

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@kali: /home/kali

File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
[(kali㉿kali)-[~]
└─$ ping -c 4 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.985 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.08 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.91 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.690 ms
...
--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.690/1.166/1.909/0.452 ms

[(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
[(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 08:33 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00044s latency).
MAC Address: 08:00:27:FB:1D:E5 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

[(root㉿kali)-[/home/kali]
└─#
```

netdiscover -r 192.168.50.101

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@kali: /home/kali

Trash File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 60
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.50.101 08:00:27:fb:1d:e5 1 60 PCS Systemtechnik GmbH
```

Crackmapsense

```
(kali㉿kali)-[~]
└─$ crackmapexec 192.168.50.101/24 ssh
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell] [--verbose]
                      {smb,mssql,winrm,ldap,ftp,rdp,ssh} ...
crackmapexec: error: argument protocol: invalid choice: '192.168.50.101/24' (choose from 'smb', 'mssql', 'winrm',
               'ftp', 'rdp', 'ssh')

(kali㉿kali)-[~]
└─$ crackmapexec ssh 192.168.50.101
SSH      192.168.50.101  22      192.168.50.101  [*] SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
└─$
```

Nmap top port - “Migliori” 10 porte aperte

```
(kali㉿kali)-[~]
└─$ nmap 192.168.50.101 -top-ports 10 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 08:55 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0045s latency).
Not shown: 3 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
(kali㉿kali)-[~]
```

Lettura informazioni DNS

```
kali@kali:~$ nmap -p- -sV -reason -dns-server ns
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 08:58 EDT
Nmap scan report for 192.168.50.101
Host is up, received syn-ack (0.0020s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON VERSION
21/tcp    open  ftp          syn-ack vsftpd 2.3.4
22/tcp    open  ssh          syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack Linux telnetd
25/tcp    open  smtp         syn-ack Postfix smtpd
53/tcp    open  domain       syn-ack ISC BIND 9.4.2
80/tcp    open  http         syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         syn-ack netkit-rsh rexecd
513/tcp   open  login?      syn-ack
514/tcp   open  shell        syn-ack Netkit rshd
1099/tcp  open  java-rmi   syn-ack GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack Metasploitable root shell
2049/tcp  open  nfs          syn-ack 2-4 (RPC #100003)
2121/tcp  open  ftp          syn-ack ProFTPD 1.3.1
3306/tcp  open  mysql        syn-ack MySQL 5.0.51a-3ubuntu5
```

Unicornscan

```
# us -mT -Iv 192.168.50.101:a -r 3000 -R 3 && us -mU -Iv 192.168.50.101:a -r 3000 -R 3
adding 192.168.50.101/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.50.101:56736 ttl 64
TCP open 192.168.50.101:1099 ttl 64
TCP open 192.168.50.101:80 ttl 64
TCP open 192.168.50.101:1524 ttl 64
TCP open 192.168.50.101:6000 ttl 64
TCP open 192.168.50.101:8009 ttl 64
TCP open 192.168.50.101:3632 ttl 64
TCP open 192.168.50.101:513 ttl 64
TCP open 192.168.50.101:22 ttl 64
TCP open 192.168.50.101:6697 ttl 64
TCP open 192.168.50.101:6667 ttl 64
TCP open 192.168.50.101:25 ttl 64
TCP open 192.168.50.101:5900 ttl 64
TCP open 192.168.50.101:48720 ttl 64
```

NMAP formato ridotto, con versione servizi

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
(root@kali)-[~/home/kali]
# nmap -SS -sV -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 17:52 EDT
Stats: 0:01:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 17:54 (0:00:04 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00026s 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?      Netkit rshd
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)
```

```
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp open  unknown
MAC Address: 08:00:27:FB:1D:E5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 172.99 seconds
```

Hping3

```
(root@kali)-[~/home/kali]
# hping3 --scan known 192.168.50.101
hping3: option requires an argument -- s
Try hping3 --help

(root@kali)-[~/home/kali]
# hping3 --scan known 192.168.50.101
Scanning 192.168.50.101 (192.168.50.101), port known
264 ports to scan, use -V to see all the replies
+---+-----+-----+-----+-----+-----+
|port| serv name | flags | ttl| id | win | len |
+---+-----+-----+-----+-----+-----+
All replies received. Done.
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http) (111 sunrpc) (139 netbios-ssn) (445 microsoft-d) (5
12 exec) (513 login) (514 shell) (1099 rmiregistry) (1524 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgres
ql) (6000 x11) (6667 ircd) (6697 ircs-u)
```

Netcat con scansione dettagliata e stato porte

The screenshot shows a terminal window titled "kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox". The terminal is running as root (@kali: /home/kali). It displays the help documentation for the nc command, which includes options like -s, -T, -t, -u, -V, -w, -C, and -z. Below the help text, it says: "port numbers can be individual or ranges: lo-hi [inclusive]; hyphens in port names must be backslash escaped (e.g. 'ftp\-\data')." Then, the user runs the command "# nc -nvz 192.168.50.101 1-1024" and receives a detailed list of open ports on the target host:

```
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open
(UNKNOWN) [192.168.50.101] 80 (http) open
(UNKNOWN) [192.168.50.101] 53 (domain) open
(UNKNOWN) [192.168.50.101] 25 (smtp) open
(UNKNOWN) [192.168.50.101] 23 (telnet) open
(UNKNOWN) [192.168.50.101] 22 (ssh) open
(UNKNOWN) [192.168.50.101] 21 (ftp) open
```

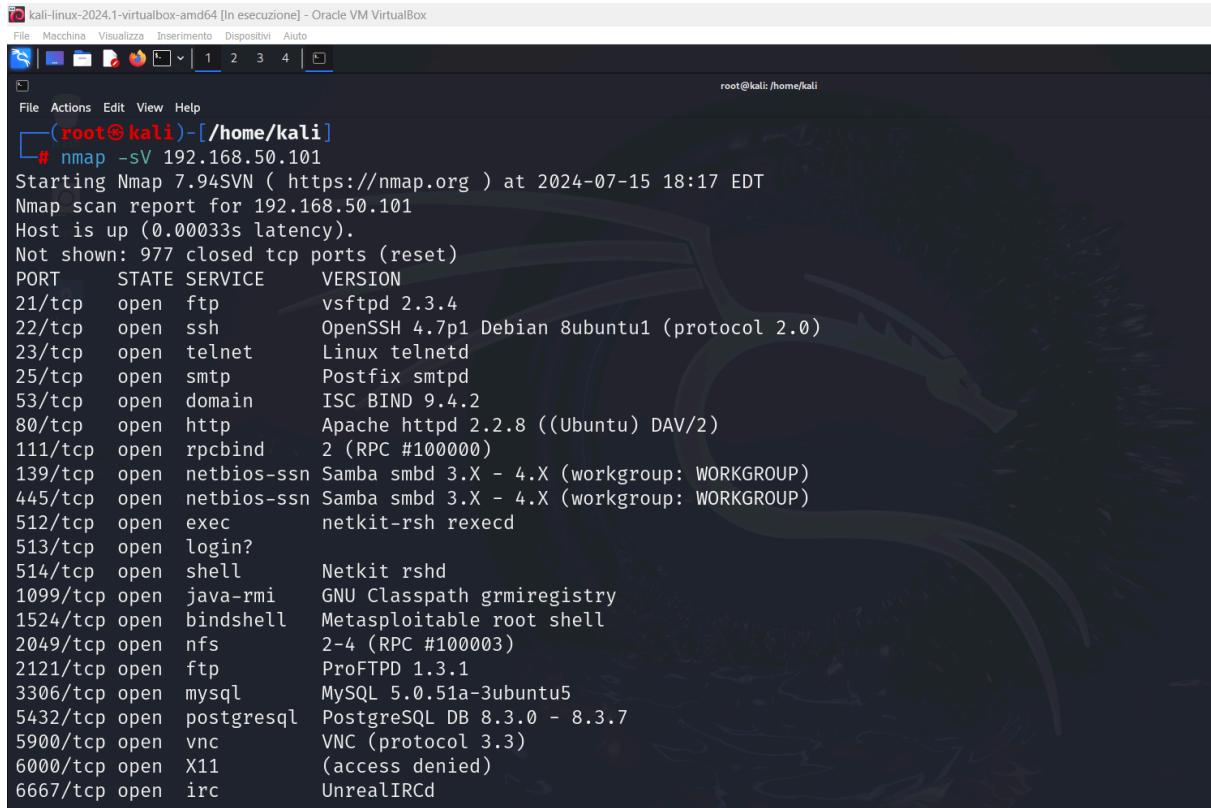
The terminal ends with a "# " prompt.

NETCAT in ascolto

The screenshot shows a terminal window titled "root@kali: /home/kali". The user runs the command "# nc -nv 192.168.50.101 22" and receives the following output:

```
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C
```

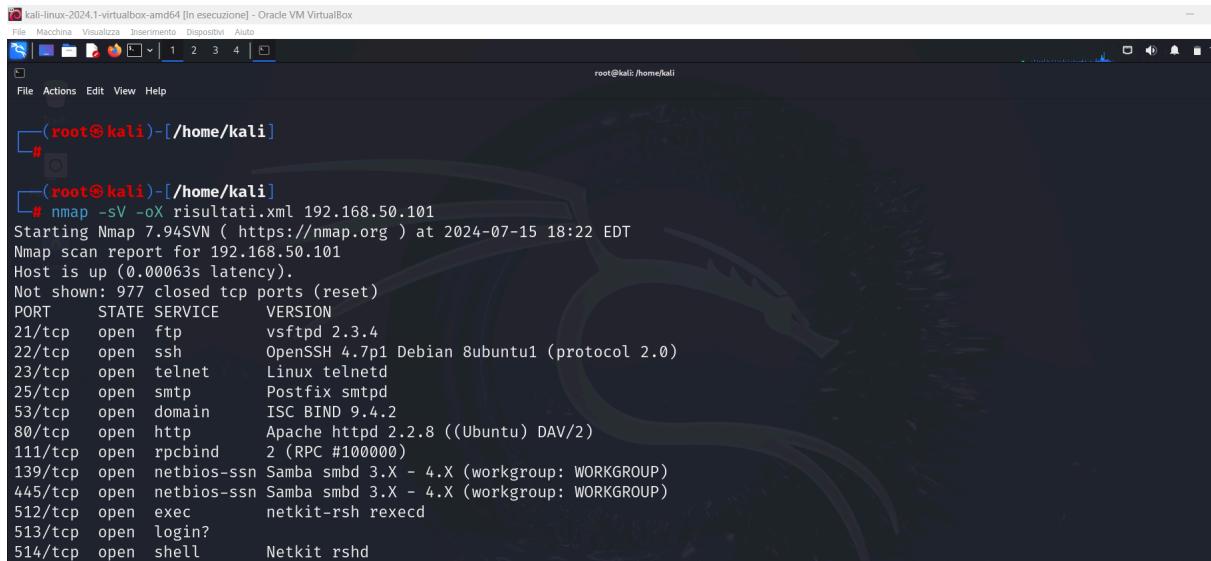
NMAP con versione servizi



```
(root㉿kali)-[~/home/kali]
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 18:17 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00033s 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?      Netkit rshd
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
```

Salvataggio su file XML



```
(root㉿kali)-[~/home/kali]
#
[root@kali ~]# nmap -sV -oX risultati.xml 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 18:22 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00063s 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?      Netkit rshd
514/tcp   open  shell        Netkit rshd
```

_faccio partire Msfconsole

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.22 seconds

[—(root@kali)-[/home/kali]
# msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

Home :oDFo:
./ym0dayMmy/
-dHJ5aGFyZGVyIQ=+-+smo~Destroy.No.Data~s`-+h2~Maintain.No.Persistence~h+-+odNo2~Above.All.Else.Do.No.Harm~Ndo`-+/SecKCoin++e.AMd`-+ssh/id_rsa.Des-:dopeAW.No<nano>o:we're.all.alike':PLACEDRINKHERE!:msfsexploit -j.:—srwxrwx:-:<script>.Ac816/:NT_AUTHORITY.Do:09.14.2011.raid:hevnsntSurb025N.:#OUTHOUSE- -s:$nmap -os:Awsm.da:
./etc/shadow.0days-Data'%200R%201=1--.No.0MN8'/.-:///+hbove.913.ElsMNh+-htN01UserWroteMe!-:is:T8iKC.sudo-.A:The.PFYroy.No.D7:yxp_cmdshell.Ab0: :Ns.B088ALICFes7:`MS146.52.No.Per:sENbove3101.404: `T:/shSYSTEM-.N:/STFU|wall.No.Pr:dNVRCOING2GIVUUP:/corykennedyData:Sso.6178306Ence:/shMTL#beats3o.No.:
```

_non sono connesso al database

```
= [ metasploit v6.3.55-dev ]+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]+ -- --=[ 1388 payloads - 46 encoders - 11 nops ]+ -- --=[ 9 evasion ]Metasploit Documentation: https://docs.metasploit.com/msf6 > db_status [*] postgresql selected, no connection msf6 > db_import risultati.xml [-] Database not connected msf6 > db_import ./risultati.xml [-] Database not connected msf6 > db_status [*] postgresql selected, no connection msf6 > db_connect [-] A URL or saved data service name is required.
```

Bypassare i filtri del FIREWALL rimpicciolendo i pacchetti

```
(root㉿kali)-[~/home/kali]
# nmap -f -mtu=512 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 18:33 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00035s 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
```

Report 192.168.50.101

- **Indirizzo IP:** 192.168.50.101
- **MAC Address:** 08:00:27:FB:1D
(Oracle VirtualBox virtual NIC)
- **Sistema Operativo:** Unix, Linux
- **Nome Host:** metasploitable.localdomain, irc.Metasploitable.LAN

PORTE INTERESSANTI

Porta	Stato	Servizio	Versione
21/tcp	Open	ftp	vsftpd 2.3.4
22/tcp	Open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
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

Le porte più comuni si espongono tutte ad exploit noti per l'obsolescenza delle versioni dei servizi in uso.