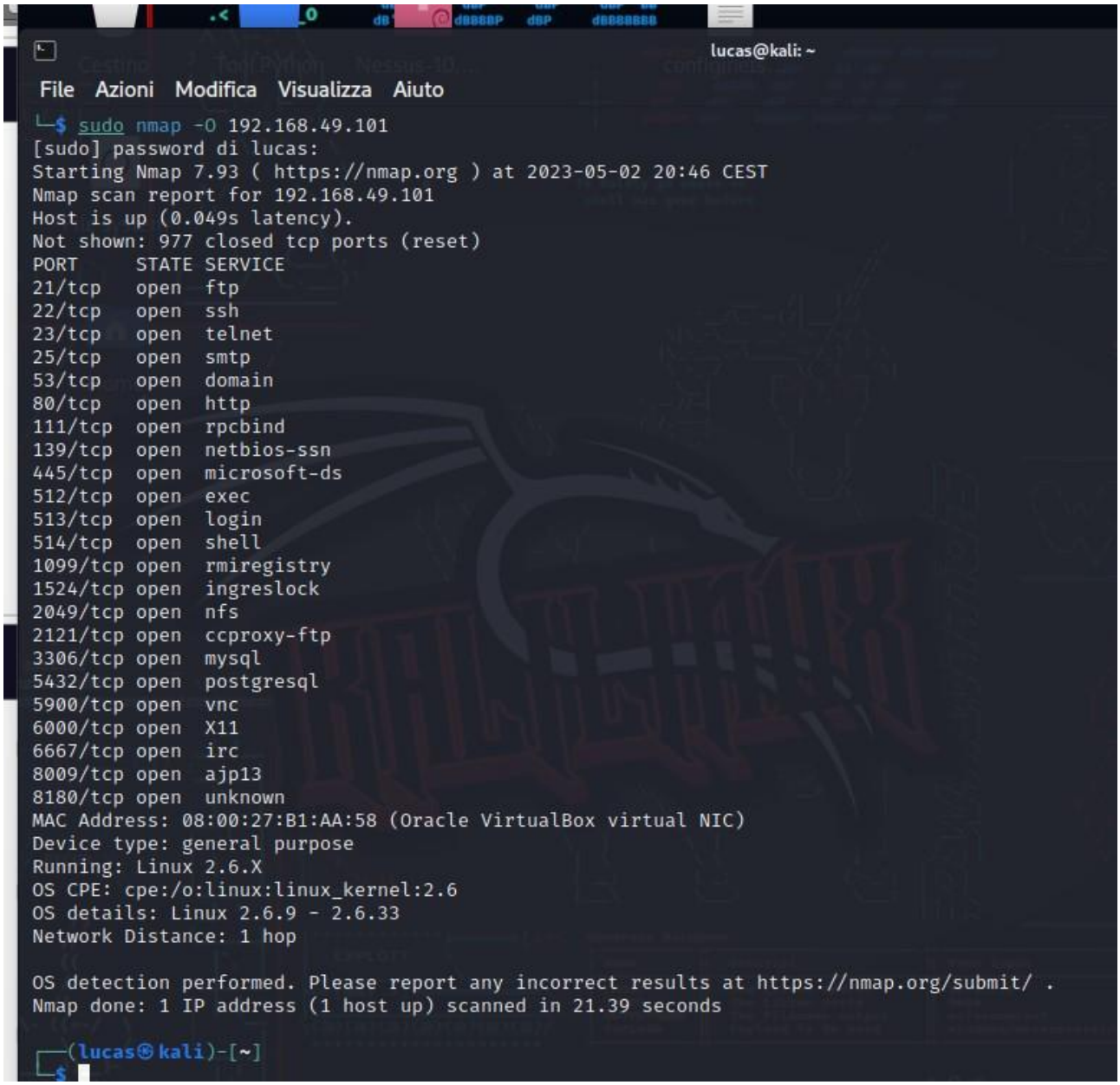
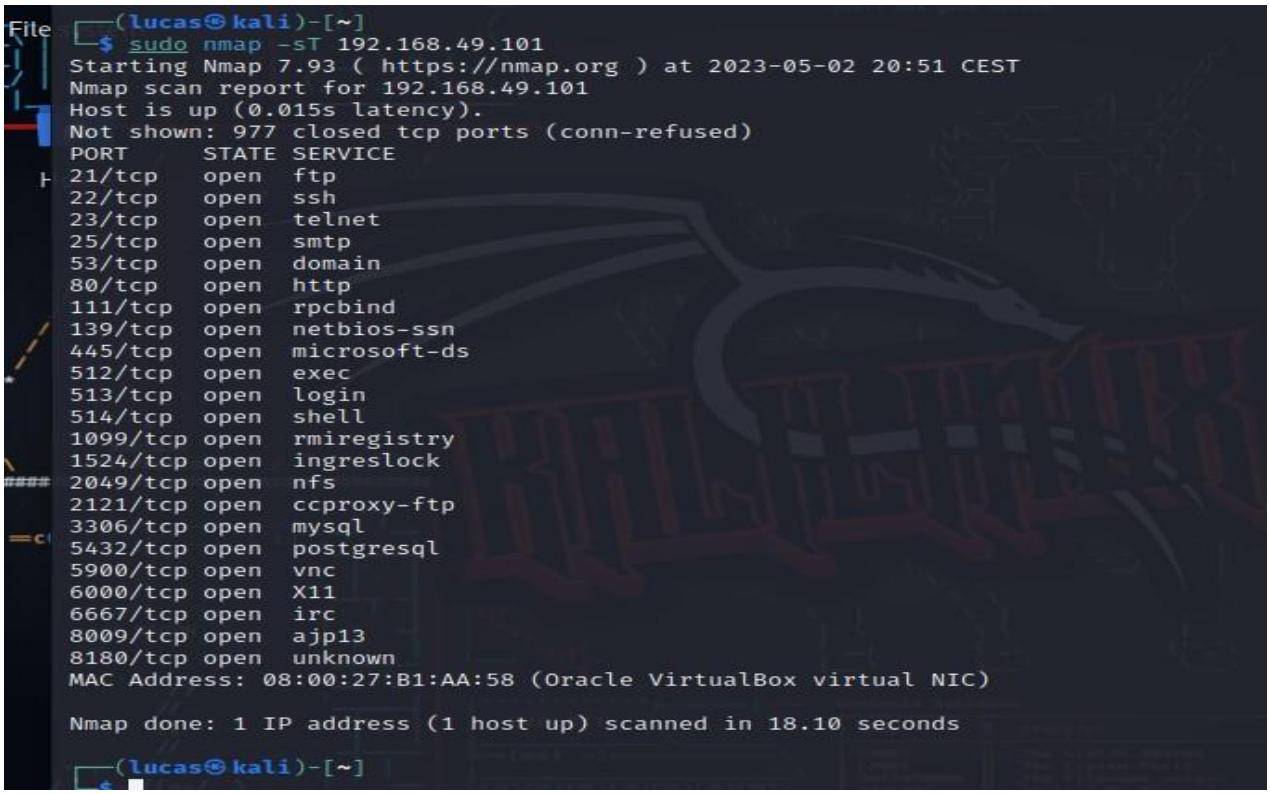
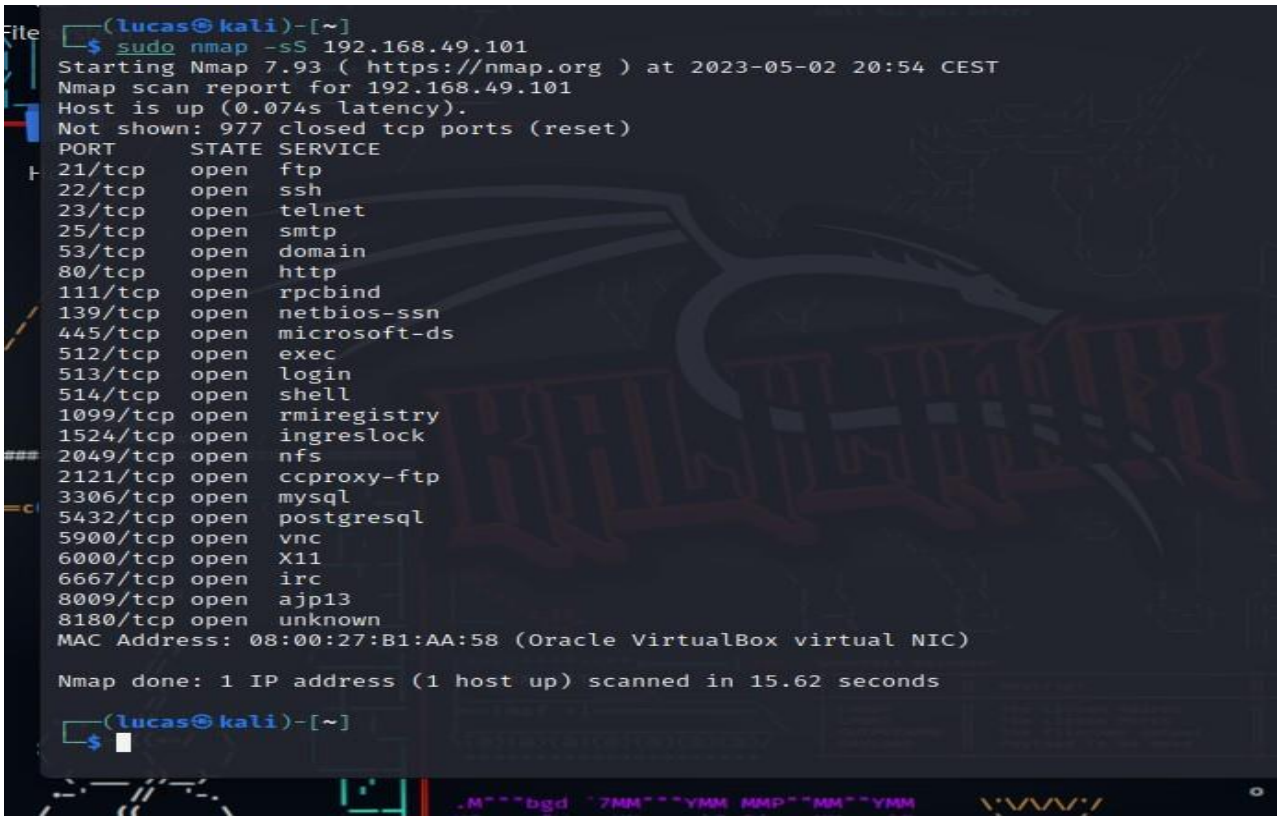
OS FINGERPRINT di META,



SCAN con TCP connect

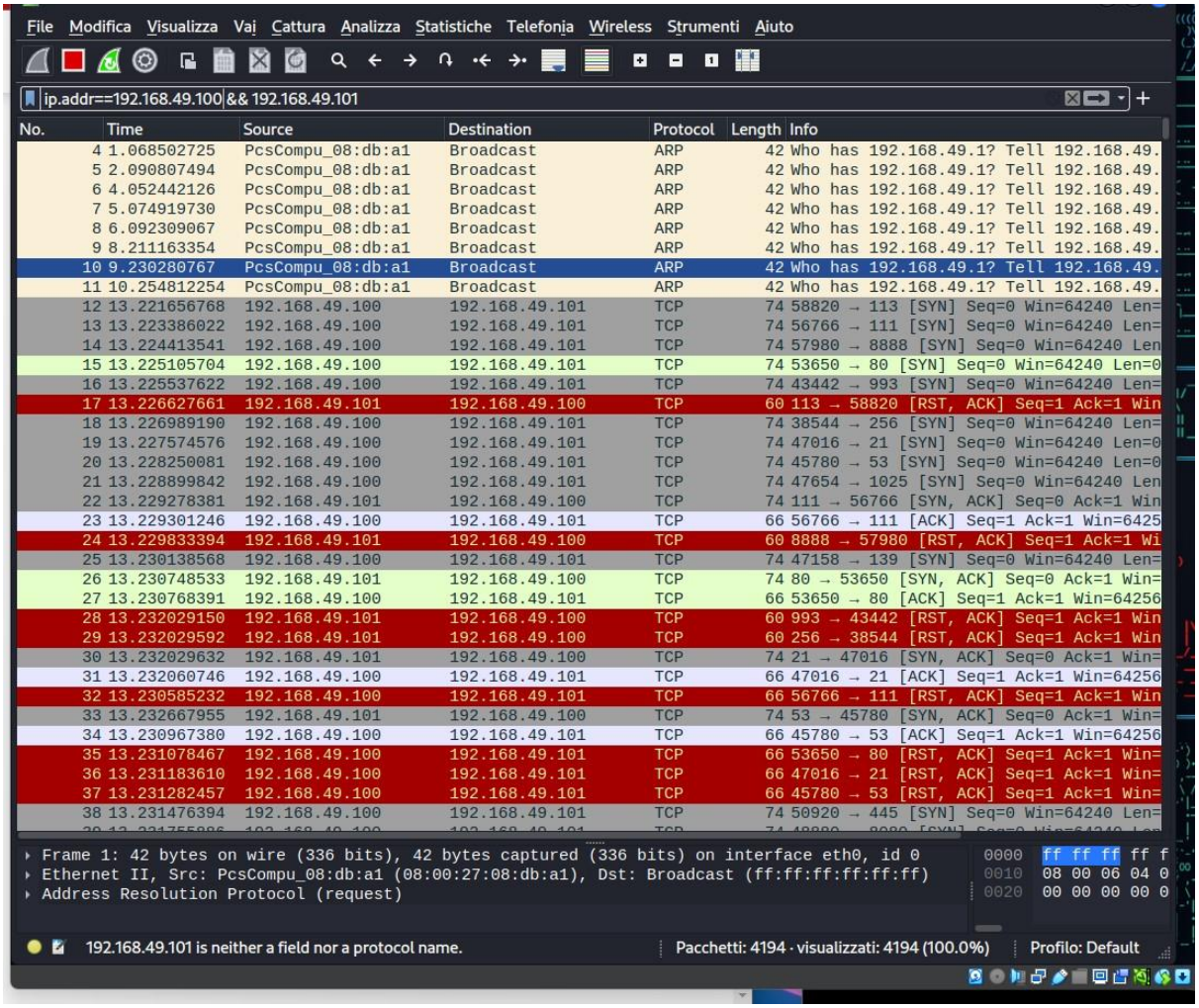


SCAN DI SOLO SYN

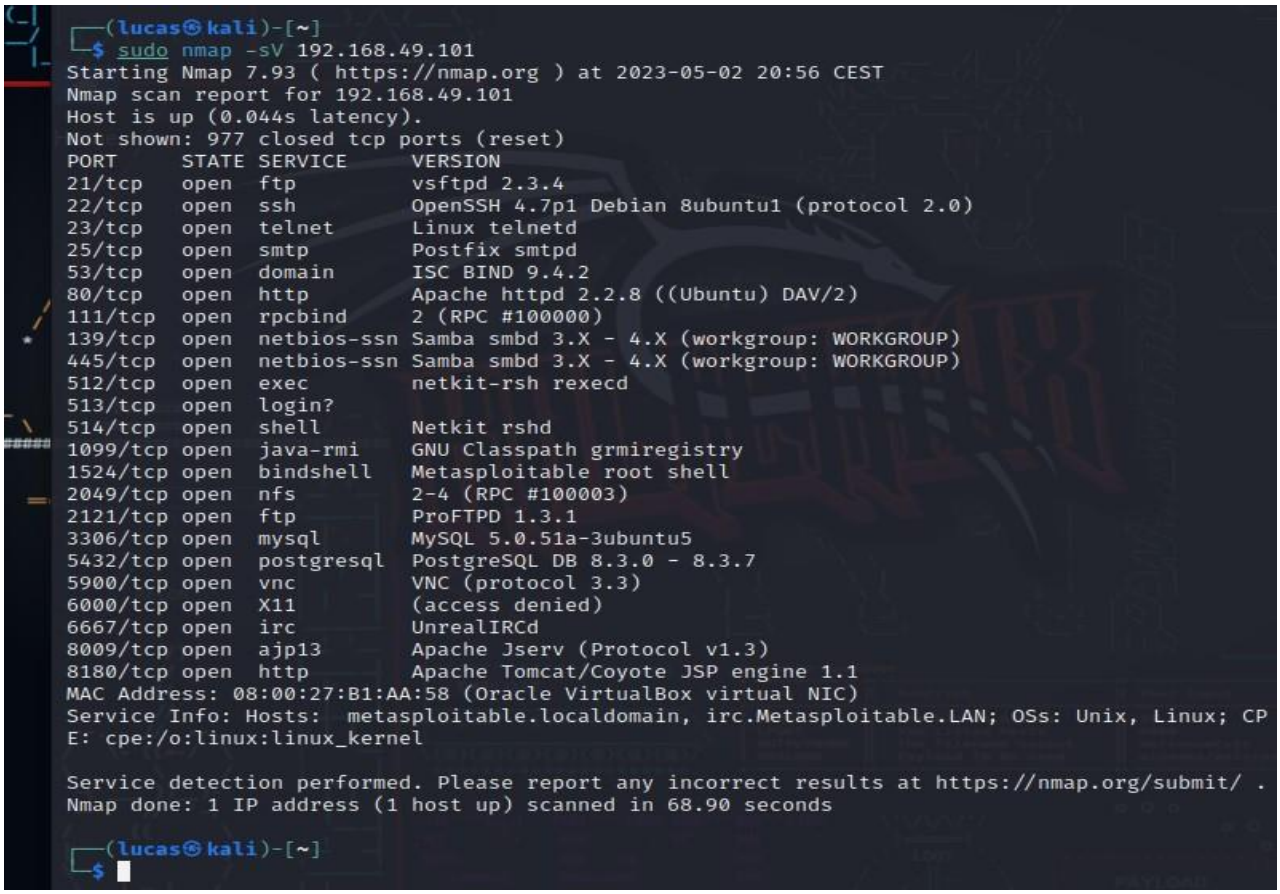


La differenza tra le due scansione è:

TCP connect(-sT) stabilisce una connessione con il demone del servizio in ascolto, completando il 3-way-handshake (SYN-SYN/ACK-ACK), quindi la porta è aperta, invece lo Scan SYN(-sS) è una scansione furtiva in quanto non stabilisce una connessione completa con il demone in target (SYN-RST/ACT) non completa il 3-way-handshake in questo caso la porta risulta chiusa.



VERSION DETECTION



Report essenziale per identificare dati sensibili:

Nmap 7.93 scan initiated Tue May 2 21:36:37 2023 as: nmap -sV -oN report2 192.168.49.101

Nmap scan report for 192.168.49.101

Host is up (0.65s 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

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o: linux: linux_kernel

Nmap done at Tue May 2 21:37:48 2023 -- 1 IP address (1 host up) scanned in 71.30 seconds

ABBIAMO IP, PORTE APERTE SERVIZI IN CUI POSSIAMO TENTARE DELLE VULNERABILITA CON DEGLI EXPLOIT TIPO SAMBA, APACHE ECC., E POSSIAMO VEDERE IL SISTEMA OPERATIVO CON LE VERSIONI ATTUALI.