Sistemi za zaznavo vdorov

Dejan Erjavec, Roman Kotnik, Andrej Kos

Fakulteta za elektrotehniko, Tržaška 25, 1000 Ljubljana
E-pošta: dejan.erjavec@ltfe.org

Intrusion detection systems

Intrusion detection and prevention systems are an important part of network security infrastructure.
In this article we test two open source implementation of intrusion detection systems.

The introduction gives an overview, technologies and types of IDS systems. We follow up with presentation of two open source IDS implementations – Snort and Suricata.

Testing conditions are presented next, with result and a conclusion at the end of the article.

1 Uvod

Detekcija vdora (angl. *intrusion detection*) je proces nadzorovanja in analize dogodkov v računalniškem sistemu ali mreži. Analiza zajema iskanje možnih incidentov, ki so kršitve ali takojšnja nevarnost kršitve varnostnih pravil oziroma dogodki, ki niso v skladu s standardno uporabniško prakso. Incidenti so lahko posledica zlonamerne programske kode (angl. *malware*), pridobitev neavtoriziranega dostopa do sistema iz medmrežja (angl. *interneta)* ali napačne uporabe oz. zlorabe privilegijev avtoriziranih uporabnikov. Čeprav je večina incidentov po naravi zlonamernih, pa se lahko zgodijo tudi nenamerno; na primer, uporabnik lahko naredi napako pri vpisu naslova in se nenamerno želi povezati na sistem za katerega nima avtoriziranega dostopa [5].

Sistem detekcije vdora (angl. *intrusion detection system* – IDS) je programska oprema, ki avtomatizira proces detekcije vdora. Sistem preprečitve vdora (angl. *intrusion prevention system* – IPS) je programska oprema, ki ima zmožnosti detekcije in tudi možnosti poizkusa preprečitve incidentov. Obe rešitvi ponujata podobne zmogljivosti in administratorji lahko onemogočijo sposobnost preprečitve vdorov v IPS produktih zato je za uporabo v nadaljevanju uporabljena združena kratica IDPS; sistemi za detekcijo in preprečevanje vdorov (angl. *intrusion detection and prevention systems*)[4][5][6][7].

1.1 Tehnologije IDPS

IDPS so primarno osredotočeni na identificiranje možnih incidentov. IDPS lahko zazna napadalca, ki ogroža sistem z izkoriščanjem varnostnih lukenj. IDPS bi nato lahko takoj poročal varnostnim administratorjem, ki s hitrim odzivom omejijo škodo povzročeno z incidentom. Veliko IDPS produktov se lahko nastavi za delovanje podobno požarnemu zidu, kar omogoča spremljanje in, po potrebi, uveljavljanje varnostne politike. Nekateri IDPS lahko nadzorujejo tudi prenos datotek in identificirajo nenavadne prenose, kot je kopiranje baze podatkov na prenosnik uporabnika [4][5].

Veliko IDPS produktov lahko prepozna tudi poizvedovalne aktivnosti (ang. *reconnaissance activity*), ki ponavadi pomenijo pripravo na napad. Primer take aktivnosti je skeniranje gostiteljev in vrat, ki ga uporablja veliko internetnih črvov. IDPS lahko blokira tako početje in obvesti varnostne administratorje, ki nato priredijo varnostne protokole in s tem preprečijo podobno zlorabo v prihodnje. Zaradi velike razširjenosti poizvedovalne aktivnosti se detekcija le te primarno izvaja v varovanih notranjih omrežjih.

Poleg zaznave incidentov in obveščanja se IDPS v organizacijah uporabljajo tudi v druge namene. Nekaj od teh:

- **Prepoznava pomankljivosti v varnostnih pravilih (angl. *security policy*).** IDPS ponuja do neke mere preverjanje implementacije varnostnih pravil. Za primer vzamemo zaznavo napačne konfiguracije požarnega zidu.

- **Dokumentiranje obstoječih nevarnosti organizaciji.** IDPS beležijo informacije o zaznanih napadih. Podatki o pogostosti in lastnostih različnih napadov na organizacijo pomagajo pri izvajanju ustreznih varnostnih ukrepov in poučevanju zaposlenih o tipih nevarnosti, ki jim grozijo.

- **Odvrača posameznika od kršenja varnostne politike.** Če se posamezniki zavedajo, da njihove aktivnosti spremlja IDPS bodo manj verjetno kršili varnostna pravila in s tem tvegali razkritje.

Zaradi vse večje odvisnosti od informacijskih sistemov in hkrati večje potencialne škode ob morebitnem napadu na le te, so IDPS produkti postali obvezen dodatek k varnostni infrastrukturi[4].

1.2 Tipi tehnologij IDPS

Obstaja več tipov IDPS tehnologij. Razdelimo jih v naslednje skupine glede na tipe dogodkov, ki jih spremljajo in načine, na kakšne so uporabljeni:

- **Omrežni (angl. *network-based*)**, ki spremljajo omrežni promet na določenih segmentih ali napravah in analizirajo obnašanje protokolov. Zaznajo lahko več zanimivih dogodkov. Največkrat so uporabljeni na meji

med omrežji (v bližini mejnih usmerjevalnikov, požarnih zidov, VPN (angl. *Virtual Private Network*, virtualnih zasebnih omrežjih) serverjev) [4][7].

- **Brezžični (wireless)** spremljajo brezžični promet in analizirajo pripadajoče brezžične protokole. Ta tip ne more zaznati sumljive aktivnosti v aplikacijskem ali višjem sloju[1].
- **Analiza obnašanja omrežja (angl. *Network Behavior Analysis* – NBA)**, ki pregleduje omrežni promet in zaznava nenavaden tok prometa, kot »denial of service« napad ali določene črve in ostalo zlonamerno programsko namero. Prav tako spremlja kršitve uporabniške politike. NBA sistemi so največkrat postavljeni za spremljanje prometa v notranjem omrežju.
- **Uporabniški (host based)** spremljajo določenega gostitelja in dogodke za možne kršitve. Ponavadi se uporabljajo na kritičnih gostiteljih kot na primer na javno dostopnih strežnikih in strežnikih z občutljivimi informacijami.

Nekateri tipi so bolj dovršeni kot drugi. Omrežni in uporabniški IDPS so v uporabi dlje časa. NBA programi so novejši sistemi, ki so nastali predvsem iz produktov za zaznavo DDoS napadov in produktov za spremljanje notranjega prometa v omrežju. Brezžični sistemi so tudi relativno novi produkti, razviti zaradi vse večje popularnosti WLAN (angl. *Wireless Local Area Network*, brezžična lokalna omrežja)[4].

1.3 Uporaba in integracija različnih tehnologij IDPS

Vsak tip IDS tehnologij ponuja v osnovi različne sposobnosti zbiranja informacij, beleženja, detekcije in preprečevanja napadov. Nekateri zaznajo dogodke, ki jih ostali ne. Nekateri ponujajo boljše zmogljivosti pri globoki analizi, drugi ponujajo bolj natančno zaznavo nevarnosti. Zaradi tega se lahko organizacije najbolje zaščitijo z uporabo večih tipov IDPS sistemov.

V večini okolij ne moremo zgraditi robustne IDPS rešitve brez uporabe večih tipov IDPS tehnologij. Na primer, omrežni tip ne more spremljati brezžičnega prometa. V tabeli 1 so navedene ključne lastnosti in primerjava posameznih tipov.

Za večino okolij je potrebna kombinacija omrežnega in uporabniškega IDPS sistema za uspešno IDPS rešitev. Poleg tega, nekatere organizacije uporabljajo tudi več produktov istega tipa. S tem ponavadi dosežemo bolj natančno detekcijo, saj različni produkti uporabljajo drugačno metodologijo zazanave. Prav tako je poleg redundance s tem tudi olajšano potrjevanje napada ali izločanje lažno-pozitivnih dogodkov[4].

Tabela 1

IDPS tip	Zaznavanje nevarne aktivnosti	Področje	Prednosti
Omrežni	Omrežni, transportni in aplikacijski TCP/IP nivo	Več pod-omrežij in skupin gostiteljev	Najširša in temeljita analiza protkolov
Brezžični	Brezžična aktivnost	Brezžična LAN omrežja, brezžični uporabniki	Edini IDPS za analizo brezžičnih protokolov
Analiza obnašanja (NBA)	Omrežna, transportna in aplikacijska TCP/IP aktivnost, ki povzroča nenavaden promet	Pod-omrežja in skupine gostiteljev	Najbolj uspešen IDPS za zaznavo DoS napadov in skeniranja portov
Uporabniški	Gostiteljske aplikacije, operacijski sistem	Posamezen gostitelj	Edini IDPS, ki lahko analizira aktivnost preko »end-to-end« kriptiranih komunikacij

2 Snort

Snort je odprtokoden omrežni sistem za zaznavo napadov. Zmožen je realnočasovne analize prometa in logiranja paketov na IP omrežjih. Lahko izvaja analizo protokolov ter išče vzorce v vsebini in se ga lahko uporabi za zaznavo veliko različnih vrst napadov in skeniranj, kot so prenapolnjenje spomina (ang. buffer overflow), skrito skeniranje vrat (ang. stealth port scan), napad na skupni vhodni vmesnik (angl. Common Gateway Interface – CGI attack), blokiranje strežniških sporočil (angl. Server Message Block – SMB) in veliko več [3].

Snort je lahko postavljen na tri načine: kot vohljač (angl. sniffer), zapisovalnik paketov (angl. packet logger) in kot omrežni sistem za zaznavo vdorov. Vohljač preprosto bere omrežne pakete in jih izpisuje v konzoli, zapisovalnik jih zapisuje v datoteke medtem ko je detektor za zaznavo vdorov najbolj kompleksen in nastavljiv način. Ta način lahko analizira promet in ga primerja proti uporabniško nastavljenim pravilom. Glede na to analizo lahko tudi izvaja določene ukrepe na mrežnem prometu[9][10].

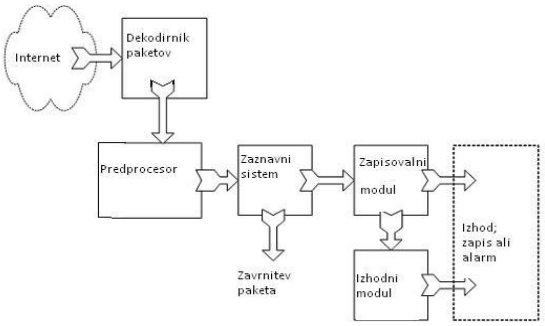
Poleg podpisov, ki so na voljo preko Snort skupnosti in podpisov na voljo registriranim uporabnikom, lahko uporabniki pišejo lastne podpise, ki so posebej prilagojeni za njihovo omrežje. Ta zmožnost zagotavlja veliko prilagodljivost pogona za varnostne potrebe različnih omrežij [3].

[1] Brezžični sistemi za zaznavo se v načinu delovanja razlikujejo od ostalih tipov. Brezžični sistem IDPS ne vidi vseh paketov na omrežju, saj mora zaradi tipa fizične povezave spremljati več kanalov brezžičnega omrežja in med njimi pogosto preklapljati.

2.1.1 Komponente Snort sistema

Snort je logično razdeljen na več komponent. Te komponente sodelujejo pri zaznavi določenih napadov in pri generiranju obvestil v zahtevanem formatu. Sistem za zaznavo vdorov temelječ na odprtokodni rešitvi Snort vsebuje naslednje komponente [10]:

- Dekodirnik paketov
- Predprocesor
- Zaznavni sistem
- Sistem za obveščanje in generiranje alarmov
- Izhodni moduli



Slika 1: Pregled komponent Snorta

3 Suricata

Suricata je odprtokodno orodje za zaznavo in preprečevanje napadov in je izdana pod licenco GPLv2 (General Public License). Za razvoj skrbi fundacija Open Information Security Fundation – OISF. Podobno kot Snort, Suricata temelji na vnaprej napisanih pravilih preko katerih spremlja omrežni promet in generira alarme v primeru zaznave napada.

Prva beta verzija Suricate je izšla 1. januarja 2010. Podpira Snort-ov format pisanja pravil in zapisovanja, večjedrno procesiranje, strojno pospeševanje, IPv6, vtičnike za interakcijo z ostalimi aplikacijami in t.i. "unified" format izpisa. Pomembna komponenta Suricate je tudi HTTP normalizator in HTP knjižnica, ki skrbi za razčlenjevanje HTTP sej, kar pomeni, da Suricata razume promet na najvišjem, sedmem nivoju ISO-OSI modela [2].

V nasprotju s Snort-om je Suricata dokaj nov sistem, ki ima nekaj dodatnih funkcionalnosti a je zelo slabo dokumentiran.

4 Primerjava Snort/Suricata

Že leta je Snort (razvit s strani SourceFire) 'de facto' standard za odprto kodni sistem za zaznavo in preprečevanje vdorov. Združuje pozitivne stvari podpisov, protokolov in zaznave na osnovi anomalij in je najbolj razširjen IDS/IPS na svetu.

Suricata, nov in manj razširjen produkt razvit s strani Open Information Security Foundation (OISF), je izšel pred kratkim in deluje obetujoče. Deluje na osnovi podpisov a vsebuje tudi nove tehnike zaznave. Pogon vsebuje HTTP normalizator in razčlenjevalnik (knjižnica HTP) za razumevanje prometa na sedmem nivoju ISO-OSI modela [1][2][3].

Primerjava obeh sistemov je povzeta v tabeli 2.

Tabela 2

Parameter	Suricata	Snort
Pravila	VRT::Snort pravila, EmergingThreats	VRT::Snort pravila, EmergingThreats, SO pravila
Večnitenje	Večnitnost	Enonitnost
Dokumentacija	Slabo dokumentirano	Dobro dokumentirano, ogromno originalne dokumentacije
Zapisovanje	Tekstovna datoteka, baza, unified2	
IPv6	Podprt	Podprt, če preveden pravilno
Pospeševalnik zajema	PF_RING, pospeševalnik zajema paketov	Brez, uporaba libpcap knjižnice
Konfiguracija	suricata.yaml, classification.conf, reference.config, threshold.config	snort.conf, threshold.conf
Analiza iz datoteke	da	
Prikazni dodatki	Squil, Aanval, BASE, Snortsnarf	

5 Testiranje

Namen našega testiranja je vzpostavitev in preverjanje delovanja dveh odprtokodnih rešitev za sistem zaznave vdora. To sta Snort in Suricata. Ugotoviti želimo katera rešitev je bolj primerna za mala do srednja podjetja (do trideset uporabnikov) z omejenimi finančnimi sredstvi namenjenim takemu sistemu. Na voljo imamo srednje zmogljiv strežnik ter predvidevamo neizkušenost administratorjev s takim sistemom.

Zaradi teh omejitev, bi bila serijska postavitev in s tem učinkovito preprečevanje napadov nemogoča (strežnik bi zaradi premajhne zmogljivosti upočasnjeval povezavo). Zato simuliramo pasivno postavitev strežnika. Želimo preveriti zmogljivosti in zahtevnost namestitve obeh rešitev ter oceniti zahtevnost naknadnega vzdrževanja takega sistema.

Za napade bomo izbirali pogoste nevarnosti, ki jih lahko pričakujemo v realnem okolju. Večinoma so to zlonamerni črvi, e-poštni napadi in izkoriščanje bolj znanih ranljivosti v raznih protokolih. Testirali bomo v praznem omrežju, kjer razen naših generiranih napadov na omrežnem vmesniku ne bo prometa. V primeru priklopa v živo omrežje in ob vseh vklopljenih alarmih je bilo v časovnem obdobju dvajsetih minut čez štiri tisoč alarmov (omrežje je razvojno, kjer je komunikacija drugačna oz. za IDS bolj nenavadna kot v normalnem omrežju) in v takem okolju je natančno testiranje nesmiselno.

Snort:

Verzija: 2.9.0 (Build 68)
Pravila: VRT Snort Rules 2.900

Suricata:

Verzija: 1.0.2
Pravila: VRT Snort Rules 2.900

5.1 Testiranje

Spisek napadov:

- HTTP DELETE
- Code Red II črv
- PHP ranljivost omjenega spomina
- Aa.bot
- Phpinclude.worm
- Nachi ping + Nachi.B WebDav
- Nimda črv
- Lupper črv

Rezultati testiranja so povzeti v tabeli 3.

Tabela 3: Osnovno testiranje

Napad	**Zaznava Suricata**	**Zaznava Snort**
CodeRed II	DA	NE
PHP memory vulnerability (ranljivost spomina)	DA	DA
aa.bot	NE	NE
Phpinclude.worm	DA	DA
Nachi.B	DA	DA (delno)
Nimda Worm	DA	DA
Lupper Worm	DA	DA
Skupaj:	**6/7**	**5.5/7**

Omeniti je potrebno tudi nezmožnost zaznavanja napadov preko E-pošte osnovne konfiguracije Snorta. Potrebno je bilo naknadno nastavljanje in optimiziranje. Suricata z zaznavanjem ni imela problemov pri osnovni namestitvi.

6 Zaključek

Pri preprostosti namestitve samega sistema ter dodatkov se je bolje izkazal Snort (možnosti paketne namestitve preko Advanced Packaging Tool – APT orodja). Čeprav ročno prevajanje in namestitev samega Snorta ni zahtevna ob predpogoju poznavanja osnov operacijskega sistema Linux, pa je potrebno globje znanje ter veliko konfiguriranja ob namestitvi dodatkov, kot sta Barnyard2 in Acidbase. Vsi dodatki, ki so kompatibilni s Snortom, so zaradi možnosti enakega formata izpisa kompatibilni tudi s Suricato.

Suricata vsebuje novosti kot so večnitno procesiranje in pospeševanje zajema paketov a trpi za manjkom dokumentacije. Snort je zrel sistem in ostaja močan IDS/IPS z dobro dokumentacijo in veliko razširjenostjo.

Naše testiranje je pokazalo, da osnovni namestitvi ne delujeta enako dobro. Ob izbiri istih podpisov tako za Snort kot za Suricato, se je veliko bolje pri zaznavanju pogostih napadov v omrežjih obnesla Suricata. Izkazalo se je, da je torej Suricata s privzeto namestitvijo bolj primerna za hitro implementacijo. Snort nas je razočaral predvsem zaradi začetnega vtisa delovanja. Brez testiranja neizkušen uporabnik nebi opazil, da nekaterih napadov Snort s privzeto konfiguracijo ne zaznava.

Obe rešitvi za optimalno delovanje potrebujeta vsakodnevno spremljanje alarmov, dodajanje pravil ter prilagajanja glede na obliko prometa v varovanem omrežju.

7 Literatura

[1] http://www.aldeid.com/index.php/Suricata-vs-snort
[2] http://www.openinfosecfoundation.org/
[3] http://www.snort.org/
[4] K. Scarfone, P.Mell, Guide to Intrusion Detection and Prevention Systems, National Institute of Standards and Technology, Gaithersburg, 2008
[5] http://en.wikipedia.org/wiki/Intrusion_detection_system
[6] http://en.wikipedia.org/wiki/Intrusion_prevention_system
[7] http://en.wikipedia.org/wiki/Network_intrusion_detection_system
[8] P. Skrobanek, Intrusion Detection Systems, InTech, Rijeka, 2011
[9] R.U. Rehman, Intrusion Detection Systems with Snort, Prentice Hall PTR, New Jersey, 2003
[10]C. Scott, P. Wolfe, B. Hayes, Snort for Dummies, Wiley Publishing, Inc., Hoboken, New Jersey, 2004
[11]D. Kozic, Izvajanje napadov v Spirent, Poročilo, Ljubljana, 2010
[12] D. Erjavec, Omrežni sistemi za zaznavo in preprečevanje vdorov na osnovi odprte kode, diplomsko delo, junij 2011