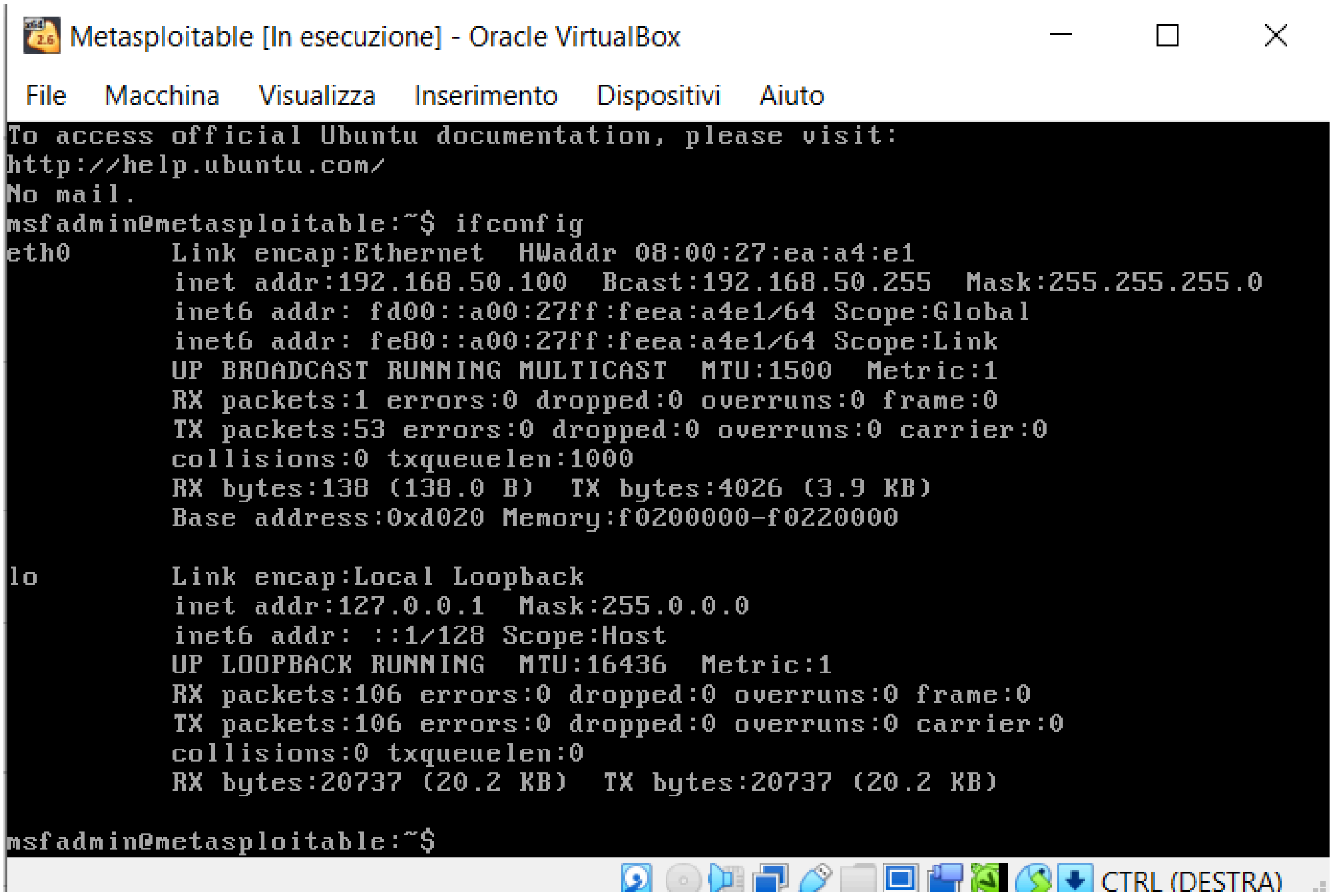
S5L2-nMap

Oggi useremo uno strumento molto potente, ovvero, nmap, che opererà come Scanner di rete, Scanner di host, Identificatore di servizi, e rilevatore di sistemi operativi scansionando anche le vulnerabilità

Come macchina cavia useremo metasploitable, dover l'IP è 192.168.50.100:

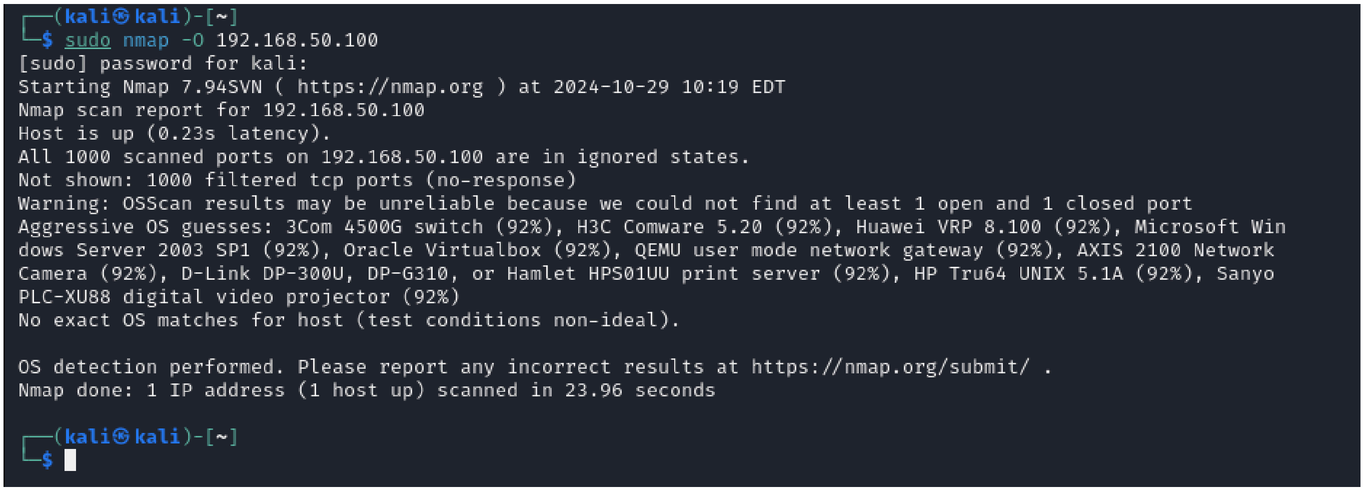

Metasploitable [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ea:a4:e1
          inet addr:192.168.50.100  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fd00::a00:27ff:feea:a4e1/64 Scope:Global
          inet6 addr: fe80::a00:27ff:feea:a4e1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:138 (138.0 B)  TX bytes:4026 (3.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20737 (20.2 KB)  TX bytes:20737 (20.2 KB)

msfadmin@metasploitable:~$
```

1) OS FingerPrint, tramite questo tipo di scansione andremo a visualizzare tutte le informazioni essenziali del sistema che andiamo a scansionare e le porte aperte e chiuse:

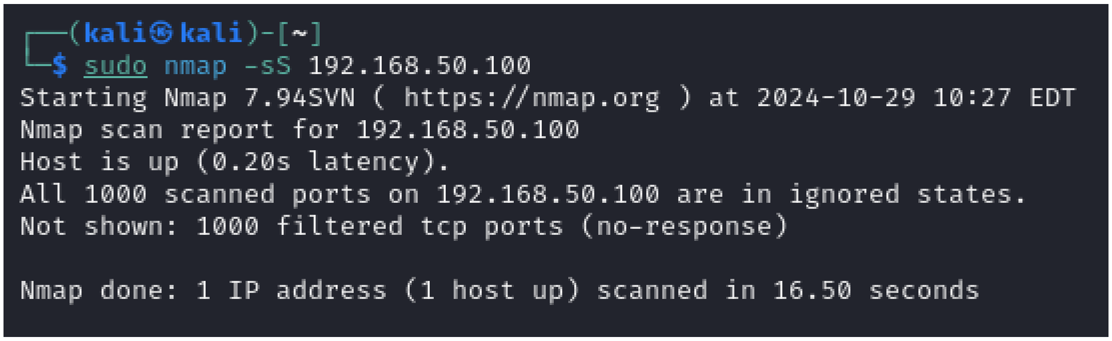


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:19 EDT
Nmap scan report for 192.168.50.100
Host is up (0.23s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%), Microsoft Win
dows Server 2003 SP1 (92%), Oracle Virtualbox (92%), QEMU user mode network gateway (92%), AXIS 2100 Network
Camera (92%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU print server (92%), HP Tru64 UNIX 5.1A (92%), Sanyo
PLC-XU88 digital video projector (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.96 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

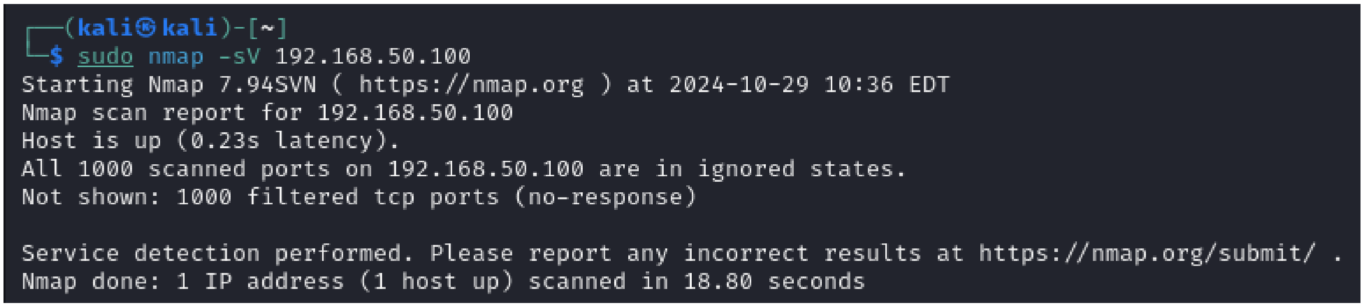
2) **Scan SYN**, tramite il comando **"sudo nmap -sS"**, possiamo identificare le porte aperte in modo più discreto, simulando richieste TCP SYN senza però completare il processo di connessione.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:27 EDT
Nmap scan report for 192.168.50.100
Host is up (0.20s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 16.50 seconds
```

3) **Version Detection**, grazie al comando **"-sV"**, vediamo quali sono le porte aperte sull'indirizzo che andiamo a scannerizzare. Ma cerca anche di stabilirci una connessione.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:36 EDT
Nmap scan report for 192.168.50.100
Host is up (0.23s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.80 seconds
```