A Breakdown of SANs Top Ten Threats

Mary M. Chaddock
October 11, 2000

Index

Overview

This document is written to help new System Administrators and Non-System Administrators process **SANs Top Ten Threats**[1] quickly, easily and as painless as possible. Nine of the ten threats apply to a UNIX environment. To successfully process each threat, four questions need answering.

1. Is the application running?
2. Is the application being used?
3. Do you need the application?
4. How can the application be disabled?

This guide will help find the answers to each question.

Essential Information

The information in this document covers BSDI and Solaris operating systems. The following terms and commands are included in this document.

- *comment out* - (term) To add a # to the beginning of a line. The # at the beginning of a line indicates the line is a comment and should not be executed.
- PS - (command) used to list the processes running on a machine[2]. For example, the following command may be executed to obtain a list of all running processes on a machine.
  - BSDI -> `ps -axjww |more`

    - Solaris -> `ps -edf |more`

- `GREP` - (command) used to search for a string of characters. For example, to search for the word mountd in the file `/etc/rc`, execute the command:
    - `grep mountd /etc/rc`

Startup/Boot Commands

- BSDI: Startup commands are located in two files, `/etc/rc` and `/etc/rc.local`.
    - To prevent an application from executing during system startup locate the file from which the command is executed and comment out the line.

- Solaris: Startup commands on Solaris are located in the directories `/etc/rc0.d`, `/etc/rc1.d`, `/etc/rc2.d`, `/etc/rc3.d` and `/etc/rcS.d`. The files in each directory are hard linked to files in the directory `/etc/init.d`.
    - To prevent an application from executing during system startup locate the file in `/etc/init.d` from which the command is executed and comment out the line.

Use extreme care when editing startup files. Whenever possible, reboot the machine after each change. Errors messages are normally logged in the file `/var/log/messages` on BSDI, and `/var/adm/messages` on Solaris. When unable to reboot the machine, record the changes in your logbook (That is the spiral notebook you keep next to your console. You *do* have one, right?). Schedule the earliest available time to reboot.

INETD

Applications that are not executed during system startup may be executed on demand by inetd. Inetd is a daemon which accepts connections for applications which are defined in the file `/etc/inetd.conf`. Applications that are run by inetd may be disabled by commenting out the entry from the /etc/inetd.conf file and restarting the inetd daemon. Additional instructions for editing and restarting inetd may be found at http://www.sunworld.com/sunworldonline/swol-10-2000/swol-1006-buildingblocks.html.

1. BIND weaknesses; nxt, qinv and in.named allow immediate root compromise.[1]

Is it running?

The name of the process that runs BIND will be `named` or `in.named`. `Named` is normally run as a daemon. Use `ps` to determine if `named` is running.

```
(BSDI)    $ ps -axjww | grep named | grep -v grep
(Solaris) $ ps -edf | grep named | grep -v grep
```

If `named` is running, a line will be returned displaying the process information. Occasionally, the `ps` output may be clipped to the width of your terminal. When

this occurs, it may falsely appear that you are not running `named`. To verify the result manually, leave off the `grep` and pipe the `ps` output to `more`.
If you have checked the processes and do not have `named` running, you are not using BIND.

Do you use it?

If `named` is running on your machine, you are probably running a DNS server. The location of log files which are used by `named` may be defined in the `/etc/named.conf` file. If the configuration file has logging set to `syslog`, the actual location of the file `named` logs to may be located in the `/etc/syslog.conf` file.
You may also determine whether you are actually using `named` or if it may have been installed by default or accident by logging into the machine running `named` and execute `nslookup` for a name or address.

Example: -> `$ nslookup sans.org`
The first two lines of the information returned, will tell you what machine is used by your machine to lookup DNS information. If the machine listed is not your machine, you are probably not intentionally running `named`. It would be easy to decide right now that you do not need `named` running, however there are times when DNS servers are misconfigured [3]. Before making the final decision to disable `named`, answer the following questions:

+ Are you responsible for more than one IP address?
+ Are you responsible for distributing IP addresses in your organization?
+ When a new server is set up in your organization, do people ask you to define an Internet name?

If you are not responsible for the above items, do you know who is? If not, you should be able to safely turn off your DNS server. However, you should avoid making this change on a Friday afternoon. After making the changes, you should wait a week or two, before you delete the `named application`.

If you know who is responsible for the above items, talk to them. Most Network Administrators have very clear idea's about who should be running DNS servers.

Is it needed?

If you are running a DNS server intentionally, you must decide if it is beneficial. Is your machine a primary or secondary DNS server for your site? If not, why are you running it?

At our site, we run a third DNS server to distribute lookups to different segments of our network. The reduced network traffic and distributed workload are beneficial. If you are unable to validate your reason for running a DNS server, you should disable `named`.

Turning it off.

Kill the active `named` process. Remove executable permissions from the application using `chmod 0` (`/usr/libexec/named` on BSDI; and

`/usr/sbin/in.named` on Solaris). If there is a file named `/etc/boot.named` on your machine, either rename or delete the file. If `/etc/boot.named` exists and you have not modified your system startup files, your system may attempt to execute `named` during the boot process.

Locate and edit your startup files to prevent the execution of `named`. Use `grep` to search your startup files for the word `named.` Comment out the line that executes `named`.

2. Vulnerable CGI programs and application extensions installed on web servers.[1]

<u>Is it running?</u>

Are you running a web server on your machine? Web servers are normally run as daemons. The name of the process will be `httpd` or `httpsd`. If you do not see the applications running, you probably are not running a web server. You can verify this by connecting to your machine using a web browser.

If you are running a web server, locate your web servers configuration directory by searching your startup files for the string `httpd`. The command that executes httpd should begin with your web servers root directory. For example in the command `/var/www/bin/httpd,` is the web servers root directory is `/var/www`. In this case, the configuration files will be located in the directory `/var/www/conf`. Some systems may execute the web server from a normal system directory. In this situation you may find the command that is being executed is a bourne shell script, which will have the configuration directory listed in the script.
Another way to locate your configuration directory is using `find` with the command:

```
find / -name httpd.conf -print
```

After you locate your web servers configuration directory, look at the file in this directory named `httpd.conf (or httpsd.conf).` Search for the word `ScriptAlias` in the `httpd.conf` (or `httpsd.conf`) file. This will tell you where the cgi files are located. Check the files in that directory. Look at each one. If you are not sure if a file is being used intentionally on your server, search your web server's access log for the filename

If your `httpd.conf` (or `httpsd.conf`) file has the line "`AddHandler cgi-script .cgi`", your web server will execute files that end with .cgi. The variable `ScriptAlias` tells your web server where to locate the default cgi directories.

<u>Do you use it?</u>

Review the files that are in the cgi-bin directories (as indicated in your `httpd.conf` file). Review you web server logfiles. Use `grep` to search your access logfiles for `cgi`. If the logfiles are rotated daily, you will want to search archived logs or watch your logs for a week or two before making a final decision. If there is no valid activity in your logfiles, you should be able to safely disable CGI support.

Is it needed?

If you discover CGI activity in your logfiles, review the cgi application listed in the logfile. What does the cgi script do? You must analyze the pro's and con's of the running the application. Enabling CGI applications can be very dangerous, but it is possible the benefits of your CGI application are worth the risk. Allow CGI extensions if the application is beneficial and delete the cgi files that are not needed.

Turning it off.

Delete all files you do not use from the cgi-bin directory. To prevent execution of any cgi scripts, modify your web servers httpd.conf file and comment out the lines that define the cgi ScriptAlias and AddHandler.

3. Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager), and rpc.statd that allow immediate root compromise.[1]

Is it running?

On Solaris, the RPC applications are processed by `rpcbind`. If `rpcbind` is not running on your machine, RPC connections cannot be processed on your machine. If `rpcbind` is running on your machine, use `rpcinfo -s` to list the RPC services which are accessible on your machine.

On BSDI, the RPC applications are processed by `portmap`. If `rpcbind` is not running on your machine, RPC connections cannot be processed on your machine. If `portmap` is running on your machine, use `rpcinfo -p` to list the RPC services which are accessible on your machine. Logging for `portmap` errors use `syslog`.

Do you use it?

Statistics for RPC services may be viewed with the command `rpcinfo -m`. If there is a number greater than zero in the success field, monitor the usage a few days. At the end of one week, if the number has not increased, you are probably not using the application.

Is it needed?

Rutgers University Computing Services wrote a great overview[4] of many RPC services and what they do. In a nutshell, these RPC programs are *fluff*. They are nice to have, but it is not likely you really need them. Review Rutgers advise and watch the stats on actual usage, then validate the use. If you cannot validate your reason for running an RPC service, you should turn it off.

Turning it off.

If RPC is currently running, you may turn it off on Solaris using the following command:

```
$ /etc/init.d/rpc stop
```

On BSDI, you will need to manually kill the process `portmap`. Once the `portmap` process is killed, you must reboot your machine to reactivate it.

Edit the startup file to prevent RPC from automatically executing during the system boot. On Solaris, search for the string `rpc` in your system startup files. On BSDI, search for the string `portmap`. Comment out the line that executes the command.

5. Sendmail buffer overflow weaknesses, pipe attacks and MIMEbo, that allow for immediate root compromise.[1]

Is it running?

Sendmail can be run as a daemon, or can be executed from `inetd`. The name of the process is `sendmail`.
The easiest and fastest way to know if you are using `sendmail` is to telnet to port 25.

```
$ telnet localhost 25
```

If `sendmail` is not running you should get a message similar to "connection refused". Normally an active email server will display the name of the mail application and version number. For example, if you connect to a `sendmail` server, you may see something similar to the following:

```
Trying 127.0.0.1...
Connected to mail.abc.edu.
Escape character is '^]'.
220 mail.abc.edu ESMTP Sendmail 8.9.3/8.9.3; Thu, 5 Oct 2000
10:31:50 -0500 (CDT)
```

Do you use it?

Do you receive email on this machine from any other machine?
Sendmail logs information using the `syslog` MAIL facility. The file `/etc/syslog.conf` will list the location of the file where mail transactions are being recorded.

Is it needed?

Do you have a designated email server at your site? Are there benefits to running an email server on this machine?

Turning it off.

If `sendmail is` running as a daemon, use the `ps` command to locate and kill all `sendmail` processes. On Solaris, you can execute the command `/etc/init.d/sendmail stop.`

If `sendmail` is executed from `inetd`, edit the file `/etc/inetd.conf` and comment out the `sendmail` line. To force `inetd` to reread the configuration file, execute the command `kill -HUP <processID>`.

Verify sendmail has been disabled by telneting to port 25 again. You should see the message "connection refused".

If you were executing sendmail as a daemon, edit the startup file to prevent sendmail from automatically executing during the system boot. Search for the string sendmail in your system startup files. Comment out the line that executes the command.

6. sadmind and mountd[1]

Is it running (sadmind)?

The application sadmind is a Solaris application. You will not find it running on BSDI. This application is run from inetd.
Look in your inetd.conf file. The line that executes sadmind will be similar to the line below. If the line starts with a comment (#) sign, sadmind is disabled.

```
#100232/10 tli    rpc/udp wait root /usr/sbin/sadmind sadmind
```

If you do not locate the sadmind in the inetd.conf file, the application is probably are not running. If sadmind is enabled it will be displayed using the command rpcinfo -p.

Is it running (mountd)?

Mountd is part of the NFS applications. NFS cannot run without mountd. If NFS is being used mountd will be running. The mountd application is run as a daemon. Execute ps and search for the word mountd. Mountd may also be listed as an RPC service. List active RPC services with rpcinfo -s. If mountd is listed, it is running.

Are you using it (sadmind)?

Sadmind is used for remote system administration by the Solstice AdminSuite applications
If you do not use the Solstice AdminSuite, you will not be using sadmind.

Are you using it (mountd)?

If you are not using NFS, you probably will not need mountd. The showmount command may be used to list the names of mounted filesystems, or showmount -a to list all available mount points

Is it needed (sadmind)?

Sadmind is convienient but is rarely needed. Are there system administrative tasks which must be run remotely?

Is it needed (mountd)?

Do other machines mount filesystems on your server? You may need mountd if you share a CD drive for remote installation of software. You also need mountd if you use NFS.

Turning it off (sadmind).

Sadmind is executed via inetd. To disable it, edit the /etc/inetd.conf file and comment or delete the line which executes sadmind.

Turning it off (mountd)

Edit the startup file to prevent `mountd` from automatically executing during the system boot. Search for the string `mountd` in your system startup files. Comment out the line that executes the command.
Normally BSDI will only execute `mountd` if the file `/etc/exports` exists.

7. Global file sharing and inappropriate information sharing via UNIX NFS exports on port 2049.[1]

Is it running?

NFS is a daemon that is executed at system startup. The name of the process is `nfsd`. Use `showmount` to list the names of mounted filesystems. Use `showmount -a` to display all available mount points. The command `rpcinfo -s` should also list NFS as a service if NFS is enabled.

Are you using it?

On Solaris, NFS is started only if there is a file named `/etc/dfs/dfstab` and there are entries in this file. Review the entries in the `dfstab` file. The commands `nfsstat` and `showmount` may also provide some insight. For a better understanding of these commands, read the man pages.
On BSDI, NFS is started only if there is a file named `/etc/exports`. Review the entries in the `exports` file. Commands `nfsstat` and `showmount` may provide more insight about current NFS usage. For a better understanding of these commands, read the man pages.

Is it needed?

If you do not need to share filesystems with NFS clients, there is no need to run an NFS server. NFS is not the same as SAMBA (which is an entire different hornets nest). You do not need `nfsd` to access other NFS Servers as a client.

Turning it off.

Kill all nfsd processes.
Edit the startup file to prevent `nfsd` from automatically executing during the system boot. Search for the string `nfsd` in your system startup files. Comment out the line that executes the command.
On Solaris delete the file `/etc/dfs/dfstab`.
On BSDI delete the file `/etc/exports`.

8. User ID's, especially root/administrator with no passwords or weak passwords.[1]

Is it running?

How many people know your root password? Are you using sudo? Do you have root logins restricted to only the console device? Is root ftp access disabled?

Are you using it?

Yes.

Is it needed?

With the use of sudo, root will probably never need to interactively login to the machine.

Turning it off.

You cannot disable or turn off root/administrator accounts.
In addition to SANs advice, consider setting the root password to something really big and difficult. Assign the machine a random number (i.e.. mail.machine.com = 32). On a piece of paper, write the password.
Example: `reallyl0ngAnDdi77icultpassword`
Place the paper in an envelope. Seal the envelope. On the outside of the envelope, write the number 32. Put the envelope in your safety deposit box. On a different piece of paper write the number and identify the machine it represents. Seal this envelope and place it in a locked file cabinet or desk.

Set up `sudo` to grant ALL to your userid. This makes you privy to root access without using the root password. Do not configure `sudo` to bypass password prompting. Sudo will require that you enter your own password before executing a command as root. Change your password frequently, and make sure you have at least one other user defined in the `sudoers` file with access to change passwords. Using `sudo`, it is always possible to change the root password.

9. IMAP and POP buffer overflow vulnerabilities or incorrect configuration.[1]

Is it running?

IMAP and POP may be run as daemons or via `inetd`. The name of the imap process is `imapd`. The name of the pop process may be `ipop3d`, `ipop2d` or `ipopd`.
The easiest way to determine if IMAP or POP is running is to connect to their standard ports. POP uses port 110. IMAP uses port 143. Execute `telnet` to connect to each port.

```
telnet localhost 110
telnet localhost 143
```

You will receive an error similar to the following if the application is not running.

```
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

You will see something similar to the following if the application is running.

```
Connected to machine.abc.edu.
Escape character is '^]'.
+OK machine.abc.edu M-Store POP3 (3.0.10)
```

Are you using it?

IMAP and POP are used by email clients. If you have users who retrieve email from your machine there is a good possibility they are using IMAP or POP to access their email. Both IMAP and POP use syslog's MAIL facility to log connections. Verify logging is enabled in the `/etc/syslog.conf` file and review the log file for any activity.

Is it needed?

If you are using it, you probably need it.

Turning it off

If you are executing `imapd` or i`pop3d` from `inetd`, edit the file `/etc/inetd.conf` and comment out the line with `imapd` and the line with `pop`. Force `inetd` to reread the configuration file by executing the command `kill -HUP <inetd processID>.`
Verify the services have been disabled by telneting to the ports again. You should see the message "connection refused".
If there is not an entry in the `inetd.conf` file for IMAP or POP, you are probably running them as daemons. Use `ps` to list your running processes. Kill each all `imapd` and `ipop3d` process.
If the services run as daemons, edit the startup file to prevent IMAP and POP from automatically executing during the system boot. Search for the strings imap and pop your system startup files. Comment out the line that executes the each command.

10. Default SNMP community strings set to 'public' and 'private'.[1]

Is it running?

SNMP is executed during system startup and run as a daemon.
The process names used by Solaris, are `snmpd; snmpdx; snmpv2d and mibiisa.` The process on BSDI is `snmpd.` Use `ps` to view your processes.
If you see any of these processes are running on your system, then you are running SNMP.

Are you using it?

Very few people actually have a need to use SNMP. According to Cisco.com, "SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth." [7].

Is it needed?

You do not need SNMP if you are not responsible for the performance of your network.

Turning it off.

SNMP is executed during system startup and run as a daemon.
Use `ps` to list your processes. BSDI only uses `snmpd`. Solaris uses `snmpd, snmpdx, snmpdv2d` and `mibiisa`. Kill each of these processes.
Edit the startup file to prevent SNMP from automatically executing during the system boot. Search for the string `snmpd` in your system startup files. Comment out the line that executes the command.
Solaris may have several files that need modified. Comment the lines that execute `snmpd`, `snmpdx`, `snmpdv2d` or `mibiisa` in all startup files.

---

[1] SANs Institute, How To Eliminate The Ten Most Critical Internet Security Threats The Experts' Consensus, v 1.27
URL: http://www.sans.org/topten.htm (Sept 8, 2000)
[2] Carnegie Mellon University, Using the ps program to examine processes for signs of intrusive activity, March 7, 2000

URL: http://www.cert.org/security-improvement/implementations/i005.01.html
[3] D. Barr, Common DNS Operational and Configuration Errors, February 1996
URL: http://www.cis.ohio-state.edu/htbin/rfc/rfc1912.html
[4] Rutgers University, Rutgers University, inetd overview, June 6, 1999
URL: http://oss.rutgers.edu/inetd.html
[5] Rutgers University, Rutgers University Security issues, February 28, 2000
URL: http://oss.rutgers.edu/security_issues.html
[6] Peter Baer Galvin, The Solaris Security FAQ - How to disable NFS, October 2, 2000
URL: http://www.sunworld.com/sunworldonline/common/security-faq.html#Q2.11
[7] Cisco Systems, Inc. Simple Network Management Protocol (SNMP), June 17, 1999
URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid21031
[8] Sandra Henry-Stocker, Square one, Paring down your network services, October 6, 2000
URL: http://www.sunworld.com/sunworldonline/swol-10-2000/swol-1006-buildingblocks.html