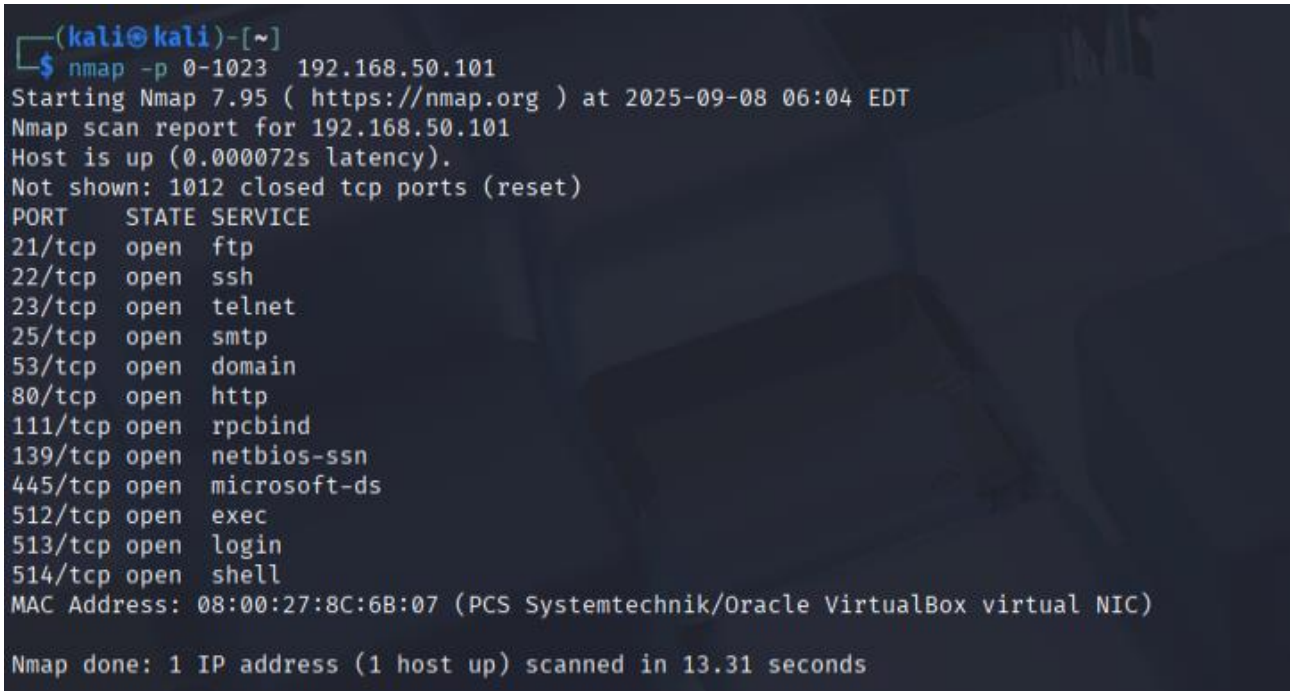
Esecuzione scansione sulla macchina metaspotable con nmap:

Scansione TCP:



Report:

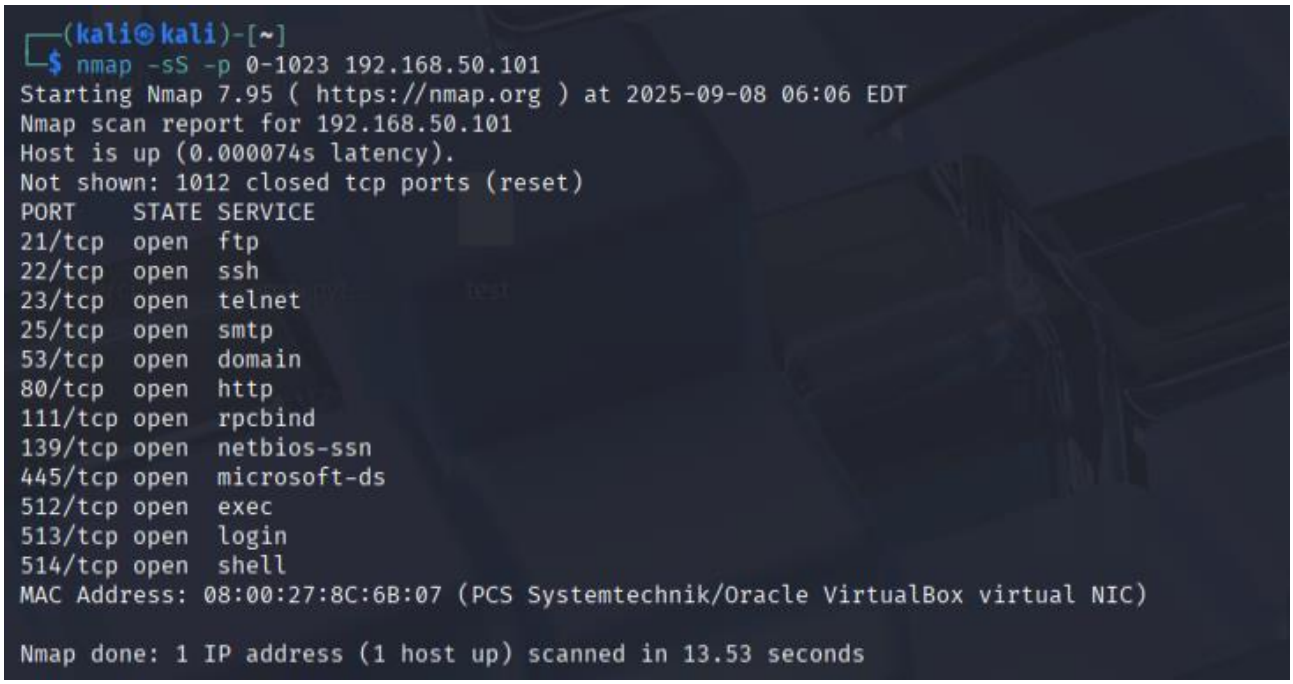
Fonte dello scan: macchina kali linux con ip 192.168.50.100

Target dello scan: macchina metaspotable con ip 192.168.50.100

Tipo di scan: scansione TCP sulle porte well-known (dalla 0 alla 1023)

Risultati: 12 porte TCP aperte

Scansione SYN



Report:

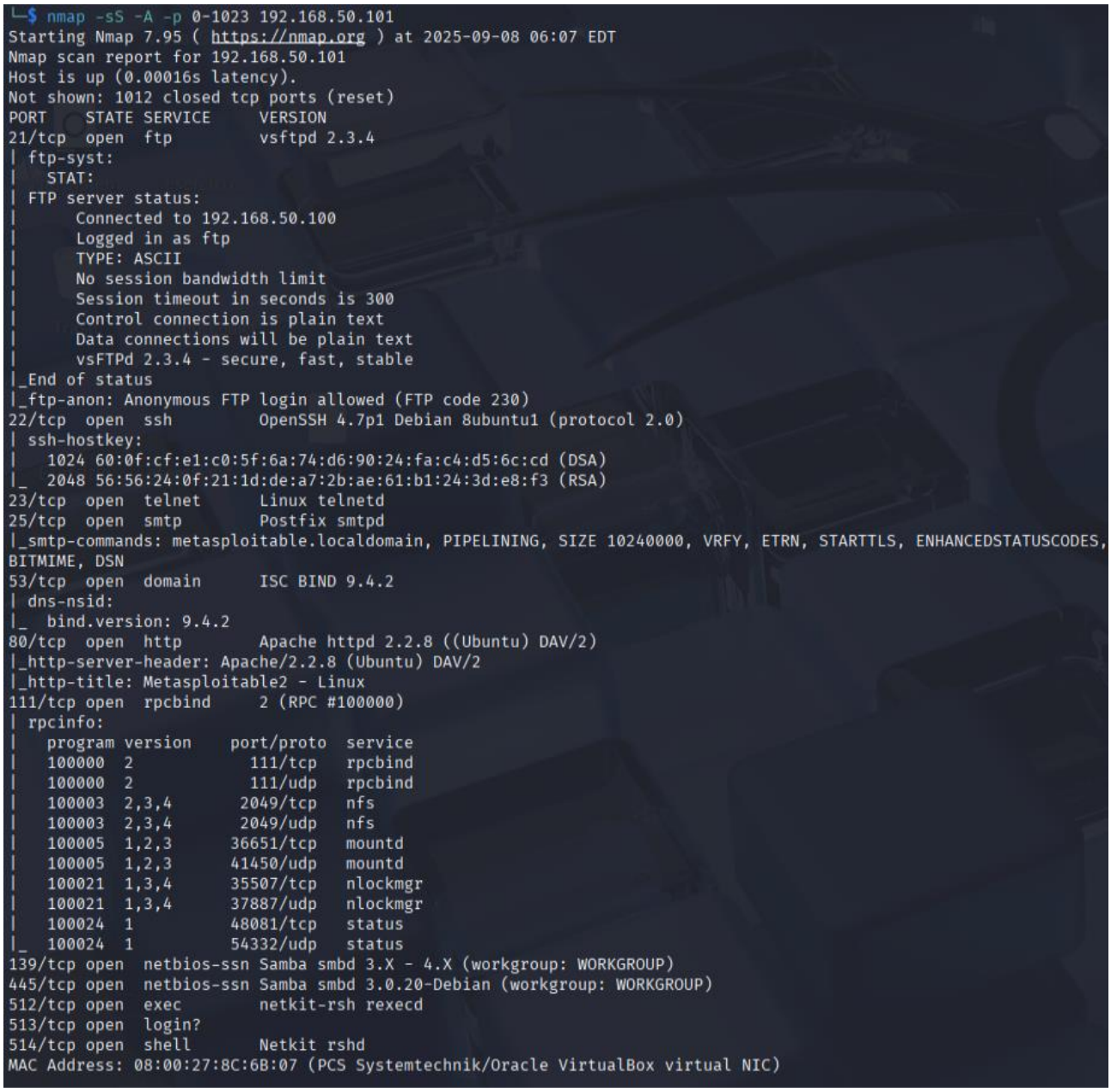
Fonte dello scan: macchina kali linux con ip 192.168.50.100

Target dello scan: macchina metaspotable con ip 192.168.50.100

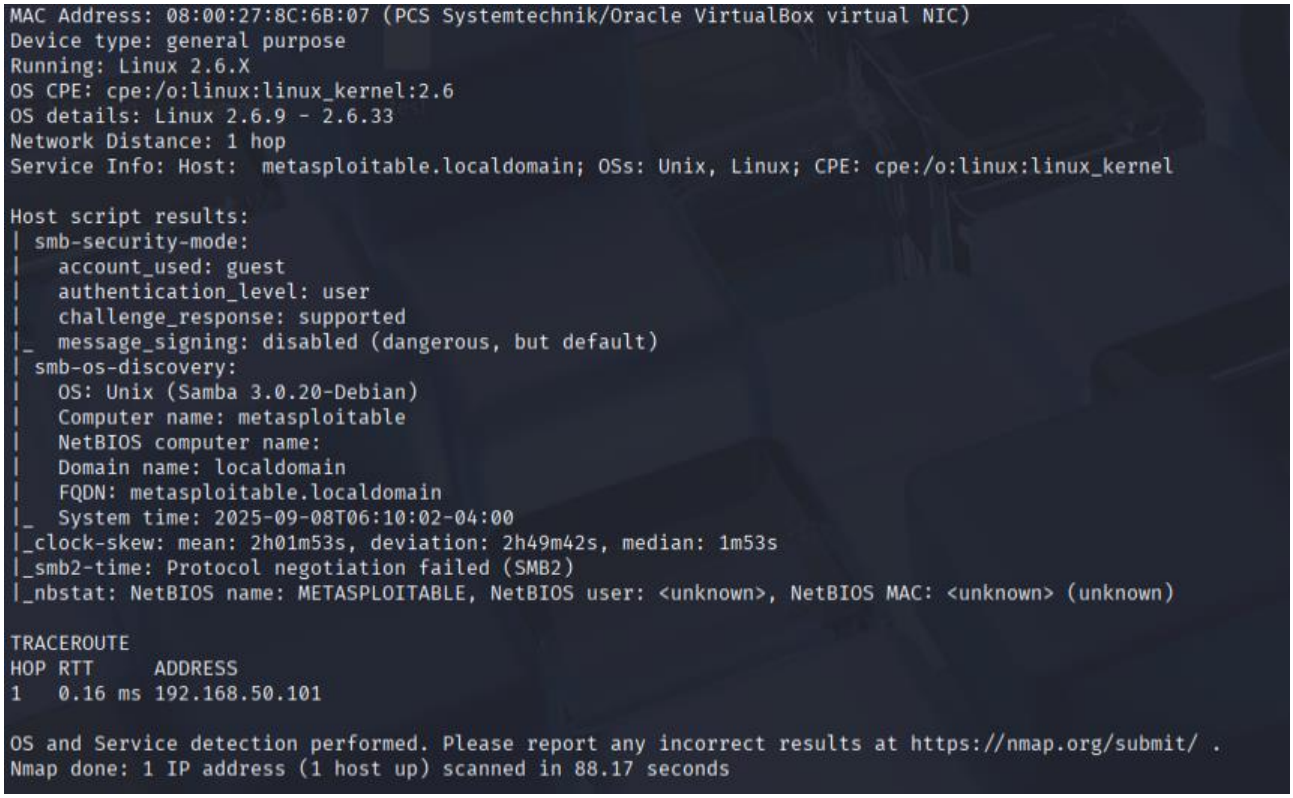
Tipo di scan: scansione SYN sulle porte well-known (dalla 0 alla 1023)

Risultati: 12 porte aperte

Scansione -A



```
└─$ nmap -sS -A -p 0-1023 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 06:07 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00016s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
BITMIME, DSN
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      36651/tcp   mountd
|   100005  1,2,3      41450/udp   mountd
|   100021  1,3,4      35507/tcp   nlockmgr
|   100021  1,3,4      37887/udp   nlockmgr
|   100024  1          48081/tcp   status
|_  100024  1          54332/udp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:8C:6B:07 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```



Report:

Fonte dello scan: macchina kali linux con ip 192.168.50.100

Target dello scan: macchina metaspotable con ip 192.168.50.100

Tipo di scan: scansione con switch «-A» sulle porte well-known (dalla 0 alla 1023)

Risultati: come da screen riportato qui sopra oltre ad aver intercettato le porte aperte con i relativi servizi in uso abbiamo altri risultati interessanti in quanto -A ci permette di intercettare il sistema operativo, i servizi e gli script.