Tripwire - Academic Source Release (ASR)

- Kurzakte -

Installation	
• Paket Tripwire aus Paketgruppe Produktivität/Sicherheit installiert nach /usr/sbin/tripwire • bei SUSE 10.0 Installation des Pakets tripwire-2.3.1-186.i586.rpm von SUSE 9.2 • Download der Quellen oder Binaries von http://sourceforge.net/projects/tripwire/	
Besondere Merkmale	
• gehört zu den Host-basierten Intrusion-Detection-Systemen (IDS), genauer: System Integrity Veryfier (SIV)	
Konfiguration des Servers und wichtige Datenbanken	
/etc/tripwire/tw.cfg	• die mit twadmin aus der ASCII-Vorlage twcfg.txt (liegt nach der rpm-Installation vor) erzeugte binäre Konfiguratonsdatei • für den Mail-Versand folgende Zeilen hinzufügen (ASCII-Datei twfg.txt) MAILPROGRAM = /usr/sbin/ipostfix MAILMETHOD = SMTP Test mit `"/usr/sbin/tripwire --test --email root"`
/etc/tripwire/tw.pol	• die mit twadmin erzeugte binäre Policydatei aus der twpol.txt • Jeder Eintrag betrifft genau ein Objekt mit einer Eigenschaftsmaske: `[!|=] Objekt -> [Auswahlmaske] [#Kommentar]` • als Objekte sind Dateien oder ganze Verzeichnisse mit absolutem Pfad erlaubt (Achtung: jedes gemountete Dateisystem separat aufführen!)
/var/lib/tripwire/datei.twd	• die Baseline-Datenbank der Tripwire-Initialisierung • dient als Grundlage zum Erkennen späterer Veränderungen • sollte zum Schutz vor Manipulationen auf ein sicheres Medium (CD-ROM) kopiert und vor Benutzung mit siggen verifiziert werden
/var/lib/tripwire/report/*.twr	• Reportdateien der Tripwire-Checks im Binärformat • im Klartext lesbar mit twprint
Anwendung von Tripwire	
4 Kommandos zum Management von Tripwire: tripwire: Basisoperationen wie Erstellen der Tw-Datenbank und Integritätschecks gegen die Datenbank twadmin: Erstellen, verschlüsseln und signieren der Tw-Policy-, -Konfigurations- und key-Files twprint: Ausgabe der Datenbank und Reportfiles in lesbarem Text siggen: Anzeige der Hash-Werte für Dateien	
tripwire --init –v	• Initialisierung erstellt eine Referenz-Datenbank. • systemkritische Dateien vorher manuell überprüfen (inetd.conf, passwd)
tripwire --check –v –l 100	• Integritätstest nur für Dateien mit hohem Risikofaktor (über 100) • Die Auskunftsfreudigkeit kann durch quiet (einzeilige Ausgaben) und verbose (zeitgleiche Ausgabe) reguliert werden. Sämtliche Signaturen werden üblicherweise in Base64-Notierung ausgegeben. print-hex erzwingt die Ausgabe als Hexadezimalzahl, was notwendig wird, wenn Signatur-Vergleiche zwischen inkompatiblen Systemen erforderlich sind. • erzeugt einen Bericht unter $REPORTFILE laut twcfg.txt mit Endung .twr
twprint --print-report –r *.twr	• Klartextausgabe eines Berichts
tripwire --update –r datei.twr	• Wartung der Datenbank, nachdem Dateien legitim geändert wurden • Änderungen sichtbar im Abschnitt "OBJECT SUMMARY" mit [x]
tripwire --update-policy p.txt	• Anpassen der Richtlinie, falls man zu viele falsche Positive erhält • Einlesen der neuen Policy-Datei (hier p.txt)
tripwire --check --interactive	• interaktive Aktualisierung der Referenz-Datenbank als wohl gebräuchlichste Wartungsmethode, erfordert gesetzte Variable EDITOR (export EDITOR=vi). • Sämtliche Inkonsistenzen, die in einem ersten Arbeitsschritt aufgespürt wurden, werden nachfolgend sogleich zur Aktualisierung angeboten.
twadmin	• administratives Frontend zur Erstellung und Darstellung von Konfigurations- und Richtliniendateien sowie zur Verschlüsselung
siggen –Option Konfigdatei	• berechnet Hash-Signaturen beliebigerDateien zum Erkennen von Manipulationen • unterstützte Hash-Formate sind Haval, SHA/SHS, MD5 und CRC32
Dokumentation	
man: twconfig (4), twpolicy (4), twfiles (5), siggen (8), tripwire (8), twadmin (8), twintro (8), twprint (8)	

Kommandofolge zur Initialsierung und Anwendung von Tripwire unter SUSE 9.2

Installation von tripwire:
Ist bei SUSE ab 9.3 nicht mehr dabei. Einfach das Paket tripwire-2.3.1-186.i586.rpm von SUSE 9.2 installieren mit "rpm –i tripwire-2.3.1-186.i586.rpm"

alternativ: Installation aus dem Binary-Paket tripwire-2.4.0.1-x86-bin.tar.bz2:
Entpacken, Kopieren mit Hilfe des Skripts contrib/install.sh, dem als Parameter die angepasste Datei install.cfg mitgegeben wird

Kopieren bzw. Erzeugen der Muster-Policy-Datei:
Red Hat: `cp /usr/share/doc/packages/tripwire/twpol.txt /etc/tripwire`
SUSE: `cp policy.pl resource.txt /etc/tripwire` # download
`perl policy.pl` # generiert die Policydatei `hostname`-policy.txt aus resource.txt
Enthaltene bzw. erzeugte Dateien:

- `policy.pl`: mit "`perl policy.pl`" ausführbares Programm
- `resource.txt`: nach Tripwire Policy-Style formatiertes File, dessen Einträge nach Überprüfung des aktuellen Linuxsystems in ein hostspezifisches Policy-File geschrieben werden.
- `$hostname-policy.txt`: das neu generierte, von Tripwire verwendbare Policy-File
- `error.txt`: Fehlermeldungen und nicht gefundene Dateien werden hier protokolliert

Sichten der von SUSE erzeugten Konfigurationsdatei twcfg.txt

```
notebookneu:/etc/tripwire # cat twcfg.txt
##
## We only set the mandatory variables to the default values.
## These are necessary to make tripwire work.
##
POLFILE         = /etc/tripwire/tw.pol
DBFILE          = /var/lib/tripwire/$(HOSTNAME).twd
REPORTFILE      = /var/lib/tripwire/report/$(HOSTNAME)-$(DATE).twr
SITEKEYFILE     = /etc/tripwire/site.key
LOCALKEYFILE    = /etc/tripwire/$(HOSTNAME)-local.key
```

Anpassen der Musterdatei an die Gegebenheiten von SUSE (Setzen von Variablen):

```
notebookneu:/etc/tripwire # vi notebookneu-policy.txt
...
@@section GLOBAL
TWROOT="/usr";
TWBIN="/usr/sbin";
TWPOL="/etc/tripwire";
TWDB="/var/lib/tripwire";
TWSKEY="/etc/tripwire";
TWLKEY="/etc/tripwire";
TWREPORT="/var/lib/tripwire/report";
HOSTNAME="notebookneu";
...
```

Generieren des Site-Schlüssels zur Verschlüsselung der Konfigurationsdateien:

```
notebookneu:~ # twadmin --generate-keys -S /etc/tripwire/site.key
Enter the site keyfile passphrase:
Verify the site keyfile passphrase:
Generating key (this may take several minutes)...Key generation complete.
```

Generieren des local-Schlüssels zum Start von tripwire:

```
notebookneu:~ # twadmin --generate-keys -L /etc/tripwire/${HOSTNAME}-local.key
Enter the local keyfile passphrase:
Verify the local keyfile passphrase:
Generating key (this may take several minutes)...Key generation complete.
notebookneu:~ # ls -l /etc/tripwire/*.key
-rw-r--r--  1 root root 931 Feb  2 14:13 /etc/tripwire/notebookneu-local.key
-rw-r--r--  1 root root 931 Feb  2 14:09 /etc/tripwire/site.key
notebookneu:~ # chmod 600 /etc/tripwire/*.key
```

Erzeugen der binär verschlüsselten Konfigurationsdatei /etc/tripwire/tw.cfg (site-Passphrase nötig):

```
notebookneu:~ # twadmin --create-cfgfile -S /etc/tripwire/site.key \
/etc/tripwire/twcfg.txt
Please enter your site passphrase:
Wrote configuration file: /etc/tripwire/tw.cfg
```

Erzeugen der binär verschlüsselten Policy-Datei /etc/tripwire/tw.pol (site-Passphrase nötig):

```
notebookneu:~ # twadmin --create-polfile -S /etc/tripwire/site.key
/etc/tripwire/`hostname`-policy.txt
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
```

Erzeugen der Referenz-Datenbank entsprechend den Policies (nachfolgend auf eine CD kopieren):
erzeugt Datei /var/lib/tripwire/${HOSTNAME}.twd mit einer Größe von mehreren MB; dauert mehrere Minuten

```
notebookneu:~ # tripwire –init [-v]
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
Wrote database file: /var/lib/tripwire/notebookneu.twd
The database was successfully generated.
notebookneu:~ # ls -lh /var/lib/tripwire/notebookneu.twd
-rw-r--r--  1 root root 5.1M Feb  2 14:27 /var/lib/tripwire/notebookneu.twd
```

regelmäßiger manueller Systemcheck mit:
erzeugt jeweils eineReportdatei /var/lib/tripwire/report/${HOSTNAME}-YYYYMMDD-HHMMSS.twr

```
notebookneu:~ # tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
Wrote report file: /var/lib/tripwire/report/notebookneu-20060202-144400.twr

Tripwire(R) 2.3.0 Integrity Check Report
Report generated by:          root
Report created on:            Thu Feb  2 14:44:00 2006
Database last updated on:     Never
================================================================================
Report Summary:
================================================================================
Host name:                    notebookneu
Host IP address:              192.168.1.200
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/notebookneu.twd
Command line used:            tripwire --check
================================================================================
...
Total violations found:  2
...
Integrity check complete....
```

regelmäßiger automatischer Systemcheck via cron (systemschonend):

```
notebookneu:~ # crontab -e
30 3 * * * nice -19 /usr/sbin/tripwire --check | /usr/bin/mail -s "Tripwire
Check" root 2>&1
```

nachträgliches Lesen der binären Reportdateien mit:

```
notebookneu:~ # twprint --print-report -r \
/var/lib/tripwire/report/notebookneu-20060202-144400.twr
```

interaktives Aktualisieren der Baseline-Datenbank hostname.twd

tripwire --check --interactive oder # erzeugt neuen Report
tripwire --update -r /var/lib/tripwire/report/hostname-zeitstempel.twr # Einlesen des letzten Reports