Traccia

https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/

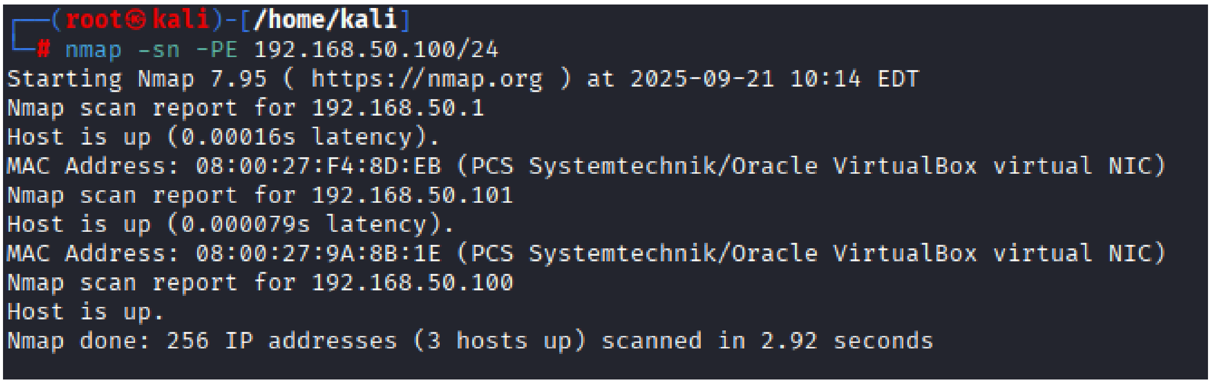
Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report.

Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

ESECUZIONE:

Premessa i primi comandi non mi davano risultati poiché meta non era sulla stessa rete quindi nmap non poteva ottenere il pacchetto perchè passava da un router/gateway quindi ho dovuto rimettere meta sulla stessa rete.

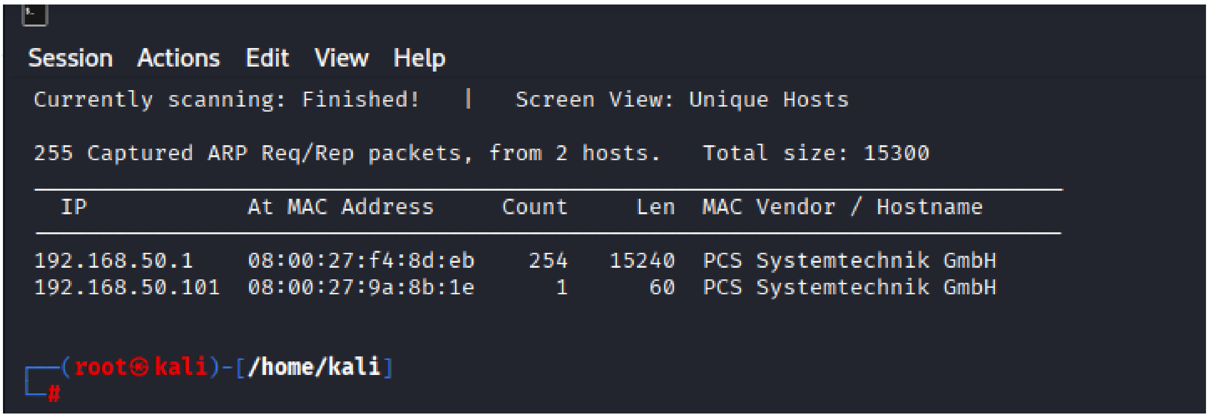
comando: nmap -sn -PE <target>



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.50.100/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 10:14 EDT
Nmap scan report for 192.168.50.1
Host is up (0.00016s latency).
MAC Address: 08:00:27:F4:8D:EB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.101
Host is up (0.000079s latency).
MAC Address: 08:00:27:9A:8B:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.100
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.92 seconds
```

-sn dice a **nmap** di non fare il port scan: esegue solo host discovery (prima fase), per scoprire quali host sono «up» (vivi) nel target, -PE   forza l'uso di ICMP Echo Request (ping ICMP, il classico "ping") come probe di discovery.

comando: netdiscover -r <target>



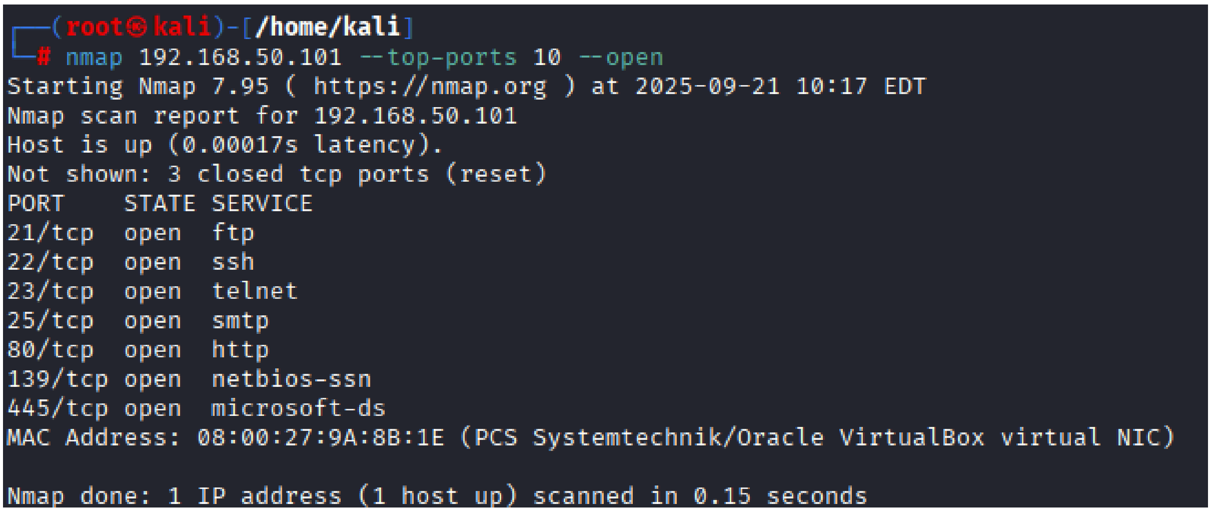
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 255 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 15300
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.50.1    08:00:27:f4:8d:eb    254   15240  PCS Systemtechnik GmbH
 192.168.50.101  08:00:27:9a:8b:1e      1      60  PCS Systemtechnik GmbH


┌──(root㉿kali)-[/home/kali]
└─#
```

netdiscover è uno strumento di ricognizione lan che usa ARP request per determinare host attivi e relativi mac address, infatti lo screenshot mostra: IP, Mac address e vendor.

comando: nmap <target> –top-ports 10 –open

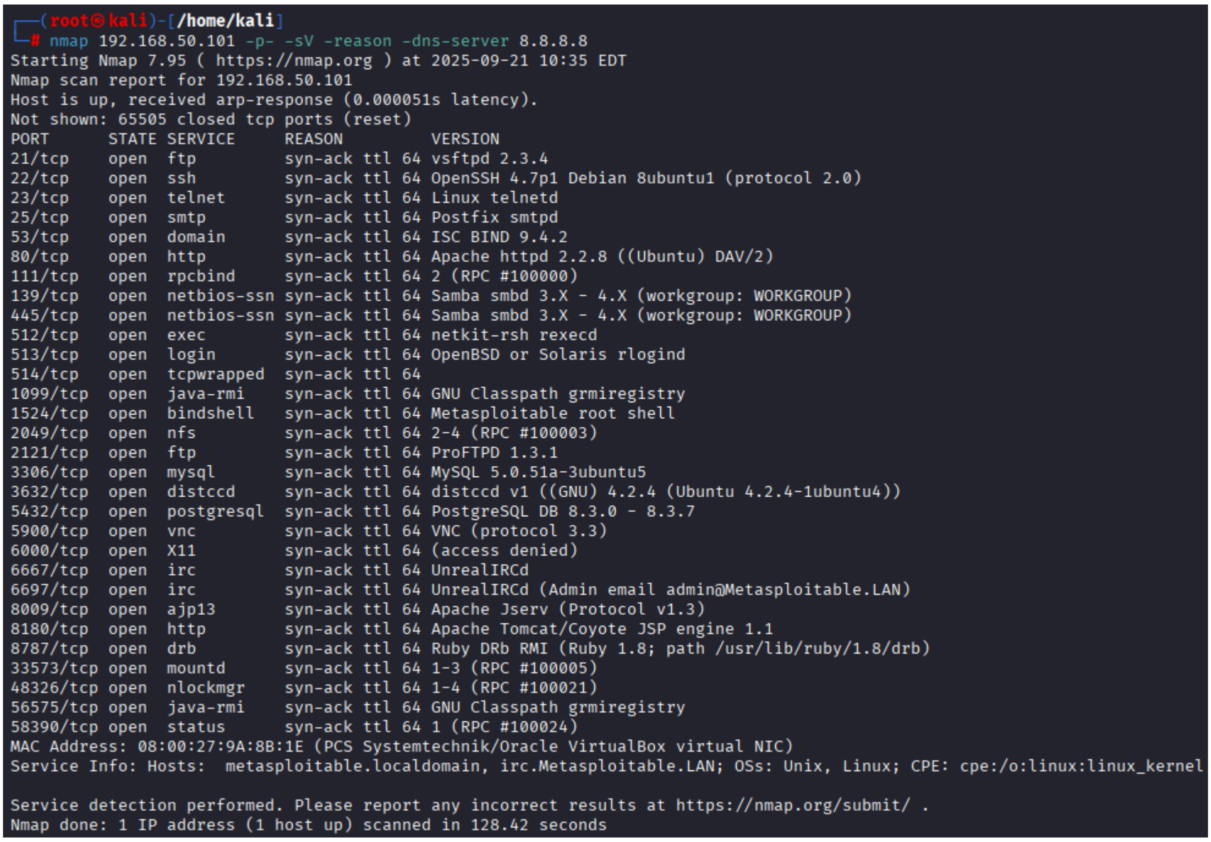


```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.50.101 --top-ports 10 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 10:17 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00017s latency).
Not shown: 3 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:9A:8B:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

top-ports open il comando scansiona le 10 porte più comuni aperte le porte filtrate o chiuse non verranno mostrate.

comando: nmap <target> -p- -sV –reason –dns-server ns

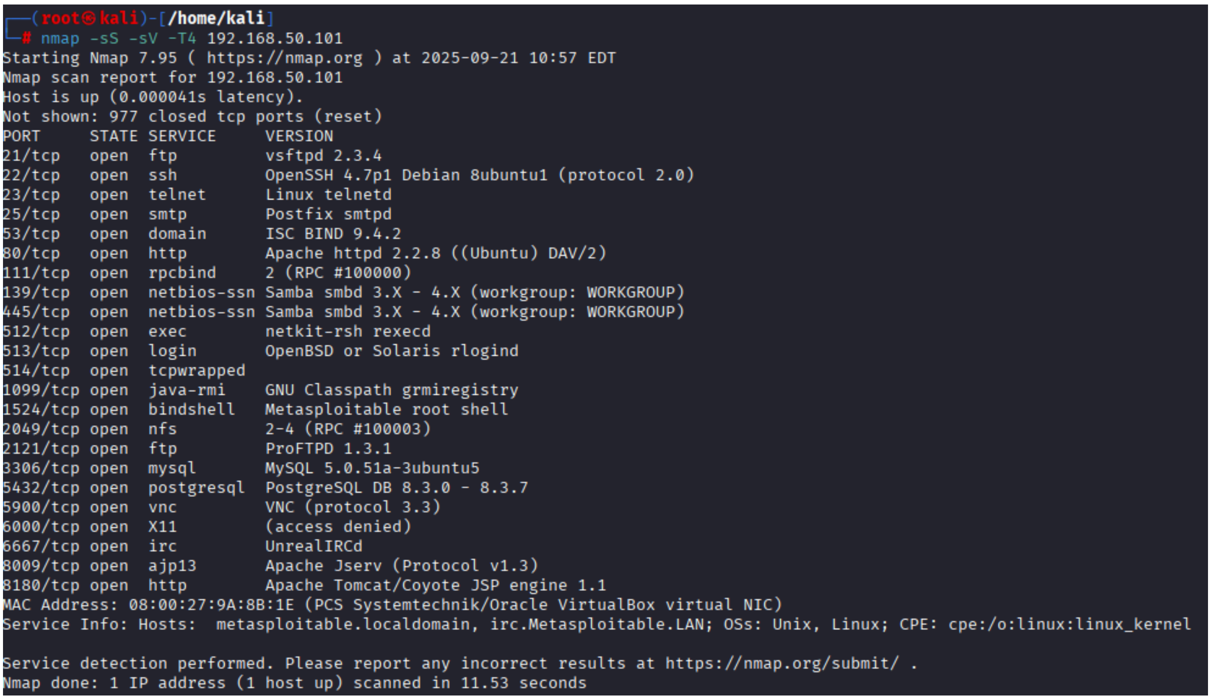


```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.50.101 -p- -sV -reason -dns-server 8.8.8.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 10:35 EDT
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.000051s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login       syn-ack ttl 64 OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped  syn-ack ttl 64
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
33573/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
48326/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
56575/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
58390/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
MAC Address: 08:00:27:9A:8B:1E (PCS Systemtechnik/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 128.42 seconds
```

questo comando esegue una scansione di tutte le porte TCP sul target identifica i servizi e le loro versioni mostra lo stato di una porta, dns server lo usa per per risoluzioni/lookup, -p- le porte tutte le porte, -sV version detection, reason considera una porta in uno stato specifico (open, filtered, closed)

comando: nmap -sS -sV -T4 <target>

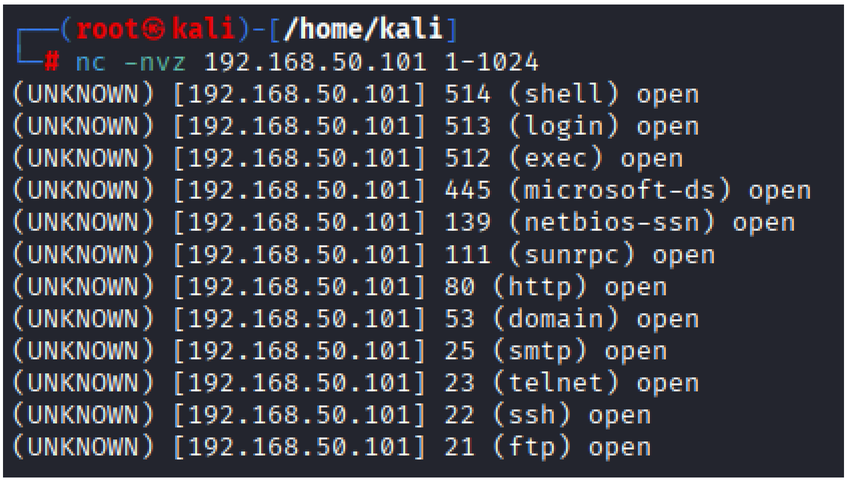


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -T4 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 10:57 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000041s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         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
MAC Address: 08:00:27:9A:8B:1E (PCS Systemtechnik/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 11.53 seconds
```

-sS syn scan -sV version detection -T4 profilo di timing (più veloce ma più aggressivo, può generare molti log e fare scattare sistemi di sicurezza)

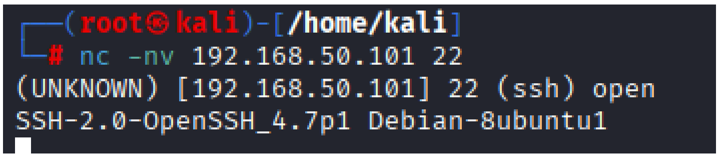
comando: nc -nvz <target> 1-1024



```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvz 192.168.50.101 1-1024
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open
(UNKNOWN) [192.168.50.101] 80 (http) open
(UNKNOWN) [192.168.50.101] 53 (domain) open
(UNKNOWN) [192.168.50.101] 25 (smtp) open
(UNKNOWN) [192.168.50.101] 23 (telnet) open
(UNKNOWN) [192.168.50.101] 22 (ssh) open
(UNKNOWN) [192.168.50.101] 21 (ftp) open
```

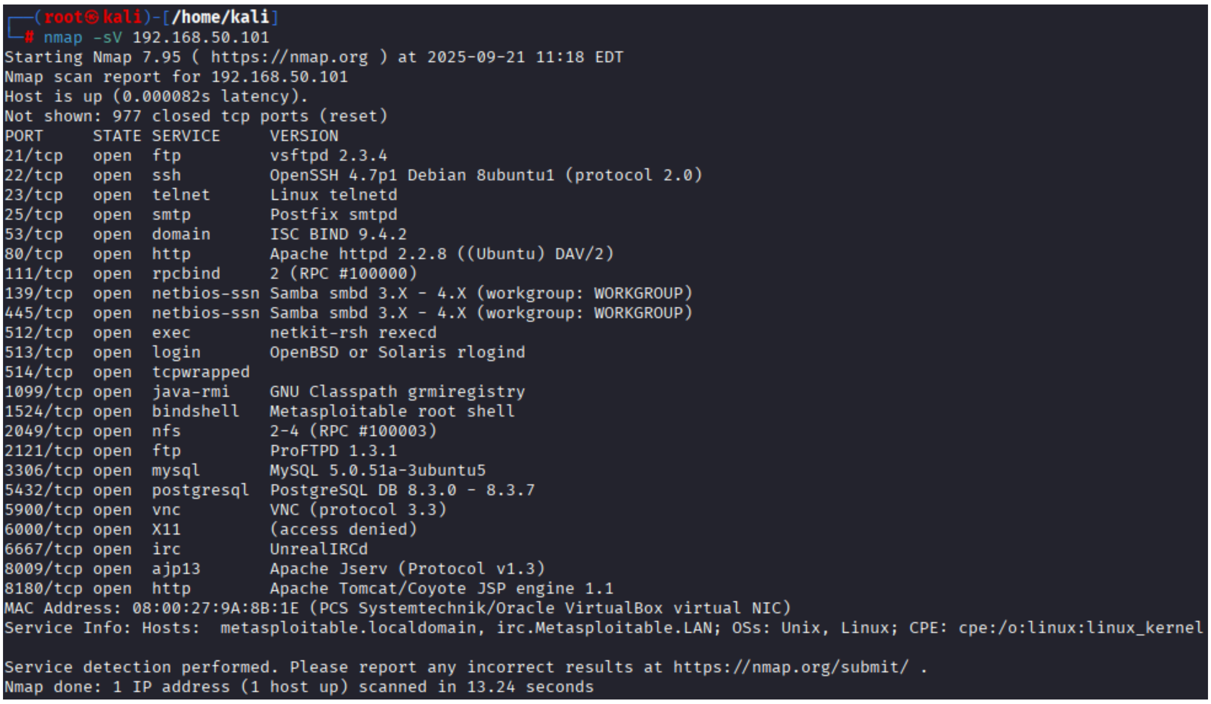
il comando nc (netcat) prova a stabilire connessioni TCP verso le porte 1-1024 e segnala quali porte rispondo, n non risolve nomi DNS usa solo indirizzi numerici, v verbose stampa informazioni, z non apre una sessione I/O serve solo per vedere se la porta accetta una connessione.

comando: nc -nv <target> 22



```
┌──(root㉿kali)-[/home/kali]
└─# nc -nv 192.168.50.101 22
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

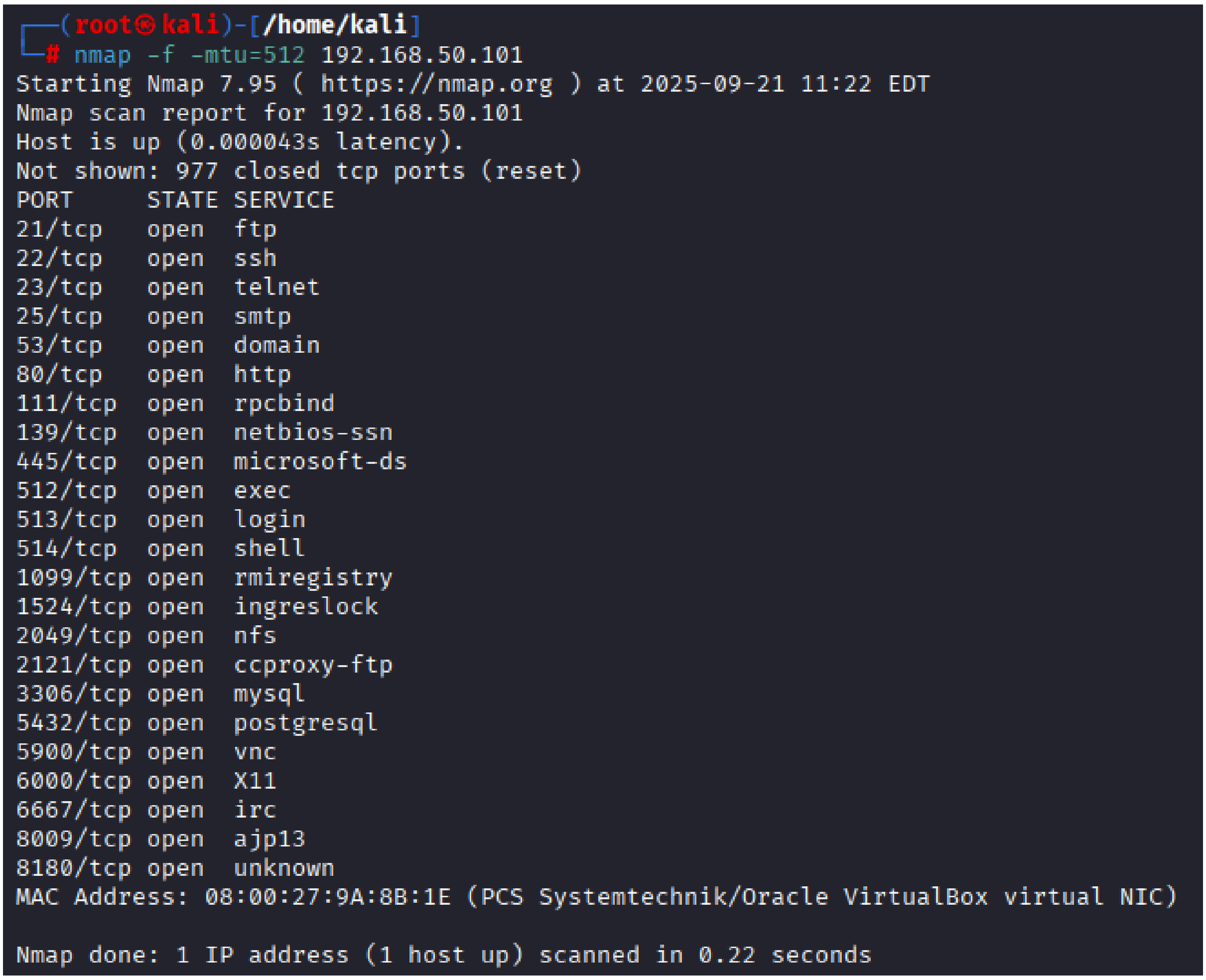
stessa spiegazione comando di prima solo che la porta è la 22 comando: nmap -sV <target>



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 11:18 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000082s 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
MAC Address: 08:00:27:9A:8B:1E (PCS Systemtechnik/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 13.24 seconds
```

sV service version detection porte aperte, identifica servizio e versione comando: nmap -f -mtu=512 <target>



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -f -mtu=512 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 11:22 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000043s 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: 08:00:27:9A:8B:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

-f attiva la frammentazione dei pacchetti ip, questo ci permette di rendere più difficile da parte dei firewall capire il contenuto dei pacchetti.
-mtu=512 specifica la lunghezza dei pacchetti in questo caso 512 byte

INFORMAZIONI TROVATE:
mac address, vendor, porte aperte servizi e versioni dei servizi.