CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment-5

Exploiting a Vulnerable Web Application

Student Info:

Name : Akhila Parankusham

Student ID: 00810899

Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

In this lab, an external Kali Linux system is used to launch an attack on a network web application. Nmap scans the network for vulnerable open ports related to Apache httpd. Armitage, a Metasploit graphical interface, is used to exploit the XAMPP WebDAV/2 vulnerability in a Windows web server. Once the web server has been accessed, the infiltration begins by collecting access logs to determine the internal IP address. Following that, pivoting tactics are used, employing a Meterpreter payload and exploiting an SMB vulnerability to obtain access to the internal Windows server, allowing deeper access within the internal network.

Objectives

- Nmap is a network reconnaissance tool that may be used to find open ports and services on target systems.
- Employ Metasploit and Armitage to identify and run exploits aimed at vulnerable web apps.
- Start a breach on the web server, go through logs for internal IP addresses, and then pivot to other systems on the network.
- Use Meterpreter payloads to gain persistent access to hacked systems, showing post-exploitation techniques including hash dumping, file uploading, and execution.
- To conceal actions, erase any evidence of penetration testing while realizing the ethical and legal repercussions of unauthorized system breaches.
- Learn how to use hacking tools such as Nmap, Meterpreter, Armitage, Metasploit, and Kali Linux to prepare for roles in ethical hacking and authorized penetration testing.
- Investigate integrating several exploits to better understand how attackers fully infiltrate target networks, while also improving defensive security skills by understanding offensive tools and methodologies.

Lab Description Details

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

Supporting Evidence

Step 1: Launch Kali 2 Attack Machine. Enter the credentials.

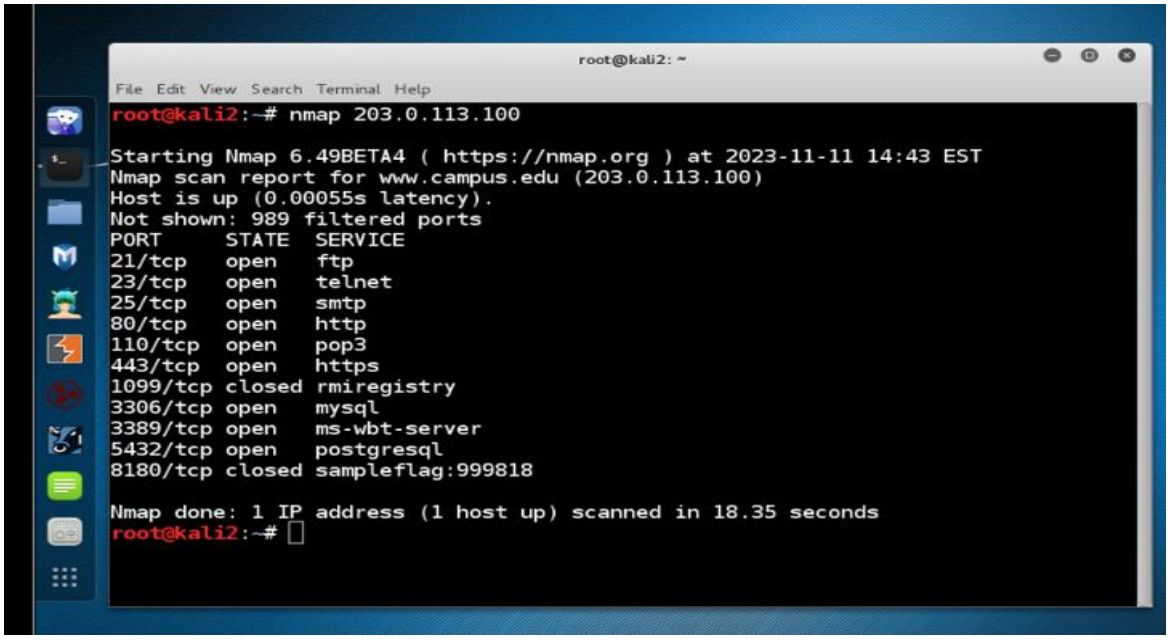
Username: root

Password: toor

Step 2: Open the terminal.

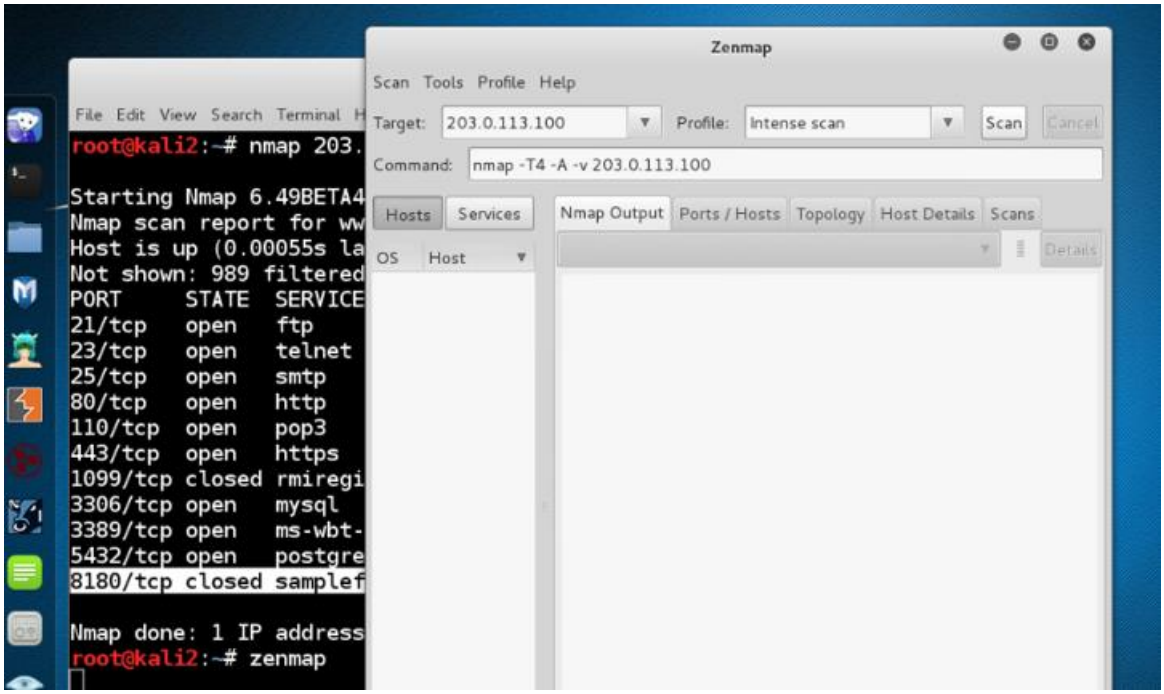
Step 3: Scan the firewall for open ports.

nmap 203.0.113.100

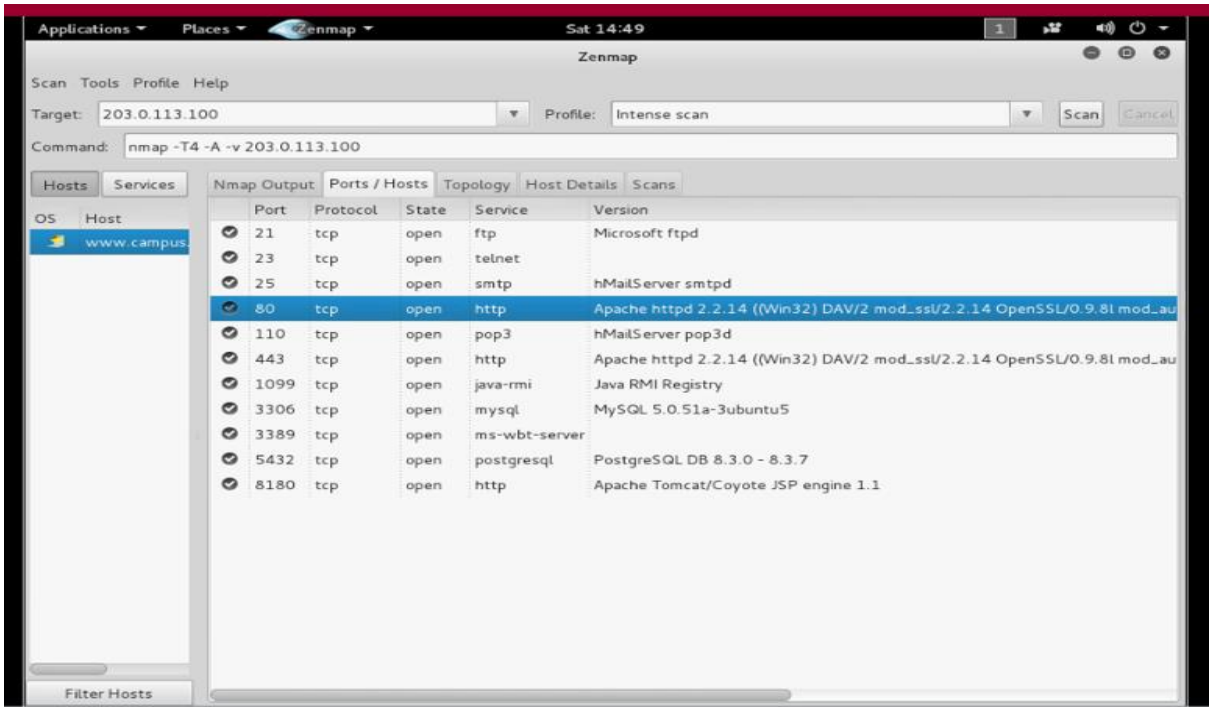


Step 4: Solve the sample challenge.

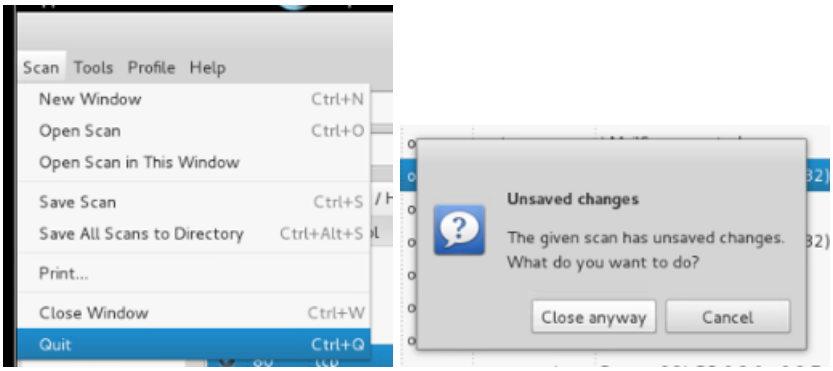
Step 5: Open Zenmap. Set the target as 203.0.113.100 and launch an intense scan.



Step 6: Click Ports/Hosts tab to view the open ports and the banner messages that are displayed. Observe Apache httpd 2.2.14 (Win32) DAV/2 banner from the results.



Step 7: Quit Zenmap.

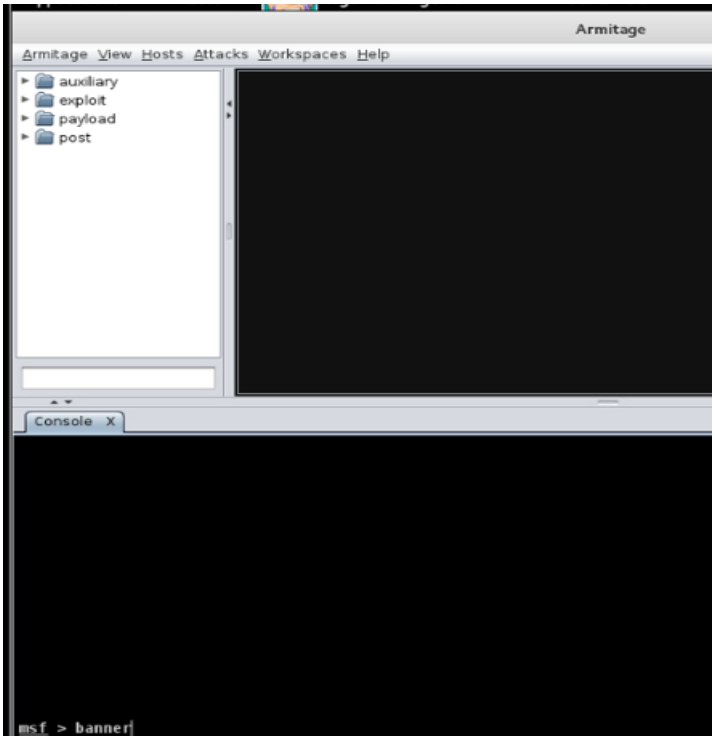


Step 8: Start postgresql service. Start Armitage directory.

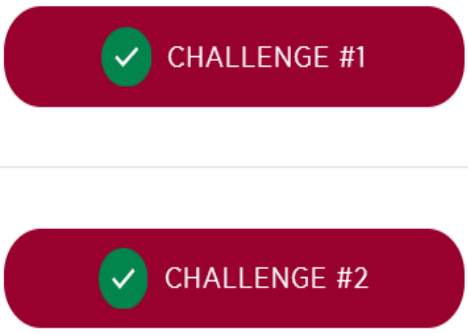
```
# service postgresql start
# cd armitage
# ./armitage
```

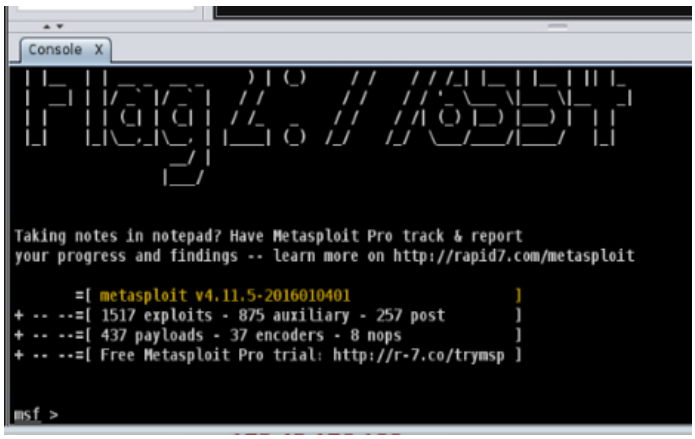
Step 9: Connect and start Metasploit.

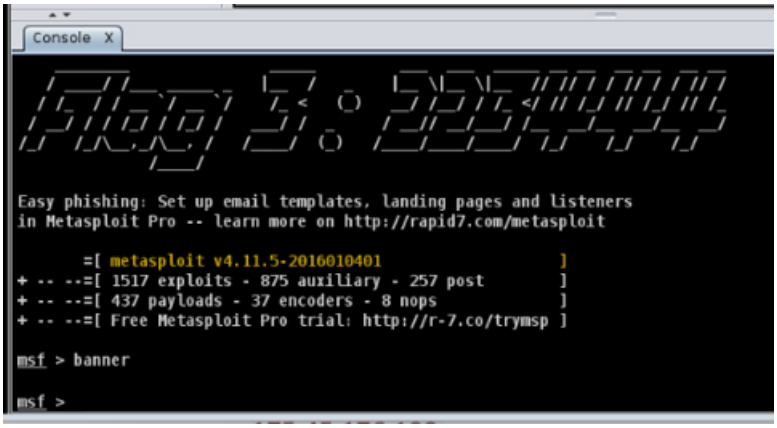
Step 10: Press enter in the banner command.



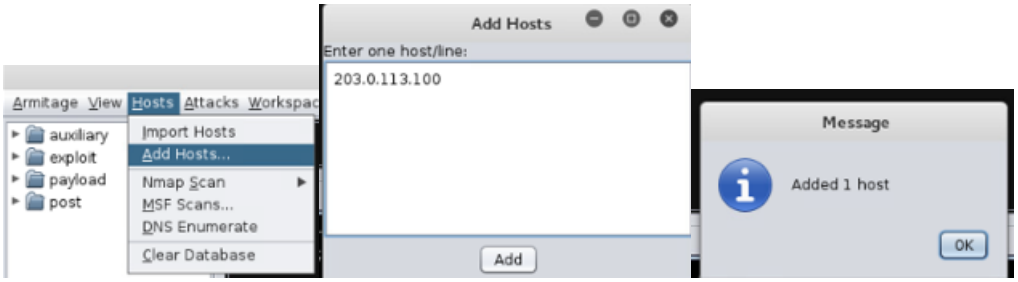
Step 11: Solve the challenges 1 and 2.



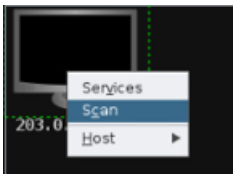




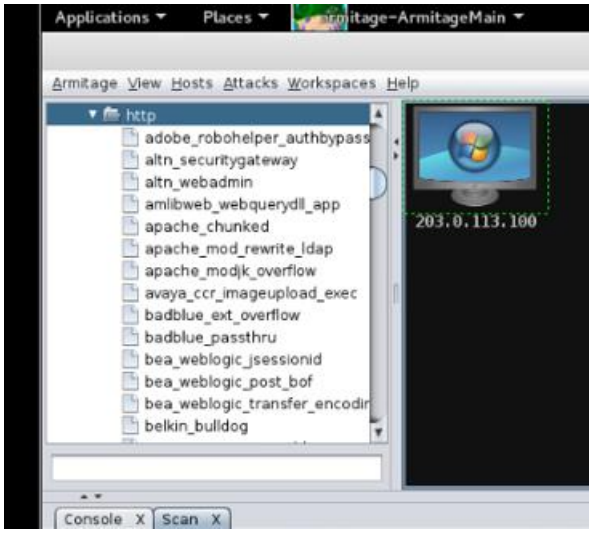
Step 12: In the Armitage tab, Select Hosts>Add Hosts>203.0.113.100

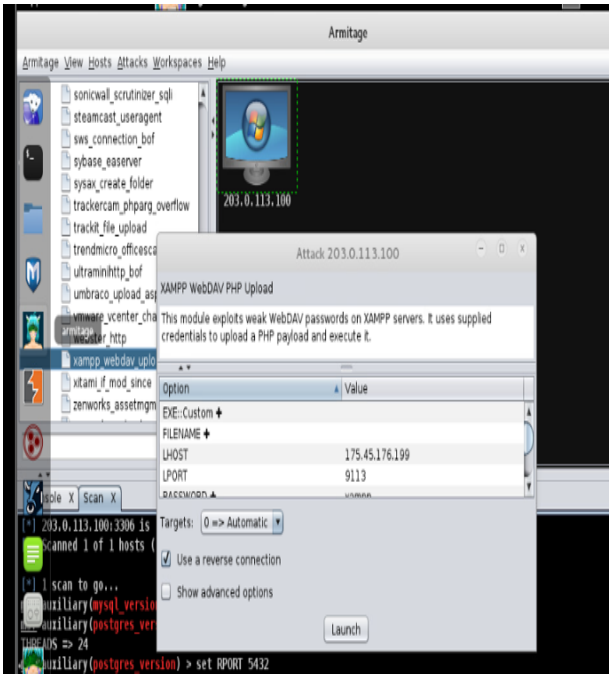


Step 13: Select the host 203.0.113.100 and scan it.

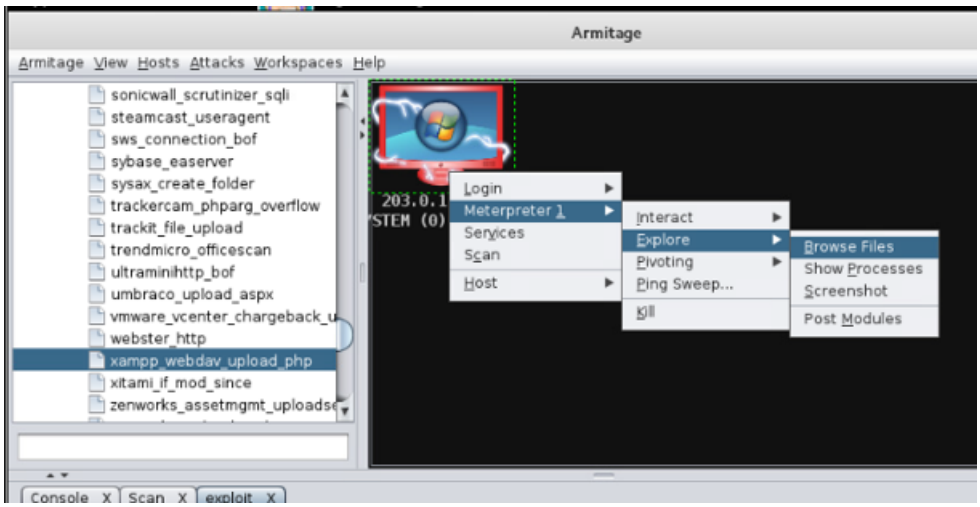


Step 14: Click exploit>windows>http>203.0.113.100>xampp_webdav_upload_php>Launch

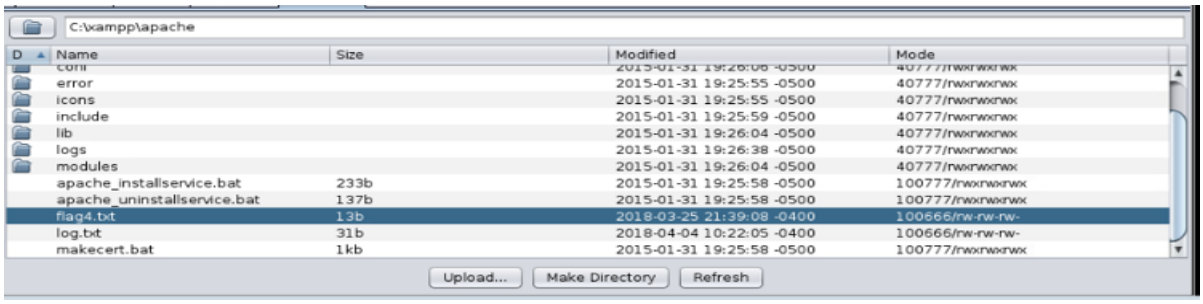


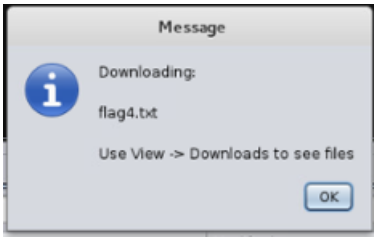


Step 15: Select the compromised victim>Meterpreter 1>Explore>Browse Files

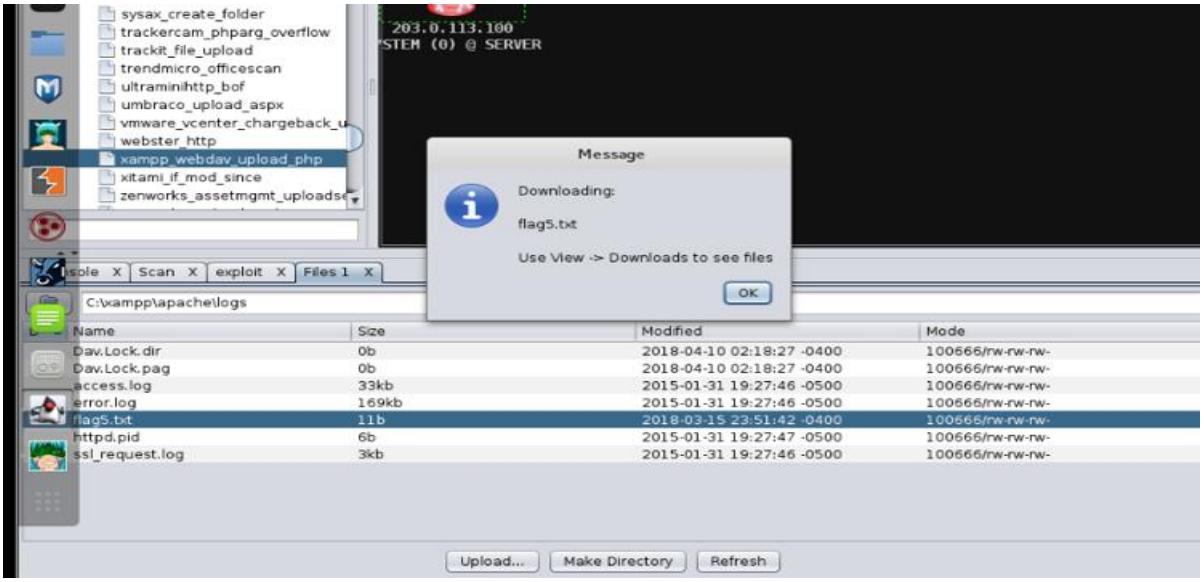


Step 16: Double-click on apache folder>flag4.txt>Download>Ok

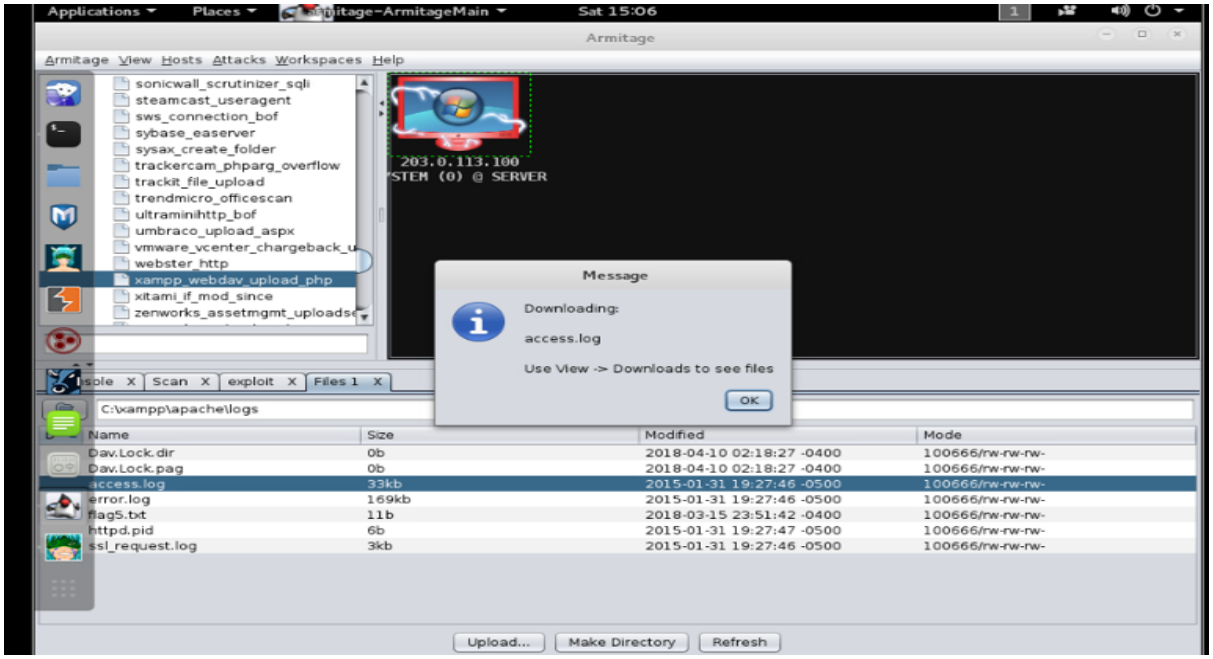




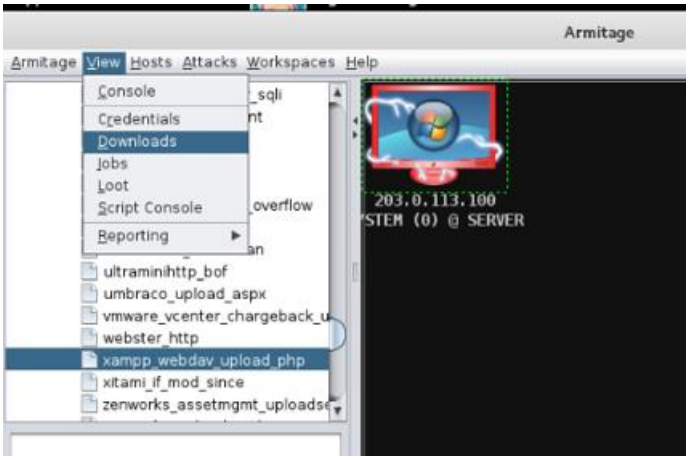
Step 17: Double-click on logs folder>flag5.txt>Download>Ok



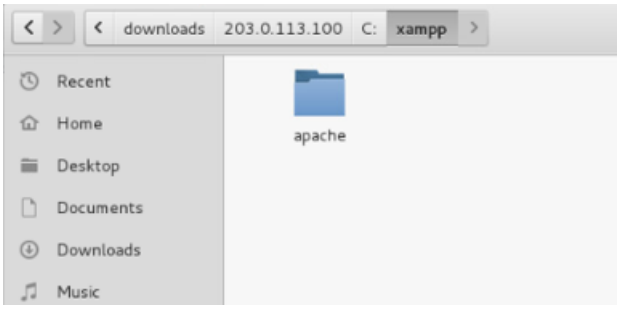
Step 18: Click on the access.log file>access log>Download



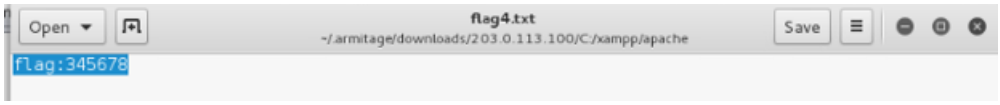
Step 19: Click on View>Armitage menu bar>Downloads



Step 20: Select access.log file>Open Folder>203.0.113.100>C:>xampp>apache

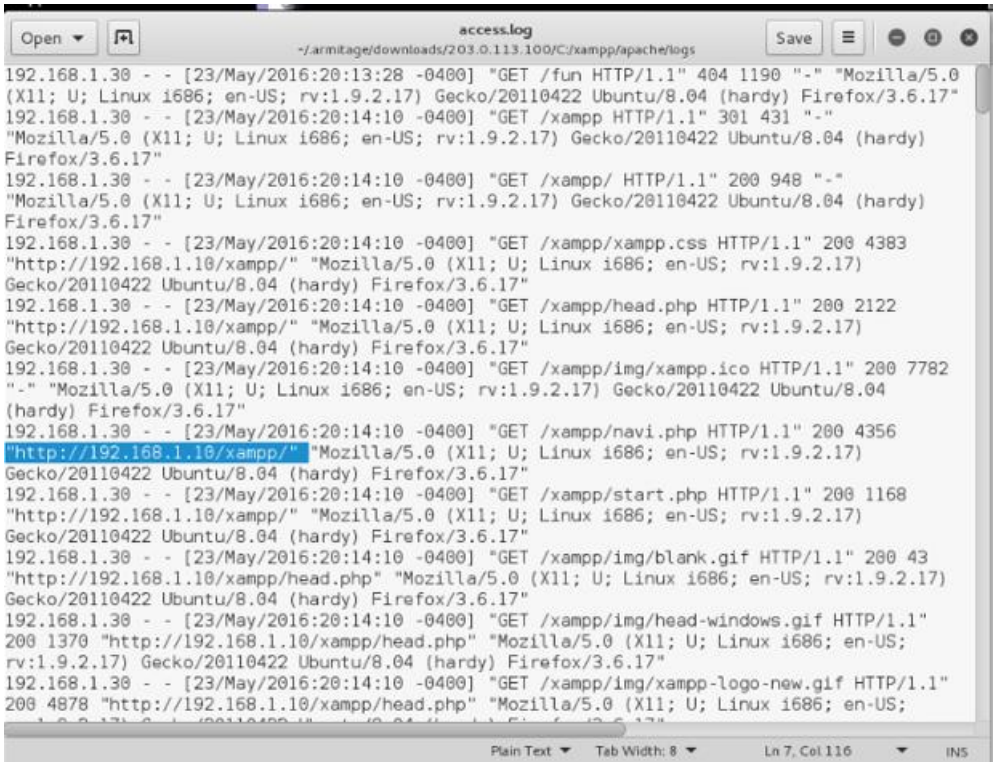


Step 21: Solve the challenge 3.

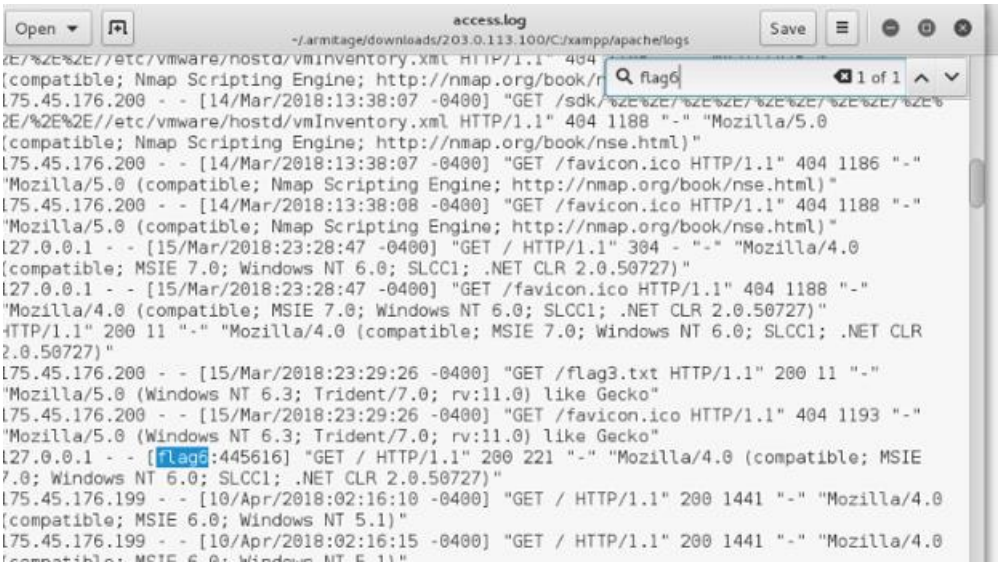


Step 22: Solve the challenge 4.

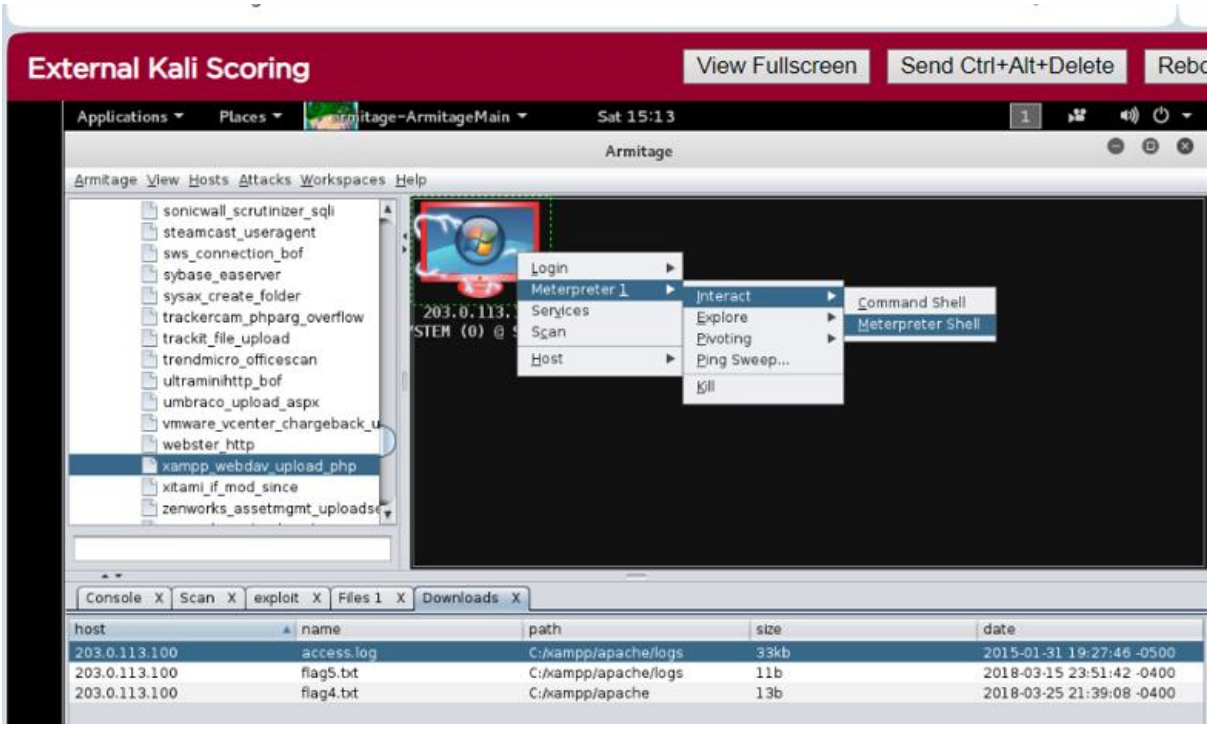
Step 23: Double-click on logs>access.log>View the IP address of the web server



Step 24: Solve the challenge 5.

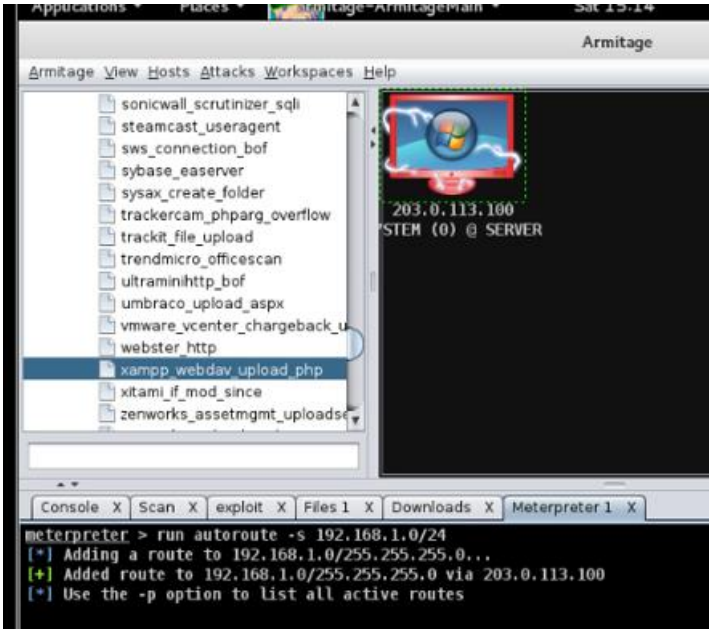


Step 25: Click on Compromised host>Meterpreter 1>Interact>Meterpreter Shell

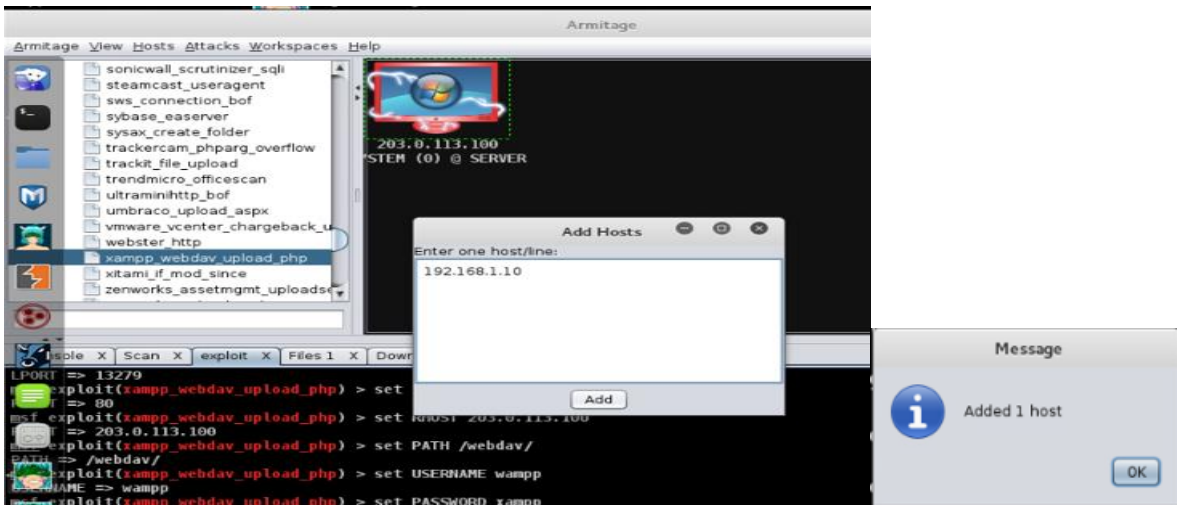


Step 26: Add a route to the victim's LAN.

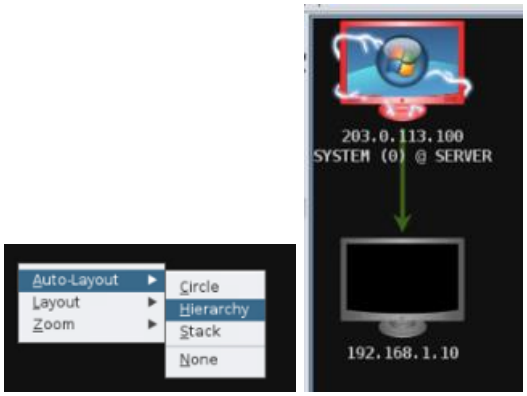
>run autoroute -s 192.168.1.0/24



Step 27: Select exploit>Hosts from Armitage menu>Add Hosts>192.168.1.10>Add>Ok



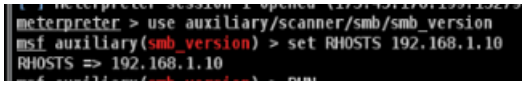
Step 28: Select Auto-Layout>Hierarchy



Step 29: Return to the msf console and set the IP address of the remote host.

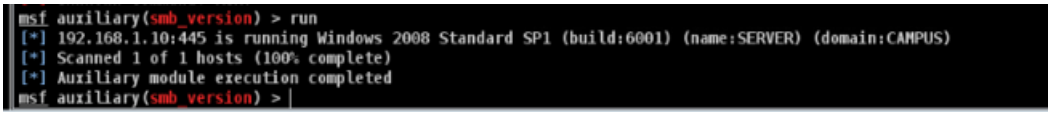
> use auxiliary/scanner/smb/smb_version

>set RHOSTS 192.168.1.10

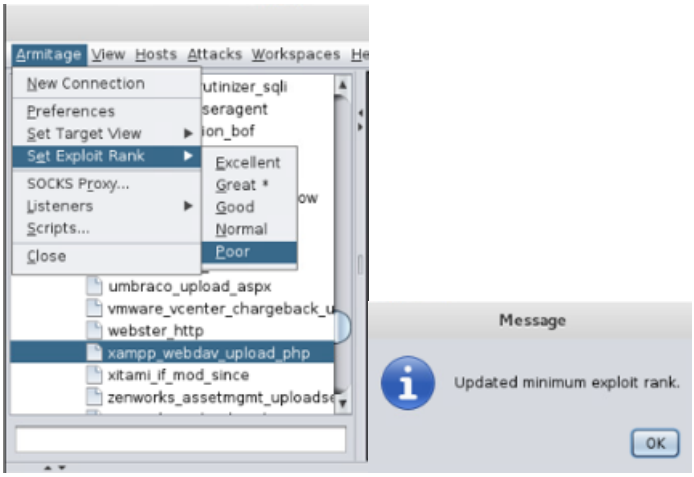


Step 30: Run the scan.

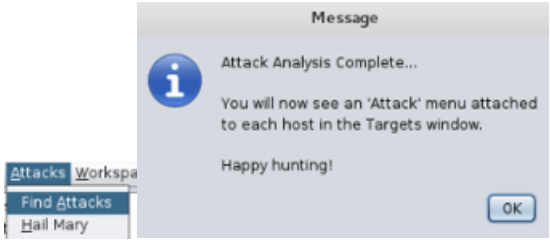
>run



Step 31: Select Armitage>Set Exploit Rank>Poor

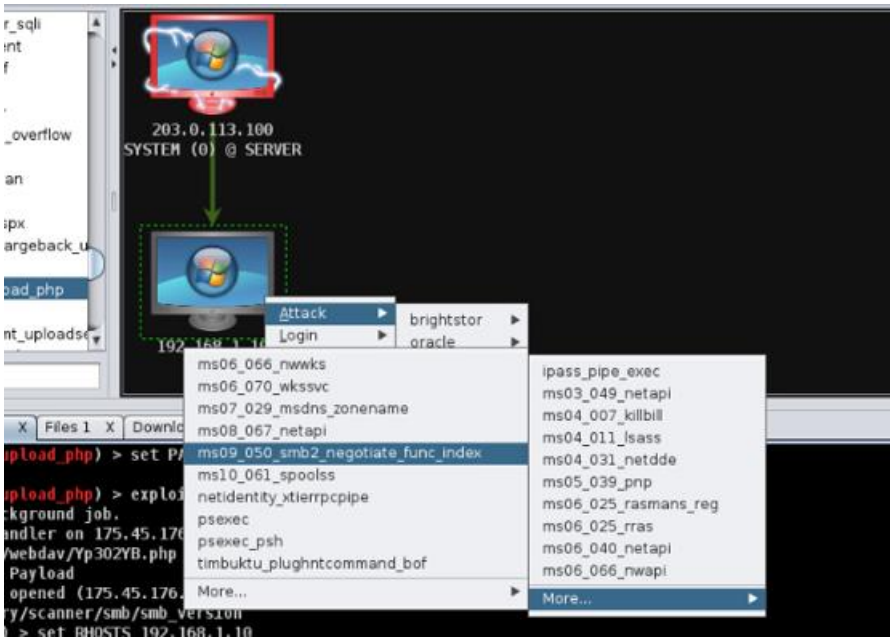


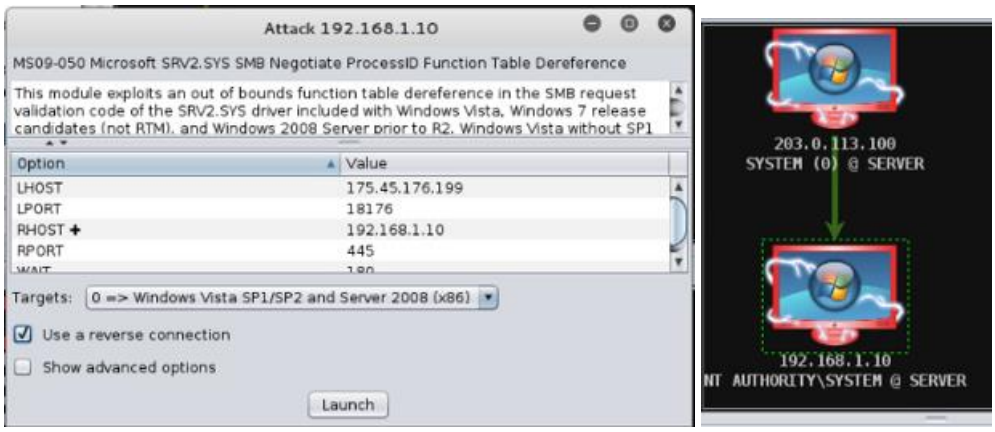
Step 32: Select Attacks>Find Attacks



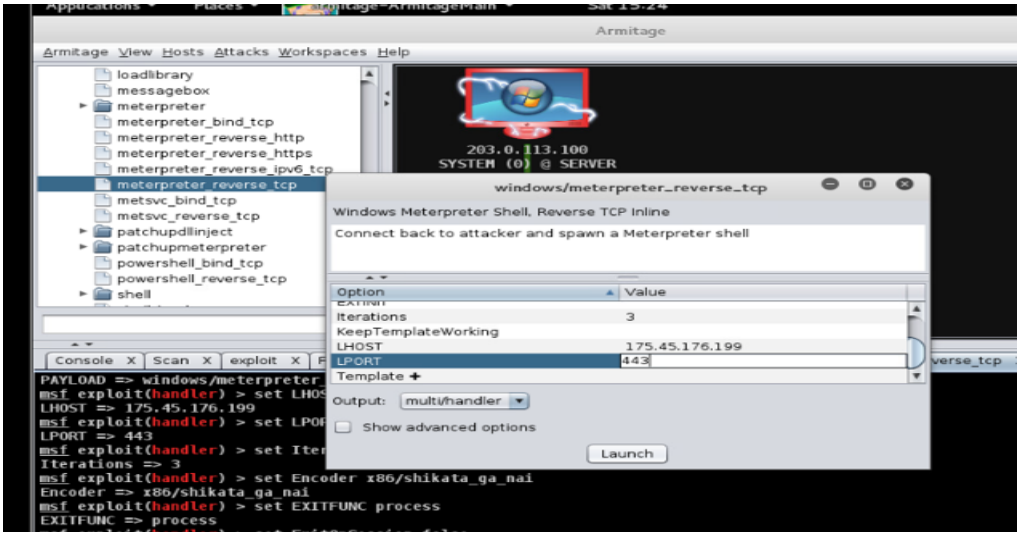
Step 33: Select

192.168.1.10>Attack>smb>more>ms09_050_smb2_negotiate_func_index>Launch

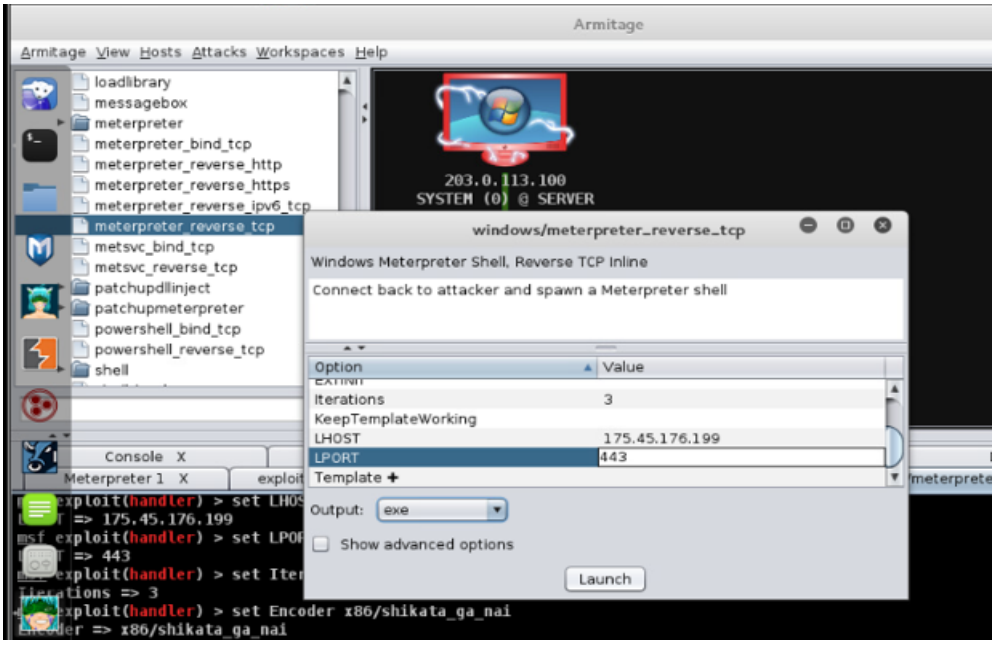




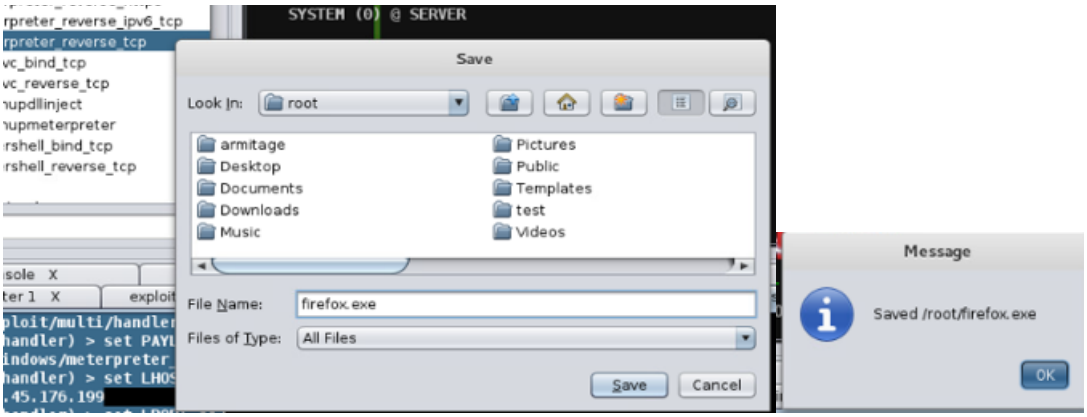
Step 34: Select Payload>Windows>meterpreter_reverse_tcp>LPORT value>443>Launch



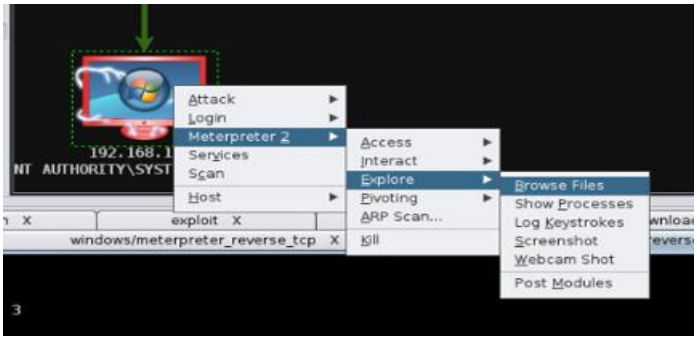
Step 35: Select windows>meterpreter_reverse_tcp>LPORT value>443>exe>Launch



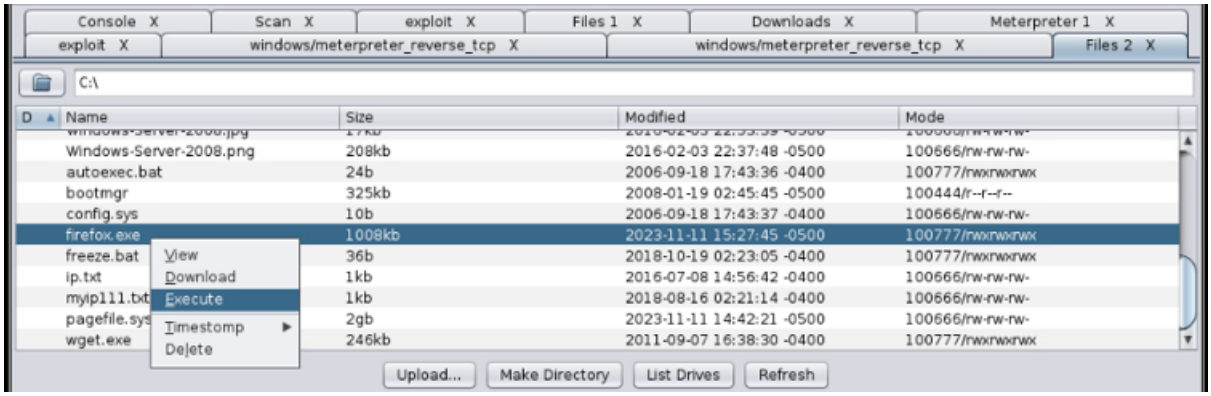
Step 36: Save the file as firefox.exe

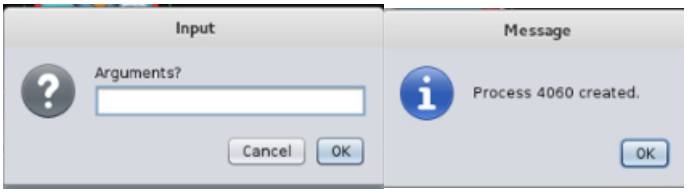


Step 37: Click on compromised victim>Meterpreter 2>Explore>Browse Files



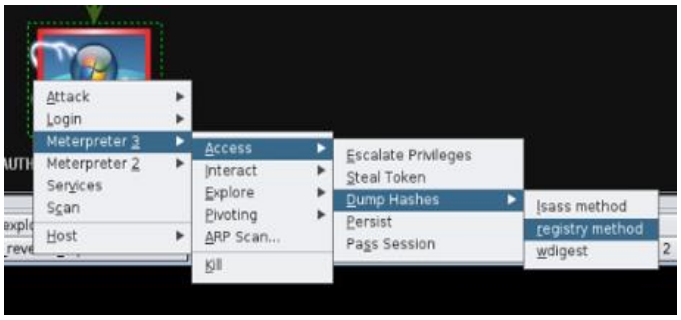
Step 38: Upload>Select firefox.exe>Open>Launch firefox.exe>Execute>Arguments



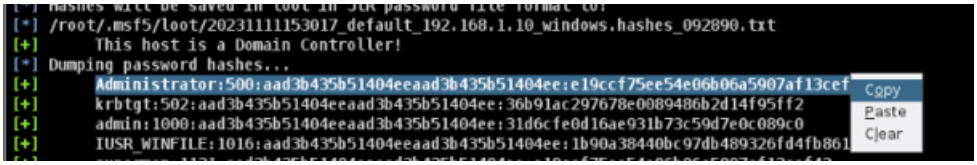


Step 39: Open windows and check that meterpreter session 3 is opened.

Step 40: Select com[romised victim 192.168.1.10>Meterpreter 3>Access>Dump Hashes>registry method>Launch



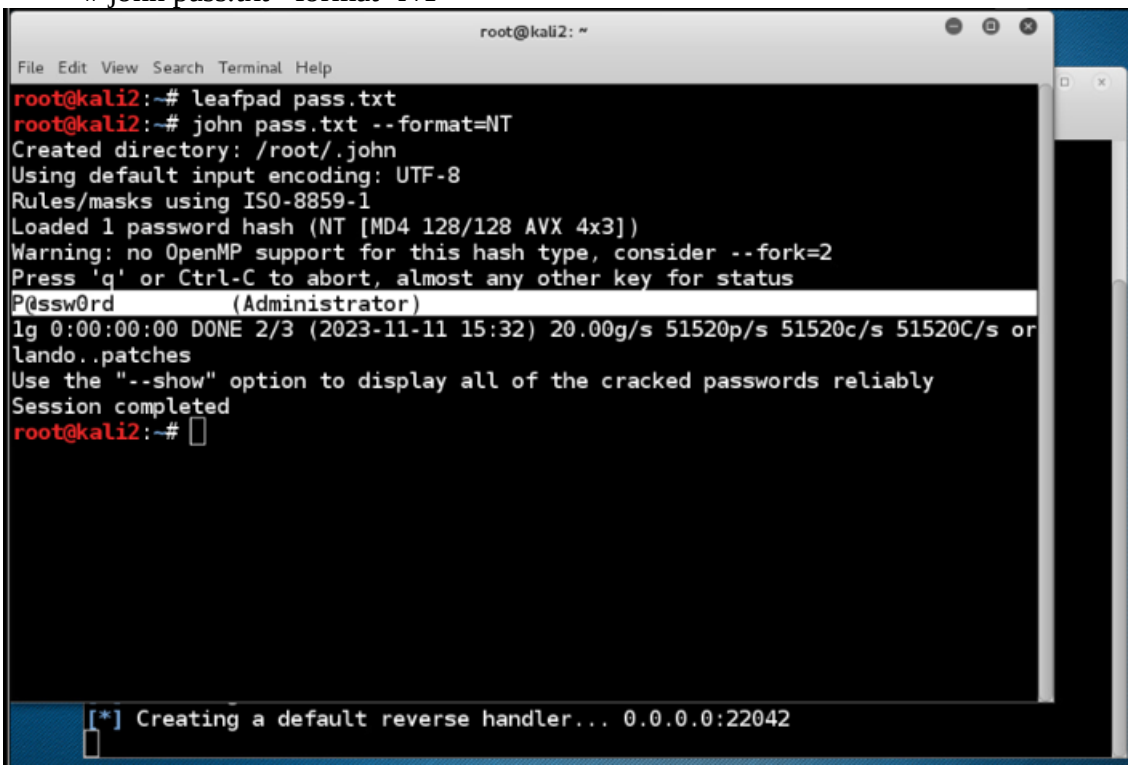
Step 41: Highlight the administrator account and two hashes and copy them.



Step 42: Select file>Open terminal>Paste>Save>Quit

Step 43: Create a text file named pass.txt

john pass.txt –format=NT



Conclusion & Wrap-Up

Summary with observations, Successes & Failures, Challenges

This lab provides hands-on experience with breaking a vulnerable web application and subsequently compromising an internal system, showcasing standard hacker tactics with Nmap, Metasploit, Armitage, and Meterpreter, as well as other penetration testing tools in Kali Linux. It highlighted the crucial necessity for complete defenses, emphasizing the limitations of depending exclusively on perimeter firewalls. Initial access by attackers via publicly known vulnerabilities highlights the importance of multi-layered internal defenses to prevent privilege escalation and lateral movement within networks. Metasploit and similar offensive tools attract attention to existing vulnerabilities, highlighting the need for defenders to address and remedy these flaws as soon as possible in order to prevent exploitation and harden system defenses.

Successes:

- Nmap network scans were successfully completed in order to identify vulnerable Apache httpd services.
- Metasploit effectively exploited the XAMPP WebDAV module by using the web server.
- Executed and installed a Meterpreter payload on the hacked Windows server, gaining post-exploitation access to extract password hashes.
- Demonstrated hacker tactics by altering paths and concealing traces to simulate real-world scenarios.

Failures:

- Managed security alerts from Metasploit components and ran into problems with invalid SSL certificates.
- Required adherence to specific procedures for payload delivery and handling post-exploitation tasks.
- Overcame difficulties brought on by numerous active Meterpreter sessions and shell interactions.

Risks:

- Noted the serious risk that unprotected software posed and emphasized the necessity of applying patches and updates on a regular basis to fend off possible assaults.
- Advocated for network segmentation and firewall rules to restrict attacker access through unused open ports, minimizing exposed services.
- Noted the risks associated with using plaintext passwords and suggested using hashed storage techniques in addition to strict password regulations for further protection.
- Emphasized the need to keep an eye on system and network activity to spot possible attacker lateral movement.
- Emphasized how important thorough event and access logging is, as it is necessary for efficient post-breach investigations.
- Urged rapid isolation of compromised systems to prevent attackers from further penetrating the network.

- Advised using anonymizing software, VPNs, and operational security (opsec) measures to avoid detection if tracks are left behind.

Remediations:

- Strengthen security measures for systems that are visible to the public and routinely check open ports and services for security flaws.
- Make sure there is a current asset inventory by conducting regular vulnerability assessments and penetration tests.
- Limit the privileges granted to users and service accounts in order to uphold the least privilege idea.
- Use network segmentation in conjunction with strong firewalls to stop lateral network migration.
- Stricter authentication protocols and the use of password management software can improve authentication techniques.
- To strengthen security procedures, keep a close eye on network traffic for strange file transfers and internal interactions.
- To proactively find security flaws, and install host-based monitoring systems and advanced behavioral analytics technologies.
- Create and implement a thorough incident response plan with the goal of quickly containing and reducing any possible hazards.