

# NEKE MOGUĆNOSTI KORIŠĆENJA SISTEMA ZA DETEKCIJU NAPADA KAO FORENZIČKOG ALATA

*D. Bulatović, M. Volar, M. Zec, Informatika ad, Beograd  
dusanb@informatika.com, milan@informatika.com, wabbit@informatika.com*

**Abstrakt:** *Sistemi za detekciju napada su razvijeni prvenstveno da funkcionišu kao alat koji služi za detekciju i sprečavanje napada na računar i/ili računarsku mrežu. Ipak, kod određivanja pravila koje oni kontrolišu i sigurnosne politike firme koju treba da realizuju, moguće je konfigurisati sisteme za detekciju napada da budu i veoma efikasan digitalni forenzički alat, koji će registrovati sve događaje potrebne za naknadnu analizu podataka u slučaju sigurnosnog incidenta.*

*Ključne reči: sistem za detekciju napada, digitalna forenzika, sigurnosna politika*

**Abstract:** *Intrusion Detection Systems are developed mostly to work as a tool that detect and prevent attacks to computer and/or computer network. However, in determining the rules they control, and company's security policy that should be enforced, it is possible to configure Intrusion Detection Systems to be efficient digital forensic tool, that audit all events necessary to trace data in case of a security incident.*

*Key words: Intrusion Detection System, digital forensic, security policy*

## 1. Uvod

Računarska forenzika je oblast koje se zadnjih godina intenzivno razvija i koja se može opisati kao analiza digitalne evidencije proistekle nakon sigurnosnog incidenta. Ona obuhvata prikupljanje i analizu forenzičkih podataka u toku istražnog postupka. Drugi značajni koraci obuhvataju pripremu za incident, detekciju i oporavak nakon incidenta. Forenzički odgovor nakon incidenta može se definisati kroz tri osnovna zahteva:

1. Prikupljanje evidencije o događaju bez promene ili narušavanja originalnih podataka.
2. Autentikacije da su prikupljenjeni podaci verni originalu.
3. Analize podataka na takav način da se ne vrši njihova modifikacija.

Računarski kriminal, vandalizam i obmane, koji su postali veoma rasprostranjena pojava često se oslanjaju na zloupotrebu računara i manifestuju se kao anomalije u ponašanju, bilo osobe koja koristi sistem, ili anomalije u ponašanju sistema u celini. I pored kontinualnog unapređivanja sigurnosti operativnih sistema, raspoložive sigurnosne karakteristike računara nisu dovoljne da detektuju anomalije u ponašanju korisnika sistema. Sigurnosni alati koji se instaliraju na perimetru lokalne mreže prema Internetu (npr., mrežna barijera), ne mogu da budu od koristi kada je napadač neko ko se nalazi unutar same lokalne mreže, a statistike pokazuje da je to najčešći vid pravljenja pronevera. Karakteristični su sledeći tipovi napada od kojih, generalno, operativni sistemi ne mogu u ovom momentu obezbediti zaštitu [4]:

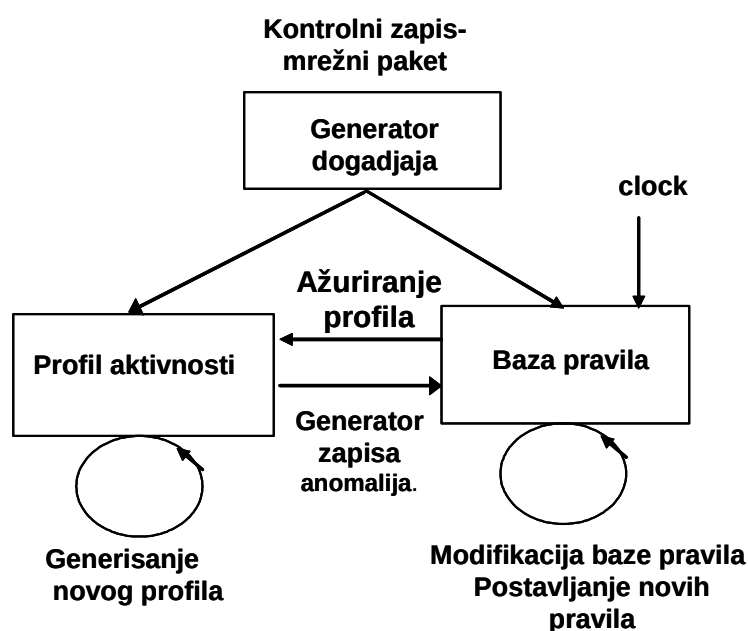
- napadači koji se predstavljaju kao legitimni korisnici,
- korisnici sa visokim stepenom privilegija koji se ponašaju destruktivno,
- legitimni korisnici koji zloupotrebljavaju greške u konfiguraciji sistema ili druge systemske ranjivosti,
- Trojanski konji, odnosno izvršni programi koji su zlonamerno modifikovani da izvršavaju nedozvoljive funkcije.

Do nedavno je bezbednost računara bila, tradicionalno, više orjentisana na sprečavanje nedozvoljenih aktivnosti i zaštitu računara i mreže od napada. Međutim, u poslednje vreme se prepoznaje da su i forenzički aspekti bezbednosti takođe od izuzetnog značaja. U tom smislu će ovaj rad biti posvećen mogućnostima konfigurisanja sistema za detekciju napada tako da u slučaju sigurnosnog incidenta sistem obezbeđuje neophodne podatke za forenzičku analizu, pri čemu će poseban akcenat biti dat na iskustvima firme Informatika ad u toj oblasti.

## 2. Sistemi za detekciju napada

Sistemi za detekciju napada se istražuju više godina [2] u pokušaju da se unese neka vrsta veštačke intelegencije u postupku identifikacije anomalija u radu sistema. Mnogi od njih svoj rad zasnivaju na ekstenzivnom korišćenju kontrolnog zapisa (loga), sa ciljem da sakupi što je moguće više znanja/informacija o korisnicima sistema.

Izvorni sistem za detekciju napada predstavila je Dorothy Denning [1] 1987 godine i on je nezavisan od sistemskog ili aplikacionog okruženja, osetljivosti sistema ili tipova napada. U nastavku teksta je dat kratak opis ovog modela sa blok dijagramom prikazanim na Slici 1, gde su prikazane osnovne finkcije sistema i veze između pojedinih komponentata.



Sl. 1. Izvorni sistem za detekciju napada

Osnovna ideja modela je da održava skup profila za subjekte (obično ali ne i obavezno korisnike sistema). Kada se generiše slog kontrolnog zapisa model ga upoređuje sa odgovarajućim profilom i potom odlučuje da li da ažurira profil na osnovu provere u bazi pravila da li je to ponašanje abnormalno. Baza ekspertskih pravila takođe može da se tokom rada ažurira na osnovu podataka o anomalijama u radu dobijenih posle upoređenja sa profilom korisnika. U toku rada posmatraju se aktivnosti sistema kao što je pristup datotekama, programi koji se izvršavaju, prijave korisnika i slično. Pri tome ne postoje specifična znanja o ciljnom sistemu i njegovim eventualnim slabostima mada ona mogu biti od izuzetne koristi.

Uprkos postojanja više formi napada oni se mogu svrstati u dve glavne kategorije, a prema tome se svrstava i metodologija prema kojoj se napadi detektuju, a to je na osnovu **zloupotrebe** sistema ili na osnovu **anomalija** u radu sistema.

- Napadi zloupotrebom sistema su dobro definisani napadi na poznate slabe tačke sistema. Oni mogu biti uočeni posmatranjem određenih akcija koje se izvode nad određenim objektima.
- Anomalije u radu sistema predstavljaju devijacije u odnosu na uobičajene uzorke aktivnosti. One se otkrivaju definisanjem profila sistema koji se posmatra, a potom detekcijom značajnih odstupanja od definisanog profila.

Kako se napadi zloupotrebom odigravaju po unapred utvrđenom uzorku događanja oni mogu i biti detektovani metodama koje se zasnivaju na prepoznavanju uzorka. Ovo može biti urađeno kao u prilazu opisanom u [5].

Međutim, anomalije u sistemu je teže detektovati. Ne postoji fiksni uzorak ponašanja koji se može očekivati nego je neophodna mogućnost prepoznavanja uzorka slična onoj koju ima čovek, kombinovana sa preciznošću računarskog programa. Na taj način bi se dobilo kontinualno posmatranje rada sistema u cilju detekcije potencijalnih napada, a postojala bi mogućnost da se ignorišu lažni napadi koji potiču od legitimnih aktivnosti korisnika. Drugim rečima cilj je minimiziranje verovatnoće pogrešne klasifikacije.

Kod detekcije anomalija zlonamerna aktivnost je najšestće podskup aktivnosti koje u sebi sadrže anomalije. Često, međutim, zlonamerna aktivnost može biti izvedena kao zbir pojedinačnih aktivnosti od kojih ni jedna u sebi ne sadrži anomalije. Sa stanovišta detekcije napada idealno bi bilo kada bi se aktivnost koja sadrži anomalije podudarala sa subverzivnom aktivnošću, međutim, to nije uvek slučaj.

Prethodna šema klasifikacije napada je zasnovana na metodologiji njihove detekcije. Druga mogućnost klasifikacije napada, prikazana u [6], zasniva se na tipu napada i deli ih na sledećih šest grupa:

1. Pokušaj proboja u sistem: detektovan na osnovu netipičnog profila ponašanja ili na osnovu kršenja sigurnosnih ograničenja.
2. Napad lažnim predstavljanjem: detektovan na osnovu netipičnog profila ponašanja ili na osnovu kršenja sigurnosnih ograničenja.
3. Probijanje kontrole sigurnosti sistema.
4. Curenje informacija: detektovano na osnovu netipičnog korišćenja I/O resursa.
5. Odbijanje servisa: detektovano na osnovu netipičnog korišćenja sistemskih resursa.
6. Zlonamerno korišćenje: detektovano na osnovu netipičnog profila ponašanja, kršenja sigurnosnih ograničenja, ili korišćenja specijalnih privilegija.

Primarni cilj sistema za detekciju napada je da identifikuje, po mogućnosti u realnom vremenu, neovlašćeno korišćenje ili zloupotrebu računara kako od spoljašnjih korisnika tako i od korisnika unutar same mreže. U slučaju napada koji se manifestuju kao anomalija u ponašanju korisnika, detekcija napada se bazira na ideji da je ta anomalija simptom koji ukazuje na ilegalnu ili kriminalnu aktivnost.

Sa druge strane, primarni cilj kada je u pitanju forenzika jeste da se dobije dovoljno informacija o kriminalu koje će dovesti do samog kriminalca. Kada je u pitanju računarski sistem mogućnost anonimnog rada ohrabruje kriminalca na destruktivnu aktivnost pri

čemu je ekstremno teško da se kasnije utvrdi identitet onog ko je to napravio. Prema tome, mogućnost da se dobije slika o uobičajenom ponašanju korisnika računara je imperativ ako se želi doći do nekih činjenica koje će omogućiti identifikaciju počinioca nelegalnih radnji.

Analiza raspoloživih log datoteka uvek predstavlja osnovu za dobijanje evidencije o događajima na računarskom sistemu. Međutim, na višem nivou, često je potrebno imati podatke koji će omogućiti dublju analizu da bi se sužilo polje podataka koji se analiziraju, ili čak da se dobije spisak potencijalnih prekršioca. Računarski kriminal je uvek rezultat ljudskih aktivnosti, bilo da su u pitanju legalni korisnici sistema ili spoljašnji napadači. Zbog toga je ne samo poželjno imati log aktivnosti na sistemu da bi se dobila tražena informacija, nego i neki mehanizam koji se zasniva na veštačkoj inteligenciji i koji će omogućiti kreiranje profila korisnika sistema. Naprimera, informacija da se korisnik A prijavio na sistem u 08 sati je beskorisna ukoliko se ne zna da se korisnik A nikada ne prijavljuje u to vreme. Sa druge strane, saznanje da se korisnik A nikada ne prijavljuje u 08 sati je jedino moguće dobiti ako se zna tipično ponašanje, odnosno profil ponašanja korisnika A. U tom smislu je sistem za detekciju napada koji se bazira na detekciji anomalija u ponašanju korisnika od neprocenjive vrednosti.

Ovakav sistem neće samo obuhvatiti podatke koji se odnose na karakteristično ponašanje napadača, nego je čak u mogućnosti i da obezbedi mehanizam koji može da isčisti podatke i da dođe do samog uzorka koji ukazuje na alarmantnu ili nedozvoljenu aktivnost na računaru. Istraživanja u ovoj oblasti su koncentrisana na klasifikaciju statističkih podataka o korisnicima upotrebom veštačke inteligencije, kao što su neuralne mreže, genetsko programiranje, ili pak Bajesove mreže [3]. Kao rezultat tih istraživanja prevaziđene su mnoge tradicionalne prepreke u detekciji napada.

### ***Detekcija anomalija u ponašanju korisnika***

Modeliranje korisničkog ponašanja može se bazirati na standardnom logu sistema kao izvoru informacija koje se daju sistemu za detekciju napada. Sledeći podaci, izvučeni iz loga, mogu poslužiti da se dobije tipično ponašanje korisnika:

- Vreme aktivnosti korisnika – Vreme u kojem je korisnik normalno aktivan na sistemu.
- Korisnikovi računari – Skup računara na koji se korisnik uobičajeno prijavljuje.
- Spoljni računari – Skup računara na koje se korisnik u svojoj normalnoj aktivnosti povezuje komandama (naprimera FTP računari).
- Skup komandi – Uobičajeni skup komandi korisnika pri normalnom radu.
- Korišćenje procesora – Tipični uzorak korišćenja CPU – a za korisnika.

U cilju postizanja efektivnosti ovakvog sistema potrebno je da prođe određeni period učenja, naprimera, dve nedelje. Nakon toga sistem za detekciju napada se može testirati unošenjem primerka neuobičajenog ponašanja različitih administratora sistema. Ovakvi događaji moraju biti prepoznati i obeleženi, da bi kasnije, u eventualnoj forenzičkoj analizi bili putokaz koji će dovesti do bržeg otkrivanja počinioca kriminalnog dela.

Eksperimenti sa praćenjem ponašanja korisnika su u firmi "Informatika ad" rađeni na sistemu za detekciju napada ***Intruder Alert***, proizvodu američke firme Symantec, čiji je Informatika *Solution partner*. Način funkcionisanja ovog sistema za detekciju napada se može definisati pravilima i sigurnosnom politikom koju sam korisnik odredi. Kao izvor svojih informacija Intruder Alert koristi sistemski log, sistemske poruke i bezbednosne

poruke. Njegova osnovna funkcija je, svakako, da pošalje poruku upozorenja administratoru u slučaju da se desi narušavanje pravila koje on kontroliše a može i aktivno da deluje prekidom veze, odjavom korisnika ili zaustavljanjem procesa. Međutim, u slučaju da se desi kriminalna radnja koju sistem nije detektovao kao napad jer se nalazi ispod praga detekcije, moguće je vršiti naknadnu analizu istih prikupljenih podataka ali sada prema drugim kriterijumima, onim koji će ukazati na neuobičajeno ponašanje korisnika.

Definisanje ovih novih pravila je funkcija izveštavanja navedenog sistema za detekciju napada, pa se praktično trenutno mogu dobiti grafički prikazi ponašanja korisnika ili sistema po najrazličitijim kriterijumima ili kombinaciji istih. Na taj način može se značajno suziti krug sumnjivih korisnika koji će potom biti podvrgnuti daljim ispitivanjima. Ipak, u slučaju navedenog sistema za detekciju napada, u forenzičkoj analizi je potrebna ljudska intervencija, dok bi se automatizam u detekciji neuobičajenog ponašanja mogao realizovati samo metodama koje koriste veštačku inteligenciju u analizi prikupljenih podataka [2].

Sistemi za detekciju napada pored praćenja aktivnosti korisnika mogu da se konfigurišu da štite integritet datoteka i direktorija, sa ciljem da alarmiraju administratora ukoliko je neka od datoteka ključnih za funkcionisanje sistema izmenjena, zamenjena, ili ako se desio neovlašćeni pristup. Korisnik može da izabere datoteke koje štiti pa čak i algoritme kojima se štiti integritet podataka a prema kojima se pravi digitalni otisak (hash) datoteka. Na osnovu takvih zahteva sistem za detekciju napada beleži u logu svaki pristup ili promenu posmatranih datoteka. U sledećem paragrafu je dat primer realizacije funkcije za dobijanje digitalnog otiska, koja, u sprezi sa sistemom za detekciju napada, može da pojednostavi dobijanje potvrde o originalnosti podataka.

### ***Detekcija promene sadržaja datoteka i direktorija pomoću digitalnog otiska***

Računarski forenzici se uglavnom oslanjaju na matematičke algoritme u dokazivanju da se sadržaj diska ili pojedinih datoteka u potpunosti podudara sa originalom. Ovi algoritmi takođe služe i kao sredstvo koje garantuje da podaci nisu promenjeni ili da im nešto nije pridodato u toku samog sudskog postupka. U prošlosti su za ovu namenu korišćeni algoritmi kao što su CRCHECK ili CRC32 koji su generisali kontrolni podatak dužine 32 bita. Ovaj kontrolni podatak je iste dužine za bilo koju datoteku na koju se odnosi pa se sa pravom mogla staviti primedba da ako u računar postoji više od  $2^{32}$  datoteka onda najmanje dve moraju imati isti digitalni otisak (hash). Zbog toga se, u uslovima savremenih računara koji su značajne procesorske snage i mogućnosti napada pretraživanjem (brute force attack), za tu namenu sada zahtevaju jači algoritmi kao što je MD5 (128 bita) ili SHA1 (160 bita).

Ukoliko se mehanizam za osiguranje integriteta poruke bazira na tajnom ključu onda se on obično naziva MAC (Message Authentication Code). MAC kôd koriste strane koje međusobno komuniciraju i koje poseduju tajni ključ za proveru autentičnosti poruke koja se prenosi između njih a može takođe da štiti uskaladištene podatke. Ukoliko MAC koristi kriptografsku "hash" funkciju u konjukciji sa tajnim ključem tada se on naziva HMAC [7]. HMAC se koristi u kombinaciji sa pouzdanom i unapred verifikovanom "hash" funkcijom, kao što je, naprimer, SHA1 algoritam. Rukovanje tajnim ključem kod generisanja i provere HMAC-a tom prilikom mora biti jednostavno i jasno definisano. HMAC se formira tako da se u slučaju potrebe "hash" funkcija može da zameni novom bržom i pouzdanijom, i da je to jednostavno izvesti.

U "Informatici ad" je razvijen alternativni metod u generisanju HMAC-a, gde se umesto SHA1 algoritma za pravljenje digitalnog otiska koristi algoritmom Rindael [8] nedavno usvojen kao AES standard (Advanced Encryption Standard) namenjen za korišćenje u bankarstvu. Za ovu namenu je uzeto da i ključ i digitalni otisak budu 256 bita što je više nego dovoljna garancija da datoteka ne može biti promenjena a da se to ne detektuje.

### 3. Zaključak

Sistemi za detekciju napada koriste različite tehnologije u detekciji i sprečavanju napada, počev od statističkih pa do upotrebe veštačke inteligencije, no bez obzira na sve to napade nije moguće u potpunosti sprečiti. Kada se napad desi po pravilu je potrebna ljudska intervencija u pretraživanju podataka koja će, eventualno, dovesti do počinioca. Međutim, ukoliko se sistemima za detekciju napada prilagodi konfiguracija tako da odgovara potrebama forenzike, oni mogu svojim prikupljenim podacima značajno olakšati pretraživanje podataka prilikom naknadne analize uslova u kojima se napad desio. Njihov automatizam u detekciji napada će u tom slučaju biti od neprocenjive koristi i kao forenzički alat za pronalaženje počinioca kriminalne radnje.

### 4. Reference

- [1] Dorothy E Denning. "An Intrusion Detection Model". In IEEE Transactions on Software Engineering, Number 2, page 222, February 1987.
- [2] Dušan Bulatović, Dušan Velašević: Sistemi za detekciju i sprečavanje napada, Stručna knjiga, Beograd, jun 2001.
- [3] Dušan Velašević, Dušan Bulatović: "Architecture and Organisation of Intrusion Detection and Prevention Systems Based on Bayesian Networks", Procc. of CCCT 2003. Orlando, 2003.
- [4] H.S. Vaccaro and G.E. Liepins, "Detection of Anomalous Computer Session Activity", 1989 IEEE Computer Society Symposium on Security and Privacy, May 1989, pp. 280-289.
- [5] Sandeep Kumar, Gene Spaford. "A Pattern Matching model for Misuse Intrusion Detection", Proceedings of the 17th National Computer Security Conference, October 1994.
- [6] Stephen E. Smaha. Haystack: "An Intrusion Detection System". In Fourth Aerospace Computer Security Applications Conference, pages 37-44, Tracor Applied Science Inc., Austin, TX, Dec 1988.
- [7] American Bankers Association, "Keyed "hash" Message Authentication Code", ANSI X9.71, Washington, D.C., 2000.
- [8] Federal Information Processing Standard FIPS 197, publikacija na Internetu: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>