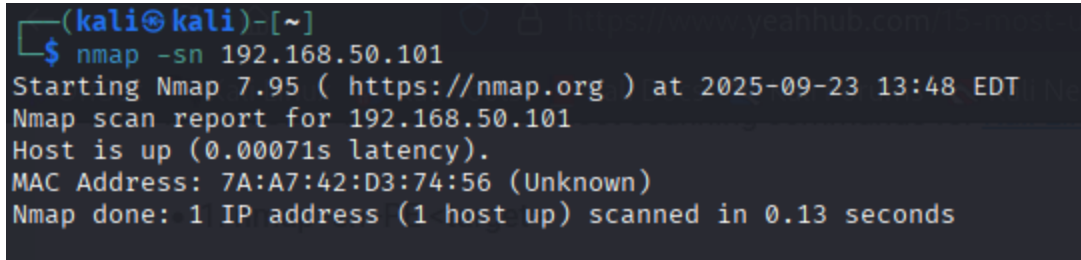


Report Bruni Gabriele

I Comandi Utilizzati dal sito we: <https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/>

1. `nmap -sn 192.168.50.101` Questo comando esegue una scansione ping per verificare se l'host è attivo senza scansionare le sue porte.

A terminal window screenshot from a Kali Linux system. The prompt is (kali@kali)-[~]. The command entered is \$ nmap -sn 192.168.50.101. The output shows: Starting Nmap 7.95 (https://nmap.org) at 2025-09-23 13:48 EDT, Nmap scan report for 192.168.50.101, Host is up (0.00071s latency), MAC Address: 7A:A7:42:D3:74:56 (Unknown), and Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds.

```
(kali@kali)-[~]  
$ nmap -sn 192.168.50.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 13:48 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00071s latency).  
MAC Address: 7A:A7:42:D3:74:56 (Unknown)  
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

2. `nmap 192.168.50.101 --top-ports 10` Questo comando esegue una scansione rapida che si concentra solo sulle 10 porte TCP più comuni, fornendo un'istantanea dei servizi più probabili.

```
* 1. nmap -sn -PE <target>
(kali@kali)-[~]
$ nmap 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 13:49 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00042s 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  vncap
6000/tcp  open  X11
6667/tcp  open  ircscan
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 7A:A7:42:D3:74:56 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

3. `nmap -f --mtu 512 192.168.50.101` Questo comando utilizza la frammentazione dei pacchetti per testare l'evasione dei firewall.

```

(kali㉿kali)-[~]
$ nmap -f --mtu 512 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 13:49 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00037s 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: 7A:A7:42:D3:74:56 (Unknown)

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

```

4. `netdiscover -r 192.168.50.101/24` Questo comando usa Netdiscover per scansionare l'intera sottorete (in questo caso, 192.168.50.0/24) usando richieste ARP per trovare tutti gli host attivi.

```

Currently scanning: Finished! | Screen View: Unique Hosts
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 84

```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.50.1	d2:11:e5:3e:4d:64	1	42	Unknown vendor
192.168.50.101	7a:a7:42:d3:74:56	1	42	Unknown vendor

```

• 2. netdiscover -r <target>
• 3. crackmapexec <target>
• 4. nmap <targets> -p- --top-ports 10 --open

```

5. `nc -nvz 192.168.50.101 1-1024` Questo comando utilizza Netcat per eseguire una

scansione di base delle porte da 1 a 1024.

```
(kali㉿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
```