



Port Scan Report

kioptrix

Arguments:	<code>nmap -vvv -p 22,111,443,80,139,32768 -A -sC -oA rustscanAggressive --script vulners -T4 10.0.2.6</code>
Scan started at:	Sat Nov 18 09:05:53 2023
Scan type:	connect
Nmap version:	7.94

The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed.

Ports and Services

Ports status and services type

HOSTS UP	PORTS	SERVICES	OS
1	6	6	0

Total Ports

6

Open Ports

6

Closed Ports

0

Filtered Ports

0

Ports:


22 (1), 80 (1), 111 (1), 139 (1), 443 (1), 32768 (1)


Services:


ssh (1), http (1), rpcbind (1), netbios-ssn (1), https (1), status (1)


10.0.2.6







Status: up, Reason: syn-ack, TTL: 0

**6**
TOTAL PORT

**6**
OPEN PORT

**0**
CLOSED PORT

**0**
FILTERED PORT

Protocol / Port	Port State	Product / Version
tcp / 22 ssh	 open	OpenSSH / 2.9p2
tcp / 80 http	 open	Apache httpd / 1.3.20
tcp / 111 rpcbind	 open	<i>No Product / 2</i>
tcp / 139 netbios-ssn	 open	Samba smbd / <i>No Version</i>
tcp / 443 https	 open	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b / <i>No Version</i>
tcp / 32768 status	 open	<i>No Product / 1</i>

NSE Scripts for 10.0.2.6:

vulners - Address: **10.0.2.6** - Port: **22**

```
cpe:/a:openbsd:openssh:2.9p2:
CVE-2002-0640 10.0 https://vulners.com/cve/CVE-2002-0640
CVE-2002-0639 10.0 https://vulners.com/cve/CVE-2002-0639
CVE-2002-0083 10.0 https://vulners.com/cve/CVE-2002-0083
CVE-2011-2895 9.3 https://vulners.com/cve/CVE-2011-2895
CVE-2006-5051 9.3 https://vulners.com/cve/CVE-2006-5051
CVE-2006-4924 7.8 https://vulners.com/cve/CVE-2006-4924
CVE-2003-1562 7.6 https://vulners.com/cve/CVE-2003-1562
CVE-2002-0575 7.5 https://vulners.com/cve/CVE-2002-0575
CVE-2001-1459 7.5 https://vulners.com/cve/CVE-2001-1459
CVE-2001-1380 7.5 https://vulners.com/cve/CVE-2001-1380
CVE-2001-0816 7.5 https://vulners.com/cve/CVE-2001-0816
SECURITYVULNS:VULN:1956 7.2 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1956
CVE-2001-0529 7.2 https://vulners.com/cve/CVE-2001-0529
SSV:64479 5.0 https://vulners.com/seebug/SSV:64479 *EXPLOIT*
SSV:6192 5.0 https://vulners.com/seebug/SSV:6192 *EXPLOIT*
SSV:60656 5.0 https://vulners.com/seebug/SSV:60656 *EXPLOIT*
SSV:16847 5.0 https://vulners.com/seebug/SSV:16847 *EXPLOIT*
PACKETSTORM:73600 5.0 https://vulners.com/packetstorm/PACKETSTORM:73600 *EXPLOIT*
PACKETSTORM:54435 5.0 https://vulners.com/packetstorm/PACKETSTORM:54435 *EXPLOIT*
EXPLOITPACK:63CFD85A8DA29BF22328E65C685CBBA3 5.0
https://vulners.com/exploitpack/EXPLOITPACK:63CFD85A8DA29BF22328E65C685CBBA3 *EXPLOIT*
EDB-ID:3303 5.0 https://vulners.com/exploitdb/EDB-ID:3303 *EXPLOIT*
CVE-2010-5107 5.0 https://vulners.com/cve/CVE-2010-5107
CVE-2007-2243 5.0 https://vulners.com/cve/CVE-2007-2243
CVE-2006-5052 5.0 https://vulners.com/cve/CVE-2006-5052
SSV:66339 4.9 https://vulners.com/seebug/SSV:66339 *EXPLOIT*
SSV:10777 4.9 https://vulners.com/seebug/SSV:10777 *EXPLOIT*
EXPLOITPACK:B5E7D30E7583980F37EF6DBC0B05FBC3 4.9
https://vulners.com/exploitpack/EXPLOITPACK:B5E7D30E7583980F37EF6DBC0B05FBC3 *EXPLOIT*
EDB-ID:8163 4.9 https://vulners.com/exploitdb/EDB-ID:8163 *EXPLOIT*
CVE-2009-0537 4.9 https://vulners.com/cve/CVE-2009-0537
CVE-2011-4327 2.1 https://vulners.com/cve/CVE-2011-4327
CVE-2008-3259 1.2 https://vulners.com/cve/CVE-2008-3259
SECURITYVULNS:VULN:1953 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1953
SECURITYVULNS:VULN:1608 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1608
SECURITYVULNS:VULN:1499 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1499
SECURITYVULNS:VULN:1488 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1488
SECURITYVULNS:VULN:1474 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1474
SECURITYVULNS:VULN:1439 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1439
SECURITYVULNS:VULN:1344 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1344
SECURITYVULNS:VULN:1262 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1262
SECURITYVULNS:VULN:1233 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1233
```

http-server-header - Address: **10.0.2.6** - Port: **80**

```
Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
```

vulners - Address: **10.0.2.6** - Port: **80**

```
cpe:/a:apache:http_server:1.3.20:
```

CVE-2002-2272 7.8 <https://vulners.com/cve/CVE-2002-2272>
CVE-2004-1082 7.5 <https://vulners.com/cve/CVE-2004-1082>
CVE-2002-2029 7.5 <https://vulners.com/cve/CVE-2002-2029>
CVE-2002-0257 7.5 <https://vulners.com/cve/CVE-2002-0257>
CVE-2003-0542 7.2 <https://vulners.com/cve/CVE-2003-0542>
SSV:66957 5.0 <https://vulners.com/seebug/SSV:66957> *EXPLOIT*
SSV:4148 5.0 <https://vulners.com/seebug/SSV:4148> *EXPLOIT*
SSV:17994 5.0 <https://vulners.com/seebug/SSV:17994> *EXPLOIT*
SSV:14432 5.0 <https://vulners.com/seebug/SSV:14432> *EXPLOIT*
PACKETSTORM:85018 5.0 <https://vulners.com/packetstorm/PACKETSTORM:85018> *EXPLOIT*
PACKETSTORM:82197 5.0 <https://vulners.com/packetstorm/PACKETSTORM:82197> *EXPLOIT*
EXPLOITPACK:44DAC602FB30402C58970DFAB1C4AF87 5.0
<https://vulners.com/exploitpack/EXPLOITPACK:44DAC602FB30402C58970DFAB1C4AF87> *EXPLOIT*
EDB-ID:9887 5.0 <https://vulners.com/exploitdb/EDB-ID:9887> *EXPLOIT*
CVE-2007-6750 5.0 <https://vulners.com/cve/CVE-2007-6750>
CVE-2004-0263 5.0 <https://vulners.com/cve/CVE-2004-0263>
CVE-2003-0460 5.0 <https://vulners.com/cve/CVE-2003-0460>
CVE-2003-0083 5.0 <https://vulners.com/cve/CVE-2003-0083>
CVE-2003-0020 5.0 <https://vulners.com/cve/CVE-2003-0020>
CVE-2002-2103 5.0 <https://vulners.com/cve/CVE-2002-2103>
CVE-2001-1556 5.0 <https://vulners.com/cve/CVE-2001-1556>
CVE-2002-1658 4.6 <https://vulners.com/cve/CVE-2002-1658>
CVE-2002-1233 2.6 <https://vulners.com/cve/CVE-2002-1233>
CVE-2001-1534 2.1 <https://vulners.com/cve/CVE-2001-1534>

rpcinfo - Address: **10.0.2.6** - Port: **111**

```
program version port/proto service
100000 2 111/tcp rpcbind
100000 2 111/udp rpcbind
100024 1 32768/tcp status
100024 1 32768/udp status
```

http-server-header - Address: **10.0.2.6** - Port: **443**

Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

Generated by
WE\$MAP
<https://github.com/Rev3rseSecurity/WebMap>