Sustavi prevencije i detekcije upada u sustav

Draženović, Marijan

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

MARIJAN DRAŽENOVIĆ

SUSTAVI PREVENCIJE I DETEKCIJE UPADA U SUSTAV

Završni rad

Pula, 2020.

Sveučilište Jurja Dobrile u Puli

Fakultet ekonomije i turizma

„Dr. Mijo Mirković“

SUSTAVI PREVENCIJE I DETEKCIJE UPADA U SUSTAV

Završni rad

Ime i prezime studenta: Marijan Draženović

JMBAG: 0303068032, redovan student

Studijski smjer: Poslovna ekonomija, Informatički menadžment

Kolegij: Elektroničko poslovanje

Mentor: prof. dr. sc. Vanja Bevanda

Pula, veljača 2020.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika ekonomije/poslovne ekonomije, smjera _____ ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine

IZJAVA

o korištenju autorskog djela

Ja, _____ dajem odobrenje Sveučilištu Jurja Dobrile

u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom _____ _____ _____ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

Sadržaj

1. UVOD

Informacijske tehnologije se svakog dana sve više i više razvijaju, s tim dolaze i novi, te napredniji alati i tehnologije koje su neophodne za obavljanje većine današnjih gospodarskih djelatnosti. Što se tiče informacijskih tehnologija, one nam pomažu i u svakodnevnom životu i gotovo je nezamislivo funkcionirati bez istih. Pametni telefoni se ne primjenjuju više samo za slanje poruka i pozive, već postoji mnoštvo novih i korisnih stvari koje se svakodnevno primjenjuju, te se s pametnim telefonom može spojiti na razne uređaje putem aplikacija. Tržište je sve veće i na njemu se pojavljuju i novi pametni uređaji kao što su pametni satovi, hladnjaci i ostali aparati koji se vrlo lako povežu sa pametnim telefonom i osobnim računalom, te tako olakšavaju našu svakodnevnicu.

Na tvrtke može imati veliki utjecaj pravilno korištenje informacijskih tehnologija, kako na razvoj tako i na smanjenje vremenskih gubitaka, te zagarantiran efikasniji rad tvrtke. Uporabom informacijskih tehnologija u tvrtki otvaramo vrata i novim radnim mjestima za razvoj i održavanje opreme. Tvrtke koje stječu veliku poslovnu efikasnost uporabom informacijskih tehnologija trebale bi obratiti pažnju na njenu sigurnosnu infrastrukturu.

Što je veća razvijenost tehnologije to je veća i kompleksnost računalnih sustava. U mnogim organizacijama današnjice računalni sustavi se sastoje od velikih broja međusobno povezanih računala. Broj povezanih računala ovisi i kompleksnosti organizacije, a to može iznositi od manje kompleksnih(oko 100 računala), do onih visoko kompleksnih organizacija(oko čak 10000 računala). Računalni sustavi koji se spajaju na Internet, odnosno sva računala koja su obuhvaćena u tom računalnom sustavu mogu postati meta nekog napada na njihovu sigurnost. Samo za računala koja nisu spojena na mrežu može se reći da su više manje sigurna, ali takva računala ne donose neku pretjeranu korist u radu organizacije, te ni ona nikada nisu 100% sigurna. Zato je pitanje o sigurnosti sustava jedna od najvažnijih komponenata u kvalitetnom radu određene tvrtke ili organizacije.

2. RAČUNALNA SIGURNOST

Računalna sigurnost označuje skup mjera i postupaka kojima se osiguravaju podatci pohranjeni u računalima, često dostupni i preko računalne mreže. U današnje doba, kada se najveći dio podataka pohranjuje u računalima, kad što i samo u tom obliku, te kada se velik dio poslovanja, komunikacije i sl. odvija u računalnom okruženju, gubitak ili zloporaba podataka može prouzročiti velike štete. Stoga je računalna sigurnost osobito važna, a obuhvaća zaštitu podataka od gubitka ili oštećenja, kao i od neovlaštena pristupa njima.[1]

2.1. Sigurnost podataka korisnika

Skup mjera i postupaka za osiguravanje određenih podataka:

- **Sigurnosne kopije**
- **Autentifikacija i kriptiranje**
- **Biometrija**
- **Lozinka**
- **PIN**
- **Token**
- **Magnetna kartica**

Sigurnosne kopije (engl. Backup) omogućavaju sigurnost pohranjenih podataka od potpunog gubitka ili oštećenja istih do kojih može doći kvarom računalnog sustava ili nekakve programske greške. Ovakva vrsta zaštite vaših podataka vrši se kopiranjem na nekakvu vanjsku memoriju (tvrdi disk, magnetska vrpca, CD ili DVD), takva memorija mora biti odvojena od one same na kojoj se nalaze izvorni podatci. Kada se napravila sigurnosna kopija podataka, u slučaju gubitka izvornih podataka, mogu se lako nadomjestiti onima koji se nalaze na mjestu pohranjenom sigurnosnom kopijom.

[1] http://www.enciklopedija.hr/Natuknica.aspx?ID=68380

Autentifikacija i kriptiranje je oblik postizanja sigurnosti ili zaštite vlastitih podataka od neželjena pristupa i korištenja istih. Ovim postupkom se prevodi određena informacija u kodirani oblik koja je razumljiva samo korisnicima koji posjeduju ključ za njegovo dekodiranje. Ovakve mjere su obično vrlo bitne kod Internet trgovine i elektroničkog bankarstva (e- bankarstvo ili internetsko bankarstvo), jer korisnik sam obavlja određene bankarske transakcije ili usluge putem pametnih telefona ili računala povezanih internetom. Utvrđivanje autentičnosti ili identiteta osobe koja pristupa podatcima naziva se Autentifikacija. Kako bi se prepoznalo o kojem identitetu osobe je riječ, korisnik unosi svoju lozinku te potvrđuje svoj identitet. Svojim računima moguće je pristupiti PIN-om, jednokratnom lozinkom dobivenom tokenom, magnetskom karticom, pametnom ili čip-karticom, skeniranjem otiska prsta ili šarenice (biometrijom).

Biometrija označava postupak utvrđivanja identiteta neke osobe pomoću njenih karakterističnih tjelesnih osobitosti. Na današnjem tržištu sve više pametnih telefona sa čitačem otiska prsta, otiskom prsta otključava se pametni telefon što čini uređaj sigurnim od neželjenih upada izvana, također postoji očitavanje šarenice, te drugi postupci koji se zajedno nazivaju biometrija.

Lozinka označava kombinaciju brojčano-slovnih znakova koje se sastoje u tajni niz, te korisniku koji je postavio tu lozinku omogućuje pristup njegovom računalnom sustavu i podatcima. Lozinka mora biti što kompleksnija kako bi se zaštitili od pokušaja upada u naš sustav i krađu podataka.

PIN (engl. Personal Identification Number) osobni je identifikacijski broj ili lozinka sačinjena od najčešće četiri znamenke. PIN se koristi za identifikaciju korisnika pri aktiviranju mobitela, ali i uporabi gotovinskih kartica.

Token služi kao uređaj za generiranje jednokratnih osobnih lozinka, kao identifikacija korisnika pri pristupu sustavima elektroničkoga (internetskoga) ili telefonskoga bankarstva.

Magnetska kartica služi pohrani manje količine podataka i identifikaciji korisnika, a na njoj se nalazi magnetna vrpca. To su kreditne ili gotovinske kartice, te zdravstvene iskaznice. Očitavanje podataka vrši se provlačenjem kartice kroz čitač. Sve je više pametnih ili čip-kartica sa integriranim sklopom, tako da u skorije vrijeme bi se trebale magnetske kartice zamijeniti njima.

2.2. Aspekti sigurnosti informacija

Napadači se koriste raznim softverima, kako bi si olakšali akciju nedopuštenog upada u računalni sustav. Napadači na računalne sustave mogu koristiti upad u sustav za ilegalne ili čak destruktivne svrhe. Neki napadi se događaju iz čiste radoznalosti napadača koliko se snalazi u takvom pothvatu, odnosno kako bih testirao vlastitu vještinu upada u neki računalni sustav i da li je uopće sposoban za takav čin. Većini napadača je glavni motiv znatiželja, potreba za učenjem ili čak zabava, ali uvijek postoje i oni napadači koji su motivirani osvetom, nepovjerenjem u druge osobe, načinom stvaranja profita, želje za pobjedom neke osobe i takvih se napadača treba paziti i znati se zaštititi od neželjenih napada koje mogu rezultirati krađom osobnih podataka, novca ili nečeg vrijednog.

Da bi se efikasno procijenile sigurnosne potrebe neke organizacije i da bi se odabrali različiti sigurnosni proizvodi, pravila, procedure i rješenja, rukovodiocu u tvrtki koji je zadužen za sigurnost potreban je sistematičan način definiranja zahtjeva u pogledu sigurnosti i kategorizacije pristupa koji omogućavaju da se ti zahtjevi zadovolje.[2]

Tri su aspekta sigurnosti informacija:

- **napad na sigurnost (security attack) –** ovakva radnja se označava kao akcija koja se dogodila, a ima za posljedicu ugrožavanje sigurnosti određenih vrsta informacija
- **sigurnosni mehanizam (safety mechanism) –** ovakav mehanizam je karakterističan po tome što bi trebao otkriti i ukloniti neželjeni napad na sustav ili ako je već došlo do napada trebao bi oporaviti sustav.
- **sigurnosna usluga (security service) –** pomoću ovakve usluge se povećava sigurnost sistema koji služi za prijenos i obradu određenih podataka. Ovakav tip usluge koristi jedan ili ako je potrebno više sigurnosnih mehanizama.

[2] http://web.studenti.math.pmf.unizg.hr/~ksekuli/napadi.htm

2.3. Kategorije napada na sigurnost

Napadi su hakerske akcije koje su usmjerene na ugrožavanje sigurnosti informacija, računalnih sustava i mreža.[3] U današnje vrijeme sve je više zlonamjernih radnji napadača koji pokušavaju pridobiti što više vaših informacija koje mogu koristiti za vlastitu potrebu. Riječ „haker“ se spominje po prvi put 1963. u MIT novinarskom članku studenata u kojem se opisuju hakerski napadi na telefonski sustav. Postoje različite vrste napada, ali se oni generalno mogu podijeliti u četiri osnovne kategorije.

Četiri osnovne kategorije napada na sigurnost:

- **Presijecanje ili prekidanje (interruption)**
- **presretanje (interception)**
- **izmjena (modification)**
- **proizvodnja (fabrication)**

Normalan tok informacija predstavlja tok kada jedna strana koja je izvor informacija bez ikakvih poteškoća šalje informacije do njenog odredišta.

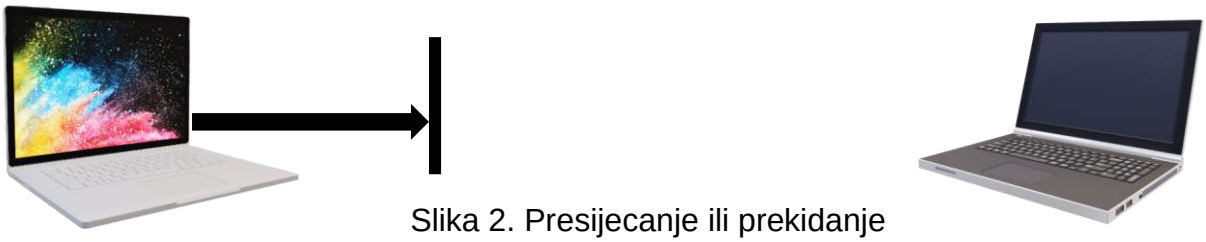
Izvor informacija Odredište informacija

Slika 1. Normalan tok informacija

Izvor: izradio autor

Presijecanje ili prekidanje (interruption) predstavlja napad na raspoloživost. Presijecanjem se prekida tok informacija, tj. onemogućava se pružanje neke usluge ili funkcioniranje nekog sustava. Ovakav napad je aktivan. [4]

[3] http://web.studenti.math.pmf.unizg.hr/~ksekuli/napadi.htm
[4] http://web.studenti.math.pmf.unizg.hr/~ksekuli/napadi.htm

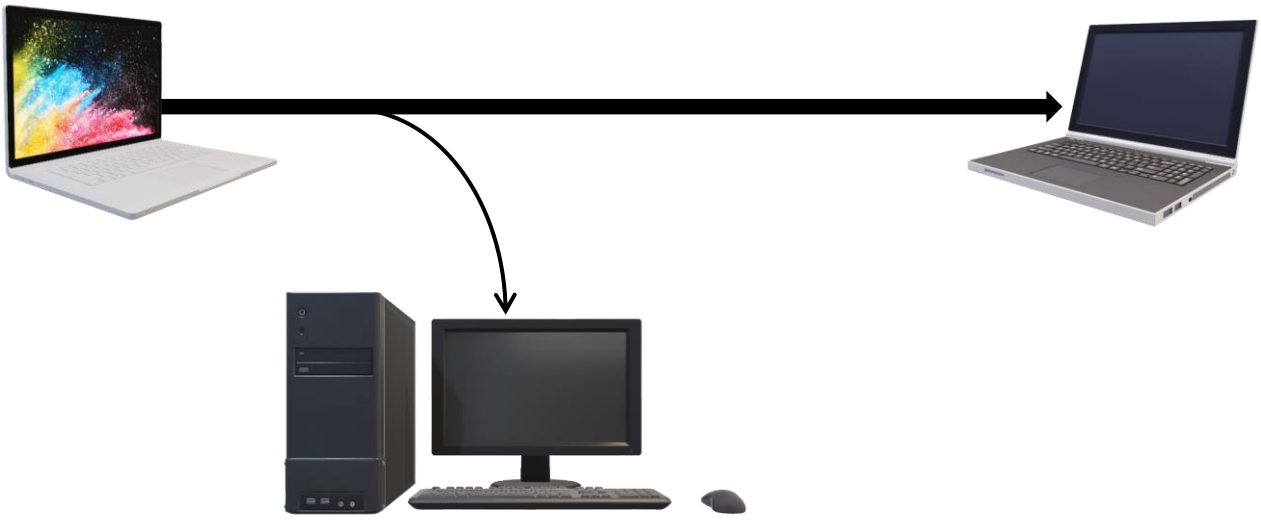


Slika 2. Presijecanje ili prekidanje

Izvor: izradio autor

Upadanjem napadača u mrežu može dovesti do nekoliko zlonamjernih radnji. Tada se korisniku koji je napadnut najčešće događaju situacije blokiranja prometa koje može dovesti do gubitka željenih podataka, nevidljivost sistemskih informacija kako ne bi otkrili počinitelja, te namjerno nagomilavanje mrežnog prometa na računalo ili mrežu koje rezultira gašenjem sustava ili cijele mreže.

Presretanje (interception) predstavlja napad na povjerljivost (confidentiality). Presretanje može biti u praksi provedeno kao prisluškivanje prometa, nadziranje njegovog intenziteta, uvid u osjetljive informacije ili slično. Kao pasivni napad, teško se otkriva jer ne mijenja podatke, ne utječe na unutrašnje funkcioniranje sustava. Ovakav tip napada ponekad je pripremna faza za neku drugu vrstu napada.[5]



Napadač

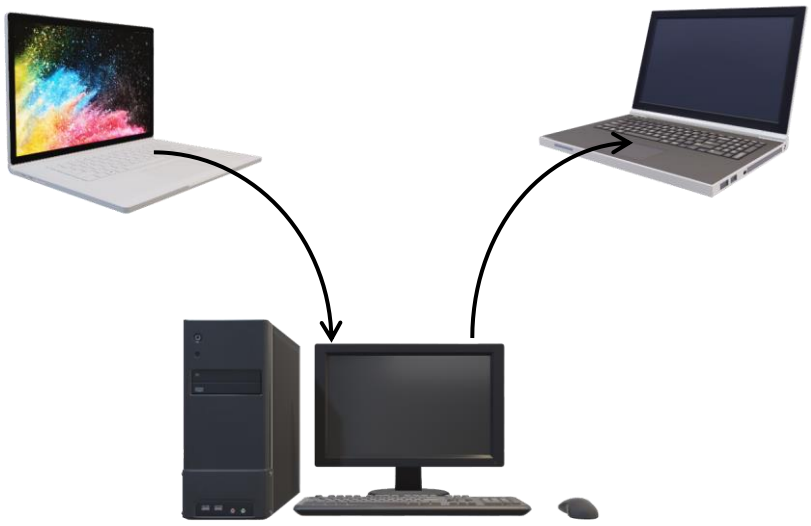
Slika 3. Presretanje

Izvor: izradio autor

[5] http://web.studenti.math.pmf.unizg.hr/~ksekuli/napadi.htm

Napadi koji se događaju presretanjem podataka su napadi na dvije osobe koje razmjenjuju određene podatke ili informacije, a treća osoba (napadač) pokušava što više prikupiti podataka koje može kasnije iskoristiti. Napadač se ubacuje u komunikaciju između te dvije osobe i informacije preusmjerava na svoje računalo.

Izmjena (modification) predstavlja napad na integritet (integrity). Po svojoj prirodi, to je aktivan napad. Ukoliko djeluje na prijenosnom putu, može se, na primjer, dogoditi napad „čovjek u sredini“ (man in the middle). Napad se može obaviti i unutar nekog računalnog sustava. U tom slučaju radi se o izmjeni podataka, pristupnih prava, načina funkcioniranja programa ili sustava i slično. Iako mijenja podatke i sustav, često ostaje neprimijećen izvjesno vrijeme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.[6]



Slika 4. Izmjena

Izvor: izradio autor

Napad izmjene podataka događa se kada dvije osobe razmjenjuju određene podatke i informacije, a treća osoba (napadač) vrši izmjenu tih podataka kako bi ugrozio onoga tko prima podatke. Ovakav tip napada se događa nakon presretanja informacija, napadač mijenja informacije bez ikakvog znanja korisnika o tome. Ovakva vrsta napada je vrlo štetna za korisnika ukoliko je primio netočne informacije, te može biti štetna za poslovanje poduzeća. Ovakvi napadi se najčešće događaju u slučaju novčanih transakcija.

[6] http://web.studenti.math.pmf.unizg.hr/~ksekuli/napadi.htm

Proizvodnja (fabrication), predstavlja napad na autentičnost (authenticity). Napadač izvodi ovakav aktivni napad tako što generira lažne podatke, lažni promet ili izdaje neovlaštene komande. Veoma često se koristi i lažno predstavljanje korisnika, usluge, poslužiteljskog računala, Web strane ili nekog drugog dijela sustava.[7]

Slika 5. Proizvodnja

Izvor: izradio autor

Napad proizvodnjom na korisnika može imati ozbiljne posljedice. Posljedica takvog napada može biti krađa i zlonamjerno iskorištavanje korisničkih podataka. Proizvodnjom lažnih podataka i umetanjem istih u korisnikovu mrežu može mu nanijeti veliku štetu i može dovesti do krađe podataka od napadača.

[7] http://web.studenti.math.pmf.unizg.hr/~ksekuli/napadi.htm

3. INFEKCIJA ZLONAMJERNIM PROGRAMOM

Zlonamjerni softver (eng. malware) općenito se može definirati kao prijetnja za računala i njihovu sigurnost koju ugrožavaju računalni špijuni (eng. spyware), virusi, računalni crvi, trojanci i botovi. To su vrlo rasprostranjeni programi koji mogu evidentirati sve što ukucate na računalu, napraviti snimke ekrana, ukrasti dokumente i datoteke i otvoriti skrivena zadnja vrata do vašeg računala. Ove informacije se zatim šalju osobi koja je instalirala neki od navedenih programa.[8]

Gledajući kroz povijest, virusi i crvi kao zlonamjerni programi nisu predstavljali preveliku prijetnju, takvi programi više su se koristili u svrhu stvaranja smetnje u normalnom radu sustava. Takvi zlonamjerni programi danas su jako napredovali, sve više napadača koristi taj tip zlonamjernih programa u svrhu upada u neki računalni sustav, jer su takvi programi sve više sofisticiraniji i teže ih je otkriti prilikom upada u sustav.

Napadači koji koriste današnje zlonamjerne programe su u mogućnosti putem istih vrlo lako upasti u nečiji sustav, a služe za još nekoliko zlonamjernih radnji. Napadači putem programa pokušavaju pretraživati vrijedne podatke korisnika kao što su PII (Personally Identifiable Information) i lozinke, a program služi za pregled komunikacije, pruža udaljeni pristup ili kontrolu nekog sustava, te automatski napad na druge sustave.

Zlonamjerni programi koje koriste napadači mogu im pružiti sposobnost „odvraćanja“ odnosno smanjuje se mogućnost identifikacije napadača, te se s time smanjuje i mogućnost kaznenog gonjenja. Pod sposobnosti „odvraćanja“ se podrazumijeva pokretanje zlonamjernih programa anonimnim metodama kao što je nesigurna, otvorena javna bežična pristupna točka. Kada zlonamjerni program dobije pristup određenom cilju, može pokrenuti upravljanje na sustavu putem distribuirane naredbe, te upravljačkim sustavom kao što su Internet Relay Chat, web-stranice, dinamički poslužitelj domena(DNS), te potpuno novi mehanizmi. Kontrola i upravljanje mrežom može sakriti identitet i lokaciju napadača, te omogućuje upravljanje mnogim kompromitiranim sustavima u svrhu poboljšanja cilja napadača. Broj kontroliranih strojeva može biti ogroman, primjer je „storm worm infection“ koja se kretala između 1

[8] https://plaviured.hr/vodici/malware-sto-je-i-kako-se-zastititi/

i 10 miliona kompromitiranih sustava. Takve velike zbirke kompromitiranih sustava naziva se „bot-net“

3.1. Klasificiranje zlonamjernih programa

Postoji više oblika zlonamjernih programa, ali se mogu klasificirati prema funkciji i određenoj metodi.

Klasificiranje zlonamjernih programa:

- **Virus**: Računalni virus je računalni program koji svojom reprodukcijom može zaraziti računala tako da bez dopuštenja ili znanja korisnika kopira samog sebe u datotečni sustav ili memoriju ciljanog računalnog sustava.[9] Sama riječ „virus“ svakodnevno se povezuje sa zlonamjernim programima kao što su programi za oglašavanje (adware) i špijunski programi (spyware). Najčešće širenje virusa se događa putem interneta, tako da se s jednog računala šire na ostala. Virusi se prenose putem e-maila, nalaze se u raznim privitcima i porukama, a mogu se širiti i vanjskim hard diskom, te putem CDa, DVDa ili USBa. Na poslužitelju koji je dostupan većim brojem korisnika, a na kojem se nalaze zaražene datoteke, mogućnost širenja virusa se povećava. Takva računala mogu biti dio „botneta“. Botnet je infrastruktura u kojoj se nalazi velik broj zaraženih računala, a imaju uspostavljenu vezu s komandnim i kontrolnim poslužiteljem. Kod takvih situacija napadač ima ovlasti nad računalima korisnika. Veliki broj virusa ima jednu od mogućih najštetnijih funkcija, a to je praćenje tipkovnice. Pomoću praćenja aktivnosti tipkovnice napadač može doznati korisnikove privatne podatke, lozinke, pa čak i brojeve kartica.

Prema načinu djelovanja virusi se dijele na dvije vrste:

- Rezidentni virusi: oni se prilikom njihovog izvršenja učitaju u memoriju i njihov kod ostaje u memoriji cijelo vrijeme rada računala. Rezidentni virusi koriste tehnike TSR („terminate and stay resident“) i manipulaciju memorijskim blokovima (MBC) kako bi se cijelo vrijeme zadržali u memoriji računala.

[9] https://www.cert.hr/virusi/

Zlonamjerni kod rezidentnih virusa koristi mehanizme operativnog sustava za svoje aktiviranje, na primjer, pokretanje koda pri svakom pokretanju bilo koje aplikacije. Tako se postiže efekt zaraze i nad novo instaliranim aplikacijama.[10]

- Nerezidentni virusi: oni se nalaze u RAM-u samo u vrijeme njihovog izvršenja, odnosno od njihovog pokretanja pa do završetka rada. Njihovo širenje se svodi na princip da dio njihovog koda pronalazi datoteke koje mogu biti zaražene na sustavu (na primjer .exe, .doc i slično), a drugi dio koda kopira virusni kod u pronađenu datoteku.[11]

Osnovne vrste virusa:

- boot sektor virusi: zlonamjerni kod se izvršava prilikom samog pokretanja računala
- programski virusi: aktivacija ovakvih virusa zahtjeva izvršenje zaražene datoteke
- makro virusi: napisani su višim programskim jezikom i imaju mogućnost kopiranja i brisanja samih sebe, kao i mijenjanja dokumenata

Tehnike prikrivanja koje virusi koriste:

„Potpis virusa“ je uzorak sastavljen od niza okteta koji je dio zlonamjernog koda određenog virusa ili skupine virusa. Ako antivirusni program pronađe takav uzorak u datoteci, obavještava korisnika da je datoteka inficirana. U svrhu težeg otkrivanja, virusi koriste razne tehnike pomoću kojih mijenjaju virusne potpise, dok se njihov kod modificira prilikom svake infekcije što znatno otežava antivirusnom alatu detektiranje virusa.[12]

- “Stealth” tehnike: skriveni je virus koji blokira zahtjeve koje šalje antivirusni alat, te šalje operativnom sustavu da nema nikakvih opasnosti.
- Polimorfni kod: kada dolazi do repliciranja virusa, on mijenja aktualni kod i dužinu, te ga je gotovo nemoguće otkriti.
- Metamorfni kod: ovakva vrsta koda je većinom složene prirode, promjenom koda ne gubi na funkcionalnosti

[10] https://www.cert.hr/virusi/
[11] https://www.cert.hr/virusi/
[12] https://www.cert.hr/virusi/

- **Crv (worm)**: Računalni su crvi programi koji sami sebe umnožavaju i šire se putem računalne mreže. Za razliku od računalnih virusa, crvi ne zahtijevaju postojanje domaćinske datoteke za svoj rad. Oni su samostalni programi koji se u većini slučajeva šire bez interakcije korisnika. Iako je moguće pronaći računalne crve koji nisu štetni, većina sigurnosnih stručnjaka sve crve smatra zlonamjernim i nepoželjnim programima.[13] Ovakva vrsta zlonamjernih programa se širi putem interneta s jednog računala na drugo. Crvi su tako programirani da u što kraćem vremenu zaraze velik broj računala, a dijele se na dva načina na koja se šire:
    - bez interakcije korisnika: ukoliko računalo ima sigurnosne nedostatke, to bi moglo dovesti do širenja zaraze. Takvi nedostatci se nalaze u operacijskom sustavu ili aplikacijama korisnika. Ukoliko postoji sigurnosni nedostatak, crv će instalirati svoju kopiju na korisnikovo računalo, a nakon instalacije potražit će druge žrtve preko mreže kako bi ih mogao zaraziti.
    - putem socijalnog inženjeringa: ovakav način širenja zaraze se obavlja putem e-mail poruke ili poruke na društvenim mrežama. U takvim porukama su skrivene datoteke crva i na korisniku je samo da je preuzme i pokrene, te dolazi do zaraze i širenja.

- **Backdoor**: stražnjim vratima (backdoor) naziva se maliciozni računalni program koji se koristi da bi napadaču omogućio neautorizirani daljinski pristup kompromitiranom PC sistemu iskorištavanjem ranjivosti njegove sigurnosti. Stražnja vrata (backdoor) rade u pozadini sistema i skrivena su od korisnika.[14] Ovakva vrsta zlonamjernih programa je vrlo opasna za korisnike, jer se ovakav program teško otkrije, a i daje mogućnost napadaču da obavlja bilo kakve operacije i procese na korisnikovu računalu. Backdoor nudi napadaču mogućnost špijuniranja korisnika, upravljanja korisnikovim datotekama, a moguće je i na korisnikovo računalo instalirati neke od zlonamjernih programa, kako bi napadač mogao napasti i druge korisnike putem korisnikova računala. Neki od ovakvih programa imaju i posebne mogućnosti kao što su bilježenje koje su tipke pritisnute

[13] https://www.cert.hr/crvi/
[14] http://virusi.hr/backdoors-straznja-vrata/

od strane korisnika (keystroke logging), snimke zaslona, infekcije i šifriranje datoteka. Stražnja vrata (backdoors) su trojanski konji, virusi, keyloggeri, spyware i alati za daljinsku administraciju, ali spadaju u posebnu kategoriju, jer su datoteke i funkcije složenije i mogu nanijeti još veću štetu od navedenih zlonamjernih programa. Ovakva vrsta programa se ne može širiti i ne može zaraziti korisnikovo računalo bez njegovog znanja. Program mora instalirati korisnik, a postoji četiri načina na koja ovakva vrsta zlonamjernog programa ulazi u računalni sustav.

Četiri glavna načina ulaska stražnjih vrata (backdoor) u sustav:

- Napadači postavljaju imena virusa koja neće izazvati nikakvu sumnju korisnika da ih ne otvori i instalira, te na taj način ulaze u sustav.
- Kako bi se napadačima olakšao pristup sustavu, oni uz pomoć virusa, trojanskog konja, ili programa spyware pokušavaju podvaliti korisniku virus backdoor. Napadači zatim ulaze u sustav neprimijećeno od strane korisnika, te utječu na svakog tko koristi kompromitirano računalo.
- U određenim aplikacijama već postoji integrirani virus stražnjih vrata. Napadač samo mora kontaktirati napadnuto računalo putem već instaliranog programa kako bi došao do pristupa računalnog sustava ili preuzimanja kontrole nad nekim programom.
- Napadači mogu ubaciti zlonamjerni program stražnjih vrata u sustav ukoliko ima određenih sigurnosnih mana u programu. Korisnik neće primijetiti nikakvu prijetnju jer na njegovom računalu neće dolaziti prozori upozorenja ili čarobnjaka za instalaciju.

- **Trojanski konj**: trojanski konj oblik je zlonamjernog softvera koji se lažno predstavlja kao neki koristan softver kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju. Termin je, zbog analogije, preuzet iz grčke mitologije. Trojanski konj može izmijeniti operacijski sustav na zaraženom računalu kako bi on prikazivao oglase (pop-up prozori) u svrhu ostvarivanja novčane koristi od strane napadača. Opasniji je slučaj kada trojanski konj omogući napadaču potpunu kontrolu nad zaraženim računalom.[15]

[15] https://www.cert.hr/trojanski_konji/

Trojanski konj omogućuje napadaču sljedeće aktivnosti na korisnikovom računalu:

- može ga koristiti kao dio „botnet“ mreže
- može se domoći privatnih informacija korisnika
- može instalirati određene zlonamjerne programe
- može slati i primati datoteke
- može pratiti i bilježiti pritisnute tipke
- može koristiti memoriju
- može srušiti sustav zaraženog računala

Načini na koji se trojanski konj širi:

- Trojanski konj se može širiti preuzimanjem zaraženog programa
- e-mail privitcima
- zlonamjernim stranicama
- ako postoji ranjivost programa

- **User-level rootkit**: rootkitovi koji spadaju u ovu kategoriju funkcionirat će na razini korisnika u operativnom sustavu. Rootkiti pomažu napadačima da zadrže kontrolu nad metom pružajući backdoor kanal, User Mode Rootkit nastoji promijeniti važne aplikacije na korisničkoj razini, skrivajući se tako i osiguravajući backdoor pristup. Korisnički modovi rootkita su promjenjivi i za Linux i za Windows.[16]

- **Kernel-level rootkit**: „kernel“ je jezgra operacijskog sustava, a korijeni razine jezgre stvaraju se dodavanjem dodatnog koda ili zamjenom dijelova jezgre operativnog sustava, s modificiranim kodom putem upravljačkih programa uređaja (u sustavu Windows) ili prijenosnim modulima kernel (Linux). Rootkiti razine kernela mogu ozbiljno utjecati na stabilnost sustava ako kôd kompleta sadrži pogreške. Kernel rootkite je teško otkriti jer imaju iste privilegije operativnog sustava te stoga mogu presresti ili subvertirati operacije operativnog sustava.[17]

[16] https://resources.infosecinstitute.com/rootkits-user-mode-kernel-mode-part-1/#gref
[17] http://www.omnisecu.com/security/rootkits.php

4. NAPADAČI I NJIHOVI MOTIVI

Napadači na računalne sustave pokušavaju na određene načine i uz pomoć određenih alata pristupiti žrtvinu računalnom sustavu. Širok je spektar motiva koji takve osobe pokreće, a nekakve radnje napadača na sustave ne moraju nužno biti štetne za korisnike, već mogu biti i korisne za obranu od zlonamjernih napadača. Nisu svi napadači na sustave zlonamjerni, neki od njih programiraju različite alate i programe za zaštitu korisnika na internetu, ali najčešći su napadači koji smišljaju na koji način se domoći žrtvina novca ili osobnih podataka. U početku većina napadača imala je potrebu za naukom i nekakvim izazovima, ali s napretkom tehnologije otvorili su se i mnogi načini za zaradu putem ilegalnih radnji, što je uzrokovalo sastavljanjem kriminalnih grupa koje su zadužene za napade u svrhu zarade.

Vrste napadača, te motivi koji ih pokreću:

- **Script Kiddy (početnici)**: pod takvim napadačima se podrazumijevaju oni koji imaju nizak stupanj znanja o napadima na sustave, te programiranju zlonamjernog koda. Ovakva vrsta napadača rijetko koristi svoj napisani kod, već uzimaju tuđi, napisan od strane nekog drugog i pomoću lakih alata za korištenje organiziraju napade.
    - **Green Hat napadači:** su početnici, ali imaju veliku radoznalost što ih motivira da prošire svoja znanja i vještine.
    - **Blue Hat napadači:** tip napadača koji su osvetoljubivi. Cilj im je osveta prema svojim neprijateljima, također su početnici.
- **Joy Rider:** ovakva vrsta napadača je karakteristična za one osobe koje imaju značajne vještine u otkrivanju ranjivosti računalnog sustava, ali rijetko imaju zle namjere kada istražuju radi zadovoljstva. Iako takvi napadači nisu zlonamjerni oni mogu biti glavni izvor ometanja rada, te troškova za administratore sustava koji moraju reagirati na upad u sustav, pogotovo ako njihov komprimirani sustav sadrži neke od osjetljivih podataka kao što su PII(Personaly Identifisble Information).
- **Mercenary**: to su osobe zaposlene u određenoj tvrtki ili osobe koje rade za partnersku tvrtku. Ovakav tip napadača su najčešće nezadovoljni radnici koje su angažirali konkurenti, u svrhu krađe poslovnih tajni i podataka tvrtke. Ovakva

vrsta napadača može biti i otpušteni radnik koji je prije odlaska iz tvrtke uspio doći do povjerljivih informacija tvrtke.

- **Nation-State Backed (državno sponzorirani napadači)**: ovakav tip napadača je angažirala određena država kako bi za nju napadač radio aktivnosti kao što su aktivno špijuniranje, socijalno inženjerstvo, upadi u sustave i širenje zlonamjernih programa. Države najčešće angažiraju ovakve osobe kako bi se domogle određenih povjerljivih informacija, te kako bi pomoću iskorištavanja takvih informacija stekle prednost u odnosu na druge države.

5. TEHNOLOGIJE ZA OTKRIVANJE I SPRJEČAVANJE UPADA U SUSTAV

Povećavanjem razvoja tehnologije i interneta potiče se i razvoj zlonamjernih programa, te je sve veći broj napada na sigurnost računalnih sustava. Kako raste broj upada u računalne sustave tako i raste broj tehnika i alata za računalnu sigurnost. Sve brži pristup internetu onemogućuje nadziranje prometa, zbog čega dolazi do sve većeg broja sigurnosnih propusta. Uvođenjem novijih tehnologija također se povećava broj sigurnosnih propusta, što uvelike olakšava napadačima razvoj alata za upadanje u ranjivi računalni sustav. Tehnologije se brzo razvijaju, te proizvođači na tržište plasiraju razne alate koji imaju sigurnosne propuste. Vatrozid (firewall) jedna je od prvih programskih rješenja, a tehnika rada joj se temelji na filtriranju paketa. Mogućnost firewalla je propuštanje paketa ili potpuna zabrana prometa putem interneta. Kako firewall ima ogroman nedostatak, a to je propuštanje ili zabrana prometa samo podatcima dostupnim na mrežnom i prijenosnom sloju, korisnicima su potrebne neke bolje tehnologije. Tehnologija IDS (Intrusion Detection System) omogućuje analizu paketa na aplikacijskom sloju, koja može utvrditi analizom sadržaja da li takva vrsta paketa može doći do korisnika ili je se treba ukloniti ukoliko je zlonamjerna. Postoji i novija tehnologija za sprječavanje upada u sustav, a to je IPS (Intrusion Prevention System) i služi blokiranju zlonamjerne radnje na mrežu. Jedan od najkorištenijih mrežnih sustava za otkrivanje i sprječavanje upada u sustav je „Snort“. Ovakav alat je dostupan svim korisnicima besplatno, a spada pod NIDS (Network Intrusion Detection System). Glavna prednost ovog alata je ta što se svakodnevno nadograđuje, tako da svakim otkrivanjem novih tehnika upada u sustav, povećava se i broj njegovih pravila.

5.1. Sustav za otkrivanje zlonamjernih aktivnosti u sustavu (IDS)

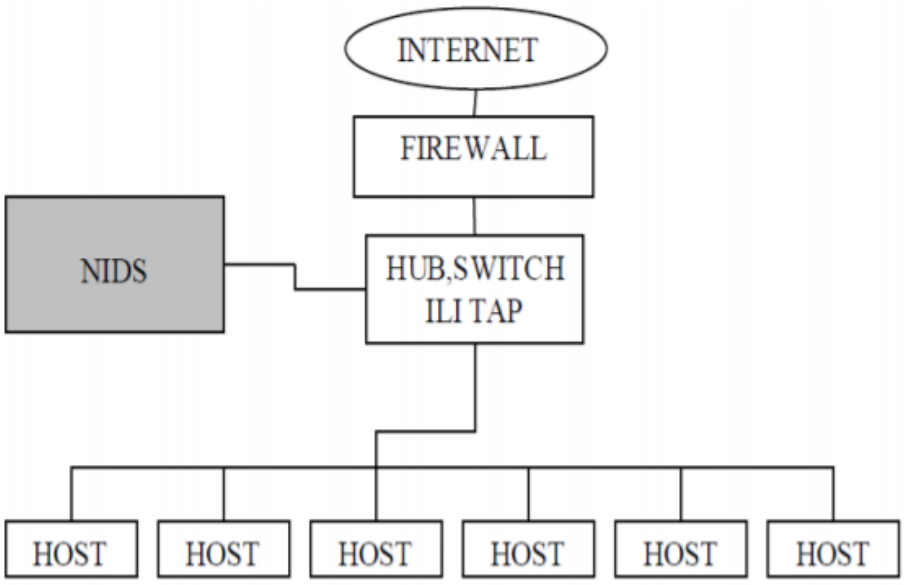
Detekcija upada IDS alatima može se okarakterizirati kao skup tehnika i metoda, u svrhu razotkrivanja neželjenih radnji na internetu odnosno mreži. Ovakvi alati nam služe i otkrivanju zlonamjernih mrežnih prometa. IDS sustav može se provesti kao program ili sklop ili kombinacija programa i sklopovlja. Alati za otkrivanje zlonamjernih aktivnosti nadgledaju mrežni promet, kako bi se detektirale zle namjere napadača koji

postavljaju ilegalni promet koji bi mogao narušiti rad sustava. Nakon detekcije zlonamjernih radnji u sustavu, IDS sustavi bilježe takve događaje u bazu podataka, u svrhu kasnijeg pregleda ili kombinacije zapisa s drugim podatcima u sustavu. Baza podataka ovakvih alata služi korisniku provjeru štete u računalnom sustavu, te donošenju odluke o politici sustava. Kako je najveća opasnost zabilježena putem mreže, cilj otkrivanja upada je promatranje ponašanja i nepravilnosti, te zlouporaba mreže. Ovakve vrste alata počele su se sve više koristiti što ojačava ukupnu infrastrukturu sigurnosti na mreži.

5.1.1.Podjela IDS sustava

IDS sustavi se dijele na tri različita sustava, a to su NIDS,DIDS i HIDS.

- **NIDS** (Network Intrusion Detection System): mrežni je IDS sustav koji ima sposobnost analiziranja mrežnog prometa radi usporedbe baze u datoteci u kojoj je zabilježen potpis napada. NIDS se koristi tehnikom „njuškanja paketa“ odnosno prima sve pakete koji su poslani putem mreže, a ne samo adresirane za korisnikovo računalo, tako da može pohvatati i one mrežne pakete koji nisu namijenjeni korisnikovu računalu već nekim drugim računalima na mreži. Ovakva vrsta sustava ima zadaću javljati korisniku da je došlo do zlonamjerne radnje, te ga upozoriti i zabilježiti taj događaj putem analize napada.



Slika 6. NIDS

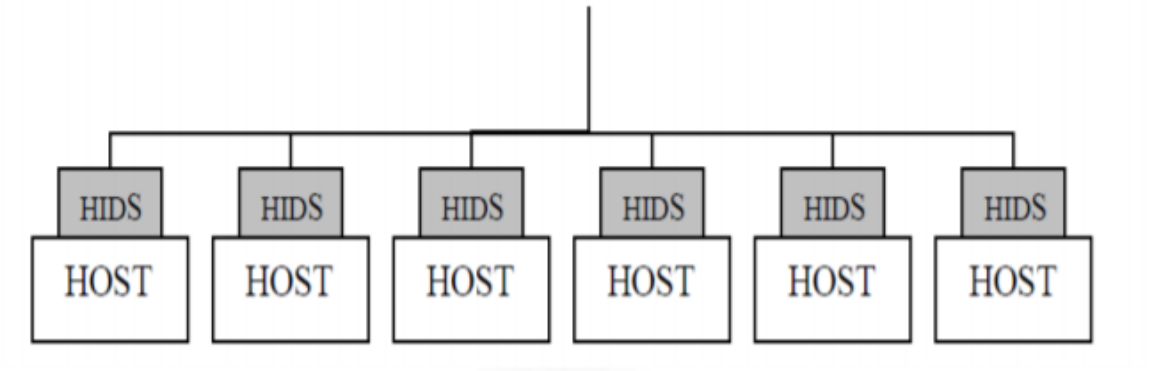
Izvor: Sistem za detekciju upada - Snort

Prikaz slike nam opisuje rad NIDS sustava (Snort). Firewall pušta određene pakete u mrežu u kojem su povezana računala sa NIDS sustavom. NIDS sustavi se mogu podijeliti na dva tipa ustava, a to su:

- **Grubi sustav za analizu:** prikuplja mrežne pakete, zatim te pakete uspoređuje sa potpisima napada koji su zapisani u bazi podataka i na kraju provjerava njihovu podudarnost. Takav se proces se naziva analizom potpisa. Iako ovi sustavi provjere podataka nisu stopostotni, uspijevaju zahvatiti velik broj podataka za provjeru putem pretrage znakovnog niza koji označava napad.

- **Pseudo inteligentni sustav:** također radi na principu prikupljanja mrežnih paketa, ali imaju mogućnost prepoznavanja protokola i pravila upravljanja njihovim radom. Kada prikupe određene mrežne pakete, rade na principu oponašanja uređaja u računalnoj mreži, zatim otkrivaju programe koji su zasnovani na mrežnom protokolu. Način rada pseudo inteligentnog sustava omogućava prepoznavanje kompleksnijih napada.

- **HIDS** (Host Based Intrusion Detection System): ovakav sustav za otkrivanje nesvakodnevnih radnji koje upućuju na upad nalazi se na uređajima u računalnoj mreži na kojima je instaliran.

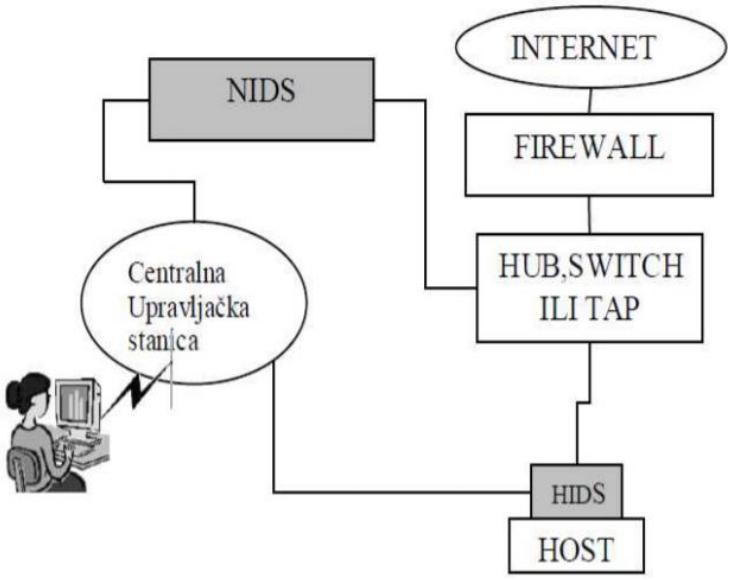


Slika 7. HIDS

Izvor: Sistem za detekciju upada - Snort

Zadatak HIDS sustava je analiza bilježaka sustava i programa koji se nalaze u datotekama, kako bi mogao otkriti nesvakodnevne radnje koje upućuju na potencijalni upad u sustav. Primjer neobičnog ponašanja na mreži je višestruki pokušaj nepravilne prijave u neki sustav. HIDS sustav isto tako provjerava i datoteke koje se nalaze u sustavu, te prati da li je došlo do nekakvih promjena u njima ili jesu li stvorene ili možda izbrisane.

- **DIDS** (Distribuited Intrusion Detection System): je distribuirani sustav koji služi za otkrivanje upada, a sastoji se od NIDS sustava, HIDS sustava ili kombinacije oba.



Slika 8. DIDS

Izvor: Sistem za detekciju upada - Snort

DIDS sustav radi na principu senzora koji su smješteni po cijeloj računalnoj mreži, a svrha ovakvog sustava je slanje izvještaja analize u središnju upravljačku jedinicu, te središnju upravljačku jedinicu koja ima bazu potpisa. Ako sustav primijeti nepravilnosti, potpisi se šalju do senzora kako bi mogao djelovati i poduzeti određene akcije. Slanje potpisa se vrši putem VPN3 (Virtual Private Network) veza između središnje upravljačke jedinice i senzora.

5.2. Sustav za sprječavanje upada u sustav (IPS)

IPS (Intrusion Prevention Systems) služi kao sustav detekcije i prevencije upada, drugim riječima to je IDPS sustav (Intrusion Detection and Prevention Systems) jer u sebi sadrži tehnike i otkrivanja i uklanjanja mogućnosti upada u sustav. IPS sustav koristi tehnike za sigurnost mreže, te nadzire mrežu i aktivnosti sustava kako bi otkrio zlonamjerne radnje. IPS se može okarakterizirati kao proširena verzija IDSa jer je kod takvog sustava glavna funkcija identifikacija zlonamjernih radnji, bilježenje podataka o zlonamjernoj radnji, prijava takvih radnji, te najbitnije sprječavanje takvih radnji. Glavna razlika između ta dva sustava je u tome što IPS ima mogućnost uklanjanja neželjenih aktivnosti u sustavu. IPS sustav radi na principu da kada otkrije opasnost odmah šalje obavijest o toj radnji, zatim propušta zlonamjerne pakete, te ponovno pokušava uspostaviti vezu ili sprječava prolaz prometa sa IP (Internet Protocol) adresa koje su zaslužne za zlonamjerne aktivnosti. Sustav sprječavanja upada ima mogućnost ispravljanja pogreške cikličke provjere redundancije i uklanjanja neželjenih opcija na mrežnom sloju.

Postoje tri metode koje IPS koristi za detekciju upada u sustav:

- Otkrivanje upada temeljeno na potpisu – ova metoda se koristi potpisima koji su potvrda da se napad dogodio i uspoređuje ih sa mrežnim prometom. Kada se dogodi poklapanje sustav pokreće određene aktivnosti.
- Otkrivanje upada temeljeno na anomalijama – metoda radi na način da stvara osnovu koju sustav uspoređuje sa mrežnim prometom. Ova metoda putem statističke analize provjerava promet, a ako se aktivnosti u mrežnom prometu razlikuju od osnove, sustav pokreće određena rješenja.
- Otkrivanje upada inteligentnom analizom protokola – ova metoda otkriva upade putem identifikacije odstupanja od protokola. Usporedbom nepravilnih događaja sa već definiranim profilima općeprihvaćenih definicija.

5.2.1. Podjela IPS sustava

IPS se dijeli na dvije vrste sustava, a to su: NIPS i HIPS

- **NIPS** (Neural Information Processing Systems): sustav NIPS sastoji se od IDS-a i firewalla, te se koristi dodatnim metodama za prevenciju zlonamjernih radnji. NIPS sustav sadrži dvije mrežne kartice kao i firewalla, prva mrežna kartica je zadužena za unutarnju mrežu, a druga za vanjsku. Dolaskom paketa na mrežno sučelje, sustav IPS pokreće analizu da bi utvrdio da li se radi o zlonamjernom paketu. Ako je sustav utvrdio zlonamjernost analiziranog paketa, on se odbacuje i ne dozvoljava mu se protok na drugu mrežu. Ukoliko postoji nekih drugih paketa povezanih sa onim zlonamjernim, također se odbacuju.

  U NIPS-u zadržane su sve funkcije firewalla. Jedna od glavnih funkcija je „stateful inspection“, a služi praćenju i analizi segmenata veze koji prođu kroz firewall. Na osnovu tog praćenja sustav donosi odluke o odbacivanju određenih paketa. NIPS sustav sadrži dubinsku analizu sadržaja paketa (Deep Packet Inspection) koje je njegovo dodatno poboljšanje. U ovu analizu spadaju određene metode pomoću kojih NIPS sustav pretražuje sadržaje paketa ili međusobno povezanih paketa, kako bi sustav uspio otkriti zlonamjerni kod ili programsku anomaliju. Sadržaj paketa koji je povezan sa IP baziranim programima se pretražuje, bilježi i na kraju filtrira. Ovakav tip analize NIPS sustavu daje mogućnost detektiranja skrivenih napada koji su usmjereni na Web, e-mail i DNS poslužitelje.

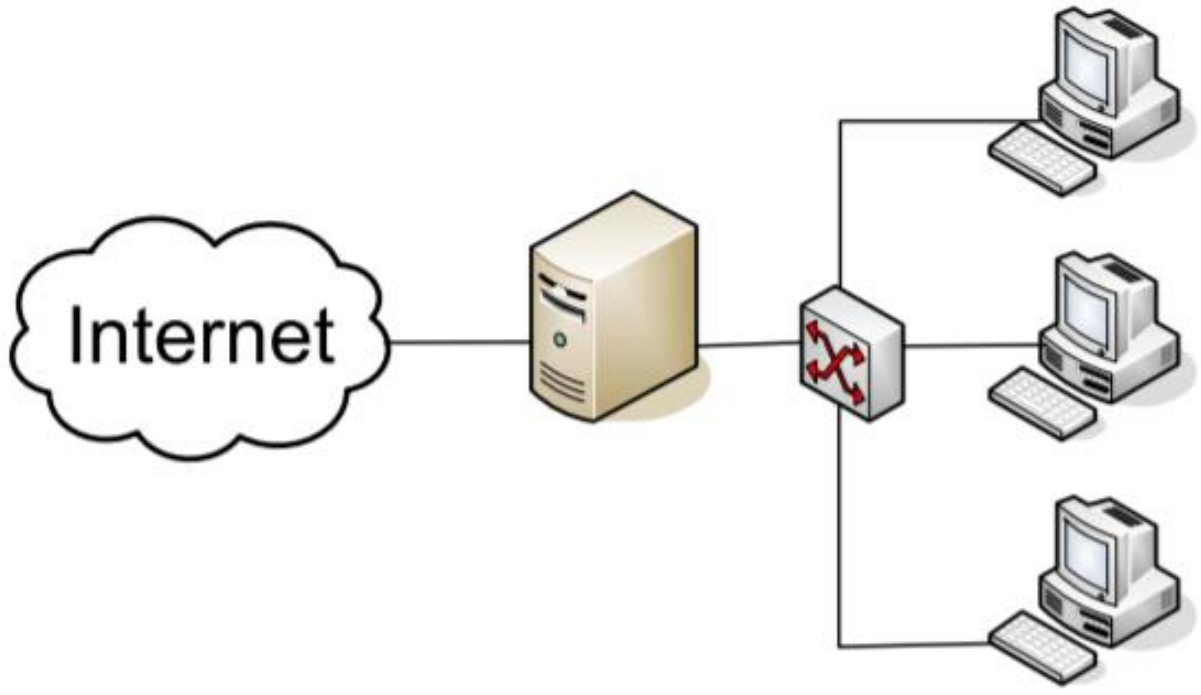
- **HIPS** (High Integrity Protection Systems): ovakav sustav se koristi općenito za osiguran pristup korisnika svim mrežnim resursima koji su im potrebni, jer HIPS sustav radi na principu blokiranja zlonamjernih radnji na mreži. HIPS se instalira kao program računala koja mogu biti klijent/poslužitelj i koristi se kao agent obrade sigurnosnih politika koje se nalaze u konfiguraciji datoteke smještenim u središnjem upravljačkom poslužitelju. Središnji nam upravljački sustav pomaže pri održavanju i kontroli sustava.

Koncepti rada HIPS sustava:

- HIPS sustav kreira bazu uobičajenih aktivnosti koja se događaju na računalu. Sustav odmah nakon instalacije počinje promatrati računalne procese, kako bih mogao raspoznati da li se radi o nepoželjnim radnjama koje treba ukloniti ili o svakodnevnim aktivnostima na računalu. U nekim slučajevima moguće je ukloniti i zaraženo računalo iz mreže, kako ne bi došlo do širenja zaraze.
- HIPS sustav radi u kombinaciji sa firewallom, što osigurava zaštitu na mrežnoj razini, kako bi se izbjegli neželjeni paketi i kako bi im se zabranio prolazak do aplikacije. Sustav ima mogućnost izvođenja pretrage neželjenih kombinacija asemblerskih naredbi koje mogu uzrokovati kopiranje spremnika (buffer overflow).

5.2.1. Primjer korištenja NIPS i HIPS sustava

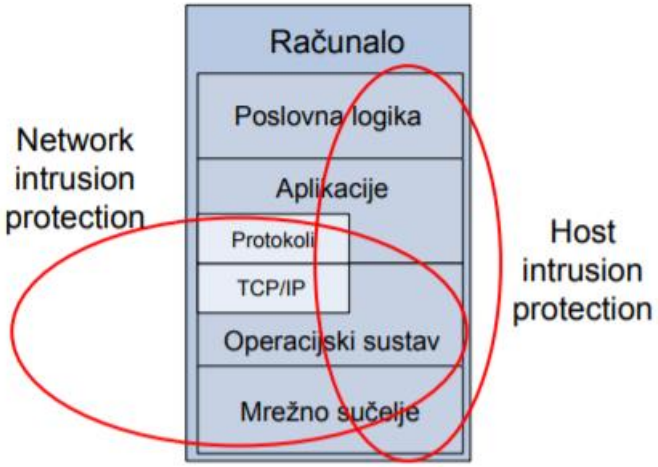
Da bi IPS sustav bio što učinkovitiji on se kombinira sa alatom za sigurnost mreže i sustavom prevencije neželjenih radnji na računalima klijenata. Kombinacija uporabe NIPS i HIPS alata prikazan je na slici 5.4. Vidi se da NIPS i HIPS alati u kombinaciji prikupljaju i analiziraju informacije o procesima računala, te prepoznaju neželjene radnje.



Slika 9. Zaštita mrežnih podataka primjenom NIPS i HIPS alata

Izvor: cert.hr

Slika 5.5 označuje prikaz osnovnih izvora informacija NIPS i HIPS sustava pomoću kojih prikupljaju potrebne podatke o aktivnostima.



Slika 10. Izvor podataka kojim se koriste NIPS i HIPS alati

Izvor: cert.hr

5.3. Najpoznatijih IDS i IPS alati danas

Neki od najkorištenijih IDS alata:

- **SolarWinds Security Event Manager**: alat za analiziranje zapisnika u Windows, Unix, Linux i Mac OS sustavima. Upravlja podacima prikupljenim od strane Snort-a, uključujući podatke u stvarnom vremenu. SEM je i sustav za sprečavanje provale, koji isporučuje preko 700 pravila za zaustavljanje zlonamjernih aktivnosti. Bitno sredstvo za poboljšanje sigurnosti, reagiranje na događaje i postizanje usklađenosti.[18]
- **Snort:** najkorišteniji je mrežni sustav otkrivanja provala.

[18] https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

- **OSSEC:** sustav za otkrivanje upada koji je besplatan za korištenje.
- **Suricata:** mrežni je sustav koji radi na principu aplikacijskog sloja za detekciju nedozvoljenih upada u sustav
- **Bro:** jedan od kvalitetnijih alata za otkrivanje provale u sustav

Neki od najkorištenijih IPS alata:

- **Splunk:** jedan od najkorištenijih alata za prevenciju upada u sustav, a dostupan je na Windows, Linux i Cloud platformi.
- **Sagan:** ovakav sustav moguće je instalirati na Unix, Linux, Mac OS i Windows. Sustav radi na principu rudarenja bilježaka datoteka, kako bi mogao osigurati sustav od upada.
- **OSSEC:** spada pod HIDS sustav i besplatan je za korištenje. Podržan je od strane sustava Windows, Unix, Linux i Mac OS, ali ne uključuje korisničko sučelje.
- **Open WIPS-NG:** namijenjen je Linux sustavu, a svrha mu je otkrivanje upada u bežične mreže.
- **Fail2Ban:** besplatan IPS alat, a dostupan je za Mac OS, Linux i Unix sustave.

5.4. Snort – najkorišteniji sustav prevencije i detekcije upada u sustav

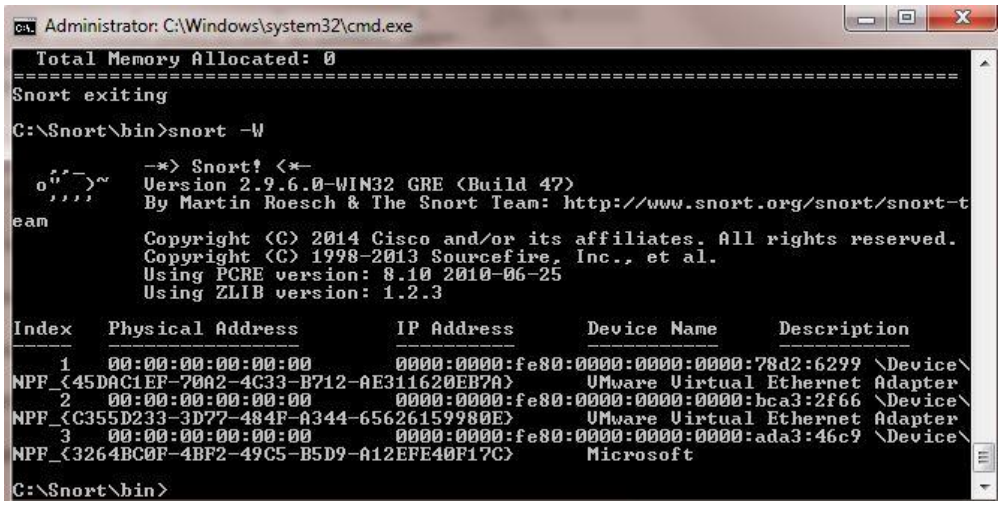
Snort je alat otvorenog koda za mrežno otkrivanje i sprječavanje upada u sustav - NIDPS (eng. Netwok Intrusion Detection and Prevention System). Izvorno ga je izdala firma Sourcefire na čelu s Martinom Roeschomp od 1998. godine. Alat ima sposobnost izvođenja analize prometa u stvarnom vremenu i zapisivanja 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.[19]

[19] https://www.cis.hr/files/dokumenti/CIS-DOC-2011-10-028.pdf

5.4.1. Instalacija i uporaba sustava Snort u Windows sustavu

Kako bi se započela instalacija Snort sustava prvo je potrebno skinuti aplikaciju sa web-mjesta Snort.org, te se moraju preuzeti pravila koja se dobiju nakon registracije Snorta. Nakon preuzete aplikacije potrebno je kliknuti na .exe kako bi se pokrenula instalacija, snort će biti instaliran u mapi „C:/Snort“. Mora se izdvojiti datoteka s pravilima koja se dobije pri registraciji, za to je potreban WinRAR (za .gz datoteku). Zatim je potrebno kopirati sve datoteke koje su izdvojene iz pravila i zalijepiti u mapu „C:/Snort/rules“. Nakon toga potrebno je kopiranje „snort.conf“ datoteke iz mape „etc“, te zalijepiti u mapu „C:/Snort/etc“. Potrebno je otvoriti naredbeni redak (cmd.exe) i navesti put do mape „C:/Snort/bin“. Za pokretanje sniffer tehnike snort sustava mora se upisati naredba npr. snort-dev -i 3. (-i) označava broj sučelja u ovom slučaju je to 3, a (-dev) koristi se za pokretanje snort alata za dohvaćanje mrežnih paketa.

Za provjeru potpisa sučelja koristi se naredba snort-W.



Slika 11. Sučelje

Izvor: https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/

Za pokretanje IDS tehnike rada, mora se konfigurirati datoteka „snort.conf“ prema mrežnom okruženju. Za određivanje mrežne adrese koja se želi zaštititi, potrebno je pretražiti varijablu HOME_NET 192.168.1.0/24 u datoteci „snort.conf“. Može se postaviti i DNS_SERVERS ako se nalaze u mreži.

```
##################################################
# Step #1: Set the network variables.  For more information, see
README.variables
##################################################

# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most
situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS 192.168.1.1

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
```

Slika 12. Mrežne adrese i serveri

Izvor: https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/

Zatim je potrebno promijeniti varijablu RULE_PATH u mapu s pravilima. (var RULE_PATH c: /snort/rules)

```
# List of ports you run SIP servers on
portvar SIP_PORTS [5060,5061,5600]

# List of file data ports for file inspection
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]

# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar AIM_SERVERS
[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12
.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9
.0/24,205.188.153.0/24,205.188.179.0/24,205.188.248.0/24]

# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an
absolute path,
# such as:  c:\snort\rules
var RULE_PATH c:\snort\rules
#var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

Slika 13. Primjena varijable RULE_PATH

Izvor: https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/

Nakon prijašnjih koraka potrebno je promijeniti putanju svih „library“ datoteka u sustavu (C: \ Snort \ lib \ snort_dynamiccpreprocessor). Ovo se mora učiniti za sve „library“ datoteke u mapi "C: \ Snort \ lib". Zatim je potrebno promijeniti putanju vrijednosti varijable u datoteci „snort.conf“. (dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll).

```
##################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort -
Dynamic Modules
##################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib
\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
```

Slika 14. Dinamički učitana biblioteka

Izvor: https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/

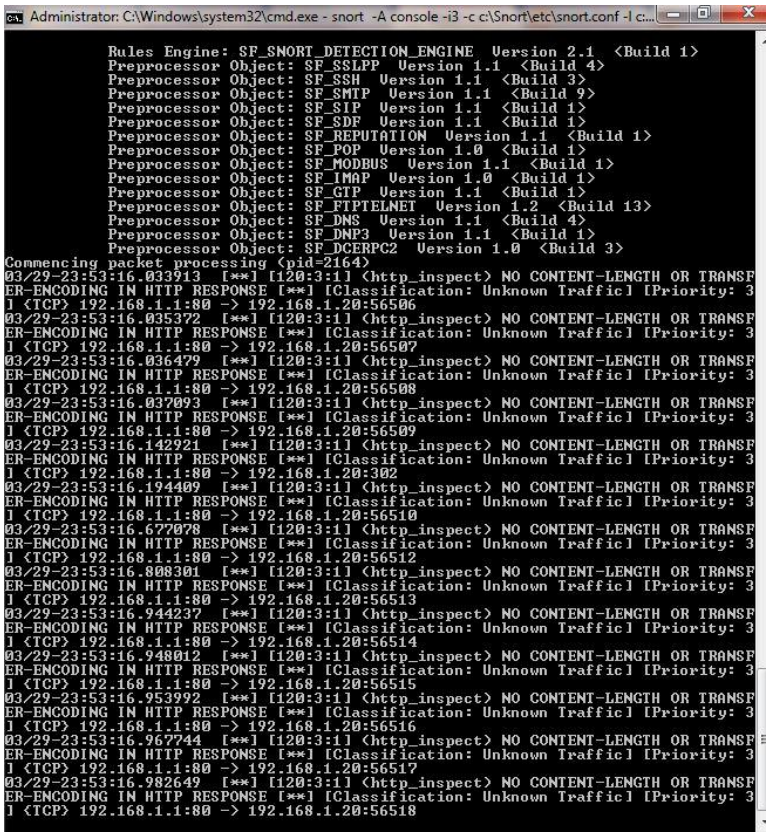
Nakon izvršenih koraka moraju se uključiti naredbe:
„include c:\snort\etc\classification.config“ i „include c:\snort\etc\reference.config“
Kada su se uključile naredbe potrebno je ukloniti komentare (#) na liniji, kako bi se omogućila ICMP-info pravila. (uključuje se $ RULE_PATH / icmp-info.rules)
Da bi se dodale datoteke dnevnika za spremanje upozorenja koje generira sustav Snort, potrebno je potražiti tekst „output log“ koji se nalazi u „snort.conf“, te dodati naredbu „output alert_fast: snort-alerts.ids“. Potrebno je dodati komentar (#) na bijelu listu $ WHITE_LIST_PATH / white_list.rules, zatim se promijeniti (nested_ip inner, \ u nested_ip inner #, \ ).

Postavite (#) na sljedeće linije, te spremite datoteku „snort.conf“.
#preprocessor normalize_ip4
#preprocessor normalize_tcp: ips ecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6

Za pokretanje snorta u IDS modu, mora se pokrenuti naredba „snort -cc: \ snort \ itd \ snort.conf -lc: \ snort \ log -i 3“. Ako se stvori dnevnik, potrebno je odaberiti odgovarajući program da bi se otvorio. Može se koristiti WordPard ili NotePad ++ za čitanje datoteke.

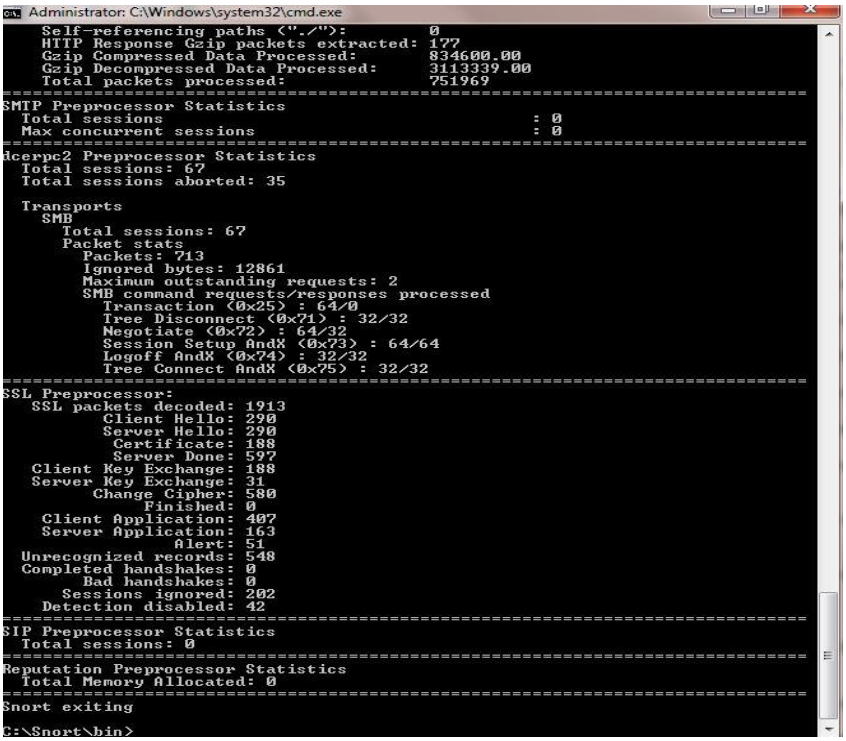
Za generiranje datoteka dnevnika u ASCII načinu, tijekom izvođenja snort u IDS načinu može se koristiti naredba:
„snort -konzola -i3 -cc: \ snort \ itd \ snort.conf -lc: \ snort \ log -K ascii“

Nakon toga potrebno je skenirati računalo koje pokreće snort s drugog računala pomoću PING ili NMap (ZenMap).
Nakon skeniranja ili tijekom skeniranja može se provjeriti datoteka snort-alerts.ids u log mapi kako bi se korisnik osigurao da se pravilno prijavi. Moguće je vidjeti da se pojavljuju mape s IP adresom.



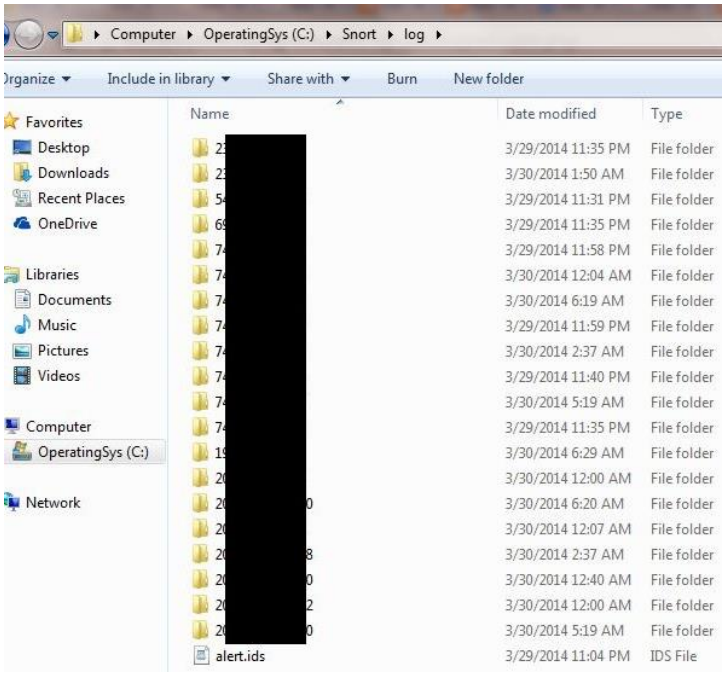
Slika 15. Snort nadzor prometa

Izvor: https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/



Slika 16. Izvještaj o zaustavljanju skeniranja sustav snort

Izvor: https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/



Slika 17. Datoteke zapisa

Izvor: https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/

6. POHRANA PODATAKA U OBLAKU (CLOUD COMPUTING)

U poslovnom svijetu sve se više kompanija odlučuje za cloud pristup pohrane podataka, te zamjenjuje svoju tradicionalnu strukturu, kako bi poboljšali zaštitu podataka tvrtke, ali i kako bi se omogućio rad na nekim drugim lokacijama a ne samo unutar tvrtke. Rad izvan tvrtke s cloud pristupom je moguć jer su vam samo potrebni Internet i uređaj preko kojeg je moguće pristupiti podatcima, a tvrtke koje imaju tradicionalan pristup mogu doći do podataka i poslovnih programa jedino unutar tvrtke, na računalu na kojem su instalirani takvi programi. Cloud computing je budućnost sigurne pohrane podataka i olakšavanja u radu svake tvrtke, jer omogućava pristup svim dokumentima i aplikacijama na raznim lokacijama izvan tvrtke, te se može pristupiti podatcima sa više uređaja. Korisnici cloud usluga vrlo brzo mogu koristiti i mijenjati podatke, jer se podatci nalaze na jednom mjestu i uvijek su dostupni, što daje korisniku mobilnost. Tvrtke koje su se odlučile za cloud usluge, ne moraju poboljšati informatičku strukturu niti zapošljavati radnike za održavanje tih usluga, jer davatelj cloud usluga se brine o administraciji, podršci i razvoju poslovnih aplikacija. Usluga nudi i razne nadogradnje, jače sigurnosne mehanizme, arhiviranje podataka. Velika je prednost clouda što kod takvih servisa su svi podatci kriptirani, tako da nitko ne može pristupiti tim podatcima osim djelatnika odnosno korisnika koji koristi cloud servis, niti može te podatke dekriptirati. Cloud pristup pohrane podataka omogućava zaštitu i od gubitka podataka, jer postoje određeni sigurnosni mehanizmi kao što su dnevne sigurnosne kopije ili spremanje podataka na više mjesta, što ukazuje na vrlo mali rizik gubitka podataka. Tvrtke koje se odluče za cloud model olakšavaju si način poslovanja, jer se tvrtke mogu fokusirati na tržište, konkurenciju i korisnika, a za tehnologiju i sigurnost podataka zaduženi su cloud servisi odnosno profesionalci s modernom tehnologijom. Cloud omogućuje tvrtkama poslovni kontinuitet, fleksibilnost, skalabilnost, veći izbor u razvoju IT strategije, te najvažnije smanjenje troškova. Cloud usluga se plaća mjesečno, sukladno potrebama koje tvrtke zahtijevaju, odnosno onoliko prostora i vrstu usluge koju tvrtka treba za njeno poslovanje.

Neki od najkorištenijih cloud servisa današnjice su:

- Dropbox
- Google Drive
- Mega
- OneDrive
- iCloud
- Box
- NextCloud

Vrste oblaka koji postoje:

- Privatni oblak - Infrastruktura privatnog oblaka posebno je namijenjena poduzećima. Podaci i aplikacije smješteni su u vlastitim podatkovnim centrima ili kod pružatelja usluga u oblaku. Oni koji podržavaju privatni oblak smatraju da se tim modelom nudi najviši stupanj kontrole, sigurnosti i privatnosti. Društvo ima potpunu kontrolu nad time kamo se smještaju njegovi podaci.[20]
- Javni oblak - Idealan za analizu velikih skupova podataka. Taj se model isto tako uobičajeno upotrebljava za pohranu manje važnih podataka. Jeftiniji je zbog opcije fleksibilnog rezerviranja ili otkazivanja prostora za pohranu. U usporedbi s uspostavom vlastitog podatkovnog centra, mala i srednja poduzeća ostvaruju korist od razina sigurnosti, fleksibilnosti i učinkovitosti javnog oblaka.[21]
- Hibridni oblak - Konceptom hibridnog oblaka objedinjena je većina funkcija kako javnog tako i privatnog oblaka. Tim se modelom društvima omogućuje da se bolje nose sa sezonskim fluktuacijama u svojem svakodnevnom poslovanju. Lokalna infrastruktura može se prilagoditi uobičajenim uvjetima rada uz istodobno povećanje računalne snage i pohrane javnog oblaka u skladu s potražnjom. Nakon sezone vršnog opterećenja mogu se ponovno smanjiti resursi koji više nisu potrebni. To je puno jeftinije nego rezerviranje namjenskih kapaciteta i računalne snage koji su većinu vremena nepotrebni.[22]

[20] https://www.tportal.hr/tehno/clanak/trebate-li-privatni-javni-ili-hibridni-oblak-20161125
[21] https://www.tportal.hr/tehno/clanak/trebate-li-privatni-javni-ili-hibridni-oblak-20161125
[22] https://www.tportal.hr/tehno/clanak/trebate-li-privatni-javni-ili-hibridni-oblak-20161125

7. ZAKLJUČAK

Svakim porastom složenosti računalnog sustava, javlja se i porast složenosti konfiguracije sustava, te neka najmanja greška u konfiguraciji nekog dijela sustava može ugroziti cijeli sustav. Kao što je navedeno porast složenosti sustava isto tako postoji i složenost programskih aplikacija, pokrenute od strane raznih sustava. U složenijim aplikacijskim programima može doći do potkradanja pogreške u konfiguraciji, te u programskom kodu aplikacija. Svim navedenim može se dovesti cijeli računalni sustav u opasnost. Svakodnevno se otkrivaju razni sigurnosni propusti na različitim aplikacijama i sustavima računala. Zlonamjerni korisnici organiziraju sve složenije napade na određene računalne sustave i aplikacije, te ih je sve teže detektirati i ponajprije ukloniti. Na internetu je dostupan veliki broj određenih alata s kojima se može vrlo lako ugroziti vlastiti računalni sustav, ukoliko se na njemu nalaze neki od sigurnosnih propusta. Zbog ponude kojekakvih alata treba se voditi računa o sigurnosti računalnog sustava i paziti kakvi se alati skidaju jer se na taj način može učiniti sustav ranjivim, što olakšava napad na računalni sustav. Da bi bili što sigurniji od štetnih napada postoje određeni alati za detekciju i prevenciju upada u računalni sustav. Takvi sustavi su dostupni besplatno za sve klijente i lako ih je preuzeti i instalirati kako bi ih omogućili za njihov rad. Pomoću alata moguće je otkriti zlonamjernu radnju na računalni sustav, te kada sustav detekcije dojavi da se radi o opasnosti, sustavi prevencije odbacuju takve štetne radnje i bilježi u bazu podataka informacije o napadu kako bi se u budućnosti lakše blokirale provale u sustav. Ovakvi sustavi su korišteni sve češće i u poslovnom svijetu, što je i razumljivo, jer svaka tvrtka ili organizacija mora voditi računa o sigurnosti svojih povjerljivih podataka i o sigurnosti podataka svojih klijenata.

POPIS INTERNET IZVORA

1. http://fzp.singidunum.ac.rs/demo/wp-content/uploads/Zbornik-Konferencija-Mre%C5%BEa-2013.pdf#page=24 [pristup: 20.07.2019.]
2. https://www.cis.hr/dokumenti/2852-snortids.html [pristup: 25.08.2019.]
3. https://csrc.nist.gov/publications/detail/sp/800-94/rev-1/draft [pristup: 27.08.2019.]
4. http://web.studenti.math.pmf.unizg.hr/~ksekuli/napadi.htm[pristup: 20.07.2019.]
5. https://www.lifewire.com/ids-and-prevention-ips-software-2487316[pristup: 28.08.2019.]
6. https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/ [pristup: 27.08.2019.]
7. https://www.comparitech.com/net-admin/network-intrusion-detection-tools/ [pristup: 22.08.2019.]
8. cert.hr [pristup: 31.07.2019.]
9. http://www.enciklopedija.hr/Natuknica.aspx?ID=68380 [pristup: 20.07.2019.]
10. https://plaviured.hr/vodici/malware-sto-je-i-kako-se-zastititi/[pristup: 24.07.2019.]
11. http://virusi.hr/backdoors-straznja-vrata/ [pristup: 31.07.2019.]
12. https://resources.infosecinstitute.com/rootkits-user-mode-kernel-mode-part-1/#gref [pristup: 10.08.2019.]
13. https://www.omnisecu.com/security/rootkits.php [pristup: 10.08.2019.]
14. http://www.sinarm.net/sto-je-cloud-computing-ili-usluga-u-oblaku/[pristup: 15.05.2020.]
15. https://zimo.dnevnik.hr/clanak/evo-sto-je-to-tocno-cloud-i-zasto-je-sigurniji-od-tradicionalnih-rjesenja---596591.html [pristup: 15.05.2020.]
16. https://www.ictbusiness.info/internet/top-10-cloud-servisa-za-pohranu-podataka [pristup: 17.05.2020.]
17. https://www.tportal.hr/tehno/clanak/trebate-li-privatni-javni-ili-hibridni-oblak-20161125 [pristup: 17.05.2020.]

LITERATURA

1. John R. Vacca (2017.) Computer and Information Security Handbook. 3nd Edition.

POPIS SLIKA

SAŽETAK

U samom uvodu rada opisuje se informacijske tehnologije i velik napredak istih što je utjecalo na bolji razvoj tvrtki. Sigurnost podataka vrlo je bitna za tvrtke, te je sve više alata pomoću kojih se štite informacijske strukture tvrtke, kako ne bi došlo do krađe i zlouporabe podataka. Drugi dio rada se odnosi na računalnu sigurnost i sprječavanje zlonamjernih radnji kako bi se došlo do korisnikovih podataka. Kako bi korisnik zaštitio svoje podatke i neželjene upade u sustav mora koristiti neke od sigurnosnih mjera i postupaka za zaštitu podataka. U drugom dijelu su opisane i neke kategorije napada na sigurnost korisnika. U trećem dijelu su opisani neki od zlonamjernih programa, te klasifikacija istih. Opisane su i opasnosti po korisnika uzrokovane takvim zlonamjernim programima. Četvrti dio se odnosi na napadače, te njihove motive, jer nisu svi napadači zlonamjerni. Neki napadači na sustave pokušavaju pomoći određenim tvrtkama da pronađu ranjivosti njihovih sustava, te da se u pravo vrijeme zaštite od stvarnih napadača. Najopširnije opisan peti dio govori o najnovijim tehnologijama za sprječavanje i otkrivanje opasnosti upada u računalni sustav. Opisan je i najkorišteniji Snort sustav za prevenciju i detekciju upada u sustav, te njegova instalacija i uporaba. Zadnji dio rada odnosi se na odabir poslovanja tvrtki cloud uslugom, te prednosti koje donosi sam cloud servis. Na kraju se nalaze popis literature, popisi internetskih izvora, popisa slika i na kraju sažetak ovoga rada.

Ključne riječi: Sigurnost, otkrivanje zlonamjernih radnji, sprječavanje zlonamjernih radnji, IDS, IPS, Snort, Cloud

SUMMARY

In the very introduction to the paper, I describe information technologies and their great progress, which has influenced the better development of companies. Data security is very important for companies, and there are more and more tools to protect the company's information structures, so that data theft and misuse do not occur. The second part of the paper deals with computer security and the prevention of malicious actions in order to obtain user data. In order for the user to protect his data and unwanted intrusions into the system, he must use some of the security measures and procedures for data protection. The second part describes some categories of user security attacks. The third part describes some of the malicious programs, and their classification. The dangers to the user caused by such malware are also described. The fourth part refers to the attackers, and their motives, because not all attackers are malicious. Some system attackers try to help certain companies find vulnerabilities in their systems, and to protect themselves from real attackers at the right time. The most comprehensively described fifth part talks about the latest technologies for preventing and detecting the danger of intrusion into a computer system. The most used Snort system for prevention and detection of intrusions into the system, as well as its installation and use are described. The last part of the paper refers to the selection of companies' business with the cloud service, and the advantages that the cloud service itself brings. Finally, there is a list of references, lists of Internet sources, lists of images and finally a summary of this paper.

Keywords: Security, Malware Detection, Malware Prevention, IDS, IPS, Snort, Cloud