|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: Nishchal Sreevathsa |  |  |  |  |

Social Engineering Using SET

Ethical hacking & Lab 15

Table of Contents

1. [Executive Summary 2](#_Toc409378035)

[Highlights](#_Toc409378036)

[Objectives](#_Toc409378037)

1. [Lab Description Details 2](#_Toc409378038)

[Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives](#_Toc409378039)

1. [Supporting Evidence 10](#_Toc409378040)
2. [Conclusion & Wrap-Up 12](#_Toc409378041)

[Summary with observations, Success & Failures, Challenges](#_Toc409378042)

# Executive Summary

## Highlights

|  |  |
| --- | --- |
|  | Social engineering is the practice of deceiving someone into disclosing private information or executing harmful software.  This lab shows how to hack a Windows server with a spear phishing assault that leverages Kali Linux's Social Engineering Toolkit (SET). |

## Objectives

|  |  |
| --- | --- |
|  | Learn how an attacker can take advantage of victims by using social engineering techniques.  Use the Social Engineering Toolkit to breach a Windows server.  Launch a spear-phishing assault.  Use the malware to steal information from a machine. |

# Lab Description Details

## Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives

**Step 1:** Accessed the external Kali Linux2 machine with IP Address 175.45.176.199 on the topology and entered **root** as username and **toor** as password.

A screenshot of a computer

Description automatically generated

**Step 2:** Opened the Linux terminal and viewed the files and folders using **ls** command.

**Challenge #1:** Retrieved **flag2.txt: 454561** using the command **more flag2.txt**.

Screens screenshots of a computer

Description automatically generated

**Step 3:** Scan the firewall for open ports using the command **setoolkit**.

**Challenge #2:** Found the **flag: 234511** next to the word codename Mr.Robot.

A screenshot of a computer

Description automatically generated

**Step 4:** In the set prompt selected **Social Engineering Attacks-> Website Attack Vector -> Metasploit Browser Exploit -> Web Templates**. Mention **no** when asked about NAT/Port Forwarding. Enter the IP Address as **175.45.176.199** for reverse connection.

A screenshot of a computer

Description automatically generated

**Step 5:** **Facebook** is selected as the template. Select **Metasploit Browser Autopwn** as the payload value. Use **Windows Reverse\_TCP Meterpreter shell**. Let the port to be used be selected as the **default port of 443**. The **server Started** message is displayed once the Metasploit is launched.

A computer screen shot of a computer program

Description automatically generated

**Getting Spear Phished**

**Step 6:** Launch the Windows Server and login as **administrator** and enter the password as **P@ssw0rd**. Open the Opera Mail and click on [**www.facebook.com**](http://www.facebook.com) link which was sent from Mark Zuckerberg.

A computer screen shot of a computer screen

Description automatically generated

**Step 7:** On the Facebook webpage enter the login using the email-id as [**student@campus.edu**](mailto:student@campus.edu) and Password as **password**.

A computer screen shot of a computer screen

Description automatically generated

**Step 8:** Once the credentials are entered, refresh the page and the page is seen blanked and hanged as the exploit began.

A computer screen shot of a computer

Description automatically generated

**Stealing Data**

**Step 9:** Go back to External Kali 2 Linux and check for the message **Successfully migrated to process** which is in green text on the terminal. Give the victims a list of all scheduled sessions. Engage in interaction with the victim machine's session. List the victim's current working directory. Alter the victim's current working directory. Enumerate the files on the victim's current directory.

A computer screen shot of a black screen

Description automatically generated

**Step 10:** Switch to the victim's share directory. Enumerate the files on the victim's current directory. Switch to the victim's share directory. Enumerate the files on the victim's current directory.

A screenshot of a computer

Description automatically generated

**Step 11:** Download the victim's files from the current directory.

A screenshot of a computer

Description automatically generated

**Step 12:** Examine the DeathStar pictures in Kali Machine's Home Folder.

A screenshot of a computer

Description automatically generated

**Challenge #3:** Opened the **Blueprint4.jpg** and found the **flag: 655913**.

A screenshot of a computer

Description automatically generated

**Challenge #4:** Opened the **Blueprint3.jpg** and found the **flag: 777558.**

**A screenshot of a computer

Description automatically generated**

**Challenge #5:** Opened the **Blueprint2.jpg** and found the **flag: 111222.**

A screenshot of a computer

Description automatically generated

# Supporting Evidence

**Screenshots, Research, Etc.**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

Organizations are seriously threatened by social engineering. Phishing emails are one method that hackers might employ to steal data. This lab demonstrated how SET may be used to infiltrate a victim system by building a phony website and sending phishing emails. Users need to be on the lookout for shady communications and should never send personal or account information by email.

**Observations:**

* It is simple to design convincing phishing attacks with the help of the SET toolkit.
* Private files and data can be easily exfiltrated if one has access to the victim system.

**Success:**

* Attack code was able to be launched on the Windows server through phishing emails.
* The victim system was given control by the Meterpreter payload, allowing file theft.

**Challenges:**

* Showing individuals how to spot phishing efforts and steer clear of them.
* Keeping users' inboxes free of fraudulent emails.

**Risks:**

* Phishing attacks that steal credentials can result in account compromise.
* Installing malware to steal confidential information, such as keyloggers.
* The use of ransomware to encrypt data and interfere with activities.
* Spread of malware known as botnets, which enables remote system control.
* Theft of intellectual property and confidential information.

**Remediations:**

* Users who receive security awareness training can recognize phishing efforts.
* sophisticated email filtering to detect harmful URLs and attachments in spear phishing emails.
* Implement multifactor authentication to stop people using credentials that have been stolen.
* Network segmentation to prevent lateral movement following a compromise.
* In order to identify data exfiltration, keep an eye out for unusual outgoing network traffic.
* The least privilege principle applies to user accounts and services.
* Patching and updating on a regular basis fixes known vulnerabilities.
* a plan for handling incidents that will swiftly neutralize dangers.
* Make a backup copy of your important data in case ransomware strikes.
* Turn off macros from unreliable sources in Office files.