TRACCIA TASK 03/12/24

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

TASK 03/12/24

Configurazione di Rete

- **Metasploitable**: 192.168.50.101
- **Windows 10**: 192.168.50.102
- **Macchina Kali Linux (Nmap)**: 192.168.50.100

Scansioni Richieste

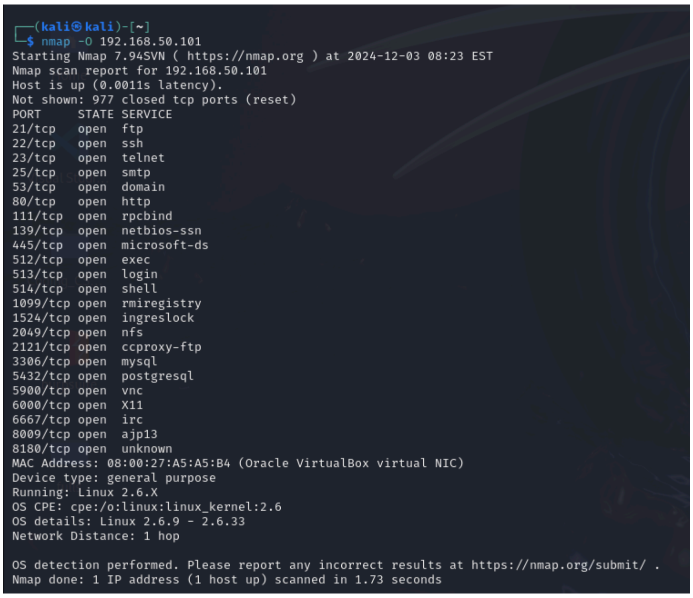
Metasploitable (192.168.50.101)

OS Fingerprint: Determinare il sistema operativo

nmap -O 192.168.50.101

Motivazione:

Il flag -O consente di identificare il sistema operativo del target analizzando le risposte ai pacchetti inviati.



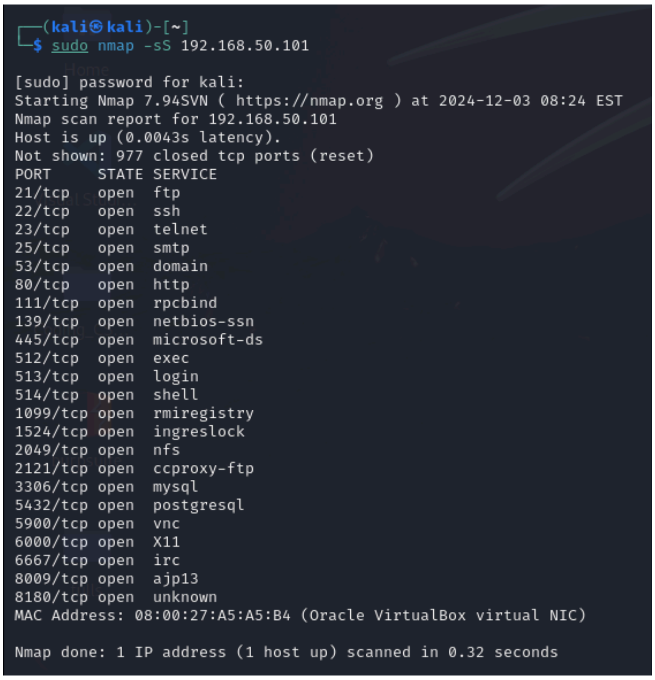
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:23 EST
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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:A5:A5:B4 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
```

Syn Scan: Eseguire una scansione con pacchetti SYN

nmap -sS 192.168.50.101

Motivazione:

Il flag -sS che invia pacchetti TCP con il flag SYN impostato per iniziare una connessione.



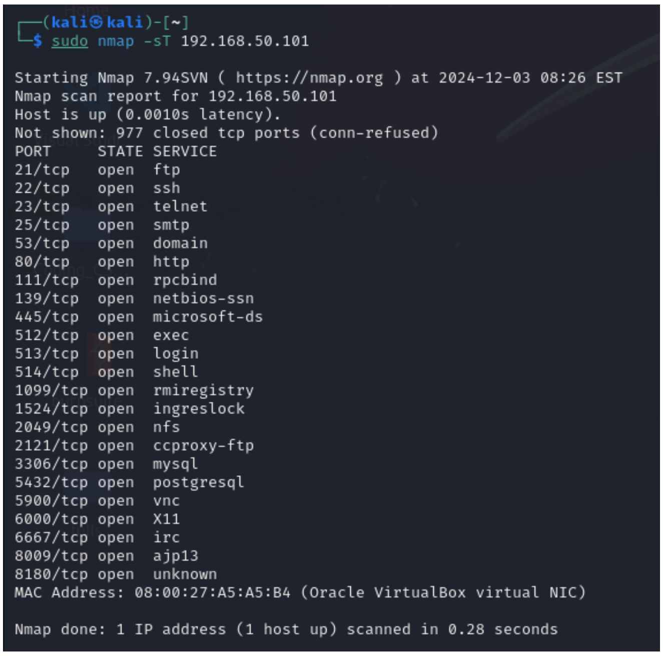
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:24 EST
Nmap scan report for 192.168.50.101
Host is up (0.0043s 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:A5:A5:B4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

TCP Connect Scan: Confrontare i risultati con la Syn Scan

nmap -sT 192.168.50.101

Motivazione:

Il flag -sT utilizza il normale processo di connessione TCP (3-way handshake).



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:26 EST
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (conn-refused)
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:A5:A5:B4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

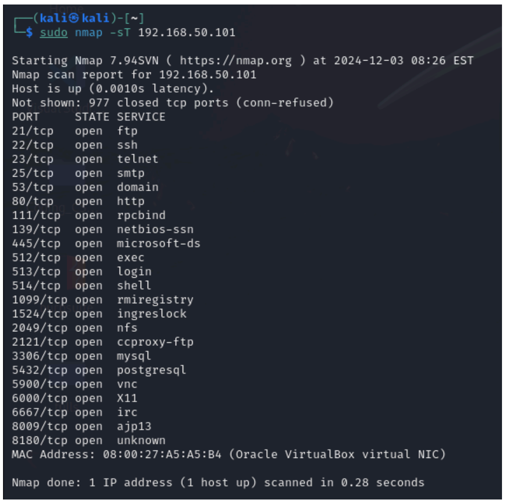
Confronto con Syn Scan:

TCP Connect Scan (-sT)

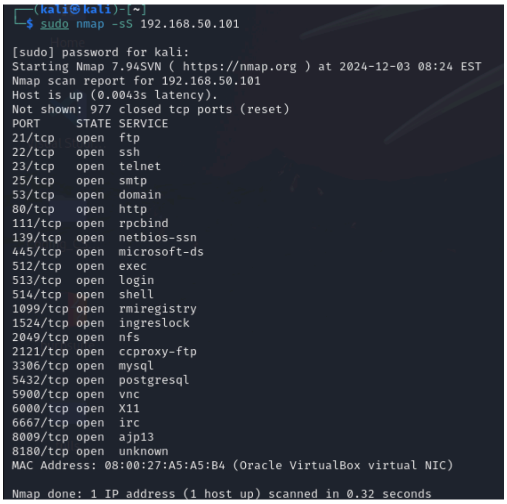
Descrizione: La TCP completa il processo di handshake per ogni porta aperta, il che la rende più affidabile ma meno discreta.

SYN Scan (-sS)

Descrizione: La SYN invia solo pacchetti SYN e non completa l'handshake. È più veloce e stealth rispetto alla TCP Connect Scan.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:26 EST
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (conn-refused)
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:A5:A5:B4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:24 EST
Nmap scan report for 192.168.50.101
Host is up (0.0043s 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:A5:A5:B4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Confronto tra i principali risultati

Porte:

- Entrambi i metodi rilevano le stesse porte aperte su Metasploitable, confermando che non ci sono porte aggiuntive rilevate da un metodo rispetto all'altro.

Prestazioni:

- La SYN Scan è significativamente più veloce rispetto alla TCP Connect Scan..
- La TCP Connect Scan richiede più tempo perché completa le connessioni.

Log del target:

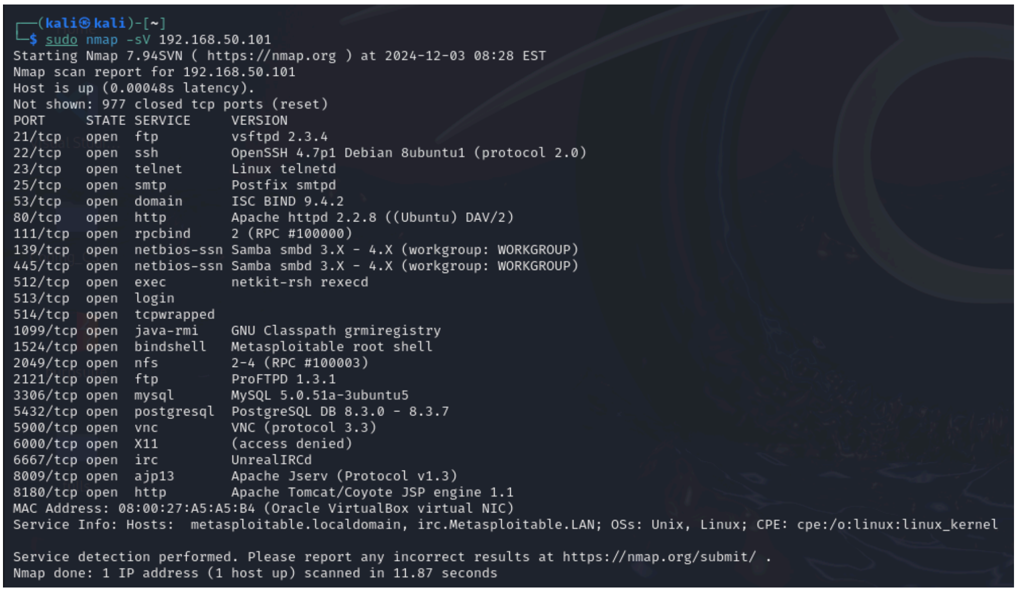
- La TCP Connect Scan lascia tracce nei log del target perché stabilisce connessioni complete.
- La SYN Scan è meno rilevabile perché interrompe la connessione prima di completare l'handshake.

Version Detection: Identificare le versioni dei servizi attivi

nmap -sV 192.168.50.101

Motivazione:

Il flag -sV consente di identificare i servizi attivi sulle porte aperte e di rilevare le loro versioni.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:28 EST
Nmap scan report for 192.168.50.101
Host is up (0.00048s 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  tcpwrapped
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  ftp         ProFTPD 1.3.1
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
MAC Address: 08:00:27:A5:A5:B4 (Oracle VirtualBox virtual NIC)
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 11.87 seconds
```

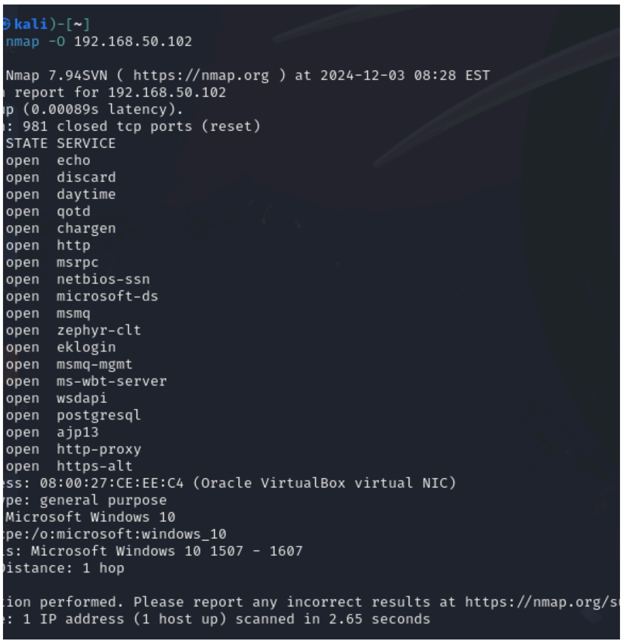
Windows 10 (192.168.50.102)

OS Fingerprint: Determinare il sistema operativo

nmap -O 192.168.50.102

Motivazione:

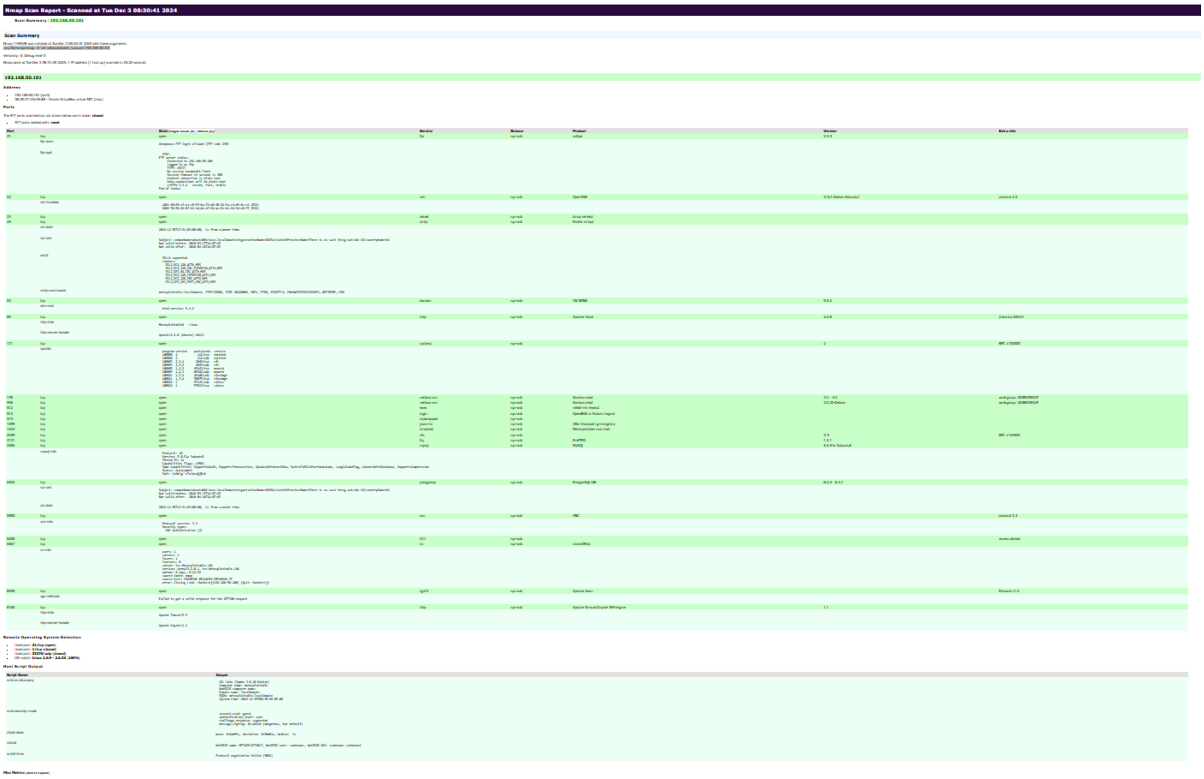
Il flag -O consente di identificare il sistema operativo del target analizzando le risposte ai pacchetti inviati.



```
㉿kali)-[~]
nmap -O 192.168.50.102

Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:28 EST
 report for 192.168.50.102
p (0.00089s latency).
: 981 closed tcp ports (reset)
STATE SERVICE
open  echo
open  discard
open  daytime
open  qotd
open  chargen
open  http
open  msrpc
open  netbios-ssn
open  microsoft-ds
open  msmq
open  zephyr-clt
open  eklogin
open  msmq-mgmt
open  ms-wbt-server
open  wsdapi
open  postgresql
open  ajp13
open  http-proxy
open  https-alt
ss: 08:00:27:CE:EE:C4 (Oracle VirtualBox virtual NIC)
pe: general purpose
Microsoft Windows 10
pe:/o:microsoft:windows_10
s: Microsoft Windows 10 1507 - 1607
istance: 1 hop

ion performed. Please report any incorrect results at https://nmap.org/s
: 1 IP address (1 host up) scanned in 2.65 seconds
```

Report in HTML

Metasploitable (192.168.50.101)



Nmap Scan Report - Scanned at Tue Dec 3 08:30:41 2024

Scan Summary | 192.168.50.101

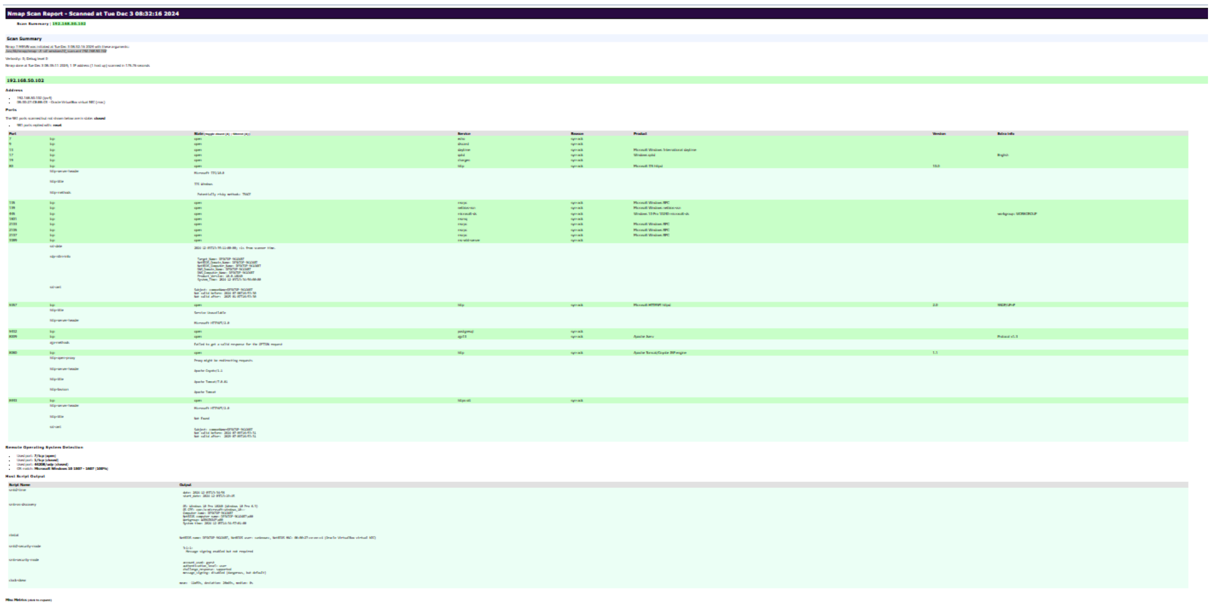
Scan Summary

192.168.50.101

Address

Ports

Windows 10 (192.168.50.102)



Nmap Scan Report - Scanned at Tue Dec 3 08:32:16 2024

Scan Summary | 192.168.50.102

Scan Summary

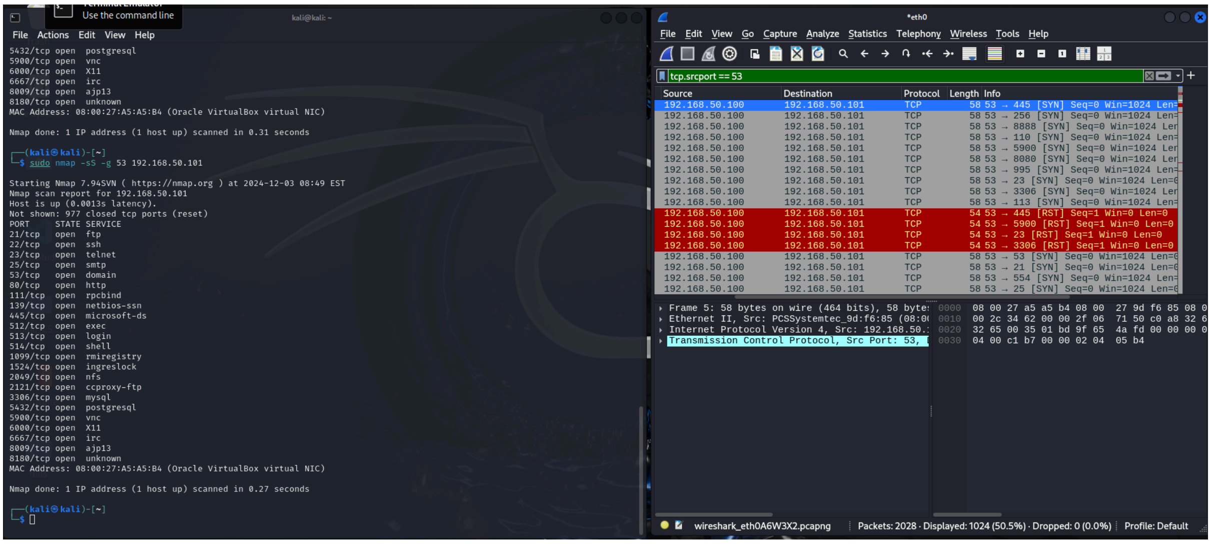
192.168.50.102

Address

Ports

EXTRA TASK 03/12/24

Comando con l'opzione -g


Use the command line
kali@kali: ~
File Actions Edit View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.srcport == 53

```
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:A5:A5:B4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -g 53 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:49 EST
Nmap scan report for 192.168.50.101
Host is up (0.0013s 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:A5:A5:B4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

```
Source          Destination     Protocol  Length Info
192.168.50.100  192.168.50.101  TCP       58 53 → 445 [SYN] Seq=0 Win=1024 Len=
192.168.50.100  192.168.50.101  TCP       58 53 → 256 [SYN] Seq=0 Win=1024 Len=
192.168.50.100  192.168.50.101  TCP       58 53 → 8888 [SYN] Seq=0 Win=1024 Len
192.168.50.100  192.168.50.101  TCP       58 53 → 110 [SYN] Seq=0 Win=1024 Len=
192.168.50.100  192.168.50.101  TCP       58 53 → 5900 [SYN] Seq=0 Win=1024 Len
192.168.50.100  192.168.50.101  TCP       58 53 → 8080 [SYN] Seq=0 Win=1024 Len
192.168.50.100  192.168.50.101  TCP       58 53 → 995 [SYN] Seq=0 Win=1024 Len=
192.168.50.100  192.168.50.101  TCP       58 53 → 23 [SYN] Seq=0 Win=1024 Len=0
192.168.50.100  192.168.50.101  TCP       58 53 → 3306 [SYN] Seq=0 Win=1024 Len
192.168.50.100  192.168.50.101  TCP       58 53 → 113 [SYN] Seq=0 Win=1024 Len=
192.168.50.100  192.168.50.101  TCP       54 53 → 445 [RST] Seq=1 Win=0 Len=0
192.168.50.100  192.168.50.101  TCP       54 53 → 5900 [RST] Seq=1 Win=0 Len=0
192.168.50.100  192.168.50.101  TCP       54 53 → 23 [RST] Seq=1 Win=0 Len=0
192.168.50.100  192.168.50.101  TCP       54 53 → 3306 [RST] Seq=1 Win=0 Len=0
192.168.50.100  192.168.50.101  TCP       58 53 → 53 [SYN] Seq=0 Win=1024 Len=0
192.168.50.100  192.168.50.101  TCP       58 53 → 21 [SYN] Seq=0 Win=1024 Len=0
192.168.50.100  192.168.50.101  TCP       58 53 → 554 [SYN] Seq=0 Win=1024 Len=
192.168.50.100  192.168.50.101  TCP       58 53 → 25 [SYN] Seq=0 Win=1024 Len=0

› Frame 5: 58 bytes on wire (464 bits), 58 byte   0000  08 00 27 a5 a5 b4 08 00  27 9d f6 85 08 0
› Ethernet II, Src: PCSSystemtec_9d:f6:85 (08:0   0010  00 2c 34 62 00 00 2f 06  71 50 c0 a8 32 6
› Internet Protocol Version 4, Src: 192.168.50.   0020  32 65 00 35 01 bd 9f 65  4a fd 00 00 00 0
› Transmission Control Protocol, Src Port: 53,    0030  04 00 c1 b7 00 00 02 04  05 b4

wireshark_eth0A6W3X2.pcapng | Packets: 2028 · Displayed: 1024 (50.5%) · Dropped: 0 (0.0%) | Profile: Default
```

sudo nmap -sS -g 53 192.168.50.101

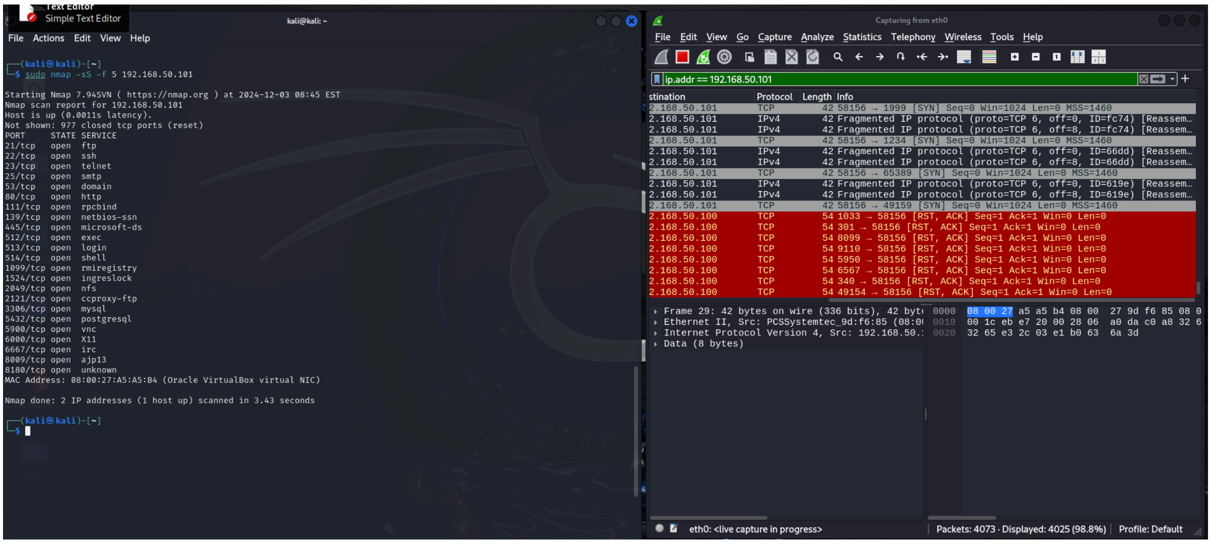
Effetto di -g:

- L'opzione -g specifica la porta sorgente per i pacchetti TCP generati da Nmap.
- Nel caso specifico, ho impostato la **porta 53**, simulando traffico DNS per cercare di aggirare firewall o IDS che considerano i pacchetti provenienti da porta 53 come affidabili.

Wireshark:

- Nei log di Wireshark, il campo **Source Port** per i pacchetti SYN inviati da Nmap è impostato a **53**, come specificato nel comando.
- Il traffico viene identificato correttamente come TCP con porta sorgente 53.
- Alcune porte del target rispondono con **RST** (Reset), segnalando che il servizio non accetta connessioni, mentre altre rispondono con SYN-ACK per indicare che sono aperte.

Comando con l'opzione -f



Simple Text Editor
kali@kali: ~
File Actions Edit View Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.50.101

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -f 5 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:45 EST
Nmap scan report for 192.168.50.101
Host is up (0.0011s 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:A5:A5:B4 (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (1 host up) scanned in 3.43 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
stination      Protocol  Length Info
2.168.50.101   TCP       42 58156 → 1999 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2.168.50.101   IPv4      42 Fragmented IP protocol (proto=TCP 6, off=0, ID=fc74) [Reassem…
2.168.50.101   IPv4      42 Fragmented IP protocol (proto=TCP 6, off=8, ID=fc74) [Reassem…
2.168.50.101   TCP       42 58156 → 1234 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2.168.50.101   IPv4      42 Fragmented IP protocol (proto=TCP 6, off=0, ID=66dd) [Reassem…
2.168.50.101   IPv4      42 Fragmented IP protocol (proto=TCP 6, off=8, ID=66dd) [Reassem…
2.168.50.101   TCP       42 58156 → 65389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2.168.50.101   IPv4      42 Fragmented IP protocol (proto=TCP 6, off=0, ID=619e) [Reassem…
2.168.50.101   IPv4      42 Fragmented IP protocol (proto=TCP 6, off=8, ID=619e) [Reassem…
2.168.50.101   TCP       42 58156 → 49159 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2.168.50.100   TCP       54 1033 → 58156 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2.168.50.100   TCP       54 301 → 58156 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2.168.50.100   TCP       54 8099 → 58156 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2.168.50.100   TCP       54 9110 → 58156 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2.168.50.100   TCP       54 5950 → 58156 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2.168.50.100   TCP       54 6567 → 58156 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2.168.50.100   TCP       54 340 → 58156 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2.168.50.100   TCP       54 49154 → 58156 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

› Frame 29: 42 bytes on wire (336 bits), 42 byt   0000  08 00 27 a5 a5 b4 08 00  27 9d f6 85 08 0
› Ethernet II, Src: PCSSystemtec_9d:f6:85 (08:0   0010  00 1c eb e7 20 00 28 06  a0 da c0 a8 32 6
› Internet Protocol Version 4, Src: 192.168.50.   0020  32 65 e3 2c 03 e1 b0 63  6a 3d
› Data (8 bytes)

eth0: <live capture in progress>    Packets: 4073 · Displayed: 4025 (98.8%)    Profile: Default
```

sudo nmap -sS -f 192.168.50.101

Effetto di -f:

- L'opzione -f frammenta i pacchetti IP generati da Nmap, rendendo più difficile per firewall e IDS analizzare il traffico.
- Questa tecnica tenta di eludere controlli di sicurezza che si basano sull'ispezione dei pacchetti completi.

Wireshark:

- Wireshark mostra chiaramente pacchetti IP frammentati, riconoscibili dal campo **Fragment Offset** nel protocollo IP.
- I servizi sulle porte aperte rispondono ai pacchetti frammentati con SYN-ACK, indicando che la frammentazione non ha ostacolato la comunicazione.

Differenze nei risultati

Opzione -g:
Tutte le porte aperte rilevate sono uguali rispetto a una scansione standard SYN (-sS), ma l'uso di una porta sorgente personalizzata (53) può eludere firewall configurati per consentire il traffico DNS.

Opzione -f:
La frammentazione dei pacchetti non influisce sul rilevamento delle porte aperte. Tuttavia, aumenta il numero totale di pacchetti inviati e può richiedere più risorse per il riassemblaggio lato target.