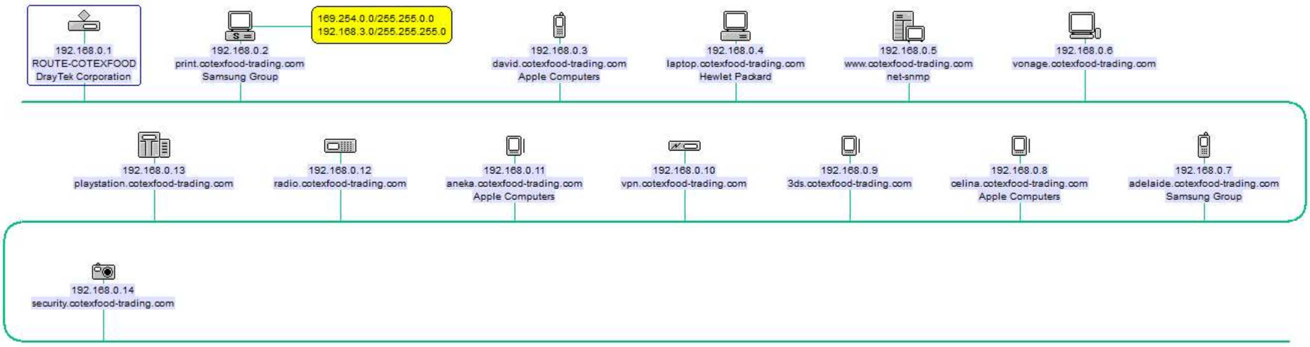

192.168.0.1
ROUTE-COTEXFOOD
DrayTek Corporation
192.168.0.2
print.cotexfood-trading.com
Samsung Group
169.254.0.0/255.255.0.0
192.168.3.0/255.255.255.0
192.168.0.3
david.cotexfood-trading.com
Apple Computers
192.168.0.4
laptop.cotexfood-trading.com
Hewlet Packard
192.168.0.5
www.cotexfood-trading.com
net-snmp
192.168.0.6
vonage.cotexfood-trading.com
192.168.0.13
playstation.cotexfood-trading.com
192.168.0.12
radio.cotexfood-trading.com
192.168.0.11
aneka.cotexfood-trading.com
Apple Computers
192.168.0.10
vpn.cotexfood-trading.com
192.168.0.9
3ds.cotexfood-trading.com
192.168.0.8
celina.cotexfood-trading.com
Apple Computers
192.168.0.7
adelaide.cotexfood-trading.com
Samsung Group
192.168.0.14
security.cotexfood-trading.com

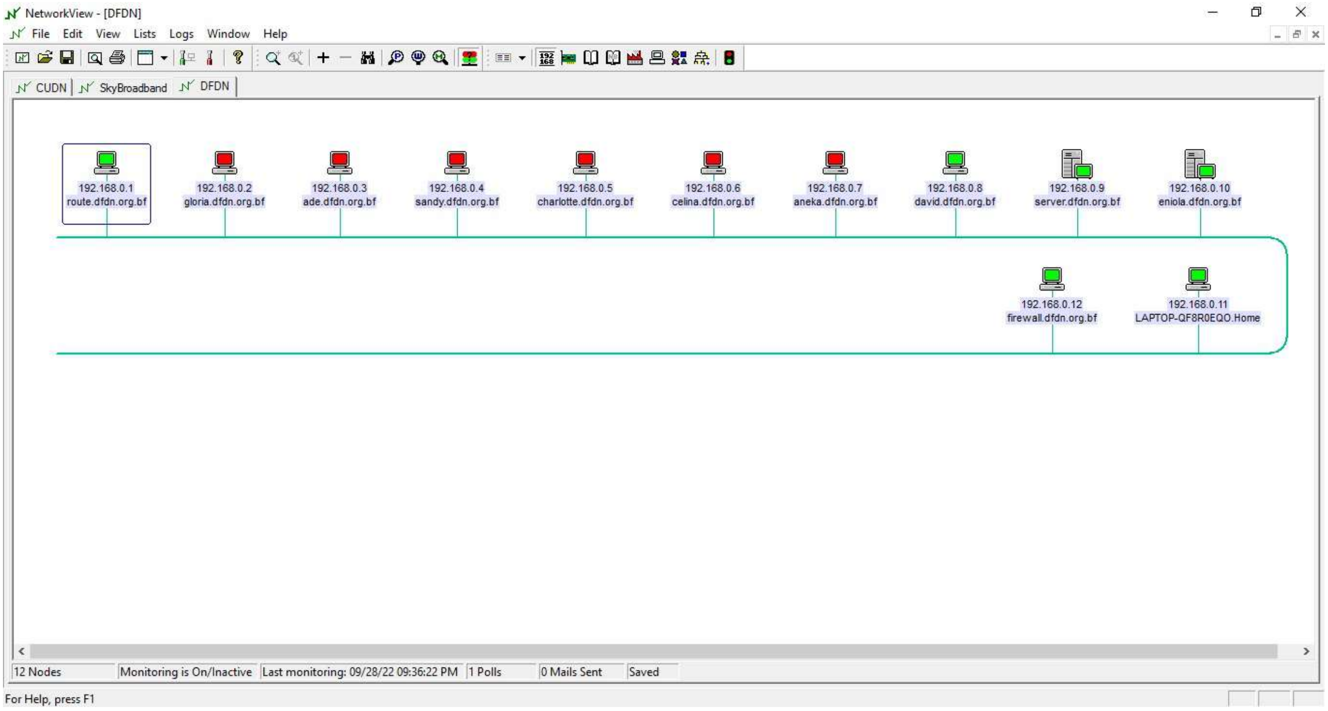
Friendly probing

Last updated Friday, 17 March 2023

-Why

I have decided to perform monthly probes of the network services offered by systems on the Network (DFDN). This will be run automatically as a ‘cron’ job and output by email and/or webpage. The probes have two main aims:

- Detecting security holes before the enemy do.
- Keeping up to date on what services are being run on our network.



12 Nodes | Monitoring is On/Inactive | Last monitoring: 09/28/22 09:36:22 PM | 1 Polls | 0 Mails Sent | Saved

For Help, press F1

The problem

- 12 Hosts under dfdn.org (with more to be added later no doubt!) Need to scale for extended family, business users, etc
- No idea what they’re running
- Security implications as they are visible to the world
- Already have Windows, Unix, IOS, Android, 3DS (a bit of everything - almost!)

- If not maintained, security holes may be discovered by outsiders. Every release of an operating system has a loophole waiting to be found. Once found, loopholes are advertised and automated attacks follow within days.
- Required servers (web, FTP, Telnet, gopher, rlogin, ssh, email etc) need to be patched – kept up to date
- Unnecessary services may be installed at installation time, should be disabled
- Security incidents got out of control on previous network some years ago
- Potential for data theft and financial loss
- A single insecure machine, device, user account or network facing software component can cause a serious security incident.

The probes

Each device/machine's probing starts by attempting a TCP connection to several well-known ports on the system. Those services that are easily interrogated for version information or banner lines are asked for this information. Some security attacks are performed, though I am very conservative about these.
At the moment we get banner or version information from the following services. Each item has a section from the manual describing the service and what the probe attempts to determine.

- domain (The DNS service)
- ftp (FTP and anonymous FTP)
- http (The WWW and CGI programs)
- ident
- imap (Mail reading and organising)
- nntp (Network News servers)
- ntp (Network Time Protocol)
- pop2 (Old mail reading protocol)
- pop3 (Mail reading protocol)
- RFP (Remote framebuffer for windows
- smtp (E-mail delivery)
- snmp (Network management)
- ssh (secure shell)
- telnet
- TFTP (Trivial file transfer)
- XDMCP
- X font server

We also attempt to detect the following:

- Anonymous FTP servers
- Back Orifice
- Forwarding finger servers
- HTTP proxies
- Known insecure CGI scripts
- Known vulnerabilities in MS's IIS and PWS
- Directories NFS exported to everyone
- Passwordless accounts
- Open SMB (Windows networking) shares
- Default community strings with too much access
- Unix RPC services

- Open X servers
- Insecure NIS (YP) servers

These will be added to over time.

The domain name service

The DNS (Domain Name System) is the system by which machines on the Internet are given names. A DNS server is a system which answers DNS queries, either by knowing the answer itself (an authoritative server) or by passing the query on to other servers that do (a recursive resolver). Recursive resolvers generally also maintain a cache to save them having to make so many external requests.

Almost all DNS servers are derived from the Berkeley Internet Name Domain (BIND). Recent versions of this daemon have a feature allowing the remote querying of the version. Older versions of the daemon lack this feature.

The daemon comes in three flavours: version 4 (ancient form), version 8 (old form), and version 9 (new form). Before a certain point there were known security holes in all three forms.

Apple's Rendezvous service discovery system uses an adaptation of the DNS protocols (called Multicast DNS or mDNS) for locating services on the local network.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

This daemon is run to provide a name *service*. It does not need to be running for hostname lookups to be possible on a machine. Typically your machine will have a reference to other name servers.

There does not need to be a name server on any particular network. The router (route.dfdn.org) provides name service for the use of out computers. However, many institutions choose to run one or two servers to provide speedier response. If you do not believe that your system is meant to be running a name server then this service should *not* be provided.

Systems advertising services using Rendezvous need to run an mDNS server.

How to disable this service

This is a daemon that runs continually. Typically there will be a start-up script for it in your system's boot sequence. The common way for this script to decide whether or not to start is to check for the existence of the configuration file. This is typically /etc/named.boot for BIND 4 servers and /etc/named.conf for BIND 8 or 9 servers. The exact location may vary with different vendors' product. If this configuration file is absent the service will not be started at boot.

The Apple mDNSresponder doesn't need any configuration, and Mac OS X 10.2 runs it unconditionally even if it isn't required.

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.

Remember: this page may not be up to date; this page was last updated on 2015-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- BIND, the canonical Unix DNS server (source releases are here as well). Versions 9.2.2, 8.3.4 and 4.9.11 are believed to be secure.

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- CA-2001-02: Multiple Vulnerabilities in BIND
- CA-1999-14: Multiple Vulnerabilities in BIND
- CA-98.05.bind_problems
- CA-97.22.bind

The File Transfer Protocol (FTP) service

The FTP daemon is the daemon that allows files to be transferred to and from a system by remote clients. There are two main versions of this daemon, the Berkeley original and the Washington University version. The former is used by most commerical vendors and has been modified extensively by them.

You may be running an FTP daemon without realising it. Certain versions of the NCSA telnet program enabled an FTP service by default. These appear on a Macintosh with the reported banner line **Macintosh Resident FTP server, ready** and are covered by a 1991 CERT advisory: CA-91:15.NCSA.Telnet.vulnerability.

Some FTP daemons permit *"anonymous"* access. This means that any user in the world can access certain files. If the anonymous access is set up correctly, only a restricted set of files is accessible anonymously. Some FTP daemons switch on support for anonymous FTP if the user ftp is defined on the system. So you may be running anonymous FTP without realising it.

The last, and least common, configuration is the *"incoming"* mode. This lets anonymous users place files on your server. While you may have intended it for use by just your friends or colleagues these servers get found by others very easily and are typically used by software pirates and pornographers. If you need to do this, you should at least read the WU-FTPD upload.configuration.HOWTO.

Warning: Under UK law if you are found with certain classes of pornography on your system you are guilty of a serious crime. No intention on your part need be proved by the prosecution.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

The daemon is not needed just to run the FTP client on a system, i.e. if you just want to be able to get files from elsewhere onto your own computer. If you allow remote users access to files through Unix clients like ftp or Macintosh clients like fetch, or if you allow anonymous FTP then you need this daemon. Otherwise you do not.

How to disable this service

To turn off FTP services altogether on a Unix box, comment out or remove the ftp line in the file /etc/inetd.conf.

After editing the /etc/inetd.conf file the inetd daemon it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.

On a system with a System V style ps: # **ps -e | grep inetd** 133 ? 0:03 inetd 1513 pts/5 0:00 grep inetd # **kill -HUP 133**

On a system with a BSD style ps: # **ps -ax | grep inetd** 212 ? S 0:00 inetd 1549 p2 S 0:00 grep inetd # **kill -HUP 212**

On a **Berkeley-derived** FTP daemon, to prevent anonymous access make sure that the ftp user does not exist on your system.

On a system using **Microsoft Internet Information Server** (IIS), FTP can be disabled by stopping the service from the IIS Console File menu, and then going into the Services Control Panel and disabling it there as well. If you need FTP in general, but not anonymous FTP, the latter can be disabled by double-clicking on the relevant service line (ftp here) in the IIS Console and unticking the Anonymous box. If you need access via ftp you are best to limit it to named machines (by IP number) and low-level (User or Domain User) accounts.

For Windows NT 4.0 go to Control Panel - Services. Find FTP service, Highlight FTP service and click STOP. Click on the Start-up Button and make sure the service is selected as being disabled.

For Windows 2000 go to Control Panel - Administrative tools - Services. Find and open the FTP service, Stop the service (if running), go to the Start-up type pull down menu and select disabled. If you are running IIS and do not need FTP services, un-install them as well.
To disable FTP access to a **Hewlett-Packard JetDirect** network printer, connect to the printer by telnet (which should have a password set), and type `ftp-config: 0` then `quit`. See this document on HP's support Web site for more details.

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.
Remember: this page may not be up to date; this page was last updated on 2012-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- Versions of the Washington University FTP daemon WU-FTPD is the most popular free FTP daemon for Unix. Version 2.6.1 is believed to be secure.
- ProFTPD - Professional FTP Daemon Another, more recent, free FTP daemon for Unix. Version 1.2.0 is believed to be secure.
- linux-ftpd, a BSD-derived FTP server for Linux; part of the Linux NetKit. Version 0.17 is believed to be secure.
- War FTP Daemon An FTP daemon for Windows. Versions 1.67b3 and 1.71 are believed to be secure.
- On a commercial Unix check that you are up-to-date on your patches.
- NetPresenz for the Macintosh is available from I Software Sales at no charge. There are no known security problems.
- NCSA Telnet: If you use this you should ensure that FTP is turned off.

Vendor documentation

These are relevant pieces of on-line documentation from various vendors of software which provides this service. If your favourite operating system isn't listed, this doesn't necessarily mean it doesn't provide the service.
Note that most documentation is for the latest version of the software. Older versions are often lacking the security features found in new ones.
Irix 6.5
ftpd(1M)
NetBSD
ftpd(8)
Solaris 7
ftpd(1M)
Tru64 Unix
ftpd(8)

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- BugTraq ID 2052: Serv-U FTP Directory Traversal Vulnerability
- CA-2000-13: Two Input Validation Problems In FTPD
- SECURITY ALERT - WAR FTP DAEMON ALL VERSIONS
- Windows 95/NT War FTPD 1.65 Buffer Overflow
- MS99-003: Patch Available for IIS "Malformed FTP List Request" Vulnerability
- CA-99-13-wuftpd.txt
- CA-99-03-FTP-Buffer-Overflows
- CA-97.16.ftpd
- CA-95.16.wu-ftpd.vul
- CA-91.15.NCSA.Telnet.vulnerability
- CA-88.01.ftpd.hole

Patches for this service

Patches vary beteween vendors. Sun's patches for Soalris tend to patch only a restricted set of binaries. Silicon Graphics tend to produce patches for software subsets. Red Hat produce updated software packages. Compaq generate a single patch file for the entire base DEC OSF/1 operating system.

Web servers and the programs they run

The HyperText Transfer Protocol (HTTP) is the language spoken by web servers. Any system running a web server must be running some program to provide that service. The default port for a web server is port 80, but other port numbers (typically featuring lots of 8s) are used as well.

- Port **98** is used by linuxconf's network interface
- Port **311** is used by AppleShare IP
- Port **591** is used by FileMaker Pro
- Port **801** is used by StarOffice
- Port **2077** is used by SGI's web admin facility
- Port **2301** is used by OSF/1's insightd
- Port **3128** is used by squid
- Port **8888** is used by dynaweb

By far the most common web server on Unix platforms is the Apache web server.

Web servers can run programs for users via Common Gateway Interface (CGI) programs, Active Server Pages (ASPs) or Server Side Includes (SSIs). Intrusions via web servers typically enter via these routes rather than directly through the static web page service.
The CGI scripts the probe tests for are those that have been mentioned in security alerts or found in hacker toolkits.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
If you are a web *server* then you need to be running this service. You do not need to be running it to browse the web.

How to disable this service

The web server is a daemon that runs continually. There will be a startup script that launches it at boot time. You can either remove this startup script or read it to see if it checks for the presence of a configuration file to decide whether to launch the daemon. Removing or renaming the configuration file would then also stop the daemon being launched.
If you want to run the web server but not the program-running components (CGI, ASP, SSI) you will need to consult the documentation for the particular server you run.
Notes for Apache to follow.

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.
Remember: this page may not be up to date; this page was last updated on 2012-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- The Apache server project (from Imperial College's SunSite)

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- Bugtraq: Vulnerability in infosrch.cgi
- MS99-061: Patch Available for "Escape Character Parsing" Vulnerability
- MS99-058: Patch Available for "Virtual Directory Naming" Vulnerability
- Imagemap CGI overflow exploit
- ISS advise37: Buffer Overflow in Netscape Enterprise and FastTrack Web Servers
- MS99-029: Patch Available for "Malformed HTTP Request Header" Vulnerability
- MS99-025: Re-Release: Unauthorized Access to IIS Servers through ODBC Data Access with RDS
- MS99-010: Patch Available for File Access Vulnerability in Personal Web Server
- MS98-004: Unauthorized Access to IIS Servers through ODBC Data Access with RDS
- CA-98.04.Win32.WebServers
- CA-97.25.CGI_metachar
- CA-97.24.Count_cgi
- CA-97.12.webdist
- CA-97.07.nph-test-cgi_script
- CA-96.11.interpreters_in_cgi_bin_dir
- CA-96.06.cgi_example_code

Identification Protocol

The "ident" service, officially described in RFC 1413 at the "Identification Protocol", is *not* an authentication protocol. Instead, it's a means by which a TCP server can gain a little extra information about an incoming connection for its logs. Typically, this is the userid of the user making the connection, but some identds retrun other information.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
Generally, running an ident server is a good idea on a multi-user system, as it allows you to track down which of your users was responsible for a given connection. It's rather less necessary on a single-user system, where one user can be assumed to be responsible for all connections.

How to disable this service

On Unix systems, ident servers are generally started from inetd, so you'll need to find the line mentioning identd in /etc/inetd.conf and comment it out or remove it.
After editing the /etc/inetd.conf file the inetd daemon it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.
On a system with a System V style ps: # **ps -e | grep inetd** 133 ? 0:03 inetd 1513 pts/5 0:00 grep inetd # **kill -HUP 133**
On a system with a BSD style ps: # **ps -ax | grep inetd** 212 ? S 0:00 inetd 1549 p2 S 0:00 grep inetd # **kill -HUP 212**

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.
Remember: this page may not be up to date; this page was last updated on 2012-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- Pidentd (the usual Unix ident server) can be obtained here. All versions are believed secure.

Internet Message Access Protocol

The Internet Message Access Protocol (IMAP) is a mechanism for reading and manipulating mail on a remote server. It comes in two versions, IMAP 2 and IMAP 4. There was an experimental protocol called IMAP 3 but it was superseded by IMAP 4 and is not used.
Security flaws (buffer overflow bugs) in various versions of the common IMAP daemons was a common means of enemy entry into both company and domestic Linux systems a few years ago, and at the time of writing probes for IMAP are still seen regularly.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
You typically do not need to be running this service. Only systems that store mail for it to be read need run this service. Systems that emit email and which use IMAP to read mail on other systems (e.g. imap.hermes.) need not run this service.

How to disable this service

IMAP is started from the inetd. Edit the /etc/inetd.conf file and comment out or delete the imap entry:

```
# imap stream tcp nowait root /usr/sbin/tcpd in.imapd
```

After editing the /etc/inetd.conf file the inetd daemon it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.
On a system with a System V style ps: # **ps -e | grep inetd** 133 ? 0:03 inetd 1513 pts/5 0:00 grep inetd # **kill -HUP 133**
On a system with a BSD style ps: # **ps -ax | grep inetd** 212 ? S 0:00 inetd 1549 p2 S 0:00 grep inetd # **kill -HUP 212**

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.
Remember: this page may not be up to date; this page was last updated on 2012-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- Pending

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- CA-98.09.imapd
- CA-97.09.imap_pop

Network News Transfer Protocol

NNTP is the service run by news servers to provide News to clients such as trn, nn Outlook, Newstap or Netscape.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
You (almost certainly) do not need to be running this service.

How to disable this service

The NNTP service is typically run continually and is started in a boot script. Find that script and turn it off.

The Network Time Protocol

The Network Time Protocol (NTP) is a means of syncronising the clock on a networked machine to a known-accurate time source.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
It's generally a good idea for systems to be running an NTP client, as this ensures that its ideas about time correspond to those of the rest of the world. This can be useful for things like correlating log-file entries from different machines when tracing a fault or investigating a breakin. Unfortunately, the standard NTP client software for Unix also acts as a server by default, and it's difficult to turn this off. Our probe indicates which stratum a machine is operating at. In general, random workstations should be at stratum 4, departmental NTP servers at stratum 3 and Main NTP servers at stratum 2.

How to disable this service

In general, turning off NTP isn't a good idea, but it's possible. The NTP server on Unix systems is a long-running process called ntpd or xntpd, and can be disabled by messing with the startup scripts in some way.

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.
Remember: this page may not be up to date; this page was last updated on 2003-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.
• The standard Unix NTP implementation. Versions of ntpd from 4.0.99k23 onwards are believed to be secure. All versions of xntpd are believed to be insecure.

Post Office Protocol

The Post Office Protocol (POP) is a mechanism for reading mail on and optionally fetching mail from a remote server. It comes in two versions, POP 2 and POP 3.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

POP 2 is an extinct protocol. You do not need to be running this.

You typically do not need to be running a POP 3 service either. Only systems that store mail for it to be read need run this service. Systems that emit email, and which use POP to read mail on other systems, need not run this service.

How to disable this service

POP daemons (one for each version) are started from the inetd. Edit the /etc/inetd.conf file and comment out or delete the pop2 and pop3 entries: # pop-2 stream tcp nowait root /usr/sbin/tcpd pop2d # pop-3 stream tcp nowait root /usr/sbin/tcpd pop3d
After editing the /etc/inetd.conf file the inetd daemon it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.
On a system with a System V style ps: # **ps -e | grep inetd** 133 ? 0:03 inetd 1513 pts/5 0:00 grep inetd # **kill -HUP 133**
On a system with a BSD style ps: # **ps -ax | grep inetd** 212 ? S 0:00 inetd 1549 p2 S 0:00 grep inetd # **kill -HUP 212**

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.
Remember: this page may not be up to date; this page was last updated on 2012-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- Pending

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- bugtraq id 283: Univ. of Washington pop2d Buffer Overflow Vulnerability
- CA-98.08.qpopper_vul
- CA-97.09.imap_pop

Simple Mail Transfer Protocol

The Simple Mail Transfer Protocol (SMTP) is the protocol by which email messages are sent from machine to machine. This does not include the reading of mail by the end user by protocols such as POP or IMAP.

There is a wrinkle with SMTP which is not present for the other services described in these pages. You may well want the mail daemon running permanently to handle outgoing mail. If you do not want it to listen for *incoming* mail you need to change its configuration.

The most common mail daemon is sendmail which is a truly ancient piece of software dating back to near the dawn of the Internet. More recently smail, qmail, exim and Postfix have risen to replace it. I have the most experience with Postfix

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

You need to be running an SMTP *listener* only if you are a mail hub. You would not be a mail hub without your machine being intentionally set up to handle mail, so it's not something that happens by accident. If you are not then you should not be running this service.

How to disable this service

As described above, you may not want to disable the daemon, but only its listening habits. The most common Unix mail daemon is sendmail and the other daemons that have followed have copied its command line arguments for compatibility's sake. It is started in an initialisation script run at boot time. If it is started with the -bd option it will run as a listener. You need to remove this option from the startup script to stop sendmail from listening after the next reboot. Then kill and restart the sendmail daemon without the option to deal with the current instance.

For Windows NT systems, see the guidance produced by NT help and documentation.

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.

Remember: this page may not be up to date; this page was last updated on 2012-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- To follow

Relevant advisories
These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- CERT Advisory CA-2012-12 Buffer Overflow in Sendmail
- CERT Advisory CA-2012-07 Remote Buffer Overflow in Sendmail
- CA-98.10.mime_buffer_overflows
- CA-97.05.sendmail
- CA-96.25.sendmail_groups
- CA-96.24.sendmail.daemon.mode
- CA-96.20.sendmail_vul
- CA-95:08.sendmail.v.5.vulnerability

Last updated: 2012-06-10

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is a protocol for managing networked devices. It's typically used by such things as network hubs and printer servers, but there are also implementations for most full-blown operating systems.
SNMP agents (as its servers are usually known) typically allow one to gather various information about the network stack of a device, and often of many of its other aspects. Most implementations also allow at least some parameters to be changed remotely.
Access to SNMP agents (at least in simple implementations) is controlled by "community strings", which are effectively passwords. Most implementations use "public" as a standard community string for read-only access. The default community-string for read-write access varies between vendors, and anyway it's a good idea to change it. Our probe attempts to detect hosts with unchanged read-write community strings. Any that are found are listed in the summary with a "BAD PASSWORDS" tag. It also detects a few "back door" community strings provided by certain SNMP agents.
There's a bug in at least some 3Com SNMP implementations whereby the read-write community strings can be read from a device if you know the read-only community string. Our probe detects that too.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

You need to be running an SNMP agent if you want to be able to manage your system remotely using SNMP. This is not likely to be the case for most workstations and servers, but may be useful for hubs, printers and the suchlike. Some systems may use SNMP without it being obvious. Hewlett-Packard's JetAdmin and 3Com's Quick Config Manager are examples.
You almost certainly do not need to have well-known read/write community strings.

How to disable this service

Since so many types of device run SNMP agents, it's almost impossible to provide generic instructions for either disabling SNMP or changing community strings. Here, we provide instructions for some systems we've tried.

Unix systems

SNMP services are usually provided by a process called snmpd, which runs continuously. You should be able to modify your system startup scripts to disable it.

Solaris (version 2.6 and 2.7)

In Solaris, the SNMP agent is in the "SUNWsasnm" package, and can be disabled by removing this package.

In Solaris 2.6, the agent defaults to allowing read-write access with the community string "private". The read/write community string can be changed by editing /etc/snmp/conf/snmpd.conf. If you only need read access, you should edit /etc/snmp/conf/mibiisa.rsrc so that the command line reads:

```
command = "/usr/lib/snmp/mibiisa -r -p $PORT"
```

Solaris 2.7 is configured like this by default.

3Com network hubs and switches

In general, the easiest way to change the community strings on 3Com hardware is using the terminal interface. This can be accessed either by telnet over the local network, or by plugging a serial console into the back of the unit. While many recent hubs have pretty Web interfaces as well, it tends not to be possible to set SNMP community strings using them.

Most 3Com hardware has three levels of user, "monitor", "manager" and "security". There are usually three users configured into the system by default, with the same names as their levels. More recent devices add an extra "security" level user called "admin". The default community strings for these users are (respectively) "public", "manager", "security" and "private".

It's usually possible to modify which users of a device are allowed to access it by which route (serial, telnet, SNMP, web), so if you don't need read-write access by SNMP, it's probably a good idea to disable SNMP access for all users except "monitor".

There follow instructions for changing the default community strings on those pieces of 3Com kit I can readily lay my hands on.

3Com SuperStack II PS Hub 40/50 (version 1.xx)

As far as I know, the command-line interface to these hubs doesn't permit the changing of community strings. Instead, you should use the Quick Config Manager (documented in the manual that came with the hub) to change each community string in turn. The relevant dialogue box is "Edit Access Levels", available from the "Access Conf" pane of tyhe "General Info" box.

3Com SuperStack II PS Hub 40/50 (version 2.10)

The community string for "manager" and "security" level users can be changed through the device's command-line. Connect to it by telnet or through the serial port, log in as a user at the appropriate level, and type `snmp community`. You will be prompted for an new community string for that user, which you should provide. You can then log out of the device by typing `logout`, and repeat the process with the other user names.

SNMP access for individual user levels can be disabled using the Quick Config Manager (Configure -> General Info -> Access Conf).

To disable all remote access to the hub (telnet, web and SNMP), connect by telnet or through the serial port, log in as a "security" level user and type `system remoteAccess disable`, then `logout`. You will now only be able to log in over the serial line.

Note that these hubs have a security hole which means that allowing any read/write SNMP access at all is dangerous. This is apparently fixed in firmware version 2.13. If your hub is running a vulnerable version, you should get the new version here

3Com SuperStack II Switch 3300 (version 1.09)

To change community strings: Over the serial line or telnet, log in as a "security" level user and type `snmp community`. You'll then be prompted for SNMP community strings for all the configured users of the switch. It's OK (and probably desirable) to leave the community string for "monitor" set to "public", but all of the others should be set to something secret.

3Com FMS, FMS II and SuperStack II Hub 10 (all versions?)

To change community strings: Using the VT100 interface, log in as the user whose community string you want to change and choose "SECURITY", "CHANGE USER", type the new community string in the field provided and choose "OK". This should be repeated for all "security" and "manager" level users.

To stop a particular level of user using SNMP at all, log in as a "security" level user, choose "SECURITY", "LOCAL SECURITY" and set the relevant entry in the "Community-SNMP" row to "Disabled".

HP JetDirect 600N print server (version G.07.03)

To change the community string: Connect to the printer by telnet (which should have a password set), and type set-cmnty-name:*comm*, where *comm* is the new community name, which should be kept secret. Leaving the community name blank seems to cause the server to accept set requests from "public", which is bad. This appears to be a change from version G.05.35 of the JetDirect firmware.

If you've got an access list set up for the printer, then only hosts on it will be able to issue SNMP set requests to the printer, so this can provide a reasonable measure of security.

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.

Remember: this page may not be up to date; this page was last updated on 2012-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- The ucd-snmp implementation for Unix.
- Solstice Enterprise Agents for Solaris. Version 1.0.3 is believed to be secure.

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- bugtraq id 986: Multiple Vendor SNMP World Writeable Community Vulnerability
- Sun #00178: SNMP
- HPSBUX9811-088: Security Vulnerability with snmp
- ISS 1387: hpov-hidden-snmp-comm

Secure Shell

Secure Shell (SSH) is a protocol for making secure terminal connections over the Internet. It also provides various other facilities such as remote command execution and X11 session forwarding. An SSH daemon (sshd) allows users of your system to access it securely from a remote location. If you want to allow users to access your system over the network, ssh is one of the safest ways to do so (if it's configured correctly).

Some versions of sshd have been known to have security problems. More details on this when I find them.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

You should be running sshd if you want to allow users of your system to log in remotely. If you're running a telnet or rsh service, you should probably also be running ssh.

How to disable this service

sshd usually runs continually, so there'll be something in your system startup scripts to launch it. Remove this to disable sshd.

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.
Remember: this page may not be up to date; this page was last updated on 2012-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- The OpenSSH web site.

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- CAN-2001-0144
- CA-98.03.ssh-agent

The TELNET protocol.

TELNET is the original (more or less) and ubiquitous Internet remote-login protocol. It's usually used to provide interactive, unencrypted remote login to a system from text terminals (or more often, emulators of them).

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
You need to be providing TELNET services if you want people to be able to log in to your system over the network, and you don't want to force them to use ssh or similar. Many embedded systems in printers and suchlike use TELNET for configuration.

How to disable this service

On Unix systems, the TELNET service is provided by a program called telnetd or in.telnetd. This is usually spawned from inetd, so to disable it you need to remove or comment out the telnet line from /etc/inetd.conf.

After editing the /etc/inetd.conf file the inetd daemon it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.
On a system with a System V style ps: # **ps -e | grep inetd** 133 ? 0:03 inetd 1513 pts/5 0:00 grep inetd # **kill -HUP 133**
On a system with a BSD style ps: # **ps -ax | grep inetd** 212 ? S 0:00 inetd 1549 p2 S 0:00 grep inetd # **kill -HUP 212**

Trivial File Transfer Protocol

The Trivial File Transfer Protocol (TFTP) is a simple UDP-based protocol for transferring files. Its two major uses are for bootstrapping diskless machines (or machines which are being installed over the network) and for installing new firmware images in networked devices such as printers and hubs.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
A computer generally only needs to run a TFTP server if it's acting as a boot server for other systems in some way, either for diskless clients, or for remote installations. For one-off firmware upgrades, it may be necessary to run a tftp server temporarily. Some devices (Allied-Telesyn hubs, for instance) can also run a TFTP server, again for firmware upgrades.
Since TFTP has no inherent access control, it's usual for the server to provide access only to a fraction of the files on a system. Our probe attempts to get a file called "/etc/passwd". If it succeeds, your system probably allows the world to get any file readable by the user the TFTP server runs as (usually nobody). This is probably a Bad Thing.

How to disable this service

On Unix systems, the TFTP service is provided by tftpd or in.tftpd. This is usually spawned fron inetd, so to disable it, comment out (with a # at the start of the line) the line in /etc/inetd.conf which begins tftp.
After editing the /etc/inetd.conf file the inetd daemon it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.
On a system with a System V style ps: # **ps -e | grep inetd** 133 ? 0:03 inetd 1513 pts/5 0:00 grep inetd # **kill -HUP 133**
On a system with a BSD style ps: # **ps -ax | grep inetd** 212 ? S 0:00 inetd 1549 p2 S 0:00 grep inetd # **kill -HUP 212**

How to secure this service

If you decide that you do need to run this service, then securing it requires a combination of keeping the software up-to-date (typically with patches) and correct configuration.
Restricting the set of directories the tftp server can access is usually accomplished by passing command-line arguments to tftpd. See your system documentation for details.

Vendor documentation

These are relevant pieces of on-line documentation from various vendors of software which provides this service. If your favourite operating system isn't listed, this doesn't necessarily mean it doesn't provide the service.
Note that most documentation is for the latest version of the software. Older versions are often lacking the security features found in new ones.
AIX 4.3
tftpd Daemon
FreeBSD
tftp(8)
IRIX 6.5
tftpd(1M)
NetBSD
tftpd(8)
Solaris 7
tftpd(1M)
Tru64 Unix 5.0
tftpd(8)

The X Display Manager Control Protocol

The X Display Manager Control Protocol (XDMCP) is used by X terminals (and X servers in general) to set up an X session with a remote system over the network.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

You need to be running this service if you want to allow remote X servers to start login sessions on your system. This isn't generally necessary on a random workstation, but can be a good idea on large multi-user machines, or and environment with lots of underpowered X terminals.

How to disable this service

On Unix systems, the XDMCP service is usually provided by the xdm daemon, which runs continuously. Since it often also provides a login service to the X server running on the same machine, disabling xdm entirely may not be a good idea. xdm's provision of display management to the world is controlled by the Xaccess file, found in /var/X11/xdm, /etc/X11/xdm or XROOT/lib/X11/xdm. If this contains no lines that aren't blank or comments, xdm will refuse to manage any remote display. For other configurations, look at the "XDMCP ACCESS CONTROL" section of xdm(1).

On systems using the Common Desktop Environment (CDE), including recent Digital Unix, Solaris and HP-UX systems, the XDMCP service is provided by dtlogin. It uses the same format of Xaccess file as xdm, but stores it in both /usr/dt/config and /etc/dt/config. You should copy it from the former to the latter before editing it, unless it's there already.

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- "gdm" remote hole

X Font Server

The X font server (xfs) provides a standard mechanism for an X server to communicate with a font renderer, frequently running on a remote machine. It usually runs on TCP port 7100 or thereabouts.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

You need to be running xfs if you want a remote X terminal to be able to use fonts from your system, or if you want to use fonts that your X server doesn't understand (and the font server does).

How to disable this service

xfs usually runs continuously, and should be disabled by suitable modifications to your startup scripts. Alternatively, if you only need access from an X server on the local machine, you can add the line "no-listen = tcp" to the xfs configuration file (usually /etc/X11/xfs/config or *XROOT*/lib/X11/xfs/config) to stop it listening on the network.

Back Orifice

Back Orifice is a Windows program which allows control of the machine over the network. Our probe attempts to detect systems running Back Orifice with no password set.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
Although it has been touted as a "remote administration" tool, the current version of Back Orifice is mostly of more dubious use. You probably shouldn't be running it.

How to disable this service

A good explanation of what Back Orifice is and how to remove it can be found here.

The Finger service

The Finger protocol is used to find out information about users on a remote system. Finger servers can usually provide either a list of logged-in users or detailed information on a single user.
Some Finger servers can be configured to allow them to forward incoming queries to arbitrary other hosts. This is a Bad Idea, and will be flagged with a WARNING if we detect it.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
You need this service if you want users of other systems to be able to use the finger program to find out about users of your system. You almost certainly do not need to be running a forwarding Finger service (Even the RFC defining Finger doesn't give any reasons to enable it.).

How to disable this service

On Unix systems, in.fingerd is usually started by inetd, and can thus be disabled by removing the finger entry from inetd.conf.
After editing the /etc/inetd.conf file the inetd daemon it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.
On a system with a System V style ps: # **ps -e | grep inetd** 133 ? 0:03 inetd 1513 pts/5 0:00 grep inetd # **kill -HUP 133**
On a system with a BSD style ps: # **ps -ax | grep inetd** 212 ? S 0:00 inetd 1549 p2 S 0:00 grep inetd # **kill -HUP 212**

How to secure this service

If you decide that you do need to run this service, then securing it requires a combination of keeping the software up-to-date (typically with patches) and correct configuration.
Turning off forwarding in the finger daemons supplied with Solaris 7 and Tru64 Unix 5.0 appears to be impossible.

Web proxies

The HyperText Transfer Protocol (HTTP) is the language spoken by web servers. Any system running a web server must be running some program to provide that service. The default port for a web server is port 80, but other port numbers (typically featuring lots of 8s) are used as well.
A web proxy is a system that takes HTTP requests and forwards them to another server. They are not, in themselves, insecure but can be used to circumvent access controls. Consider an ill-advised attempt to restrict access to certain web pages to our domain by only permitting accesses from addresses within that domain. An external (non-DFDN) host can connect to a proxy within and ask it to request the page(s). The proxy makes the request and makes it from within so the request is honoured. The request is then forwarded to the external system, circumventing the naïve attempt at restriction.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
Unless you are running an internal web cache you do not need to be running this service.

How to disable this service

Apache, the Internet's most popular web server, can be configured to be a proxy server but is not by default. Comment out the proxying part of the httpd.conf file and restart the daemon to disable this service.

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.
Remember: this page may not be up to date; this page was last updated on 2012-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- The Apache server project (from Imperial College's SunSite)

Microsoft's Internet Information Service (Web server)

Microsoft's web server, IIS, is enabled by default on installation of the underlying operating system. Most IIS instances on the Internet are unintended.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
If you are a web *server* then you need to be running this service. You do not need to be running it to browse the web.
Numerous security holes have made IIS a target for worms and other malware, such as the ‘code red’ or ‘Nimda’ worms.You might therefore like to consider running Apache on NT, rather than IIS.

How to disable this service

Instructions to follow.

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.
Remember: this page may not be up to date; this page was last updated on 2001-07-24. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- The current version of IIS is 5.0. You should not be running older versions than 4.0.

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- MS01-023
- MS01-033

Insecure NFS exports

The Network File System (NFS) is Unix's most common way of sharing directory trees between systems. Unfortunately, the standard syntax for the file controlling the exports is very messy and leads the administrator into making dangerous mistakes. The default export, for example, is read-write to the world.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
If you want to share ("export" in the jargon) some of your files with other systems then you need to be running the service. Otherwise you do not. You do need to decide whether the exports really need to be read-write or whether read-only would suffice.
You do not need to be running the NFS server to import other servers' file systems.

How to secure this service

If you decide that you do need to run this service, then securing it requires a combination of keeping the software up-to-date (typically with patches) and correct configuration.
/etc/exports
This file consists of a series of lines. Each starts with the directory to be exported and then has a series of options for the export which define which machines it is to be exported to and with what options.
The simple line /fubar exports the directory /fubar to the world, read-write. Even if the individual files in the directory are not writable, root on the client end could override the permissions. This extremely insecure configuration is, unfortunately, what you get with no options.
The exact syntax uses varies between systems. RTFM.
/etc/dfs/dfstab

How to disable this service

If you don't want to export anything simply stop the NFS service. How this is done varies from system to system.
The NFS service is started by some start up scripts. These vary between systems.
On a RedHat 5 box, run # **chkconfig --level 0123456 nfs off** # **/etc/rc.d/init.d/nfs stop** Shutting down NFS services: to stop the service being started at subsequent reboots and then to stop the current running service.
More O/Ses!

Passwordless accounts

Some Unices ship with passwordless accounts. This probe tests for the more common ones through the rsh service.

How to secure this service

If you decide that you do need to run this service, then securing it requires a combination of keeping the software up-to-date (typically with patches) and correct configuration.
The passwords are probably defined in /etc/passwd or /etc/shadow. See the document How to check for passwordless accounts for details.

The Server Message Block protocol

The Server Message Block (SMB) protocol is a protocol used by various Microsoft operating systems for, amongst other things, sharing files and printers. It can be implemented over many low-level network protocols including TCP/IP. Under Windows, SMB is referred to as "Microsoft Networking".

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

You probably need to be running an SMB service if you want to make files and printers available to Windows systems, although there are other protocols they can use.

How to disable this service

How to disable SMB services will depend on the kind of system you're using.
Windows NT
By default NT is configured to start SMB automatically. Log in as administrator (or equivalent). From the Services icon in the Control Panel (under Settings in the Start Menu), find the Server service. If the Server is started then you are potentially offering SMB / printer services from your workstation. If you have no intention of offering SMB or Printer services to anyone i.e. sharing printers or folders with anybody then firstly stop the service (via the stop button) and then double-click on the Server line. You will be offered the choice of manually or automatically starting the Server service, or disabling it. Disable it and close the panel.
If you wish to offer services, then make sure that only the directories which need to be shared are offering the service and ensure that sharing is switched off on any which aren't needed. It is also a good idea to offer the share on a specific directory which only has the files offered in it (for this level of protection you really need to have the partition formatted as NTFS, not FAT). If possible do not share the root of any drive, even if the share is hidden. Make sure that any shares being offered are only accessible by offering some kind of credentials (at the very least a password).
You should be aware that the default permissions on a share offered from NT are "Everyone: Full Control". This is wholly insecure; for example the Guest account is often left enabled and without a password, thereby giving anyone who can connect to the share complete access to it. You should:

- Disable the Guest account.
- Remove the permission "Everyone: Full Control" and assign only those permissions to only those groups of users which are needed.

NB do not be tempted to apply "Everyone: No Access" to a share. "No Access" overrides any other assigned or inherited permissions, and the effect will be to deny every user access, including Administrator. This is probably more security than you actually want.

Unix (Samba):

SMB services are provided by processes called smbd and nmbd. These can either be permanently-running, in which case they'll be started by the system startup scripts, or started by inetd. If they're started by inetd, there'll be two lines in /etc/inetd.conf beginning netbios-ssn and netbios-ns, whcih can be commented out or removed to disable the service.

Mac OS X

In the "Sharing" panel of System Preferences, turn off "Windows File Sharing".
After editing the /etc/inetd.conf file the inetd daemon it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.
On a system with a System V style ps: # **ps -e | grep inetd** 133 ? 0:03 inetd 1513 pts/5 0:00 grep inetd # **kill -HUP 133**
On a system with a BSD style ps: # **ps -ax | grep inetd** 212 ? S 0:00 inetd 1549 p2 S 0:00 grep inetd # **kill -HUP 212**

Current versions

These are the latest versions of the software. Unless marked otherwise we knew of no security holes in the versions when this page was written. Where possible these entries are links to the latest versions of the software.
Remember: this page may not be up to date; this page was last updated on 2012-06-10. If a security warning later than this brought you to this page then the versions below may not contain the right fixes yet.

- Samba, a free SMB implementation for Unix. Versions 2.2.8a and later are believed to be secure.

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- Security bug in Samba 1.9.17p1 and earlier
- Security bug in Samba 1.9.18p5 and earlier
- Security bug in Samba 2.0.4b and earlier
- VU#267873: Samba contains multiple buffer overflows

DRAFT - Sun Remote Procedure Call

This is a draft page and is still under construction.

Sun RPC is used widely by Unix systems and not just Suns. It provides a simple way to write networked applications and has proved mildly popular.

In essence a Sun RPC network server does not connect directly to a well known port, but rather asks another service called the "portmapper" or "rpcbind" to assign it a port. It then binds to that port. When a client wants to find that service it queries the portmapper (which *does* live on a well known port (111) and asks for the location of the RPC service it wants. The portmapper tells it and the client then connects to the relevant port.

There are several problems with RPC itself, some more security related than others. The portmapper itself can be persuaded to "forward" requests to services which may then be fooled into thinking that they come from the local machine. The standard portmappers provide very little in the way of access control or logging. Wietse Venema has a version of the portmapper which does provide these extra services.

The more common problems are with the RPC services themselves. They are typically appallingly badly written from the security perspective and are a common source of network weaknesses.

Our probing software contacts the portmapper and asks for the list of services offered on the probed system. In the sections below we list some of the more common RPC services with commentaries on when you need to run them and links to their patches or security advisories.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

This probe identifies a number of different services. You need to consider each service in turn. If you want to run no RPC services at all then you should disable the portmapper itself too.

rpcbind

This service name corresponds to the portmapper itself. If you want to run *any* RPC service then you need to be running the portmapper.

nfs, mountd, nfs_acl

The **Network Filing System**. If you want to share some of your files with other systems then you must run these services. nfs_acl is the same as nfs but has support for Access Control Lists as well. See CERT advisory CA-98.12.mountd for details of a common security hole in this service.

status, llockmgr, nlockmgr

These services are used for file locking over NFS. You need them if you are exporting your own files or importing someone else's.
walld
A utility for letting people send messages to every user of the system. Rarely useful and more often a pain in the arse.
rstatd
A utility for letting remote systems know your load average. Rarely useful but the perfmeter tool needs it.
Ypserver: All systems in a YP (a.k.a. NIS) domain need to be running this service. If you are not using YP then you should not be running it.
ypserv
All YP servers (Master and Slave servers) should be running this service. YP clients should not.
tooltalk
This is used for some graphical operations like drag and drop, we think. See CERT advisory CA-98.11.tooltalk for details about a common security hole in this service.
cmsd
This is the CDE Calendar Manager service which is rarely used and was the source of a serious security hole. (See CERT advisory CA-99-08-cmsd for details.)

How to disable this service

Each of the various RPC services may have a different start up procedure.

The portmapper itself is typically started from the system start-up scripts at boot time. On a Solaris box look for "/etc/rc2.d/S71rpc". This script starts up the portmapper and any of the YP services that may be needed. On an Irix or Linux box you can disable it (and many of the other RPC services) with chkconfig.

Some RPC services are started by inetd. RPC lines in the inetd.conf file have a characteristic first entry, corresponding to the RPC number of the service. For example: 100068/2-5 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd Those RPC services not started by inetd are started by boot scripts.

After editing the /etc/inetd.conf file the inetd daemon it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.
On a system with a System V style ps: # ps -e | grep inetd 133 ? 0:03 inetd 1513 pts/5 0:00 grep inetd # kill -HUP 133
On a system with a BSD style ps: # ps -ax | grep inetd 212 ? S 0:00 inetd 1549 p2 S 0:00 grep inetd # kill -HUP 212
Wietse Venema's replacements for portmapper or rpcbind to provide logging and access control.

CA-99-08-cmsd
CA-99-05-statd-automountd
CA-98.12.mountd
CA-98.11.tooltalk
CA-98.06.nisd
CA-97.26.statd

Insecure X servers

The X server runs on systems with a graphical display capable of displaying windows from remote (typically Unix) systems. It listens on the network for incoming (mainly graphical) instructions from the remote client programs.

Access to the display needs to be controlled. If any X client can display to the screen then anyone could pop up windows on your screen. They can also take snapshots of your screen and spy on your activity.

This probe makes a request to the X server asking for information about the server's configuration. The request is not one that will snoop on the windows currently displayed or pop up any windows of its own. The machine and account the probe is done from should have no rights at all over the X server and the request for information should be denied. If it is not denied then a warning is generated that the X server is running in an insecure manner.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
You need to be running this server if you want to be able to pop up X windows (xterm etc.). It is one of the most commonly run services.

How to secure this service

If you decide that you do need to run this service, then securing it requires a combination of keeping the software up-to-date (typically with patches) and correct configuration.

The Network Information Service (alias Yellow Pages)

The Network Information Service (NIS, historically known as YP) is a mechanism invented by Sun for sharing Unix password files and the suchlike across a network. Some implementations share them a little too widely, though, and this probe tries to detect these.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.
You need to be running a NIS server if you want to allow other systems on your network to use your password file for authentication. You probably don't want to be sharing your

password file with the entire world, though. The latter is what this probe has detected when it gives a WARNING. Note that the probe only tries a few NIS domain names when requesting a map, so our probe not spotting a hole doesn't mean you're safe.

How to secure this service

If you decide that you do need to run this service, then securing it requires a combination of keeping the software up-to-date (typically with patches) and correct configuration.
The NIS service is usually provided by a process called ypserv, which runs continuously and will be started by your system startup scripts. The precise mechanism for controlling access to the NIS maps is system-dependent.
SunOS 4, Solaris 2, Irix 6.5 and later, Tru64 Unix
The file /var/yp/securenets contains the list of YP clients. Note that SunOS 4 needs patches to make this work (see the list below -- they fix bug number 1036869). The SunOS 4.1.3 patch apparently works on 4.1.1 as well.

Irix 6.4 and earlier:

The NIS server is always open to the world. Either upgrade, or use an entirely random domain name. This is SGI bug number 269544, and has been decreed not to be a bug.
NetBSD 1.4 and later

Access is controlled through /etc/hosts.allow and /etc/hosts.deny.

Vendor documentation

These are relevant pieces of on-line documentation from various vendors of software which provides this service. If your favourite operating system isn't listed, this doesn't necessarily mean it doesn't provide the service.
Note that most documentation is for the latest version of the software. Older versions are often lacking the security features found in new ones.
Irix
securenets(4)
NetBSD
ypserv(8), hosts_access(5)
Solaris
securenets(4)
Tru64 Unix
ypserv(8)

Patches for this service

Patches vary beteween vendors. Sun's patches for Soalris tend to patch only a restricted set of binaries. Silicon Graphics tend to produce patches for software subsets. Red Hat produce updated software packages. Compaq generate a single patch file for the entire base DEC OSF/1 operating system.
Operating
system

SunOS 4.1.3	100482-08.tar.Z
SunOS 4.1.3C	100482-08.tar.Z
SunOS 4.1.3_U1	101435-04.tar.Z
SunOS 4.1.4	103833-02.tar.Z

Miscellaneous TCP

This probe checks for processes listening on various common TCP ports for which we don't yet have specific probes. They are:

70 (gopher)
A precursor to the World Wide Web.

427 (svrloc)
Apparently used by something under Mac OS.

513 (login)
BSD remote login (rlogin).

515 (printer)
The BSD lpr printing protocol.

548 (afpovertcp)
AppleShare IP, for sharing files with newish Macs.

555
The default port for the phAse Zero backdoor under Windows.

600 (ipcserver)
A common port for back doors.

1214
KaZaA filesharing

1524 (ingreslock)
An even more common port for back doors.

1433
Micorsoft SQL server

4710
Remote-Anything, PC remote access system

4711
Remote-Anything, PC remote access system

5190
SongSpy filesharing

6346
Gnutella filesharing

6347
Gnutella filesharing

6776
A port used by the SubSeven backdoor under Windows.

6969
The port used by the GateCrasher 1.2 backdoor under Windows.

6666
Yoink filesharing or IRC

6667
Yoink filesharing or IRC

7788
BuddyShare filesharing

9099, 9100

Raw connections to HP JetDirects.

9200
: The same, but for Lexmark printers.

12345
: The default port for the NetBus backdoor under Windows.

21554
: The port used by the GirlFriend 1.3x backdoor under Windows.

23456
: The port used by the EvilFTP backdoor under Windows.

30100
: The port used by the NetSphere 1.30 backdoor under Windows.

31337
: Traditional port for Unix backdoors

31785
: The port used by the Hack'a'Tack backdoor under Windows.

54320
: The default port for the Back Orifice 2000 trojan.

Note that this probe is very simple and just checks for a listener on each port. It makes no attempt to determine that the listener is actually what it expects it to be. Many of these probe results may be false positives.

Should you be running this service?

It is a general maxim of computer security that the fewer network services you run the more secure your system will be. You do not need to pay attention to security alerts and patches for services you do not run.

Of course, the need for these services varies widely. You need these services if...

70 (gopher)
: ... you want to provide a gopher service. If you don't know what this is, don't bother.

427 (svrloc)
: Not sure about this one. Ideas?

513 (login)
: ... you want to allow network logins without needing passwords (using host-based authentication), but don't want to have to use ssh.

515 (printer)
: ... you want to allow Unix (and Mac OS) systems to print to your printers.

548 (afpovertcp)
: ... you want to share your files with Macintoshes

600 (ipcserver)
: ... nil. This service generally indicates your machine's been broken into.

1524 (ingreslock), 31337
: ... nil. These services generally indicates your machine's been broken into.

9099, 9100, 9200
: ... you want to allow unfettered access to your printer.

555, 6776, 6969, 12345, 21554, 23456, 30100, 31785, 54320
: ... you want the world to be able to do evil things to your Windows box.

How to disable this service

The mechanisms for diabling these services varies widely. On Unix systems, most of them are run by inetd and can be disabled by removing or commenting out the relevant line in /etc/inetd.conf.

After editing the /etc/inetd.conf file the inetd daemon it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.

On a system with a System V style ps:

```
# ps -e | grep inetd
133 ? 0:03 inetd
1513 pts/5 0:00 grep inetd
# kill -HUP 133
```

On a system with a BSD style ps:

```
# ps -ax | grep inetd
212 ? S 0:00 inetd
1549 p2 S 0:00 grep inetd
# kill -HUP 212
```

There follow a few more specific instructions:

Gopher on Microsoft Internet Information Server (IIS)

Stop the service from the Internet Information Server Console File menu and then go into Control Panel>Services, find it in the list, double-click it and disable it.

Relevant advisories

These are the security advisories from various organisations (including the CERT and the vendors) regarding this service on various platforms.

- CA-95:14.Telnetd_Environment_Vulnerability
- CA-91:02a.SunOS.telnetd.vulnerability
- ISS advise30: Windows Backdoor Update III
- ISS 1228: win-netbus-installed