


ESERCITAZIONE WEEK 11 DAY 2

 **EPICODE**


W11D1 - Pratica (1) PDF

Esercizio
Scansione dei servizi

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

 **EPICODE**

Esercizio
Scansione dei servizi

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. 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
- ☐ Descrizione dei servizi

<https://www.poftut.com/nmap-output/>

nmap -oN report1 IP

1 Caso di macchine su reti diverse (con PfSense)

IP Kali Linux: 192.168.50.102;

IP Metasploitable: 192.168.51.100;

```
Enter an option: 7

Enter a host name or IP address: 192.168.51.100
^CVirtualBox Virtual Machine - Netgate Device ID: bcac747642af444f7d0e
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.51.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

1 A OS fingerprinting

```
└─$ sudo nmap -O 192.168.51.100
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 10:27 EST
Nmap scan report for 192.168.51.100
Host is up (0.00098s 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
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
```

1 B SYN Scan

```
└─$ sudo nmap -sS 192.168.51.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 10:36 EST
Nmap scan report for 192.168.51.100
Host is up (0.00068s 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

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

1_C TCP CONNECT

```
└─$ sudo nmap -sT 192.168.51.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 10:37 EST
Nmap scan report for 192.168.51.100
Host is up (0.0024s 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 0.14 seconds
└─(kali@kali)~[~]
```

Rispetto alla precedente scansione SYN, non ci sono differenze nei risultati ma nel modo in cui queste scansioni avvengono.

1_D VERSION DETECTION

Questa scansione richiede più tempo delle altre, per via dei dettagli nelle informazioni che vengono ricercate.

```
└─$ sudo nmap -sV 192.168.51.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 10:39 EST
Nmap scan report for 192.168.51.100
Host is up (0.00074s 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  ccproxy-ftp?
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: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: 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 173.23 seconds
└─(kali@kali)~[~]
```

Report risultati ottenuti

Indirizzo IP Target	192.168.51.100																																																																																																				
Sistema Operativo	OS CPE: cpe:/o:linux:linux_kernel:2.6 OS details: Linux 2.6.15 - 2.6.26 (likely embedded)																																																																																																				
Porte aperte	21/tcp 22/tcp 23/tcp 25/tcp 53/tcp 80/tcp 111/tcp 139/tcp 445/tcp 512/tcp 513/tcp 514/tcp 1099/tcp 1524/tcp 2049/tcp 2121/tcp 3306/tcp 5432/tcp 5900/tcp 6000/tcp 6667/tcp 8009/tcp 8180/tcp																																																																																																				
Servizi in ascolto con versione	<table><tr><th>PORT</th><th>STATE</th><th>SERVICE</th><th>VERSION</th></tr><tr><td>21/tcp</td><td>open</td><td>ftp</td><td>vsftpd 2.3.4</td></tr><tr><td>22/tcp</td><td>open</td><td>ssh</td><td>OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)</td></tr><tr><td>23/tcp</td><td>open</td><td>telnet</td><td>Linux telnetd</td></tr><tr><td>25/tcp</td><td>open</td><td>smtp</td><td>Postfix smtpd</td></tr><tr><td>53/tcp</td><td>open</td><td>domain</td><td>ISC BIND 9.4.2</td></tr><tr><td>80/tcp</td><td>open</td><td>http</td><td>Apache httpd 2.2.8 ((Ubuntu) DAV/2)</td></tr><tr><td>111/tcp</td><td>open</td><td>rpcbind</td><td>2 (RPC #100000)</td></tr><tr><td>139/tcp</td><td>open</td><td>netbios-ssn</td><td>Samba smbd 3.X - 4.X (workgroup: WORKGROUP)</td></tr><tr><td>445/tcp</td><td>open</td><td>netbios-ssn</td><td>Samba smbd 3.X - 4.X (workgroup: WORKGROUP)</td></tr><tr><td>512/tcp</td><td>open</td><td>exec</td><td>netkit-rsh rexecd</td></tr><tr><td>513/tcp</td><td>open</td><td>login?</td><td></td></tr><tr><td>514/tcp</td><td>open</td><td>shell</td><td>Netkit rshd</td></tr><tr><td>1099/tcp</td><td>open</td><td>java-rmi</td><td>GNU Classpath grmiregistry</td></tr><tr><td>1524/tcp</td><td>open</td><td>bindshell</td><td>Metasploitable root shell</td></tr><tr><td>2049/tcp</td><td>open</td><td>nfs</td><td>2-4 (RPC #100003)</td></tr><tr><td>2121/tcp</td><td>open</td><td>ccproxy-ftp?</td><td></td></tr><tr><td>3306/tcp</td><td>open</td><td>mysql</td><td>MySQL 5.0.51a-3ubuntu5</td></tr><tr><td>5432/tcp</td><td>open</td><td>postgresql</td><td>PostgreSQL DB 8.3.0 - 8.3.7</td></tr><tr><td>5900/tcp</td><td>open</td><td>vnc</td><td>VNC (protocol 3.3)</td></tr><tr><td>6000/tcp</td><td>open</td><td>X11</td><td>(access denied)</td></tr><tr><td>6667/tcp</td><td>open</td><td>irc</td><td>UnrealIRCd</td></tr><tr><td>8009/tcp</td><td>open</td><td>ajp13</td><td>Apache Jserv (Protocol v1.3)</td></tr><tr><td>8180/tcp</td><td>open</td><td>http</td><td>Apache Tomcat/Coyote JSP engine 1.1</td></tr><tr><td colspan="2">Service Info:</td><td colspan="2">Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel</td></tr></table>	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	ccproxy-ftp?		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:		Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel	
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	ccproxy-ftp?																																																																																																			
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:		Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel																																																																																																			

2. Caso con macchine su stessa rete

IP Kali Linux 192.168.50.102;

IP Metasploitable 192.168.50.103;

```
(kali@kali)-[~]
└─$ ping 192.168.50.103
PING 192.168.50.103 (192.168.50.103) 56(84) bytes of data:
64 bytes from 192.168.50.103: icmp_seq=1 ttl=64 time=0.419 ms
64 bytes from 192.168.50.103: icmp_seq=2 ttl=64 time=0.904 ms
64 bytes from 192.168.50.103: icmp_seq=3 ttl=64 time=0.716 ms
^C
--- 192.168.50.103 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2028ms
rtt min/avg/max/mdev = 0.419/0.679/0.904/0.199 ms
```

```
msfadmin@metasploitable:~$ 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=64 time=4.33 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=64 time=0.983 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=64 time=0.441 ms
--- 192.168.50.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.441/1.919/4.334/1.722 ms
msfadmin@metasploitable:~$
```

2. A OS fingerprinting

```
└─$ sudo nmap -O 192.168.50.103
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 11:04 EST
Nmap scan report for 192.168.50.103
Host is up (0.00063s 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: 08:00:27:84:48:BA (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 14.67 seconds
```

2. B SYN SCAN

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 11:07 EST
Nmap scan report for 192.168.50.103
Host is up (0.00013s 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: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.70 seconds
```

2. C TCP CONNECT

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 11:08 EST
Nmap scan report for 192.168.50.103
Host is up (0.00085s 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: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

2. D VERSION DETECTION

```
└─$ sudo nmap -sV 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-20 11:09 EST
Nmap scan report for 192.168.50.103
Host is up (0.000059s 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: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; O
Ss: 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 65.57 seconds
```

Report risultati ottenuti

Indirizzo IP Target	192.168.50.103
Sistema Operativo	Running: Linux 2.6.X OS CPE: cpe:/o:linux:linux_kernel:2.6 OS details: Linux 2.6.9 - 2.6.33
Porte aperte	21/tcp 22/tcp 23/tcp 25/tcp 53/tcp 80/tcp 111/tcp 139/tcp 445/tcp 512/tcp 513/tcp 514/tcp 1099/tcp 1524/tcp 2049/tcp 2121/tcp 3306/tcp 5432/tcp 5900/tcp 6000/tcp 6667/tcp 8009/tcp 8180/tcp
Servizi in ascolto con versione	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	ccproxy-ftp?	
	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:	Hosts:	metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel