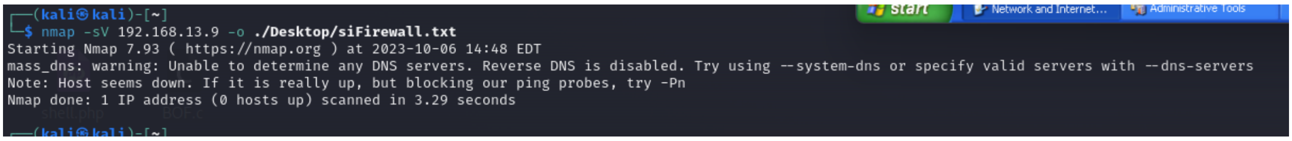
Con firewall disattivo, se eseguo un nmap da kali verso Windows, il risultato sarà

```
GNU                                   nano                                    7.2
noFirewall.txt

# Nmap 7.93 scan initiated Fri Oct  6 14:19:39 2023 as: nmap -sV -o ./Desktop/noFirewall.txt
192.168.13.9

mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
--system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.13.9

Host is up (0.00018s latency).

Not shown: 997 closed tcp ports (conn-refused)

PORT    STATE SERVICE      VERSION

135/tcp open  msrpc        Microsoft Windows RPC

139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn

445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .

# Nmap done at Fri Oct  6 14:19:46 2023 -- 1 IP address (1 host up) scanned in 7.50 seconds
```

Nessun log viene emesso dalla schermata logs per windows

Se invece attivo il firewall



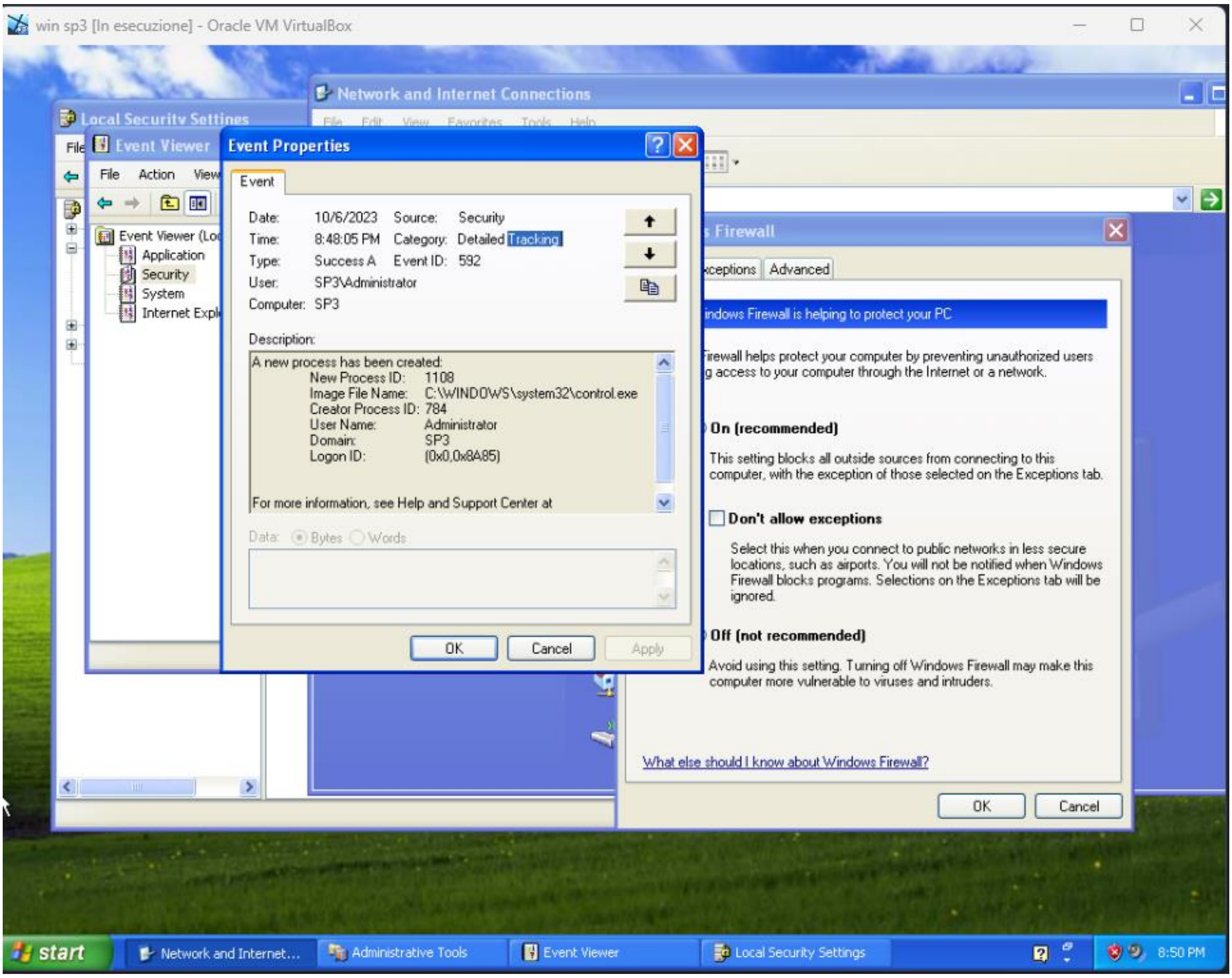
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.13.9 -o ./Desktop/siFirewall.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-06 14:48 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.29 seconds

┌──(kali㉿kali)-[~]
```

Per attivare i logs su windows

Start, Control Panel, Administrative Tools, Local Security Settings, Local Policies, Audit Policy, doppio click su audit logons events e spuntare success ed error

Start, Control Panel, Administrative Tools, Event Viewer per vedere i vari logs.

In questo caso notiamo che sono stati tentati delle azioni di *detail tracking,* bloccate dal firewall e loggate dal sistema



Date: 10/6/2023 Source: Security
Time: 8:48:05 PM Category: Detailed Tracking
Type: Success A Event ID: 592
User: SP3\Administrator
Computer: SP3

Description:

```
A new process has been created:
        New Process ID:     1108
        Image File Name:    C:\WINDOWS\system32\control.exe
        Creator Process ID: 784
        User Name:          Administrator
        Domain:             SP3
        Logon ID:           (0x0,0x8A85)

For more information, see Help and Support Center at
```

Data: ● Bytes ○ Words

indows Firewall is helping to protect your PC

irewall helps protect your computer by preventing unauthorized users g access to your computer through the Internet or a network.

On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?