

The background features a dark blue field with several concentric circles in lighter shades of blue. On the right side, there is a red fingerprint pattern that overlaps with the circles.

Scansione dei servizi con Nmap

```
Initiating OS detection (try #1) against 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.0025s 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  filtered 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  filtered ajp13
8180/tcp  open  unknown
MAC Address: 2E:29:34:08:0D:08 (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.8 - 2.6.30
Uptime guess: 0.006 days (since Wed May 8 16:06:58 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.03 seconds
Raw packets sent: 1028 (46.074KB) | Rcvd: 1012 (41.242KB)
```

sudo nmap -O

identificare da remoto il sistema operativo di un host attraverso il fingerprint dello stack TCP/IP. Nmap invia una serie di pacchetti TCP ed UDP all'host remoto ed esamina ogni bit ricevuto in risposta.

sudo nmap -sS

con l'opzione -sS, si sta specificando di eseguire una "scansione SYN". Questo tipo di scansione invia pacchetti SYN (iniziali) ai porti di destinazione e ascolta le risposte. Se viene ricevuta una risposta SYN/ACK, il porto è considerato aperto, se viene ricevuta una risposta RST, il porto è considerato chiuso.

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-08 16:22 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 978 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  filtered  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  filtered  ajp13
MAC Address: 2E:29:34:08:0D:08 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
```

sudo nmap -sT

L'opzione -sT in nmap specifica una "scansione TCP connect", che è una tecnica di scansione più tradizionale e meno furtiva rispetto alla scansione SYN. In questa modalità, nmap tenta di stabilire una connessione TCP completa con il target sui porti specificati. Se la connessione ha successo, il porto viene considerato aperto, altrimenti viene considerato chiuso

```
(kali㉿kali)-[~]
$ nmap -sT 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-08 16:26 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0025s latency).
Not shown: 977 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  filtered 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  filtered ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.31 seconds
```


sudo nmap -sV

L'opzione -sV in nmap indica di eseguire una "scansione di versione". Questo tipo di scansione va oltre la semplice identificazione delle porte aperte, cercando di determinare anche le versioni dei servizi che rispondono su tali porte.

Quando si esegue `sudo nmap -sV`, nmap cercherà di determinare non solo lo stato delle porte (aperte o chiuse) tramite la scansione TCP, ma anche di identificare quali servizi sono in esecuzione su tali porte e, se possibile, determinare la versione di tali servizi. Questo è utile per capire quali software specifici stanno girando su una determinata macchina, il che può aiutare a valutare la sicurezza della rete e individuare potenziali vulnerabilità.

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-08 16:31 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0026s latency).
Not shown: 977 closed tcp ports (conn-refused)
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  filtered ingreslock
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  filtered ajp13
8180/tcp  open  unknown
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 187.00 seconds
```

```
(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.103
[sudo] password di kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-08 16:37 CEST
Nmap scan report for 192.168.50.103
Host is up (0.0054s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 7E:03:BE:74:74:34 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
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 19.70 seconds
```

sudo nmap -sV

L'opzione -O in nmap indica di eseguire il rilevamento del sistema operativo. Quando si utilizza questa opzione, nmap cercherà di determinare il sistema operativo del target in base alle risposte ottenute durante la scansione. Questo comando esegue una scansione del target specificato e cerca di identificare il sistema operativo del target basandosi su caratteristiche di risposta specifiche durante la scansione.