

Report di Scansione Host

Data: 26/04/2024

Eseguito da: Simone Cisbaglia

Introduzione

Questo documento descrive i risultati delle scansioni host utilizzando i comandi specifici per Kali Linux.

Comandi di Scansione

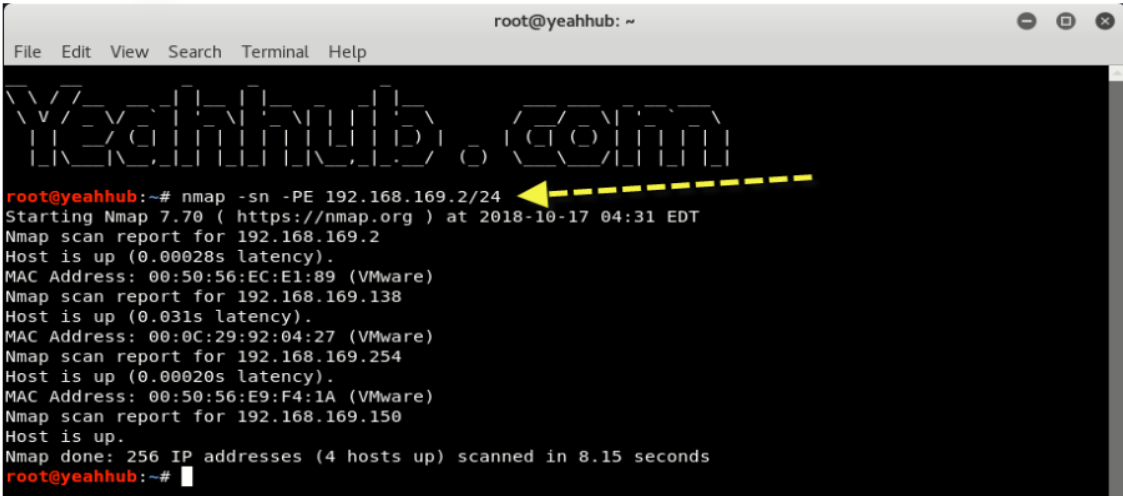
1. nmap -sn -PE <target>


Risultati:

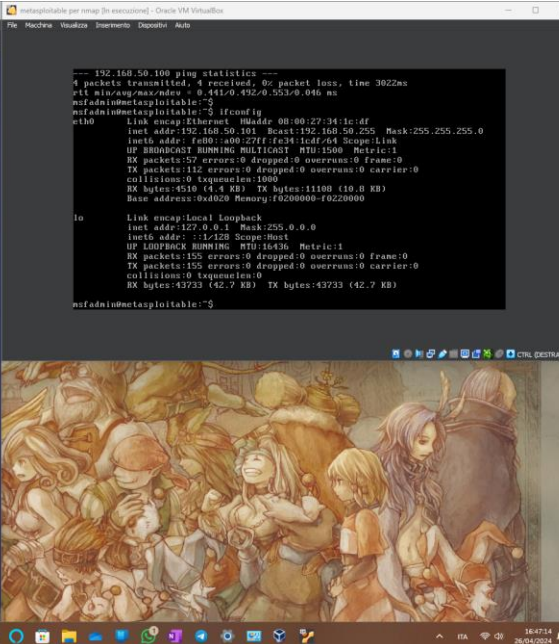
Esempio 1 – Ricognizione attiva con Nmap

Gli aggressori possono eseguire ricognizioni o monitorare la rete in molti modi diversi. Con l'aiuto di nmap, puoi facilmente effettuare una ricognizione attiva contro qualsiasi bersaglio come mostrato di seguito:

Sintassi: `nmap -sn -PE <target>`







2. netdiscover -r <target>

Risultati:

Esempio 2: trovare host attivi con Netdiscover

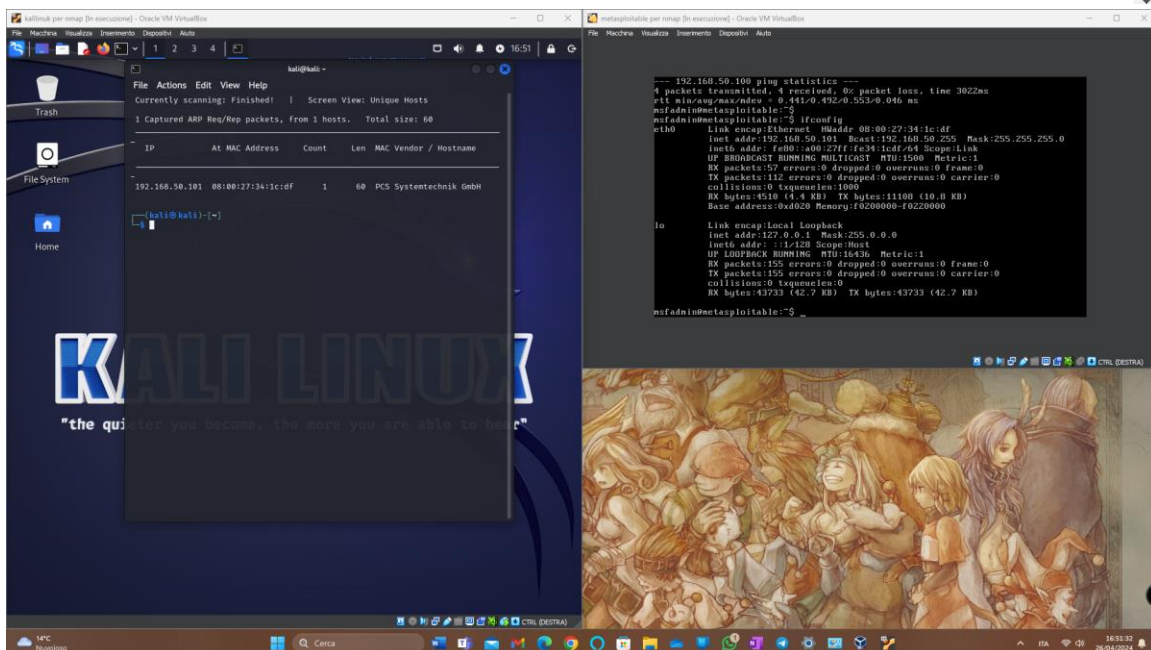
NetDiscover è uno strumento molto utile per trovare host su reti wireless o commutate. Può essere utilizzato sia in modalità attiva che passiva.

Sintassi: `netdiscover -r <destinazione>`

```
root@yeahhub: ~  
File Edit View Search Terminal Help  
Yeahhub.com  
root@yeahhub:~# netdiscover -r 192.168.169.2/24  
Currently scanning: Finished! | Screen View: Unique Hosts  
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180  


| IP              | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|-----------------|-------------------|-------|-----|-----------------------|
| 192.168.169.2   | 00:50:56:ec:e1:89 | 1     | 60  | VMware, Inc.          |
| 192.168.169.138 | 00:0c:29:92:04:27 | 1     | 60  | VMware, Inc.          |
| 192.168.169.254 | 00:50:56:e9:f4:1a | 1     | 60  | VMware, Inc.          |


```



3. crackmapexec <target>

Risultati:

Esempio 3 – Individuazione dell'host con CrackMapExec

CrackMapExec (noto anche come CME) è uno strumento post-exploitation che aiuta ad automatizzare la valutazione della sicurezza di reti Active Directory di grandi dimensioni. Costruito pensando alla furtività, CME segue il concetto di " *Vivere fuori dalla terra* ": abusare delle funzionalità/protocolli integrati di Active Directory per ottenere le sue funzionalità e consentire di eludere la maggior parte delle soluzioni di protezione endpoint/IDS/IPS.

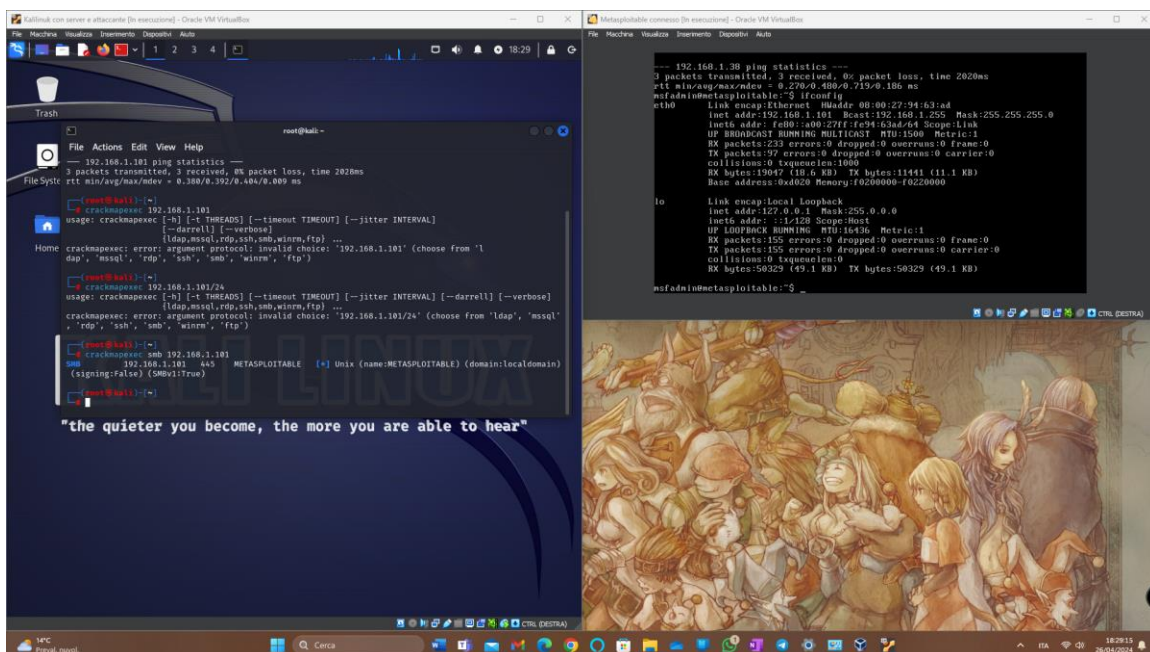
Per installare [crackmapexec](#) , è necessario eseguire il comando " **apt-get install crackmapexec** " nel terminale Linux.

Se non si installa utilizzando il comando precedente, ti consigliamo di eseguire un " **apt-get update && apt-get upgrade** " per assicurarti di avere i pacchetti più recenti e migliori di Offensive Security e della squadra Kali.

Sintassi: `crackmapexec <obiettivo>`



```
root@yeahhub: ~  
File Edit View Search Terminal Help  
root@yeahhub:~# crackmapexec 192.168.169.2/24  
CME 192.168.169.138:445 METASPLOITABLE [*] Unix (name:METASPLOITABLE) (domain:METASPLOITABLE)  
[*] KTHXBYE!  
root@yeahhub:~#
```



4. nmap <target> -top-ports 10 -open

Risultati:

Esempio 4 – Trova le prime 10 porte aperte con Nmap (Fast Scan)

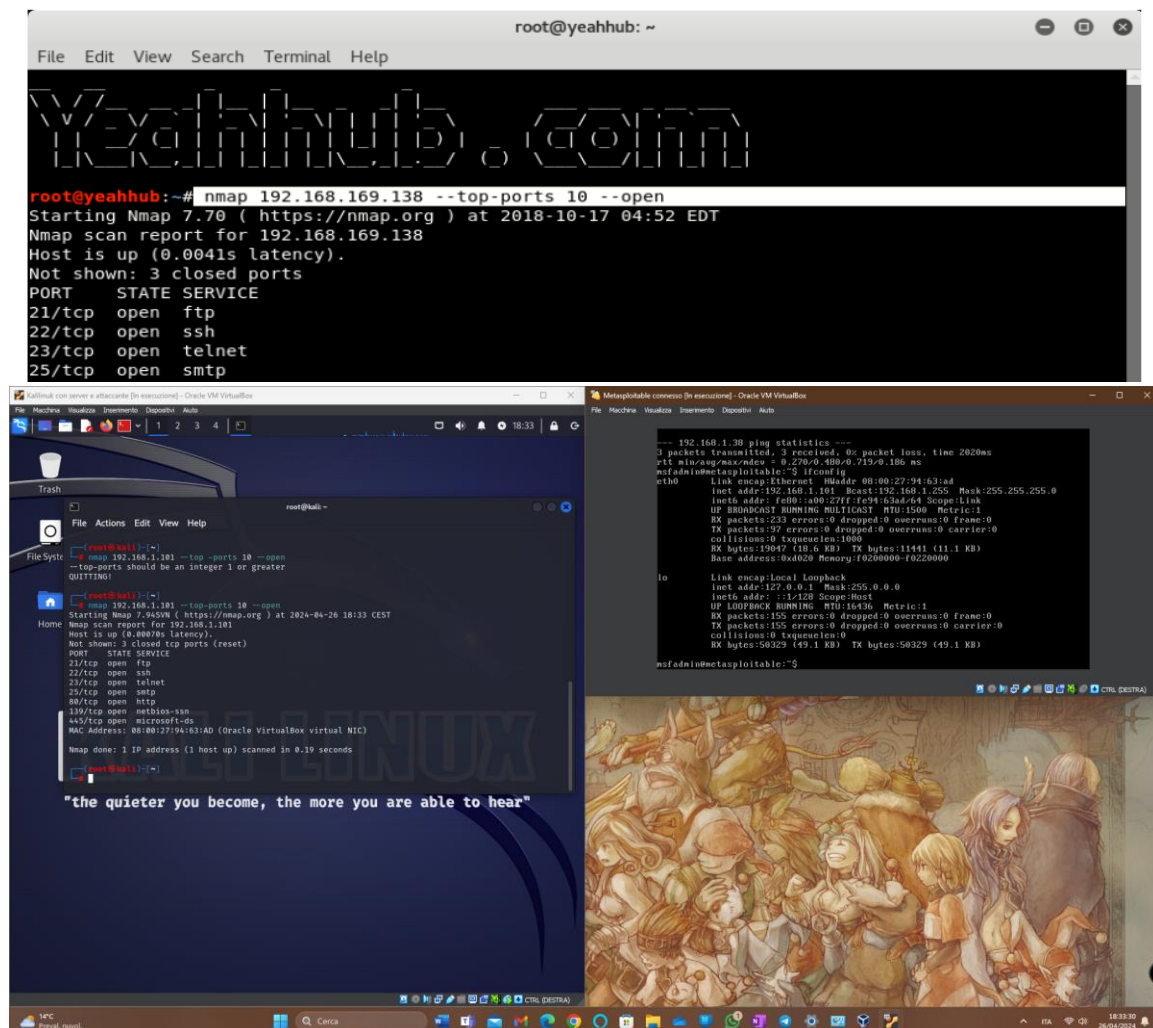
C'è molto altro che puoi fare con nmap.

Con l'opzione **-top-ports**, puoi facilmente identificare le prime 10 porte aperte in qualsiasi rete digitando il comando seguente:

```
Sintassi: nmap <target> -top-ports 10 -open
```

Attualmente, **-top-ports** seleziona le porte più popolari dal file `nmap-services` o dall'elenco di porte fornito sulla riga di comando.

Se una qualsiasi delle porte indicate sulla riga di comando non è elencata nel file `nmap-services`, non verrà scansionata.



```
root@yeahhub: ~
File Edit View Search Terminal Help

YeahHub.com

root@yeahhub:~# nmap 192.168.169.138 --top-ports 10 --open
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-17 04:52 EDT
Nmap scan report for 192.168.169.138
Host is up (0.0041s latency).
Not shown: 3 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp

-- 192.168.1.38 ping statistics --
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/stdev = 0.270/0.408/0.719/0.106 ms
msfadminmetasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:94:63:ad
          inet6 addr: fe80::a00:27fff:fe94:63ad/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:235 errors:0 dropped:0 overruns:0 frame:0
          TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19047 (18.6 KB)  TX bytes:11441 (11.1 KB)
          Base address: 0xd020  Memory: f0200000-f0220000

lo        Link encap:Local Loopback
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)
msfadminmetasploitable:~$
```


5. nmap <target> -p -sV --reason --dns-server ns

Risultati:

Esempio 5 – Ricognizione DNS con Nmap (Scansione Lenta)

Per impostazione predefinita, un output di Nmap indica se un host è attivo o meno, ma non descrive i test di rilevamento a cui l'host ha risposto. Può essere utile comprendere il motivo per cui una porta è contrassegnata come **aperta**, **chiusa** o **filtrata** e perché l'host è contrassegnato come **vivo**. Questo può essere fatto usando il flag `--reason`. Ecco un esempio:

Sintassi: `nmap <target> -p -sV --reason --dns-server ns`

Le informazioni DNS per la rete di destinazione sono spesso informazioni di ricognizione molto utili. Le informazioni DNS sono informazioni disponibili al pubblico e la loro enumerazione dai server DNS non richiede alcun contatto con l'obiettivo e non informerà l'azienda target di alcuna attività.

```
root@yeahhub:~# nmap 192.168.169.138 -p -sV --reason --dns-server ns
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-17 04:53 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-
dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.169.138
Host is up, received arp-response (0.0043s latency).
Not shown: 65505 closed ports
Reason: 65505 resets
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 64  vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 64  OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64  Linux telnetd
25/tcp    open  smtp         syn-ack ttl 64  Postfix smtpd
53/tcp    open  domain       syn-ack ttl 64  ISC BIND 9.4.2
```

```
root@yeahhub:~# nmap 192.168.169.138 -p -sV --reason --dns-server ns
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-17 04:53 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-
dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.169.138
Host is up, received arp-response (0.0043s latency).
Not shown: 65505 closed ports
Reason: 65505 resets
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 64  vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 64  OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64  Linux telnetd
25/tcp    open  smtp         syn-ack ttl 64  Postfix smtpd
53/tcp    open  domain       syn-ack ttl 64  ISC BIND 9.4.2
```

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

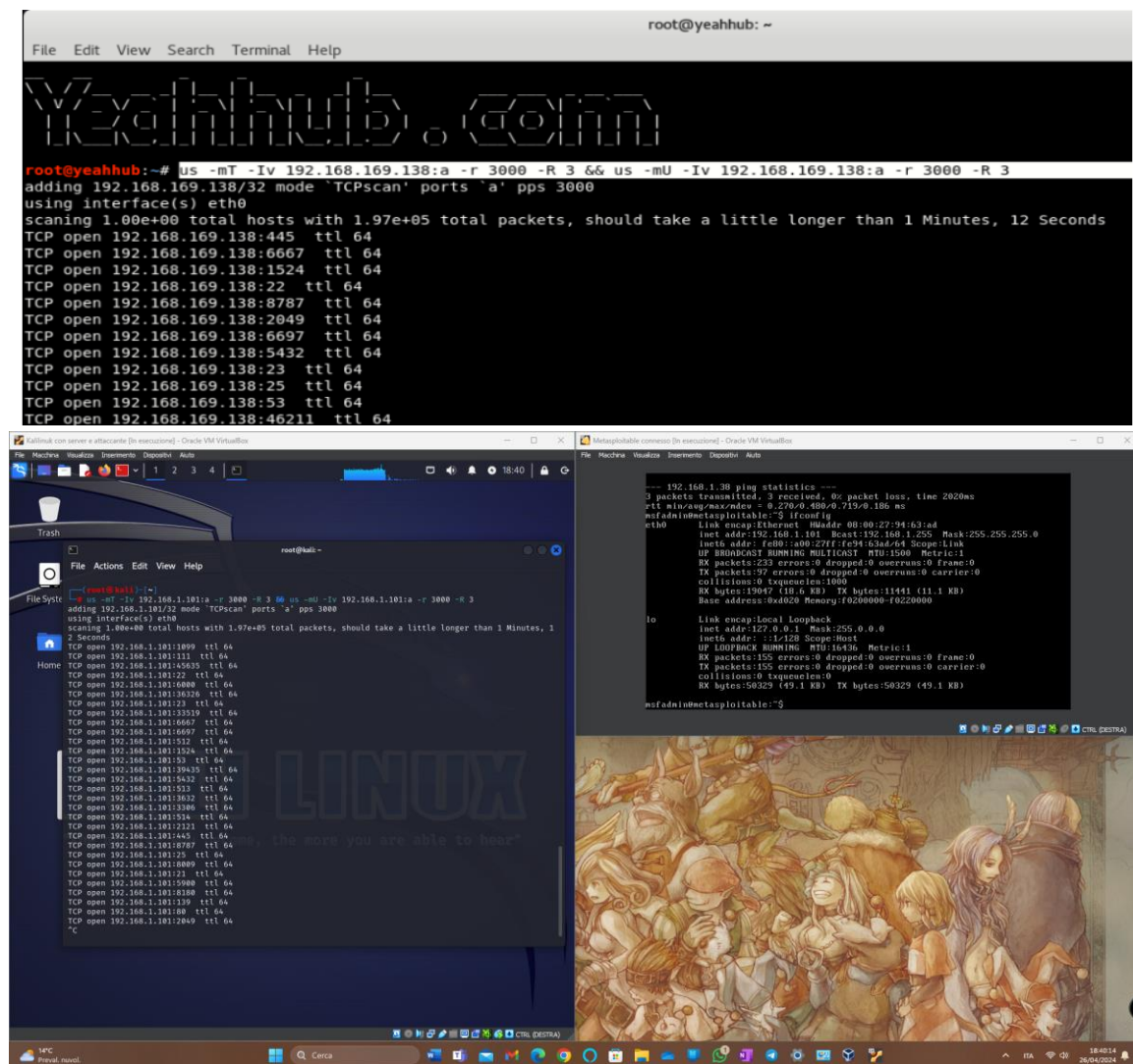
Risultati:

Esempio 6 – Scansione con Unicornscan

Unicornscan è un nuovo motore di raccolta e correlazione delle informazioni creato per e dai membri delle comunità di ricerca e test sulla sicurezza. È stato progettato per fornire un motore scalabile, accurato, flessibile ed efficiente.

Unicornscan utilizza per impostazione predefinita una scansione TCP/UDP, a differenza di nmap. Per impostazione predefinita, invia una scansione SYN. Diciamo che vogliamo scansionare il nostro IP (192.168.169.138), cercando tutte le porte e inviando 3000 pacchetti al secondo che potremmo scrivere;

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



```
root@yeahhub: ~  
File Edit View Search Terminal Help  
root@yeahhub:~# us -mT -lv 192.168.169.138:a -r 3000 -R 3 && us -mU -lv 192.168.169.138:a -r 3000 -R 3  
adding 192.168.169.138/32 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 192.168.169.138:445 ttl 64  
TCP open 192.168.169.138:6667 ttl 64  
TCP open 192.168.169.138:1524 ttl 64  
TCP open 192.168.169.138:22 ttl 64  
TCP open 192.168.169.138:8787 ttl 64  
TCP open 192.168.169.138:2049 ttl 64  
TCP open 192.168.169.138:6697 ttl 64  
TCP open 192.168.169.138:5432 ttl 64  
TCP open 192.168.169.138:23 ttl 64  
TCP open 192.168.169.138:25 ttl 64  
TCP open 192.168.169.138:53 ttl 64  
TCP open 192.168.169.138:46211 ttl 64
```

7. nmap -sS -sV -T4 <target>

Risultati:

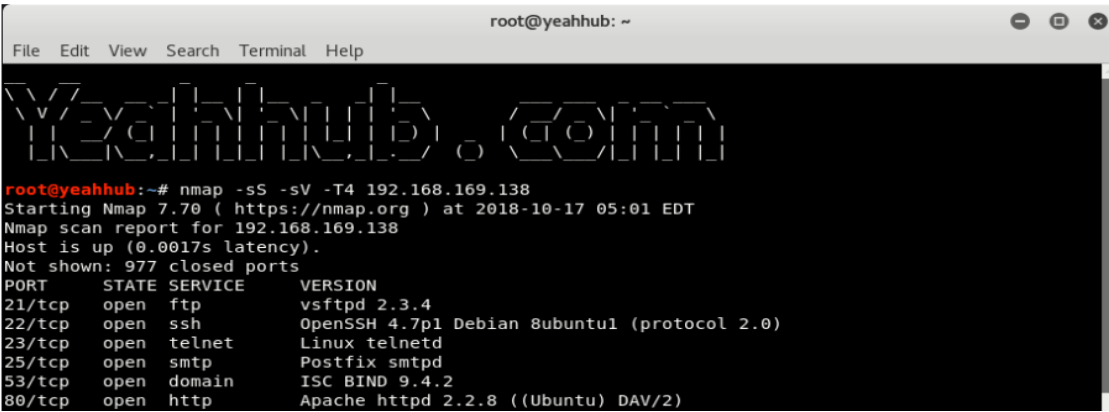
Esempio 7 – TCP Syn Scan con Nmap

Il comando seguente determina se la porta è in ascolto. L'utilizzo di questo comando è una tecnica chiamata scansione semiaperta.

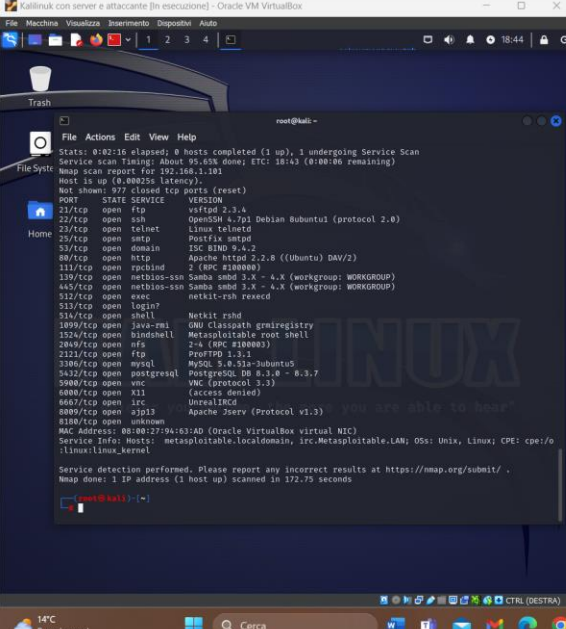
Si chiama scansione semiaperta perché non viene stabilita una connessione TCP completa. Invece, invii solo un pacchetto SYN e attendi la risposta. Se ricevi una risposta SYN/ACK significa che la porta è in ascolto:

Con l'opzione **-sV**, puoi anche stampare il noto servizio nominato da un elenco di database di circa 2.200.

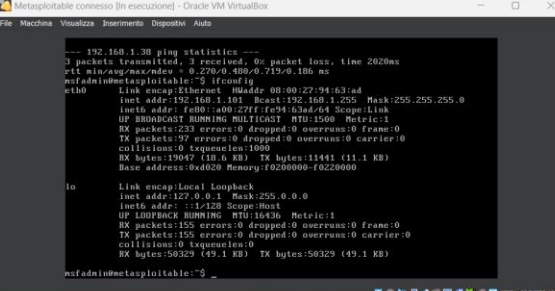
Sintassi: `nmap -sS -sV -T4 <target>`



```
root@yeahhub:~# nmap -sS -sV -T4 192.168.169.138
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-17 05:01 EDT
Nmap scan report for 192.168.169.138
Host is up (0.0017s latency).
Not shown: 977 closed ports
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)
```



```
Stats: 0:02:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan timing: About 95.03% done; ETC: 18:43 (0:00:06 remaining)
Nmap scan report for 192.168.1.138
Host is up (0.000255s 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  rsh      2 (TCP 818000)
139/tcp   open  smb      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  smb      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rshcd
513/tcp   open  login?   netkit-rsh rshcd
514/tcp   open  shell    Netkit rshd
1099/tcp  open  java-rmi GNU Classpath gmrregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2.4 (RPC 818000)
2121/tcp  open  ftp      ProFTPD 1.3.1
3306/tcp  open  mysql    MySQL 5.6.33-8ubuntu5
5432/tcp  open  postgres PostgreSQL DB 8.3.0 - 8.3.7
5988/tcp  open  vnc      VNC (protocol 3.3)
6000/tcp  open  x11      (access denied)
6667/tcp  open  irc      UnrealIRCd
8080/tcp  open  http     Apache/2.2.8 (Ubuntu)
8180/tcp  open  unknown
```



```
--- 192.168.1.38 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.279/0.480/0.715/0.186 ms
mifadim@metasploitable:~$ ifconfig
Link encap:Ethernet  HWaddr 08:00:27:94:63:ad
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe94:63ad::ad Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
RX packets:233 errors:0 dropped:0 overruns:0 frame:0
TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:15047 (14.6 KB)  TX bytes:11441 (11.1 KB)
Base address: 0x4020 Memory: f0200000-f0220000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1 Scope:Host
UP LOOPBACK RUNNING  MTU:65536 Metric:1
RX packets:155 errors:0 dropped:0 overruns:0 frame:0
TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)
mifadim@metasploitable:~$
```


8. hping3 --scan known <target>

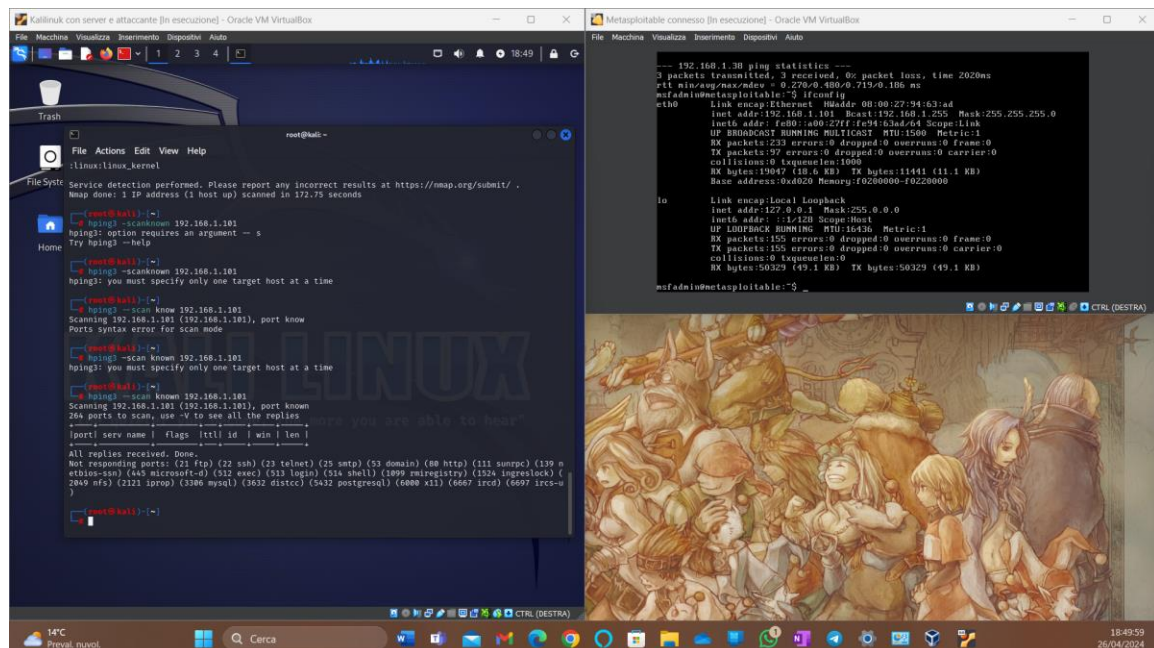
Risultati:

Esempio 8 – Scansione con HPING3

hping è un assembler/analizzatore di pacchetti TCP/IP orientato alla riga di comando. L'interfaccia è ispirata al comando ping unix, ma hping non è solo in grado di inviare richieste echo ICMP. Supporta anche i protocolli TCP, UDP, ICMP e RAW-IP, ha una modalità traceroute, la capacità di inviare file tra un canale coperto e molte altre funzionalità.

Sintassi: hping3 --scanknown <target>

```
root@yeahhub: ~  
File Edit View Search Terminal Help  
Yeahhub.com  
root@yeahhub:~# hping3 --scan known 192.168.169.138  
Scanning 192.168.169.138 (192.168.169.138), port known  
337 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) (13  
9 netbios-ssn) (445 microsoft-d) (512 exec) (513 login) (514 shell) (1099 rmiregistry) (1524 ingresl  
ock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (66  
97 ircs-u)  
root@yeahhub:~#
```



9. nc -nvz <target> 1-1024

Risultati:

Esempio 9 – Scansione delle porte con Netcat

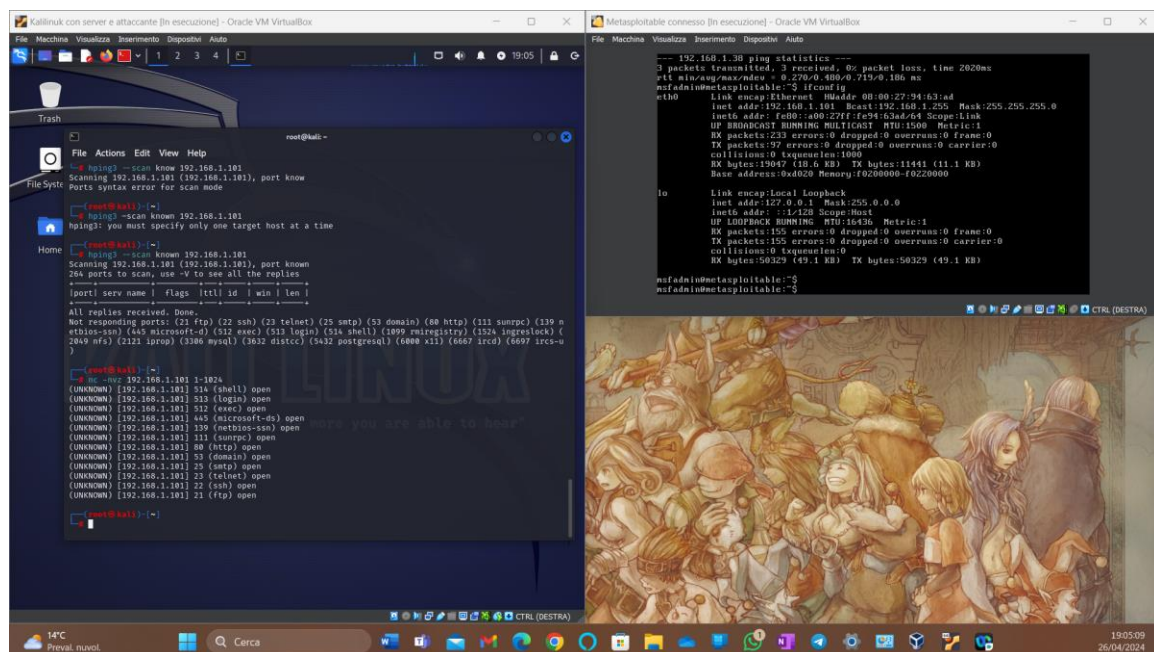
[Netcat](#) è un'utilità di rete in grado di leggere e scrivere dati attraverso connessioni di rete, utilizzando il protocollo TCP/IP.

Sebbene netcat non sia probabilmente lo strumento più sofisticato per questo lavoro (nmap è una scelta migliore nella maggior parte dei casi), può eseguire semplici scansioni delle porte per identificare facilmente le porte aperte digitando il comando seguente:

Sintassi: nc -nvz <destinazione> 1-1024

Qui -n flag viene utilizzato per specificare che non è necessario risolvere l'indirizzo IP utilizzando DNS.

```
root@yeahhub: ~  
File Edit View Search Terminal Help  
Yeahhub.com  
root@yeahhub:~# nc -nvz 192.168.169.138 1-1024  
(UNKNOWN) [192.168.169.138] 514 (shell) open  
(UNKNOWN) [192.168.169.138] 513 (login) open  
(UNKNOWN) [192.168.169.138] 512 (exec) open  
(UNKNOWN) [192.168.169.138] 445 (microsoft-ds) open  
(UNKNOWN) [192.168.169.138] 139 (netbios-ssn) open  
(UNKNOWN) [192.168.169.138] 111 (sunrpc) open  
(UNKNOWN) [192.168.169.138] 80 (http) open  
(UNKNOWN) [192.168.169.138] 53 (domain) open  
(UNKNOWN) [192.168.169.138] 25 (smtp) open  
(UNKNOWN) [192.168.169.138] 23 (telnet) open  
(UNKNOWN) [192.168.169.138] 22 (ssh) open  
(UNKNOWN) [192.168.169.138] 21 (ftp) open  
root@yeahhub:~#
```



10. nc -nv <target> 22

Risultati:

Esempio 10 – Acquisizione di banner con Netcat

Netcat non si limita all'invio di pacchetti TCP e UDP. Può anche ascoltare su una porta connessioni e pacchetti. Questo ci dà l'opportunità di connettere due istanze di netcat in una relazione client-server.

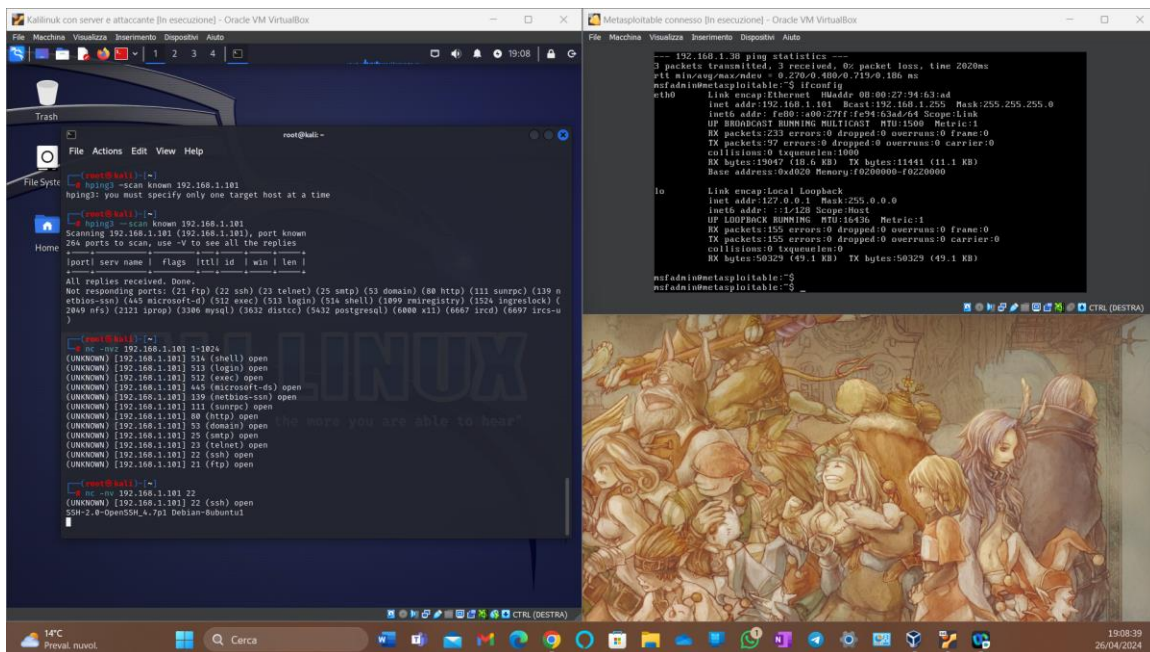
Con netcat, puoi persino eseguire la scansione di un particolare numero di porta rispetto a qualsiasi destinazione.

Sintassi: nc -nv <destinazione> <numero porta>

Qui possiamo vedere che la porta 22 sul computer remoto rileva il nome e la versione del servizio.

```
root@yeahhub: ~
File Edit View Search Terminal Help

root@yeahhub:~# nc -nv 192.168.169.138 22
(UNKNOWN) [192.168.169.138] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```



11. nmap -sV <target>

Risultati:

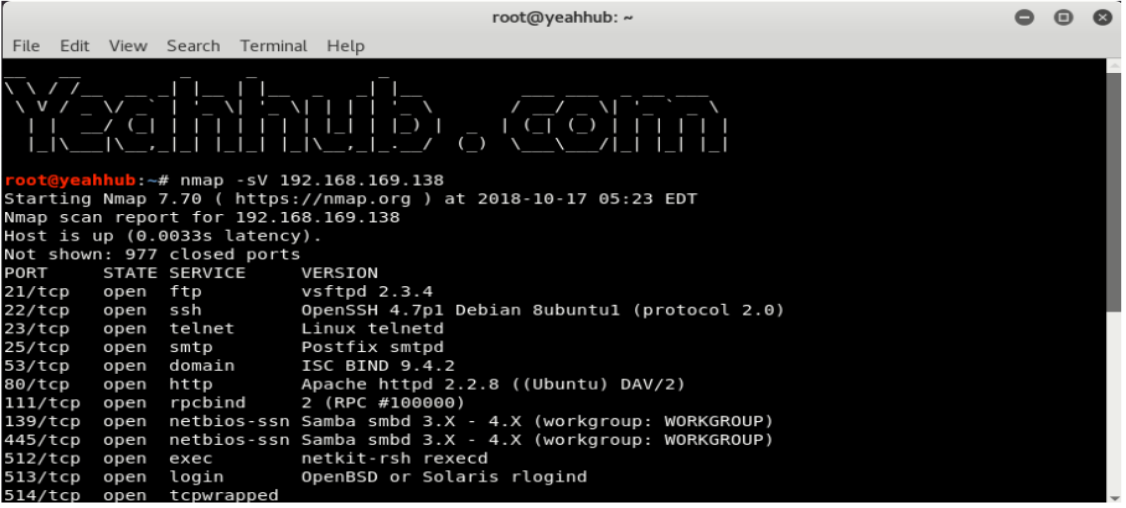
Esempio 11 – Scansione della versione con Nmap

Sebbene Nmap faccia molte cose, la sua caratteristica più fondamentale è la scansione delle porte. Punta Nmap verso una macchina remota e potrebbe dirti che le porte 25/tcp, 80/tcp e 53/udp sono aperte.

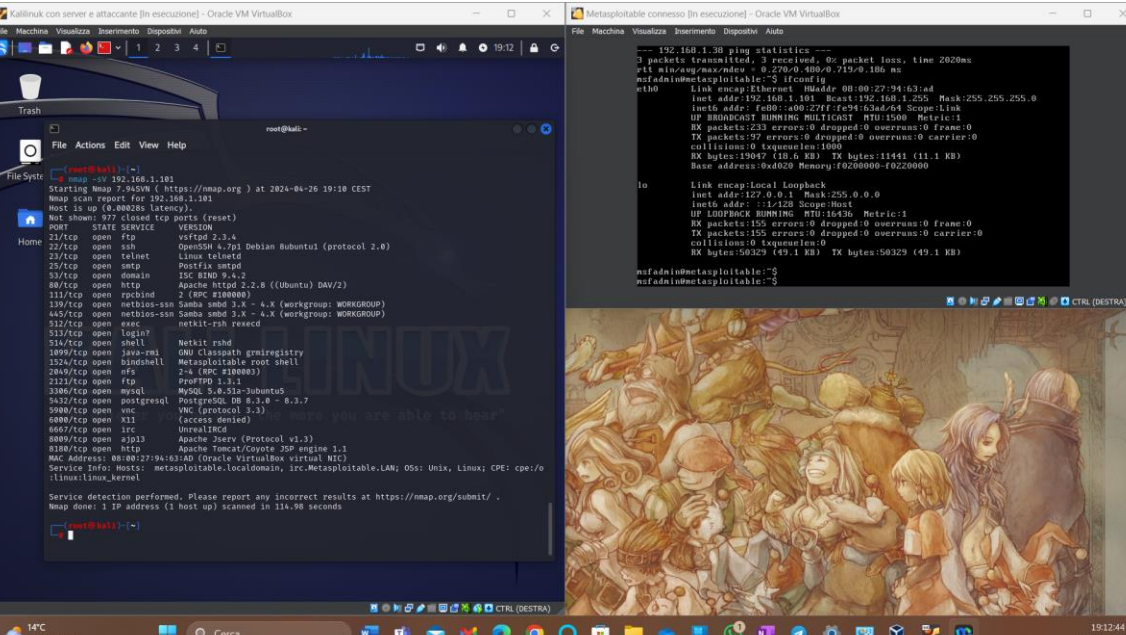
Utilizzando il suo database nmap-services di oltre 2.200 servizi ben noti, Nmap riporterebbe che tali porte probabilmente corrispondono rispettivamente a un server di posta (SMTP), un server web (HTTP) e un server dei nomi (DNS).

Il sottosistema di scansione della versione Nmap ottiene tutti questi dati collegandosi a porte aperte e interrogandole per ulteriori informazioni utilizzando sonde comprensibili ai servizi specifici. Ciò consente a Nmap di fornire una valutazione dettagliata di ciò che è realmente in esecuzione, piuttosto che solo dei numeri di porta aperti.

Sintassi: nmap -sV <target>



```
root@yeahhub:~# nmap -sV 192.168.169.138
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-17 05:23 EDT
Nmap scan report for 192.168.169.138
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports
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 rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
```



```
192.168.1.38 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.270/0.400/0.719/0.106 ms
msfadmin@metasploitable:~$ ifconfig
eth0
Link encap:Ethernet HWaddr 08:00:27:94:63:ed
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe94:63ed/64 Scope:link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:235 errors:0 dropped:0 overruns:0 frame:0
TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 sequence:1900
RX bytes:19047 (18.6 KB) TX bytes:11441 (11.1 KB)
Base address:0xd020 Memory:10200000-10220000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:155 errors:0 dropped:0 overruns:0 frame:0
TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 sequence:0
RX bytes:50329 (49.1 KB) TX bytes:50329 (49.1 KB)
msfadmin@metasploitable:~$
```


12. db_import <file.xml> (For Metasploit Framework)

Risultati:

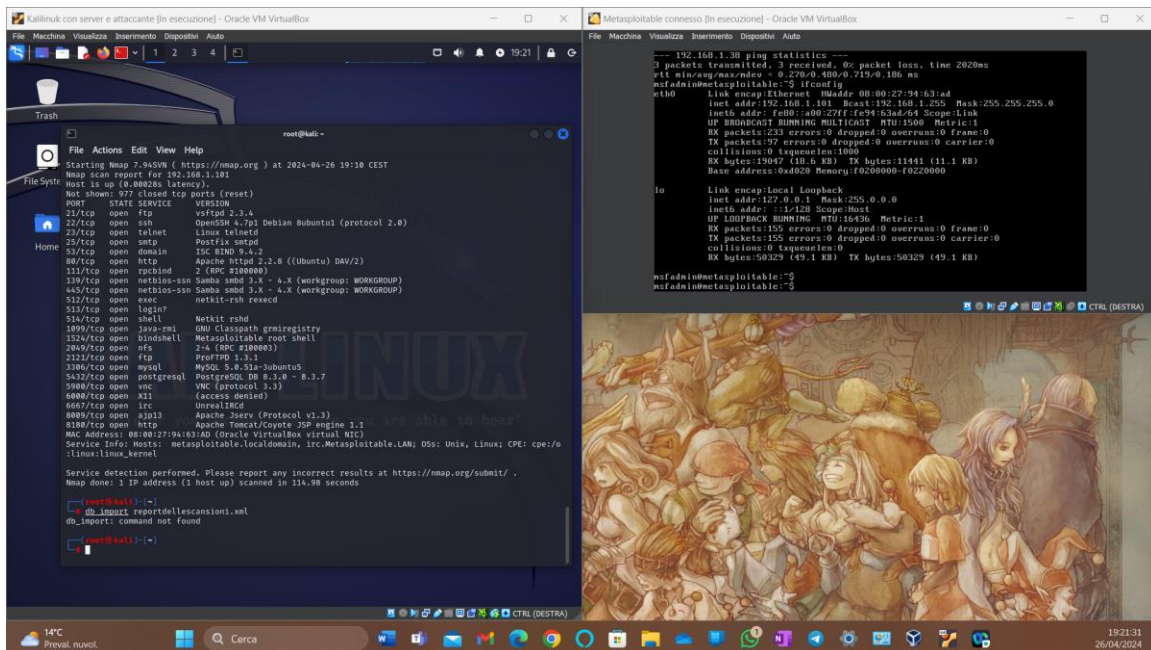
Esempio 12 – Scansione con Metasploit Framework

Al completamento di una scansione di base con nmap, puoi anche importare tutte le informazioni sugli host nel [framework metasploit](#) per un ulteriore sfruttamento salvando i risultati in formato **.xml**.

Sintassi: db_import <nomefile.xml>

Dopo aver importato il file, puoi semplicemente eseguire il comando **host** per elencare gli host presenti nel file xml.

```
msf > db_status
[*] postgresql connected to msf
msf > db_import ./output-yeahhub.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.8.4'
[*] Importing host 192.168.169.138
[*] Successfully imported /root/output-yeahhub.xml
```



13. nmap -f --mtu=512 <target>

Risultati:

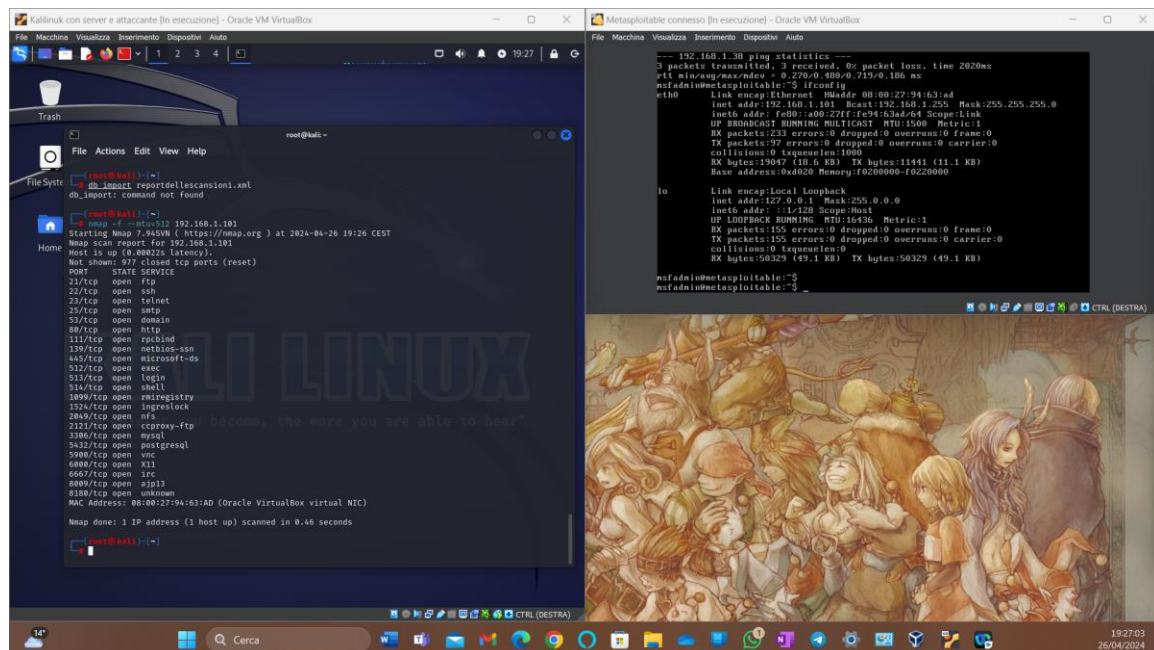
Esempio 13 – Bypass del firewall

Con le opzioni -f e --mtu, puoi facilmente aggirare le restrizioni del firewall tramite la frammentazione dei pacchetti.

Sintassi: nmap -f --mtu=512 <destinazione>

L'opzione -f fa sì che la scansione richiesta (incluse le scansioni ping) utilizzi piccoli pacchetti IP frammentati. L'idea è di suddividere l'intestazione TCP su più pacchetti per rendere più difficile per i filtri dei pacchetti, i sistemi di rilevamento delle intrusioni e altri fastidi rilevare ciò che stai facendo.

```
root@yeahhub: ~  
File Edit View Search Terminal Help  
Yeahhub.com  
root@yeahhub:~# nmap -f --mtu=512 192.168.169.138  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-17 14:51 EDT  
Nmap scan report for 192.168.169.138  
Host is up (0.0036s latency).  
Not shown: 977 closed ports  
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
```



14. masscan <network> -p80 --banners --source-ip <target>

Risultati:

Esempio 14 – Scansione con Masscan

Questo è lo scanner di porte Internet più veloce. Può scansionare l'intera Internet in meno di 6 minuti, trasmettendo 10 milioni di pacchetti al secondo.

Un'altra caratteristica di Masscan è che oltre a rilevare le porte aperte/chiuso, può anche acquisire semplici informazioni "banner". Il vincolo che deve affrontare è che Masscan ha il proprio stack TCP/IP.

Quando il sistema locale riceve un SYN-ACK dal target analizzato, risponde con un pacchetto TST che interrompe la connessione prima che le informazioni del banner possano essere acquisite. Il modo più semplice per evitare ciò è assegnare a Masscan un indirizzo IP diverso:

Sintassi: masscan <rete> -p80 --banners --source-ip <destinazione>

```
root@yeahhub: ~  
File Edit View Search Terminal Help  
Yeahhub.com  
root@yeahhub:~# masscan 192.168.169.2/24 -p80 --banners --source-ip 192.168.169.150  
Starting masscan 1.0.4 (http://bit.ly/14GZzcT) at 2018-10-17 18:56:26 GMT  
-- forced options: -ss -Pn -n --randomize-hosts -v --send-eth  
Initiating SYN Stealth Scan  
Scanning 256 hosts [1 port/host]  
Discovered open port 80/tcp on 192.168.169.138  
Rate: 0.00-kpps, 100.00% done, waiting -10-secs, found=1
```

