```
*********************************************************************
*                      Penetration Test Report                      *
*********************************************************************
Time of scan: 09:53
Device found on Network: 1
Device IP address found: 192.168.125.131
Open ports found on Network: 29
IP address scanned: 192.168.125.131

*********************************************************************
*     Open Ports and Services ON Target IP Address 192.168.125.131    *
*********************************************************************
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
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)
37585/tcp open  mountd      1-3 (RPC #100005)
38770/tcp open  nlockmgr    1-4 (RPC #100021)
45139/tcp open  java-rmi    GNU Classpath grmiregistry
51705/tcp open  status      1 (RPC #100024)

*********************************************************************
*                  Usernames and Passwords Found                    *
*********************************************************************
login:postgres password:postgres
login:user password:user
login:service password:service

*********************************************************************
*                       Vulnerabilities found                       *
*********************************************************************
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
21/tcp    open  ftp         vsftpd 2.3.4
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|   cpe:/a:openbsd:openssh:4.7p1:
|           CVE-2010-4478     7.5   https://vulners.com/cve/CVE-2010-4478
|           CVE-2008-1657     6.5   https://vulners.com/cve/CVE-2008-1657
|           CVE-2010-5107     5.0   https://vulners.com/cve/CVE-2010-5107
|           CVE-2012-0814     3.5   https://vulners.com/cve/CVE-2012-0814
|           CVE-2011-5000     3.5   https://vulners.com/cve/CVE-2011-5000
```

```
|           CVE-2008-5161     2.6   https://vulners.com/cve/CVE-2008-5161
|           CVE-2011-4327     2.1   https://vulners.com/cve/CVE-2011-4327
|           CVE-2008-3259     1.2   https://vulners.com/cve/CVE-2008-3259
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|     IDs:  BID:70574  CVE:CVE-2014-3566
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.openssl.org/~bodo/ssl-poodle.pdf
|     IDs:  BID:74733  CVE:CVE-2015-4000
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|     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
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|           CVE-2011-3192     7.8   https://vulners.com/cve/CVE-2011-3192
|           CVE-2017-7679     7.5   https://vulners.com/cve/CVE-2017-7679
|           CVE-2017-3167     7.5   https://vulners.com/cve/CVE-2017-3167
|           CVE-2009-1891     7.1   https://vulners.com/cve/CVE-2009-1891
|           CVE-2009-1890     7.1   https://vulners.com/cve/CVE-2009-1890
|           CVE-2012-0883     6.9   https://vulners.com/cve/CVE-2012-0883
|           CVE-2016-5387     6.8   https://vulners.com/cve/CVE-2016-5387
|           CVE-2014-0226     6.8   https://vulners.com/cve/CVE-2014-0226
|           CVE-2017-9788     6.4   https://vulners.com/cve/CVE-2017-9788
|           CVE-2009-1956     6.4   https://vulners.com/cve/CVE-2009-1956
|           CVE-2009-3555     5.8   https://vulners.com/cve/CVE-2009-3555
|           CVE-2013-1862     5.1   https://vulners.com/cve/CVE-2013-1862
|           CVE-2017-9798     5.0   https://vulners.com/cve/CVE-2017-9798
|           CVE-2016-8743     5.0   https://vulners.com/cve/CVE-2016-8743
|           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-2010-1452     5.0   https://vulners.com/cve/CVE-2010-1452
|           CVE-2010-0408     5.0   https://vulners.com/cve/CVE-2010-0408
|           CVE-2009-3095     5.0   https://vulners.com/cve/CVE-2009-3095
|           CVE-2009-2699     5.0   https://vulners.com/cve/CVE-2009-2699
|           CVE-2008-2364     5.0   https://vulners.com/cve/CVE-2008-2364
|           CVE-2007-6750     5.0   https://vulners.com/cve/CVE-2007-6750
|           CVE-2009-1195     4.9   https://vulners.com/cve/CVE-2009-1195
|           CVE-2012-0031     4.6   https://vulners.com/cve/CVE-2012-0031
|           CVE-2011-3607     4.4   https://vulners.com/cve/CVE-2011-3607
|           CVE-2016-4975     4.3   https://vulners.com/cve/CVE-2016-4975
|           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-2008-2939     4.3   https://vulners.com/cve/CVE-2008-2939
|           CVE-2008-0455     4.3   https://vulners.com/cve/CVE-2008-0455
|           CVE-2008-0005     4.3   https://vulners.com/cve/CVE-2008-0005
|           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
|_          CVE-2011-4415     1.2   https://vulners.com/cve/CVE-2011-4415
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
|           CVE-2011-4130    9.0   https://vulners.com/cve/CVE-2011-4130
|           CVE-2019-12815   7.5   https://vulners.com/cve/CVE-2019-12815
|           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
|           CVE-2009-3639    5.8   https://vulners.com/cve/CVE-2009-3639
|           CVE-2020-9272    5.0   https://vulners.com/cve/CVE-2020-9272
|           CVE-2019-19272   5.0   https://vulners.com/cve/CVE-2019-19272
|           CVE-2019-19271   5.0   https://vulners.com/cve/CVE-2019-19271
|           CVE-2019-19270   5.0   https://vulners.com/cve/CVE-2019-19270
|           CVE-2019-18217   5.0   https://vulners.com/cve/CVE-2019-18217
|           CVE-2016-3125    5.0   https://vulners.com/cve/CVE-2016-3125
|           CVE-2011-1137    5.0   https://vulners.com/cve/CVE-2011-1137
|           CVE-2008-7265    4.0   https://vulners.com/cve/CVE-2008-7265
|           CVE-2017-7418    2.1   https://vulners.com/cve/CVE-2017-7418
|           CVE-2012-6095    1.2   https://vulners.com/cve/CVE-2012-6095
|_          CVE-2021-46854   0.0   https://vulners.com/cve/CVE-2021-46854
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
|           CVE-2009-2446    8.5   https://vulners.com/cve/CVE-2009-2446
|           CVE-2008-0226    7.5   https://vulners.com/cve/CVE-2008-0226
|           CVE-2009-5026    6.8   https://vulners.com/cve/CVE-2009-5026
|           CVE-2009-4028    6.8   https://vulners.com/cve/CVE-2009-4028
|           CVE-2010-1848    6.5   https://vulners.com/cve/CVE-2010-1848
|           CVE-2010-1850    6.0   https://vulners.com/cve/CVE-2010-1850
|           CVE-2008-7247    6.0   https://vulners.com/cve/CVE-2008-7247
|           CVE-2010-3833    5.0   https://vulners.com/cve/CVE-2010-3833
|           CVE-2010-1849    5.0   https://vulners.com/cve/CVE-2010-1849
|           PRION:CVE-2021-2356    4.9   https://vulners.com/prion/PRION:CVE-
2021-2356
|           PRION:CVE-2023-21980   4.6   https://vulners.com/prion/PRION:CVE-
2023-21980
|           CVE-2008-4098    4.6   https://vulners.com/cve/CVE-2008-4098
|           CVE-2008-2079    4.6   https://vulners.com/cve/CVE-2008-2079
|           PRION:CVE-2022-21417   4.0   https://vulners.com/prion/PRION:CVE-
2022-21417
|           CVE-2012-0490    4.0   https://vulners.com/cve/CVE-2012-0490
|           CVE-2012-0484    4.0   https://vulners.com/cve/CVE-2012-0484
|           CVE-2012-0102    4.0   https://vulners.com/cve/CVE-2012-0102
|           CVE-2012-0101    4.0   https://vulners.com/cve/CVE-2012-0101
|           CVE-2012-0087    4.0   https://vulners.com/cve/CVE-2012-0087
|           CVE-2010-3838    4.0   https://vulners.com/cve/CVE-2010-3838
|           CVE-2010-3837    4.0   https://vulners.com/cve/CVE-2010-3837
|           CVE-2010-3836    4.0   https://vulners.com/cve/CVE-2010-3836
|           CVE-2010-3834    4.0   https://vulners.com/cve/CVE-2010-3834
|           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-2009-4019    4.0   https://vulners.com/cve/CVE-2009-4019
|           CVE-2008-3963    4.0   https://vulners.com/cve/CVE-2008-3963
|           PRION:CVE-2023-22053   3.6   https://vulners.com/prion/PRION:CVE-
2023-22053
|           CVE-2010-1626    3.6   https://vulners.com/cve/CVE-2010-1626
|           PRION:CVE-2023-22007   3.3   https://vulners.com/prion/PRION:CVE-
2023-22007
|           CVE-2012-0114    3.0   https://vulners.com/cve/CVE-2012-0114
|           PRION:CVE-2022-21444   2.1   https://vulners.com/prion/PRION:CVE-
2022-21444
```

```
|_          CVE-2012-0075     1.7   https://vulners.com/cve/CVE-2012-0075
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
|     IDs:  CVE:CVE-2004-2687
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|     IDs:  BID:70574  CVE:CVE-2014-3566
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.openssl.org/~bodo/ssl-poodle.pdf
|       http://www.openssl.org/news/secadv_20140605.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
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
|     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
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|           PRION:CVE-2023-26044    5.0   https://vulners.com/prion/PRION:CVE-
2023-26044
|_          PRION:CVE-2022-36032    5.0   https://vulners.com/prion/PRION:CVE-
2022-36032
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
37585/tcp open  mountd      1-3 (RPC #100005)
38770/tcp open  nlockmgr    1-4 (RPC #100021)
45139/tcp open  java-rmi    GNU Classpath grmiregistry
51705/tcp open  status      1 (RPC #100024)
```