# REPORT
# W11-D2
# NMAP SCAN

INFORMAZIONI
RICAVATE DALLO
SCAN DELL'HOST

# Informazioni sull'host:

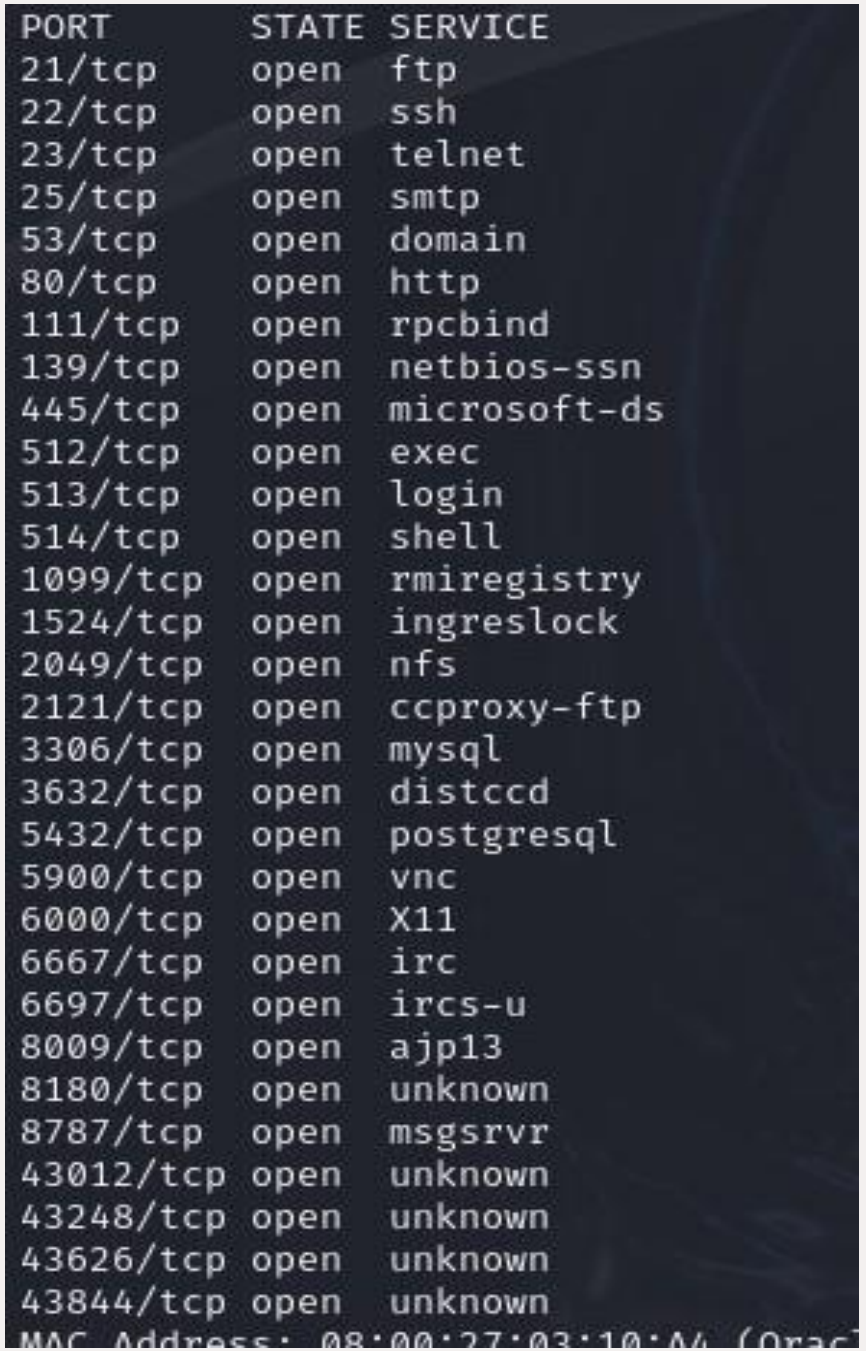
**Scansione eseguita all'host Metasploitable:**

- ***Indirizzo IP***: 192.168.32.101/24;
- ***Sistema Operativo rilevato***: Linux 2.6.9 - 2.6.33.

```
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

# Porte rilevate aperte:

Eseguendo le diverse scansioni (Syn scan, Os fingerprinting, Version scan e TCP connect scan) su tutte le 65535 porte, ne abbiamo rilevate 23 aperte:



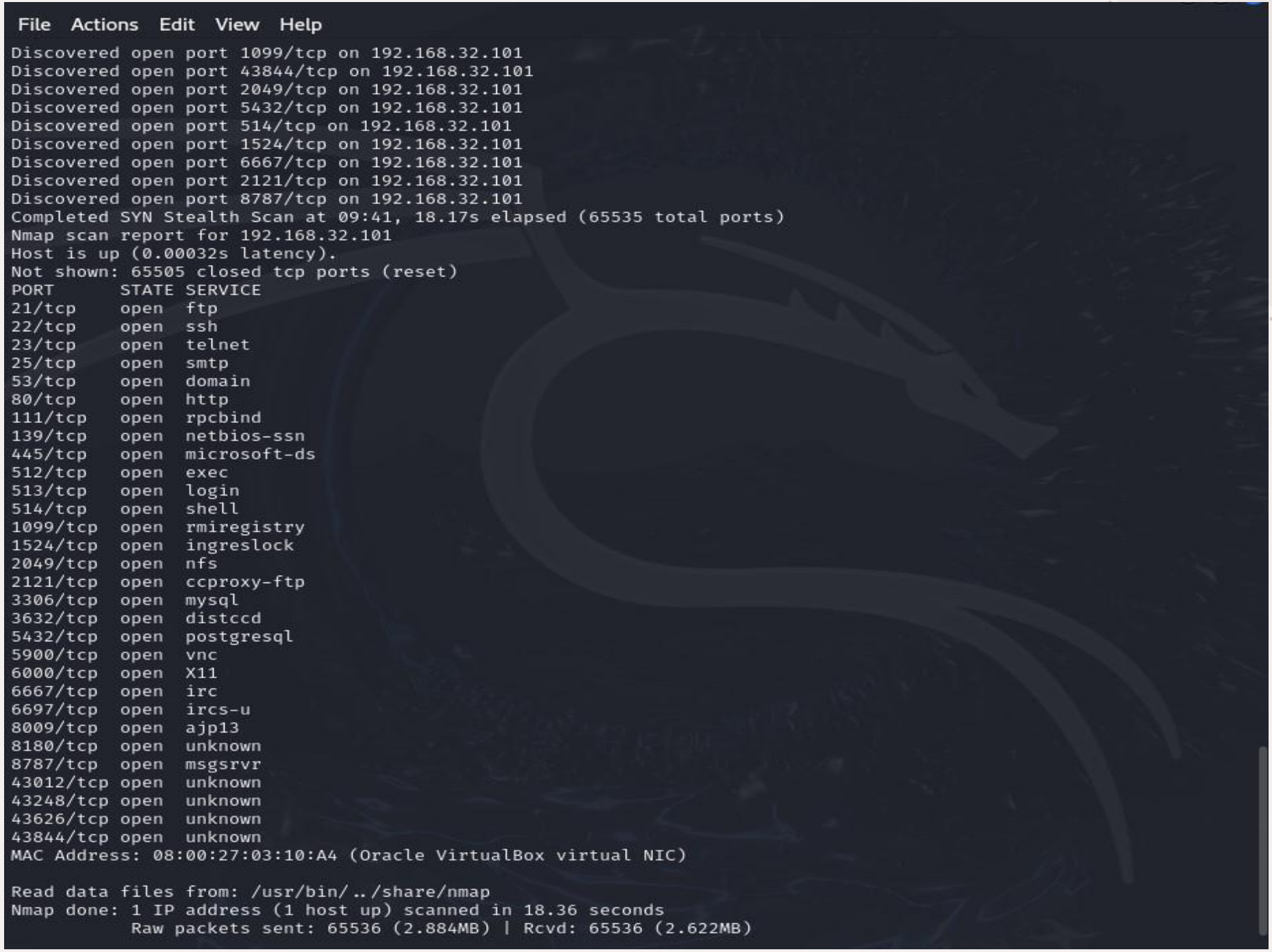
```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
43012/tcp open  unknown
43248/tcp open  unknown
43626/tcp open  unknown
43844/tcp open  unknown
MAC Address: 08:00:27:03:10:A4 (Orac
```

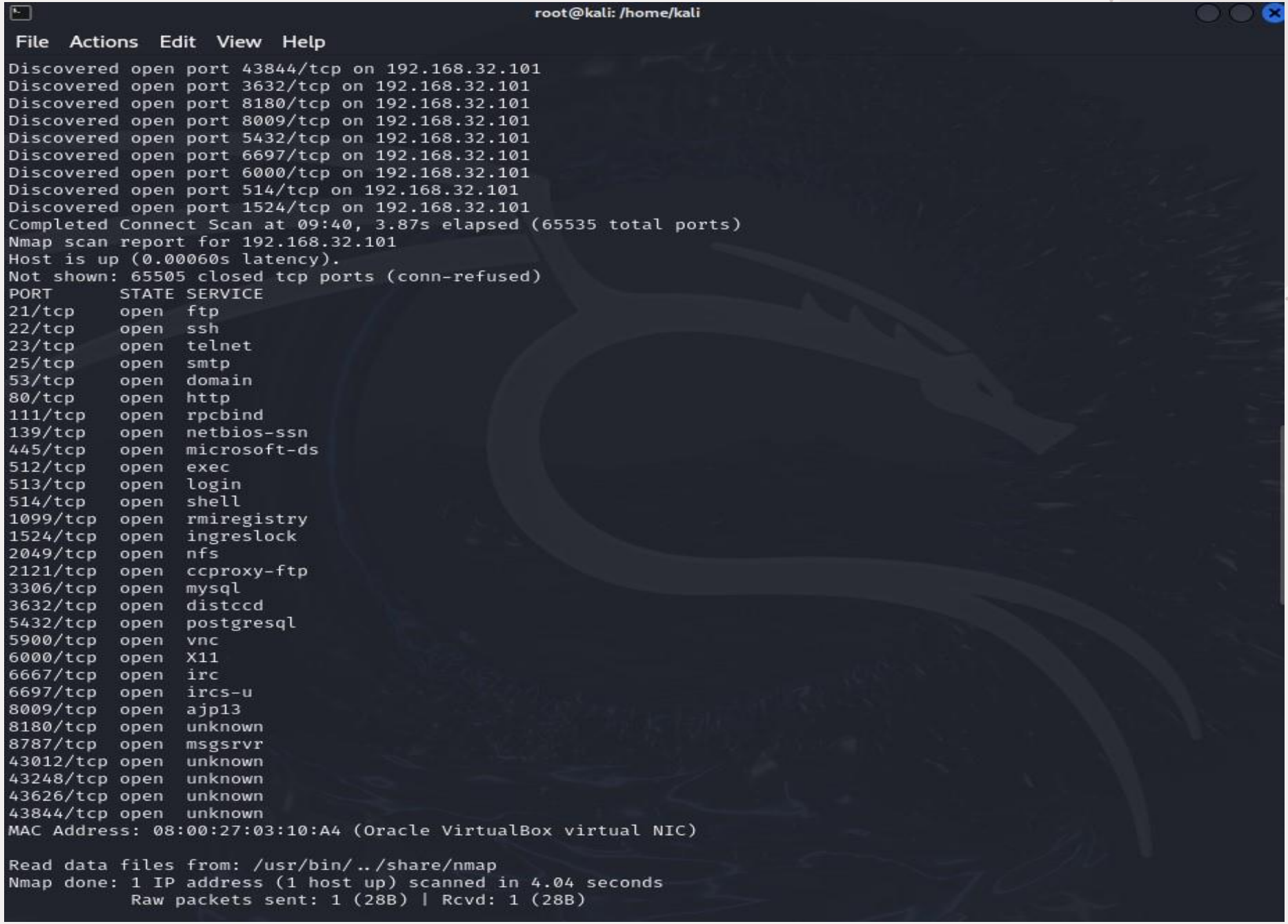
# Servizi in ascolto:

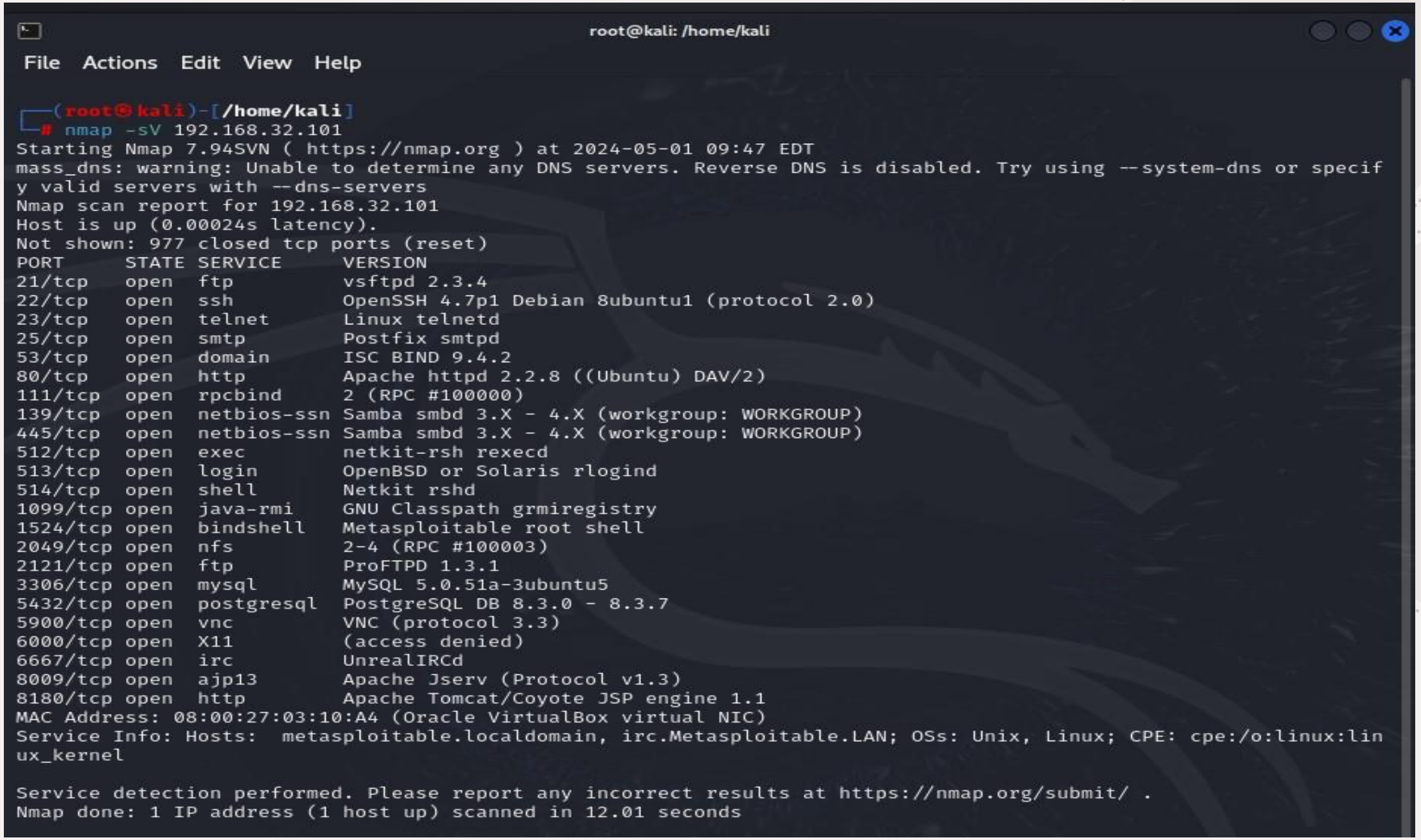
| PORTA | SERVIZIO | VERSIONE | DESCRIZIONE |
|---|---|---|---|
| 21/TCP | Ftp | vsftpd 2.3.4 | File Transfer Protocol |
| 22/TCP | Ssh | OpenSSH 4.7p1 | Secure Shell |
| 23/TCP | Telnet | Linux telnetd | Login remoto non sicuro |
| 25/TCP | Smtp | Postfix smtpd | Simple Mail Transfer Protocol |
| 53/TCP | Domain | ISC BIND 9.4.2 | Domain Name System |
| 80/TCP | http | Apache httpd 2.2.8 | Hyper Text Transfer Protocol |
| 111/TCP | Rpcbind | 2 (RPC #100000) | Remote Procedure Call |
| 139/TCP | netbios-ssn | Samba smbd 3.X - 4.X | Network Basic Input/Output System |
| 445/TCP | netbios-ssn | Samba smbd 3.X - 4.X | Network Basic Input/Output System |
| 512/TCP | Exec | netkit-rsh rexecd | Run Program on a remote server |
| 513/TCP | Login | OpenBSD or Solaris rlogind | Remote shell for rcp |
| 514/TCP | Shell | Netkit rshd | Remote shell for rsh |
| 1099/TCP | Java-rmi | GNU Classpath grmiregistry | Java remote method invocation |
| 1524/TCP | Bindshell | Metasploitable root shell | Remote shell |

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 09:30 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specif
y valid servers with --dns-servers
Nmap scan report for 192.168.32.101
Host is up (0.00081s 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: 08:00:27:03:10:A4 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds
```


File Actions Edit View Help
Discovered open port 1099/tcp on 192.168.32.101
Discovered open port 43844/tcp on 192.168.32.101
Discovered open port 2049/tcp on 192.168.32.101
Discovered open port 5432/tcp on 192.168.32.101
Discovered open port 514/tcp on 192.168.32.101
Discovered open port 1524/tcp on 192.168.32.101
Discovered open port 6667/tcp on 192.168.32.101
Discovered open port 2121/tcp on 192.168.32.101
Discovered open port 8787/tcp on 192.168.32.101
Completed SYN Stealth Scan at 09:41, 18.17s elapsed (65535 total ports)
Nmap scan report for 192.168.32.101
Host is up (0.00032s latency).
Not shown: 65505 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
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open ircs-u
8009/tcp open ajp13
8180/tcp open unknown
8787/tcp open msgsrvr
43012/tcp open unknown
43248/tcp open unknown
43626/tcp open unknown
43844/tcp open unknown
MAC Address: 08:00:27:03:10:A4 (Oracle VirtualBox virtual NIC)
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 18.36 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.622MB)


root@kali: /home/kali
File Actions Edit View Help
Discovered open port 43844/tcp on 192.168.32.101
Discovered open port 3632/tcp on 192.168.32.101
Discovered open port 8180/tcp on 192.168.32.101
Discovered open port 8009/tcp on 192.168.32.101
Discovered open port 5432/tcp on 192.168.32.101
Discovered open port 6697/tcp on 192.168.32.101
Discovered open port 6000/tcp on 192.168.32.101
Discovered open port 514/tcp on 192.168.32.101
Discovered open port 1524/tcp on 192.168.32.101
Completed Connect Scan at 09:40, 3.87s elapsed (65535 total ports)
Nmap scan report for 192.168.32.101
Host is up (0.00060s latency).
Not shown: 65505 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
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open ircs-u
8009/tcp open ajp13
8180/tcp open unknown
8787/tcp open msgsrvr
43012/tcp open unknown
43248/tcp open unknown
43626/tcp open unknown
43844/tcp open unknown
MAC Address: 08:00:27:03:10:A4 (Oracle VirtualBox virtual NIC)
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.04 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)


root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 09:47 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.32.101
Host is up (0.00024s 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 OpenBSD or Solaris rlogind
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: 08:00:27:03:10:A4 (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 12.01 seconds