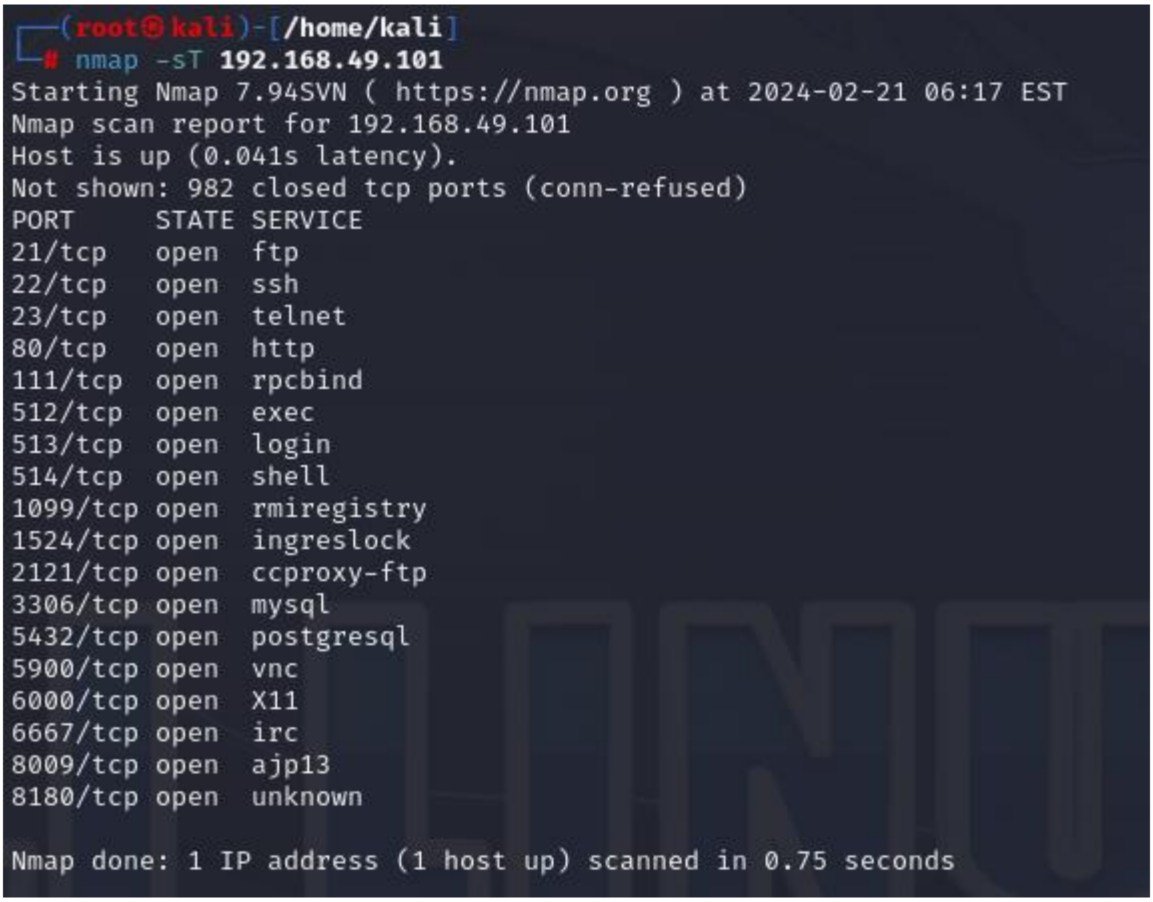
TCP connect: tipo di scansione che viene registrato nel log delle applicazioni che ascoltano sulla rete target. Questo accade perché la scansione TCP connect stabilisce una connessione con il demone del servizio in ascolto, completando il three-way-handshake.

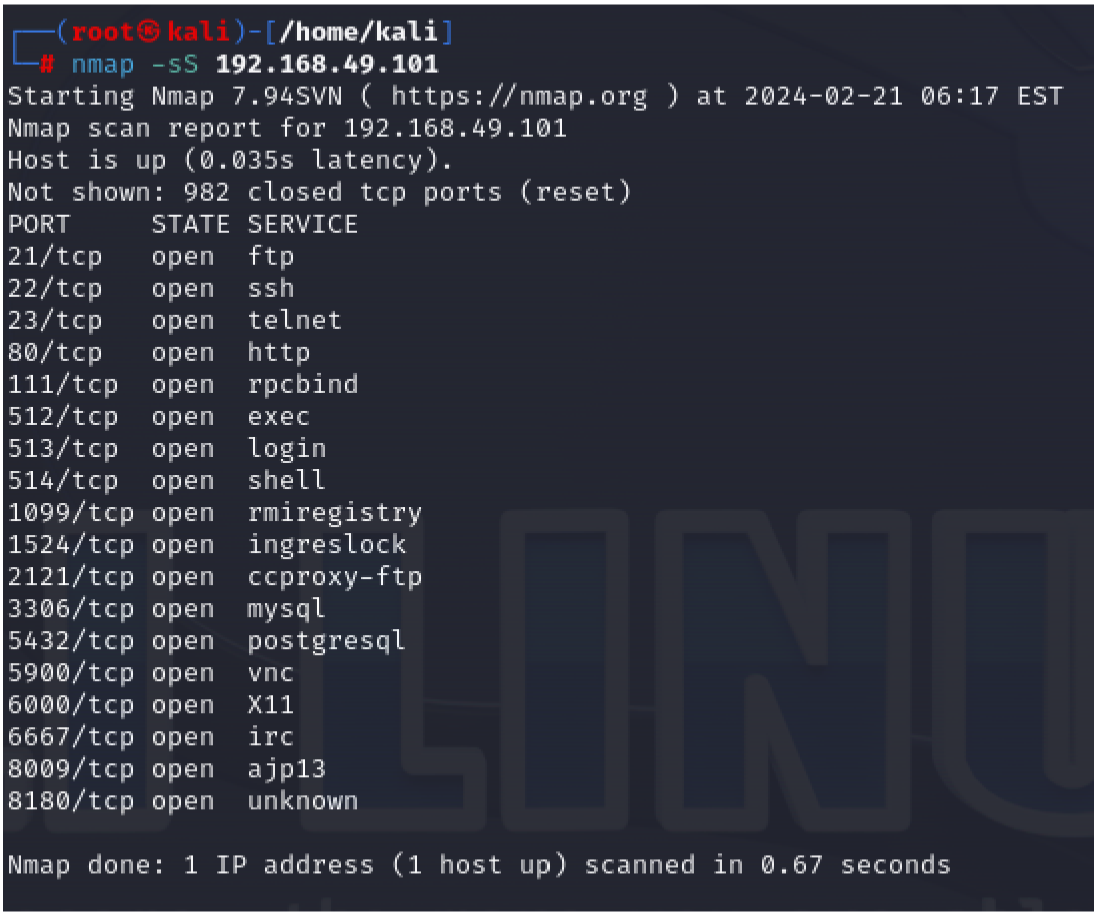
Da Kali a Metasploitable.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 06:17 EST
Nmap scan report for 192.168.49.101
Host is up (0.041s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
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

Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds
```

SYN scan: non viene stabilita una connessione completa con il demone target. Le richieste, tuttavia, possono essere rilevate da un IDS/IPS configurato in maniera appropriata (esempio con un controllo sui pacchetti SYN in entrata).
Da Kali a Metasploitable.

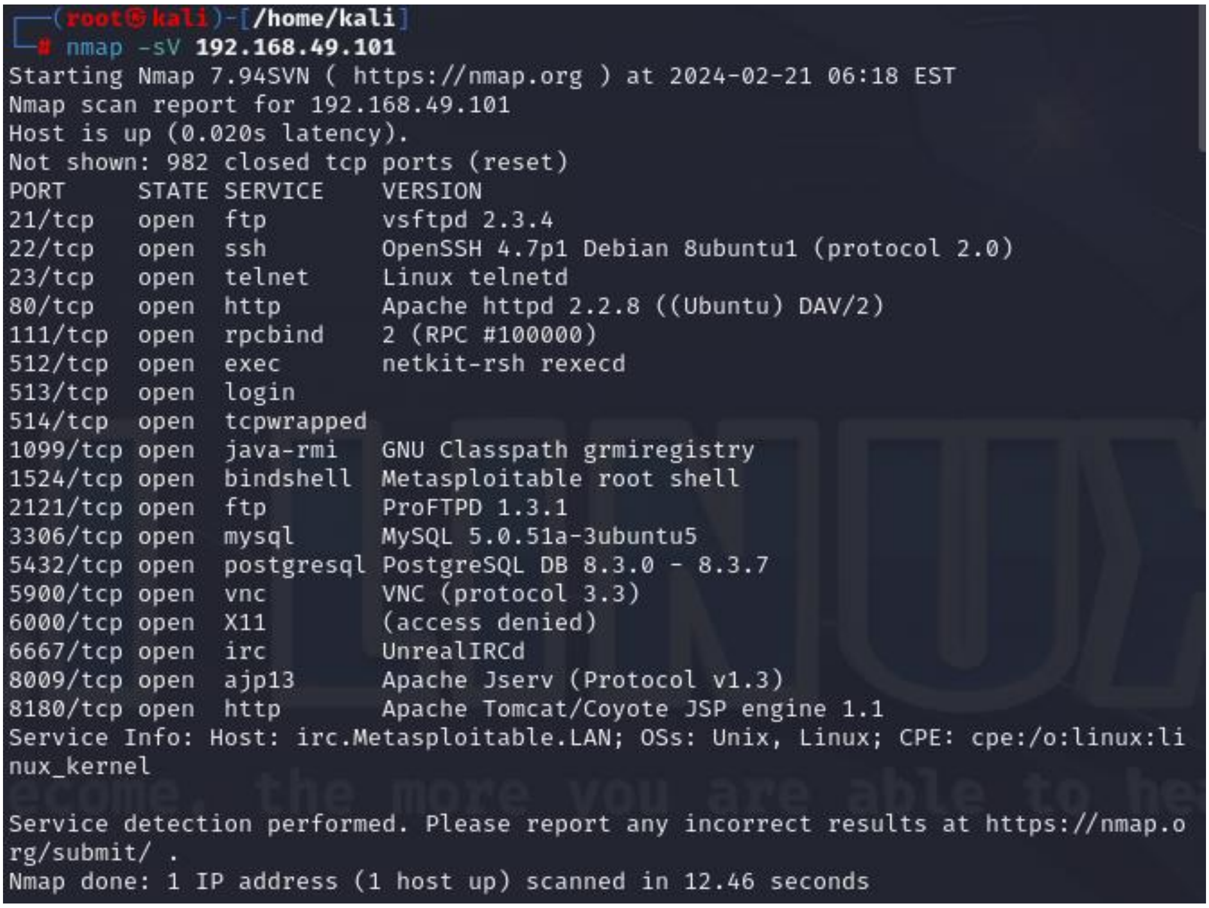


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 06:17 EST
Nmap scan report for 192.168.49.101
Host is up (0.035s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
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

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

Version detection: è a tutti gli effetti una scansione TCP connect con l’aggiunta di specifici test per la rilevazione dei servizi in ascolto su una porta. Così come la scansione TCP connect è piuttosto facile

da rilevare in quanto genera molto traffico di rete.
Da Kali a Metasploitable.

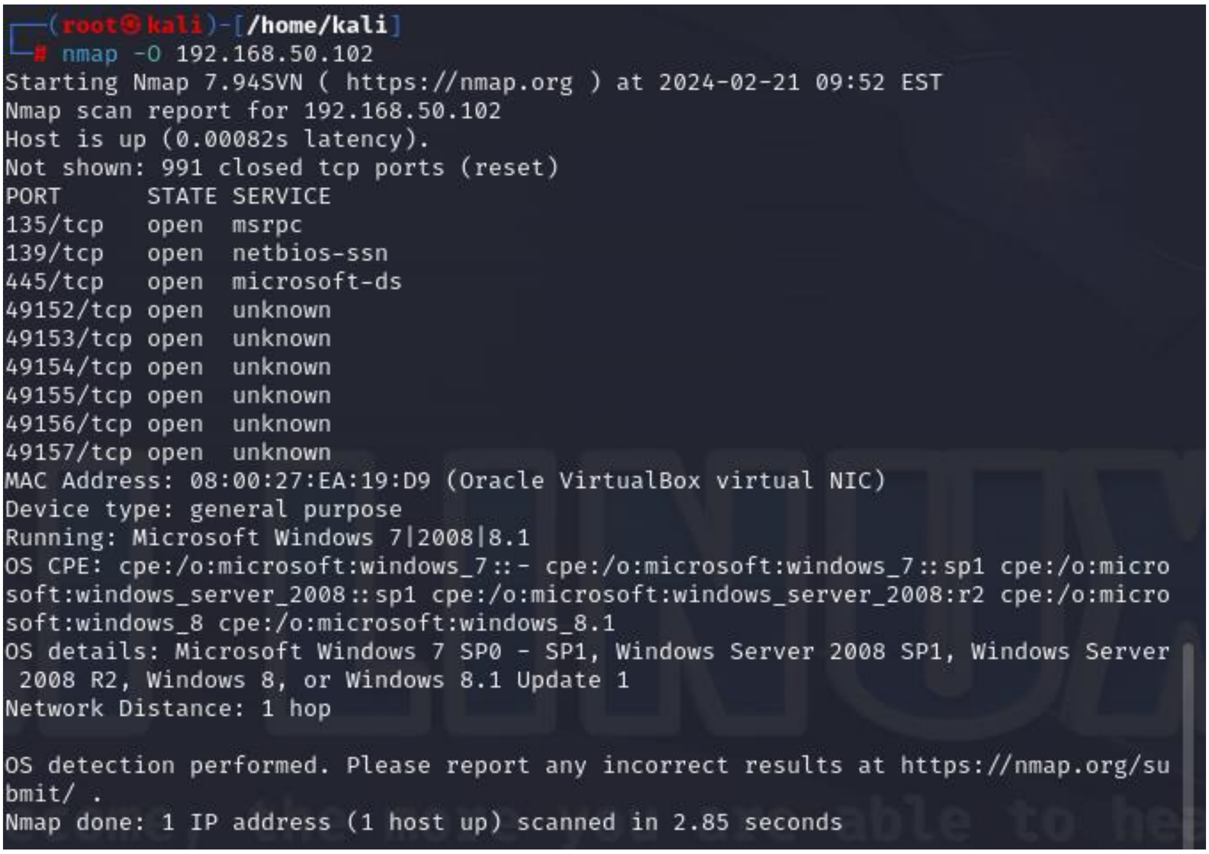


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 06:18 EST
Nmap scan report for 192.168.49.101
Host is up (0.020s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.3.4
22/tcp   open  ssh        OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet     Linux telnetd
80/tcp   open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind    2 (RPC #100000)
512/tcp  open  exec       netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi   GNU Classpath grmiregistry
1524/tcp open  bindshell  Metasploitable root shell
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
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.46 seconds
```

Os fingerprint: Questa funzionalità stima il sistema operativo target ispezionando i pacchetti di risposta ricevuti. questo è dovuto al fatto che i sistemi operativi differiscono in alcune

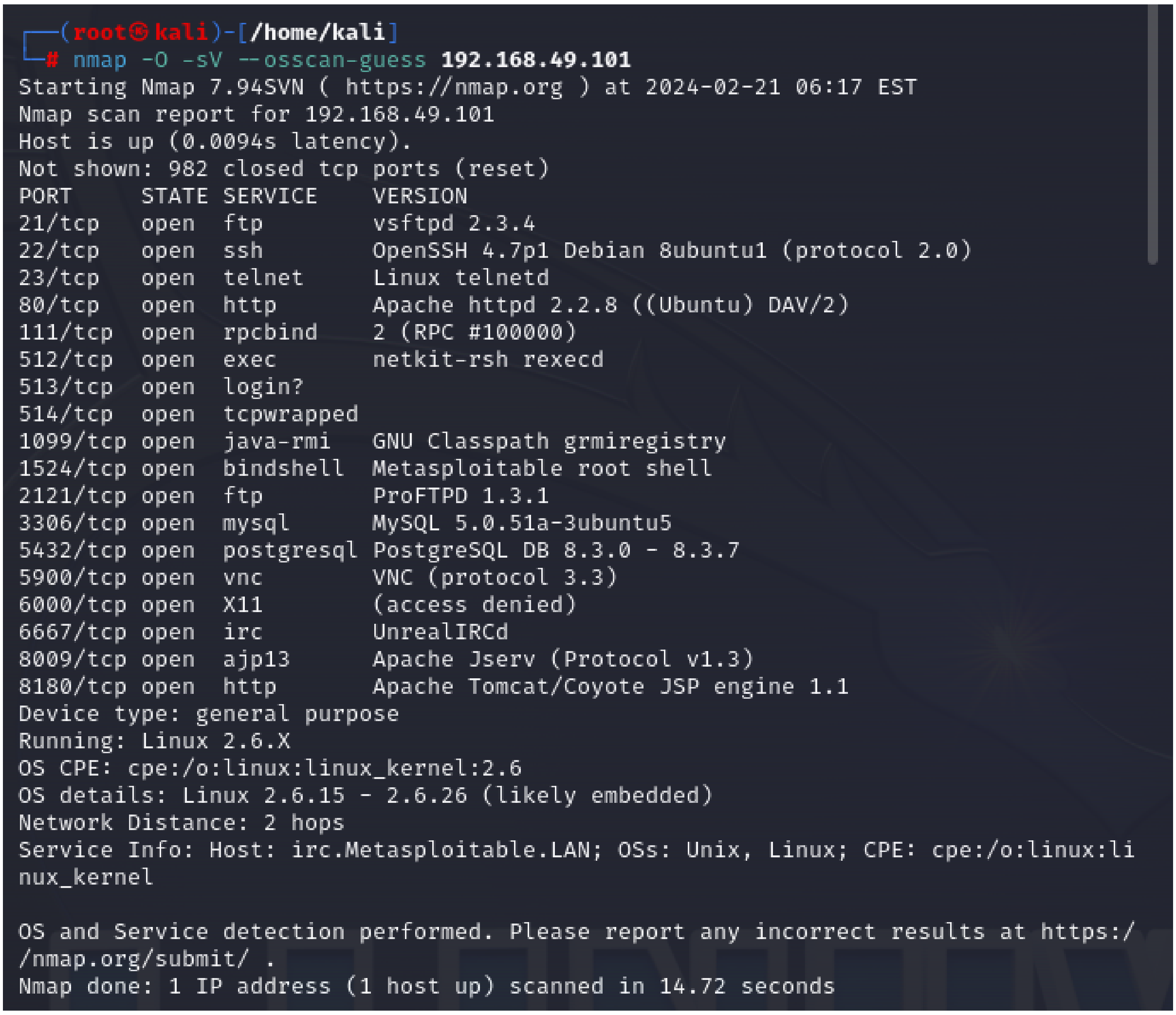
implementazioni dello stack di rete, come ad esempio I valori del TTL e la grandezza della finestra TCP. Nmap recupera queste info dalle risposte degli host e le confronta con le info in suo possesso.
Da Kali a Windows.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:52 EST
Nmap scan report for 192.168.50.102
Host is up (0.00082s 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:EA:19:D9 (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:micro
soft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:micro
soft: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, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.85 seconds
```

In questo caso abbiamo aggiunto un comando per ricevere la lista dei servizi attivi su un dato host con dettaglio sulla versione e una lista dei sistemi operativi in maniera meno precisa con –osscan-geuss.
Da Kali a Metasploitable.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O -sV --osscan-guess 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 06:17 EST
Nmap scan report for 192.168.49.101
Host is up (0.0094s latency).
Not shown: 982 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
80/tcp   open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind    2 (RPC #100000)
512/tcp  open  exec       netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi   GNU Classpath grmiregistry
1524/tcp open  bindshell  Metasploitable root shell
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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

OS and Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.72 seconds
```