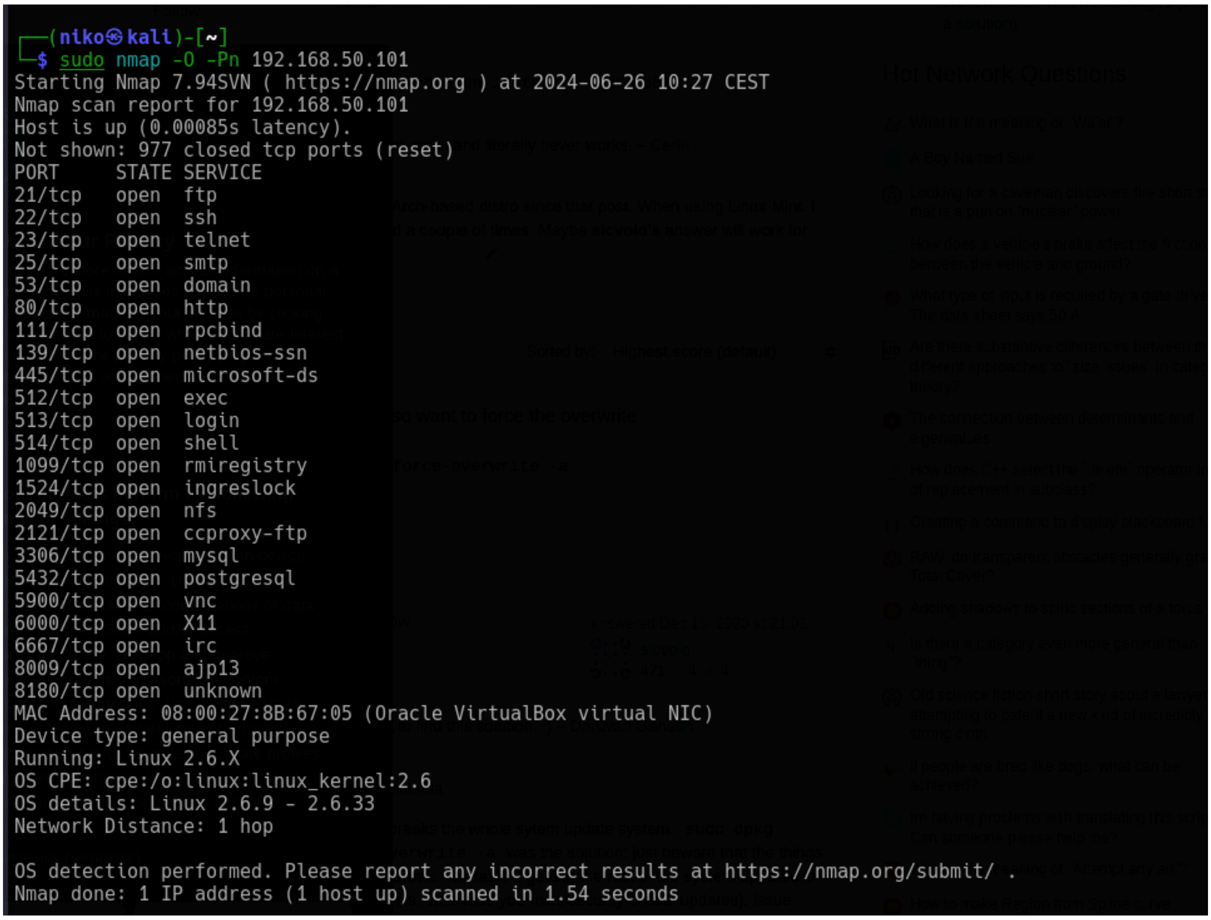
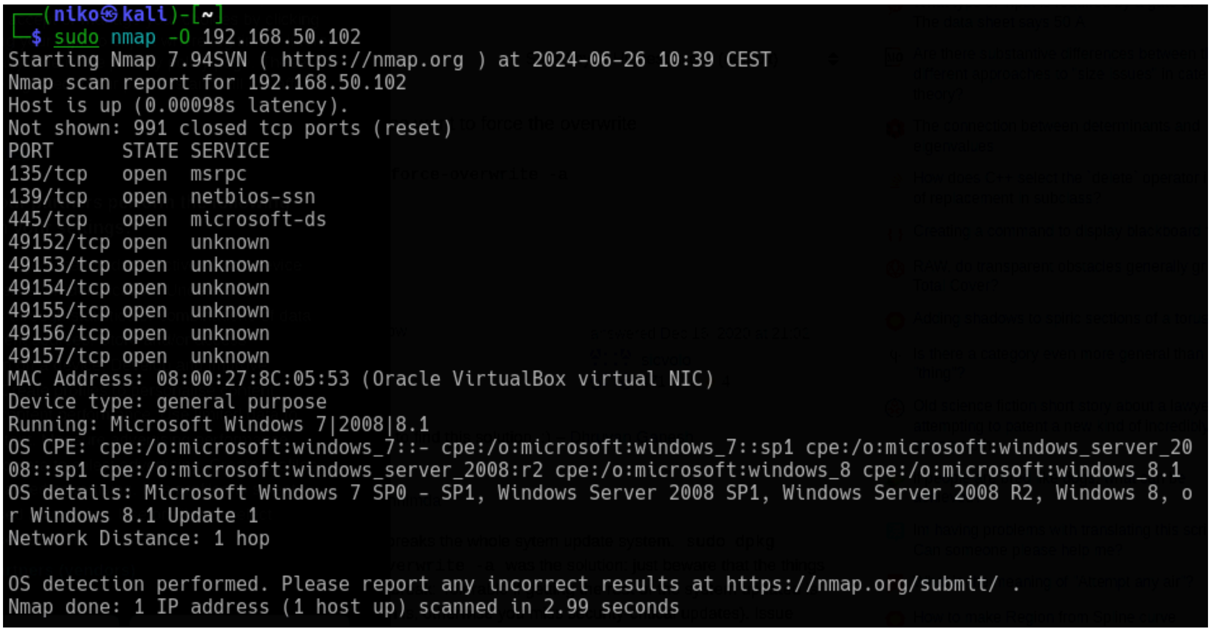
OS fingerprinting della metasploitable



```
┌──(niko㉿kali)-[~]
└─$ sudo nmap -O -Pn 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 10:27 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00085s 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: 08:00:27:8B:67:05 (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 1.54 seconds
```

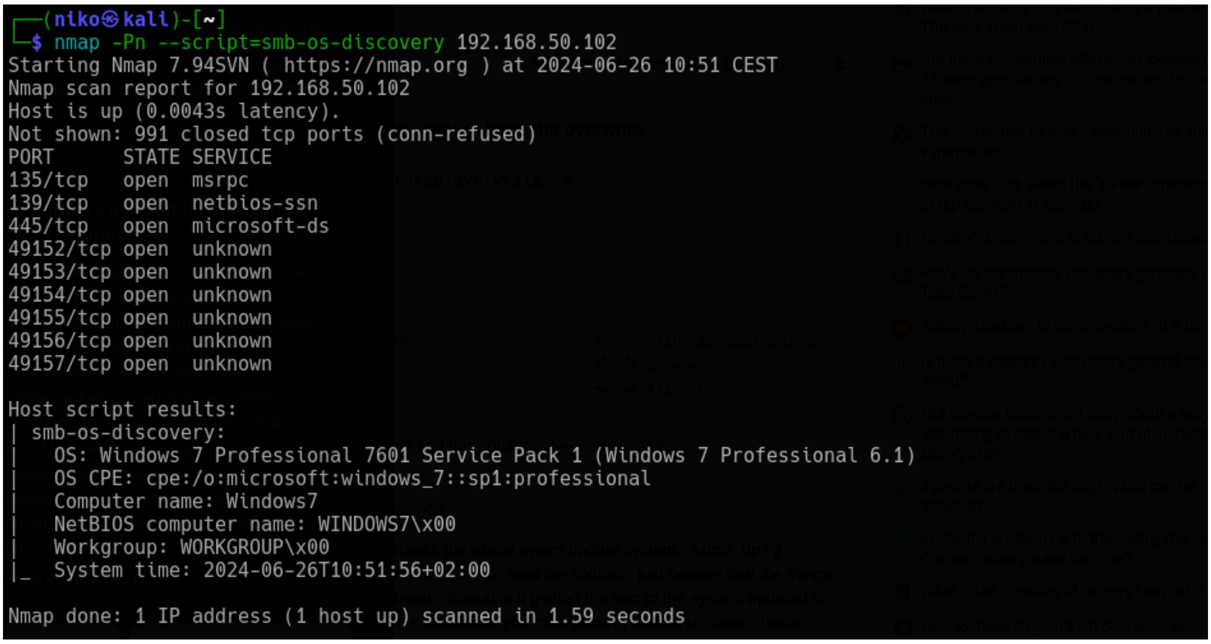
OS fingerprinting di Windows 7 (991 porte chiuse o filtrate accessibili con altre tecniche (-T1)



```
┌──(niko㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 10:39 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00098s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:8C:05:53 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_20
08::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, o
r Windows 8.1 Update 1
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 2.99 seconds
```

In alternativa per scoprire l’OS si può usare uno script preinstallato

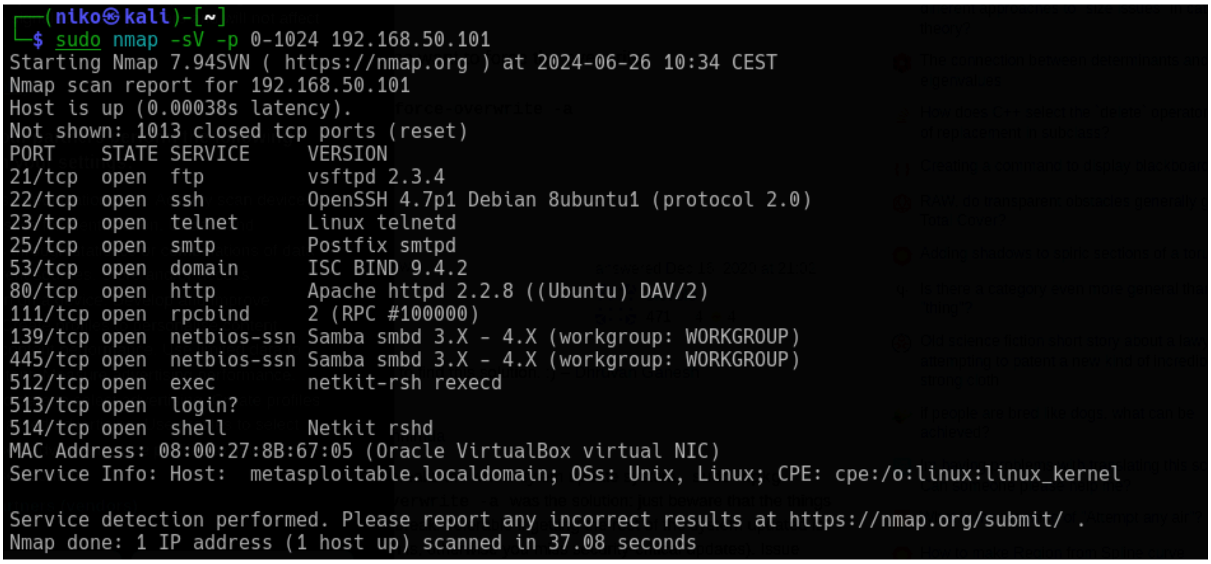


```
┌──(niko㉿kali)-[~]
└─$ nmap -Pn --script=smb-os-discovery 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 10:51 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0043s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Windows7
|   NetBIOS computer name: WINDOWS7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-06-26T10:51:56+02:00

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

Scansione porte da 0 a 1024 e versione servizi su metasploitable

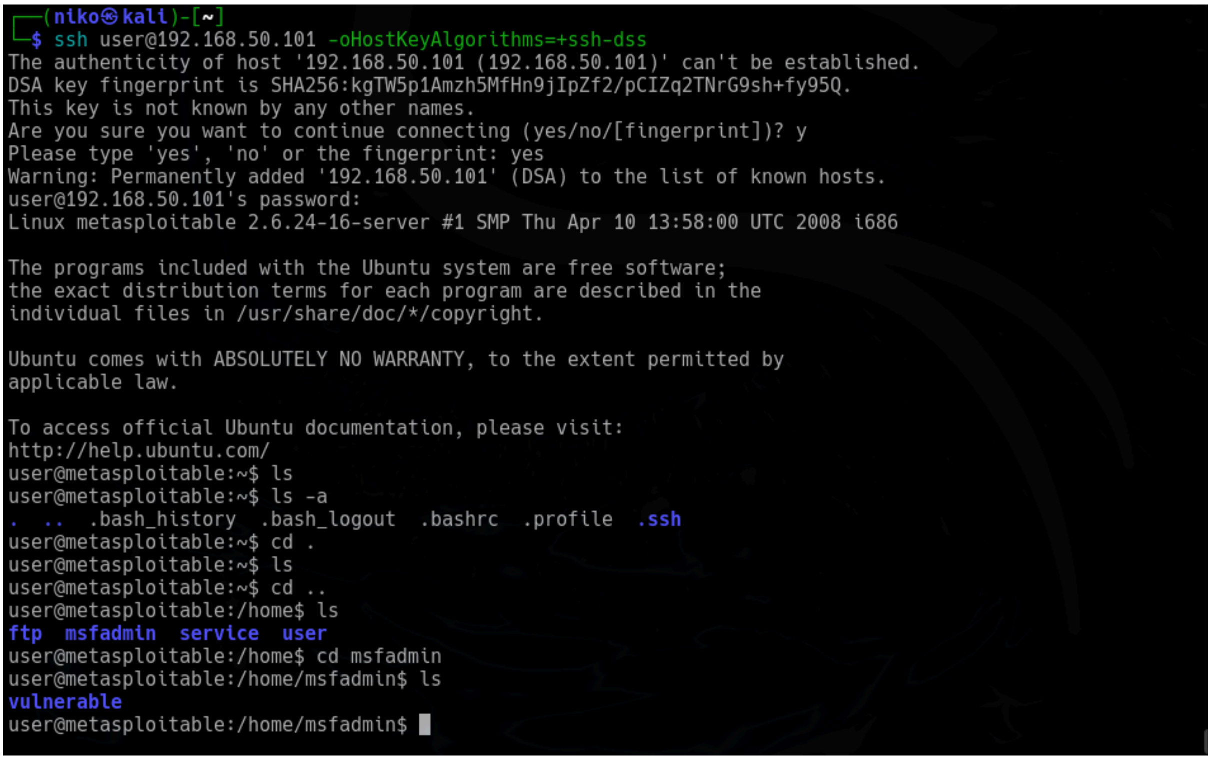


```
┌──(niko㉿kali)-[~]
└─$ sudo nmap -sV -p 0-1024 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 10:34 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00038s latency).
Not shown: 1013 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         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  shell       Netkit rshd
MAC Address: 08:00:27:8B:67:05 (Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; 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 37.08 seconds
```

La principale differenza tra l’opzione -sS e -sT è il metodo con cui viene effettuata la scansione sulla porta, -sS usa SYN e non conclude la connessione mentre -sT fa un 3-way handshake ed è più invasivo.

Dopo aver fatto un brute force attack per scoprire user e pass del servizio ssh con uno script preinstallato possiamo accedere da remoto alla metasploitable sulla port 22 con user:user



```
┌──(niko㉿kali)-[~]
└─$ ssh user@192.168.50.101 -oHostKeyAlgorithms=+ssh-dss
The authenticity of host '192.168.50.101 (192.168.50.101)' can't be established.
DSA key fingerprint is SHA256:kgTW5p1Amzh5MfHn9jIpZf2/pCIZq2TNrG9sh+fy95Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.50.101' (DSA) to the list of known hosts.
user@192.168.50.101's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
user@metasploitable:~$ ls
user@metasploitable:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .profile  .ssh
user@metasploitable:~$ cd .
user@metasploitable:~$ ls
user@metasploitable:~$ cd ..
user@metasploitable:/home$ ls
ftp  msfadmin  service  user
user@metasploitable:/home$ cd msfadmin
user@metasploitable:/home/msfadmin$ ls
vulnerable
user@metasploitable:/home/msfadmin$ 
```