

The image shows a screenshot of a Kali Linux virtual machine running in Oracle VM VirtualBox. The terminal window displays the output of an Nmap scan performed on the IP address 192.168.50.101. The scan was executed using the command `sudo nmap -sT -p 0-1023 192.168.50.101`. The output indicates that the host is up and lists 15 open ports with their corresponding services. The background of the terminal features a large, stylized 'KALI LINUX' logo and the quote 'the quieter you become, the more you are able to hear'.

```
(kali@kali)-[~]
$ sudo nmap -sT -p 0-1023 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 12:46 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00057s latency).
Not shown: 1012 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
MAC Address: 08:00:27:56:7C:8E (Oracle VirtualBox virtual NIC)

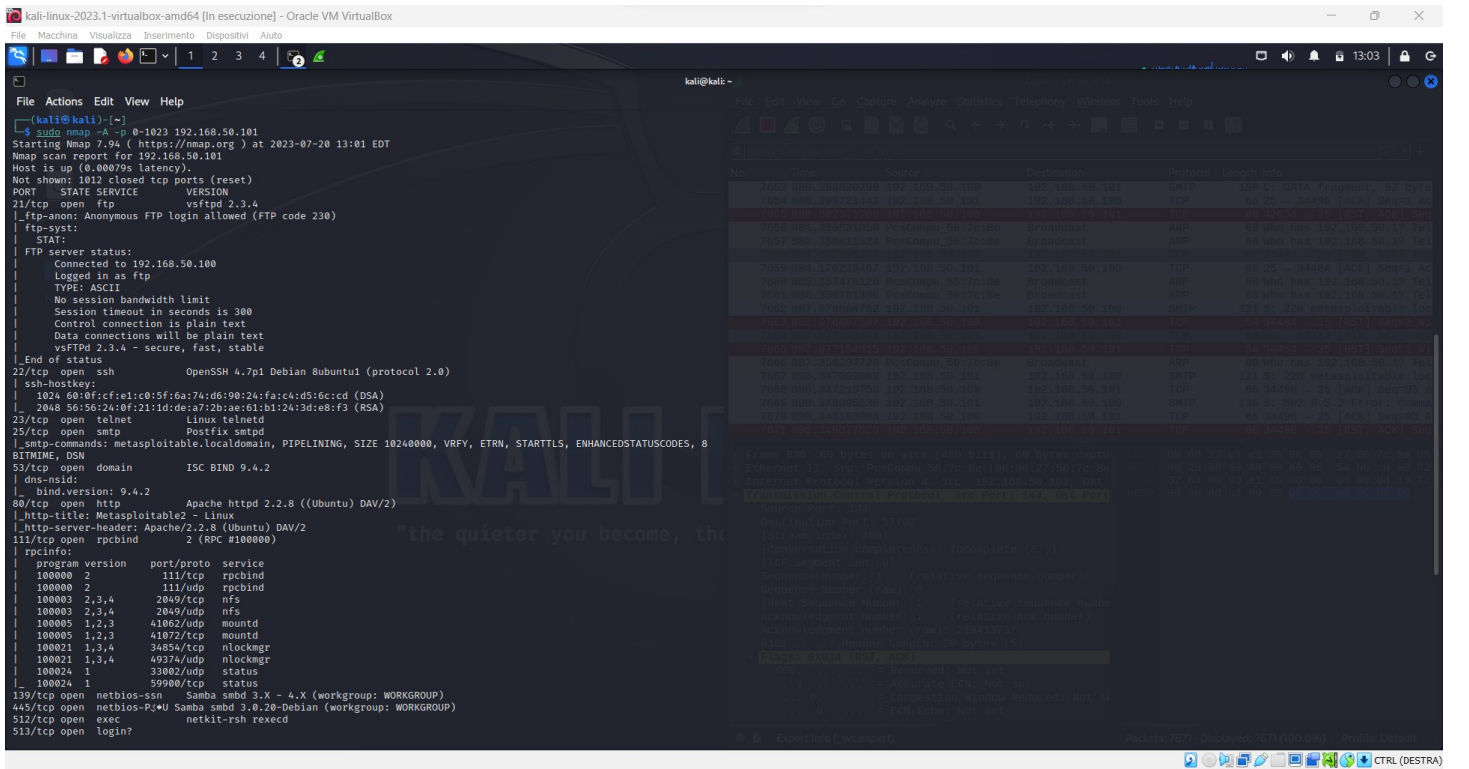
Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds

(kali@kali)-[~]
$
```

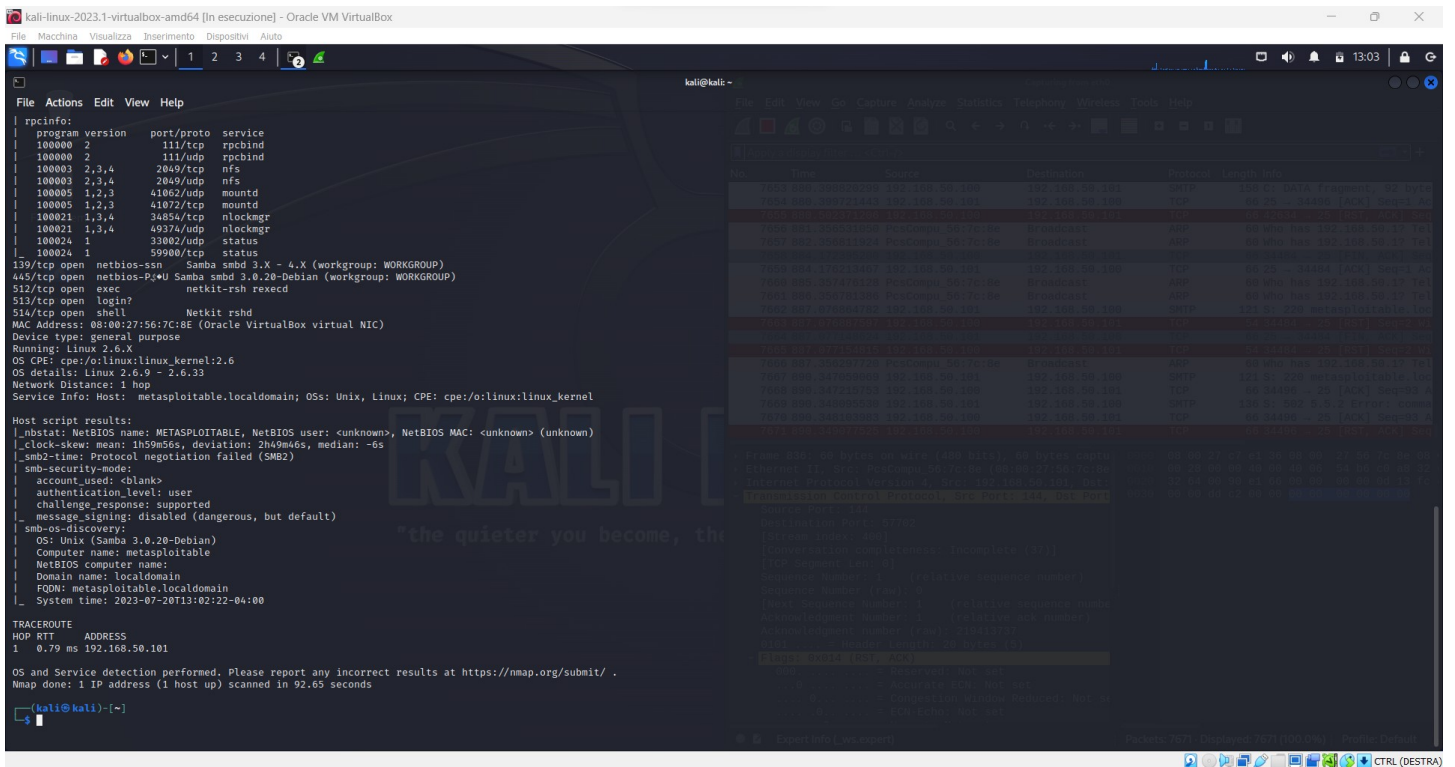
Scansione TCP su ip target delle well-known ports.

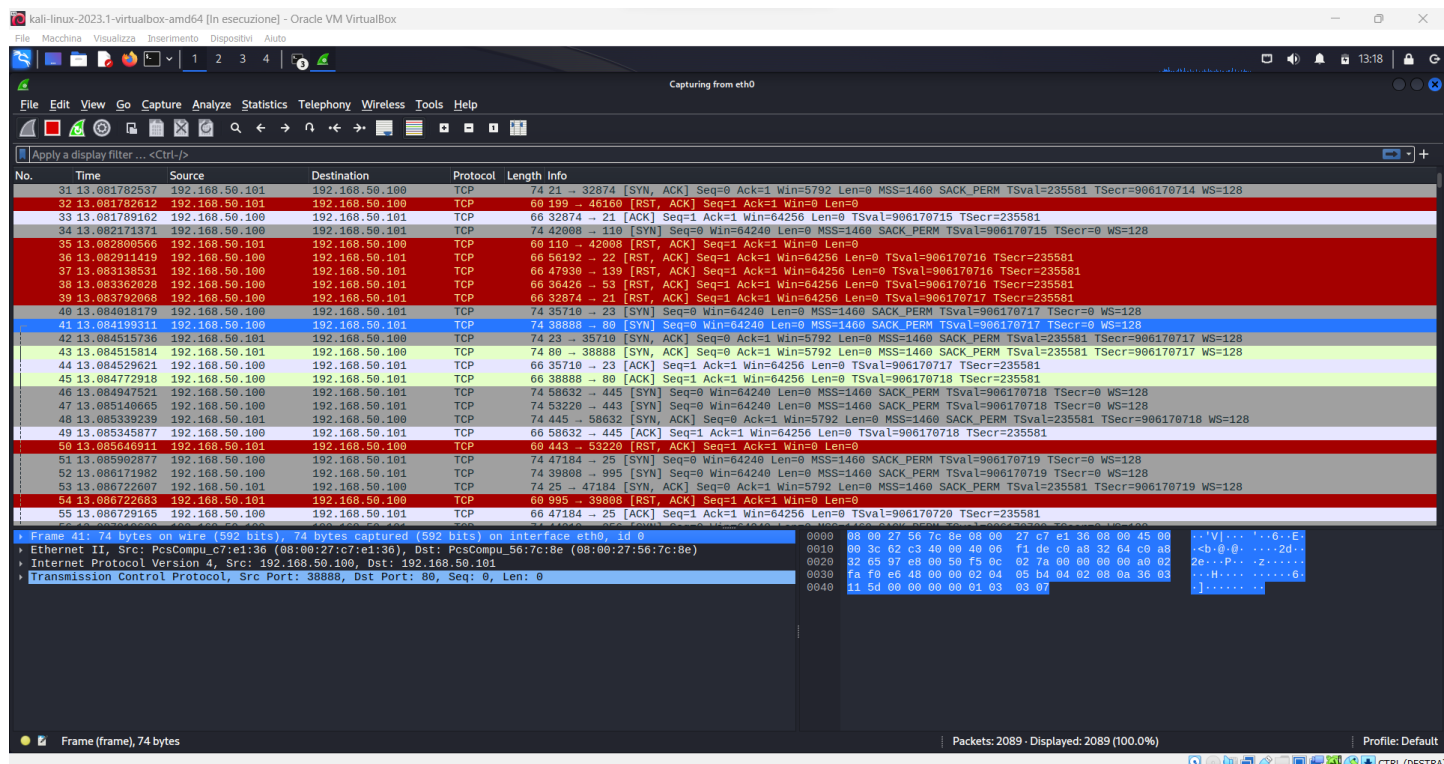
```
(kali㉿kali)-[~]  
$ sudo nmap -sS -p 0-1023 192.168.50.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 12:54 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00035s latency).  
Not shown: 1012 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    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  
MAC Address: 08:00:27:56:7C:8E (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds  
  
(kali㉿kali)-[~]  
$
```

Scansione SYN dell'ip target delle well-known ports.



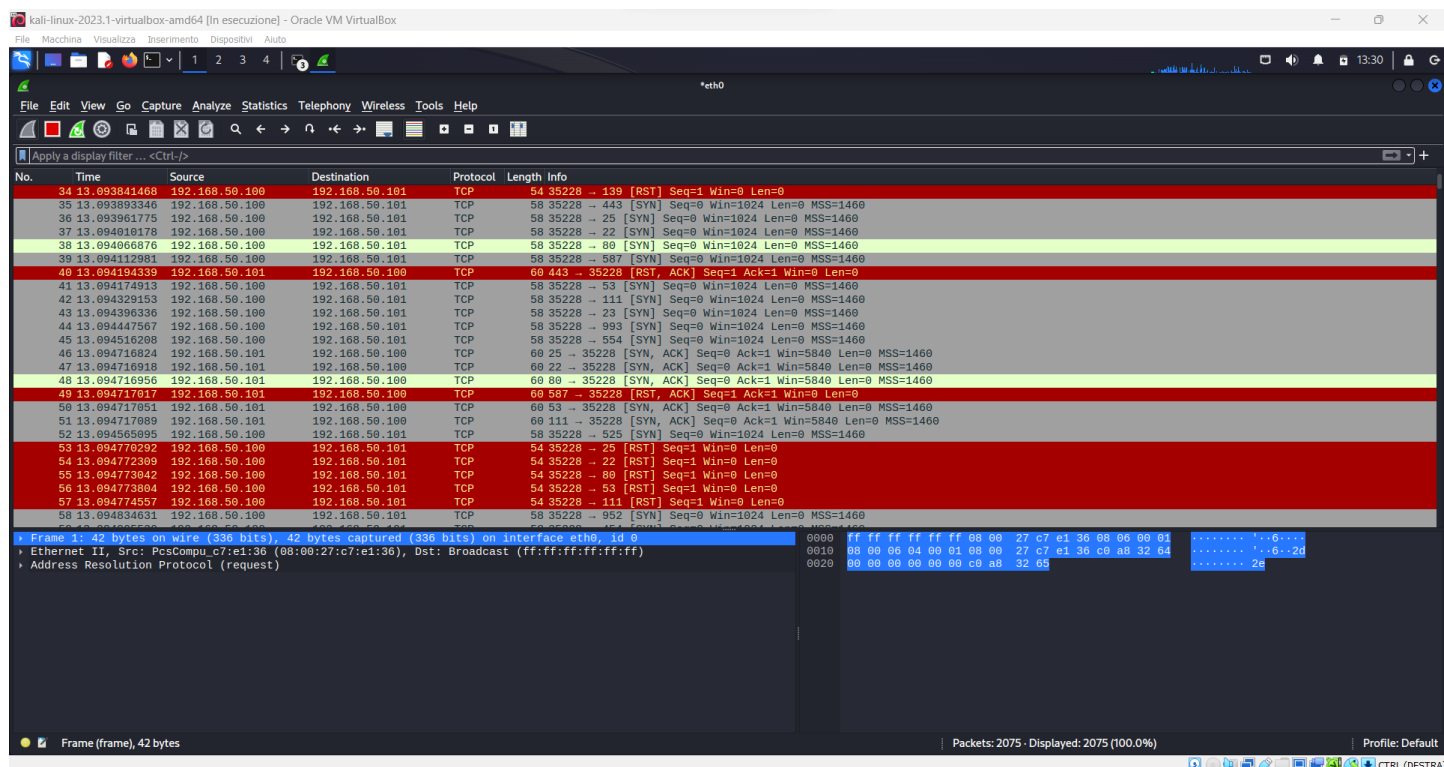
Scansione Aggressiva su ip target delle well-known ports





Cattura su wireshark dei pacchetti della scansione TCP sull'ip address.

La scansione TCP crea un handshake a differenza della scansione SYN che effettua la richiesta ma poi non porta a termine il 3way handshake.



Cattura dei pacchetti della scansione SYN, la richiesta viene effettuata ma non viene stabilito un 3way-handshake.

