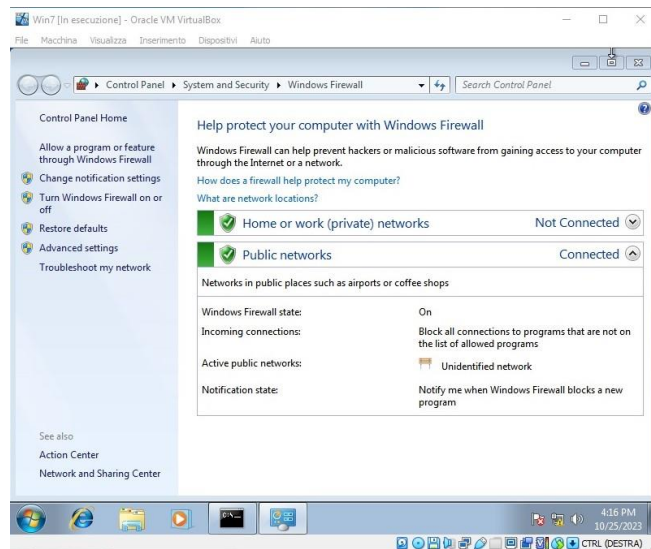


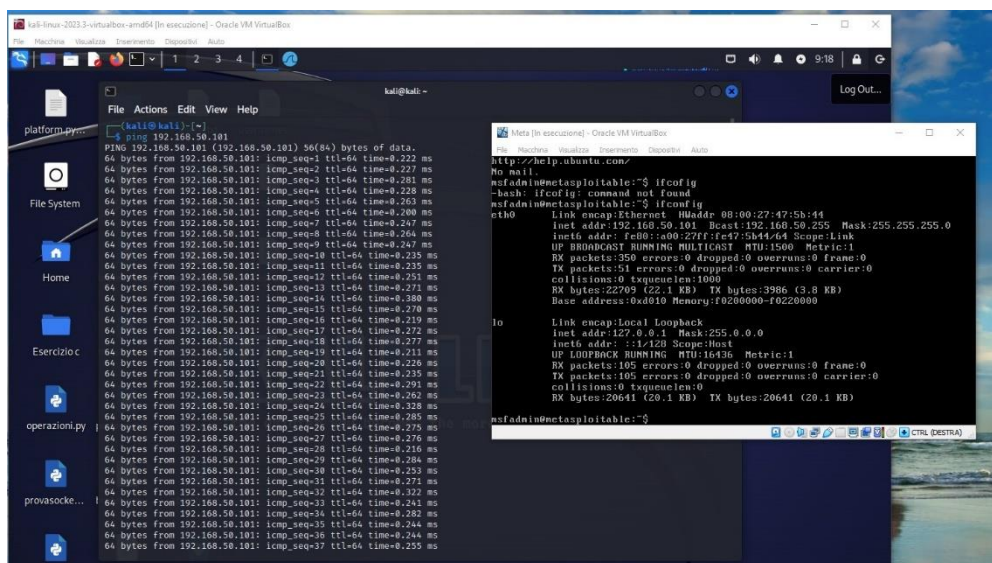
Esercitazione 25/10/2023

Nell'esercizio odierno ci viene richiesto di effettuare delle scansioni sui target Metasploitable e Win7

Per cominciare preciso di aver disattivato il firewall da Win7 poiché mi bloccava la richiesta

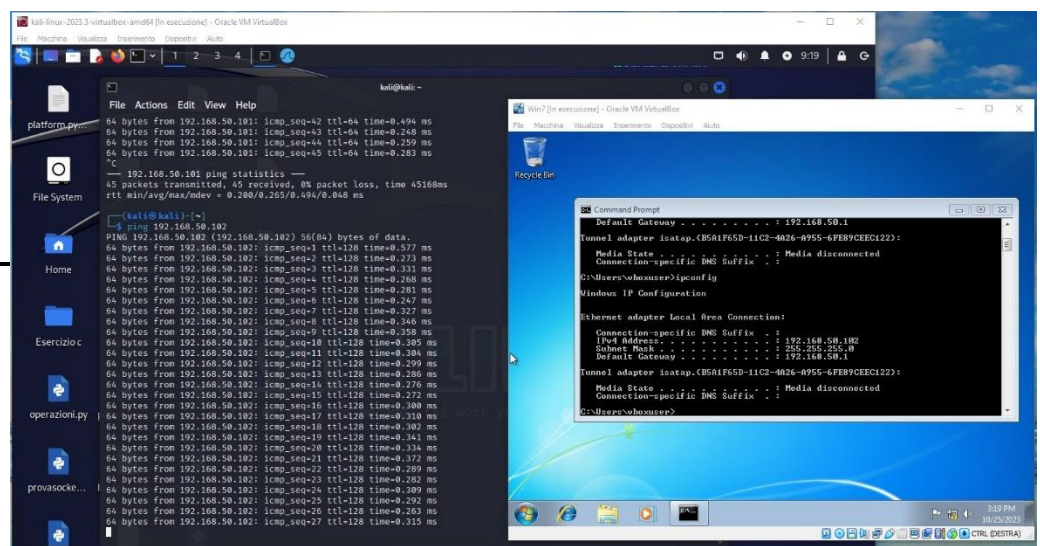


Dopo di ciò ho controllato che le macchine pingassero correttamente (100 Kali – 101 Meta – 102 Win7)



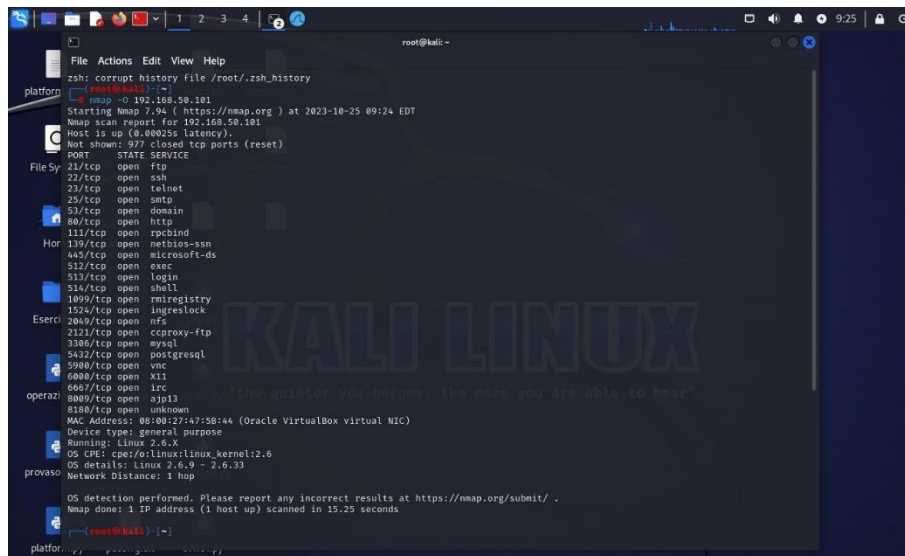
Meta

Win 7



OS fingerprint (l'unico che viene richiesto di effettuare su entrambe le macchine)

Il sistema operativo viene rilevato attraverso il comando nmap -O ip



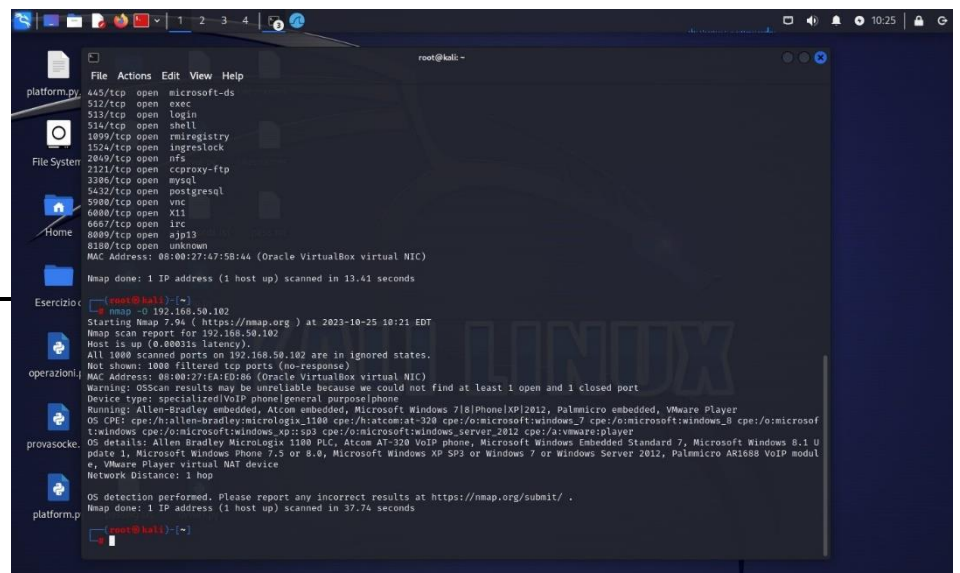
Meta

Ha rilevato il sistema operativo Linux

Win 7

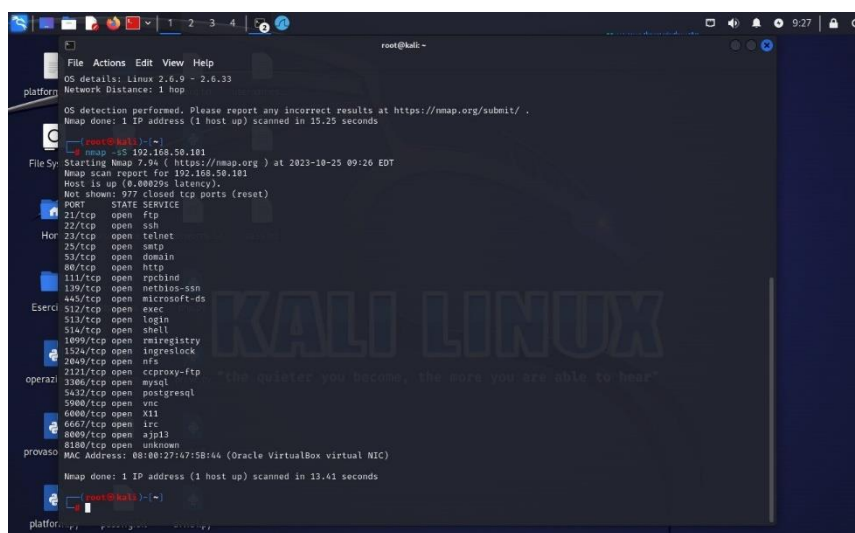
Ha rilevato il sistema operativo

Windows (stranamente varie versioni)



Syn Scan

Il Syn Scan viene rilevato dal comando nmap -sS ipe e mi da la possibilità di rilevare le porte e sapere se sono aperte



TCP Connect

La TCP è il cosiddetto “Three-way-handshake”, la stretta di mano a tre vie (syn – syn akt – akt), quella che ci permette di vedere porte e protocolli che girano in un dispositivo e ne attende la risposta.

Avviene tramite il comando `nmap -sT ip`

```

root@kali: ~
File Actions Edit View Help
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EA:ED:86 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.50.100
Host is up (0.000011s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 110 IP addresses (3 hosts up) scanned in 34.75 seconds

root@kali: ~
root@kali: ~# nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 09:59 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00055s 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
113/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
8089/tcp	open	ajp13
8189/tcp	open	unknown

```

MAC Address: 08:00:27:47:5B:44 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds

root@kali: ~#

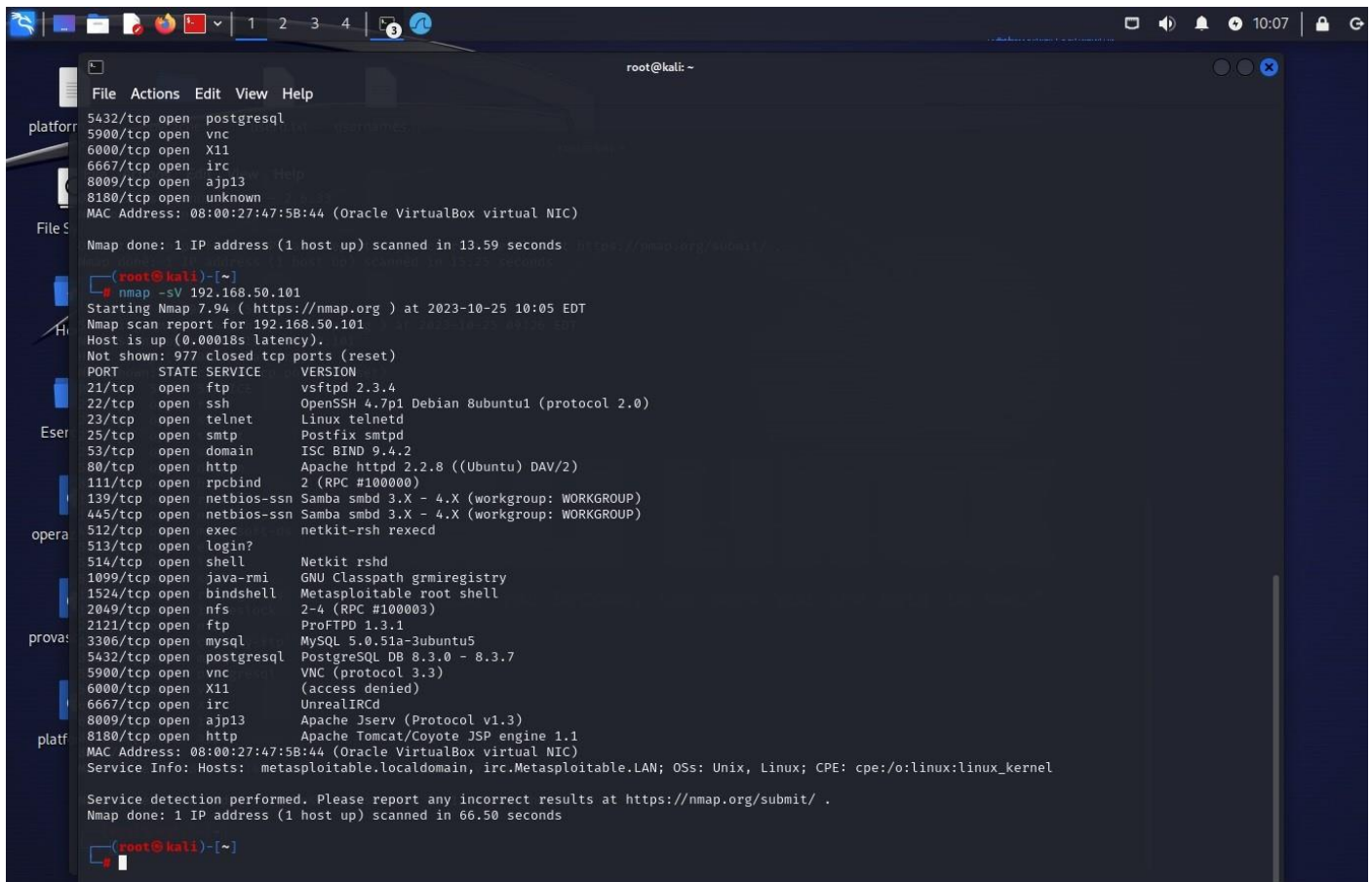
```

La differenza con il Syn scan è semplicemente nella latenza, TCP connect, essendo più completa, più affidabile e più invasiva è anche più lenta. Di seguito il confronto

The image displays two terminal windows from a Kali Linux system. The left window shows an Nmap scan of 192.168.50.101, identifying it as a host up with 977 closed TCP ports. The right window shows an Nmap scan of 192.168.50.100, identifying it as a host up with 110 IP addresses scanned (3 hosts up). Both scans were performed using Nmap 7.94. The terminal windows are titled 'root@kali: ~' and show the command prompt '#'. The background of the terminal windows features a Kali Linux logo and the text 'the quieter you become'.

Version Detection

Il Version detection ci da il banner che ci indica la versione corrente del sistema e si avvia con il comando nmap -sV ip



```
root@kali: ~  
File Actions Edit View Help  
platform 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: 08:00:27:47:5B:44 (Oracle VirtualBox virtual NIC)  
File S Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds (https://nmap.org/xkbs)  
root@kali: ~  
# nmap -sV 192.168.50.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 10:05 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00018s 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: 08:00:27:47:5B:44 (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 66.50 seconds  
root@kali: ~
```