Tecniche di scansione con Nmap

Metasploitable

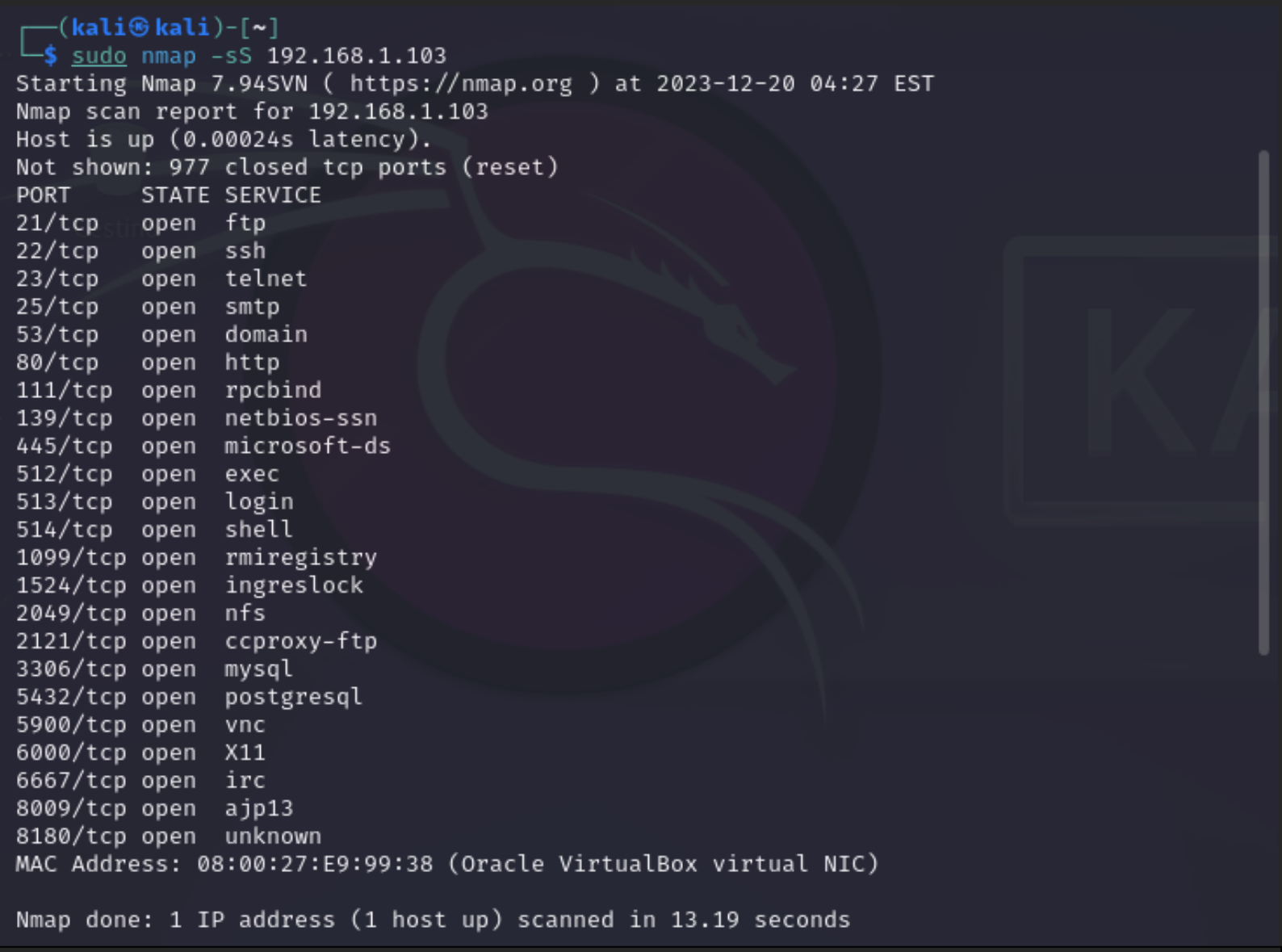
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.103
[sudo] password di kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:26 EST
Nmap scan report for 192.168.1.103
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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:E9:99:38 (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 14.57 seconds
```

OS fingerprint

sudo nmap -O 192.168.1.103

Metasploitable



Syn Scan

sudo nmap -sS 192.168.1.103

Metasploitable

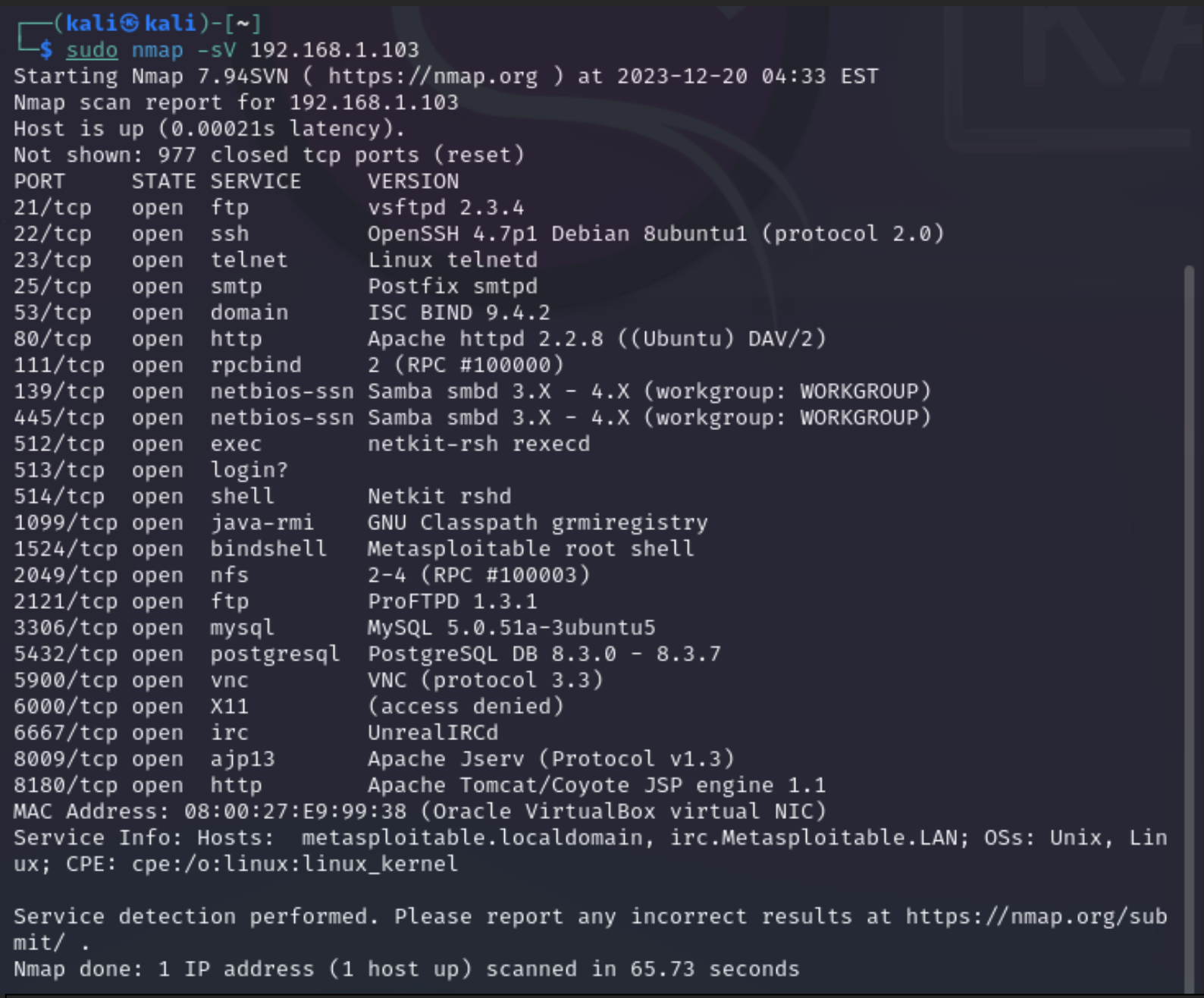
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.1.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:31 EST
Nmap scan report for 192.168.1.103
Host is up (0.00087s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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
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:E9:99:38 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

TCP connect

sudo nmap -sT 192.168.1.103

Metasploitable



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:33 EST
Nmap scan report for 192.168.1.103
Host is up (0.00021s 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:E9:99:38 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Lin
ux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.73 seconds
```

Version Detection

sudo nmap -sV 192.168.1.103

Windows 7

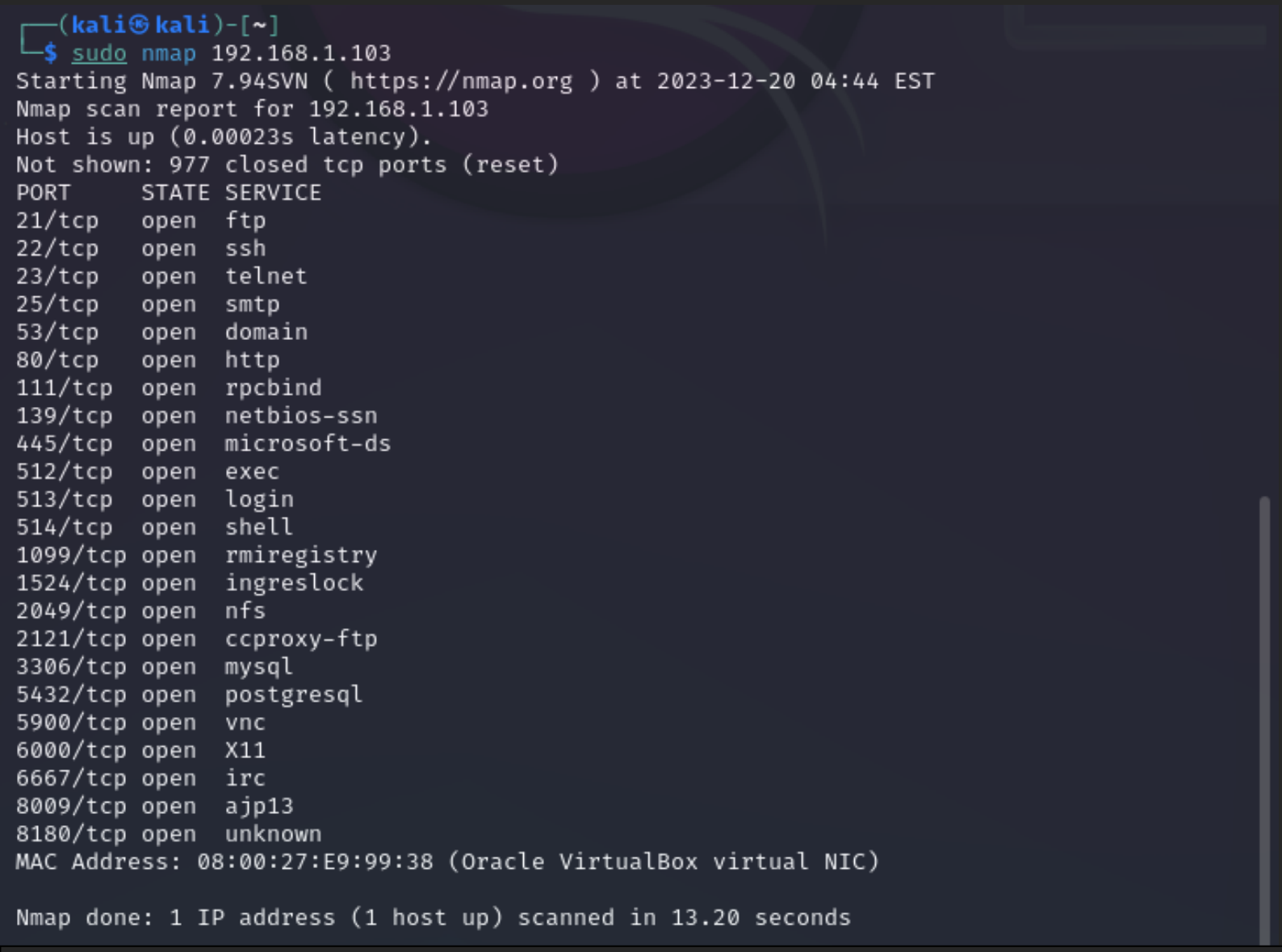
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:41 EST
Nmap scan report for 192.168.1.106
Host is up (0.00051s latency).
All 1000 scanned ports on 192.168.1.106 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:93:D2:E5 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Pa
lmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:window
s_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3
 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Window
s Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.
0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP m
odule, VMware Player virtual NAT device
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 35.07 seconds
```

OS fingerprint

sudo nmap -O 192.168.1.106

Metasploitable



Scansione Nmap Metaspoitable

sudo nmap 192.168.1.103

Windows 7

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.1.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:45 EST
Nmap scan report for 192.168.1.106
Host is up (0.00050s latency).
All 1000 scanned ports on 192.168.1.106 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:93:D2:E5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.28 seconds
```

Scansione Nmap Windows 7

sudo nmap 192.168.1.106

Metasploitable

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sV 192.168.1.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:49 EST
Nmap scan report for 192.168.1.103
Host is up (0.00016s latency).
Not shown: 65505 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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
40687/tcp open  status      1 (RPC #100024)
48753/tcp open  mountd      1-3 (RPC #100005)
54486/tcp open  nlockmgr    1-4 (RPC #100021)
55585/tcp open  java-rmi    GNU Classpath grmiregistry
MAC Address: 08:00:27:E9:99:38 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Lin
ux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 190.40 seconds
```

Scansione Porte Aperte e

Servizi in ascolto con Versione

sudo nmap -p- -sV 192.168.1.103

Windows 7

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 1-100 -sV 192.168.1.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:57 EST
Nmap scan report for 192.168.1.106
Host is up (0.00031s latency).
All 100 scanned ports on 192.168.1.106 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: 08:00:27:93:D2:E5 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.40 seconds
```

Scansione Porte Aperte da 1-100 e

Servizi in ascolto con Versione

sudo nmap -p 1-100 -sV 192.168.1.106

Indirizzi IP

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.108  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe5c:b5d9  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:5c:b5:d9  txqueuelen 1000  (Ethernet)
        RX packets 75035  bytes 4832773 (4.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 170093  bytes 10254221 (9.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 62  bytes 6160 (6.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62  bytes 6160 (6.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

IP Address Kali

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e9:99:38
          inet addr:192.168.1.103  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee9:9938/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:75084 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71991 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5071768 (4.8 MB)  TX bytes:3988574 (3.8 MB)
          Base address:0xd020 Memory:f1200000-f1220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:455 errors:0 dropped:0 overruns:0 frame:0
          TX packets:455 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:165709 (161.8 KB)  TX bytes:165709 (161.8 KB)
```

IP Address Metaspoitable

```
C:\Users\admin>ipconfig

Configurazione IP di Windows


Scheda Ethernet Connessione alla rete locale (LAN):

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::c0c:fb2c:b160:3754%1
1
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.1.106
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.1.1

Scheda Tunnel isatap.{0F539D87-7B8C-4C7A-83D8-9FAEF64C575D}:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:
```

IP Address Windows

Differenza tra le Scansioni Delle Porte e considerazioni

Scansione Metasploitable 192.168.1.103

Risultati:

Un'ampia varietà di porte è aperta, mostrando una diversità di servizi in esecuzione.

Versioni specifiche dei servizi sono state identificate, fornendo dettagli sulla configurazione del sistema.

Sono presenti servizi comuni come FTP, SSH, Telnet, SMTP, HTTP, MySQL, ecc.

Il sistema operativo è identificato come Unix/Linux.

Considerazioni:

Questa scansione offre una panoramica completa delle porte aperte e dei servizi in esecuzione sul sistema target.

Utile per una valutazione dettagliata della configurazione e delle versioni dei servizi.

Scansione Windows 192.168.1.106

Risultati:

Tutte le 100 porte scansionate sono in uno stato "ignored" o "filtered", senza informazioni sullo stato specifico delle porte.

Non vengono fornite informazioni sui servizi e le versioni associati alle porte.

Considerazioni:

La scansione non offre informazioni approfondite sulle configurazioni dei servizi o sullo stato delle porte.

Il risultato potrebbe indicare problemi di accesso o filtraggio delle porte sul sistema target.