# ENUMERAZIONE SERVIZI E SCANSIONE (1)
## FASE DI RACCOLTA INFORMAZIONI

**Traccia**

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.

Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

### nmap -sn -PE <target>

Il comando nmap -sn -PE <target> viene utilizzato per eseguire una scansione ping sull'host di destinazione. Questa scansione viene utilizzata per determinare quali host sono attivi e in esecuzione sulla rete. L'opzione -sn indica a Nmap di non eseguire una scansione delle porte dopo l'individuazione dell'host e l'opzione -PE indica a Nmap di utilizzare la richiesta echo ICMP anziché i pacchetti TCP SYN per l'individuazione dell'host

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.50.109
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 01:46 CEST
Nmap scan report for 192.168.50.109
Host is up (0.0022s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.02 seconds
```

### nmap <target> –top-ports 10 –open

Con l'opzione *–top-ports*, puoi facilmente identificare le prime 10 porte aperte in qualsiasi rete. In questo caso i servizi ftp, ssh, telnet, smtp, http, netbios-ssn e microsoft-ds sono aperti mentre i servizi pop3, https e ms-wbt-server sono chiusi

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.109 -top-ports 10-open
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 01:48 CEST
Nmap scan report for 192.168.50.109
Host is up (0.0024s latency).

PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
23/tcp   open   telnet
25/tcp   open   smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  open   netbios-ssn
443/tcp  closed https
445/tcp  open   microsoft-ds
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
```

## nmap -sS -sV -T4 <target>

Il comando seguente determina se la porta è in ascolto. L'utilizzo di questo comando è una tecnica chiamata scansione semiaperta. Si chiama scansione semiaperta perché non si stabilisce una connessione TCP completa. Invece, si invia solo un pacchetto SYN e si attende la risposta. Se ricevi una risposta SYN/ACK significa che la porta è in ascolto:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -T4 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 01:51 CEST
Nmap scan report for 192.168.50.109
Host is up (0.0014s 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  shell       Netkit rshd
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
MAC Address: 08:00:27:BC:3B:1B (Oracle VirtualBox virtual NIC)
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 24.79 seconds
```

## nc -nvz <target> 1-1024

Netcat è un'utilità di rete in primo piano che legge e scrive dati attraverso le connessioni di rete, utilizzando il protocollo TCP / IP. Qui il flag -n viene utilizzato per specificare che non è necessario risolvere l'indirizzo IP utilizzando DNS.

```
┌──(kali㉿kali)-[~]
└─$ nc -nvz 192.168.50.109 1-1080
(UNKNOWN) [192.168.50.109] 514 (shell) open
(UNKNOWN) [192.168.50.109] 513 (login) open
(UNKNOWN) [192.168.50.109] 512 (exec) open
(UNKNOWN) [192.168.50.109] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.109] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.109] 111 (sunrpc) open
(UNKNOWN) [192.168.50.109] 80 (http) open
(UNKNOWN) [192.168.50.109] 53 (domain) open
(UNKNOWN) [192.168.50.109] 25 (smtp) open
(UNKNOWN) [192.168.50.109] 23 (telnet) open
(UNKNOWN) [192.168.50.109] 22 (ssh) open
(UNKNOWN) [192.168.50.109] 21 (ftp) open
```

**nmap <target> -p- -sV –reason —dns-server ns**

Può essere utile comprendere il motivo per cui una porta è contrassegnata come **aperta**, **chiusa** o **filtrata** e perché l'host è contrassegnato come **attivo**. Questo può essere fatto usando il flag –reason.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.109 -p- -sV --reason --dns-server ns
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 02:01 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid serv
ers with --dns-servers
Nmap scan report for 192.168.50.109
Host is up, received syn-ack (0.0019s 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  shell       syn-ack Netkit rshd
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
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)
38735/tcp open  status      syn-ack 1 (RPC #100024)
53056/tcp open  nlockmgr    syn-ack 1-4 (RPC #100021)
54415/tcp open  java-rmi    syn-ack GNU Classpath grmiregistry
57181/tcp open  mountd      syn-ack 1-3 (RPC #100005)
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 141.58 seconds
```

**nmap -sV <target>**

A volte, potrebbe essere necessario rilevare informazioni sul servizio e sulla versione da porte aperte. Ciò è utile per la risoluzione dei problemi, la scansione delle vulnerabilità o l'individuazione dei servizi che devono essere aggiornati.