HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Alati za provjeru integriteta datoteka

CCERT-PUBDOC-2002-12-08

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Programski alati za provjeru integriteta datotečnog sustava (engl. *file integrity checkers*) su programi koji u kombinaciji s ostalim alatima za detekciju neovlaštenih aktivnosti omogućuju implementaciju naprednijeg sigurnosnog modela računalnih sustava.

Za razliku od vatrozida i IDS sustava koji pružaju zaštitu na mrežnom nivou, alati za provjeru integriteta datotečnog sustava orijentirani su prema pojedinim radnim stanicama, odnosno poslužiteljima (engl. *host based tool*).

Instalacijom programa ovog tipa omogućuje se pravovremeno uočavanje neovlaštenih promjena unutar datotečnog sustava, što ih čini posebno korisnima u postupcima detekcije i prevencije malicioznih aktivnosti. Isti su se također pokazali vrlo korisnima i kod forenzičke analize kompromitiranih računala, budući da omogućuju prilično jednostavnu detekciju promijenjenih datoteka i direktorija.

Predviđeni su za instalaciju na onim poslužiteljima koji imaju poseban značaj unutar organizacije i koji samim time predstavljaju potencijalne mete napada neovlaštenih korisnika. Također se mogu primijeniti i na svim ostalim vitalnim dijelovima računalnog sustava (vatrozidi, IDS sustavi, mrežna oprema ...), gdje je potrebno posebnu pažnju posvetiti sigurnosti.

2. Način rada

Gotovo svi programi ovog tipa rade na sličan način. U prvom koraku provodi se skeniranje vitalnih dijelova datotečnog sustava, na temelju kojeg se kasnije kreira jedinstveni "otisak" sustava u poznatom, sigurnom stanju. Pod vitalnim dijelovima sustava smatraju se svi oni direktoriji i datoteke koji imaju poseban značaj unutar sustava i čije se neovlaštene promjene žele kontrolirati.

Nakon što je kreiran "otisak" sustava moguće je u bilo kojem trenutku pokrenuti provjeru integriteta (engl. *check integrity*), kojom se uspoređuje trenutno stanje sustava s ranije kreiranim "otiskom".

Sve promjene u odnosu na inicijalno stanje biti će prijavljene te se mogu tretirati kao pokazatelji potencijalnog kompromitiranja sustava. Budući da postoji mogućnost da su promjene na sustavu posljedica legitimnog korištenja, administrator sustava treba analizirati izvještaj provjere te utvrditi ozbiljnost uočenih promjena.

Ukoliko promjene ukazuju na maliciozne aktivnosti neovlaštenih korisnika, potrebno je poduzeti odgovarajuće sigurnosne mjere definirane sigurnosnom politikom organizacije. Ukoliko su uočene promjene posljedica legitimnih aktivnosti korisnika, iste se mogu tretirati kao lažna upozorenja (engl. *false positive*) te se mogu zanemariti.

Učestalo pojavljivanje lažnih upozorenja pokazatelj su neprikladne konfiguracije korištenog alata za provjeru integriteta, što u većini slučajeva zahtjeva preinake. Preinake na konfiguraciji tipično uključuju modificiranje objekata (direktorija i datoteka) koji su uključeni u analizu, čime se u određenoj mjeri umanjuje udio lažnih upozorenja.

Lažna upozorenja osim što su vrlo zamorna za analizu, također umanjuju i vjerojatnost uočavanja detalja koji mogu biti pokazatelj ozbiljnih malicioznih aktivnosti. Iz tog razloga posebno je bitno u što većoj mjeri smanjiti njihov udio u dobivenim izvještajima. Reduciranje lažnih upozorenja iterativni je postupak kojim se dolazi do optimalne konfiguracije na sustavu. Nakon što su napravljene promjene na konfiguraciji programa, potrebno je napraviti novi "otisak" sustava koji će uključiti obavljene promjene.

3. Programski alati (Linux)

U ovome dokumentu opisano je nekoliko programskih alata za provjeru integriteta datotečnog sustava za Linux i MS Windows operacijske sustave.

Za Linux operacijske sustave opisani su programski paketi,

- Tripwire,
- AIDE.

3.1. Tripwire

Tripwire programski paket jedan je od najpoznatijih alata za provjeru integriteta datotečnog sustava za Linux operacijske sustave.

Treba napomenuti da danas postoje dvije međusobno odvojene grane Tripwire projekta koje su rezultirale dvjema različitim licencama ovog programa. Besplatna inačica programa razvijena je u okviru SourceForge Tripwire projekta te je dostupna pod GPL (**G**eneral **P**ublic **L**icense) licencom na URL adresi www.tripwire.org.

Druga, komercijalna grana istog projekta, rezultirala je Tripwire programom koji se plaća i koji je dostupan na URL adresi http://www.tripwire.com.

Postoji nekoliko osnovnih razlika između spomenutih inačica Tripwire programa, koje su dane u sljedećoj tablici (*Tablica 1*).

Svojstvo	Open Source Tripwire	Komercijalni Tripwire
cijena	besplatan	plaća se
verzija	2.3.1-2	3.0
podržani operacijski sustavi	Linux	Linux BSD Solaris Windows NT Windows 2000 Windows XP

Tablica 1 - Razlike između komercijalne i Open source inačice Tripwire programa

U nastavku su opisani osnovni postupci instalacije i korištenja besplatne inačice Tripwire programskog paketa.

3.1.1. Instalacija

U svrhu pisanja dokumenta instalirana je *open source* inačica Tripwire programskog paketa iz bin.tar.gz arhive (tripwire-2.3-47.bin.tar.gz). Postupak instalacije programa vrlo je jednostavan. Nakon raspakiravanje arhive naredbom:

```
# tar -xzvf tripwire-2.3-47.bin.tar.gz
```

potrebno je ući u novonastali tripwire-2.3 direktorij te pokrenuti install.sh skriptu za instalaciju programa.

```
# ./install.sh
```

Budući da install.sh skripta postupak instalacije provodi na temelju konfiguracije definirane install.cfg i policy/twpol.txt datotekama, prije pokretanja iste preporučuje se njihovo prilagođavanje osobnim potrebama.

Install.cfg skripta uglavnom definira lokacije datoteka Tripwire programskog paketa, dok twpol.txt datoteka unutar policy direktorija definira koji će se sve objekti i na koji način kontrolirati Tripwire programom.

Nakon pokretanja skripte uslijediti će postupak instalacije programa na temelju definirane konfiguracije, tijekom kojeg će od korisnika biti traženo da unese dva *passphrase* niza koja će se koristiti u postupku enkripcije datoteka.

Kao mehanizam zaštite povjerljivih konfiguracijskih datoteka programa Tripwire koristi El Gamal asimetričnu kriptografiju s 1024-bitnom enkripcijom. Na ovaj način željela se onemogućiti neovlaštena modifikacija datoteka programa, kojom bi se mogla ugroziti njegova vjerodostojnost.

3.1.2. Konfiguracija

U ovom poglavlju opisani su osnovni postupci konfiguracije koje je potrebno obaviti kako bi se Tripwire program pripremio za rad. Postupci opisani u ovom poglavlju tipično se provode samo jednom prije nego što se baza prvi puta inicijalizira. Nakon što je baza jednom inicijalizirana sve ostale radnje provode se na način opisan u sljedećem poglavlju.

Konfiguracija sustava uključuje sljedeće postupke:

- uređivanje konfiguracijske datoteke
- obavještavanje e-mail porukama

- uređivanje politike provjere integriteta
- inicijalizacija baze programa

Uređivanje konfiguracijske datoteke

Konfiguracijska datoteka (`/etc/tripwire/tw.cfg`) definira osnovno ponašanje `Tripwire` programskog paketa. Ovom datotekom ne definiraju se objekti koji se žele štititi `Tripwire` programom, već samo općenite postavke programa, kao što su lokacije datoteka, način generiranja izvještaja i sl.

Inicijalna verzija `tw.cfg` datoteke stvorena je za vrijeme instalacije programa, na temelju parametara navedenih u `install.cfg` datoteci. Ukoliko je ova datoteka prikladno uređena prije postupka instalacije kasnije neće biti potrebe za preuređivanjem iste.

Iz sigurnosnih razloga `tw.cfg` datoteka je na tvrdom disku pohranjena u kriptiranom obliku i nije je moguće izravno uređivati tekstualnim editorom. Sve promjene obavljaju se nad tekstualnom verzijom iste datoteke (`/etc/tripwire/twcfg.txt`) na temelju koje se unesene promjene mogu preslikati na originalnu konfiguracijsku datoteku (naravno, uz poznavanje odgovarajućeg *pasphrase* niza).

Preinake na konfiguracijskoj datoteci opravdane su u situacijama kada se želi promijeniti:

- način na koji Tripwire obavlja provjeru integriteta zadanih objekata
- način slanja izvještaja e-mail sustavom
- lokacija datoteka Tripwire datoteka

U nastavku je dan primjer inicijalne tekstualne konfiguracijske datoteke `Tripwire` programa:

```
ROOT            =/usr/sbin
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/teuta-local.key
EDITOR          =/usr/bin/vi
LATEPROMPTING =false
LOOSEDIRECTORYCHECKING =false
MAILNOVIOLATIONS =true
EMAILREPORTLEVEL =3
REPORTLEVEL     =3
MAILMETHOD      =SENDMAIL
SYSLOGREPORTING =false
MAILPROGRAM     =/usr/lib/sendmail -oi -t
```

Iz sigurnosnih razloga preporučuje se ili brisanje ili pohranjivanje na sigurno mjesto svih tekstualnih kopija konfiguracijskih datoteka `Tripwire` programa.

Ukoliko je tekstualna kopija konfiguracijske datoteke trajno izgubljena istu je moguće dobiti zadavanjem sljedeće naredbe.

```
# twadmin –print-cfgfile > twcfg.txt
```

Nakon promjena na tekstualnoj kopiji potrebno je unesene promjene preslikati na enkripcijom zaštićenu verziju konfiguracijske datoteke. To je moguće postići sljedećom naredbom.

```
# twadmin --create-cfgfile --site-keyfile /etc/tripwire/site.key
twcfg.txt
```

Obavještavanje e-mail porukama

`Tripwire` programski paket implementira mogućnost slanja izvještaja obavljene provjere integriteta putem e-mail poruka. Ovakav mehanizam vrlo je praktičan za administratore, budući da omogućava jednostavno praćenje promjena na sustavu te pravovremeno poduzimanje odgovarajućih mjera.

Obavještavanje putem e-mail poruka omogućeno je u inicijalnoj instalaciji programa, a eventualne promjene u konfiguraciji moguće je obaviti na način kako je to opisano u prethodnom poglavlju.

Osnovni parametri konfiguracijske datoteke kojima se definira mogućnost e-mail obavješćivanja su `MAILPROGRAM` i `MAILMETHOD` parametri, iako postoje i drugi. Testiranje mogućnosti obavještavanja putem e-mail poruka moguće je provesti zadavanjem sljedeće naredbe:

```
# tripwire --test --email korisničko ime@ime domene
```

Ukoliko je sve ispravno podešeno, na navedenu e-mail adresu trebala bi stići test poruka `Tripwire` programa.

Uređivanje politike provjere integriteta datotečnog sustava

Definiranje objekata (direktorija i datoteka) koji će biti uključeni u provjeru integriteta obavlja se pomoću politike `Tripwire` programskog paketa (datoteka `/etc/twpol.txt`). Uređivanje ove datoteke najvažniji je korak podešavanja budući da se njome definira koji će objekti i na koji način biti uključeni u provjeru.

Kao i u slučaju konfiguracijske datoteke `tw.cfg`, niti ovu datoteku nije moguće izravno uređivati. Sve promjene provode se na tekstualnoj kopiji datoteke (`twpol.txt`), nakon čega se iste posebnom naredbom preslikavaju na originalnu datoteku, zaštićenu odgovarajućim *passphrase* nizom. U Prilogu na kraju dokumenta (Prilog A) dan je primjer tekstualne kopije `Tripwire` politike.

Za razliku od konfiguracijske datoteke `Tripwire` programa, ovu datoteku je potrebno mnogo češće uređivati kako bi se ista prilagodila pojedinom sustavu te na taj način smanjila lažna upozorenja.

S `Tripwire` programskim paketom dolazi inicijalna `twpol.txt` datoteka prilagođena Red Hat 7.0 operacijskom sustavu, koju će u većini slučajeva biti potrebno prilagoditi specifičnim potrebama pojedinih operacijskih sustava.

Nakon što su obavljene odgovarajuće promjene, potrebno je na temelju nje generirati enkripcijom zaštićenu verziju iste datoteke. To je moguće postići naredbom:

```
# twadmin --create-polfile twpol.txt
```

Iz sigurnosnih razloga i u ovom slučaju preporučuje se uklanjanje tekstualne kopije definirane politike ili njeno pohranjivanje na sigurno mjesto.

Inicijalizacija baze programa

Nakon što je definirana politika prema kojoj će se napraviti "otisak" datotečnog sustava i prema kojoj će se dalje obavljati provjere, potrebno je inicijalizirati `Tripwire` bazu.

Ovim postupkom analizira se politika definirana `tw.pol` datotekom, prikupljaju se potrebni podaci sa sustava te se na temelju toga kreira jedinstveni "otisak" sustava, tzv. `Tripwire` baza. Kreirana baza također je zaštićena enkripcijom kako bi se na taj način zaštitila od neautoriziranih promjena.

Treba napomenuti kako se baza inicijalizira samo jednom prilikom inicijalne konfiguracije `Tripwire` programskog paketa, opisane u ovom poglavlju. Sve naknadne promjene na istoj provode se na drugačiji način, o čemu će biti više riječi u nastavku dokumenta (3.1.3).

Inicijalizacija `Tripwire` baze, odnosno kreiranje "otiska" provodi se naredbom:

```
# tripwire –init
```

Nakon ovog koraka baza će biti pohranjena na lokaciju definiranoj `DBFILE` varijablom unutar konfiguracijske datoteke programa. Inicijalna vrijednost varijable `DBFILE` je `/var/lib/$(HOSTNAME).twd`.

3.1.3. Korištenje programa

Nakon što je program ispravno konfiguriran spreman je za korištenje. Ovdje su uključeni sljedeći postupci:

- provođenje provjere integriteta
- analiza izvještaja
- osvježavanje baze
- promjene definirane politike
- promjena passphrase nizova

Provođenje provjere integriteta

Nakon što je `Tripwire` baza inicijalizirana, moguće je u bilo kojem trenutku obaviti provjeru integriteta datotečnog sustava. Pokretanjem provjere uspoređuje se trenutno stanje datotečnog sustava s ranije uzetim "otiskom" istog sustava u poznatom sigurnom stanju. Sve promjene u odnosu na ranije zabilježeno stanje biti će prijavljene kao potencijalna mogućnost kompromitiranja sustava.

Provjera integriteta sustava pokreće se zadavanjem sljedeće naredbe:

```
# tripwire --check
```

Nakon obavljene provjere rezultat će biti ispisan na standardni izlaz (*stdout*), a kopija izvještaja biti će pohranjena u datoteci definiranoj `REPORTFILE` varijablom unutar konfiguracijske datoteke poslužitelja. U prilogu na kraju dokumenta (Prilog B) dan je primjer izvještaja `Tripwire` programa.

Prosljeđivanjem parametra `–twrfile` gore navedenoj naredbi moguće je definirati alternativnu lokaciju u kojoj će biti pohranjen izvještaj provjere:

```
# tripwire --check --twrfile /var/lib/report/izvjestaj.twr
```

Za slanje istog izvještaja na politikom definiranu e-mail adresu potrebno je zadati sljedeću naredbu:

```
# tripwire --check --email-report
```

Nakon obavljene provjere na adresu administratora sustava stići će kopija izvještaja, čiji je format definiran `REPORTLEVEL` varijablom unutar konfiguracijske datoteke. `REPORTLEVEL` varijablom definira se opsežnost izvještaja koji će biti generiran, a može poprimiti vrijednost od nula do četiri (četiri je najopsežniji format izvještaja). Inicijalna vrijednost ove varijable je tri. Zadavanjem naredbe:

```
# tripwire --check --email-report --email-report-level 2
```

može se eksplicitno definirati opsežnost izvještaja `--email-report-level 2` parametrom.

Naredba `tripwire` prima još nekoliko parametara kojima se može preciznije definirati postupak provođenja provjere. Moguće je točno navesti koji se objekti žele provjeriti, a koji ignorirati, moguće je definirati grupu pravila koja se žele provjeriti s obzirom na sigurnosni rizik koji predstavljaju (parametar `severity`) i slično.

Analiza izvještaja

Nakon svake obavljene provjere `Tripwire` će ispisati izvještaj na standardni izlaz, pohraniti će kopiju izvještaja u datoteku definiranu `REPORTFILE` varijablom te poslati istu kopiju na proizvoljan broj e-mail adresa definiranih politikom programa.

Datoteka definirana `REPORTFILE` varijablom pohranjena je u binarnom obliku i nije ju moguće izravno pregledavati. Ukoliko se na temelju iste želi generirati tekstualna datoteka za jednostavniju analizu potrebno je zadati naredbu:

```
# twprint --print-report --twrfile /var/lib/report/report.twr > izvjestaj.txt
```

Na temelju generiranog izvještaja administrator provodi analizu rezultata i odlučuje da li je koja od uočenih promjena posljedica malicioznih aktivnosti neovlaštenih korisnika. Ukoliko su uočene maliciozne aktivnosti, potrebno je poduzeti odgovarajuće mjere definirane sigurnosnom politikom organizacije.

Ukoliko izvještaj sadrži veći broj lažnih upozorenja treba razmotriti mogućnost redefiniranja definirane politike te osvježavanje baze.

Osvježavanje Tripwire baze

Nakon obavljene provjere integriteta u većini slučajeva potrebno je ponovno osvježiti `Tripwire` bazu, kako bi se zabilježilo novo trenutno stanje sustava.

Bez obzira da li su uočene promjene posljedica legitimnog korištenja sustava ili malicioznih aktivnosti neovlaštenih korisnika, potrebno je iznova osvježiti bazu programa. Bazu je moguće osvježiti naredbom:

```
tripwire --update --twrfile /var/lib/report/report.twr
```

Zadavanjem parametra `--interactive` moguće je pokrenuti osvježavanje baze odmah nakon obavljene provjere. U tom slučaju naredba za pokretanje provjere izgleda ovako:

```
# tripwire --check –interactive
```

Pokretanjem bilo koje od gore navedenih naredbi rezultirati će otvaranjem tekstualnog editora definiranog varijablom `EDITOR`, u kojem će biti redom navedene sve promjene uočene tijekom provjere datotečnog sustava.

Kraj svakog prekršenog pravila ostavljeno je mjesto između dvije uglate zagrade, gdje je moguće označiti kako će se uočena promjena tretirati prilikom postupka osvježavanja baze.

```
Modified:
[x] "/usr/local/tw"
drwxr -xr -x root(0) 512 Tue Nov 22 17:19:15 1999
```

Ukoliko je promjena označena znakom `x`, nakon pokretanja postupka osvježavanja baze ova će promjena biti uzeta u obzir u novom "otisku" sustava. Ukoliko se znak `x` ukloni, novonastala promjena neće biti uzeta u obzir prilikom osvježavanja baze.

Promjene Tripwire politike

Potrebe za modifikacijom definirane politike mogu nastati zbog:

- potrebe za dodavanjem novih objekata u sustav provjere

- velike količine lažnih upozorenja
- promjena atributa postojećih pravila (način grupiranja pravila, obavještavanje putem e-mail poruka, nivo sigurnosnog rizika i sl.)

Nakon što je `Tripwire` baza jednom inicijalizirana (postupak opisan u poglavlju 3.1.2) sve promjene na politici obavljaju se putem `tripwire` *Policy Update* moda, a ne `twadmin` naredbom kao što je to bilo prilikom prvog definiranja politike.
Svaka promjena na politicizahtjeva ponovnu re-inicijalizaciju baze programa kako bi se uzele u obzir navedene promjene te napravio novi "otisak" koji odgovara novo definiranoj politici.
Promjene na politici uključuju sljedeće korake:

- kreiranje tekstualne kopije politike
  `# twadmin --print-polfile > nova_politika.txt`
- uređivanje politike
- osvježavanje postojeće politike novo definiranim pravilima
  `# tripwire --update-policy nova_politika.txt`

Ovi koraci će generirati i potpisati novu politiku sustava definiranu `POLFILE` datotekom te osvježiti bazu s unesenim promjenama.

Promjena passphrase nizova

Generiranje parova ključeva koji se koriste za enkripciju datoteka provodi se u trenutku instalacije `Tripwire` programskog paketa. Postoje dva glavna ključa koja se generiraju tijekom instalacije programa. To su: *site key* i *local key* parovi tajni/javni ključ koji su pohranjeni u datotekama definiranim u konfiguracijskoj datoteci programa (`site.key` i `$HOSTNAME-local.key`, gdje varijabla `$HOSTNAME` predstavlja ime računala za koji je ključ generiran).
Site key par ključeva koristi se za enkripciju konfiguracijske (`tw.cfg`) datoteke i datoteke kojom je definirana politika `Tripwire` programa (`tw.pol`). Budući da se ista konfiguracija i politika `Tripwire` programa može koristiti na više poslužitelja slične arhitekture, ovaj ključ ima širi značaj od *local key* ključa..
Local key ključ koristi se za lokalnu enkripciju baze i izvještaja `Tripwire` programa te stoga svaki od njih ima značaj samo na računalu na kojem je baza kreirana.
Ovakva struktura administratoru omogućuje definiciju odgovarajuće politike i konfiguracije za više računala, koje su potpisane *site key* ključem i odgovarajućim *passphrase* nizom koji je samo njemu poznat.
Održavanje baze i provođenje provjere integriteta na pojedinim strojevima moguće je delegirati njihovim administratorima putem generiranja novih *local key* ključeva i odgovarajućih *passphrase* nizova koji imaju lokalni značaj na pojedinim računalima.
Passphrase nizovi služe za zaštitu tajnih ključeva i definirani su prilikom instalacije sustava. Posebno je naglasiti važnost *passphrase* nizova, budući da bez njih nije moguće korištenje tajnih ključeva, a samim time i cijelog programa. Nepovratni gubitak ovih ključeva onemogućiti će korištenje programa, budući da ne postoji mehanizam njihove rekonstrukcije.
S obzirom na vezu između postojećih *passphrase* nizova i generiranih ključeva, jedini način da se isti promjene je generiranje novih parova ključeva. Nove ključeve moguće je generirati naredbama:

```
# twadmin --generate-keys --local-keyfile /etc/tripwire/site.key
# twadmin --generate-keys --site-keyfile /etc/tripwire/$HOSTNAME-local.key
```

Za svaku kriptiranu datoteku `Tripwire` programa moguće je sljedećom naredbom utvrditi kojim je ključem ista kriptirana:

```
# twadmin --examine ime_datoteke
```

Dekripciju kriptiranih datoteka moguće je obaviti naredbom:

```
# twadmin --remove-encryption ime_datoteke
```

a ponovnu enkripciju tekstualnih datoteka moguće je obaviti zadavanjem naredbi:

```
# twadmin --encrypt --local-keyfile /etc/tripwire/sitekey.key ime_datoteke
twadmin --encrypt --site-keyfile /etc/tripwire/sitekey.key file1 ime_datoteke
```

3.2. AIDE

AIDE (**A**dvanced **I**ntrusion **D**etection **E**nviroment) je besplatna alternativa komercijalnom Tripwire programskom paketu. AIDE programski paket razvijen je s primarnim ciljem da zamjeni komercijalnu inačicu Tripwire programa te da je eventualno nadopuni novim mogućnostima.
AIDE programski paket razvijen je pod GPL licencom i dostupan je za sljedeće operacijske sustave:

- Linux 2.0, 2.2, 2.4
- Solaris 2.5.1,2.6,7,8,9
- FreeBSD 2.2.8,3.4
- Unixware 7.0.1
- BSDi 4.1
- OpenBSD 2.6,3.0
- AIX 4.2
- TRU64 4.0x
- Cygwin

Princip rada programa gotovo je identičan testiranom Tripwire programskom paketu. Na temelju konfiguracijske datoteke (aide.conf) kreira se "otisak" sustava u poznatome sigurnom stanju, na temelju kojeg se kasnije usporedbom s trenutnim stanjem sustava obavlja provjera integriteta.
U nastavku će biti opisani osnovni postupci instalacije i korištenja AIDE programskog paketa.

3.2.1. Instalacija

U svrhu testiranja AIDE programa instalirana je zadnja objavljena inačica programa iz tar.gz arhive (aide-0.9.tar.gz). Postupak instalacije programa klasičan je za programe koji dolaze u tar.gz arhivi. Nakon raspakiravanja arhive naredbom

```
# tar -xzvf aide-0.9.tar.gz
```

potrebno je ući u novonastali aide-0.9 direktorij te pokrenuti sljedeće naredbe:

```
#./configure
# make
# make install
```

3.2.2. Konfiguracija

Korištenje AIDE programa vrlo je slično Tripwire programskom paketu, čime se može zaključiti kako je AIDE program razvijen po uzoru na Tripwire.
Prvi korak korištenja programa je uređivanje aide.conf (/usr/local/etc/aide.conf) konfiguracijske datoteke na temelju koje se inicijalizira AIDE baza, odnosno kreira "otisak" sustava. Aide.conf datoteka formatom je vrlo slična tw.cfg konfiguracijskoj datoteci, čime se olakšava transformacija jednog formata u drugi. Ovakav format olakšava korištenje programa onoj grupi korisnika koja se navikla na Tripwire sintaksu. U Prilogu (Prilog C) dan je primjer konfiguracijske datoteke AIDE programa.
Uređivanjem konfiguracijske datoteke programa definira se koji će objekti biti uključeni u analizu i koji će se atributi definiranih objekata promatrati. Za konfiguraciju AIDE programa vrijede slična pravila kao i za Tripwire programski paket. Potrebno je pažljivo odabrati objekte datotečnog sustava koji se žele nadzirati, kako bi se u što većoj mjeri smanjila lažna upozorenja.
Općenito se ne preporučuje uključivanje objekata koji se često mijenjaju kao što su /tmp, /spool, /proc i sl., budući da isti mogu ozbiljno utjecati na veličinu i kompleksnost izvještaja.
Veliki izvještaji osim što su kompleksni su za analizu, dodatno otežavaju uočavanje promjena koje mogu biti posljedica aktivnosti malicioznih korisnika. Log datoteke dosta su diskutabilne, budući da su podložne učestalim promjenama, a ujedno su dosta važne za praćenje i analizu. Neovlaštene promjene log datoteka mogu biti jasan pokazatelj neovlaštenih aktivnosti, budući da se njihovom modifikacijom često uklanjaju tragovi malicioznog djelovanja.
Teško je dati precizne i općenite upute koje bi jedinstveno odredile način definiranja politike provjere integriteta. Svakom poslužitelju, ovisno o namjeni i tipu, potrebno je prilagoditi politiku kojom će se najbolje moći nadzirati promjene na sustavu. Valja još jednom naglasiti kako je ispravno uređivanje politike svih programa ovog tipa najvažniji korak za njegovu funkcionalnost.

Ovdje se neće ulaziti u detalje konfiguracije programa, budući da je program vrlo sličan ranije opisanom Tripwire programskom paketu (3.1).

3.2.3. Korištenje programa

Prvi korak korištenja AIDE programa je inicijalizacija baze na temelju koje će se kasnije provoditi provjere integriteta datotečnog sustava. Inicijalizacija baze obavlja se naredbom:

```
# aide –init
```

identično kao i kod Tripwire programskog paketa. Pokretanjem ove naredbe kreira se baza na temelju definirane konfiguracijske datoteke. Posebno važan korak korištenja AIDE programa je zaštita konfiguracijske datoteke te ostalih datoteka programa od neautoriziranog pristupa. Uvidom u konfiguracijsku datoteku, neovlašteni korisnik može uočiti način rada programa te zaobići sigurnosne mjere programa. AIDE za razliku od Tripwire programa ne koristi enkripciju ključnih datoteka, čime važnost zaštite istih dobiva još veću vrijednost. Iz sigurnosnih razloga preporučuje se pohranjivanje važnih datoteka na medije poput disketa, CD-a i sl. ili na neko drugo zaštićeno računalo.

Nakon što je kreirana baza sustava moguće je u bilo kojem trenutku obaviti provjeru integriteta, zadavanjem naredbe:

```
# aide –check
```

Njenim pokretanjem uspoređuje se AIDE baza s trenutnim stanjem sustava, kako bi se uočile eventualne promjene koje ukazuju na maliciozno djelovanje.

Ukoliko se iz određenih razloga javi potreba za promjenom konfiguracijske datoteke, odnosno politike AIDE programa, potrebno je ponovo osvježiti bazu kako bi se na taj način uzele u obzir novonastale promjene. Baza programa osvježava se naredbom:

```
# aide --update
```

Pokretanjem ove naredbe provodi se u jednom koraku provjera integriteta sustava (aide --check) zajedno s osvježavanjem baze. Periodičkim pokretanjem ove naredbe, ovisno o odluci administratora sustava, moguće je vrlo precizno urediti konfiguracijsku datoteku koja će davati kvalitetne rezultate.

4. Programski alati (MS Windows)

Za MS Windows operacijske sustave opisani su sljedeći programi:

- Tripwire
- GFI Languard File Integrity Checker
- Data Sentinel

4.1. Tripwire (Windows)

Komercijalna grana Tripwire projekta rezultirala je različitim inačicama Tripwire programa, između kojih je i ona namijenjena Windows operacijskim sustavima. Način rada programa vrlo je sličan onome za Linux operacijske sustave. Program se sastoji od dvije osnovne komponente:

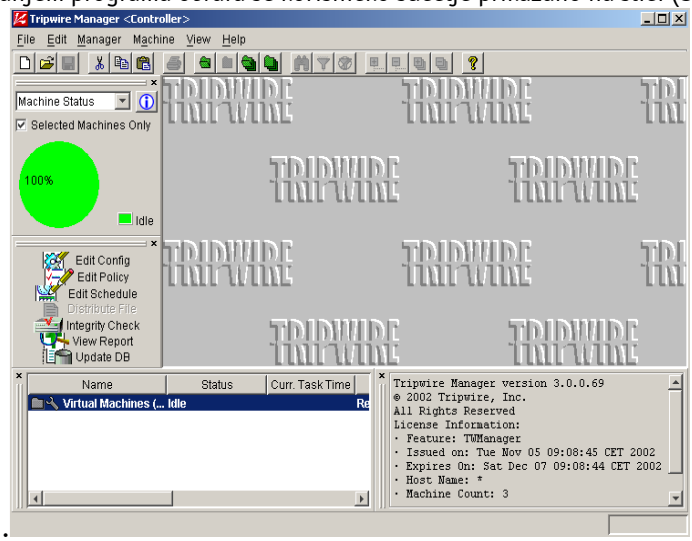
- Tripwire for Servers – komponenta zadužena za obavljanje svih zadaća vezanih za provjeru integriteta. Program se instalira na sva računala na kojima se želi obavljati provjera integriteta.
- Tripwire Manager – Aplikacija pisana u Javi koja omogućuje centralizirano upravljanje Tripwire agentima na ostalim računalima.

4.1.1. Instalacija programa

Evaluacijska verzija Tripwire programskog paketa može se dobaviti s URL adrese http://www.tripwire.com/downloads/. Postupak Instalacija provodi se pokretanjem TW-evalkit.exe programa. U svrhu testiranja instalirane su obje komponente programa kako bi se uvidjele raspoložive mogućnosti.

4.1.2. Konfiguracija programa

Pokretanjem programa otvara se korisničko sučelje prikazano na slici (*Slika 1*)

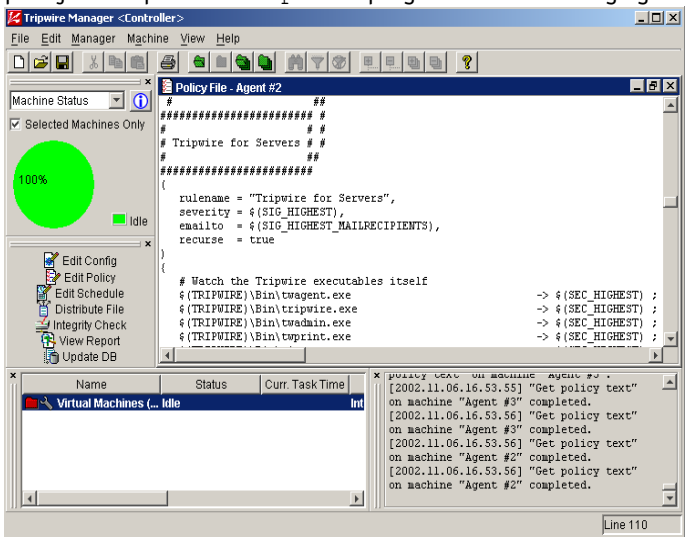


Slika 1 - Korisničko sučelje Tripwire Manager aplikacije

Unutar prikazanog sučelja moguće je centralizirano provođenje svih zadaća vezanih za provjeru integriteta na svim `Tripwire` agentima. Pritiskom na karticu *Manager -> Add Machines* unutar trake s padajućim izbornicima potrebno je navesti sve `Tripwire` agente koji se žele administrirati.

Nakon što su definirani svi `Tripwire` agenti, za svaki od njih moguće je odvojeno definirati politiku provjere integriteta i konfiguraciju programa. Moguće je odvojeno provođenje provjere integriteta, zatim pregledavanje izvještaja i sl.

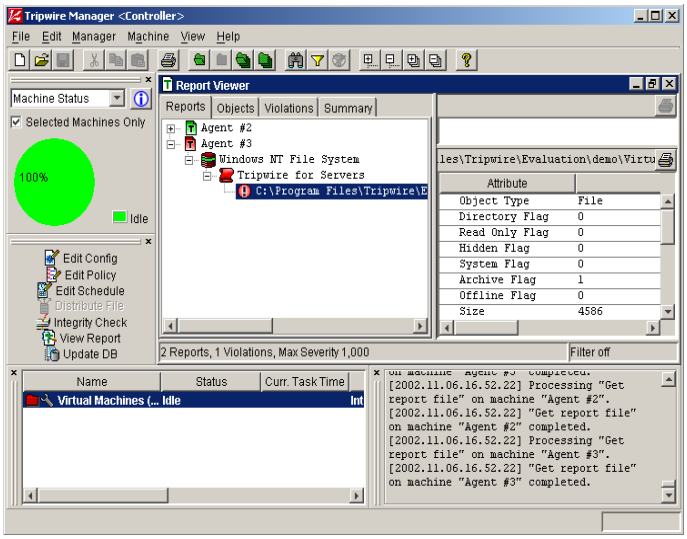
Pritiskom na karticu *Edit Policy* s lijeve strane sučelja otvara se prozor unutar kojega je moguće unošenje direktnih promjena na politiku `Tripwire` programa za odabranog agenta (*Slika 2*).



Slika 2 - Sučelje za uređivanje politike Tripwire programskog paketa

Pritiskom na karticu *Edit Config*, moguće je na sličan način uređivati i konfiguracijsku datoteku odabranog `Tripwire` agenta.

Provjera integriteta datotečnog sustava provodi se jednostavno pritiskom na karticu *Integrity Check*, a izvještaj provjere moguće je vidjeti pritiskom na karticu *View Report* (*Slika 3*) .



Slika 3 - Izvještaj obavljene provjere integriteta

Jednostavnim selektiranjem odgovarajućeg `Tripwire` agenta u donjem dijelu prozora moguće je odabrati na kojem će se računalu provoditi odgovarajuća akcija. Na ovaj način administratoru se omogućuje jednostavna i istovremena administracija više računala s instaliranim `Tripwire` programskim paketom, što je posebno praktična mogućnost, pogotovo u okolinama s većim brojem poslužitelja.

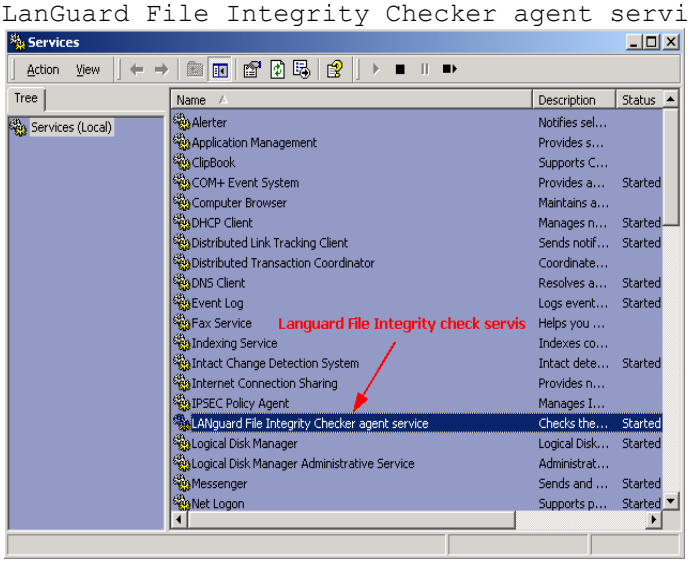
4.2. GFI Languard File Integrity Checker

`GFI Languard File Integrity Checker` je vrlo jednostavan, besplatan i praktičan alat za provjeru integriteta datotečnog sustava pod Windows operacijskim sustavima (trenutno podržane platforme su Windows NT i Windows 2000).

4.2.1. Instalacija programa

Instalaciju `GFI Languard File Integrity Checker` programa moguće je dobaviti s URL adrese http://www.gfi.com/downloads/. Postupak instalacije vrlo je jednostavan i tipičan je za Windows operacijske sustave. Dovoljno je pokrenuti `lanfilecheck.exe` program koji će nakon nekoliko standardnih pitanja obaviti instalaciju programa.

Ukoliko je postupak instalacije prošao bez greške program će se automatski pokrenuti kao Windows servis pod imenom `LanGuard File Integrity Checker agent service` (Slika 4).



Slika 4- File Integrity Check servis

Ukoliko se nakon uspješne instalacije program sam automatski ne pokrene kao servis, to je moguće obaviti ručno, zadavanjem sljedeće naredbe:

```
C:\Program Files\LANguard File Integrity Checker>CFService.exe –startservice
```

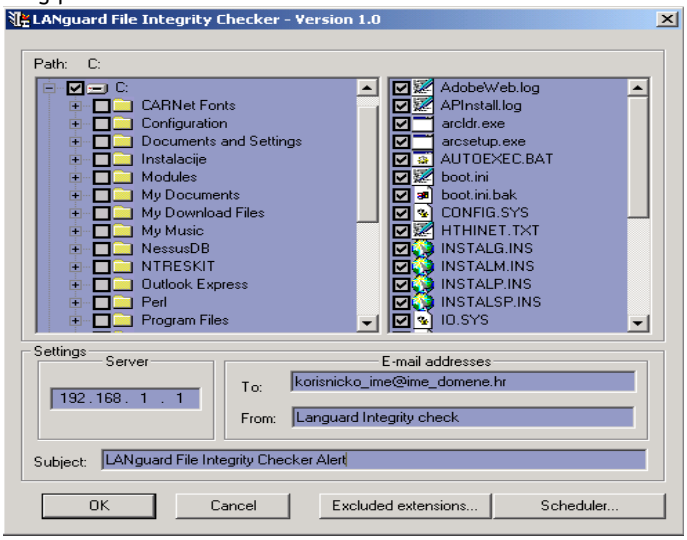
Nakon što je program uspješno instaliran i pokrenut moguće je pristupiti konfiguraciji istoga.

4.2.2. Konfiguracija programa

Korisničkom sučelju za konfiguraciju programa moguće je pristupiti ili putem windows start mape (*Start->Programs-> Languard File Integrity Checker -> configuration*) ili putem naredbenog retka:

```
C:\Program Files\LANguard File Integrity Checker>CFCommand.exe c
```

Na slici (*Slika 5*) prikazan je izgled sučelja za konfiguraciju `LanGuard File Integrity Checker` programskog paketa.

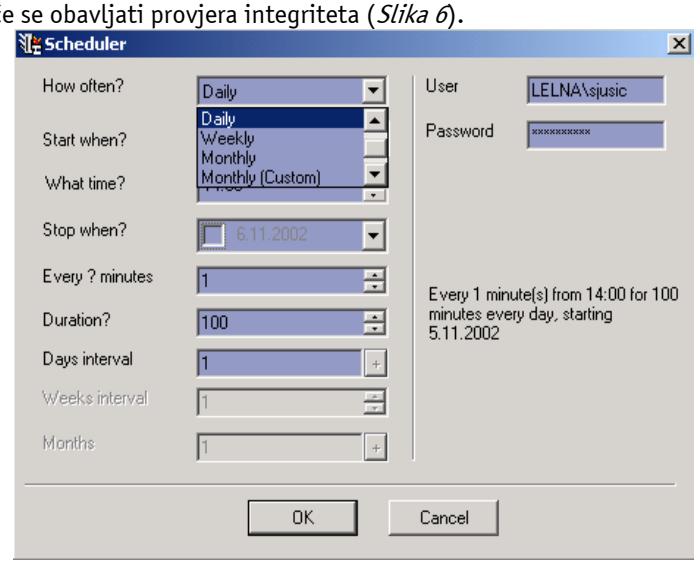


Slika 5- Sučelje za konfiguraciju Languard File Integrity Checker programa

Odabir objekata (direktoriji i datoteke) koji će biti uključeni u provjeru integriteta obavlja se jednostavnim selektiranjem odgovarajućeg *checkbox* polja. Unutar lijevog okvira konfiguracijskog sučelja moguće je u provjeru uključiti odgovarajuće direktorije sustava, dok se unutar desnog prozora istog sučelja odabiru pojedine datoteke.

Nakon što su definirani svi objekti uključeni u provjeru integriteta, potrebno je definirati ime poslužitelja te e-mail adresu na koju će se slati izvještaj obavljene provjere.

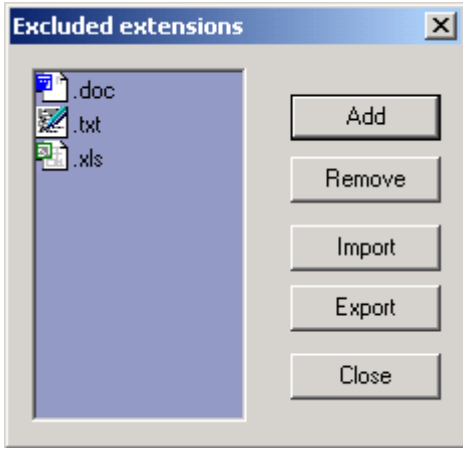
Pritiskom na karticu *Scheduler* otvara se konfiguracijsko sučelje unutar kojeg je moguće je definirati periode u kojima će se obavljati provjera integriteta (*Slika 6*).



Slika 6 - Definiranje perioda u kojima će se obavljati provjere

Provjere je moguće definirati na jednokratnoj, dnevnoj, tjednoj te mjesečnoj bazi.

Iz provjere je također moguće isključiti datoteke s određenim nastavcima, pritiskom na karticu *Exclude Extension*. Unutar sučelja prikazanog na slici (Slika 7), moguće je definirati niz tipova datoteka koje se žele isključiti iz povjere, čime se dodatno može smanjiti broj lažnih upozorenja.
Nakon svake obavljene provjere izvještaj će biti poslan na zadanu e-mail adresu. Primjer izvještaja `Languard File Integrity Checker` programskog paketa dan je u Prilogu (Prilog E) na kraju dokumenta (*Slika 7*).



Slika 7 - Tip datoteka isključenih iz provjere

4.3. Data Sentinel

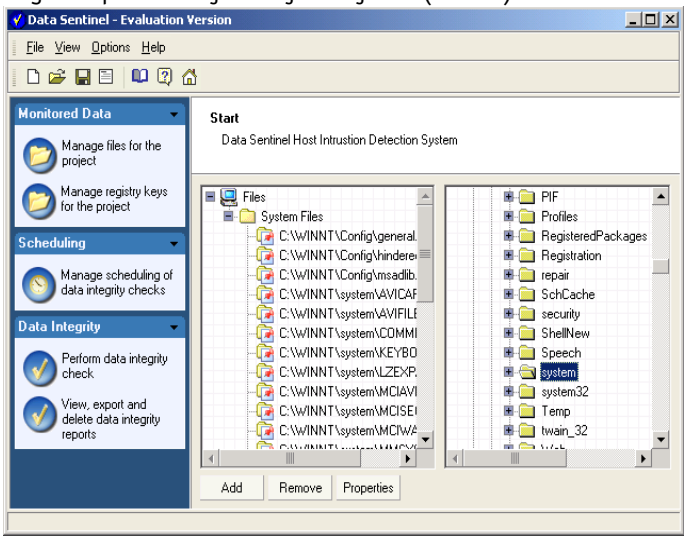
`Data Sentinel` još je jedan program koji omogućuje provjeru integriteta datotečnog sustava te Windows *registry*-a. Program je proizvod tvrtke Ionx i namijenjen je Windows operacijskim sustavima. Za razliku od dosad opisanih programa koji su bili besplatni (osim `Tripwire` programa za Windowse), ovaj program se plaća. Cijena mu je 399 £.

4.3.1. Instalacija programa

Evaluacijska verzija programa dostupna je na web stranicama tvrtke Ionx (http://www.ionx.co.uk/). Instalaciju programa moguće je obaviti pokretanjem `DataSentinelEvaluation.exe` instalacijskog programa. Nakon nekoliko standardnih Windows upita o instalaciji programa, uslijediti će sam postupak instalacije istog.

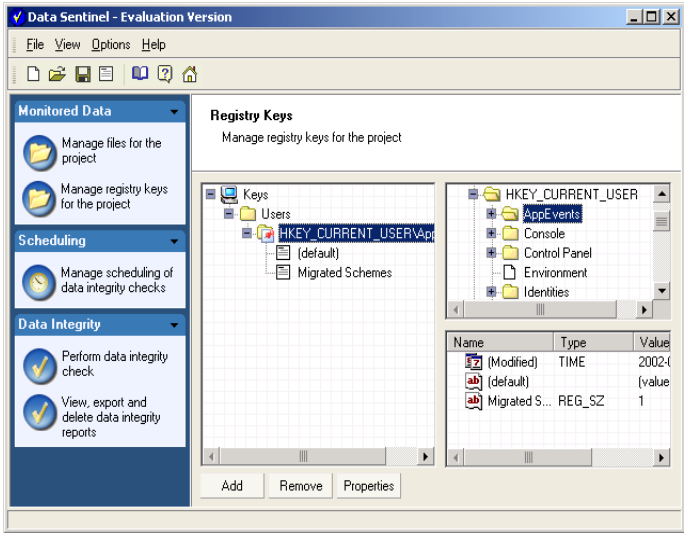
4.3.2. Konfiguracija programa

Korisničko sučelje programa prikazano je na sljedećoj slici (*Slika 8*).



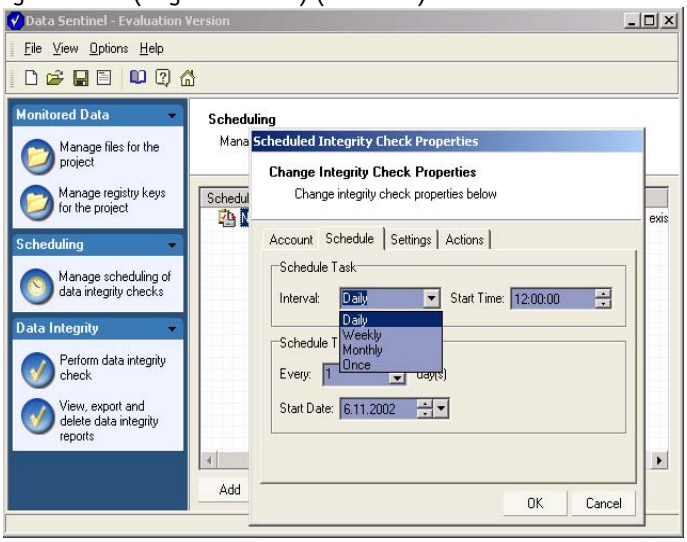
Slika 8 - Korisničko sučelje Data Sentiel programa

Definiranje objekata datotečnog sustava koji se žele pratiti obavlja se pritiskom na karticu *Manage files for the project*. Pritiskom na istu otvara se prozor podijeljen na dva dijela (*Slika 8*).
Unutar desnog okvira glavnog prozora prikazana je struktura datotečnog sustava računala na kojem je program instaliran, dok je s lijeve strane prikazan sadržaj objekata uključenih u provjeru integriteta.
`Data Sentinel` program odabrane objekte postavlja u grupe, kako bi se administratoru omogućila jednostavnija kontrola. Na ovaj način moguće je međusobno odvojiti različite kategorije datoteka i direktorija uključenih u provjeru. Npr. moguće je definirati grupu koja sadrži sistemske datoteke, zatim grupu koja sadrži log datoteke i sl.
Definiranje novih grupa, odnosno dodavanje novih objekata moguće je obaviti pritiskom na karticu *Add (*dodavanje objekata također je moguće obaviti standardnim *drag and drop* akcijama).
Za svaku grupu mogu se vidjeti definirana svojstva pritiskom na karticu *Properties*. Pritiskom na istu otvara se korisnički dijalog unutar kojeg je moguće definirati ime grupe te svojstva koja se žele pratiti za objekte iz te grupe.
Definiranje `registry` objekata obavlja se na sličan način Pritiskom na karticu *Manage registry keys for the project* otvara se korisničko sučelje prikazano na slici (*Slika 9*) unutar kojeg je moguće odabrati *1*objekte.



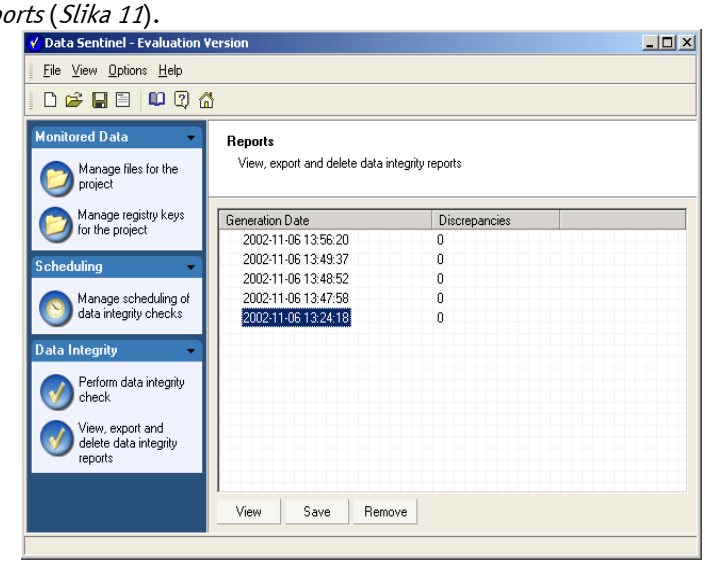
Slika 9 - Odabir registry objekata

Provjeru integriteta moguće je pokrenuti trenutno pritiskom na karticu *Perform Integrity checks* ili putem ugrađenog organizatora (eng. *scheduler*) (Slika 10).



Slika 10 - Data Sentiel scheduler

Putem organizatora moguće je definirati učestalost provjere integriteta na dnevnoj, tjednoj ili mjesečnoj bazi. Moguće je definiranje i drugih parametara kao što je e-mail adresa na koju će se slati izvještaj, zatim format izvještaja (HTML, XML, CSV) i sl.
Nakon obavljene provjere izvještaj iste može se dobiti pritiskom na karticu *View, export and delete data integrity reports* (*Slika 11*).



Slika 11 - Analiza izvještaja Data Sentinel programa

5. Zaključak

5.1. Linux

Provedenim testiranjima može se zaključiti kao su `AIDE` i `Tripwire` programski paketi vrlo slični prema svojim mogućnostima i karakteristikama. Mala prednost može se dati `Tripwire` programskom paketu, s obzirom na podršku za enkripciju važnih datoteka programa, nešto bogatiju dokumentaciju, te nešto kvalitetnije izvještaje obavljenih provjera.
Dodatna prednost `Tripwire` programa pred `AIDE` programom je mogućnost interaktivnog osvježavanja baze (`tripwire –interactive`). Na ovaj način moguće je u jednom koraku pokrenuti provjeru integriteta te na temelju nje odrediti koje se promjene žele prihvatiti, a koje ne. Na osnovi toga može se napraviti osvježavanje baze. `AIDE` ne podržava ovu mogućnost.
Izvještaji `Tripwire` programa vrlo su detaljni i opsežni. Omogućuju preglednu analizu svih rezultata, što također ide u prilog ovom programu. `AIDE`, osim toga, također generira kvalitetne, ali nešto oskudnije izvještaje. U slučaju da ne postoje promjene u odnosu na poznato stanje sustava, `AIDE` neće generirati nikakav izvještaj, što može zbuniti manje iskusne korisnike.
Najveća prednost `AIDE` programa pred `Tripwire`-om je brzina rada. Provedenim testovima pokazalo se da `AIDE` radi znatno brže u odnosu na `Tripwire` programski paket, što na sustavima s većim brojem korisnika može igrati važnu ulogu.
Usprkos svim ovim navedenim razlikama, oba programa pokazala su se kao vrlo dobra i svakako se preporučuje njihovo korištenje.

5.2. Windows

Svi alati za provjeru integriteta datotečnog sustava testirani na Windows platformama pokazali su zadovoljavajuće rezultate. Mala prednost može se dati `Tripwire` i `Data Sentinel` programskim paketima koji sadrže nešto više mogućnosti od opisanog `GFI Languard File Integrity Checker` programa, pri čemu treba napomenuti da je ovaj potonji besplatan. Za razliku od `GFI Languard` programa, `Data Sentinel` i `Tripwire` dodatno omogućuju provjeru integriteta Windows *registry*-a.

Data Sentinel programski paket odlikuje se izvrsnim dizajnom i mnoštvom opcija koje administartoru omogućuju kvalitetno provođenje provjere integriteta.
Kod Tripwire programa pažnju je privukla Tripwire Manager aplikacija koja omogućuje centraliziranu administraciju više računala sa instaliranim Tripwire programskim paketom. Ova mogućnost čini se posebno korisnom u okolinama sa velikim brojem računala koja se žele nadzirati. Tripwire agenti dostupni su i za Linux operacijske sustave što centraliziranu administraciju ne ograničava samo na Windows platforme.

6. Prilog A

Konfiguracijska datoteka Tripwire programskog paketa:

```
##########################################################################
#   Primjer konfiguracijske datoteke Tripwire programskog paketa   #
#                                                                        #
##########################################################################

@@section GLOBAL
TWDOCS="/usr/doc/tripwire";
TWBIN="/usr/sbin";
TWPOL="/etc/tripwire";
TWDB="/var/lib/tripwire";
TWSKEY="/etc/tripwire";
TWLKEY="/etc/tripwire";
TWREPORT="/var/lib/tripwire/report";
HOSTNAME=teuta;

@@section FS
SEC_CRIT      = $(IgnoreNone)-SHa ;  # Critical files that cannot change
SEC_SUID      = $(IgnoreNone)-SHa ;  # Binaries with the SUID or SGID flags
set
SEC_BIN       = $(ReadOnly) ;        # Binaries that should not change
SEC_CONFIG    = $(Dynamic) ;         # Config files that are changed
infrequently but accessed often
SEC_LOG       = $(Growing) ;         # Files that grow, but that should
never change ownership
SEC_INVARIANT = +tpug ;              # Directories that should never change
permission or ownership
SIG_LOW       = 33 ;                 # Non-critical files that are of
minimal security impact
SIG_MED       = 66 ;                 # Non-critical files that are of
significant security impact
SIG_HI        = 100 ;                # Critical files that are significant
points of vulnerability


# Tripwire Binaries
(
  rulename = "Tripwire Binaries",
  severity = $(SIG_HI)
)
{
  $(TWBIN)/siggen                     -> $(SEC_BIN) ;
  $(TWBIN)/tripwire                   -> $(SEC_BIN) ;
  $(TWBIN)/twadmin                    -> $(SEC_BIN) ;
  $(TWBIN)/twprint                    -> $(SEC_BIN) ;
}

# Tripwire Data Files - Configuration Files, Policy Files, Keys, Reports,
Databases
(
  rulename = "Tripwire Data Files",
```

```
  severity = $(SIG_HI)
)
{

$(TWDB)                                -> $(SEC_CONFIG) -i ;
  $(TWPOL)/tw.pol                        -> $(SEC_BIN) -i ;
  $(TWPOL)/tw.cfg                        -> $(SEC_BIN) -i ;
  $(TWLKEY)/$(HOSTNAME)-local.key        -> $(SEC_BIN) ;
  $(TWSKEY)/site.key                     -> $(SEC_BIN) ;

  #don't scan the individual reports
  $(TWREPORT)                            -> $(SEC_CONFIG) (recurse=0) ;
}

(
  rulename = "Invariant Directories",
  severity = $(SIG_MED)
)

{
  /                                      -> $(SEC_INVARIANT) (recurse = 0) ;
  /home                                  -> $(SEC_INVARIANT) (recurse = 0) ;
  /etc                                   -> $(SEC_INVARIANT) (recurse = 0) ;
}


################################################
#                                              #
# File System and Disk Administration Programs #
#                                              #
################################################

(
  rulename = "File System and Disk Administraton Programs",
  severity = $(SIG_HI)
)

{
  /sbin/tripwire_test                -> $(SEC_CRIT);
  /usr/sbin/accton                       -> $(SEC_CRIT) ;
  /sbin/badblocks                        -> $(SEC_CRIT) ;
  /sbin/e2fsck                           -> $(SEC_CRIT) ;
  /sbin/debugfs                          -> $(SEC_CRIT) ;
  /sbin/dumpe2fs                         -> $(SEC_CRIT) ;
  /sbin/e2label                          -> $(SEC_CRIT) ;
  /sbin/fdisk                            -> $(SEC_CRIT) ;
  /sbin/fsck                             -> $(SEC_CRIT) ;
  /sbin/fsck.ext2                        -> $(SEC_CRIT) ;
  /sbin/fsck.minix                       -> $(SEC_CRIT) ;
  /usr/sbin/mkboot                       -> $(SEC_CRIT) ;
  /sbin/mke2fs                           -> $(SEC_CRIT) ;
  /sbin/mkfs                             -> $(SEC_CRIT) ;
  /sbin/mkfs.ext2                        -> $(SEC_CRIT) ;
  /sbin/mkfs.minix                       -> $(SEC_CRIT) ;
  /sbin/mkswap                           -> $(SEC_CRIT) ;
  /sbin/quotacheck                       -> $(SEC_CRIT) ;
  /sbin/quotaon                          -> $(SEC_CRIT) ;
  /sbin/resize2fs                        -> $(SEC_CRIT) ;
  /sbin/sfdisk                           -> $(SEC_CRIT) ;
  /sbin/tune2fs                          -> $(SEC_CRIT) ;
  /sbin/update                           -> $(SEC_CRIT) ;
  /bin/mount                             -> $(SEC_CRIT) ;
  /bin/umount                            -> $(SEC_CRIT) ;
  /bin/touch                             -> $(SEC_CRIT) ;
  /bin/mkdir                             -> $(SEC_CRIT) ;
```

```
  /bin/mknod                              -> $(SEC_CRIT) ;
  /bin/mktemp                             -> $(SEC_CRIT) ;
  /bin/rm                                 -> $(SEC_CRIT) ;
  /bin/rmdir                              -> $(SEC_CRIT) ;
  /bin/chgrp                              -> $(SEC_CRIT) ;
  /bin/chmod                              -> $(SEC_CRIT) ;
  /bin/chown                              -> $(SEC_CRIT) ;
  /bin/cp                                 -> $(SEC_CRIT) ;
  /bin/cpio                               -> $(SEC_CRIT) ;
}

#################################
#                               #
# Kernel Administration Programs #
#                               #
#################################

(
  rulename = "Kernel Administration Programs",
  severity = $(SIG_HI)
)
{
  /sbin/depmod                            -> $(SEC_CRIT) ;
  /sbin/insmod                            -> $(SEC_CRIT) ;
  /sbin/klogd                             -> $(SEC_CRIT) ;
  /sbin/ldconfig                          -> $(SEC_CRIT) ;
  /sbin/modinfo                           -> $(SEC_CRIT) ;
  /sbin/sysctl                            -> $(SEC_CRIT) ;
}

######################
#                    #
# Networking Programs #
#                    #
######################

(
  rulename = "Networking Programs",
  severity = $(SIG_HI)
)
{
  /usr/sbin/arp                               -> $(SEC_CRIT) ;
  /sbin/getty                             -> $(SEC_CRIT) ;
  /sbin/ifconfig                          -> $(SEC_CRIT) ;
  /sbin/ifdown                            -> $(SEC_CRIT) ;
  /sbin/ifup                              -> $(SEC_CRIT) ;
  /sbin/ipchains                          -> $(SEC_CRIT) ;
  /sbin/ipfwadm                           -> $(SEC_CRIT) ;
  /sbin/ipmaddr                           -> $(SEC_CRIT) ;
  /sbin/iptunnel                          -> $(SEC_CRIT) ;
  /sbin/plipconfig                        -> $(SEC_CRIT) ;
  /sbin/portmap                           -> $(SEC_CRIT) ;
  /sbin/route                             -> $(SEC_CRIT) ;
  /bin/ping                               -> $(SEC_CRIT) ;
}

#################################
#                               #
# System Administration Programs #
#                               #
#################################

(
  rulename = "System Administration Programs",
  severity = $(SIG_HI)
```

```
)
{


  /sbin/halt                            -> $(SEC_CRIT) ;
  /sbin/init                            -> $(SEC_CRIT) ;
  /sbin/initlog                         -> $(SEC_CRIT) ;
  /sbin/killall5                        -> $(SEC_CRIT) ;
  /sbin/linuxconf                       -> $(SEC_CRIT) ;
  /sbin/linuxconf-auth                  -> $(SEC_CRIT) ;
  /sbin/pwdb_chkpwd                     -> $(SEC_CRIT) ;
  /sbin/remadmin                        -> $(SEC_CRIT) ;
  /sbin/rescuept                        -> $(SEC_CRIT) ;
  /sbin/rmt                             -> $(SEC_CRIT) ;
  /sbin/rpc.lockd                       -> $(SEC_CRIT) ;

  /sbin/shutdown                        -> $(SEC_CRIT) ;
  /sbin/sulogin                         -> $(SEC_CRIT) ;
  /sbin/swapon                          -> $(SEC_CRIT) ;
  /sbin/syslogd                         -> $(SEC_CRIT) ;
  /bin/pwd                              -> $(SEC_CRIT) ;
  /bin/uname                            -> $(SEC_CRIT) ;
}

########################################
#                                      #
# Hardware and Device Control Programs #
#                                      #
########################################

(
  rulename = "Hardware and Device Control Programs",
  severity = $(SIG_HI)
)
{
  /sbin/cardctl                         -> $(SEC_CRIT) ;
  /sbin/cardmgr                         -> $(SEC_CRIT) ;
  /sbin/hwclock                         -> $(SEC_CRIT) ;
  /sbin/isapnp                          -> $(SEC_CRIT) ;
  /sbin/kbdrate                         -> $(SEC_CRIT) ;
  /sbin/losetup                         -> $(SEC_CRIT) ;
  /sbin/lspci                           -> $(SEC_CRIT) ;
  /sbin/pnpdump                         -> $(SEC_CRIT) ;
  /sbin/probe                           -> $(SEC_CRIT) ;
  /sbin/pump                            -> $(SEC_CRIT) ;
  /sbin/setpci                          -> $(SEC_CRIT) ;
  /sbin/shapecfg                        -> $(SEC_CRIT) ;
}

##############################
#                            #
# System Information Programs #
#                            #
##############################
(
  rulename = "System Information Programs",
  severity = $(SIG_HI)
)
{
  /sbin/consoletype                     -> $(SEC_CRIT) ;
  /sbin/kernelversion                   -> $(SEC_CRIT) ;
  /sbin/runlevel
```

```
###################################
#                                 #
# Application Information Programs #
#                                 #
###################################

(
  rulename = "Application Information Programs",
  severity = $(SIG_HI)
)
{
  /sbin/genksyms                        -> $(SEC_CRIT) ;
  /sbin/rtmon                           -> $(SEC_CRIT) ;
  /sbin/sln                             -> $(SEC_CRIT) ;
}



#########################
#                       #
# Shell Related Programs #
#                       #
#########################

(
  rulename = "Shell Releated Programs",
  severity = $(SIG_HI)
)
{
  /sbin/getkey                          -> $(SEC_CRIT) ;
  /sbin/sash                            -> $(SEC_CRIT) ;
}

################
#              #
# OS Utilities #
#              #
################
(
  rulename = "Operating System Utilities",
  severity = $(SIG_HI)
)
{
  /bin/cat                              -> $(SEC_CRIT) ;
  /bin/date                             -> $(SEC_CRIT) ;
  /bin/dd                               -> $(SEC_CRIT) ;
  /bin/df                               -> $(SEC_CRIT) ;
  /bin/echo                             -> $(SEC_CRIT) ;
  /bin/egrep                            -> $(SEC_CRIT) ;
  /bin/false                            -> $(SEC_CRIT) ;
  /bin/fgrep                            -> $(SEC_CRIT) ;
  /bin/gawk                             -> $(SEC_CRIT) ;
  /bin/gawk-3.0.4                       -> $(SEC_CRIT) ;
  /bin/grep                             -> $(SEC_CRIT) ;
  /bin/true                             -> $(SEC_CRIT) ;
  /bin/arch                             -> $(SEC_CRIT) ;
  /bin/ash                              -> $(SEC_CRIT) ;
  /bin/ash.static                       -> $(SEC_CRIT) ;
  /bin/aumix-minimal                    -> $(SEC_CRIT) ;
  /bin/basename                         -> $(SEC_CRIT) ;
  /bin/consolechars                     -> $(SEC_CRIT) ;
  /bin/dmesg                            -> $(SEC_CRIT) ;
  /bin/doexec                           -> $(SEC_CRIT) ;
```

```
  /bin/ed                                 -> $(SEC_CRIT) ;
  /bin/gunzip                             -> $(SEC_CRIT) ;
  /bin/gzip                               -> $(SEC_CRIT) ;
  /bin/hostname                           -> $(SEC_CRIT) ;
  /bin/igawk                              -> $(SEC_CRIT) ;
  /bin/ipcalc                             -> $(SEC_CRIT) ;
  /bin/kill                               -> $(SEC_CRIT) ;
  /bin/ln                                 -> $(SEC_CRIT) ;
  /bin/loadkeys                           -> $(SEC_CRIT) ;
  /bin/login                              -> $(SEC_CRIT) ;
  /bin/ls                                 -> $(SEC_CRIT) ;
  /bin/mail                               -> $(SEC_CRIT) ;
  /bin/more                               -> $(SEC_CRIT) ;
  /bin/mt                                 -> $(SEC_CRIT) ;
  /bin/mv                                 -> $(SEC_CRIT) ;
  /bin/netstat                            -> $(SEC_CRIT) ;
  /bin/nice                               -> $(SEC_CRIT) ;
  /bin/ps                                 -> $(SEC_CRIT) ;
  /bin/rpm                                -> $(SEC_CRIT) ;
  /bin/sed                                -> $(SEC_CRIT) ;
  /bin/setserial                          -> $(SEC_CRIT) ;
  /bin/sfxload                            -> $(SEC_CRIT) ;
  /bin/sleep                              -> $(SEC_CRIT) ;
  /bin/sort                               -> $(SEC_CRIT) ;
  /bin/stty                               -> $(SEC_CRIT) ;
  /bin/su                                 -> $(SEC_CRIT) ;
  /bin/sync                               -> $(SEC_CRIT) ;
  /bin/tar                                -> $(SEC_CRIT) ;
  /bin/usleep                             -> $(SEC_CRIT) ;
  /bin/vi                                 -> $(SEC_CRIT) ;
  /bin/vimtutor                           -> $(SEC_CRIT) ;
  /bin/zcat                               -> $(SEC_CRIT) ;
  /bin/zsh                                -> $(SEC_CRIT) ;
  /bin/zsh-3.0.8                          -> $(SEC_CRIT) ;
}

##############################
#                            #
# Critical Utility Sym-Links #
#                            #
##############################
(
  rulename = "Critical Utility Sym-Links",
  severity = $(SIG_HI)
)
{
  /sbin/askrunlevel                       -> $(SEC_CRIT) ;
  /sbin/clock                             -> $(SEC_CRIT) ;
  /sbin/dnsconf                           -> $(SEC_CRIT) ;
  /sbin/fixperm                           -> $(SEC_CRIT) ;
  /sbin/fsconf                            -> $(SEC_CRIT) ;
  /sbin/ipfwadm-wrapper                   -> $(SEC_CRIT) ;
  /sbin/kallsyms                          -> $(SEC_CRIT) ;
  /sbin/ksyms                             -> $(SEC_CRIT) ;
  /sbin/mailconf                          -> $(SEC_CRIT) ;
  /sbin/managerpm                         -> $(SEC_CRIT) ;
  /sbin/modemconf                         -> $(SEC_CRIT) ;
  /sbin/lsmod                             -> $(SEC_CRIT) ;
  /sbin/modprobe                          -> $(SEC_CRIT) ;
  /sbin/mount.ncp                         -> $(SEC_CRIT) ;
  /sbin/mount.ncpfs                       -> $(SEC_CRIT) ;
  /sbin/mount.smb                         -> $(SEC_CRIT) ;
  /sbin/mount.smbfs                       -> $(SEC_CRIT) ;
  /sbin/netconf                           -> $(SEC_CRIT) ;
  /sbin/pidof                             -> $(SEC_CRIT) ;
```

```
  /sbin/poweroff                        -> $(SEC_CRIT) ;
  /sbin/quotaoff                        -> $(SEC_CRIT) ;
  /sbin/raid0run                        -> $(SEC_CRIT) ;
  /sbin/raidhotadd                      -> $(SEC_CRIT) ;
  /sbin/raidhotremove                   -> $(SEC_CRIT) ;
  /sbin/raidstop                        -> $(SEC_CRIT) ;
  /sbin/rdump.static                    -> $(SEC_CRIT) ;
  /sbin/rrestore                        -> $(SEC_CRIT) ;
  /sbin/rrestore.static                 -> $(SEC_CRIT) ;
  /sbin/swapoff                         -> $(SEC_CRIT) ;
  /sbin/rdump                           -> $(SEC_CRIT) ;
  /sbin/reboot                          -> $(SEC_CRIT) ;
  /sbin/rmmod                           -> $(SEC_CRIT) ;
  /sbin/telinit                         -> $(SEC_CRIT) ;
  /sbin/userconf                        -> $(SEC_CRIT) ;
  /sbin/uucpconf                        -> $(SEC_CRIT) ;
  /bin/awk                              -> $(SEC_CRIT) ;
  /bin/dnsdomainname                    -> $(SEC_CRIT) ;
  /bin/domainname                       -> $(SEC_CRIT) ;
  /bin/ex                               -> $(SEC_CRIT) ;
  /bin/gtar                             -> $(SEC_CRIT) ;
  /bin/nisdomainname                    -> $(SEC_CRIT) ;
  /bin/red                              -> $(SEC_CRIT) ;
  /bin/rvi                              -> $(SEC_CRIT) ;
  /bin/rview                            -> $(SEC_CRIT) ;
  /bin/view                             -> $(SEC_CRIT) ;
  /bin/xnmap                            -> $(SEC_CRIT) ;
  /bin/ypdomainname                     -> $(SEC_CRIT) ;
}

################################
#                              #
# Critical configuration files #
#                              #
################################
(
  rulename = "Critical configuration files",
  severity = $(SIG_HI)
)

{
     /etc/conf.linuxconf                -> $(SEC_BIN) ;
     /etc/crontab                       -> $(SEC_BIN) ;
     /etc/cron.hourly                   -> $(SEC_BIN) ;
     /etc/cron.daily                    -> $(SEC_BIN) ;
     /etc/cron.weekly                   -> $(SEC_BIN) ;
     /etc/cron.monthly                  -> $(SEC_BIN) ;
     /etc/default                       -> $(SEC_BIN) ;
     /etc/fstab                         -> $(SEC_BIN) ;
     /etc/exports                       -> $(SEC_BIN) ;
     /etc/group-                        -> $(SEC_BIN) ;
     /etc/host.conf                     -> $(SEC_BIN) ;
     /etc/hosts.allow                   -> $(SEC_BIN) ;
     /etc/hosts.deny                    -> $(SEC_BIN) ;
     /etc/httpd/conf                    -> $(SEC_BIN) ;
     /etc/protocols                     -> $(SEC_BIN) ;
     /etc/services                      -> $(SEC_BIN) ;
     /etc/rc.d/init.d                   -> $(SEC_BIN) ;
     /etc/rc.d                          -> $(SEC_BIN) ;
     /etc/mail.rc                       -> $(SEC_BIN) ;
     /etc/motd                          -> $(SEC_BIN) ;
     /etc/passwd                        -> $(SEC_CONFIG) ;
     /etc/passwd-                       -> $(SEC_CONFIG) ;
     /etc/profile.d                     -> $(SEC_BIN) ;
     /var/lib/nfs/rmtab                 -> $(SEC_BIN) ;
```

```
        /usr/sbin/fixrmtab              -> $(SEC_BIN) ;
        /etc/rpc                        -> $(SEC_BIN) ;
        /etc/sysconfig                  -> $(SEC_BIN) ;
        /etc/smb.conf                   -> $(SEC_CONFIG) ;
        /etc/gettydefs                  -> $(SEC_BIN) ;
        /etc/nsswitch.conf              -> $(SEC_BIN) ;
        /etc/yp.conf                    -> $(SEC_BIN) ;
        /etc/hosts                      -> $(SEC_CONFIG) ;
        /etc/inetd.conf                 -> $(SEC_CONFIG) ;
        /etc/inittab                    -> $(SEC_CONFIG) ;
        /etc/resolv.conf                -> $(SEC_CONFIG) ;
        /etc/syslog.conf                -> $(SEC_CONFIG) ;

}
```

7. Prilog B

Izvještaj `Tripwire` programskog paketa:

```
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:          root
Report created on:            Mit 06 Mär 2002 19:57:50 CET
Database last updated on:     Never

===============================================================================
Report Summary:
===============================================================================
Host name:                    merlin.fbunet.de
Host IP address:              192.168.0.3
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/merlin.fbunet.de.twd
Command line used:            /usr/sbin/tripwire --check

===============================================================================
Rule Summary:
===============================================================================
-------------------------------------------------------------------------------
Section: Unix File System
-------------------------------------------------------------------------------
Rule Name       Severity Level    Added    Removed  Modified
---------      --------------    -----    -------
* (/)                           0                1        0        8


Total objects scanned:  46498
Total violations found:  9

===============================================================================
Object Summary:
===============================================================================
-------------------------------------------------------------------------------
# Section: Unix File System
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Rule Name:  (/)
Severity Level: 0
-------------------------------------------------------------------------------
Added:
"/var/lib/tripwire/report/merlin.fbunet.de-20020306-190525.twr"

Modified:
```

```
"/etc/aide/aide.conf"
"/etc/aide/aide.db"
"/home/fridtjob/.bash_history"
"/root/.bash_history"
"/root/.viminfo"
"/var/lib/tripwire/merlin.fbunet.de.twd"
"/var/lib/tripwire/merlin.fbunet.de.twd.bak"
"/var/run/utmp"

---------------------------------------------------------------------------
Error Report:
---------------------------------------------------------------------------

No Errors

---------------------------------------------------------------------------
*** End of report ***
```

8. Prilog C

Konfiguracijska datoteka AIDE programa:

```
#################################################################
#              ***Primjer AIDE conf datoteke***                 #
#################################################################
#                                                               #
#  Svojstva objekata (datoteka i direktorija) koja se mogu      #
#               provjeravati AIDE programom                     #
#                                                               #
#################################################################
# p:      permissions
# i:      inode
# n:      number of links
# u:      user
# g:      group
# s:      size
# b:      block count
# m:      mtime
# a:      atime
# c:      ctime
# S:      check for growing size
# md5:    md5 checksum
# sha1:   sha1 checksum
# rmd160: rmd160 checksum
# tiger:  tiger checksum
# R:      p+i+n+u+g+s+m+c+md5
# L:      p+i+n+u+g
# E:      Empty group
# >:      Growing logfile p+u+g+i+n+S

# Moguće je definirati i vlastita pravila provjere integriteta
# Sintaksa je sljedeća:

Pravilo = p+i+n+u+g+s+b+m+c+md5+sha1

# Uključivanje objekata koji se žele kontrolirati

# Za /etc direktorij provjeri ovlasti pristupa, korisnika, grupu
# te inode podatke

/etc p+i+u+g

# Na /bin, /sbin i /var direktorije primjenjuje se posebno definirano
# pravilo Pravilo
```

```
/bin Pravilo
/sbin MyRule
/var MyRule

# Sljedeće datoteke i direktoriji se ignoriraju zbog učestalih
# promjena:

!/var/log/.*
!/var/spool/.*
!/var/adm/utmp$
```

9. Prilog D

Primjer izvještaja AIDE programa:

```
AIDE found differences between database and filesystem!!
Start timestamp: 2002-03-06 19:45:29
Summary:
Total number of files=46464,added files=1,removed files=1,changed
files=1

Added files:
added:/var/lib/tripwire/report/merlin.fbunet.de-20020306-190525.twr
Removed files:
removed:/etc/aide/aide.db.new
Changed files:
changed:/etc/aide/aide.db
Detailed information about changes:

File: /etc/aide/aide.db
  Size     : 1690827                          , 3510053

  Inode    : 81686                            , 81685

  MD5      : XpIshBwEv+pl8N34dKcpWw==          , JIYQfKePwB6GvhTl50o+rg==

  SHA1     : BYD4MihoVGDqJXPM7N9RtEOdeVw=      ,
Z1KnSYUMQjgWHmuu/FE7wG84SPs=

  CRC32    : v2Fr1A==                         , JgtoAg==

  HAVAL    : AKPwwjumHKpIShn3PVc8CaVxolFU31e5yjL/0Yj,
/wrlj+dBbsFpp6DhfosR/q5ASx+G6NLyUd4kNOC
```

10. Prilog E

Primjer izvještaja `GFI Languard File Integrity Checker` programa:

```
This is an automatic message. Do not reply !
Report generated by LANguard File Integrity Checker on 11/05/02 14:58:45
********************************************************************************
******
- C:\WINNT\Installer\e67d5.msi has changed!
File: e67d5.msi
Size before change: 2349568
Size after change: 2349568
Size difference: 0

- C:\WINNT\Installer\{B1EEFF4A-C2C3-47DF-A02D-D21B47543042}\intactico was
added to the system!
File: intactico
Size: 766
Creation Date: 11/05/02 14:25:59
```

```
Modification Date: 11/05/02 14:25:59

- C:\WINNT\system32\MSVBVM60.DLL has changed!
File: MSVBVM60.DLL
Size before change: 1388544
Size after change: 1388544
Size difference: 0

- C:\WINNT\system32\config\SAM.LOG has changed!
File: SAM.LOG
Size before change: 4096
Size after change: 4096
Size difference: 0

- C:\WINNT\system32\config\software.LOG has changed!
File: software.LOG
Size before change: 1024
Size after change: 8192
Size difference: 7168

- C:\WINNT\Installer\MSI1D6.tmp was added to the system!
File: MSI1D6.tmp
Size: 665072
Creation Date: 11/05/02 14:52:49
Modification Date: 11/05/02 14:52:53

- C:\WINNT\Installer\{B1EEFF4A-C2C3-47DF-A02D-D21B47543042}\ was added to
the system!
Folder: WINNT\Installer\{B1EEFF4A-C2C3-47DF-A02D-D21B47543042}
Creation Date: 11/05/02 14:25:59
Modification Date: 11/05/02 14:25:59

- C:\WINNT\ has changed!
Folder: WINNT
Creation Date: 05/02/02 13:16:06
Modification Date: 11/05/02 14:24:45

- C:\WINNT\hpbafd.ini has changed!
File: hpbafd.ini
Size before change: 455
Size after change: 455
Size difference: 0

- C:\WINNT\system32\spool\PRINTERS\ has changed!
Folder: WINNT\system32\spool\PRINTERS
Creation Date: 05/02/02 13:28:52
Modification Date: 11/05/02 14:40:21

- C:\winzip.log has changed!
File: winzip.log
Size before change: 148542
Size after change: 150539
Size difference: 1997

- C:\WINNT\Installer\11e77b2.msi was added to the system!
File: 11e77b2.msi
Size: 1135104
Creation Date: 11/05/02 14:25:57
Modification Date: 11/05/02 14:25:58

- C:\WINNT\system32\config\software has changed!
File: software
Size before change: 16281600
Size after change: 16281600
Size difference: 0
```

```
- C:\WINNT\Crystal\u2ddisk.dll was added to the system!
File: u2ddisk.dll
Size: 28672
Creation Date: 02/03/01 06:05:56
Modification Date: 02/03/01 06:05:56

- C:\WINNT\Crystal\u2fwordw.dll was added to the system!
File: u2fwordw.dll
Size: 106496
Creation Date: 02/03/01 06:05:56
Modification Date: 02/03/01 06:05:56

- C:\WINNT\Crystal\Cdo32.dll was added to the system!
File: Cdo32.dll
Size: 53248
Creation Date: 01/22/01 08:33:42
Modification Date: 01/22/01 08:33:42

- C:\WINNT\SchedLgU.Txt has changed!
File: SchedLgU.Txt
Size before change: 32580
Size after change: 32130
Size difference: 450

- C:\WINNT\system32\config\SAM has changed!
File: SAM
Size before change: 20480
Size after change: 20480
Size difference: 0

- C:\WINNT\system32\ has changed!
Folder: WINNT\system32
Creation Date: 05/02/02 13:16:06
Modification Date: 11/05/02 14:30:13

- C:\WINNT\Installer\{B1EEFF4A-C2C3-47DF-A02D-D21B47543042}\ControlPanel was
added to the system!
File: ControlPanel
Size: 766
Creation Date: 11/05/02 14:25:59
Modification Date: 11/05/02 14:25:59

- C:\WINNT\Tasks\Languard File Integrity Checker.job has changed!
File: Languard File Integrity Checker.job
Size before change: 444
Size after change: 444
Size difference: 0

- C:\WINNT\Crystal\u2fxls.dll was added to the system!
File: u2fxls.dll
Size: 212992
Creation Date: 02/03/01 06:05:56
Modification Date: 02/03/01 06:05:56

- C:\WINNT\Crystal\ was added to the system!
Folder: WINNT\Crystal
Creation Date: 11/05/02 14:24:45
Modification Date: 11/05/02 14:24:45

- C:\WINNT\system32\wbem\Logs\wbemcore.log has changed!
File: wbemcore.log
Size before change: 35618
Size after change: 35674
Size difference: 56
```

```
- C:\WINNT\Crystal\u2dapp.dll was added to the system!
File: u2dapp.dll
Size: 28672
Creation Date: 11/08/00 13:46:00
Modification Date: 11/08/00 13:46:00

- C:\WINNT\Installer\ has changed!
Folder: WINNT\Installer
Creation Date: 05/02/02 11:43:28
Modification Date: 11/05/02 14:52:48

- C:\WINNT\Crystal\P2smon.dll was added to the system!
File: P2smon.dll
Size: 163840
Creation Date: 02/03/01 05:26:54
Modification Date: 02/03/01 05:26:54

- C:\WINNT\Crystal\crxf_pdf.dll was added to the system!
File: crxf_pdf.dll
Size: 270336
Creation Date: 02/03/01 01:22:28
Modification Date: 02/03/01 01:22:28

- C:\WINNT\Crystal\u2fhtml.dll was added to the system!
File: u2fhtml.dll
Size: 45056
Creation Date: 02/03/01 06:05:56
Modification Date: 02/03/01 06:05:56

- C:\WINNT\Installer\1370513.ipi was added to the system!
File: 1370513.ipi
Size: 7680
Creation Date: 11/05/02 14:52:48
Modification Date: 11/05/02 14:52:48
```