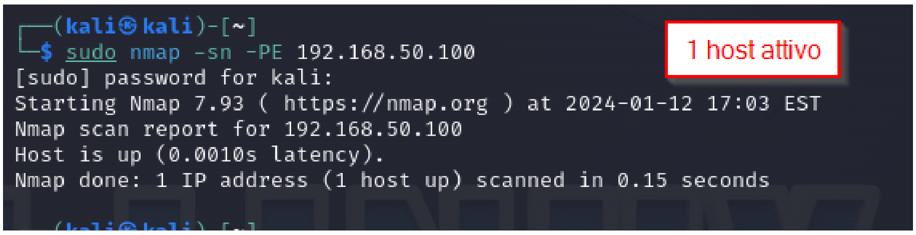
ESERCIZIO W10D4

La traccia prevede l'utilizzo di diversi strumenti di scansione sulla macchina metasploitable, accompagnati dal riepilogo delle informazioni raccolte.

1. sudo nmap -sn -PE 192.168.50.100

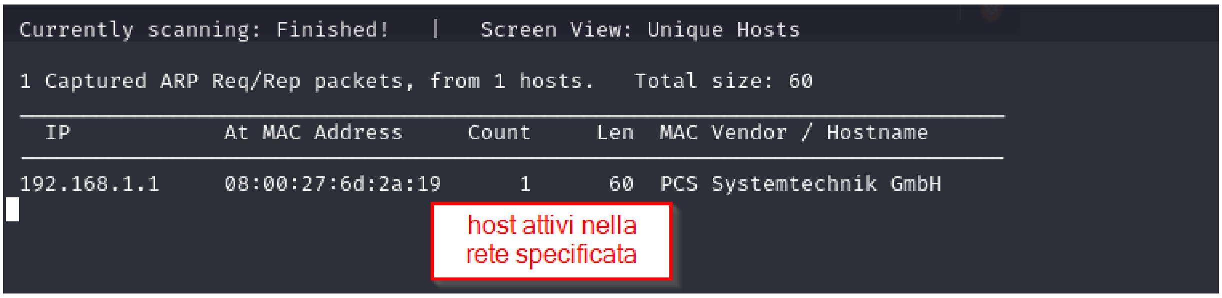


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-12 17:03 EST
Nmap scan report for 192.168.50.100
Host is up (0.0010s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

1 host attivo

Con questa riga di codice verifichiamo la presenza attiva di un host nell'indirizzo specificato, ovvero quello di Metasploitable. Per verificarlo, Kali invia un pacchetto ICMP Echo request.

2. sudo netdiscover -r 192.168.50.100



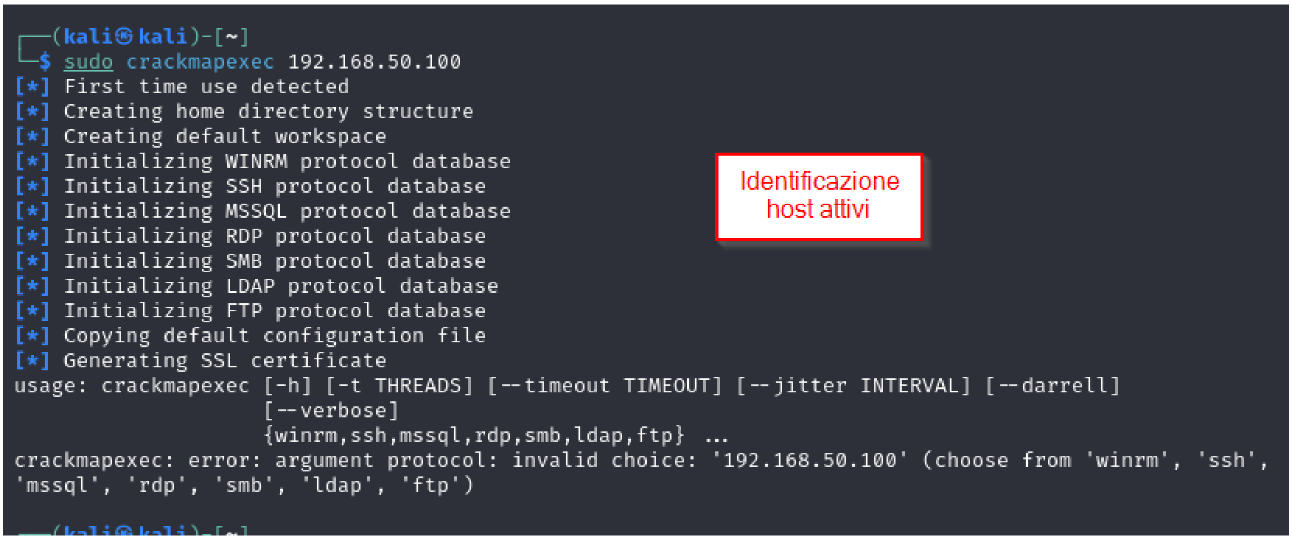
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     08:00:27:6d:2a:19      1      60  PCS Systemtechnik GmbH
```

host attivi nella rete specificata

Il codice andrà ad identificare i dispositivi attualmente connessi nell'intervallo di IP specificato. Sono entrato con Kali sul server web di

Metasploitable2, per vedere se funzionava. Dopo due secondi, il tool mi ha mostrato live il dispositivo connesso.

3. sudo crackmapexec 192.168.50.100

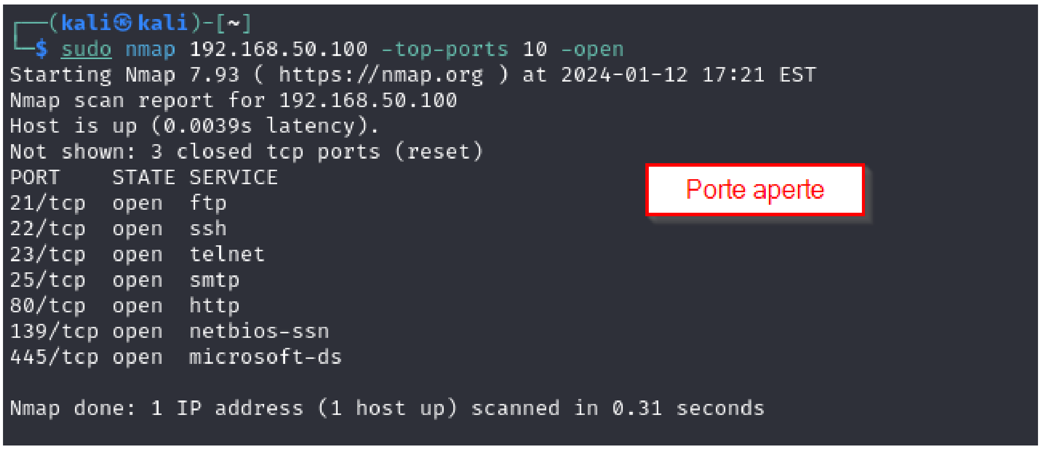


```
┌──(kali㉿kali)-[~]
└─$ sudo crackmapexec 192.168.50.100
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing WINRM protocol database
[*] Initializing SSH protocol database
[*] Initializing MSSQL protocol database
[*] Initializing RDP protocol database
[*] Initializing SMB protocol database
[*] Initializing LDAP protocol database
[*] Initializing FTP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell]
                    [--verbose]
                    {winrm,ssh,mssql,rdp,smb,ldap,ftp} ...
crackmapexec: error: argument protocol: invalid choice: '192.168.50.100' (choose from 'winrm', 'ssh',
'mssql', 'rdp', 'smb', 'ldap', 'ftp')

┌──(kali㉿kali)-[~]
```

Identificazione host attivi

Questo tool di post-esplorazione, valuta automaticamente le vulnerabilità delle reti e degli ambienti active directory. Vengono analizzati tutti i servizi presenti.

4. Sudo nmap 192.168.50.100 -top-ports 10 -open

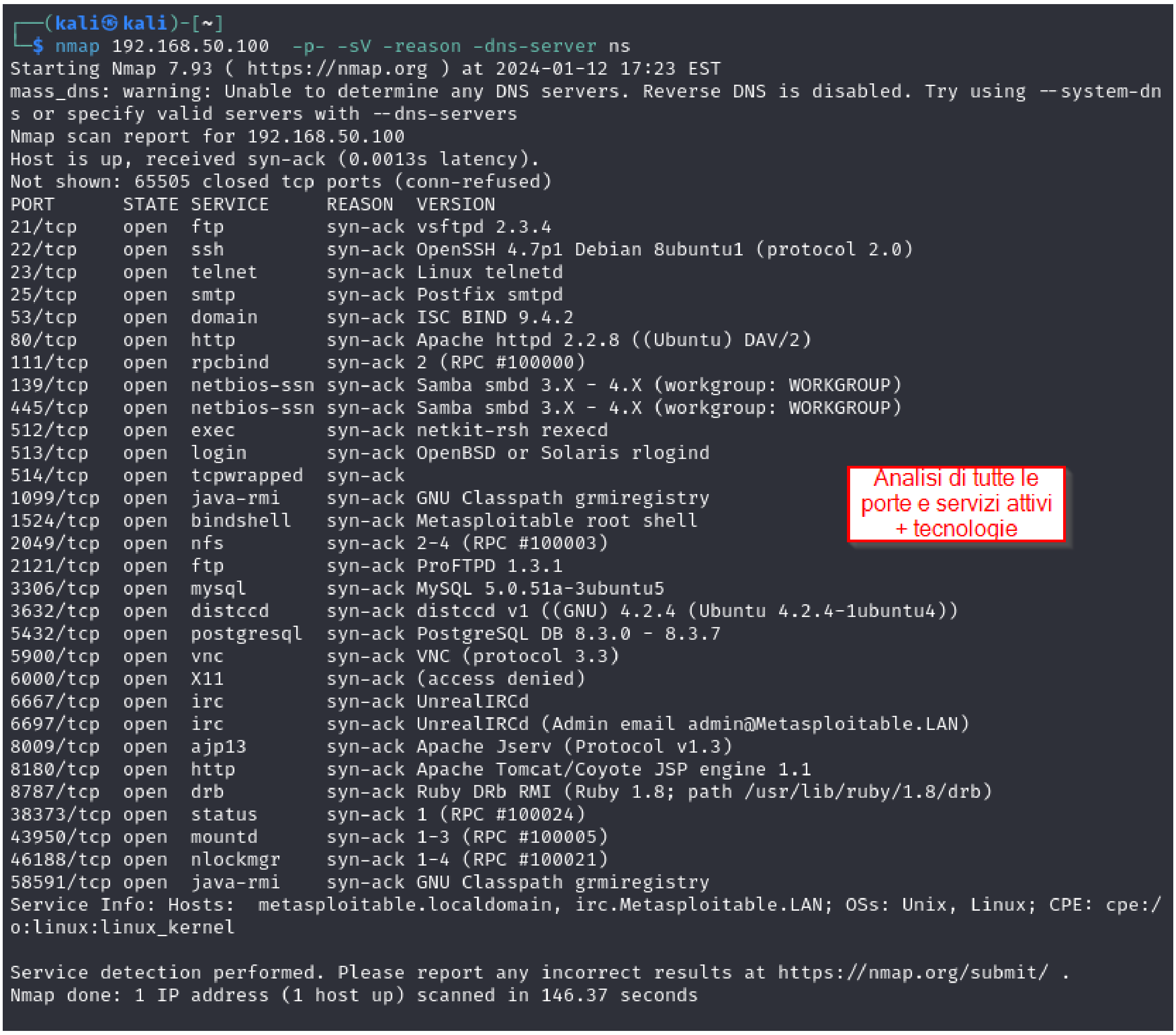


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.50.100 -top-ports 10 -open
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-12 17:21 EST
Nmap scan report for 192.168.50.100
Host is up (0.0039s latency).
Not shown: 3 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

Porte aperte

Nmap, per mezzo di questa sintassi, scannerizzerà le 10 porte più comuni.

5. nmap 192.168.50.100 -p- -sV –reason –dns-server ns

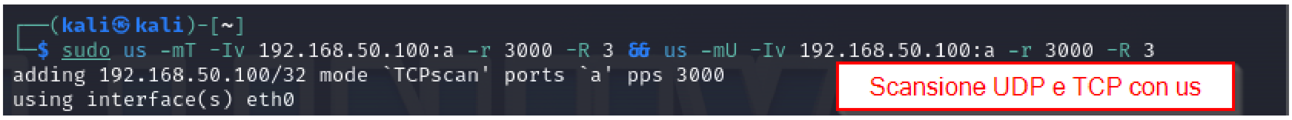


```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.100  -p- -sV -reason -dns-server ns
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-12 17:23 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dn
s or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.100
Host is up, received syn-ack (0.0013s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     REASON  VERSION
21/tcp    open  ftp         syn-ack vsftpd 2.3.4
22/tcp    open  ssh         syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack Linux telnetd
25/tcp    open  smtp        syn-ack Postfix smtpd
53/tcp    open  domain      syn-ack ISC BIND 9.4.2
80/tcp    open  http        syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack netkit-rsh rexecd
513/tcp   open  login       syn-ack OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped  syn-ack
1099/tcp  open  java-rmi    syn-ack GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack Metasploitable root shell
2049/tcp  open  nfs         syn-ack 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack (access denied)
6667/tcp  open  irc         syn-ack UnrealIRCd
6697/tcp  open  irc         syn-ack UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       syn-ack Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
38373/tcp open  status      syn-ack 1 (RPC #100024)
43950/tcp open  mountd      syn-ack 1-3 (RPC #100005)
46188/tcp open  nlockmgr    syn-ack 1-4 (RPC #100021)
58591/tcp open  java-rmi    syn-ack GNU Classpath grmiregistry
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 146.37 seconds
```

Analisi di tutte le porte e servizi attivi + tecnologie

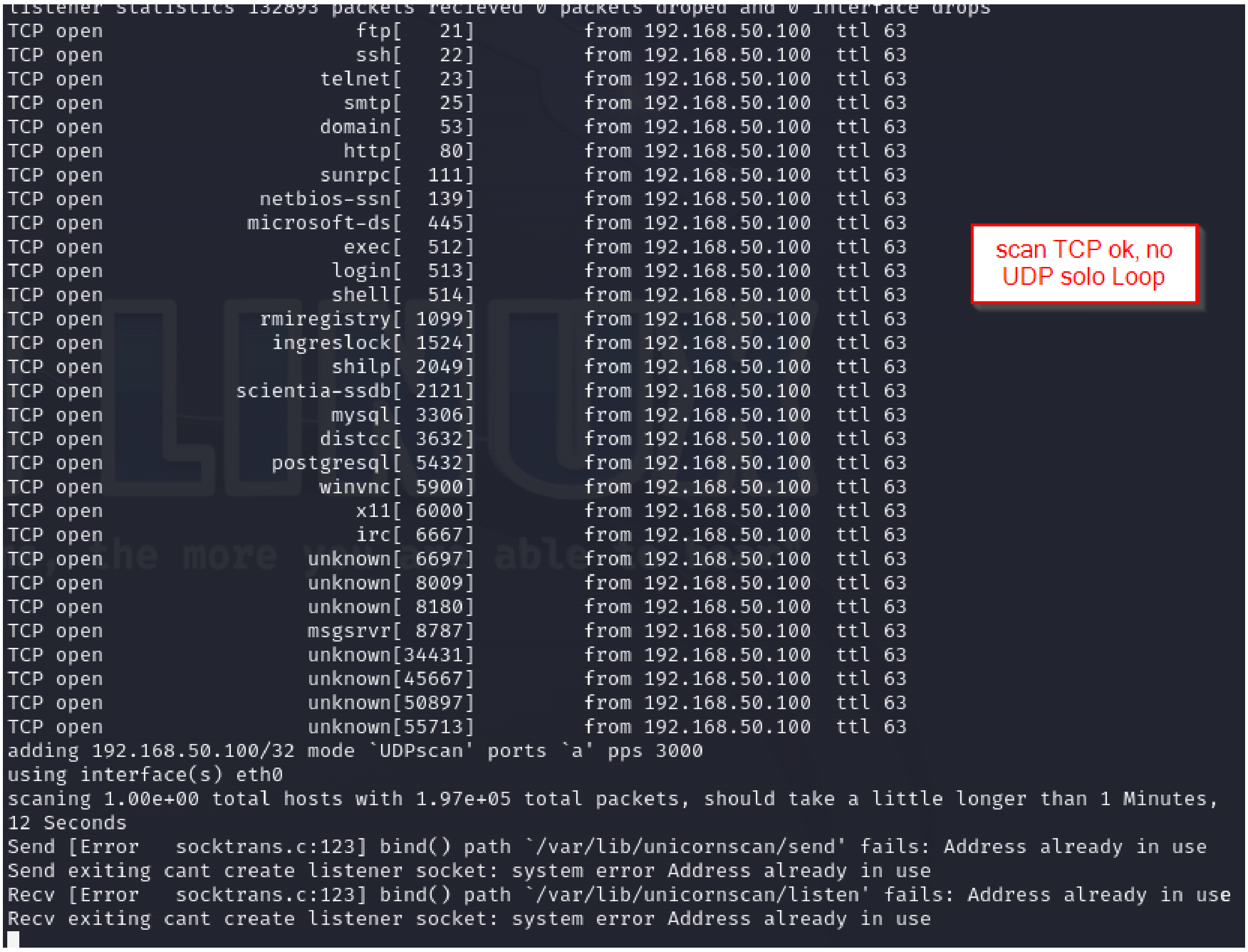
Lo scan andrà a determinare tutti i servizi attivi sopra le porte Metasploitable, andando ad includere nelle analisi le versioni utilizzate ed il perché una port è aperta o chiusa.

6. us -mT -Iv 192.168.50.100:a -r 3000 -R 3 && us -mU -Iv 192.168.50.100:a -r 3000 -R 3



```
┌──(kali㉿kali)-[~]
└─$ sudo us -mT -Iv 192.168.50.100:a -r 3000 -R 3 && us -mU -Iv 192.168.50.100:a -r 3000 -R 3
adding 192.168.50.100/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
```

Scansione UDP e TCP con us

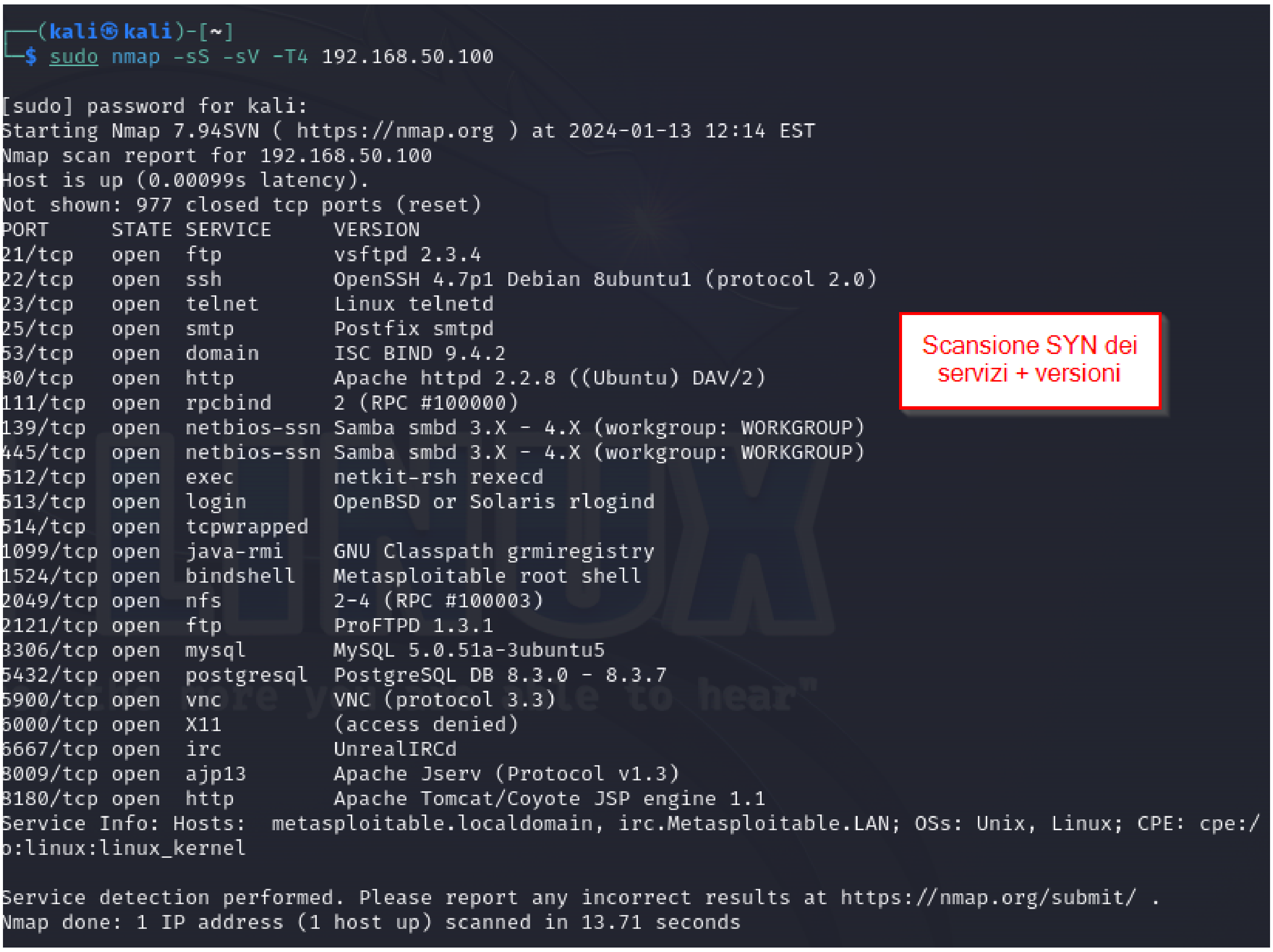


```
listener statistics 132893 packets recieved 0 packets droped and 0 interface drops
TCP open                     ftp[   21]         from 192.168.50.100  ttl 63
TCP open                     ssh[   22]         from 192.168.50.100  ttl 63
TCP open                  telnet[   23]         from 192.168.50.100  ttl 63
TCP open                    smtp[   25]         from 192.168.50.100  ttl 63
TCP open                  domain[   53]         from 192.168.50.100  ttl 63
TCP open                    http[   80]         from 192.168.50.100  ttl 63
TCP open                  sunrpc[  111]         from 192.168.50.100  ttl 63
TCP open             netbios-ssn[  139]         from 192.168.50.100  ttl 63
TCP open            microsoft-ds[  445]         from 192.168.50.100  ttl 63
TCP open                    exec[  512]         from 192.168.50.100  ttl 63
TCP open                   login[  513]         from 192.168.50.100  ttl 63
TCP open                   shell[  514]         from 192.168.50.100  ttl 63
TCP open             rmiregistry[ 1099]         from 192.168.50.100  ttl 63
TCP open              ingreslock[ 1524]         from 192.168.50.100  ttl 63
TCP open                   shilp[ 2049]         from 192.168.50.100  ttl 63
TCP open            scientia-ssdb[ 2121]        from 192.168.50.100  ttl 63
TCP open                   mysql[ 3306]         from 192.168.50.100  ttl 63
TCP open                  distcc[ 3632]         from 192.168.50.100  ttl 63
TCP open              postgresql[ 5432]         from 192.168.50.100  ttl 63
TCP open                  winvnc[ 5900]         from 192.168.50.100  ttl 63
TCP open                     x11[ 6000]         from 192.168.50.100  ttl 63
TCP open                     irc[ 6667]         from 192.168.50.100  ttl 63
TCP open                 unknown[ 6697]         from 192.168.50.100  ttl 63
TCP open                 unknown[ 8009]         from 192.168.50.100  ttl 63
TCP open                 unknown[ 8180]         from 192.168.50.100  ttl 63
TCP open                 msgsrvr[ 8787]         from 192.168.50.100  ttl 63
TCP open                 unknown[34431]         from 192.168.50.100  ttl 63
TCP open                 unknown[45667]         from 192.168.50.100  ttl 63
TCP open                 unknown[50897]         from 192.168.50.100  ttl 63
TCP open                 unknown[55713]         from 192.168.50.100  ttl 63
adding 192.168.50.100/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
Send [Error   socktrans.c:123] bind() path `/var/lib/unicornscan/send' fails: Address already in use
Send exiting cant create listener socket: system error Address already in use
Recv [Error   socktrans.c:123] bind() path `/var/lib/unicornscan/listen' fails: Address already in use
Recv exiting cant create listener socket: system error Address already in use
```

scan TCP ok, no UDP solo Loop

Il tool unicorn scan va ad effettuare per tre volte due scansioni dettagliate, una TCP e un'altra UDP. Queste analisi sono tarate su un timeout di tre secondi.

7. sudo nmap -sS -sV -T4 192.168.50.100

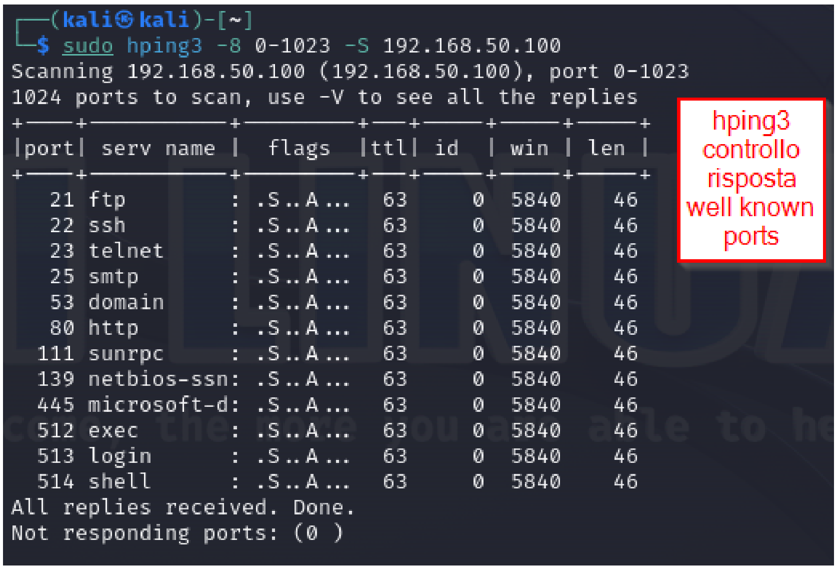


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -T4 192.168.50.100

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-13 12:14 EST
Nmap scan report for 192.168.50.100
Host is up (0.00099s 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 13.71 seconds
```

Scansione SYN dei servizi + versioni

Questa sintassi effettua uno scan stealth dei servizi di Metasploitable assieme alle loro versioni attuali. T4 rende più aggressivo lo scan.

8. sudo hping3 -8 0-1023 -S 192.168.50.100

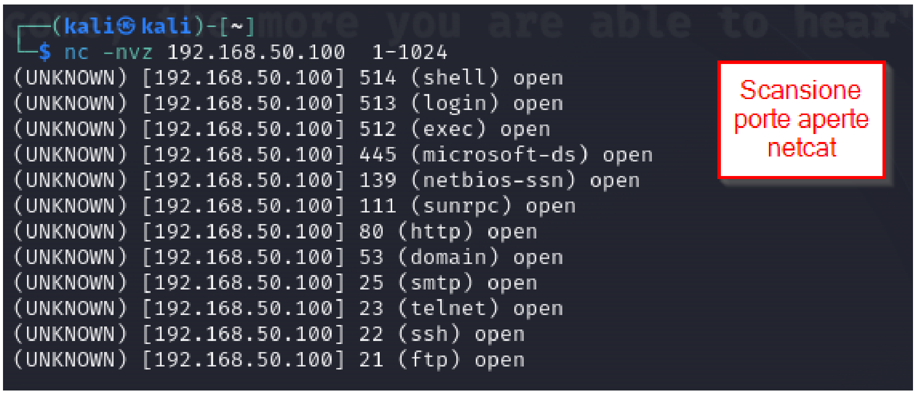


```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -8 0-1023 -S 192.168.50.100
Scanning 192.168.50.100 (192.168.50.100), port 0-1023
1024 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   21 ftp        : .S..A...  63     0  5840    46
   22 ssh        : .S..A...  63     0  5840    46
   23 telnet     : .S..A...  63     0  5840    46
   25 smtp       : .S..A...  63     0  5840    46
   53 domain     : .S..A...  63     0  5840    46
   80 http       : .S..A...  63     0  5840    46
  111 sunrpc     : .S..A...  63     0  5840    46
  139 netbios-ssn: .S..A...  63     0  5840    46
  445 microsoft-d: .S..A...  63     0  5840    46
  512 exec       : .S..A...  63     0  5840    46
  513 login      : .S..A...  63     0  5840    46
  514 shell      : .S..A...  63     0  5840    46
All replies received. Done.
Not responding ports: (0 )
```

hping3 controllo risposta well known ports

Hping3 è un’unità di ping avanzata, che analizza le risposte pervenutegli da tutte le well known ports. La scansione è di tipo TCP.

9. nc -nvz 192.168.50.100 1-1024

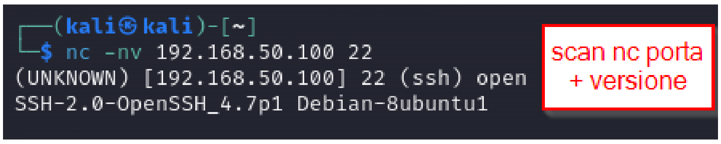


```
┌──(kali㉿kali)-[~]
└─$ nc -nvz 192.168.50.100  1-1024
(UNKNOWN) [192.168.50.100] 514 (shell) open
(UNKNOWN) [192.168.50.100] 513 (login) open
(UNKNOWN) [192.168.50.100] 512 (exec) open
(UNKNOWN) [192.168.50.100] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.100] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.100] 111 (sunrpc) open
(UNKNOWN) [192.168.50.100] 80 (http) open
(UNKNOWN) [192.168.50.100] 53 (domain) open
(UNKNOWN) [192.168.50.100] 25 (smtp) open
(UNKNOWN) [192.168.50.100] 23 (telnet) open
(UNKNOWN) [192.168.50.100] 22 (ssh) open
(UNKNOWN) [192.168.50.100] 21 (ftp) open
```

Scansione porte aperte netcat

netcat scansiona le porte disponibili nel range senza stabilire un collegamento completo.

10. nc -nv 192.168.50.100 22

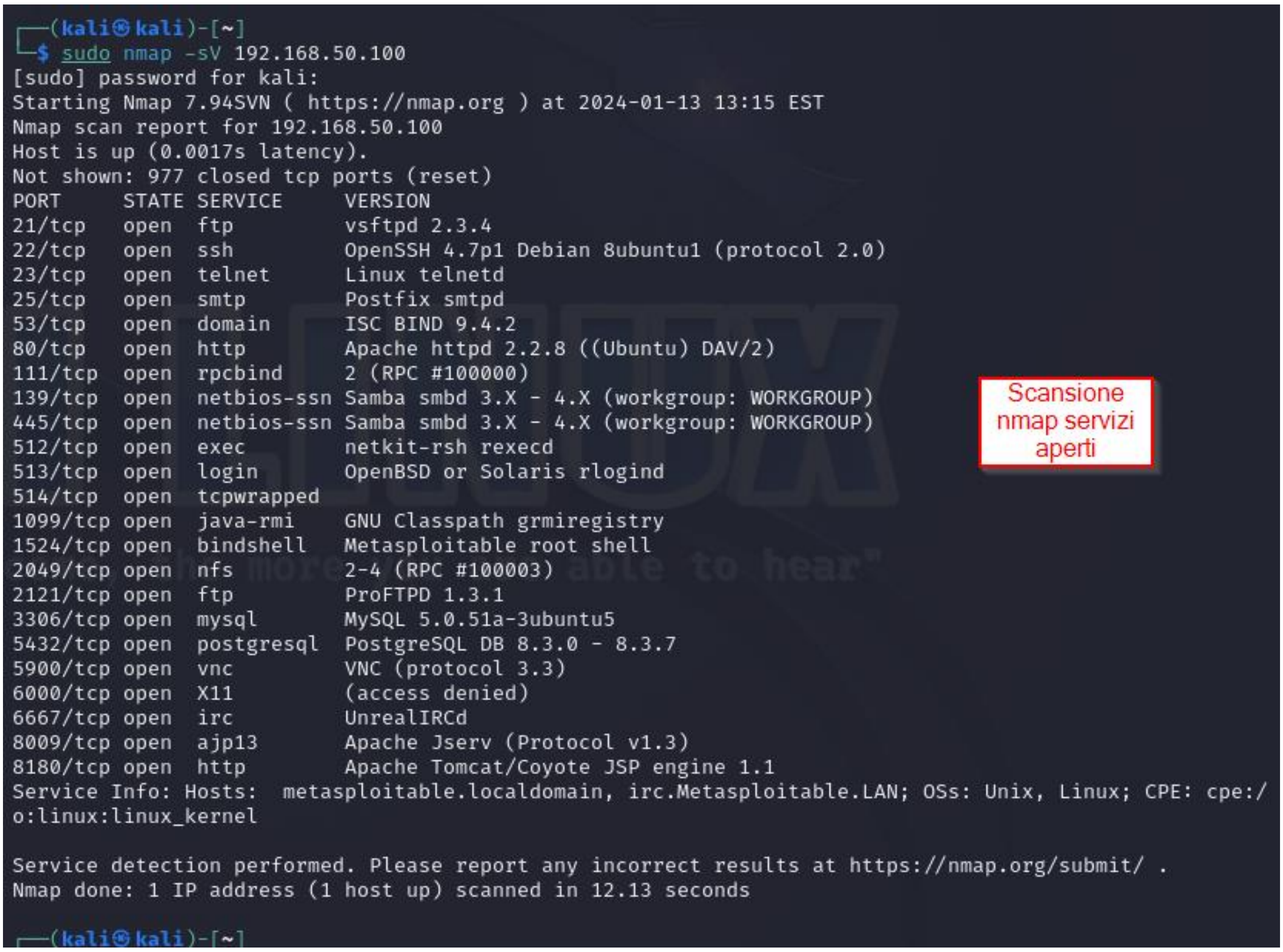


```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.50.100 22
(UNKNOWN) [192.168.50.100] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

scan nc porta + versione

In questo caso netcat effettua una scansione completa della sola porta 22(ssh) di Metasploitable, andando a rivelare la versione ed il sistema.

11. sudo nmap -sV 192.168.50.100

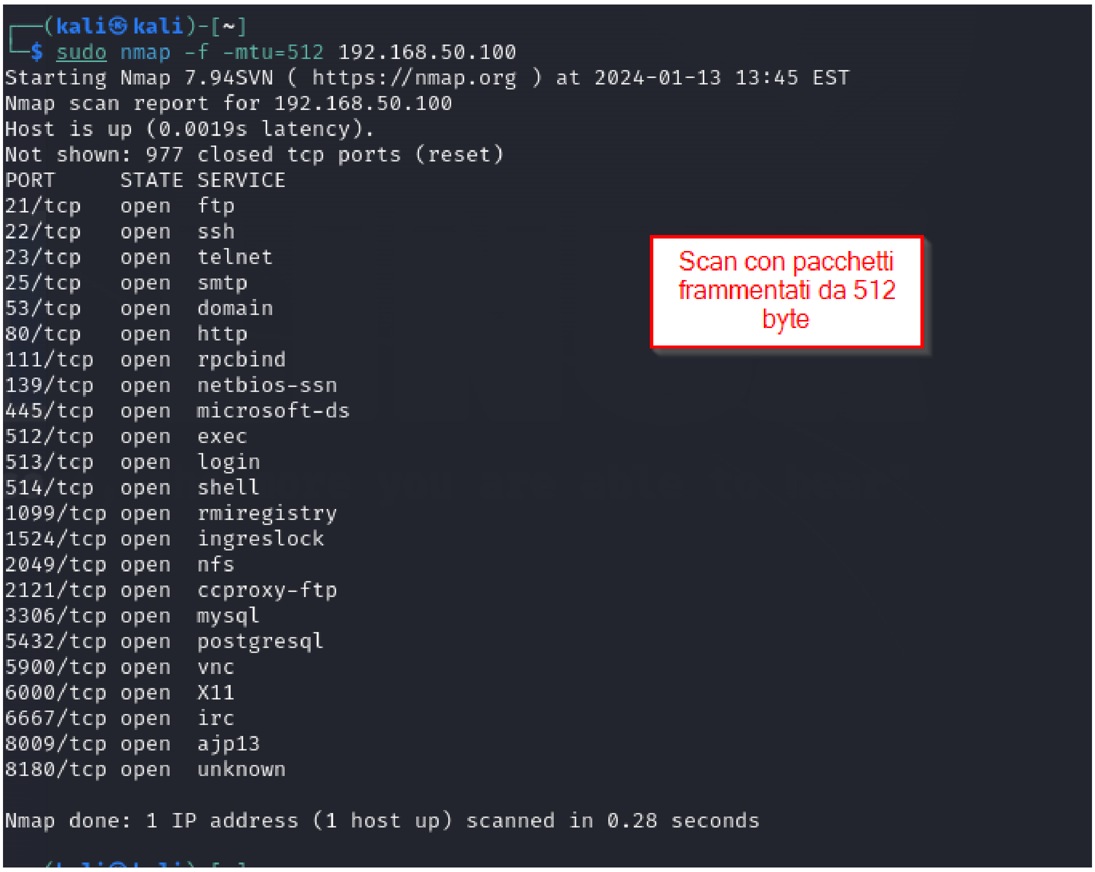


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-13 13:15 EST
Nmap scan report for 192.168.50.100
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  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 12.13 seconds

┌──(kali㉿kali)-[~]
```

Scansione nmap servizi aperti

Nmap scansiona le porte attive e ne definisce le versioni.

12. sudo nmap -f -mtu=512 192.168.50.100

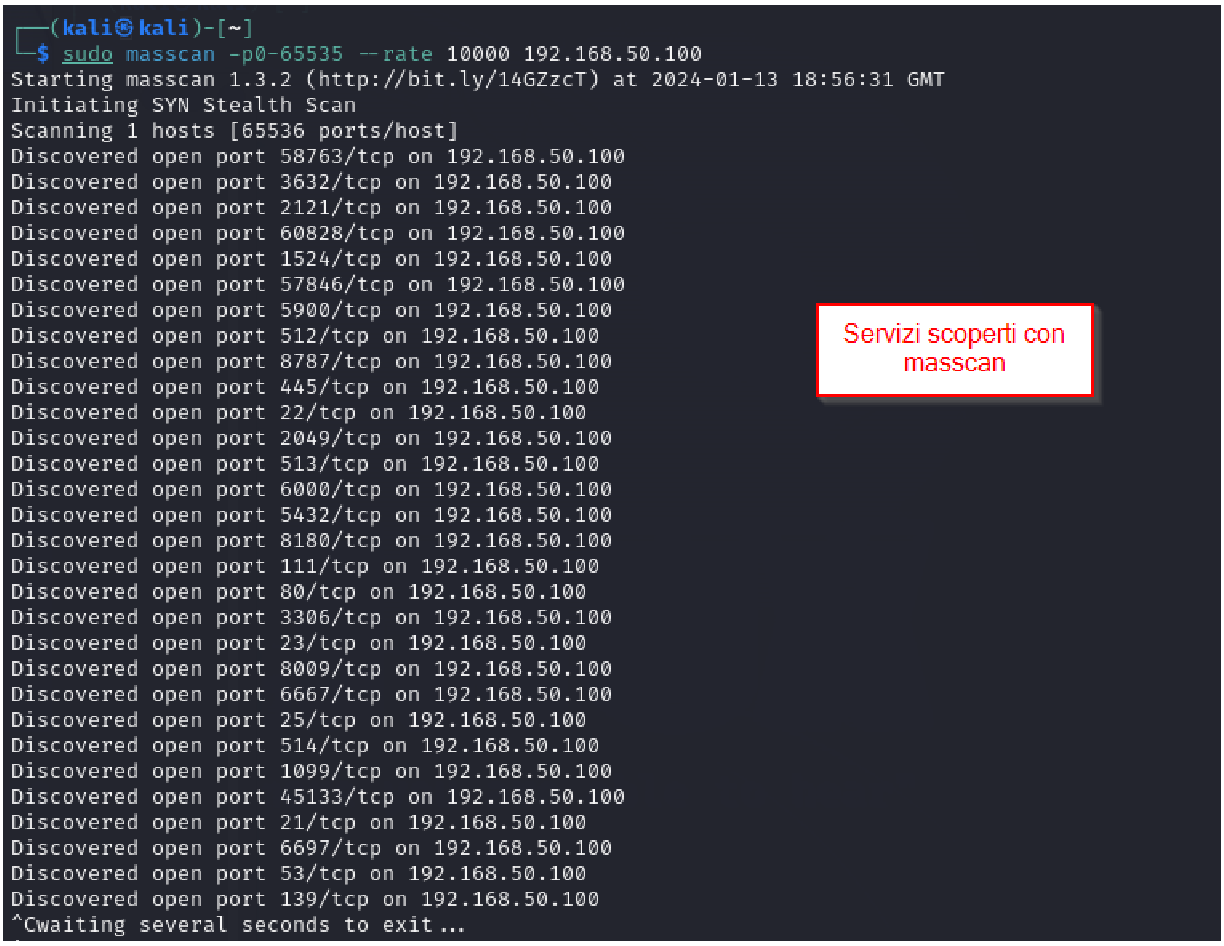


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -f -mtu=512 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-13 13:45 EST
Nmap scan report for 192.168.50.100
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Scan con pacchetti frammentati da 512 byte

In questo caso andiamo a testare la resilienza delle porte di Metasploitable 2. Per mezzo di -f i pacchetti vengono inviati frammentati, mentre L'MTU viene settato a 512 byte.

13. sudo masscan -p0-65535 –rate 1000 192.168.50.100



```
┌──(kali㉿kali)-[~]
└─$ sudo masscan -p0-65535 --rate 10000 192.168.50.100
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-01-13 18:56:31 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
Discovered open port 58763/tcp on 192.168.50.100
Discovered open port 3632/tcp on 192.168.50.100
Discovered open port 2121/tcp on 192.168.50.100
Discovered open port 60828/tcp on 192.168.50.100
Discovered open port 1524/tcp on 192.168.50.100
Discovered open port 57846/tcp on 192.168.50.100
Discovered open port 5900/tcp on 192.168.50.100
Discovered open port 512/tcp on 192.168.50.100
Discovered open port 8787/tcp on 192.168.50.100
Discovered open port 445/tcp on 192.168.50.100
Discovered open port 22/tcp on 192.168.50.100
Discovered open port 2049/tcp on 192.168.50.100
Discovered open port 513/tcp on 192.168.50.100
Discovered open port 6000/tcp on 192.168.50.100
Discovered open port 5432/tcp on 192.168.50.100
Discovered open port 8180/tcp on 192.168.50.100
Discovered open port 111/tcp on 192.168.50.100
Discovered open port 80/tcp on 192.168.50.100
Discovered open port 3306/tcp on 192.168.50.100
Discovered open port 23/tcp on 192.168.50.100
Discovered open port 8009/tcp on 192.168.50.100
Discovered open port 6667/tcp on 192.168.50.100
Discovered open port 25/tcp on 192.168.50.100
Discovered open port 514/tcp on 192.168.50.100
Discovered open port 1099/tcp on 192.168.50.100
Discovered open port 45133/tcp on 192.168.50.100
Discovered open port 21/tcp on 192.168.50.100
Discovered open port 6697/tcp on 192.168.50.100
Discovered open port 53/tcp on 192.168.50.100
Discovered open port 139/tcp on 192.168.50.100
^Cwaiting several seconds to exit...
```

Servizi scoperti con masscan

Lo strumento masscan scansiona tutte le porte di Meta con una velocità di 1000 pacchetti al secondo.

SCAN SOURCE	SCAN TARGET	SCAN TYPE	RESULTS
-OS: Kali GNU/Linux(2023.4) -Tool: nmap	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- sudo nmap -sn -PE 192.168.50.100	- 1 host attivo
-OS: Kali GNU/Linux(2023.4) -Tool: netdiscover	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- sudo netdiscover -r 192.168.50.100	- un indirizzo trovato nel network del target, esso ha: - IP 192.168.1.1 - MAC 08:00:27:6D:2°:19 - MAC vendor PCS systemtecnick GmbH
-OS: Kali GNU/Linux(2023.4) -Tool: crackmapexec	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- sudo crackmapexec 192.168.50.100	- 7 servizi scansionati, tra cui: - WINRM, SSH, MSSQL, RDP, SMP, LDAP, FTP
-OS: Kali GNU/Linux(2023.4) -Tool: nmap	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- Sudo nmap 192.168.50.100 -top-ports 10 -open	- Scansione di 10 porte TCP aperte e principali, tra cui: -21/FTP, 22/SSH, 23/telnet, 25/SMTP,

			80/HTTP, 139/netbios-ssn, 445/Microsoft-ds
-OS: Kali GNU/Linux(2023.4) -Tool: nmap	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- nmap 192.168.50.100 -p- -sV –reason –dns-server ns	- Scansione di tutte le porte attive + versioni tecnologie + REASON collegamento
-OS: Kali GNU/Linux(2023.4) -Tool: unicornscan	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- us -mT -Iv 192.168.50.100:a -r 3000 -R 3 && us -mU -Iv 192.168.50.100:a -r 3000 -R 3	- Scansione di tutte le porte TCP e tentata scansione di tutte le porte UDP
-OS: Kali GNU/Linux(2023.4) -Tool: nmap	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- sudo nmap -sS -sV -T4 192.168.50.100	- Scansione Stealth di tutte le porte aperte + versione di ciascuna
-OS: Kali GNU/Linux(2023.4) -Tool: hping3	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- sudo hping3 -8 0-1023 -S 192.168.50.100	- Scansione TCP di tutte le well known ports per controllo risposta (ICMP)
-OS: Kali GNU/Linux(2023.4)	-OS: Unix (Samba	- nc -nvz 192.168.50.100 1-1024	- Scansione Steealth delle porte disponibili

-Tool: netcat	3.0.20-Debian) IPV4: 192.168.50.100		nel range 1-1024
-OS: Kali GNU/Linux(2023.4) -Tool: netcat	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- nc -nv 192.168.50.100 22	Scansione TCP completa della sola porta 22/SSH - versione 2.0 OpenSSH_4.7p1
-OS: Kali GNU/Linux(2023.4) -Tool: nmap	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- sudo nmap -sV 192.168.50.100	- Scansione di tutte le porte attive + versioni
-OS: Kali GNU/Linux(2023.4) -Tool: nmap	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- sudo nmap -f -mtu=512 192.168.50.100	- Scansione porte ed testing resilienza. Invio pacchetti frammentati aventi MTU da 512 byte
-OS: Kali GNU/Linux(2023.4) -Tool: masscan	-OS: Unix (Samba 3.0.20-Debian) IPV4: 192.168.50.100	- sudo masscan -p0-65535 –rate 1000 192.168.50.100	- Scansione porte completa