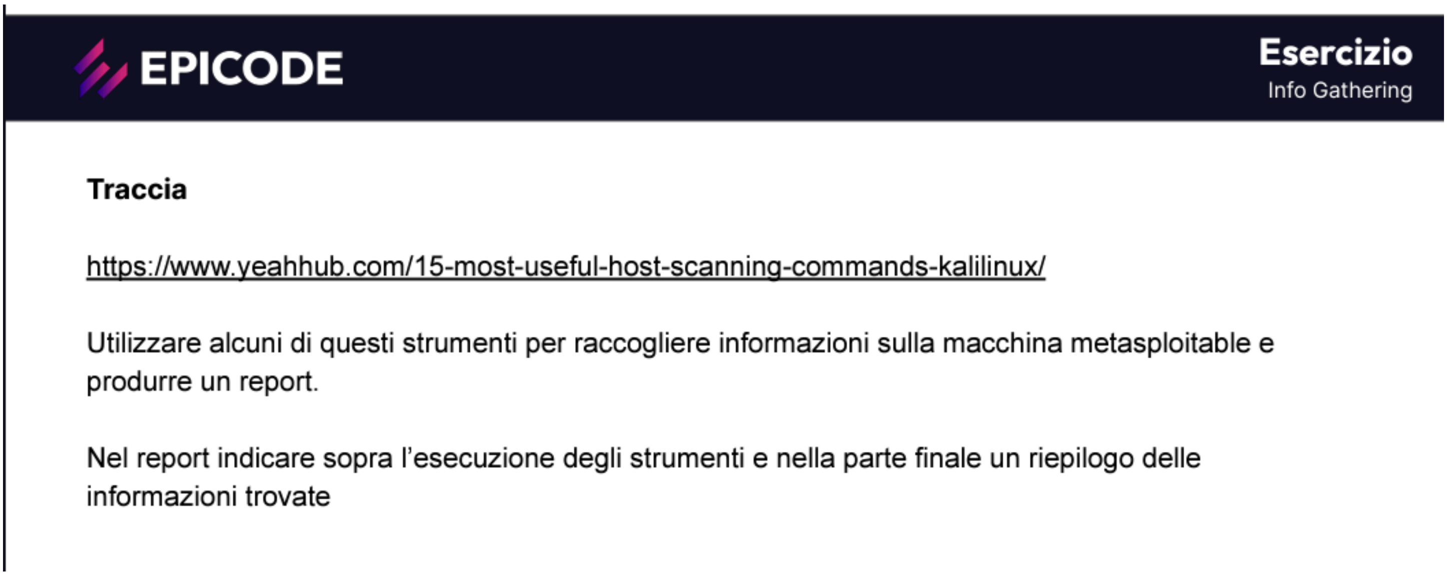
ESERCITAZIONE W10D4



EPICODE

Esercizio
Info Gathering

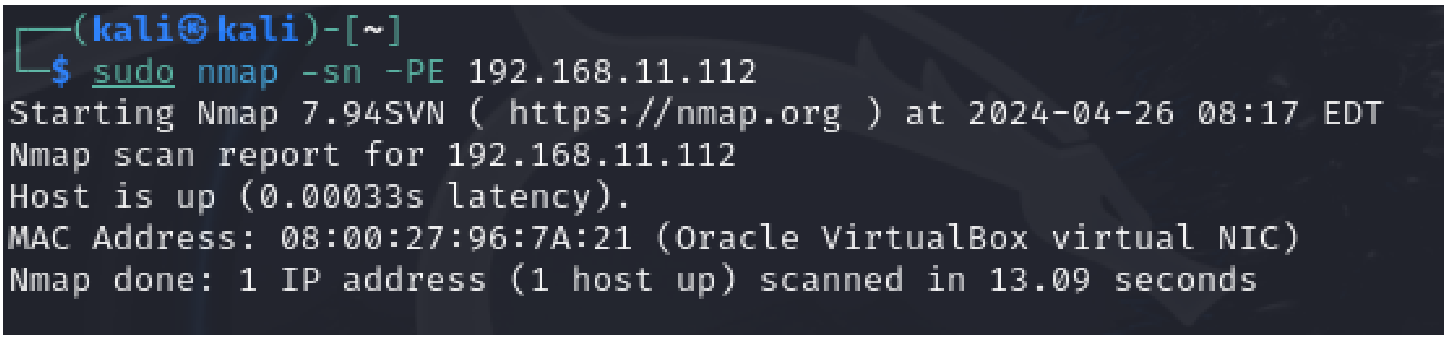
Traccia

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.

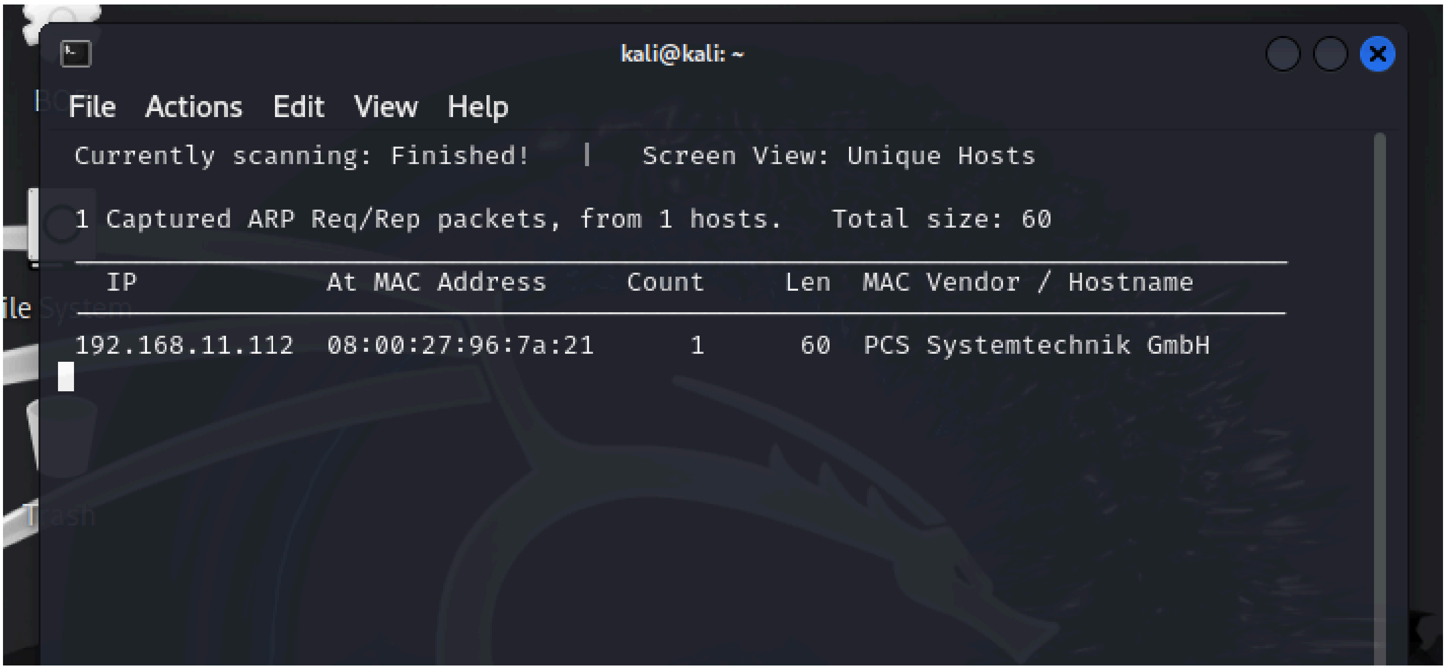
Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

1) Ricognizione attiva con Nmap



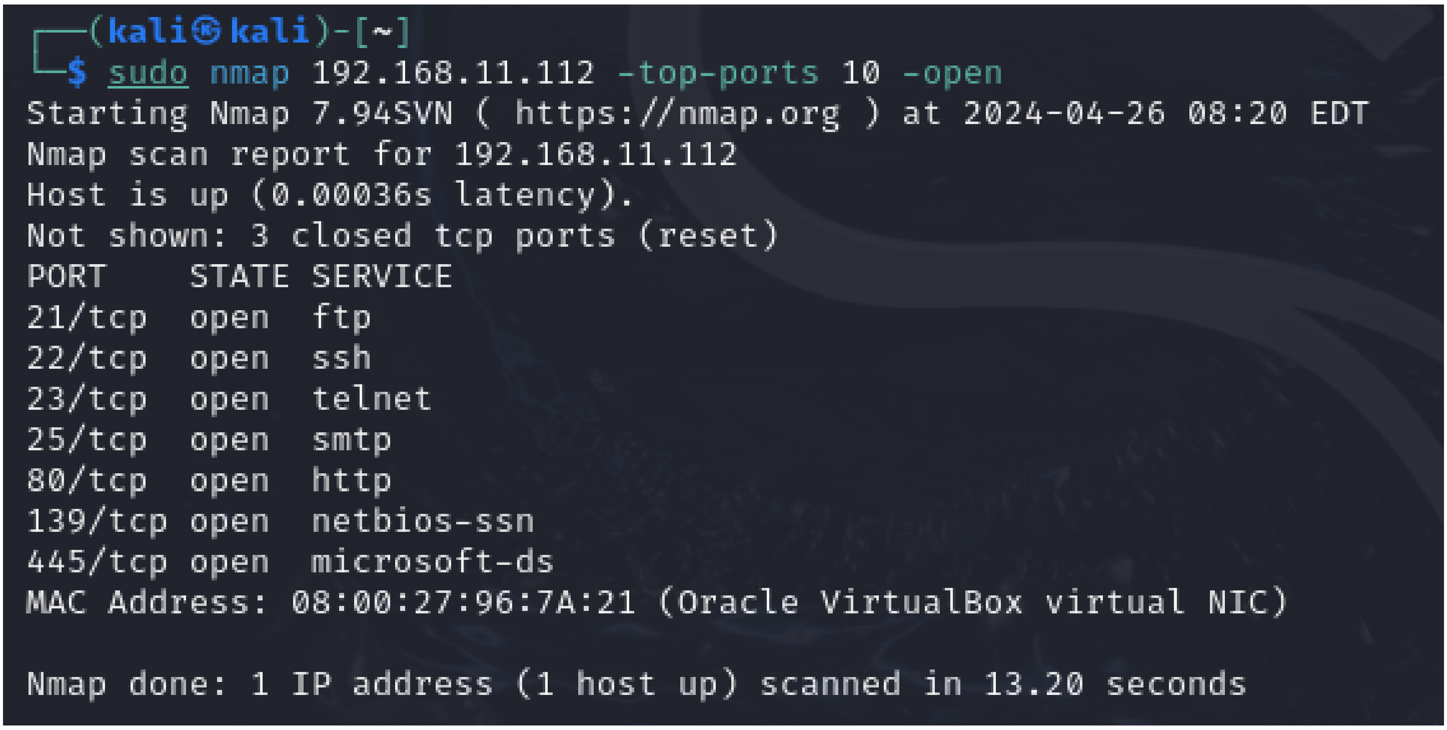
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 08:17 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00033s latency).
MAC Address: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
```

2) trovare host attivi con Netdiscover



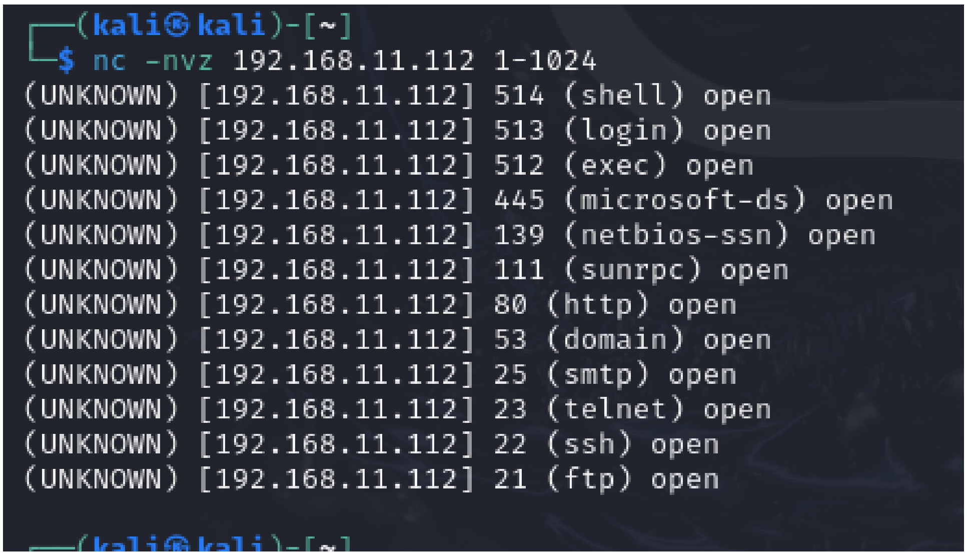
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.11.112  08:00:27:96:7a:21      1      60  PCS Systemtechnik GmbH
```

3) Trova le prime 10 porte aperte con Nmap (Fast Scan)



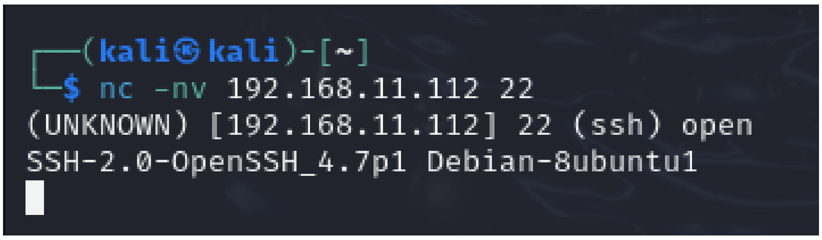
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.11.112 -top-ports 10 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 08:20 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00036s latency).
Not shown: 3 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:96:7A:21 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```

4) Scansione delle porte con Netcat



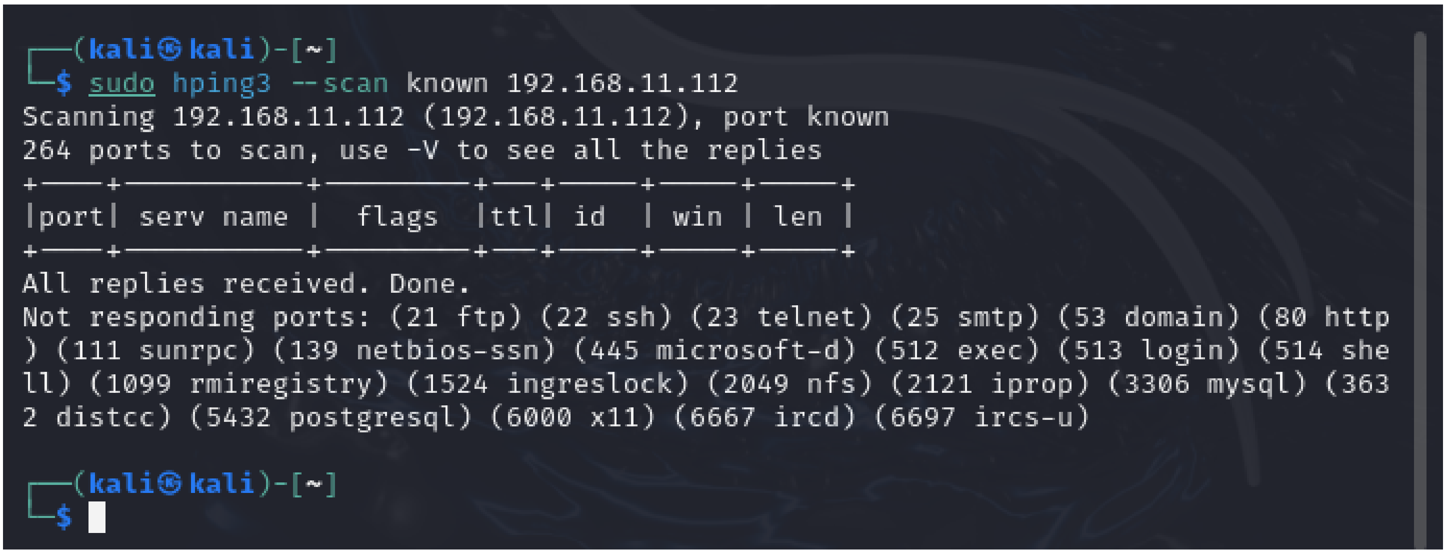
```
┌──(kali㉿kali)-[~]
└─$ nc -nvz 192.168.11.112 1-1024
(UNKNOWN) [192.168.11.112] 514 (shell) open
(UNKNOWN) [192.168.11.112] 513 (login) open
(UNKNOWN) [192.168.11.112] 512 (exec) open
(UNKNOWN) [192.168.11.112] 445 (microsoft-ds) open
(UNKNOWN) [192.168.11.112] 139 (netbios-ssn) open
(UNKNOWN) [192.168.11.112] 111 (sunrpc) open
(UNKNOWN) [192.168.11.112] 80 (http) open
(UNKNOWN) [192.168.11.112] 53 (domain) open
(UNKNOWN) [192.168.11.112] 25 (smtp) open
(UNKNOWN) [192.168.11.112] 23 (telnet) open
(UNKNOWN) [192.168.11.112] 22 (ssh) open
(UNKNOWN) [192.168.11.112] 21 (ftp) open

┌──(kali㉿kali)-[~]
```

5)Acquisizione di banner con Netcat



```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.11.112 22
(UNKNOWN) [192.168.11.112] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
█
```

6) Scansione con HPING3



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --scan known 192.168.11.112
Scanning 192.168.11.112 (192.168.11.112), port known
264 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
All replies received. Done.
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http
) (111 sunrpc) (139 netbios-ssn) (445 microsoft-d) (512 exec) (513 login) (514 she
ll) (1099 rmiregistry) (1524 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (363
2 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-u)

┌──(kali㉿kali)-[~]
└─$ 
```