HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

OSSEC HIDS

CCERT-PUBDOC-2008-03-222

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

Sustavi za otkrivanje neovlaštenog upada (eng. *Intrusion Detection Systems* - IDS) namijenjeni su uočavanju neuobičajenih i/ili nedozvoljenih aktivnosti na računalnim sustavima. Neovlašteni upadi otkrivaju se uočavanjem obrazaca zlonamjernih radnji koje mogu ugroziti sigurnost napadnutog računala. Neke od tih radnji su mrežni napadi usmjereni na pojedine ranjive usluge, napadi posebno oblikovanim podatkovnim strukturama (eng. *data driven attack*) te pokušaji neovlaštenog stjecanja povišenih korisničkih ovlasti, neovlaštene prijave u sustav ili neovlaštenog pristupa potencijalno osjetljivim podacima.

Među IDS sustavima osnovna je podjela na NIDS (eng. *Network-based IDS*) sustave za detekciju neovlaštenih aktivnosti u mreži te HIDS (eng. *Host-based IDS*) sustave za detekciju neovlaštenih aktivnosti na računalu – lokalnom sustavu.

Ovaj dokument opisuje jedno od postojećih lokalnih IDS rješenja, alat OSSEC HIDS. Prezentirane su neke od mogućnosti alata, načini korištenja te su dane upute za samu instalaciju, kao i osvrt na postojeće konkurentske proizvode. Osim toga, dokument donosi i kratku sistematiku sustava za detekciju neovlaštenih upada.

2. Sustavi za detekciju neovlaštenog pristupa

IDS (eng. *Intrusion Detection System*) sustavi, odnosno sustavi za detekciju neovlaštenog pristupa koriste se za otkrivanje različitih tipova napada, koji mogu kompromitirati sigurnost računalnog sustava. U takve se napade ubrajaju primjerice napadi na ranjive mrežne servise, napadi na aplikacije i tzv. "*host based*" napadi, u koje se ubraja povećanje ovlasti, neovlaštena prijava i pristup osjetljivim informacijama te napadi korištenjem zlonamjernih programa (eng. *malware*), kao što su virusi, trojanski konji i crvi.

IDS sustavi sastoje se od nekoliko komponenti:

- senzora koji otkrivaju sigurnosne prijetnje,
- upravljačke ploče koja služi za praćenje događaja i uzbuna te kontrolu senzora i
- središnjeg uređaja koji događaje zabilježene senzorima sprema u bazu podataka te, uz pomoć sustava pravila, generira uzbune (eng. *alert*) na temelju uočenih događaja.

U jednostavnim implementacijama IDS sustava, sve tri komponente ugrađene su u jedan uređaj.

Postoji nekoliko vrsta sustava za detekciju upada:

- NIDS (eng. *network intrusion detection system*) – neovisna platforma koja identificira upade provjerom mrežnog prometa i praćenjem većeg broja računala. Takvi sustavi dobivaju pristup mrežnom prometu povezujući se na parični obnavljač (eng. *hub*) ili komutator (eng. *switch*), koji su konfigurirani za preslikavanje priključaka (eng. *port mirroring* – kopiranje mrežnih paketa s jednog priključka na drugi) ili sl. Primjer ovakvog sustava je alat *Snort.*
- PIDS (eng. *protocol-based intrusion detection system*) – radi se o sustavu ili agentu koji se obično instalira na poslužitelju te prati i analizira komunikacijski protokol (primjerice HTTP – eng. *Hypertext Transfer Protocol*) između povezanih uređaja (računala ili sustava).
- APIDS (eng. *application protocol-based intrusion detection system*) – radi se o sustavu ili agentu koji obično između grupe poslužitelja prati i analizira komunikaciju specifičnim aplikacijskim protokolima. Npr. za web poslužitelj s bazom podataka pratio bi se SQL protokol.
- HIDS (eng. *host-based intrusion detection system*) – radi se o agentu vezanom uz jedno računalo. On identificira upade pomoću analize sistemskih poziva, aplikacijskih zapisnika, izmjena datotečnih sustava i drugih računalnih aktivnosti i stanja. Primjer takvog sustava je upravo OSSEC HIDS.

Osim spomenutih, postoje i sustavi koji kombiniraju nekoliko prethodno opisanih pristupa. Također, postoji i podjela na pasivne i reaktivne sustave – pasivni sustavi uoče potencijalnu opasnost, zabilježe odgovarajuće informacije i generiraju uzbunu, dok reaktivni sustavi, koji se često nazivaju i IPS (eng. *intrusion prevention system*), reagiraju na uočeni problem resetiranjem veze, reprogramiranjem vatrozida i sl.

2.1. Općenito o OSSEC HIDS alatu

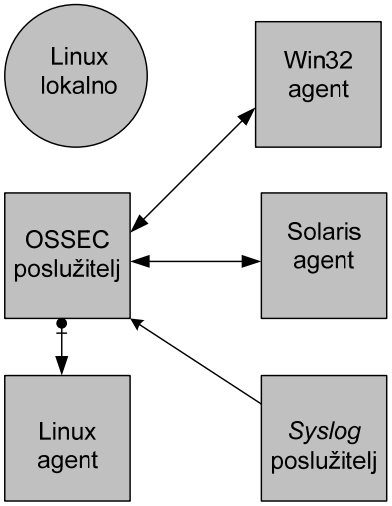
OSSEC HIDS je besplatan alat, otvorenog programskog koda, namijenjen detekciji neovlaštenog pristupa. Provodi analizu dnevničkih zapisa (eng. *log*) i provjeru integriteta datoteka, prati Windows *registry* zapisnik, detektira zlonamjerne programe (npr. *rootkit* programi), generira uzbune i obavlja unaprijed definirane akcije. Može se koristiti na jednom računalu ili više njih (npr. u slučaju administracije nekoliko sustava), pri čemu se jedno računalo odabire za OSSEC poslužitelj, dok su druga računala agenti, koji uočene događaje prosljeđuju poslužitelju za daljnju analizu. Na taj je način moguće pratiti nekoliko sustava iz jedne središnje točke.

OSSEC je namijenjen većini popularnih operacijskih sustava, kao što su Linux (Slackware, Ubuntu, Red Hat, Suse, Fedora, Debian), OpenBSD, FreeBSD, MacOS, Solaris i Windows (2000, XP i 2003).

3. Instalacija alata

3.1. Vrste instalacije

OSSEC je potrebno instalirati na svako računalo koje se želi pratiti. U slučaju instalacije alata na samo jedno računalo (osobno računalo ili malen poslužitelj), potrebno je odabrati lokalnu instalaciju. Ovaj je tip instalacije jednostavniji i prilagođen samo jednom sustavu. Ako je potrebno pratiti sigurnost nekoliko sustava, jedno se računalo odabire za OSSEC poslužitelj i na njemu se provede odgovarajuća (*server*) instalacija. Na ostalim računalima provodi se tzv. *agent* instalacija, što tada omogućava središnje upravljanje svim sustavima – agenti prosljeđuju zabilježene prijetnje poslužitelju, koji ih analizira i, ako je potrebno, generira uzbune. Tako su sva pravila vezana uz detekciju neželjenog pristupa na jednom mjestu, što omogućava lakšu administraciju i konfiguraciju.



Slika 1. Arhitektura OSSEC HIDS zaštite

3.2. Redoslijed instalacije

Redoslijed kojim se instalira bitan je samo u slučaju *agent/server* instalacije, dakle instalacije na nekoliko računala istovremeno. U tom je slučaju potrebno prvo instalirati alat na odabrani poslužitelj, gdje se također obavlja autorizacija svih agenata s kojima poslužitelj planira komunicirati – slati i primati informacije, događaje i zapise. Ovaj je postupak jednostavan i potrebno ga je provesti samo jednom, a detaljnije će biti opisan u nastavku dokumenta.

Nakon instalacije alata na poslužitelju, odabire se *agent* tip instalacije i provodi se na svim ostalim računalima. Ovaj je tip instalacije puno jednostavniji i u pravilu zahtjeva samo IP adresu poslužitelja. Svako računalo agent mora imati autentikacijski dokument, koji se generira prilikom prethodno spomenute autorizacije agenata.

3.3. Upute za instalaciju

U nastavku će biti opisan postupak instalacije OSSEC alata na Ubuntu Linux operacijskom sustavu, pri čemu će detaljnije biti opisan postupak lokalne instalacije (na samo jedno računalo), a ukratko će biti spomenute i razlike koje postoje kod poslužitelj/agent instalacije. Isto tako, za Windows operacijske sustave postoji samo mogućnost instalacije agenta, što znači da je potrebno na Unix/Linux platformi odrediti računalo poslužitelj, koji tada komunicira s agentom na Windows sustavu.

Za početak, potrebno je preuzeti najnoviju inačicu paketa (u trenutku pisanja ovog dokumenta aktualna inačica je 1.4) te instalirati nekoliko komponenti za potrebe kasnije kompilacije. Sljedećih nekoliko naredbi obavlja spomenute zadatke:

```
sudo apt-get install build-essentials
cd ~
mkdir src
cd src
wget http://www.ossec.net/files/ossec-hids-1.4.tar.gz
```

Sljedeći je korak raspakiravanje preuzete arhive:

```
tar -zxvf ossec-hids-1.4.tar.gz
cd ossec-hids-1.4
```

Pokretanje instalacijske skripte:

```
sudo -s
./install.sh
```

Nakon toga slijedi odabir jezika instalacije, upozorenje o potrebnom C prevodiocu i ispis nekih općenitih informacija o sustavu (inačica jezgre, trenutno prijavljeni korisnik, naziv računala).
Budući da je ovo primjer lokalne instalacije, u sljedećem se koraku odabire taj tip te se prihvaća podrazumijevano odredište instalacije:

```
1- What kind of installation do you want (server, agent,
local or help)? local <enter>

- Choose where to install the OSSEC HIDS [/var(ossec]:
<enter>
```

Slijedi odabir različitih opcija izvješćivanja (primanje obavijesti putem elektroničke pošte, omogućavanje provjere integriteta datoteka, detekcije zlonamjernih programa i sl.). Korisnicima koji nisu sigurni u odgovore, preporuča se odabir odgovora DA (eng. *Yes*), radi postizanja veće sigurnosti sustava.
Nakon odabranih željenih opcija, u sljedećem koraku obavlja se konfiguracija alata, na temelju korisničkih odgovora na postavljena pitanja:

```
3.6- Setting the configuration to analyze the following logs:
    -- /var/log/messages
    -- /var/log/auth.log
    -- /var/log/syslog
    -- /var/log/mail.info
    -- /var/log/apache2/error.log (apache log)
    -- /var/log/apache2/access.log (apache log)

 - If you want to monitor any other file, just change
   the ossec.conf and add a new localfile entry.
   Any questions about the configuration can be answered
   by visiting us online at http://www.ossec.net .


   --- Press ENTER to continue ---
```

Slijedi kompilacija, nakon čega je moguće pokrenuti OSSEC sljedećom naredbom:

```
/var/ossec/bin/ossec-control start
```

Ako je odabrana konfiguracija zaštite koja uključuje poslužitelj, potrebno je povesti računa o nekim dodatnim elementima. Npr., ako postoji vatrozid između poslužitelja i agenata, potrebno je u njemu otvoriti priključak 1514 (UDP). Osim toga treba obratiti pažnju na prethodno spomenutu autorizaciju agenata. Za svakog agenta, radi sigurne komunikacije s poslužiteljem, potrebno je generirati autentikacijski ključ na poslužitelju te ga prenijeti u odgovarajućem trenutku na računalo agent. Opisani se postupak provodi u nekoliko koraka:
Prvo se agenti dodaju na poslužitelj. To se postiže pokretanjem naredbe "manage_agents", nakon čega se navodi IP adresa agenta te željeno ime za nj.

```
(server)# /var/ossec/bin/manage_agents

****************************************
* OSSEC HIDS v1.4 Agent manager.       *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your actions: A,E,R or Q: a

- Adding a new agent (use 'q' to return to main menu).
  Please provide the following:
    * A name for the new agent: ime_agenta
    * The IP Address for the new agent: IP_adresa_agenta
* An ID for the new agent[001]:
Agent information:
    ID:001
    Name:ime_agenta
    IP Address:IP_adresa_agenta

Confirm adding it?(y/n): y
Added.
```

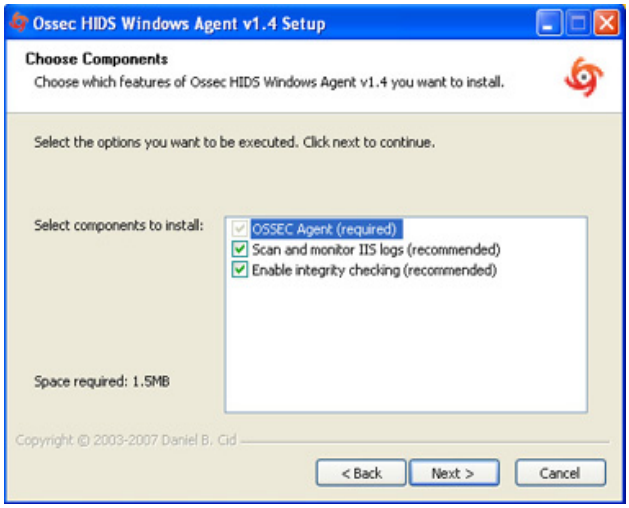
U drugom koraku izdvaja se autentikacijski ključ s poslužitelja i prenosi se agentu. Za to je u prethodno opisanom postupku potrebno odabrati opciju "E" i upisati ID agenta. Ključ se tada ispisuje na ekranu i moguće ga je jednostavno kopirati na odgovarajuće mjesto u računalu agent.

```
Choose your actions: A,E,R or Q: e

Available agents:
    ID: 001, Name: ime_prvog_agenta, IP_adresa1
    ID: 002, Name: ime_drugog_agenta, IP_adresa2
Provide the ID of the agent you want to extract the key: 001

Agent key information for '001' is:
CDAxIGxpbnX4MSAxOTIuMTY4LjAuMzIgOWM5MENlYzNXXXYYYZZZZZ==

** Press ENTER to continue
```

Kopiranje ključa u računalo agent obavlja se pokretanjem iste naredbe (*manage_agents*) koja, međutim, u ovom slučaju nudi različite opcije:

```
(agent)# /var/ossec/bin/manage_agents

****************************************
* OSSEC HIDS v1.4 Agent manager.       *
* The following options are available: *
****************************************
   (I)mport key for the server (I).
   (Q)uit.
   Choose your actions: I or Q: i

* Provide the Key generated from the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here:
CDAxIGxpbnX4MSAxOTIuMTY4LjAuMzIgOWM5MENlYzNXXXYYYZZZZZ==

Agent information:
    ID:001
    Name:ime_agenta
    IP Address:IP_adresa_agenta

Confirm adding it?(y/n): y

Added.
** Press ENTER to continue.

****************************************
* OSSEC HIDS v0.8 Agent manager.       *
* The following options are available: *
****************************************
    (I)mport key for the server (I).
    (Q)uit.
Choose your actions: I or Q: q

manage_agents: Exiting ..
```

Isti se postupak provodi za sve agente. Nakon uspješno obavljenih prethodnih nekoliko koraka, moguće je pokrenuti OSSEC na poslužitelju, a zatim na svim agentima.
Na Windows sustavima omogućena je samo instalacija agenta, dok poslužitelj, koji će analizirati informacije primljene od agenata, i dalje mora biti instaliran na Unix/Linux sustavu. Instalacija se provodi jednostavnim pokretanjem auto-instalacijskog alata, koji zahtjeva unošenje autentikacijskog ključa generiranog na poslužitelju.



Slika 2. Odabir mogućnosti kod instalacije Windows agenta

Slika 3. Unošenje IP adrese poslužitelja i autentikacijskog ključa

4. Konfiguracija i korištenje alata

Konfiguracija OSSEC HIDS alata provodi se unutar *ossec.conf* datoteke (koja se nalazi u */var/ossec/etc/* direktoriju). Radi se o XML (eng. *eXtensibla Markup Language*) datoteci kojoj je korijenski element *ossec_config*. Korijenski elemnt može sadržavati jednu ili više sljedećih opcija:

- *global* –podrazumijevane opcije cijelog sustava,
- *email_alerts* – opcije slanja uzbuna putem elektroničke pošte,
- *rules* – popis pravila koja se žele uključiti,
- *syscheck* – konfiguracija vezana uz provjeru integriteta,
- *rootcheck* – konfiguracija vezana uz detekciju zlonamjernih programa,
- *alerts* – mogućnosti vezane uz zapisnike uzbuna i slanje putem elektroničke pošte,
- *localfile* – opcije vezane uz zapisnike (eng. *log*) koje je potrebno pratiti,
- *remote* – konfiguracija vezana uz udaljene veze,
- *client* – opcije koje je moguće izmijeniti kod agenata,
- *database_output* – opcije izlaznih informacija baze podataka,
- *command* – konfiguracija aktivnog odgovora (reakcije na neovlaštene radnje, eng. *active response*) i
- *active-response* – također konfiguracija reakcije sustava.

Neke od spomenutih opcija moguće je koristiti na samo određenim tipovima instalacije, kako slijedi:

- poslužitelj – *global, email_alerts, rules, syscheck, rootcheck, alerts, localfile, remote, command* i *active-response,*
- agent - *client, syscheck, rootcheck* i *localfile* te
- lokalna instalacija - *global, email_alerts, rules, syscheck, rootcheck, alerts, localfile, command* i *active-response.*

4.1. Opis konfiguracijskih mogućnosti

4.1.1. Globalne opcije

Neke od globalnih opcija su sljedeće:

- omogućavanje slanja uzbuna (eng. *alert*) putem elektroničke pošte te postavljanje izvora i odredišta takve komunikacije,
- odabir SMTP poslužitelja,
- postavljanje maksimalnog broja poruka elektroničke pošte koje se šalju po satu,
- postavljanje različitih razina uzbune za pojedine prijetnje,
- popis IP adresa koje ne smiju biti blokirane reakcijama na uzbune i dr.

4.1.2. Slanje uzbuna putem elektroničke pošte

Kod slanja uzbuna putem elektroničke pošte, moguće je odabrati sljedeće opcije:

- odabir primatelja pošte,
- maksimalna razina uzbuna koje se šalju elektroničkom poštom,
- postavljanje grupa kojima uzbune moraju pripadati, kako bi bile proslijeđene,
- postavljanje lokacija kojima uzbune moraju odgovarati, kako bi bile proslijeđene,
- specifikacija formata poruke,
- postavljanje opcije za slanje elektroničke pošte bez odgode i
- postavljanje opcije za individualno slanje poruke, bez pripadnosti određenoj grupi.

4.1.3. Pravila

U slučaju ovog elementa, moguće je odabrati samo dodavanje pravila koja poslužitelj koristi prilikom analize pojedinih događaja. Pravila moraju biti popisana u datoteci */var/ossec/rules*.

4.1.4. *Syscheck* opcije

Unutar ovog elementa, moguće je iskoristiti razne opcije. Neke od njih su:

- dodavanje direktorija koje je potrebno pratiti ili specifikacija obavljanja svih mogućih provjera integriteta,
- specifikacija korištenja MD5 metode prilikom provjere integriteta datoteka,
- provjera promjena veličine, vlasnika i grupa kojima datoteke pripadaju te promjena ovlasti nad datotekama,
- popis datoteka ili direktorija koje je potrebno ignorirati,
- frekvencija provjere integriteta (zadana u sekundama),
- specifikacija ignoriranja datoteka koje se često mijenjaju,
- specifikacija uzbuna prilikom kreiranja novih datoteka,
- provjera unosa u Windows *registry* zapisnik i
- popis unosa u *registry* zapisnik koje je potrebno ignorirati.

4.1.5. Detekcija zlonamjernih programa

Opcije koje je moguće zadati kod detekcije neželjenih programa su sljedeće:

- odabir datoteke koja sadrži popis tzv. *rootkit* programa,
- odabir datoteke koja sadrži popis trojanskih konja,

- odabir opcije za pretraživanje čitavog sustava (što može dovesti do nekih lažno-pozitivnih grešaka, odnosno otkrivanja prijetnji koje ne postoje),
- postavljanje učestalosti obavljanja ovakvih provjera i
- onemogućavanje detekcije zlonamjernih programa.

4.1.6. Opcije generiranja uzbuna

Moguće je postaviti sljedeće vrijednosti:

- minimalnu razinu uzbune za slanje putem elektroničke pošte i
- minimalnu razinu uzbune za spremanje poruka u zapisnik (eng. *log messages*).

4.1.7. Opcije lokalnih datoteka

Moguće je specificirati:

- lokaciju zapisnika (eng. *log*) kojeg je potrebno provjeravati i
- format zapisnika koji će se čitati (*syslog, snort-full, snort-fast, squid, iis, eventlog,nmapg* ili *apache*).

4.1.8. Opcije udaljenih veza

Nekoliko je mogućnosti kod izmjene postavki udaljenih veza:

- specifikacija tipa veze koja će biti omogućena (sigurna ili korištenjem *syslog* servisa),
- odabir priključka na kojem se osluškuje,
- popis IP adresa računala koja smiju/ne smiju slati *syslog* poruke poslužitelju te
- odabir lokalnih IP adresa s kojima se moguće povezati.

4.1.9. Opcije klijenta

Unutar spomenutog elementa, moguće je specificirati:

- IP adresu poslužitelja za analizu,
- ime računala koje se koristi kao OSSEC poslužitelj i
- priključak za komunikaciju s poslužiteljem (podrazumijevana vrijednost je 1514).

4.1.10. Izlaz u bazu podataka

Sekcija opisuje bazu podataka koja čuva informacije o uočenim problemima. Moguće je specificirati slijedeće parametre:

- IP adresu poslužitelja baze podataka,
- korisničko ime i zaporku za pristup bazi,
- naziv baze za spremanje uzbuna i
- tip baze podataka (*MySQL* ili *PostgreSQL*).

4.1.11. Reakcija na prijetnje (eng. *Active response*)

Radi se o opciji alata, koja korisnicima omogućava automatsko izvođenje naredbi ili nekog drugog tipa reakcije na određeni događaj. Naredbe je moguće izvoditi bilo na agentima, bilo na poslužitelju. Postoji niz prednosti, ali i rizika kod omogućavanja ove opcije. Prednost je činjenica da je uključivanjem ove opcije moguće neposredno nakon detekcije napada provesti određenu akciju. Posebno su dobro razvijene metode obrane od napada skeniranjem priključaka (eng. *port scan*), napada grubom silom (eng. *brute force attack*) i drugih načina neovlaštenog prikupljanja informacija. Rizik je mogućnost detekcije tzv. lažnih pozitivnih prijetnji, odnosno prijetnji koje ne postoje, a moguće je i da napadač otkrije korištenje ove metode te ju pokuša iskoristiti za izvođenje nekog oblika napada uskraćivanja usluga (eng. *Denial of Service*).
Konfiguracija spomenute opcije provodi se u dva dijela – kreiranjem naredbi koje će se izvoditi nakon detekcije određene prijetnje te povezivanjem tih naredbi s pravilima i događajima.

4.2. Analiza zapisnika i međuovisnost pravila

Pravila za analizu događaja generiraju se u XML datoteku, u kojoj se može specificirati točno što je potrebno izvršiti kod primitka obavijesti o određenoj prijetnji. Neke od mogućnosti koje nude takva pravila su sljedeće:

- povezivanje s prethodno definiranim pravilima, pri čemu je moguće specificirati i ovisnost o određenim grupama pravila,
- kreiranje grupa na temelju ozbiljnosti problema, korisničkih imena, identifikacijskih atributa, izvorišnih IP adresa, i sl.,
- specificiranje učestalosti pojave određenog pravila (događaja vezanog uz pravilo) prije generiranja uzbune te
- korištenje već ugrađenih pravila, vezanih uz usporedbu IDS (eng. *Intrusion Detection System*) napada, vatrozida i zapisnika temeljenih na webu, uz detekciju neželjenih poruka elektroničke pošte, pogrešne primjene posrednih (eng. *proxy*) poslužitelja, napada grubom silom, napada uskraćivanja usluga, itd.

5. Usporedba s konkurencijom

Osim OSSEC HIDS alata, neki od poznatijih HIDS sustava su:

- Tripwire,
- Samhain,
- Osiris i
- Tiger.

5.1. Tripwire

Tripwire je programski paket otvorenog koda, namijenjen očuvanju sigurnosti programske podrške i provjeri integriteta podataka. Funkcionalnost temelji na praćenju specifičnih promjena nad datotekama i generiranju uzbuna uslijed njihove pojave. Prilikom prvog pokretanja i inicijalizacije, pretražuje čitav datotečni sustav i informacije o svim datotekama sprema u bazu podataka. Ponovnim pokretanjem provodi se pretraživanje istih datoteka i usporedba rezultata s onima zapisanim u bazi te se sve uočene izmjene priopćuju korisniku. Za usporedbu datoteka nije potrebno spremati sadržaj čitave datoteke u bazu, već se u tu svrhu koriste kriptografske *hash* funkcije. Osim detekcije neovlaštenog pristupa, omogućava i osiguranje integriteta, praćenje izmjena i poštivanje sigurnosne politike. Sličnu funkcionalnost pruža još nekolicina paketa, među kojima je najpoznatiji programski paket AIDE. Tripwire je namijenjen Linux i Unix operacijskim sustavima.

5.2. Samhain

Samhain je sustav za detekciju neovlaštenog pristupa, otvorenog koda, namijenjen Unix/Linux (*BSD, Solaris 2.x, AIX 5.x, AIX 4.x, HP-UX 10.20, HP-UX 11, Unixware 7.1.0, Alpha/True64, Mac OS X i većina Linux sustava) i Windows (2000 i XP) operacijskim sustavima. Omogućava provjeru integriteta datoteka, detekciju zlonamjernih programa (eng. *rootkit*), te detekciju skeniranja priključaka, zlonamjernih SUID (eng. *set user id*) izvršnih datoteka i skrivenih procesa. Pomoću Samhain alata, moguće je pratiti aktivnosti jednog ili većeg broja računala koji mogu imati različite operacijske sustave.

Informacije o prijetnjama spremaju se u bazu podataka. Podržane su *Oracle, MySql* i *PostgreSQL* baze. Kao poseban paket, nudi se i upravljačka ploča temeljena na web sučelju (*Beltane*), koja također omogućava praćenje aktivnosti klijenata i poslužitelja, pregled klijentskih izvještaja i nadogradnju baze podataka.

5.3. Osiris

Osiris je alat za praćenje integriteta računalnog sustava, koji svoju funkcionalnost temelji na praćenju jednog ili više računala i bilježenju uočenih promjena, koje mogu biti posljedica neovlaštenog upada ili kompromitacije sustava. Alat generira zapisnike s detaljnim informacijama o izmjenama učinjenim nad datotečnim sustavom, korisničkim ili grupnim listama, raznim jezgrinim modulima i sl. Može se

konfigurirati za slanje generiranih zapisnika administratoru sustava, preko poruka elektroničke pošte. Računala se pretražuju periodički i moguće je sačuvati generirane rezultate za kasnija istraživanja i usporedbe. Uz pomoć Osiris alata, administratori su u svakom trenutku obaviješteni o mogućim napadima i/ili pronađenim trojanskim konjima. Osiris koristi OpenSSL (eng. *Secure Sockets Layer*) metodu za enkripciju i autentikaciju svih komponenti.

5.4. Tiger

Tiger je programski paket namijenjen Unix operacijskim sustavima, a koristi se za sigurnosnu kontrolu i detekciju neovlaštenog pristupa. Prvotno je razvijen u sklopu A&M kampusa teksaškog sveučilišta, a njegov razvoj prestaje 1994. godine. 2002. godine javlja se nova inačica paketa, 3.0, koja nudi brojne nove mogućnosti i podršku za novije inačice operacijskih sustava. Podržava većinu Unix platformi i besplatan je, a trenutno je aktivna inačica 3.2.2. Može se koristiti kao dopuna prethodno spomenutim alatima, a osigurava i okruženje u kojem svi alati mogu raditi zajedno. Funkcionalnost mu se ne temelji na provjeri zapisnika i integriteta podataka, već na provjeri konfiguracije i stanja sustava. Primjer jedne od mogućnosti koje Tiger nudi jest modul *check findelete*, namijenjen detekciji mrežnih poslužitelja koji koriste obrisane datoteke, a pokrenuti su na sustavu. Tiger se razvija s namjerom da jednog dana zamijeni mnoštvo sigurnosnih alata koji se danas koriste na Linux/*BSD sustavima.

6. Zaključak

Sustavi za otkrivanje neovlaštenih upada predstavljaju značajnu sigurnosnu komponentu svakog računalnog sustava, uz ostale sustave kao što su vatrozid i antivirusni alati. Bez obzira na način otkrivanja upada svi IDS sustavi mogu se podijeliti na lokalne i mrežne sustave. Obje navedene skupine imaju karakteristične prednosti i nedostatke te odluka o korištenju mrežnog ili lokalnog sustava ovisi prije svega o okruženju i postavljenim zahtjevima. Ipak, poželjno je implementirati oba sustava kako bi se njihovim komplementarnim djelovanjem mogućnost nezamijećenog upada svela na minimum.

OSSEC HIDS predstavlja jedno od rješenja namijenjenih upravo lokalnoj zaštiti. On ni u kom slučaju nije savršen alat jer pojedini elemeti njegove funkcionalnosti uključuju i određene rizike. Unatoč tome, predstavlja dobar korak naprijed u postizanju većeg stupnja zaštite. Moguće ga je primijeniti za zaštitu pojedinog računala ili cijele računalne mreže, pri čemu podržava rad na većini popularnih platformi. Jednostavno ga je instalirati i prilagoditi, a sadrži i velik skup ugrađenih pravila za poznate probleme. Dodatno ga je moguće koristiti i za izgradnju vlastitih sigurnosnih rješenja.

Sve spomenuto potvrđuje kako se radi o moćnom alatu koga, ne samo da vrijedi iskoristiti za postizanje bolje zaštite sustava, nego ga je moguće upotrijebiti i kao dobru podlogu za daljnju nadogradnju i razvoj novih, još boljih rješenja.

7. Reference

[1] OSSEC, http://www.ossec.net/en/home.html, ožujak 2008.

[2] OSSEC Manual, http://www.ossec.net/main/manual/, ožujak 2008.

[3] Intrusion detection system, http://en.wikipedia.org/wiki/Intrusion-detection_system, ožujak 2008.

[4] Introduction to Intrusion Detection Systems, http://netsecurity.about.com/cs/hackertools/a/aa030504.htm, ožujak 2008.

[5] OSSEC, Open Source HIDS, http://www.ossec.net/ossec-docs/OSSEC-Presentation-mw.swf, ožujak 2008.

[6] Howto setup OSSEC HIDS on your Ubuntu box, http://ubuntuforums.org/showthread.php?t=213445, ožujak 2008.

[7] The Samhain file integrity / host-based intrusion detection system, http://la-samhna.de/samhain/index.html, ožujak 2008.

[8] Osiris, http://osiris.shmoo.com/index.html, ožujak 2008.

[9] Tiger UNIX security tool – Summary, http://savannah.nongnu.org/projects/tiger/, ožujak 2008.

[10] Open Source Tripwire, http://en.wikipedia.org/wiki/Tripwire_%28software%29, ožujak 2008.