HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza IPAudit alata

CCERT-PUBDOC-2005-11-140

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 4

2. INSTALACIJA ALATA 5

3. KORIŠTENJE ALATA 7

3.1. MREŽNI IZVJEŠTAJI 8

4. ZAKLJUČAK 12

5. REFERENCE 12

1. Uvod

IPAudit je programski alat za prikupljanje i analizu mrežnog prometa. Alat je napisan u Perl programskom jeziku, te je namijenjen instalaciji na Linux/Unix operacijskim sustavima. Osnovno upravljanje programom vrši se putem naredbenog retka, iako je za jednostavniju i praktičniju uporabu moguće dodatno instalirati i grafičko korisničko sučelje. Sučelje je realizirano u obliku specijalno prilagođene Web aplikacije, te je za njeno korištenje na sustavu potrebno imati funkcionalni Web poslužitelj. Izvještaji koji su dostupni putem Web sučelja generiraju se periodički putem `cron` skripti koje se podešavaju prilikom instalacije programskog paketa Web sučelja. Web sučelju je moguće pristupiti putem bilo kojeg Web preglednika, što predstavlja dodatnu pogodnost.

S obzirom na velike količine podataka i zapisa koje `ipaudit` programski paket generira, korištenje spomenutog grafičkog Web sučelja svakako se preporučuje budući da korisniku nudi brojne funkcionalnosti. Dostupni su različiti grafički i tabelarni prikazi te izvještaji koji bitno olakšavaju analizu prikupljenih podataka, a moguće je i jednostavno pretraživanje podataka prema različitim kriterijima što dodatno pridonosi kvaliteti programa. Praćenje i generiranje podataka o mrežnom prometu odvija se uz pomoć `libpcap` programske biblioteke koju je unaprijed potrebno imati instaliranu na sustavu.

IPAudit programski paket prikuplja sav mrežni promet na lokalnoj mreži postavljanjem mrežnog sučelja u promiskuitetni način rada, te također podržava promatranje prometa na više mrežnih sučelja. Alat omogućava analizu svih paketa koji prolaze lokalnom mrežom, te nudi detalje o računalima, mrežnim portovima i protokolima. IPAudit može služiti za analizu mrežne propusnosti i identifikaciju "uskih grla", detekciju kompromitiranih računala, te otkrivanje adresa s kojih se vrši skeniranje mreže. Također, funkcionalnosti alata olakšavaju detekciju onih lokalnih računala koja neprimjereno koriste računalne resurse te na taj način krše sigurnosnu politiku organizacije. Obzirom na upravo navedene mogućnosti korištenja ovog alata, može se zaključiti da IPAudit predstavlja dobro rješenje za upotpunjavanje nedostataka sigurnosne slike lokalne mreže koju potencijalno ostavljaju IDS i IPS alati.

Dokument opisuje osnovne postupke instalacije i podešavanja IPAudit programa, te također osnovne funkcionalnosti i mogućnost njihove primjenu u praksi.

2. Instalacija alata

IPAudit programski paket namijenjen je instalaciji isključivo na sustavima koji se baziraju na Linux/Unix operacijskim sustavima, te bi na svim distribucijama trebao raditi bez većih problema. Obzirom da IPAudit pruža podršku i za Web pristup, alat je moguće koristiti i sa Windows operacijskih sustava putem Web preglednika. Za ispravan rad alata na sustavu je potrebno imati već instaliranu programsku biblioteku `libpcap`, te Perl programski paket uz modul `Time::ParseDate`. Kako je IPAudit implementiran u programskom jeziku Perl, potreba za Perl programskim paketom je očita, dok se `libpcap` biblioteka unutar alata koristi za prikupljanje mrežnog prometa. Za korištenje grafičkog sučelja dodatno su na sustavu potrebni funkcionalni Apache Web poslužitelj, te GNUplot programski paket za prikaz prikupljenih podataka u obliku grafova.

IPAudit je dostupan sa i bez grafičkog sučelja, ali se u svakom slučaju preporuča korištenje Web sučelja zbog bolje preglednosti i jednostavnosti korištenja. Web sučelje alata dolazi kao zasebni programski paket, te ga je potrebno dodatno instalirati na sustavu. Kao što je već napomenuto, za korištenje Web pristupa potreban je i Apache Web poslužitelj. Alat je dostupan i u obliku Debian (`deb`) paketa, te ga je na Debian sustavima moguće instalirati i putem `apt-get` servisa.

U nastavku dokumenta biti će opisan postupak instalacije IPAudit programskog paketa sa Web sučeljem, te će također biti opisane promjene u postavkama samog alata i Apache Web poslužitelja koje je potrebno načiniti kako bi alat bio funkcionalan.

Prvi korak instalacije je kreiranje novog korisnika pod korisničkim imenom `ipaudit`. Novo kreiranom korisniku potrebno je kreirati i `home` direktorij (uobičajeno `/home/ipaudit`).

```
# adduser ipaudit
Adding user `ipaudit'...
Adding new group `ipaudit' (1012).
Adding new user `ipaudit' (1012) with group `ipaudit'.
Creating home directory `/home/ipaudit'.
Copying files from `/etc/skel'
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Pod ovlastima `ipaudit` korisnika potrebno je dohvatiti i raspakirati paket, te pokrenuti `configure` i `make` skripte.

```
# su ipaudit
# tar xvfz ipaudit-1.0BETA2.tar.gz
# cd ipaudit-1.0BETA2
# ./configure
# make
```

Pod `root` ovlastima slijedi pokretanje `make install` naredbe.

```
# su root
Password:
# make install
```

Ovime koracima je `ipaudit` alat instaliran na sustavu, te ga je moguće pokrenuti iz naredbenog retka kako je prikazano u nastavku.

```
# ipaudit

Usage: ipaudit [OPTIONS] [interface[:interface[:interface..]]]
  Read and record info on ip connections and optionally
  dump packets to file
```

Slijedi instalacija Web sučelja, koja je analogna upravo opisano postupku.

```
# su ipaudit
# tar zxvf ipaudit-web-1.0BETA9.tar.gz
# cd ipaudit-web-1.0BETA9/compile/
# ./configure
# make
# su root
Password:
# make install
# make install-cron
```

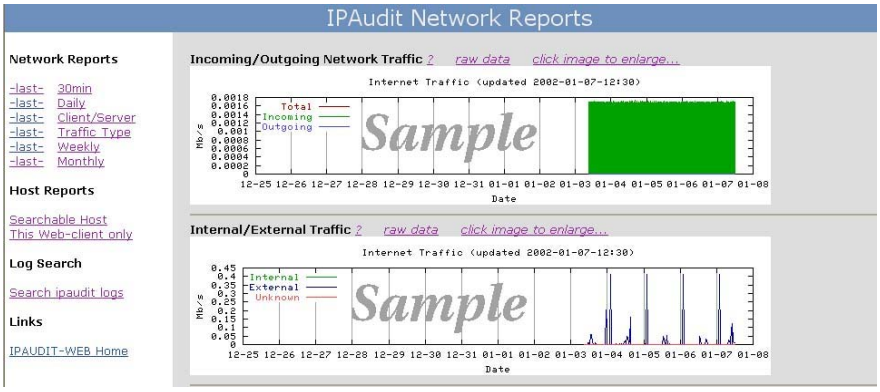
Naredba `make install-cron` služi za automatsko podešavanje `ipaudit` alata kao `cron` skripte. `Cron` skripta je podešena tako da svakih 30 minuta generira zapis prikupljenih podataka. Upravo se iz ovih podataka kreiraju izvještaji kojima je moguće pristupiti putem Web sučelja.
Nakon instalacije preostaje podešavanje konfiguracijskih datoteka `ipaudit` programa i Apache Web poslužitelja.

```
# joe ipaudit-web.conf

#  --------------------------------
#  REQUIRED CHANGES
#  --------------------------------
#Direktiva za definiranje lokalne mreze
LOCALRANGE=127.0.0
#Direktiva za definiranje mreznog sucelja
INTERFACE=eth0
#
```

Unutar `ipaudit` konfiguracijske datoteke potrebno je podesiti postavke koje definiraju lokalnu mrežu i mrežno sučelje na kojem će se prikupljati promet.

```
<Directory /home/*/public_html>
        AllowOverride All
        Options MultiViews Indexes Includes FollowSymLinks
        Order allow,deny
        Allow from all
</Directory>

<Directory /home/*/public_html/cgi-bin>
        Options +ExecCGI -Includes -Indexes
        SetHandler cgi-script
</Directory>
```

Dodatno podešavanje Apache Web poslužitelja sastoji se od omogućavanja pristupa direktoriju gdje je alat instaliran. Nakon ponovnog pokretanja Web poslužitelja moguće je pristupiti Web sučelju `ipaudit` alata usmjeravanjem Web preglednika na URL adresu http://web-posluzitelj/~ipaudit. Ovo je slučaj samo ukoliko je alat zaista instaliran u `home` direktoriju `ipaudit` korisnika. Iz sigurnosnih razloga preporučuje se dodatna zaštita ovog direktorija korisničkom zaporkom, kako bi se neautoriziranim korisnicima onemogućilo pregledavanje povjerljivih informacija o zabilježenom mrežnom prometu.
Izgled Web sučelja alata prilikom prvog pristupanja, kada još ne postoje prikupljeni podaci o mrežnom prometu, prikazan je na sljedećoj slici (Slika 1).



Slika 1: Web sučelje alata prilikom prvog pristupa

Izvještaji se generiraju svakih 30 minuta, te se nakon svakog generiranog izvještaja o prikupljenom prometu graf iscrtava korištenjem GNUplot programskog paketa.

3. Korištenje alata

Prilikom korištenja alata iz naredbenog retka, `ipaudit` program se pokreće uz navođenje dodatnih opcija te mrežnog sučelja na kojem se želi prikupljati promet. Treba napomenuti da je mrežni promet moguće prikupljati na više od jednog mrežnog sučelja ukoliko za to postoji potreba.

```
# ipaudit [OPTIONS] [interface[:interface]]
```

Lista opcija koje alat podržava je vrlo opširna te između ostalog uključuje:

- `-c npacket` – izvođenje programa prekida se nakon uhvaćenih `npacket` paketa,
- `-e` – omogućuje zapisivanje Ethernet adrese svakog računala,
- `-m` – pokretanje programa bez stavljanja mrežnog sučelja u promiskuitetni način rada,
- `-o outfile` – zapisivanje prometa u `outfile` datoteku. Bez ove opcije uhvaćeni promet se ispisuje na standardni izlaz,
- `-q` – izlaz se formatira kao SQL izraz, te je na ovaj način moguće izlaz direktno usmjeriti u podržane baze podataka kao što su MySQL, Postgres i Oracle. Primjer korištenja naredbe uz ovu opciju:

```
ipaudit -q eth0 | mysql -ppassword ipaudit
```

  Pritom se pretpostavlja da baza podataka i odgovarajuće tablice već postoje, te su nazvane *ipaudit*. Format tablice je moguće pronaći na `man` stranicama alata,
- `-r dumpfile` – korištenjem ove opcije `ipaudit` ne čita podatke s mrežnog sučelja, već iz `dumpfile` datoteke, koju je moguće stvoriti pomoću `ipaudit`, `tcpdump`, `ethereal` i drugih programa slične namjene.

Ovo su samo neke od opcija programa, dok se kompletna lista svih opcija može pronaći na `man` stranicama alata, ili pokretanjem `ipaudit` programa u naredbenom retku bez dodatnih argumenata.
Izlaz koji IPAudit generira opisuje konekciju između dva računala. Opis konekcije s e sastoji para IP adresa, brojeva koji opisuju protokol i korišteni mrežni port, te također količinu izmijenjenih podataka između navedenog para izraženu i u oktetima i u broju paketa.
Na slijedećem primjeru pokazana je struktura zapisa IPAudit programa sa odgovarajućim podacima o konekciji između dva računala.

```
Par IP adresa 1, 2
Oznaka protokola (1=icmp, 6=tcp, 17=udp)
Mrežni port računala 1, 2
Broj primljenih okteta na računalu 1, 2
Broj primljenih paketa na računalu 1, 2

161.053.064.240  222.145.127.078  6   4662 2481  238 180    4 3
161.053.064.003  161.053.064.120  17  53 32772   3320 5520  40 40
```

Instalacijom Web sučelja IPAudit alata, automatski se podešavaju `cron` skripte koje se pokreću u određenim vremenskim intervalima, te su zadužene za generiranje mrežnih izvještaja kojima je

moguće pristupiti putem Web sučelja. Glavna `cron` skripta je ona koja se pokreće svakih 30 minuta, jer se kroz nju obavlja pokretanje `ipaudit` programa, terminiranje prethodne instance, te generiranje polusatnih izvještaja. Ostale skripte iz polusatnih izvještaja generiraju izvještaje većeg vremenskog opsega (na dnevnoj, tjednoj i mjesečnoj bazi).
Uz instalaciju IPAudit alata dolaze još dva programa:

- `ipstrings` – program za čitanje znakovnih nizova iz datoteka generiranih od strane pcap programa,
- `total` – program za računanje sume i podsume iz stupčastih datoteka (`ipaudit` izlazne datoteke).

3.1. Mrežni izvještaji

Putem Web sučelja moguće je pristupiti generiranim izvještajima koji se stvaraju na vremenskom uzorku od 30 minuta. Osim ovog izvještaja najmanjeg vremenskog opsega, postoje izvještaji koji se generiraju na dnevnoj, tjednoj, te mjesečnoj osnovi. Izgledi svih ovih izvještaja su identični, te se razlikuju samo po već spomenutom vremenskom uzorku u kojem se mrežni promet prikuplja.
Na početnoj stranici IPAudit Web sučelja s lijeve strane se nalazi glavni izbornik, dok se na središnjem dijelu nalaze grafovi različitih kategorija mrežnih izvještaja. Da bi iscrtavanje grafova radilo u stvarnom vremenu, sa svakim novim generiranim izvještajem, na sustavu je potrebno imati instaliran GNUplot programski paket.
Mrežni izvještaji se dijele u više različitih kategorija:

- **Općenita mrežna statistika** – u ovom izvještaju prikazani su neki generalni podaci o prikupljenom mrežnom prometu, kao što je broj konekcija, paketa, okteta, te podaci o odlaznom i dolaznom mrežnom prometu. Na sljedećoj slici (Slika 2) prikazan je primjer izvještaja ovog tipa.

General Stats		Incoming/Outgoing Traffic (bytes)		Internal/External Traffic (bytes)		Local Hosts		Remote Hosts	
Connections	176,806	**Incoming**	94,630,826	**Internal**	27,522,153	**Probed**	104	**Probed**	124,399
Packets	3,368,995	**Outgoing**	1,719,253,660	**External**	53,300	**Responding**	20	**Responding**	145,059
Bytes	1,841,669,057	**Total**	1,813,884,486	**Other**	209,118	**Total**	108	**Total**	147,052

Slika 2: općenita mrežna statistika

- **Lista adresa potencijalnih skeniranja lokalne mreže** – ovaj mrežni izvještaj prezentira listu računala s kojih se odvijaju potencijalna skeniranja lokalne mreže. Tablica se sastoji od IP adrese i naziva računala, te kolikom je broju računala na lokalnoj mreži pristupano s navedene adrese. Ovu tablicu bi trebalo pratiti na dnevnoj ili najmanje tjednoj osnovi ukoliko se IPAudit koristi za praćenje i detekciju neovlaštenih aktivnosti na lokalnoj računalnoj mreži. Neovlašteno skeniranje računala na lokalnoj mreži može biti posljedica pojave novog mrežnog crva ili nekog drugog malicioznog programa, pokušaja provođenja neovlaštenih aktivnosti na segmentu mreže koji se nadzire, a moguće je da postoji kompromitirano računalo s kojeg se dalje skeniraju ostala računala u sustavu. Primjer ovog izvještaja prikazan je na sljedećoj slici (Slika 3).

Possible Incoming Scan Hosts		
IP	Host Name	Local Hosts Contacted
221.211.255.010		84
202.111.174.002		77
083.103.048.231	83-103-48-231.ip.fastwebnet.it	76
202.111.173.082		63
085.065.080.064	85-65-80-64.barak-online.net	59
221.005.251.195		58
219.146.161.010		57
222.141.067.125		54
065.019.084.199	host-199.ccsvt.org	53
133.087.179.035	scylla.ist.hokudai.ac.jp	50
161.053.212.173		47
221.010.182.013		44
067.120.245.181	adsl-67-120-245-181.dsl.sndg02.pacbell.net	43

Slika 3: Lista potencijalnih skeniranja lokalne mreže

- **Lista adresa potencijalnih skeniranja s lokalne mreže** – Jedina razlika u odnosu na prethodni tip izvještaja je ta što se ovdje radi o lokalnim adresama s kojih se potencijalno provode skeniranja prema javnom Internetu. Dok je skeniranje lokalne mreže korisno za proaktivne mjere, ovaj izvještaj pomaže pri reaktivnom djelovanju. Ukoliko na listi postoje lokalna računala s velikim brojem konekcija prema računalima na javnome Internetu, također postoji mogućnost da se radi o kompromitiranom sustavu (pogotovo ukoliko se računalo spaja na potencijalno "sumnjive" servise ili adrese na Internetu). Rijetko je slučaj da radne stanice pristupaju više od 1000 različitih računala na Internetu tako da se na ovaj način mogu detektirati brojna "neuobičajena" ponašanja koja ukazuju na nelegitimno iskorištavane računalnih resursa. Osim računala kompromitiranih od strane neovlaštenih korisnika na ovaj način moguće je detektirati i računala zaražena različitim *spyware* i *ad-aware* malicioznim programima. Primjer ovog izvještaja prikazan je na slici (Slika 4).

Possible Outgoing Scan Hosts		
IP	Host Name	Remote Hosts Contacted
[redacted]	[redacted]	2001

Slika 4: Lista potencijalnih skeniranja s lokalne mreže

- **Lista najprometnijih lokalnih računala** – ova lista sadrži popis računala na lokalnoj mreži s kojih i prema kojim se odvijalo najviše mrežnog prometa. Ovaj izvještaj je koristan prilikom utvrđivanja računala između kojih se prenosi najviše podataka. Logično je da se pri vrhu ove liste nalaze glavni poslužitelji na računalnoj mreži, kao što su Web poslužitelj ili poslužitelj elektroničke pošte. Kontinuiranim praćenjem ove liste kroz nešto duže vrijeme, moguće je steći uvid koja računala su najprometnija, te se pojavom novih adresa na vrhu ove liste preporuča podrobnije istraživanje aktivnosti na dotičnom računalu. Lista se uz IP adresu i naziv računala sastoji od količine dolaznog, odlaznog i ukupnog mrežnog prometa izraženog u oktetima. U vrijeme kada je iznimno popularno korištenje različitih P2P (eng. *peer to peer*) programa, na ovaj način moguće je prilično jednostavno detektirati one korisnike koji krše sigurnosnu politiku organizacije (ukoliko ista postoji) i koji potencijalno narušavaju sigurnost informacijskog sustava. Na slijedećoj slici prikazan je ovaj primjer (Slika 5).

Busiest Local Hosts				
IP	Host Name	Incoming	Outgoing	Total
[redacted]	[redacted]	88,443,791	1,717,362,521	1,805,806,312
[redacted]		353,064	1,721,877	2,074,941
[redacted]	[redacted]	1,394,313	0	1,394,313

Slika 5: lista najprometnijih lokalnih računala

- **Lista najprometnijih udaljenih računala** – Ovaj izvještaj daje informaciju s kojih i prema kojim udaljenim računalima se odvija najviše mrežnog prometa. Praćenjem liste ovih adresa moguće je otkriti potencijalno sumnjive transakcije. Primjer je prikazan na slici (Slika 6).

Busiest Remote Hosts				
IP	Host Name	Incoming	Outgoing	Total
067.068.184.216	Toronto-HSE-ppp3770809.sympatico.ca	2,591,391	92,045,518	94,636,909
081.236.128.109	h109n1-m-rg-gr100.ias.bredband.telia.com	2,479,664	87,005,954	89,485,618
085.060.008.072	85-60-8-72.mad5.adsl.uni2.es	1,918,103	71,792,458	73,710,561
071.194.058.133		1,989,347	69,766,077	71,755,424
062.193.108.113		2,595,830	61,818,720	64,414,550

Slika 6: Lista najprometnijih udaljenih računala

- **Lista najprometnijih parova računala** – ovaj izvještaj prikazuje parove računala između kojih se odvijalo najviše mrežnog prometa (Slika 7). Ova lista je korisna za nadgledanje regularnosti provedenih transakcija. Za svaki od parova u listi navedena je ukupna količina međusobno izmijenjenih podataka.

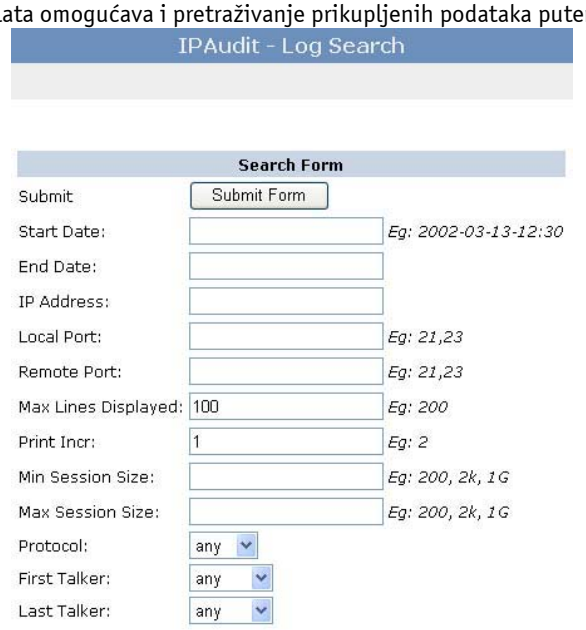
Busiest Host Pairs						
Local IP	Remote IP	Local Host Name	Remote Host Name	Incoming	Outgoing	Total
	067.068.184.216		Toronto-HSE-ppp3770809.sympatico.ca	2,591,391	92,045,518	94,636,909
	081.236.128.109		h109n1-m-rg-gr100.ias.bredband.telia.com	2,479,664	87,005,954	89,485,618

Slika 7: Najprometniji parovi računala

Osim upravo navedenih mrežnih izvještaja, također je moguće dobiti pregled IP adresa na kojima su pokrenuti jedni od slijedećih servisa:

- HTTP,
- HTTPS,
- Mail,
- Telnet,
- SSH.

Putem ovog izvještaja također je moguće detektirati kompromitirana računala. Kao primjer može se navesti otkrivanje radne stanice pri vrhu SMTP poslužitelja, što navodi na zaključak da je računalo vrlo vjerojatno zaraženo i pritom iskorišteno za širenje neželjene elektroničke pošte (SPAM).
Web sučelje IPAudit alata omogućava i pretraživanje prikupljenih podataka putem forme (*Slika 8*).



Slika 8: Forma za pretraživanje

Forma omogućuje detaljno pretraživanje svih do tada prikupljenih podataka o mrežnom prometu. Vremenski period je podesiv sve do minute, dok IP adrese koje se pretražuju mogu biti lokalne adrese, ali isto tako i adrese s vanjskih mreža i javnog Interneta. Nakon polja u koja se unose mrežni portovi, slijede dva polja koja definiraju način ispisa pronađenih rezultata. Kroz definiranje veličine sjednice moguće je razlikovati prijenose podataka od skeniranja mrežnih portova. Padajući izbornik omogućava izbor jednog od protokola (ICMP, TCP, UDP), dok posljednja dva izbornika definiraju tko je započeo a tko završio komunikaciju.

4. Zaključak

IPAudit je alat s velikim brojem funkcionalnosti koji omogućava više načina prikaza mrežnog prometa putem Web sučelja. Instalacija je vrlo jednostavna, dok za upoznavanje korištenja svih opcija nije potrebno utrošiti mnogo vremena. Putem dodatnog paketa za pregled prikupljenog mrežnog prometa putem Web sučelja, dostupni su brojni izvještaji koji omogućuju pregledan i temeljit uvid u aktivnosti na lokalnoj računalnoj mreži, te informacije o eventualnim sigurnosnim incidentima i anomalijama.
Kao dodatna kvaliteta ovog alata može se navesti činjenica da je u potpunosti besplatan, te zaista predstavlja vrlo dobro rješenje za nadgledanje mrežnog prometa na lokalnoj mreži, naročito u kombinaciji sa već postojećim IDS alatima na sustavu.

5. Reference

[1] IPAudit man page, http://www.sp.uconn.edu/~jrifkin/ipaudit/
[2] IPAudit home page, http://ipaudit.sourceforge.net/
[3] Introduction to IPAudit, http://www.securityfocus.com/