**Lab - Nmap Scripting Engine (NSE)**

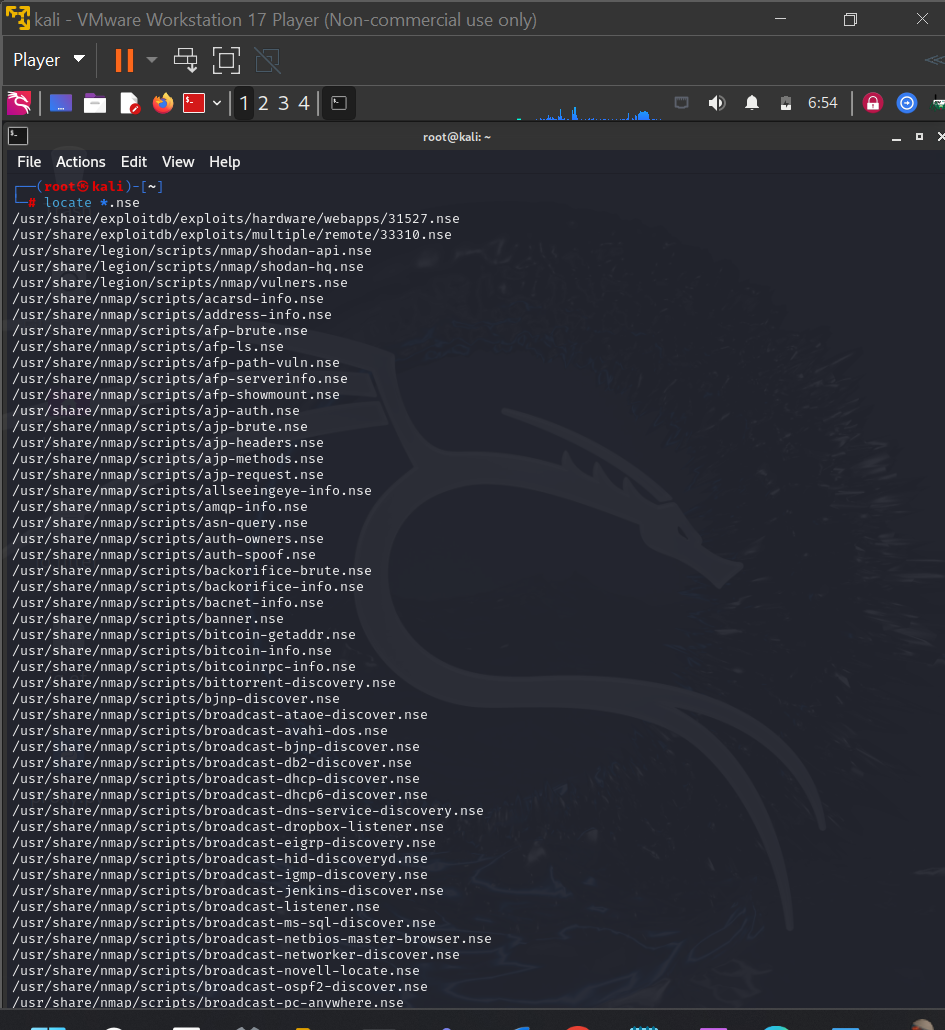
**150182 -Kipruto Isaac**

**Begin the lab**

• Start Kali & Open a Terminal.

• Open your Windows XP VM.

Find the Nmap Scripts



**Finding Vulnerability Scanning Scripts**

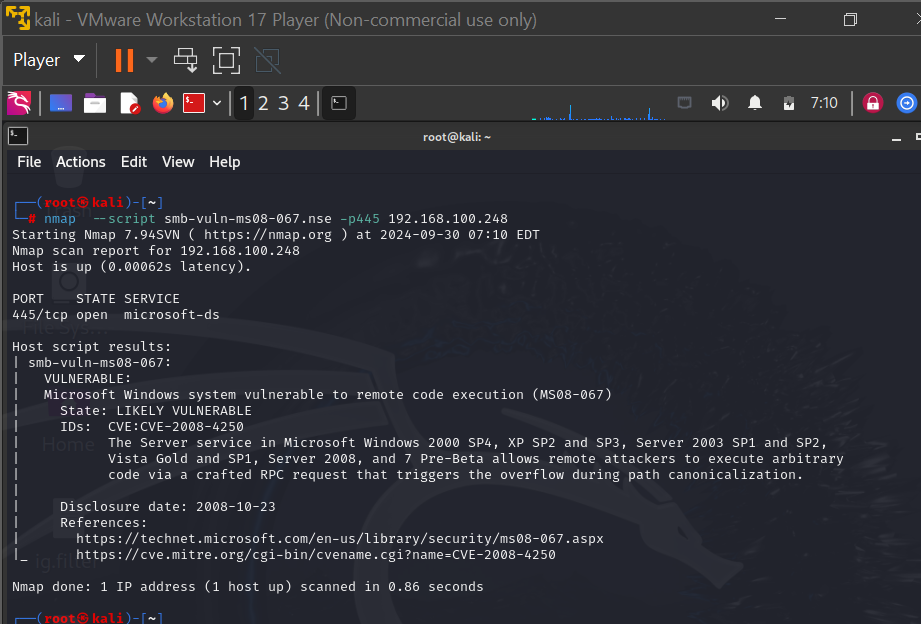
Among the most useful to us are the vulnerability scanning scripts. These scripts are usually designed to find a specific vulnerability or type of vulnerability that we can then come back later and exploit. To locate those scripts that we can use for vulnerability scanning, we can type

A screenshot of a computer

Description automatically generated

**Running the Script**

Ensure the Windows XP Virtual Machine is up and running. You will need the IP address of your victim to run this script. Think back to Lab 3, what Nmap commands could you use to footprint and discover the IP of your Windows XP victim? You can also get the IP by logging on to the victim and running IPCONFIG from a command prompt.



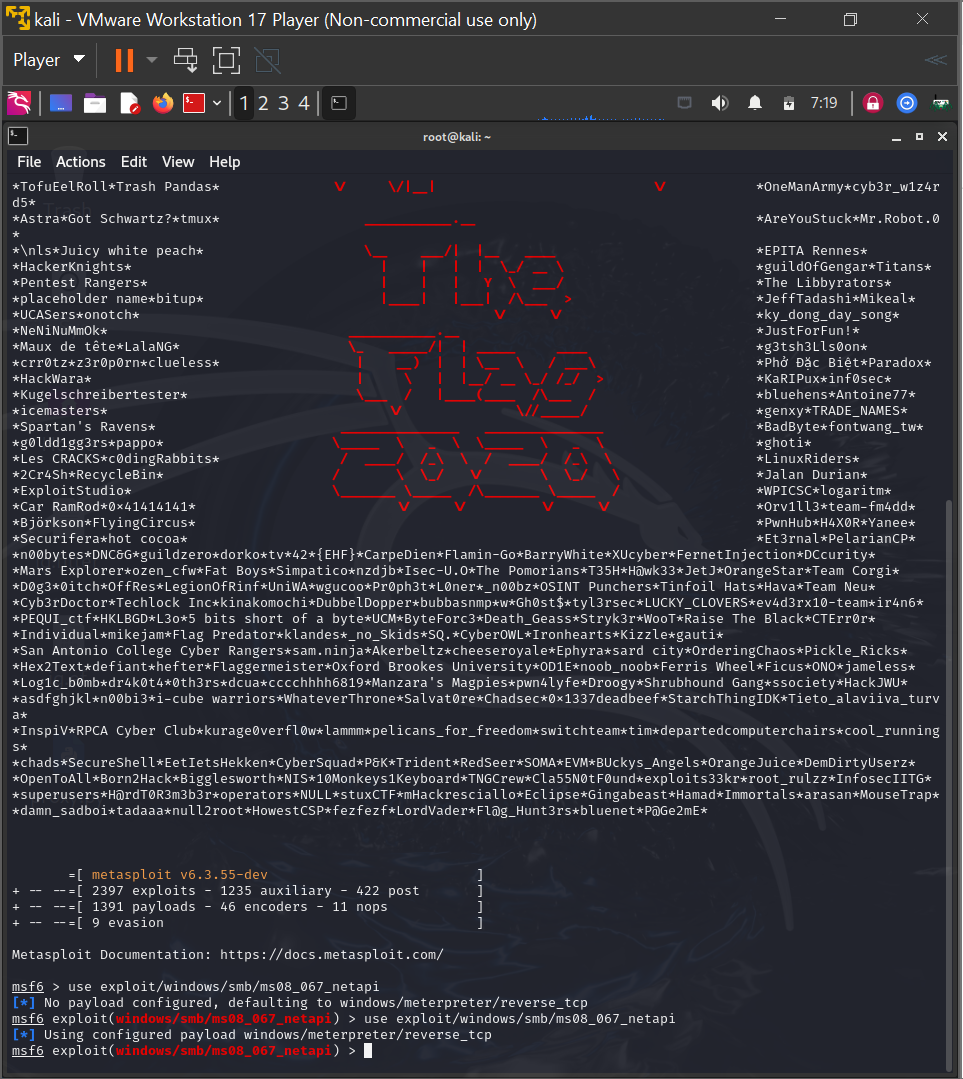
As you can see, it tells me that MS08-067 is vulnerable, so now I know I can use that module in Metasploit to exploit that system!

1. From your Terminal, type exit.

2. Type clear.

3. To launch Metasploit, type msfconsole at the kali prompt

To choose our exploit, type “use exploit/windows/smb/ms08\_067\_netapi”



Again, the RHOST is the remote machine or the machine we are attacking. To set this, I’ll enter “set RHOST 192.168.100.248″ at the exploit prompt

