HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Detekcija neovlaštenih upada (IDS)

CCERT-PUBDOC-2000-09-04

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. DEFINICIJE 4

3. POTREBA ZA IDS ALATIMA 4

4. IMPLEMENTACIJA IDS ALATA 5

4.1. DETEKCIJA POTPISIMA 5
4.2. DETEKTIRANJE STATISTIČKIM ANOMALIJAMA 6

5. ODGOVOR NA NAPADE 6

6. PROTOTIP IDS ALATA RAZVIJENOG NA LSS, ZESOI, FER 7

7. DRUGI MODELI 7

8. SMJEROVI ISTRAŽIVANJA 8

9. ZAKLJUČAK 8

10. LITERATURA 9

1. Uvod

Detekcija neovlaštenih upada (eng. Intrusion detection) predstavlja izrazito važnu komponentu čitavog sigurnosnog sustava. Sigurnosne mehanizme sustava potrebno je tako dizajnirati da onemogućavaju neovlašteni pristup računalnim resursima i podacima. Međutim, kako je potpuno sprečavanje neovlaštenog pristupa nemoguće izvesti, današnja dostignuća sigurnosnih sustava pokušavaju detektirati neovlaštene upade na osnovu kojih se poduzimaju određene akcije prije nego što je neovlašteni korisnik počinio štetu.

Anderson [1], koji je predstavio koncept detekcije neovlaštenih upada još 1980. definira pokušaj upada ili ugrožavanje sustava (eng. Intrusion attempt) kao pokušaj pristupa privatnim informacijama, manipulacijom tih informacija ili pokušajem onesposobljavanja ili sprječavanja rada udaljenog računalnog sustava.

Od tada, definirano je nekoliko tehnika za detekciju neovlaštenih upada. Ovaj dokument opisuje zašto su sustavi za detekciju neovlaštenih upada potrebni, glavne tehnike, današnja dostignuća i budućnost. Na kraju dokumenta je dan i uvid u prototip alata za detekciju neovlaštenih upada razvijen na LSS, ZESOI, FER.

2. Definicije

U ovom dokumentu korišteni su slijedeći termini:

Mrežna sigurnost specificira da računalni sustavi i mrežni elementi ispunjavaju svoju ulogu kao što je očekivano u svezi zaštite korisničkih podataka i informacija. Ciljevi mrežne sigurnosti predstavljaju povjerljivost podataka (što osigurava da samo ovlašteni korisnici mogu pregledavati određene informacije), kontrola (samo autorizirani korisnici mogu mijenjati dozvole za pregledavanje određenih informacija) i integritet (samo autorizirani korisnici mogu mijenjati ili brisati određene informacije), autentičnost (ispravnost atributa ili opisa informacija).

Detekcija neovlaštenih aktivnosti zasnovana je na skupljanju informacija sa čitavog niza mrežnih i računalnih izvora i analiziranju tih informacija sa ciljem otkrivanja eventualnih nedozvoljenih aktivnosti i zlouporaba.

Sigurnosna politika je definicija organizacije prema sigurnosti sustava. Ona definira što pojedina organizacija smatra važnim i specificira kako se te važne informacije treba zaštititi. U praktičnoj upotrebi, sigurnosna politika se definira pravilima i procedurama koja specificiraju kako se sigurnosna politika provodi na računalnim sustavima i mreži.

3. Potreba za IDS alatima

Velika učestalost napada na računalne sustave na Internetu implicira nužnost uporabe IDS alata za provođenjem i uspostavljanjem sigurnosne politike organizacije na javno, ali i interno dostupnim računalnim sustavima. Istraživanja pokazuju da najveći broj neovlaštenih upada na računalne sustave dolazi upravo sa internih računalnih mreža, odnosno zaposlenika organizacija.

Postoje dva načina sprječavanja neovlaštenih aktivnosti korisnika. Prvi način je izrada potpuno sigurnog računalnog sustava. Moguće je napraviti takav računalni sustav koji će zahtijevati od svih korisnika potpunu identifikaciju i autentikaciju, te koji će zaštititi podatke različitim kriptografskim metodama i vrlo striktnim mehanizmima za kontrolu pristupa. Međutim, ovo rješenje nije moguće izvesti iz nekoliko razloga:

U praksi, nije moguće izraditi potpuno sigurni računalni sustav. Miller [2] daje iscrpan izvještaj o sigurnosnim rupama popularnih programa i operacijskih sustava koji ukazuje da (a) ne postoji operacijski sustav ili program bez sigurnosnih rupa i (b) da se proizvođači niti ne trude napraviti takav operacijski sustav ili program. Dizajniranje i implementiranje potpuno sigurnog računalnog sustava je izrazito kompliciran zadatak. Osim toga, kriptografske metode imaju druge probleme – zaporke je moguće otkriti, korisnici mogu izgubiti ili zaboraviti svoje zaporke i cijeli kriptografski sustavi mogu biti provaljeni.

Osim navedenih sigurnosnih propusta potrebno je napomenuti da i na potpuno siguran sustav može biti provaljeno ukoliko korisnici iznutra zlouporabe svoje korisničke privilegije.

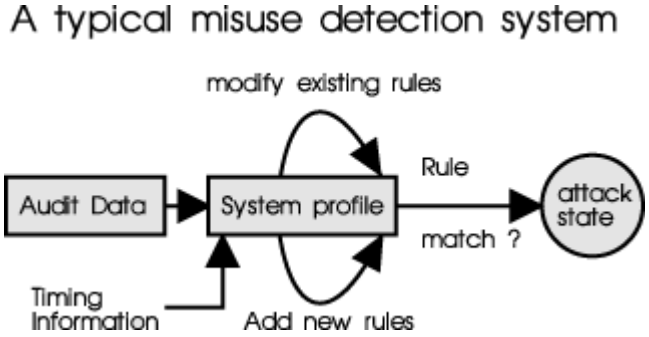
Drugi način sprječavanja neovlaštenih aktivnosti korisnika je upravo detekcija tih aktivnosti. Ukoliko postoji napad na neki računalni sustav, potrebno je taj napad detektirati što je prije moguće (poželjno u stvarnom vremenu) da bi se mogla poduzeti neka akcija. Ovo esencijalno predstavlja predmet rada alata za detekciju neovlaštenih upada (IDS-a). IDS alati obično ne poduzimaju preventivne mjere kada su detektirane neovlaštene aktivnosti, već obično samo obavještavaju za to nadležne osobe.
Najčešći način detektiranja neovlaštenih aktivnosti implementiran u IDS alatima je pregledavanje logova generiranih od strane operacijskog sustava. Logove predstavljaju zapise aktivnosti korisnika na računalnim sustavima koji su zapisani u pojedine datoteke kronološkim redoslijedom. Budući da se u njih zapisuju sve aktivnosti korisnika neovlaštene aktivnosti je moguće detektirati i ručnim pregledavanjem datoteka sa logovima od strane administratora sustava. Međutim, ove datoteke su iznimno velike što ručno pregledavanje čini nemogućim. IDS alati automatiziraju pregledavanje datoteka sa logovima.
U mnogo slučajeva, čak i nakon napada, važno je analizirati podatke o aktivnostima iz log datoteka kako bi se mogla ustanoviti pričinjena šteta ili otkrivanje neovlaštenih korisnika, kao i koraci koje je potrebno poduzeti da bi se takvi napadi onemogućili u budućnosti. IDS alat se također može koristiti za analiziranje tih podataka.
Spaffordov izvještaj [3] koji govori o nužnosti implementiranja IDS alata pokazuje da je krađa informacija porasla za 250% u zadnjih 5 godina, da je 99% velikih organizacija prijavilo barem jedan sigurnosni incident i da šteta pričinjena neovlaštenim upadima u računalne sustave raste na 10 milijardi US dolara godišnje. Zbog ovdje navedenih činjenica vidimo nužnost implementacije dobrog IDS alata na računalne sustave.

4. Implementacija IDS alata

Prilikom postavljanja IDS alata administratori mrežnih sustava moraju odgovoriti na dva ključna pitanja: Gdje je potrebno postaviti IDS alat i kako će funkcionirati taj IDS alat? Što se tiče pitanja gdje, IDS može biti postavljen na računalu na kojem rade korisnici, na mreži gdje skuplja podatke ili u kombinaciji računala i mreže. Drugo pitanje je kompliciranije. Većina današnjih komercijalnih IDS paketa koristi jedan od dva pristupa za detektiranje neovlaštenih aktivnosti: pregledavanje eksplicitnih potpisa poznatih napada ili pregledavanje za statističke anomalije preko poznatih uzoraka. Ova dva pristupa za detektiranje neovlaštenih aktivnosti u suprotnosti jedan sa drugim. Prvi pristup pregledava eksplicitno podatke za koje se zna da su neovlašteni dok drugi smatra bilo koju anomaliju implicitno neovlaštenom. Naravno, postoje dobre i loše strane svakog od ovih pristupa.

4.1. Detekcija potpisima

Detekcija potpisima je prilično jednostavna za implementaciju [5]. Ovaj način podrazumijeva skupljanje podataka mrežnog prometa ili zapisa iz sigurnosnih logova. Podaci koji su ovako dobiveni šalju se u pretraživački program gdje se uspoređuju sa predefiniranim potpisima za napade neovlaštenih korisnika (uzorci ili atributi koji definiraju napad). Ako jedna grupa ovih podataka odgovara potpisu za pojedini napad, podaci se dalje šalju na funkciju za odgovor IDS alata.



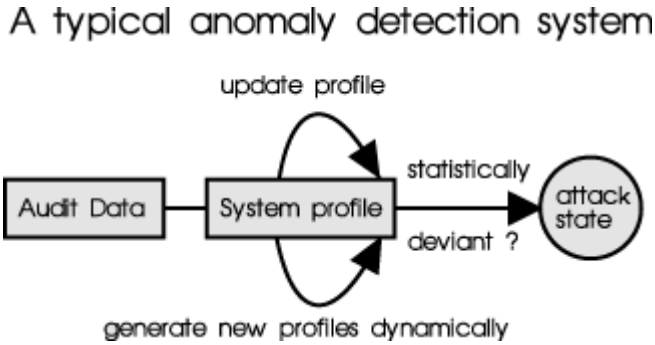
Loša stvar kod IDS alata koji koriste metodu detekcije potpisima je očita. Naime, oni mogu detektirati samo napad koji je eksplicitno definiran u potpisima koji se nalaze u njihovoj bazi (kao i alati za detektiranje virusa). Problem koji s time nastaje je također očit: što je potpis za pojedini napad općenitiji to će IDS alat prijavljivati više lažnih napada. Ove lažno pozitivne detekcije napada znače

da ova detekcija neće biti vrlo pouzdana. Dakle, da bi metoda detekcijom potpisa bila efektivna, potpis napada mora biti jako dobro postavljen na granicu između previše općenitog (koji otkriva napade koji ne postoje) i previše specifičnog potpisa (koji izostavlja malo promijenjene napade). Još jedan problem koji je karakterističan za metode detekcije potpisima je problem prevelikog trošenja računalnih resursa. U provedenom istraživanju pokazano je da neovlašteni korisnici obično koriste distribuirane napade prolongirane preko dugih vremenskih perioda. Detektiranje takvih napada sa IDS alatom za detekciju u stvarnom vremenu metodom detekcije potpisa može biti vrlo komplicirano, budući da sustav na kojem se nalazi IDS mora držati ogromne količine podataka za vrijeme dugog perioda. Količina potrebnih računalnih resursa (memorije) tako za takav IDS sustav raste do praktički nemoguće.

Da bi detektirali napade koji nastaju u velikom vremenskom razdoblju, neki IDS sustavi procesiraju podatke koji su zapisani prethodno (kao što su mrežni paketi ili logovi). Ova metoda, međutim, povećava zahtjeve za procesorskim vremenom, budući da je potrebno izvoditi veće proračune. Međutim, ovakav način detektiranja može biti prihvatljiv za napade koji traju vrlo dugo budući da će biti detektirani prije nego što su do kraja završeni.

4.2. Detektiranje statističkim anomalijama

Kao što i ime kaže, ova metoda detektiranja neovlaštenih aktivnosti analizira statistiku skupljenih podataka da bi ustanovila neovlaštene aktivnosti u tijeku. Ovakav IDS alat prvo ustanovljava normalne aktivnosti na mreži ili računalima koja se promatraju. Da bi napravio ovakav profil, IDS alat uzima statističke uzorke računalnih podataka za neko specifično vrijeme normalnih, ovlaštenih, operacija i korištenja sustava. Nakon toga IDS koristi ove podatke za pravljenje karakterističnih atributa sustava i operacija kao što su prosječno korištenje procesorskog vremena, memorije ili količina mrežnog prometa. Statistički uzorci ovih atributa koriste se za izradu profila normalnog korištenja sustava. Nakon toga IDS alat cijelo vrijeme nadgledava praćene atribute i gleda statistički važne devijacije prema ovom profilu. Ako je devijacija uočena, podaci se šalju na IDS-ovu funkciju za odgovor. Neki sustavi bazirani na detektiranju statističkim anomalijama cijelo vrijeme ispravljaju profil normalnog korištenja rabeći sofisticirane algoritme kako bi osigurali da je kompletan sustav za detekciju pouzdaniji tijekom dugog vremena korištenja.



Jedna od glavnih prednosti metode detektiranja statističkim anomalijama je ta da IDS sustav, budući da traži ne-karakteristične događaje, može detektirati nove napade. Povijesno gledano, međutim, IDS alati bazirani na ovoj metodi uvijek su generirali veliki broj lažno-pozitivnih i lažno-negativnih napada. Sa druge strane, ako pojedini napad ne stvara dovoljno veliku promjenu u odnosnu na profil normalnog korištenja sustava, IDS alat koji koristi ovu metodu detektiranja ga neće otkriti. Također, ako greška u profilu normalnog korištenja sustava dovede do generiranja velike promjene sustav će detektirati napad koji zapravo ne postoji. Istraživanja na ovoj metodi se i dalje provode.

5. Odgovor na napade

Kao i metode detekcije, funkcije za odgovor IDS na detektirane neovlaštene aktivnosti variraju od jednog rješenja do drugog, koja uključuju sva moguća zbivanja: od logiranja neovlaštenih aktivnosti za buduće analiziranje do obavještavanja administratora sustava ili mijenjanja konfiguracija mrežnih uređaja. Tradicionalne metode obavještavanja administratora uključuju e-mail, paging i Simple

Network Management Protocol (SMNP), koji se koristi za direktnu komunikaciju između sustava i mrežnih komponenata. Ovo su u principu najsigurniji načini odgovora na napade IDS alata.
Kao što je i za očekivati, funkcija za odgovor na napade IDS alata koja mijenja konfiguraciju sustava i mrežnih komponenti može biti prilično opasna. Lažno pozitivno detektirani napadi mogu dovesti do sprječavanja normalnog funkcioniranja sustava dok lažno negativne detekcije mogu ostaviti sustav otvoren neovlaštenim korisnicima. U nekim slučajevima, neovlašteni korisnici mogu koristiti i lažne izvore da navedu IDS alat na odgovor na napad na krivo računalo, što efektivno dovodi do smanjenja funkcionalnosti sustava prema toj mreži.

6. Prototip IDS alata razvijenog na LSS, ZESOI, FER

IDS alat razvijen na LSS, ZESOI, FER još je u ranoj fazi. Alat trenutno radi samo na Sun Solaris operacijskim sustavima, ali nije isključeno da će se implementirati na ostale Unix operacijske sustave.
Ovaj alat koristi jako jednostavnu tehniku koja analizira korisnikove aktivnosti i traži poznate potpise za neovlaštene aktivnosti kao što je objašnjeno u točki 4.1. Nažalost, ovakav sustav za detekciju neovlaštenih aktivnosti ima puno otežavajućih činjenica – ljuske operacijskih sustava omogućavaju korisnički definirane zamjenske komande što otežava implementaciju ove tehnike osim ako se ne koristi raspisivanje zamjenskih komandi i semantička analiza komandi koje se koriste. Metoda također ne analizira pokretanje programa već samo korisnikove aktivnosti. Ovo znači da neovlašteni program koji iskorištava neku sigurnosnu rupu na pokrenutom računalnom sustavu ne može biti detektiran.
Pozitivna strana ovog sustava za detekciju neovlaštenih aktivnosti u odnosu na IDS alate koji pregledavaju mrežni promet je ta da neovlašteni korisnici ne mogu sakriti svoje aktivnosti korištenjem različitih programa za enkriptiranje podataka na mreži.
Tijekom ispitivanja prototipa pokazano je da neovlašteni korisnici najčešće koriste ssh kao javno dostupni paket za enkriptiranje podataka između dva računalna sustava. U ovom slučaju IDS alati koji pregledavaju mrežni promet nemogu detektirati neovlaštene aktivnosti.
Osim ovoga, IDS sustav koristi autonomne agente kao što su predložili Crosbie i Spafford [8]. Umjesto korištenja jednog velikog IDS sustava, ovaj pristup postavlja koliko je potrebno malih procesa agenata koji međusobno surađuju i prijavljuju svoje podatke na jedno centralizirano mjesto. Ovaj pristup ima nekoliko bitnih prednosti kao što su efikasnost, fault tolerance (pad jednog agenta ne uzrokuje pad cijelog IDS sustava) i skalabilnost. Loša strana ovog pristupa je svakako veliki broj procesa.
U budućem razvoju alata probati će se implementirati sustav za umjetnu inteligenciju koji će zajedno sa pregledavanjem potpisa neovlaštenih aktivnosti služiti za njihovu detekciju. Osim toga, interesantna mogućnost se otvara korištenjem autonomnih agenta koji omogućuju aktivno odgovaranje na neovlaštene aktivnosti korisnika.

7. Drugi modeli

Dorothy Denning [6] predstavila je općeniti model sustava za detektiranje neovlaštenih aktivnosti (eng. Generic Intrusion Detection Model) koji je neovisan o operacijskom sustavu, aplikacijskom okružju ili vrsti neovlaštene aktivnosti. Osnovna ideja ovog modela je držanje profila za određene subjekte (obično, ali ne obvezno korisnici sustava). Kada se generira zapis u log datoteku, sustav pronalazi profil koji odgovara tom zapisu i zatim provjerava aktivnosti i prijavljuje pronađene anomalije. Da bi ovo funkcioniralo, sustav pregledava aktivnosti poput pristupa datotekama, izvođenja programa i prijave korisnika na računalo. Sustav nema nikakva specifična znanja o sigurnosnim problemima na promatranom operacijskom sustavu, iako bi ovo povećalo vrijednost detektiranja modela. Intrusion Detection Expert System (IDES) razvijen je na osnovi ovog općenitog modela uz male modifikacije.
NSM (Network Security Monitor) je sustav za detekciju neovlaštenih aktivnosti razvijen na University of California – Davis. NSM predstavlja mrežni sustav za detekciju neovlaštenih upada koji se razlikuje od gore opisanih sustava po tome što ne pregledava log datoteke na sustavima već pregledava mrežni promet da bi detektirao neovlaštene aktivnosti [7]. Kako će u budućnosti prevladavati mrežni napadi na udaljene računalne sustave, NSM bi mogao postati važan alat za detekciju tih napada. NSM ima nekoliko značajnih prednosti. Prva je ta da odmah dolazi do podataka na mreži. Osim toga, NSM je skriven od neovlaštenog korisnika budući da pasivno analizira mrežni promet. Na dalje, NSM je moguće

koristiti sa bilo kojim operacijskim sustavima budući da on samo analizira mrežni promet i protokole koji su standardizirani (TCP, UDP). Lošu stranu NSM-a predstavlja nemogućnost detektiranja neovlaštenih aktivnosti ukoliko se koristi neki način enkripcije mrežnog prometa između udaljenih računalnih sustava.

8. Smjerovi istraživanja

Prije nego što definiramo smjerove istraživanja metoda detektiranja neovlaštenih aktivnosti, potrebno je postaviti neka realistična očekivanja mogućnosti komercijalnih IDS alata. Do sada je pokazano da je poprilično ne-realistično očekivati od bilo kojeg računalno zasnovanog sustava da prepoznaje nove klase napada ili neovlaštene aktivnosti. Velike tvrtke koje se bave ovakvim alatima i vladine organizacije isprobavale su detektiranje neovlaštenih aktivnosti korištenjem sustava sa umjetnom inteligencijom [4] (eng. Artificial Intelligence - AI), ali većina komercijalnih IDS alata koristi vrlo malo AI mogućnosti. Bez obzira na sve, vrlo je logično očekivati od računalno baziranog IDS sustava da prepoznaje derivative ili kombinacije poznatih klasa napada i neovlaštenih aktivnosti. Ovo znači da, kako se povećava sofisticiranost IDS alata, bi oni trebali biti u mogućnosti detektirati većinu, ako ne i sve, nove derivative i kombinacijske napade bazirane na napadima koje IDS alat već poznaje. Međutim, vrlo je za očekivati da IDS alati nikada neće moći detektirati sve nove napade, budući da jedan dio tih napada uvijek koristi neke nove metode, koje još nisu bile viđene.

Nedavno, nekoliko vodećih proizvođača IDS alata najavili su da će njihovi proizvodi imati uključene i tehnologije detektiranja baziranih na računalima i mrežnim komponentama. Ovo je dobar primjer onoga što možemo očekivati slijedećih godina: hibridne sustave koji koriste kombinacije tehnologija o kojima smo pisali u ovom tekstu, kao i evolucijska unaprjeđenja u individualnim tehnologijama. Osim unaprjeđenja u mogućnostima otkrivanja neovlaštenih aktivnosti, za očekivati je i unaprjeđenja u skalabilnosti, upravljanju i ostalim funkcijama postojećih komercijalnih produkata.

Kako tehnologije koje neovlašteni korisnici rabe za napade također evolviraju da bi prošli neotkriveni od strane raznih IDS alata, sustavi će se unaprjeđivati da bi ih detektirali. U budućim inačicama, neki će IDS sustavi biti u mogućnosti detektirati i visoko distribuirane i spore napade, koji trenutno prođu nedetektirani od strane većine IDS sustava. Kao što smo rekli ranije, distribuirani napadi pokrenuti su simultano sa različitih lokacija, drugih država pa i kontinenata. Spori napadi pokrenuti su korak po korak u velikim vremenskim razmacima. Da bi detektirali ove nove tehnike napada, IDS sustavi moraju efikasno pohranjivati podatke o računalima i mrežama koje se koriste u napadu za duže vremenske periode. Za očekivati je i da ćemo doživjeti velike promjene na ovim područjima dodavanjem komponenti za hijerarhijsko ili centralizirano pohranjivanje podataka.

U idealnom slučaju, IDS alat će detektirati poznate napade u stvarnom vremenu kao i distribuirane napade prije nego što se oni završe. Da bi detektirali poznate napade u stvarnom vremenu, većina IDS agenata ili skupljača podataka (koji su pokrenuti na svakom računalu ili segmentu mreže koja se promatra) će i dalje biti bazirani na detektiranju metodom potpisa. Međutim, agenti će također pohranjivati podatke na centralnim lokacijama. Druge tehnike koristit će se za detektiranje kompliciranih, sporih i/ili distribuiranih napada koristeći ove podatke. Sa ovim i drugim unaprjeđenjima, evolucija IDS alata je u tijeku. Ovisno koliko će se daleko stići sa ovim tehnološkim napretkom, slijedeća bi godina mogla predstavljati revolucionarnu godinu za detekciju neovlaštenih aktivnosti.

9. Zaključak

Detekcija neovlaštenih aktivnosti je još uvijek novo područje istraživanja. Međutim, već počinje zauzimati izuzetno važnu poziciju u današnjem okružju računalnih sustava i mreža. Kombinacija činjenica o izuzetnom rastu Interneta, ogromnih financijskih mogućnosti koje otvara elektronička trgovina i nedostatak potpuno sigurnih računalnih sustava čine sustave za detekciju neovlaštenih aktivnostima izrazito važnim područjem istraživanja. Trendovi najnovijih istraživanja idu prema modelima koji su hibridi detekcije potpisima i statističkih anomalija – polako se prihvaća činjenica da niti jedan od ovih modela sam ne može detektirati sve neovlaštene aktivnosti.

10. Literatura

[1] J.P Anderson. Computer Security Threat Monitoring and Surveillance. Technical report, James P Anderson Co., Fort Washington, Pennsylvania, April 1980.

[2] Barton P Miller, David Koski, Cjin Pheow Lee, Vivekananda Maganty, Ravi Murthy, Ajitkumar Natarajan, Jeff Steidl. Fuzz Revisited: A Re-examination of the Reliability of UNIX Utilities and Services. Computer Sciences Department, University of Wisconsin, 1995.

[3] Eugene H Spafford. Security Seminar, Department of Computer Sciences, Purdue University, Jan 1996.

[4] Teresa F Lunt. A survey of intrusion detection techniques. In Computers and Security, 12(1993), stranice 405-418.

[5] Sandeep Kumar. Classification and Detection of Computer Intrusions. Ph.D. Dissertation, August 1995.

[6] Dorothy E Denning. An Intrusion Detection Model. In IEEE Transactions on Software Engineering, Number 2, page 222, February 1987.

[7] Biswanath Mukherjee, L Todd Heberlein and Karl N Levitt. Network Intrusion Detection, IEEE Network, May/June 1994, stranice 26-41.

[8] Mark Crosbie and Eugene Spafford. Defending a Computer System Using Autonomous Agents. Technical Report CSD-TR-95-022, Department of Computer Sciences, Purdue University, 1995.