Centar Informacijske Sigurnosti

Snort IDS

listopad 2011.

CIS-DOC-2011-10-028

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

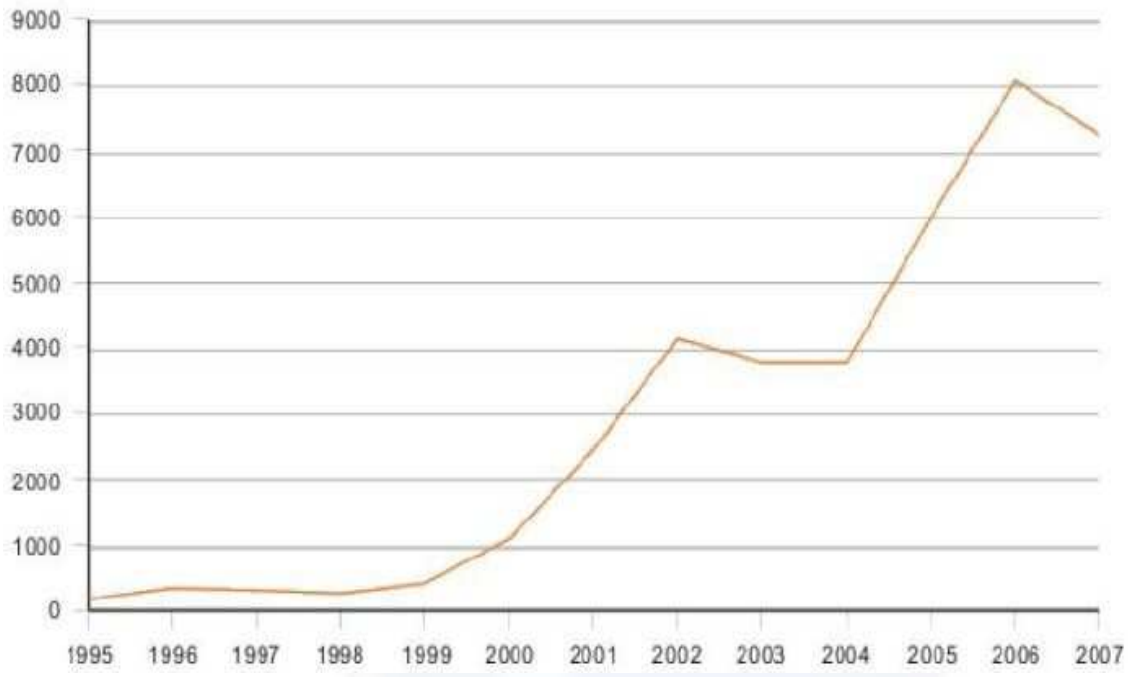
Prava korištenja

Sadržaj

1. Uvod

Brzi razvoj Interneta i tehnologija potiče razvoj računalnih virusa i povećanje broja pokušaja upada u sustav te se zbog toga razvija sve više tehnika za računalnu sigurnost. Upadi u sustav su neovlašteni pristupi informacijama uz njihovo korištenje ili mijenjanje. Skoro svakodnevno se otkrivaju nove vrste upada i propusti u sustavima koji se iskorištavaju. Prema podacima iz organizacije CERT (eng. *Computer Emergence Response Team*) u 15 godina broj prijavljenih sigurnosnih aktivnosti porastao je gotovo 1000 puta, a udvostručuje se svake sljedeće godine (Slika 1).

Pristup Internetu postaje sve brži i zbog toga je teško nadzirati promet pa dolazi do raznih propusta koji se iskorištavaju u svrhu upada u sustav. Uvođenje novih tehnologija donosi veliki broj sigurnosnih propusta pa napadači imaju prostora za razvoj alata s kojima će moći neovlašteno ući ili onesposobiti rad ranjivog sustava. To se događa zbog toga što se tehnologije i trendovi jako brzo razvijaju, a proizvođači na tržište puštaju alate koji imaju velike sigurnosne propuste. Jedan od poznatijih primjera je protokol WEP[1] (eng. Wired Equivalent Protocol) kojem su nakon samo dvije godine pronađeni veliki sigurnosni propusti te je napravljen veliki broj alata koji su to iskorištavali. Velikim napretkom Interneta, kao i time što je postao dostupan svakome, mnoge tehnologije za narušavanje sigurnosti se mogu pronaći njegovim jednostavnim pretraživanjem.



Slika 1. Porast broja sigurnosnih incidenata
Izvor:CERT

Porastom broja korisnika povećao se i mrežni promet te ga je jako teško nadzirati. Jedna od prvih tehnika za zaštitu je vatrozid (eng. *firewall*) koji je sklopovsko ili programsko rješenje i radi na principu filtriranja paketa. Moguće je propuštati određene pakete kroz mrežu ili u potpunosti zabraniti promet. Glavni nedostatak vatrozida je taj što je moguće propuštanje ili zabranjivanje prometa samo u ovisnosti o podacima dostupnim na mrežnom i prijenosnom sloju.

Za bolju zaštitu potrebna je neka nova tehnologija koja će moći analizirati sadržaj paketa na aplikacijskom sloju i na osnovu toga odlučiti može li paket proći dalje (do korisnika) ili će ga sustav za zaštitu odbaciti. Nova tehnologija je sustav za otkrivanje upada – IDS (eng. *Intrusion Detection System*) koja analizira pakete tako da ih uspoređuje s njihovim potpisima koji se nalaze u bazi podataka ili provjerava određene nepravilnosti. Postoji i novija tehnologija za sprječavanje upada u sustav – IPS (eng. *Intrusion Prevention System*), i koristi se za sprečavanje napada na mrežu.

[1] Protokol WEP je sigurnosni prokol, specificiran u okviru IEEE Wireless Fidelity (Wi-Fi) standarda 802.11b. Kada se pojavio 1997. godine WEP je trebao bežičnim lokalnim mrežama osigurati određeni stupanj sigurnosti i privatnosti koju pružaju standardne žične lokalne mreže.

Snort je besplatni alat otvorenog koda koji predstavlja mrežni sustav za otkrivanje upada – NIDS (eng. *Network Intrusion Detection System*). Jedna od velikih prednosti je ta da se Snort svakim danom nadograđuje, odnosno svakim otkrivanjem novih načina upada u sustav i/ili sigurnosnih propusta on povećava broj (ili korigira postojeća) pravila. Dodatna prednost je mogućnost prilagodbe alata specifičnim potrebama korisnika.

2. IDS/IPS sustavi

Sustavi za otkrivanje i sprječavanje upada su nove tehnike za zaštitu od zlonamjernih upada u računalni sustav. IDS nadgleda promet u mreži kako bi mogao otkriti neželjene aktivnosti. Dijeli se na:

- mrežni IDS – NIDS, može analizirati mrežni promet i usporediti s datotekom u kojoj se nalazi baza potpisa napada;
- uređaj u računalnoj mreži (eng. *Host*) s IDS-om – HIDS, njegovi zadaci su analizirati zapise sustava i aplikacija koji se nalaze u datotekama te prepoznati netipične aktivnosti koje bi mogle biti označavati upad;
- distribuirani sustav za otkrivanje upada – DIDS, sastoji se od sustava NIDS, HIDS ili oba.

Glavne funkcije sustava za sprječavanje upada su identificiranje zlonamjernih aktivnosti, zapisivanje informacija o tome i pokušavanje blokiranja tih aktivnosti.

2.1. Sustav za otkrivanje upada - IDS

Otkrivanje upada je skup tehnika i metoda koje se koriste za otkrivanje sumnjivih aktivnosti na mreži, odnosno otkrivanje neželjenog mrežnog prometa.

Sustav za otkrivanje upada može biti implementiran programski, sklopovski ili kao kombinacija sklopovlja i programa. On nadgleda promet u mreži kako bi mogao otkriti neželjene aktivnosti i događaje kao što su ilegalni, zlonamjerni promet te promet koji narušava sigurnosnu politiku. Mnogi IDS alati zapisuju otkrivanje takvog događaja u bazu podataka kako bi se kasnije mogli pregledati ili kako bi kombinirali ovaj događaj s drugim podacima. Na temelju vlastite izgrađene baze podataka o napadima mogu se donositi odluke o politici sustava ili o provjeri štete.

Glavni cilj otkrivanja upada je nadgledati mrežu kako bi se mogle otkriti nepravilnosti u ponašanju i zlouporaba. Ovaj koncept postoji skoro dvadeset godina, ali je tek nedavno doživio dramatičan rast popularnosti i konstruiranja u ukupnoj infrastrukturi informacijske sigurnosti.

2.1.1. Povijest IDS sustava

Početak IDS sustava je bio 1980. godine s radom Jamesa Andersona „*Computer Security Threat Monitoring and Surveillance*“ kada je rođena ideja otkrivanja upada. Od tada je zabilježeno nekoliko događaja koji su imali najvažniji značaj u razvoju sustava za otkrivanje upada i formirali ga u današnji oblik.

U radu Jamesa Andersona, napisanog za vladine organizacije, govori se o tehnici koja provjerava zapise te posjeduje značajne informacije o upadima. Informacije mogu biti važne za praćenje zlouporabe ili da se naprave obrasci korisnikovog ponašanja. Nakon izdavanja ovog rada pojavio se koncept za otkrivanje zlouporabe i događaja samog korisnika. Njegov uvid u pregled podataka i njihova važnost doveli su do velikog poboljšanja u provjeravanju podsustava u gotovo svakom operacijskom sustavu. Andersonove pretpostavke su osigurale temelj za buduće sustave za otkrivanje upada i njihov razvoj.

Godine 1983. Institut za istraživanje na Stanfordu - SRI (*eng. Stanford Research Institute*) i dr. Dorothy Denning započeli su rad na vladinom projektu koji je pokrenuo nova zalaganja u razvoju sustava IDS. Njihov zadatak je bio analizirati zapisane tragove iz glavnog državnog računala i stvaranje profila korisnika na temelju njihovih aktivnosti. Godinu dana poslije dr. Denning je pomagala u razvoju prvog modela za otkrivanje uljeza, IDES (eng. *Intrusion*

Detection Expert System), koji je pružio temelje za razvoj IDS tehnologije koja će brzo uslijediti.

U 1984. godini institut SRI je također razvio način za praćenje i analiziranje zapisanih podataka koji sadrže informacije o provjeri autentičnosti korisnika mreže ARPANET[2]. Ubrzo nakon toga SRI je završio ugovor s mornaricom i ostvario prvi funkcionalni sustav IDS. Koristeći svoje istraživanje i razvoj dok je radila za institut SRI, dr. Denning objavljuje presudan rad, koji je otkrio potrebne informacije za komercijalni razvoj sustava IDS. Njezin rad je osnova za budući rad i razvoj sustava IDS koji je brzo uslijedio.

U međuvremenu je bilo i drugih značajnih napredaka na sveučilištu University of California u laboratoriju Davis Lawrence Lovemore Laobratories. Godine 1988. na projektu Haystak napravljena je druga inačica sustava IDS za ratno zrakoplovstvo SAD-a. Ovaj projekt proizveo je IDS alat koji analizira zapise podataka uspoređujući ih s definiranim obrascima.

Naknadna inačica ovog alata nazvana je sustav za distribuirano otkrivanje upada – DIDS (eng. *Distributed Intrusion Detection System*). Sustav DIDS je proširio postojeće rješenje praćenjem uređaja klijenata kao i poslužitelja. Konačno su 1989. godine programeri s projekta Haystack formirali komercijalnu firmu Haystach Labs i proizveli posljednju generaciju ove tehnologije, Stalker. Projekt Haystack spojen s radom dr. Denning i institutom SRI omogućio je napredak razvoja tehnologija za otkrivanje upada.

Na početku devedesetih godina prošlog stoljeća Davis Todd Heberlein predstavio je ideju o mrežnom otkrivanju upada. Godine 1990. Heberlein je bio glavni autor i programer alata NSM (eng. *Network Security Monitora*). NSM je prvi mrežni detektor upada u sustav i raspoređen je na glavna državna postrojenja gdje analiza mrežnog prometa daje goleme količine informacija. Ova nova svijest proizvodi više interesa u području otkivanja upada i dovodi do porasta ulaganja u to tržište. Heberleinov doprinos se proširio na projekt DIDS gdje je zajedno s timom Haystack predstavio prvu ideju hibridnih otkrivanja upada. Rad projekta Haystack i predstavljanje alata NSM je donijelo revoluciju sustava IDS i donijelo ga u komercijalni svijet.

Komercijalni razvoj tehnologija otkrivanja upada počeo je 1990. godine. Haystack Labs je prvi komercijalni prodavač alata IDS. Istovremeno je Kriptološki centar za podršku ratnog zrakoplovstva razvio Automatizirani mjerni sustav sigurnosti – ASIM (eng. *Automated Security Measurement System*) za praćenje mrežnog prometa. ASIM je bio prvo rješenje koje je uključivalo i programska i sklopovska rješenja za mrežno otkrivanje upada i još je uvijek u uporabi po cijelome svijetu. Kao što se često događa, razvojna skupina projekta ASIM formirala je komercijalnu tvrtku 1994. godine koja se zove Wheel Group, a njihov proizvod je alat NetRanger koji je prvi komercijalno održiv. Ipak, komercijalni sustavi za otkrivanje upada polako su se razvijali tijekom tih godina, a jedini pravi procvat dogodio se u drugoj polovici desetljeća.

Tržište za otkrivanje upada počelo je dobivati popularnost i uistinu ostvarivati prihode od 1997. godine. Te godine je lider na tržištu mrežnog osiguranja, ISS (eng. *Internet Security Systems*), razvio sustav za mrežno otkrivanje upada i nazvao ga RealSecure. Godinu dana poslije CISCO je prepoznao važnost ovoga i kupio je Wheel Group, zbog sigurnosnih rješenja koja mogu pružiti svojim korisnicima. Od tada se proširilo tržište komercijalnih sustava IDS.

Trenutno, statistika tržišta pokazuje da su sustavi IDS među najprodavanijima tehnologijama za sigurnost, a taj bi se trend trebao nastaviti. Nadalje, vlada inicijativama također dodaje poticaj za razvoj takvih sustava. Napredak u sustavima IDS u konačnici će postaviti sigurnosnu tehnologiju u novo poprište automatizirane sigurnosne inteligencije. Sustav za otkrivanje upada dijeli su u dvije osnovne kategorije:

- sustav za otkrivanje upada koji se temelji na potpisu,
- sustav za otkrivanje nepravilnosti.

Uljezi imaju svoj potpis, baš kao i računalni virusi, te se on može otkriti pomoću odgovarajućeg programa. Sustav funkcionira tako da se pokuša pronaći paket podataka koji sadrži bilo koji poznati potpis koji je povezan s upadima u sustav ili nepravilnosti koje su povezane s Internet protokolima. Sustav za otkrivanje temelji se na skupu potpisa i pravila

[2] ARPANET (eng. *Advanced Research Projects Agency network*) računalna mreža nastala unutar američkog ministarstva obrane 1969. godine. Osnovna funkcija mu je bila prijenos podataka između vladinih laboratorija. Kasnije je proširena na određene akademske institucije i mreže,

te se mogu pronaći i zapisati sumnjive aktivnosti i stvoriti upozorenja. Sustavi za otkrivanje nepravilnosti rade tako da traže nepravilnosti u paketima. Nepravilnosti se obično nalaze u jednom dijelu naslova paketa. U nekim slučajevima ova metoda daje bolje rezultate od metode koja se temelji na potpisima. Obično otkrivanje upada u sustav „snima“ podatke iz mreže i primjenjuje pravila za tu vrstu podataka ili otkriva nepravilnosti u njemu.

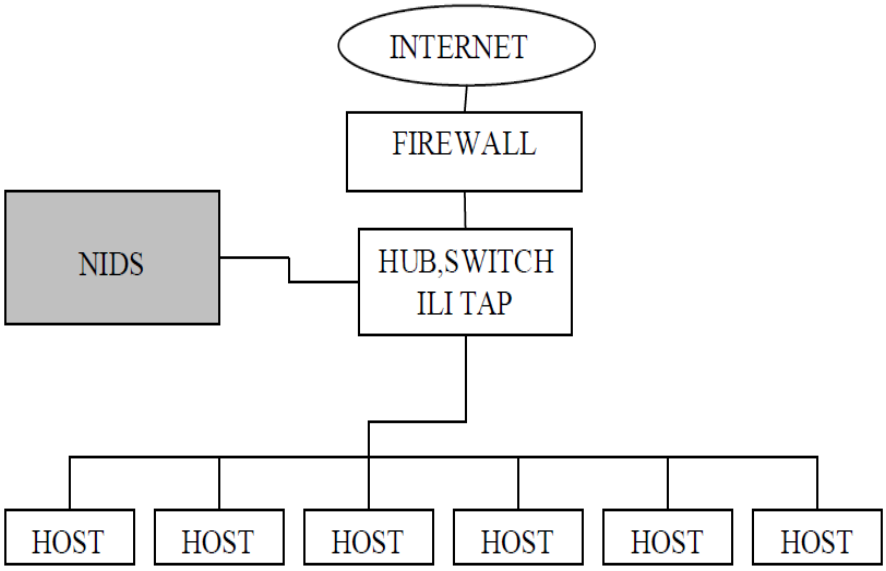
2.1.2. Podjela IDS sustava

IDS sustavi se mogu podijeliti na:

- **Mrežni IDS – NIDS** (*eng. Network Intrusion Detection System*) može analizirati mrežni promet i usporediti ga s datotekom u kojoj se nalazi baza potpisa napada. Mrežni IDS koristi mrežne priključnice koje su postavljenje u tzv. promiscue modu rada (primaju sve mrežne pakete, ne samo one adresirane za to računalo/uređaj) kako bi mogao „uhvatiti“ pakete koji su namijenjeni drugim uređajima u mreži. Zadatak ovog sustava je stvarati upozorenja ako dođe do napada (i to se mora napraviti u stvarnom vremenu) te stvarati zapise za pomoć kod analize napada nakon što se napad već dogodio. Slika 2 prikazuje jedan tipičan primjer rada mrežnog IDS-a (Snort). Vatrozid propušta pakete u računalnu mrežu u kojoj se nalaze uređaji koji su spojeni s mrežnim sustavom IDS.

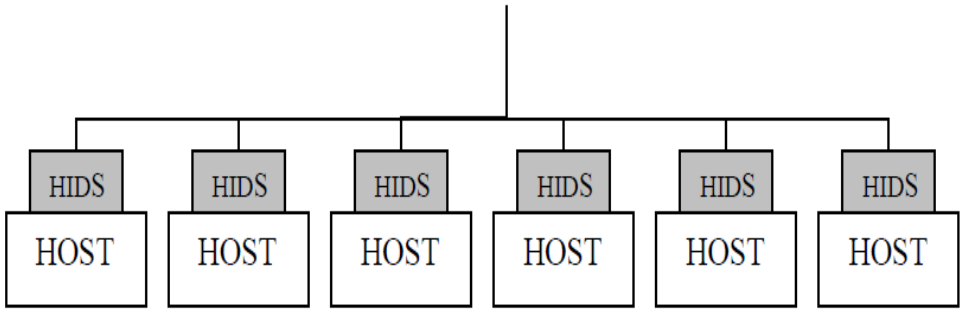
  Postoje dva osnovna tipa mrežnih IDS sustava:

  1. Grubi sustav za analizu - dohvaća pakete podataka iz mreže i uspoređuje ih s potpisima napada koji se nalaze u bazi podataka te provjerava podudarnost. Opisani proces se naziva analiziranje potpisa. Ovakav sustav ne obavlja obradu podataka paketa koje dohvati, već jednostavno pretražuje podatke i traži nizove znakova koji označavaju potencijalni napad. Zbog ograničene brzine rada, ovi sustavi se ne obavezuju da će uspjeti provjeriti sve podatke.
  2. Pseudo inteligentni sustavi isto kao i prethodno opisani sustavi dohvaćaju podatke iz mrežnog prometa, ali oni mogu prepoznati protokole i pravila koja upravljaju njihovim radom. Kad dohvate promet s mreže, pseudo inteligenti sustavi pokušavaju oponašati uređaj u računalnoj mreži i otkrivaju aplikacije koje se zasnivaju na mrežnom protokolu. Ovaj način rada pruža sustav koji smanjuje broj lažno pozitivnih prijava i omogućuje prepoznavanje složenijih napada. Pseudo inteligentni sustavi ne mogu obaviti svoje zadatke ako rade na mreži s velikom propusnosti jer im je potrebno znatno duže vrijeme za analizu prikupljenih podataka.



Slika 2. Mrežni IDS
Izvor: Sistem za detekciju upada – Snort

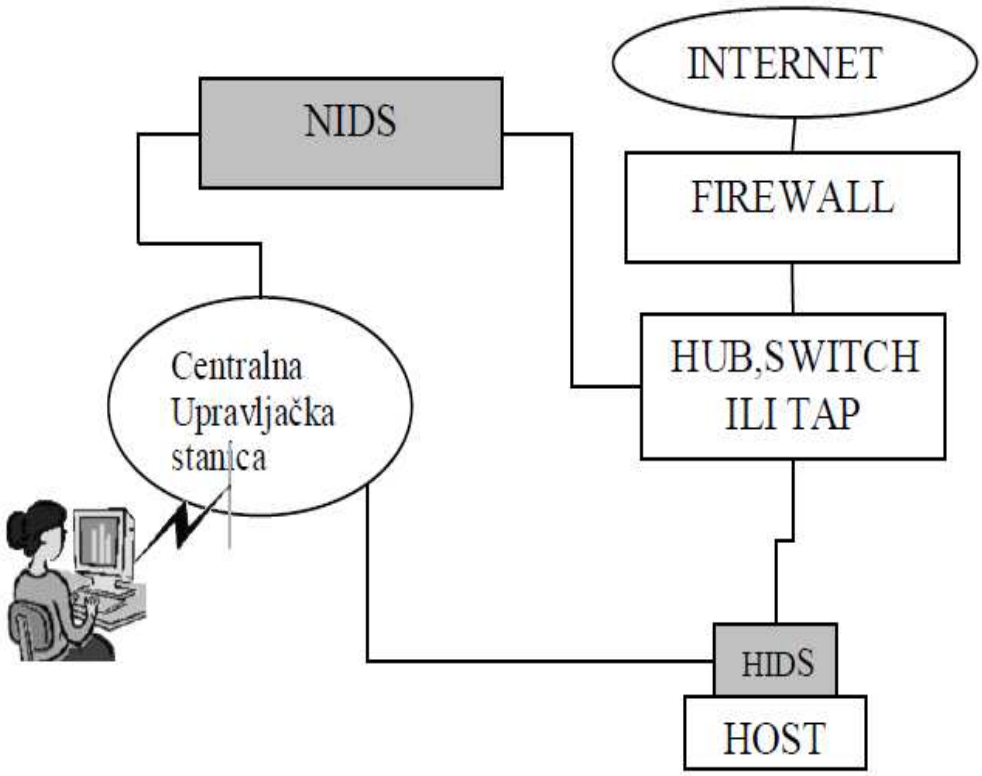
- **Uređaj u računalnoj mreži s IDS-om - HIDS** (eng. *Host Based Intrusion Detection System*) nalazi se instaliran na uređajima u računalnoj mreži (Slika 3). Njegovi zadaci su analizirati zapise sustava i aplikacija koji se nalaze u datotekama te prepoznati netipične aktivnosti koje bi mogle biti označavati upad. On prati promet koji ulazi u mrežu na jednom računalu kako bi mogao detektirati upade i pri tome koristi otkrivanje upada koje je bazirano na nepravilnostima ili potpisima. Ako se primijeti neobično ponašanje na mreži, HIDS analizira zapise sustava. Primjer ovakvog neobičnog događaja je pokušaj višestrukog nepravilnog prijavljivanja u neki sustav. Provjeravaju se i datoteke u sustavu tako da se prati je li bilo promjena u njima i jesu li stvorene ili izbrisane.



Slika 3. Host sustav s IDS-om
Izvor: Sistem za detekciju upada – Snort

- **Distribuirani sustav za otkrivanje upada – DIDS** (eng. *Distributed Intrusion Detection System*) sastoji se od sustava NIDS, HIDS ili oba, a njegov način rada prikazuje Slika 4. DIDS se sastoji od senzora smještenih po cijeloj mreži koji šalju izvještaje u središnju upravljačku jedinicu te središnje upravljačke jedinice koja sadrži bazu potpisa. Ako za to dođe potreba, ti se potpisi šalju do određenog

senzora kako bi on mogao provesti određenu akciju. Između središnje upravljačke jedinice i senzora koristi se kriptirana VPN[3] (eng. *Virtual Private Network*)veza.



Slika 4. Distribuirani sustav za otkrivanje upada
Izvor: Sistem za detekciju upada – Snort

2.2. Sustav za sprječavanje upada – IPS

Sustav za sprječavanje upada – IPS (eng. *Intrusion Prevention Systems*) poznat je kao sustav za otkrivanje i sprječavanje upada – IDPS (*eng. Intrusion Detection and Prevention Systems*) zbog toga što u sebi već sadrži tehnike za otkrivanje upada. IPS je tehnika za sigurnost mreže i ona nadzire mrežu i/ili aktivnosti sustava zbog potrage za zlonamjernim aktivnostima. Glavne funkcije sustava za sprječavanje upada su identificirati zlonamjerne aktivnosti, zapisati informacije o tome i pokušati blokirati/zaustaviti tu aktivnost te ju prijaviti. Sustavi IPS smatraju se proširenjem sustava IDS zbog toga što oba sustava mogu nadzirati promet u mreži i/ili aktivnosti sustava u potrazi za zlonamjernim aktivnostima. Glavna razlika je u tome što IPS za razliku od sustava IDS može aktivno spriječiti/blokirati upade koji su otkriveni. Točnije, IPS može poduzeti određene akcije tako da šalje obavijest, ispušta zlonamjerne pakete, ponovo uspostavlja vezu i/ili blokira promet s IP (eng. *Internet Protocol*) adresama koje su izvele napad. Sustav IPS može ispraviti pogreške cikličke provjere redundancije te „očistiti“ neželjene opcije mrežnog sloja. Većina sustava IPS koristi jednu od tri metode otkrivanja upada:

1. **Otkrivanje upada temeljeno na potpisu** - koristi potpise koji su uzorak za napad te su unaprijed podešeni i definirani. Ova metoda promatra mrežni promet i uspoređuje ga s tim potpisima. Jednom kad se pronađe poklapanje IPS sustav poduzima odgovarajuće mjere.
2. **Otkrivanje upada temeljeno na anomalijama** –metoda koja stvara osnovu, a kasnije sustav povremeno pomoću statističke analize ispituje mrežni promet kako bi se mogli usporediti uzorci s ranije stvorenom osnovicom. IPS poduzima odgovarajuće radnje ako se aktivnosti razlikuju od osnovice.

[3] Virtualna privatna mreža – VPN je tehnologija koja omogućava sigurno povezivanje privatnih mreža u zajedničku (virtualnu) mrežu kroz javnu mrežnu infrastrukturu (Internet).

3. **Otkrivanje upada inteligentnom analizom protokola** - identificira odstupanja od stanja protokola tako da uspoređuje promatrane događaje s unaprijed definiranim profilima općeprihvaćenih definicija.

3. Snort

Snort je alat otvorenog koda za mrežno otkrivanje i sprječavanje upada u sustav - NIDPS (eng. *Netwok Intrusion Detection and Prevention System*). Izvorno ga je izdala firma *Sourcefire* na čelu s Martinom Roeschomp od 1998. godine. Alat ima sposobnost izvođenja analize prometa u stvarnom vremenu i zapisivanja paketa u IP mrežama. Isprva je bio poznat pod nazivom „lagana" tehnologija otkrivanja upada, a razvio se u zrelu IPS tehnologiju punu bogatih osobina i postao skoro pa standardom za otkrivanje i sprječavanje upada u sustav. Ima gotovo 4 milijuna preuzimanja i 400 000 registriranih korisnika. Postao je najrasprostranjenija tehnologija za sprječavanje upada u svijetu.

3.1. Povijest Snort-a

Snort je besplatan alata koji je zbog toga što je pisan kao program otvorenog koda (eng. *Open source*) postao vrlo moćan i neizostavan element u sigurnosti sustava i mreža. Napisao ga je Martin Roesch 1998. godine i tada je imao samo 120 linija programskog koda. On je krenuo u izradu alata koji bi služio kao „slušač" (eng. *Sniffer*) mrežnog prometa. Ime je dobio po engleskoj riječi koja u prijevodu znači šmrkati, njušiti. Ovakav alat mu je bio potreban za provjeru prometa na njegovom modemu i provjeru pogrešaka. Roesch nije bio zadovoljan alatom „*tcpdump"*, koji je na izlazu davao cijele pakete u heksadecimalnom zapisu te su se morali ručno dešifrirati. Zbog toga je napravio alat Snort, u kojem je bilo automatsko dešifriranje i predprocesiranje. Mjesec dana od nastanka alata Martin Roesch podijelio je svoj rad sa zajednicom otvorenog koda (eng. *Open source community*). Nakon vrlo kratkog vremena članovi ove zajednice primijetili su alat Snort i dodane su nove mogućnosti koje su automatizirale praćenje prometa. Martin Roesch napisao je jednostavan jezik za obradu pravila s kojima je bilo moguće raditi prepoznavanje potpisa paketa. Ovim posljednjim dodatkom privučena je velika pažnja mnogobrojnih članova koji su željeli pridonijeti daljnjem razvoju i usavršavanju alata. Početkom 1999. godine izašla je inačica Snort 1.0. koja nije imala predprocesore. U jesen 1999. godine Snort je već imao nekoliko novih tehnologija pa je tako dobio dekoder i modularni sustav za otkrivanje upada. Ova osnova alata Snort ostala je do danas. Sljedeći nedostatak koji se rješavao je taj što se za svaku varijaciju HTTP (eng. *Hypertext Transfer Protocol*) protokola moralo raditi novo pravilo i onda se dodao predprocesor koji je riješio problem. Tokom sljedećih mjeseci razvijali su se modularni sustavi za izlaze i za predprocesore te pravila. Posljednja samostalna inačica alata je Snort 1.7. jer od tada postaje dio alata tvrtke Sourcefire koju je osnovao sam tvorac alata Snort, Martin Roesch. Trenutno su u alat ugrađene komercijalne mogućnosti koje ga uvode u novi svijet velikih poslovnih mreža. Tvrtka Sourcefire je počela proizvoditi sklopovska rješenja za otkrivanje upada u sustav koja u sebi imaju ugrađeni Snort te je napravila i sustav za podršku korisnicima. Iako je ovaj cijeli napredak golem, Snort je i dalje ostao besplatan program kojega se može skinuti s web stranice:

www.snort.org

Preuzimanjem besplatne inačice alata Snort ne dobiva se korisnička podrška i neki napredni moduli za velike poslovne mreže.

Vrlo brzi razvoj Interneta donosi sve veće brzine prijenosa pa tako u jednom vremenskom intervalu prođe jako puno paketa kroz mrežu i teško je te sve pakete podataka nadzirati u stvarnom vremenu. Moglo bi se dogoditi da neki paketi podataka prođu kroz mrežu, a da nisu provjereni. Napredak alata Snort krenuo je od toga da se tijekom nadzora mreže provjeravaju samo ona pravila koja mogu doći u obzir s obzirom na vrstu upada u sustav. Ovakvim načinom

se ne mora prolaziti kroz sva pravila i nepotrebno gubiti vrijeme na ona koja ne mogu doći u obzir jer je novih upada svakim danom sve više, a time i novih pravila.

Snort je izvorno napisan za sustav Linux, a s vremenom je počeo razvoj i za druge operacijske sustave. Danas je dostupan za sljedeće platforme: Linux, OpenBSD, FreeBSD, NetBSD, Solaris (Sparc i i386), HP-UX, AIX, IRIX, MacOS i Windows.

3.2. Snort danas

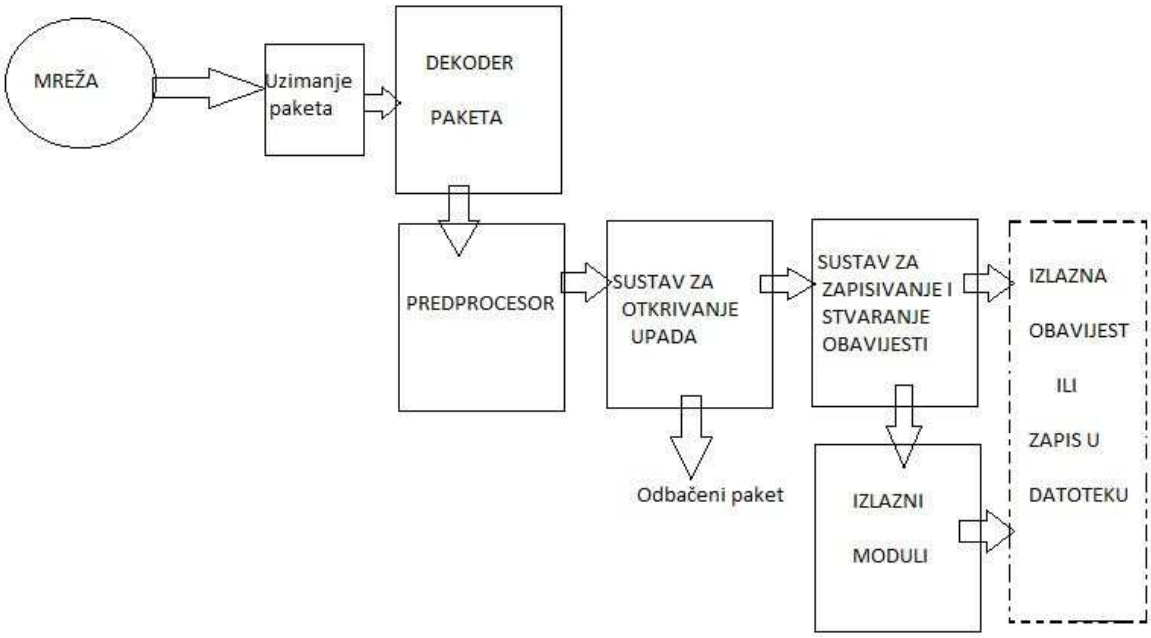
Snort može analizirati mrežni promet na IP mrežama i stvarati zapise u stvarnom vremenu. Radi pomoću pravila, ali postoje i dodaci (eng. *plug-ins*) koji mogu pronaći nepravilnosti u jednom paketu. Pravila pomoću kojih Snort otkriva neovlaštene upade u sustav zapisuju se u tekstualnim datotekama tako da ih korisnici mogu sami prilagođavati (nadopunjavati, brisati) prema svojim potrebama. Pravila se grupiraju u kategorije kako se za vrijeme nadziranja mreže ne bi trebalo prolaziti kroz sva pravila, nego kroz određenu kategoriju. Svaka kategorija spremljena je u svoj zasebni tekstualni dokument.

3.3. Komponente Snort-a

Snort je logički podijeljen na više komponenata koje međusobno surađuju kako bi otkrile napad u mreži. Alat se sastoji od sljedećih komponenata:

- dekoder paketa (eng. *Packet decoder*),
- predprocesori (eng. *Preprocessors*),
- mehanizam otkrivanja (eng. *Detection engine*),
- sustav stvaranja zapisa i obavijesti (eng. *Logging and alerting system*),
- izlazni moduli (eng. *Output modules*).

Slika 5 prikazuje raspored komponenata alata Snort i slijed akcija nad paketom koji se analizira. Nakon preuzimanja paketa iz mreže isti se prosljeđuje dekoderu. Uzimanje paketa obavlja poseban dio programa, a nakon toga se obavlja i samo dešifriranje. Paketi podataka nakon obrade u dekoderu dolaze u predprocesore, koji služe kako bi pakete podataka sortirali ili promijenili prije nego što dođu do mehanizma za otkrivanje. Mehanizam za otkrivanje najvažniji je dio alata Snort i on mora otkriti maliciozne pakete (koje su napadači stvorili). Koristi pravila koja su učitana u interne strukture podataka. Kad dođe do poklapanja paketa s nekim pravilom, obavlja definirane radnje nad tim paketom ili se on jednostavno odbacuje. Radnja koja se može obavljati nad paketom je zapisivanje paketa ili stvaranje obavijesti, a mogu se i obje radnje izvoditi simultano. Ovisno o tome što mehanizam za otkrivanje otkrije, sustav za stvaranje zapisa i obavijesti obavlja zapis podataka u datoteku ili se stvara odgovarajuća obavijest. Izlazni moduli mogu obavljati različite radnje ovisno o tome kako se želi sačuvati izlaz iz sustava stvaranja zapisa i obavijesti. Mogu se zapisivati podaci u datoteke, slati poruke, zapisivati u bazu podataka i slično.



Slika 5. Komponente alata Snort
Izvor: Sistem za detekciju upada – Snort

3.4. Način rada i mogućnosti

Načini rada alata Snort su:

- ***Sniffer*** - najjednostavniji način rada koji se pokreće na početku kako bi se upoznali s alatom. U ovom načinu rada alat Snort prati promet paketa podataka na mreži i obavlja rezultat u komandnoj liniji. Pokretanje ovog načina rada obavlja se naredbom „*snort-v*“, a na zaslonu se dobije ispis prometa paketa u mreži. Naredbe koje se još koriste u ovom načinu su:

  „*snort –w*“ - ispisuje popis mrežnih kartica u mreži koju alat Snort nadzire,

  „*snort-v-i**“ - pokretanje alata Snort, * označava mrežnu karticu s kojom se nadziru paketi

- ***Packet Logger*** - način rada u kojem se ispituju mogućnosti stvaranja zapisa paketa alatom Snort sljedećom naredbom „*snort-dev-l Snortpath\log*“. Bolja mogućnost od ove bila bi zapisati pakete u binarnu datoteku jer se s njima može brže raditi, a naredba za provođenje toga je „snort-b-l Snortpath\log“. Na računalu se mogu pronaći, otvoriti i provjeriti datoteke koje je alat Snort stvorio. Kad se paketi zapišu u binarnu datoteku, mogu se čitati s bilo kojim alatom koji podržava „*tcpdump*“ format.

- **Mrežni IDS** je najsloženiji način rada i za njegovo ispravno funkcioniranje potrebno je postaviti neke opcije: mrežne postavke (eng. *Network Settings*), postavke pravila (eng. *Rules Settings*), postavke izlaza (eng. *Output Settings*) i postavke uključivanja (eng. *Include Settings*).

  Mrežne postavke su mjesto gdje se određuje koji dio IP adrese treba nadzirati. Osnovna postavka konfiguracije datoteke obavlja se naredbom „varHOME-NET any“ pomoću koje alat Snort nadzire cijelu mrežu na koju je priključen.

  U postavkama pravila alatu Snort se pokazuje lokacija gdje se nalazi datoteka koja sadrži pravila (naredba „varRULE_PATH SnortPath\rules“).

  Postavke izlaza služe kako bi se odredilo kako će izlazne informacije biti predstavljene, a to su zapisivanje s naredbom „output logdir“ (mjesto gdje je instaliran Snort, npr. c\snort\log) i obavijest naredbom „output alert_fast:alert.ids“.

3.5. Optimizacija Snort-a

3.5.1. Smanjivanje pogrešnih upozorenja

Alat Snort se može konfigurirati kako bi se smanjio broj pogrešnih upozorenja. Jedan od načina, a koji je ujedno i najjednostavniji, je isključiti nepotrebna pravila. Svaki korisnik može dodavati nova pravila i brisati ona koja su za njega nepotrebna. Uz alat Snort dolazi jako puno pravila, a njihov broj se povećava dodavanjem vlastitih. Najčešće je otprilike samo pola pravila dovoljno za funkcioniranje sustava. Najbolje mjesto gdje bi se trebalo početi s brisanjem pravila je kad se pogleda mapa s rasporedom uređaja u mreži. U velikim mrežama postoji puno mrežnih dijagrama pomoću kojih se može vidjeti gdje se u mreži nalaze određene mrežne tehnologije, sklopovlje, operacijski sustavi i aplikacije.

Najbrži način da se vidi da li postoje neželjeni sustavi ili računala u mreži je skeniranje mreže. To daje prikaz isti onakav kakav ima napadač i može biti vrlo korisno, jer daje na uvid kako napadač namjerava upasti u sustav. Postoje brojni alati za to, a jedan od njih je NMAP[4] (eng. *(Network Mapper*) koji daje realnu sliku kako mrežu vidi napadač.

Još jedan način kako se može dobiti uvid u sustave u mreži i njihove propuste je alat za ispitivanje sigurnosti mreže. Primjer takvog alata je OpenVAS[5] koji može dati listu otvorenih uređaja na mreži i detalje koje aplikacije rade s tim uređajima.

Ako se koristi operacijski sustav Windows 7 u mreži onda se mogu isključiti sva pravila za druge operacijske sustave tako da se ispred njih stavi znak #. Veliko je gubljenje vremena da alat Snort pretražuje sva pravila ako nema potrebe za tim.

3.5.2. Stvaranje novih pravila

Ponekad je potrebno napraviti nova pravila, a situacije koje to zahtijevaju mogu biti neke od sljedećih:

- Primjećivanje nekog nestandardnog ponašanja u mreži kao što može biti prijenos velike količine podataka bez nekog vidljivog razloga. U tom slučaju treba te podatke analizirati, pokupiti uzorke prometa s alatom Snort te, ako je to potrebno, napraviti odgovarajuće pravilo.
- Napravljen je novi oblik napada na mrežu i pravila koja su zapisana u datoteci alata Snort ne sadrže ovaj novi napad te se napad ne može registrirati. Potrebno je stvoriti novo pravilo, barem privremeno dok ne izađe službena inačica koja sadrži ekvivalentno pravilo. Ovaj slučaj nije čest jer se rijetko dogodi da se mora samostalno stvoriti pravilo prije nego je izdana službena inačica.

Alat Snort ima više tipova pravila, a to su:

- pravila protokola (jer alat Snort može otkriti protokol IP u mreži),
- pravila vezana uz uređaje u računalnoj mreži (jer se pretražuje određeni uređaj. U ovim pravilima podaci u paketu nisu važni, nego samo protokol, odnosno broj priključka (eng. *port*). S ovom vrstom pravila treba biti pažljiv jer se može preopteretiti alat Snort kad se koristi s uobičajenim priključkom.
- aplikacijska pravila se koriste zbog toga što se ponekad neobično ponašanje dogodi u aplikaciji ili protokolu i to onda treba otkriti.

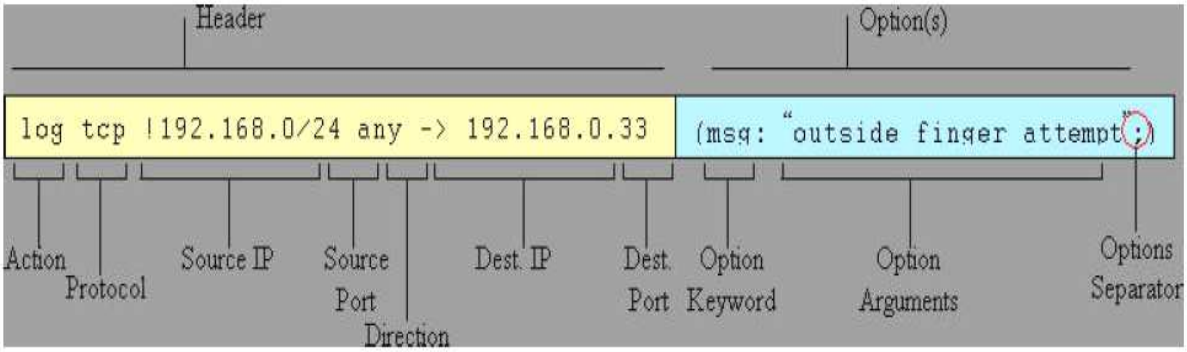
Pravila alata Snort imaju osnovni format koji se može proširivati za neke određene potrebe, a izgleda ovako:

[4] NMAP je besplatni programski paket otvorenog koda za analizu i prikupljanje informacija o računalnim sustavima. Osnovna namjena je pregledavanje TCP i UDP portova te identifikacija operacijskih sustava, iako ima i brojne druge korisne mogućnosti (identifikacija aktivnih računala na računalnoj mreži, lažiranje izvorišne adrese paketa, i sl.). Nmap program objavljen je pod GPL (eng. *General Public License*) licencom i trenutno se smatra najkvalitetnijim i najnaprednijim programom ove namjene. Iako je program primarno razvijen za Linux/Unix operacijske sustave, zbog njegove kvalitete razvijena je i Windows inačica programa.

[5] OpenVAS programski paket danas je jedan od najpopularnijih alata za provjeru sigurnosnih ranjivosti u računalnim sustavima. Besplatan je za vlastitu upotrebu (na vlastitoj mreži i na vlastitom računalu), a inače ga je potrebno kupiti.

```
<snort action> <protocol> <src IP> <src PORT> <direction> <dst
IP> <dst port> (msg:"Tell the user what I'm tracking"; <optional
classtype>;<optional snort ID (sid)>; <optional revision (rev)
number>;)
```

i može se vidjeti na slici u nastavku (Slika 6).



Slika 6. *Zaglavlje i opcije pravila alata Snort*
Izvor: Sistem za detekciju upada – Snort

Ključne riječi iz osnovnog formata pravila znače:

- ***Snort action*** - radnje koje poduzima alat Snort. Ovdje može stajati jedna od tri ključne riječi: *Alert* (obavijest) šalje obavijest na osnovu potpisa, *Log* (zapis) ne stvara se obavijest nego se samo zapisuje ovaj događaj u određenu datoteku te *Pass* (prolaz) govori sustavu za otkrivanje da se propuste oni paketi koji zadovoljavaju uvjete o potpisu.
- ***Protocol*** - u ovom dijelu se označava alatu Snort koji protokol se treba nadzirati. Neki od najčešćih protokola su *TCP (*eng. *Transmission Control Protocol)*, *UDP (*eng. *User Datagram Protocol)* i *ICMP (*eng. *Internet Control Message Protocol)* ili može biti općenito IP protokol.
- ***Source IP*** - skupina IP adresa iz kojih alat Snort može vidjeti od kuda je uspostavljena veza.
- ***Direction*** - pokazuje da li je veza uspostavljena iz izvorne ili odredišne IP adrese.
- ***Destination port*** - odredišni priključak prometa: 80 za HTTP, 21 za FTP (eng. *File Transfer Protocol*) i 23 za *telnet* veze.
- ***Message*** - polje gdje se uz obavijesti mogu ostaviti komentari, a informacija se prikaže na mjestu za obavijesti
- ***Class type*** - oznaka prioriteta. Ako postoji više pravila koji se slažu s dijelom mrežnog prometa, ovaj parametar pomaže da se definira koje će se pravilo koristiti.
- ***Snort Identification (SID) number*** - jedinstveni broj koji je dodijeljen određenom pravilu. Pri stvaranju vlastitog pravila dodjeljuje se broj SID koji je iznad 1 000 000. Ovime se stvara vidljiva razlika između pravila alata Snort i pravila koja je korisnik sam stvorio.
- ***Revision number*** - opcionalni dio, a koristan je ako se stvara više inačica istog pravila te ako se prate promjene pravila za cijeli sustav IDS.

3.6. Primjena Snort-a u organizacijama

U organizacijama je potrebna zaštita od upada zbog zaštite onoga čime se organizacija bavi, privatnih podataka, intelektualnog vlasništva, identiteta zaposlenika i drugih stvari. Ponekad sami zaposlenici sudjeluju u zločinima, a da toga nisu ni svjesni. Korištenjem određenih alata za slušanje ili ilegalno preuzimanje glazbe i filmova na računala na poslu mogu dovesti do ugrožavanja sigurnosti računalnih sustava. Mnogi alati koji služe za dijeljenje datoteka, kao što

su *Kazaa* i *Gnutella*, koriste se za dijeljenje sadržaja koji su zabranjeni (jer se povezuju s drugim računalima u svijetu i tako čine savezne zločine).

Svaka organizacija ima različite razloge za instalaciju alata Snort i različite ciljeve u nadziranju svojih mreža. Multimedijski promet postaje značajan problem u mnogim mrežama gdje korisnici preuzimaju takav sadržaj na svoja računala. Postoji primjer kad je škola za umjetnost i dizajn Ringling uspjela smanjiti mrežni promet za 80% koristeći alat Snort za identifikaciju i sprječavanje P2P (eng. *Peer-to-peer*) aktivnosti. Mnoge škole i fakulteti željeli bi sačuvati svoju propusnost na mreži u svrhu edukacije i isto tako ukinuti narušavanje autorskih prava zbog P2P aktivnosti. Osim potrošnje propusnosti, razvijeni su i novi napadi koji su jedinstveni za multimedijski sadržaj (npr. Trojan.Brisv.A). Broj napada na multimediju se povećava povećavanjem broja medijskih formata i protokola koji su razvijeni i uvedeni.

Škole mogu koristiti Snort kao obrazovni alat i kao alat za otkrivanje upada u sustav. Utah Valley State College ima uključen alat Snort u preddiplomski mrežni program kao dio jeftinog laboratorija koji radi s ovim alatom otvorenog koda. Koledž je razvio laboratorijsku vježbu u kojoj koriste alat Snort kako bi mogli uočiti mjesto upada. Snort može biti integriran i u druge dijelove IT (eng. *Information technology*) nastavnog plana i programa. Jedan dodatak koji bi se mogao uklopiti u nastavni plan i program je alat Barnyard. Radi se o alatu otvorenog koda koji preuzima odgovornost za punjenje baze podataka s izlazom iz alata Snort. Usmjeravanje izlaza alata Snort pruža stvarne prilike za pisanje dodataka i programa za obavještavanje. Veliki broj lažno pozitivnih obavijesti koje stvara alat Snort dovode do toga da se puno podataka mora zapisati u bazu podataka. Također, jedna od obrazovnih mogućnosti za integriranje alata Snort u nastavni plan i program je pisanje izlaznih datoteka.

Za pisanje srednje-složenog izlaznog dodatka trebalo bi programeru s umjerenim vještinama dva do četiri tjedna. Razvijanje izlaznih dodataka je zadatak primjerene veličine za skupinu poslijediplomskih studenata kako bi demonstrirali svoje vještine u pisanju programa i razumijevanju mrežnog otkrivanju upada.

4. Usporedba s dugim IDS/IPS alatima

Snort je najpopularniji i najbolje ocijenjeni alat otvorenog koda koji se koristi kao sustav za mrežno otkrivanje upada. Odlično je oružje u borbi protiv mrežnih upada pa može konkurirati komercijalnim IDS alatima. Navedeni alat je alat otvorenog koda za mrežno otkrivanje i sprječavanje upada u sustav i koristi jezik koji se zasniva na pravilima. Snort kombinira prednosti rada s potpisima i rada s nepravilnostima. Ima i jako dobru korisničku podršku, a to je često glavni razlog za odabir tog alata.

Snorrt se razvija već više od deset godina i postoji velika količina dostupnih dokumenata koji pomažu početnicima u radu s alatom. Danas može raditi na svim najpopularnijim operacijskim sustavima. Licence za sklopovlje i operacijski sustav kompanijama stvaraju veliki trošak te onda traže jeftinije programsko rješenje za mrežnu sigurnost. Rješenje ovog problema može biti alat koji radi na svim operacijskim sustavima i koji je besplatan.

Snort se može rabiti i kao skriveni alat jer se može postaviti tako da bude skriven na mreži, te na taj način bude zaštićen od napadača. Kada je ovako skriven može nastaviti s radom i zapisivati upade ako mreža postane ugrožena. Postavljanjem alata Snort u ovakav mod rada, da mu se iz mreže ne može pristupiti, omogućava da se zapisivanje nastavi čak i tijekom upada. Ovakvim načinom pomaže se u pripremi mreže od budućih napada takve vrste što uvelike povećava njegovu praktičnu vrijednost.

Drugi alat za mrežni IDS je alat Bro, koji je stvorio Vern Paxon u institutu Lawrence Berkley National Labaratory and International Computer Science Institute. Radi se o vrlo naprednom alatu koji se koristi kao mrežni IDS. Bro je alat otvorenog koda, koji je napisan za platformu UNIX i služi za mrežno otkrivanje upada. Mogućnosti navedenog alata slične su onima koje ima alat Snort. Bro nadzire mrežni promet koristeći skup pravila otvorenog koda kako bi mogao tražiti sumnjivi promet. Od kad je alat Bro dobio mogućnost da ga se može samostalno prilagođavati, administratori mogu određivati i provjeravati mogućnosti koje će se postaviti na mrežu. Otkrivanjem novih oblika mrežnih napada, pravila se mogu mijenjati i dodavati tako da imaju sadržane potpise tih novih napada (zbog čega se mreža može bolje nadzirati). Kao i alat Snort, Bro može otkriti nepravilnosti u mrežnom prometu i te nepravilnosti zapisati u za to određene datoteke. Naknadno se zatim istražuju uočene nepravilnosti te formira obavijest (npr. e-mail poruka administratoru sustava).

Platforma alata Bro je sustav otvorenog koda i pokreće se na vrlo stabilnom operacijskom sustavu UNIX. Prema tome, alat Bro nije namijenjen kao rješenje za poduzeća koja ne koriste operacijski sustav UNIX (jer zahtjeva posebna znanja o tom sustavu). Ovo može biti ograničavajući faktor u donošenju odluka o njegovom korištenju u poduzećima. Osnovna prednost alata su velika sposobnost da u rukama stručnjaka postane alat za zaštitu mreža u stvarnom svijetu. Bro može pružiti izvrstan mrežni IDS sustav za poduzeća za jako nisku cijenu. Dodatna prednost mu je i što je prilagođen tako da može koristiti datoteke s potpisima alata Snort.

Bro otkriva upade tako da uspoređuje mrežni promet s prilagodljivim skupom pravila za opis događaja koji se smatraju problematičnima, baš kao i Snort. Ako se s alatom Bro otkrije nekakvo odstupanje, može se izvoditi zapis toga u datoteku, stvarati obavijest operatoru u stvarnom vremenu ili pokrenuti izvođenje određene naredbe. Bro bi mogao biti snažniji alat od Snort-a za mrežni IDS zbog toga što je napravljen tako da je više mrežno orijentiran te može otkriti i prijaviti sve strane aktivnosti na mreži.

Alati Snort i Bro napravljeni su kako bi se u potpunosti integrirali u mrežu. Potpuno iskorištavanje mogućnosti koje nude ova dva alata zavisi o stručnosti operatera (administratora) u organizaicijama koji rade na njima i koji ih uključuju (i naravno kasnije održavaju) u sustav. Oba alata su otvorenog koda pa je kod na raspolaganju stručnjacima za korištenje i daljnji razvoj. U kombinaciji, ova dva alata pružaju drugi sloj zaštite koji je potreban za ispravno štićenje od slabosti sustava.

AIDE (eng. *Advanced Intrusion Detection Envirnonment*) je mrežni IDS alat koji radi na operacijskom sustavu UNIX. Glavni nedostatak ovog alata je manjak dokumentacije za podršku korisnicima. Još uvijek je u razvoju, ali ima potencijala da postane značajan alat. Ovaj alat bi trebao biti prvi izbor ako se traži mrežni IDS za operacijski sustav UNIX.

Shadow IDS je IDS alat otvorenog koda, nastao kao dio projekta koji je pokrenuo CIDER (eng. *Cooperative Intrusion Detection Environment*). Naval Surface Warfare Center je okosnica ovog projekta zajedno s nekoliko drugih vladinih agencija. Ovaj projekt se razvija od 1998. godine te ima dobru dokumentaciju za podršku svojim korisnicima. Shadow koristi biblioteke „tcpdump“ i „libcap“. Njegova prednost u odnosu na alat Snort je ta što omogućava administratoru da postavi senzore kroz cijelu mrežu, tj. može se koristiti kao distribuirani IDS.

Tripwire se zasniva na uređaju u računalnoj mreži s IDS-om, a razvijen je kao projekt sveučilišta Purde University. Dostupan je kao komercijalna inačica ili kao inačica alata otvorenog koda koja je dostupna za preuzimanje na stranici:

www.tripwire.org

Tripwire je jedan od najstarijih alata za IDS, a razvijen je 1992. godine. Napravili su ga dr. Eugene Spafford i Gene Kim u laboratoriju sveučilišta. Može se instalirati na operacijskim sustavima Linux ili FreeBSD.

5. Sustavi za zaobilaženje IDS/IPS sustava

„Anti IDS“ sustavi su sustavi za zaobilaženje sigurnosnih mjera koje postavljaju IDS sustavi. Ideja koja se primjenjuje u ovim sustavima je da se zahtjevi pokušaju što bolje maskirati kako bi mogli zaobići sigurnosne provjere koje provode IDS sustavi. Ovi zahtjevi moraju biti dovoljno regularni tako da ih mrežni poslužitelji prepoznaju i obrade.

Svi mrežni IDS sustavi, bez obzira na tehnike koje upotrebljavaju imaju propuste i svoje slabosti. One su:

1. **Lažno-pozitivna detekcija** (*eng. False Pozitive*) - Lažne obavijesti koje stvara sustav za otkrivanje upada kad otkrije napad koji nije pravi. Ovakva detekcija može biti opasna jer skreće pažnju s pravog napada. Do ovih lažnih obavijesti dolazi kad mrežni promet izgleda slično napadu i kad se rade radnje koje nisu tipične u sustavu.
2. **Lažno-negativna detekcija** (*eng. False Negative*) - Propušteni napad kojeg IDS nije uspio otkriti i zbog toga nije napravio obavijest o tome. Razlozi zbog kojih IDS nije otkrio napad mogu biti: nepostojanje potpisa u bazi podataka, trenutno preopterećenje IDS sustava (zbog čega se neki paketi preskaču) ili uspješno izveden napad na IDS sustav.

3. **Preopterećenje mreže** - Čak i grubi IDS sustavi imaju problema s mrežama koje imaju veliku propusnost.
4. **Smanjivanje učinkovitosti IDS sustava** - Postoje brojne tehnike koje mogu smanjiti učinkovitost IDS sustava.

Tehnike koje smanjuju učinkovitost IDS sustava:

1. **Odbijanje usluge** (*eng. Denial of Service*)

   Tehnike odbijanja usluge su napravljene tako da rade jedno od ove dvije stvari:

   a. Učiniti mrežni IDS sustav neučinkovitim tako da mu zadaju previše posla. Ako se mrežni IDS „bombardira“ s lažnim aktivnostima i pravi napadi mogu proći nezapaženo. Promet može biti usmjeren izravno na mrežni IDS sustav ili na uređaj u mreži koji je se nalazi u izvorišnoj adresi.

   Opaska: Ako je paket usmjeren na uređaj u mreži, mora biti izražen tako da ga on odbije nakon provjere autentičnosti, ali će ga mrežni IDS ipak obraditi. Primjer takvog paketa je nevažeće zaglavlje IP broja za provjeru.

   b. Sprječavanje mrežnog IDS sustava od obavljanja bilo kakvih analiza. Mrežni IDS je ili instaliran na standardni operacijski sustav ili na neke druge uređaje koji rade s prilagođenim operacijskim sustavima namještenim da samo pokrenu aplikaciju. Nijedan sustav nije 100% siguran i moguće ga je srušiti slanjem nevaljanih podataka na TCP/IP stog i tako ga činiti neučinkovitim.

   Do nedavno su opisani problemi bile samo teorijske ranjivosti koje bi potencijalno mogle narušiti sigurnost mreže. Nedavno su napravljeni alati koji mogu koristi obje opisane metode i tako narušiti sigurnost mreže.

2. **Umetanje paketa** (*eng. Insertion*)

   Paket može biti pažljivo konstruiran tako da ga IDS prihvati i obradi, ali ga ignorira ciljani uređaj u mreži.

   a. Kodiranje URL niza (*eng. URL Encoding*) - To je tehnika kada se unutar URL (eng. *Uniform Resource Locator*) niza zamijene znakovi s njihovim heksadecimalnim ekvivalentom. Pseudo inteligentni mrežni IDS neće moći prevariti ovaj način zbog toga što će analizirati zahtjev prije pokretanja. U teoriji sustav s grubom analizom najvjerojatnije će biti osjetljiviji na napad zbog toga što se ne obavlja obrada podataka. Ova tehnika je dobro dokumentirana i ugrađena u mnoge alate i najvjerojatnije neće prevariti IDS sustav.

   b. Obrnuti obilazak (*eng. Reversed Traversal*) - Još jedan način kako bi se pokušao omesti mrežni IDS sustav je tako da se „zakomplicira“ zahtjev. Zahtjev će se i dalje točno rješavati na ciljanom uređaju u merži, ali će mrežni IDS odbaciti paket. Ovaj napad je jako star i IDS najčešće otkriva ove pokušaje napada te pravilno reagira na njih.

   c. Samoreferentni direktoriji (*eng. Self-Referencing Directories*) - Ova tehnika je slična tehnici obrnutog obilaska. Dodavanjem znaka „/.“ u bilo koji zahtjev neće imati utjecanja na značenje zbog toga što to znači da je sadašnja pozicija u trenutnom direktoriju. Npr. /cgi-bin/test-cgi postaje /./cgi-bin/./test.cgi. Ovo je novija tehnika za upad u sustav od tehnike obrnutog obilaska i prošlo je neko vrijeme dok je nisu autori IDS sustava uspjeli otkrili.

   d. Skrivanje parametara (*eng. Parameter Hiding*)

      Zahtjev može sadržavati dodatne informacije (parametre) koji se koriste za izgradnju dinamičnih stranica. Parametri se obično koriste kod zahtjeva za pretraživanjem i preuzimaju sljedeći oblik:

```
/anypage.php?attack=paramhiding&evasion=blackhat&success...
```

      Parametri su navedeni nakon znaka „?“ i pseudo inteligentni IDS će vjerojatno ignorirati sve podatke poslije njega kako bi poboljšao učinkovitost obrade. Znak „?“ može se koristiti kako bi se sakrili važni podaci.

   e. Dugi URL nizovi (eng. *Long URLs*) - Čak i grubi mrežni IDS ima tehnike uzorkovanja koje su napravljene kako bi se poboljšala učinkovitost. Jedna takva tehnika je

ograničiti količinu uzoraka podataka za svaki okvir. Očito će okvir koji premašuje određenu dužinu biti samo dijelom pročitan i analiziran. Ako je paket povećan na ovu duljinu onda će bilo koji opasni sadržaj (izvan okvira) proći bez provjere.

f. Više kosih crta (*eng. Multiple slashes*) - Moguće je poslati zahtjev na web poslužitelj koji zamjenjuje jednostruke kose crte s više kosih crta i web poslužitelju će i dalje ti zahtjevi izgledati valjani. Napad je uspješan ako mrežni IDS sustav ne može uspješno usporediti zahtjev s pravilima. Pseudo inteligentni sustavi ne mogu tako lako biti prevareni, dok su rani grubi IDS sustavi uspjeli biti zavarani. No danas su se i oni razvili i ni njih se više ne može prevariti ovom metodom.

3. **Izbjegavanje** (*eng. Evasion*)

Pažljivo izrađene pakete mogu prihvatiti krajnji sustavi, ali ih mrežni IDS može ignorirati.

a. Sporo skeniranje (*eng. Slow Scans*) - Mrežni IDS nadziranjem učestalosti prometa dane IP adrese otkrije aktivnost skeniranja mreže. Ako alat za skeniranje može umjetno raširiti aktivnost skeniranja na duže vrijeme, mrežni IDS možda neće otkriti ovu aktivnost.

b. Metoda podudaranja (*eng. Method Matching*) - Sasvim je legitimno unutar HTTP RFC[6]-a (eng. *Request for Comment*) poslati alternativnu metodu da bi se dobio odgovor koja je metoda izvorno bila jedina dostupna. Alternativne metode su vrlo korisne napadačima zbog toga što omogućavaju otkrivanje prisutnosti CGI (eng. *Common Gateway Interface*) skripta (čije su ranjivosti dobro poznate) na web poslužitelju.

c. Zahtjev za prijevremeni kraj (*eng. Premature Request Ending*) - Ova tehnika je napravljena kako bi se zavarao pseudo inteligentni mrežni IDS. Metoda pokušava postaviti kraj zahtjeva prije njegovog stvarnog završetka i prije zlonamjernih podataka.

d. Netočno formatiranje HTTP zahtjeva (*eng. HTTP Mis-Formating*) - Iako postoji jasno definirana struktura za bilo koji HTTP zahtjev, mnogi web poslužitelji će prihvatiti zahtjev koji ne odgovara točno određenom obliku. Zahtjev koji odgovara točno formi izgleda na sljedeći način:

```
Method <space> URI <space> HTTP/ Version CRLF CRLF
```

Neki web poslužitelji dopuštaju i druge načine razdvajanja, kao:

```
Method <tab> URI <tab> HTTP/ Version CRLF CRLF
```

Bilo koja IDS analiza koja ovisi o RFC formatu tada neće uspjeti.

e. Sintaksa DOS direktorija (*eng. DOS directory syntax*) - DOS (eng. *Disk Operating System*) je opći naziv za operacijske sustave koji su se počeli pojavljivati krajem 70ih godina 20. stoljeća. DOS je također i abstrakcijski sloj u operacijskim sustavima ili samo dio operacijskog sustava kao u ranim verzijama Windows operacijskog sustava.Kad je Bil Gates napisao DOS odlučio je izbaciti Unix i koristiti znak „\“ za razdvajanje direktorija umjesto „/“. Kao rezultat ovoga, web poslužitelji koji se zasniva na DOS-u morali su prevesti kosu crtu unaprijed u kosu crtu unatrag.

f. Prepoznavanje velikog i malog slova (*eng. Case Sensitivity*) - Kod operacijskog sustava Unix sljedeći izrazi imaju drugačije značenje: Password, PASSWORD, PassWord.. Sustav DOS bi gore navedene nizove znakova interpretirao kao iste dokumente. Prema tome, ako se pošalje zahtjev koji ima sva velika slova, on će se i dalje interpretirati točno. Pseudo inteligentni IDS je još uvijek ranjiv na ovu taktiku.

g. Fragmentacija (*eng. Fragmentation*) - Fragmentacija je metoda pomoću koje protokol TCP/IP rješava problem prelaženja s globalnih mreža različitih širina pojasa

[6] RFC je dokument koji je izdao Internet Engineering Task Force (IETF). Dokumenti obično opisuju metode, ponašanja, istraživanja, ili inovacije primjenjive na Internet i povezana računala. Putem internetske zajednice, inženjeri i računalni znanstvenici mogu objaviti svoj rad u obliku RFC dokumenta, bilo za pregled ili kako bi prezentirali nove koncepte, informacije ili (ponekad) inženjerski humor.

ili sposobnost MTU[7] (eng. *Maximum Transmissible Unit*) jedinice. TCP usmjerena veza dozvoljava različite scenarije za dostavljanje paketa, kao što su paketi koji dolaze izvan slijeda ili duplikat unutar protoka podataka. Oba mrežna IDS sustava ne provode fragmentaciju i zbog toga će svaki paket koji ima zlonamjerni sadržaj i koji je fragmentiran proći nezapaženo.

h. Spajanje sjednica (*eng. Session Splicing*) - Spajanje sjednica je različito od fragmentacije i radi samo slanje HTTP podataka u dijelovima, sa svrhom sprečavanja oba mrežna IDS sustava da uspješno otkriju podudaranje niza znakova. Ponovo sastavljanje je moguće, potencijalno s pseudo inteligentnim IDS-om, ali nije vjerojatno obzirom na velike obrade podataka koje su nastale.

i. Metode za obradu NULL znaka (*eng. NULL Method Processing*) - Ova se tehnika oslanja na činjenici da se u programskom jeziku C koristi NULL znak za označavanje kraja niza znakova. Pseudo inteligentni IDS sustav analizirati će zahtjev i interpretirati ga netočno te ignorirati zlonamjerne podatke.

6. Budućnost

Sustavi za otkrivanje upada u mrežu još se uvijek brzo razvijaju i očekuje se da će se nastaviti nadograđivati novim tehnologijama. Postali su nezamjenjivi dio sigurnosnog sustava uz ostale tehnologije koje pomažu u sprečavanju neželjenih upada u sustav. Postoje malo više od deset godina i napredovali su od primitivnih sustava do mreži nevidljivih distribuiranih sustava koji rade u stvarnom vremenu.

Sve se više razvijaju sustavi za sprječavanje upada i za očekivati je da će se u budućnosti nastaviti još i više razvijati, jer oni mogu otkriti i spriječiti upade u sustav.

Sve više će razvoj biti usmjeren na objedinjavanje više sigurnosnih komponenti unutar jednog programskog paketa kao što je današnji projekt Honeynet. Honeynet je mreža postavljena tako da ima namjerno stvorene propuste i na taj način kada dođe do napada oni se mogu proučavati. U današnje vrijeme postoji sve manja razlika između računalnih i mrežnih sustava pa se može očekivati njihovo objedinjavanje.

Izazov za budućnost je nadziranje kriptiranih kanala i nadzor mreže s IPv6[8].

[7] MTU je maksimalna veličina paketa koja može biti u mreži.

[8] IPv6 ili Internet protokol verzija 6 je relativno nova verzija Internet protokola koja će najvjerojatnije postati sljedeća standardna verzija komunikacijskog protokola na najvećoj računaloj mreži danas - Internetu. Najvažnija karakteristika IPv6 je da koristi 128-bitnu IP adresu, tj. propisana duljina svake IP adrese u ovoj verziji protokola je 128 bita.

7. Zaključak

Sustavi za otkrivanje upada su još uvijek novi sustavi za zaštitu i sigurnost računala i mreža te se očekuje njihov daljnji napredak razvojem Interneta i tehnologije. Pokazalo se da se dobra zaštita sustava ne može postići samo s jednom tehnologijom nego ih se treba više objediniti. Sustavi za otkrivanje upada se stalno nadograđuju i svakodnevno se ugrađuju nova pravila za prepoznavanje upada. Razvija se i sustav za sprječavanje upada te se očekuje njegov veći razvoj u budućnosti zbog toga što, ne samo da može otkriti upade u sustav, nego ih može i spriječiti.

U sigurnosti sustava imaju veliku ulogu operateri koji upravljaju ovim sustavima te je vrlo važno da oni dobro poznaju i razumiju same sustave zaštite te da ih pravilno integriraju u svoju mrežu.

Sustavi za otkrivanje upada našli su veliku primjenu u organizacijama. Mnogim kompanijama je vrlo važno imati dobar sustav zaštite koji će štiti njihovu mrežu od upada i zaštiti njihove privatne podatke te spriječiti krađu intelektualnog vlasništva. Škole i fakulteti uključuju IDS u svoj nastavni program i na nekim fakultetima postoje laboratorijske vježbe i određeni projekti koji obrađuju ove sustave.

Snort je kao besplatni alat otvorenog koda postao vrlo raširen i jedan od najboljih alata za otkrivanje upada u sustav. Njegov razvoj počeo je od ideje da bude „slušač“ mrežnog prometa, a postao je neizostavan element u sigurnosti mreža. Razvijao se brzo zbog toga što je otvorenog koda pa su mnogi programeri pridonijeli svojim idejama. Svi su vidjeli njegov veliki potencijal i njegov razvoj je krenuo velikom brzinom. Prednost alata Snort je i ta što ga se može prilagođavati svojim potrebama. Danas se koristi u brojnim organizacijama, a za njegovo rukovanje potreban je administrator koji ima dosta znanja o IPS/IDS problematici (što često zna biti problem). Na stranicama alata Snort postoji velika količina dokumentacije iz koje se može naučiti kako postaviti Snort u mrežu. Također, postoje i mnogi drugi alati koji imaju u sebi ugrađen alat Snort što ga stavlja u ulogu jednog od najvažnijih alata u sigurnosti informacijskih sustava.

8. Leksikon pojmova

DOS napad - Napad uskraćivanjem usluge

Napad na sigurnost na način da se određeni resurs opterećuje onemogućujući mu normalan rad. http://searchsoftwarequality.techtarget.com/definition/denial-of-service,

Priključnica

Krajnje točke u komunikaciji transportnih protokola - Brojčane vrijednosti temeljem kojih računalo po prihvatu podataka zna koju uslužnu programsku potporu (servise) mora aktivirati te na koji način razmjenjivati podatke na transportnom sloju.

http://searchnetworking.techtarget.com/definition/port-number

TCP (Transmission Control Protocol)

Jedan od dva protokola usmjeravanja koja se koriste u Internetu, uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. TCP se nalazi na transportnom sloju OSI modela. - Jedan od dva protokola usmjeravanja koja se koriste u Internetu. Uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos.

http://www.webopedia.com/TERM/T/TCP.html

IP - IP protokol (Internet Protocol)

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

URL (Uniform Resource Locator)

URL predstavlja adresu određenog resursa na Internetu. Resurs na koji pokazuje URL adresa može biti HTML dokument, slika, datoteka ili bilo koja datoteka koja se nalazi na određenom web poslužitelju.
http://searchnetworking.techtarget.com/definition/URL

HTTP - HTTP protokol (HyperText Transfer Protocol)

Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priljučak 80), čekajući da klijent inicira komunikaciju. - Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priključak 80), čekajući da klijent inicira komunikaciju.
http://hr.wikipedia.org/wiki/HTTP

E-mail - Elektronička pošta

Predstavlja način prijenosa tekstualnih poruka putem komunikacijskih mreža, najčešće Interneta. Usluga omogućava umetanje dodatnih datoteka kao privitke (engl. attachment), a ovisno o poslužitelju usluge može postojati ograničenje na količinu, veličinu i tip datoteka. Elektronička pošta je postala standard za poslovnu komunikaciju, te je zamijenilo standardne dopise (dopisi se i dalje

šalju ali putem elektroničke pošte). Nedugo nakon popularizacije elektronička pošta je postala medij za prijenos raznih zlonamjernih, štetnih programa kao što su crvi i virusi. Uporabom raznih heurističkih metoda prepoznavanja ovo se većinom spriječilo, no i dalje se dnevno razmjenjuju razne (bezopasne) spam ili junk poruke kojima je cilj reklamirati neki proizvod ili uslugu. - Predstavlja način prijenosa tekstualnih poruka putem komunikacijskih mreža, najčešće Interneta. Usluga omogućuje umetanje dodatnih datoteka kao privitke (engl. attachment), a ovisno o poslužitelju usluge može postojati ograničenje na količinu, veličinu i tip datoteka. Elektronička pošta je postala standard za poslovnu komunikaciju, te je zamijenilo standardne dopise (dopisi se i dalje šalju ali putem elektroničke pošte). Nedugo nakon popularizacije elektronička pošta je postala medij za prijenos raznih zlonamjernih, štetnih programa kao što su crvi i virusi. Uporabom raznih heurističkih metoda prepoznavanja ovo se većinom spriječilo, no i dalje se dnevno razmjenjuju razne (bezopasne) spam ili junk poruke kojima je cilj reklamirati neki proizvod ili uslugu. http://www.webopedia.com/TERM/E/e_mail.html

URI (Uniform Resource Identifier)

URI je niz znakova koji se koristi za identifikaciju imena ili nekog drugog resursa na Internetu. URI sintaksa započinje URI shemom (npr. http, ftp, mailto, sip), nakon čega slijedi dvotočka i niz znakova koji ovisi o odabranoj shemi.

http://searchsoa.techtarget.com/definition/URI

Obrnuti inženjering - Reverzni inženjering

Otkrivanje tehnoloških principa i načina rada određenog entiteta. - Proces obrnutog inženjerstva podrazumijeva otkrivanje tehnoloških principa i načina rada određenog uređaja, objekta ili sustava analizom njegove unutrašnje strukture. Često uključuje fizičko otkrivanje unutrašnjih dijelova (npr., mehanički uređaj, elektronička komponente, računalni program) i detaljno analiziranje. Ovisno o primjeni ciljevi mogu biti različiti. Moguće je otkriti određenu poslovnu tajnu rada uređaja, otkrivanje tajnog algoritma koji se implementira i drugo. Prilikom analize programske potpore najčešće se žali zaobići određen dio koda koji implementira određenu sigurnosnu politiku. - Proces reverznog inženjerstva podrazumijeva otkrivanje tehnoloških principa i načina rada određenog uređaja, objekta ili sustava analizom njegove unutrašnje strukture. Često uključuje fizičko otkrivanje unutrašnjih dijelova (npr., mehanički uređaj, elektronička komponente, računalni program) i detaljno analiziranje. Ovisno o primjeni ciljevi mogu biti različiti. Moguće je otkriti određenu poslovnu tajnu rada uređaja, otkrivanje tajnog algoritma koji se implementira i drugo. Prilikom analize programske potpore najčešće se žali zaobići određen dio koda koji implementira određenu sigurnosnu politiku. http://searchcio-midmarket.techtarget.com/definition/reverse-engineering

Razmjerni rast - Mogućnost obrade rastuće količine zadataka

U telekomunikacijama i programskom inženjerstvu, razmjerni rast je sposobnost sustava, mreže ili procesa da obradi rastući količinu zadataka na zadovoljavajući način, odnosno na njegovu sposobnost da bude dovoljno velik da smjesti taj porast.

http://searchdatacenter.techtarget.com/definition/scalability

WWW (eng. World Wide Web)

World Wide Web je jedna od najkorištenijih usluga Interneta koja omogućava dohvaćanje dokumenata. Dokumenti mogu sadržavati tekst, slike i multimedijalne sadržaje, a međusobno su povezani poveznicama (eng. hiperlink).

http://www.webopedia.com/TERM/W/World_Wide_Web.html

Payload - Koristan teret

Na području informacijske sigurnosti, koristan teret označava odsječak koda pomoću kojeg se iskorištava određeni propust računala mete. Na primjer, koristan teret računalnog crva može sadržati modul za širenje vlastite kopije putem globalne mreže Internet. http://searchsecurity.techtarget.com/definition/payload

Pristupnik - Mrežni element

Pristupnik je složeni mrežni element koji stoji na rubu jedne mreže i povezuje ju s drugom mrežom. Pristupnik često ujedno obavlja funkcije posredničkog poslužitelja, vatrozida, DNS poslužitelja i sl.

http://compnetworking.about.com/od/networkdesign/g/network-gateway.htm

IPv6 (Internet Protocol version 6)

IPv6 je nova inačica IP protokola. Trenutna inačica (IPv4) koristi 32 bita za IP adrese, dok IPv6 koristi IP adrese od 128 bita. Time se uvelike povećao adresni prostor što je jedan od glavnih problema IPv4 inačice. IPv6 također unosi bolju podršku za mobilnost i višeodredišne adrese, kao i neke dodatne mogućnosti koje nisu dostupne u trenutnoj inačici.

http://www.networkworld.com/news/2011/082911-ipv6-250196.html

9. Reference

[1] Rafeeq Ur Rehman, Intrusion Detection Systems with Snort, http://ptgmedia.pearsoncmg.com/imprint_downloads/informit/perens/0131407333.pdf

[2] Wikipedia, Snort (Software), http://en.wikipedia.org/wiki/Snort_(software)

[3] Wikipedia, Intrusion detection system evasion techniques, http://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

[4] Nikolina Pavković, Detekcija upada u sustav, http://os2.zemris.fer.hr/ns/2007_pavkovic/IDS.html#_Toc167125895

[5] Paul Innella, The Evolution of Intrusion Detection Systems http://www.symantec.com/connect/articles/evolution-intrusion-detection-systems

[6] Kenan Rizvić, Diplomski rad, Sistem za detekciju upada – Snort, http://elektroni.hes78.com/rile_diplomski/kenan-diplomski-detekcija-upada-snort.pdf

[7] SANS Institute InfoSec Reading Room, Anti-IDS Tools and Tactics, http://www.sans.org/reading_room/whitepapers/detection/anti-ids-tools-tactics_339

[8] Craig Gosselin, Open Source Intrusion Detection and Prevention, http://www.infosecwriters.com/text_resources/pdf/Open_Source_CGosselin.pdf

[9] Sourcefire, Snort, http://www.snort.org/