Att installera och konfigurera Tripwire

Ett steg åt ökad säkerhet för ditt nätverk är att installera och använda Tripwire. Tripwire är ett program som använder MD5 algoritm för att kalkylera en checksumma för viktiga filer. Dessa checksummor jämförs sedan periodvis för att se om någon förändring har skett.

Tripwire använder jag på min filserver. I mitt nätverk är det den viktigaste enheten och jag vill att den skall vara så säker som möjligt. Programmet kan konfigureras att även kontrollera andra datorer på nätverket.

Installation

Steg 1: Logga in på systemet som root.

Steg 2: Installera tripwire genom att vid prompten skriva in: rpm –i tripwire-1.2 -1.i386.rpm.

```
[root@ /root]# rpm –i tripwire-1.2-1.i386.rpm
<ENTER>
```

Starta upp tripwire

Tripwire har fyra arbetssätt som den opererar i; **generering av databas, uppdatering av databas, "interactive update"** som fungerar som uppdatering av databas men frågar användare innan uppdatering samt **kontroll** så att ingen fil har ändrats.

Steg 3: För att initiera databasen skriv följande kommando in vid prompten: /usr/sbin/tripwire –init .

```
[root@ /root]# /usr/sbin/tripwire -init <ENTER>
```

På skärmen kommer det att se ut som följer:

```
###   Warning:    creating ./databases directory!
###
###   Phase 1:    Reading configuration file
###   Phase 2:    Generating file list
###   Phase 3:    Creating file information database
###
###   Warning:    Database file placed in
                  ./databases/tw.db_din_maskins_namn
###
```

Själva genereringen av databasfilen kan ta en bra stund.

Testa tripwire

För att se om tripwire fungerar som förväntat, skall vi göra en förändring i en systemfil. Filen vi skall använda oss av är /etc/passwd och vi testar med att utföra kommandot touch. Touch gör ingenting förutom att den förändra tidstämpeln på filen.

Steg 4: För att testa tripwire, skriver vi in följande kommando vid prompten: touch /etc/passwd .

```
[root@ /root]# touch /etc/passwd <ENTER>
```

Steg 5: Låt nu tripwire upptäcka att något har förändrats. Skriv in följande kommando vid prompten: tripwire –interactive .

```
[root@ /root]# /usr/sbin/tripwire -interactive
<ENTER>
```

tripwire visar att /etc/passwd har förändrats och du måste bekräfta förändringen.

Utdrag ur lista som presenteras på skärm:

```
###Attr   Observed (what it is) Expected (what it should be)
### ================================================
/etc/passwd
   st_ctime Sat Sep 4 11:03:32 1999 Mon Aug 18 17:16:20 1999
---> File: '/etc/passwd'
---> Update entry [YN(y)Nh?]
```

Svara Y om du är säker på att vara den ende på systemet.

För att upprätthålla ditt systems säkerhet, förvara filen med databasen på ett säkert sätt.

Att få email från tripwire

Ett bra sätt att underlätta mitt arbete, är att låta tripwire köras automatiskt för att sedan skicka ett meddelande via email med resultatet av körningen.

RedHat tripware rpm placerar en fil i katalog /etc/cron.daily, tripwire.verify. Körs automatiskt av cron, resultatet av körningen skickas som email till root.

Problem

Fungerar utan problem i RedHat 5.2. Mandrake 6.0 fungerade det inte.