

## REPORT W10-D5

### 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.

### COMANDO 1/2

```
Currently scanning: Finished! | Screen View: Unique Hosts
1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 60
+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.32.101 | 08:00:27:44:95:b6 | 1     | 60  | PCS Systemtechnik GmbH |
+-----+-----+-----+-----+-----+-----+

(kali㉿kali)-[~]
$ nmap -sn -PE 192.168.32.100
Warning: You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 14:49 EDT
Nmap scan report for 192.168.32.100
Host is up (0.000082s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds
```

### COMANDO 3

```
(kali㉿kali)-[~]
$ crackmapexec ssh 192.168.32.101
SSH 192.168.32.101 22 192.168.32.101 [*] SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

(kali㉿kali)-[~]
$ crackmapexec rdp 192.168.32.101

(kali㉿kali)-[~]
$ crackmapexec ftp 192.168.32.101
FTP 192.168.32.101 21 192.168.32.101 [*] Banner: (vsFTPD 2.3.4)
```

## REPORT W10-D5

### COMANDO 4

```
(kali㉿kali)-[~]
$ nmap 192.168.32.101 -top-ports 10 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 14:55 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00081s latency).
Not shown: 3 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
```

### COMANDO 5

```
(kali㉿kali)-[~]
$ nmap -f --mtu=512 192.168.32.101
Sorry, but fragscan requires root privileges.
QUITTING!

(kali㉿kali)-[~]
$ sudo nmap -f --mtu=512 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 15:07 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00062s 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: 08:00:27:44:95:B6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

### COMANDO 6

```
su: invalid option -- 'T'
Try 'su --help' for more information.

(kali㉿kali)-[~]
$ sudo us -mT -Iv 192.168.32.101:a -r 3000 -R 3 66 us -mU -Iv 192.168.32.101:a -r 3000 -R 3
adding 192.168.32.101/32 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, 1
TCP open 192.168.32.101:445    ttl 64
TCP open 192.168.32.101:513    ttl 64
TCP open 192.168.32.101:80     ttl 64
TCP open 192.168.32.101:111    ttl 64
TCP open 192.168.32.101:58934  ttl 64
TCP open 192.168.32.101:6667   ttl 64
TCP open 192.168.32.101:25     ttl 64
TCP open 192.168.32.101:139    ttl 64
TCP open 192.168.32.101:6697   ttl 64
TCP open 192.168.32.101:1099   ttl 64
TCP open 192.168.32.101:35486  ttl 64
TCP open 192.168.32.101:3306   ttl 64
TCP open 192.168.32.101:2121   ttl 64
TCP open 192.168.32.101:8180   ttl 64
TCP open 192.168.32.101:512    ttl 64
TCP open 192.168.32.101:3632   ttl 64
TCP open 192.168.32.101:8787   ttl 64
TCP open 192.168.32.101:514    ttl 64
TCP open 192.168.32.101:8009   ttl 64
TCP open 192.168.32.101:6000   ttl 64
TCP open 192.168.32.101:2049   ttl 64
TCP open 192.168.32.101:49312  ttl 64
TCP open 192.168.32.101:22     ttl 64
TCP open 192.168.32.101:5432   ttl 64
TCP open 192.168.32.101:23     ttl 64
TCP open 192.168.32.101:1524   ttl 64
TCP open 192.168.32.101:53     ttl 64
TCP open 192.168.32.101:5900   ttl 64
TCP open 192.168.32.101:21     ttl 64
TCP open 192.168.32.101:44254  ttl 64
^C

(kali㉿kali)-[~]
$
```

### RIEPILOGO FINALE

Per riassumere le informazioni acquisite tramite tutti questi comandi, elenchiamo tutte le info ricavate:

- Tramite il **COMANDO 1** (*nmap -sn -PE "TARGET"*) viene eseguita una scansione di tipo ping dal tool. Lo switch "-sn" va ad indicare ad Nmap di eseguire una scansione tramite ping ai target selezionati disabilitando lo

## **REPORT W10-D5**

scan delle ports, mentre -PE indica il tipo di ping in questo caso ICMP ECHO. Il risultato dello scan indica il target attivo.

- Tramite il **COMANDO 2** (*netdiscover -r "TARGET"*) andiamo ad eseguire il tool netdiscover è uno strumento di discovery di rete utilizzato per identificare dispositivi sulla stessa rete locale. Inserendo lo switch "-r" andiamo a specificare il range di indirizzo da scannerizzare (si potrebbe inserire anche la notazione in CIDR /24).
- Tramite il **COMANDO 3** (*crackmapexec "TARGET"*) utilizzeremo crackmapexec, uno strumento utilizzato per l'automazione e l'esecuzione di attacchi di penetration testing, che utilizzeremo per controllare le ports aperte. Tramite "SSH" e "FTP" abbiamo effettuato banner grabbing alle porte 21-22.
- Tramite il **COMANDO 4** (*nmap "TARGET" -top-ports 10 -open*) in cui lo switch "-top-ports 10" indica 10 delle well known port e "-open" indica di mostrare a schermo solo quelle che risultano aperte.
- Tramite il **COMANDO 5** (*sudo nmap -MTU=512 "TARGET"*) si va a selezionare la dei Maximum Transmission Unit (MTU) a 512 byte tramite lo switch "-MTU".
- Tramite il **COMANDO 6** (*us -mT -lv "TARGET":a -r 3000 -R 3 && us -mU -lv "TARGET":a -r 3000 -R 3*), suddiviso in 2 comandi dal "&" in cui si richiede una TCP scan dallo switch "-mT" e un UDP scan dal "-mU", mentre "-r" indica 3000 pacchetti al secondo e "-R" imposta a 3 il numero dei tentativi falliti.