Exploiting a Vulnerable web Application

ETHICAL HACKING & LAB Assignment 5

Student Info
Name: SRIJA PABBA
Student ID: 00866719
Email: spabb6@unh.newhaven.edu

Table of Contents

Executive Summary

Highlights

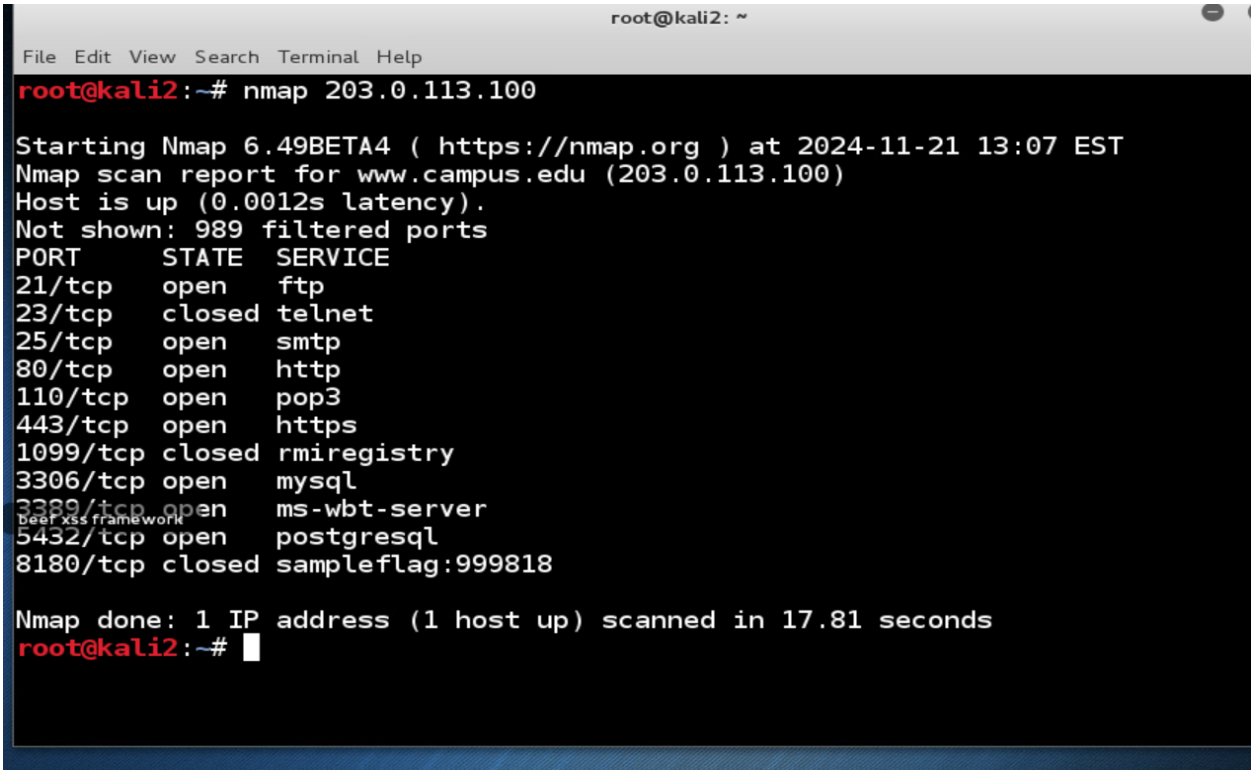
> *In this lab, I learned how to exploit a vulnerable web application using tools like nmap, Zenmap, and Armitage. I performed network scanning to identify open ports, exploited the XAMPP WebDAV vulnerability to gain access, and pivoted to exploit a Windows Server SMB vulnerability (MS09-50). I also practiced advanced techniques such as autorouting and using Meterpreter for internal network exploitation.*

Objectives

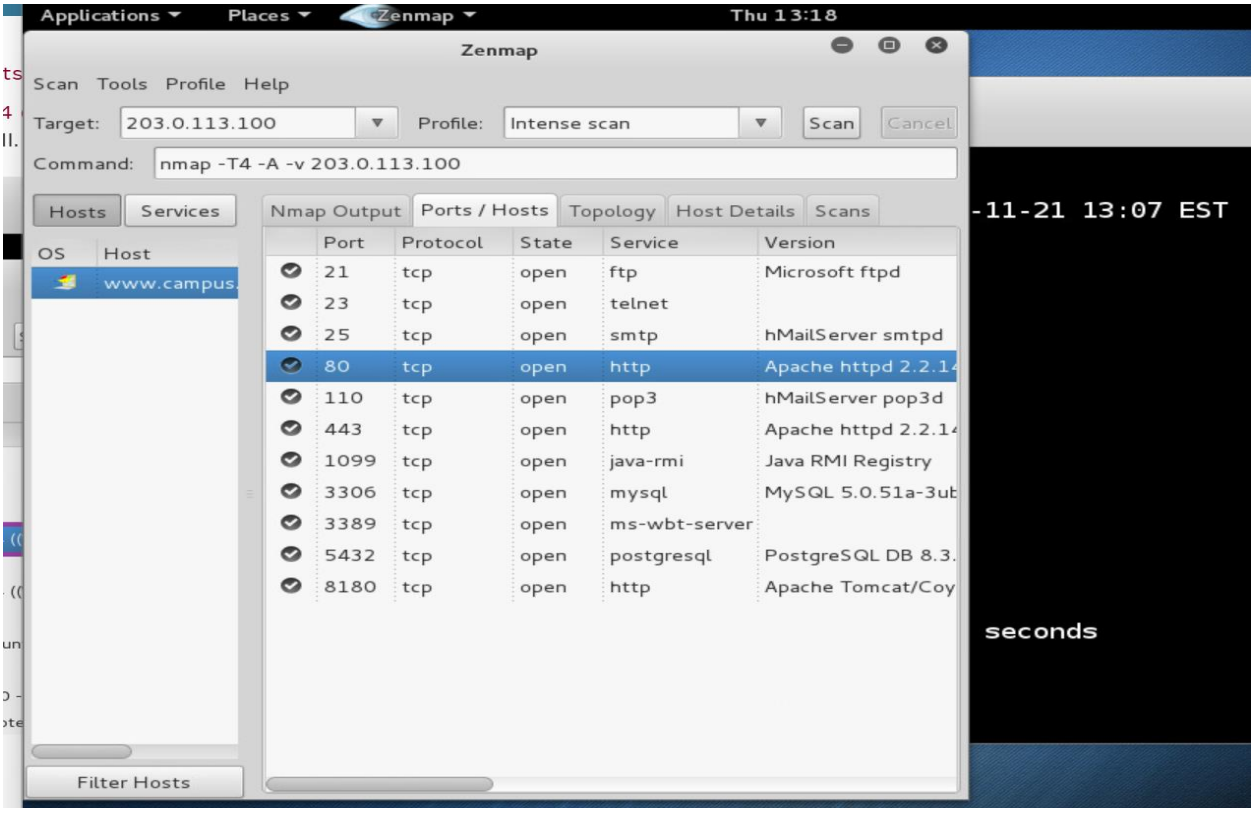
> *My objective in this lab was to enhance my skills in network scanning, exploiting web application vulnerabilities using Metasploit, and pivoting to internal networks. I focused on leveraging the XAMPP WebDAV exploit, performing SMB attacks on Windows servers, and building expertise in multi-layered attack scenarios.*

Lab Description Details

Scanning the firewall for open ports

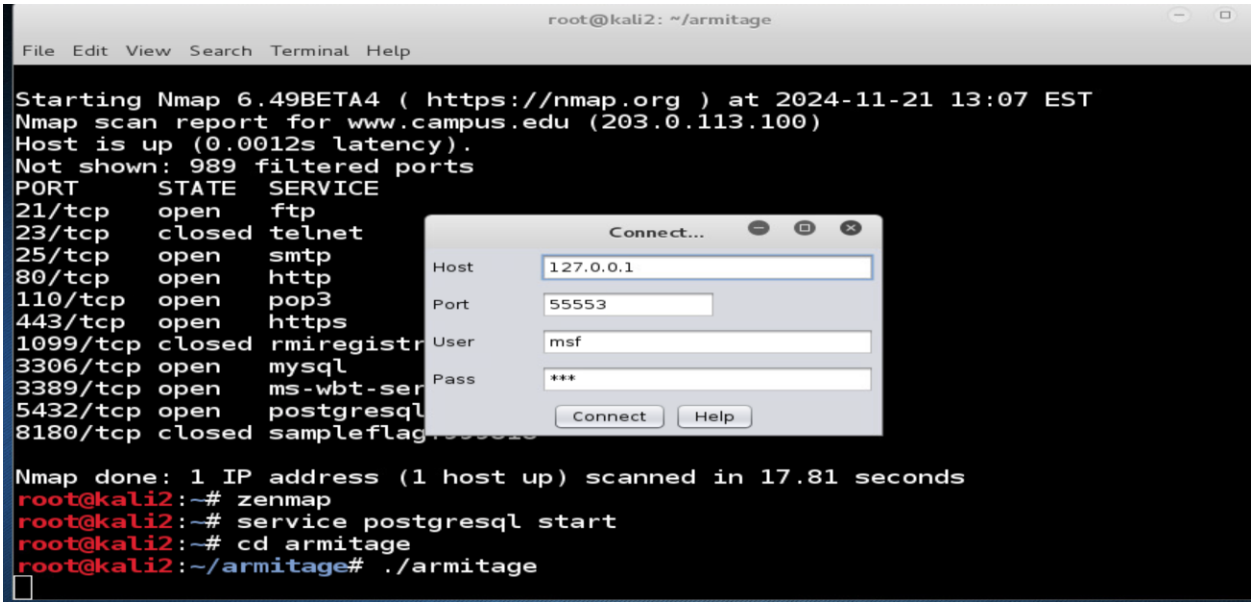


Typing the Command “zenmap ” to launch the intense scan for the target “203.0.113.100”.

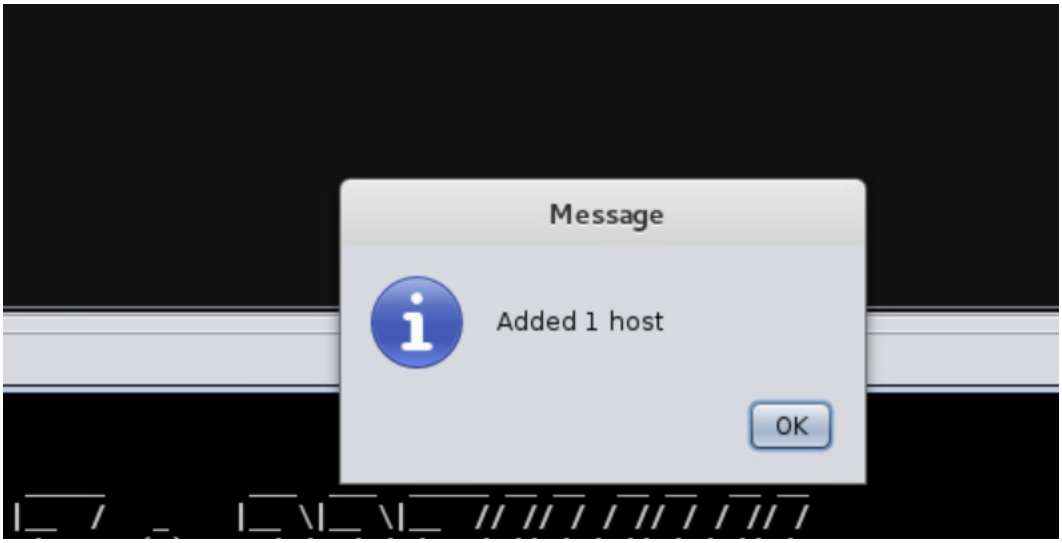


Screenshot shows the open ports and corresponding banner messages

To start the postgresql service and started the Armitage directory.

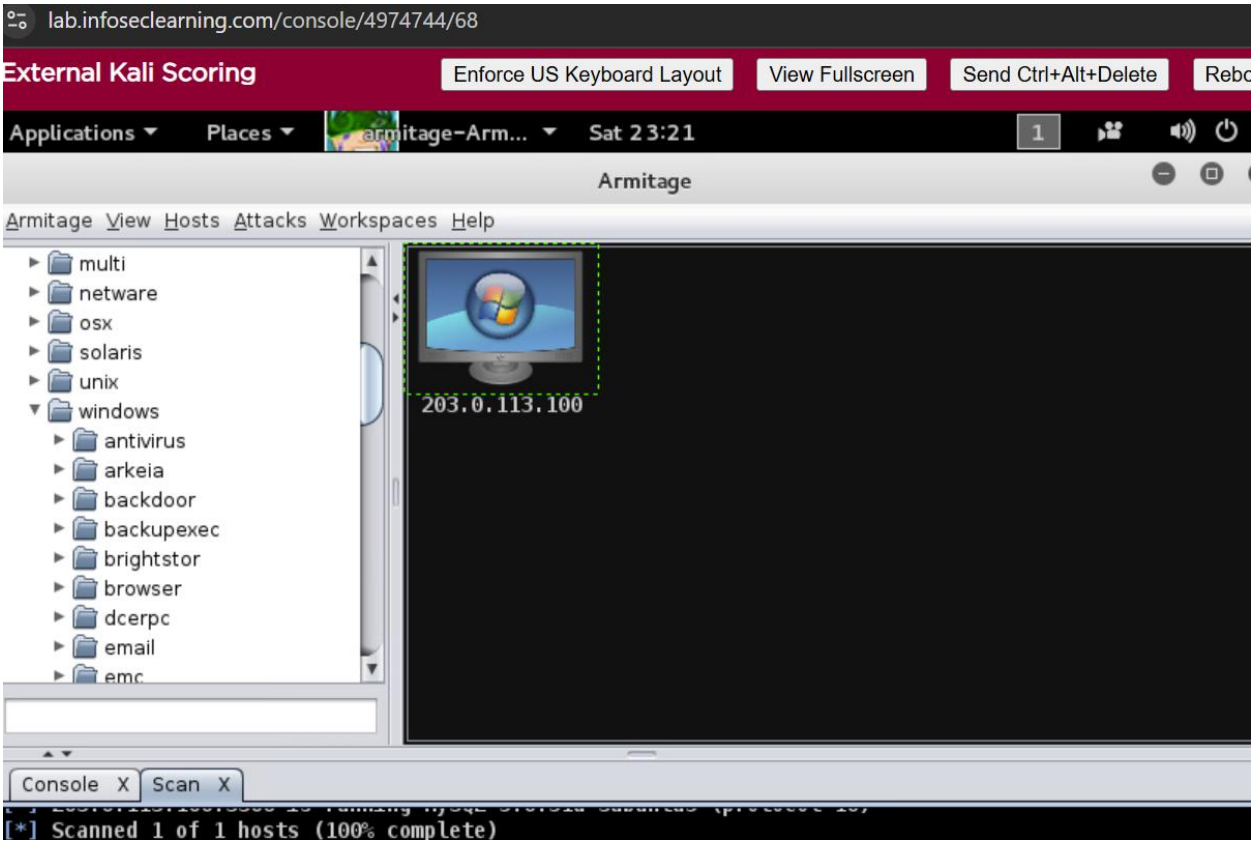


Screenshot shows that connecting to start the metasploit

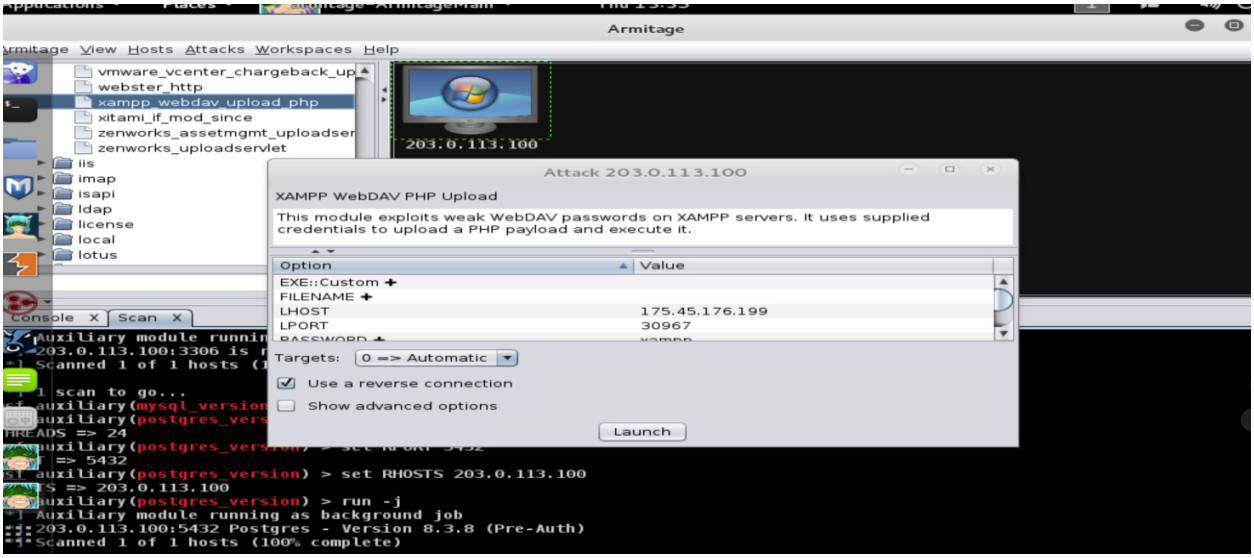


Screenshot shows that 1 host is added

Scanning the “203.0.113.100” host, it indicates that the remote system is running the windows operating system.

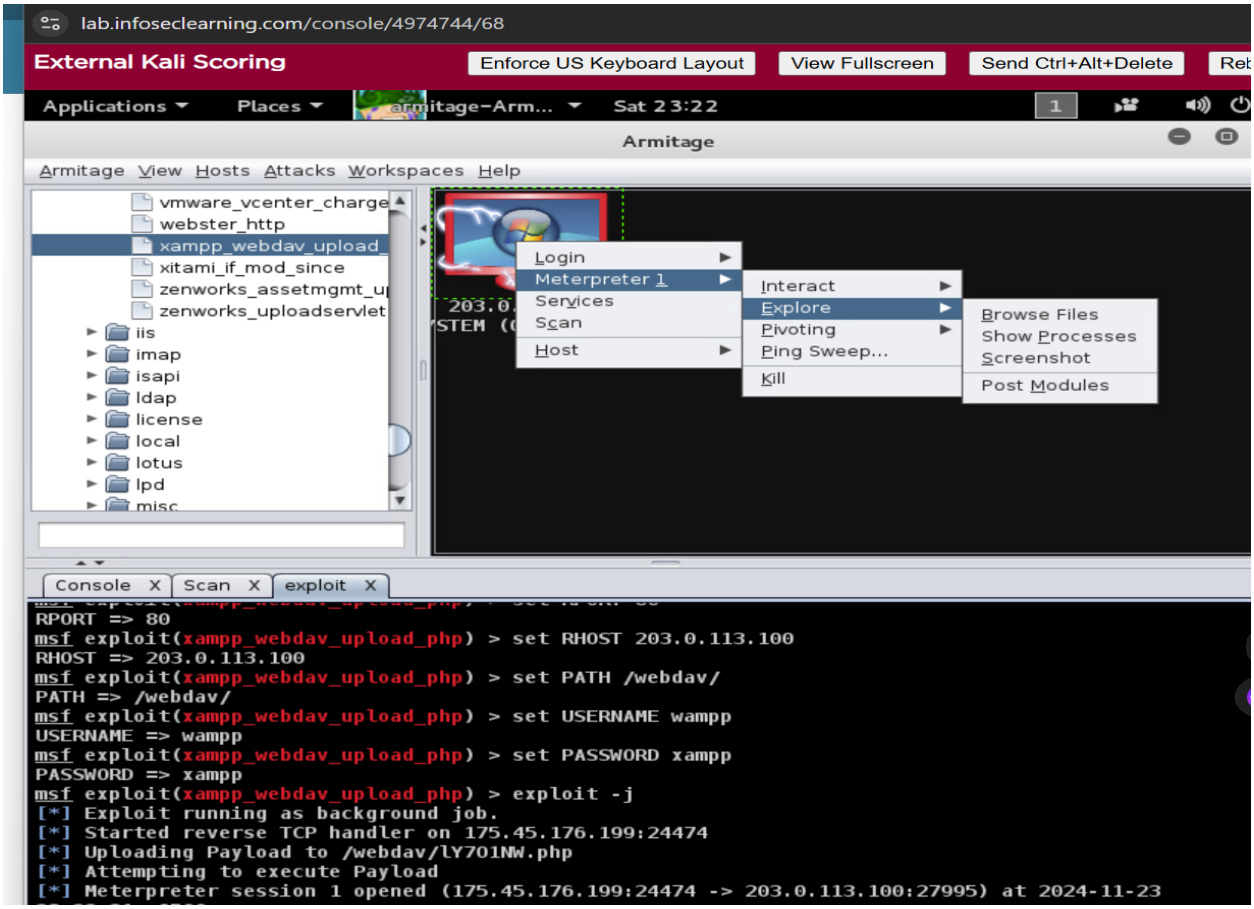


Expanding the exploit and also the windows in that expanding the host. Clicking host and in the http directory we find “xampp_webdev_upload_php opening it.

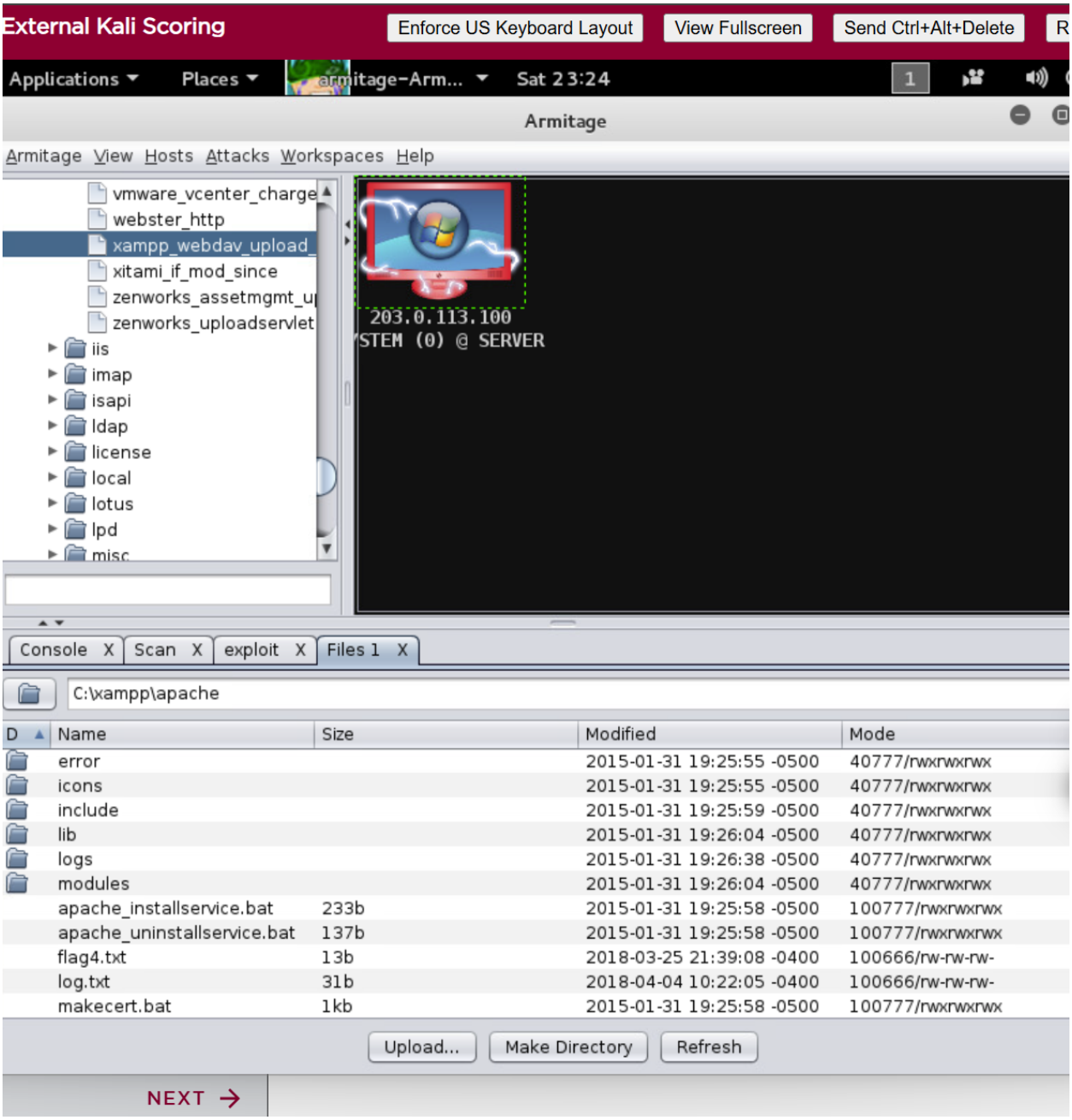


Screenshot shows that I found it and launched it to compromise the host

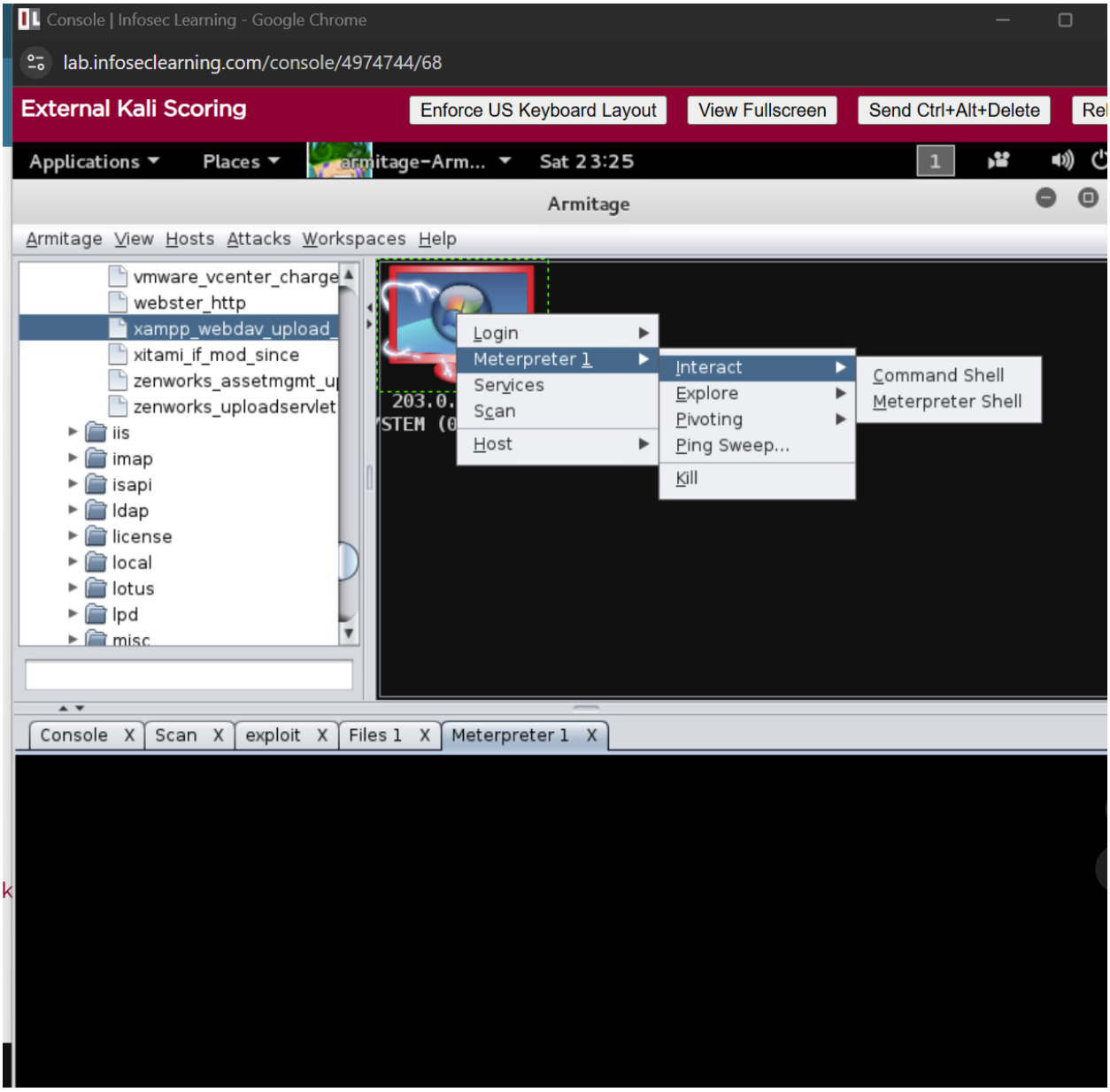
The victim will be compromised and selected the meterpreter 1, explore and browse files



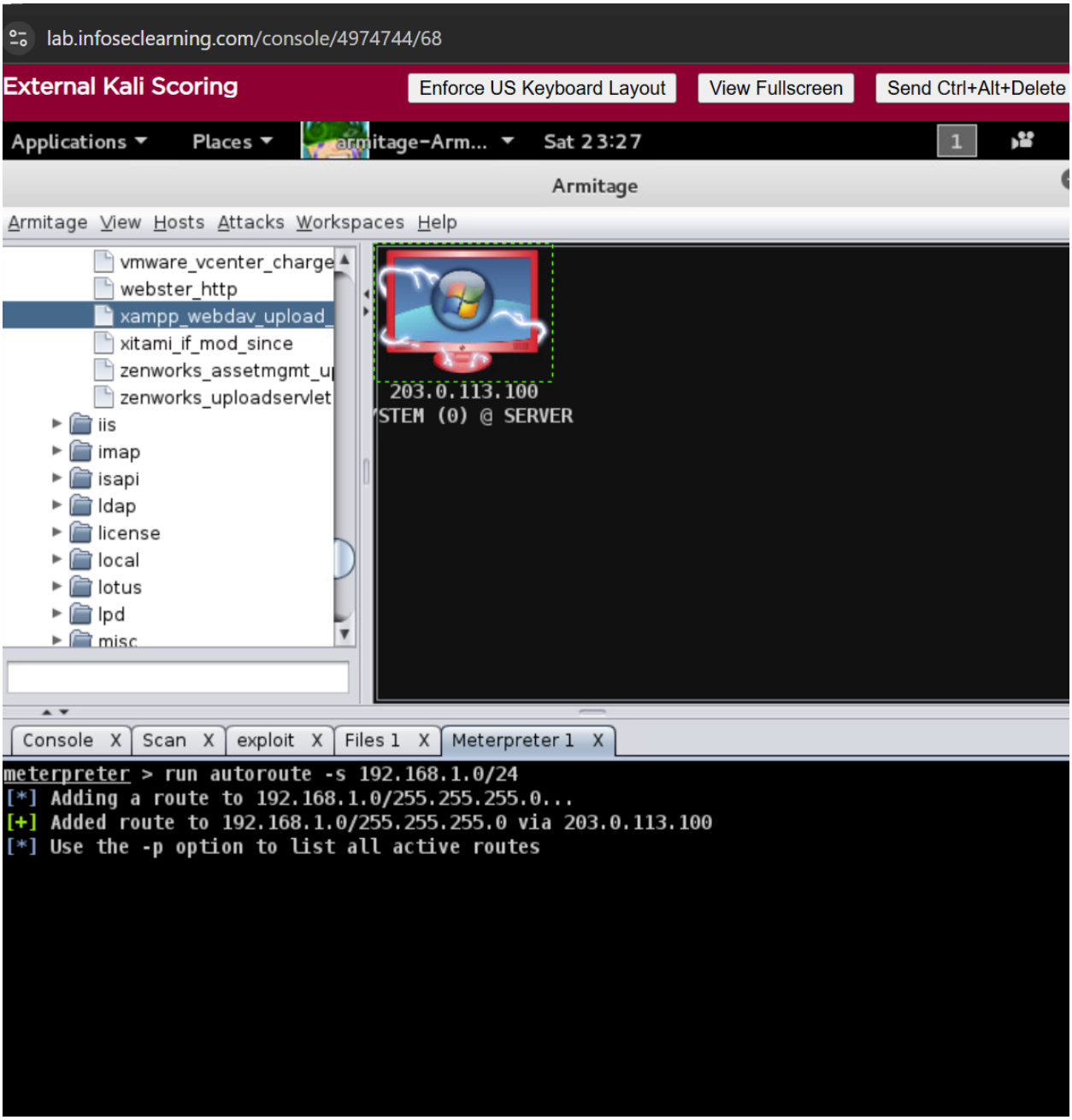
and open the apache folder to complete the below provided challenge tasks



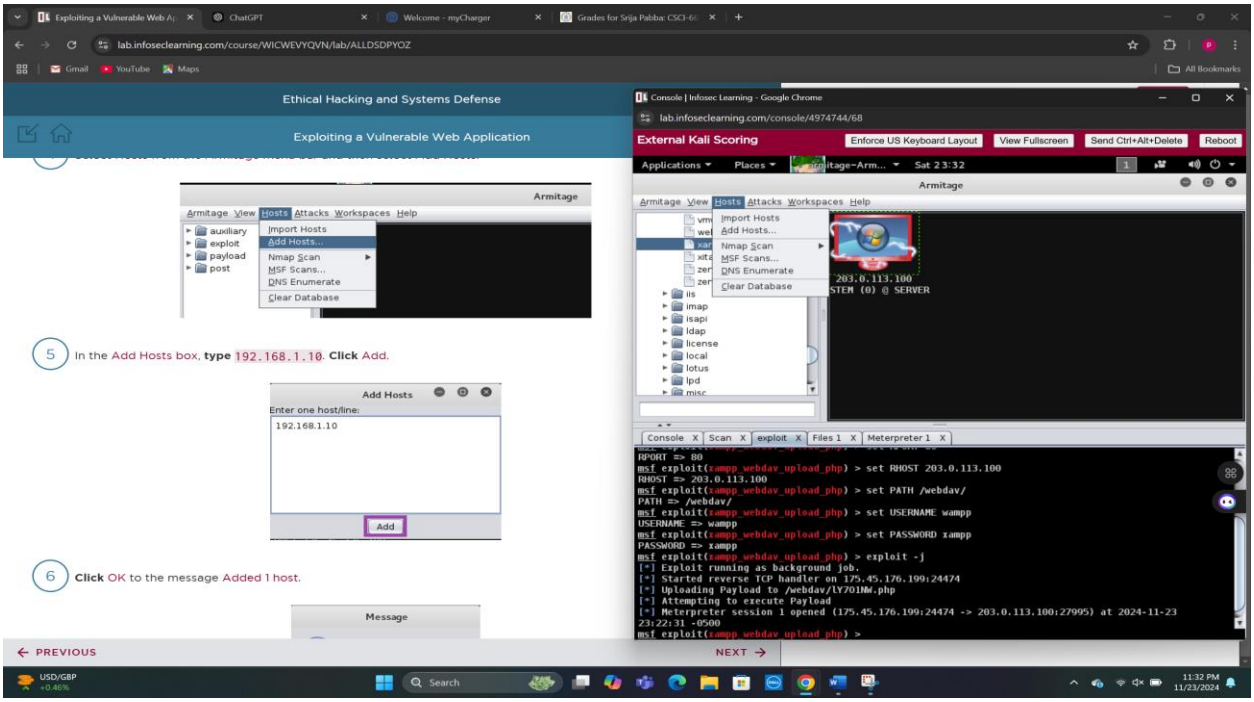
On right-clicking on the compromised host, selected the meterpreter 1, interact and meterpreter shell. Typed the following command to add a route to the victim's local area network(LAN)

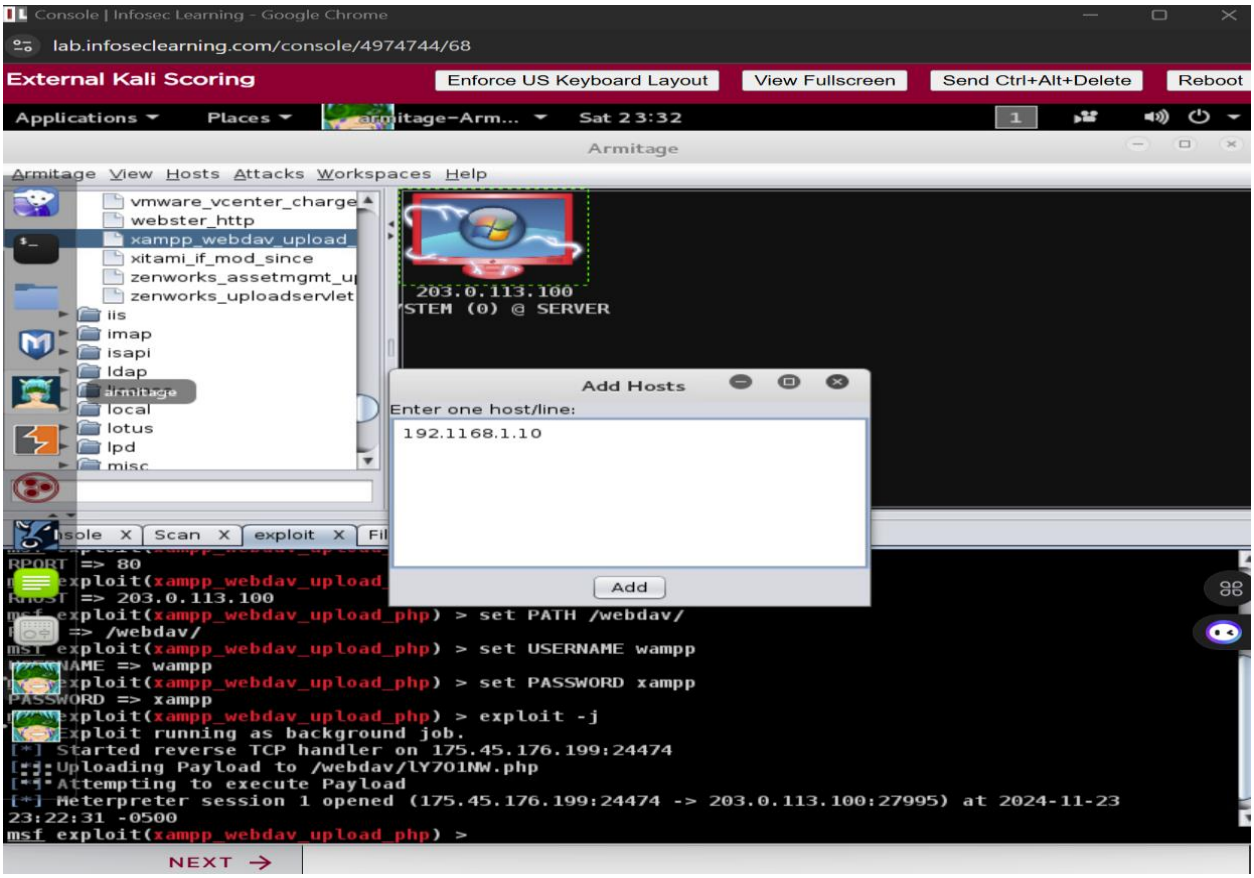


“run autoroute -s 192.168.1.0/24”



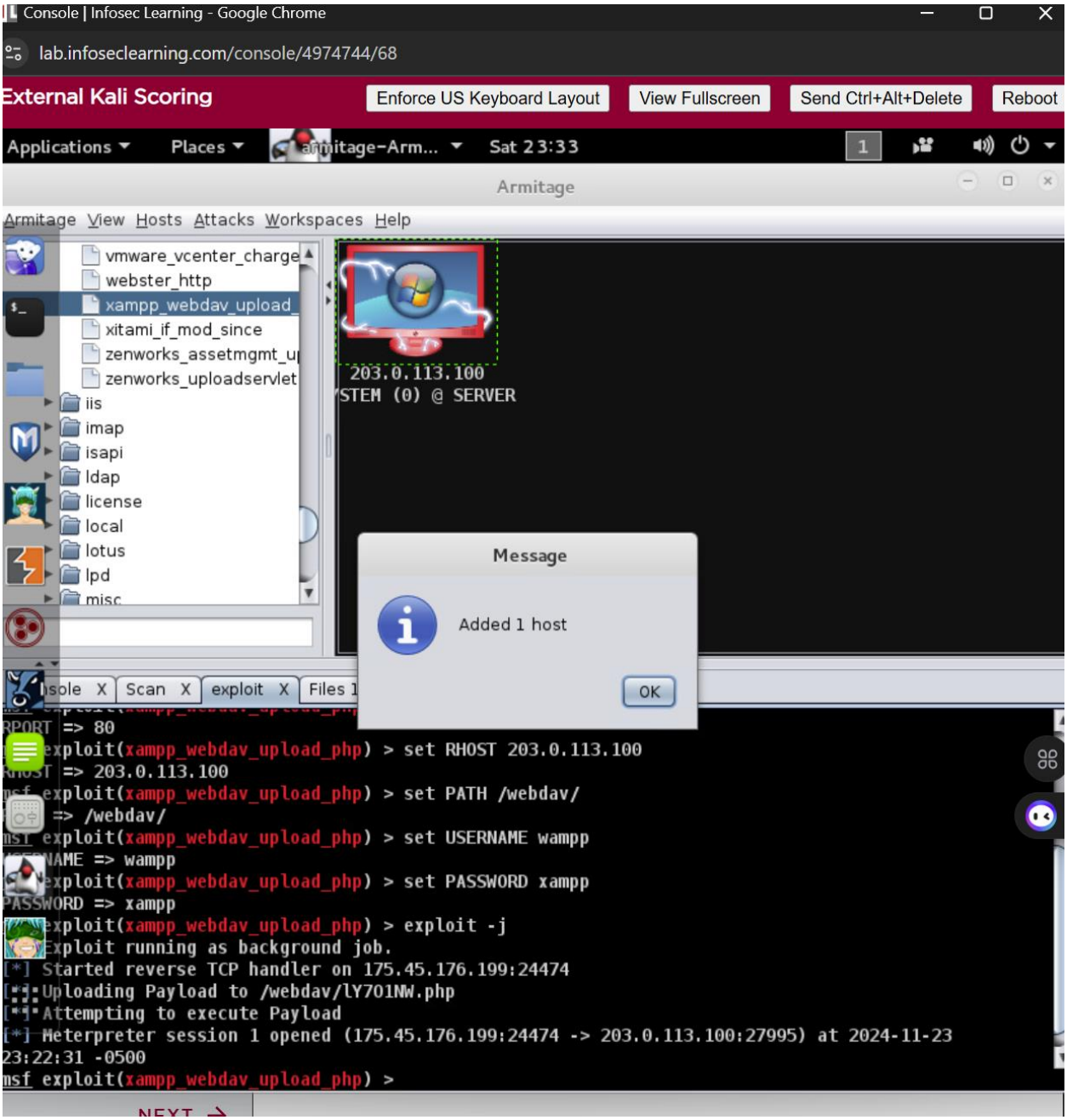
After Clicking the exploit tab and select add the hosts



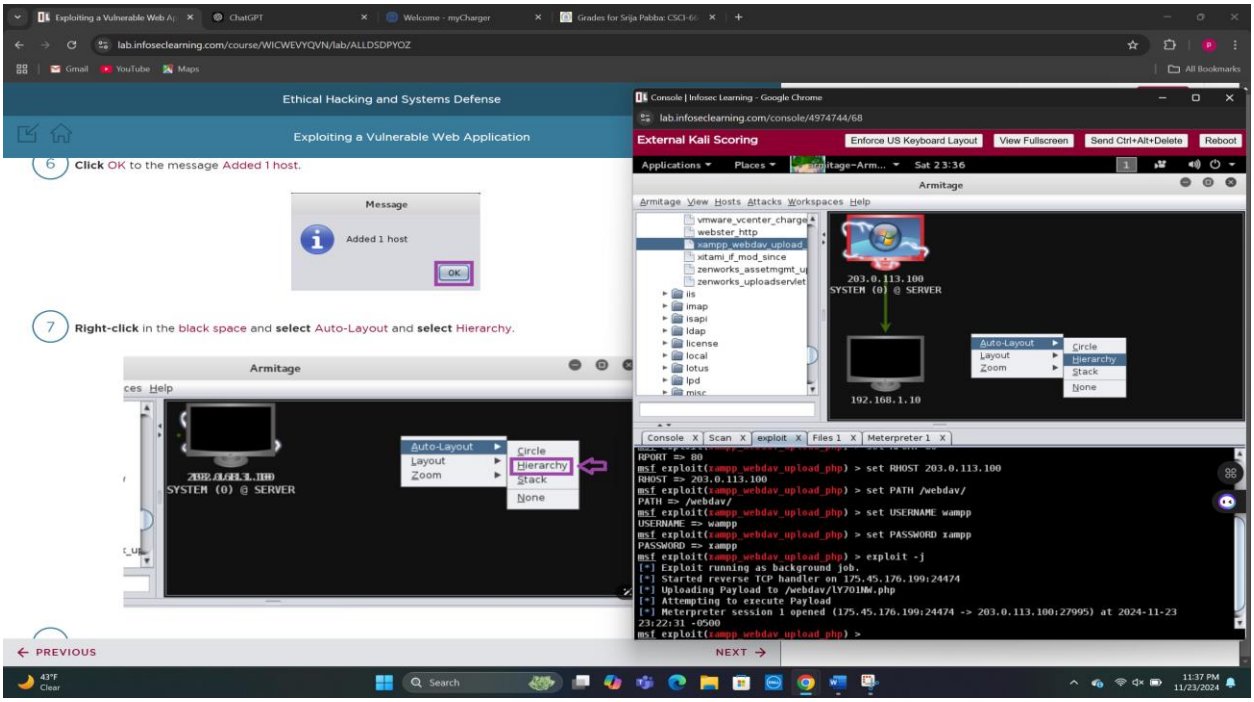


Screenshot shows that the host is added

Message showing that the host “192.168.1.10” is added

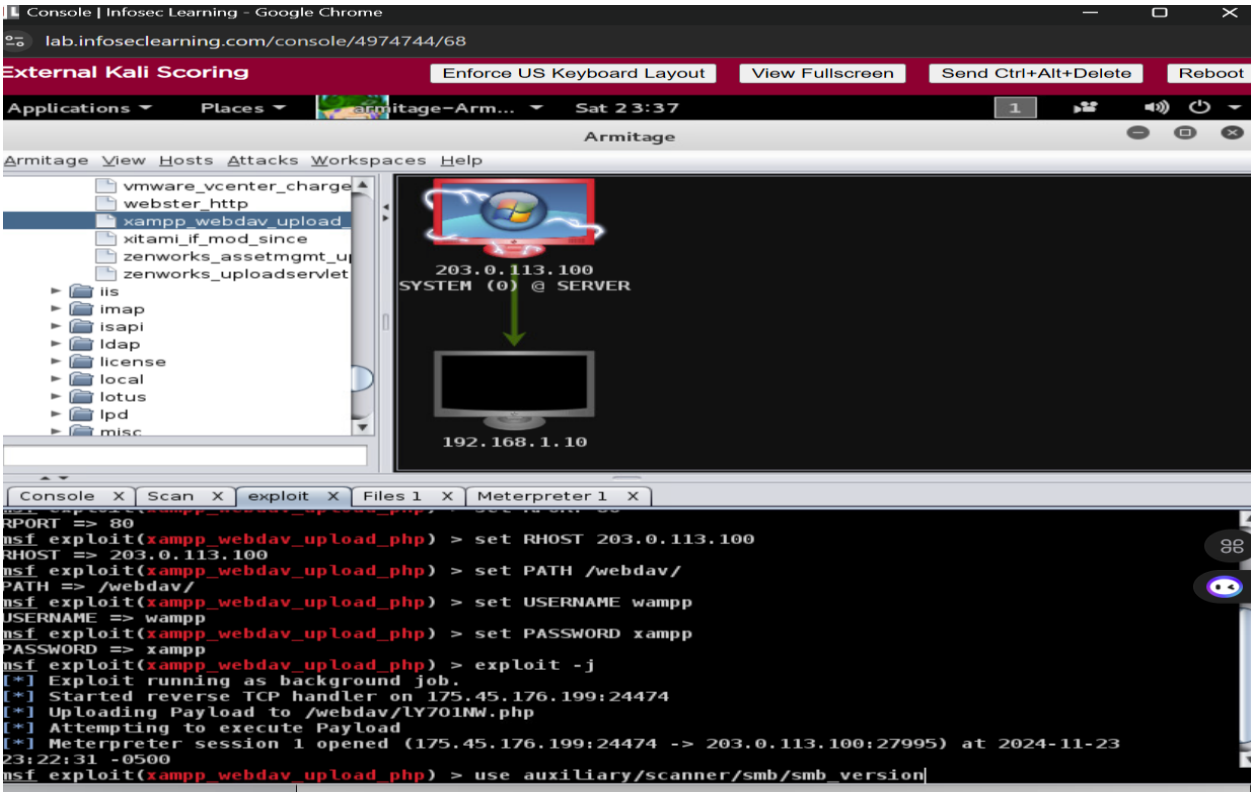


Clicking on the black space and selecting Auto-Layout and Hierarchy



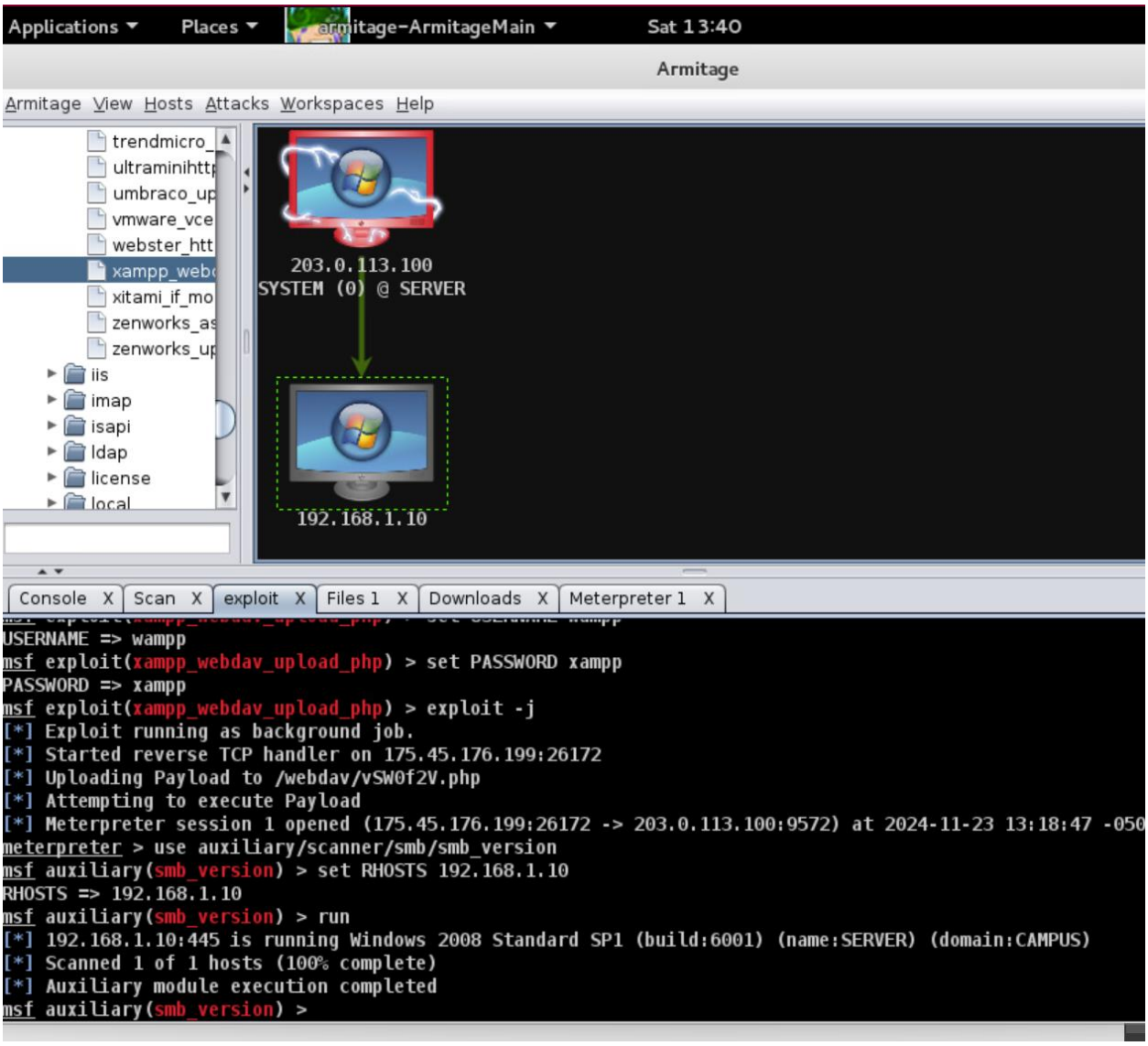
Screenshot shows that the host is appeared below the previous host

Using the command to go back to the msf prompt



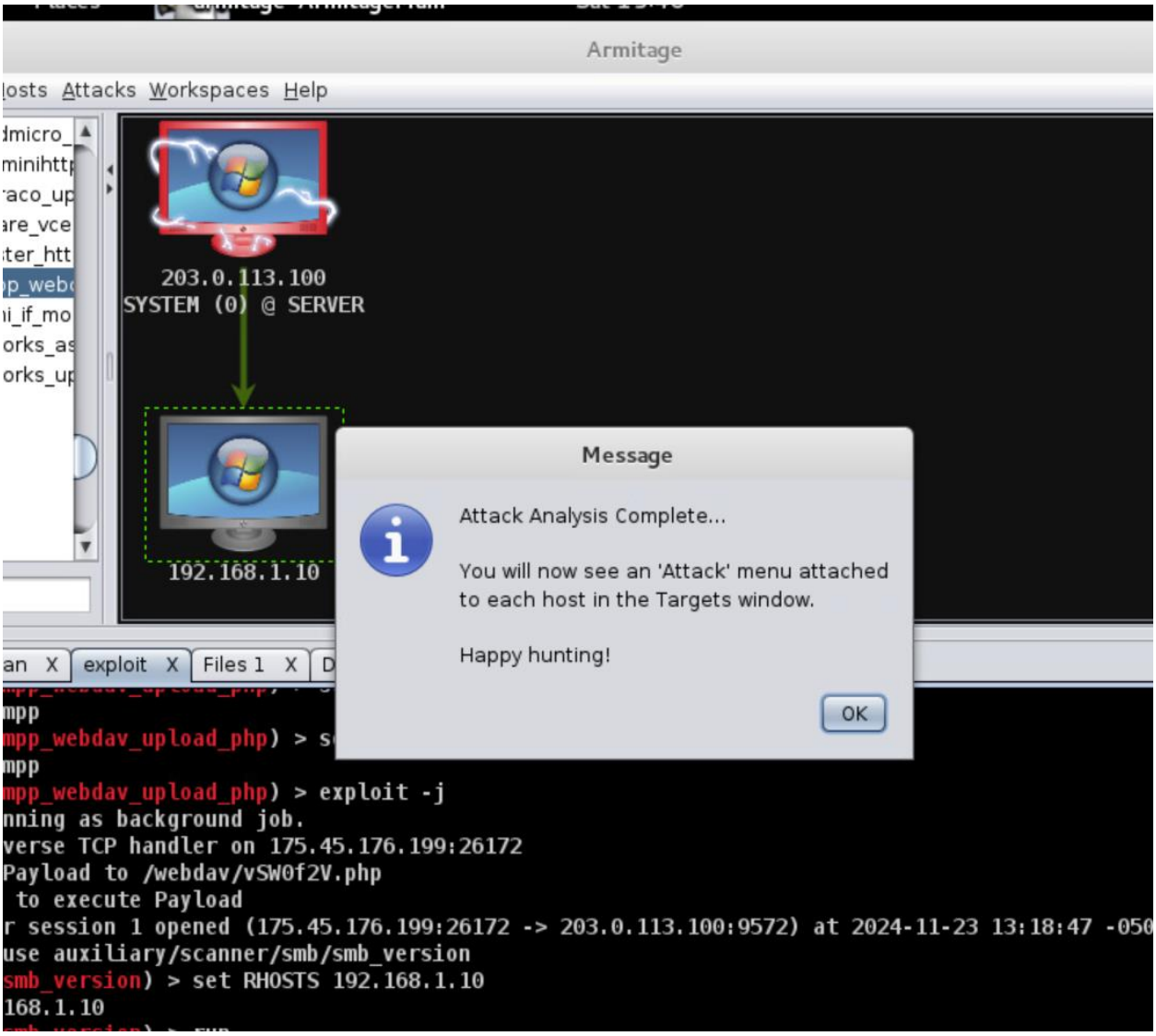
Setting the IP address of the remote host by the following command

“set RHOSTS 192.168.1.10”



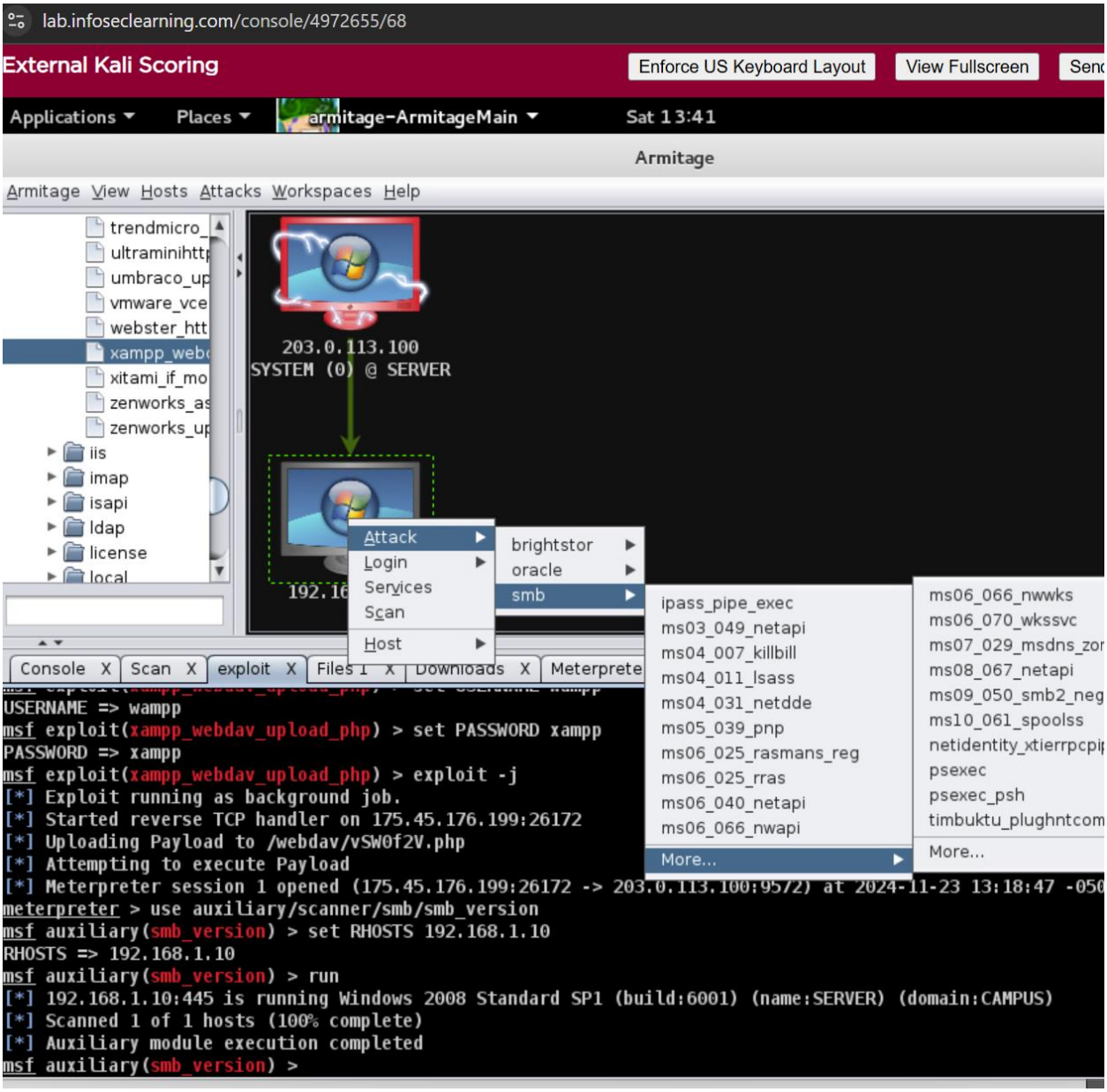
Screenshot showing that using “run” to identify the host as windows

Selecting the Exploit Rank as Poor and selecting OK to update minimum exploit rank



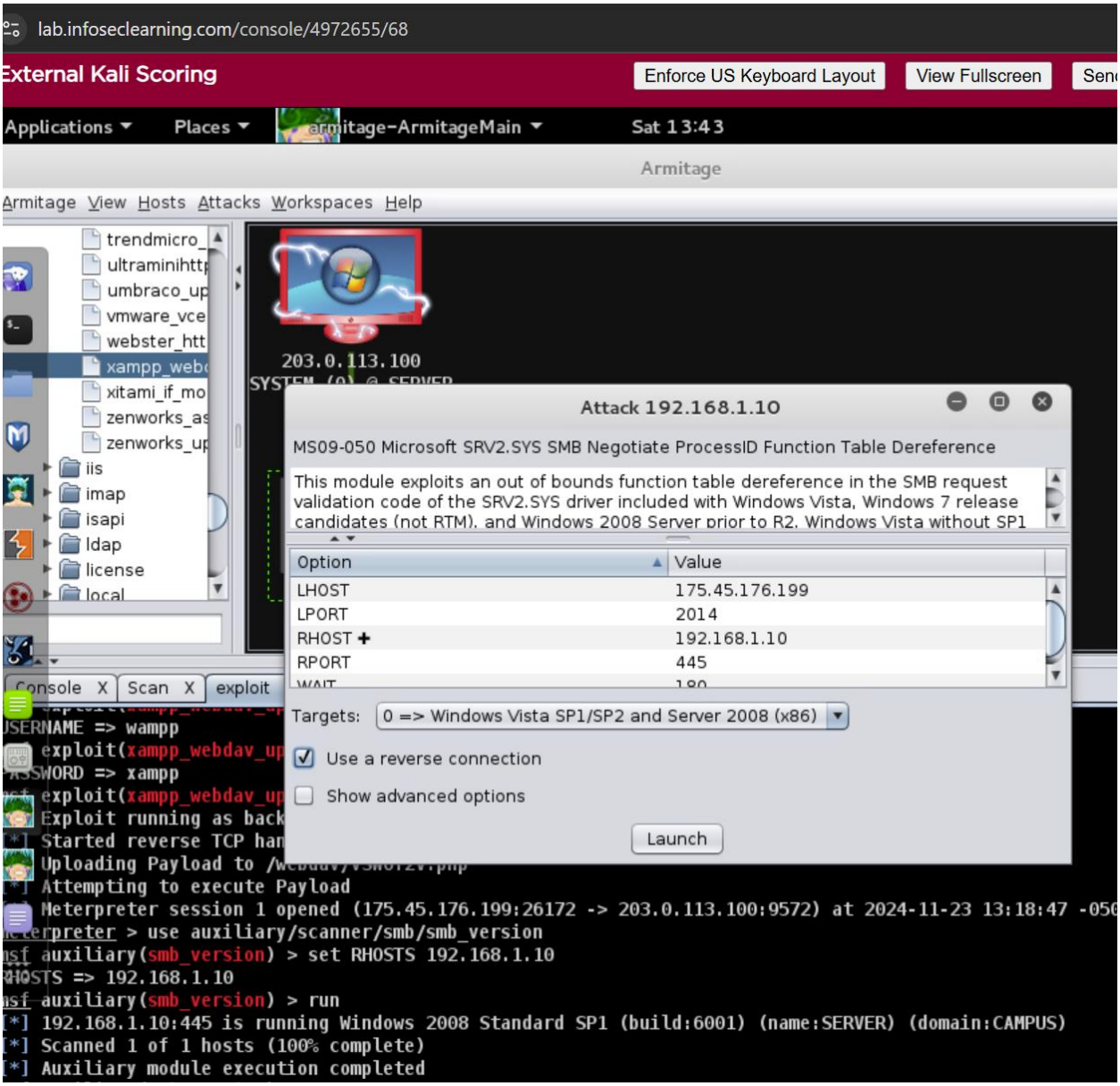
Screenshot showing that the Attack analysis is complete

Selecting the Attack and then smb and the more to select the below showing options

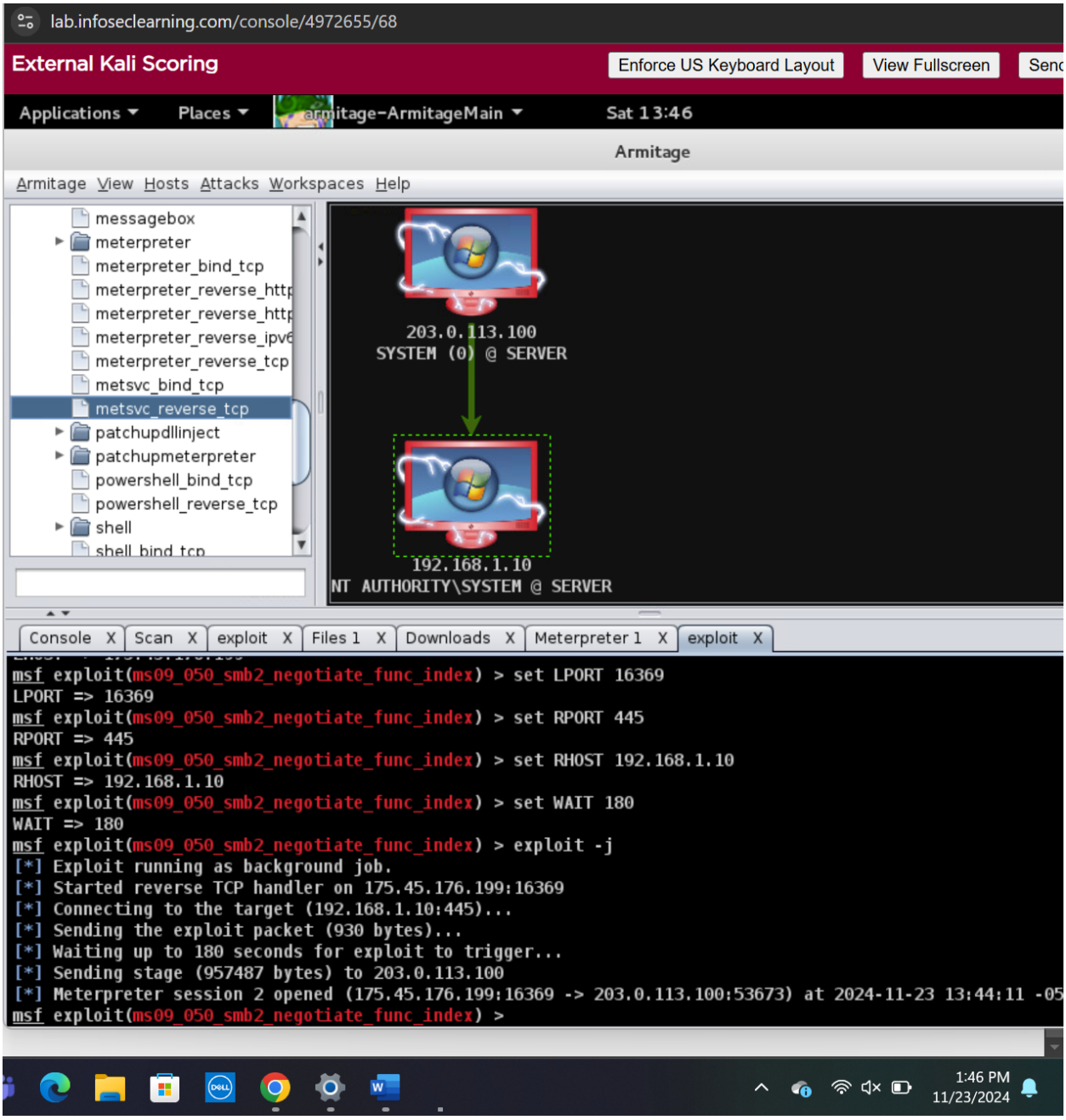


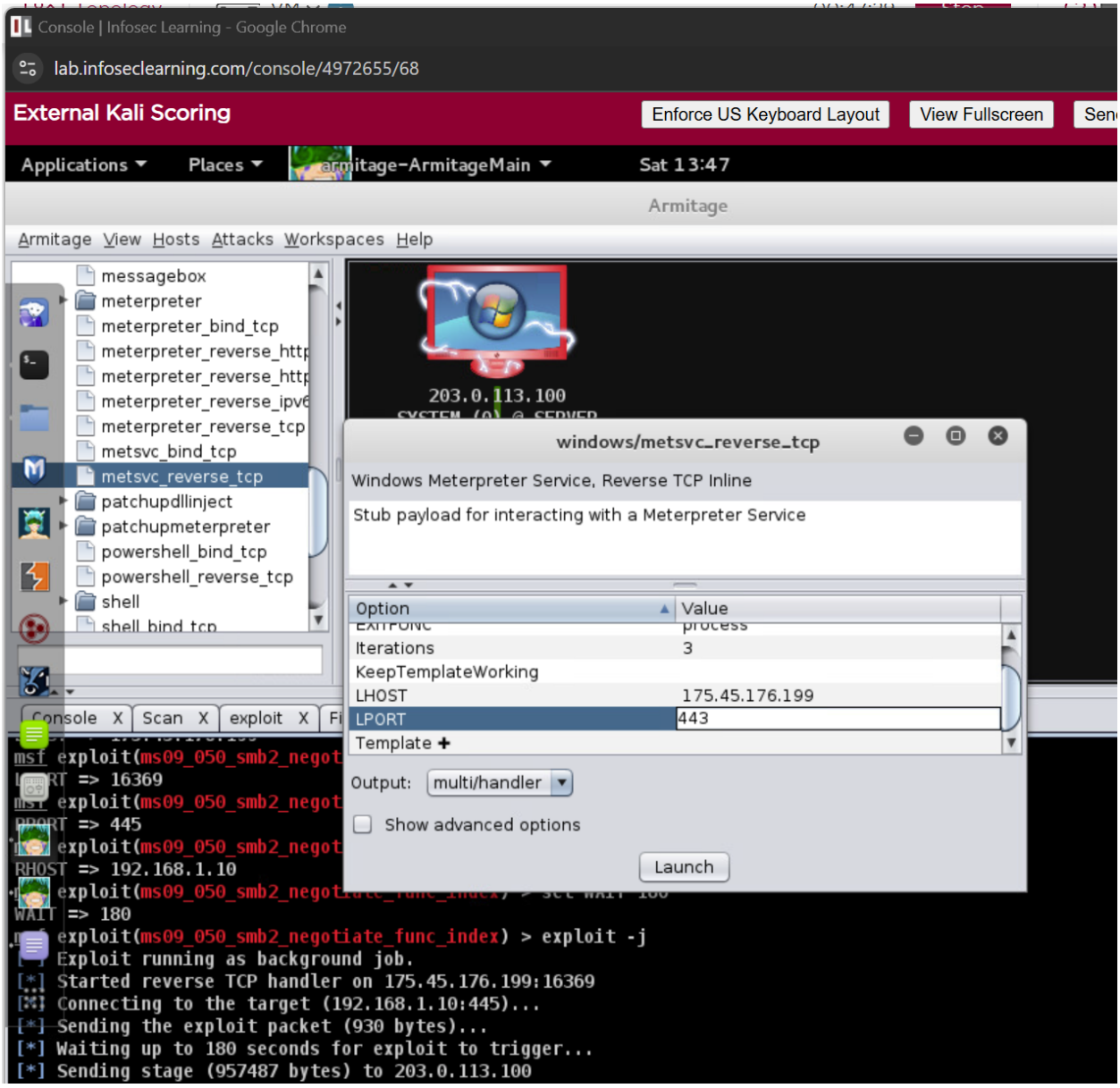
Screenshot showing that the "ms09_050_smb2_negotiate_func_index

Check the reverse connection and launch the attack.



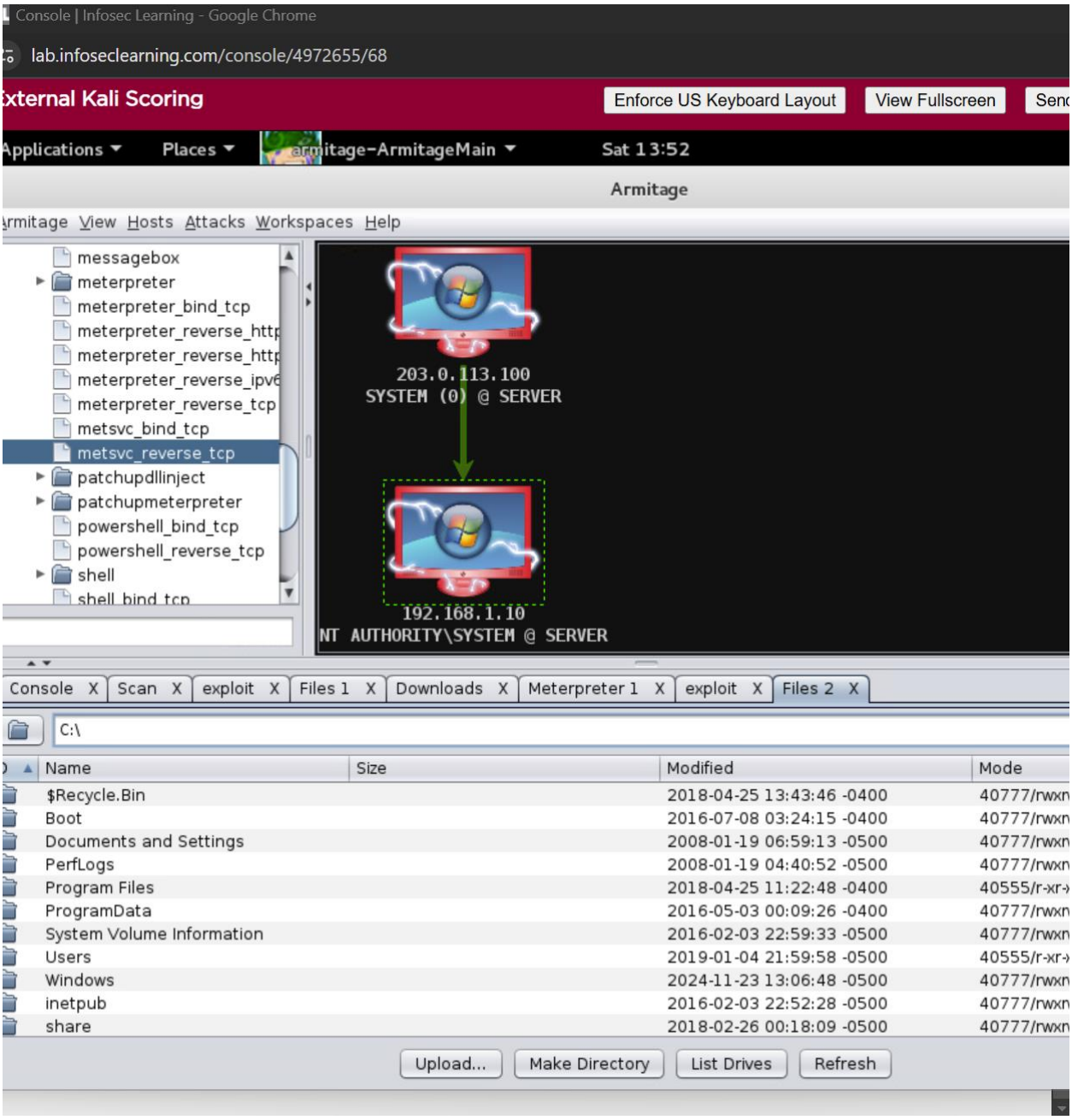
Now the 192.168.1.10 victim will also become compromised





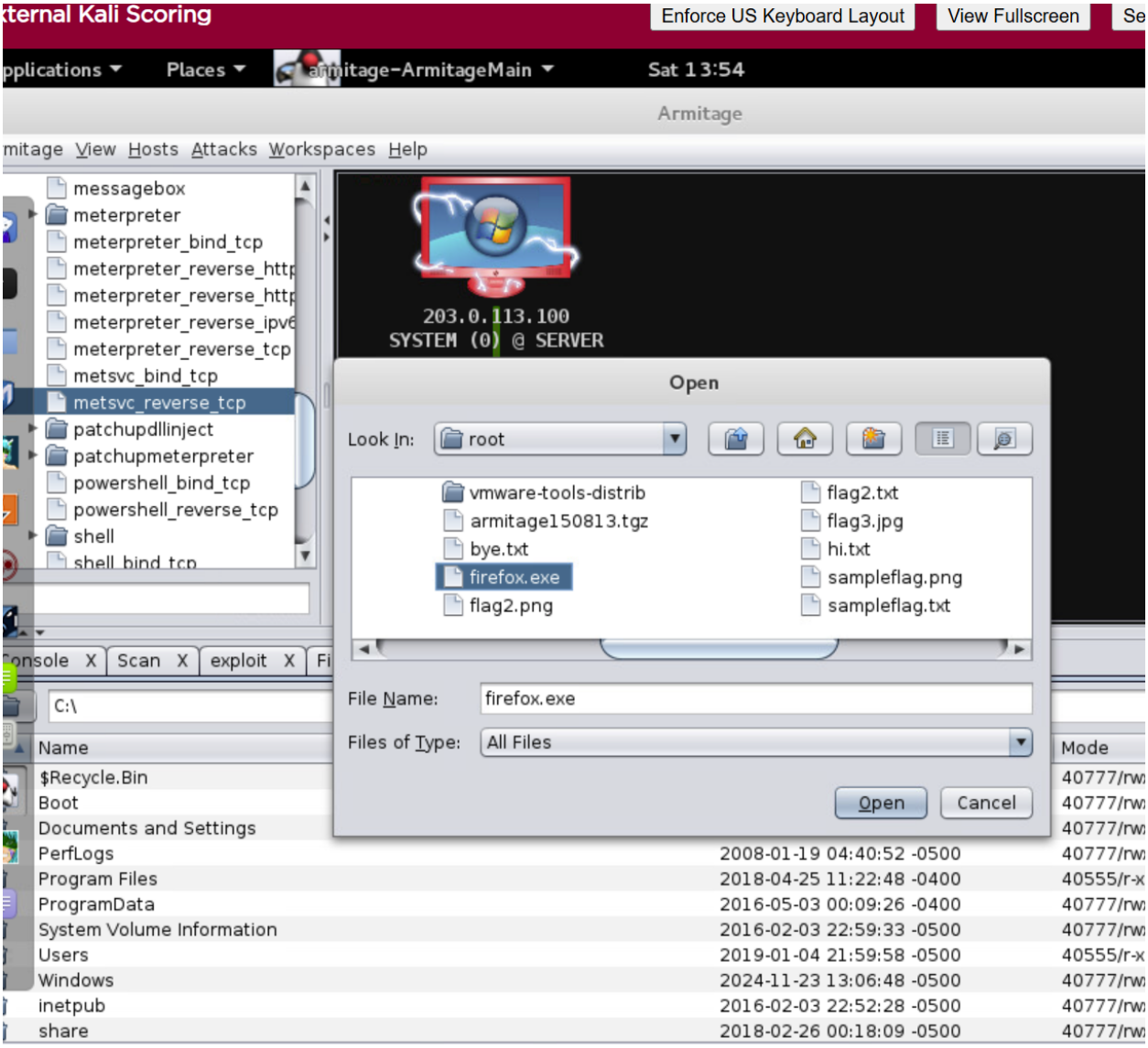
Screenshot shows that the LPORT value is chsnged to "443" and launching

Again opening "meterpreter_reverse_tcp" and select the output to "exe" and launch it. And change the file name to firefox.exe and save it

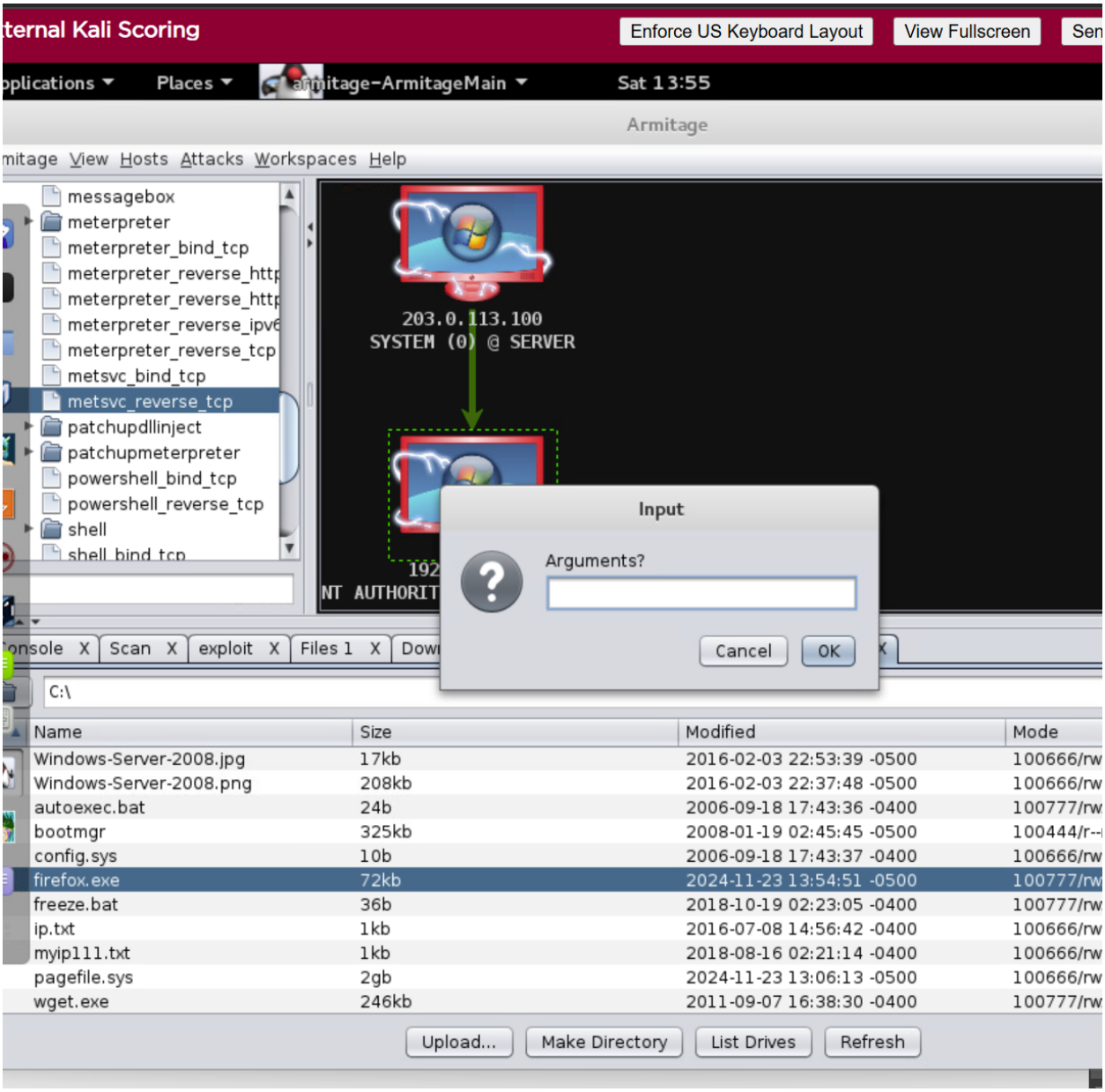


Screenshot showing the firefox.exe file is uploading

Open the firefox.exe and execute the file

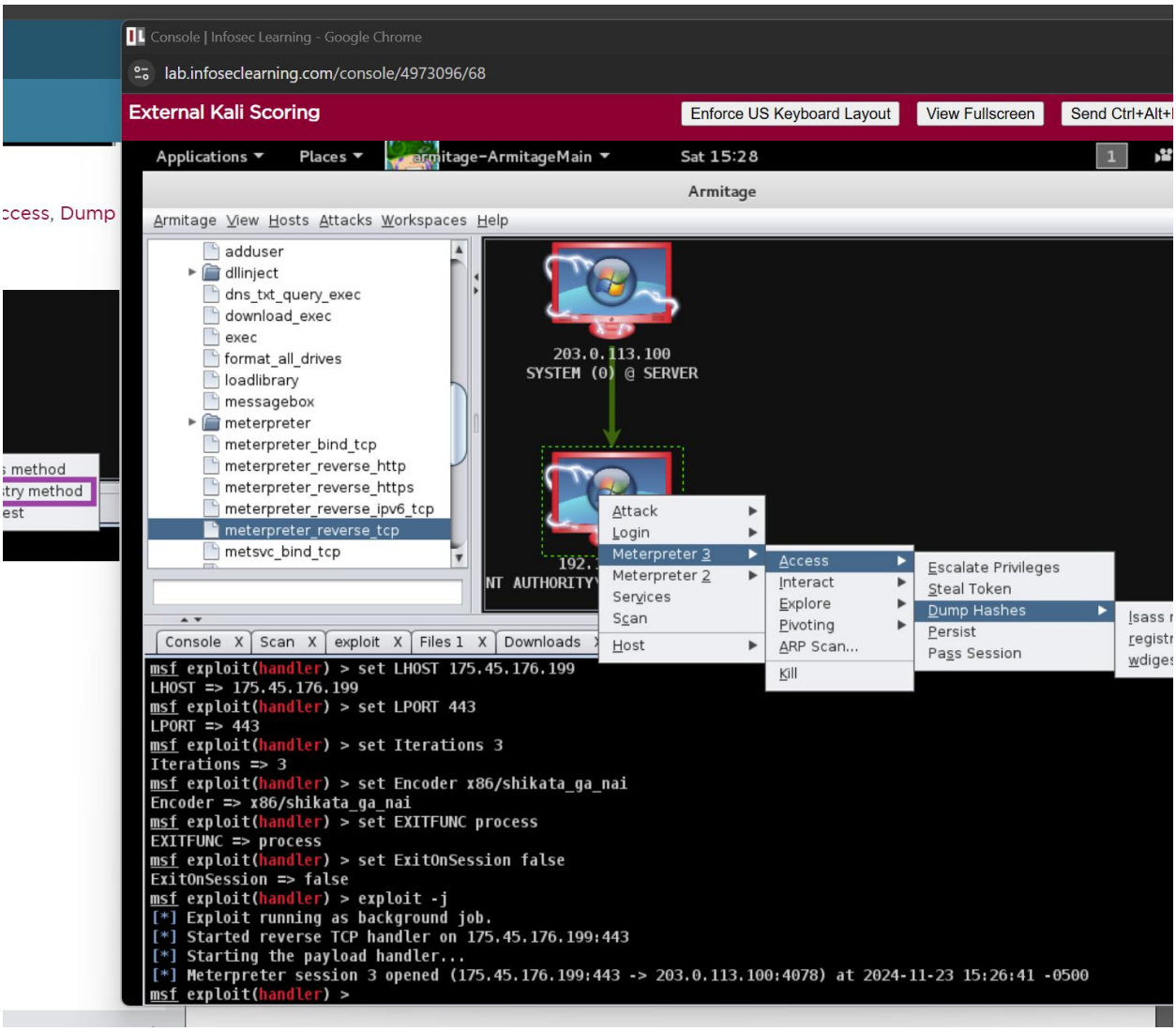


Screenshot showing that file is uploaded

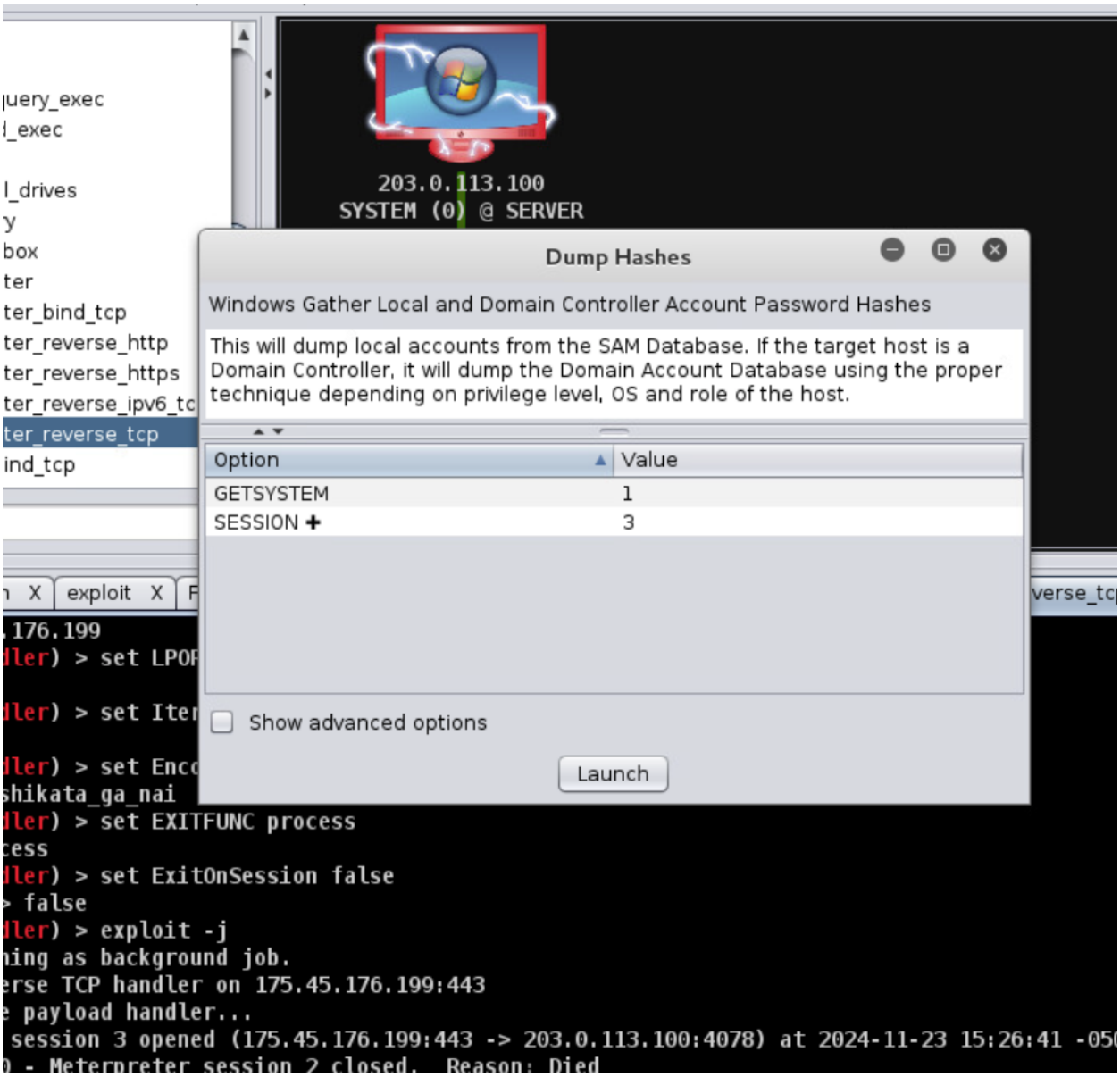


Screenshot showing that the file is executed and process created

Meterpreter session 3 opened and after that clicking on the compromised victim and selecting meterpreter 3, Access, Dump hashes and registry method

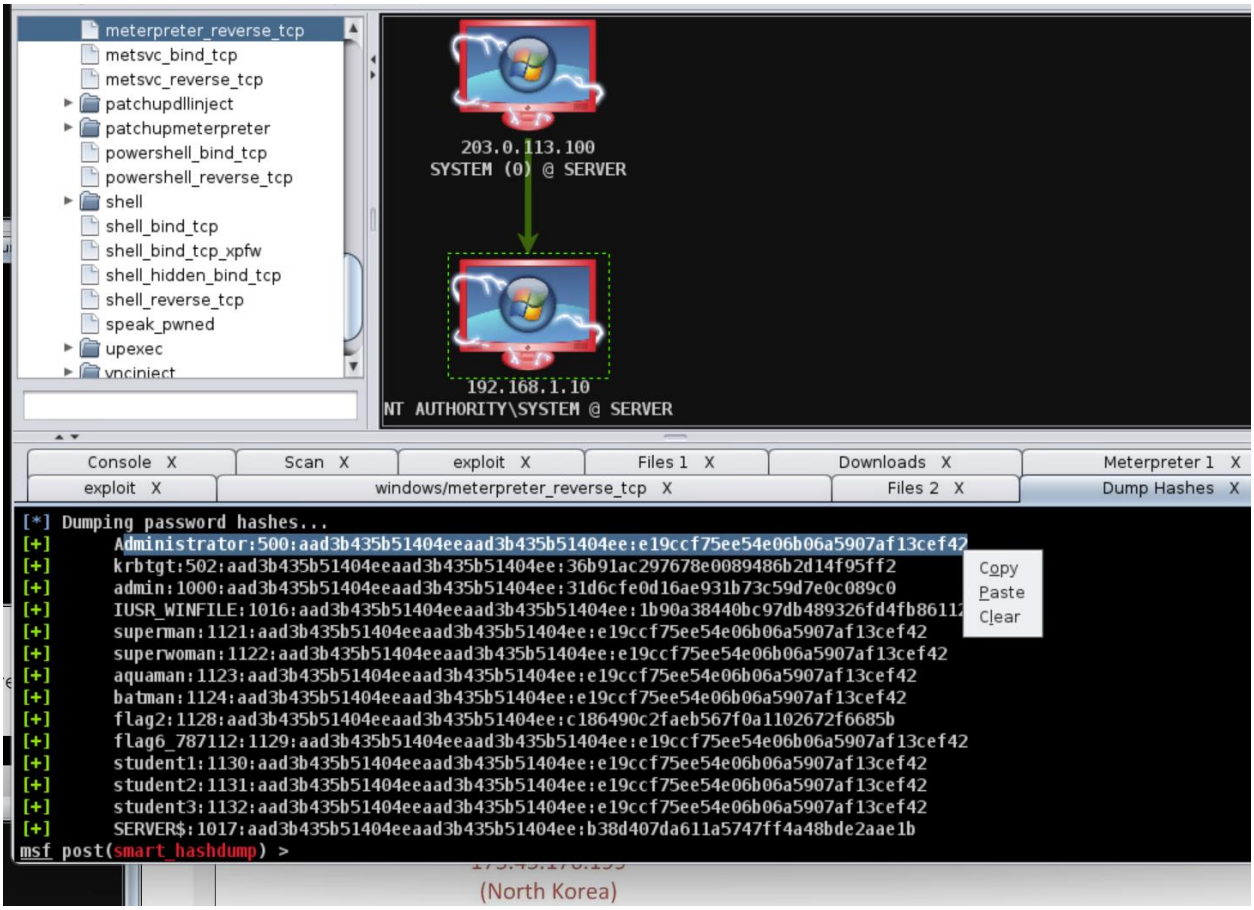


Screenshot shows that the registry is created

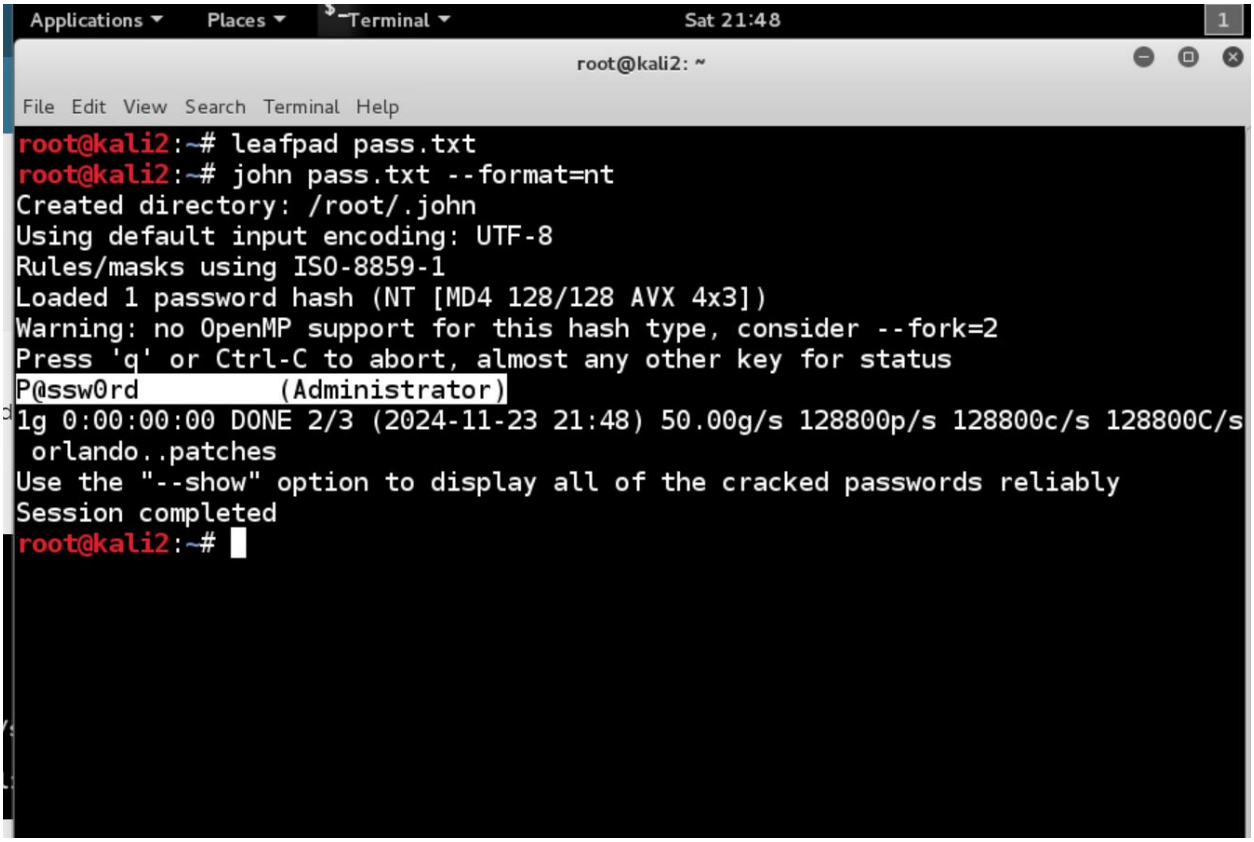


Screenshot showing that the Dump hashes are launched

Highlighted the Administrator account and the two hashes and copied



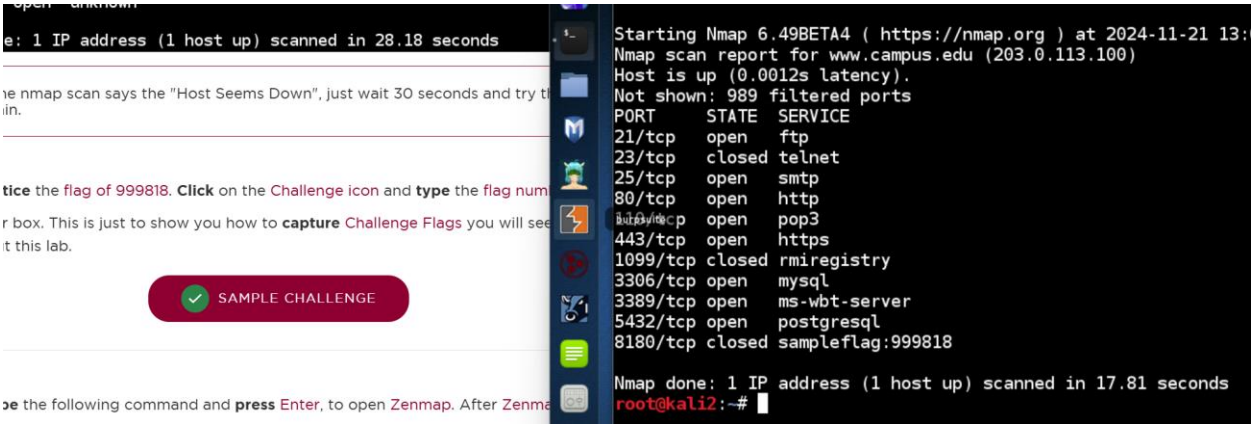
Screenshot showing that the copied text is pasted in the leafpad



Screenshot showing that the text file is created

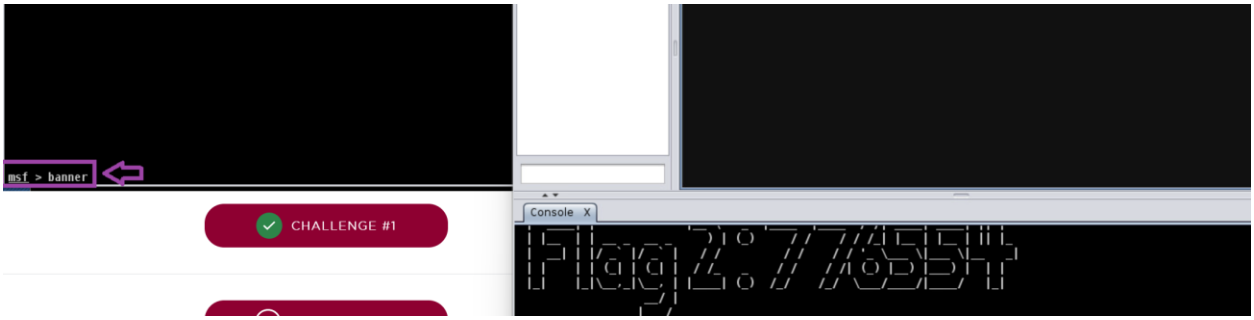
Supporting Evidence

These are the challenge tasks I got while doing the lab

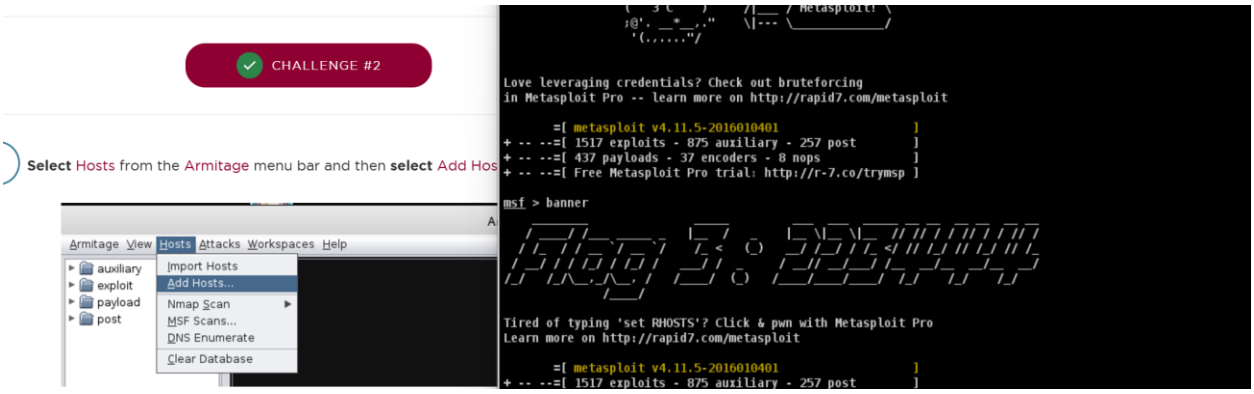


Screenshot shows that the sample challenge found in the postgresql

After launching the Metasploit, The banner command gives the flag 2



The same way to complete the challenge 3, Typed the banner till it shows the Flag 3

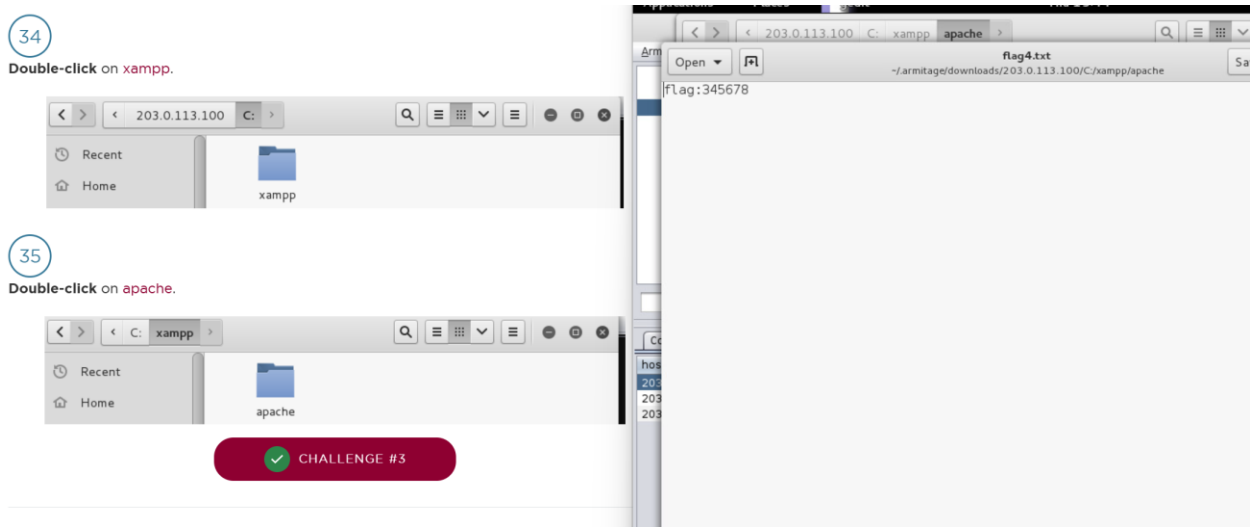


Screenshot shows that the Flag 3 is displayed after typing the "banner" command

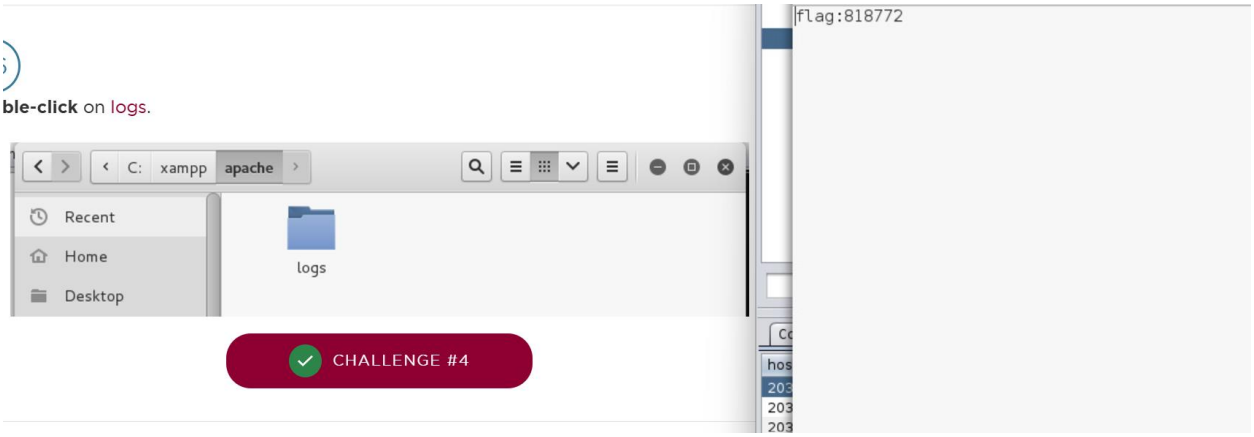
Downloaded all the tasks from the apache folder, Below the modules folder found the flag4.txt to downaload.

The same way downloaded the flag5.txt from the logs folder and access.log file

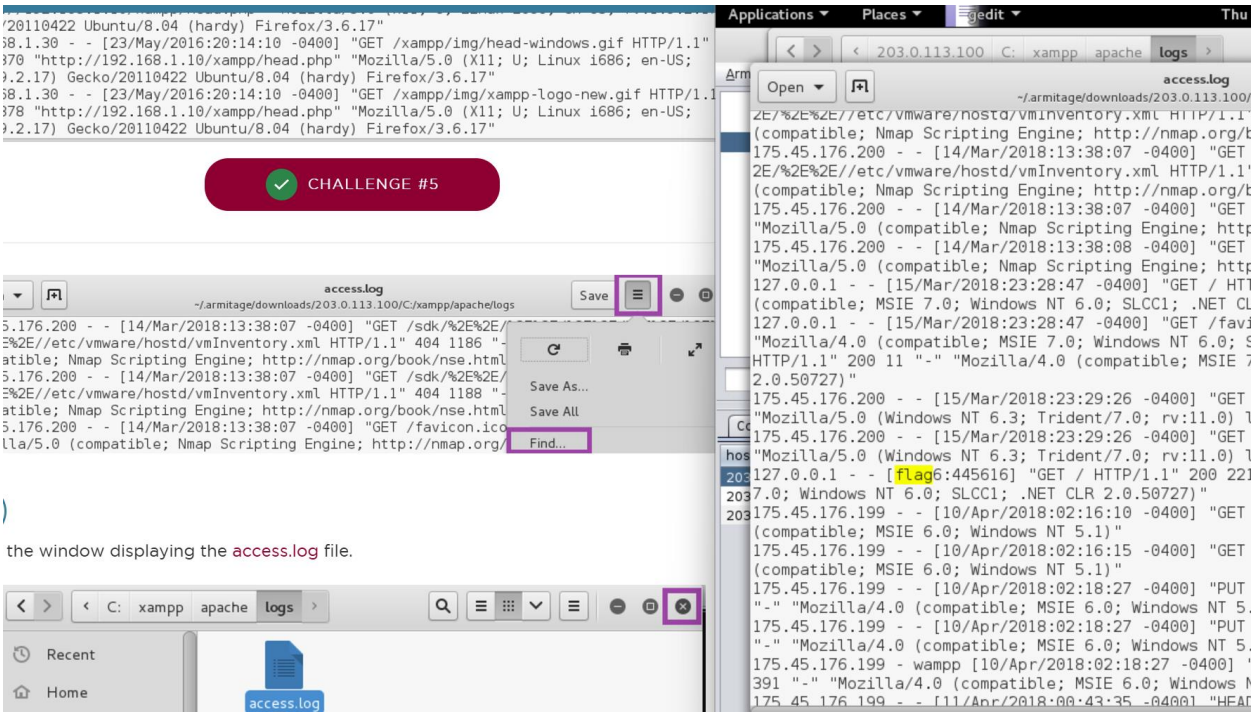
These all files wre found in the downloads of view section of armitage menu bar



Screenshot showing that the challenge 3 is text found in apache



Screenshot showing that the challenge 4 is text found in logs



Screenshot showing that the challenge 5 is text found in access.log file

Conclusion & Wrap-Up

Summary with:

Observations

In this lab, I learned how to exploit a vulnerable web application on a WAN using a Kali attack machine. I used tools like **nmap**, **Zenmap**, **Metasploit**, and **Armitage** to find and exploit weaknesses in a XAMPP WebDAV service. I then pivoted to the internal network to exploit a Windows server with an SMB vulnerability. The lab showed how external vulnerabilities can lead to serious internal breaches if security is weak.

Identified risks

I found that using **default WebDAV credentials** made it easy to compromise the web server. The Windows server had an **unpatched SMB vulnerability**, which allowed remote exploitation. The lack of **network segmentation** also made it possible to move from the web server to internal systems. These risks highlighted the dangers of poor password management, outdated software, and weak internal protections.

Suggested recommendations

To fix these issues, I recommend replacing default passwords with strong ones, keeping systems updated through regular patching, and using **network segmentation** to isolate external systems from internal ones. Adding **intrusion detection systems (IDS)** and improving **logging and monitoring** would help detect and respond to threats more quickly.

Successes & Failures

I successfully exploited the XAMPP WebDAV service and the SMB vulnerability on the Windows server, showing how attackers can use these weaknesses to compromise systems. However, the lab also showed failures like relying on default credentials, outdated software, and poor internal defenses, which made the attacks possible.

Challenges

I had trouble setting up tools like **Metasploit** and configuring the pivot route for internal exploitation. Understanding **nmap** results and the network setup was also challenging and required more practice. And it was difficulty in compromise the windows

Detailed Risks

Default Credentials:
Default WebDAV credentials on the XAMPP server provided an easy entry point for attackers. These credentials are widely known and commonly exploited, emphasizing the need for secure configurations during setup.

Unencrypted Communications:
WebDAV and SMB services often use plaintext or outdated encryption, allowing attackers to intercept credentials or sensitive data using tools like Wireshark. This lack of encryption increases risks like credential harvesting.

Open and Exposed Ports:
Ports like 80 (WebDAV) and those for SMB were exploited in the lab. Unrestricted open ports expand the attack surface, making it easier for attackers to identify and exploit services.

Unpatched Vulnerabilities:
The SMB vulnerability (MS09-50) was exploited due to outdated software. This highlights the critical need for regular patch management to protect against known exploits.

Pivoting from the Web Server:
The ability to move from the compromised web server to internal systems revealed a lack of network segmentation. Without proper isolation, attackers can access sensitive internal resources.

Why These Risks Matter:
These risks reflect systemic weaknesses that attackers exploit to breach systems and move deeper into networks. Addressing them through secure configurations, regular updates, and robust access controls is essential to protect sensitive data and infrastructure.

Table format outlining the risk priority

Risk	Priority	Description	Remediation
Default Credentials	High	Default WebDAV credentials allow easy unauthorized access to the web server.	Replace default credentials with strong, unique passwords during system setup.
Unpatched Vulnerabilities	High	SMB vulnerability (MS09-50) enables remote code execution due to outdated software.	Implement a robust patch management policy to ensure systems are regularly updated.

Pivoting from Web Server	High	Lack of network segmentation allows attackers to move to internal systems after compromising the web server.	Enforce network segmentation to isolate external-facing systems from internal networks.
Unencrypted Communications	Medium	WebDAV and SMB services use plaintext or weak encryption, enabling credential theft and data interception.	Enable secure protocols like HTTPS and SMB signing, and ensure encryption for all communications.
Open and Exposed Ports	Medium	Open ports like 80 and SMB ports increase the attack surface for unauthorized access.	Restrict unnecessary open ports and implement a firewall with access controls.
Inadequate Logging and Alerts	Low	No alerts for failed login attempts or unusual activity hindered early detection.	Implement robust logging mechanisms and configure alerts for abnormal system behavior.
Weak Network Access Controls	Low	Internal resources were accessible without strict restrictions.	Apply role-based access controls and restrict internal communications to authorized devices only.