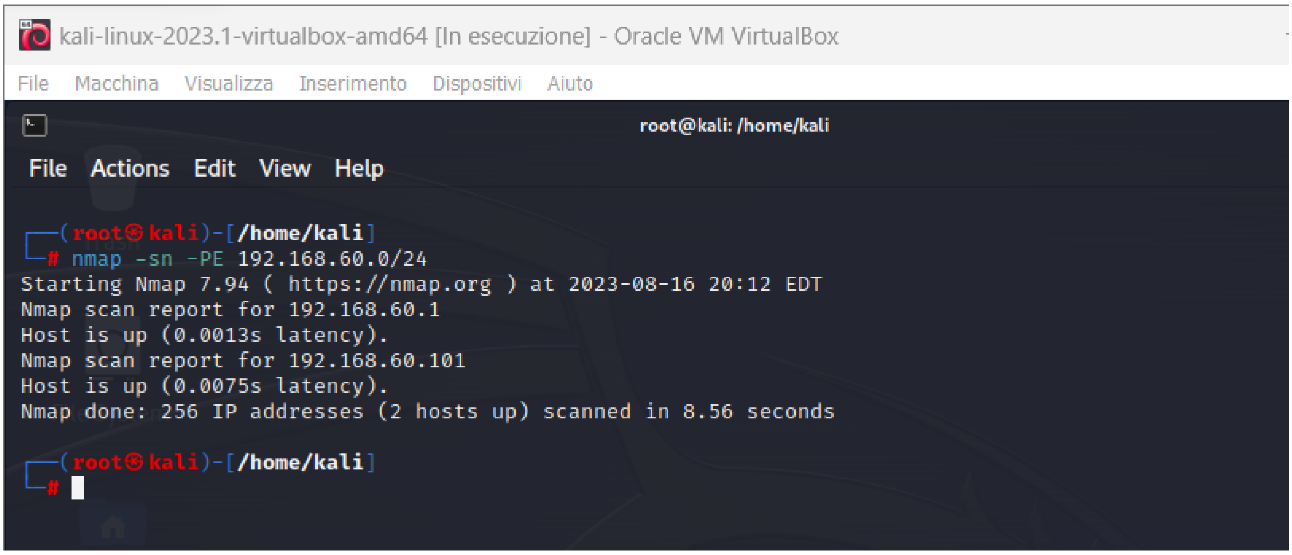
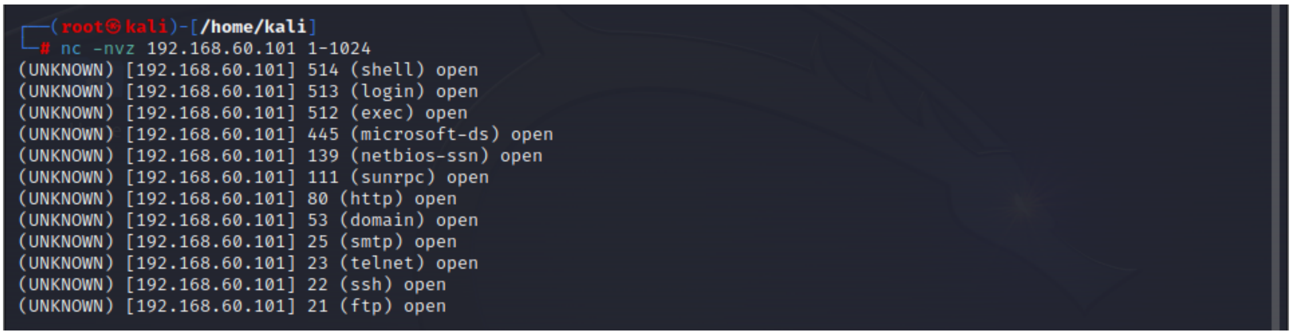

kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@kali: /home/kali
File Actions Edit View Help

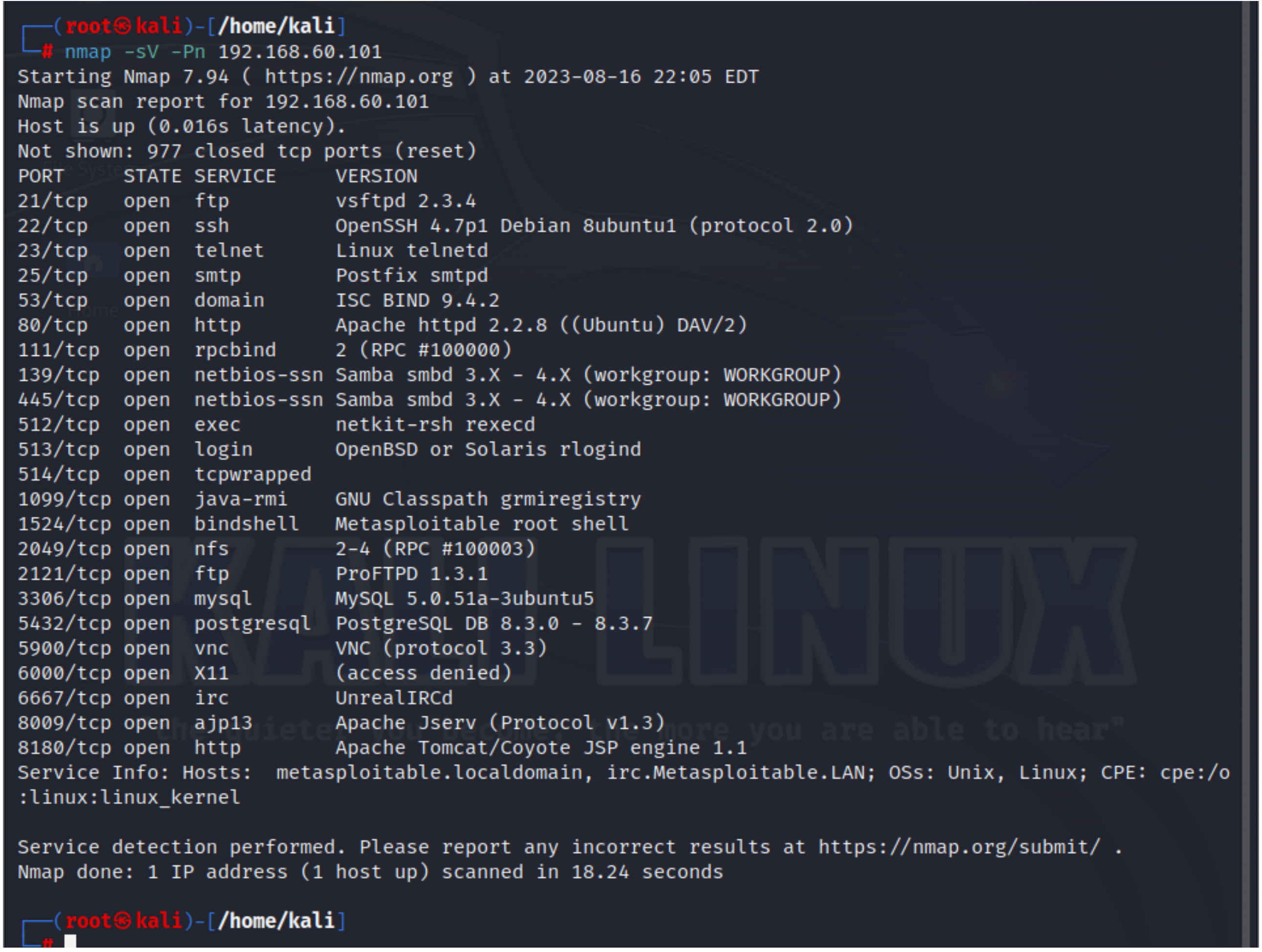
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.60.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-16 20:12 EDT
Nmap scan report for 192.168.60.1
Host is up (0.0013s latency).
Nmap scan report for 192.168.60.101
Host is up (0.0075s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 8.56 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```

Scansione rete per identificare bersaglio

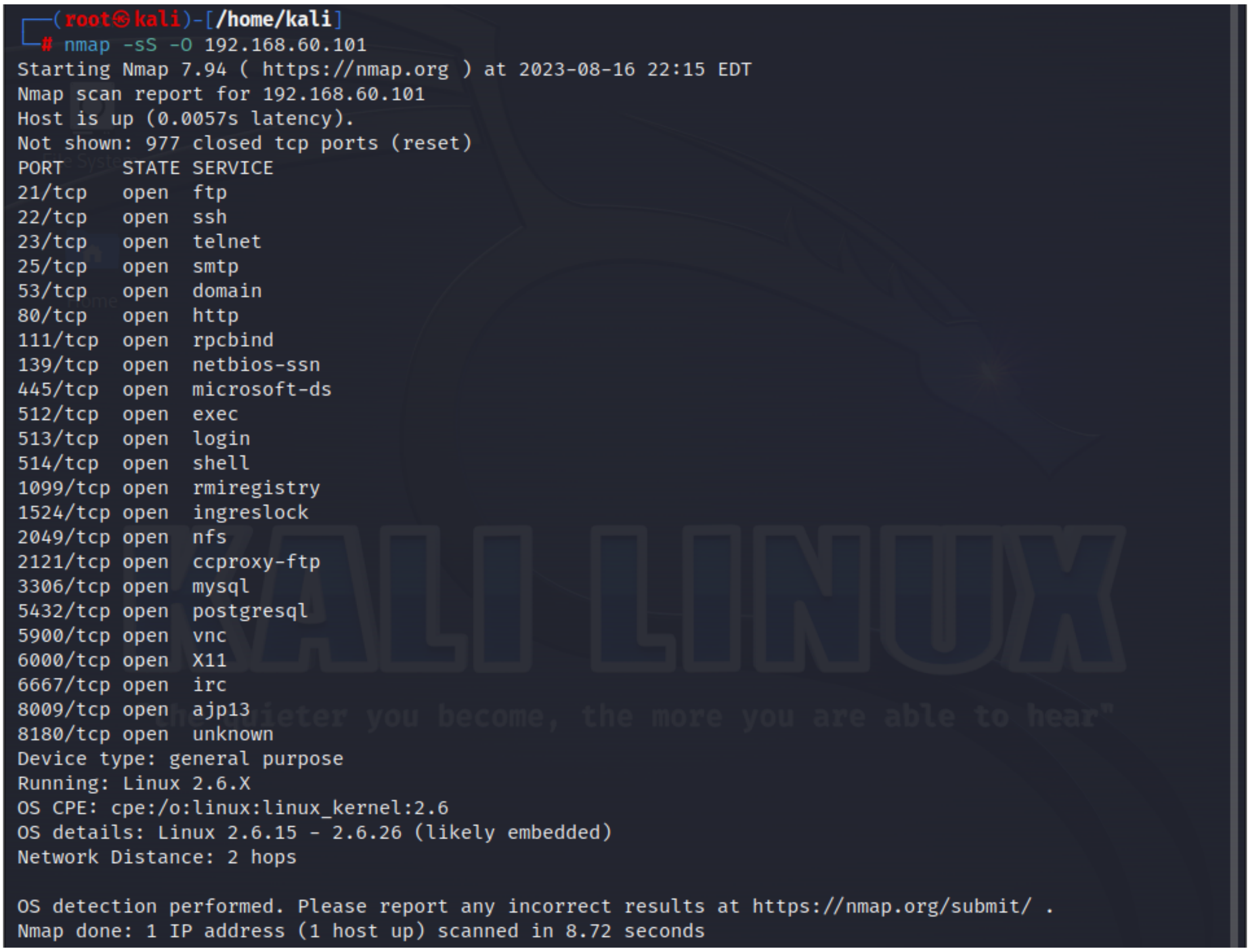


```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvz 192.168.60.101 1-1024
(UNKNOWN) [192.168.60.101] 514 (shell) open
(UNKNOWN) [192.168.60.101] 513 (login) open
(UNKNOWN) [192.168.60.101] 512 (exec) open
(UNKNOWN) [192.168.60.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.60.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.60.101] 111 (sunrpc) open
(UNKNOWN) [192.168.60.101] 80 (http) open
(UNKNOWN) [192.168.60.101] 53 (domain) open
(UNKNOWN) [192.168.60.101] 25 (smtp) open
(UNKNOWN) [192.168.60.101] 23 (telnet) open
(UNKNOWN) [192.168.60.101] 22 (ssh) open
(UNKNOWN) [192.168.60.101] 21 (ftp) open
```

utilizzo di nc per identificare le commonly open ports.
&
scansione porte e servizi con nmap

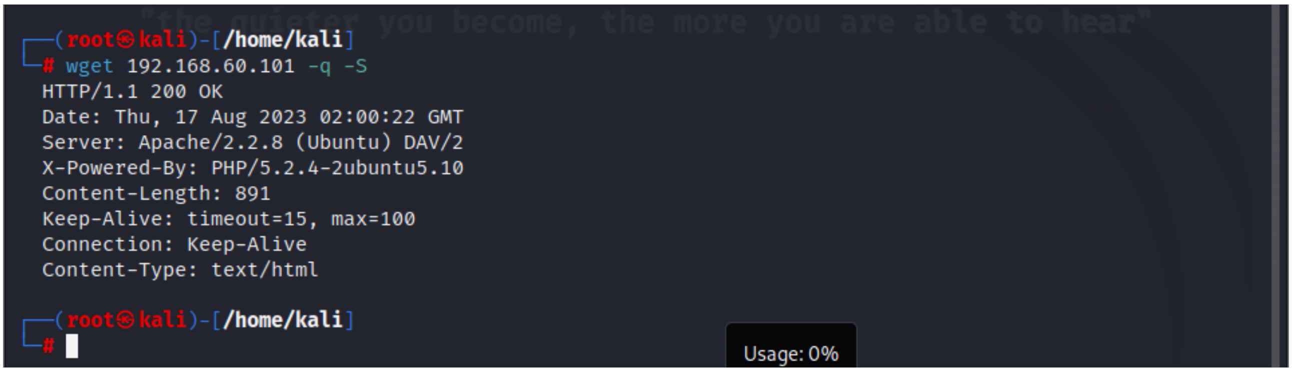


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -Pn 192.168.60.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-16 22:05 EDT
Nmap scan report for 192.168.60.101
Host is up (0.016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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  tcpwrapped
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.24 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -O 192.168.60.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-16 22:15 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0057s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.72 seconds
```

scansione del sistema operativo con nmap



```
┌──(root㉿kali)-[/home/kali]
└─# wget 192.168.60.101 -q -S
  HTTP/1.1 200 OK
  Date: Thu, 17 Aug 2023 02:00:22 GMT
  Server: Apache/2.2.8 (Ubuntu) DAV/2
  X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Content-Length: 891
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Content-Type: text/html

┌──(root㉿kali)-[/home/kali]
└─# 
```

stampa risposta server in quet mode con wget