HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Linux Firewalling

CCERT-PUBDOC-2002-11-05

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

U posljednjih nekoliko godina znatno se povećala popularnost korištenja Linux operativnog sustava kao platforme za vatrozid sustave (*engl. firewall*). Osim same cijene Linux platforme (potpuno besplatan, s dostupnim izvornim kodom), tome je u velikoj mjeri pridonio i razvoj programskih modula koji omogućuju njihovu implementaciju (ipfwadm, ipchains, iptables).
Dio Linux operativnog sustava koji omogućuje implementaciju vatrozid sustava prošao je niz razvojnih faza od trenutka prve objave. Kao dio Linux jezgre 1.1 prvi je puta objavljen ipfwadm paket, a nastao je na temelju BSD-ovog ipfw programa. S jezgrom 2.2.0 objavljen je ipchains paket, naprednija inačica istog programa.
Zadnje promjene na kodu rezultirale su objavom novog, dodatno poboljšanog i mogućnostima bogatijeg netfilter/iptables paketa za filtriranje koji se pojavio s 2.4 jezgrom. Osim iptables paketa, jezgra 2.4 donosi i brojna druga sigurnosna poboljšanja, koja Linux svrstavaju u grupu sigurnijih operativnih sustava (poboljšane metode enkripcije, kontrole pristupa i sl.)
S obzirom na veću kompleksnost i brojne nove mogućnosti iptables programa, postupci njegove konfiguracije i održavanja kod većih sustava može biti prilično nepraktično, što može lagano dovesti do pogrešaka.
U ovom dokumentu biti će ukratko opisane mogućnosti iptables paketa te postojeći alati koji olakšavaju njegovo održavanje i konfiguraciju. Osnovna ideja je da se na taj način administratorima pojednostavni i olakša konfiguracija sustava te da se mogućnost pogreške svede na što manju mjeru. Biti će pokazane prednosti ovakvih alata, ali i neke od mana koje predstavljaju ozbiljna ograničenja na mogućnost njihove primjene.
Detaljnije informacije o iptables paketu i njegovim mogućnostima mogu se naći u HOWTO dokumentu pod nazivom Linux iptables HOWTO, na adresi http://www.telematik.informatik.uni-karlsruhe.de/lehre/seminare/LinuxSem/downloads/netfilter/iptables-HOWTO.html

2. Poteškoće s konfiguracijom putem komandne linije

Konfiguracija `iptables` programa iz komandne linije provodi se upotrebom `iptables` naredbe kojoj se prosljeđuju argumenti koji definiraju kako će se tretirati pojedini mrežni paketi. Ovakav način konfiguracije prilično je nezahvalan budući da zahtjeva dosta iskustva i napora te izvrsno poznavanje TCP/IP grupe protokola. Potrebno je precizno definirati pravila filtriranja za sve tipove paketa (dolazne i odlazne) kako bi se na taj način implementirala željena sigurnosna politika. Nepažljiva i površna konfiguracija mogu biti uzrok brojnih problema budući da loše konfigurirani vatrozid korisnicima daje prividni osjećaj sigurnosti.
`Iptables`, slično kao i njegov prethodnik `ipchains` programski paket, pravila filtriranja paketa grupira unutar tzv. lanaca (*engl.chains*). Postoje tri inicijalna lanca u kojima `iptables` grupira pravila filtriranja (*engl. rules*). To su:

- INPUT lanac
- FORWARD lanac
- OUTPUT lanac

Osim gore navedenih inicijalnih lanaca postoji mogućnost dodavanja vlastitih korisničkih lanaca. Na taj način moguće je preciznije definirati način rada `iptables` programa te pravila filtriranja prilagoditi osobnim potrebama.
Svaki od primljenih paketa uspoređuje se po redu sa pravilima u definiranim lancima, sve dok se ne naiđe na pravilo koje odgovara primljenom paketu i koje definira kako će se paket dalje procesirati.
Tipične akcije koje se provode nad paketima su ACCEPT (prihvati paket), DROP, REJECT (odbacuju pakete) i sl., a postoji mogućnost definiranja pravila koja će primljeni paket jednostavno proslijediti nekom drugom lancu na daljnju analizu.
Sve ove mogućnosti administratoru ostavljaju velik broj mogućnosti konfiguracije, ali jednako tako postoji prilično velika mogućnost pogreške. Vjerojatnost pogreške znatno je veća ukoliko se želi implementirati nešto kompleksniji vatrozid kao jedan od mehanizama zaštite u sklopu složenijih računalnih mreža.

Za ispravnu i pouzdanu konfiguraciju potrebno je i dobro poznavanje načina rada pojedinih mrežnih (TCP i UDP) servisa. Neki su protokoli jednostavni za filtriranje (npr. POP3, Telnet i sl.), a neki su nešto kompleksniji (npr. FTP) te je stoga za pravilnu konfiguraciju potrebno dobro poznavanje istih.
Potrebno je jednako voditi računa o paketima u oba smjera (dolaznim i odlaznim) za pojedini servis ukoliko se želi ispravno implementirati definirana sigurnosna politika. Stvari dodatno može zakomplicirati translacija adresa (NAT) te druge specifičnosti koje mogu biti uzrok vrlo kompleksnog sustava filtriranja paketa.
U nastavku će biti vrlo kratko opisan postupak konfiguracije `iptables` filtara paketa, a detaljnije informacije mogu se naći u Linux `iptables` HOWTO. dokumentu na adresi http://www.telematik.informatik.uni-karlsruhe.de/lehre/seminare/LinuxSem/downloads/netfilter/iptables-HOWTO.html.

2.1. Konfiguracija `iptables` programa

`Iptables` programski paket bazira svoj rad na pravilima filtriranja koja definiraju način na koji će paketi biti procesirani. Pravila se definiraju zadavanjem `iptables` naredbe te prosljeđivanjem odgovarajućih opcija koje će detaljnije opisati ponašanje iste naredbe.
Osnovna grupa opcija koje je moguće proslijediti `iptables` programu omogućuje upravljanje definiranim lancima. Neke od takvih opcija su:

- N – stvaranje novog iptables lanca
- X – brisanje praznog lanca (onaj koji ne sadrži niti jedno pravilo)
- P – mijenjanje sigurnosne politike postojećeg lanca
- L – ispis pravila u lancu
- F – pražnjenje pravila iz lanca (*engl. flush*)

Osim opcija koje omogućuju upravljanje cijelim lancima postoji niz opcija koje omogućuju upravljanje samim pravilima. Neke od njih su:

- A – dodaje se novo pravilo u lanac
- D – briše se pravilo iz lanca

Navedene opcije omogućuju precizno definiranje pravila za sve odlazne i dolazne pakete na vatrozidu s dvije ili više mrežnih kartica, ili čak na računalu s jednom karticom.

2.2. Prednosti korištenja `iptables` programa

Prije upoznavanja s programima koji olakšavaju konfiguraciju `iptables` programa, potrebno je spomenuti neke od njegovih prednosti u odnosu na ranije inačice `(ipcahains)`.

- Mogućnost implementacije tzv. stateful vatrozida. Stateful vatrozidi posjeduju mogućnost praćenja stanja pojedinih mrežnih sesija, što omogućuje implementaciju naprednijih mogućnosti filtriranja paketa. Ovakav pristup posebno je koristan u slučaju filtriranja servisa kao što su FTP, DNS i drugi.
- Mogućnost filtriranja paketa na temelju bilo koje kombinacije TCP zastavica ili čak na temelju Ethernet MAC adresa. Ova potonja može biti vrlo korisna ukoliko se želi postaviti vatrozid unutar iste lokalne računalne mreže.
- Naprednije mogućosti logiranja u odnosu na ipcahains paket.
- Netfilter/ipcahains arhitektura korisnicima pruža kvalitetniju podršku za translaciju adresa (NAT) i transparentne proxy sustave.
- Mogućnost blokiranja napada uskraćivanjem računalnih resursa (DoS).

3. Alati za konfiguraciju `iptables` programa

U ovom dijelu biti će navedeni programski alati koji omogućuju jednostavniju konfiguraciju `iptables` programa, odnosno olakšavaju postupak definiranja pravila filtriranja paketa. Za svaki od testiranih alata biti će navedena osnovna svojstva, fleksibilnost te mogućnosti primjene.
U razmatanje su uključeni programski alati prikazani u sljedećoj tabeli:

Ime paketa	Inačica	Autor	URL adresa
MonMotha's Firewall	2.3.5	MomMotha	http://mirkk.kurd.nu/~monmotha/firewall/index.php
Firewallscript (iptables 4.4c-3 devel)		Patrik Hildigsson	http://my.netfilter.se/
Ferm-0.0.18	0.0.18	Auke Kok	http://www.geo.vu.nl/~koka/ferm/
AGT-0.83	0.83	Andy Gilligan	http://sourceforge.net/projects/agt
Knetfilter-1.2.4	1.2.4	Luigi Genoni	http://expansa.sns.it:8080/knetfilter/
gShield-2.0.2	2.0.2	R. Gregory	http://muse.linuxmafia.org/gshield.html

3.1. MonMotha's Firewall 2.3.5

`MonMotha's Firewall` je jednostavna BASH skripta ljuske (*engl. shell script*) srednje veličine (oko 30k). S obzirom na ograničenost opcija koje su trenutno implementirane unutar skripte, ista se može preporučiti eventualno za korištenje na računalu s jednom mrežnom karticom.

Neke od naprednijih opcija `iptables` programa trenutno nisu implementirane što ograničava područje primjene programa. Postupak instalacije vrlo je jednostavan. Dovoljno je skriptu kopirati u neki od `rc` direktorija, čime će se ona automatski izvršiti prilikom podizanja sustava te konfigurirati `iptables` vatrozid.

Postupak konfiguracije bazira se na ručnom editiranju skripte, gdje je potrebno postaviti varijable na vrijednosti koje odgovaraju osobnim potrebama. Ne postoji nikakva zasebna konfiguracijska datoteka. Tu je moguće definirati razne parametre kao što su liste TCP i UDP portova koje se žele filtrirati, zatim IP adrese strojeva kojima se posebno želi ograničiti ili dozvoliti pristup određenim servisima, sigurnosna ograničenja, adrese lokalnih strojeva koje se žele zaštititi, podatci o DMZ zonama (ukoliko postoje) i sl.

Bez prilagođavanja koda skripte osobnim potrebama, skripta se neće moći izvršiti te će biti prijavljena odgovarajuća greška.

Dodatni nedostatak ove skripte je taj što dokumentacija praktički ne postoji. Jedine raspoložive upute koje korisnika vode kroz postupak konfiguracije vatrozida su one koje se nalaze kao komentari unutar skripte.

Korištenje ovakve implementacije može se preporučiti eventualno korisnicima s modemskim pristupom Internetu ili manjim poslužiteljima koji zahtijevaju osnovne mehanizme zaštite putem filtriranja paketa. Zbog nešto kompliciranije konfiguracije programa, isti se preporučuje na korištenje naprednijim korisnicima koji imaju iskustva u ovom području.

3.2. Firewallscript

`FirewallScript` je također `iptables` skripta ljuske, samo ovoga puta nešto bogatijih mogućnosti i veličine od 85 k. S obzirom na implementirane mogućnosti `FirewallScript` se pokazala kao prikladno rješenje za zaštitu pojedinačnih računala, ali jednako tako i za zaštitu manjih mrežnih sustava.

Prilikom prvog pokretanja skripta automatski generira inicijalne konfiguracijske datoteke vatrozida. Ovakvu inicijalnu konfiguraciju potrebno je prilagoditi okolini u kojoj se sustav želi implementirati. Provedeni testovi pokazali su da ova inicijalna konfiguracija sama po sebi nije funkcionalna.

Budući da je skripta prilično kompleksna, a dokumentacija i u ovom slučaju vrlo štura, pravilna i pouzdana konfiguracija zahtijevati će vrlo često detaljnu analizu koda skripte te često pokretanje `iptables` naredbe s `-L` opcijom (ispis definiranih pravila u pojedinim lancima).

Za razliku od nekih drugih programa iste namjene, `FirewallScript` testira i po potrebi učitava module koji su potrebni za rad `iptables` programa. Još jedna vrlo praktična i često korisna mogućnost je memoriranje posljednje konfiguracije sustava, čime se vrlo jednostavno u slučaju pogreške sustav može vratiti na zadnju valjanu koniguraciju.

3.3. Ferm

`Ferm` (**F**or **E**asy **R**ule **M**aking) je Perl skripta koja omogućuje parsiranje konfiguracijskih datoteka napisanih u posebnom formatu koji skripta razumije. Ovaj posebno razvijeni jezik vrlo je jednostavan za analizu što u velikoj mjeri olakšava konfiguriranje `iptables` vatrozida ovim putem.
Dokumentacija koja dolazi s programom prilično je temeljita, a i primjeri koji su dostupni u velikoj mjeri olakšavaju definiranje vlastitih pravila filtriranja paketa.
Ovdje je dan primjer jedne konfiguracijske datoteke Ferm programa:

```
# primjer koniguracijske datoteke Ferm programa

chain input {
    if ppp0 # put your outside interface here
    {
        proto tcp goto fw_tcp;
        proto udp goto fw_udp;
        proto icmp goto fw_icmp;
    }
}

chain fw_tcp proto tcp {
    dport ssh ACCEPT;
    syn DENY log;
    dport domain ACCEPT;
    dport 0:1023 DENY log;
}

chain fw_udp proto udp {
    DENY log;
}


chain fw_icmp proto icmp {
    icmptype (
        destination-unreachable time-exceeded
    ) ACCEPT;
    DENY log;
}
```

`Ferm` skripta će na temelju ovako zadane konfiguracijske datoteke definirati iptables pravila koja će implementirati navedena pravila. U ovom slučaju dozvoljava se TCP ssh i DNS izlazni promet, kompletni UDP promet je blokiran i dozvoljena su samo dva tipa ICMP paketa (Time Exceeded i Destination Unreachable).
Na počeku je potrebno definirati sučelje na koje se pravila odnose (u primjeru je to `ppp0` sučelje, ali može biti bilo koje drugo), kako bi se znalo na koje je pakete potrebno primijeniti definirana pravila.
Iz primjera se može vrlo jednostavno shvatiti kako su definirana pravila filtriranja u ovom slučaju. Svi paketi koji dolaze u INPUT lanac prosljeđuju se a analizu drugim lancima ovisno o tipu paketa:

- TCP paketi prosljeđuju se fw_tcp lancu
- UDP paketi prosljeđuju se fw_udp lancu
- ICMP paketi prosljeđuju se fw_icmp lancu

Nakon ovakve definicije INPUT lanca definiraju se pravila za svaki od navedenih tipova IP paketa (`fw_tcp`, `fw_udp` i `fw_icmp` lanci). Može se odmah primijetiti kako je ovakav način definiranja pravila filtriranja paketa puno jednostavniji i pregledniji, a i vjerojatnost pogreške je bitno manja.
To je prvenstveno posljedica činjenice što se ovakvim pristupom pravila definiraju na višem nivou apstrakcije, čovjeku razumljivijem, a `Ferm` skripta je ta koja pravila direktno implementira pomoću `iptables` naredbi.

3.4. AGT

AGT je program napisan u C programskom jeziku koji na temelju parsiranja konfiguracijskih datoteka konfigurira iptables vatrozid. Iako se ideja programa čini vrlo dobra, program je još u ranoj fazi razvoja te se iz toga razloga mogu očekivati određeni problemi.
Da bi se program ispravno preveo potrebno je ručno uređivati Makefile datoteku (automake nije podržan). Iako dokumentacija programa nije bogata, dostupni su primjeri konfiguracije koji administratoru olakšavaju njegovo korištenje.
Ovdje je dan primjer jedne konfiguracijske datoteke AGT programa:

```
NEW | FROM-INT
NEW | RESET

|| FROM-INT | icmp | ACCEPT |||||
|| FROM-INT | tcp  | ACCEPT ||||| pop3
|| FROM-INT | tcp  | ACCEPT ||||| imap

                  || RESET | tcp  | REJECT --reject-with tcp-reset |||||
```

Za razliku od Ferm programa, ovakva konfiguracija bez dodatne dokumentacije čini se prilično nejasnom. Mišljenje je kako učenje i savladavanje ovako definiranog jezika za konfiguraciju AGT programa nije ništa jednostavnije od iptables opcija.
Eventualna prednost ovakvog načina konfiguracije je nešto intuitivnija i apstraktnija mogućnost definiranja pravila kada se korisnik jednom dobro upozna sa ovakvom posebno definiranom sintaksom.

3.5. Knetfilter

Knetfilter je program koji korisniku omogućuje konfiguraciju iptables vatrozida putem grafičkog okruženja. Knetfilter je KDE aplikacija koja osim mogućnosti konfiguracije iptables varozida omogućuje upravljanje tcpdump i nmap programima.
Grafičko okruženje programa u velikoj mjeri olakšava postupak konfiguracije, održavanja i testiranja iptables vatrozida, što je naročito velika prednost za manje iskusne korisnike u ovom području.
Testiranje i analiza rada programa dodatno je olakšana mogućnošću korištenja tcpdump programa (analizator mrežnog prometa) iz istog sučelja. Implementirana je također i mogućnost podešavanja translacije i maskiranja IP adresa (NAT, IP Masquerading).
Nedostatak programa je taj što ne postoji mogućnost konfiguracije dial-up sustava, budući da program zahtijeva fiksnu IP adresu i ne podržava ppp0 *dial-up* sučelje.
Iako dokumentacija programa nije isuviše opsežna, intuitivno grafičko sučelje korisniku omogućuje prilično jednostavno snalaženje i korištenje programa.

3.6. GsShield

GsShield BASH skripta ljuske čini se kao najkompletniji alat od svih dosad navedenih programa u ovom području. Skripta dolazi sa bogatom i detaljnom dokumentacijom, konfiguracijske datoteke su prilično intuitivne, podržana je translacija adresa (NAT) te dinamičke (ppp) i statičke (eth) IP adrese.
U razvoju je i opcionalno grafičko sučelje programa pod nazivom gShieldConf koje je dostupno na adresi http://members.home.com/vhodges/gshieldconf.html.
Ovdje je u svrhu primjera izdvojen dio konfiguracijske datoteke GsShield programa:

```
FW_ROOT="/etc/firewall"
IPTABLES=`which iptables`
LOCALIF="eth0"
DNS="24.31.195.65"
LTIME="20/m"
ALLOW_DHCP_LEASES="YES"
...
```

Inicijalna konfiguracija `gShield` programa dovoljna je za ispravan rad programa, iako se strogo preporučuje barem pregledavanje cijele konfiguracijske datoteke na temelju koje se definiraju pravila filtriranja.

4. Zaključak

Slijedi tabela u kojoj je dan kratki pregled svih programa opisanih u ovom poglavlju s njihovim osnovnim karakteristikama:

Ime programa	Verzija	Tip	Konfiguracija
MonMotha's firewall	2.3.5	skripta ljuske	slabo riješena, ručno editiranje
FirewallScript	-	skripta ljuske	automatska, ručno editiranje
Ferm	0.17	perl skripta	dobro riješena, jednostavna
AGT	0.82	C program	slabo riješena
KnetFilter	1.2.4	GUI (C++, Qt)	grafičko sučelje
gsShield	2.0.3	skripta	dobro riješena, grafičko sučelje

Ideja razvoja pomoćnih programskih alata koji bi omogućili jednostavniju, bržu te pouzdanu konfiguraciju vatrozid sustava baziranih na `iptables` paketu, prilično je dobra, ali još uvijek traži kompletnu i kvalitetno riješenu implementaciju.
Iako su neki od programa opisanih u prethodnom poglavlju (3) u velikoj mjeri olakšali taj postupak, još uvijek se mogu naći brojne zamjerke koje bi trebalo riješiti.
Možda najveći nedostatak većine navedenih programa je taj što ne implementiraju sve mogućnosti `iptables` programa. U odnosu na svoje prethodnike (`ipfwadm` i `ipchains`) `iptables` program unio je velik broj noviteta i naprednih mogućnosti koje administratorima omogućuju implementaciju vrlo kvalitetnih vatrozidnih sustava. No, za potpunu implementaciju istih, izgleda da je za sada jedini način ručno zadavanje `iptables` naredbi s odgovarajućim parametrima. Ovakav pristup je naravno potpuno neprihvatljiv sa stajališta manje iskusnih korisnika koji nisu u potpunosti upoznati s tehničkim detaljima oko filtriranja paketa.
Težnja je razviti takav konfiguracijski alat koji bi implementirao sve mogućnosti `iptables` programa, a da ujedno korisnicima s minimalnim poznavanjem tehničkih detalja omogući kvalitetnu implementaciju te održavanje sustava.
Dodatni nedostatak nekih od gore spomenutih programa je štura dokumentacija, što još više otežava njihovo korištenje.
S obzirom da su neki od alata još uvijek u ranoj fazi razvoja te da se učestalo javljaju nove ideje i pristupi može se u skoroj budućnosti očekivati pojava novih i još kvalitetnijih alata koji će se približiti težnjama korisnika.

5. Reference

[1] SecurityFocus - http://online.securityfocus.com/infocus/1410

[2]Linux Iptables HOWTO - http://www.telematik.informatik.uni-karlsruhe.de/lehre/seminare/LinuxSem/downloads/netfilter/iptables-HOWTO.html

[3] Iptables/netfilter - http://netfilter.samba.org/