Installation tripwire

Trojan Horse Detector

19th of October 2000

Document name:	Installation tripwire-V1.0.pdf
Version:	V 1.0
Author:	Ivan Buetler, Compass Security AG
	ivan.buetler@csnc.ch
	http://www.csnc.ch/
References:	tripwire README
Date of delivery:	19th of October 2000
Document state:	PUBLIC

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

CONTENT

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1 Installation

1.1 Introduction

Tripwire creates cryptographic chechsum over files you can define. After you have created the reference database, tripwire can check the checksum all 6 hours for you. This will help you to identify modified binaries within your Solaris distribution.

1.2 Version control

Version	Author	Description	Filename
1.0	Ivan Buetler ivan.buetler@csnc.ch	Initial version saved on http://www.csnc.ch/download/	Installation-tripwire-V1.0.pdf

[Ivan] If you feel like having something you would like to see in this document, pls. Let me know. I will leave the version control chapter in the future. So everybody can see who did what on this document.

1.3 Download source

Download tripwire from:

http://www.tripwiresecurity.com/

Please read the license agreement.

1.4 Copy the source to /opt/download

Compass recommends to copy or move all sources to the /opt/download directory. After the sucessfull compilation and installation, the sources goes to /opt/installed directory. If the Solaris Administrator wants to check weither a package is already installed or not, he can use the traditional pkginfo (Solaris packages) and the list of /opt/installed to check versions of installed packages.

1.5 Unpack the source

gzip -d tripwire.tar.gz
tar –xvf tripwire.tar

This will untar the sources into /opt/download/tripwire directory

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1.6 PATH configurations before compilation

```
Corro:tripwire-1.3.1# find . -type f |xargs grep "/var/adm/tripwire"
./Makefile:DESTDIR = /var/adm/tripwire/bin
./Makefile:DATADIR = /var/adm/tripwire
./include/config.h:#define CONFIG_PATH     "/var/adm/tripwire/config"
./include/config.h:#define DATABASE_PATH   "/var/adm/tripwire/database"
```

1.7 Configure software

- read the README at least once
- read the FAQ file
- edit the include/config.h file to set the appropriate values for your site
- "make && make test"
- go back and read the README and FAQ for real to understand why the test failed.
- move the Tripwire binary, any contrib/* scripts or programs, and copies of the configuration files to their final destination.
- edit your copy of the config file to suit local needs
- run Tripwire in initialization mode
- set the destination directory's disk to "read-only" in hardware, and/or take stand-alone signatures of all the files using the "siggen" utility.
- resume normal operations.

1.8 Configuration example

Tripwire is in

/var/adm/tripwire

```
Corro :tripwire-1.3.1# cd /var/adm/tripwire/
Corro :tripwire# find . –print
./bin
./bin/tripwire
./bin/siggen
./bin/databases
./bin/databases/tw.db_corro
./bin/8.9.00:10.22.tripwire.log
./bin/8.9.00:16.07.tripwire.log
./database
./database/tw.db_corro
./config
./config/tw.config
./8.9.00:16.07.tripwire.log
./log
./log/tripwire.log
./log/tripwire.log.09.08.00-16:37
./log/tripwire.log.09.11.00-06:00
./log/tripwire.log.09.11.00-12:00
./log/tripwire.log.09.11.00-16:00
./log/tripwire.log.09.12.00-06:00
./log/tripwire.log.09.12.00-16:00
./log/tripwire.log.09.13.00-06:00
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1.9 Create tripwire configfile

Edit

/var/adm/tripwire/conf/tw.config

for your needs

1.10 Create reference database

cd /var/adm/tripwire/bin
./tripwire –initialize

1.11 Copy new created reference to used-database directory

mv /var/adm/tripwire/bin/database/tw_db_corro /var/adm/tripwire/database/tw_db_corro

1.12 Automated tripwire check done by crontab

```
corro:tripwire-1.3.1# crontab -l
#ident  "@(#)root       1.14    97/03/31 SMI"   /* SVr4.0 1.1.3.1       */
#
# The root crontab should be used to perform accounting data collection.
#
# The rtc command is run to adjust the real time clock if and when
# daylight savings time changes.
#
10 3 * * 0,4 /etc/cron.d/logchecker
10 3 * * 0   /usr/lib/newsyslog
15 3 * * 0 /usr/lib/fs/nfs/nfsfind
1 2 * * * [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1
0 6,12,16 * * 1-5 /root/scripts/tripwire > /dev/null 2>&1
```

```
corro:tripwire-1.3.1# cat /root/scripts/tripwire
#! /bin/csh -f
################################################################################
#       Autor:          BUT
#       Zweck:          Tripwire Check
#       Aenderung:      1. Mar 2000
#       Name:           /root/scripts/tripwire
################################################################################
set path=(/bin /usr/sbin /usr/bin /var/adm/tripwire/bin /usr/ucb /etc .)
# Variablen setzen:
#
set logfile = "/var/adm/tripwire/log/tripwire.log"
set d=`date '+%m.%d.%y-%H:%M%n'`
#
if ( -e $logfile ) then
        rm  $logfile
else
        echo "file exist. nicht" >> $logfile
endif

##########################################
# Tripwire Aufruf
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
/var/adm/tripwire/bin/tripwire >& $logfile

##########################################
# Kopieren von tripwire.log zu tripwire.log.datum

if ( -e $logfile ) then
        cp  $logfile $logfile.$d
        mail -s "tripwire corro" root < $logfile.$d
else
        echo file exist. nicht >> $logfile
endif
```

This will mail the change to root

1.13 Clean-up Installation

Compass recommends to tar the already running distribution and move it to /opt/installed directory.

cd /opt/download/tripwire
tar –cvpf tripwire-compiled.tar *
mv ./tripwire-compiled.tar /opt/installed

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch