

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 scansione 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 Metasploitable 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

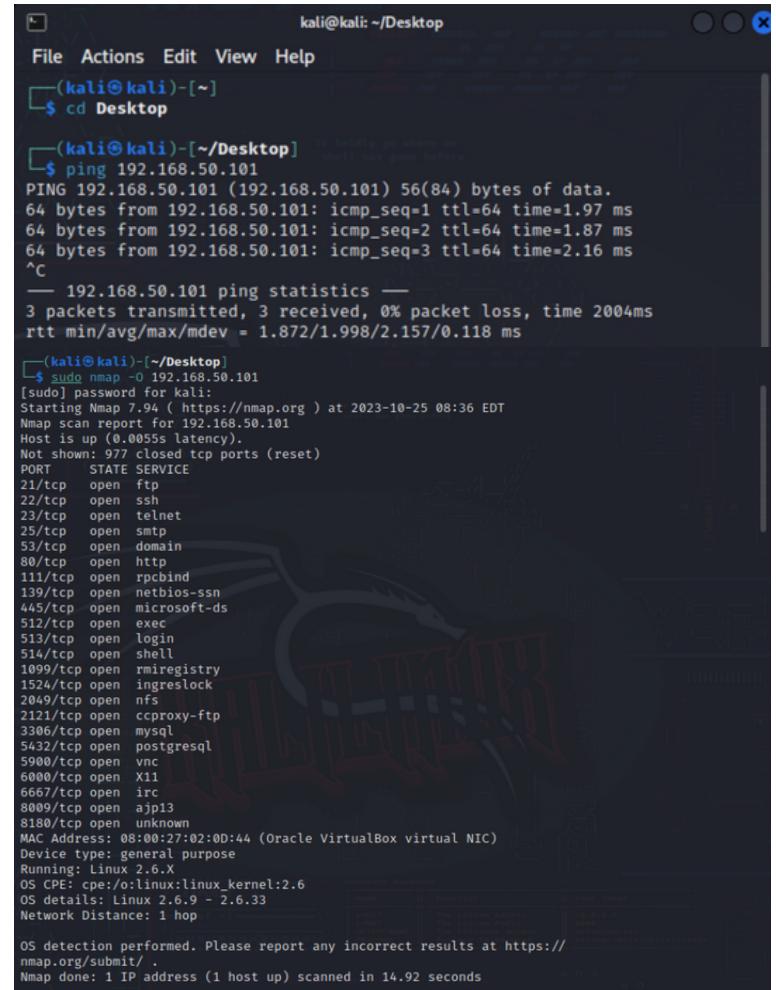
```
address 192.168.40.100
netmask 255.255.255.0
network 192.168.40.0
broadcast 192.168.50.255
gateway 192.168.40.2
```

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.



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
```

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 perché 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

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

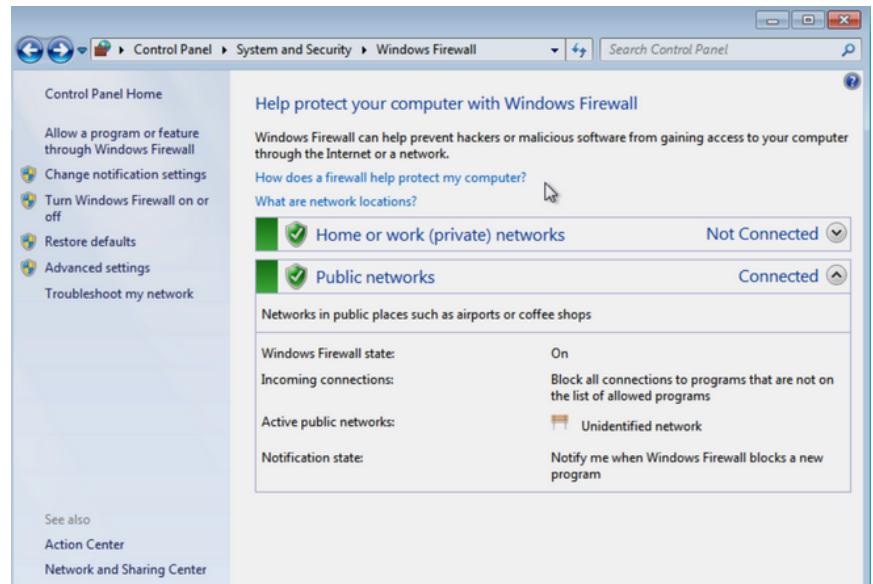
```
(kali㉿kali)-[~/Desktop]
$ nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:41 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0069s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp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

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

```
(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        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
```



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.

```

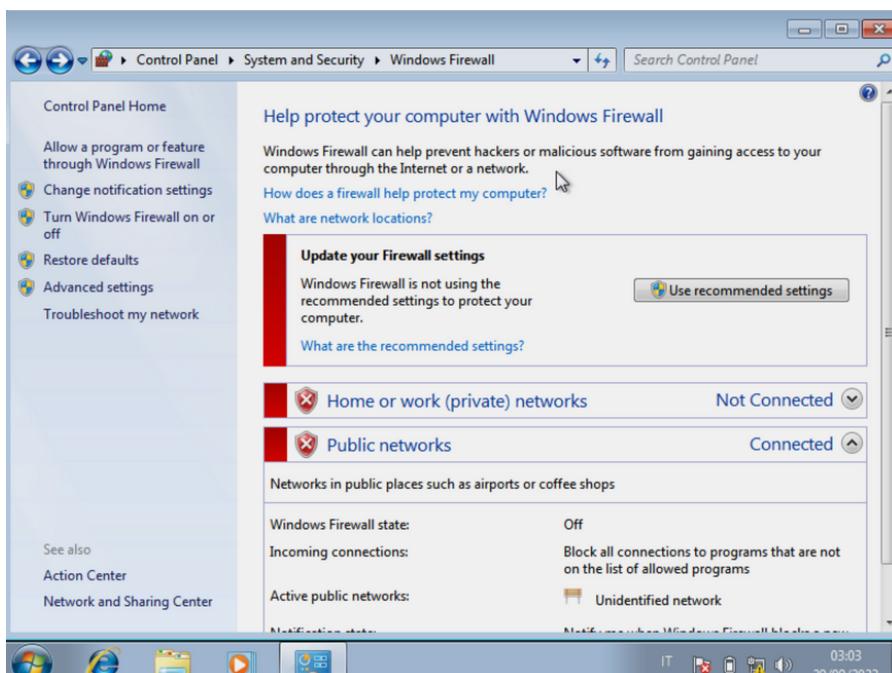
File Actions Edit View Help
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.76 seconds
└─(kali㉿kali)-[~/Desktop]
└─$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=2.81 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=2.75 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=2.96 ms
^C
--- 192.168.50.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.745/2.838/2.958/0.088 ms

└─(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:58 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 08:00:27:1D:F4:13 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 close
d port
Device type: phone
Running: Microsoft Windows Phone
OS CPE: cpe:/o:microsoft:windows
OS details: Microsoft Windows Phone 7.5 or 8.0
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 19.86 seconds

└─(kali㉿kali)-[~/Desktop]
└─$ nmap -sT 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:59 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds

```



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 serviranno per il report finale

```
kali㉿kali:[~/Desktop]
File Actions Edit View Help
└─$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=1.41 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=2.15 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.882 ms
^C
--- 192.168.50.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.882/1.480/2.151/0.520 ms

└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 09:03 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  icslap
5357/tcp   open  wsddapi
10243/tcp  open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49159/tcp  open  unknown
MAC Address: 08:00:27:10:F4:13 (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_server_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, Windows 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 15.48 seconds
```

```
kali㉿kali:[~/Desktop]
File Actions Edit View Help
└─$ cd Desktop
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 09:39 EDT
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 38.46% done; ETC: 09:40 (0:00:34 remaining)
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 76.92% done; ETC: 09:40 (0:00:18 remaining)
Stats: 0:01:46 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 92.31% done; ETC: 09:41 (0:00:08 remaining)
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc      Microsoft Windows RPC
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup)
554/tcp    open  rtsp?
2869/tcp   open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp  open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc      Microsoft Windows RPC
49153/tcp  open  msrpc      Microsoft Windows RPC
49154/tcp  open  msrpc      Microsoft Windows RPC
49155/tcp  open  msrpc      Microsoft Windows RPC
49156/tcp  open  msrpc      Microsoft Windows RPC
49159/tcp  open  msrpc      Microsoft Windows RPC
Service Info: Host: LYDUCTIN-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.02 seconds
```

```
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\lyductin>ipconfig /all
Windows IP Configuration

Host Name . . . . . : lyductin-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address . . . . . : 08-00-27-1D-F4-13
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::74e3:6e58:3eca:1730%11<Preferred>
IPv4 Address . . . . . : 192.168.50.102<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.50.1
DHCPv6 IID. . . . . : 235495351
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-A7-65-80-08-00-27-1D-F4-13
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{3C0FB036-D2BA-422D-B537-7AE9DCEPD3FB}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : Microsoft ISATAP Adapter
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
```

Report Finale

	Metasploitable	Windows 7	Porte Aperte	Servizi in ascolto	versione
IP	192.168.50.101	192.168.50.102	21/tcp	ftp	sftpd 2.3.4
Sistema Operativo	Linux 2.6.X	Microsoft Windows 7 2008 8.1	22/tcp	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
			23/tcp	telnet	Linux telnetd
			25/tcp	smtp	Postfix smtpd
Windows 7	135/tcp	msrpc	53/tcp	domain	ISC BIND 9.4.2
	139/tcp	netbios-ssn	80/tcp	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
	445/tcp	microsoft-ds	111/tcp	rpcbind	2 (RPC #100000)
	554/tcp	rtsp?	139/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
	2869/tcp	http	445/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
	5357/tcp	http	512/tcp	exec	netkit-rsh rexecd
	10243/tcp	http	513/tcp	login?	
	49152/tcp	msrpc	514/tcp	shell	Netkit rshd
	49153/tcp	msrpc	1099/tcp	java-rmi	GNU Classpath grmiregistry
	49154/tcp	msrpc	1524/tcp	bindshell	Metasploitable root shell
	49155/tcp	msrpc	2049/tcp	nfs	2-4 (RPC #100003)
	49156/tcp	msrpc	2121/tcp	ftp	ProFTPD 1.3.1
	49159/tcp	msrpc	3306/tcp	mysql	MySQL 5.0.51a-3ubuntu5
			5432/tcp	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
Metasploitable			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	