Report of a Nessus scan

Nessus Security Scanner

February 23, 2003

Contents

1 10.163.156.10 **iv**
1.1 Open ports (TCP and UDP) iv
1.2 Details of the vulnerabilities v
1.2.1 Problems regarding : echo (7/tcp) v
1.2.2 Problems regarding : telnet (23/tcp) vi
1.2.3 Problems regarding : ssh (22/tcp) vii
1.2.4 Problems regarding : ftp (21/tcp) ix
1.2.5 Problems regarding : chargen (19/tcp) xi
1.2.6 Problems regarding : daytime (13/tcp) xii
1.2.7 Problems regarding : smtp (25/tcp) xii
1.2.8 Problems regarding : time (37/tcp) xv
1.2.9 Problems regarding : finger (79/tcp) xv
1.2.10 Problems regarding : sunrpc (111/tcp) xvii
1.2.11 Problems regarding : login (513/tcp) xvii
1.2.12 Problems regarding : exec (512/tcp) xvii
1.2.13 Problems regarding : printer (515/tcp) xviii
1.2.14 Problems regarding : shell (514/tcp) xviii
1.2.15 Problems regarding : uucp (540/tcp) xviii
1.2.16 Problems regarding : sometimes-rpc16 (32776/udp) xviii
1.2.17 Problems regarding : sometimes-rpc14 (32775/udp) xix
1.2.18 Problems regarding : sometimes-rpc10 (32773/udp) xix
1.2.19 Problems regarding : lockd (4045/udp) xx
1.2.20 Problems regarding : snmp (161/udp) xx
1.2.21 Problems regarding : sometimes-rpc22 (32779/udp) xxii
1.2.22 Problems regarding : general/tcp xxii
1.2.23 Problems regarding : sometimes-rpc18 (32777/udp) xxiii
1.2.24 Problems regarding : sometimes-rpc20 (32778/udp) xxiv
1.2.25 Problems regarding : dtspc (6112/tcp) xxiv
1.2.26 Problems regarding : sometimes-rpc13 (32775/tcp) xxv
1.2.27 Problems regarding : sometimes-rpc9 (32773/tcp) xxv
1.2.28 Problems regarding : sunrpc (111/udp) xxvi
1.2.29 Problems regarding : sometimes-rpc8 (32772/udp) xxvi
1.2.30 Problems regarding : sometimes-rpc5 (32771/tcp) xxvii
1.2.31 Problems regarding : sometimes-rpc12 (32774/udp) xxvii
1.2.32 Problems regarding : sometimes-rpc7 (32772/tcp) xxvii
1.2.33 Problems regarding : sometimes-rpc11 (32774/tcp) xxvii
1.2.34 Problems regarding : lockd (4045/tcp) xxviii
1.2.35 Problems regarding : sometimes-rpc24 (32780/udp) xxviii
1.2.36 Problems regarding : sometimes-rpc15 (32776/tcp) xxviii
1.2.37 Problems regarding : unknown (32785/udp) xxix
1.2.38 Problems regarding : sometimes-rpc19 (32778/tcp) xxix
1.2.39 Problems regarding : unknown (32788/udp) xxix
1.2.40 Problems regarding : sometimes-rpc21 (32779/tcp) xxix
1.2.41 Problems regarding : xdmcp (177/udp) xxx

1.2.42 Problems regarding : font-service (7100/tcp) xxx
1.2.43 Problems regarding : echo (7/udp) xxx
1.2.44 Problems regarding : daytime (13/udp) xxxi

2 10.163.156.9 xxxii
2.1 Open ports (TCP and UDP) xxxii
2.2 Details of the vulnerabilities xxxiii
2.2.1 Problems regarding : smtp (25/tcp) xxxiii
2.2.2 Problems regarding : ftp (21/tcp) xxxv
2.2.3 Problems regarding : chargen (19/tcp) xxxvi
2.2.4 Problems regarding : qotd (17/tcp) xxxvi
2.2.5 Problems regarding : daytime (13/tcp) xxxvii
2.2.6 Problems regarding : echo (7/tcp) xxxvii
2.2.7 Problems regarding : http (80/tcp) xxxviii
2.2.8 Problems regarding : nntp (119/tcp) xli
2.2.9 Problems regarding : loc-srv (135/tcp) xlii
2.2.10 Problems regarding : netbios-ssn (139/tcp) xlviii
2.2.11 Problems regarding : https (443/tcp) xlix
2.2.12 Problems regarding : printer (515/tcp) l
2.2.13 Problems regarding : afpovertcp (548/tcp) l
2.2.14 Problems regarding : nntps (563/tcp) l
2.2.15 Problems regarding : blackjack (1025/tcp) l
2.2.16 Problems regarding : unknown (1028/tcp) li
2.2.17 Problems regarding : unknown (1035/tcp) li
2.2.18 Problems regarding : netinfo (1033/tcp) lii
2.2.19 Problems regarding : iad2 (1031/tcp) lii
2.2.20 Problems regarding : ms-sql-s (1433/tcp) liii
2.2.21 Problems regarding : ms-sql-m (1434/udp) liii
2.2.22 Problems regarding : general/tcp liii
2.2.23 Problems regarding : general/udp liv
2.2.24 Problems regarding : snmp (161/udp) liv
2.2.25 Problems regarding : netbios-ns (137/udp) lvi
2.2.26 Problems regarding : echo (7/udp) lvii
2.2.27 Problems regarding : ms-term-serv (3389/tcp) lvii
2.2.28 Problems regarding : daytime (13/udp) lvii
2.2.29 Problems regarding : qotd (17/udp) lviii
2.2.30 Problems regarding : iad1 (1030/udp) lviii
2.2.31 Problems regarding : chargen (19/udp) lix
2.2.32 Problems regarding : iad3 (1032/udp) lix

3 10.163.155.4 lxi
3.1 Open ports (TCP and UDP) lxi
3.2 Details of the vulnerabilities lxi
3.2.1 Problems regarding : ftp (21/tcp) lxi
3.2.2 Problems regarding : http (80/tcp) lxi
3.2.3 Problems regarding : loc-srv (135/tcp) lxii

3.2.4 Problems regarding : netbios-ssn (139/tcp) lxiii
3.2.5 Problems regarding : blackjack (1025/tcp) lxv
3.2.6 Problems regarding : general/tcp lxv
3.2.7 Problems regarding : general/udp lxvi
3.2.8 Problems regarding : netbios-ns (137/udp) lxvi
3.2.9 Problems regarding : unknown (1026/udp) lxvi

4 10.163.155.3 lxvii
4.1 Open ports (TCP and UDP) lxvii
4.2 Details of the vulnerabilities lxvii
4.2.1 Problems regarding : ftp (21/tcp) lxvii
4.2.2 Problems regarding : http (80/tcp) lxviii
4.2.3 Problems regarding : svrloc (427/tcp) lxx
4.2.4 Problems regarding : afpovertcp (548/tcp) lxx
4.2.5 Problems regarding : general/tcp lxx
4.2.6 Problems regarding : general/udp lxx
4.2.7 Problems regarding : x11 (6000/tcp) lxxi

5 10.163.155.2 lxxii
5.1 Open ports (TCP and UDP) lxxii
5.2 Details of the vulnerabilities lxxii
5.2.1 Problems regarding : ftp (21/tcp) lxxii
5.2.2 Problems regarding : http (80/tcp) lxxii
5.2.3 Problems regarding : snmp (161/udp) lxxiv
5.2.4 Problems regarding : general/tcp lxxv

6 10.163.156.1 lxxvi
6.1 Open ports (TCP and UDP) lxxvi
6.2 Details of the vulnerabilities lxxvi
6.2.1 Problems regarding : ssh (22/tcp) lxxvi
6.2.2 Problems regarding : ftp (21/tcp) lxxvii
6.2.3 Problems regarding : http (80/tcp) lxxvii
6.2.4 Problems regarding : general/tcp lxxvii
6.2.5 Problems regarding : general/udp lxxvii

7 10.163.155.6 lxxix
7.1 Open ports (TCP and UDP) lxxix
7.2 Details of the vulnerabilities lxxix
7.2.1 Problems regarding : ftp (21/tcp) lxxix
7.2.2 Problems regarding : http (80/tcp) lxxix
7.2.3 Problems regarding : loc-srv (135/tcp) lxxxi
7.2.4 Problems regarding : netbios-ssn (139/tcp) lxxxv
7.2.5 Problems regarding : blackjack (1025/tcp) lxxxvi
7.2.6 Problems regarding : general/tcp lxxxvii
7.2.7 Problems regarding : general/udp lxxxvii
7.2.8 Problems regarding : netbios-ns (137/udp) lxxxvii

7.2.9 Problems regarding : ms-term-serv (3389/tcp) lxxxviii
7.2.10 Problems regarding : unknown (1027/udp) lxxxviii

8 10.163.156.205 lxxxix
8.1 Open ports (TCP and UDP) lxxxix
8.2 Details of the vulnerabilities xc
8.2.1 Problems regarding : rtmp (1/tcp) xc
8.2.2 Problems regarding : telnet (23/tcp) xc
8.2.3 Problems regarding : ftp (21/tcp) xci
8.2.4 Problems regarding : chargen (19/tcp) xcii
8.2.5 Problems regarding : daytime (13/tcp) xcii
8.2.6 Problems regarding : echo (7/tcp) xciii
8.2.7 Problems regarding : smtp (25/tcp) xciii
8.2.8 Problems regarding : time (37/tcp) xcvi
8.2.9 Problems regarding : finger (79/tcp) xcvi
8.2.10 Problems regarding : sunrpc (111/tcp) xcvi
8.2.11 Problems regarding : exec (512/tcp) xcvii
8.2.12 Problems regarding : printer (515/tcp) xcvii
8.2.13 Problems regarding : shell (514/tcp) xcvii
8.2.14 Problems regarding : login (513/tcp) xcvii
8.2.15 Problems regarding : ldaps (636/tcp) xcviii
8.2.16 Problems regarding : blackjack (1025/tcp) xcviii
8.2.17 Problems regarding : LSA-or-nterm (1026/tcp) xcviii
8.2.18 Problems regarding : kdm (1024/tcp) xcix
8.2.19 Problems regarding : esl-lm (1455/tcp) c
8.2.20 Problems regarding : general/tcp c
8.2.21 Problems regarding : blackjack (1025/udp) c
8.2.22 Problems regarding : sunrpc (111/udp) ci
8.2.23 Problems regarding : general/udp ci
8.2.24 Problems regarding : xdmcp (177/udp) ci
8.2.25 Problems regarding : echo (7/udp) cii
8.2.26 Problems regarding : daytime (13/udp) cii

9 10.163.156.16 ciii
9.1 Open ports (TCP and UDP) ciii
9.2 Details of the vulnerabilities civ
9.2.1 Problems regarding : smtp (25/tcp) civ
9.2.2 Problems regarding : telnet (23/tcp) cviii
9.2.3 Problems regarding : ftp (21/tcp) cix
9.2.4 Problems regarding : chargen (19/tcp) cx
9.2.5 Problems regarding : daytime (13/tcp) cxi
9.2.6 Problems regarding : echo (7/tcp) cxi
9.2.7 Problems regarding : time (37/tcp) cxii
9.2.8 Problems regarding : finger (79/tcp) cxii
9.2.9 Problems regarding : sunrpc (111/tcp) cxiii
9.2.10 Problems regarding : login (513/tcp) cxiii

9.2.11 Problems regarding : exec (512/tcp) cxiv
9.2.12 Problems regarding : printer (515/tcp) cxiv
9.2.13 Problems regarding : shell (514/tcp) cxiv
9.2.14 Problems regarding : uucp (540/tcp) cxiv
9.2.15 Problems regarding : general/tcp cxv
9.2.16 Problems regarding : dtspc (6112/tcp) cxv
9.2.17 Problems regarding : sunrpc (111/udp) cxv
9.2.18 Problems regarding : sometimes-rpc8 (32772/udp) cxvi
9.2.19 Problems regarding : sometimes-rpc21 (32779/tcp) cxvi
9.2.20 Problems regarding : sometimes-rpc12 (32774/udp) cxvi
9.2.21 Problems regarding : sometimes-rpc14 (32775/udp) cxvi
9.2.22 Problems regarding : sometimes-rpc10 (32773/udp) cxvi
9.2.23 Problems regarding : unknown (32790/tcp) cxvi
9.2.24 Problems regarding : sometimes-rpc16 (32776/udp) cxvii
9.2.25 Problems regarding : unknown (32791/tcp) cxvii
9.2.26 Problems regarding : sometimes-rpc18 (32777/udp) cxvii
9.2.27 Problems regarding : sometimes-rpc20 (32778/udp) cxvii
9.2.28 Problems regarding : sometimes-rpc22 (32779/udp) cxvii
9.2.29 Problems regarding : lockd (4045/udp) cxviii
9.2.30 Problems regarding : unknown (32792/tcp) cxviii
9.2.31 Problems regarding : unknown (32793/tcp) cxviii
9.2.32 Problems regarding : sometimes-rpc24 (32780/udp) cxviii
9.2.33 Problems regarding : unknown (32794/tcp) cxviii
9.2.34 Problems regarding : lockd (4045/tcp) cxix
9.2.35 Problems regarding : unknown (32812/udp) cxix
9.2.36 Problems regarding : unknown (32795/tcp) cxix
9.2.37 Problems regarding : unknown (32813/udp) cxix
9.2.38 Problems regarding : unknown (32796/tcp) cxix
9.2.39 Problems regarding : snmp (161/udp) cxx
9.2.40 Problems regarding : xdmcp (177/udp) cxx
9.2.41 Problems regarding : general/udp cxx
9.2.42 Problems regarding : font-service (7100/tcp) cxxi
9.2.43 Problems regarding : echo (7/udp) cxxi
9.2.44 Problems regarding : daytime (13/udp) cxxi

Introduction

In this test, Nessus has tested 9 hosts and found **54 severe security holes**, as well as 113 security warnings and 303 notes.These problems can easily be used to break into your network. You should have a close look at them and correct them as soon as possible.
Note that there is a big number of problems for a single network of this size.
We strongly suggest that you correct them as soon as you can, although we know it is not always possible.
We recommand that you take a closer look at `10.163.156.10`, as it is the host that is the most likely to be the entry point of any cracker. On the overall, Nessus has given to the security of this network the mark E because of the number of vulnerabilities found. A script kid should be able to break into your network rather easily.
There is room for improvement, and **we strongly suggest that you take the appropriate measures to solve these problems *as soon as possible*** If you were considering hiring some security consultant to determine the security of your network, we strongly suggest you do so, because this should save your network.

1 10.163.156.10

1.1 Open ports (TCP and UDP)

`10.163.156.10` has the following ports that are open :

- `echo (7/tcp)`
- `telnet (23/tcp)`
- `ssh (22/tcp)`
- `ftp (21/tcp)`
- `chargen (19/tcp)`
- `daytime (13/tcp)`
- `discard (9/tcp)`
- `smtp (25/tcp)`
- `time (37/tcp)`
- `finger (79/tcp)`
- `sunrpc (111/tcp)`
- `login (513/tcp)`
- `exec (512/tcp)`
- `printer (515/tcp)`
- `shell (514/tcp)`
- `uucp (540/tcp)`
- `sometimes-rpc16 (32776/udp)`
- `sometimes-rpc14 (32775/udp)`
- `sometimes-rpc10 (32773/udp)`
- `lockd (4045/udp)`
- `snmp (161/udp)`
- `sometimes-rpc22 (32779/udp)`
- `general/tcp`
- `sometimes-rpc18 (32777/udp)`
- `sometimes-rpc20 (32778/udp)`

- dtspc (6112/tcp)
- sometimes-rpc13 (32775/tcp)
- sometimes-rpc9 (32773/tcp)
- sunrpc (111/udp)
- sometimes-rpc8 (32772/udp)
- sometimes-rpc5 (32771/tcp)
- sometimes-rpc12 (32774/udp)
- sometimes-rpc7 (32772/tcp)
- sometimes-rpc11 (32774/tcp)
- lockd (4045/tcp)
- sometimes-rpc24 (32780/udp)
- sometimes-rpc15 (32776/tcp)
- unknown (32785/udp)
- sometimes-rpc19 (32778/tcp)
- unknown (32788/udp)
- sometimes-rpc21 (32779/tcp)
- xdmcp (177/udp)
- font-service (7100/tcp)
- echo (7/udp)
- daytime (13/udp)

You should disable the services that you do not use, as they are potential security flaws.

1.2 Details of the vulnerabilities

1.2.1 Problems regarding : echo (7/tcp)

Security warnings :

- The 'echo' port is open. This port is
  not of any use nowadays, and may be a source of problems,
  since it can be used along with other ports to perform a denial
  of service. You should really disable this service.

  Risk factor : Low

  Solution : comment out 'echo' in /etc/inetd.conf
  CVE : CVE-1999-0103

Security note :

- An echo server is running on this port

1.2.2 Problems regarding : telnet (23/tcp)

Security holes :

- The Telnet server does not return an expected number of replies
  when it receives a long sequence of 'Are You There' commands.
  This probably means it overflows one of its internal buffers and
  crashes. It is likely an attacker could abuse this bug to gain
  control over the remote host's superuser.

  For more information, see:
  http://www.team-teso.net/advisories/teso-advisory-011.tar.gz

  Solution: Comment out the 'telnet' line in /etc/inetd.conf.
  Risk factor : High
  CVE : CVE-2001-0554
  BID : 3064

- It is possible to reboot the remote host by connecting to the telnet
  port and providing a bad username and password.

  This vulnerability is documented as Cisco Bug ID CSCdw81244.

  An attacker may use this flaw to prevent your access point from
  working properly.

  Solution : http://www.cisco.com/warp/public/707/Aironet-Telnet.shtml
  Risk factor : High
  CVE : CAN-2002-0545
  BID : 4461

Security warnings :

- The Telnet service is running.
  This service is dangerous in the sense that
  it is not ciphered - that is, everyone can sniff
  the data that passes between the telnet client
  and the telnet server. This includes logins
  and passwords.

  You should disable this service and use OpenSSH instead.
  (www.openssh.com)

  Solution : Comment out the 'telnet' line in /etc/inetd.conf.

  Risk factor : Low
  CVE : CAN-1999-0619

Security note :

- A telnet server seems to be running on this port
- Remote telnet banner :

  SunOS 5.8

1.2.3 Problems regarding : ssh (22/tcp)

Security holes :

- You are running a version of OpenSSH which is older than 3.4

  There is a flaw in this version that can be exploited remotely to
  give an attacker a shell on this host.

  Note that several distribution patched this hole without changing
  the version number of OpenSSH. Since Nessus solely relied on the
  banner of the remote SSH server to perform this check, this might
  be a false positive.

  If you are running a RedHat host, make sure that the command :
            rpm -q openssh-server

  Returns :

```
 openssh-server-3.1p1-6


Solution : Upgrade to OpenSSH 3.4 or contact your vendor for a patch
Risk factor : High
CVE : CAN-2002-0639, CAN-2002-0640
BID : 5093
```

- ```
  You are running a version of OpenSSH which is older than 3.0.2.

  Versions prior than 3.0.2 are vulnerable to an environment
  variables export that can allow a local user to execute
  command with root privileges.
  This problem affect only versions prior than 3.0.2, and when
  the UseLogin feature is enabled (usually disabled by default)

  Solution : Upgrade to OpenSSH 3.0.2 or apply the patch for prior
  versions. (Available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH)

  Risk factor : High (If UseLogin is enabled, and locally)
  CVE : CVE-2001-0872
  BID : 3614
  ```

- ```
  You are running a version of OpenSSH which is older than 3.0.1.

  Versions older than 3.0.1 are vulnerable to a flaw in which
  an attacker may authenticate, provided that Kerberos V support
  has been enabled (which is not the case by default).
  It is also vulnerable as an excessive memory clearing bug,
  believed to be unexploitable.

  *** You may ignore this warning if this host is not using
  *** Kerberos V

  Solution : Upgrade to OpenSSH 3.0.1
  Risk factor : Low (if you are not using Kerberos) or High (if kerberos
   is enabled)
  CVE : CVE-2002-0083
  BID : 3560, 4560, 4241
  ```

- ```
  You are running a version of OpenSSH older than OpenSSH 3.2.1

  A buffer overflow exists in the daemon if AFS is enabled on
  your system, or if the options KerberosTgtPassing or
  AFSTokenPassing are enabled.  Even in this scenario, the
  vulnerability may be avoided by enabling UsePrivilegeSeparation.
  ```
  ```

```
Versions prior to 2.9.9 are vulnerable to a remote root
exploit. Versions prior to 3.2.1 are vulnerable to a local
root exploit.

Solution :
Upgrade to the latest version of OpenSSH

Risk factor : High
CVE : CAN-2002-0575
BID : 4560
```

Security warnings :

- ```
  The remote SSH daemon supports connections made
  using the version 1.33 and/or 1.5 of the SSH protocol.

  These protocols are not completely cryptographically
  safe so they should not be used.

  Solution :
   If you use OpenSSH, set the option 'Protocol' to '2'
   If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

  Risk factor : Low
  ```

Security note :

- ```
  An ssh server is running on this port
  ```
- ```
  The remote SSH daemon supports the following versions of the
  SSH protocol :

    . 1.33
    . 1.5
    . 1.99
    . 2.0
  ```
- ```
  Remote SSH version : SSH-1.99-OpenSSH_2.3.0p1
  ```

1.2.4 Problems regarding : ftp (21/tcp)

Security holes :

- The remote FTP server seems to be vulnerable to an exhaustion attack which may makes it consume all available memory on the remote host when it receives the command :

  NLST /../*/../*/../*/../*/../*/../*/../*/../*/../*/../

  Solution : upgrade to ProFTPd 1.2.2 if the remote server is proftpd, or contact your vendor for a patch.

  Reference : http://online.securityfocus.com/archive/1/169069

  Risk factor : High

- You seem to be running an FTP server which is vulnerable to the 'glob heap corruption'
  flaw, which is known to be exploitable remotely against this server. An attacker may use
  this flaw to execute arbitrary commands on this host.

  Solution: Upgrade your ftp server software to the latest version.
  Risk factor : High

  CVE : CVE-2001-0550
  BID : 3581

Security warnings :

- This FTP service allows anonymous logins. If you do not want to share data with anyone you do not know, then you should deactivate
  the anonymous account, since it can only cause troubles.
  Under most Unix system, doing :
  echo ftp >> /etc/ftpusers
  will correct this.

  Risk factor : Low
  CVE : CAN-1999-0497

- It is possible to gather the
  real path of the public area of the ftp server
  (like /home/ftp) by issuing the following
  command :

  CWD

```
This problem may help an attacker to find where
to put a .rhost file using other security
flaws.

Risk factor : Low
CVE : CVE-1999-0201
```

- ```
  The remote FTP server allows users to make any amount
  of PASV commands, thus blocking the free ports for legitimate services
   and
  consuming file descriptors.

  Solution: upgrade your FTP server to a version which solves this
   problem.

  Risk factor : Medium
  CVE : CVE-1999-0079
  BID : 271
  ```

Security note :

- ```
  An FTP server is running on this port.
  Here is its banner :
  220 unknown FTP server (SunOS 5.8) ready.
  ```
- ```
  Remote FTP server banner :
  220 unknown FTP server (SunOS 5.8) ready.
  ```

1.2.5 Problems regarding : chargen (19/tcp)

Security warnings :

- ```
  The chargen service is running.
  The 'chargen' service should only be enabled when testing the machine.


  When contacted, chargen responds with some random characters
   (something
  like all the characters in the alphabet in a row). When contacted via
   UDP, it
  will respond with a single UDP packet. When contacted via TCP, it will

  continue spewing characters until the client closes the connection.

  An easy attack is 'pingpong' in which an attacker spoofs a packet
   between two
  ```

```
machines running chargen. This will cause them to spew characters at
 each
other, slowing the machines down and saturating the network.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103
```

Security note :

- Chargen is running on this port

1.2.6 Problems regarding : daytime (13/tcp)

Security warnings :

- The daytime service is running.
  The date format issued by this service
  may sometimes help an attacker to guess
  the operating system type.

  In addition to that, when the UDP version of
  daytime is running, an attacker may link it
  to the echo port using spoofing, thus creating
  a possible denial of service.

  Solution : disable this service in /etc/inetd.conf.

  Risk factor : Low
  CVE : CVE-1999-0103

1.2.7 Problems regarding : smtp (25/tcp)

Security holes :

- The remote sendmail server, according to its version number,
  may be vulnerable to the -bt overflow attack which
  allows any local user to execute arbitrary commands as root.

  Solution : upgrade to the latest version of Sendmail
  Risk factor : High
  Note : This vulnerability is _local_ only

- The remote sendmail server, according to its version number, may be vulnerable to a buffer overflow its DNS handling code.

  The owner of a malicious name server could use this flaw to execute arbitrary code on this host.

  Solution : Upgrade to Sendmail 8.12.5
  Risk factor : High
  CVE : CAN-2002-0906
  BID : 5122

Security warnings :

- The remote SMTP server answers to the EXPN and/or VRFY commands.

  The EXPN command can be used to find the delivery address of mail aliases, or even the full name of the recipients, and the VRFY command may be used to check the validity of an account.

  Your mailer should not allow remote users to use any of these commands, because it gives them too much information.

  Solution : if you are using Sendmail, add the option
  O PrivacyOptions=goaway
  in /etc/sendmail.cf.

  Risk factor : Low
  CVE : CAN-1999-0531

- The remote SMTP server is vulnerable to a redirection attack. That is, if a mail is sent to :

  user@hostname1@victim

  Then the remote SMTP server (victim) will happily send the mail to :
  user@hostname1

Using this flaw, an attacker may route a message
through your firewall, in order to exploit other
SMTP servers that can not be reached from the
outside.

*** THIS WARNING MAY BE A FALSE POSITIVE, SINCE
SOME SMTP SERVERS LIKE POSTFIX WILL NOT
COMPLAIN BUT DROP THIS MESSAGE ***

Solution : if you are using sendmail, then at the top
of ruleset 98, in /etc/sendmail.cf, insert :
R$*@$*@$* $#error $@ 5.7.1 $: '551 Sorry, no redirections.'

Risk factor : Low

- The remote SMTP server allows the relaying. This means that
it allows spammers to use your mail server to send their mails to
the world, thus wasting your network bandwidth.

Risk factor : Low/Medium

Solution : configure your SMTP server so that it can't be used as a
relay
any more.
CVE : CAN-1999-0512

- The remote SMTP server allows anyone to
use it as a mail relay, provided that the source address
is set to '<>'.
This problem allows any spammer to use your mail server
to spam the world, thus blacklisting your mailserver, and
using your network resources.

Risk factor : Medium

Solution : reconfigure this server properly
CVE : CVE-1999-0819

- The remote sendmail server, according to its version number,
might be vulnerable to a queue destruction when a local user
runs
sendmail -q -h1000

If you system does not allow users to process the queue (which
is the default), you are not vulnerable.

```
Solution : upgrade to the latest version of Sendmail or
do not allow users to process the queue (RestrictQRun option)
Risk factor : Low
Note : This vulnerability is _local_ only
CVE : CAN-2001-0714
BID : 3378
```

- ```
  According to the version number of the remote mail server,
  a local user may be able to obtain the complete mail configuration
  and other interesting information about the mail queue even if
  he is not allowed to access those information directly, by running
   sendmail -q -d0-nnnn.xxx
  where nnnn & xxx are debugging levels.

  If users are not allowed to process the queue (which is the default)
  then you are not vulnerable.

  Solution : upgrade to the latest version of Sendmail or
  do not allow users to process the queue (RestrictQRun option)
  Risk factor : Very low / none
  Note : This vulnerability is _local_ only
  CVE : CAN-2001-0715
  BID : 3898
  ```

Security note :

- ```
  An SMTP server is running on this port
  Here is its banner :
  220 sparky.fr.nessus.org ESMTP Sendmail 8.9.3+Sun/8.9.3; Fri, 21 Feb
   2003 15:53:28 GMT
  ```
- ```
  Remote SMTP server banner :
  220 sparky.fr.nessus.org ESMTP Sendmail 8.9.3+Sun/8.9.3; Fri, 21 Feb
   2003 15:54:20 GMT
  ```

1.2.8 Problems regarding : time (37/tcp)

Security note :

- ```
  A time server seems to be running on this port
  ```

1.2.9 Problems regarding : finger (79/tcp)

Security warnings :

- The 'finger' service provides useful information
  to attackers, since it allow them to gain usernames, check if a
   machine
  is being used, and so on...

  Risk factor : Low

  Solution : comment out the 'finger' line in /etc/inetd.conf
  CVE : CVE-1999-0612

- The remote finger daemon accepts
  to redirect requests. That is, users can perform
  requests like :
    finger user@host@victim

  This allows an attacker to use your computer
  as a relay to gather information on another
  network, making the other network think you
  are making the requests.

  Solution: disable your finger daemon (comment out
  the finger line in /etc/inetd.conf) or
  install a more secure one.

  Risk factor : Low
  CVE : CAN-1999-0105

- There is a bug in the finger service
  which will make it display the list of the accounts that
  have never been used, when anyone issues the request :

    finger 'a b c d e f g h'@target

  This list will help an attacker to guess the operating
  system type. It will also tell him which accounts have
  never been used, which will often make him focus his
  attacks on these accounts.

  Solution : disable the finger service in /etc/inetd.conf, or
  apply the patches from Sun.

  Risk factor : Medium
  BID : 3457

Security note :

- A finger server seems to be running on this port

1.2.10 Problems regarding : sunrpc (111/tcp)

Security note :

- RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port
- RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port
- RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port

1.2.11 Problems regarding : login (513/tcp)

Security warnings :

- The rlogin service is running.
  This service is dangerous in the sense that
  it is not ciphered - that is, everyone can sniff
  the data that passes between the rlogin client
  and the rlogin server. This includes logins
  and passwords.

  You should disable this service and use openssh instead
  (www.openssh.com)

  Solution : Comment out the 'rlogin' line in /etc/inetd.conf.

  Risk factor : Low
  CVE : CAN-1999-0651

1.2.12 Problems regarding : exec (512/tcp)

Security warnings :

- The rexecd service is open.
  Because rexecd does not provide any good
  means of authentication, it can be
  used by an attacker to scan a third party
  host, giving you troubles or bypassing
  your firewall.

  Solution : comment out the 'exec' line
  in /etc/inetd.conf.

```
Risk factor : Medium
CVE : CAN-1999-0618
```

1.2.13 Problems regarding : printer (515/tcp)

Security note :

- A LPD server seems to be running on this port

1.2.14 Problems regarding : shell (514/tcp)

Security warnings :

- The rsh service is running.
  This service is dangerous in the sense that
  it is not ciphered - that is, everyone can sniff
  the data that passes between the rsh client
  and the rsh server. This includes logins
  and passwords.

  You should disable this service and use ssh instead.

  Solution : Comment out the 'rsh' line in /etc/inetd.conf.

  Risk factor : Low
  CVE : CAN-1999-0651

1.2.15 Problems regarding : uucp (540/tcp)

Security note :

- An UUCP server seems to be running on this port

1.2.16 Problems regarding : sometimes-rpc16 (32776/udp)

Security warnings :

- The sprayd RPC service is running.
  If you do not use this service, then
  disable it as it may become a security
  threat in the future, if a vulnerability
  is discovered.

```
Risk factor : Low
CVE : CAN-1999-0613
```

Security note :

- RPC program #100012 version 1 'sprayd' (spray) is running on this port

1.2.17 Problems regarding : sometimes-rpc14 (32775/udp)

Security warnings :

- The rusersd RPC service is running.
  It provides an attacker interesting
  information such as how often the
  system is being used, the names of
  the users, and so on.

  It usually not a good idea to leave this
  service open.

  Risk factor : Low
  CVE : CVE-1999-0626

Security note :

- RPC program #100002 version 2 'rusersd' (rusers) is running on this port
- RPC program #100002 version 3 'rusersd' (rusers) is running on this port

1.2.18 Problems regarding : sometimes-rpc10 (32773/udp)

Security holes :

- The sadmin RPC service is running.
  There is a bug in Solaris versions of
  this service that allow an intruder to
  execute arbitrary commands on your system.

  Solution : disable this service
  Risk factor : High
  CVE : CVE-1999-0977
  BID : 866

Security note :

- RPC program #100232 version 10 'sadmind' is running on this port

1.2.19 Problems regarding : lockd (4045/udp)

Security warnings :

- The nlockmgr RPC service is running.
  If you do not use this service, then
  disable it as it may become a security
  threat in the future, if a vulnerability
  is discovered.

  Risk factor : Low
  CVE : CVE-2000-0508
  BID : 1372

Security note :

- RPC program #100021 version 1 'nlockmgr' is running on this port
- RPC program #100021 version 2 'nlockmgr' is running on this port
- RPC program #100021 version 3 'nlockmgr' is running on this port
- RPC program #100021 version 4 'nlockmgr' is running on this port

1.2.20 Problems regarding : snmp (161/udp)

Security holes :

- The device answered to more than 4 community strings.
  This may be a false positive or a community-less SNMP server
  HP printers answer to all community strings.

  SNMP Agent responded as expected with community name: public
  SNMP Agent responded as expected with community name: private
  SNMP Agent responded as expected with community name: write
  SNMP Agent responded as expected with community name: all
  SNMP Agent responded as expected with community name: monitor
  SNMP Agent responded as expected with community name: agent
  SNMP Agent responded as expected with community name: manager
  SNMP Agent responded as expected with community name: OrigEquipMfr
  SNMP Agent responded as expected with community name: admin

```
SNMP Agent responded as expected with community name: default
SNMP Agent responded as expected with community name: password
SNMP Agent responded as expected with community name: tivoli
SNMP Agent responded as expected with community name: openview
SNMP Agent responded as expected with community name: community
SNMP Agent responded as expected with community name: snmp
SNMP Agent responded as expected with community name: snmpd
SNMP Agent responded as expected with community name: Secret C0de
SNMP Agent responded as expected with community name: security
SNMP Agent responded as expected with community name: all private
SNMP Agent responded as expected with community name: rmon
SNMP Agent responded as expected with community name: rmon_admin
SNMP Agent responded as expected with community name: hp_admin
SNMP Agent responded as expected with community name: NoGaH$@!
SNMP Agent responded as expected with community name: 0392a0
SNMP Agent responded as expected with community name: xyzzy
SNMP Agent responded as expected with community name: agent_steal
SNMP Agent responded as expected with community name: freekevin
SNMP Agent responded as expected with community name: fubar
SNMP Agent responded as expected with community name: secret
SNMP Agent responded as expected with community name: cisco
SNMP Agent responded as expected with community name: apc
SNMP Agent responded as expected with community name: ANYCOM
SNMP Agent responded as expected with community name: cable-docsis
SNMP Agent responded as expected with community name: c
SNMP Agent responded as expected with community name: cc
SNMP Agent responded as expected with community name: Cisco router
SNMP Agent responded as expected with community name: cascade
SNMP Agent responded as expected with community name: comcomcom
CVE : CAN-1999-0186
BID : 177
```

- ```
  It was possible to disable the remote SNMP daemon by sending
  a malformed packet advertising bogus length fields.

  An attacker may use this flaw to prevent you from using
  SNMP to administer your network (or use other flaws
  to execute arbitrary code with the privileges of the
  SNMP daemon)

  Solution : see www.cert.org/advisories/CA-2002-03.html
  Risk factor : High
  CVE : CAN-2002-0013
  ```

Security warnings :
  ```

- A SNMP server is running on this host

Security note :

- Using SNMP, we could determine that the remote operating system is : Sun SNMP Agent, Ultra-1

1.2.21 Problems regarding : sometimes-rpc22 (32779/udp)

Security holes :

- The cmsd RPC service is running.
  This service has a long history of
  security holes, so you should really
  know what you are doing if you decide
  to let it run.

  * NO SECURITY HOLE REGARDING THIS
    PROGRAM HAS BEEN TESTED, SO
    THIS MIGHT BE A FALSE POSITIVE *

  We suggest that you disable this
  service.

  Risk factor : High
  CVE : CVE-1999-0320, CVE-1999-0696
  BID : 428

Security note :

- RPC program #100068 version 2 is running on this port
- RPC program #100068 version 3 is running on this port
- RPC program #100068 version 4 is running on this port
- RPC program #100068 version 5 is running on this port

1.2.22 Problems regarding : general/tcp

Security note :

- QueSO has found out that the remote host OS is
  * Standard: Solaris 2.x, Linux 2.1.???, Linux 2.2, MacOS

  CVE : CAN-1999-0454

1.2.23 Problems regarding : sometimes-rpc18 (32777/udp)

Security holes :

- The rpc.walld RPC service is running.
  Some versions of this server allow an attacker to gain
  root access remotely, by consuming the resources of the
  remote host then sending a specially formed packet with
  format strings to this host.

  Solaris 2.5.1, 2.6, 7 and 8 are vulnerable to this
  issue. Other operating systems might be affected as well.

  *** Nessus did not check for this vulnerability,
  *** so this might be a false positive

  Solution : Deactivate this service.
  Risk factor : High
  CVE : CAN-2002-0573
  BID : 4639

Security warnings :

- The walld RPC service is running.
  It is usually used by the administrator
  to tell something to the users of a
  network by making a message appear
  on their screen.

  Since this service lacks any kind
  of authentication, an attacker
  may use it to trick users into
  doing something (change their password,
  leave the console, or worse), by sending
  a message which would appear to be
  written by the administrator.

  It can also be used as a denial of service
  attack, by continually sending garbage
  to the users screens, preventing them
  from working properly.

  Solution : Deactivate this service.

  Risk factor : Medium
  CVE : CVE-1999-0181

Security note :

- RPC program #100008 version 1 'walld' (rwall shutdown) is running on this port

1.2.24 Problems regarding : sometimes-rpc20 (32778/udp)

Security warnings :

- The rstatd RPC service is running.
  It provides an attacker interesting
  information such as :

  - the CPU usage
  - the system uptime
  - its network usage
  - and more

  Usually, it is not a good idea to let this
  service open

  Risk factor : Low
  CVE : CAN-1999-0624

Security note :

- RPC program #100001 version 2 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
- RPC program #100001 version 3 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
- RPC program #100001 version 4 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port

1.2.25 Problems regarding : dtspc (6112/tcp)

Security holes :

- The 'dtspcd' service is running.

  Some versions of this daemon are vulnerable to
  a buffer overflow attack which allows an attacker
  to gain root privileges

```
*** This warning might be a false positive,
*** as no real overflow was performed

Solution : See http://www.cert.org/advisories/CA-2001-31.html
to determine if you are vulnerable or deactivate
this service (comment out the line 'dtspc' in /etc/inetd.conf)

Risk factor : High
CVE : CVE-2001-0803
BID : 3517
```

1.2.26 Problems regarding : sometimes-rpc13 (32775/tcp)

Security holes :

- ```
  The cachefsd RPC service is running.
  Some versions of this server allow an attacker to gain
  root access remotely, by consuming the resources of the
  remote host then sending a specially formed packet with
  format strings to this host.

  Solaris 2.5.1, 2.6, 7 and 8 are vulnerable to this
  issue. Other operating systems might be affected as well.

  *** Nessus did not check for this vulnerability,
  *** so this might be a false positive

  Solution : Deactivate this service - there is no patch at this time
      /etc/init.d/cachefs.daemon stop
  Risk factor : High
  CVE : CAN-2002-0084, CAN-2002-0033
  BID : 4631
  ```

Security note :

- ```
  RPC program #100235 version 1 is running on this port
  ```

1.2.27 Problems regarding : sometimes-rpc9 (32773/tcp)

Security holes :

- ```
  The tooltalk RPC service is running.

  There is a format string bug in many versions
  ```
  ```

```
of this service, which allow an attacker to gain
root remotely.

In addition to this, several versions of this service
allow remote attackers to overwrite abitrary memory
locations with a zero and possibly gain privileges
via a file descriptor argument in an AUTH_UNIX
procedure call which is used as a table index by the
_TT_ISCLOSE procedure.

*** This warning may be a false positive since the presence
*** of the bug was not verified locally.

Solution : Disable this service or patch it
See also : CERT Advisories CA-2001-27 and CA-2002-20

Risk factor : High
CVE : CAN-2002-0677, CVE-2001-0717, CVE-2002-0679
BID : 3382
```

Security note :

- `RPC program #100083 version 1 is running on this port`

1.2.28 Problems regarding : sunrpc (111/udp)

Security note :

- `RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port`
- `RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port`
- `RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port`

1.2.29 Problems regarding : sometimes-rpc8 (32772/udp)

Security note :

- `RPC program #100300 version 3 'nisd' (rpc.nisd) is running on this port`

1.2.30 Problems regarding : sometimes-rpc5 (32771/tcp)

Security note :

- RPC program #100300 version 3 'nisd' (rpc.nisd) is running on this port

1.2.31 Problems regarding : sometimes-rpc12 (32774/udp)

Security warnings :

- The rquotad RPC service is running.
  If you do not use this service, then
  disable it as it may become a security
  threat in the future, if a vulnerability
  is discovered.

  Risk factor : Low
  CVE : CAN-1999-0625

Security note :

- RPC program #100011 version 1 'rquotad' (rquotaprog quota rquota) is running on this port

1.2.32 Problems regarding : sometimes-rpc7 (32772/tcp)

Security note :

- RPC program #100002 version 2 'rusersd' (rusers) is running on this port
- RPC program #100002 version 3 'rusersd' (rusers) is running on this port

1.2.33 Problems regarding : sometimes-rpc11 (32774/tcp)

Security note :

- RPC program #100221 version 1 is running on this port

1.2.34 Problems regarding : lockd (4045/tcp)

Security note :

- RPC program #100021 version 1 'nlockmgr' is running on this port
- RPC program #100021 version 2 'nlockmgr' is running on this port
- RPC program #100021 version 3 'nlockmgr' is running on this port
- RPC program #100021 version 4 'nlockmgr' is running on this port

1.2.35 Problems regarding : sometimes-rpc24 (32780/udp)

Security warnings :

- The statd RPC service is running.
  This service has a long history of
  security holes, so you should really
  know what you are doing if you decide
  to let it run.

  * NO SECURITY HOLES REGARDING THIS
    PROGRAM HAVE BEEN TESTED, SO
    THIS MIGHT BE A FALSE POSITIVE *

  We suggest that you disable this
  service.

  Risk factor : High
  CVE : CVE-1999-0493
  BID : 450

Security note :

- RPC program #100024 version 1 'status' is running on this port
- RPC program #100133 version 1 is running on this port

1.2.36 Problems regarding : sometimes-rpc15 (32776/tcp)

Security note :

- RPC program #100024 version 1 'status' is running on this port
- RPC program #100133 version 1 is running on this port

1.2.37 Problems regarding : unknown (32785/udp)

Security note :

- RPC program #100249 version 1 is running on this port

1.2.38 Problems regarding : sometimes-rpc19 (32778/tcp)

Security holes :

- The remote RPC service 100249 (snmpXdmid) is vulnerable
  to a heap overflow which allows any user to obtain a root
  shell on this host.

  Solution : disable this service (/etc/init.d/init.dmi stop) if you
   don't use
  it, or contact Sun for a patch
  Risk factor : High
  CVE : CVE-2001-0236
  BID : 2417

Security note :

- RPC program #100249 version 1 is running on this port

1.2.39 Problems regarding : unknown (32788/udp)

Security note :

- RPC program #300598 version 1 is running on this port
- RPC program #805306368 version 1 is running on this port

1.2.40 Problems regarding : sometimes-rpc21 (32779/tcp)

Security note :

- RPC program #300598 version 1 is running on this port
- RPC program #805306368 version 1 is running on this port

1.2.41 Problems regarding : xdmcp (177/udp)

Security warnings :

- The remote host is running XDMCP.

  This protocol is used to provide X display connections for
  X terminals. XDMCP is completely insecure, since the traffic and
  passwords are not encrypted.

  An attacker may use this flaw to capture all the keystrokes of
  the users using this host through their X terminal, including
  passwords.

  Risk factor : Medium
  Solution : Disable XDMCP

1.2.42 Problems regarding : font-service (7100/tcp)

Security holes :

- The remote X Font Service (xfs) might be vulnerable to a buffer
  overflow.

  An attacker may use this flaw to gain root on this host
  remotely.

  *** Note that Nessus did not actually check for the flaw
  *** as details about this vulnerability are still unknown

  Solution : See CERT Advisory CA-2002-34
  Risk factor : High
  CVE : CAN-2002-1317

1.2.43 Problems regarding : echo (7/udp)

Security warnings :

- The 'echo' port is open. This port is
  not of any use nowadays, and may be a source of problems,
  since it can be used along with other ports to perform a denial
  of service. You should really disable this service.

  Risk factor : Low

```
Solution : comment out 'echo' in /etc/inetd.conf
CVE : CVE-1999-0103
```

1.2.44 Problems regarding : daytime (13/udp)

Security warnings :

- ```
  The daytime service is running.
  The date format issued by this service
  may sometimes help an attacker to guess
  the operating system type.

  In addition to that, when the UDP version of
  daytime is running, an attacker may link it
  to the echo port using spoofing, thus creating
  a possible denial of service.

  Solution : disable this service in /etc/inetd.conf.

  Risk factor : Low
  CVE : CVE-1999-0103
  ```
  ```

2 10.163.156.9

2.1 Open ports (TCP and UDP)

`10.163.156.9` has the following ports that are open :

- `smtp (25/tcp)`
- `ftp (21/tcp)`
- `chargen (19/tcp)`
- `qotd (17/tcp)`
- `daytime (13/tcp)`
- `discard (9/tcp)`
- `echo (7/tcp)`
- `nameserver (42/tcp)`
- `http (80/tcp)`
- `nntp (119/tcp)`
- `loc-srv (135/tcp)`
- `netbios-ssn (139/tcp)`
- `microsoft-ds (445/tcp)`
- `https (443/tcp)`
- `printer (515/tcp)`
- `afpovertcp (548/tcp)`
- `nntps (563/tcp)`
- `blackjack (1025/tcp)`
- `unknown (1028/tcp)`
- `unknown (1035/tcp)`
- `netinfo (1033/tcp)`
- `iad2 (1031/tcp)`
- `ms-sql-s (1433/tcp)`
- `ms-sql-m (1434/udp)`
- `general/tcp`

- general/udp
- snmp (161/udp)
- netbios-ns (137/udp)
- echo (7/udp)
- ms-term-serv (3389/tcp)
- daytime (13/udp)
- qotd (17/udp)
- iad1 (1030/udp)
- chargen (19/udp)
- iad3 (1032/udp)

You should disable the services that you do not use, as they are potential security flaws.

2.2 Details of the vulnerabilities

2.2.1 Problems regarding : smtp (25/tcp)

Security holes :

- The remote SMTP server did not complain when issued the command :
  MAIL FROM: root@this_host
  RCPT TO: /tmp/nessus_test

  This probably means that it is possible to send mail directly to files, which is a serious threat, since this allows anyone to overwrite any file on the remote server.

  *** This security hole might be a false positive, since
  *** some MTAs will not complain to this test, but instead
  *** just drop the message silently.
  *** Check for the presence of file 'nessus_test' in /tmp !

  Solution : upgrade your MTA or change it.

  Risk factor : High

- The remote SMTP server did not complain when issued the command :
  MAIL FROM: |testing

```
This probably means that it is possible to send mail
that will be bounced to a program, which is
a serious threat, since this allows anyone to execute
arbitrary commands on this host.

*** This security hole might be a false positive, since
*** some MTAs will not complain to this test, but instead
*** just drop the message silently

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CVE-1999-0203
BID : 2308
```

- ```
  The remote SMTP server did not complain when issued the
  command :
   MAIL FROM: root@this_host
   RCPT TO: |testing

  This probably means that it is possible to send mail directly
  to programs, which is a serious threat, since this allows
  anyone to execute arbitrary commands on this host.

  *** This security hole might be a false positive, since
  *** some MTAs will not complain to this test, but instead
  *** just drop the message silently.

  Solution : upgrade your MTA or change it.

  Risk factor : High
  CVE : CAN-1999-0163
  ```

Security note :

- ```
  An SMTP server is running on this port
  Here is its banner :
  220 gabbo Microsoft ESMTP MAIL Service, Version: 5.0.2195.5329 ready
   at  Fri, 21 Feb 2003 15:45:19 -0800
  ```
- ```
  Remote SMTP server banner :
  220 gabbo Microsoft ESMTP MAIL Service, Version: 5.0.2195.5329 ready
   at  Fri, 21 Feb 2003 15:48:26 -0800
  ```
  ```

- For some reason, we could not send the EICAR test string to this MTA

2.2.2 Problems regarding : ftp (21/tcp)

Security holes :

- The remote FTP server closes
  the connection when one of the commands is given
  a too long argument.

  This probably due to a buffer overflow, which
  allows anyone to execute arbitrary code
  on the remote host.

  This problem is threatening, because
  the attackers don't need an account
  to exploit this flaw.

  Solution : Upgrade your FTP server or change it
  Risk factor : High
  CVE : CAN-2000-0133
  BID : 961

Security warnings :

- This FTP service allows anonymous logins. If you do not
  want to share data with anyone you do not know, then you should
  deactivate
  the anonymous account, since it can only cause troubles.
  Under most Unix system, doing :
  echo ftp >> /etc/ftpusers
  will correct this.

  Risk factor : Low
  CVE : CAN-1999-0497

Security note :

- An FTP server is running on this port.
  Here is its banner :
  220 gabbo Microsoft FTP Service (Version 5.0).
- Remote FTP server banner :
  220 gabbo Microsoft FTP Service (Version 5.0).

2.2.3 Problems regarding : chargen (19/tp)

Security warnings :

- The chargen service is running.
  The 'chargen' service should only be enabled when testing the machine.

  When contacted, chargen responds with some random characters (something
  like all the characters in the alphabet in a row). When contacted via UDP, it
  will respond with a single UDP packet. When contacted via TCP, it will

  continue spewing characters until the client closes the connection.

  An easy attack is 'pingpong' in which an attacker spoofs a packet between two
  machines running chargen. This will cause them to spew characters at each
  other, slowing the machines down and saturating the network.

  Solution : disable this service in /etc/inetd.conf.

  Risk factor : Low
  CVE : CVE-1999-0103

Security note :

- Chargen is running on this port

2.2.4 Problems regarding : qotd (17/tcp)

Security warnings :

- The quote service (qotd) is running.

  A server listens for TCP connections on TCP port 17. Once a connection

  is established a short message is sent out the connection (and any
  data received is thrown away). The service closes the connection
  after sending the quote.

  Another quote of the day service is defined as a datagram based
  application on UDP. A server listens for UDP datagrams on UDP port

```
 17.
When a datagram is received, an answering datagram is sent containing
a quote (the data in the received datagram is ignored).


An easy attack is 'pingpong' which IP spoofs a packet between two
 machines
running qotd. This will cause them to spew characters at each other,
slowing the machines down and saturating the network.



Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103
```

Security note :

- `qotd seems to be running on this port`

2.2.5 Problems regarding : daytime (13/tcp)

Security warnings :

- ```
  The daytime service is running.
  The date format issued by this service
  may sometimes help an attacker to guess
  the operating system type.

  In addition to that, when the UDP version of
  daytime is running, an attacker may link it
  to the echo port using spoofing, thus creating
  a possible denial of service.

  Solution : disable this service in /etc/inetd.conf.

  Risk factor : Low
  CVE : CVE-1999-0103
  ```

2.2.6 Problems regarding : echo (7/tcp)

Security warnings :
  ```

- The 'echo' port is open. This port is
  not of any use nowadays, and may be a source of problems,
  since it can be used along with other ports to perform a denial
  of service. You should really disable this service.

  Risk factor : Low

  Solution : comment out 'echo' in /etc/inetd.conf
  CVE : CVE-1999-0103

Security note :

- An echo server is running on this port

2.2.7 Problems regarding : http (80/tcp)

Security holes :

- The IIS server appears to have the .HTR ISAPI filter mapped.

  At least one remote vulnerability has been discovered for the .HTR
  filter. This is detailed in Microsoft Advisory
  MS02-018, and gives remote SYSTEM level access to the web server.

  It is recommended that even if you have patched this vulnerability
   that
  you unmap the .HTR extension, and any other unused ISAPI extensions
  if they are not required for the operation of your site.

  Solution:
  To unmap the .HTR extension:
   1.Open Internet Services Manager.
   2.Right-click the Web server choose Properties from the context menu.

   3.Master Properties
   4.Select WWW Service -> Edit -> HomeDirectory -> Configuration
  and remove the reference to .htr from the list.

  Risk factor : High
  CVE : CAN-2002-0071
  BID : 4474

- The web server is probably susceptible to a common IIS vulnerability
   discovered by
  'Rain Forest Puppy'. This vulnerability enables an attacker to execute

```
 arbitrary
commands on the server with Administrator Privileges.

*** Nessus solely relied on the presence of the file /msadc/msadcs.dll
*** so this might be a false positive

See Microsoft security bulletin (MS99-025) for patch information.
Also, BUGTRAQ ID 529 on www.securityfocus.com (
 http://www.securityfocus.com/bid/529 )

Risk factor : High
CVE : CVE-1999-1011
BID : 529
```

Security warnings :

- The IIS server appears to have the .IDA ISAPI filter mapped.

  ```
  At least one remote vulnerability has been discovered for the .IDA
  (indexing service) filter. This is detailed in Microsoft Advisory
  MS01-033, and gives remote SYSTEM level access to the web server.

  It is recommended that even if you have patched this vulnerability
   that
  you unmap the .IDA extension, and any other unused ISAPI extensions
  if they are not required for the operation of your site.

  Solution:
  To unmap the .IDA extension:
   1.Open Internet Services Manager.
   2.Right-click the Web server choose Properties from the context menu.

   3.Master Properties
   4.Select WWW Service -> Edit -> HomeDirectory -> Configuration
  and remove the reference to .ida from the list.

  Risk factor : Medium
  CVE : CAN-2002-0071
  BID : 4474
  ```

- IIS 5 has support for the Internet Printing Protocol(IPP), which is enabled in a default install. The protocol is implemented in IIS5 as an ISAPI extension. At least one security problem (a buffer overflow) has been found with that extension in the past, so we recommend you disable it if you do not use this functionality.

Solution:
To unmap the .printer extension:
1.Open Internet Services Manager.
2.Right-click the Web server choose Properties from the context menu.

3.Master Properties
4.Select WWW Service -> Edit -> HomeDirectory -> Configuration
and remove the reference to .printer from the list.

Reference : http://online.securityfocus.com/archive/1/181109

Risk factor : Low

- Your webserver supports the TRACE and/or TRACK methods. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for 'Cross-Site-Tracing', when used in conjunction with various weaknesses in browsers.

  An attacker may use this flaw to trick your legitimate web users to give him their credentials.

  Solution: Disable these methods.

  If you are using Apache, add the following lines for each virtual host in your configuration file :

  ```
  RewriteEngine on
  RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
  RewriteRule .* - [F]
  ```

  If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy.

  See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
  http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html

  Risk factor : Medium

- It is possible to retrieve the listing of the remote directories accessible via HTTP, rather than their index.html, using the Index Server service which provides WebDav capabilities to this server.

  This problem allows an attacker to gain more knowledge about the remote host, and may make him aware of hidden HTML files.

  Solution : disable the Index Server service, or see http://www.microsoft.com/technet/support/kb.asp?ID=272079
  Risk factor : Low
  CVE : CVE-2000-0951
  BID : 1756

- The remote web server appears to be running with Frontpage extensions.

  You should double check the configuration since a lot of security problems have been found with FrontPage when the configuration file is not well set up.

  Risk factor : High if your configuration file is not well set up
  CVE : CAN-2000-0114

Security note :

- A web server is running on this port
- The remote web server type is :

  Microsoft-IIS/5.0

  Solution : You can use urlscan to change reported server for IIS.

- The following directories were discovered:
  /_vti_bin, /images
  The following directories require authentication:
  /printers

2.2.8 Problems regarding : nntp (119/tcp)

Security note :

- An NNTP server is running on this port
- Remote NNTP server version : 200 NNTP Service 5.00.0984 Version: 5.0.2195.5329 Posting Allowed
- This NNTP server allows unauthenticated connections
  For your information, we counted 4 newsgroups on this NNTP server:
  0 in the alt hierarchy, 0 in rec, 0 in biz, 0 in sci, 0 in soc, 0 in misc, 0 in news, 0 in comp, 0 in talk, 0 in humanities.
  Although this server says it allows posting, we were unable to send a message
  (posted in alt.test)

2.2.9 Problems regarding : loc-srv (135/tcp)

Security warnings :

- DCE services running on the remote can be enumerated
  by connecting on port 135 and doing the appropriate
  queries.

  An attacker may use this fact to gain more knowledge
  about the remote host.

  Solution : filter incoming traffic to this port.
  Risk factor : Low

Security note :

- A DCE service is listening on this host
  UUID: 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1
  Endpoint: ncacn_np:\\GABBO[\pipe\WinsPipe]
- A DCE service is listening on this host
  UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
  Endpoint: ncalrpc[LRPC00000238.00000001]
- A DCE service is listening on this host
  UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1

```
      Endpoint: ncalrpc[LRPC00000238.00000001]
```

- A DCE service is listening on this host
```
      UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
      Endpoint: ncalrpc[LRPC00000238.00000001]
```

- A DCE service is listening on this host
```
      UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
      Endpoint: ncalrpc[LRPC00000238.00000001]
```

- A DCE service is listening on this host
```
      UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
      Endpoint: ncalrpc[LRPC000004a0.00000001]
```

- A DCE service is listening on this host
```
      UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
      Endpoint: ncalrpc[LRPC000004a0.00000001]
```

- A DCE service is listening on this host
```
      UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
      Endpoint: ncalrpc[ntsvcs]
      Annotation: Messenger Service
```

- A DCE service is listening on this host
```
      UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
      Endpoint: ncacn_np:\\GABBO[\PIPE\ntsvcs]
      Annotation: Messenger Service
```

- A DCE service is listening on this host
```
      UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
      Endpoint: ncacn_np:\\GABBO[\PIPE\scerpc]
      Annotation: Messenger Service
```

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncalrpc[DNSResolver]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 82ad4280-036b-11cf-972c-00aa006887b0, version 2
  Endpoint: ncalrpc[OLEc]

- A DCE service is listening on this host
  UUID: 82ad4280-036b-11cf-972c-00aa006887b0, version 2
  Endpoint: ncalrpc[INETINFO_LPC]

- A DCE service is listening on this host
  UUID: 82ad4280-036b-11cf-972c-00aa006887b0, version 2
  Endpoint: ncacn_np:\\GABBO[\PIPE\INETINFO]

- A DCE service is listening on this host
  UUID: 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3
  Endpoint: ncalrpc[OLEc]

- A DCE service is listening on this host
  UUID: 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3
  Endpoint: ncalrpc[INETINFO_LPC]

- A DCE service is listening on this host
  UUID: 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3
  Endpoint: ncacn_np:\\GABBO[\PIPE\INETINFO]

- A DCE service is listening on this host
  UUID: 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3
  Endpoint: ncalrpc[SMTPSVC_LPC]

- A DCE service is listening on this host
  UUID: 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3
  Endpoint: ncacn_np:\\GABBO[\PIPE\SMTPSVC]

- A DCE service is listening on this host
  UUID: bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1
  Endpoint: ncalrpc[OLEc]

- A DCE service is listening on this host
  UUID: bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1
  Endpoint: ncalrpc[INETINFO_LPC]

- A DCE service is listening on this host
  UUID: bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1
  Endpoint: ncacn_np:\\GABBO[\PIPE\INETINFO]

- A DCE service is listening on this host
  UUID: bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1
  Endpoint: ncalrpc[SMTPSVC_LPC]

- A DCE service is listening on this host
  UUID: bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1
  Endpoint: ncacn_np:\\GABBO[\PIPE\SMTPSVC]

- A DCE service is listening on this host
  UUID: bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1
  Endpoint: ncacn_at_dspGABBO[DynEpt 590.1]

- A DCE service is listening on this host
  UUID: 4f82f460-0e21-11cf-909e-00805f48a135, version 4
  Endpoint: ncalrpc[OLEc]

- A DCE service is listening on this host
  UUID: 4f82f460-0e21-11cf-909e-00805f48a135, version 4
  Endpoint: ncalrpc[INETINFO_LPC]

- A DCE service is listening on this host
  UUID: 4f82f460-0e21-11cf-909e-00805f48a135, version 4
  Endpoint: ncacn_np:\\GABBO[\PIPE\INETINFO]

- A DCE service is listening on this host
  UUID: 4f82f460-0e21-11cf-909e-00805f48a135, version 4
  Endpoint: ncalrpc[SMTPSVC_LPC]

- A DCE service is listening on this host
  UUID: 4f82f460-0e21-11cf-909e-00805f48a135, version 4
  Endpoint: ncacn_np:\\GABBO[\PIPE\SMTPSVC]

- A DCE service is listening on this host
  UUID: 4f82f460-0e21-11cf-909e-00805f48a135, version 4
  Endpoint: ncacn_at_dspGABBO[DynEpt 590.1]

- A DCE service is listening on this host
  UUID: 4f82f460-0e21-11cf-909e-00805f48a135, version 4
  Endpoint: ncalrpc[NNTPSVC_LPC]

- A DCE service is listening on this host
  UUID: 4f82f460-0e21-11cf-909e-00805f48a135, version 4
  Endpoint: ncacn_np:\\GABBO[\PIPE\NNTPSVC]

- A DCE service is listening on this host
  UUID: 3d267954-eeb7-11d1-b94e-00c04fa3080d, version 1
  Endpoint: ncalrpc[LRPC00000504.00000001]

- A DCE service is listening on this host
  UUID: 3d267954-eeb7-11d1-b94e-00c04fa3080d, version 1
  Endpoint: ncacn_np:\\GABBO[\pipe\HydraLsPipe]

- A DCE service is listening on this host
  UUID: 12d4b7c8-77d5-11d1-8c24-00c04fa3080d, version 1
  Endpoint: ncalrpc[LRPC00000504.00000001]

- A DCE service is listening on this host
  UUID: 12d4b7c8-77d5-11d1-8c24-00c04fa3080d, version 1
  Endpoint: ncacn_np:\\GABBO[\pipe\HydraLsPipe]

- A DCE service is listening on this host
  UUID: 493c451c-155c-11d3-a314-00c04fb16103, version 1
  Endpoint: ncalrpc[LRPC00000504.00000001]

- A DCE service is listening on this host
  UUID: 493c451c-155c-11d3-a314-00c04fb16103, version 1
  Endpoint: ncacn_np:\\GABBO[\pipe\HydraLsPipe]

- A DCE service is listening on this host
  UUID: 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1
  Endpoint: ncalrpc[LRPC0000053c.00000001]

- A DCE service is listening on this host
  UUID: 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1
  Endpoint: ncacn_np:\\GABBO[\pipe\WinsPipe]

- A DCE service is listening on this host
  UUID: 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1
  Endpoint: ncalrpc[LRPC0000053c.00000001]

2.2.10 Problems regarding : netbios-ssn (139/tcp)

Security holes :

- . It was possible to log into the remote host using a NULL session.
  The concept of a NULL session is to provide a null username and
  a null password, which grants the user the 'guest' access

  To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and
  Q246261 (Windows 2000).
  Note that this won't completely disable null sessions, but will
  prevent them from connecting to IPC$
  Please see
   http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html

  . All the smb tests will be done as ''/''
  CVE : CVE-2000-0222
  BID : 990

Security warnings :

- The domain SID can be obtained remotely. Its value is :

  COOLDOMAIN : 0-0-0-0-0

  An attacker can use it to obtain the list of the local users of this
   host
  Solution : filter the ports 137 to 139 and 445
  Risk factor : Low

  CVE : CVE-2000-1200
  BID : 959

- The host SID can be obtained remotely. Its value is :

  GABBO : 5-21-842925246-1563985344-2146861395

  An attacker can use it to obtain the list of the local users of this
   host
  Solution : filter the ports 137 to 139 and 445
  Risk factor : Low

  CVE : CVE-2000-1200
  BID : 959

- The host SID could be used to enumerate the names of the local users

```
of this host.
(we only enumerated users name whose ID is between 1000 and 1020
for performance reasons)
This gives extra knowledge to an attacker, which
is not a good thing :
- Administrator account name : Administrator (id 500)
- Guest account name : Guest (id 501)
- TsInternetUser (id 1000)
- NetShowServices (id 1001)
- NetShow Administrators (id 1002)
- IUSR_GABBO (id 1003)
- IWAM_GABBO (id 1004)
- DHCP Users (id 1005)
- DHCP Administrators (id 1006)
- WINS Users (id 1007)

Risk factor : Medium
Solution : filter incoming connections this port

CVE : CVE-2000-1200
BID : 959
```

- Here is the browse list of the remote host :

```
GABBO -


This is potentially dangerous as this may help the attack
of a potential hacker by giving him extra targets to check for

Solution : filter incoming traffic to this port
Risk factor : Low
```

Security note :

- The remote native lan manager is : Windows 2000 LAN Manager
  The remote Operating System is : Windows 5.0
  The remote SMB Domain Name is : COOLDOMAIN

2.2.11 Problems regarding : https (443/tcp)

Security note :

- An unknown service is running on this port.
  It is usually reserved for HTTPS

2.2.12 Problems regarding : printer (515/tcp)

Security note :

- An unknown server is running on this port.
  If you know what it is, please send this banner to the Nessus team:
  00: 01 .

2.2.13 Problems regarding : afpovertcp (548/tcp)

Security note :

- This host is running an AppleShare File Services over IP.
  Machine type: Windows NT
  Server name: GABBO
  UAMs: ClearTxt Passwrd/Microsoft V1.0/MS2.0
  AFP Versions: AFPVersion 2.0/AFPVersion 2.1/AFP2.2

2.2.14 Problems regarding : nntps (563/tcp)

Security note :

- An unknown service is running on this port.
  It is usually reserved for NNTPS

2.2.15 Problems regarding : blackjack (1025/tcp)

Security note :

- A DCE service is listening on this port
  UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1025]

- A DCE service is listening on this port
  UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1

```
Endpoint: ncacn_ip_tcp:10.163.156.9[1025]
```

- A DCE service is listening on this port
  ```
  UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1025]
  ```

- A DCE service is listening on this port
  ```
  UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1025]
  ```

2.2.16 Problems regarding : unknown (1028/tcp)

Security note :

- A DCE service is listening on this port
  ```
  UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1028]
  ```

- A DCE service is listening on this port
  ```
  UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1028]
  ```

2.2.17 Problems regarding : unknown (1035/tcp)

Security note :

- A DCE service is listening on this port
  ```
  UUID: 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1035]
  ```

- A DCE service is listening on this port
  ```
  UUID: 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1035]
  ```

2.2.18 Problems regarding : netinfo (1033/tcp)

Security note :

- A DCE service is listening on this port
  UUID: 3d267954-eeb7-11d1-b94e-00c04fa3080d, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1033]

- A DCE service is listening on this port
  UUID: 12d4b7c8-77d5-11d1-8c24-00c04fa3080d, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1033]

- A DCE service is listening on this port
  UUID: 493c451c-155c-11d3-a314-00c04fb16103, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1033]

2.2.19 Problems regarding : iad2 (1031/tcp)

Security note :

- A DCE service is listening on this port
  UUID: 82ad4280-036b-11cf-972c-00aa006887b0, version 2
  Endpoint: ncacn_ip_tcp:10.163.156.9[1031]

- A DCE service is listening on this port
  UUID: 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3
  Endpoint: ncacn_ip_tcp:10.163.156.9[1031]

- A DCE service is listening on this port
  UUID: bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1
  Endpoint: ncacn_ip_tcp:10.163.156.9[1031]

- A DCE service is listening on this port
  UUID: 4f82f460-0e21-11cf-909e-00805f48a135, version 4
  Endpoint: ncacn_ip_tcp:10.163.156.9[1031]

2.2.20 Problems regarding : ms-sql-s (1433/tcp)

Security note :

- It is possible that Microsoft's SQL Server is installed on the remote computer.
  CVE : CAN-1999-0652

2.2.21 Problems regarding : ms-sql-m (1434/udp)

Security warnings :

- Here is the reply to a MS SQL 'ping' request : ServerName;GABBO;InstanceN
  *** Note that the version number might be inaccurate, as Microsoft
  *** decided to not increase it with new releases of its software
  It is suggested you filter incoming traffic to this port

2.2.22 Problems regarding : general/tcp

Security warnings :

- The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

  An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

  Solution : Contact your vendor for a patch
  Risk factor : Low

Security note :

- QueSO has found out that the remote host OS is
  * WindowsNT, Cisco 11.2(10a), HP/3000 DTC, BayStack Switch

  CVE : CAN-1999-0454

2.2.23 Problems regarding : general/udp

Security note :

- For your information, here is the traceroute to 10.163.156.9 :
  ?
  10.163.156.9

2.2.24 Problems regarding : snmp (161/udp)

Security holes :

- SNMP Agent responded as expected with community name: public
  CVE : CAN-1999-0186
  BID : 177

Security warnings :

- It was possible to obtain the list of SMB users of the
  remote host via SNMP :

  . Guest
  . IUSR_GABBO
  . IWAM_GABBO
  . Administrator
  . TsInternetUser
  . NetShowServices

  An attacker may use this information to set up brute force
  attacks or find an unused account.

  Solution : disable the SNMP service on the remote host if you do not
  use it, or filter incoming UDP packets going to this port
  Risk factor : Medium

- It was possible to obtain the list of Lanman services of the
  remote host via SNMP :

  . Server
  . Alerter
  . Event Log
  . Messenger
  . Telephony
  . DNS Client

. DHCP Client
. MSSQLSERVER
. Workstation
. SNMP Service
. Plug and Play
. Print Spooler
. RunAs Service
. Task Scheduler
. Computer Browser
. Indexing Service
. Automatic Updates
. COM+ Event System
. IIS Admin Service
. Protected Storage
. Removable Storage
. Terminal Services
. IPSEC Policy Agent
. Remote Storage File
. TCP/IP Print Server
. Logical Disk Manager
. Remote Storage Media
. Remote Storage Engine
. FTP Publishing Service
. Simple TCP/IP Services
. Distributed File System
. License Logging Service
. Remote Registry Service
. File Server for Macintosh
. Security Accounts Manager
. System Event Notification
. Print Server for Macintosh
. Remote Procedure Call (RPC)
. Terminal Services Licensing
. TCP/IP NetBIOS Helper Service
. Windows Media Monitor Service
. Windows Media Program Service
. Windows Media Station Service
. Windows Media Unicast Service
. Internet Authentication Service
. NT LM Security Support Provider
. Distributed Link Tracking Client
. World Wide Web Publishing Service
. Windows Management Instrumentation
. Distributed Transaction Coordinator
. Windows Internet Name Service (WINS)
. Simple Mail Transport Protocol (SMTP)

```
. Network News Transport Protocol (NNTP)
. Windows Management Instrumentation Driver Extensions

An attacker may use this information to gain more knowledge about
the target host.
Solution : disable the SNMP service on the remote host if you do not
           use it, or filter incoming UDP packets going to this port
Risk factor : Low
```

- It was possible to obtain the list of network interfaces of the remote host via SNMP :

```
. MS TCP Loopback interface
. Realtek RTL8029(AS) Ethernet Adapt

An attacker may use this information to gain more knowledge about
the target host.
Solution : disable the SNMP service on the remote host if you do not
           use it, or filter incoming UDP packets going to this port
Risk factor : Low
```

Security note :

- Using SNMP, we could determine that the remote operating system is : Hardware: x86 Family 6 Model 6 Stepping 0 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)

2.2.25 Problems regarding : netbios-ns (137/udp)

Security warnings :

-
```
. The following 9 NetBIOS names have been gathered :
GABBO
GABBO
COOLDOMAIN
COOLDOMAIN
GABBO
COOLDOMAIN
  __MSBROWSE__
INet~Services
IS~GABBO
. The remote host has the following MAC address on its adapter :
   0x00 0x40 0x05 0x65 0x01 0xa2

If you do not want to allow everyone to find the NetBios name
```

of your computer, you should filter incoming traffic to this port.

Risk factor : Medium

2.2.26 Problems regarding : echo (7/udp)

Security warnings :

- The 'echo' port is open. This port is
  not of any use nowadays, and may be a source of problems,
  since it can be used along with other ports to perform a denial
  of service. You should really disable this service.

  Risk factor : Low

  Solution : comment out 'echo' in /etc/inetd.conf
  CVE : CVE-1999-0103

2.2.27 Problems regarding : ms-term-serv (3389/tcp)

Security note :

- The Terminal Services are enabled on the remote host.

  Terminal Services allow a Windows user to remotely obtain
  a graphical login (and therefore act as a local user on the
  remote host).

  If an attacker gains a valid login and password, he may
  be able to use this service to gain further access
  on the remote host.

  Solution : Disable the Terminal Services if you do not use them
  Risk factor : Low

2.2.28 Problems regarding : daytime (13/udp)

Security warnings :

- The daytime service is running.
  The date format issued by this service
  may sometimes help an attacker to guess
  the operating system type.

```
In addition to that, when the UDP version of
daytime is running, an attacker may link it
to the echo port using spoofing, thus creating
a possible denial of service.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103
```

2.2.29 Problems regarding : qotd (17/udp)

Security warnings :

- The quote service (qotd) is running.

  A server listens for TCP connections on TCP port 17. Once a connection

  is established a short message is sent out the connection (and any
  data received is thrown away). The service closes the connection
  after sending the quote.

  Another quote of the day service is defined as a datagram based
  application on UDP. A server listens for UDP datagrams on UDP port
  17.
  When a datagram is received, an answering datagram is sent containing
  a quote (the data in the received datagram is ignored).

  An easy attack is 'pingpong' which IP spoofs a packet between two
  machines
  running qotd. This will cause them to spew characters at each other,
  slowing the machines down and saturating the network.

  Solution : disable this service in /etc/inetd.conf.

  Risk factor : Low
  CVE : CVE-1999-0103

2.2.30 Problems regarding : iad1 (1030/udp)

Security note :

- A DCE service is listening on this port
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncadg_ip_udp:10.163.156.9[1030]
  Annotation: Messenger Service

2.2.31 Problems regarding : chargen (19/udp)

Security warnings :

- The chargen service is running.
  The 'chargen' service should only be enabled when testing the machine.

  When contacted, chargen responds with some random characters
  (something
  like all the characters in the alphabet in a row). When contacted via
  UDP, it
  will respond with a single UDP packet. When contacted via TCP, it will

  continue spewing characters until the client closes the connection.

  An easy attack is 'pingpong' in which an attacker spoofs a packet
  between two
  machines running chargen. This will cause them to spew characters at
  each
  other, slowing the machines down and saturating the network.

  Solution : disable this service in /etc/inetd.conf.

  Risk factor : Low
  CVE : CVE-1999-0103

2.2.32 Problems regarding : iad3 (1032/udp)

Security note :

- A DCE service is listening on this port
  UUID: bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1
  Endpoint: ncadg_ip_udp:10.163.156.9[1032]

- A DCE service is listening on this port

```
UUID: 4f82f460-0e21-11cf-909e-00805f48a135, version 4
Endpoint: ncadg_ip_udp:10.163.156.9[1032]
```

3 10.163.155.4

3.1 Open ports (TCP and UDP)

10.163.155.4 has the following ports that are open :

- ftp (21/tcp)
- http (80/tcp)
- loc-srv (135/tcp)
- netbios-ssn (139/tcp)
- microsoft-ds (445/tcp)
- blackjack (1025/tcp)
- general/tcp
- general/udp
- netbios-ns (137/udp)
- unknown (1026/udp)

You should disable the services that you do not use, as they are potential security flaws.

3.2 Details of the vulnerabilities

3.2.1 Problems regarding : ftp (21/tcp)

Security note :

- The service closed the connection after 0 seconds without sending any data
  It might be protected by some TCP wrapper

3.2.2 Problems regarding : http (80/tcp)

Security holes :

- The remote proxy server seems to be ooops 1.4.6 or older.

  This proxy is vulnerable to a buffer overflow that
  allows an attacker to gain a shell on this host.

  *** Note that this check made the remote proxy crash

```
Solution : Upgrade to the latest version of this software
Risk factor : High
CVE : CAN-2001-0029
BID : 2099
```

Security warnings :

- The misconfigured proxy accepts requests coming
  from anywhere. This allows attackers to gain some anonymity when
   browsing
  some sensitive sites using your proxy, making the remote sites think
   that
  the requests come from your network.

  Solution: Reconfigure the remote proxy so that it only accepts
   requests coming
  from inside your network.

  Risk factor : Low/Medium

Security note :

- A web server is running on this port
- An HTTP proxy is running on this port

3.2.3 Problems regarding : loc-srv (135/tcp)

Security warnings :

- DCE services running on the remote can be enumerated
  by connecting on port 135 and doing the appropriate
  queries.

  An attacker may use this fact to gain more knowledge
  about the remote host.

  Solution : filter incoming traffic to this port.
  Risk factor : Low

Security note :

- A DCE service is listening on this host
  UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1

```
      Endpoint: ncalrpc[LRPC0000027c.00000001]
```

- A DCE service is listening on this host
  ```
      UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
      Endpoint: ncalrpc[LRPC0000027c.00000001]
  ```

- A DCE service is listening on this host
  ```
      UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
      Endpoint: ncalrpc[ntsvcs]
      Annotation: Messenger Service
  ```

- A DCE service is listening on this host
  ```
      UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
      Endpoint: ncacn_np:\\BENDER[\PIPE\ntsvcs]
      Annotation: Messenger Service
  ```

- A DCE service is listening on this host
  ```
      UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
      Endpoint: ncacn_np:\\BENDER[\PIPE\scerpc]
      Annotation: Messenger Service
  ```

3.2.4 Problems regarding : netbios-ssn (139/tcp)

Security holes :

- ```
  . It was possible to log into the remote host using a NULL session.
  The concept of a NULL session is to provide a null username and
  a null password, which grants the user the 'guest' access

  To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and
  Q246261 (Windows 2000).
  Note that this won't completely disable null sessions, but will
  prevent them from connecting to IPC$
  Please see
   http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html

  . All the smb tests will be done as ''/'' in domain WORKGROUP
  ```
  ```

```
CVE : CVE-2000-0222
BID : 990
```

Security warnings :

- The domain SID can be obtained remotely. Its value is :

  ```
  WORKGROUP : 0-0-0-0-0

  An attacker can use it to obtain the list of the local users of this
   host
  Solution : filter the ports 137 to 139 and 445
  Risk factor : Low

  CVE : CVE-2000-1200
  BID : 959
  ```

- The host SID can be obtained remotely. Its value is :

  ```
  BENDER : 5-21-1884898659-186063924-2090620667

  An attacker can use it to obtain the list of the local users of this
   host
  Solution : filter the ports 137 to 139 and 445
  Risk factor : Low

  CVE : CVE-2000-1200
  BID : 959
  ```

- The host SID could be used to enumerate the names of the local users of this host.
  (we only enumerated users name whose ID is between 1000 and 1020 for performance reasons)
  This gives extra knowledge to an attacker, which
  is not a good thing :
  - Administrator account name : Administrateur (id 500)
  - Guest account name : Invit (id 501)
  - Renaud (id 1000)

  ```
  Risk factor : Medium
  Solution : filter incoming connections this port

  CVE : CVE-2000-1200
  BID : 959
  ```

- Here is the browse list of the remote host :

```
BENDER -
XP -


This is potentially dangerous as this may help the attack
of a potential hacker by giving him extra targets to check for

Solution : filter incoming traffic to this port
Risk factor : Low
```

Security note :

- The remote native lan manager is : Windows 2000 LAN Manager
  The remote Operating System is : Windows 5.0
  The remote SMB Domain Name is : WORKGROUP

3.2.5 Problems regarding : blackjack (1025/tcp)

Security note :

- A DCE service is listening on this port
  UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
  Endpoint: ncacn_ip_tcp:10.163.155.4[1025]

- A DCE service is listening on this port
  UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
  Endpoint: ncacn_ip_tcp:10.163.155.4[1025]

3.2.6 Problems regarding : general/tcp

Security note :

- QueSO has found out that the remote host OS is
  * FreeBSD, NetBSD, OpenBSD

CVE : CAN-1999-0454

3.2.7 Problems regarding : general/udp

Security note :

- For your information, here is the traceroute to 10.163.155.4 :
  ?
  10.163.156.1
  10.163.155.4

3.2.8 Problems regarding : netbios-ns (137/udp)

Security warnings :

- . The following 5 NetBIOS names have been gathered :
  BENDER = This is the computer name registered for
  workstation services by a WINS client.
  WORKGROUP = Workgroup / Domain name
  BENDER
  BENDER = Computer name that is registered for the messenger
  service on a computer that is a WINS client.
  WORKGROUP = Workgroup / Domain name (part of the Browser
  elections)
  . The remote host has the following MAC address on its adapter :
  0x00 0x02 0x2d 0x28 0xf3 0x16

  If you do not want to allow everyone to find the NetBios name
  of your computer, you should filter incoming traffic to this port.

  Risk factor : Medium

3.2.9 Problems regarding : unknown (1026/udp)

Security note :

- A DCE service is listening on this port
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncadg_ip_udp:10.163.155.4[1026]
  Annotation: Messenger Service

4 10.163.155.3

4.1 Open ports (TCP and UDP)

10.163.155.3 has the following ports that are open :

- ftp (21/tcp)
- http (80/tcp)
- svrloc (427/tcp)
- afpovertcp (548/tcp)
- general/tcp
- general/udp
- x11 (6000/tcp)

You should disable the services that you do not use, as they are potential security flaws.

4.2 Details of the vulnerabilities

4.2.1 Problems regarding : ftp (21/tcp)

Security holes :

- It was possible to make the remote FTP server
  crash by issuing this command :

  CEL aaaa[...]aaaa

  This problem is known has the 'AIX FTPd' overflow and
  may allow the remote user to easily gain access to the
  root (super-user) account on the remote system.

  Solution : If you are using AIX FTPd, then read
  IBM's advisory number ERS-SVA-E01-1999:004.1,
  or contact your vendor for a patch.

  Risk factor : High
  CVE : CVE-1999-0789
  BID : 679

- The remote FTP server closes
  the connection when one of the commands is given
  a too long argument.

```
This probably due to a buffer overflow, which
allows anyone to execute arbitrary code
on the remote host.

This problem is threatening, because
the attackers don't need an account
to exploit this flaw.

Solution : Upgrade your FTP server or change it
Risk factor : High
CVE : CAN-2000-0133
BID : 961
```

Security note :

- An FTP server is running on this port.
  Here is its banner :
  220 10.163.155.3 FTP server (lukemftpd 1.1) ready.
- Remote FTP server banner :
  220 10.163.155.3 FTP server (lukemftpd 1.1) ready.

4.2.2 Problems regarding : http (80/tcp)

Security warnings :

- Your webserver supports the TRACE and/or TRACK methods. It has been
  shown that servers supporting this method are subject
  to cross-site-scripting attacks, dubbed XST for
  'Cross-Site-Tracing', when used in conjunction with
  various weaknesses in browsers.

  An attacker may use this flaw to trick your
  legitimate web users to give him their
  credentials.

  Solution: Disable these methods.

  If you are using Apache, add the following lines for each virtual
  host in your configuration file :

  ```
  RewriteEngine on
  RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
  RewriteRule .* - [F]
  ```

If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE
requests or to permit only the methods needed to meet site requirements
and policy.

See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html

Risk factor : Medium

- The misconfigured proxy accepts requests coming
from anywhere. This allows attackers to gain some anonymity when browsing
some sensitive sites using your proxy, making the remote sites think that
the requests come from your network.

Solution: Reconfigure the remote proxy so that it only accepts requests coming
from inside your network.

Risk factor : Low/Medium

Security note :

- A web server is running on this port
- An HTTP proxy is running on this port
- The remote web server type is :

squid/2.5.PRE13

Solution : We recommend that you configure (if possible) your web server to return
a bogus Server header in order to not leak information.

- This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by some information gathering plugin

4.2.3 Problems regarding : svrloc (427/tcp)

Security note :

- An unknown server is running on this port.
  If you know what it is, please send this banner to the Nessus team:
  00: 02 02 ..

4.2.4 Problems regarding : afpovertcp (548/tcp)

Security holes :

- This AppleShare File Server allows the 'guest' user to connect.

Security note :

- This host is running an AppleShare File Services over IP.
  Machine type: Macintosh
  Server name: betrayal
  UAMs: DHCAST128/DHX2/Cleartxt Passwrd/No User Authent
  AFP Versions: AFP3.1/AFPX03/AFP2.2/AFPVersion 2.1/AFPVersion
  2.0/AFPVersion 1.1

4.2.5 Problems regarding : general/tcp

Security note :

- QueSO has found out that the remote host OS is
  * FreeBSD, NetBSD, OpenBSD

  CVE : CAN-1999-0454

4.2.6 Problems regarding : general/udp

Security note :

- For your information, here is the traceroute to 10.163.155.3 :
  10.163.155.3

4.2.7 Problems regarding : x11 (6000/tcp)

Security warnings :

- This X server does *not* allow any client to connect to it however it is recommended that you filter incoming connections to this port as attacker may send garbage data and slow down your X session or even kill the server.

  Here is the server version : 11.0
  Here is the message we received : No protocol specified

  Solution : filter incoming connections to ports 6000-6009
  Risk factor : Low
  CVE : CVE-1999-0526

5 10.163.155.2

5.1 Open ports (TCP and UDP)

10.163.155.2 has the following ports that are open :

- ftp (21/tcp)
- http (80/tcp)
- snmp (161/udp)
- general/tcp

You should disable the services that you do not use, as they are potential security flaws.

5.2 Details of the vulnerabilities

5.2.1 Problems regarding : ftp (21/tcp)

Security note :

- The service closed the connection after 0 seconds without sending any
  data
  It might be protected by some TCP wrapper

5.2.2 Problems regarding : http (80/tcp)

Security warnings :

- Your webserver supports the TRACE and/or TRACK methods. It has been
  shown that servers supporting this method are subject
  to cross-site-scripting attacks, dubbed XST for
  'Cross-Site-Tracing', when used in conjunction with
  various weaknesses in browsers.

  An attacker may use this flaw to trick your
  legitimate web users to give him their
  credentials.

  Solution: Disable these methods.

  If you are using Apache, add the following lines for each virtual
  host in your configuration file :

```
    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

If you are using Microsoft IIS, use the URLScan tool to deny HTTP
 TRACE
requests or to permit only the methods needed to meet site
 requirements
and policy.



See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
    http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html

Risk factor : Medium
```

- ```
  The misconfigured proxy accepts requests coming
  from anywhere. This allows attackers to gain some anonymity when
   browsing
  some sensitive sites using your proxy, making the remote sites think
   that
  the requests come from your network.

  Solution: Reconfigure the remote proxy so that it only accepts
   requests coming
  from inside your network.

  Risk factor : Low/Medium
  ```

Security note :

- ```
  A web server is running on this port
  ```
- ```
  An HTTP proxy is running on this port
  ```
- ```
  The remote web server type is :

  squid/2.5.PRE13

  Solution : We recommend that you configure (if possible) your web
   server to return
  a bogus Server header in order to not leak information.
  ```

5.2.3 Problems regarding : snmp (161/udp)

Security holes :

- The device answered to more than 4 community strings.
  This may be a false positive or a community-less SNMP server
  HP printers answer to all community strings.

  SNMP Agent responded as expected with community name: public
  SNMP Agent responded as expected with community name: private
  SNMP Agent responded as expected with community name: ilmi
  SNMP Agent responded as expected with community name: ILMI If the
  target is a Cisco Product, please read
  http://www.cisco.com/warp/public/707/ios-snmp-ilmi-vuln-pub.shtml
  SNMP Agent responded as expected with community name: system
  SNMP Agent responded as expected with community name: write
  SNMP Agent responded as expected with community name: all
  SNMP Agent responded as expected with community name: monitor
  SNMP Agent responded as expected with community name: agent
  SNMP Agent responded as expected with community name: manager
  SNMP Agent responded as expected with community name: OrigEquipMfr
  SNMP Agent responded as expected with community name: admin
  SNMP Agent responded as expected with community name: default
  SNMP Agent responded as expected with community name: password
  SNMP Agent responded as expected with community name: tivoli
  SNMP Agent responded as expected with community name: openview
  SNMP Agent responded as expected with community name: community
  SNMP Agent responded as expected with community name: snmp
  SNMP Agent responded as expected with community name: snmpd
  SNMP Agent responded as expected with community name: Secret C0de
  SNMP Agent responded as expected with community name: security
  SNMP Agent responded as expected with community name: all private
  SNMP Agent responded as expected with community name: rmon
  SNMP Agent responded as expected with community name: rmon_admin
  SNMP Agent responded as expected with community name: hp_admin
  SNMP Agent responded as expected with community name: NoGaH$@!
  SNMP Agent responded as expected with community name: 0392a0
  SNMP Agent responded as expected with community name: xyzzy
  SNMP Agent responded as expected with community name: agent_steal
  SNMP Agent responded as expected with community name: freekevin
  SNMP Agent responded as expected with community name: fubar
  SNMP Agent responded as expected with community name: secret
  SNMP Agent responded as expected with community name: cisco
  SNMP Agent responded as expected with community name: apc
  SNMP Agent responded as expected with community name: ANYCOM
  SNMP Agent responded as expected with community name: cable-docsis

```
SNMP Agent responded as expected with community name: c
SNMP Agent responded as expected with community name: cc
SNMP Agent responded as expected with community name: Cisco router
SNMP Agent responded as expected with community name: cascade
SNMP Agent responded as expected with community name: comcomcom
CVE : CAN-1999-0186
BID : 177
```

Security warnings :

- A SNMP server is running on this host

Security note :

- Using SNMP, we could determine that the remote operating system is : Base Station V3.81 Compatible

5.2.4 Problems regarding : general/tcp

Security warnings :

- The remote host is a Wireless Access Point.
  You should ensure that the proper physical and logical controls exist around the AP.

  Risk factor : Medium/Low

6 10.163.156.1

6.1 Open ports (TCP and UDP)

10.163.156.1 has the following ports that are open :

- ssh (22/tcp)
- ftp (21/tcp)
- http (80/tcp)
- general/tcp
- general/udp

You should disable the services that you do not use, as they are potential security flaws.

6.2 Details of the vulnerabilities

6.2.1 Problems regarding : ssh (22/tcp)

Security warnings :

- The remote SSH daemon supports connections made
  using the version 1.33 and/or 1.5 of the SSH protocol.

  These protocols are not completely cryptographically
  safe so they should not be used.

  Solution :
   If you use OpenSSH, set the option 'Protocol' to '2'
   If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

  Risk factor : Low

Security note :

- An ssh server is running on this port
- The remote SSH daemon supports the following versions of the
  SSH protocol :

    . 1.33
    . 1.5
    . 1.99
    . 2.0

- Remote SSH version : SSH-1.99-OpenSSH_3.5

6.2.2 Problems regarding : ftp (21/tcp)

Security note :

- The service closed the connection after 0 seconds without sending any data
  It might be protected by some TCP wrapper

6.2.3 Problems regarding : http (80/tcp)

Security holes :

- The remote proxy server seems to be ooops 1.4.6 or older.

  This proxy is vulnerable to a buffer overflow that
  allows an attacker to gain a shell on this host.

  *** Note that this check made the remote proxy crash

  Solution : Upgrade to the latest version of this software
  Risk factor : High
  CVE : CAN-2001-0029
  BID : 2099

Security note :

- A web server is running on this port
- An HTTP proxy is running on this port

6.2.4 Problems regarding : general/tcp

Security note :

- QueSO has found out that the remote host OS is
  * FreeBSD, NetBSD, OpenBSD

  CVE : CAN-1999-0454

6.2.5 Problems regarding : general/udp

Security note :

- For your information, here is the traceroute to 10.163.156.1 :
  ?
  10.163.156.1

7 10.163.155.6

7.1 Open ports (TCP and UDP)

`10.163.155.6` has the following ports that are open :

- `ftp (21/tcp)`
- `http (80/tcp)`
- `loc-srv (135/tcp)`
- `netbios-ssn (139/tcp)`
- `microsoft-ds (445/tcp)`
- `blackjack (1025/tcp)`
- `general/tcp`
- `general/udp`
- `netbios-ns (137/udp)`
- `ms-term-serv (3389/tcp)`
- `unknown (1027/udp)`

You should disable the services that you do not use, as they are potential security flaws.

7.2 Details of the vulnerabilities

7.2.1 Problems regarding : ftp (21/tcp)

Security note :

- ```
  The service closed the connection after 0 seconds without sending any
   data
  It might be protected by some TCP wrapper
  ```

7.2.2 Problems regarding : http (80/tcp)

Security holes :

- ```
  It was possible to kill the web server by
  sending an invalid request with a too long HTTP 1.1 header
  (Accept-Encoding, Accept-Language, Accept-Range, Connection,
  Expect, If-Match, If-None-Match, If-Range, If-Unmodified-Since,
  Max-Forwards, TE, Host)
  ```

A cracker may exploit this vulnerability to make your web server
crash continually or even execute arbirtray code on your system.

Solution : upgrade your software or protect it with a filtering
 reverse proxy
Risk factor : High

Security warnings :

- Your webserver supports the TRACE and/or TRACK methods. It has been
shown that servers supporting this method are subject
to cross-site-scripting attacks, dubbed XST for
'Cross-Site-Tracing', when used in conjunction with
various weaknesses in browsers.

An attacker may use this flaw to trick your
legitimate web users to give him their
credentials.

Solution: Disable these methods.

If you are using Apache, add the following lines for each virtual
host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

If you are using Microsoft IIS, use the URLScan tool to deny HTTP
 TRACE
requests or to permit only the methods needed to meet site
 requirements
and policy.

See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html

Risk factor : Medium

- The misconfigured proxy accepts requests coming
from anywhere. This allows attackers to gain some anonymity when
 browsing

```
some sensitive sites using your proxy, making the remote sites think
 that
the requests come from your network.

Solution: Reconfigure the remote proxy so that it only accepts
 requests coming
from inside your network.

Risk factor : Low/Medium
```

Security note :

- A web server is running on this port
- An HTTP proxy is running on this port
- The remote web server type is :

  ```
  squid/2.5.PRE13

  Solution : We recommend that you configure (if possible) your web
   server to return
  a bogus Server header in order to not leak information.
  ```

- This port was detected as being open by a port scanner but is now
  closed.
  This service might have been crashed by a port scanner or by some
  information gathering plugin

7.2.3 Problems regarding : loc-srv (135/tcp)

Security warnings :

- DCE services running on the remote can be enumerated
  by connecting on port 135 and doing the appropriate
  queries.

  An attacker may use this fact to gain more knowledge
  about the remote host.

  Solution : filter incoming traffic to this port.
  Risk factor : Low

Security note :

- A DCE service is listening on this host
  UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
  Endpoint: ncalrpc[wzcsvc]

- A DCE service is listening on this host
  UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
  Endpoint: ncalrpc[OLE3]

- A DCE service is listening on this host
  UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
  Endpoint: ncacn_np:\\XP[\PIPE\atsvc]

- A DCE service is listening on this host
  UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
  Endpoint: ncalrpc[wzcsvc]

- A DCE service is listening on this host
  UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
  Endpoint: ncalrpc[OLE3]

- A DCE service is listening on this host
  UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
  Endpoint: ncacn_np:\\XP[\PIPE\atsvc]

- A DCE service is listening on this host
  UUID: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1
  Endpoint: ncalrpc[wzcsvc]

- A DCE service is listening on this host
  UUID: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1
  Endpoint: ncalrpc[OLE3]

- A DCE service is listening on this host
  UUID: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1
  Endpoint: ncacn_np:\\XP[\PIPE\atsvc]

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncalrpc[wzcsvc]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncalrpc[OLE3]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncacn_np:\\XP[\PIPE\atsvc]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncacn_np:\\XP[\PIPE\AudioSrv]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncacn_np:\\XP[\PIPE\wkssvc]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncacn_np:\\XP[\PIPE\SECLOGON]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncacn_np:\\XP[\pipe\trkwks]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncalrpc[trkwks]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncacn_np:\\XP[\PIPE\W32TIME]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncacn_np:\\XP[\pipe\keysvc]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncalrpc[keysvc]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncalrpc[senssvc]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncacn_np:\\XP[\PIPE\srvsvc]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncalrpc[srrpc]
  Annotation: Messenger Service

- A DCE service is listening on this host
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncacn_np:\\XP[\PIPE\msgsvc]
  Annotation: Messenger Service

7.2.4 Problems regarding : netbios-ssn (139/tcp)

Security holes :

- . It was possible to log into the remote host using a NULL session.
  The concept of a NULL session is to provide a null username and
  a null password, which grants the user the 'guest' access

  To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and
  Q246261 (Windows 2000).
  Note that this won't completely disable null sessions, but will
  prevent them from connecting to IPC$
  Please see
   http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html

  . All the smb tests will be done as ''/'' in domain WORKGROUP
  CVE : CVE-2000-0222
  BID : 990

Security warnings :

- The domain SID can be obtained remotely. Its value is :

  WORKGROUP : 0-0-0-0-0

  An attacker can use it to obtain the list of the local users of this
   host
  Solution : filter the ports 137 to 139 and 445
  Risk factor : Low

  CVE : CVE-2000-1200
  BID : 959

- The host SID can be obtained remotely. Its value is :

  XP : 5-21-583907252-2111687655-1957994488

  An attacker can use it to obtain the list of the local users of this
   host
  Solution : filter the ports 137 to 139 and 445
  Risk factor : Low

  CVE : CVE-2000-1200
  BID : 959

- Here is the browse list of the remote host :

  BENDER -
  XP -

  This is potentially dangerous as this may help the attack
  of a potential hacker by giving him extra targets to check for

  Solution : filter incoming traffic to this port
  Risk factor : Low

Security note :

- The remote native lan manager is : Windows 2000 LAN Manager
  The remote Operating System is : Windows 5.1
  The remote SMB Domain Name is : WORKGROUP

7.2.5 Problems regarding : blackjack (1025/tcp)

Security note :

- A DCE service is listening on this port
  UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
  Endpoint: ncacn_ip_tcp:10.163.155.6[1025]

- A DCE service is listening on this port
  UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
  Endpoint: ncacn_ip_tcp:10.163.155.6[1025]

- A DCE service is listening on this port
  UUID: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1
  Endpoint: ncacn_ip_tcp:10.163.155.6[1025]

- A DCE service is listening on this port
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncacn_ip_tcp:10.163.155.6[1025]
  Annotation: Messenger Service

7.2.6 Problems regarding : general/tcp

Security note :

- QueSO has found out that the remote host OS is
  * FreeBSD, NetBSD, OpenBSD

  CVE : CAN-1999-0454

7.2.7 Problems regarding : general/udp

Security note :

- For your information, here is the traceroute to 10.163.155.6 :
  ?
  10.163.155.6

7.2.8 Problems regarding : netbios-ns (137/udp)

Security warnings :

- . The following 7 NetBIOS names have been gathered :
  XP = This is the computer name registered for
  workstation services by a WINS client.
  WORKGROUP = Workgroup / Domain name
  XP = Computer name that is registered for the messenger
  service on a computer that is a WINS client.

```
XP
WORKGROUP       = Workgroup / Domain name (part of the Browser
elections)
WORKGROUP
  __MSBROWSE__
. The remote host has the following MAC address on its adapter :
  0x00 0x60 0x1d 0x21 0xa9 0x49

If you do not want to allow everyone to find the NetBios name
of your computer, you should filter incoming traffic to this port.

Risk factor : Medium
```

7.2.9 Problems regarding : ms-term-serv (3389/tcp)

Security note :

- The Terminal Services are enabled on the remote host.

  Terminal Services allow a Windows user to remotely obtain
  a graphical login (and therefore act as a local user on the
  remote host).

  If an attacker gains a valid login and password, he may
  be able to use this service to gain further access
  on the remote host.

  Solution : Disable the Terminal Services if you do not use them
  Risk factor : Low

7.2.10 Problems regarding : unknown (1027/udp)

Security note :

- A DCE service is listening on this port
  UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
  Endpoint: ncadg_ip_udp:10.163.155.6[1027]
  Annotation: Messenger Service

8 10.163.156.205

8.1 Open ports (TCP and UDP)

`10.163.156.205` has the following ports that are open :

- `rtmp (1/tcp)`
- `telnet (23/tcp)`
- `ftp (21/tcp)`
- `chargen (19/tcp)`
- `daytime (13/tcp)`
- `discard (9/tcp)`
- `echo (7/tcp)`
- `smtp (25/tcp)`
- `time (37/tcp)`
- `finger (79/tcp)`
- `sunrpc (111/tcp)`
- `exec (512/tcp)`
- `printer (515/tcp)`
- `shell (514/tcp)`
- `login (513/tcp)`
- `ldaps (636/tcp)`
- `blackjack (1025/tcp)`
- `LSA-or-nterm (1026/tcp)`
- `kdm (1024/tcp)`
- `ms-lsa (1029/tcp)`
- `esl-lm (1455/tcp)`
- `general/tcp`
- `blackjack (1025/udp)`
- `sunrpc (111/udp)`
- `general/udp`

- xdmcp (177/udp)
- echo (7/udp)
- daytime (13/udp)

You should disable the services that you do not use, as they are potential security flaws.

8.2 Details of the vulnerabilities

8.2.1 Problems regarding : rtmp (1/tcp)

Security note :

- An unknown server is running on this port.
  If you know what it is, please send this banner to the Nessus team:
  00: 2d 53 65 72 76 69 63 65 20 6e 6f 74 20 61 76 61 -Service not ava
  10: 69 6c 61 62 6c 65 0d 0a ilable..

8.2.2 Problems regarding : telnet (23/tcp)

Security holes :

- The account 'guest' has the password guest
  An attacker may use it to gain further privileges on this system

  Risk factor : High
  Solution : Set a password for this account or disable it
  CVE : CAN-1999-0502
- The account 'demos' has no password set.
  An attacker may use it to gain further privileges on this system

  Risk factor : High
  Solution : Set a password for this account or disable it
  CVE : CAN-1999-0502
- The account 'EZsetup' has no password set.
  An attacker may use it to gain further privileges on this system

  Risk factor : High
  Solution : Set a password for this account or disable it
  CVE : CAN-1999-0502

- The account ’root’ has the password root
  An attacker may use it to gain further privileges on this system

  Risk factor : High
  Solution : Set a password for this account or disable it
  CVE : CAN-1999-0502

- The account ’lp’ has no password set.
  An attacker may use it to gain further privileges on this system

  Risk factor : High
  Solution : Set a password for this account or disable it
  CVE : CAN-1999-0502

Security warnings :

- The Telnet service is running.
  This service is dangerous in the sense that
  it is not ciphered - that is, everyone can sniff
  the data that passes between the telnet client
  and the telnet server. This includes logins
  and passwords.

  You should disable this service and use OpenSSH instead.
  (www.openssh.com)

  Solution : Comment out the ’telnet’ line in /etc/inetd.conf.

  Risk factor : Low
  CVE : CAN-1999-0619

Security note :

- A telnet server seems to be running on this port
- Remote telnet banner :

  IRIX (IRIS)

8.2.3 Problems regarding : ftp (21/tcp)

Security note :

- An FTP server is running on this port.
  Here is its banner :
  220 IRIS.fr.nessus.org FTP server ready.
- Remote FTP server banner :
  220 IRIS.fr.nessus.org FTP server ready.

8.2.4 Problems regarding : chargen (19/tcp)

Security warnings :

- The chargen service is running.
  The 'chargen' service should only be enabled when testing the machine.

  When contacted, chargen responds with some random characters
  (something
  like all the characters in the alphabet in a row). When contacted via
  UDP, it
  will respond with a single UDP packet. When contacted via TCP, it will

  continue spewing characters until the client closes the connection.

  An easy attack is 'pingpong' in which an attacker spoofs a packet
  between two
  machines running chargen. This will cause them to spew characters at
  each
  other, slowing the machines down and saturating the network.

  Solution : disable this service in /etc/inetd.conf.

  Risk factor : Low
  CVE : CVE-1999-0103

Security note :

- Chargen is running on this port

8.2.5 Problems regarding : daytime (13/tcp)

Security warnings :

- The daytime service is running.
  The date format issued by this service
  may sometimes help an attacker to guess

```
the operating system type.

In addition to that, when the UDP version of
daytime is running, an attacker may link it
to the echo port using spoofing, thus creating
a possible denial of service.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103
```

8.2.6 Problems regarding : echo (7/tcp)

Security warnings :

- ```
  The 'echo' port is open. This port is
  not of any use nowadays, and may be a source of problems,
  since it can be used along with other ports to perform a denial
  of service. You should really disable this service.

  Risk factor : Low

  Solution : comment out 'echo' in /etc/inetd.conf
  CVE : CVE-1999-0103
  ```

Security note :

- ```
  An echo server is running on this port
  ```

8.2.7 Problems regarding : smtp (25/tcp)

Security holes :

- ```
  The remote sendmail server, according to its version number,
  may be vulnerable to the -bt overflow attack which
  allows any local user to execute arbitrary commands as root.

  Solution : upgrade to the latest version of Sendmail
  Risk factor : High
  Note : This vulnerability is _local_ only
  ```
- ```
  The remote sendmail server, according to its version number,
  may be vulnerable to a buffer overflow its DNS handling code.
  ```

The owner of a malicious name server could use this flaw
to execute arbitrary code on this host.

Solution : Upgrade to Sendmail 8.12.5
Risk factor : High
CVE : CAN-2002-0906
BID : 5122

Security warnings :

- The remote SMTP server
  answers to the EXPN and/or VRFY commands.

  The EXPN command can be used to find
  the delivery address of mail aliases, or
  even the full name of the recipients, and
  the VRFY command may be used to check the
  validity of an account.

  Your mailer should not allow remote users to
  use any of these commands, because it gives
  them too much information.

  Solution : if you are using Sendmail, add the
  option
   O PrivacyOptions=goaway
  in /etc/sendmail.cf.

  Risk factor : Low
  CVE : CAN-1999-0531

- The remote sendmail server, according to its version number,
  might be vulnerable to a queue destruction when a local user
  runs
   sendmail -q -h1000

  If you system does not allow users to process the queue (which
  is the default), you are not vulnerable.

  Solution : upgrade to the latest version of Sendmail or
  do not allow users to process the queue (RestrictQRun option)
  Risk factor : Low
  Note : This vulnerability is _local_ only

```
CVE : CAN-2001-0714
BID : 3378
```

- ```
  According to the version number of the remote mail server,
  a local user may be able to obtain the complete mail configuration
  and other interesting information about the mail queue even if
  he is not allowed to access those information directly, by running
   sendmail -q -d0-nnnn.xxx
  where nnnn & xxx are debugging levels.

  If users are not allowed to process the queue (which is the default)
  then you are not vulnerable.

  Solution : upgrade to the latest version of Sendmail or
  do not allow users to process the queue (RestrictQRun option)
  Risk factor : Very low / none
  Note : This vulnerability is _local_ only
  CVE : CAN-2001-0715
  BID : 3898
  ```

Security note :

- ```
  An SMTP server is running on this port
  Here is its banner :
  220 IRIS.fr.nessus.org ESMTP Sendmail SGI-8.9.3/8.9.3; Fri, 21 Feb
   2003 06:09:50 -0800 (PST)
  ```
- ```
  Remote SMTP server banner :
  220 IRIS.fr.nessus.org ESMTP Sendmail SGI-8.9.3/8.9.3; Fri, 21 Feb
   2003 06:11:07 -0800 (PST)
  ```

- ```
  Nessus sent several emails containing the EICAR
  test strings in them to the postmaster of
  the remote SMTP server.

  The EICAR test string is a fake virus which
  triggers anti-viruses, in order to make sure
  they run.

  Nessus attempted to e-mail this string five times,
  with different codings each time, in order to attempt
  to fool the remote anti-virus (if any).


  If there is an antivirus filter, these messages should
  all be blocked.
  ```

```
*** To determine if the remote host is vulnerable, see
*** if any mail arrived to the postmaster of this host

Solution: Install an antivirus / upgrade it

Reference : http://online.securityfocus.com/archive/1/256619
Reference : http://online.securityfocus.com/archive/1/44301
Reference : http://online.securityfocus.com/links/188

Risk factor : Low
```

8.2.8 Problems regarding : time (37/tcp)

Security note :

- A time server seems to be running on this port

8.2.9 Problems regarding : finger (79/tcp)

Security warnings :

- The 'finger' service provides useful information
  to attackers, since it allow them to gain usernames, check if a machine
  is being used, and so on...

  Risk factor : Low

  Solution : comment out the 'finger' line in /etc/inetd.conf
  CVE : CVE-1999-0612

Security note :

- A finger server seems to be running on this port

8.2.10 Problems regarding : sunrpc (111/tcp)

Security note :

- RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port

8.2.11 Problems regarding : exec (512/tcp)

Security warnings :

- The rexecd service is open.
  Because rexecd does not provide any good
  means of authentication, it can be
  used by an attacker to scan a third party
  host, giving you troubles or bypassing
  your firewall.

  Solution : comment out the 'exec' line
  in /etc/inetd.conf.

  Risk factor : Medium
  CVE : CAN-1999-0618

8.2.12 Problems regarding : printer (515/tcp)

Security note :

- A LPD server seems to be running on this port

8.2.13 Problems regarding : shell (514/tcp)

Security warnings :

- The rsh service is running.
  This service is dangerous in the sense that
  it is not ciphered - that is, everyone can sniff
  the data that passes between the rsh client
  and the rsh server. This includes logins
  and passwords.

  You should disable this service and use ssh instead.

  Solution : Comment out the 'rsh' line in /etc/inetd.conf.

  Risk factor : Low
  CVE : CAN-1999-0651

8.2.14 Problems regarding : login (513/tcp)

Security warnings :

- The rlogin service is running.
  This service is dangerous in the sense that
  it is not ciphered - that is, everyone can sniff
  the data that passes between the rlogin client
  and the rlogin server. This includes logins
  and passwords.

  You should disable this service and use openssh instead
  (www.openssh.com)

  Solution : Comment out the 'rlogin' line in /etc/inetd.conf.

  Risk factor : Low
  CVE : CAN-1999-0651

8.2.15 Problems regarding : ldaps (636/tcp)

Security note :

- RPC program #391017 version 1 is running on this port

8.2.16 Problems regarding : blackjack (1025/tcp)

Security note :

- RPC program #391029 version 1 is running on this port

8.2.17 Problems regarding : LSA-or-nterm (1026/tcp)

Security holes :

- The tooltalk RPC service is running.
  An possible implementation fault in the
  ToolTalk object database server may allow an
  attacker to execute arbitrary commands as
  root.

  *** This warning may be a false
  *** positive since the presence
  *** of this vulnerability is only accurately
  *** identified with local access.

  Solution : Disable this service.
  See also : CERT Advisory CA-98.11

```
Risk factor : High
CVE : CVE-1999-0003, CVE-1999-0693
BID : 122
```

- The tooltalk RPC service is running.

```
There is a format string bug in many versions
of this service, which allow an attacker to gain
root remotely.

In addition to this, several versions of this service
allow remote attackers to overwrite abitrary memory
locations with a zero and possibly gain privileges
via a file descriptor argument in an AUTH_UNIX
procedure call which is used as a table index by the
_TT_ISCLOSE procedure.

*** This warning may be a false positive since the presence
*** of the bug was not verified locally.

Solution : Disable this service or patch it
See also : CERT Advisories CA-2001-27 and CA-2002-20

Risk factor : High
CVE : CAN-2002-0677, CVE-2001-0717, CVE-2002-0679
BID : 3382
```

Security note :

- RPC program #100083 version 1 is running on this port

8.2.18 Problems regarding : kdm (1024/tcp)

Security warnings :

- The fam RPC service is running.
  Several versions of this service have
  a well-known buffer overflow condition
  that allows intruders to execute
  arbitrary commands as root on this system.

```
Solution : disable this service in /etc/inetd.conf
More information :
 http://www.nai.com/nai_labs/asp_set/advisory/16_fam_adv.asp
```

```
Risk factor : High
CVE : CVE-1999-0059
BID : 353
```

Security note :

- RPC program #391002 version 1 'sgi_fam' (fam) is running on this port
- RPC program #391002 version 2 'sgi_fam' (fam) is running on this port

8.2.19 Problems regarding : esl-lm (1455/tcp)

Security note :

- The service closed the connection after 0 seconds without sending any data
  It might be protected by some TCP wrapper

8.2.20 Problems regarding : general/tcp

Security note :

- QueSO has found out that the remote host OS is
  * IRIX 6.x?

```
CVE : CAN-1999-0454
```

8.2.21 Problems regarding : blackjack (1025/udp)

Security warnings :

- The rstatd RPC service is running.
  It provides an attacker interesting
  information such as :

  - the CPU usage
  - the system uptime
  - its network usage
  - and more

  Usually, it is not a good idea to let this
  service open

```
Risk factor : Low
CVE : CAN-1999-0624
```

Security note :

- RPC program #100001 version 1 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
- RPC program #100001 version 2 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
- RPC program #100001 version 3 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port

8.2.22 Problems regarding : sunrpc (111/udp)

Security note :

- RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port

8.2.23 Problems regarding : general/udp

Security note :

- For your information, here is the traceroute to 10.163.156.205 : 10.163.156.205

8.2.24 Problems regarding : xdmcp (177/udp)

Security warnings :

- The remote host is running XDMCP.

  This protocol is used to provide X display connections for X terminals. XDMCP is completely insecure, since the traffic and passwords are not encrypted.

  An attacker may use this flaw to capture all the keystrokes of the users using this host through their X terminal, including passwords.

  Risk factor : Medium
  Solution : Disable XDMCP

8.2.25 Problems regarding : echo (7/udp)

Security warnings :

- The 'echo' port is open. This port is
  not of any use nowadays, and may be a source of problems,
  since it can be used along with other ports to perform a denial
  of service. You should really disable this service.

  Risk factor : Low

  Solution : comment out 'echo' in /etc/inetd.conf
  CVE : CVE-1999-0103

8.2.26 Problems regarding : daytime (13/udp)

Security warnings :

- The daytime service is running.
  The date format issued by this service
  may sometimes help an attacker to guess
  the operating system type.

  In addition to that, when the UDP version of
  daytime is running, an attacker may link it
  to the echo port using spoofing, thus creating
  a possible denial of service.

  Solution : disable this service in /etc/inetd.conf.

  Risk factor : Low
  CVE : CVE-1999-0103

9 10.163.156.16

9.1 Open ports (TCP and UDP)

10.163.156.16 has the following ports that are open :

- smtp (25/tcp)
- telnet (23/tcp)
- ftp (21/tcp)
- chargen (19/tcp)
- daytime (13/tcp)
- discard (9/tcp)
- echo (7/tcp)
- time (37/tcp)
- finger (79/tcp)
- sunrpc (111/tcp)
- login (513/tcp)
- exec (512/tcp)
- printer (515/tcp)
- shell (514/tcp)
- uucp (540/tcp)
- xaudio (1103/tcp)
- general/tcp
- dtspc (6112/tcp)
- sunrpc (111/udp)
- sometimes-rpc8 (32772/udp)
- sometimes-rpc21 (32779/tcp)
- sometimes-rpc12 (32774/udp)
- sometimes-rpc14 (32775/udp)
- sometimes-rpc10 (32773/udp)
- unknown (32790/tcp)

- sometimes-rpc16 (32776/udp)
- unknown (32791/tcp)
- sometimes-rpc18 (32777/udp)
- sometimes-rpc20 (32778/udp)
- sometimes-rpc22 (32779/udp)
- lockd (4045/udp)
- unknown (32792/tcp)
- unknown (32793/tcp)
- sometimes-rpc24 (32780/udp)
- unknown (32794/tcp)
- lockd (4045/tcp)
- unknown (32812/udp)
- unknown (32795/tcp)
- unknown (32813/udp)
- unknown (32796/tcp)
- snmp (161/udp)
- xdmcp (177/udp)
- general/udp
- font-service (7100/tcp)
- echo (7/udp)
- daytime (13/udp)

You should disable the services that you do not use, as they are potential security flaws.

9.2 Details of the vulnerabilities

9.2.1 Problems regarding : smtp (25/tcp)

Security holes :

- The remote SMTP server did not complain when issued the command :
  MAIL FROM: |testing

  This probably means that it is possible to send mail that will be bounced to a program, which is a serious threat, since this allows anyone to execute arbitrary commands on this host.

  *** This security hole might be a false positive, since
  *** some MTAs will not complain to this test, but instead
  *** just drop the message silently

  Solution : upgrade your MTA or change it.

  Risk factor : High
  CVE : CVE-1999-0203
  BID : 2308

Security warnings :

- The remote SMTP server answers to the EXPN and/or VRFY commands.

  The EXPN command can be used to find the delivery address of mail aliases, or even the full name of the recipients, and the VRFY command may be used to check the validity of an account.

  Your mailer should not allow remote users to use any of these commands, because it gives them too much information.

  Solution : if you are using Sendmail, add the option
  O PrivacyOptions=goaway
  in /etc/sendmail.cf.

  Risk factor : Low
  CVE : CAN-1999-0531

- The remote SMTP server is vulnerable to a redirection attack. That is, if a mail is sent to :

```
  user@hostname1@victim

Then the remote SMTP server (victim) will happily send the
mail to :
  user@hostname1

Using this flaw, an attacker may route a message
through your firewall, in order to exploit other
SMTP servers that can not be reached from the
outside.

*** THIS WARNING MAY BE A FALSE POSITIVE, SINCE
    SOME SMTP SERVERS LIKE POSTFIX WILL NOT
    COMPLAIN BUT DROP THIS MESSAGE ***


Solution : if you are using sendmail, then at the top
of ruleset 98, in /etc/sendmail.cf, insert :
R$*@$*@$*       $#error $@ 5.7.1 $: '551 Sorry, no redirections.'

Risk factor : Low
```

- The remote SMTP server allows the relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth.

  Risk factor : Low/Medium

  Solution : configure your SMTP server so that it can't be used as a relay
  any more.
  CVE : CAN-1999-0512

- The remote SMTP server allows anyone to use it as a mail relay, provided that the source address is set to '<>'.
  This problem allows any spammer to use your mail server to spam the world, thus blacklisting your mailserver, and using your network resources.

  Risk factor : Medium

  Solution : reconfigure this server properly
  CVE : CVE-1999-0819

- The remote SMTP server seems to allow remote users to

```
send mail anonymously by providing arguments that are
too long to the HELO command (more than 1024 chars).

This problem may allow malicious users to send hate
mail or threatening mail using your server,
and keep their anonymity.

Risk factor : Low

Solution : If you are using sendmail, upgrade to
version 8.9.x or newer. If you do not run sendmail, contact
your vendor.
CVE : CAN-1999-0098
```

Security note :

- An unknown service is running on this port.
  It is usually reserved for SMTP
- Remote SMTP server banner :
  220 unknown. Sendmail SMI-8.6/SMI-SVR4 ready at Fri, 21 Feb 2003
  15:10:24 GMT

- An unknown server is running on this port.
  If you know what it is, please send this banner to the Nessus team:

```
00: 32 32 30 20 75 6e 6b 6e 6f 77 6e 2e 20 53 65 6e    220 unknown.
 Sen
10: 64 6d 61 69 6c 20 53 4d 49 2d 38 2e 36 2f 53 4d    dmail
 SMI-8.6/SM
20: 49 2d 53 56 52 34 20 72 65 61 64 79 20 61 74 20    I-SVR4 ready at

30: 46 72 69 2c 20 32 31 20 46 65 62 20 32 30 30 33    Fri, 21 Feb
 2003
40: 20 31 35 3a 30 38 3a 33 38 20 47 4d 54 0d 0a 35     15:08:38
 GMT..5
50: 30 30 20 43 6f 6d 6d 61 6e 64 20 75 6e 72 65 63    00 Command
 unrec
60: 6f 67 6e 69 7a 65 64 0d 0a 35 30 30 20 43 6f 6d    ognized..500
 Com
70: 6d 61 6e 64 20 75 6e 72 65 63 6f 67 6e 69 7a 65    mand
 unrecognize
80: 64 0d 0a                                           d..
```

9.2.2 Problems regarding : telnet (23/tcp)

Security holes :

- The remote /bin/login seems to crash when it receives too many environment variables.

  An attacker may use this flaw to gain a root shell on this system.

  See also : http://www.cert.org/advisories/CA-2001-34.html
  Solution : Contact your vendor for a patch (or read the CERT advisory)
  Risk factor : High
  CVE : CVE-2001-0797
  BID : 3681

- The Telnet server does not return an expected number of replies when it receives a long sequence of 'Are You There' commands. This probably means it overflows one of its internal buffers and crashes. It is likely an attacker could abuse this bug to gain control over the remote host's superuser.

  For more information, see:
  http://www.team-teso.net/advisories/teso-advisory-011.tar.gz

  Solution: Comment out the 'telnet' line in /etc/inetd.conf.
  Risk factor : High
  CVE : CVE-2001-0554
  BID : 3064

- There is a bug in the remote /bin/login which allows an attacker to gain a shell on this host, without even sending a shell code.

  An attacker may use this flaw to log in as any user (except root) on the remote host.

  Here is the output of the command 'cat /etc/passwd' :
  cat /etc/passwd
  root:x:0:1:Super-User:/:/sbin/sh
  daemon:x:1:1::/:
  bin:x:2:2::/usr/bin:
  sys:x:3:3::/:
  adm:x:4:4:Admin:/var/adm:
  lp:x:71:8:Line Printer Admin:/usr/spool/lp:
  smtp:x:0:0:Mail Daemon User:/:
  uucp:x:5:5:uucp Admin:/usr/lib/uucp:

```
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
renaud:x:100:1::/home/renaud:/bin/sh
$

Solution : See http://www.cert.org/advisories/CA-2001-34.html
Risk factor : High
CVE : CVE-2001-0797
BID : 3681
```

Security warnings :

- ```
  The Telnet service is running.
  This service is dangerous in the sense that
  it is not ciphered - that is, everyone can sniff
  the data that passes between the telnet client
  and the telnet server. This includes logins
  and passwords.

  You should disable this service and use OpenSSH instead.
  (www.openssh.com)

  Solution : Comment out the 'telnet' line in /etc/inetd.conf.

  Risk factor : Low
  CVE : CAN-1999-0619
  ```

Security note :

- ```
  A telnet server seems to be running on this port
  ```
- ```
  Remote telnet banner :


  SunOS 5.6
  ```

9.2.3 Problems regarding : ftp (21/tcp)

Security holes :

- ```
  You seem to be running an FTP server which is vulnerable to the
  ```

```
'glob heap corruption' flaw.
An attacker may use this problem to execute arbitrary commands on this
 host.

*** Nessus relied solely on the banner of the server to issue this
 warning,
*** so this alert might be a false positive

Solution : Upgrade your ftp server software to the latest version.
Risk factor : High

CVE : CVE-2001-0550
BID : 3581
```

Security note :

- An FTP server is running on this port.
  Here is its banner :
  220 unknown FTP server (SunOS 5.6) ready.
- Remote FTP server banner :
  220 unknown FTP server (SunOS 5.6) ready.

9.2.4 Problems regarding : chargen (19/tcp)

Security warnings :

- The chargen service is running.
  The 'chargen' service should only be enabled when testing the machine.

```
When contacted, chargen responds with some random characters
 (something
like all the characters in the alphabet in a row). When contacted via
 UDP, it
will respond with a single UDP packet. When contacted via TCP, it will

continue spewing characters until the client closes the connection.

An easy attack is 'pingpong' in which an attacker spoofs a packet
 between two
machines running chargen. This will cause them to spew characters at
 each
other, slowing the machines down and saturating the network.
```

```
Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103
```

Security note :

- Chargen is running on this port

9.2.5 Problems regarding : daytime (13/tcp)

Security warnings :

- The daytime service is running.
  The date format issued by this service
  may sometimes help an attacker to guess
  the operating system type.

  In addition to that, when the UDP version of
  daytime is running, an attacker may link it
  to the echo port using spoofing, thus creating
  a possible denial of service.

  Solution : disable this service in /etc/inetd.conf.

  Risk factor : Low
  CVE : CVE-1999-0103

9.2.6 Problems regarding : echo (7/tcp)

Security warnings :

- The 'echo' port is open. This port is
  not of any use nowadays, and may be a source of problems,
  since it can be used along with other ports to perform a denial
  of service. You should really disable this service.

  Risk factor : Low

  Solution : comment out 'echo' in /etc/inetd.conf
  CVE : CVE-1999-0103

Security note :

- An echo server is running on this port

9.2.7 Problems regarding : time (37/tcp)

Security note :

- A time server seems to be running on this port

9.2.8 Problems regarding : finger (79/tcp)

Security warnings :

- The 'finger' service provides useful information
  to attackers, since it allow them to gain usernames, check if a
  machine
  is being used, and so on...

  Risk factor : Low

  Solution : comment out the 'finger' line in /etc/inetd.conf
  CVE : CVE-1999-0612

- The remote finger daemon accepts
  to redirect requests. That is, users can perform
  requests like :
  finger user@host@victim

  This allows an attacker to use your computer
  as a relay to gather information on another
  network, making the other network think you
  are making the requests.

  Solution: disable your finger daemon (comment out
  the finger line in /etc/inetd.conf) or
  install a more secure one.

  Risk factor : Low
  CVE : CAN-1999-0105

- There is a bug in the finger service
  which will make it display the list of the accounts that
  have never been used, when anyone issues the request :

  finger 'a b c d e f g h'@target

  This list will help an attacker to guess the operating
  system type. It will also tell him which accounts have
  never been used, which will often make him focus his

```
attacks on these accounts.

Solution : disable the finger service in /etc/inetd.conf, or
apply the patches from Sun.

Risk factor : Medium
BID : 3457
```

Security note :

- A finger server seems to be running on this port

9.2.9 Problems regarding : sunrpc (111/tcp)

Security note :

- RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port
- RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port
- RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port

9.2.10 Problems regarding : login (513/tcp)

Security warnings :

- ```
  The rlogin service is running.
  This service is dangerous in the sense that
  it is not ciphered - that is, everyone can sniff
  the data that passes between the rlogin client
  and the rlogin server. This includes logins
  and passwords.

  You should disable this service and use openssh instead
  (www.openssh.com)

  Solution : Comment out the 'rlogin' line in /etc/inetd.conf.

  Risk factor : Low
  CVE : CAN-1999-0651
  ```
  ```

9.2.11 Problems regarding : exec (512/tcp)

Security warnings :

- The rexecd service is open.
  Because rexecd does not provide any good
  means of authentication, it can be
  used by an attacker to scan a third party
  host, giving you troubles or bypassing
  your firewall.

  Solution : comment out the 'exec' line
  in /etc/inetd.conf.

  Risk factor : Medium
  CVE : CAN-1999-0618

9.2.12 Problems regarding : printer (515/tcp)

Security note :

- A LPD server seems to be running on this port

9.2.13 Problems regarding : shell (514/tcp)

Security warnings :

- The rsh service is running.
  This service is dangerous in the sense that
  it is not ciphered - that is, everyone can sniff
  the data that passes between the rsh client
  and the rsh server. This includes logins
  and passwords.

  You should disable this service and use ssh instead.

  Solution : Comment out the 'rsh' line in /etc/inetd.conf.

  Risk factor : Low
  CVE : CAN-1999-0651

9.2.14 Problems regarding : uucp (540/tcp)

Security note :

- The service closed the connection after 0 seconds without sending any data
  It might be protected by some TCP wrapper

9.2.15 Problems regarding : general/tcp

Security note :

- QueSO has found out that the remote host OS is
  * Solaris 2.x

  CVE : CAN-1999-0454

9.2.16 Problems regarding : dtspc (6112/tcp)

Security holes :

- The 'dtspcd' service is running.

  Some versions of this daemon are vulnerable to
  a buffer overflow attack which allows an attacker
  to gain root privileges

  *** This warning might be a false positive,
  *** as no real overflow was performed

  Solution : See http://www.cert.org/advisories/CA-2001-31.html
  to determine if you are vulnerable or deactivate
  this service (comment out the line 'dtspc' in /etc/inetd.conf)

  Risk factor : High
  CVE : CVE-2001-0803
  BID : 3517

9.2.17 Problems regarding : sunrpc (111/udp)

Security note :

- RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port
- RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port

- RPC program #100000 version 2 ’portmapper’ (portmap sunrpc rpcbind) is running on this port

9.2.18 Problems regarding : sometimes-rpc8 (32772/udp)

Security note :

- RPC program #100300 version 3 ’nisd’ (rpc.nisd) is running on this port

9.2.19 Problems regarding : sometimes-rpc21 (32779/tcp)

Security note :

- RPC program #100300 version 3 ’nisd’ (rpc.nisd) is running on this port

9.2.20 Problems regarding : sometimes-rpc12 (32774/udp)

Security note :

- RPC program #100232 version 10 ’sadmind’ is running on this port

9.2.21 Problems regarding : sometimes-rpc14 (32775/udp)

Security note :

- RPC program #100011 version 1 ’rquotad’ (rquotaprog quota rquota) is running on this port

9.2.22 Problems regarding : sometimes-rpc10 (32773/udp)

Security note :

- RPC program #100024 version 1 ’status’ is running on this port

9.2.23 Problems regarding : unknown (32790/tcp)

Security note :

- RPC program #100024 version 1 ’status’ is running on this port

9.2.24 Problems regarding : sometimes-rpc16 (32776/udp)

Security note :

- RPC program #100002 version 2 'rusersd' (rusers) is running on this port
- RPC program #100002 version 3 'rusersd' (rusers) is running on this port

9.2.25 Problems regarding : unknown (32791/tcp)

Security note :

- RPC program #100002 version 2 'rusersd' (rusers) is running on this port
- RPC program #100002 version 3 'rusersd' (rusers) is running on this port

9.2.26 Problems regarding : sometimes-rpc18 (32777/udp)

Security note :

- RPC program #100012 version 1 'sprayd' (spray) is running on this port

9.2.27 Problems regarding : sometimes-rpc20 (32778/udp)

Security note :

- RPC program #100008 version 1 'walld' (rwall shutdown) is running on this port

9.2.28 Problems regarding : sometimes-rpc22 (32779/udp)

Security note :

- RPC program #100001 version 2 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
- RPC program #100001 version 3 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
- RPC program #100001 version 4 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port

9.2.29 Problems regarding : lockd (4045/udp)

Security note :

- RPC program #100021 version 1 'nlockmgr' is running on this port
- RPC program #100021 version 2 'nlockmgr' is running on this port
- RPC program #100021 version 3 'nlockmgr' is running on this port
- RPC program #100021 version 4 'nlockmgr' is running on this port

9.2.30 Problems regarding : unknown (32792/tcp)

Security note :

- RPC program #100221 version 1 is running on this port

9.2.31 Problems regarding : unknown (32793/tcp)

Security note :

- RPC program #100235 version 1 is running on this port

9.2.32 Problems regarding : sometimes-rpc24 (32780/udp)

Security note :

- RPC program #100068 version 2 is running on this port
- RPC program #100068 version 3 is running on this port
- RPC program #100068 version 4 is running on this port
- RPC program #100068 version 5 is running on this port

9.2.33 Problems regarding : unknown (32794/tcp)

Security note :

- RPC program #100083 version 1 is running on this port

9.2.34 Problems regarding : lockd (4045/tcp)

Security note :

- RPC program #100021 version 1 'nlockmgr' is running on this port
- RPC program #100021 version 2 'nlockmgr' is running on this port
- RPC program #100021 version 3 'nlockmgr' is running on this port
- RPC program #100021 version 4 'nlockmgr' is running on this port

9.2.35 Problems regarding : unknown (32812/udp)

Security note :

- RPC program #300598 version 1 is running on this port
- RPC program #805306368 version 1 is running on this port

9.2.36 Problems regarding : unknown (32795/tcp)

Security note :

- RPC program #300598 version 1 is running on this port
- RPC program #805306368 version 1 is running on this port

9.2.37 Problems regarding : unknown (32813/udp)

Security note :

- RPC program #100249 version 1 is running on this port

9.2.38 Problems regarding : unknown (32796/tcp)

Security note :

- RPC program #100249 version 1 is running on this port

9.2.39 Problems regarding : snmp (161/udp)

Security holes :

- ```
  SNMP Agent responded as expected with community name: public
  SNMP Agent responded as expected with community name: private
  SNMP Agent responded as expected with community name: all private
  CVE : CAN-1999-0186
  BID : 177
  ```

Security warnings :

- ```
  It was possible to obtain the list of network interfaces of the
  remote host via SNMP :

  . /etc/snmp/conf/snmpdx.rsrc
  . /etc/snmp/conf

  An attacker may use this information to gain more knowledge about
  the target host.
  Solution : disable the SNMP service on the remote host if you do not
             use it, or filter incoming UDP packets going to this port
  Risk factor : Low
  ```

9.2.40 Problems regarding : xdmcp (177/udp)

Security warnings :

- ```
  The remote host is running XDMCP.

  This protocol is used to provide X display connections for
  X terminals. XDMCP is completely insecure, since the traffic and
  passwords are not encrypted.

  An attacker may use this flaw to capture all the keystrokes of
  the users using this host through their X terminal, including
  passwords.

  Risk factor : Medium
  Solution : Disable XDMCP
  ```

9.2.41 Problems regarding : general/udp

Security note :
  ```

- For your information, here is the traceroute to 10.163.156.16 :
  ?
  10.163.156.16

9.2.42 Problems regarding : font-service (7100/tcp)

Security holes :

- The remote X Font Service (xfs) might be vulnerable to a buffer overflow.

  An attacker may use this flaw to gain root on this host remotely.

  *** Note that Nessus did not actually check for the flaw
  *** as details about this vulnerability are still unknown

  Solution : See CERT Advisory CA-2002-34
  Risk factor : High
  CVE : CAN-2002-1317

9.2.43 Problems regarding : echo (7/udp)

Security warnings :

- The 'echo' port is open. This port is
  not of any use nowadays, and may be a source of problems,
  since it can be used along with other ports to perform a denial
  of service. You should really disable this service.

  Risk factor : Low

  Solution : comment out 'echo' in /etc/inetd.conf
  CVE : CVE-1999-0103

9.2.44 Problems regarding : daytime (13/udp)

Security warnings :

- The daytime service is running.
  The date format issued by this service
  may sometimes help an attacker to guess
  the operating system type.

```
In addition to that, when the UDP version of
daytime is running, an attacker may link it
to the echo port using spoofing, thus creating
a possible denial of service.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103
```

Conclusion

A security scanner, such as Nessus, is not a garantee of the security of your network.
A lot of factors can not be tested by a security scanner : the practices of the users of the network, the home-made services and CGIs, and so on... So, you should not have a false sense of security now that the test are done. We recommand that you monitor actively what happens on your firewall, and that you use some tools such as tripwire to restore your servers more easily in the case of an intrusion.
In addition to that, you must know that new security holes are found each week. That is why we recommand that you visit `http://www.nessus.org/scripts.html`, which is a page that contains the test for all the holes that are published on public mailing lists such as BugTraq (see `http://www.securityfocus.com` for details) and test the security of your network on a (at least) weekly basis with the checks that are on this page.
This report was generated with Nessus, the open-sourced security scanner. See http://www.nessus.org for more information