

scans

nmap

PORT STATE SERVICE VERSION

21/tcp open ftp ProFTPD 1.3.1

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

| 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

|_ ssl-date: 2020-07-18T14:58:48+00:00; +2s from scanner time.

|_ sslv2:

|_ SSLv2 supported

|_ ciphers:

|_ SSL2_DES_192_EDE3_CBC_WITH_MD5

|_ SSL2_DES_64_CBC_WITH_MD5

|_ SSL2_RC2_128_CBC_WITH_MD5

|_ SSL2_RC4_128_WITH_MD5

|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

|_ SSL2_RC4_128_EXPORT40_WITH_MD5

53/tcp open domain ISC BIND 9.4.2

|_ dns-nsid:

|_ bind.version: 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)

|_ http-methods:

|_ Potentially risky methods: TRACE

|_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch

|_ http-title: Site doesn't have a title (text/html).

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

|_ mysql-info:

|_ Protocol: 10

|_ Version: 5.0.51a-3ubuntu5

|_ Thread ID: 8

|_ Capabilities flags: 43564

|_ Some Capabilities: SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsTransactions, SupportsCompression, Speaks41ProtocolNew, Support41Auth, LongColumnFlag

|_ Status: Autocommit

|_ Salt: }'Fi_"(BTaila"%2kFY0

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

|_ ssl-date: 2020-07-18T14:58:47+00:00; +1s from scanner time.

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|_ ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|_ http-favicon: Apache Tomcat

|_ http-server-header: Apache-Coyote/1.1

|_ http-title: Apache Tomcat/5.5

MAC Address: 08:00:27:8D:BE:EB (Oracle VirtualBox virtual NIC)

Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_ clock-skew: mean: 1h00m01s, deviation: 2h00m00s, median: 1s

|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

|_ smb-os-discovery:

|_ OS: Unix (Samba 3.0.20-Debian)

|_ Computer name: metasploitable

|_ NetBIOS computer name:

|_ Domain name: localdomain

|_ FQDN: metasploitable.localdomain

|_ System time: 2020-07-18T10:58:39-04:00

|_ smb-security-mode:

|_ account_used: <blank>

|_ authentication_level: user

|_ challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

|_ smb2-time: Protocol negotiation failed (SMB2)