

Network Scanning

Target: Metasploitable Machine

Types Of Scanning:

TCP: TCP connect scan used for detecting open ports upon the completion of the three-way handshake. It works by establishing a full connection and then dropping it by sending a packet.

```
root@kali:~# nmap -sT 192.168.25.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-21 10:02 CDT
Nmap scan report for 192.168.25.130
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
MAC Address: 00:0C:29:81:6B:28 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Syn: Stealth scan is used for bypassing firewall and logging mechanisms. It works by resetting the TCP connection before the three-way handshake is completed, which in turn makes the connection half open.

```

root@kali:~# nmap -sS 192.168.25.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-21 10:09 CDT
Nmap scan report for 192.168.25.130
Host is up (0.0027s 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: 00:0C:29:81:6B:28 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds

```

UDP: UDP scanning uses UDP protocol to test whether the port is open or closed. In this scan there is no flag manipulation. So, if a packet is sent to a port and the port is unreachable then packet is returned, then that means that the port is closed. If, however, there is no response, then the port is open.

```

root@kali:~# nmap -sU 192.168.25.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-21 10:09 CDT
Stats: 0:05:18 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 30.84% done; ETC: 10:27 (0:11:53 remaining)
Stats: 0:05:20 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 31.14% done; ETC: 10:27 (0:11:50 remaining)
Stats: 0:06:53 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 40.09% done; ETC: 10:27 (0:10:17 remaining)
Stats: 0:08:13 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 47.78% done; ETC: 10:27 (0:08:59 remaining)
Stats: 0:15:39 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 90.04% done; ETC: 10:27 (0:01:44 remaining)
Stats: 0:17:00 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 98.21% done; ETC: 10:27 (0:00:19 remaining)
Nmap scan report for 192.168.25.130
Host is up (0.00086s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE      SERVICE
53/udp    open       domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open       rpcbind
137/udp   open       netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open       nfs
MAC Address: 00:0C:29:81:6B:28 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1071.74 seconds

```

TCP with all ports, version and OS:

It finds information about ports mentioned, which OS is being used and OS version.

```

root@kali:~# nmap -sT -p1-9000 -sV -O 192.168.25.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-21 10:37 CDT
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.15% done; ETC: 10:38 (0:00:03 remaining)
Stats: 0:01:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 10:39 (0:00:00 remaining)
Nmap scan report for 192.168.25.130
Host is up (0.0013s latency).
Not shown: 8974 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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc          UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13?
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
MAC Address: 00:0C:29:81:6B:28 (VMware)
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

```

Syn file saved into xml and converted to html file

The information found by the network scanning technique is saved in .xml file and then that file is converted to .html file.

```

root@kali:~# nmap -sS -p1-9000 -sV -O 192.168.25.130 -oX Nscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-21 10:48 CDT
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.15% done; ETC: 10:49 (0:00:02 remaining)
Nmap scan report for 192.168.25.130
Host is up (0.0017s latency).
Not shown: 8974 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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13?
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
MAC Address: 00:0C:29:81:6B:28 (VMware)
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_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 129.99 seconds

```

```
root@kali:~# xsltproc Nscan.xml -> Nscan.html
root@kali:~# ls
Desktop Documents Downloads embedded-browser-no-sandbox.json Music Nscan.html Nscan.xml Pictures Public Templates Videos
root@kali:~# cat Nscan.html
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html xmlns:fo="http://www.w3.org/1999/XSL/Format">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<!--generated with nmap.xsl - version 0.9c by Benjamin Erb - http://www.benjamin-erb.de/nmap_xsl.php --><style type="text/css">
/* stylesheet print */
@media print
{
#menu {
display:none;
}

body {
font-family: Verdana, Helvetica, sans-serif;
}

h1 {
font-size: 13pt;
font-weight:bold;
margin:4pt 0pt 0pt 0pt;
padding:0;
}

h2 {
font-size: 12pt;
font-weight:bold;
margin:3pt 0pt 0pt 0pt;
padding:0;
}

h3, a:link, a:visited {
font-size: 9pt;
font-weight:bold;
margin:1pt 0pt 0pt 20pt;
padding:0;
text-decoration: none;
}
```

Nmap Scan Report - Scanned at Wed Sep 21 10:48:18 2022

Scan Summary | 192.168.25.130

Scan Summary

Nmap 7.92 was initiated at Wed Sep 21 10:48:18 2022 with these arguments:
`nmap -sS -p1-9000 -sV -O -oX Nscan.xml 192.168.25.130`

Verbosity: 0; Debug level 0

Nmap done at Wed Sep 21 10:50:27 2022; 1 IP address (1 host up) scanned in 129.99 seconds

192.168.25.130

Address

- 192.168.25.130 (ipv4)
- 00:0C:29:81:6B:28 - VMware (mac)

Ports

The 8974 ports scanned but not shown below are in state: **closed**

- 8974 ports replied with: **reset**

Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra info
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	OpenBSD or Solaris rlogind		
514	tcp open	tcpwrapped	syn-ack			
1099	tcp open	java-rmi	syn-ack	GNU Classpath gmrregistry		
1524	tcp open	bindshell	syn-ack	Metasploitable root shell		
2049	tcp open	rfs	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	
3632	tcp open	distccd	syn-ack	distccd	v1	(GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
5432	tcp open	postgresq	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7	
5900	tcp open	vnc	syn-ack	VNC		protocol 3.3
6000	tcp open	X11	syn-ack			access denied
6667	tcp open	irc	syn-ack	UnrealIRCd		
6697	tcp open	irc	syn-ack	UnrealIRCd		
8009	tcp open	ap13	syn-ack			
8180	tcp open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	
8787	tcp open	drb	syn-ack	Ruby DRb RMI		Ruby 1.8; path /usr/lib/ruby/1.8/drb

Remote Operating System Detection

Nmap Scripting:
This is done to find if the target system has any vulnerability. It extends Nmap’s capabilities to enable it to perform a variety of tasks and report the results along with Nmap’s normal output.


```

root@kali:~# nmap -sV --script=vulners.nse 192.168.25.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-21 12:59 CDT
Nmap scan report for 192.168.25.130
Host is up (0.0042s 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

| vulners:
| cpe:/a:isc:bind:9.4.2:
| SSV:60184      8.5 https://vulners.com/seebug/SSV:60184 *EXPLOIT*
| CVE-2012-1667 8.5 https://vulners.com/cve/CVE-2012-1667
| SSV:60292      7.8 https://vulners.com/seebug/SSV:60292 *EXPLOIT*
| CVE-2014-8500 7.8 https://vulners.com/cve/CVE-2014-8500
| CVE-2012-5166 7.8 https://vulners.com/cve/CVE-2012-5166
| CVE-2012-4244 7.8 https://vulners.com/cve/CVE-2012-4244
| CVE-2012-3817 7.8 https://vulners.com/cve/CVE-2012-3817
| CVE-2008-4163 7.8 https://vulners.com/cve/CVE-2008-4163
| CVE-2010-0382 7.6 https://vulners.com/cve/CVE-2010-0382
| EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2 7.2 https://vulners.com/exploitpack/EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2 *EXPLOIT*
| EDB-ID:42121 7.2 https://vulners.com/exploitdb/EDB-ID:42121 *EXPLOIT*
| CVE-2017-3141 7.2 https://vulners.com/cve/CVE-2017-3141
| CVE-2015-8461 7.1 https://vulners.com/cve/CVE-2015-8461
| CVE-2021-25216 6.8 https://vulners.com/cve/CVE-2021-25216
| CVE-2015-8704 6.8 https://vulners.com/cve/CVE-2015-8704
| CVE-2009-0025 6.8 https://vulners.com/cve/CVE-2009-0025
| CVE-2015-8705 6.6 https://vulners.com/cve/CVE-2015-8705
| CVE-2010-3614 6.4 https://vulners.com/cve/CVE-2010-3614
| SSV:4636       5.8 https://vulners.com/seebug/SSV:4636 *EXPLOIT*
| SSV:30099      5.0 https://vulners.com/seebug/SSV:30099 *EXPLOIT*
| SSV:20595      5.0 https://vulners.com/seebug/SSV:20595 *EXPLOIT*
| PACKETSTORM:157836 5.0 https://vulners.com/packetstorm/PACKETSTORM:157836 *EXPLOIT*
| FBC03933-7A65-52F3-83F4-4B2253A490B6 5.0 https://vulners.com/githubexploit/FBC03933-7A65-52F3-83F4-4B2253A490B6 *EXPLOIT*
| CVE-2021-25219 5.0 https://vulners.com/cve/CVE-2021-25219
| CVE-2021-25215 5.0 https://vulners.com/cve/CVE-2021-25215
| CVE-2020-8616 5.0 https://vulners.com/cve/CVE-2020-8616
| CVE-2017-3145 5.0 https://vulners.com/cve/CVE-2017-3145
| CVE-2016-9444 5.0 https://vulners.com/cve/CVE-2016-9444
| CVE-2016-9131 5.0 https://vulners.com/cve/CVE-2016-9131
| CVE-2016-8864 5.0 https://vulners.com/cve/CVE-2016-8864
| CVE-2016-2848 5.0 https://vulners.com/cve/CVE-2016-2848

| CVE-2016-1286 5.0 https://vulners.com/cve/CVE-2016-1286
| CVE-2015-8000 5.0 https://vulners.com/cve/CVE-2015-8000
| CVE-2012-1033 5.0 https://vulners.com/cve/CVE-2012-1033
| CVE-2011-4313 5.0 https://vulners.com/cve/CVE-2011-4313
| CVE-2011-1910 5.0 https://vulners.com/cve/CVE-2011-1910
| CVE-2009-0265 5.0 https://vulners.com/cve/CVE-2009-0265
| SSV:11919      4.3 https://vulners.com/seebug/SSV:11919 *EXPLOIT*
| CVE-2020-8617 4.3 https://vulners.com/cve/CVE-2020-8617
| CVE-2017-3143 4.3 https://vulners.com/cve/CVE-2017-3143
| CVE-2017-3142 4.3 https://vulners.com/cve/CVE-2017-3142
| CVE-2016-2775 4.3 https://vulners.com/cve/CVE-2016-2775
| CVE-2016-1285 4.3 https://vulners.com/cve/CVE-2016-1285
| CVE-2010-0097 4.3 https://vulners.com/cve/CVE-2010-0097
| CVE-2009-0696 4.3 https://vulners.com/cve/CVE-2009-0696
| 1337DAY-ID-34485 4.3 https://vulners.com/zdt/1337DAY-ID-34485 *EXPLOIT*
| CVE-2020-8622 4.0 https://vulners.com/cve/CVE-2020-8622
| CVE-2016-6170 4.0 https://vulners.com/cve/CVE-2016-6170
| CVE-2010-0290 4.0 https://vulners.com/cve/CVE-2010-0290
| SSV:14986      2.6 https://vulners.com/seebug/SSV:14986 *EXPLOIT*
| CVE-2009-4022 2.6 https://vulners.com/cve/CVE-2009-4022
| PACKETSTORM:142800 0.0 https://vulners.com/packetstorm/PACKETSTORM:142800 *EXPLOIT*
| 1337DAY-ID-27896 0.0 https://vulners.com/zdt/1337DAY-ID-27896 *EXPLOIT*

80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp    open  rpcbind      2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 46057/tcp mountd
| 100005 1,2,3 59120/udp mountd
| 100021 1,3,4 43902/udp nlockmgr
| 100021 1,3,4 46768/tcp nlockmgr
| 100024 1 41472/tcp status
|_ 100024 1 45097/udp status
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        OpenBSD or Solaris rlogind
514/tcp    open  tcpwrapped
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
vulners:
  cpe:/a:proftpd:proftpd:1.3.1:
    SAINT:FD1752E124A72FD3A26FEB9B315E8382  10.0  https://vulners.com/saint/SAINT:FD1752E124A72FD3A26FEB9B315E8382  *EXPLOIT*
    SAINT:950EB68D408A40399926A4CCAD3CC62E  10.0  https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC62E  *EXPLOIT*
    SAINT:63FB77B9136D48259E4F0D4CDA35E957  10.0  https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E957  *EXPLOIT*
    SAINT:1B08F4664C28B180EEC9617B41D9A2C  10.0  https://vulners.com/saint/SAINT:1B08F4664C28B180EEC9617B41D9A2C  *EXPLOIT*
    PROFTPD_MOD_COPY  10.0  https://vulners.com/canvas/PROFTPD_MOD_COPY  *EXPLOIT*
    PACKETSTORM:162777  10.0  https://vulners.com/packetstorm/PACKETSTORM:162777  *EXPLOIT*
    PACKETSTORM:132218  10.0  https://vulners.com/packetstorm/PACKETSTORM:132218  *EXPLOIT*
    PACKETSTORM:131567  10.0  https://vulners.com/packetstorm/PACKETSTORM:131567  *EXPLOIT*
    PACKETSTORM:131555  10.0  https://vulners.com/packetstorm/PACKETSTORM:131555  *EXPLOIT*
    PACKETSTORM:131505  10.0  https://vulners.com/packetstorm/PACKETSTORM:131505  *EXPLOIT*
    EDB-ID:49908  10.0  https://vulners.com/exploitdb/EDB-ID:49908  *EXPLOIT*
    1337DAY-ID-36298  10.0  https://vulners.com/zdt/1337DAY-ID-36298  *EXPLOIT*
    1337DAY-ID-23720  10.0  https://vulners.com/zdt/1337DAY-ID-23720  *EXPLOIT*
    1337DAY-ID-23544  10.0  https://vulners.com/zdt/1337DAY-ID-23544  *EXPLOIT*
    SSV:26016  9.0  https://vulners.com/seebug/SSV:26016  *EXPLOIT*
    SSV:24282  9.0  https://vulners.com/seebug/SSV:24282  *EXPLOIT*
    CVE-2011-4130  9.0  https://vulners.com/cve/CVE-2011-4130  *EXPLOIT*
    SSV:96525  7.5  https://vulners.com/seebug/SSV:96525  *EXPLOIT*
    CVE-2019-12815  7.5  https://vulners.com/cve/CVE-2019-12815  *EXPLOIT*
    739FE495-4675-5A2A-BB93-EEF94AC07632  7.5  https://vulners.com/githubexploit/739FE495-4675-5A2A-BB93-EEF94AC07632  *EXPLOIT*
    SSV:20226  7.1  https://vulners.com/seebug/SSV:20226  *EXPLOIT*
    PACKETSTORM:95517  7.1  https://vulners.com/packetstorm/PACKETSTORM:95517  *EXPLOIT*
    CVE-2010-3867  7.1  https://vulners.com/cve/CVE-2010-3867  *EXPLOIT*
    SSV:12447  6.8  https://vulners.com/seebug/SSV:12447  *EXPLOIT*
    SSV:11950  6.8  https://vulners.com/seebug/SSV:11950  *EXPLOIT*
    EDB-ID:33128  6.8  https://vulners.com/exploitdb/EDB-ID:33128  *EXPLOIT*
    CVE-2010-4652  6.8  https://vulners.com/cve/CVE-2010-4652  *EXPLOIT*
    CVE-2009-0543  6.8  https://vulners.com/cve/CVE-2009-0543  *EXPLOIT*
    SSV:12523  5.8  https://vulners.com/seebug/SSV:12523  *EXPLOIT*
    CVE-2009-3639  5.8  https://vulners.com/cve/CVE-2009-3639  *EXPLOIT*
    CVE-2020-9272  5.0  https://vulners.com/cve/CVE-2020-9272  *EXPLOIT*
    CVE-2019-19272  5.0  https://vulners.com/cve/CVE-2019-19272  *EXPLOIT*
    CVE-2019-19271  5.0  https://vulners.com/cve/CVE-2019-19271  *EXPLOIT*
    CVE-2019-19270  5.0  https://vulners.com/cve/CVE-2019-19270  *EXPLOIT*
    CVE-2019-18217  5.0  https://vulners.com/cve/CVE-2019-18217  *EXPLOIT*
    CVE-2016-3125  5.0  https://vulners.com/cve/CVE-2016-3125  *EXPLOIT*
    CVE-2011-1137  5.0  https://vulners.com/cve/CVE-2011-1137  *EXPLOIT*
    CVE-2008-7265  4.0  https://vulners.com/cve/CVE-2008-7265  *EXPLOIT*
    CVE-2017-7418  2.1  https://vulners.com/cve/CVE-2017-7418  *EXPLOIT*
    CVE-2012-6095  1.2  https://vulners.com/cve/CVE-2012-6095  *EXPLOIT*
3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
vulners:
```

```
MySQL 5.0.51a-3ubuntu5:
  CVE-2009-0819  4.0  https://vulners.com/cve/CVE-2009-0819  *EXPLOIT*
  CVE-2007-5925  4.0  https://vulners.com/cve/CVE-2007-5925  *EXPLOIT*
  NODEJS:602  0.0  https://vulners.com/nodejs/NODEJS:602  *EXPLOIT*
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
vulners:
  cpe:/a:postgresql:postgresql:8.3:
    SSV:60718  10.0  https://vulners.com/seebug/SSV:60718  *EXPLOIT*
    CVE-2013-1903  10.0  https://vulners.com/cve/CVE-2013-1903  *EXPLOIT*
    CVE-2013-1902  10.0  https://vulners.com/cve/CVE-2013-1902  *EXPLOIT*
    SSV:30015  8.5  https://vulners.com/seebug/SSV:30015  *EXPLOIT*
    SSV:19652  8.5  https://vulners.com/seebug/SSV:19652  *EXPLOIT*
    POSTGRESQL:CVE-2013-1900  8.5  https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900  *EXPLOIT*
    POSTGRESQL:CVE-2010-1169  8.5  https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1169  *EXPLOIT*
    CVE-2010-1447  8.5  https://vulners.com/cve/CVE-2010-1447  *EXPLOIT*
    CVE-2010-1169  8.5  https://vulners.com/cve/CVE-2010-1169  *EXPLOIT*
    SSV:19754  7.5  https://vulners.com/seebug/SSV:19754  *EXPLOIT*
    SSV:30152  6.8  https://vulners.com/seebug/SSV:30152  *EXPLOIT*
    SECURITYVULNS:VULN:10252  6.8  https://vulners.com/securityvulns/SECURITYVULNS:VULN:10252  *EXPLOIT*
    POSTGRESQL:CVE-2013-0255  6.8  https://vulners.com/postgresql/POSTGRESQL:CVE-2013-0255  *EXPLOIT*
    POSTGRESQL:CVE-2012-0868  6.8  https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0868  *EXPLOIT*
    POSTGRESQL:CVE-2009-3231  6.8  https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3231  *EXPLOIT*
    CVE-2013-0255  6.8  https://vulners.com/cve/CVE-2013-0255  *EXPLOIT*
    CVE-2012-0868  6.8  https://vulners.com/cve/CVE-2012-0868  *EXPLOIT*
    CVE-2009-3231  6.8  https://vulners.com/cve/CVE-2009-3231  *EXPLOIT*
    SSV:62083  6.5  https://vulners.com/seebug/SSV:62083  *EXPLOIT*
    SSV:62016  6.5  https://vulners.com/seebug/SSV:62016  *EXPLOIT*
    SSV:61543  6.5  https://vulners.com/seebug/SSV:61543  *EXPLOIT*
    SSV:19018  6.5  https://vulners.com/seebug/SSV:19018  *EXPLOIT*
    SSV:15153  6.5  https://vulners.com/seebug/SSV:15153  *EXPLOIT*
    SSV:15097  6.5  https://vulners.com/seebug/SSV:15097  *EXPLOIT*
    SSV:15095  6.5  https://vulners.com/seebug/SSV:15095  *EXPLOIT*
    SECURITYVULNS:VULN:10803  6.5  https://vulners.com/securityvulns/SECURITYVULNS:VULN:10803  *EXPLOIT*
    SECURITYVULNS:VULN:10473  6.5  https://vulners.com/securityvulns/SECURITYVULNS:VULN:10473  *EXPLOIT*
    POSTGRESQL:CVE-2014-0065  6.5  https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0065  *EXPLOIT*
    POSTGRESQL:CVE-2014-0064  6.5  https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0064  *EXPLOIT*
    POSTGRESQL:CVE-2014-0063  6.5  https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0063  *EXPLOIT*
    POSTGRESQL:CVE-2014-0061  6.5  https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0061  *EXPLOIT*
    POSTGRESQL:CVE-2012-0866  6.5  https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0866  *EXPLOIT*
    POSTGRESQL:CVE-2010-4015  6.5  https://vulners.com/postgresql/POSTGRESQL:CVE-2010-4015  *EXPLOIT*
    POSTGRESQL:CVE-2009-4136  6.5  https://vulners.com/postgresql/POSTGRESQL:CVE-2009-4136  *EXPLOIT*
    POSTGRESQL:CVE-2009-3230  6.5  https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3230  *EXPLOIT*
    CVE-2014-0065  6.5  https://vulners.com/cve/CVE-2014-0065  *EXPLOIT*
    CVE-2014-0064  6.5  https://vulners.com/cve/CVE-2014-0064  *EXPLOIT*
```



```

CVE-2014-0063 6.5 https://vulners.com/cve/CVE-2014-0063
CVE-2014-0061 6.5 https://vulners.com/cve/CVE-2014-0061
CVE-2012-0866 6.5 https://vulners.com/cve/CVE-2012-0866
CVE-2010-4015 6.5 https://vulners.com/cve/CVE-2010-4015
SECURITYVULNS:VULN:11183 6.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:11183
POSTGRESQL:CVE-2010-3433 6.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2010-3433
POSTGRESQL:CVE-2010-1170 6.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1170
CVE-2010-3433 6.0 https://vulners.com/cve/CVE-2010-3433
CVE-2010-1170 6.0 https://vulners.com/cve/CVE-2010-1170
SSV:15154 5.8 https://vulners.com/seebug/SSV:15154 *EXPLOIT*
SSV:15096 5.8 https://vulners.com/seebug/SSV:15096 *EXPLOIT*
POSTGRESQL:CVE-2009-4034 5.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2009-4034
SSV:19669 5.5 https://vulners.com/seebug/SSV:19669 *EXPLOIT*
POSTGRESQL:CVE-2010-1975 5.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1975
CVE-2010-1975 5.5 https://vulners.com/cve/CVE-2010-1975
SSV:61546 4.9 https://vulners.com/seebug/SSV:61546 *EXPLOIT*
SSV:60334 4.9 https://vulners.com/seebug/SSV:60334 *EXPLOIT*
POSTGRESQL:CVE-2014-0062 4.9 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0062
POSTGRESQL:CVE-2012-3488 4.9 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-3488
CVE-2014-0062 4.9 https://vulners.com/cve/CVE-2014-0062
CVE-2012-3488 4.9 https://vulners.com/cve/CVE-2012-3488
SSV:61544 4.6 https://vulners.com/seebug/SSV:61544 *EXPLOIT*
CVE-2014-0067 4.6 https://vulners.com/cve/CVE-2014-0067
POSTGRESQL:CVE-2012-2143 4.3 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-2143
POSTGRESQL:CVE-2012-0867 4.3 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0867
CVE-2012-2143 4.3 https://vulners.com/cve/CVE-2012-2143
SSV:61547 4.0 https://vulners.com/seebug/SSV:61547 *EXPLOIT*
SSV:61545 4.0 https://vulners.com/seebug/SSV:61545 *EXPLOIT*
SSV:60335 4.0 https://vulners.com/seebug/SSV:60335 *EXPLOIT*
SSV:60186 4.0 https://vulners.com/seebug/SSV:60186 *EXPLOIT*
SSV:4928 4.0 https://vulners.com/seebug/SSV:4928 *EXPLOIT*
SECURITYVULNS:VULN:9765 4.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:9765
POSTGRESQL:CVE-2014-0066 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0066
POSTGRESQL:CVE-2014-0060 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0060
POSTGRESQL:CVE-2012-3489 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-3489
POSTGRESQL:CVE-2012-2655 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2012-2655
POSTGRESQL:CVE-2009-3229 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3229
POSTGRESQL:CVE-2009-0922 4.0 https://vulners.com/postgresql/POSTGRESQL:CVE-2009-0922
CVE-2014-0066 4.0 https://vulners.com/cve/CVE-2014-0066
CVE-2014-0060 4.0 https://vulners.com/cve/CVE-2014-0060
CVE-2012-3489 4.0 https://vulners.com/cve/CVE-2012-3489
CVE-2012-2655 4.0 https://vulners.com/cve/CVE-2012-2655
CVE-2009-3229 4.0 https://vulners.com/cve/CVE-2009-3229
SSV:19322 3.5 https://vulners.com/seebug/SSV:19322 *EXPLOIT*
PACKETSTORM:127092 3.5 https://vulners.com/packetstorm/PACKETSTORM:127092 *EXPLOIT*
CVE-2010-0733 3.5 https://vulners.com/cve/CVE-2010-0733
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13?
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:81:6B:28 (VMware)
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 128.28 seconds

```