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 permited without express written permission.

GIAC SECURITY UNIX PRACTICAL ASSIGNMENT

SANS NETWORK SECURITY 2000 TRACK 6 -UNIX

Securing Unix Step-by-Step

Amy Aton

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Overview of Anonymous FTP server

The purpose of this server is to provide anonymous FTP capabilities for the internet public. Specific requirements include the ability via anonymous ftp to download public domain reports, and permit information. Via individual guest accounts, allow access from the internet public to write and read drawing files corresponding to specific projects. This guest accounts will require authentication into a blind area of the ftp server.

The server is an Ultra sparc10 running solaris 2.7. The server contains 512 mb of memory. Internet connectivity is via a Cisco router and a Raptor firewall. The firewall allows traffic via ftp ports 20/21 from the internet to the server and SSH access is allowed to the server from the internal network. No remote dial up access is allowed.

Physical security is provided via building security personnel in lobby and on patrol on all floors. Constant surveillance by way of building cameras, monitoring access of elevators and corridors. Computer room access is controlled via electronic cipher-locks.

The following instructions are basic system setup instructions for any server residing on the Internet Accessible Segment (IAS), and specifically providing Anonymous FTP services.

Hardware Platform:

The Anonymous FTP server will be housed upon a Ultra Sparc 10 with 18 gig of disk and 512 meg of memory.

General consideration when building an IAS server include:

- Creating root partition with minimal amount of space needed to house the Core System O/S installation. General rule of thumb is 100MB of disk for root partition.
- Create a /var partition large enough to accommodate system logging per corporate policy on logging and retention requirements. General rule of thumb is 500MB.
- Create a /usr partition with 75MB file space
- Create a /opt partition for third party software. General rule of thumb is 100MB
- Creation of /swap partition. General rule of thumb for swap is "the amount of memory + (10 to 30) MB disk space".
- The rest of the file system is for local usage.

****NOTE**: Either do not have network cable connected during install or configuration or isolate system in a lab setting**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

O/S Installation:

Install the standard "Core System Support" O/S installation, Solaris version 2.7

Install any associated patches. A short list would include:

Packages to install

SUNWter	-support for different terminal display types
SUNWaccr & SUNWaccu	-accounting
SUNWlibC, SUNWdoc, SUNWman	-man pages (need all three due to dependencies)
SUNWntpr, SUNWntpu	-ntp software for time sync
SUNWscpu	-berkeley Unix binaries /usr/ucb

Remove dependencies on /usr/apg4/bin/grep from the patchadd script

```
# mv /usr/sbin/patchadd /usr/sbin/patchadd-orig
# sed s/\\/xpg4// /usr/sbin/patchadd-orig >  /usr/sbin/patchadd
# chmod 555 /usr/sbin/patchadd
# chgrp bin /usr/sbin/patchadd
```

```
# mount -r -F hsfs /dev/dsk/C0t2d0s0 /cdrom
```

```
# cd /cdrom/Solaris_ 2.x/Product
```

```
# pkgadd -d . SUNWter SUNWacc* SUNWntp* SUNWlibC SUNWdoc SUNWman
```

Once complete, load the current cluster patches.

- From an internet accessible workstation download the current cluster patches from ftp://sunsolve1.sun.com/pub/patches
- Save file to tape then restore file onto FTP server, within the /var/tmp directory
- Unzip patch cluster and install utilizing the -nosave option.
    - ./install_cluster -nosave

  Return Code 8 = patch applies to package not on system
  Return Code 2 = patch already on system

****NOTE**: Document all 'Return Code #' not equal to 2 or 8**

When install process has completed. Reboot system

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Removing files and directories of unnecessary services:

***NOTE: The following services are installed during the boot process. These services are not required to support the operation of a ftp server. By stripping out all non essential services, you minimize areas of vulnerability.

Services to be eliminated from the rc.# directories include

Remove S30sysid.net, S71sysid.sys S72autoinstall
(files supporting auto configuration)
Remove S71rpc, S76nscd, K60nfs.server, S73nfs.client, S74autofs, *cachefs*
(files supporting NFS/RPC)
Remove S80PRESERVE, S88sendmail
(misc security problems, not needed on FTP/IAS server)
Disable /etc/rcS.d/S50devfsadm (by renaming it .K50devfsadm)
(stops system from rebuilding BSD-style /dev entries)

Remove unnecessary files and directories that not required to run the system.

```
rm -rf /var/tmp *Recommended*
remove sendmail daemons
```

Remove NFS related files .

```
rm /etc/auto_*   /etc/dfs/dfstab
```

Remove crontab files not required to support AIS server

```
cd /var/spool/cron/crontabs
rm adm lp sys
```

Remove all .rhosts support from /etc/pam.conf

```
grep -v rhosts_auth /etc/pam.conf > /etc/pam.new
mv /etc/pam.new /etc/pam.conf
chown root /etc/pam.conf
chgrp sys /etc/pam.conf
chmod 644 /etc/pam.conf
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Files and directories to be created or modified:

Create /etc/defaultrouter file
touch /etc/defaultrouter

Modify /etc/hosts file

add entry for dns server
add entry for corporate syslog server, designating it as loghost

Create /etc/resolv.conf

add dns server and domain information

Modify /etc/nsswitch.conf

change hosts: line to hosts: files dns

Modify /etc/syslog.conf file to write all log files both locally and to syslog server

uncomment auth.notice ifdef(`LOGHOST', /var/log/authlog, @loghost) line

Modify /etc/rmmount.conf to preventing set-UID programs being accessed or controlled via removable media.

Add to /etc/rmmount.conf file
mount hsfs –o nosuid
mount ufs –o nosuid

Modify /etc/system to prevent some buffer overrun attacks by adding:

set sys:corpdumpsize=0
set noexec_user_stack=1
set noexec_user_stack_log=1

Modify /etc/default/passwd

MAXWEEKS= 8
MINWEEKS=1
PASSLENGTH=8

Modify /etc/default/login

Remove comment line for UMASK

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Modify /etc/default/kbd and disable the <stop-A> functionality

KEYBOARD_ABORT=disabled

Modify /etc/default/inetinit changing TCP initial sequence generation parameters from 1 to 2 providing RFC 1948 compliant sequence number generation with unique per connections ids.

TCP_STRONG_ISS=2

Create sulog

touch /var/adm/sulog
chmod 600 /var/adm/sulog
chown root /var/adm/sulog
chgrp sys /var/adm/sulog

Create loginlog

touch /var/adm/loginlog
chmod 600 /var/adm/loginlog
chown root /var/adm/loginlog
chgrp sys /var/adm/loginlog

Create the proper authlog file:

touch /var/log/authlog
chmod 600 /var/log/authlog
chown root /var/log/authlog

Modify /etc/inet/inetd.conf

Strip out all lines but ftp
Modify ftp line to support proftpd with tcpwrappers

chmod 600 /var/adm/messages
chmod 600 /var/log/syslog

Modify /etc/passwd file

Using /usr/sbin/passmgmt, remove uucp nuucp adm, lp smtp and listen user accounts
Create an user account for ftp with a /bin/false as the shell
Create accounts for system administrators

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Modify the /etc/ftpusers eliminating the ftp capabilities for the following accounts:

root
daemon
sys
bin
adm
lp
smtp
uucp
nuucp
listen
nobody
noaccess,
nobody4

Create /etc/issue file

Insert text containing the obligatory DOD unauthorized access warning messages.

Control crontab access and usage to root only via cron.allow and at.allow files

```
echo root > /etc/cron.d/cron.allow
echo root > /etc/cron.d/at.allow
chown root /etc/cron.d/*.allow
chgrp root  /etc/cron.d/*.allow
chmod 400  /etc/cron.d/*.allow
rm –f /etc/cron.d/*.deny
```

Modify the following files adding "umask 027"

/etc/.login
/etc/profile
/etc/skel/local.cshrc
/etc/skel/local.login
/etc/skel/local.profile
/etc/default/login

Modify the /etc/inet/ntp.conf file to allow Network Time syncs

server <corporate ntp server name>

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Control process rights at startup:

set umask for all system daemons

```
echo 'umask 022' >/etc/init.d/umask.sh
chmod 744 /etc/init.d/umask.sh

for dir in /etc/rc?.d
do
        ln -s /etc/init/umask.sh  $dir/S00umask.sh
done
```

Eliminate common DOS attacks by editing the /etc/init.d/inetinit file. ADD the following at the END of the file:

```
ndd -set /dev/tcp tcp_conn_req_max_q0 1024  (sets limits for half open tcp connections)
ndd -set /dev/ip ip_ignore_redirect 1       (ignores redirects used in DOS attacks)
ndd -set /dev/ip ip_send_redirects 0        (won't send redirects)
ndd -set /dev/ip ip_ire_flush_interval 60000    (causes arp flush every 60 sec vs 20min)
ndd -set /dev/arp arp_cleanup_interval 60000    (causes arp flush every 60 sec vs 20min)
ndd -set /dev/ip ip_forward_src_routed 0    (prevent forwarding pkt w/src routing on)
ndd -set /dev/ip ip_forwarded_directed_broadcasts 0 (will not forward broadcasts)
ndd -set /dev/ip ip_forwarding 0            (stops machine from forwarding pkts not its)
ndd -set /dev/ip ip_strict_dst_multihoming 1    (s/a)
```

Additional considerations:

Eliminate serial port access by modifying /etc/inittab

Remove line (DO NOT comment out, MUST be deleted)

```
sc:234:respawn:/usr/lib/saf/sac -t 300
```

reboot system

Install TCP Wrappers

***NOTE: TCP Wrappers allows you to monitor and filter incoming requests for the configured network services.

Modify syslog.conf to support tcpwrapper logging to syslog server
Redirect local logging to standard logging directory
Remember to touch tcpwrap.log file in logging directory
Edit /etc/inet/inetd.conf
    Remove all services except ftp service
    Modify Proftpd service line implementing wrapper

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Install SSH

Ported over from other server source.
Create startup script for SSH, place it in rc2.d directory starting after syslogd

Install Axent Intruder Alert
Select client install
Configure to log to corporate master server

Install ProFTPd

Configure ProFTPd generally following the sample anonymous ftp server configuration provided. Configuration modified to meet corporate specific requirements including blind directories and guest accounts for users allowed to write data to the server. And insert text containing the obligatory DOD unauthorized access warning messages.

Managing Logging Data:

Syslog.conf file has been modified to performing logging of specified information in prior sections. The next step is the modification of scripts to allow the rotation of logs keeping them in a managible state to facilitate regular and reoccuring review.

Modify /usr/lib/newsyslog
Adding the rotation of tcpwrapper logs
Adding the rotation of authlog logs
Add functionality to allow the logs most recently rotated to be ftped via cron to syslog server.

Creation of cron script executing every five minutes gathering **sar** data into a designated log file. Every evening a second cron job executes transfering the log file (date:time stamped) via ftp to the syslog server for analysis and benchmarking.

Lock down EEPROM:

Configuring EEPROM security mode to force the system administrator to enter a password whenever an EEPROM command is issued allows addition security at the physical security level and limits the abilities of an intruder with regard to rebooting the system.

To set EEPROM security mode:
eeprom security-mode=command
Changing PROM password:
New password: <enter non-root password>
Retype new password: <enter non-root password again>

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Document all EEPROM passwords then seal them in an envelope. Document the outside of the envelope with the generic contents. The envelope is then added to the corporation IT safe with other sealed envelopes containing password and security information for other corporate server as part of corporate contingency and recovery policies.

Install the fix-modes program:

Download latest version from (different from 6.6 Solaris Practicum page1-103):

http://www.fwi.uva.nl/pub/solaris to separate internet accessible server

Once fix-modes.tar.gz has been downloaded, unzipped, untarred and make on remote server within directory specified. Once make is complete, tar specified directory to tape, then restore on Anonymous FTP server. From restored directory execute program.

./fix-modes

Backup System:

Boot system in single user mode

```
reboot -- -s
```

Mount all filesystems

```
fschk
mount -a
```

Perform two ufs backups of the file system

```
mt /dev/rmt/0 rewind
for dir in / /usr//var/local
do
        ufsdump 0f /dev/rmt/0n $dir
done
mt /dev/rmt/0 eject
```

Take both backups to a different system and verify backup

Store one backup locally and one at corporate offsite storage location

Place system into production:

Change system IP address to reflect location on IAS.
Shutdown system
Connect network cable to appropriate subnet
Boot system

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Backup Policy

Due to the function of this server, the data is assumed suspect. Upon server establishment and after subsequent patch update, a CD is burned with the O/S, MD5 checksum information and file structure minus the public ftp data areas. The primary public domain reports, drawing files and permit information is housed on an internal server which is routinely pushed to out to anonymous ftp server. Should an intrusion be detected, the system will be taken offline and rebuild utilizing backup media.

Weekly incremental backups will be run on this system. Index of files that were backed up is emailed to ssa for review. Full backups are performed monthly.

Full backups are retained for a period of 6 months. Incremental backups are retained for 1 month. Full backups are stored at our corporate offsite storage facility. Incremental backups are stored locally in our corporate tape vault.

Recovery Plan

Non Disk Hardware Failures:

Support contract in place with a 4 hour response time.

Disk Drive Hardware Failures:

Replacement disks are onsite.

Install and configure disk
Perform system restore from tape
Push data from internal system

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Documents and Reference Sites

- The Solaris Security FAQ http://www.sunworld.com/common/security-faq.html
- Sun AnswerBook http://docs.sun.com
- CERT http://www.cert.org
- CIAC http://ciac.llnl.gov
- SANS http://www.sans.org
- Casper Dik (fix-modes.tar.gz) http://www.fwi.uva.nl/pub/solaris
- Solaris Security Guide http://www.sabernet.net/papers/Solaris.html
- NIST (National Institute of Standards and Technology) Principles and Practices for Securing IT Systems http://csrc.nist.gov/nistpubs/800-14.pdf

• Reference Material

- Practical Unix & Internet Security, Second Edition
  Simson Garfinkel and Gene Spafford, O'Reilly & Associates, ISBN1-56592-148-8

- Sun Performance and Tuning
  Adrian Cockcroft and Richard Pettit, Sun Microsystems Press, A Prentice Hall Title, ISBN 0-13-095249-4

- SANS Institute's Solaris Security, Step by Step Version 1.0
  Hal Pomeranz, Deer Run Associates, SANS Institute
- SANS Solaris Practicum
  Hal Pomeranz, Deer Run Associates, SANS Institute

Software Tools

- Solaris Patches http://sunsolve.sun.com
- SSH http://www.ssh.org
- ProFTPd http://www.ProFTPd.com
- Axent Intruder Alert http://www.axent.com
- Tcpwrapper ftp://ftp.porcupine.org/pub/security/tcpwappers_7.6.tar.gz

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.