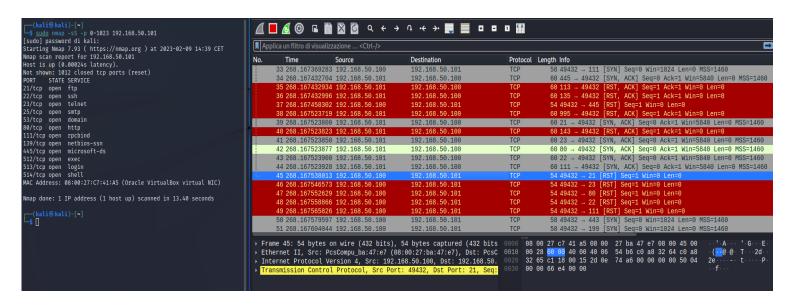
## **Host discovery**

```
–(kali⊛kali)-[~]
$\sudo nmap -F -sS
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 12:50 CET
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds
$ sudo nmap -F -sS 192.168.50.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 12:50 CET
Host is up (0.000097s latency).
Not shown: 82 closed tcp ports (reset)
         STATE SERVICE
PORT
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
513/tcp open login
514/tcp open shell
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
8009/tcp open ajp13
MAC Address: 08:00:27:C7:41:A5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.100
Host is up (0.0000050s latency).
All 100 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 100 closed tcp ports (reset)
Nmap done: 256 IP addresses (2 hosts up) scanned in 30.50 seconds
```

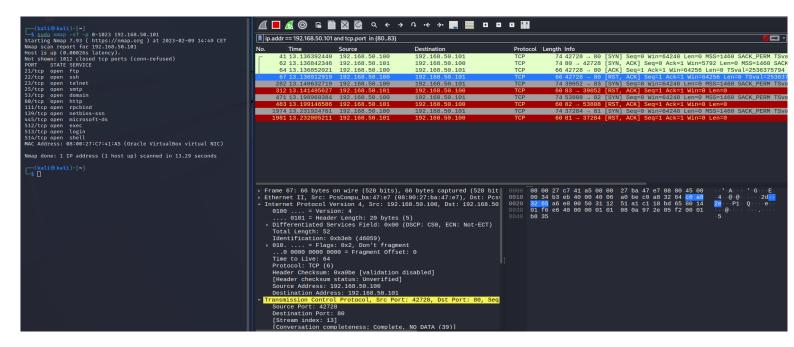
Ho scannerizzato la rete con nmap ed è stata correttamente individuata la macchina metaesploitable. Utilizzando lo switch –F, nmap testa le 100 porte di solito più utilizzate, e in questo caso sono state trovate 18 aperte.

## Sys scan su porte well-know



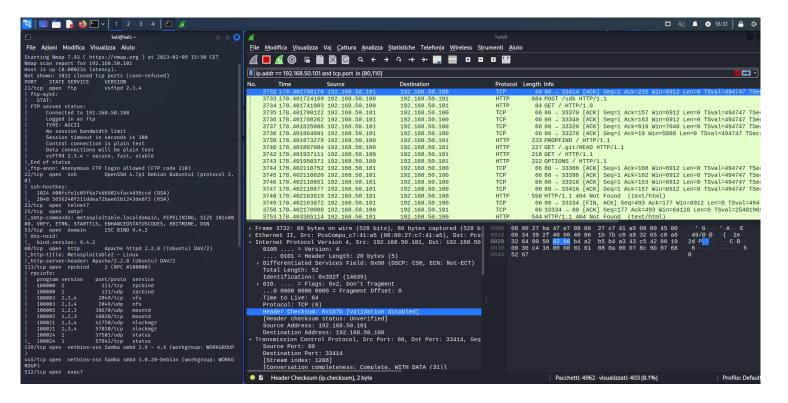
Fonte	Target	Tipo Scan	Risultato
Kali(192.168.50.100)	Metasploitable (192.168.50.101)	sS	12 servizi attivi su
			porte 0-1023

## Tcp Scan su porte well-know



Fonte	Target	Tipo Scan	Risultato
Kali(192.168.50.100)	Metasploitable(192.168.50.101)	sT	12 servizi attivi su porte 0-1023

## Scan con switch -A



Fonte	Target	Tipo Scan	Risultato
Kali(192.168.50.100)	Metasploitable (192.168.50.101)	sT -A	12 servizi attivi su porte 0-1023, incluse versioni e info sui servizi e S.O.