



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Securing Linux/Unix (Security 506)"  
at <http://www.giac.org/registration/gcux>

# SANS DC2000 GIAC Practical: Track 6, UNIX Security

---

## Executive Summary

This document analyses the security of *blue.troll.nil*. *blue.troll.nil* runs Sun Microsystems's Solaris operating system, well under-patched. This system provides `email` and `FTP` access for a third-party's web site, which is hosted at *troll.nil*.

The administrative team for this machine consists of two people. Both of whom have administrative power over many machines. Neither of whom have spent a great deal of energy securing this machine. *blue* is at an adequate security level, despite a few troubling problems.

*blue.troll.nil* resides in a data center with machines of varying types and uses. Multiple people (who have no relationship to *blue*) have physical access to the machine. Too many users have too much access. System administrators of other machines have access to *blue*, simply because the `NIS+` domains are easier to maintain that way. Customers have shell access who do not need it. The machine is poorly patched. This opens it up to a wide variety of vulnerabilities. For example, `sendmail` at it's current patch level has more than one vulnerability; one of which is that it will follow symbolic links out of the `/var/mail` directory.

The `FTP` daemon could be configured slightly more securly by placing it in a `chroot`'d environment. The `POP3` server has a buffer overflow exploit. There are unused network services running. And with all this, there is no file integrity checker installed on the system.

Despite all of this, with a few changes, this machine can be up and running in great shape. Many services are already turned off. There are not a large number of users with shell access to the machine. It provides a very small set of tasks. *blue.troll.nil* can be secured fairly well and fairly easily.

---

## Analysis

### Operating System

*blue.troll.nil* runs Sun Microsystems Solaris 7 UNIX operating system. This is a standard build of this system. No permissions have been turned down for utilities which are not in use.

This machine serves as a non-anonymous, non-guest `FTP` server. For this reason, even though most access is gated from producing a shell prompt, world and group readable or writable files are a problem.

The user configuration places all non-system users in the group `nobody`. This is a very bad idea because it increases the chance that the `nobody` user may be able to read a file. In the current configuration, the `nobody` user is only used in mapping root `NFS` queries to the user `nobody`. If the reason for this is to allow the root user to access files, a better solution would be to have the root user execute `NFS` queries as a different ID so as not to be mapped to `nobody`.

The operating system has not had Casper Dik's `fix-modes` program run yet; this should always be a first step in configuring a new Solaris installation. I suggest getting [YASSP](#) (Yet Another Solaris Security Package). YASSP incorporates `fix-modes` with a number of other usefull security nuggets. This application is easy to configure and run.

### Physical Access

Physical access to the data center is gated by a physical-key locked door. Operators without natural access to *blue* also have access to this room. This provides them access to reboot *blue.troll.nil* and to confiscate any removable media from the system, such as CDs and Backup Tapes. Tampering with this machine is minimized by the use of multiple security cameras in the data center. The floors are rased above the floor of an existing room, so the walls go down to the floor. However, the drop-ceilings provide unauthoried access to anything or anyone who can fit. Concoidering the restricted access to the building, room, and the type of business which is being run, physical security is minimally adequate.

Physical security could be enhanced in a couple ways. The walls should extend to the real ceiling. Physical-key locks should be replaced with smart-cards to allow for better logging of entry. And, machines administered by different people should be locked away in different cages.

## System Access

Only system accounts are stored in the local system `passwd` file. All other accounts are granted access via `NIS+`. Most users of the system only use the `FTP` and `POP3` services. `FTP` is used to upload files to an `NFS` mounted drive which serves `HTTP` services on another machine. These users' shells are a symbolic link to `/bin/false`. Since these users cannot login, they have account aging disabled. *There is no way for these users to change their passwords.* The administrators, administrators of other machines, some managers, and a small number of administrators from the client's site have shell access. Administrative access is relegated to the console for the `login` program, but is allowed via `SSH`.

A system *must* be setup whereby users can change their passwords. Firstly, these passwords are given to them by the administrators, and these passwords follow a pattern. Secondly, users should be responsible --for legal reasons-- for their passwords should they ever become compromised. Below is a short and overly simplified `perl` script used to compromise more than half of these accounts. This script could be easily optimized to increase the rate of compromise.

```
#!/usr/local/bin/perl

$users_crypt=shift;

@former=('aaaa' .. 'zzzz');

@latter=(0 .. 9999);

foreach $former (@former) {
    foreach $latter (@latter) {
        $my_text=sprintf("%4s%04s", $former, $latter);
        if($users_crypt eq crypt($my_text, $users_crypt)) {
            print $my_text, "\n";
            exit(0);
        }
    }
}

exit(1);
```

The administrators from the client's site only use their access to look at web logfiles and check the web server's configuration files for correctness. This access should be tightened up by removing shell access from the client's administrators and having them `FTP` (or a secure replacement) these files down to their local site. This appears to be what they do with these files anyway.

Administrators of other machines should have their access revoked. Proper `NIS+` domains should be set up to enforce this access restriction. The administrators' manager's access should also be revoked, since they have not logged in a very long time, and their passwords have long since expired.

## Administration

There are two authorized administrators for *blue.troll.nil*. Both administrators share the root password; however, access is normally granted using `sudo`. `sudo` is configured to allow non-passworded access to the administrative account for these two

users. Administrators for other systems have shell access to the system via the NIS+ map. Administrative tasks are loosely delegated between the two administrators via personal conversations and email. There is no session logging other than standard system logs, those of `sudo`, and TCP Wrappers.

The administrators need to document their daily tasks and procedures. A method for formal notification of changes and a more extended use of RCS (Revision Control System) should be employed. The NIS+ domain needs to be configured to disallow access to `blue.troll.nil` by system administrators of other systems.

`sudo` should be configured to require a password to gain administrative privilege. The SUID (Set-UID) bit should be removed from the system `su` command, since it is not being used.

## Patching

The patching of `blue.troll.nil` is in an awful state. `blue.troll.nil` is missing vital security patches, as well as other important system updates. Keeping Solaris up-to-date with patches is often a daunting task, and an often overlooked one. However, this is one of the most glaring problems with this system.

A policy needs to be developed which defines the patching procedure, as well as an audit of that procedure. This policy needs to incorporate where new patch information will be pulled from, how much time may pass before a decision is to be made regarding whether or not to apply the patch, and written notice if a patch is not applied. This last point holds especially true for security patches. I suggest a four level rating scheme for security patching under Solaris:

1. **Severe and immediate concern.** This problem directly affects the system and leaves it immediately vulnerable to a root compromise. *This machine must be patched as soon as possible.*
2. **Medium level of concern.** This problem can potentially cause a system to crash, or behave oddly. There is a potential, albeit low, chance for damage. *This patch should be evaluated and tested, then placed on the system within one to two weeks.*
3. **Low level of concern.** This problem deals with an unused service, or affects only sandbox machines. This causes no affect on production systems, except for maybe a DOS. *This patch should be installed with the quarterly bundle.*
4. **The patch cannot be installed for some reason.** This reason should be documented, signed by management, and filed away. *You may still want to test this patch, incase you can use it in the future.*

After this policy is developed, it must be adhered to. An audit must be part of the process. Subscribe to mailing lists, such as [BUGTRAQ](#) to know which security problems affect your system, and when to start looking for patches to solve these problems.

Below I have attached output from the Pogostick [Patchdiag](#) tool. It provides patches for components of `blue.troll.nil` which should not have been installed to begin with. However, I am attaching the entire list in the event these sub-systems do not get removed, like they should.

```
=====
System Name: Remote System          SunOS Vers: 5.7          Arch: sparc
Cross Reference File Date: 11/Aug/00

PatchDiag Version: 1.0.4
=====

Report Note:
```

Recommended patches are considered the most important and highly recommended patches that avoid the most critical system, user, or security related bugs which have been reported and fixed to date. A patch not listed on the recommended list does not imply that it

should not be used if needed. Some patches listed in this report may have certain platform specific or application specific dependencies and thus may not be applicable to your system. It is important to carefully review the README file of each patch to fully determine the applicability of any patch with your system.

=====

INSTALLED PATCHES

Patch ID	Installed Revision	Latest Revision	Synopsis
106146	05	14	SunOS 5.7: M64 Graphics Patch
106147	01	06	SunOS 5.7: VIS/XIL Graphics Patch
106541	04	12	SunOS 5.7: Kernel update patch
106793	02	05	SunOS 5.7: ufsdump and ufsrestore patch
106812	04	CURRENT	OBSOLETE by 107432
106857	04		
106879	01	CURRENT	SunOS 5.7: sys-suspend patch
106917	01	CURRENT	SunOS 5.7: when view mails change charset, dtmail dump core.
106924	01	06	SunOS 5.7: isp driver patch
106925	01	04	SunOS 5.7: glm driver patch
106934	03	CURRENT	CDE 1.3: libDtSvc Patch
106936	01	CURRENT	SunOS 5.7: /etc/cron.d/logchecker patch
106938	01	04	SunOS 5.7: libresolv patch
106940	01	CURRENT	SunOS 5.7: /usr/sbin/makedbm patch
106942	01	07	SunOS 5.7: libnsl, rpc.nisd and nis_cachemgr patch
106944	01	03	SunOS 5.7: /kernel/fs/fifofs and /kernel/fs/sparcv9/fifofs patch
106946	01	CURRENT	SunOS 5.7: /usr/sbin/sar patch
106948	01	CURRENT	SunOS 5.7: /kernel/drv/qe and /kernel/drv/sparcv9/qe patch
106949	01	CURRENT	SunOS 5.7: BCP (binary compatibility) patch
106950	03	11	SunOS 5.7: Linker patch
106952	01	CURRENT	SunOS 5.7: /usr/bin/uux patch
106959	01	CURRENT	SunOS 5.7: Last portion of audio file gets chopped or repeats
106960	01	CURRENT	SunOS 5.7: Manual Pages for patchadd.lm and patchrm.lm
106963	01	CURRENT	SunOS 5.7: /kernel/drv/esp and /kernel/drv/sparcv9/esp patch
106978	06	10	SunOS 5.7: sysid patch
106980	04	11	SunOS 5.7: libthread patch

106982	01	CURRENT	SunOS 5.7: /kernel/drv/fas and /kernel/drv/sparcv9/fas patch
106985	01	CURRENT	SunOS 5.7: /usr/sbin/uadmin and /sbin/uadmin patch
106987	02	CURRENT	SunOS 5.7: /usr/sbin/tar patch
106999	01	CURRENT	SunOS 5.7: /usr/lib/adb/sparcv9/adbsub.o patch
107001	01	CURRENT	OBSOLETE by 107887
107003	03	CURRENT	SunOS 5.7: Updated Lucida Hebrew Fonts for Solaris 7
107011	01	CURRENT	CDE 1.3: sdtwebclient patch
107014	01	02	XIL 1.4: Deskset Loadable Pipeline Libraries Patch
107018	01	02	SunOS 5.7: /usr/sbin/in.named patch
107022	02	06	CDE 1.3: Calendar Manager patch
107031	01	CURRENT	OBSOLETE by 106541
107038	01	CURRENT	SunOS 5.7: apropos/catman/man/whatis patch
107044	01	CURRENT	SunOS 5.7: Russian and Polish print failure on some printers
107049	01	CURRENT	SunOS 5.7: dtlogin language menu displays wrong info
107059	01	CURRENT	SunOS 5.7: /usr/bin/sort and /usr/xpg4/bin/sort patch
107063	01	CURRENT	SunOS 5.7: Thai engine crashes in 64bit mode
107072	01	CURRENT	CDE 1.3: Spell Checker patch
107074	01	CURRENT	SunOS 5.7: SUNWultratest doesn't support sun4us platform
107076	01	CURRENT	SunOS 5.7: /usr/kernel/drv/vol and /usr/kernel/drv/sparcv9/vol pat
107081	03	21	Motif 1.2.7 and 2.1.1: Runtime library patch for Solaris 7
107094	02	08	CDE 1.3: dtterm libDtTerm.so.2 Patch
107115	01	05	SunOS 5.7: LP patch
107117	03	05	OBSOLETE by 106541
107121	01	02	OBSOLETE by 107458
107127	02	CURRENT	SunOS 5.7: /usr/lib/autofs/automountd patch
107147	03	08	SunOS 5.7: pci driver patch
107148	03	08	SunOS 5.7: /kernel/fs/cacheufs patch
107171	02	06	SunOS 5.7: Fixes for patchadd and patchrm
107178	01	CURRENT	CDE 1.3: libDtHelp.so.1 patch
107180	04	22	CDE 1.3: dtlogin patch
107185	01	CURRENT	SunOS 5.7: Miscellaneous Russian KOI8-R problems
107187	01	02	SunOS 5.7: Miscellaneous Eastern European locale problems
107200	03	12	CDE 1.3: dtmail patch
107219	01	02	OBSOLETE by 107885
107226	03	12	CDE 1.3: dtwm patch
107233	01	CURRENT	OpenWindows 3.6.1: xterm patch

107248	01	02	CDE 1.3: sdtaudio patch
107250	02	CURRENT	OpenWindows 3.6.1: libsv8.so.1 Patch
107259	01	CURRENT	SunOS 5.7: /usr/sbin/vold patch
107285	01	02	SunOS 5.7: passwd & pam library patch
107292	01	06	SunOS 5.7: ifp driver patch
107293	01	CURRENT	SunOS 5.7: libgss.so.1 and gsscred patch
107306	01	03	CDE 1.3: dtfile patch
107316	01	CURRENT	SunOS 5.7: localeconv() returns wrong results for French
107318	04	CURRENT	OBSOLETE by 108068
107330	01	CURRENT	SunOS 5.7: /usr/sbin/ntpdate patch
107359	01	02	SunOS 5.7: Patch for SPARCompiler Binary Compatibility Libraries
107401	01	CURRENT	SunOS 5.7: /usr/bin/iostat patch
107403	01	CURRENT	SunOS 5.7: rlmod & telmod patch
107430	01	CURRENT	SunOS 5.7: Installer utility used by NCR breaks under Solaris 7
107437	02	03	SunOS 5.7: support IBM Cp837 and Cp874 iconv modules(th_TH)
107438	01	02	SunOS 5.7: iso8859-15 locale copy and paste fix
107441	01	02	SunOS 5.7: /usr/bin/mailx patch
107443	03	12	SunOS 5.7: packaging utilities patch
107445	01	03	OBSOLETE by 107709
107448	01	CURRENT	SunOS 5.7: /usr/lib/fs/cachefs/cachefsd patch
107450	01	CURRENT	SunOS 5.7: /platform/SUNW,Ultra-Enterprise-10000/lib/cvcd patch
107451	01	04	SunOS 5.7: /usr/sbin/cron patch
107453	01	CURRENT	SunOS 5.7: Ultra-80 platform patch
107454	01	05	SunOS 5.7: /usr/bin/ftp patch
107456	01	CURRENT	SunOS 5.7: /etc/nsswitch.dns patch
107458	01	10	SunOS 5.7: dad, sd, ssd, uata drivers patch
107459	01	CURRENT	SunOS 5.7: qec driver patch
107460	01	07	SunOS 5.7: st driver patch
107462	01	CURRENT	SunOS 5.7: /kernel/sched/TS patch
107499	02	CURRENT	SunOS 5.7: koi8-R -ow hanged before dtlogin screen
107546	02	CURRENT	OpenWindows 3.6.1: Ultra 80 Support Patch

=====

UNINSTALLED RECOMMENDED PATCHES

Patch	Ins	Lat	Age	Require	Incomp	Synopsis
-------	-----	-----	-----	---------	--------	----------

ID	Rev	Rev	ID	ID
107544	N/A	03	297	SunOS 5.7: /usr/lib/fs/ufs/fsck patch
107587	N/A	01	467	SunOS 5.7: /usr/lib/acct/lastlogin patch
107636	N/A	05	12	SunOS 5.7: X Input & Output Method patch
107684	N/A	01	465	SunOS 5.7: Sendmail patch
107709	N/A	06	132	SunOS 5.7: libssasmp/libssagent/snmpdx/mibiisa patch
107792	N/A	02	215	SunOS 5.7: /usr/bin/pax patch
107972	N/A	01	355	SunOS 5.7: /usr/sbin/static/rcp patch
108301	N/A	02	109	SunOS 5.7: /usr/sbin/in.tftpd patch
108327	N/A	01	136	SunOS 5.7: /usr/bin/cu patch
108331	N/A	01	136	SunOS 5.7: /usr/bin/uustat patch
108482	N/A	02	109	SunOS 5.7: /usr/sbin/snoop patch
108484	N/A	01	202	SunOS 5.7: aset patch
108662	N/A	01	233	SunOS 5.7: Patch for sadmind
108721	N/A	01	177	SunOS 5.7: admintool patch
108798	N/A	01	69	SunOS 5.7: /usr/bin/tip patch
108838	N/A	02	61	SunOS 5.7: allocate/mkdevmaps/mkdevalloc patch
109104	N/A	03	25	SunOS 5.7: /kernel/fs/sockfs patch
109253	N/A	01	96	SunOS 5.7: /usr/bin/mail patch
109404	N/A	01	72	SunOS 5.7: /usr/vmsys/bin/chkperm patch
107885	N/A	06	251	106934-03 CDE 1.3: dtprintinfo Patch
107887	N/A	09	86	CDE 1.3: Actions Patch
108219	N/A	01	335	CDE 1.3: dtaction Patch
108221	N/A	01	335	CDE 1.3: dtspcd Patch
108343	N/A	03	68	108374-01 CDE 1.3: sdtperfmeter patch
108374	N/A	03	2	CDE 1.3: libDtWidget Patch
106725	N/A	02	236	OpenWindows 3.6.1: mailtool vacation security patch
107337	N/A	01	513	OpenWindows 3.6.1: KCMS configure tool has a security vulnerabilit
107650	N/A	07	23	108376-01 OpenWindows 3.6.1 X11R6.4 Xprint Extension Patch
107893	N/A	07	131	OpenWindows 3.6.1: Tooltalk patch
108376	N/A	08	53	OpenWindows 3.6.1: Xsun Patch

**UNINSTALLED SECURITY PATCHES**

**NOTE: This list includes the Security patches that are also Recommended**



Patch ID	Ins Rev	Lat Rev	Age	Require ID	Incomp ID	Synopsis
107684	N/A	01	465			SunOS 5.7: Sendmail patch
107709	N/A	06	132			SunOS 5.7: libssasmp/libssagent/snmpdx/mibiisa patch
107792	N/A	02	215			SunOS 5.7: /usr/bin/pax patch
107972	N/A	01	355			SunOS 5.7: /usr/sbin/static/rcp patch
108301	N/A	02	109			SunOS 5.7: /usr/sbin/in.tftpd patch
108327	N/A	01	136			SunOS 5.7: /usr/bin/cu patch
108331	N/A	01	136			SunOS 5.7: /usr/bin/uustat patch
108482	N/A	02	109			SunOS 5.7: /usr/sbin/snoop patch
108484	N/A	01	202			SunOS 5.7: aset patch
108662	N/A	01	233			SunOS 5.7: Patch for sadmind
108721	N/A	01	177			SunOS 5.7: admintool patch
108798	N/A	01	69			SunOS 5.7: /usr/bin/tip patch
108838	N/A	02	61			SunOS 5.7: allocate/mkdevmaps/mkdevalloc patch
109253	N/A	01	96			SunOS 5.7: /usr/bin/mail patch
109404	N/A	01	72			SunOS 5.7: /usr/vmsys/bin/chkperm patch
107885	N/A	06	251	106934-03		CDE 1.3: dtprintinfo Patch
107887	N/A	09	86			CDE 1.3: Actions Patch
108219	N/A	01	335			CDE 1.3: dtaction Patch
108221	N/A	01	335			CDE 1.3: dtspcd Patch
106725	N/A	02	236			OpenWindows 3.6.1: mailtool vacation security patch
107337	N/A	01	513			OpenWindows 3.6.1: KCMS configure tool has a security vulnerabilit
107650	N/A	07	23	108376-01		OpenWindows 3.6.1 X11R6.4 Xprint Extension Patch
107893	N/A	07	131			OpenWindows 3.6.1: Tooltalk patch
108376	N/A	08	53			OpenWindows 3.6.1: Xsun Patch

UNINSTALLED Y2K PATCHES

NOTE: This list includes the Y2K patches that are also Recommended

Patch ID	Ins Rev	Lat Rev	Age	Require ID	Incomp ID	Synopsis
----------	---------	---------	-----	------------	-----------	----------

```

-----
107587 N/A 01 467 SunOS 5.7: /usr/lib/acct/lastlogin patch
108343 N/A 03 68 108374-01 CDE 1.3: sdtperfmeter patch
108815 N/A 02 33 OpenWindows 3.6.1: Calendar Manager patch
=====

```

OTHER RELATED UNINSTALLED PATCHES

NOTE: This is determined by the packages that have been installed on the system.

When one patch refers to multiple packages, we list the additional packages in the next lines.

The various 'S','R','\*' marks denote unbundled packages that is designated as an 'Security' or 'Recommended'.

- S = Security
- R = Recommended Unbundled
- \* = Both Security and Recommended Unbundled

Patch ID	Package Name	Lat	Age	Synopsis
106144	SUNWafb SUNWafbcbf SUNWafbwb SUNWafbxb SUNWafbxbg	20	75	SunOS 5.7: Elite3D AFB Graphics Patch
106145	SUNWffb SUNWffbcf SUNWffbw SUNWfffbx SUNWfffbxg	17	104	SunOS 5.7: Creator 7 FFB Graphics Patch
106148	SUNWxfb SUNWxfbx	12	104	SunOS 5.7: XFB Graphics Patch

106300 SUNWlibCx 09 86 SunOS 5.7: Shared library patch for 64bit C++

106327 SUNWlibC 08 86 SunOS 5.7: Shared library patch for C++

106733 SUNWadmC 07 250 SunOS 5.7: Create a patch analyzer

106748 SUNWsprot 04 219 SunOS 5.7: /usr/ccs/bin/sccs and /usr/ccs/bin/make patch  
SUNWxcu4t

106871 SUNWqfed 01 566 Sun Quad FastEthernet 2.2: POINT PATCH: to fix interrupt distribut  
SUNWqfedu  
SUNWqfedx

106887 SUNWrtvcl 02 404 SunOS 5.7: SunVideo 1.4 Patch

106888 SUNWdialh 02 135 SunOS 5.7: Buttons/Dials Patch

107058 SUNWsprot 01 578 SunOS 5.7: Patch for assembler

107175 SUNWman 01 551 SunOS 5.7: Manual page for date.1

107261 SUNWcsu 01 523 SunOS 5.7: POINT PATCH: 1235385 - pkgtrans/pkgadd check std SVR4 A

107324 SUNWplow 01 537 SunOS 5.7: Euro locales, user interface refresh is very slow

107332 SUNWarc 02 345 SunOS 5.7: libadm patch  
SUNWcs1  
SUNWcs1x

107350 SUNWxgldg 03 103 XGL 3.3.1: XGL Patch (unstripped version)  
SUNWxglrt

107351 SUNWxgldg 03 102 XGL 3.3.1: XGL Patch (stripped version)  
SUNWxglrt

107374 SUNWolinc 01 501 OpenWindows 3.6.1: Xview Patch  
SUNWolrte  
SUNWolslb

107431 SUNWwsr 01 417 SunOS 5.7\_x86: Installer utility used by NCR breaks under Solaris

107432 SUNWisolc 03 340 SunOS 5.7: CTL printing patch  
SUNWisolx  
SUNWplc1x  
SUNWploc1  
SUNWplow1

107465 SUNWcarx 02 340 SunOS 5.7: /kernel/fs/hsfs and /kernel/fs/sparcv9/hsfs patch  
SUNWcsr

107469 SUNWhea 07 47 SunOS 5.7: sf & social drivers patch  
SUNWluxd  
SUNWluxdx  
SUNWluxl

SUNWluxlx

107470 SUNWadmc 01 270 SunOS 5.7: CD install support for devfsadm

107472 SUNWses 02 269 SunOS 5.7: ses driver patch

SUNWsesx

107473 SUNWluxop 06 68 SunOS 5.7: luxadm patch

107474 SUNWcsu 01 410 SunOS 5.7: ifp adb macro patch

SUNWcsxu

107475 SUNWcsu 01 317 SunOS 5.7: /usr/sbin/in.telnetd patch

107477 SUNWcsu 02 250 SunOS 5.7: /usr/lib/nfs/mountd patch

107551 SUNWcsu 01 496 SunOS 5.7: /usr/bin/date and /usr/xpg4/bin/date patch

SUNWxcu4

107553 SUNWpppk 01 466 SunOS 5.7: /usr/kernel/drv/ipdcm & /usr/kernel/drv/sparcv9/ipdcm p

SUNWpppkx

107555 SUNWldapx 01 459 SunOS 5.7: /usr/lib/libldap.so.3 & /usr/lib/sparcv9/libldap.so.3 p

SUNWlldap

107557 SUNWaccu 02 353 SunOS 5.7: /usr/sbin/sag patch

107560 SUNWisolc 02 447 SunOS 5.7: (32bit) Support for ISO8859-1/IBM-500 iconv conversion

107562 SUNWisolx 02 447 SunOS 5.7: (64bit) Support for ISO8859-1/IBM-500 iconv conversion

107584 SUNWvolu 01 468 SunOS 5.7: /usr/lib/vold/dev\_cdrom.so.1 patch

107589 SUNWcar 03 269 SunOS 5.7: se, zs, kbd and kbio.h patch

SUNWcarx

SUNWcsr

SUNWcsu

SUNWhea

SUNWpd

SUNWpdx

107624 SUNWcsu 01 460 SunOS 5.7: /usr/lib/fs/ufs/df patch

107652 SUNWxwman 06 187 OpenWindows 3.6.1: X11R6.4 XKB Extension Patch

SUNWxwplt

SUNWxwpmn

107654 SUNWxwman 06 187 OpenWindows 3.6.1: X11R6.4 LBX & XRX Extensions Patch

SUNWxwplt

107656 SUNWxwplt 06 187 OpenWindows 3.6.1: libXt Patch

SUNWxwplx

SUNWxwpmn

SUNWxwslb

107658 SUNWxwpmn 05 187 OpenWindows 3.6.1: X11R6.4 API man pages Patch

107680 SUNWcarx 01 335 SunOS 5.7: /kernel/sys/msgsys and /kernel/sys/sparcv9/msgsys patch  
SUNWcsr

107702 SUNWdtwm 04 181 CDE 1.3: dtsession patch

107716 TSIPgpx 08 66 SunOS 5.7: PGX32 Graphics Patch  
TSIPgxm  
TSIPgxw  
TSIPgxx

107723 SUNWoldst 01 446 OpenWindows 3.6.1: printtool patch

107743 SUNWqfed 04 80 SunOS 5.7: Sun Quad FastEthernet 2.2 qfe driver  
SUNWqfedu  
SUNWqfedx

107744 SUNWcsu 01 445 SunOS 5.7: /usr/bin/du and /usr/xpg4/bin/du patch  
SUNWxcu4

107796 SUNWcarx 03 138 SunOS 5.7: /kernel/fs/lofs patch  
SUNWcsr

107799 SUNWesu 02 142 SunOS 5.7: compress/uncompress/zcat patch

107807 SUNWxwplt 01 438 OpenWindows 3.6.1: xrdb patch

107813 SUNWjiu8 01 425 SunOS 5.7: Japanese UTF-8 iconv patch  
SUNWjiu8x

107834 SUNWcsr 03 221 SunOS 5.7: dkio.h & commands.h patch  
SUNWhea

107836 SUNWcsu 01 326 SunOS 5.7: /usr/sbin/format patch

107838 SUNWtnfc 01 412 SunOS 5.7: libtnfctl patch  
SUNWtnfcx

107841 SUNWcarx 02 3 SunOS 5.7: rpcsec patch  
SUNWcsr  
SUNWhea

107843 SUNWcsr 01 326 SunOS 5.7: /sbin/init and /usr/sbin/init patch  
SUNWcsu

107853 SUNWxwopt 01 412 OpenWindows 3.6.1: xdm patch

107883 SUNWdtim 05 256 CDE 1.3: sdtimage Patch  
SUNWdtma

107900 SUNWploc 01 20 SunOS 5.7: Broken backward compatibility for some Solaris locales  
SUNWploc1

107919 SUNWhea 01 318 SunOS 5.7: /usr/include/sys/mhd.h patch

107921 SUNWxwplt 01 387 OpenWindows 3.6.1: xwininfo patch

107939 SUNWqfed 01 425 Sun Quad FastEthernet 2.2: POINT PATCH: qfe driver for Solaris 7  
SUNWqfedu  
SUNWqfedx

107941 SUNWploc1 02 125 SunOS 5.7: Incorrect day order in Portuguese and Brazilian locales

107962 SUNWciu8 01 383 SunOS 5.7: iconv from UTF-8 to euc requires a buffer with 1 extra  
SUNWciu8x  
SUNWhiu8  
SUNWhiu8x

108029 SUNWwsr 02 303 SunOS 5.7: S899 u3 prodreg fixes for Java 1.1 and Java 1.2 VM

108036 SUNWpflow 01 373 SunOS 5.7: Keyboards don't recognize SunFA\_Acute characters

108068 SUNWman 03 216 SunOS 5.7: Manual Page updates for Solaris 7

108089 SUNWcsu 02 355 SunOS 5.7: /usr/bin/tail patch  
SUNWxcu4

108117 SUNWxwfs 03 44 OpenWindows 3.6.1: Font Server patch

108147 SUNWxilcg 01 353 SunOS 5.7: SX Graphics Patch

108148 SUNWcsu 01 352 SunOS 5.7: prtconf patch  
SUNWcsxu

108151 SUNWdtezt 02 257 CDE 1.3: sdtname patch

108158 SUNWcsu 01 331 SunOS 5.7: /usr/lib/fs/nfs/share patch

108162 SUNWcsr 02 96 SunOS 5.7: jsh, rsh, sh patch  
SUNWcsu

108168 SUNWxwinc 01 334 OpenWindows 3.6.1: X Window include files patch

108170 SUNWadm 01 326 SunOS 5.7: showrev patch

108175 SUNWadm 01 340 SunOS 5.7: DSR Upgrade patch for localization packages

108197 SUNWdtdst 01 324 CDE 1.3: dtpad patch

108203 SUNWcsu 03 53 SunOS 5.7: adb macro & headers for fibre channel transport layer  
SUNWcsxu  
SUNWhea

108224 SUNWcar 01 296 SunOS 5.7: envctrl driver patch  
SUNWcarx

108227 SUNWpflow 01 195 SunOS 5.7: OpenWindows applications 8-bit character corruption

108240 SUNWpflow 01 290 SunOS 5.7: Incorrect Compose file for iso8859-1 and iso8859-15

108244 SUNWcsl 01 244 SunOS 5.7: libaio patch  
SUNWcslx

108263 SUNWhmd 05 82 SunOS 5.7: hme driver patch

SUNWhmdu

SUNWhmdx

108299 SUNWcsu 01 241 SunOS 5.7: /usr/sbin/rmt patch

108311 SUNWcsu 01 272 SunOS 5.7: /usr/bin/head patch

108318 SUNWpd 03 156 SunOS 5.7: ecpp driver patch

SUNWpdx

108319 SUNWcsu 01 279 SunOS 5.7: /usr/bin/at patch

108325 SUNWfns 01 243 SunOS 5.7: libfnsp.so.1 patch

SUNWfnsx

108378 SUNWxwslb 01 187 OpenWindows 3.6.1: X11R6.4 Lint Libraries Patch

SUNWxwslx

108381 SUNWcarx 01 247 SunOS 5.7: ptsl driver patch

SUNWcsr

108383 SUNWcsu 01 272 SunOS 5.7: /usr/kernel/sys/sysacct patch

SUNWcsxu

108414 SUNWcsu 01 270 SunOS 5.7: /usr/bin/cpio patch

108451 SUNWcarx 05 3 SunOS 5.7: rpcmod patch

SUNWcsr

108592 SUNWxwinc 01 216 Openwindows 3.6.1: X Window Include Files Patch

108610 SUNWdhcsu 01 186 SunOS 5.7: /usr/sbin/pntadm patch

108665 SUNWatfsr 01 179 SunOS 5.7: /kernel/fs/autofs patch

SUNWcarx

108683 SUNWpppk 01 165 SunOS 5.7: /usr/kernel/strmod/ppp patch

SUNWpppkx

108790 SUNWplc1x 02 62 SunOS 5.7: Cultural settings update for European locales

SUNWplcx

SUNWploc

SUNWploc1

108800 SUNWcsu 01 163 SunOS 5.7: /usr/lib/fs/cache/fs/cfsadmin patch

108831 SUNWolimt 01 60 OpenWindows 3.6.1: imagetool patch

108912 SUNWdhcsu 01 152 SunOS 5.7: /usr/lib/inet/in.dhcpd patch

109001 SUNWcsu 01 130 SunOS 5.7: /usr/sbin/in.rshd patch

109203 SUNWcsu 01 103 SunOS 5.7: edit & vi patch

SUNWxcu4

109205 SUNWbtool 01 104 SunOS 5.7: /usr/ccs/bin/yacc patch

109359 SUNWplow 01 39 SunOS 5.7: Accent key not working in western european locales

```

109372  SUNWcarx  01  80 SunOS 5.7: /kernel/strmod/ldterm patch
        SUNWcsr
109377  SUNWplc1x 01  18 SunOS 5.7: Incorrect int_frac_digits,frac_digits in Norwegian loca
        SUNWploc1
109409  SUNWntpu  01  82 SunOS 5.7: /usr/lib/inet/xntpd patch
109439  SUNWcar  01  80 SunOS 5.7: simba driver patch
        SUNWcarx
109649  SUNWcsl  02   5 SunOS 5.7: nss_nisplus.so.1 & libnss_nisplus.so.1 patch
        SUNWcslx
109711  SUNWcsu  01  24 SunOS 5.7: /usr/bin/cat patch
109768  SUNWcsu  01  31 SunOS 5.7: Australia timezone patch
109770  SUNWcsu  01  11 SunOS 5.7: /usr/sbin/dumpadm patch

```

=====

See URL <http://www.pogostick.net/~pdiag/> for more info on this service.

You can download the patches with anonymous ftp with the URL

<ftp://sunsite.uio.no/pub/sun/sun-patches/>

or <ftp://sunsolve.sun.com/pub/>

## FTP Access and Configuration

FTP is a primary service of *blue.troll.nil*. There are no entries in `/etc/ftpusers`. There are no access restrictions on who can connect to the FTP server. There is no control of connection methods from the client's site. Anonymous and guest access are disabled. Users of FTP have access to the entire filesystem.

The client should start connecting through a more secure method of file transfer, such as SFTP (Secure-Shell FTP). More information about SFTP can be found in then [SSH FAQ](#). SFTP encrypts the data transfer and provides a more reliable authentication method.

All system accounts, as well as the accounts of the administrators should be placed in the proper `ftpusers` file to disable access for these accounts to FTP. These accounts should only copy files through a more secure mechanism. The FTP daemon should be run out of a `chroot'd` environment, only allowing access to the `/export/home` directory structure. This will greatly diminish the chance of users accessing unauthorized information.

TCP Wrappers are installed on the system, and they should be used with FTP. Currently, any host on the Internet may connect to the FTP service on *blue.troll.nil*. An IP Address range should be configured into TCP Wrappers to allow connections only from the client's site. This will also allow for better logging to aid in the detection of attacks.

## POP3 Access and Configuration

*blue.troll.nil* uses QPopper 2.2. This version contains a root compromise and should be upgraded as soon as possible. Serving



POP3 is a primary service for this system, and this application needs to be upgraded to keep uncompromised service. The QPopper [Homepage](#) recommends anyone using an old version of QPopper like this to upgrade as soon as possible.

To serve mail, *blue.troll.nil* should be configured to use and IMAP over SSL server. IMAP-SSL encrypts the session, so the users mail is not available clear-text over the internet, and neither is the user's password.

Stop using QPopper 2.2. It is vulnerable to a root compromise.

## **sendmail Access and Configuration**

*blue.troll.nil* uses Sendmail **8.8.5**. This version of sendmail has multiple compromises. One as simple as tracing symbolic link of a mailfile back to where it is pointing, even if it is a `.rhosts` or `passwd` file.

Instead of upgrading sendmail, consider going with [QMail](#) instead. QMail was designed with security in mind from the ground up, and there are no publicly know exploits.

## **Network Services**

The main goal of *blue.troll.nil* is to provide network access for a third-party. This machine is running more services than it needs to. The remainder of this sub-section deals with unneeded and/or reconfiguring services.

### **SSH Access and Configuration**

Currently, only people from *troll.nil* use `ssh` on this system. `ssh` allows root logins. There are no machine-level access restrictions in place for `ssh` access.

`ssh` should be redeployed on this system with `libwrap` built-in. `libwrap` allows TCP Wrappers, which are already installed on the system, to gate access based on IP Address ranges. This will mitigate the chance of unauthorized access and provide a better login facility to detect attacks. `ssh` should also be configured to disallow root logins. The system administrators accounts can be added locally to the system to belay concerns of NIS+ going down.

### **Telnet**

As per the TCP Wrappers settings, only machines local to *troll.nil* and the client's site have telnet access to *blue.troll.nil*. As mentioned earlier, this access should be revoked for the client site, and internal people should use `ssh` to connect in. Then, the `telnet` server should be shutdown by removing it's entry from `/etc/inetd.conf` and restarting `inetd`.

### **in.rshd**

Remote Shell capability should be turned off. `ssh` access should be used to replace it entirely.

### **uucp and tftp**

These services are rejected by TCP Wrappers, so they should be taken out of `inetd.conf` to avoid any confusion.

### **nfsd**

*blue.troll.nil* is running an NFS daemon, but is not exporting any filesystems. Turn this off.

## **Non-System Packages**

There are a number of non-base Solaris packages installed as well as third-party packages. They are mostly configured well; however, there are a few minor problems with some of them.

## **Miscellaneous**

### **Syslog**

*blue.troll.nil* logs everything above \*.debug to /var/adm/messages. These logfiles are rolled on a nightly basis, and one-week's worth of data is kept. There are no procedures by which to review these logs, nor are there any automated processes.

*blue.troll.nil*'s syslogd should be logging to a remote log server. This server should be running a program like [swatch](#) or [LogCheck](#). These programs should be configured to recognize out of the ordinary events and report based on the information contained in the syslog messages forwarded to the LogHost.

## File Integrity and Tripwire

No file integrity assessments are currently being done on *blue.troll.nil*. Tripwire creates cryptographic hashes of files on your system and places them in a database with other file attributes (such as mod. time, size, permissions, etc.). These attributes can, then, be checked on a routine basis to see if anything has changed. Tripwire can be found at [Tripwire Security Systems](#).

## Backups

Backups of local drives are done off a locally connected SCSI DAT drive. This part of the system is fairly unchanging, so backups are done only once a week. A cron job starts this process the same time every week, and usage is rotated between ten different tapes. When one tape is physically removed from the drive, another is placed in the drive for the next backup. These tapes are stored in a lock box in the system administrator's office space, one building away from the Data Center. I was unable to ascertain whether or not a copy was even moved off site or how often tapes are swapped out of circulation.

There are no written policies regarding backups. A written policy should be established requiring tapes to be moved off-site at regular intervals, no more than one month. Also, the contents of a backup should be checked for accuracy after each backup; this should at least consist of an after backup script which picks a random set of files and compares them to the originals. This policy should also incorporate a self-audit or preferably an external audit.

---

## Vulnerabilities

The following is a list, in order of most important to least important, of the things which are wrong with the configuration of *blue.troll.nil*.

1. *blue.troll.nil* is far behind in patches.
2. sendmail 8.8.5 has multiple exploits.
3. QPopper has a buffer overflow exploit.
4. There is no way for users to change their passwords, and the passwords given to them by the administrators are weak.
5. Fix-modes has not been run.
6. There is no file integrity checking system running.
7. POP3 users passwords are being transmitted clear-text.
8. FTP users passwords are being transmitted clear-text.
9. syslog does not log remotely.
10. FTP users have access to the entire filesystem.
11. Any machine on the Internet can connect to the FTP daemon on *blue.troll.nil*.
12. The ftpusers file is not there. It should have all system accounts as well as the accounts of the administrators.
13. Some non-essential users have shell access to *blue.troll.nil*
14. Administrators have no documentation of daily tasks and procedures.
15. Administrative access is gained through sudo without a password for the administrators.
16. All users are in a default group of nobody.
17. There are unnecessary network services running.
18. Backup tapes are easy to steal and are not checked for consistency.
19. Equipment is accessible by non-administrators.
20. Data Center access is gated by a physical-key, and not some form of smart-card.

---

## Recommendations

The following is a list, in order of most important to least important, of the things which need to be done to fix the

1. *blue.troll.nil* needs to be patched. A poor patching cycle indicates an even bigger problem: apathy on the part of the system administrators. Beyond patching, a policy on patching must be put into place to avoid this in the future.
2. Either sendmail has to get upgraded, or it has to be replaced. This machine serves mail, so it must have an MTA running at all times. I suggest removing the sendmail package, and installing QMail. QMail was designed with security in mind from the very beginning.
3. QPopper has a buffer overflow exploit. This application provides means for a serious attack. It should be upgraded or replaced for an application which is more secure.
4. Get and install the fix-modes program, or get and install YASSP. YASSP incorporates the fix-modes program into a larger, more complete, framework.
5. Get and run Tripwire. Tripwire can notice changes in files and directories, it serves as a test for tape backups, it helps diagnose exactly what a patch changes, and a number of other utilities under UNIX.
6. Replace POP3 with an IMAP over SSL solution. This will keep cleartext passwords from making it onto the network.
7. FTP should be replaced with a more secure alternative, such as the sftp application which comes with ssh. This will encrypt passwords and datafile over the network.
8. Setup a syslog server. Run some program which allows you to sift through the syslog data and determine what is normal, and what is not.
9. The FTP daemon should be run in a chroot'd environment. This will keep the FTP-only users from accessing files outside of the NFS-mounted directories.
10. TCP Wrappers should be configured to allow incoming FTP connections only from the client's site.
11. The ftpusers file should have all system accounts as well as the accounts of the administrators. Only users from the client's site should be using FTP, and this access should be revoked long-term.
12. The NIS+ domain should be set up so as to limit access to *blue.troll.nil* on a need-only base. System administrators of other machines do not have a need to access this system.
13. The administrators must create a logbook of daily activities. Their procedures and tasks need to be documented in case of accident or emergency.
14. The file `/etc/sudoers` needs to be modified to require a password to gain administrative access. This helps deter accidents from unlocked displays.
15. A group called `users` should be created, and all users from the client's site should be a member. This is better than the `nobody` user if the `nobody` id is ever used on this machine.
16. `inetd.conf` has entries for services which cannot even run, because they are disabled through TCP Wrappers. Also, `telnet`, `in.rshd`, and `tftpd` should all be disabled.
17. The tape backup procedure needs to be completely revisited. Tapes should not be accessible to those without administrative access over the machine. A Cage should be placed around the different areas of the Data Center to ensure proper physical access.
18. A Smart-Card or ADT-badge system should be put into place to log entry into a particular room.

# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced