GIAC
CERTIFICATIONS

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.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

SCO OpenServer 5.05 Security for the Systems Administrator
Brian McBee

Introduction

I was recently given a batch of SCO systems to administer. These were originally set up without much thought given to security, so I set about trying to get them up to snuff.

SCO OpenServer 5.05 is a popular Unix server version in use in small business environments. It is possible to create a reasonably secure Unix environment using this operating system. However, the default installation leaves much to be desired. This paper is intended to get you from a default installation to something closer to a secure environment.

Installation – Security Profiles

Install SCO OpenServer 5.05 directly from the installation CD. During installation, you will be asked to select a Security Profile. This selection can be changed after installation, and individual components of these choices can also be modified later. The choices for Security Profile are (in order of increasing security):

Low – Allows anything for a password, including a null password. Allows unlimited password failures. Default umask is 022. No C2 features. All users can schedule jobs. Home directory permissions are set to 755. 8 significant characters in password. Use of the su command is not logged. No use of shadow passwords.

Traditional – Same as Low, except: Minimum password length of 3 characters. Allows 99 failed login attempts and pauses 1 second between each attempt. Clears SUID/SGID bit on writing to a file. Logs use of the su command. Adds shadow passwords.

Improved – Same as Traditional, except: Expires passwords every 42 days. Password lifetime of 365 days. Minimum password length 5. Passwords are checked for triviality. Passwords are required for login. Maximum of 9 unsuccessful login attempts. Delay 2 seconds between attempts, default umask 027. User accounts cannot be deleted. All users are locked out if the security database is corrupted. Trusted Computing Base is used.

High – Same as Improved, except: Minimum time between password changes is 14. Password lifetime is 90 days. Passwords are generated, users cannot choose their own. Minimum password length is 8 characters. Strong password obviousness checks are in place. Maximum of 5 unsuccessful login attempts. Default umask is set to 077. All daemons must be run as a specific user.

"Improved" and "High" are intended to be C2 compliant. I would recommend setting it to "High". If your system is already up and running, you can still change this setting. Run `scoadmin` from the command line, select system, then security, the Security Profile Manager. It will take a reboot for any changes to take effect.

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

Patches

Download and install the latest Release Supplement (rs505a) from http://www.sco.com/support/ftplists/osr5list.html

Download and install the latest security patches from http://www.sco.com/security/ At this writing, the patches listed there are from October 23 2000. The ones that apply to OpenServer 5.05 at this writing (In January of 2001) are:
SSE014B – imapd
SSE016 – mscreen
SSE017 – ordist and rdist
SSE018 – bootpd
SSE019 – calserver
SSE020 – rshd and scheme
SSE022 – sendmail
SSE024B – xserver
SSE037C – multiple vulnerabilities
SSE050C – multiple vulnerabilities
SSE055 – pkg* tool fixes
SSE062 – MMDF
SSE063 – ARCserve
SSE068D – userOsa
SSE069C – libX11 and libXt
SSE070B – wu-ftpd
SSE071 – scohelp
Unfortunately, you have to download and install these patches by hand. Note also that SSE050C must be installed from single user mode.

Emergency boot floppies

Do create an emergency boot floppy set and make sure that you have all the files and drivers needed to access your backup media. These can save your bacon in the case of an unbootable system. You can boot from the floppy, and run fsck if it will not run all the way through when booting off the hard drive. You can also use it to repartition the hard drive and restore files or the whole system from backups. The instructions to do this are in chapter 5 of the SCO OpenServer Handbook.

Auditing and Logging

SCO OpenServer has built-in auditing capability as part of its C2 capabilities. The audit manager can be accessed by running

```
scoadmin au
```

at the command line. I turned on auditing with the default settings, which tracks the following actions: System startups and shutdowns, logins and logoffs, file writes, file/message/semaphore creation, deletion, and permission or ownership changes, permission denials, system admin and operator actions, tasks that fail due to insufficient privileges, and resource denials (missing files or insufficient memory). Once auditing is turned on, reports can also be run from the audit manager.

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

By default, syslog is configured to send all messages from all facilities at all levels to /usr/adm/syslog. You may want to remove the logging of all mail messages from here as they are a lot to wade through. It is also a good idea to send logging information to another machine setup to be a syslog host. Sample syslog.conf entries might look something like this:

```
# send all messages except mail and authpriv to syslog file
*.debug;mail.none;authpriv.none    /var/adm/syslog
# send mail messages to separate file
mail.*                             /var/adm/maillog
# send authpriv messages to separate file, and send them to
# our syslog server
authpriv.*                         /var/adm/secure
authpriv.*                         @sysloghost.mydomain
# send emergency messages to all terminals, and our
# syslog server
*.emerg                            *
*.emerg                            @sysloghost.mydomain
```

You will probably want to remove the cleanup script from root's crontab, or at least modify it. By default, it clears wtmp once a week by default.

Disable services

When first installed, SCO OpenServer enables quite a few services by default. The list of services run by inetd includes: ftpd, telnetd, rshd, rlogind, rexecd, fingerd, comsat, ntalk, pop3, and the "internal" services tcpmux, echo, discard, chargen, daytime, and time. You should comment out all of these except the ones you absolutely need in your environment.

Most other tcp/ip services are started from files in the /etc/rc2.d directory. You can disable these by renaming the startup file to start with a dot or period. I renamed all of these on my system. Here are the daemons and which files start them:

nfsd	S89nfs
nis	S85nis
sco-inet daemon	S91manahttp
sendmail daemon	P86sendmail
rpc server	S84rpcinit
netscape fasttrack server	S90fasttrack AND S90atlas

Disable snmpd by renaming /etc/snmpd.conf to /etc/snmpd.old.
Disable the scohelp server by running at the command line:
`/etc/scohttp disable`
You will also have to remove the http line from /etc/inittab, or it will start back up when you reboot the server. NOTE: if you disable this, man pages will no longer work ;-(

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

Once I disabled these, and rebooted the server, the only tcp port that was still listening was port 6000 (X-windows)

Password Policy

Regardless of which Security Profile you selected when you installed the operating system, you can change the password policy to match your security policies. Edit the files /etc/default/passwd and /etc/default/goodpw. The man pages for these two files explain the various settings.

You can also change the password policy for a specific user by using Account Manager. You can run Account Manager by typing:

```
scoadmin a
```

on the command line. Select the user you want to change, and pull down the Users menu to Password Restrictions.

TCPWrapper

Unfortunately this is not available in binary form. You will either have to install the development system, or get the GNU development tools installed. I didn't have the development system, so I installed GCC, GNU make, GZIP, and the GNU fileutils and binutils from the Skunkware 2000 CD. If you don't have this CD, it is all available from the SCO website at:
http://www.sco.com/skunkware
You will also have to install the "SCO OpenServer Linker and Software Development Libraries" from the SCO OpenServer installation CD.

Download, compile and install from
ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz
This compiled just fine for me once I had all the proper tools in place. Follow the instructions in the README file to see how to use this to protect your inetd services.

Install Secure Shell

There is a binary distribution for this. I first tried downloading and compiling the source both for the commercial version off ssh and for OpenSSH, failing miserably both times. I was finally able to find binaries for this at:
ftp://drake.strhold.it/sco_security/
Read the README.ssh file, as it tells you how to install the software and create your host keys.

To make this work, you will also have to install the Zlib. Source for this is available at:
http://www.freesoftware.com/pub/infozip/zlib/
Make the "shared library" version of this to use with ssh.

Once I had it installed, I created a file in /etc/rc2.d called S99sshd to start the daemon up at system bootup:

```
#! /bin/sh
```

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

```
case $state in
'start')
        if [ ! -f /usr/local/ssh/sbin/sshd ]
        then
                exit
        fi
        su root -c "/usr/local/ssh/sbin/sshd" > /dev/null &
        ;;
'stop')
        if [ -f /usr/local/ssh/etc/sshd.pid ]
        then
                su root -c "kill `cat
//usr/local/ssh/etc/sshd.pid`"
        fi
        ;;
esac
```

Tripwire

Download, compile and install from
http://www.tripwire.com/products/asr.cfm
I had to install GNU flex and bison from the Skunkware CD to make this. Follow the instructions in the README file.

Sendmail configuration

The version of sendmail that is installed is 8.8.8. If you are not going to be receiving email on this machine, you don't need sendmail running as a daemon. You can still send outgoing mail just fine.

If you do need to receive incoming email on this machine, run scoadmin, and select sendmail configuration. Run through each of the menu items, configuring those that apply to your situation.

If you disabled the sendmail daemon earlier, you will need to re-enable it by renaming /etc/rc2.d/.P86sendmail to /etc/rc2.d/P86sendmail (remove the dot).

BIND configuration

A whole new set of BIND vulnerabilities has recently been found, so if you are going to use your machine as a DNS server, you need to have the latest version. As of this writing, that is 8.2.3. This is available at:
http://www.isc.org/products/BIND/bind8.html
I followed the instructions in the INSTALL document, copied port/sco50/Makefile.set.gcc to port/sco50/Makefile.set, and ran:
`make clean; make depend; make all`
I then found that it wouldn't install properly. I had to edit the port/sco50/tools/libbind.sh script, changing two occurences of
`/bin/ar` to `/usr/local/bin/ar`

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

and on occurrence of
`/bin/cc -b elf` to `/usr/local/bin/cc -melf`

Once I did that, I ran `make install` and everything installed properly. You will have to change the /etc/rc2.d/S85tcp file which starts up named to point to the new executables. Change one occurrence of
`/etc/named` to `/usr/local/etc/named`
and two occurences of
`/etc/ndc` to `/usr/local/etc/ndc`
You can then configure your /etc/named.conf file as usual.

Summary

It was a twisty turny road trying to get things setup on this system. I went down many blind alleys trying to get tools downloaded and compiled. Hopefully this will make it a little easier for the next person in my situation. With a little work, SCO OpenServer 5.0.5 can be made into a reasonably secure system.

Notes

Santa Cruz Operation, Inc, "SCO OpenServer 5.0.5 Documentation Library." 22 January 2001, URL: http://osr5doc.sco.com:1997/ (22 January 2001)

Santa Cruz Operation, Inc, "SCO Security Home Page." 22 January 2001. URL: http://www.sco.com/security/ (22 January 2001)

Brotzman Lee E., and Ranch, David A., editors, "Securing Linux Step-by-Step Version 1.0."

Venema, Weitse, "TCP WRAPPER: Network monitoring, access control, and booby traps." 31 August 1992. URL: ftp://ftp.porcupine.org/pub/security/tcp+wrapper.txt.Z (22 January 2001)

Green, John, "Basic Unix Auditing", 9 Feb 2000.

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