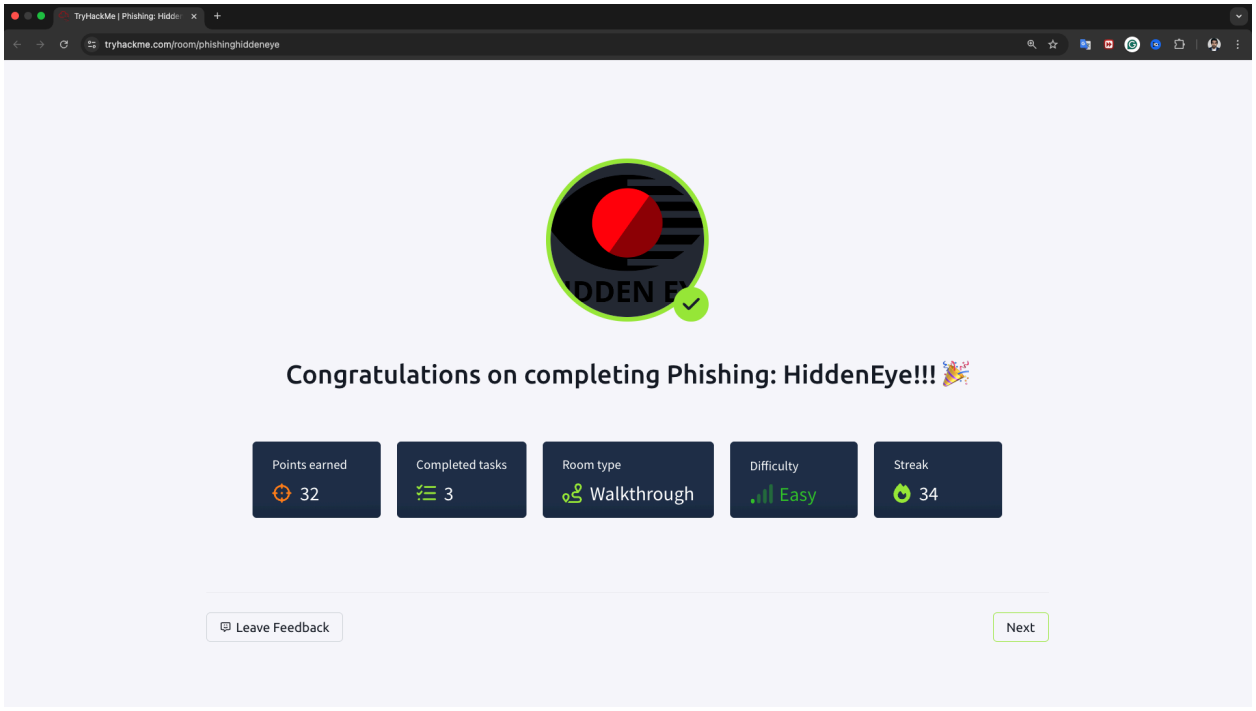
The **TryHackMe Phishing: HiddenEye** lab walked through various phases of setting up phishing campaigns, including:

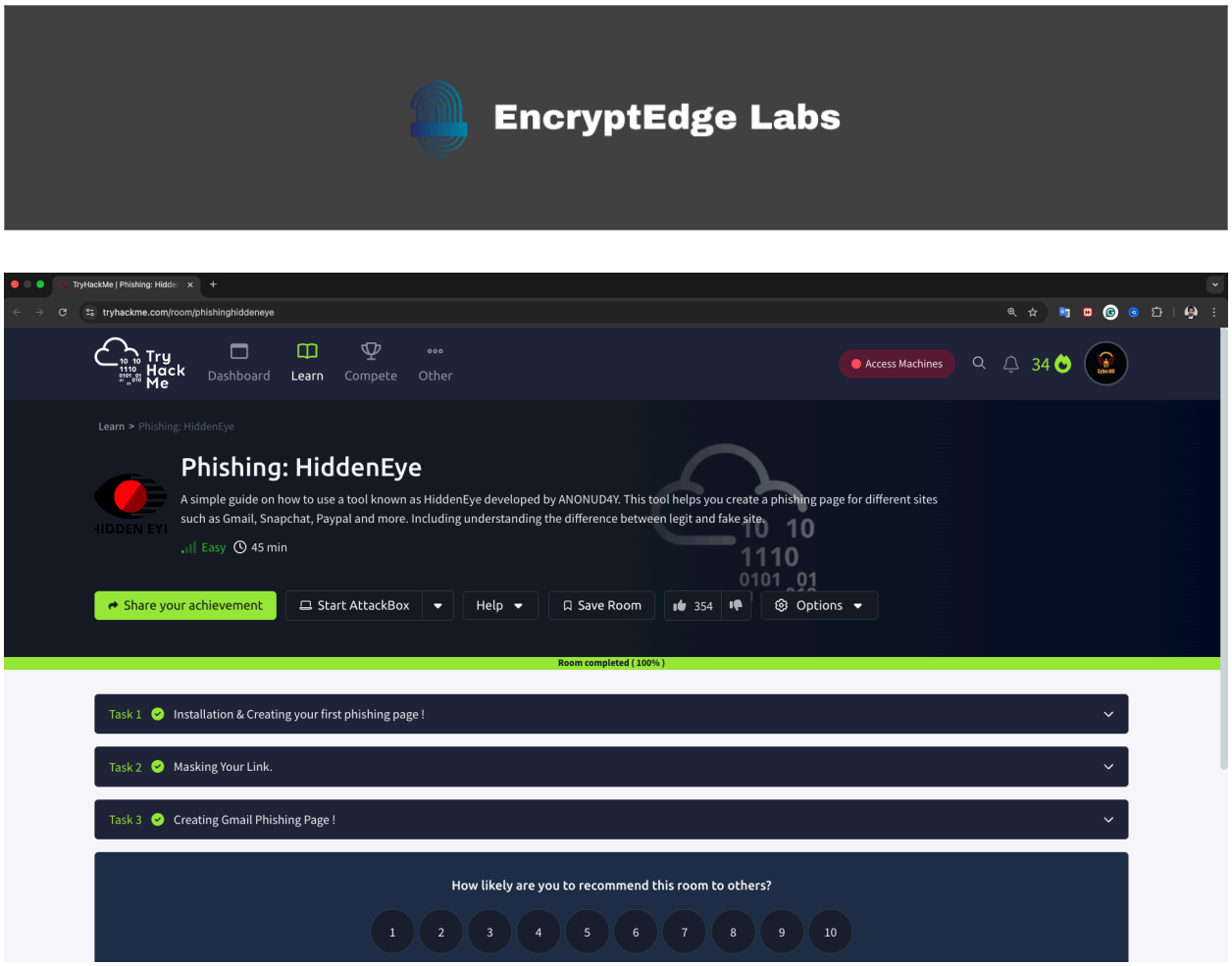
- Configuring HiddenEye
- Selecting a phishing target
- Generating a phishing link using ngrok
- Deploying the phishing page
- Capturing simulated credentials

By completing this lab, I was able to apply my learning from the previous section, where I worked with HiddenEye to simulate a phishing attack.

5.2 Lab Completion Screenshot

Below is the screenshot showing the successful completion of the TryHackMe **Phishing: HiddenEye** lab:





This screenshot confirms that the lab was completed successfully and provides proof of my hands-on experience with phishing simulations.

5.3 Reflection on the Lab

The **Phishing: HiddenEye** lab offered a practical and in-depth understanding of phishing attacks. It was particularly valuable for gaining real-time experience in simulating phishing scenarios, learning how attackers craft fake login pages, and understanding the process of capturing sensitive data like credentials. The lab reinforced the importance of cybersecurity awareness and the need for continuous vigilance against social engineering tactics like phishing.

6.0 Reflection

6.1 Personal Learning Experience

The **Phishing Identification** task provided an excellent opportunity to explore the practical side of social engineering in cybersecurity, particularly phishing. By working hands-on with **HiddenEye** and completing the **TryHackMe** lab, I gained a deeper understanding of how these attacks are carried out and how effective they can be in bypassing traditional security measures.

Throughout the task, I learned how attackers leverage human psychology—such as trust, curiosity, and urgency—to manipulate targets into revealing sensitive information like login credentials. The ability to create realistic phishing campaigns and simulate attacks was eye-opening, as it showcased the effectiveness of phishing in exploiting human vulnerabilities rather than relying solely on technical flaws.

6.2 Challenges Encountered

While working on the task, I encountered several challenges:

- **Tool Installation Issues:** Initially, I faced difficulties with missing dependencies and module errors (such as `pgrep`). However, these issues were resolved by editing the code and removing the problematic dependencies, allowing me to proceed.

- **Understanding Ethical Implications:** One of the more abstract challenges was understanding the ethical considerations behind using social engineering techniques in a professional environment. The line between ethical testing and malicious use can sometimes be thin, and it's essential to ensure that such techniques are used responsibly, within the confines of consent and legal boundaries.

Despite these challenges, the process provided valuable hands-on experience in recognizing the risks associated with phishing and how to defend against it.

6.3 Future Considerations in Red Teaming

Reflecting on the task, I have a better understanding of how social engineering attacks fit into the larger scope of **red teaming** activities. As a cybersecurity analyst, it is crucial to not only identify and mitigate phishing attacks but also to engage in regular awareness training for employees and stakeholders. Incorporating simulated phishing exercises into training programs can be a powerful tool for improving an organization's overall security posture.

In the future, I will continue to focus on the ethical use of social engineering tactics, ensuring that any red team exercises I participate in are conducted with the proper consent and in a manner that minimizes harm. Additionally, I will look into expanding my skills to other forms of social engineering, such as **pretexting** and **baiting**, and improve my ability to identify and defend against them.

6.4 Conclusion

This task reinforced the importance of human factors in cybersecurity and how social engineering, particularly phishing, remains a significant threat. The hands-on experience I gained with HiddenEye and the TryHackMe lab has been invaluable in solidifying my understanding of phishing tactics and the ethical considerations that come with employing such techniques. Moving forward, I feel better equipped to recognize, simulate, and defend against social engineering attacks in my role as a Cybersecurity Analyst.

EncryptEdge Labs

This Internship Task report was developed on [April, 06, 2025]

By:

atalmamun@gmail.com