**Lab - Using Meterpreter to backdoor Windows XP**

**Hardware requirements for these labs:**

1. Do not use a Wi-Fi connection. Use an Ethernet cable to connect to the network. Wi-Fi is configured for IPSec which can impede the labs from working. The additional transport and tunneling protocols do not play well with Kali or Metasploit.

**Stop!!!**

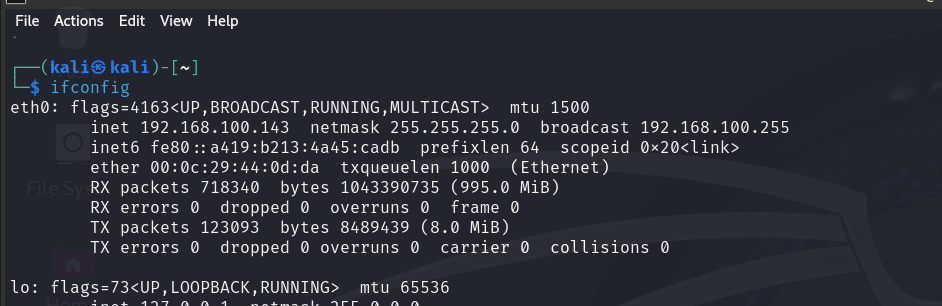
1. You need to have XP installed as either a virtual machine or as stand alone.
2. Windows XP will need to be up running and available on the same network as your Kali install. You will need to know the IP address of your Windows XP victim and be able to ping it from your kali install.
3. You will need to ensure that the Windows XP firewall is disabled.
4. \*\*\* RDP or remote access must be enabled on the remote XP victim. \*\*\*\*

**Overview**

In this lab, we see how easy Meterpreter can be used create a backdoor into Windows using nothing more than built-in system tools. We will also see how easy it is to detect and disable the Windows firewall if it is running on our victim machine. Lastly, we’ll want to remove any traces of our presence from the Windows log files.

First, we cannot find anything or anyone unless Kali or our host can see the network. That means if you check your IP address on your Kali or host machine, you should see the network portion of your IP address in the results.

On your Kali machine, open a terminal and find your host IP address. Look at the first three octets that is your network IP. The last octet represents you host IP.



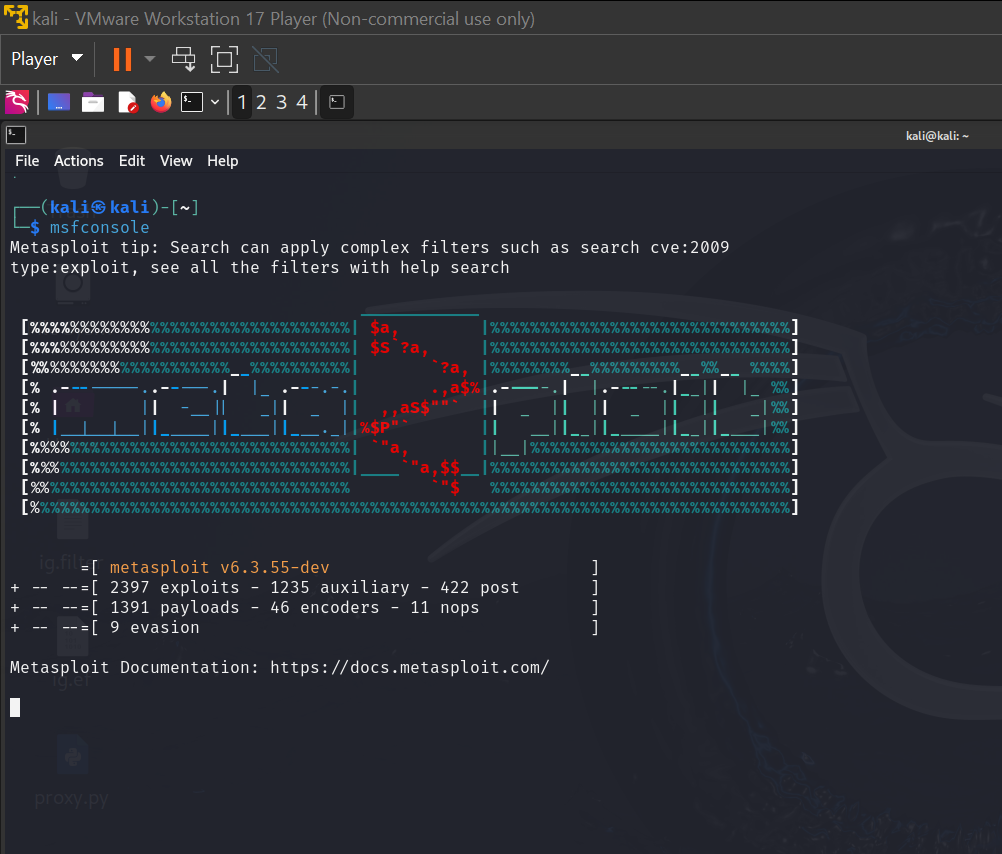
Once we have identified the network range for our victim’s network, we can use Nmap to scan the network for our Windows XP victim. Make sure you have your Windows XP machine up and running.

A screenshot of a computer

Description automatically generated

We now have two pieces of information we need to launch a remote session using Meterpreter, out host IP and the IP of our XP victim. Make sure you have these two pieces of information, and they are correct.

We can now launch Metasploit from a terminal session inside of Kali.



We next need to create a shell session using Meterpreter.

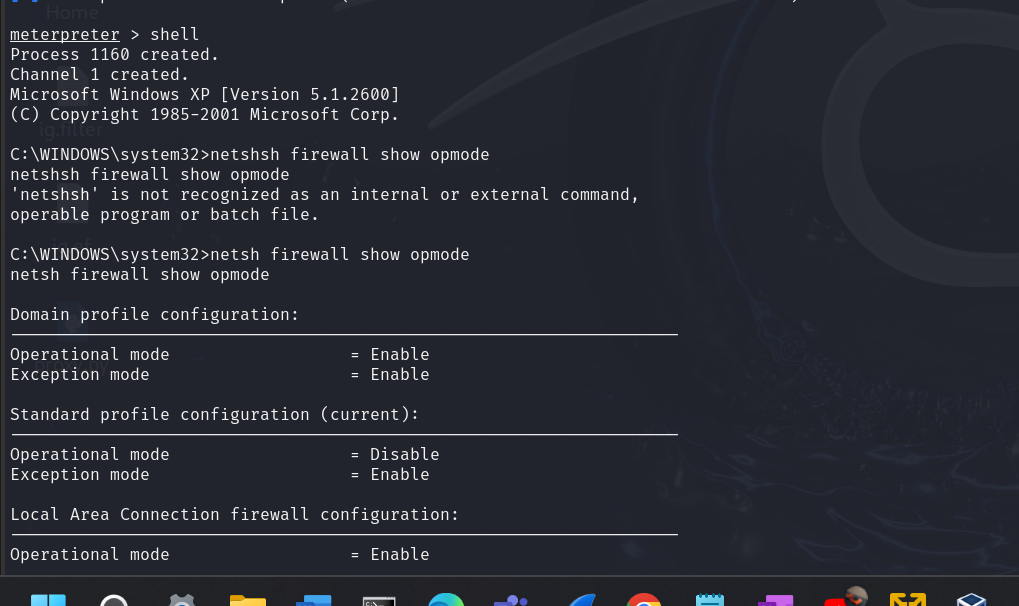
For this, we will **use** the exploit **/windows/smb/ms08\_067\_netapi**

use windows/smb/ms08\_067\_netapi



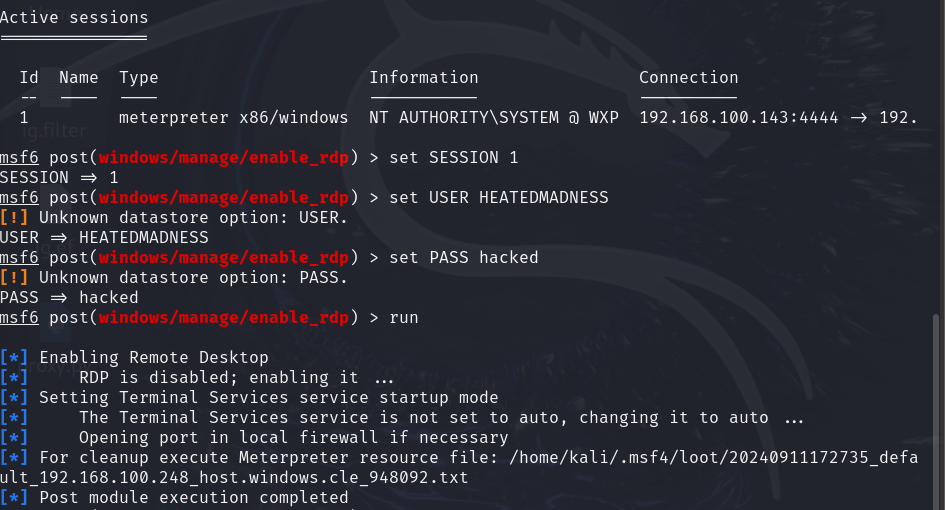
Let’s check and see if the machine has a firewall and if it is enabled. We do this by opening a shell or terminal session with the Windows XP victim. Therefore, we needed the Meterpreter session.

At the Meterpreter prompt, type **shell**

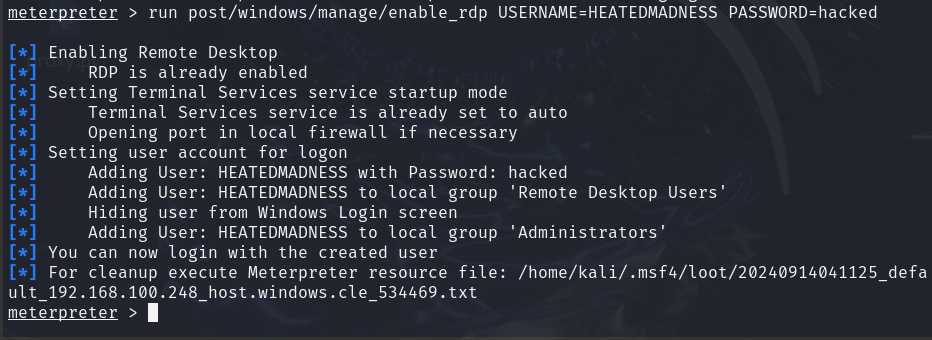


At the Windows command prompt, type exit. This brings us back to the **meterpreter** prompt.

We will now connect using an RDP session using an all-in script that will do all the work for us.

ex

Type: **run getgui -u maddog -p hacked (**you can use any username or password you want) This username and password will be added to the local administrator group.



We now have to get back to a normal command prompt so just keep typing exit until you’re back to the kali prompt. At the prompt, you will need to type in the rdesktop command as you see it typed in the next image. Remember…. this is my IP address for my windows XP machine. If your username and password were different, you would need to use those.

Let’s test the connection to see if it can really be that easy.

A screenshot of a computer

Description automatically generated

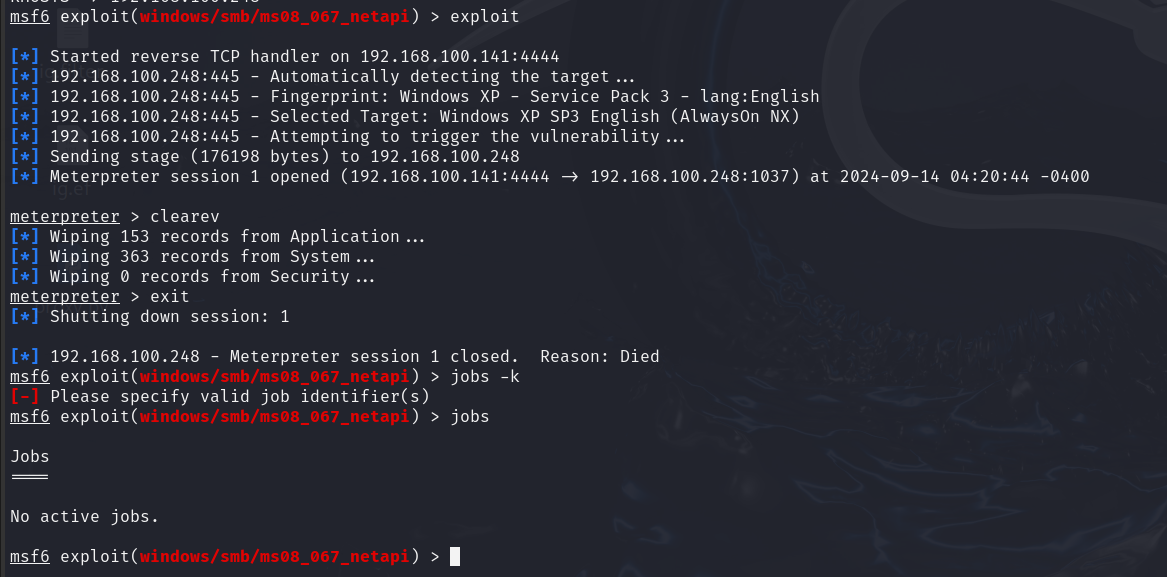
**Summary**

We used the ‘rdesktop’ command and specified the username and password we want to use for the login. We then received an error message letting us know a user was already logged into the console of the system, and that if we continue, that user will be disconnected. This is expected behavior for a Windows XP desktop system, so we can see everything is working as expected. Note that Windows Server allows concurrent graphical logins, so you may not encounter this warning message.

Remember, these sorts of changes can be very powerful so use your powers wisely, as all these steps alter the systems in ways that can be used by forensic investigators to track what sort of actions were taken on the system. The more changes are made; the more evidence we leave behind.

When you are done with the current system, you will want to run the cleanup script provided to remove the added account. This script is particular to each session, so you will have to get your script command from your Kali terminal.

While we are here let’s cover all our tracks and remove any event log files.



**To prevent this type of attack:**

1. Ensure your Windows machine is patched and updated
2. Your firewall is enabled.
3. Your Anti-virus is up to date.
4. RDP is disabled Not too shabby!

End of the lab!