----------Scan Metaspotable----------

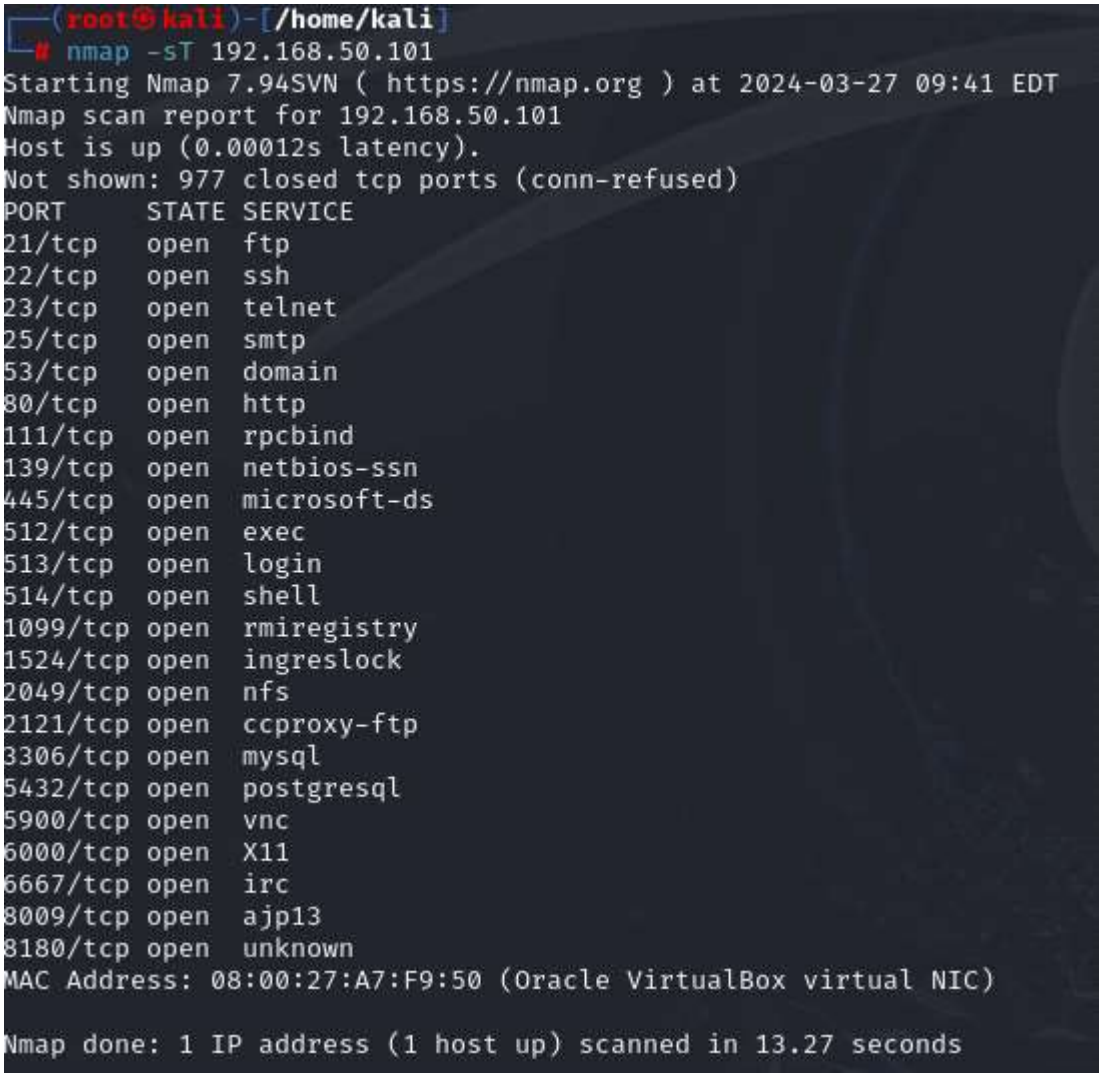
Os fingerprint:


```
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
```

Scan Syn:

```
(root㉿kali)-[/home/kali]
# nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:39 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000043s 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:A7:F9:50 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

Scan TCP:



Gli scan SYN e TCP sono risultati praticamente simili, con lo scan tcp che ha impiegato qualche decimo di secondo in più, in larga scala ovviamente questa differenza si noterà di più

Scan Versioni:

```
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:50 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000050s latency).
Not shown: 977 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
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:A7:F9:50 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: c
pe:/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 65.60 seconds
```

----------Scan Windows----------

OS Fingerprint:

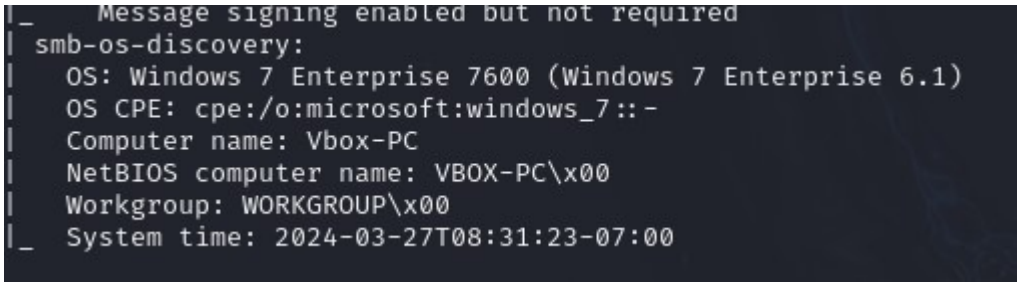
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:57 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00015s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
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:ED:0F:D4 (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_ser
ver_2008::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, Window
s 8, or 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 22.78 seconds
```

Come si può notare dopo lo scan con -O su una macchina windows, la fingerprint dell'os rimane vaga, questo perchè le macchine windows al contrario di quelle linux, danno risposte

più generiche che rende difficile identificare l'os di provenienza

Una possibile soluzione per quanto meno stealth è eseguire il comando

Così da poter ottenere informazioni anche sull'os



----------Report Finali----------

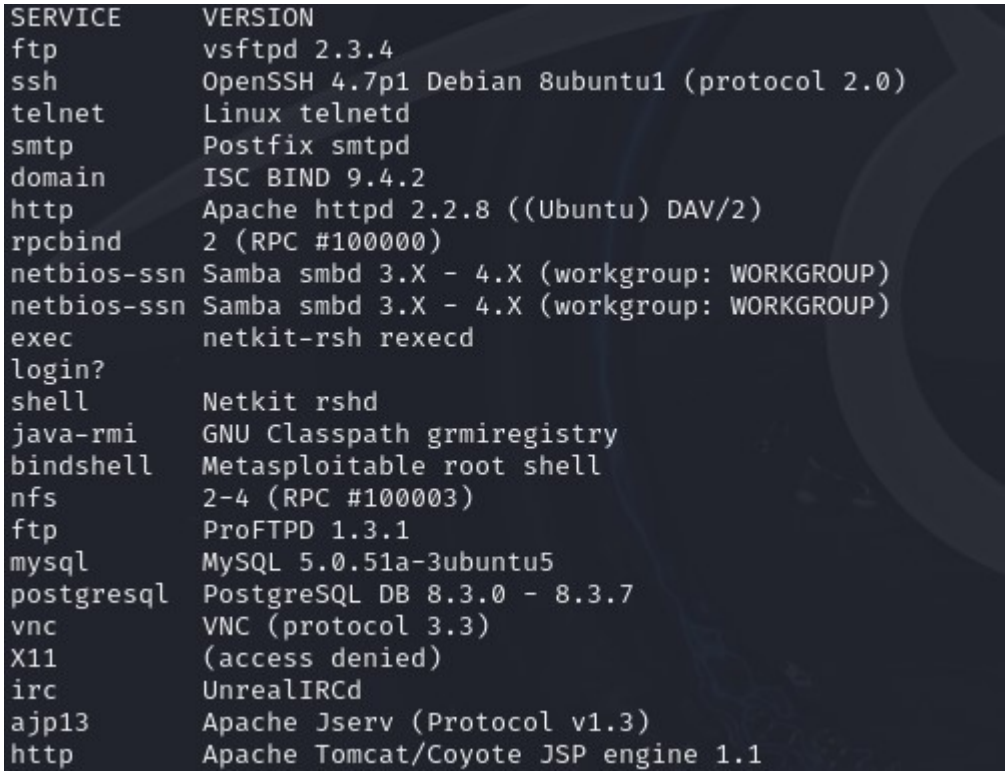
Macchina: Metaspotable

Ip: 192.168.50.101

OS: Linux 2.6.X

Porte Aperte:
21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5900,6000,6667,8009,8180

Servizi in ascolto e versioni:



```
SERVICE     VERSION
ftp         vsftpd 2.3.4
ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
telnet      Linux telnetd
smtp        Postfix smtpd
domain      ISC BIND 9.4.2
http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
rpcbind     2 (RPC #100000)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
exec        netkit-rsh rexecd
login?
shell       Netkit rshd
java-rmi    GNU Classpath grmiregistry
bindshell   Metasploitable root shell
nfs         2-4 (RPC #100003)
ftp         ProFTPD 1.3.1
mysql       MySQL 5.0.51a-3ubuntu5
postgresql  PostgreSQL DB 8.3.0 - 8.3.7
vnc         VNC (protocol 3.3)
X11         (access denied)
irc         UnrealIRCd
ajp13       Apache Jserv (Protocol v1.3)
http        Apache Tomcat/Coyote JSP engine 1.1
```

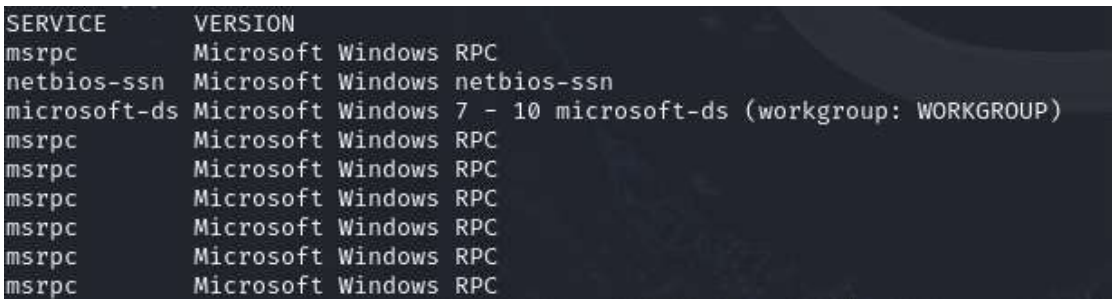
Macchina: Windows

Ip: 192.168.50.102

OS: Windows 7 Enterprise 7600

Porte Aperte:135,139,445,49152,49153,49154,49155,49156,49157

Servizi in ascolto e versioni:



```
SERVICE      VERSION
msrpc        Microsoft Windows RPC
netbios-ssn  Microsoft Windows netbios-ssn
microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
msrpc        Microsoft Windows RPC
msrpc        Microsoft Windows RPC
msrpc        Microsoft Windows RPC
msrpc        Microsoft Windows RPC
msrpc        Microsoft Windows RPC
msrpc        Microsoft Windows RPC
```