HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Prelude IDS

CCERT-PUBDOC-2007-04-189

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

Zbog sve većeg prisustva računala u svim sferama poslovanja i društvenih djelovanja i sve važnijih i osjetljivijih poslova koji se obavljaju na njima, sve se više pažnje ulaže u računalnu sigurnost. U vrijeme prije interneta i velikih računalnih mreža računalna sigurnost se uglavnom svodila na ograničavanje fizičkog pristupa tadašnjim računalima. Spajanjem računala u mreže, a posebno sve većom rasprostranjenošću širokopojasnog interneta koncept računalne sigurnosti se u potpunosti promijenio. Internet je omogućio pristupanje računalnim sustavima i podacima pohranjenima na njima s bilo kojeg mjesta u svijetu. Međutim to je donijelo i velik broj sigurnosnih rizika. Povećanjem dostupnosti sustava legitimnim korisnicima, sustav postaje dostupan i sve većem broju onih zlonamjernih.

Među mnogobrojnim alatima namijenjenim povećanju sigurnosti nalaze se i sustavi za detekciju neovlaštenog pristupa (*eng. Intrusion Detection System*) ili skraćeno IDS. Njihova svrha je što ranije otkrivanje neovlaštenog pristupa te brzo obavještavanje administratora kako bi što ranije poduzeo odgovarajuće mjere zaštite. Zbog kompleksnosti računalnih sustava i velikog broja mrežnih usluga, ne postoji jedan alat koji bi mogao pokriti sva područja i koji bi mogao zajamčiti apsolutnu učinkovitost u otkrivanju neovlaštenog pristupa. Zbog toga je potrebno kombinirati veći broj različitih alata. Iako ovakvo rješenje povećava vjerojatnost otkrivanja neovlaštenog pristupa ono zahtjeva i daleko više administratorskog rada jer se mora nadzirati veći broj dnevničkih zapisa. Kako bi im se posao olakšao osmišljena su hibridna IDS okruženja. Ona prikupljaju i filtriraju podatke dobivene iz različitih alata te omogućuju njihovo grupiranje u logičke cjeline u kojima je lakše pratiti rad računalnog sustava, a ujedno i uočiti događaje koji predstavljaju sigurnosni rizik.

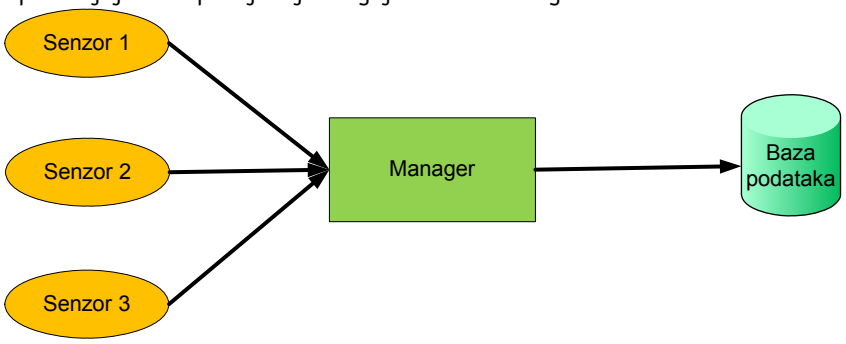
Jedno od takvih okruženja je i Prelude IDS. U ovom dokumentu ukratko se opisuju instalacija i postavljanje Prelude IDS okruženja te daje pregled njegovih mogućnosti.

2. Prelude IDS

Prelude IDS je hibridno IDS okruženje tj. program koji svim sigurnosnim programima, bez obzira jesu li otvorenog ili zatvorenog koda, omogućuje prijavljivanje incidenata na centralizirano mjesto. Kako bi to omogućio Prelude IDS se oslanja na IDMEF (eng. *Intrusion Detection Message Exchange Format*) standard IETF-a (eng. *The Internet Engineering Task Force*) koji definira format podataka i procedure za njihovu razmjenu između IDS-a i sustava s kojima IDS-ovi interagiraju.
"Hibridno" u opisu programa Prelude znači da je moguće kombinirati podatke dobivene iz bilo kojeg programa za sigurnost.

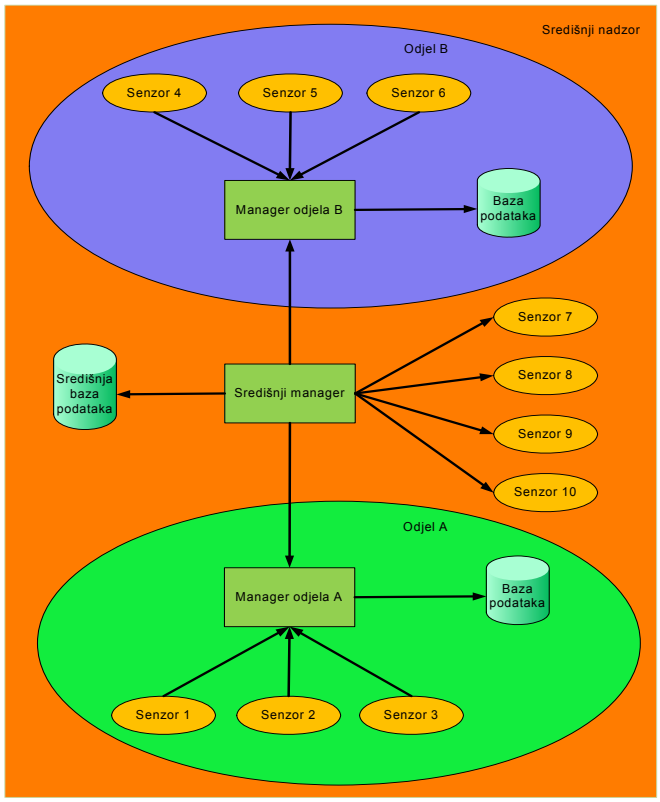
2.1. Arhitektura

Prelude okruženje sastoji se od dva osnovna djela: senzora i managera. Senzori su svi programi koji prikupljaju podatke o sigurnosnim događajima. Manager je dio programa koji prima podatke od senzora te ih pohranjuje ili ih prosljeđuje drugoj instanci managera.



Slika 1: Prikaz najjednostavnije arhitekture Prelude sustava

Prelude je moguće instalirati u nekoliko načina rada odnosno arhitektura. U najjednostavnijem načinu sve komponente (senzori i prelude-manager) nalaze se na istom računalu. Takva arhitektura prikazana je na slici 1. Osim ovog jednostavnog načina moguće je okruženje postaviti tako da jedan prelude-manager prosljeđuje sve informacije drugom prelude-manageru. Na slici 2. prikazan je primjer složenije arhitekture u kojoj manageri iz odjela A i B prosljeđuju sve informacije središnjem manageru. Manageri odjela A i B djeluju neovisno jedan o drugom. Podaci prikupljeni u odjelu A nisu vidljivi manageru u odjelu B i obrnuto. Ovakva arhitektura svakom odjelu omogućuje nadzor nad vlastitim podsustavom, ali istovremeno osigurava i središnji nadzor cjelokupnog sustava. Svaki odjel u ovom prikazu može se sastojati od proizvoljnog broja računala tj. svaki senzor prikazan na shemi može se nalaziti na zasebnom računalu ili može predstavljati sve senzore na jednom računalu. Također je moguće unakrsno povezati dva managera kako bi se osigurao integritet podataka u slučaju kompromitacije jedne instance managera.
Osim prikazanih postoji i mogućnost tzv. obrnutog prosljeđivanja. Ono je potrebno kada prelude-manager koji se nalazi u jednoj mreži ne može pristupiti manageru u drugoj mreži. Primjer ovakve situacije je mreža zatvorena vatrozidom (*eng. DeMilitarized Zone* - DMZ) koji blokira spajajanje na vanjsku mrežu. U takvoj se situaciji prelude-manager iz vanjske mreže može spojiti na manager u unutrašnjoj mreži i od njega zatražiti pohranjene informacije.



Slika 2: Prikaz složene arhitekture

2.2. Komponente

Osnovni dijelovi Prelude okruženja su:

- Prelude biblioteka - libprelude je biblioteka koja omogućava sigurnu komunikaciju s jednim ili nekoliko Prelude-managera i pruža API (eng. *Application Programming Interface*) za kreiranje događaja temeljenih na IDMEF standardu.
  Također osigurava i spremanje obavijesti u lokalnu datoteku u slučaju nedostupnosti nekog od prelude-managera (eng. *failover*).
- Prelude-manager - servis visoke dostupnosti koji prikuplja i normalizira informacije dobivene od senzora i sprema ih u bazu podataka. Također može prosljeđivati informacije drugom prelude-manageru kao i filtrirati primljene događaje kako bi omogućio različite reakcije za različite skupine događaja.
- Prelude-LML - komponenta za analizu dnevničkih zapisa (eng. *log*) na računalu. Neki od dnevničkih zapisa koje može analizirati su: Cisco PIX, Clamav, Grsecurity, ipchains, Netfilter, ipfw, Nokia ipso, Apache ModSecurity, Ms-SQL, Nagios, Norton Antivirus Corporate Edition, NTsyslog, Pam, Portsentry, Postfix, Proftpd, ssh i mnogi drugi.
- PreludeDB - biblioteka koja omogućuje jednostavan pristup bazi podataka u kojoj Prelude čuva informacije. Zahvaljujući ovoj biblioteci moguće je pristup podacima realizirati neovisno o vrsti baze podataka s kojom se radi.
- Prewikka - aplikacija koja pruža napredne mogućnosti filtriranja i pregledavanja podataka te prikazuje prikupljene podatke u ljudima lako čitljivom obliku.

3. Instalacija

3.1. Instalacija komponenti

Prelude IDS okruženje prvenstveno je razvijano za GNU/Linux operacijski sustav, ali također radi i na *BSD sustavu kao i na svim platformama koje zadovoljavaju POSIX standard. Prije instalacije samog okruženja potrebno je instalirati slijedeće programe:

- GnuTLS,
- Python,
- PCRE,
- MySQL i/ili PostgreSQL.

MySQL i PostgreSQL su potrebni za pohranjivanje sigurnosnih događaja u bazu podataka. Ukoliko se sigurnosni događaji pohranjuju u tekstualnu datoteku ili se prosljeđuju udaljenom manageru nije potrebno instalirati MySQL ni PostgreSQL.

Komponente koje je potrebno instalirati ovise o načinu rada alata Prelude. Osnovna komponenta koja je potrebna u svim načinima rada je *libprelude*. Na računalima na kojima će biti *prelude-manager* potrebno je osim njega instalirati i *libpreludedb*. Osim već prije spomenutog *prelude-lml* senzora moguće je instalirati Snort i Samhain programe na računala nad kojima se vrši nadzor.

Izvorni kod svih programa može se preuzeti sa stranica Prelude IDS-a [2.]

Instalaciju Prelude sustava započinjemo postavljanjem *libprelude* biblioteke kao osnovne komponente sustava. Nakon preuzimanja i raspakiranja koda potrebno je izvršiti slijedeći niz naredbi:

```
$ ./configure
$ make
$ make install
$ ldconfig
```

Nakon uspješne instalacije *libprelude* biblioteke nastavljamo s instalacijom ostalih potrebnih komponenti ovisno o arhitekturi sustava. Postupak instalacije *libpreludedb* identičan je onom za instalaciju *libprelude*. Ukoliko želimo da Prelude podatke sprema u bazu podataka po završetku instalacije *libpreludedb* potrebno je kreirati tablice i posebnog korisnika kojim će Prelude pristupati dodjeljenim tablicama.

Instalacija *prelude-lml* i *prelude-manager* komponenti razlikuje se od instalacije prethodne dvije komponente utoliko što na kraju nije potrebno izvršiti naredbu *ldconfig*.

Prilikom instaliranja Snort paketa potrebno je prilikom izvršavanja *configure* naredbe uključiti opciju *--enable-prelude*, a za Samhain *–with-prelude*. Postupak instalacije i konfiguracije Snort i Samhain programa detaljnije je opisan u dokumentima objavljenim na stranicama CERT-a [3.][4.]

Instalacija Prewikka komponente u potpunosti je različita od instalacije ostalih komponenti sustava. Za nju su potrebni Python 2.3 i Cheetah predložci za Python. Oni se mogu preuzeti sa njihove web stranice [5.] Nakon raspakiranja koda potrebno je izvršiti slijedeću naredbu:

```
$ python setup.py install
```

3.2. Registracija senzora

Da bi senzori mogli komunicirati s *prelude-managerom* potrebno ih je registrirati. Postupak registracije sastoji se od nekoliko koraka:

- dodjeljivanja jedinstvenog imena senzoru,
- kreiranja direktorija kojeg će senzor koristiti i
- registracije kod *prelude-managera* s kojim će senzor komunicirati, tj. dodjeljivanja X509 certifikata koji osigurava komunikaciju korištenjem dodjeljenih prava.

Informacije o jedinstvenom imenu, direktoriju i certifikatu pohranjuju se u profil senzora. Profil se identificira po imenu. Prilikom pokretanja senzor će pokušati učitati profil istog imena kao i sam senzor tj. ukoliko se senzor zove *prelude-lml* tad će pokušati učitati profil koji se zove *prelude-lml*. Ime profila moguće je zadati dodatnim parametrom prilikom pokretanja senzora.

Cjelovit proces registracije senzora obavlja se korištenjem alata zvanog *prelude-adduser*.

```
$ prelude-adduser register <ime profila> <tražena prava> <adresa
managera> --uid <uid> --gid <gid>
```

Prilikom registracije potrebno je obratiti pažnju na to s kojim se uid-om i gid-om registrira senzor. Moguće ga je registrirati s bilo kojim uid-om i gid-om koji postoje na sustavu, ali mu je neophodno osigurati pravo pristupa informacijama iz biblioteke *libprelude* (ključ, certifikat i dr.)
Postoje dvije skupine prava koja se mogu dodijeliti jednom senzoru:

- idmef i
- admin.

Obje skupine mogu sadržavati dozvolu za čitanje (*r*) i/ili dozvolu za pisanje (*w*). Budući da senzor obično ima potrebu za pisanjem IDMEF poruka manageru i čitanja administracijskih naredbi koje mu se šalju, uobičajena postavka prava izgleda ovako:

```
idmef:w admin:r
```

Adresa managera je adresa na kojoj se nalazi *prelude-manager* kojem će senzor dojavljivati podatke. Ukoliko se i senzor i manager nalaze na istom računalu kao adresu je potrebno navesti *localhost*.
U slučaju da nismo sigurni koje je vrijednosti potrebno postaviti za neku od opcija dovljno je samo pokrenuti senzor što će izazvati ispis svih potrebnih parametara.

```
prelude-client-profile: error creating prelude-client: Could not
open AnalyzerID file.

Basic file configuration does not exist. Please run :
prelude-adduser register prelude-lml "idmef:w admin:r" <manager
address> --uid 1000 --gid 100
program to setup the analyzer.

Be aware that you should replace the "<manager address>" argument
with
the server address this analyzer is reporting to as argument.
"prelude-adduser" should be called for each configured server
address.
```

Automatski ponuđeni *uid* i *gid* parametri pripadaju korisniku koji pokreće senzor. Ukoliko taj korisnik nema pravo pristupa informacijama iz biblioteke *libprelude*, potrebno je ponuđene uid i gid vrijednosti zamijeniti parametrima korisnika koji na sustavu ima potrebna prava.
Slijedi demostracija registriracije *prelude-lml* senzora pri *prelude-manageru* koji se nalazi na istom računalu:

```
$ prelude-adduser register prelude-lml "idmef:w admin:r" localhost
```

Nakon izvršavanja *prelude-adduser* će zatražiti pokretanje iste skripte na računalu na kojem se nalazi *prelude-manager*:

```
  You now need to start "prelude-adduser" on the server host where
  you need to register to:

  use: "prelude-adduser registration-server <analyzer profile>"
  example: "prelude-adduser registration-server prelude-manager"

  This is used in order to register the 'sending' analyzer to the
'receiving'
  analyzer. <analyzer profile> should be set to the profile name of
the
  'receiving' analyzer, the one where 'sending' analyzer will
register to.

  Please remember that "prelude-adduser" should be used to register
```

```
  every server used by this analyzer.
```

Dakle, na poslužitelju je potrebno pokrenuti slijedeću naredbu:

```
$ prelude-adduser registration-server prelude-manager
```

Njenim izvršavanjem dobiva se :

```
- Starting registration server.
  - generated one-shot password is "deadbeaf".

    This password will be requested by "prelude-adduser" in order
to connect.
    Please remove the first and last quote from this password
before using it.

  - Waiting for install request from peer...
```

Lozinku dobivenu izvršavanjem prethodne naredbe potrebno je upisati u instanci pokrenutoj na strani senzora. Nakon unošenja lozinke ispisuje se poruka o uspješnom dodavanju senzora:

```
  - Enter registration one shot password
  - Please confirm one shot password
  - connecting to registration server (localhost:5553)...
  - Sending certificate request.
  - Receiving CA signed certificate.
  - Receiving CA certificate.

- prelude-lml registration to localhost successful.
```

Na strani poslužitelja također se ispisuje poruka o uspješnoj registraciji:

```
  - Waiting for install request from peer...
  - Connection from 127.0.0.1:57232.
  - Waiting for client certificate request.
  - Analyzer with ID="1537698187535812" ask for registration with
permission="idmef:w admin:r".
    Approve registration [y/n]: y
    Registering analyzer "1537698187535812" with permission
"idmef:w admin:r".
  - Generating signed certificate for client.
  - Sending server certificate to client.
  - 127.0.0.1:30098 successfully registered.
```

Nakon registracije preostaje samo pokrenuti senzor:

```
$ /etc/init.d/prelude-lml start
```

4. Postavke

4.1. Postavke senzora

Svi Prelude senzori imaju jedinstven skup postavki definiran Prelude okruženjem. Svaka od tih postavki može se promijeniti globalno na razini računala ili na razini pojedinog senzora, ukoliko senzor pruža tu mogućnost. Globalne konfiguracijske datoteke su samo predlošci koje će senzori koristiti ukoliko neke postavke nisu definiranje u njihovim vlastitim konfiguracijskim datotekama.
Cjelokupna konfiguracija na razini računala sadržana je u tri datoteke koje se najčešće nalaze u */usr/etc/prelude/default/* direktoriju. One su:

- *client.conf*,
- *global.conf* i
- *idmef-client.conf*.

U datoteci *client.conf* navode se podaci potrebni klijentskom dijelu okruženja za spajanje na *prelude-manager*. Prilikom navođenja potrebnih podataka dozvoljena je uporaba logičkih operatora || (logičko "ili") i && (logičko "i"). Podaci potrebni za spajanje sadrže adresu poslužitelja na kojem se nalazi prelude-manager te port na kojem manager sluša ukoliko ne sluša na standardnom portu. Bez obzira na podatke navedene u ovoj datoteci, svi podaci koji se šalju kroz prelude okruženje spremaju se za slučaj nedostupnosti udaljenog prelude-managera. U tom slučaju klijent pokušava periodički uspostaviti vezu s managerom i poslati sve spremljene podatke.
Slijede tri primjera konfiguracije u datoteci *client.conf*:

```
server-addr = x.x.x.x
```

```
server-addr = x.x.x.x && y.y.y.y
```

```
server-addr = x.x.x.x:z || y.y.y.y
```

U prvom primjeru manager se postavlja tako da se spaja na računalo x.x.x.x. U drugom slučaju spaja se na računala x.x.x.x i y.y.y.y i oboma šalje podatke. Za razliku od toga, u trećem primjeru klijent očekuje manager aplikaciju na portu z adrese x.x.x.x, a, ukoliko ju tamo ne pronađe, pokušava se spojiti na računalo y.y.y.y.
Ukoliko se klijentski dio aplikacije (senzori) nalaze na istom računalu kao i manager tada je adresa na koju se klijent treba spajati 127.0.0.1.

Datoteku *global.conf* koriste svi dijelovi Prelude okruženja (i senzori i prelude-manager, ukoliko je instaliran na dotičnom računalu). Ona osigurava jedinstven predložak sa uobičajenim IDMEF atributima. Sve postavke u ovoj datoteci su opcionalne, ali su vrlo bitne jer olakšavaju snalaženje u snimljenim podacima, posebno u velikim sustavima s velikim brojem distribuiranih senzora.
Postavke sadržane u ovoj datoteci su:

- heartbeat-interval – koliko često se klijent prijavljuje manageru u situaciji kad ne prijavljuje nikakav sigurnosni događaj. Takvo prijavljivanje je bitno kako bi se moglo razlikovati neispravan senzor od senzora na sustavu bez sigurnosnih događaja koje je potrebno prijaviti,
- node-name – ime opreme na kojoj se nalazi senzor (najčešće ime računala),
- node-location – lokacija opreme (grad, prostorija u kojoj se nalazi računalo sa serverom ili sl.),
- node-category – tip čvora na kojem su pokrenuti klijenti,
- address – adresa opreme,
- netmask – mrežna maska za adresu,
- vlan-name – ime virtualnog LAN-a na kojem se nalazi oprema,
- vlan-num – broj virtualnog LAN-a na kojem se nalazi oprema i
- category – tip navedene adrese (najčešće *ipv4-addr* ili *ipv6-addr*).

Datoteka *idmef-client.conf* sadrži datoteke *client.conf* i *global.conf* te ju nije preporučljivo izravno mijenjati.
Konfiguracijske datoteke pojedinih senzora nalaze se u /etc/profil/ direktoriju, gdje je profil ime profila s kojim je senzor registriran.

4.2. Postavke prelude-manager poslužitelja

Prelude-manager je poslužitelj visoke dostupnosti koji prihvaća sigurne konekcije od distribuiranih senzora ili drugih managera i sprema primljene događaje na korisnički zadan medij (baza podataka, dnevnički zapisi, elektronička pošta itd.). Poslužitelj je u stanju rukovati velikim brojem konekcija i obraditi veliku količinu događaja. Koristi poseban red (eng. *queue*) kako bi se osiguralo prioritetno obrađivanje događaja prema njihovoj ozbiljnosti.

Konfiguracijska datoteka u kojoj se nalaze parametri potrebni za rad *prelude-managera* nalazi se u */etc/prelude-manager/* direktoriju i zove se *prelude-manager.conf*.
Nakon obrađivanja događaja manager koristi dodatke za prijavljivanje kako bi pretvorio binarni IDMEF format u razne izlazne formate. Postoji nekoliko dodataka za prijavljivanje:

- *db* – za baze podataka (MySQL i PostgreSQL),
- *xmlmod* – za XML (eng. *eXtended Markup Language*) format,
- *textmod* – za tekstualni format,
- *relaying* – za prosljeđivanje informacija drugim managerima i
- *smtp* – komercijalni dodatak za slanje tekstualnih upozorenja putem elektroničke pošte.

Svaki dodatak za prijavljivanje moguće je učitati više puta s različitim postavkama kako bi se podaci spremali na više različitih lokacija. Tako je npr. moguće dva puta učitati db dodatak kako bi se događaji spremili u dvije različite baze podataka.

4.2.1. Baza podataka

Da bi prelude-manager spremao događaje u bazu podataka potrebno je iskoristiti *db* dodatak. Njegovo korištenje ukjučuje i specifikaciju slijedećih parametara

- *type* – vrsta baze podataka (mysql ili pgsql),
- *host* – adresa poslužitelja na kojem se nalazi baza podataka,
- *port* – port na kojem sluša baza podataka,
- *name* – ime baze podataka,
- *user* – korisničko ime za spajanje na bazu i
- *pass* – lozinka za spajanje na bazu.

4.2.2. Prosljeđivanje

Prelude-manager može događaje prosljeđivati drugim prelude-managerima koristeći *relaying* dodatak. Ova mogućnost je vrlo korisna kad je mreža podijeljena na više podmreža.
Da bi manager radio u ovom načinu rada potrebno ga je pokrenuti na slijedeći način:

```
prelude-manager --relaying --parent-managers "x.x.x.x"
```

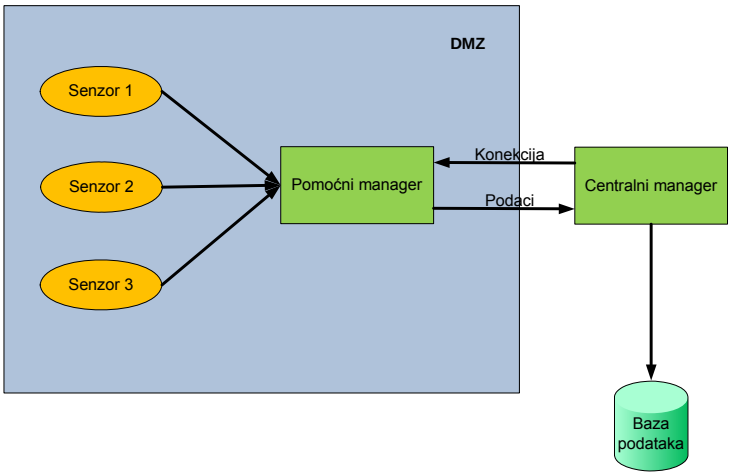
ili u konfiguracijsku datoteku zapisati:

```
[relaying]
parent-managers = x.x.x.x
```

gdje je x.x.x.x adresa managera kojem prosljeđuje događaje. Kod navođenja adresa moguće je korištenje logičkih operatora || (ili) i && (i) kao i kod navođenja adresa za spajanje prelude senzora.

4.2.3. Obrnuto prosljeđivanje

U nekim situacijama (npr. DMZ mreže) zbog tehničkih ili sigurnosnih ograničenja analizatori se ne mogu spajati na manager koji se nalazi u drugoj mreži. Međutim ukoliko su dozvoljene konekcije prema mreži u kojoj se nalaze analizatori moguće je koristiti obrnuto prosljeđivanje. U ovoj situaciji manager kontaktira analizatore da bi primio podatke.



Slika 3: Shematski prikaz obrnutog prosljeđivanja

Obrnuto prosljeđivanje inicira se pokretanjem "glavnog" managera uz opciju *--child-managers «x.x.x.x»* u naredbenom retku ili zapisivanjem slijedeće linije u konfiguracijsku datoteku;

```
child-managers = "x.x.x.x"
```

Pri tome je x.x.x.x adresa "pomoćnog" managera. Kod ove mogućnosti također je dozvoljeno korištenje logičkih operatora kao i kod običnog prosljeđivanja.

4.3. Postavke prelude-lml alata

Prelude LML (eng. *Prelude Log Monitor Lackey*) je dio okruženja zadužen za nadzor dnevničkih zapisa. On može nadzirati zapise koje je kreirao *syslog* servis, ali može simulirati i vlastiti *syslog* poslužitelj. Neke od platformi koje mogu generirati dnevničke zapise korištenjem *syslog* servisa su:

- UNIX sustavi,
- mrežni razdjelnici i koncentratori,
- vatrozidi,
- pisači i
- Windows NT/2K/XP uz korištenje dodatnih alata (primjerice Ntsyslog).

Postavljanjem prelude-lml alata u mrežno okruženje i prilagodbom postavki ostalih računala tako da svoje dnevničke zapise šalju na mrežni *syslog* servis, moguće je nadzirati zapise cijele mreže s jednog mjesta.

Prelude-lml ima sustav dodataka koji obavljaju partikularne zadatke vezane uz analizu i nadzor dnevničkih zapisa. Jedan od tih dodataka je Pcre, a on implementira mehanizam regularnih izraza temeljen na PCRE (eng. *Perl Compatible Regular Expression*) biblioteci. Njime je iz skupa svih pristiglih zapisa moguće izdvojiti one koji zadovoljavaju određeni skup regularnih izraza. Čak štoviše izrađeni su i skupovi regularnih izraza koji izdvajaju neke uobičajene vrste zapisa. Neki od njih su:

- Cisco PIX,
- Cisco router,
- Cisco VPN concentrator,
- Clam antivirus,
- GRSecurity,
- Netfilter,
- Postfix,
- ProFTPd,
- SELinux,
- PAM,
- Sendmail,
- Squid proxy,
- Open SSH,

- Exim i
- Oracle.

Kako bi prelude-lml obavljao određenu funkciju, obično je potrebno definirati neke njegove postavke. Pri tome je bitno uočiti da prelude-lml sadrži pravila za velik raspon uređaja, od kojih se mnogi ne nalaze u svakoj mreži. Svaki od skupova pravila koji nije potreban, a ostane uključen dodatno opterećuje računalo na kome prelude-lml radi. Najjednostavniji način za poboljšanje efikasnosti rada prelude-lml alata je isključivanje nepotrebnih skupova pravila. Pravila je moguće isključiti na dva mjesta:

- /etc/prelude-lml/ruleset/pcre.rules
- /etc/prelude-lml/ruleset/single.rules

5. Zaključak

Prelude IDS je kvalitetno okruženje za praćenje rada svih sigurnosnih programa na računalu ili u mreži. Svojom mogućnošću nadzora cjelokupne mreže s jednog mjesta uvelike olakšava posao administratorima, smanjujući vrijeme potrebno za pregled velikog broja dnevničkih zapisa te im na taj način ostavljajući više vremena za aktivnu prevenciju i poboljšanje sigurnosti sustava. Među svojstvima sustava ističu se jednostavnost dodavanja novih senzora te mogućnost razdvajanja podataka iz odvojenih mreža uz njihovu istovremenu centralizaciju.

Korištenjem Prelude IDS-a vrlo je lako postići redundanciju pri pohrani podataka bilo pohranom na različite diskove jednog računala, bilo pohranom na različita računala u mreži ili čak na različita računala na različitim mrežama.

Jedan od većih nedostataka uočenih kod besplatne inačice Prelude IDS-a je nepostojanje dodataka za informiranje administratora o kritičnim sigurnosnim događajima.

Unatoč ovom relativno velikom nedostatku Prelude IDS je alat koji pronalazi svoju primjenu u velikom broju različitih okruženja.

6. Reference

[1] – Opis IDMEF standarda, http://tools.ietf.org/rfc/rfc4765.txt, travanj 2007.
[2] – Prelude IDS-a, http://www.prelude-ids.org/spip.php?rubrique6, travanj 2007.
[3] – CARNet CERT, http://www.cert.hr/documents.php?id=61, travanj 2007.
[4] – CARNet CERT, http://www.cert.hr/documents.php?id=31, travanj 2007.
[5] – Cheetah template engine, http://cheetahtemplate.org/, travanj 2007.