



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 con -sn e -PE ci permette di capire se il target è up o down.

```
(kali㉿kali)-[~]  
$ sudo nmap -sn -PE 192.168.2.99  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 07:37 EST  
Nmap scan report for 192.168.2.99  
Host is up (0.0052s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Netdiscover con il -r target ci offre una cattura dei pacchetti

```
kali@kali: ~  
Currently scanning: Finished! | Screen View: Unique Hosts  
3 Captured ARP Req/Rep packets, from 2 hosts. Total size: 180  
+-----+-----+-----+-----+-----+-----+  
IP           At MAC Address  Count  Len  MAC Vendor / Hostname  
+-----+-----+-----+-----+-----+-----+  
192.168.2.1   08:00:27:92:fd:69    1     60  PCS Systemtechnik GmbH  
192.168.2.99  08:00:27:9c:24:72    2    120  PCS Systemtechnik GmbH
```

Nmap con opzione -sV globale di porte e servizi aperti su un target con anche la descrizione della versione

```
kali@kali: ~  
(kali@kali)-[~]  
$ sudo nmap -sV 192.168.2.99  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 07:48 EST  
Nmap scan report for 192.168.2.99  
Host is up (0.0083s 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?         
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  ccproxy-ftp?   
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 173.29 seconds
```

Con l'utilizzo di unicorn scan sono state identificate porte alte aperte in TCP come la 34844 e la 48655

```
(kali@kali)-[~]  
$ sudo us -mT -Iv 192.168.2.99:a -r 3000 -R 3 56 us -mU -Iv 192.168.2.99:a -r 3000 -R 3  
adding 192.168.2.99/32 mode 'TCPscan' ports 'a' pps 3000  
using interface(s) eth0  
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds  
TCP open 192.168.2.99:512 ttl 63  
TCP open 192.168.2.99:445 ttl 63  
TCP open 192.168.2.99:5432 ttl 63  
TCP open 192.168.2.99:34844 ttl 63  
TCP open 192.168.2.99:48655 ttl 63  
TCP open 192.168.2.99:8787 ttl 63  
TCP open 192.168.2.99:22 ttl 63  
TCP open 192.168.2.99:6000 ttl 63  
TCP open 192.168.2.99:2049 ttl 63  
sender statistics 2917.1 pps with 196608 packets sent total  
TCP open 192.168.2.99:21 ttl 63  
listener statistics 29385 packets recieved 0 packets dropped and 0 interface drops  
TCP open ftp[ 21] from 192.168.2.99 ttl 63  
TCP open ssh[ 22] from 192.168.2.99 ttl 63  
TCP open microsoft-ds[ 445] from 192.168.2.99 ttl 63  
TCP open exec[ 512] from 192.168.2.99 ttl 63  
TCP open shilp[ 2049] from 192.168.2.99 ttl 63  
TCP open postgresql[ 5432] from 192.168.2.99 ttl 63  
TCP open x11[ 6000] from 192.168.2.99 ttl 63  
TCP open msgsrvr[ 8787] from 192.168.2.99 ttl 63  
TCP open unknown[34844] from 192.168.2.99 ttl 63  
TCP open unknown[48655] from 192.168.2.99 ttl 63  
adding 192.168.2.99/32 mode 'UDPscan' ports 'a' pps 3000  
using interface(s) eth0  
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds  
Send [Error socktrans.c:123] bind() path '/var/lib/unicornscan/send' fails: Address already in use  
Send exiting cant create listener socket: system error Address already in use  
Recv [Error socktrans.c:123] bind() path '/var/lib/unicornscan/listen' fails: Address already in use  
Recv exiting cant create listener socket: system error Address already in use
```