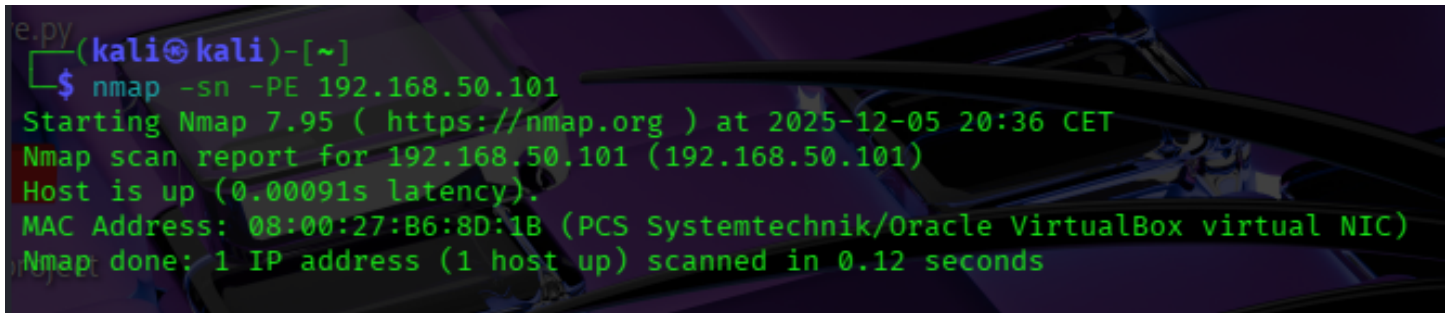


## Traccia Esercizio

Dopo aver visitato il sito <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.

### **nmap -sn -PE <target>**

A terminal window with a dark background and green text. The prompt is '(kali㉿kali)-[~]'. The command '\$ nmap -sn -PE 192.168.50.101' has been entered. The output shows the Nmap version (7.95), the target IP (192.168.50.101), and the result 'Host is up (0.00091s latency)'. It also displays the MAC address '08:00:27:B6:8D:1B' and identifies it as a 'PCS Systemtechnik/Oracle VirtualBox virtual NIC'. The scan completed in 0.12 seconds.

```
e.py(kali㉿kali)-[~]  
$ nmap -sn -PE 192.168.50.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 20:36 CET  
Nmap scan report for 192.168.50.101 (192.168.50.101)  
Host is up (0.00091s latency).  
MAC Address: 08:00:27:B6:8D:1B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Con questo primo scan riusciamo a scoprire che la macchina target è attiva

### **netdiscover -r <target>**

```
root@kali: /home/kali
Session Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
6 Captured ARP Req/Rep packets, from 3 hosts. Total size: 360
+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.1.1  | 50:42:89:7d:79:1f | 2     | 120 | zte corporation       |
| 192.168.1.2  | 8c:4f:00:04:0d:e4 | 2     | 120 | Espressif Inc.        |
| 192.168.1.4  | 10:97:bd:93:67:d8 | 2     | 120 | Espressif Inc.        |
+-----+-----+-----+-----+-----+-----+
```

Qui possiamo vedere tutti i dispositivi attivi in una determinata rete, compresi di indirizzo MAC

## crackmapexec protocollo <target>

```
(root@kali)-[/home/kali]
# crackmapexec smb 192.168.50.101
SMB 192.168.50.101 445 METASPLOITABLE [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)
```

Ecco qui che scopriamo che la macchina con cui comunichiamo ha come OS metasploitable

## nmap <target> -top-ports 10 -aperto

```
(root@kali)-[/home/kali]
# nmap 192.168.50.101 -top-ports 10 -open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 20:51 CET
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00076s 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:B6:8D:1B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.78 seconds
```

In questo caso il comando è autoesplicativo, scopriamo altre informazioni importanti, cioè le porte aperte sulla macchina

## nmap <target> -p- -sV -reason -dns-server ns

```
root@kali: /home/kali
Session Actions Edit View Help
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-il <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
--sn: List Scan - simply list targets to scan
--sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given port
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports sequentially - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
-sC: equivalent to --script=default
```

**-p-** → scansiona **tutte le porte (1-65535)**

**-sV** → identifica la **versione dei servizi** su ogni porta aperta

**--reason** → ti mostra **perché** una porta risulta aperta/chiusa (il “motivo” del risultato)

**--dns-server <ns>** → usa **quel DNS specifico** invece di quello di default

# info raccolte

IP: 192.168.50.101

DISPOSITIVI NELLA RETE: 3

OS: META

PORTE APERTE: 21 22 23 25 80 139 445

MAC: 08:00:27:B6:8D:1B