**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.

**ES:**

**Ambiente:**
Due VM con installati:
-Kali Linux con ip 192.168.1.100 (scheda di rete bridged);
-Metasploitable con ip 192.168.1.101 (scheda di rete bridged).

**Svolgimento:**
Lo scopo di questo esercizio è rintracciare il maggior numero di informazioni riguardo l'obiettivo. Utilizziamo la VM con Kali Linux come macchina "attaccante" mentre Metasploitable come target.
Alcuni comandi dovranno essere eseguiti come root, mentre altri potranno essere eseguiti normalmente da shell:

- nmap -sn -PE <target>

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 10:10 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0010s latency).
MAC Address: 08:00:27:1D:18:5B (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.1.101
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 10:10 EDT
Nmap scan report for 192.168.1.101
Host is up (0.012s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

- netdiscover -r <target>

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

61 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 3660
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.1     08:16:05:c5:66:60     55    3300  Vodafone Italia S.p.A.
192.168.1.5     2c:9e:00:bb:4b:b0      1      60  Sony Interactive Entertainment Inc.
192.168.1.9     70:1a:b8:7f:aa:49      1      60  Intel Corporate
192.168.1.11    50:d4:5c:2d:a4:3c      1      60  Amazon Technologies Inc.
192.168.1.4     1e:10:09:49:e7:38      1      60  Unknown vendor
192.168.1.6     e0:d0:45:32:f1:e5      1      60  Intel Corporate
192.168.1.101   08:00:27:1d:18:5b      1      60  PCS Systemtechnik GmbH
```

- crackmapexec <target>

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec ssh 192.168.1.101
SSH         192.168.1.101   22     192.168.1.101    [*] SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

- nmap <target> –top-ports 10 –open

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.101 --top-ports 10 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 10:03 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0015s 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 0.04 seconds
```

- us -mT -lv <target>:a -r 3000 -R 3 && us -mU -lv <target>:a -r 3000 -R 3

```
┌──(kali㉿kali)-[~]
└─$ us -mT -lv 192.168.1.101:a -r 3000 -R 3 && us -mU -lv 192.168.1.101:a -r 3000 -R 3
Send [Error   socktrans.c:123] bind() path `/var/lib/unicornscan/send' fails: Permission denied
Send exiting cant create listener socket: system error Permission denied
Recv [Error   socktrans.c:123] bind() path `/var/lib/unicornscan/listen' fails: Permission denied
Recv exiting cant create listener socket: system error Permission denied
```

- hping3 –scan known <target>

```
┌──(kali㉿kali)-[~]
└─$ hping3 --scan known 192.168.1.101
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket
```

**Conclusioni:**
Come abbiamo notato tramite la combinazione di diversi tools si può arrivare ad avere informazioni molto importanti riguardo le porte e le comunicazioni attive su un determinato target. In alcuni casi però la macchina bersaglio blocca le richieste e gli scan non fornendo così le informazioni specifiche, ma comunque dando una risposta che resta utile ai nostri fini.