Esercizio S5L3

Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable**:

- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E le seguenti sul target Windows 7:

- OS fingerprint .

A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un report contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione

Quesito extra (al completamento dei quesiti sopra):

Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

L'esercizio richiedeva di effettuare delle scansioni su Windows 7 e Metasplotable con l'applicazione Nmap di Kali Linux per ricavare alcuni parametri scritti nella consegna ma prima di iniziare con la scansione abbiamo messo tutte e tre le macchine nella stessa rete.

Metasploitable

```
address 192.168.50.101
network 192.168.50.0
netmask 255.255.255.0
broadcast 192.168.50.255
gateway 192.168.50.1
```

Kali Linux

```
address 192.168.40.100
netmask 255.255.255.0
network 192.168.40.0
broadcast 192.168.50.255
gateway 192.168.40.2
```

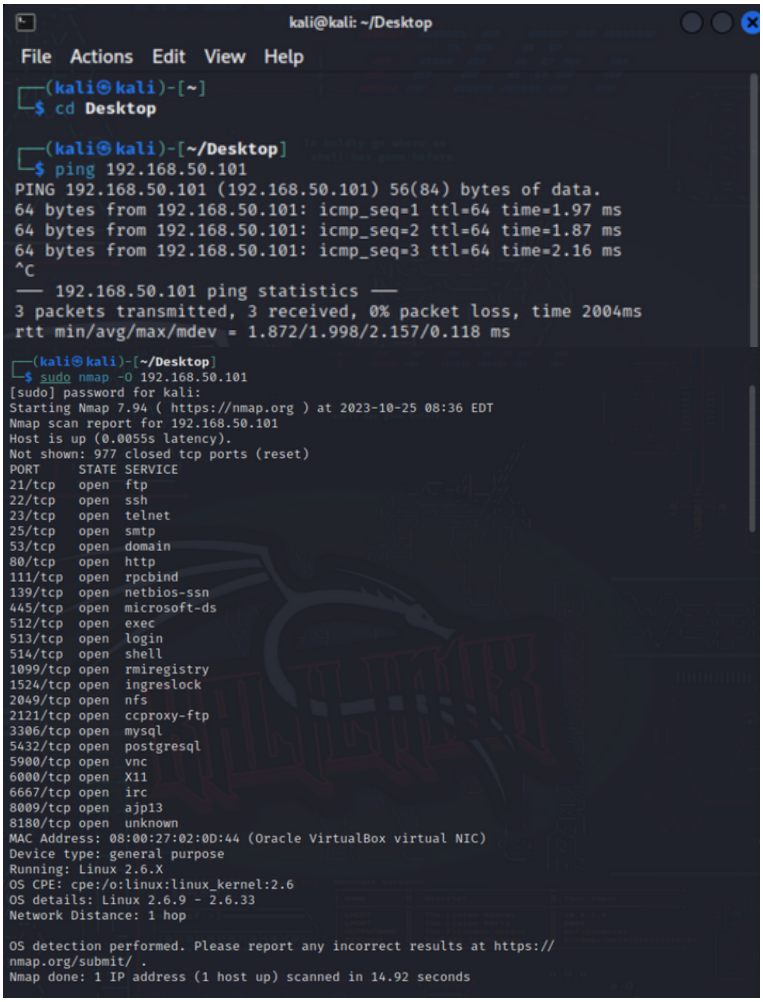
Windows 7

IPv4 Address	192.168.50.102
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.50.1

Da qui si inizia a scansionare Metasploitable:
1) Si ricava il sistema operativo con il comando mostrata nell'immagine affianco.

il comando viene chiamato fingerprint che serve esattamente per ricavare il sistema operativo attraverso l'indirizzo IP

sistema operativo --->



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:39 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00095s 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: 08:00:27:02:0D:44 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
```

2) Si ricavano le porte e servizi aperte con il comando sudo nmap -sS indirizzo IP della macchina bersaglio

Il comando serve per ottenere tutte le porte aperte in modo meno rumoroso così di non essere facilmente rintracciabile ma è meno preciso

3) Si ricavano le porte e i servizi aperte con il comando nmap -sT indirizzo IP della macchina bersaglio

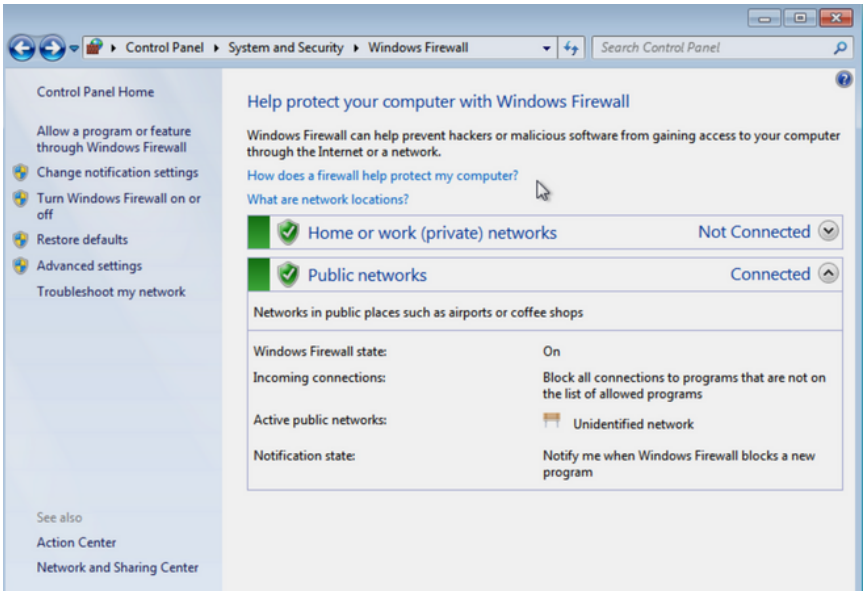
il comando serve per ricavare tutte le porte aperte in modo più aggressivo quindi più rumoroso e facilmente rintracciabile ma è più preciso,affidabile e lento rispetto al comando con -sS perchè usa la tecnica della stretta di mano a tre vie(syn,syn/ack,ack).

La differenza tra -sS e -sT sono:1) la latenza dato che la -sS invia i pacchetti usando soltanto la syn della tecnica della stretta di mano a tre vie invece - sT usa tutte e tre (syn,syn/ack,ack); 2) la mancanza dell'indirizzo MAC su -sT

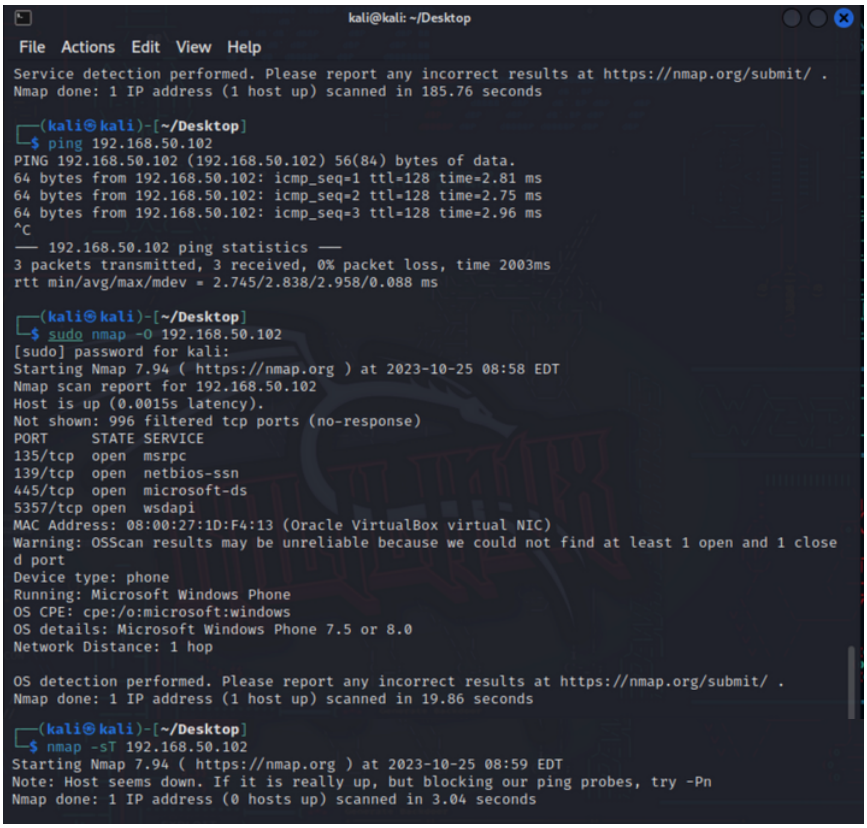
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:41 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0069s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

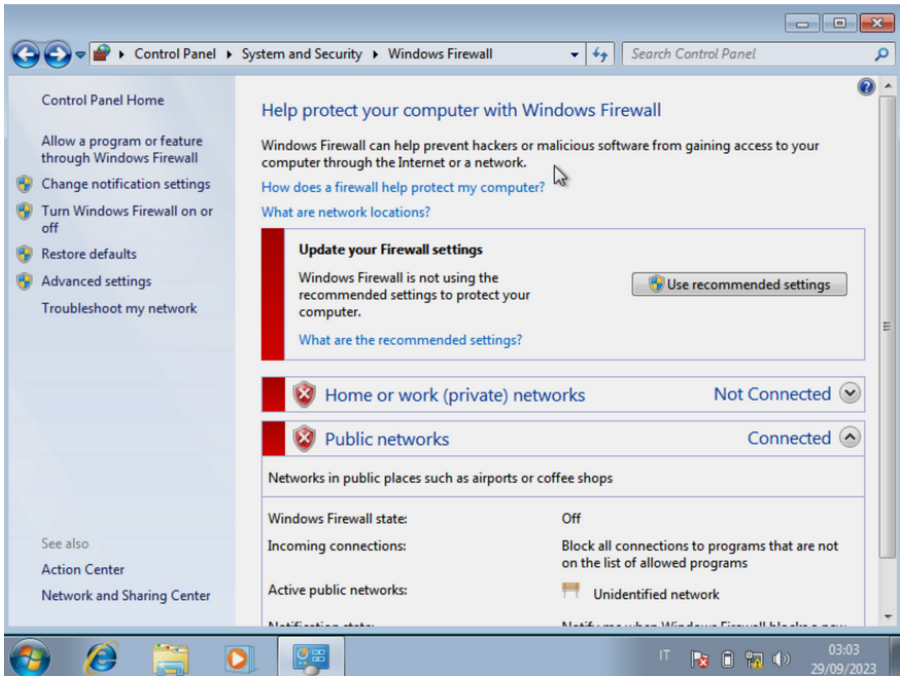
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:46 EDT
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 95.65% done; ETC: 08:48 (0:00:04 remaining)
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 95.65% done; ETC: 08:48 (0:00:04 remaining)
Stats: 0:02:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 95.65% done; ETC: 08:48 (0:00:05 remaining)
Stats: 0:02:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 95.65% done; ETC: 08:49 (0:00:06 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0083s latency).
Not shown: 977 closed tcp ports (conn-refused)
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  unknown
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 185.76 seconds
```

4) Si ricava le porte e i servizi aperte,e le versioni dei servizi con il comando nmap -sV indirizzo IP bersaglio



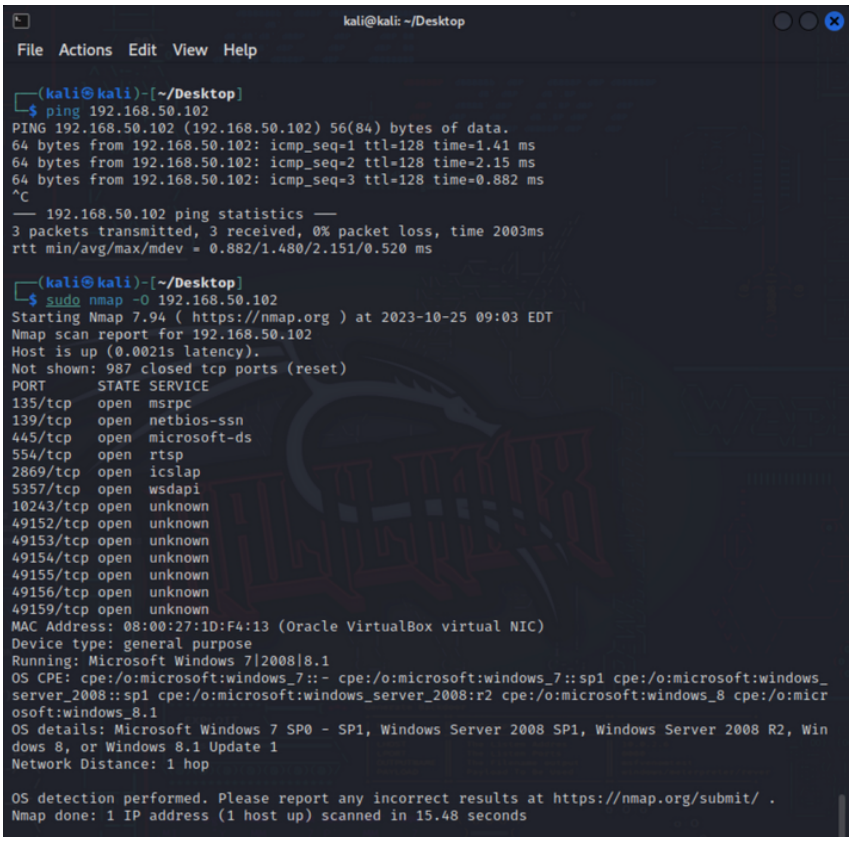
5) Come mostrato nelle immagini affianco il firewall di Windows 7 non permette di scansionare totalmente le porte e i servizi.Allora per poter continuare con la scansione si va ad disattivare il firewall.

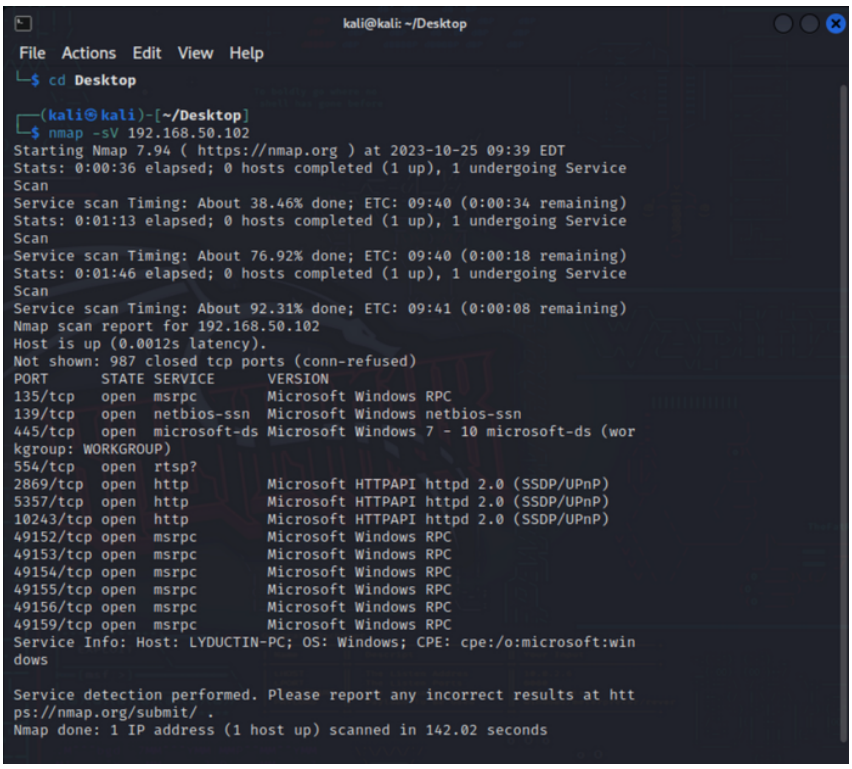


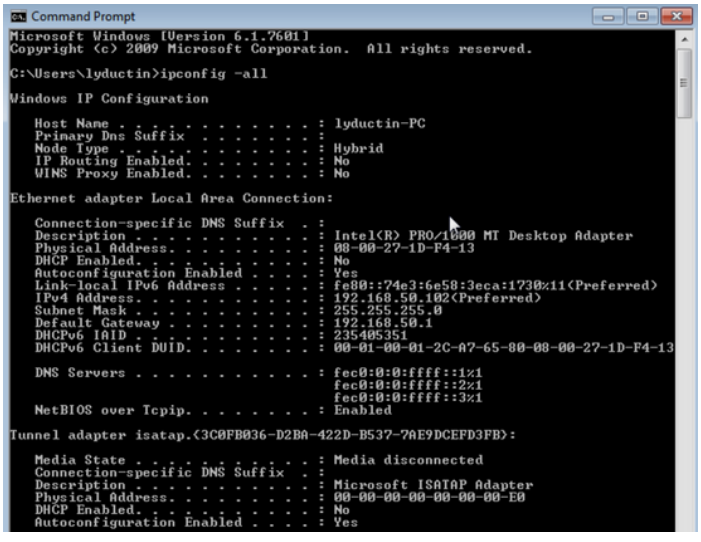


per disattivare si va nel “Turn Windows Firewall on or off” nella barra a sinistra.

6) Poi si ripete le procedure precedenti di Metasploitable anche per Windows 7 per avere le informazioni che ci servirano per il report finale







Report Finale

	Metasploitable	Windows 7
IP	192.168.50.101	192.168.50.102
Sistema Operativo	Linux 2.6.X	Microsoft Windows 7|2008|8.1

Windows 7

Porte Aperte	Servizi in ascolto	versione
135/tcp	msrpc	Microsoft Windows RPC
139/tcp	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp	rtsp?	
2869/tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp	msrpc	Microsoft Windows RPC
49153/tcp	msrpc	Microsoft Windows RPC
49154/tcp	msrpc	Microsoft Windows RPC
49155/tcp	msrpc	Microsoft Windows RPC
49156/tcp	msrpc	Microsoft Windows RPC
49159/tcp	msrpc	Microsoft Windows RPC

Metasploitable

Porte Aperte	Servizi in ascolto	versione
21/tcp	ftp	sftpd 2.3.4
22/tcp	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	telnet	Linux telnetd
25/tcp	smtp	Postfix smtpd
53/tcp	domain	ISC BIND 9.4.2
80/tcp	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	rpcbind	2 (RPC #100000)
139/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	exec	netkit-rsh rexecd
513/tcp	login?	
514/tcp	shell	Netkit rshd
1099/tcp	java-rmi	GNU Classpath grmiregistry
1524/tcp	bindshell	Metasploitable root shell
2049/tcp	nfs	2-4 (RPC #100003)
2121/tcp	ftp	ProFTPD 1.3.1

Metasploitable

3306/tcp	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	vnc	VNC (protocol 3.3)
6000/tcp	X11	(access denied)
6667/tcp	irc	UnrealIRCd
8009/tcp	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	unknown	