UDK: 343.85:[343.533::004

SISTEM ZA DETEKCIJU UPADA U MREŽNU INFRASTRUKTURU

*Petar Čisar
Kriminalističko-policijska akademija, Beograd

Sažetak: Detekcija upada je oblast računarske sigurnosti koja se bavi detekcijom neželjenih manipulacija računarima i računarskim mrežama. Ona se koristi za praćenje i hvatanje upada u pojedinačne računare i računarske sisteme koji imaju za cilj da kompromituju njihovu sigurnost. Mnogi upadi (napadi) se manifestuju dramatičnim promenama u intenzitetu mrežnih pojava. Od sistema za detekciju upada se traži da detektuje sve tipove zlonamernog mrežnog saobraćaja i upotrebe računara koji ne mogu biti identifikovani uobičajenim načinima. Ovaj sigurnosni metod je neophodan u današnjem računarskom okruženju, jer je bez njega vrlo teško održati ravnotežu između trenutnih i potencijalnih pretnji i ranjivosti informacionih sistema. Rad predstavlja opšti pregled sistema za detekciju upada.

Ključne reči: upad, detekcija, komponente, karakteristike, kategorizacija.

1. Uvod

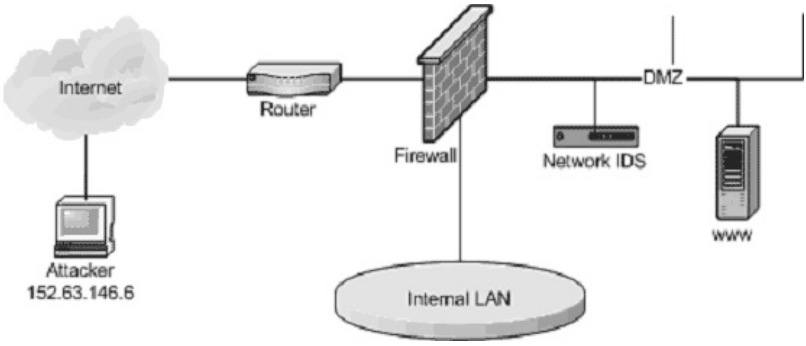
Informacioni sistem, imajući u vidu njegov strateški značaj, mora imati obezbeđen visok nivo sigurnosti podataka kojima operiše. Jedan od načina za obezbeđenje primarne sigurnosti je sistem za detekciju upada u informatičku infrastrukturu, koji ima ulogu da otkrije neželjene manipulacije. Skup zlonamernih manipulacija koje dovode do neregularnog rada računarskog sistema naziva se malfunkcijama. Malfunkcije mogu biti izvedene u formi napada od strane zlonamernih hakera ili upotrebom automatizovanih sofisticiranih sredstava. Između zloupotrebe i upada treba napraviti razliku – pod zloupotrebom se podrazumeva napad koji potiče od strane unutrašnje mreže, dok se upad odnosi na napad spolja. U ovom radu će biti reči o napadima spolja koji se realizuju koristeći transportne protokole, od kojih je najčešći internet protokol. Najveći broj napada je usmeren na internet servere, koji predstavljaju jedan od najznačajnijih infrastrukturnih faktora elektronske komunikacije. Sistem za detekciju upada (engl.

* E-mail: petar.cisar@kpa.edu.rs

Intrusion Detection System – IDS) treba da otkrije sve tipove zlonamernog mrežnog saobraćaja i upotrebe računara, koji ne mogu biti otkriveni uobičajenim *firewall*-om. Opravdanost implementacije IDS-a se bazira na tome, da čak i najbolje filtriranje paketa može propustiti dosta upada u sistem. Ovaj sigurnosni metod je potreban u računarskom okruženju današnjice, jer se u praksi pokazalo nemogućim održati tempo sa trenutnim i potencijalnim pretnjama i ranjivostima računarskih sistema.

2. Pojam i uloga IDS

Detekcija upada se može definisati kao akt detekcije takvih aktivnosti, koje su usmerene na kompromitovanje poverljivosti, integriteta i raspoloživosti resursa. Preciznije, cilj detekcije upada je identifikacija entiteta koji pokušavaju da naruše postojeći sistem sigurnosnih kontrola. Praksa je pokazala da čak i detaljno filtriranje paketa, stalna inspekcija i *proxy firewall* mogu propustiti nedopustivo mnogo upada. Svojim dizajnom, *firewall* je uređaj prvenstveno namenjen za zaštitu graničnog područja jedne mreže i koji se ne bavi internim ponašanjem mreže, sistema ili korisnika. To otvara prostor za mrežne napade prema povredivim servisima, napade pomoću podataka koji su usmereni ka aplikacijama, napade usmerene ka hostovima (eskalacija privilegija, neautorizovani login i pristup osetljivim datotekama i maliciozne pretnje – virusi, trojanci i crvi).



Slika 1 – *IDS – osnovna konfiguracija (Izvor: http://www.sans.org/security-resources/idfaq/role.php)*

ID obezbeđuje pouzdaniju zaštitu dvostrukom proverom efikasnosti ostalih kontrola pristupa. Primarna namena IDS-a je detektovanje eksternih napada, kao i internih zloupotreba računarskih i mrežnih resursa ili informacija svojstvenih ovim resursima, pa se u tom smislu proverava dolazeći ili odlazeći saobraćaj i identifikuju sumnjivi mrežni uzorci.

Pretnje od strane malicioznog „insajdera" se mogu materijalizovati u kompromitovanoj fizičkoj sigurnosti sistema, kompromitovanim lozinkama (engl. *Masquerade*) ili korisnicima koji pokušavaju pristupiti informacijama za koje nemaju odgovarajuća ovlašćenja. Ovde su od interesa uspešno izvedeni napadi, baš kao i pokušaji napada. Uspešni napadi mogu kompromitovati integritet, poverljivost ili

dostupnost izvora ili informacija, dok pokušaj napada može poslužiti kao važno upozorenje o nivou pretnje i o vrsti resursa koji je ugrožen.

Neautorizovani napad spolja može se izvesti:

- prolaskom kroz *firewall*, koristeći njegove sigurnosne slabosti,
- tunelovanjem kroz benigne komunikacione protokole,
- izbegavanjem rutinskih sigurnosnih kontrola (merenja).

Osnovni izazov u detekciji upada je prepoznavanje i razdvajanje abnormalnih od normalnih događaja. Pod abnormalnim događajima podrazumevaju se aktuelni napadi na računarski sistem, kao i nedozvoljeno ispitivanje informacija, koje je mnogo suptilniji i teži slučaj za detekciju. Sledeći izazov u detekciji upada odnosi se na lažne pozitive. Lažni pozitivi u ID se javljaju kada jedan IDS izveštava o pojavi upada, a on se u stvarnosti nije dogodio. Količnik lažnih pozitiva smatra se jednim od najvažnijih faktora za ocenu rada jednog IDS-a.

ID tehnologije adresiraju jedan konkretan problem u realnom vremenu. Podaci se moraju analizirati kako pristižu, njihova analiza mora biti brza i kompletna, a alarmi moraju biti blagovremeni kako bi se sprečila daljnja šteta od upada.

Neke od funkcija koje IDS omogućava su:

- monitoring i analiza aktivnosti korisnika i sistema,
- pregled sistemskih konfiguracija i ranjivosti,
- ocena integriteta kritičnog sistema, podataka i datoteka,
- prepoznavanje uzoraka koji ukazuju ne neke od poznatih napada,
- statistička analiza na abnormalnu aktivnost uzoraka,
- prepoznavanje korisničkih aktivnosti koje ukazuju na kršenje sigurnosne politike.

Neki sistemi omogućavaju i dodatne mogućnosti kao što su:

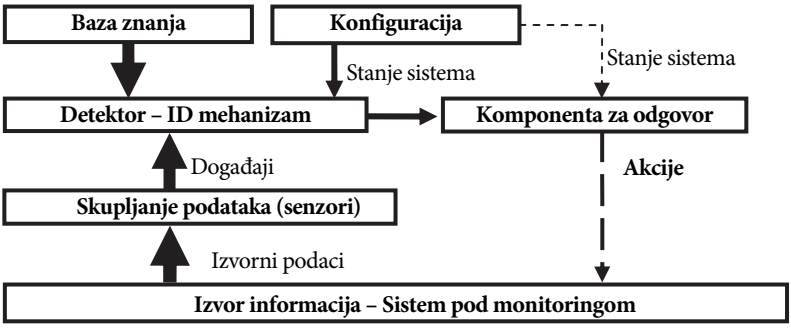
- automatska instalacija regularnih softverskih programa sa korigovanim uočenim nedostacima (engl. *patch*),
- instalacija i puštanje u rad lažnih servera za snimanje informacija o napadačima.

3. Komponente IDS

Iako su IDS sistemi izuzetno različiti u pogledu primenjenih tehnika za sakupljanje i analizu podataka, većina njih počiva na relativno opštem arhitekturalnom okviru. Generalna arhitektura jednog IDS sistema je prikazana na slici 2.

- Uređaj za skupljanje podataka (senzori) – odgovoran je za skupljanje podataka od sistema koji se nalazi pod monitoringom.
- Detektor (mehanizam za analizu ID) – obrađuje podatke skupljene od senzora s ciljem identifikacije intruzivnih aktivnosti; koristi sistem pravila za generisanje alarma od primljenih sigurnosnih događaja.
- Baza znanja (baza podataka) – sadrži informacije skupljene od senzora, ali u preprocesnom obliku (npr. baza znanja o napadima i njihovim potpisima, filtriranim podacima, profajlovima podataka itd.). Ove informacije se obično dobijaju s mreže ili od sigurnosnih eksperata.

- Uređaj za konfiguraciju – obezbeđuje informaciju o trenutnom stanju sistema za detekciju upada.
- Komponenta za odgovor – inicira akciju u slučaju detekcije upada. Ovi odgovori mogu biti automatizovani (aktivni) ili sa ljudskom interakcijom (inaktivni).



Slika 2 – *Generalna arhitektura IDS (Lazarevic, Kumar & Srivastava, 2005)*

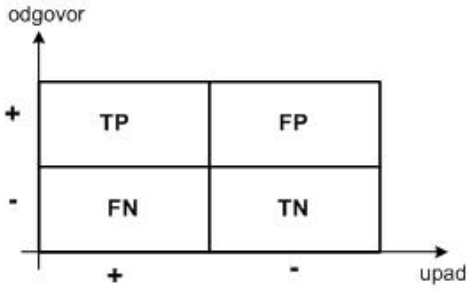
4. Karakteristike IDS

Ciljne karakteristike jednog IDS sistema se mogu identifikovati kao sledeće:

Performansa predviđanja (engl. *prediction*) – Kod detekcije upada, merenje tačnosti predviđanja, nije adekvatno. Na primer, mrežni upadi tipično predstavljaju vrlo mali procenat ukupnog mrežnog saobraćaja (tj. 1%), pa i trivijalni IDS koji celokupan mrežni saobraćaj označi kao normalan može postići tačnost od 99%. S ciljem postizanja dobrog predviđanja, IDS mora da zadovolji dva kriterijuma:

1) korektno identifikovanje upada i
2) ne sme legitimne akcije u sistemskom okruženju identifikovati kao upad.

Tipične kategorije za evaluaciju performansi IDS-a su osetljivost, određenost i tačnost. Za ocenu karakteristika softvera za detekciju upada koristi se dijagram reakcije, koji definiše različite slučajeve alarma i odgovor IDS-a na njih.



Slika 3 – *Dijagram reakcije (Pleskonjić, Đorđević, Maček & Carić, 2006)*

Na gornjem dijagramu osa upada označava da li se upad stvarno desio: „+“ se odnosi na slučaj da je postojao upad, a „-“ da upada nije bilo. Osa „odgovor“ odnosi

se na reakciju IDS-a: „+“ za slučaj da je IDS reagovao na upad kao stvaran i „-“ kada IDS nije reagovao. Na dijagramu su prikazana četiri različita slučaja:

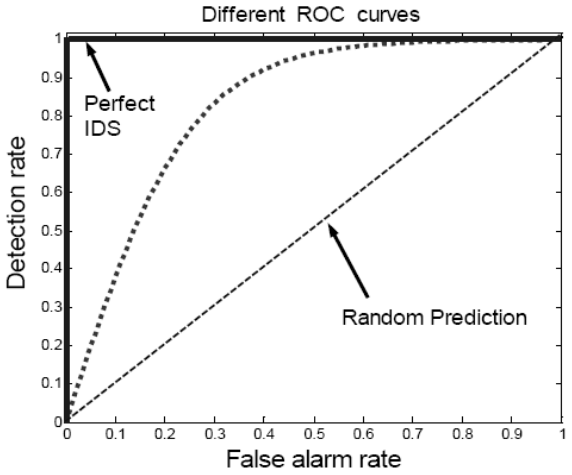
- TP (engl. *True Positive* – pravi alarm) odnosi se na slučaj kada je upad ispravno detektovan.
- FP (engl. *False Positive* – lažni alarm) označava da je IDS detektovao nepostojeći upad kao stvarni.
- FN (engl. *False Negativ* – propušten alarm) odnosi se na događaj kada IDS nije detektovao postojeći upad.
- TN (engl. *True Negativ* – ispravno legitiman) označava da IDS nije detektovao nepostojeći upad, tj. radi se o korektnoj detekciji normalne aktivnosti.

Osetljivost – količnik broja stvarnih upada koje je IDS detektovao (TP) i zbira pravih alarma i propuštenih alarma (TP + FN).

Određenost – količnik ispravno detektovanih legitimnih aktivnosti (TN) i sume stvarno negativnih i lažnih alarma (TN + FP).

Tačnost – odnos svih rezultata (pozitivnih i negativnih) koji su ispravni.

Stepen detekcije (engl. *detection rate*) se definiše kao odnos broja korektno detektovanih napada i ukupnog broja napada, dok je količnik lažnih alarma (engl. *false alarm rate*) odnos broja normalnih konekcija koje su pogrešno klasifikovane kao napadi i ukupnog broja normalnih konekcija. U praksi je veoma teško oceniti ove dve mere, s obzirom da je obično nemoguće imati saznanja o svim napadima. Pošto su stepen detekcije i količnik lažnih alarma često u suprotnosti, evaluacija IDS-a se takođe može sprovesti pomoću krive operativne karakteristike primaoca (engl. *Receiver Operating Characteristics* – ROC). To je jedan od načina grafičkog prikaza zavisnosti osetljivosti od određenosti. ROC kriva predstavlja kompromis između stepena detekcije i količnika lažnih alarma. Što je ROC bliže gornjem levom uglu grafa (tačka kojoj odgovara 0% lažnih alarma i 100% stepen detekcije), to je IDS efikasniji.



Slika 4 – *ROC kriva (Lazarevic et al., 2005)*

Vremenska performansa – Ovaj tip performanse IDS se odnosi na ukupno vreme koje je potrebno da bi IDS detektovao upad. Ovo vreme u sebi sadrži vreme potrebno za obradu (engl. *processing time*) i vreme propagacije (engl. *propagation time*). Vreme procesiranja direktno zavisi od brzine procesiranja, koje predstavlja brzinu kojom IDS obrađuje događaje. Vreme propagacije je vreme koje je potrebno da obrađena informacija stigne do analizatora zaduženog za sigurnost. Potrebno je da oba vremena budu što kraća, kako bi se omogućilo dovoljno vremena za analizatora da reaguje na napad pre nego što je učinjena neka veća šteta, kao i da uspešno zaustavi napadača u svojoj aktivnosti.

Tolerancija na grešku – Sistem za detekciju upada mora da bude zavisan, robustan i otporan na napade, sa sposobnošću da se brzo oporavi od uspešno realizovanih napada i nastavi da vrši svoju sigurnosnu funkciju. Ovo je posebno značajno u slučajevima vrlo velikih distribuiranih DoS napada, napada s prekoračenjem bafera i različitih osmišljenih napada usmerenih na isključenje računarskog sistema, a sa njim i IDS. Ova karakteristika je posebno važna za ispravno funkcionisanje IDS-a, pošto mnogi od komercijalnih IDS-a rade na operativnim sistemima i mrežama koje su ranjive na različite tipove napada. Pored toga, IDS-i moraju biti otporni i na scenario kada neprijatelj generiše veliki broj lažnih alarma. Takvi alarmi mogu lako imati negativan uticaj na raspoloživost sistema, a IDS treba da ima sposobnost da ih prevaziđe.

Evaluacija sistema za detekciju upada – U odnosu na gore navedene ciljne karakteristike sistema za detekciju upada, može se uspostaviti sistem ocenjivanja, koji će pružiti odgovor na pitanje u kojoj meri jedan određeni sistem za detekciju upada zadovoljava neophodne karakteristike sigurnosti. U analizi sistema za detekciju upada, generalno, razmatraju se dva tipa napada: napadi realizovani kroz jednostruku konekciju i napadi realizovani kroz višestruke (neprekidne) konekcije. Standardna metrika definisana sledećom tabelom, slično tretira oba tipa napada.

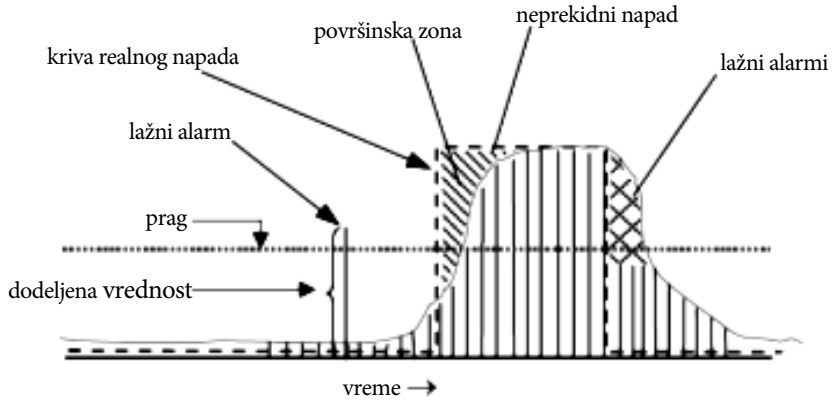
Tabela 1 – *Standardna metrika za evaluaciju napada kroz jednostruku konekciju (Lazarevic, Ertoz, Ozgur, Srivastava & Kumar, 2003)*

Standardna metrika		**Predviđeni naziv konekcije**	
		Normalni	Upadi (napadi)
Aktuelni naziv konekcije	Normalni	Stvarni negativ	Lažni alarm
	Upadi (napadi)	Lažni negativ	Korektno detektovani napadi

Zavisno od tipa napada, mogu se primeniti različite vrste analize: analiza napada kroz jednostruku konekciju i analiza napada kroz višestruke konekcije. Bez obzira na različitost, prvi korak kod oba tipa analiza čini izračunavanje i dodeljivanje vrednosti za svaku mrežnu konekciju. Ova rezultirajuća vrednost predstavlja verovatnoću pridruživanja upada posmatranoj mrežnoj konekciji.

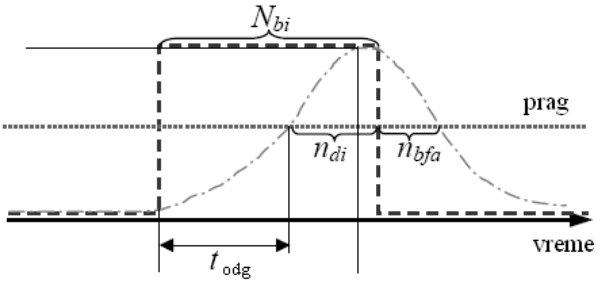
U cilju realizacije pomenutih analiza, može se prihvatiti polazni pristup kod koga se za konkretni mrežni saobraćaj, svakoj ostvarenoj konekciji dodeljuje određena vrednost, predstavljena na donjoj slici vertikalnom linijom. Isprekidanom linijom je označena kriva realnog napada, koja ima vrednost 0 za neintruzivne (normalne) mrežne konekcije i 1 za intruzivne konekcije. Punom linijom je na slici

obeležena kriva predviđenog napada, koja je za svaku konekciju jednaka njenoj dodeljenoj vrednosti. Ove dve krive omogućavaju da se izračuna greška za svaku konekciju, kao razlika između realne vrednosti konekcije (1 – za konekcije pridružene napadu i 0 – za normalne konekcije) i dodeljene vrednosti konekcije.



Slika 5 – *Dodela vrednosti kod IDS-a (Lazarevic et al., 2003)*

Višestepeni pristup u ocenjivanju upada u mrežni saobraćaj primenjuje izračunate greške za svaku konekciju, s ciljem da se dođe do novih evaluacionih metrika. Prva dobijena metrika odgovara površinskoj zoni između krive realnog napada i krive predviđenog napada. Što je manja površina između ovih krivih, bolji je primenjeni algoritam za detekciju upada. Ipak, može se reći da analiza svedena samo na površinske zone nije dovoljno precizna, jer ne daje odgovor na mnoge aspekte algoritama za detekciju upada (npr. koliko je konekcija pridruženo jednom napadu, koliko je brz korišćeni algoritam za detekciju upada itd.). Zbog toga je potrebno primeniti i druge dodatne metrike, koje bi bile podrška osnovnoj metrici površinske zone ispod krive napada. Pretpostavimo da je N ukupan broj mrežnih konekcija. Broj N je tada jednak sumi ukupnog broja normalnih mrežnih konekcija (N_n) i ukupnog broja mrežnih konekcija koje su pridružene upadima (N_i). Broj n_{fa} odgovara broju neintruzivnih (normalnih) mrežnih konekcija koje imaju vrednost veću od vrednosti praga i zbog toga su pogrešno klasifikovane kao intruzivne. Sada se mogu definisati dodatne metrike kao:



Slika 6 – *Dodatne metrike za evaluaciju IDS-a (Lazarevic et al., 2003)*

1) *Stepen detekcije bloka* (engl. *burst detection rate* – bdr) se definiše za svaki blok i predstavlja odnos između ukupnog broja intruzivnih mrežnih konekcija n_{di} koje imaju rezultat veći od praga, u okviru blokovskog (neprekidnog) napada i ukupnog broja intruzivnih mrežnih konekcija u okviru napadačkih intervala (N_{bi}). Prema definiciji, $bdr = n_{di} / N_{bi}$, gde je suma svih N_{bi} jednaka N_i. Slična metrika je korišćena kod DARPA 1998 evaluacije.

U skladu sa gornjom slikom mogu se formulisati definicije sledećih metrika:

Tabela 2 – *Definicija metrika*

Metrika	Definicija
bdr	n_{di} / N_{bi}
n_{di}	Broj intruzivnih konekcija koje imaju vrednost veću od vrednosti praga.
n_{bfa}	Broj normalnih konekcija koje prate napad i koje su pogrešno klasifikovane kao intruzivne.
t_{odg}	Vreme odgovora – vreme dostizanja vrednosti praga.

2) *Vreme odgovora* predstavlja proteklo vreme od početka napada do momenta kada prva mrežna konekcija dostigne vrednost veću od vrednosti praga. Slična metrika je korišćena kod DARPA 1999 evaluacije, gde je bio dozvoljen interval od 60 s za detekciju blokovskog napada.

5. Kategorizacija IDS

Jedna od najstarijih podela IDS odnosi se na to šta se ovim sistemom detektuje. U tom smislu, IDS sistemi se mogu podeliti na:

- sisteme za detekciju zloupotreba (engl. *misuse intrusion detection*),
- sisteme za detekciju anomalija (engl. *anomaly intrusion detection*).

Detekcija zloupotreba se odnosi na otkrivanje poznatih napada usmerenih na poznate slabosti sistema. Detekcija anomalija usmerena je ka otkrivanju neuobičajenih aktivnosti, koje mogu indicirati upad u sistem.

Prema mehanizmu detekcije, može se izvršiti kategorizacija IDS-a na:

- IDS na bazi anomalija,
- IDS na bazi potpisa,
- hibridni IDS – koristi obe tehnologije.

IDS na bazi anomalija je sistem za detekciju računarskih upada i zloupotreba putem monitoringa sistemskih aktivnosti i njihove klasifikacije na normalne i neuobičajene. Ova kategorija se znatno više bazira na heuristici ili pravilima, nego na sekvencama ili potpisima i omogućava detekciju bilo koje vrste zloupotrebe koja izlazi izvan okvira normalnog (očekivanog) ponašanja sistema. Ona je suprotna sistemima koji su bazirani na potpisu, a koji mogu detektovati samo one napade za koje su odgovarajući potpisi prethodno kreirani. Pojmovi „na bazi znanja" i „na bazi zloupotrebe" su sinonimi za „na bazi potpisa". Ovo je koncept sličan antivirusnom softveru koji skenira fajlove i memoriju na poznate sekvence kompjuterskih virusa. IDS na bazi potpisa ima stoga nedostatak da može da detektuje samo prethodno poznate napade, dok IDS na bazi anomalija može biti u

stanju da detektuje i nove napade. Na primer, ako jedan IDS na bazi anomalije detektuje stotine pokušaja logina u intervalu od nekoliko sekundi, on će generisati alarm na sumnjivu aktivnost. Nedostaci sistema na bazi potpisa su još i: postojanje različitih varijanti, lažni pozitivi i negativi i preopterećenje podacima. Pošto se baziraju na potpisima, za ove sisteme se može kreirati nova varijanta napada, s ciljem izbegavanja detekcije. Pored toga, i sami potpisi mogu kreirati lažne pozitive, ukoliko nisu ispravno napisani ili ako je priroda napada takva da se teško može izolovati od karakteristika normalnog saobraćaja. Sistem na bazi potpisa ne može detektovati napade koji u sebi ne sadrže potpis – oni ne reaguju dobro na nepoznate situacije. Preopterećenje podacima se može pojaviti u slučaju kada senzor ili analitičar zadaju previše informacija za efektivno analiziranje.

Različite analize saobraćaja koje se izvršavaju na aktuelnom mrežnom saobraćaju mogu umanjiti nedostatke sistema za detekciju baziranih samo na potpisu, jer one imaju zadatak da detektuju anomalije. Važno je napomenuti da sistemi na bazi anomalija ne mogu zameniti sisteme bazirane na potpisu. Idealno bi bilo kada bi analitičar imao oba alata na raspolaganju. Sistem baziran na analizi saobraćaja može detektovati različite varijante napada, s obzirom da on ne traži unapred definisane napadačke sekvence, već okida na neuobičajenu prirodu konekcije (nepoznat IP, nepoznat port, neregularna dužina paketa ili podešavanje indikatora – *flag*), događaj, stanje, sadržaj ili ponašanje, koji su nenormalni u odnosu na prethodno definisane standarde normalnog.

Neki primeri nenormalnog ponašanja:

- HTTP saobraćaj na nestandardnom portu, npr. portu 53 (anomalija protokola),
- servis „zadnjih vrata" na poznatom standarnom portu, npr. *peer-to-peer* deljenje datoteka koristeći Gnutella na portu 80 (anomalija protokola i statistička anomalija),
- segment binarnog koda u korisničkom *password*-u (aplikaciona anomalija),
- previše UDP u odnosu na TCP saobraćaj (statistička anomalija),
- veći broj bajtova koji dolaze od HTTP brauzera, nego što idu ka njemu (aplikaciona i statistička anomalija).

Lažni pozitivni alarmi su takođe slabost detekcije anomalija, ali ukoliko se alarmi koji potiču od obe metode prethodno mogu dovesti u korelaciju, relevantnost alarma je moguće poboljšati. Snaga detekcije anomalija je u njenom malom broju lažnih negativnih alarma. Novi napadi, za koje još nisu razvijeni potpisi za okidanje sistema baziranog na potpisu, nenormalni su po svojoj prirodi. Sistem detekcije baziran na anomaliji ne bi mogao uhvatiti najnoviji IIS UNICODE, ali bi zato promena u ponašanju kompromitovanog sistema privukla njegovu pažnju. Smanjenje preopterećenja podacima se ostvaruje korišćenjem *data mining*-a i vizualizacionih tehnika. Sažimanjem podataka i njihovim vizuelnim predstavljanjem, može detektovati anomalije i sekvence koje heuristika sistema za analizu saobraćaja nije u stanju da uradi.

Kao i metod na bazi potpisa, i detekcija upada na bazi anomalija se zasniva na skupu informacija koje definišu šta je normalno, a šta nije u ponašanju mreže. Ovaj skup informacija se naziva profil i predstavlja ključ efikasnog sistema za detekciju upada na bazi anomalija. Da bi ovaj sistem bio efikasan, mora imati robustan profil,

koji karakteriše normalno ponašanje. Objekat monitoringa može biti host/IP adresa, VLAN ili fizički LAN segment. Profil se sastoji od obimne liste parametara, koji se odnose specijalno na objekat koji je predmet nadzora – npr. normalno vreme logovanja, trajanje login sesije, opterećenje procesora, korišćenje diska, omiljeni editori itd. Ovaj robusni profil mora biti stabilan i konzistentan u definisanju normalnog ponašanja objektnog okruženja. Efikasan profil anomalija mora takođe biti i osetljiv prema pojavama bilo kojih događaja koji bi mogli ugroziti sigurnost. Konstruisanje efikasnog profila podrazumeva prethodno detaljno prikupljanje informacija o ponašanju i aktivnosti na mreži. Profili mogu varirati u kompleksnosti, od nekoliko prostih graničnih vrednosti do složenih karakterizacija sadržaja sa multi – varijabilnom raspodelom. Pored toga što moraju biti robusni i osetljivi, profili bazirani na mrežnom saobraćaju treba da budu adaptivni i samoučeći. Adaptivni profili uzimaju u obzir normalne promene u saobraćaju mreže, pri tome ne stvarajući lažne alarme. Samoučenje je kritično za osiguranje široke i uspešne primene mehanizama za detekciju na bazi anomalija, a odnosi se na mogućnost mehanizma za detekciju da nauči normalno ponašanje saobraćaja i obezbedi detekciju baziranu na naučenom profilu. Generalno, može se reći da je veoma teško ručno postaviti profile, pre svega zbog kompleksnosti i dinamičkih promena u mrežnoj statistici.

Na osnovu gore iznetog, može se zaključiti da se rad mrežnog sistema za detekciju upada može učiniti znatno efikasnijim ako on u sebi pored kontrole podudarnosti potpisa, sadrži i mogućnost analize aktuelnog saobraćaja. Analizom saobraćaja, anomalija se identifikuje kao potencijalni upad. U proces analize saobraćaja nije uključena kontrola potpisa, pa stoga on više liči na detektovanje novih nezabeleženih napada, čiji potpisi tek treba da budu razvijeni. Analiza saobraćaja se ne bavi sadržajem poruke, već njenim ostalim karakteristikama kao što su npr. izvor, destinacija, ruting, dužina poruke, vreme kada je poslata, frekvencija komunikacije i dr. Sadržaj poruke nije uvek dostupan za analizu – saobraćaj može biti enkriptovan, VPN linkovi mogu prolaziti kroz posmatrani prostor ili je jednostavno analiza paketskog sadržaja u suprotnosti sa politikom. Za potrebe detekcije mrežnog upada, ove karakteristike se dobijaju ili iz samog aktuelnog mrežnog saobraćaja (pomoću metoda kao što je *tcpdump*) ili iz log-fajlova koji potiču od mrežnih senzora (*firewall*-a ili rutera). Ovi podaci se dalje mogu procesirati pomoću vizuelizacije ili tehnika *data mining*-a, s ciljem da generišu alarm i omoguće korisnu informaciju za određivanje mesta analiziranog resursa.

Prema domenu ili području u kome rade, IDS se dele na:

- mrežno bazirane,
- host-bazirane,
- hibridne.

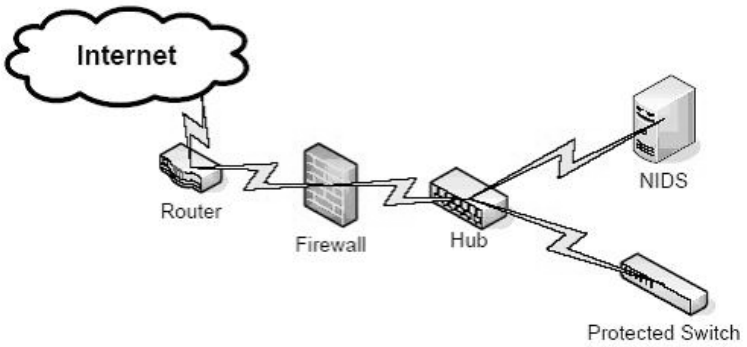
Kod mrežno baziranih sistema (engl. *Network-based IDS* – NIDS) senzori su locirani na čvornim mestima u mreži, često u demilitarizovanoj zoni ili na granicama mreže. Senzor hvata celokupan mrežni protok i analizira sadržaj svakog pojedinog paketa na zlonamerni saobraćaj. Kod host-baziranih sistema (engl. *Host-based IDS* – HIDS) senzor se često sastoji od softverskog agenta koji vrši monitoring svih aktivnosti hosta na kome je instaliran.

- NIDS je nezavisna platforma koja identifikuje upade ispitivanjem mrežnog saobraćaja i monitoringom višestrukih hostova. NIDS obezbeđuje pristup mrežnom saobraćaju putem konekcije na hab, mrežni svič konfigurisan na preslikavanje porta ili mrežni pristupni port – tap (engl. *Test Access Port* – TAP). Problem kod ovih sistema predstavlja enkriptovani saobraćaj, saobraćajno preopterećenje mreže i procena namere neke određene akcije.
- Host-bazirani IDS se sastoji od agenta na hostu koji identifikuje upade analiziranjem poziva sistema, aplikacionih logova, promene sistema datoteka (binarne, password datoteke, sposobnost/acl baze podataka) i druge aktivnosti i stanja hosta. Najčešći problem sa host-baziranim sistemima je to što na analizu dobijaju samo one podatke koje su aplikacije već upisale u logove.
- Hibridni IDS kombinuje oba prethodna pristupa. Podaci od hostovog agenta se kombinuju sa mrežnom informacijom s ciljem formiranja jednog šireg pogleda na stanje mreže.

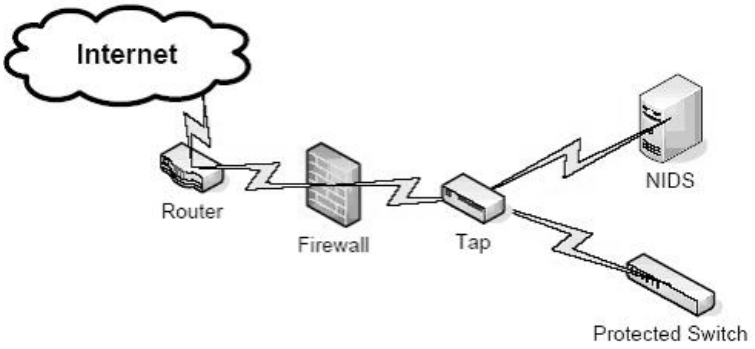
NIDS – Mrežno bazirana detekcija upada ima za cilj da identifikuje neautorizovano, nedozvoljeno i abnormalno ponašanje bazirano isključivo na mrežnom saobraćaju. Mrežni IDS koristeći tap, span (engl. *switch port analyzer* – SPAN) port ili hab, sakuplja pakete koji idu preko date mreže. Koristeći prikupljene podatke, IDS sistem obrađuje i obeležava bilo kakav sumnjivi saobraćaj. Za razliku od sistema za sprečavanje upada (engl. *intrusion prevention system* – IPS), IDS sistem ne blokira aktivno mrežni saobraćaj. Uloga mrežnog IDS-a je pasivna, svedena na prikupljanje, identifikovanje, registrovanje operacija i alarmiranje. NIDS mora biti u stanju da kontroliše celokupan saobraćaj na zaštićenom mrežnom segmentu. Postoji više načina za postizanje ovog cilja, pri čemu svi oni imaju svoje prednosti i nedostatke.

Najjednostavniji i najjeftiniji metod za rešenje ovog problema je dodavanje haba na mestu čvorne tačke, a zatim priključenje IDS-a na hab. Na ovaj način je kreiran sledeći segment: svič 1 (S1) → hab sa priključenim IDS → svič 2 (S2). Bilo koji saobraćaj koji ide između S1 i S2 će biti primećen od strane IDS (slika 7). Ovaj tip rešenja ima dobru stranu što nije potrebna rekonfiguracija *firewall*-a, niti dodatno podešavanje IDS-a. Ovo je ujedno i najmanje efikasan metod, jer dodavanje haba ukida mnoge prednosti koje ima komutirana mreža. Istovremeni dvosmerni saobraćaj je na ovaj način eliminisan, čime je efektivni mrežni propusni opseg prepolovljen. Pored toga, hab je još jedno mesto za potencijalnu grešku u sistemu. Zbog navedenih nedostataka, ova konfiguracija nije preporučljiva. Primer softverskog mrežnog IDS-a: SNORT.

Konfiguracija sa mrežnim tapom je veoma slična konfiguraciji sa habom i koja omogućava NIDS-u da kontroliše ceo saobraćaj na komutiranoj mreži. Tap tipično izgleda kao troportni svič: port 1 će biti vezan na svič 1, port 2 na svič 2, a port 3 na NIDS (slika 8). Svaki paket koji se prosleđuje između svičeva 1 i 2 će biti preslikan na NIDS. Tap ne prekida istovremenu dvosmernu prirodu komunikacije. Otporan je na grešku, jer većina komercijalnih uređaja u slučaju otkaza napajanja ne prekida vezu između rutera i sviča. Važni nedostaci u korišćenju tapa su njegova cena, kao i potreba za dodatnim modifikacijama u slučaju monitoringa dvosmernog saobraćaja.



Slika 7 – *NIDS koji koristi hab (Izvor: http://danielowen.com/NIDS)*

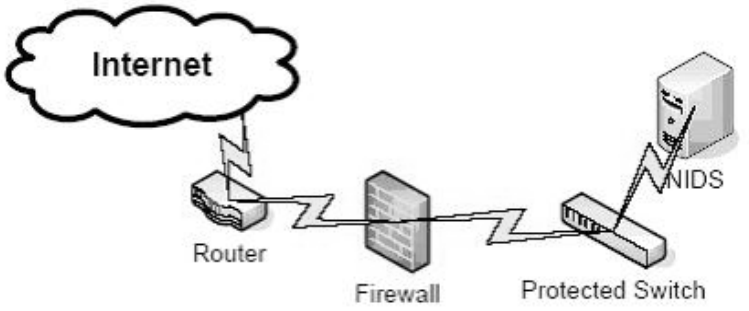


Slika 8 – *NIDS koji koristi tap (Izvor: http://danielowen.com/NIDS)*

Tapovi mogu povećati sigurnost sistema za detekciju upada. Razlog za to je jednostavan: IDS-i iza tapova ne zahtevaju postojanje adrese, pošto tap preuzima sve podatke sa linije i preusmerava ih direktno na IDS interfejs, eliminišući tako potrebu za adresiranjem. Kako IDS u ovom slučaju nema adresu, tako nije moguće ni uputiti saobraćaj direktno na IDS. Ova činjenica štiti IDS sistem od usmerenih napada i može dovesti napadače u pogrešno verovanje da nema instaliranog IDS-a koji bi ih identifikovao i ušao u trag njihovim napadima. Pored navedenih prednosti, tap ne utiče na protok saobraćaja i ne dovodi do degradacije mreže.

Čest oblik implementacije njuškala (engl. *sniffer* – programski alat za merenje efikasnosti i nivoa korišćenja mreže praćenjem protoka podataka kroz mrežu) bilo kog tipa na mrežu je upotreba span porta na sviču koji je pod monitoringom. Span port se formira odgovarajućim konfigurisanjem sviča tako da kopira sve pakete (iz otpremnog i prijemnog komunikacionog smera) koji su mu poslati sa jednog porta na drugi – na kome bi bio instaliran NIDS (slika 9). Veoma slično tapu, ni u ovom slučaju ne dolazi do prekida *full duplex*-ne prirode komutiranog saobraćaja. Dobra strana rešenja sa span portovima je i jednostavna instalacija, koja ne zahteva dodatnu rekonfiguraciju *firewall*-a. Osnovni nedostatak span portova se ogleda u tome što oni mogu imati štetan efekat na ostali saobraćaj kroz svič. Naime, u situaciji kada je svič veoma opterećen, može se desiti da veći saobraćaj ide kroz njega nego što može biti

preslikan na jedan određeni port. Pored toga, za neke primene span portova je dokazano da dovode do velikih problema u korišćenju resursa na sviču čak i na relativno niskim nivoima korišćenja mreže. Ovde je potrebno imati u vidu i da se, zavisno od položaja NIDS-a u mreži, ARP (engl. *address resolution protocol*) zahtevi tipično ne prosleđuju na span portove. To znači da ARP napadi neće moći biti primećeni. Neke implementacije NIDS-a nemaju mogućnost detekcije ARP napada, pa stoga ova konfiguracija, zavisno od izabranog NIDS rešenja, može biti sporan momenat s aspekta sigurnosti. Nedostatak ove opcije je i to da je često moguće imati samo jedan span port po sviču. U ovom slučaju, ako na portu već postoji aktivno njuškalo, tada se taj port ne može koristiti za IDS. Ukoliko je potreban monitoring više od jednog porta, tada se mora uraditi span za opseg portova (npr. span portovi 1–5 na port 6). Imajući u vidu sve pomenute nedostatke span porta, često je to najlakši i najjeftiniji način implementacije NIDS-a.

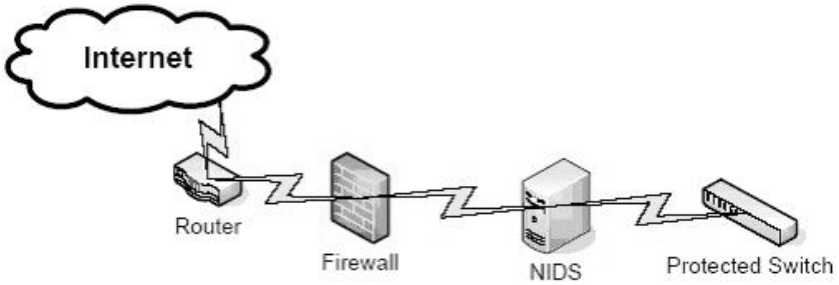


Slika 9 – *Upotreba span porta (Izvor: http://danielowen.com/NIDS)*

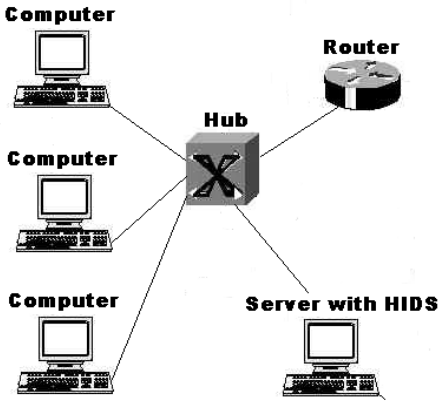
Poslednja konfiguracija mrežnog sistema za detekciju upada je linijski NIDS. Linijski NIDS po svojoj topologiji izgleda kao *bridge* (slika 10). NIDS se tipično konfiguriše bez IP adrese, pa zato, u komunikacionom smislu, ne odgovara na bilo kakav saobraćaj. IPS će prihvatiti saobraćaj na jednom NIC-u (engl. *network interface card*) i proslediti ga nepromenjenog na drugi NIC, kao što to radi standardni *bridge*. Ova konfiguracija je posebno popularna kod IDS sistema s aktivnim odgovorom. U ovom slučaju, NIDS može prekinuti saobraćaj slično kao *firewall*, pošto je fizički smešten u čvornoj tački. U skladu sa konfiguracijom uređaja, najčešće hardverske verzije linijskog NIDS-a u slučaju otkaza mogu ostati u otvorenom ili zatvorenom stanju. Softverski bazirani linijski NIDS u slučaju otkaza tipično ostaje u zatvorenom stanju, što dovodi do prestanka usluge, s obzirom da IDS koji je stao sa radom prekida saobraćaj kroz zaštićenu mrežu.

HIDS – Host-bazirana detekcija upada ima za cilj da identifikuje neautorizovano, nedozvoljeno i abnormalno ponašanje na nekom specifičnom uređaju. HIDS generalno podrazumeva agenta instaliranog na svakom sistemu koji vrši monitoring i alarmiranje na lokalnom operativnom sistemu, kao i aplikacionu aktivnost. Instalirani agent koristi kombinaciju potpisa, pravila i heuristike da bi identifikovao neautorizovanu aktivnost. Uloga host IDS je pasivna i svodi se samo na prikupljanje, identifikovanje, registrovanje operacija i alarmiranje. Primeri HIDS-a:

OSSEC – *Open Source Host-based Intrusion Detection System*, *Tripwire*, AIDE – *Advanced Intrusion Detection Environment*, *Prelude Hybrid IDS*.



Slika 10 – *Linijski NIDS (Izvor: http://danielowen.com/NIDS)*



Slika 11 – *HIDS konfiguracija (Izvor: http://www.securitydocs.com/library/3009)*

Prema tipu reakcije na napad, IDS sistemi mogu biti pasivni i reaktivni.

- Pasivni sistemi – Ovi sistemi u slučaju detekcije sumnjivog ili zlonamernog saobraćaja generišu alarm, koji se šalje administratoru ili korisniku, koji zatim odlučuju o daljim postupcima.
- Reaktivni sistemi – Ova vrsta sistema pored detekcije i alarmiranja, preduzimaju i unapred definisanu akciju kao odgovor na pretnju. Obično je to blokiranje mrežnog saobraćaja od neke IP adrese ili korisnika.

6. Zaključak

Sistem za detekciju upada je ključni deo defanzivnih operacija, koji dopunjuje uobičajene statičke oblike odbrane računarske mreže. U osnovi, sistemi za detekciju upada kontrolišu mrežni saobraćaj, traže znakove napada i obeležavaju ih kada ih detektuju. U nekim slučajevima, oni mogu da preduzmu akcije u cilju zaustavljanja napada putem zatvaranja konekcije ili izveštavanja administratora mreže o uočenom incidentu. U skladu sa metodologijom detekcije, sistemi za detekciju upada su tipično

kategorisani kao sistemi za detekciju mrežnih nepravilnosti i anomalija. Iz perspektive podele, oni se generalno klasifikuju na mrežno bazirane ili host-bazirane, iako takva kategorizacija postepeno nestaje kod savremenih sistema za detekciju upada, kod kojih se informacije prikupljaju i od strane mrežnih i od strane host resursa. U pogledu performansi, sistemi za detekciju upada postaju sve precizniji, jer su sposobni da detektuju sve više različitih tipova napada, a da pri tom generišu sve manje lažnih alarma. Budući razvoj IDS-a ide u pravcu integrisanja veće količine informacija iz različitih izvora (tzv. senzorska fuzija), koristeći i mogućnosti veštačke inteligencije u cilju minimizacije log-fajlova neophodnih za podršku bazama potpisa. Ljudska intervencija u smislu kontrole je neophodna i sigurno će to i ostati u doglednoj budućnosti.

7. Literatura

1. Čisar, P., Maravić Čisar, S., Ivković, M., Milanov, D., Markoski, B. (2012). *Proposal of Algorithms for Statistical Intrusion Detection*, Metalurgia International, Vol. 17, No. 5, pp. 73–77.
2. Čisar, P., Bošnjak, S., Maravić Čisar, S. (2010). *Statistics of Network Local Maxima in Function of Intrusion Detection*, 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2010, Proceedings Vol. V, pp. 176–179.
3. Dulanović, N., Hinić, D., Simić, D. (2008). An Intrusion Prevention System as a Proactive Security Mechanism in Network Infrastructure, *YUJOR – Yugoslav Journal of Operations Research*, Vol. 18, No. 1, pp. 109–122.
4. Lazarevic, A., Kumar, V., & Srivastava, J. (2005). *Managing Cyber Threats: Issues, Approaches and Challenges*, Chapter: A survey of Intrusion Detection techniques. Boston: Kluwer Academic Publishers.
5. Lazarevic, A., Ertoz, L., Ozgur, A., Srivastava, J., & Kumar, V. (2003). *A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection*, Proceedings of the Third SIAM International Conference on Data Mining, San Francisco, pp. 25–36.
6. Pleskonjić, D., Đorđević, B., Maček, N., & Carić, M. (2006). *Sigurnost računarskih mreža*. Beograd: Viša elektrotehnička škola.
7. Ranđelović, D., Đorđević, V. (2011). A Test of IDS Application Open Source and Commercial Source, *NBP – Journal of Criminalistics and Law*, Kriminalističko-policijska Akademija, Beograd, pp. 45–65.
8. SANS Institute, Intrusion Detection, *FAQ Can you explain traffic analysis and anomaly detection?*, http://www.sans.org/resources/idfaq/anomaly_detection.php.

SYSTEM FOR DETECTION INTRUSIONS INTO INFORMATION INFRASTRUCTURE

Summary

Intrusion detection (ID) is an area of computer security that involves the detection of unwanted manipulations to computers and computer networks. ID is used to monitor and capture intrusions into computer and network systems which attempt to compromise their security. Many intrusions (attacks) manifest

in dramatic changes in the intensity of network events. An ID system is required to detect all types of malicious network traffic and computer usage that cannot be identified by a conventional firewall. This security method is needed in today's computing environment because it is impossible to keep pace with the current and potential threats and vulnerabilities in information systems. This paper gives a general overview of intrusion detection systems.