HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sustavi za sprečavanje neovlaštenih aktivnosti (IPS)

CCERT-PUBDOC-2006-01-145

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

Sprečavanje neovlaštenih aktivnosti (eng. *Intrusion prevention*) predstavlja jednu od tehnologija koja omogućava podizanje sigurnosti sustava. Razvojem i uporabom sve naprednijih metoda napada na računalne sustave, pojavljuje se potreba za kombinacijom različitih sustava i alata, koji ispravno podešeni i održavani omogućavaju održavanje potrebne razine sigurnosti. Naime, postojeći mrežni vatrozidi (eng. *Network Firewalls*) i sustavi za detekciju neovlaštenih aktivnosti – IDS (eng. *Intrusion Detection Systems*) mogu razdvajati mrežni promet na dozvoljeni i nedozvoljeni. Međutim, oni uglavnom postaju nemoćni u slučaju kriptiranog mrežnog prometa, budući da ne mogu analizirati sadržaj mrežnih paketa i na osnovi provedene analize sprečavati zlonamjerne aktivnosti u stvarnom vremenu. Sljedeći problem javlja se kod preklapanih mreža (eng. *switched networks*) gdje bi trebalo postaviti veliki broj agenata koji bi omogućili praćenje mrežnog prometa na svim njenim segmentima. I na kraju, IDS alati javljaju veliki broj lažnih napada na sustav, čime otežavaju praćenje i nadgledanje prometa i aktivnosti.

Sustavi za sprečavanje neovlaštenih aktivnosti – IPS (eng. *Intrusion Prevention Systems*) mogu se realizirati kao samostalan program ili u kombinaciji sa specijaliziranim sklopovljem. Takvi programi sposobni su prepoznati poznate, ali i određene nepoznate napade te onemogućiti iste prije nego dođu do računala prema kojima su bili usmjereni. Sustavi za sprečavanje neovlaštenih napada mogu biti namijenjeni zaštiti pojedinih računala i/ili zaštiti cjelokupnih mreža.

Ovaj dokument opisuje razvoj IPS alata iz alata za detekciju neovlaštenih aktivnosti, vrste i način korištenja sustava za sprečavanje neovlaštenih aktivnosti te zahtjeve koji se postavljaju pred IPS alate. Na kraju dokumenta dan je i popis češće korištenih IPS alata.

2. IDS – preteča i osnovica IPS alata

U većini slučajeva se za zaštitu računalnih resursa koriste antivirusni programi i vatrozidi namijenjeni blokiranju neovlaštenih aktivnosti, kao i specijalizirani sustavi za detekciju neovlaštenih aktivnosti - IDS. Takva kombinacija sigurnosnih mehanizama sprečava velik broj neovlaštenih aktivnosti. Ponekad je međutim potrebno koristiti i druge tehnologije zaštite. Vatrozidi npr. mogu blokirati različite portove i protokole pa čak i pratiti stanje pojedinih veza (eng. *stateful inspection*), ali oni ipak ne mogu učiniti mnogo ukoliko se napad izvršava preko dozvoljenih protokola i portova. U takvim slučajevima mogu jedino pružiti zaštitu od napada velikim količinama paketa (eng. *Denial of Service*). Nedovoljnu zaštitu pružaju i sustavi za detekciju neovlaštenih aktivnosti. Njihov rad zasniva se na prikupljanju informacija sa čitavog niza mrežnih i računalnih izvora i analiziranju tih informacija sa ciljem otkrivanja eventualnih nedozvoljenih aktivnosti i zlouporaba. Oni prate i analiziraju mrežni promet, ali ne čine ništa da bi spriječili neželjeni promet. Ukoliko se on uoči, najčešće se samo obavještavaju nadležne osobe.

IDS alati dijele se u dvije grupe:

- Računalno bazirani IDS sustavi (eng. *Host IDS*) - sustavi namijenjeni analiziranju mrežnog prometa koji je usmjeren prema samom računalu na kojem je postavljen IDS.
- Mrežni IDS sustavi (eng. *Networks IDS*) – sustavi namijenjeni prikupljanju i analiziranju mrežnog prometa koji nije nužno proizveden ili usmjeren prema računalu na kojem je postavljen IDS.

Rad IDS alata zasniva se na pregledavanju različitih dnevničkih zapisa (eng. *log*) te sadržaja mrežnih paketa. Obje vrste podataka sadrže informacije o aktivnostima korisnika pa je na temelju analize njihovog sadržaja moguće identificirati neovlaštene aktivnosti. Za to se uobičajene koriste dvije metode koje se u novije vrijeme i kombiniraju:

- Prepoznavanje potpisima – sadržaj dnevničkih zapisa i/ili mrežnih paketa šalje se u pretraživački program gdje se uspoređuje s unaprijed definiranim potpisima napada.
- Prepoznavanje statističkim anomalijama – na temelju profila uobičajenog rada sustava koji se dobiva prikupljanjem i statističkom obradom tih podataka prepoznaju se anomalije koje se prijavljuju kao napad na sustav.

Prednost korištenja IDS-a je u tome što oni ne usporavaju mrežni promet. Analizu mrežnog prometa moguće je obavljati na računalu posebno namijenjeno samo svrsi prepoznavanja i praćenja napada na određeno računalo, odnosno aplikaciju.

Uz brojne prednosti, postoje i određeni nedostaci IDS-ova:

- Detekcija bez sprečavanja – IDS-ovi uglavnom ne mogu zaustaviti ili usporiti aktivne mrežne napade. Naime, zbog mogućih dojava o lažnim napadima na sustav, nije niti poželjno da IDS-ovi prekidaju uspostavljene veze, što bi rezultiralo velikim brojem prekida u radu.
- Vremenski raskorak između napada i detekcije – zbog velikog broja zapisa koje IDS treba analizirati te moguće potrebe za naknadnom provjerom dojave o napadu od strane administratora, IDS-ovi pružaju spor odgovor na napade na računalne i mrežne resurse.
- Lažne dojave – IDS-ovi pregledavajući sadržaj mrežnih paketa i dnevničkih zapisa često krivo okarakteriziraju dozvoljeni promet kao nedozvoljeni, odnosno nedozvoljeni promet kao dozvoljeni, do čega dolazi uslijed previše općenitih definicija potpisa pojedinih napada.
- Velike količine dnevničkih zapisa o napadima – zbog činjenice da IDS nije u mogućnosti prekinuti napade, IDS generira onoliko upozorenja koliko ima dnevničkih zapisa o samim napadima. Pošto se ponekad i legitimni promet neopravdano prepoznaje kao napad, količina upozorenja za administratore se time dodatno povećava.
- Izostanak detekcije novih vrsta napada – kako IDS-ovi uglavnom uspoređuju sadržaje dnevničkih zapisa i mrežnih paketa s definiranim potpisima za napade, novi napadi nisu sadržani u bazi potpisa pa ih IDS ne prepoznaje. Detekcija nepoznatih napada moguća je samo ukoliko je IDS zasnovan ili kombiniran s metodom prepoznavanja statističkih anomalija.

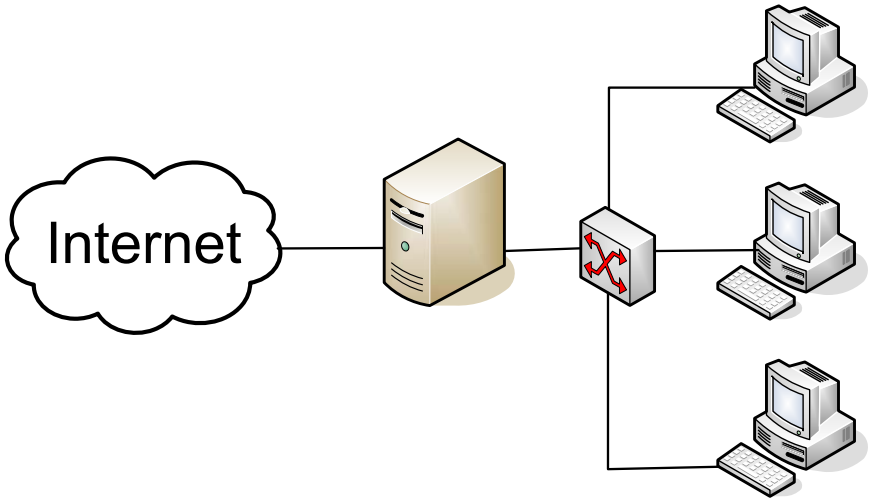
Zbog spomenutih nedostataka nužno je razinu sigurnosti pomaknuti s detekcije zlonamjernih aktivnosti na njihovo sprečavanje, pa je tako i došlo do razvoja sustava za sprečavanje neovlaštenih aktivnosti koji omogućavaju preventivno djelovanje glede računalnih napada i izbjegavanje nastajanja štete koja bi bila prouzročena tim napadima.

3. Potreba za IPS alatima

Zbog porasta zlonamjernih aktivnosti u računalnim mrežama, potrebno je kontinuirano održavati sigurnost računalnih i mrežnih resursa na odgovarajućoj razini. Implementacijom različitih sigurnosnih alata ne uspijevaju se međutim, u potpunosti zaštititi mreže i računala od različitih napada. Prijetnju pri tome ne predstavljaju samo vanjski napadači koji mogu ostvariti svoje zlonamjerne aktivnosti oslanjajući se na propuste u programskim paketima i operacijskim sustavima, već i lokalni zlonamjerni korisnici koji mogu poznavanje svoje mrežne organizacije također iskoristiti za razne zlonamjerne aktivnosti. Ukoliko se takve aktivnosti ne otkriju na vrijeme, one mogu prouzročiti veliku financijske štete zbog npr. nedostupnosti nekog računalnog ili mrežnog resursa.
Sustavi za sprečavanje neovlaštenih aktivnosti smatraju se „nasljednicima“ sustava za prepoznavanje neovlaštenih aktivnosti. Njihova sposobnost zaštite računala od definiranih, ali i nedefiniranih nepoznatih napada, izrazito je korisna, osobito u okolnostima sve različitijih i sve naprednijih zlonamjernih aktivnosti. Najčešće nije dovoljno samo prepoznavanje izvedenih napada što omogućavaju IDS-ovi, jer naknadno mijenjanje sigurnosne politike ne sprečava već nastalu štetu. Stoga je za održavanje sigurnosti u računalnom i mrežnom okruženju vrlo često potrebno implementirati i sustave za sprečavanje neovlaštenih aktivnosti.

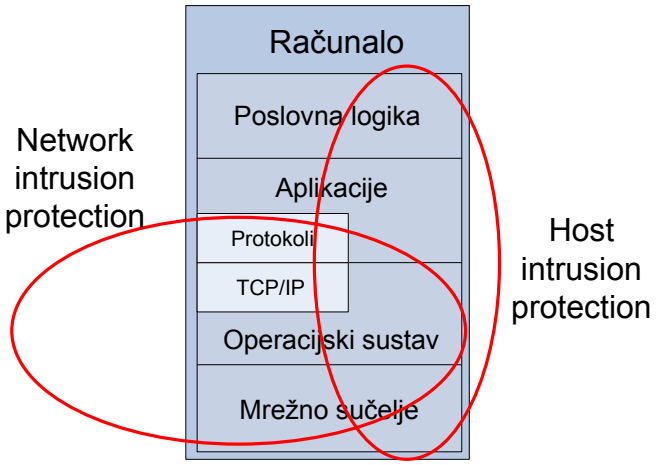
4. IPS implementacije

IPS alati namijenjeni su zaštiti mreža (eng. *NIPS – Network IPS*) ili zaštiti klijentskih i poslužiteljskih računala (eng. HIPS - *Host IPS*). Vrlo često potrebno je kombinirati IPS alate za zaštitu mreža i sustave za sprečavanje neovlaštenih aktivnosti na klijentskim računalima. Na slici *Slika 1* prikazan je jedan od primjera mogućeg korištenja kombinacije NIPS i HIPS alata.



Slika 1: Primjer korištenja NIPS i HIPS alata koji omogućava potpuniju zaštitu računalnih resursa

NIPS i HIPS alati prikupljaju podatke o aktivnostima unutar sustava i analiziraju ih te prepoznaju neovlaštene aktivnosti. Na slici *Slika 2* prikazani su osnovni izvori informacija od kojih NIPS i HIPS alati prikupljaju potrebne podatke o aktivnostima.



Slika 2: Osnovni izvori informacija NIPS i HIPS alata

4.1. HIPS - IPS za zaštitu pojedinih računala

Uslijed rastuće količine različitih zlonamjernih programa poput virusa, crva, trojanaca, programa koji otvaraju različite nepoželjne reklame (eng. *adware*) te programa koji neovlašteno prate aktivnosti korisnika (eng. *spyware*), zaštita samog računala na razini operacijskog sustava postaje sve važnije područje računalne sigurnosti. Zbog opasnosti koje su prisutne na internetu, jedno od prijašnjih rješenja održavanja potrebne razine sigurnosti sustava predlagalo je da se pristup na internet omogući samo pouzdanim zaposlenicima. Takav način rada danas nije prihvatljiv. Korisnici moraju imati siguran pristup različitim mrežnim resursima. Jedna od mogućnosti da se to osigura jest korištenje HIPS alata za sprečavanje neovlaštenih aktivnosti.

HIPS se realizira kao aplikacija koja je instalirana na računalu (klijent ili poslužitelj) i ta aplikacija radi kao agent koji obrađuje različite sigurnosne politike pročitane iz konfiguracijske datoteke koja može biti smještena na središnjem upravljačkom poslužitelju. Korištenjem središnjeg upravljačkog poslužitelja olakšava se održavanje i praćenje cijelog sustava.

Metode koje se koriste za implementaciju HIPS-a mogu varirati. Na primjer, HIPS može nakon instalacije neko vrijeme pratiti rad svih procesa na računalu te ih spremati u svoju bazu uobičajenih aktivnosti računala. Nakon što je „naučio“ uobičajeni aktivnosti u radu računala, HIPS može prepoznati sve procese koji se ponašaju drugačije od uobičajenog ponašanja pa te procese može prepoznati i dojaviti da se radi o nedopuštenim aktivnostima ili ih ukloniti. Također, u ekstremnim uvjetima moguće je s mreže ukloniti i ugroženo računalo, kako se ne bi zarazila ostala računala. Pod pretpostavkom da je svaka promjena nepoželjna, računala u mreži će se uspješno štititi od svih nepoznatih napada koji predstavljaju promjenu u uobičajenom načinu rada računala.

Drugi koncepti rada HIPS-a uključuju integraciju s vatrozidom instaliranim na istom računalu. Time se ostvaruje zaštita računala na mrežnoj razini pa se potencijalni zlonamjerni paket odbacuje prije nego što uopće dospije do aplikacije kojoj je usmjeren. Također, moguće su i izvedbe zasnovane na traženju različitih zlonamjernih kombinacija asemblerskih naredbi koje bi mogle uzrokovati prepisivanje spremnika (eng. *buffer overflow*) i slično.

4.2. NIPS - IPS za zaštitu mreže

NIPS kombinira odlike standardnih IDS-ova i vatrozida s dodatnim metodama sprečavanja zlonamjernih aktivnosti. Kao i tipični vatrozid, tako i NIPS ima dvije mrežne kartice, jednu namijenjenu unutarnjoj mreži, a drugu namijenjenu vanjskoj mreži. Po pojavi paketa na bilo kojem mrežnom sučelju, IPS ih analizira i odlučuje da li predstavljaju prijetnju. Ukoliko je paket, koji može biti i dio dozvoljene veze, prepoznat kao zlonamjeran – paket se odbacuje i ne propušta na drugu mrežu. Ostali paketi koji su povezani s tim paketom i dijele istu sjednicu, automatski se odbacuju. Opisani način rada IPS-a je preventivan za razliku od IDS-a koji prosljeđuje pakete pa tek onda kontrolira da li paket predstavlja prijetnju.

Pojedini IDS-ovi, nakon što ustanove da je uspostavljena veza nelegitimna, tu vezu mogu i prekinuti, ali paketi koji su stigli prije spoznaje o nelegitimnosti veze ipak bivaju proslijeđeni na svoja odredišta gdje mogu uzrokovati probleme u radu.

Sve funkcionalnosti vatrozida zadržane su i u NIPS-u. Glavna zadržana funkcionalnost je *stateful inspection* tehnologija koja se zasniva na kontinuiranom praćenju i analizi pojedinih segmenata veze koji prolaze kroz vatrozid, kako bi se na temelju njih u stvarnom vremenu mogle donositi pravilne odluke o filtriranju paketa.
Glavno poboljšanje koje je dodano kod NIPS-a je dubinska analiza sadržaja paketa (eng. *Deep Packet Inspection*) u stvarnom vremenu. Dubinska analiza sadržaja paketa u stvarnom vremenu označava različite metode pomoću kojih NIPS može pretraživati sadržaj pojedinih paketa ili skupine paketa koji su elementi iste veze. Pretraga se obavlja u potrazi za zlonamjernim kodom ili sličnim programskim anomalijama. Pri tomu se registrira, analizira i filtrira sadržaj paketa koji su povezani s IP baziranim aplikacijama.
Dubinska analiza sadržaja paketa u stvarnom vremenu omogućava NIPS-u da uoči prikrivene napade prvenstveno usmjerene na Web, e-mail i DNS poslužitelje. Pošto se unutar jednog mrežnog paketa ne može otkriti zlonamjerni sadržaj, NIPS prikuplja veće količine mrežnih paketa te ih skupno obrađuje. Paketi se analiziraju, nanovo sastavljaju i u slučaju nepronalaženja sumnjivog zlonamjernog sadržaja prosljeđuju na odredište (lokalna aplikacija ili mrežno sučelje) na koje su paketi i usmjereni. Takvim radom NIPS može dobiti potpunu sliku o podacima koji su primljeni te primijeniti proceduru koju definira korisnik. Prilikom ponovnog slaganja paketa NIPS može ispraviti nepravilnosti u poretku paketa koje su eventualno nastale u prijenosu ili koje su namjerno izazvane od strane napadača.

5. Zahtjevi na IPS alate

Pred IPS alate postavljaju se brojni zahtjevi koje oni trebaju ispuniti kako bi se omogućilo da funkcionalno odrađuju svoj zadatak u stvarnom vremenu. Najvažniji su sljedeći zahtjevi:

- Slijedno postavljanje – IPS mora biti postavljen na takvu poziciju u mreži koja osigurava da ga paketi ne zaobilaze. Jedino na takav način IPS može provoditi potpunu kontrolu svih dolaznih paketa te automatski odbacivati pakete koji se prepoznaju kao zlonamjerni, kao i one pakete koji slijede prethodno odbačene pakete.
- Pouzdanost i dostupnost – IPS ne smije uzrokovati nedostupnost resursa (eng. *Denial of Service*) na mreži. Korisniku je dozvoljeno definiranje pravila prema kojem se u slučaju prestanka rada IPS-a sav promet preusmjerava na neki drugi kontrolni mehanizam. Ukoliko rezervni kontrolni mehanizam nije dostupan ili dovoljno pouzdan, korisniku je dozvoljeno definiranje pravila koje omogućava da se sav promet propušta ili zabranjuje, ovisno o tome kako je propisano sigurnosnom politikom. Dostupnost mora biti takva da IPS može izvršiti nadogradnju s novo definiranim pravilima i potpisima bez ponovnog podizanja sustava.
- Visoka učinkovitost obrade – IPS mora obrađivati pakete brzinom koja minimalno utječe na brzinu prijenosa. Brzina obrade paketa praktički mora biti jednaka brzini koju podržavaju preklopnici, a svakako veća od brzine koju pružaju mrežni vatrozidi.
- Neupitna preciznost – kvalitetna obrada paketa je imperativ koji IPS mora postići. Svaki pogrešno odbačeni paket uzrokovao bi nedostupnost resursa, što zahtjeva redovit unos novih potpisa za detekciju zlonamjernih aktivnosti. Za aktivnosti za koje se sa sigurnošću ne može utvrditi da su zlonamjerne, IPS treba generirati upozorenja pomoću kojih će se daljnjom analizom definirati nova pravila.
- Napredne metode upozoravanja – svako pristiglo upozorenje na središnjoj se konzoli analizira i ukoliko je moguće povezuje s ostalim upozorenjima. Ovim postupkom smanjuje se potreba za ručnom obradom te se na taj način izbjegavaju eventualne greške koje mogu nastati ručnom obradom upozorenja.
- Otpornost na nove napade – IPS treba posjedovati metode obrade podataka koje omogućavaju prepoznavanje zlonamjernih aktivnosti koje nisu definirane u potpisima.

6. IPS alati

Iako brojni proizvođači uz svoje alate stavljaju naznaku da je riječ o IPS alatima, nije ih moguće sve takvima i smatrati. Primjerice, alati koji prosljeđuju potencijalno zlonamjerne pakete na odredište pa tek naknadno prepoznaju da ta veza sadrži određenu zlonamjernu aktivnost, nisu pravi IPS alati iako ih proizvođači takvima predstavljaju.
U nastavku su navedeni neki od poznatijih i češće korištenih NIPS i HIPS alata.

NIPS alati:

- Sentivist IPS
  http://www.nfr.com/solutions/sentivist-ips.php
- DefensePro
  http://www.radware.com/content/products/dp/default.asp
- UnityOne
  http://www.tippingpoint.com/products.html
- Border Guard
  http://www.stillsecure.com/index.jsp?sector=products&sub_sector=bg&cur_page=bg_gateway
- Hogwash
  http://hogwash.sourceforge.net
- StoneGate IPS
  http://www.stonesoft.com/products/IPS/
- IntruShield
  http://www.mcafeesecurity.com/us/products/mcafee/network_ips/category.htm?cid=10355
- iP Enforcer
  http://www.ipolicynet.com/solutions/e_ipenforcer.html
- Magnia 2000Ri
  http://cn.toshiba.co.jp/prod/iaserver/magnia/2000ri/anti/
- Netscreen
  http://www.juniper.net/products/intrusion/
- RealSecure Guard
  http://www.iss.net/products_services/enterprise_protection/rsnetwork/guard.php

HIPS alati:

- DefenseWall HIPS
  http://www.softsphere.com
- McAfee Host Intrusion Prevention
  http://www.mcafee.com
- Cisco Security Agent
  http://www.cisco.com
- Host Intrusion Prevention Service
  http://www.secureworks.com
- Third Brigade Deep Security
  http://www.thirdbrigade.com
- Symantec Critical System Protection
  http://www.symantec.com
- SecureHost
  http://www.intrusion.com
- ThreatSentry
  http://www.privacyware.com
- Proventia Desktop
  http://www.iss.net
- WehnTrust
  http://www.wehnus.com
- AppDefend
  http://www.ghostsecurity.com

7. Zaključak

Sustavi za sprečavanje neovlaštenih aktivnosti štite računalne mreže i/ili pojedina računala podižući sigurnosnu zaštitu na višu razinu. Grupiranje mrežnih paketa te analiziranje cjelokupnog sadržaja namijenjenog određenim aplikacijama prije nego što stignu do same aplikacije, omogućava pravovremenu detekciju i sprečavanje zlonamjernih aktivnosti. Prilagođeno upozoravanje bez ponavljanja istih upozorenja olakšava administratorima nadzor i upravljanje sustavom. Mogućnost detekcije nedefiniranih zlonamjernih aktivnosti olakšava rad i smanjuje ukupne financijske troškove uslijed veće dostupnosti mrežnih i računalnih resursa.

Ipak, pred sustave za sprečavanje neovlaštenih aktivnosti postavljaju se veliki zahtjevi. Jedan od osnovnih zahtjeva je zahtjev za održavanjem visokih performansi sustava koji je vrlo teško ostvariti, budući da sustavi za sprečavanje neovlaštenih aktivnosti analiziraju ne samo oznake mrežnih paketa, kao što to rade vatrozidi, već i sadržaj pa time usporavaju protok prometa. Također, za implementaciju sustava koji bi zadovoljio sve postavljene zahtjeve trebalo bi osigurati visoka financijska sredstva, stoga prilikom planiranja ovakvih sustava treba usporediti troškove realizacije sustava s troškovima za slučaj nedostupnosti mrežnih i računalnih resursa uslijed neovlaštenih aktivnosti.

8. Literatura

[1] Pete Lindstrom: Intrusion Prevention Systems (IPS): next generation firewalls, Spire Research Report, ožujak 2004.
[2] Top Layer Networks, Inc., Beyond IDS: Essentials of Network Intrusion Prevention, studeni 2002
[3] NSS Group, Intrusion Prevention Systems (IPS), siječanj 2004.
[4] Neil Desai, Intrusion Prevention Systems: the Next Step in the Evolution of IDS, veljača 2003.
[5] Network Intrusion Prevention Systems, http://www.networkintrusion.co.uk/inline.htm, siječanj 2005.
[6] Host Intrusion Prevention Systems, http://www.networkintrusion.co.uk/hips.htm, siječanj 2005.
[7] Secure Computing Corporation, Intrusion Prevention Systems (IPS), Part one: Deciphering the inline Intrusion Prevention hype, and working toward a real-world, proactive security solution, 2003.