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

Exploiting a Vulnerable Web Application

Ethical Hacking & Lab 10

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 19](#_Toc409378040)
2. [Conclusion & Wrap-Up 21](#_Toc409378041)

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

# Executive Summary

## Highlights

|  |  |
| --- | --- |
|  | In this lab, a network web application is attacked via an external Kali Linux computer. Nmap is utilized for scanning the network for vulnerable open ports on Apache httpd. After that, the XAMPP WebDAV/2 vulnerability on a Windows web server is exploited using Armitage, the graphical front-end for Metasploit. Access logs are downloaded following the compromise of the web server in order to determine the internal IP address of the victim web server. Next, pivoting is employed with a Meterpreter payload and an SMB vulnerability to compromise the internal Windows server. Deeper access to the internal network is made possible by this. |

## Objectives

|  |  |
| --- | --- |
|  | Nmap can be used for network reconnaissance to find open ports and services on target systems.  To choose and launch an exploit against a weak web application, use Metasploit and Armitage.  Hack the web server, examine the logs to find internal IP addresses, and switch to other systems.  Utilize Meterpreter payloads to gain continuous access to compromised systems.  Showcase post-exploitation methods such as hash dumping, file uploading, and execution.  Cover your tracks by removing any proof that you conducted penetration testing.  Recognize the moral and legal ramifications of breaking into systems without authorization and conducting penetration tests.  Get practical experience with hacking tools such as Nmap, Meterpreter, Armitage, Metasploit, and Kali Linux.  Gain useful skills that are relevant to jobs in ethical hacking and authorized penetration testing.  Discover how to combine several exploits to allow attackers to fully infiltrate target networks.  Gain a better understanding of offensive tools and techniques to enhance defensive security skills. |

# Lab Description Details

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

**Scanning and Finding a Exploit**

**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:** In command prompt we search for open ports in the firewall for IP Address 203.0.113.100 using **nmap**.

Command: **nmap 203.0.113.100**

Found the **Sample Flag:999818** for TCP port number 8180.

Screens screenshot of a computer

Description automatically generated

**Step 3:** **Zenmap** Application is then opened from the command prompt using the command: **zenmap**. Once after the application gets opened enter [**203.0.113.100**](http://www.campus.edu) in the Target field and select the scan button to perform the intense scan. After several minutes the number of open ports will be displayed in **Ports/Host Tab**. Then close the zenmap without saving. When you run a firewall scan, take note of the **Apache httpd 2.2.14 (Win32) DAV/2** banner that appears for port 80.

A screenshot of a computer

Description automatically generated

**Attacking the Target**

**Step 4:** Launch the Armitage directory after starting the Postgresql service, then spin up the Armitage.

A screenshot of a computer

Description automatically generated

**Challenge #1:** When entered the banner command multiple times in Armitage console, captured the **flag2 number:** **776554**.

A screenshot of a computer

Description automatically generated

**Challenge #2:** When entered the banner command multiple times in Armitage console, captured the **flag3 number:** **223444**.

A screenshot of a computer

Description automatically generated

**Step 5:** In Armitage GUI, **add** the host **203.0.113.100**.

A screenshot of a computer

Description automatically generated

**Step 6:** We determine the host's operating system once the scan is finished.

A screenshot of a computer

Description automatically generated

**Step 7:** Locate **xampp\_webdev\_upload\_php** in the http directory, then upload it to the victim's machine.

A computer screen shot of a computer

Description automatically generated

**Step 8:** Upload it, then initiate the assault. Attack is made on Victim Machine. Press Enter after performing a right-click on the compromised victim, choosing Meterpreter 1, Exploration, Browse Files, and **Erase WebDAV**.

A screenshot of a computer

Description automatically generated

**Step 9:** Download the **flag4.txt** file by opening the apache folder, the module folder, and the flag4.txt file.

A screenshot of a computer

Description automatically generated

**Step 10:** Download the **flag5.txt** file by opening the logs folder and finding the file there.

A screenshot of a computer

Description automatically generated

**Step 11:** To highlight the access.log file, click on it. Then choose Download by performing a right-click on the access log. On the Downloads tab, select the access.log file and press the Open Folder button.

A screenshot of a computer

Description automatically generated

**Step 12:** Click on 203.0.113.100 -> C: -> xampp -> apache.

**Challenge #3:** Opened the **flag4.txt** file and captured the **flag number: 345678**.

A screenshot of a computer

Description automatically generated

**Challenge #4:** Opened the logs folder and captured the **flag:818772** for **flag5.txt**.

A screenshot of a computer

Description automatically generated

**Challenge #5:** Opened the access.log folder and captured the **flag: 445616** for **flag6.txt**.

A screenshot of a computer

Description automatically generated

**Post Exploitation**

**Step 13:** Next, add a route to the local area network (LAN) of the victim.

A computer screen shot of a computer

Description automatically generated

**Step 14:** Add the host, 192.168.1.10, to the route now.

A screenshot of a computer

Description automatically generated

**Step 15:** The **203.0.113.100** host will be positioned beneath the **192.168.1.10** host. Verify the **smb\_version** using the msf prompt. set the remote host's IP address. Do the scan now. Windows will be recognized as 192.168.1.10.

A computer screen shot of a computer

Description automatically generated

**Step 16:** Navigate to Armitage in the menu bar, choose **Poor**, then Set Exploit Rank.

A screenshot of a computer

Description automatically generated

**Step 17:** Right-click the host after it has been added, then choose which attack to launch. Use a reverse connection, pick the **m09\_050\_smb2\_negotiate\_func\_index**, and start it.

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer

Description automatically generated

**Step 18:** Choose the exploit and enter **443** as the port for the **meterpreter\_reverse\_tcp** connection.

A screenshot of a computer

Description automatically generated

**Step 19:** Launch the attack extension after saving it as **firefox.exe**.

A screenshot of a computer

Description automatically generated

**Step 20:** Click on browse file and select **Erase Windows\system32** on the compromised machine, which is 192.168.1.10.

A screenshot of a computer

Description automatically generated

**Step 21:** Choose firefox.exe and click the upload button to **launch** it.

A screenshot of a computer

Description automatically generated

**Step 22:** Locate **firefox.exe** by searching the **C:\ Drive**. After highlighting the firefox.exe file with a click, right-click it and choose Execute.

A screenshot of a computer

Description automatically generated

**Step 23:** The **windows/meterpreter\_reverse\_tcp** tab should be clicked. **Meterpreter session 3** ought to be open.

A screenshot of a computer

Description automatically generated

**Step 24:** When you perform a right-click on the compromised victim, 192.1688.1.10, you can choose Registry method, Meterpreter 3, Access, and **Dump Hashes**. Press Start.

A screenshot of a computer

Description automatically generated

**Step 25:** **Copy the two hashes** and the Administrator account by selecting them.

A computer screen shot of a computer

Description automatically generated

**Step 26:** Using the terminal, create and open the **leafpad pass.txt** file, then paste the copied text into it.

A screenshot of a computer

Description automatically generated

**Step 27:** Now that the firefox payload has been successfully executed, we can use **John the Ripper** to decode it and dump the hashes.

A screenshot of a computer

Description automatically generated

# Supporting Evidence

**Screenshots, Research, Etc.**

**A screenshot of a computer

Description automatically generated**

**Screens screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

This lab gave participants real-world experience breaking into a web application that was vulnerable and then turning around to compromise another internal system. Common hacker techniques were demonstrated using Nmap, Metasploit, Armitage, and Meterpreter, among other Kali Linux penetration testing tools.

The lab made clear how crucial comprehensive defenses are. It is insufficient to rely only on perimeter firewalls because attackers can gain initial access through publicly disclosed vulnerabilities. To prevent privilege escalation and lateral movement, multi-layered internal protections are essential. Metasploit and other offensive tools draw attention to vulnerabilities that defenders need to fix right away.

**Success:**

* Concluded the use of Nmap to scan networks for vulnerable Apache httpd services.
* Successfully used the XAMPP WebDAV module in Metasploit to exploit the web server.
* On the compromised Windows server, the Meterpreter payload was uploaded and run.
* Recovered password hashes via post-exploitation access to Meterpreter.
* Exhibited typical hacker tactics, such as changing directions and hiding tracks.

**Challenges:**

* Handling security warnings from Metasploit components and invalid SSL certificates.
* Keeping in mind the procedures for payload delivery and post-exploitation tasks.
* Handling several active Meterpreter sessions and shells.
* Technical difficulties with uploading files, launching Armitage, and configuring exploit ranks.
* Completing every stage of exploitation in the allotted lab time.

**Risks:**

* Vulnerable software presents a serious risk since attackers may find it simple to gain initial access to publicly accessible services. It is essential to keep software updated and patched.
* Unused ports that are open provide access points for attackers. Use network segmentation and firewall rules to limit the services that are exposed.
* Passwords in plaintext carry a significant risk of compromise. Implement hash storage and strict password policies.
* An attacker can access more systems and data by moving laterally without being noticed. Check the network and systems for any strange activity.
* After a breach, inadequate logging makes investigations challenging. Make sure that sufficient event and access logging is turned on.
* Via systems that are exploited, attackers can move farther into the network. Rapidly isolate compromised systems.
* If tracks are not covered, an attacker may be identified. Employ anonymizing software, VPNs, and other opsec precautions.
* It is unethical and illegal to perform live exploitation without consent. Practice offensive techniques only in ranges or labs that are authorized.

**Remediations:**

* Tighten up public-facing systems and examine open ports and exposed services.
* Conduct penetration tests and vulnerability scanning on a regular basis. Keep your asset inventory up to date.
* Apply the least privilege principle. Limit the privileges of service accounts and users.
* To restrict lateral movement, use network segmentation and firewalls.
* Use a password manager and implement more robust authentication procedures.
* Keep an eye out for strange file transfers and internal communications in network traffic.
* Install behavioral analytics software and host-based monitoring to find security vulnerabilities.
* Create and implement an incident response strategy to eliminate and contain hazards.
* Train end users in cybersecurity awareness to make them aware of the risks.