Esercitazione WEEK 11 D4

Scansione dei servizi con Nmap

Ettore Farris - 21/01/2024

Descrizione sintetica

Scansione di un host, senza e con completamento del 3-way handshake

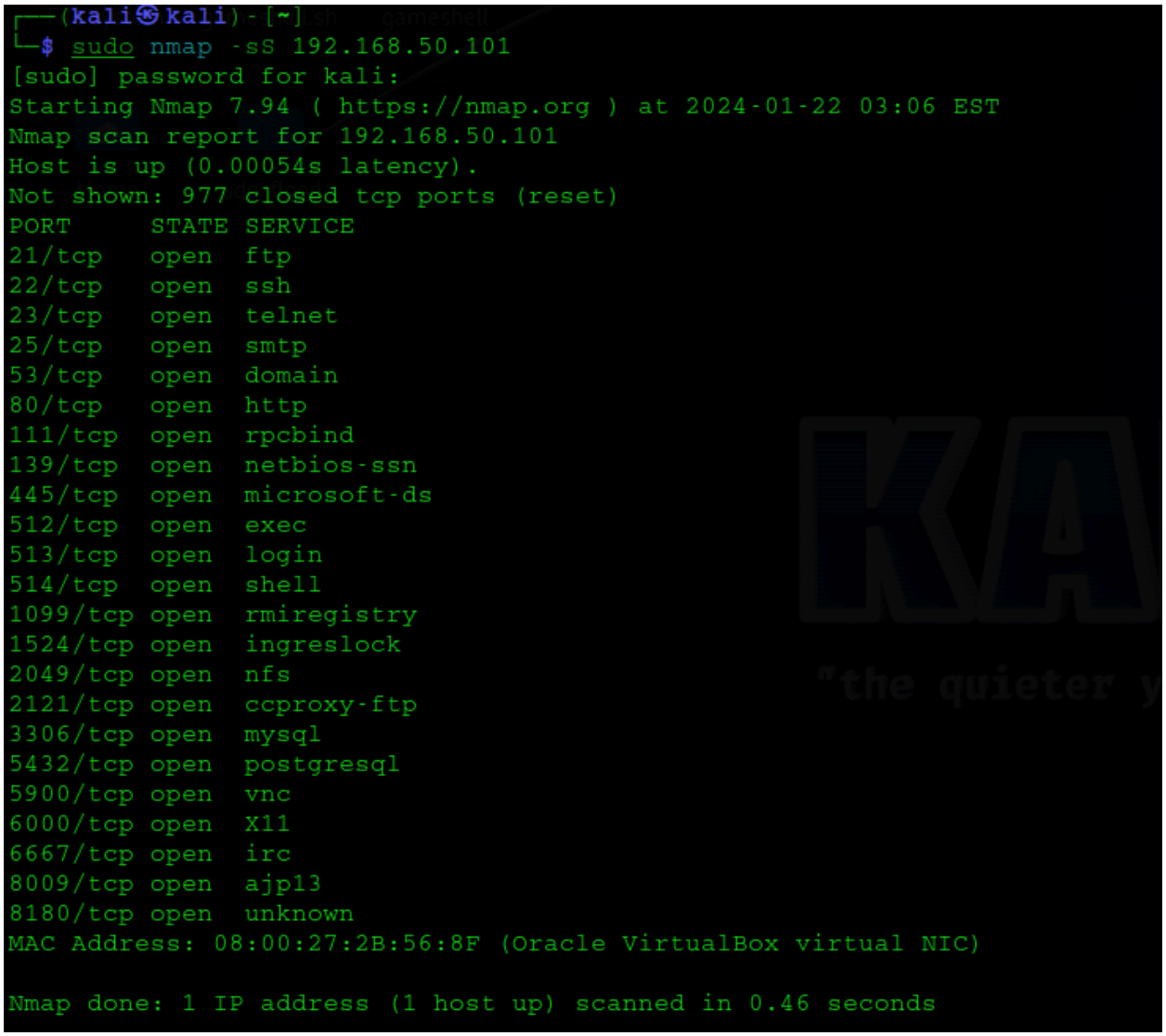
Questo esercizio può essere utile per lo studente per prendere dimestichezza con i vari comandi di nmap. Poiché su Linux è un potente tool di scansione della rete, si richiede di utilizzare i seguenti comandi e trascrivere i vari risultati su un report:

- SYN: # nmap -sS ip address
- scansione completa: # nmap -A ip address
- output su file: # nmap -sV -oN file.txt ip address
- scansione su porta: # nmap -sS -p 8080 ip address
- scansione tutte le porte: # nmap -sS -p- ip address
- scansione UDP: # nmap -sU -r -v ip address
- scansione sistema operativo: # nmap -O ip address
- scansione versione servizi: # nmap -sV ip address
- scansione common 100 ports: # nmap -F ip address
- scansione tramite ARP: # nmap -PR ip address
- scansione tramite PING: # nmap -sP ip address
- scansione senza PING: # nmap -PN ip address

Infine, disegnare 3-4 grafici delle scansioni effettuate, esplicitando le varie fasi di syn, syn/ack ecc.

1) STEALTH SCAN (SYN SCAN):

sudo nmap -sS 192.168.50.101

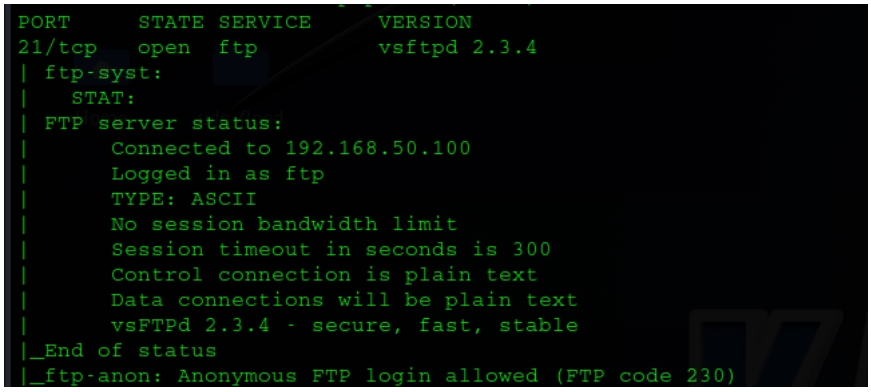


2) SCANSIONE COMPLETA: -A SCAN

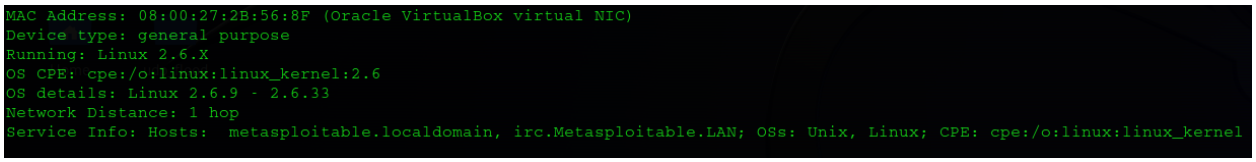
nmap -A 192.168.50.101

L'output di questa scansione è abbastanza lungo. Questo tipo di scan è particolarmente aggressiva e rumorosa, restituisce tantissimi dati sul target, come OS detection, scansione servizi, traceroute e script scanning. La scansione, oltre che ad eseguire la scan esegue degli script dalla libreria di nmap.) This is an aggressive scan. Riporto degli screen da confrontare con le altre scansioni presenti nel documento circa i risultati ottenuti per:

- Porta FTP



- OS Detection

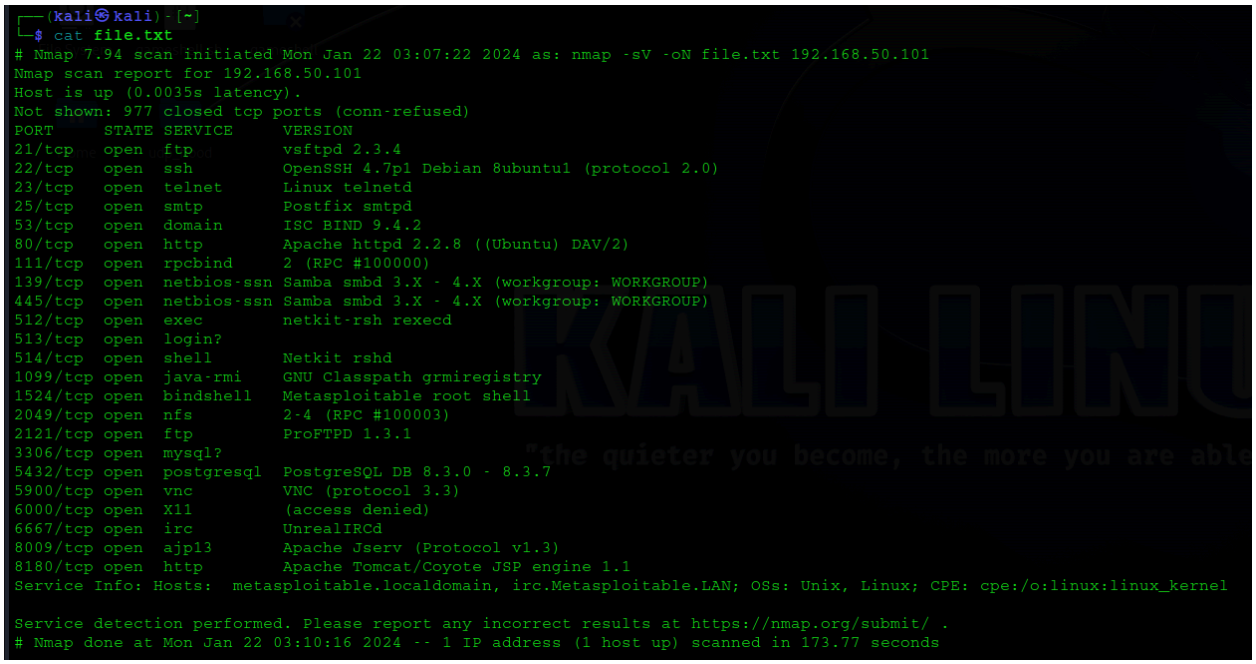


- Traceroute

3) SCANSIONE CON OUTPUT SU FILE

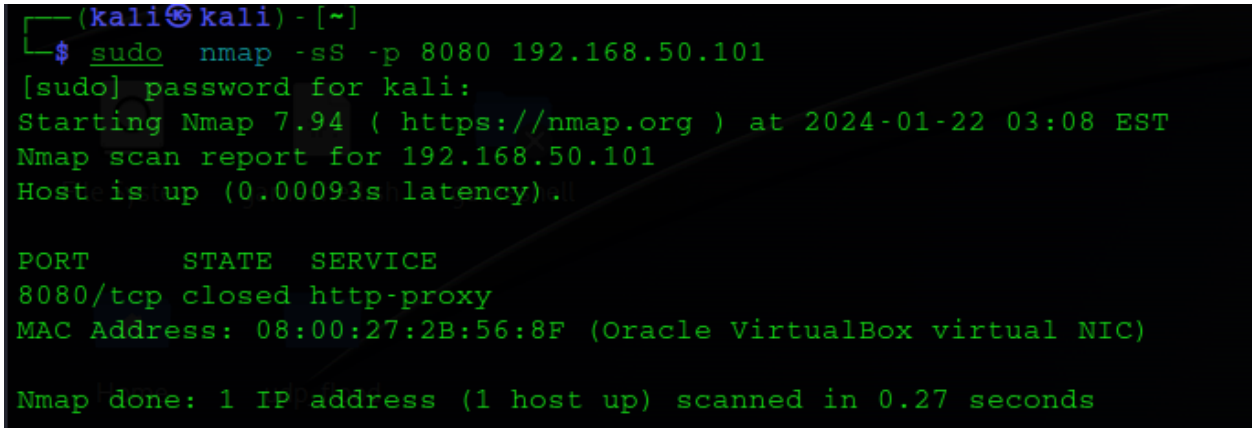
nmap -sV -oN file.txt 192.168.50.101

cat file.txt



4) SCANSIONE SU PORTA SPECIFICA

sudo nmap -sS -p 8080 192.168.50.101



5) SCANSIONE SU TUTTE LE PORTE

sudo nmap 192.168.50.101 -p-

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.50.101 -p-
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 03:15 EST
Nmap scan report for 192.168.50.101
Host is up (0.00053s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
42540/tcp open  unknown
44645/tcp open  unknown
49577/tcp open  unknown
49791/tcp open  unknown
MAC Address: 08:00:27:2B:56:8F (Oracle VirtualBox virtual NIC)
```

6) SCANSIONE SULLE PORTE UDP

sudo nmap -sU -r -v 192.168.50.101

```
Not shown: 953 closed udp ports (port-unreach)
PORT     STATE         SERVICE
21/udp   open|filtered ftp
37/udp   open|filtered time
38/udp   open|filtered rap
49/udp   open|filtered tacacs
53/udp   open          domain
67/udp   open|filtered dhcps
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
80/udp   open|filtered http
111/udp  open          rpcbind
112/udp  open|filtered mcidas
113/udp  open|filtered auth
120/udp  open|filtered cfdptkt
135/udp  open|filtered msrpc
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
139/udp  open|filtered netbios-ssn
161/udp  open|filtered snmp
162/udp  open|filtered snmptrap
177/udp  open|filtered xdmcp
199/udp  open|filtered smux
207/udp  open|filtered at-7
217/udp  open|filtered dbase
389/udp  open|filtered ldap
402/udp  open|filtered genie
407/udp  open|filtered timbuktu
434/udp  open|filtered mobileip-agent
443/udp  open|filtered https
464/udp  open|filtered kpasswd5
497/udp  open|filtered retrospect
500/udp  open|filtered isakmp
512/udp  open|filtered biff
513/udp  open|filtered who
515/udp  open|filtered printer
517/udp  open|filtered talk
520/udp  open|filtered route
559/udp  open|filtered teedtap
623/udp  open|filtered asf-rmcp
631/udp  open|filtered ipp
643/udp  open|filtered sanity
664/udp  open|filtered secure-aux-bus
683/udp  open|filtered corba-iiop
685/udp  open|filtered mdc-portmapper
687/udp  open|filtered asipregistry
689/udp  open|filtered nmap
767/udp  open|filtered phonebook
2049/udp open          nfs
MAC Address: 08:00:27:2B:56:8F (Oracle VirtualBox virtual NIC)
```

7) SCANSIONE SISTEMA OPERATIVO

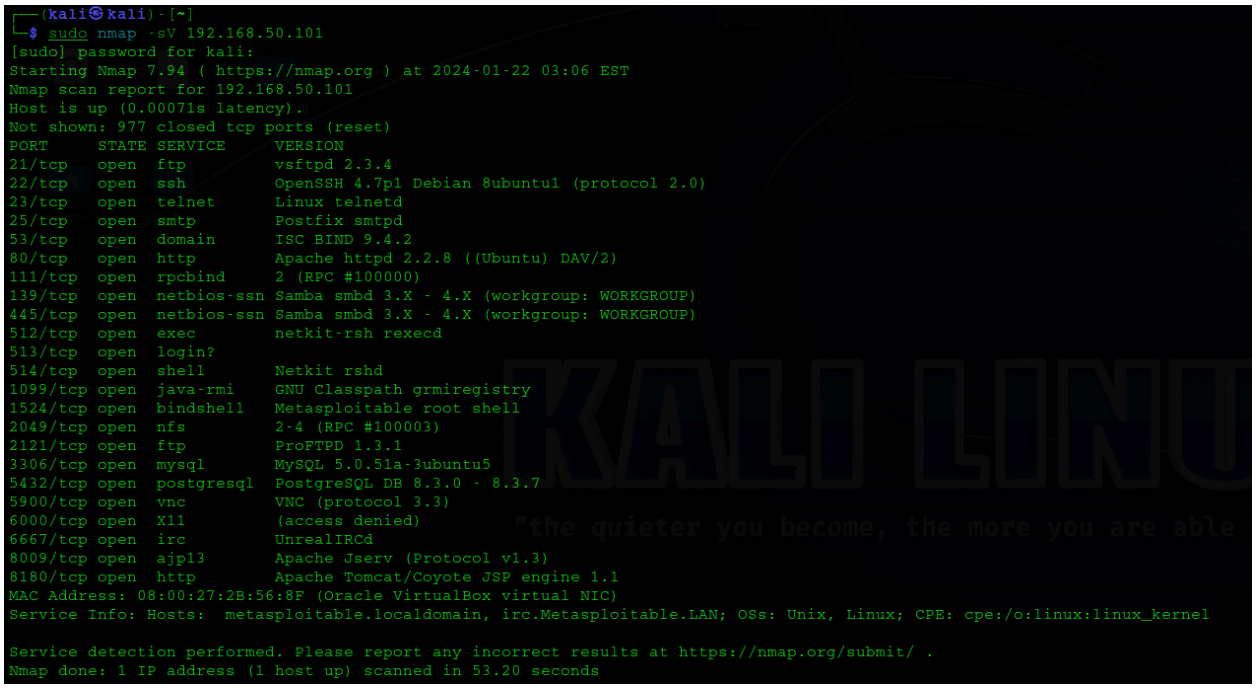
sudo nmap -O 192.168.50.101

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 04:24 EST
Nmap scan report for 192.168.50.101
Host is up (0.00086s 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: 08:00:27:2B:56:8F (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 1.68 seconds
```

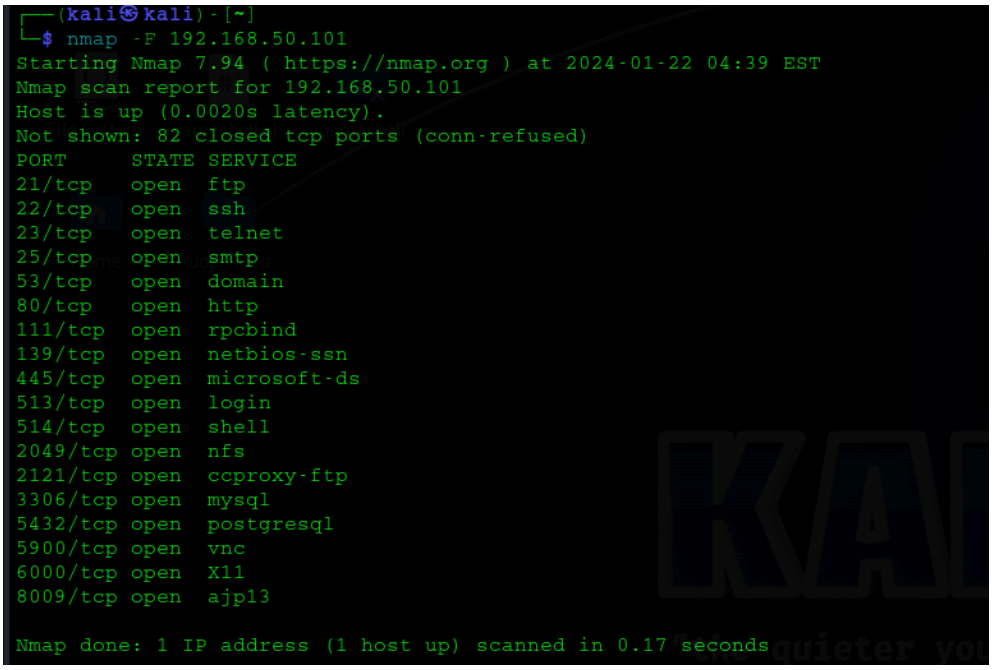
8) SCANSIONE VERSIONE SERVIZI (-sV SCAN)

sudo nmap -sV 192.168.50.101



9) SCANSIONE TOP 100 PORTE (FAST SCAN)

nmap -F 192.168.50.101



10) ARP SCAN

nmap -PR 192.168.50.101

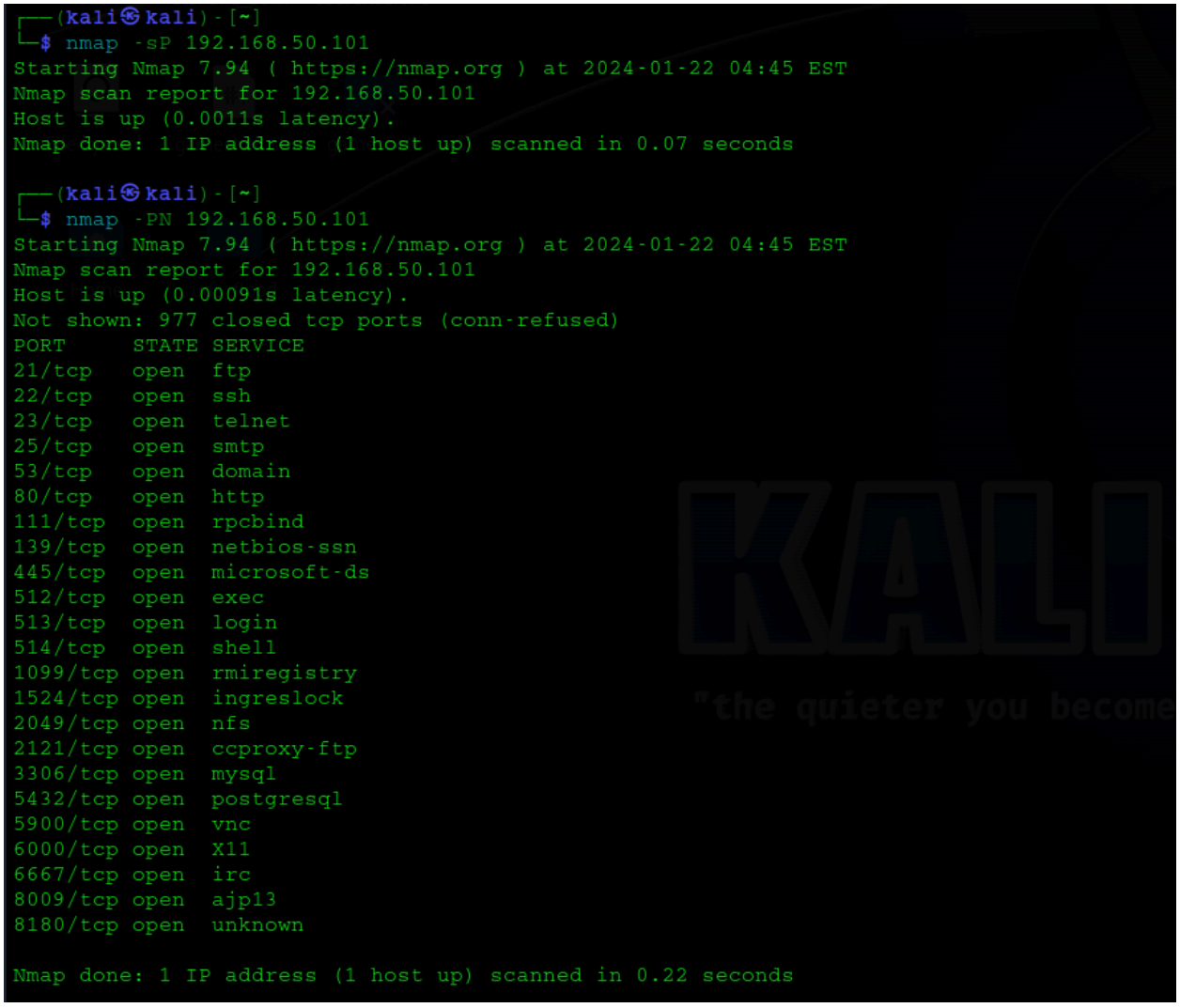
```
┌──(kali㉿kali)-[~]
└─$ nmap -PR 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 04:43 EST
Nmap scan report for 192.168.50.101
Host is up (0.0036s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

11) SCANSIONE CON PING (-sP) E SENZA PING (-PN)

nmap -sP 192.168.50.101

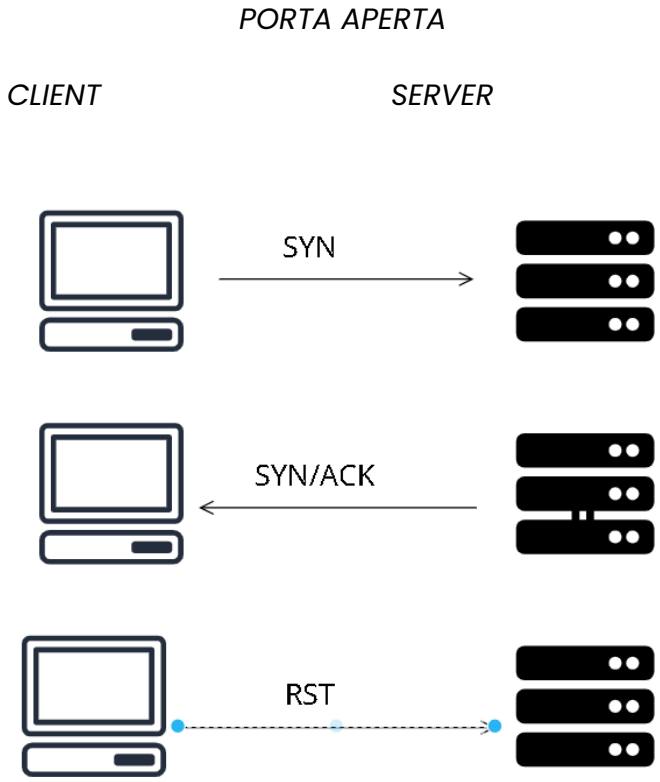
nmap -PN 192.168.50.101



12) GRAFICI SCANSIONI

SYN SCAN

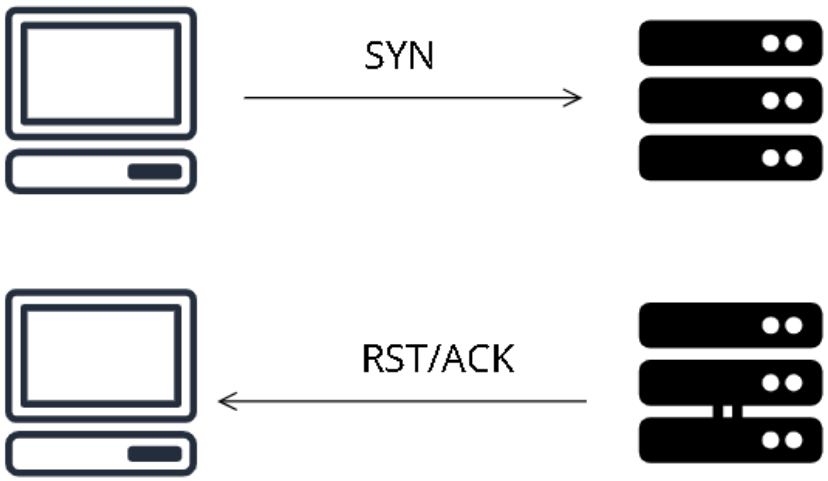
sudo nmap -sS 192.168.50.101



	Time	Source	Destination	Protocol	Length	Info
10	0.156061532	192.168.50.100	192.168.50.101	TCP	58	35897 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	0.156821290	192.168.50.101	192.168.50.100	TCP	60	80 → 35897 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
25	0.157016851	192.168.50.100	192.168.50.101	TCP	54	35897 → 80 [RST] Seq=1 Win=0 Len=0

PORTA CHIUSA

CLIENT *SERVER*

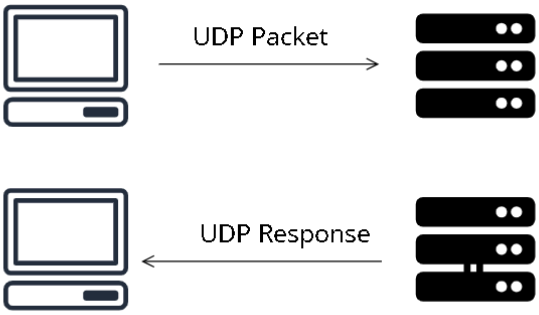


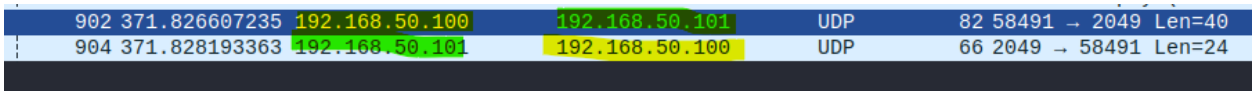
	Time	Source	Destination	Protocol	Length	Info
1940	841.528050259	192.168.50.100	192.168.50.101	TCP	58	41983 → 8569 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1941	841.528839200	192.168.50.101	192.168.50.100	TCP	60	8569 → 41983 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

UDP SCAN

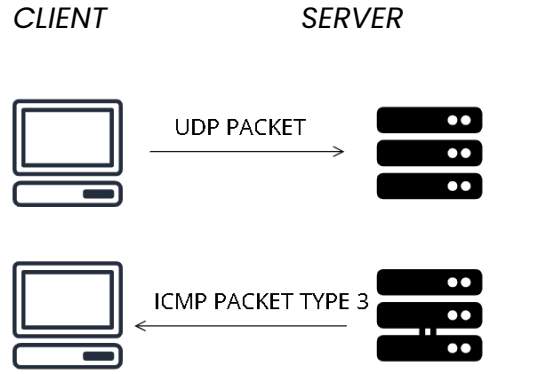
nmap -sU -r -v 192.168.50.101

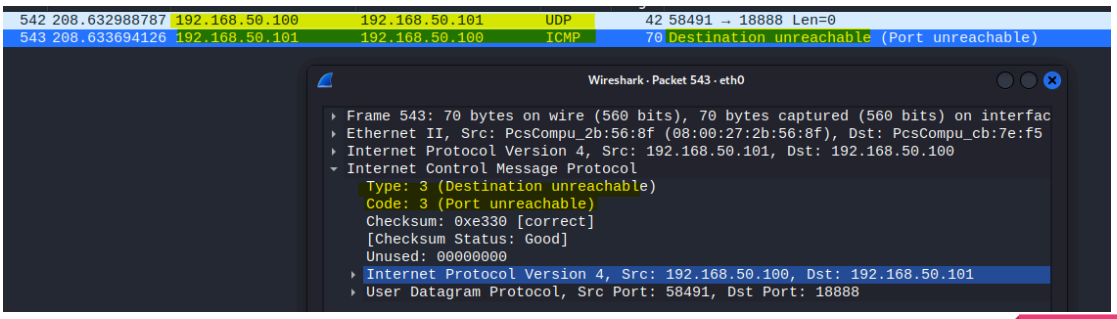
PORTA APERTA





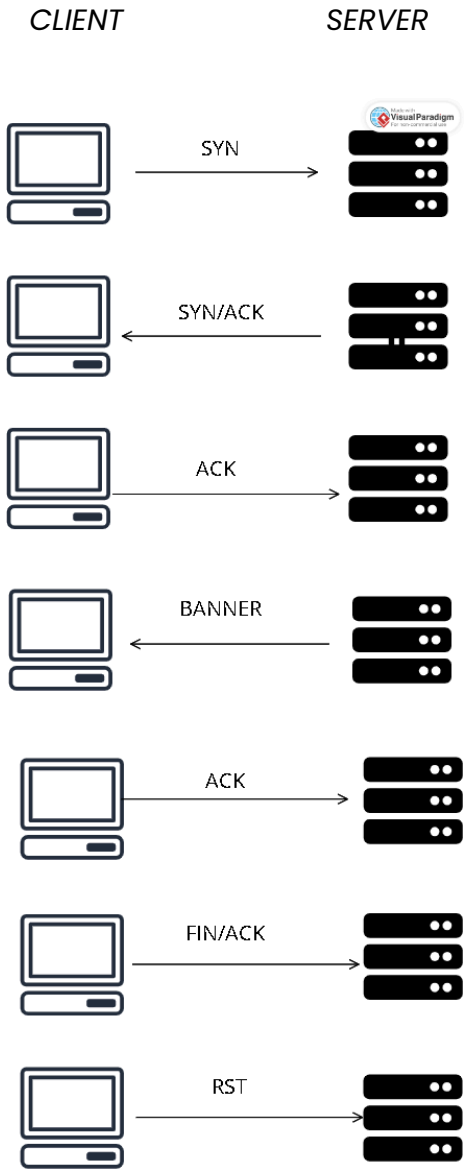
PORTA CHIUSA





SCANSIONE VERSIONE SERVIZI

nmap -sv 192.168.50.101



26	19.460694242	192.168.50.100	192.168.50.101	TCP	74 57874 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=61041728 TSecr=0
27	19.461757531	192.168.50.101	192.168.50.100	TCP	74 21 → 57874 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=5358400
28	19.461846806	192.168.50.100	192.168.50.101	TCP	66 57874 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=61041729 TSecr=5358400
29	19.464878147	192.168.50.101	192.168.50.100	FTP	86 Response: 220 (vsFTPd 2.3.4)
30	19.464968497	192.168.50.100	192.168.50.101	TCP	66 57874 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=61041732 TSecr=5358401
31	19.465204835	192.168.50.100	192.168.50.101	TCP	66 57874 → 21 [FIN, ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=61041732 TSecr=5358401
32	19.466947835	192.168.50.101	192.168.50.100	FTP	76 Response: 500 OOPS:
33	19.466982472	192.168.50.100	192.168.50.101	TCP	54 57874 → 21 [RST] Seq=2 Win=0 Len=0
34	19.467597152	192.168.50.101	192.168.50.100	FTP	96 Response: vsf_sysutil_recv_peek: no data
35	19.467637755	192.168.50.100	192.168.50.101	TCP	54 57874 → 21 [RST] Seq=2 Win=0 Len=0