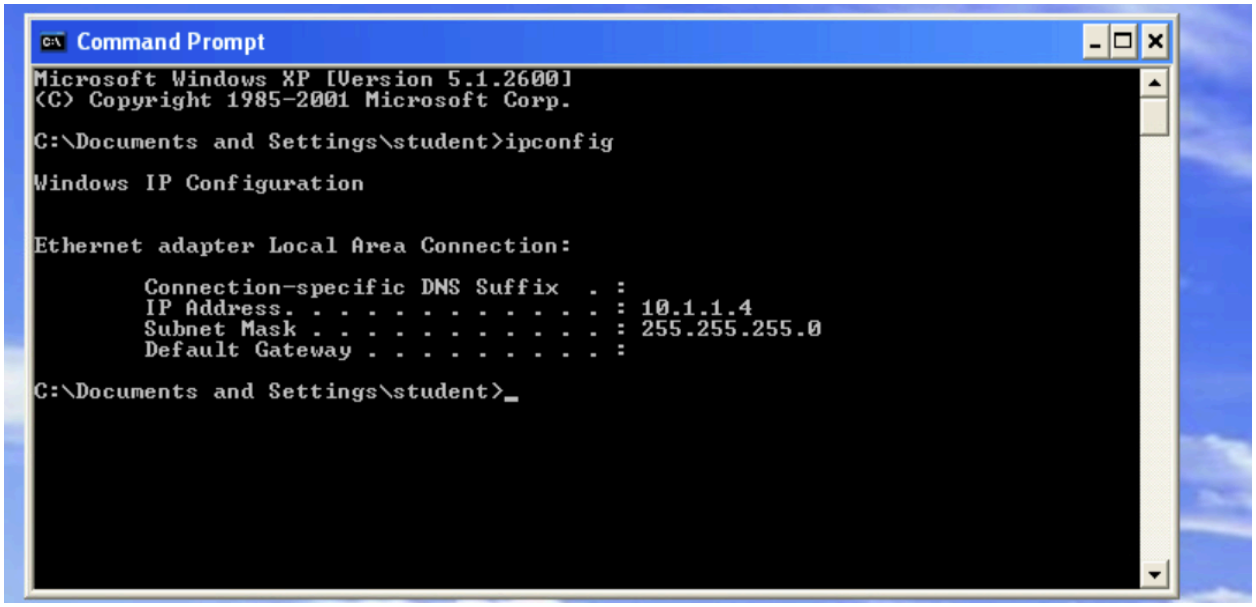
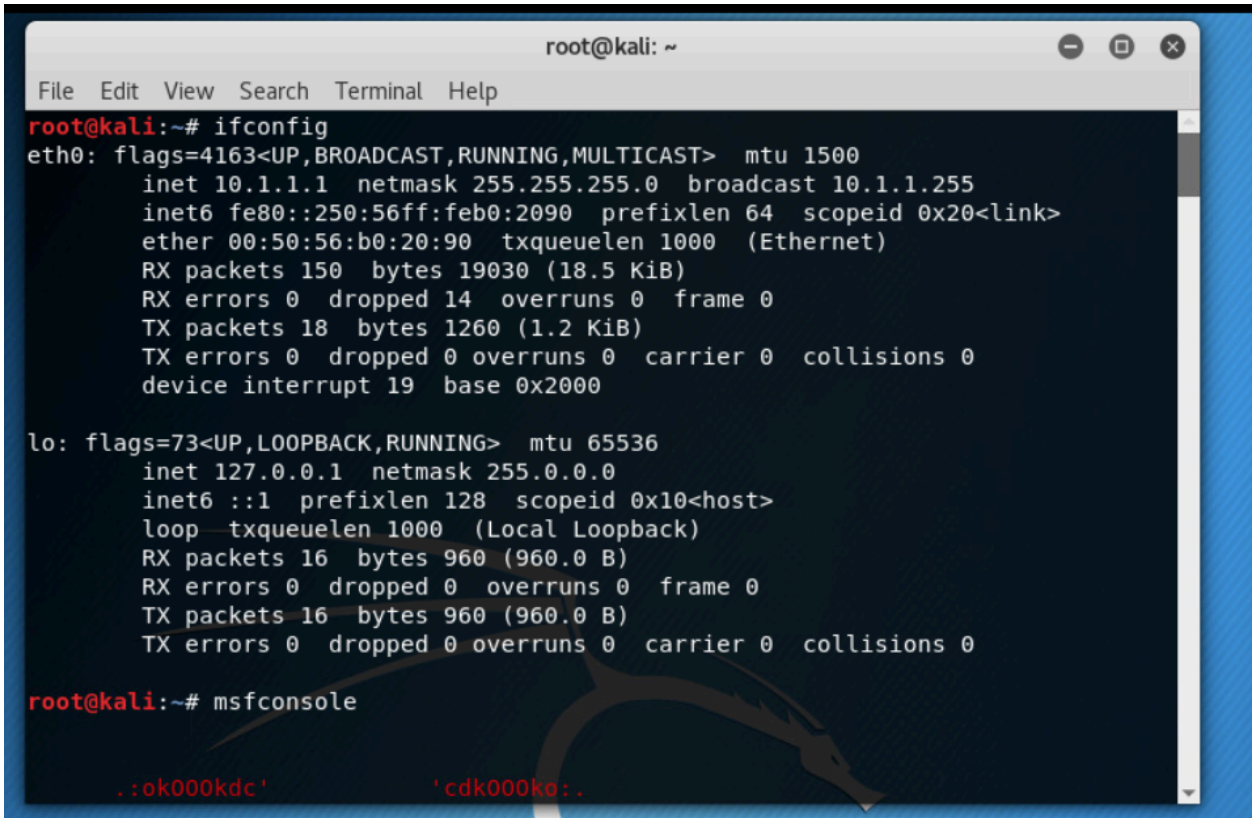
Lab 6: Write-up
RPC BUFFER OVERFLOW WITH METASPLOIT

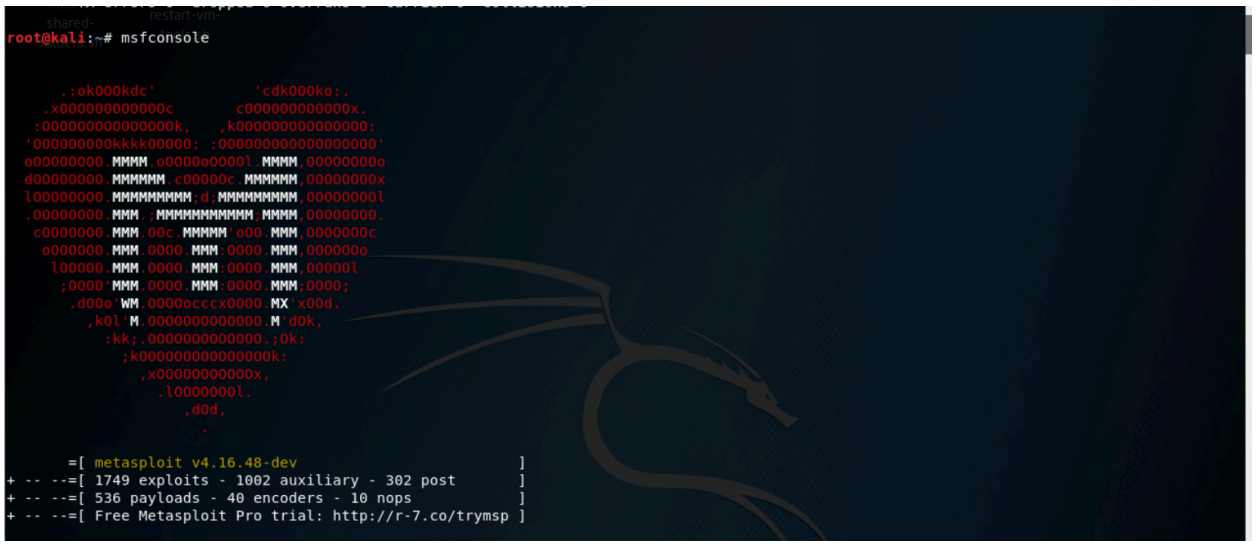
SHRIRAM KARPOORA SUNDARA PANDIAN
CSEC 742: COMPUTER SYSTEM SECURITY

Step 1: For performing this lab, I am noting the IP addresses of the XP machine and my Kali machine.



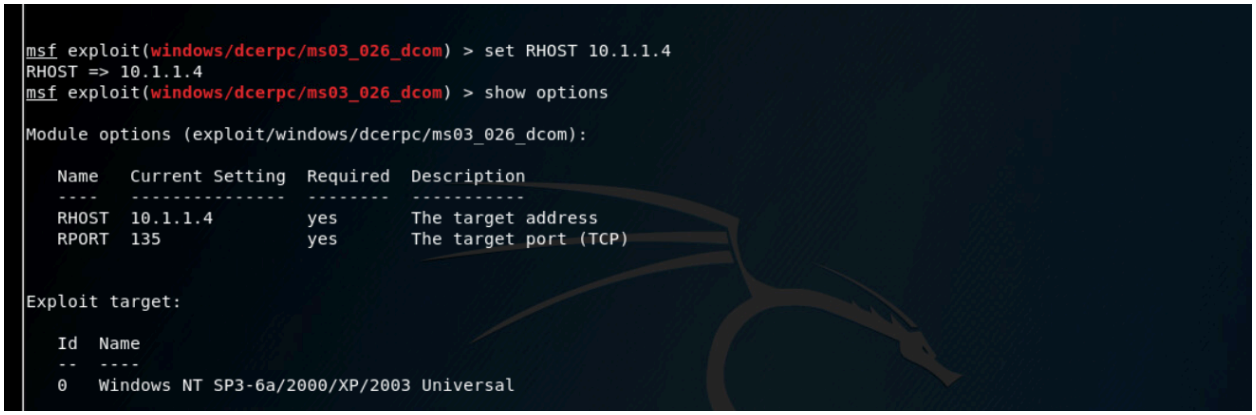


Step 2: I am starting my msfconsole which is metasploit.

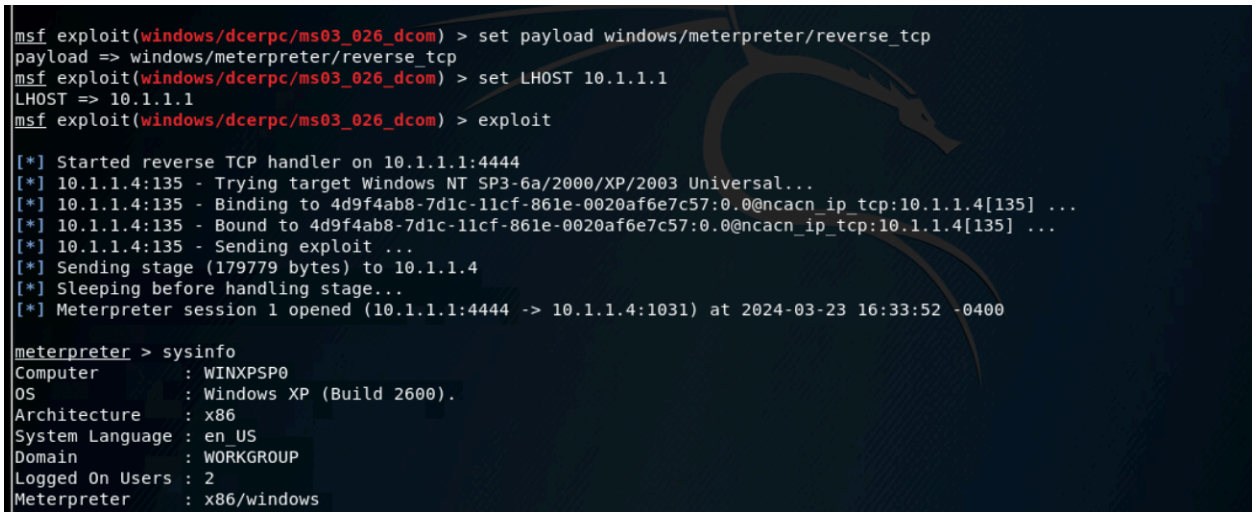


Step 3: I am searching for the dcom exploit and I am particularly looking of r ms03_026 one.

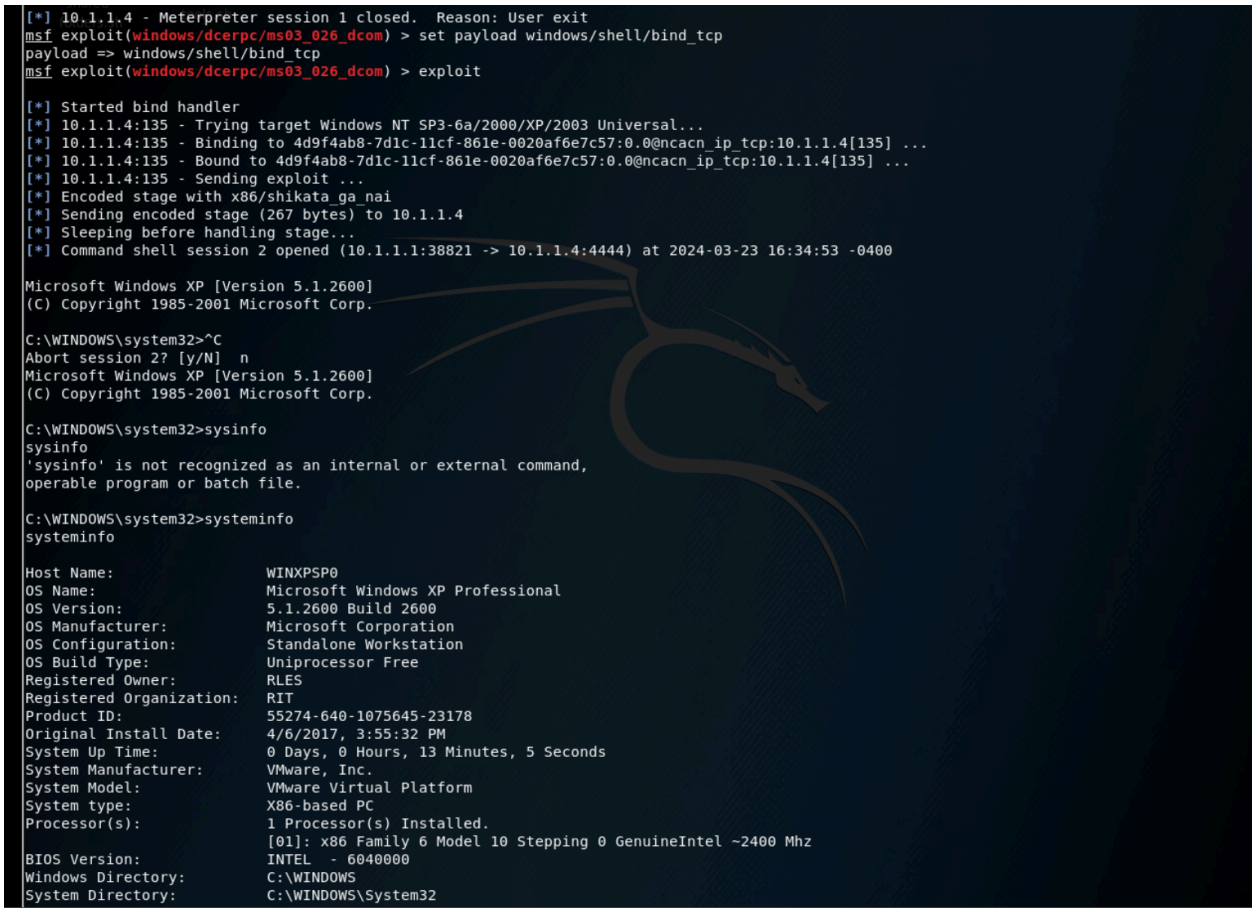
Step 5: I am setting my RHOSTS, which are the IP of my XP machine, and my LHOST, which is the IP of my Kali machine.



Step 6: I am searching for the payload, which is the reverse TCP one for building the reverse connection from XP to my Kali machine. And finally, I am trying to exploit it. Reverse TCP we will get the meterpreter session from the victim to our machine, which will help when there is a firewall on the Windows user's machine. Finally we got the meterpreter session we wanted.

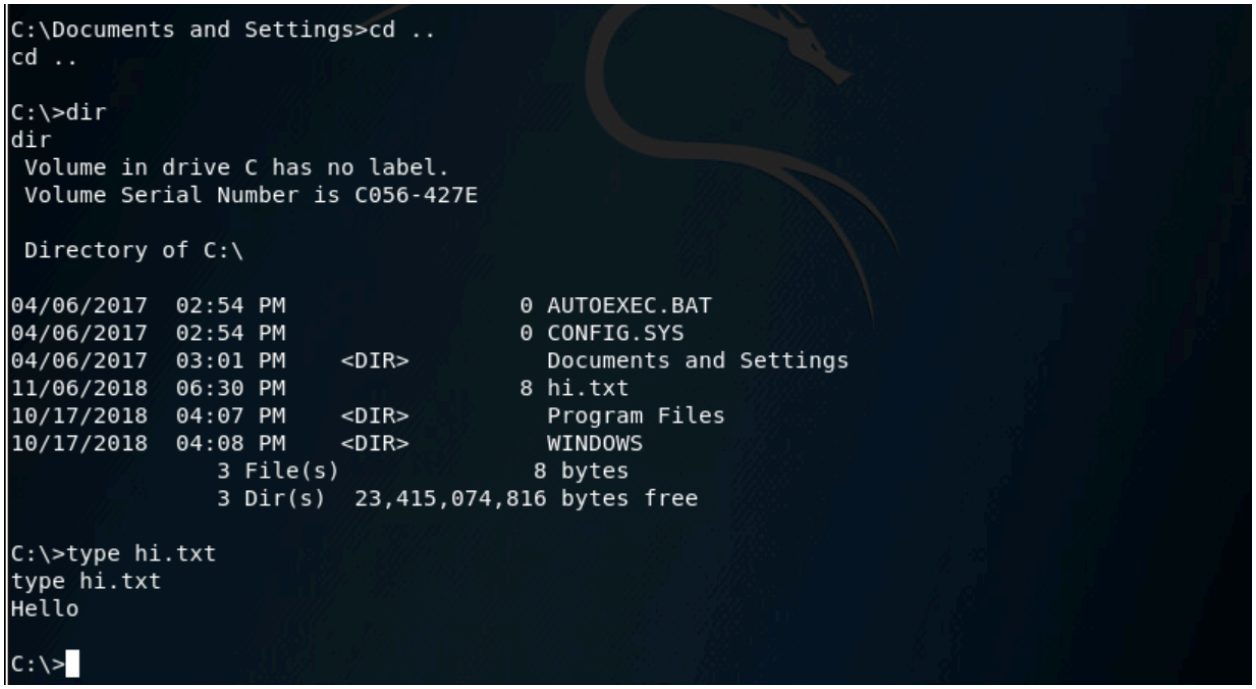


Step 7: Then I am trying to use the bind_tcp payload as the payload choice and trying to exploit. In this, we successfully got the session between the Windows and Kali machines. Socket shell connection was successfully created and we got full access to the Windows machine.



Using these two payloads, I was able to exploit XP and get the session back from the Windows machine.

Step 8 : While searching for any files in windows machine, I saw the text file in C folder which is hi.txt and its content is “hello”, we can see that in the below screenshot.



So we successfully exploited the windows machine and got the content we needed.