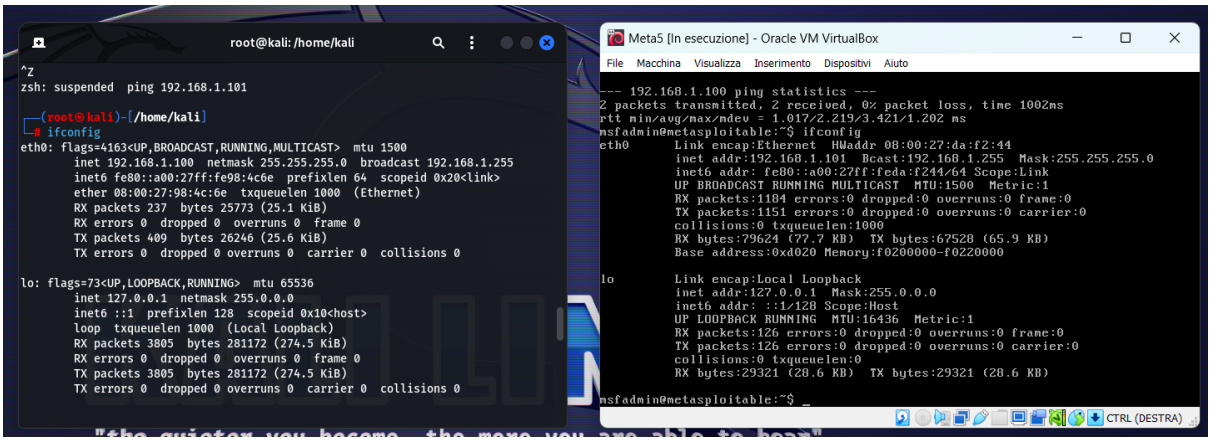
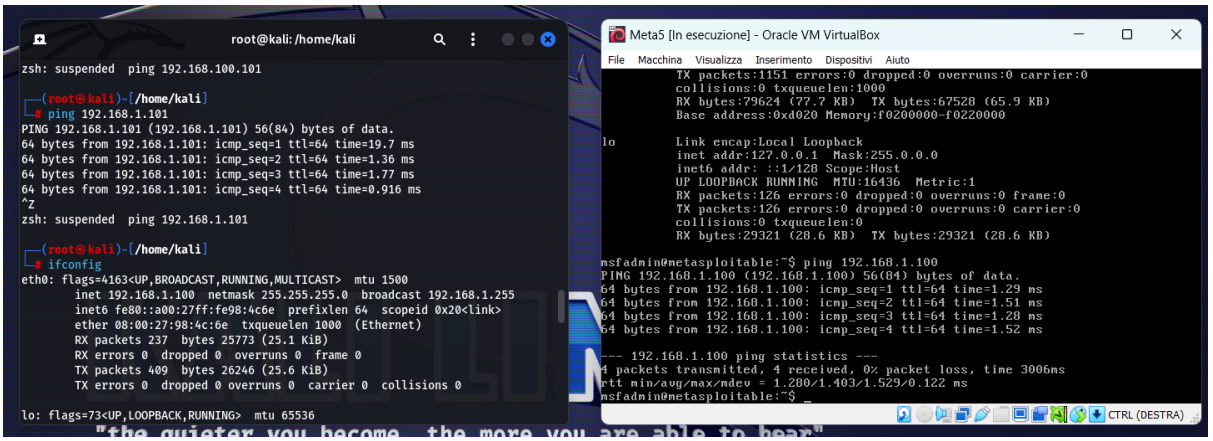
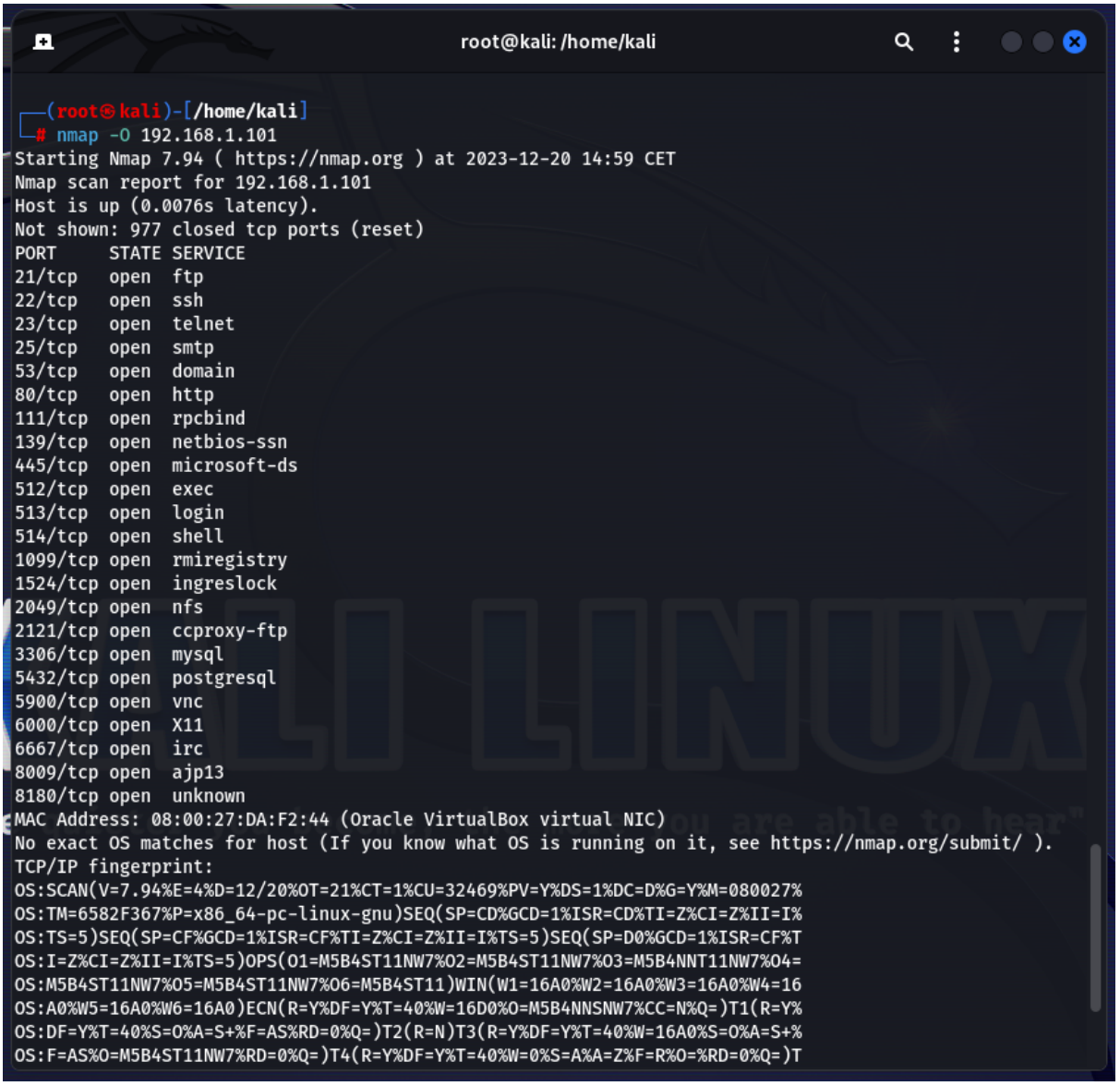
CONSEGNA S5/L3

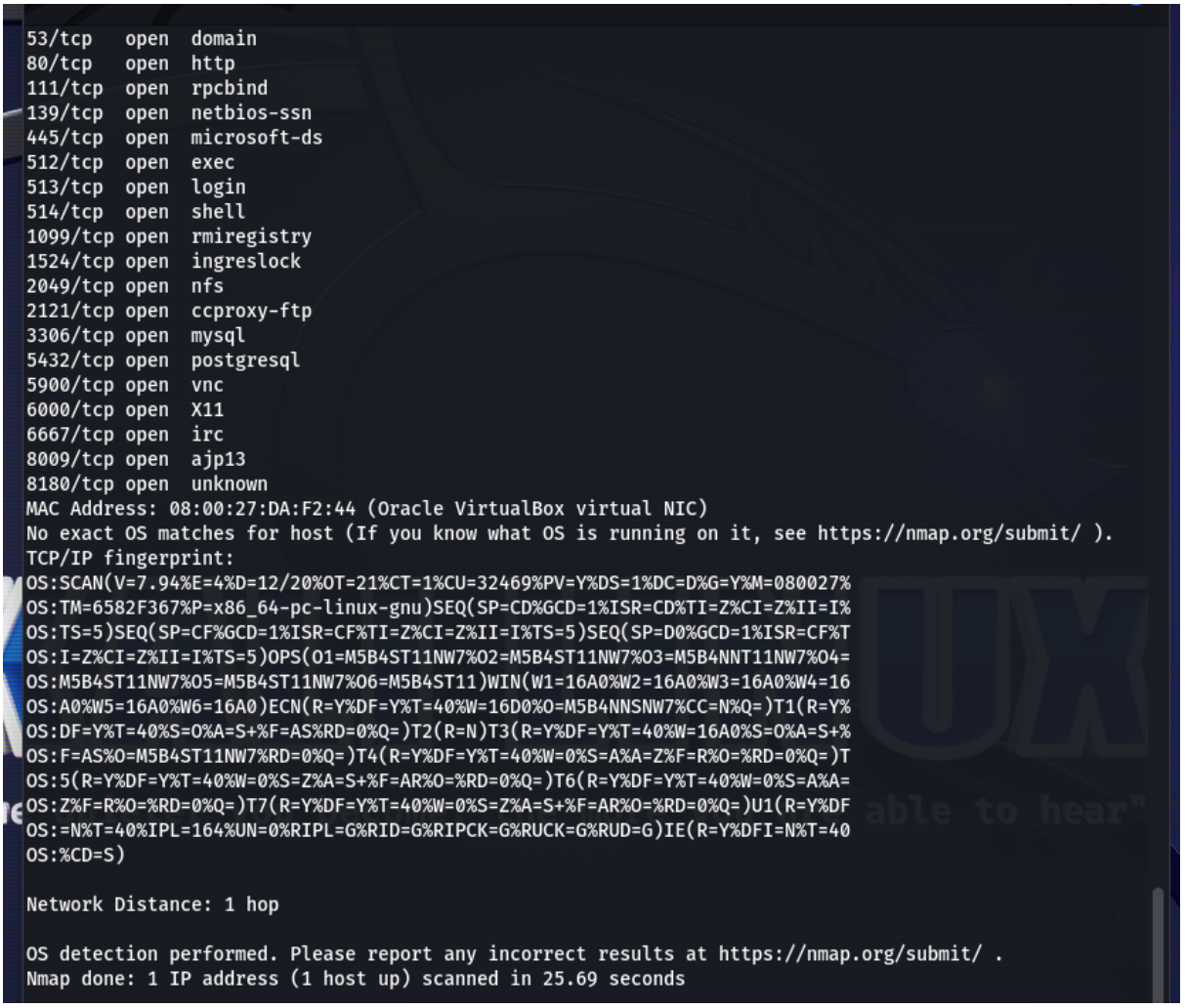


Kali Linux e Metasploitable sono sulla stessa rete

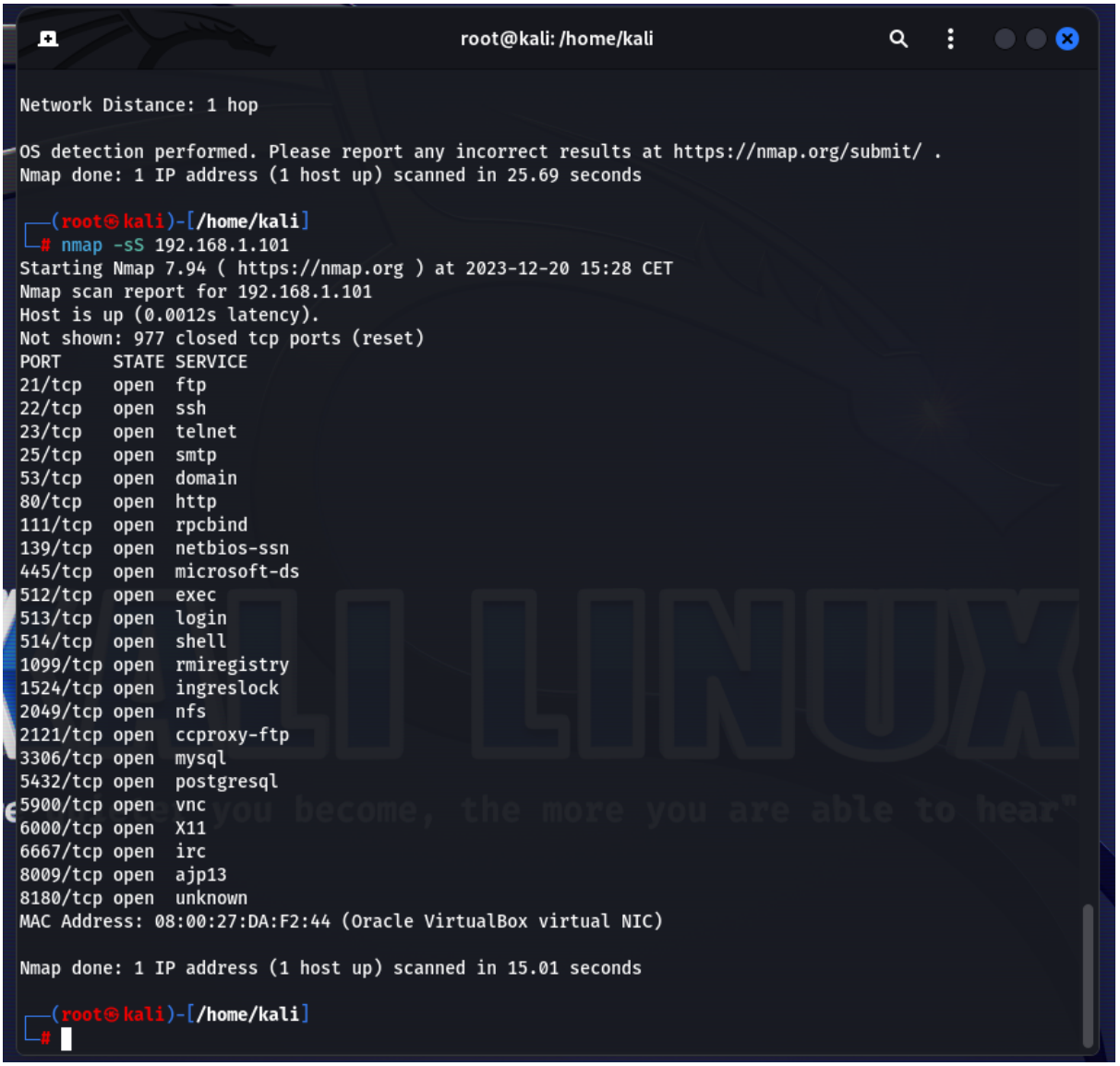


Le due macchine pingano correttamente

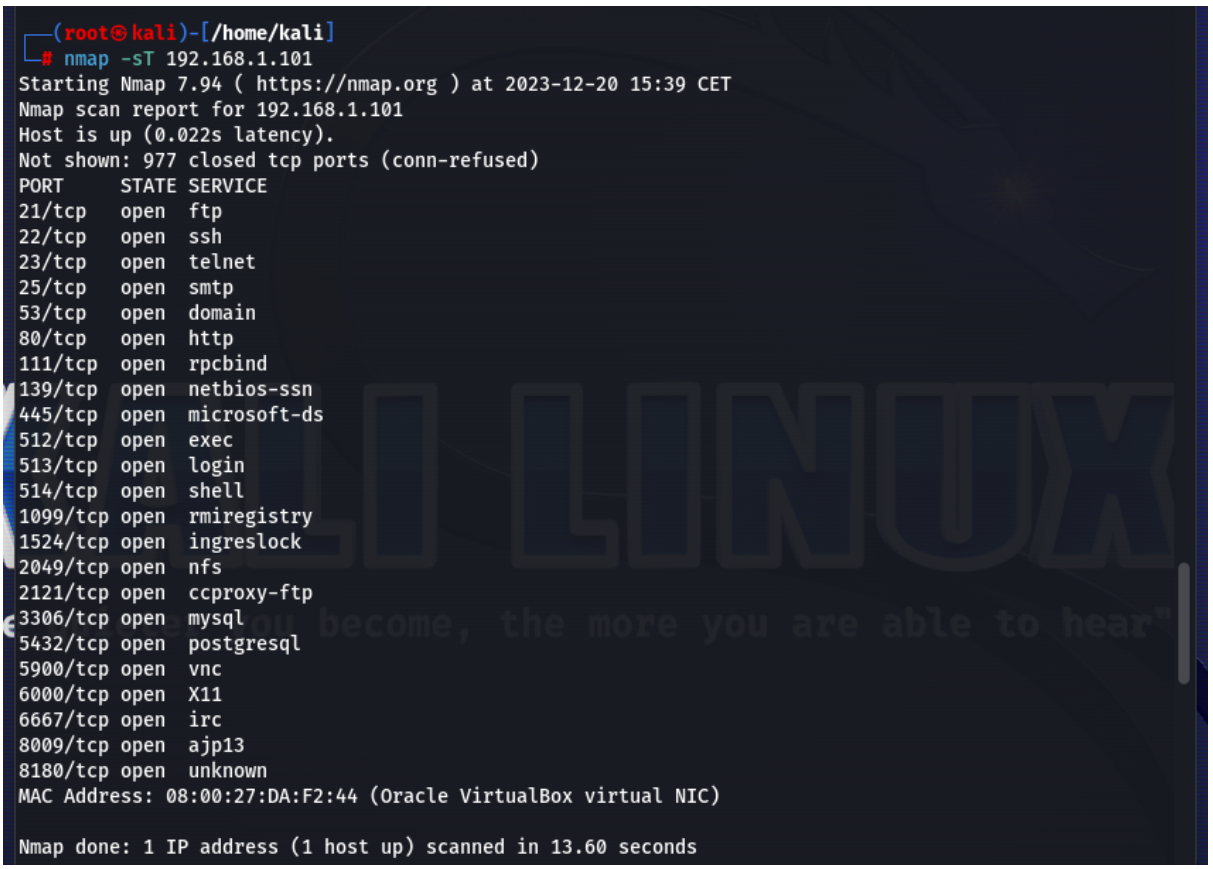

root@kali: /home/kali
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.101
Starting Nmap 7.94 (https://nmap.org) at 2023-12-20 14:59 CET
Nmap scan report for 192.168.1.101
Host is up (0.0076s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp 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:DA:F2:44 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=12/20%OT=21%CT=1%CU=32469%PV=Y%DS=1%DC=D%G=Y%M=080027%
OS:TM=6582F367%P=x86_64-pc-linux-gnu)SEQ(SP=CD%GCD=1%ISR=CD%TI=Z%CI=Z%II=I%
OS:TS=5)SEQ(SP=CF%GCD=1%ISR=CF%TI=Z%CI=Z%II=I%TS=5)SEQ(SP=D0%GCD=1%ISR=CF%T
OS:I=Z%CI=Z%II=I%TS=5)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=
OS:M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16
OS:A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW7%CC=N%Q=)T1(R=Y%
OS:DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%
OS:F=AS%O=M5B4ST11NW7%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T



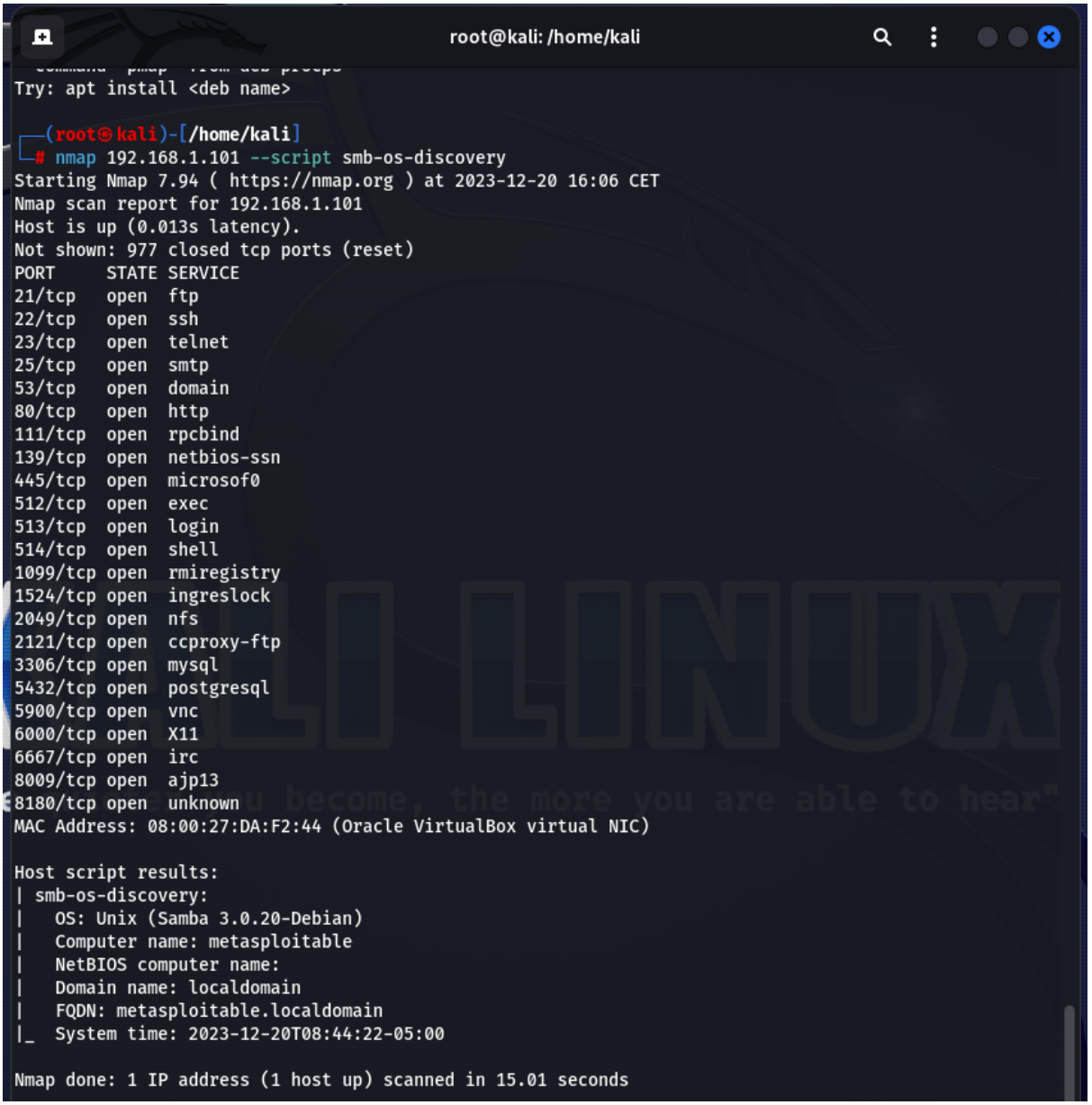
OS Fingerprint su Metasploitable



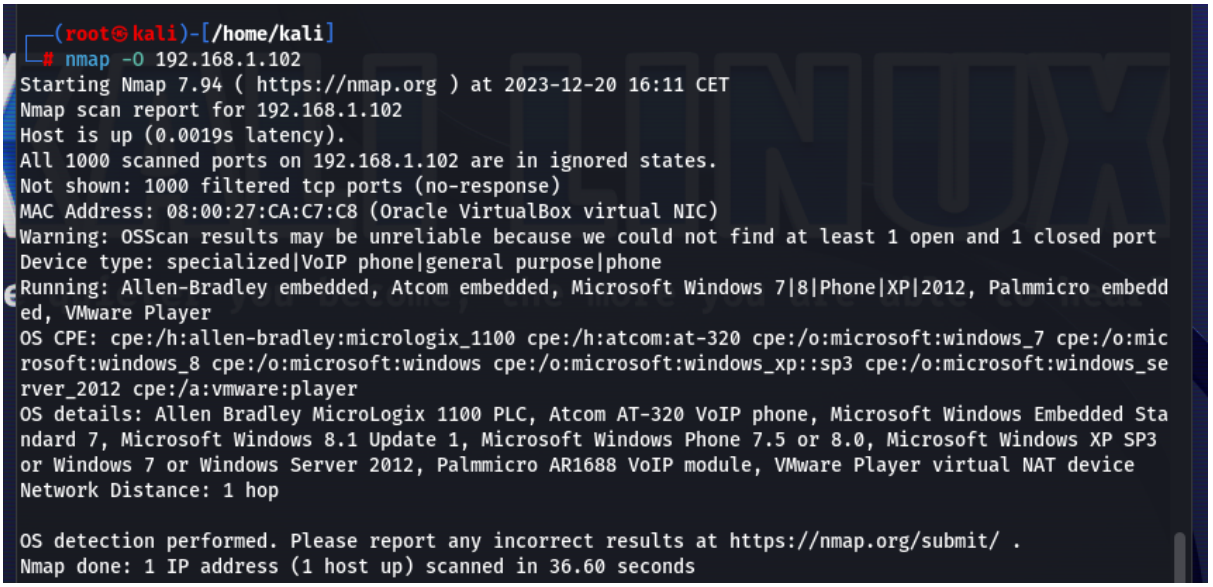
SYN Scan su Metasploitable



TCP Scan su Metasploitable



Version detection su Metasploitable



OS Fingerprint su Windows 7