HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Postavljanje IDS-a sa Snort paketom

CCERT-PUBDOC-2001-05-03

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

Veliki rast i popularnost Interneta i pritisak od strane različitih tvrtki otvara novi aspekt računalne sigurnosti. Međutim, budući da Internet raste eksponencijalnom brzinom, tako isto rastu i potencijalni sigurnosni problemi. Rješenja koja se svakodnevno pružaju obično su u vidu postavljanja vatrozidnih sustava i paketnih filtera.

Danas, međutim, ovakva rješenja više nisu dovoljna. Vatrozidni sustavi nisu u stanju otkriti prijenos različitih malicioznih programa, specijalno u slučajevima kada se ne koristi nekakva inačica proxy vatrozidnog rješenja. U tu svrhu postavljaju se alati za detekciju neovlaštenih aktivnosti (eng. *Intrusion Detection System*) kao dodatni dio sigurnosne arhitekture mreže.

U ovom dokumentu opisane su osnove današnjih sustava za otkrivanje neovlaštenih aktivnosti korisnika. Opisan je i postupak implementiranja općenitog sigurnosnog sustava korištenjem Snort programskog paketa, sa uputama za postavljanje sigurnosnih logova i centraliziranog logiranje preko `syslog`-a.

1.1. Terminologija

Ovdje je objašnjena terminologija i neki osnovni koncepti korišteni u ovom dokumentu. Prilikom implementacije ovakvog IDS sustava (i IDS sustava općenito), potrebno je dobro znanje TCP/IP stoga. Osim toga, najčešće korišteni paket za logiranje mrežnog prometa je danas svakako `tcpdump`, tako da bi korisnici trebali biti upoznati sa načinom rada i izgledom logova ovog paketa.

- ID potpis – Potpis može predstavljati specijalno TCP stanje kao što je npr. postavka SYN ili RST zastavice u jednom paketu, specijalni okteti u zaglavlju ili određeni slijed okteta u tijelu paketa.
- Lažni alarmi, lažno pozitivni, lažno negativni – Lažni alarmi nastaju kao rezultat ili pogrešne konfiguracije ili lažno pozitivnih detekcija. Lažno pozitivne detekcije nastaju kada ID sustav detektira mrežni promet koji izgleda jednako određenom potpisu. Ovakvi slučajevi obično nastaju prilikom pogrešne konfiguracije IDS alata ili zbog nepravilno postavljenih potpisa. Lažno negativne detekcije su zapravo one koje su IDS alatu promakle, opet ili zbog nepravilno postavljene konfiguracije IDS alata ili zbog nedovoljnog potpisa u bazi. Očigledno, lažno negativne detekcije neće biti prijavljene.
- Baza potpisa i incidenata – Ove baze su javno dostupne i sadrže potpise promatranih i dokumentiranih neovlaštenih aktivnosti korisnika. Snort, kao i drugi IDS alati, daje identifikacijski broj baze sa potpisima u kojoj se može naći više informacija o određenoj neovlaštenoj aktivnosti korisnika. Snort ima tablicu referenci baza podataka sa incidentima:

Sustav	Primjer	URL
IDS	IDS182	http://www.whitehats.com/IDS/182
CVE	CVE-2000-0138	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0138
Bugtraq	BugtraqID 1	http://www.securitfocus.com/vdb/bottom.html?vid=1
McAfee	McAfee 10225	http://www.securitfocus.com/vdb/bottom.html?vid=1

2. Pregled IDS sustava

Današnji IDS alati dijele se u dvije skupine:

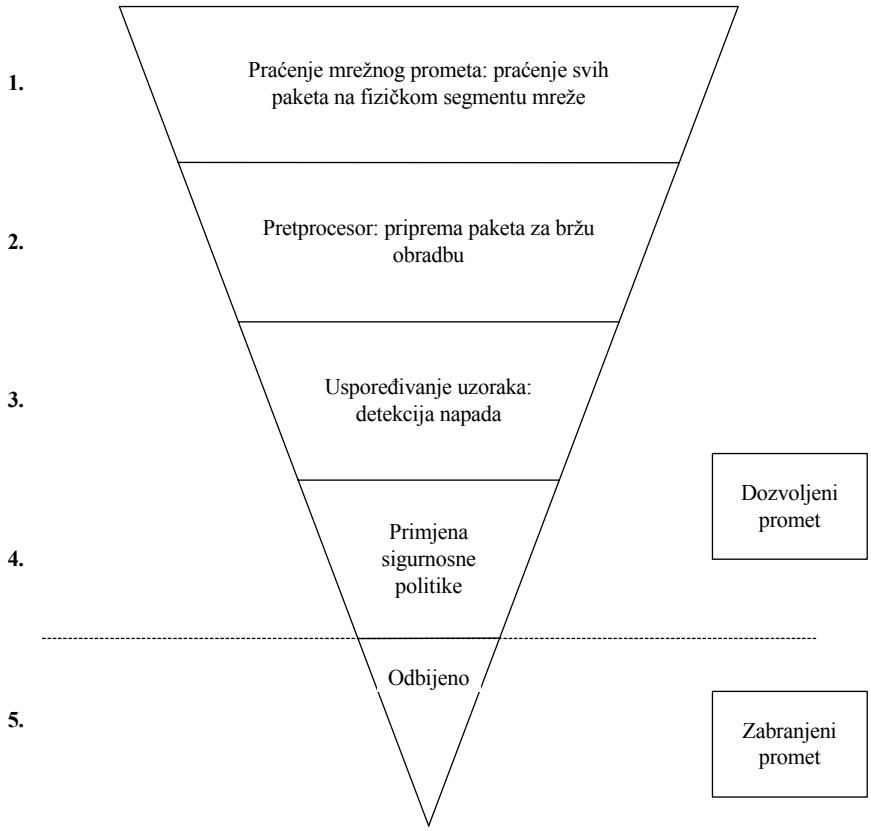
- računalno bazirani IDS sustavi (eng. Host based IDS)
- mrežni IDS sustavi (eng. *Network based IDS*)

Računalno bazirani IDS sustavi definiraju sigurnost na samom računalu. Ove komponente mogu imati različitu svrhu i uglavnom su dostupne za sve popularne, moderne, operacijske sustave. Za Unix

operacijske sustave mogu se pronaći sve vrste ovakvih alata, počevši od popularnog TripWire sustava za sigurnost korisničkog prostora, do alata poput kstat ili carbonite koji služe za nadgledavanje kernel prostora. Dodaci poput lomac, RSBAC ili selinux programskih paketa mogu stvoriti vrlo napredan računalno bazirani IDS sustav na GNU/Linux operacijskim sustavima.
Glavna namjena mrežnih IDS sustava je pregledavanje mrežnog prometa i uspoređivanje s određenim uzorcima. Ako je prihvaćen mrežni promet jednak određenom uzorku, odnosno potpisu, IDS će aktivirati alarm. Jedan primjer takvog IDS alata je Snort, koji je dostupan za velik broj popularnih operacijskih sustava. Snort je jedini napredni alat za otkrivanje neovlaštenih aktivnosti korisnika pod Open Source licencom koji se može mjeriti sa komercijalnim alatima poput NFS, Dragon ili ISS RealSecure.

2.1. Uvod u Snort

Snort je vrlo napredan alat za detekciju neovlaštenih aktivnosti korisnika koji je razvio Martin Roech uz pomoć libpcap biblioteke. Za kompletne mogućnosti Snort alata može se pogledati adresa priložena u referencama.
Slijedeći dijagram prikazuje način rada Snort-a kao alata za detekciju neovlaštenih aktivnosti korisnika. Način rada Snort-a opisan je u slijedećim poglavljima.



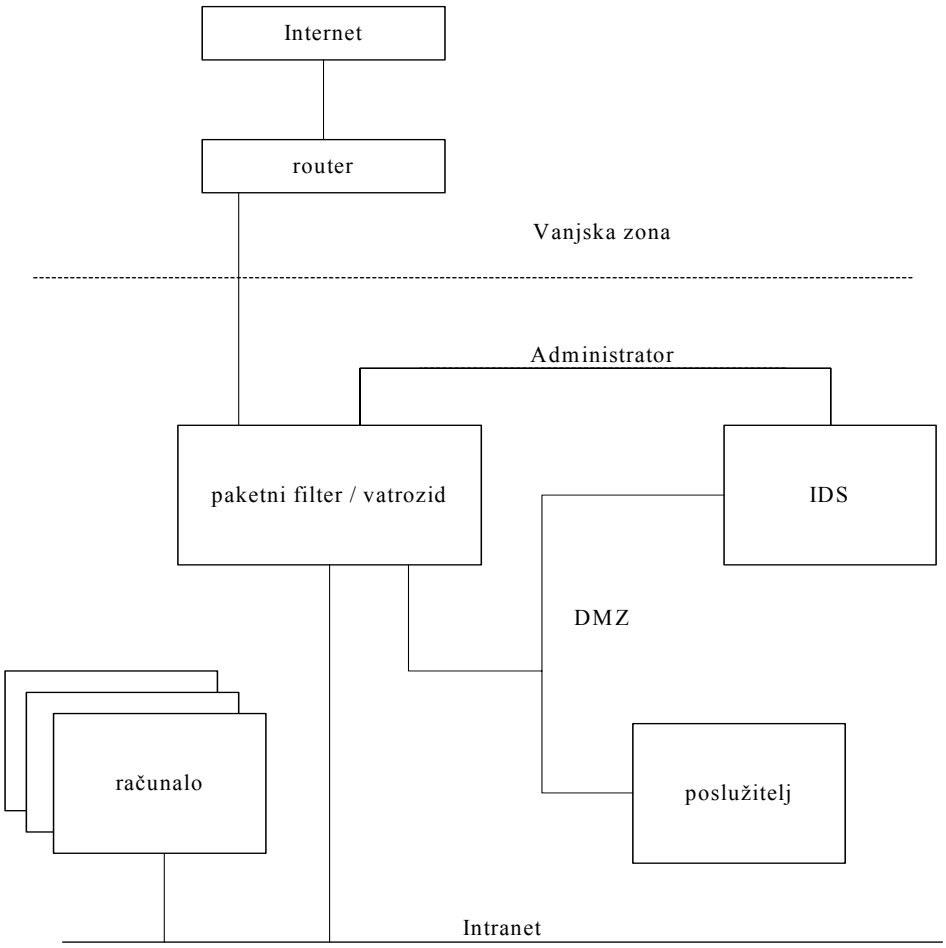
3. Postavljanje IDS alata

Prema prikazanoj shemi IDS alat je postavljen sa dva mrežna sučelja na svaku mrežu koja nije spojena na korporacijski intranet. Greška koju administratori često naprave je ta da se IDS alat sa dva (ili više) mrežnih sučelja tako postavlja da s jednim mrežnim sučeljem gleda na korporacijski intranet, dok je druga mrežna kartica spojena izravno na Internet čime je čak premošćen i vatrozid. Ovakva postavka računala sa IDS-om je, naravno, iznimno opasna budući da je korporacijski intranet potencijalno otvoren neovlaštenom korisniku preko računala sa IDS-om, bez obzira na implementirani vatrozid. Računalo sa IDS-om bi se po pravilu trebalo postavljati na svaku pod mrežu. Znači, svaka pod mreža

trebala bi imati posebno računalo sa IDS-om. U slučajevima kada pojedine pod mreže generiraju male količine prometa, zbog uštede je preporučljivo instalirati manji broj računala sa IDS-ovima koja onda imaju višestruke mrežne kartice. Ovo se može primijeniti i u slučajevima kada se radi o pod mrežama koje su interne. Neke postupke nužno je primijeniti prilikom instaliranja i implementacije računala sa IDS alatom kako bi se postigao što veći nivo sigurnosti, budući da vatrozid ne može zaštiti računalo sa IDS alatom.

- Preporučljivo je ukloniti sve servise sa računala sa IDS alatom;
- Mrežna sučelja ne bi trebala imati bilo kakve IP adrese – drugim riječima, računalo sa IDS alatom trebalo bi biti nedostupno preko mreže. Na Linux operacijskim sustavima ovo konkretno znači da je mrežno sučelje dovoljno pokrenuti sa ifconfig eth0 up komandom;
- Moguće je koristiti i jednosmjerne mrežne kablove (ethernet). No, kako ovi kablovi nisu lako dostupni ova se metoda rijetko koristi. U svakom slučaju, metoda je zanimljiva budući da je računalu sa IDS alatom i potreban samo jednosmjeran promet (prema njemu) jer samo izvodi analizu prometa;
- Također se preporučuje onemogućiti okvire za ethernet kontrolu (LLC 802.3) koji se koriste za pregovaranje o brzini komunikacije. Međutim, neke mrežne kartice ne dozvoljavaju isključivanje slanja ovih okvira.

Nakon raspakiravanja Snort programskog paketa, početna pravila koja su uključena u njegovu distribuciju nisu optimizirana za pojedinu mrežu već su općenita. Konfiguracija koja je opisana u ovom dokumentu prilagođena je i za velike korporacijske mreže i to tako da se smanji broj lažno pozitivnih prijavljenih neovlaštenih aktivnosti korisnika. Sa ovom konfiguracijom Snort programskog paketa moguće je provjeriti konfiguraciju vatrozida.



3.1. Tablica prometa i portova

Konfiguracija se počinje raditi ispunjavanjem port tablice vatrozida, koja će pomoći prilikom konfiguracije Snort IDS alata. Jedna takva tablica prikazana je na slici:

Raspored mreža:

```
Universe      : 0.0.0.0/0              : IDS-if = eth0

intranet      : 172.24.0.0/16          : IDS-if = not connected
dmz-net       : 192.168.1.0/24         : IDS-if = eth1
admin-net     : 192.168.2.0/29         : IDS-if=eth2(only administration)
front-zone    : 194.245.91.0/24        : IDS-if = eth0
fw-if0        : 194.245.91.1/32        : IDS-if = eth0

Default policy: DENY!
```

	To From	(A) Universe	(B) dmz-net	(C) fw-if0
(a)	universe		80/tcp	
(b)	dmz-net	53/udp	22/tcp	
(c)	fw-if0	80/tcp 53/udp 22/tcp	22/tcp	

```
eth0: [Aa-Ca] and [Aa-Ac] -> /etc/ids/eth0/policyrules/pass.rules
eth0: [Ac-Cc] and [Ca-Cc] -> /etc/ids/eth0/policyrules/pass.rules
eth1: [Ab-Cb] and [Ba-Bc] -> /etc/ids/eth1/policyrules/pass.rules
```

Konfiguracija vatrozida prema gore navedenoj tablici omogućila bi npr. spajanje svih računala sa korporacijskog intraneta na port 80 (Web) na bilo kojem računalu na Internetu. Naravno, dozvoljeno je spajanje samo sa aplikacija koje koriste port veći od 1024, budući da za ovaj postupak nije potrebno koristiti rezervirane portove. Komunikacijski zahtjevi na Internetu zapravo su maskirani (NAT – eng. Network Address Translation) i kao izvornu adresu prikazuju samo javnu IP adresu vatrozida, budući da je on taj koji kontaktira udaljeno računalo.

Ovakva je konfiguracija tipična za većinu korporacijskih mreža koje se preko jednog vatrozida i stalne veze spajaju na Internet.

Također, iz sheme se može vidjeti da je postavljeno jedno računalo sa alatom za detekciju neovlaštenih aktivnosti korisnika koje zapisuje i pregledava mrežni promet. Kasnije u dokumentu objašnjeni su eventualni sigurnosni problemi koji mogu nastati prilikom upotrebe ovakve konfiguracije.

Slijedeća skripta iskorištena je za izradu početnih direktorija i datoteka:

```
#! /bin/bash
IDS_CONFIG=/etc/ids
IDS_LOG=/var/log/ids
# prepare the directories for the 2 different networks and create the
  policy
# rules files and the logfile directories
for NIC in eth0 eth1; do
      mkdir -p $IDS_CONFIG/$NIC/policyrules
      mkdir -p $IDS_LOG/$NIC
      > $IDS_CONFIG/$NIC/ids.conf
      for LOCALRULES in drop.rules pass.rules; do
```

```
            > $IDS_CONFIG/$NIC/policyrules/$LOCALRULES
      done
      echo "deny ip any any -> any any (msg: "malicious traffic";)"
  >\
            $IDS_CONFIG/$NIC/policyrules/deny.rules
done
mkdir -p $IDS_CONFIG/idrules
```

Nakon izvođenja ove skripte potrebno je ručno kopirati pravila rada Snorta koja se nalaze u izvornom programskom paketu Snorta u `/etc/ids/idrules` direktorij.

3.2. Konfiguracija Snorta

Sada je potrebno postaviti specifične konfiguracijske datoteke `ids.conf`. U primjeru koji je korišten u ovom dokumentu datoteka je postavljena za eth0 mrežno sučelje i nalazi se u `/etc/ids/eth0/ids.conf`. Isti postupak potrebno je ponovo provesti i za ostala mrežna sučelja i postaviti te konfiguracijske datoteke u odgovarajuće direktorije.

```
 1 #
 2 # ids.conf
 3 #
 4
 5 # base config
 6 config ghetto_msg:      url
 7 config umask:           0177
 8 config alert_with_interface_name:
 9 config utc:
10 config show_year:
11
12
13 # new rule types
14 ruletype drop
15 {
16         type pass
17 }
18
19 ruletype deny
20 {
21         type log
22         output log_tcpdump: deny
23         output alert_syslog: LOG_LOCAL7 LOG_INFO
24 }
25
26 ruletype info
27 {
28         type log
29         output log_tcpdump: info
30 }
31
32 config order: drop activation dynamic alert pass info deny
33
34 # variables
35 var Universe            0.0.0.0/0
36 var DMZ                 192.168.1.0/24
37 var FRONT               194.245.91.0/24
38 var INTRANET            172.23.0.0/16
39 var FWIF0               194.245.91.1
40
```

```
41 # needed for alert rules
42 var EXTERNAL_NET        [$Universe]
43 var HOME_NET            [$FRONT,$DMZ]
44 var SMTP                [$FWIF0]
45 var DNS_SERVER          $HOME_NET
46 var HTTP_SERVERS        $HOME_NET
47 var SQL_SERVERS         $HOME_NET
48 var DNS_SERVERS         $HOME_NET
49
50 # preprocessor
51 preprocessor defrag
52 preprocessor http_decode: 80 81 3128 8080 -unicode
53 preprocessor portscan: $FRONT 4 3 portscan.log
54 preprocessor portscan-ignorehosts: $FRONT
55
56 # output plugins
57 output alert_syslog: LOG_LOCAL7 LOG_INFO
58 output log_tcpdump: alert
59
60 include /etc/ids/idrules/classification.config
61
62 # local rules
63 # change interfaces for multiple network cards
64 include /etc/ids/eth0/policyrules/drop.rules
65 include /etc/ids/eth0/policyrules/pass.rules
66 include /etc/ids/eth0/policyrules/deny.rules
67
68 # IDS rules
69 include /etc/ids/idrules/exploit.rules
70 include /etc/ids/idrules/scan.rules
71 include /etc/ids/idrules/finger.rules
72 include /etc/ids/idrules/ftp.rules
73 include /etc/ids/idrules/telnet.rules
74 include /etc/ids/idrules/smtp.rules
75 include /etc/ids/idrules/rpc.rules
76 include /etc/ids/idrules/rservices.rules
77 include /etc/ids/idrules/backdoor.rules
78 include /etc/ids/idrules/dos.rules
79 include /etc/ids/idrules/ddos.rules
80 include /etc/ids/idrules/dns.rules
81 include /etc/ids/idrules/netbios.rules
82 include /etc/ids/idrules/web-cgi.rules
83 include /etc/ids/idrules/web-coldfusion.rules
84 include /etc/ids/idrules/web-frontpage.rules
85 include /etc/ids/idrules/web-misc.rules
86 include /etc/ids/idrules/web-iis.rules
87 include /etc/ids/idrules/icmp.rules
88 include /etc/ids/idrules/misc.rules
```

Direktive u konfiguracijskoj datoteci (linije 6-10) koriste se za dodavanje nekih komandno linijskih opcija za Snort koje onda u ovom slučaju nije potrebno specificirati. Npr., `config_show_year` zamjenjuje `-y` opciju prilikom pokretanja Snorta.
Slijedeći dio konfiguracijske datoteke određuje pravila (linije 14-30). U ovom dijelu moguće je definirati nova pravila kao i nove karakteristike tih pravila. Npr., moguće je definirati novi tip zapisivanja logova koji ne samo da zapisuje tcpdump logove na tvrdi disk već i šalje poruku preko syslog servisa. Definicija pravila za Snort je donekle komplicirana i preporučuje se proučavanje priručnika prije definiranja novih pravila. U konfiguracijskoj datoteci koja je prikazana u ovom dokumentu dodano je nekoliko novih pravila koja poboljšavaju točnost i mogućnost smanjivanja

pozitivno lažnih uzbuna definirajući logički slijed pravila koja se procesiraju sekvencijalno. Ovdje je potrebno napomenuti da se unutar jednog pravila ne može specificirati slijed izvršavanja. Zbog toga, ukoliko postoji pravilo s npr. tri definirana stanja uzbune, nemoguće je znati kojim će redoslijedom Snort procesirati to pravilo. Slijed izvršavanja konfiguracijske datoteke može se riješiti preko mogućnosti postavljanja granulacije na pet različitih nivoa, kao što je definirano u liniji 32:

```
config order: drop activation dynamic alert pass info deny
```

Drop pravilo koristi se uglavnom za micanje lažno pozitivnih uzbuna koje bi bile generirane sa alert pravilom. Kao što se vidi u konfiguracijskoj datoteci, potrebno je predati pravilo za provjeravanje sigurnosne politike vatrozida. Najočitiji problem sa lažno pozitivnim uzbunama može se prikazati na slijedećem primjeru. Ako je odlučeno da vatrozid prihvaća `icmp_echo_request` pakete, što je dodano i u tablicu i u pravila, moguće je da Snort zbog neke greške prijavljuje ove pakete kao lažno pozitivnu uzbunu. Problem koji nastaje prilikom ovakve konfiguracije je očit – Snort će generirati lažno pozitivne uzbune koje će puniti log datoteku u koju se one upisuju. Zbog toga će se ovo pravilo sigurnosne politike vatrozida upisati u Drop pravilo koje će zatim biti odbačeno od Snorta prilikom provjeravanja pravila. Još jedan tip upotrebe Drop pravila je onaj za promet koji se ne želi pregledavati već mu se eksplicitno vjeruje. Međutim, ovo je, naravno, potencijalni sigurnosni problem kod kojeg neovlašteni korisnik može maskirati svoj mrežni promet iza onog kojem se eksplicitno vjeruje. Upravo zbog toga je `drop.rules` datoteka koja dolazi sa Snort programskim paketom potpuno prazna.
Alert pravilo predstavlja treći nivo. Potpisi napada koje koristi Alert pravilo nalaze se u datoteci /etc/ids/idrules. Primjer koji detektira napad na Web cgi skripte je:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI w3-msql
solaris x86  access"; flags: A+; uricontent: "/bin/shA-cA/usr/openwin";
nocase; reference:cve,CVE-1999-0276;
reference:arachnids,211;classtype:attempted-recon;)
```

U ovom slučaju Snort uspoređuje potpis sa analiziranim mrežnim prometom i generira uzbunu u slučaju da potpis odgovara mrežnom prometu.
Pass pravilo predstavlja četvrti nivo. Na ovom nivou se implementira tablica prometa i portova koja je prikazana u točki 3.1. Pass pravilo zapravo služi za provjeravanje ispunjavanja uvjeta sigurnosne politike implementirane na vatrozidu. Ukoliko se pojave uzbune u log datoteci nakon Pass pravila, to znači da je postojala neovlaštena aktivnost korisnika, lažno pozitivna uzbuna ili da je vatrozid krivo konfiguriran. Log datoteke se mogu provjeriti u točkama prije i nakon vatrozida; ako se razlikuju potrebno je provjeriti konfiguraciju vatrozida.
Predzadnje pravilo je Info, koje služi za logiranje podataka sa nanovo definiranim izlaznim funkcijama u linijama 26-30. Konfiguracija iz dokumenta postavljena je tako da Snort logira pakete u tcpdump formatu kako bi se oni kasnije mogli čitati s tcpdump programom. Ova mogućnost najviše se koristi za mrežni promet koji nije dozvoljen po sigurnosnoj politici, kao npr. promet koji generira pogrešno konfigurirano računalo sa Windows NT operacijskim sustavom koji šalje bootpc zahtjeve. Ovakav promet ne predstavlja klasičnu neovlaštenu aktivnost korisnika, ali unosi smetnje u log datoteku u koju se upisuju generirane uzbune. Zbog toga je napisano novo pravilo kako bi se sve ovakve interpretacije zapisale u drugu log datoteku.
Deny pravilo koristi se za logiranje svih paketa koji do tog nivoa nisu nigdje zapisani i koji ne pripadaju dozvoljenom mrežnom prometu vatrozida. Ovo pravilo predstavlja peti nivo i vrlo je bitno za minimiziranje broja lažno pozitivno generiranih uzbuna. Ono nam također omogućava i provjeravanje da li je mrežni promet iza vatrozida onakav kako je očekivano. Ako nije, biti će zapisan od strane Deny pravila koje glasi:

```
deny    ip      any     any     ->      any     any
```

Cilj ovakvog pravila je da se ciljna datoteka sa logovima drži što je moguće manja. Svaki zapis koji odlazi u ovu datoteku mora biti detaljno analiziran. Pri ispravnoj konfiguraciji paketi nikad ne bi trebali biti zapisani u ovu datoteku.
Zadnja stvar koju je potrebno konfigurirati je provjera sigurnosne politike implementirane na vatrozidu. Ova konfiguracija je različita za svako mrežno sučelje i postavlja se u različite datoteke da bi se dobio bolji pregled rezultirajućih Snort izlaznih datoteka.

```
/etc/ids/eth0/policyrules/pass.rules
 pass tcp $Universe 1024: <> $DMZ      80
      pass tcp $FWIF0    1024: <> $Universe 80
      pass tcp $FWIF0    1024: <> $Universe 22
      pass udp $FWIF0    1024: <> $Universe 53
      /etc/ids/eth1/policyrules/pass.rules
      pass tcp $Universe 1024: <> $DMZ      80
      pass tcp $DMZ      1024: <> $DMZ      22
      pass udp $DMZ      1024: <> $Universe 53
```

Na kraju je potrebno postaviti i syslog servis za zapisivanje prijavljenih generiranih uzbuna. Konfiguracija Snorta je slijedeća:

```
#
# syslog-ng configuration file for the IDS
#
options { keep_hostname(on); long_hostnames(off); sync(0); };
source s_src { unix-stream("/dev/log"); internal(); };
source s_net { udp(ip(127.0.0.1) port(514)); };
source s_krn { file("/proc/kmsg"); };
destination d_auth      { file("/var/log/authlog"); };
destination d_kern      { file("/var/log/kernlog"); };
destination d_mesg      { file("/var/log/messages"); };
destination d_cron      { file("/var/log/cronlog"); };
destination d_ids       { file("/var/log/idslog"); };
destination d_loghost   { tcp("loghost" port(1514)); };
filter f_auth           { facility(auth, authpriv); };
filter f_kernel         { facility(kern); };
filter f_cron           { facility(cron); };
filter f_mesg           { facility(daemon, mail, security); };
filter f_ids            { facility(local7); };
log  { source(s_src); filter(f_auth);   destination(d_auth); };
log  { source(s_krn); filter(f_kernel); destination(d_kern); };
log  { source(s_src); filter(f_cron);   destination(d_cron); };
log  { source(s_src); source(s_net); filter(f_ids); destination(d_ids);
};
log  { source(s_src); source(s_net); filter(f_ids);
destination(d_loghost); };
log  { source(s_src); source(s_net); filter(f_mesg);
destination(d_mesg); };
```

4. Mogući problemi

Kao što je prilikom testiranja i pokazano, slučaj kada nema prijavljenih uzbuna ne postoji. U log datotekama pojavljuju se brojni pokušaji pregledavanja podignutih servisa na računalu, lažno pozitivne uzbune i drugi neželjeni promet. Prilikom ispitivanja slijedeći su problemi bili naročito istaknuti:

- Brzina – Kod prebrzih lokalnih mreža nekad IDS alat ne stigne provjeriti sav mrežni promet što može rezultirati u lažno pozitivnim ili lažno negativnim uzbunama.
- Mogućnost napada umetanjem i izbacivanjem podataka.

– Različite implementacije TCP/IP stoga kod IDS alata i operacijskog sustava na drugom kraju mogu uzrokovati različite probleme. Jedan poznati problem nastaje kod fragmenata paketa koji se prepisuju budući da su različito prihvaćeni na strani IDS alata, odnosno na strani ciljnog računala.

5. Zaključak

Važnost IDS alata za korporacijski intranet je neupitna. Snort je vrlo napredan IDS alat koji uživa veliku popularnost i brzo izdavanje novih inačica (posebno potpisa) koje su u stanju otkrivati najnovije sigurnosne probleme. Zajedno s dobrim alatom za nadgledanje, pomoću Snorta se može vrlo lagano podići nivo sigurnosti cijelog sustava.