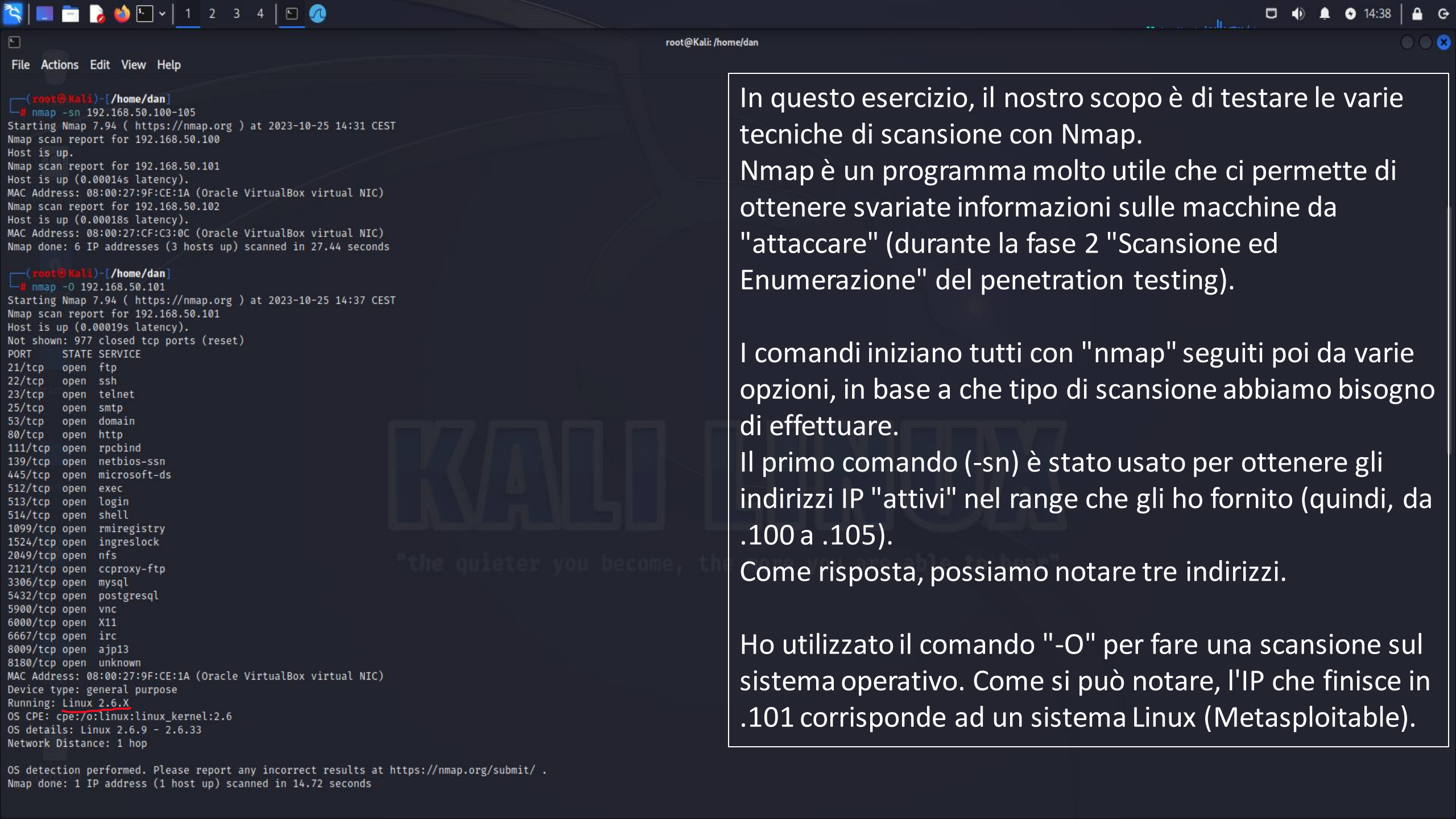
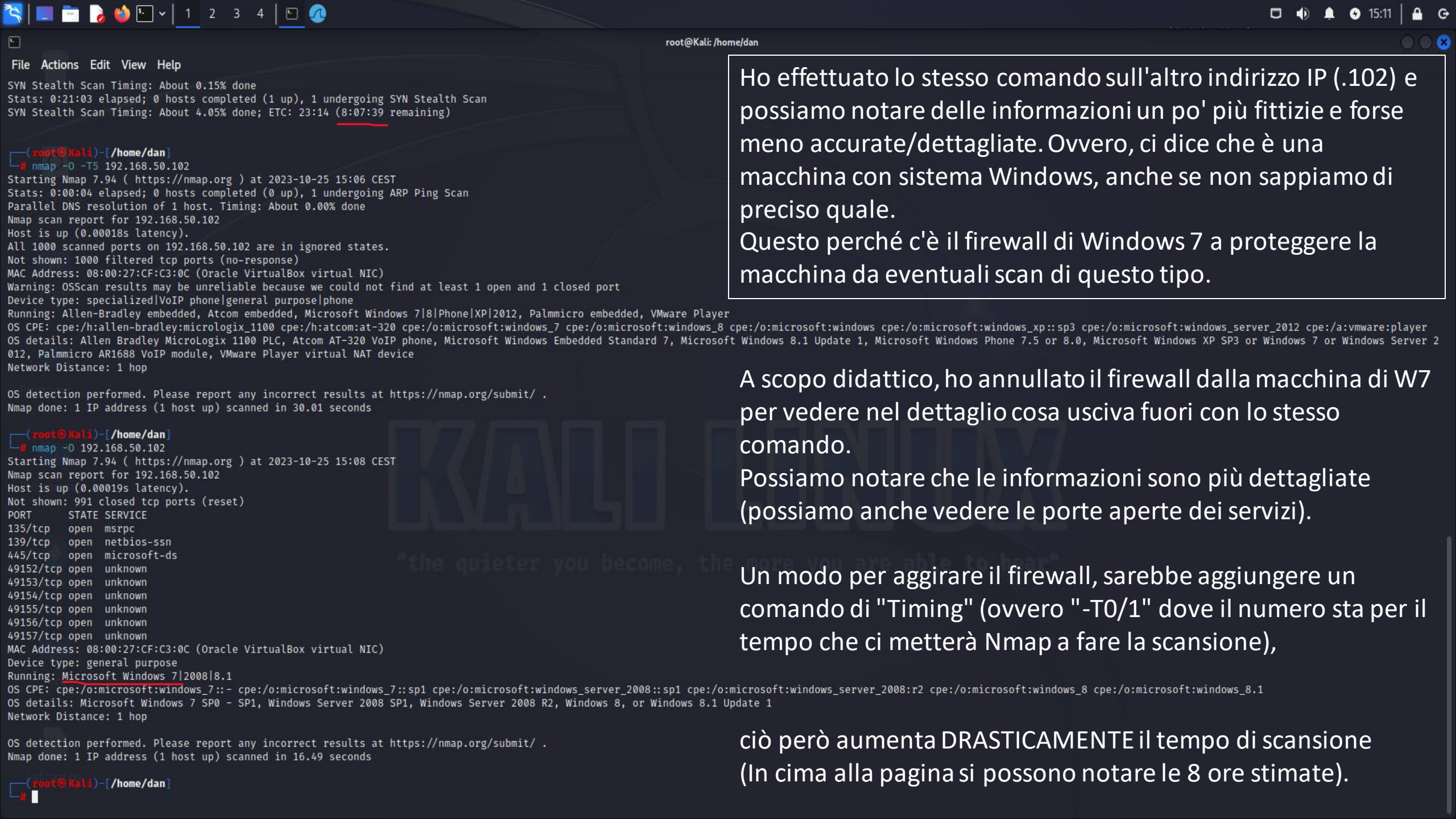


In questo esercizio, il nostro scopo è di testare le varie tecniche di scansione con Nmap.
Nmap è un programma molto utile che ci permette di ottenere svariate informazioni sulle macchine da "attaccare" (durante la fase 2 "Scansione ed Enumerazione" del penetration testing).

I comandi iniziano tutti con "nmap" seguiti poi da varie opzioni, in base a che tipo di scansione abbiamo bisogno di effettuare.
Il primo comando (-sn) è stato usato per ottenere gli indirizzi IP "attivi" nel range che gli ho fornito (quindi, da .100 a .105).
Come risposta, possiamo notare tre indirizzi.

Ho utilizzato il comando "-O" per fare una scansione sul sistema operativo. Come si può notare, l'IP che finisce in .101 corrisponde ad un sistema Linux (Metasploitable).



Ho effettuato lo stesso comando sull'altro indirizzo IP (.102) e possiamo notare delle informazioni un po' più fittizie e forse meno accurate/dettagliate. Ovvero, ci dice che è una macchina con sistema Windows, anche se non sappiamo di preciso quale.
Questo perché c'è il firewall di Windows 7 a proteggere la macchina da eventuali scan di questo tipo.

A scopo didattico, ho annullato il firewall dalla macchina di W7 per vedere nel dettaglio cosa usciva fuori con lo stesso comando.
Possiamo notare che le informazioni sono più dettagliate (possiamo anche vedere le porte aperte dei servizi).

Un modo per aggirare il firewall, sarebbe aggiungere un comando di "Timing" (ovvero "-T0/1" dove il numero sta per il tempo che ci metterà Nmap a fare la scansione),

ciò però aumenta DRASTICAMENTE il tempo di scansione
(In cima alla pagina si possono notare le 8 ore stimate).

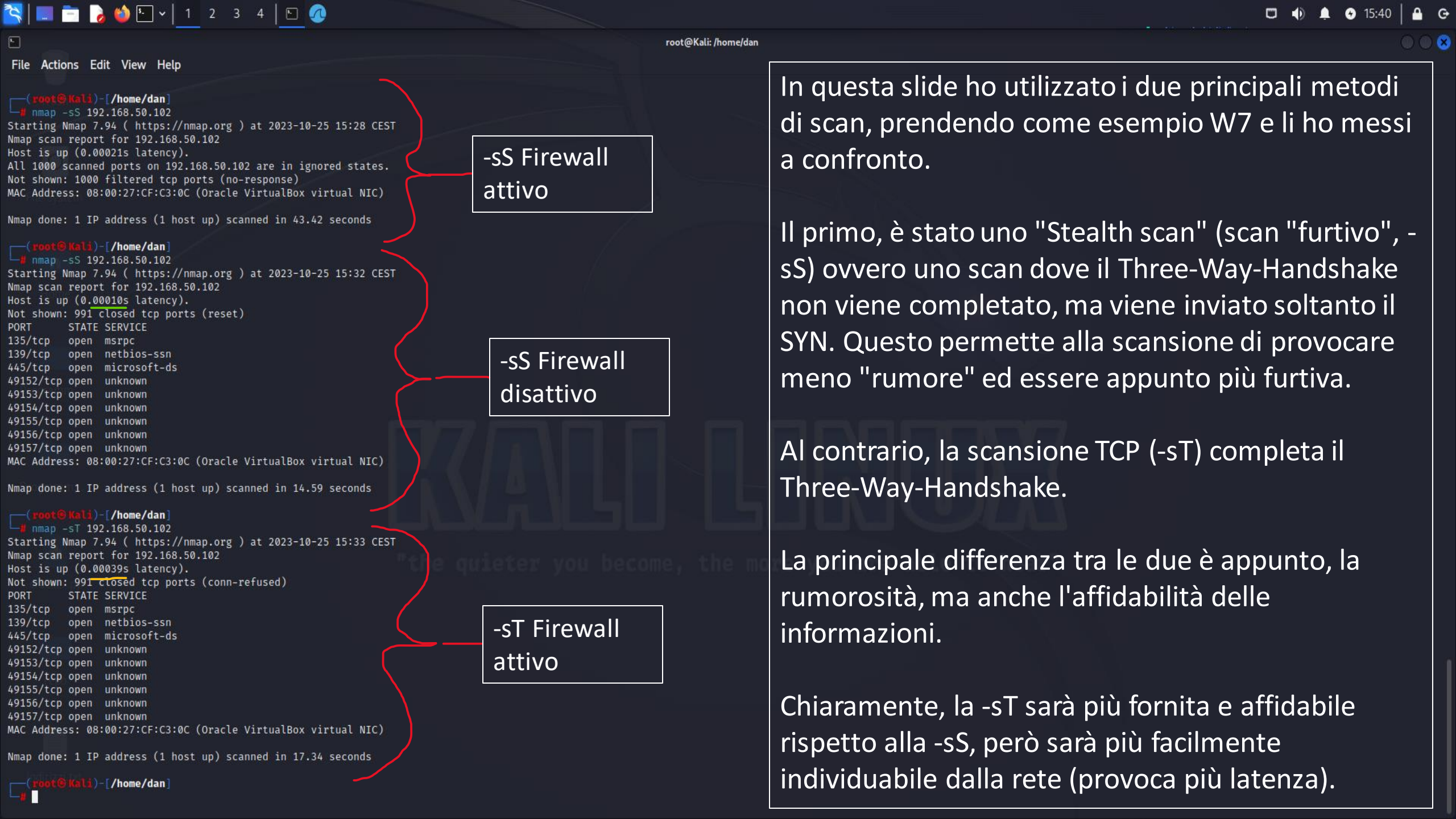
root@Kali: /home/dan

File Actions Edit View Help

```
Nmap scan report for 192.168.50.101
Host is up (0.00011s latency).
Not shown: 977 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  shell       Netkit rshd
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:9F:CE:1A (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 65.96 seconds

┌──(root㉿Kali)-[/home/dan]
└─#

┌──(root㉿Kali)-[/home/dan]
└─# nmap -sV 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:24 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00017s latency).
Not shown: 991 closed tcp ports (reset)
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:CF:C3:0C (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Qui ho utilizzato il comando "-sV" per scansionare in dettaglio le varie versioni delle porte e dei servizi attivi sulla macchina target.

Si può notare il sistema operativo della macchina in fondo alla lista (sezione "Service info:").



In questa slide ho utilizzato i due principali metodi di scan, prendendo come esempio W7 e li ho messi a confronto.

Il primo, è stato uno "Stealth scan" (scan "furtivo", -sS) ovvero uno scan dove il Three-Way-Handshake non viene completato, ma viene inviato soltanto il SYN. Questo permette alla scansione di provocare meno "rumore" ed essere appunto più furtiva.

Al contrario, la scansione TCP (-sT) completa il Three-Way-Handshake.

La principale differenza tra le due è appunto, la rumorosità, ma anche l'affidabilità delle informazioni.

Chiaramente, la -sT sarà più fornita e affidabile rispetto alla -sS, però sarà più facilmente individuabile dalla rete (provoca più latenza).

root@Kali: /home/dan

File Actions Edit View Help

```
┌──(root㉿Kali)-[/home/dan]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:25 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00016s latency).
Not shown: 977 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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:9F:CE:1A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds

┌──(root㉿Kali)-[/home/dan]
└─# nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:26 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00040s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
```

Stessa cosa accade per Metasploitable, semplicemente non abbiamo un firewall da aggirare.

Anche qui possiamo notare la differenza in latenza (seppur millimesimale), tra le due metodologie di scan.