

```
(root@kali)~[/home/kali]
# nmap -O 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:30 EST
Nmap scan report for 192.168.49.101
Host is up (0.0030s 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    filtered 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 3.18 seconds
```

L'analisi condotta tramite Nmap ha fornito una visione dettagliata dei servizi in esecuzione su un host specifico (Indirizzo IP: 192.168.49.101) sulla rete target. Questo report mira a sintetizzare i risultati ottenuti da tale scansione.

Risultati dell'Analisi: Durante l'analisi, sono stati identificati diversi servizi in esecuzione sull'host target. Di seguito sono riportati i dettagli specifici relativi alle porte aperte e ai servizi associati:

- **Porte e Servizi Aperti:**
 - 21/tcp - Servizio: ftp
 - 22/tcp - Servizio: ssh
 - 23/tcp - Servizio: telnet
 - 25/tcp - Servizio: smtp
 - 53/tcp - Servizio: domain
 - 111/tcp - Servizio: rpcbind
 - 139/tcp - Servizio: netbios-ssn
 - 445/tcp - Servizio: microsoft-ds
 - 512/tcp - Servizio: exec
 - 513/tcp - Servizio: login
 - 514/tcp - Servizio: shell
 - 1099/tcp - Servizio: rmiregistry
 - 1524/tcp - Servizio: ingreslock
 - 2049/tcp - Servizio: nfs
 - 2121/tcp - Servizio: ccproxy-ftp
 - 3306/tcp - Servizio: mysql
 - 5432/tcp - Servizio: postgresql
 - 5900/tcp - Servizio: vnc
 - 6000/tcp - Servizio: X11
 - 6667/tcp - Servizio: irc

- 8009/tcp - Servizio: ajp13
- 8180/tcp - Servizio: unknown
- **Tipo di Dispositivo:** Dispositivo a uso generale
- **Sistema Operativo:** Linux 2.6.X
- **Dettagli OS:** Si ritiene che il sistema operativo in esecuzione sia una versione di Linux compresa tra la 2.6.15 e la 2.6.26, con alta probabilità di essere incorporato in un dispositivo.

Analisi dei Risultati: L'analisi ha rivelato una vasta gamma di servizi in esecuzione sull'host target, inclusi servizi di rete comuni come SSH (22/tcp), FTP (21/tcp), SMTP (25/tcp), e servizi di database come MySQL (3306/tcp) e PostgreSQL (5432/tcp). La presenza di servizi come Telnet (23/tcp) e IRC (6667/tcp) può indicare potenziali rischi per la sicurezza, in quanto tali protocolli sono noti per le vulnerabilità associate.

Conclusioni: Basandoci sui risultati dell'analisi Nmap, possiamo concludere che l'host target è un dispositivo Linux con una vasta gamma di servizi attivi.

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:32 EST
Nmap scan report for 192.168.49.101
Host is up (0.0035s 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    filtered 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 1.65 seconds
```

L'analisi tramite Nmap ha rivelato un singolo host attivo con un totale di 24 porte TCP aperte su di esso. La scansione ha rilevato un'attività minima di latenza, indicando una connessione di rete stabile e reattiva.

Dettagli dell'Host:

- **Indirizzo IP:** 192.168.49.101
- **Latency:** 0.0055s

Porte Aperte e Servizi:

- 21/tcp - ftp
- 22/tcp - ssh

- 23/tcp - telnet
- 25/tcp - smtp
- 53/tcp - domain
- 80/tcp - http (filtrato)
- 111/tcp - rpcbind
- 139/tcp - netbios-ssn
- 445/tcp - microsoft-ds
- 512/tcp - exec
- 513/tcp - login
- 514/tcp - shell
- 1099/tcp - rmiregistry
- 1524/tcp - ingreslock
- 2049/tcp - nfs
- 2121/tcp - ccproxy-ftp
- 3306/tcp - mysql
- 5432/tcp - postgresql
- 5900/tcp - vnc
- 6000/tcp - X11
- 6667/tcp - irc
- 8009/tcp - ajp13
- 8180/tcp - unknown

Tempo di Scansione:

- Scansione completata in 1.78 secondi

Conclusioni: L'host 192.168.49.101 ospita una vasta gamma di servizi, tra cui protocolli di rete comuni come FTP, SSH e Telnet, nonché servizi di database come MySQL e PostgreSQL. È importante notare che la porta 80/tcp è filtrata, indicando una possibile restrizione nell'accesso tramite HTTP.

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:34 EST
Nmap scan report for 192.168.49.101
Host is up (0.013s 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    filtered  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 1.68 seconds
```

L'analisi condotta tramite Nmap sull'indirizzo IP 192.168.49.101 ha rivelato un totale di 23 porte aperte su questo host. Di seguito sono riportati i dettagli relativi alle porte aperte e ai servizi associati:

- **Porte e Servizi Aperti:**
 - 21/tcp - Servizio: ftp
 - 22/tcp - Servizio: ssh
 - 23/tcp - Servizio: telnet
 - 25/tcp - Servizio: smtp
 - 53/tcp - Servizio: domain
 - 80/tcp - Stato: filtrato (http)
 - 111/tcp - Servizio: rpcbind
 - 139/tcp - Servizio: netbios-ssn
 - 445/tcp - Servizio: microsoft-ds
 - 512/tcp - Servizio: exec
 - 513/tcp - Servizio: login
 - 514/tcp - Servizio: shell
 - 1099/tcp - Servizio: rmiregistry
 - 1524/tcp - Servizio: ingreslock
 - 2049/tcp - Servizio: nfs
 - 2121/tcp - Servizio: ccproxy-ftp
 - 3306/tcp - Servizio: mysql
 - 5432/tcp - Servizio: postgresql
 - 5900/tcp - Servizio: vnc
 - 6000/tcp - Servizio: X11

- 6667/tcp - Servizio: irc
- 8009/tcp - Servizio: ajp13
- 8180/tcp - Servizio: sconosciuto

Analisi dei Risultati: L'host 192.168.49.101 presenta una vasta gamma di servizi attivi, che includono protocolli di rete comuni come SSH (22/tcp), FTP (21/tcp), SMTP (25/tcp), e servizi di database come MySQL (3306/tcp) e PostgreSQL (5432/tcp). Tuttavia, la porta 80/tcp è stata contrassegnata come "filtrata", il che suggerisce che potrebbe esserci un firewall o un filtro di rete che impedisce l'accesso al servizio HTTP su questa porta.

Conclusioni: L'analisi Nmap ha fornito una panoramica dettagliata dei servizi in esecuzione sull'host 192.168.49.101.

```
(root@kali) ~ /home/kali
nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:37 EST
Nmap scan report for 192.168.49.101
Host is up (0.0068s 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    filtered http
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?
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
514/tcp   open  java-rmi     GNU Classpath g miregistry
1099/tcp  open  bindshell    Metasploitable root shell
1524/tcp  open  bindshell    2-4 (RPC #100003)
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 64.97 seconds
```

L'analisi tramite Nmap ha rivelato un singolo host attivo con un totale di 21 porte TCP aperte su di esso. La scansione ha evidenziato una latenza minima, indicando una connessione di rete reattiva e stabile.

Dettagli dell'Host:

- **Indirizzo IP:** 192.168.49.101
- **Latency:** 0.0061s

Porte Aperte e Servizi:

- 21/tcp - ftp (vsftpd 2.3.4)
- 22/tcp - ssh (OpenSSH 4.7p1 Debian 8ubuntu1)
- 23/tcp - telnet (Linux telnetd)
- 25/tcp - smtp (Postfix smtpd)
- 53/tcp - domain (ISC BIND 9.4.2)
- 111/tcp - rpcbind (2 - RPC #100000)
- 139/tcp - netbios-ssn (Samba smbd 3.X - 4.X)
- 445/tcp - netbios-ssn (Samba smbd 3.X - 4.X)
- 512/tcp - exec?

- 513/tcp - login (OpenBSD or Solaris rlogind)
- 514/tcp - tcpwrapped
- 1099/tcp - java-rmi (GNU Classpath grmiregistry)
- 1524/tcp - bindshell (Metasploitable root shell)
- 2049/tcp - nfs (2-4 - RPC #100003)
- 2121/tcp - ftp (ProFTPD 1.3.1)
- 3306/tcp - mysql (MySQL 5.0.51a-3ubuntu5)
- 5432/tcp - postgresql (PostgreSQL DB 8.3.0 - 8.3.7)
- 5900/tcp - vnc (VNC - protocollo 3.3)
- 6000/tcp - X11 (accesso negato)
- 6667/tcp - irc (UnrealIRCd)
- 8009/tcp - ajp13 (Apache Jserv - Protocollo v1.3)
- 8180/tcp - http (Apache Tomcat/Coyote JSP engine 1.1)

Informazioni sui Servizi:

- Hosts: metasploitable.localdomain, irc.Metasploitable.LAN
- Sistemi Operativi: Unix, Linux
- CPE: cpe:/o:linux:linux_kernel

Tempo di Scansione:

- Scansione completata in 67.19 secondi

Conclusioni: L'host 192.168.49.101 ospita una vasta gamma di servizi, tra cui protocolli di rete comuni come FTP, SSH e SMTP, nonché servizi di database come MySQL e PostgreSQL

```
(root@kali) ~ [~/home/kali]
# nmap -O 192.168.49.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:47 EST
Nmap scan report for 192.168.49.102
Host is up (0.0033s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msvcpc
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
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista:- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008::sp2
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows
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 2.11 seconds

(root@kali) ~ [~/home/kali]
# nmap -O 192.168.49.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:48 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds

(root@kali) ~ [~/home/kali]
# nmap -O -Pn 192.168.49.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:49 EST
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.00% done; ETC: 09:52 (0:02:49 remaining)
Stats: 0:02:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 72.50% done; ETC: 09:52 (0:00:55 remaining)
Nmap scan report for 192.168.49.102
Host is up.
All 1000 scanned ports on 192.168.49.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.87 seconds
```

Abbiamo infine notato che sulla macchina Windows7, il firewall rende la comunicazione impossibile.

L'analisi tramite Nmap con l'opzione -O per la rilevazione del sistema operativo è stata condotta sull'indirizzo IP 192.168.49.102. Tuttavia, l'host sembra essere non raggiungibile o inattivo durante la scansione.

Dettagli dell'Host:

- **Indirizzo IP:** 192.168.49.102
- **Stato dell'Host:** Non raggiungibile o inattivo

Tempo di Scansione:

- Scansione completata in 3.16 secondi

Conclusioni: L'analisi tramite Nmap non è riuscita a rilevare l'host 192.168.49.102 attivo durante la scansione. È possibile che l'host sia effettivamente inattivo o che blocchi le sonde di ping inviate da Nmap

Abbiamo provato anche senza effettuare il ping con l'opzione -Pn.

L'analisi tramite Nmap con l'opzione -O e -Pn per la rilevazione del sistema operativo è stata condotta sull'indirizzo IP 192.168.49.102. Durante la scansione, l'host è risultato attivo, ma tutti i 1000 porte TCP scansionate sono state rilevate come ignorate o filtrate.

Dettagli dell'Host:

- **Indirizzo IP:** 192.168.49.102
- **Stato dell'Host:** Attivo

Risultati della Scansione:

- **Porte TCP Scansionate:** 1000
- **Stato delle Porte Scansionate:** Ignorate o filtrate
 - Non mostrate: 1000 porte TCP filtrate (no-response)

Conclusioni: L'analisi tramite Nmap ha rilevato l'host 192.168.49.102 come attivo, ma tutte le porte TCP scansionate sono state rilevate come ignorate o filtrate, senza risposta

Disattivando invece il firewall, riceviamo le risposte come da screen.