# Sustavi za detekciju i prevenciju upada u računalne sustave

**Mlinar, Dorian**

VELEUČILIŠTE U VIROVITICI

Stručni prijediplomski studij Elektrotehnika

DORIAN MLINAR

# SUSTAVI ZA DETEKCIJU I PREVENCIJU UPADA

ZAVRŠNI RAD

VIROVITICA, 2023.

VELEUČILIŠTE U VIROVITICI

Stručni prijediplomski studij Elektrotehnika

# SUSTAVI ZA DETEKCIJU I PREVENCIJU UPADA

ZAVRŠNI RAD

Predmet: Sigurnost informacijskih sustava

Mentor: Student:

Enes Ciriković, dipl.ing., v.pred. Dorian Mlinar

VIROVITICA, 2023.

# Veleučilište u Virovitici

Stručni prijediplomski studij Elektrotehnike - Smjer Telekomunikacije i informatika

OBRAZAC 1b

ZADATAK ZAVRŠNOG RADA

Student/ica: MLINAR DORIAN JMBAG: 0307017410

Imenovani mentor: Enes Ciriković, dipl. ing., v. pred.
Imenovani komentor: Naslov rada:

| Sustavi za detekciju i prevenciju upada u računalne sustave |
|---|

Puni tekst zadatka završnog rada:

Student će se u završnom radu osvrnuti na temeljna načela IDS/IPS sustava te će potom na primjeru jednog odabranog sustava praktično demonstrirati neke od opisanih značajki.

---

Datum uručenja zadatka studentu/ici: 31.07.2023. Rok za predaju gotovog rada: 08.09.2023.

Mentor:

Enes Ciriković, dipl. ing., v. pred.

Enes Ciriković

Dostaviti:
1. Studentu/ici
2. Povjerenstvu za završni rad - tajniku

# SUSTAVI ZA DETEKCIJU I PREVENCIJU UPADA

***Sažetak***

*Tema rada je teorijska obrada IDS i IPS sustava te praktični primjer njihove koristi. U teorijskom dijelu se opisuju IDS i IPS sustavi, njihove funkcionalnosti, arhitekture, primjene u stvarnome svijetu te njihovi načini obrade i analize sigurnosnih incidenata. Opisuju se razlike između IDS i IPS sustava. Navode se načini na koje se dijele različite vrste IDS sustava te razlike između njih. Navode se sposobnosti reakcije ali i potencijalne ranjivosti IDS sustava na različite vrste napada te odgovarajuće mjere obrane. U praktičnom se u okruženju GNS3 mrežnog simulatora implementira testna mreža sa Snort sustavom ugošćenog u sastavu Mikrotik usmjeritelja. NA temelju zadane mreže te simulacije pokušavaju se pokazati neke osnovne značajke IDS/IPS sustava Snort.*

***Ključne riječi:*** *IDS, IPS, Pravila, Snort, Sigurnost*

# INTRUSION DETECTION AND PREVENTION SYSTEMS

# 1. Uvod

U suvremenom digitalnom okruženju, sveprisutna povezanost i visoka razina digitalne aktivnosti donose sa sobom i povećani rizik od različitih kibernetičkih prijetnji. S obzirom na ovu izazovnu dinamiku, tema sustava za detekciju i prevenciju upada (IDS i IPS) postaje od suštinskog značaja za očuvanje sigurnosti informacijskih sustava. Izbor ove teme proizlazi iz nužnosti razumijevanja kako se ovi sustavi koriste za zaštitu od kibernetičkih prijetnji te kako se razlikuju u svojim funkcijama i arhitekturi. U nastavku ovog rada, bit će istražene razlike između IDS i IPS sustava, dviju ključnih komponenata u zaštiti informacijskih sustava od neovlaštenih upada. Prvo će biti izvršena usporedba ovih sustava kako bi se bolje razumjele njihove različite uloge i mogućnosti. Nakon toga, bit će provedena analiza arhitekture IDS sustava s ciljem dobivanja dubljih uvida u njihovu funkcionalnost. Na kraju, bit će prikazan praktičan primjer primjene IDS sustava u stvarnom svijetu s namjerom ilustracije njegove važnosti i učinkovitosti u borbi protiv kibernetičkih prijetnji.

# 2. Detekcija upada u sustav

Praćenje i analiza događaja koji se odvijaju u računalnom sustavu ili mreži u svrhu pronalaženja dokaza o provalama - pokušajima narušavanja povjerljivosti, integriteta ili dostupnosti računalnog sustava ili mreže - predstavlja postupak detekcije upada u sustav. Softverska ili hardverska rješenja nazvana sustavi za detekciju upada u sustav (IDS) automatiziraju ovaj postupak praćenja i analize.

IDS (engl. *Intrusion Detection System*) sustavi su ključne komponente sigurnosti računalnih mreža i sustava. Njihova osnovna svrha je detektirati neovlaštene i potencijalno zlonamjerne aktivnosti unutar računalnih okolina. IDS sustavi prate mrežni promet i sustavsku aktivnost kako bi identificirali anomalije, potencijalne napade ili nepravilnosti u ponašanju korisnika. Postoje dvije glavne kategorije IDS sustava: NIDS (*Network IDS*) koji nadziru promet na mreži i HIDS (*Host IDS*) koji prate aktivnosti na pojedinim računalima ili uređajima. IDS sustavi koriste različite metode, uključujući pravila, potpise i analizu anomalija, kako bi identificirali sigurnosne prijetnje i omogućili brzu reakciju ili upozorenje administratora na potencijalne rizike.

# 3. Razlika između vatrozida i IDS sustava

Iako i IDS sustav i vatrozid spadaju u mrežnu sigurnost, postoje razlike između njih. Naime vatrozid ima mogućnost blokiranja i dopuštanja prolaska paketa po već prije definiranim pravilima te ih primjenjuje na temelju faktora kao što su izvorišne i odredišne IP adrese, portovi i protokoli. IDS konstantno osluškuje cijeli mrežni promet te traži neuobičajene aktivnosti i/ili pokušaje upada u sustav te ima mogućnost slanja obavijesti administratorima ili odgovornim osobama  da je došlo do napada na sustav.

Ukratko može se reći da je vatrozid prva linija obrane te što njemu promakne to bi u teoriji trebao detektirati IDS sustav. No mora se napomenuti da ovi alati nisu svemoćni te da dovoljno vješte osobe i dalje mogu pronaći ranjivosti i infiltrirati se u sustav.

# 4. Razlika između IDS i IPS sustava

Iako su IDS i IPS (engl. *Intrusion prevention system*) sustavi sigurnosni mehanizmi koji se koriste u računalnim mrežama i sustavima, postoje razlike između njih.

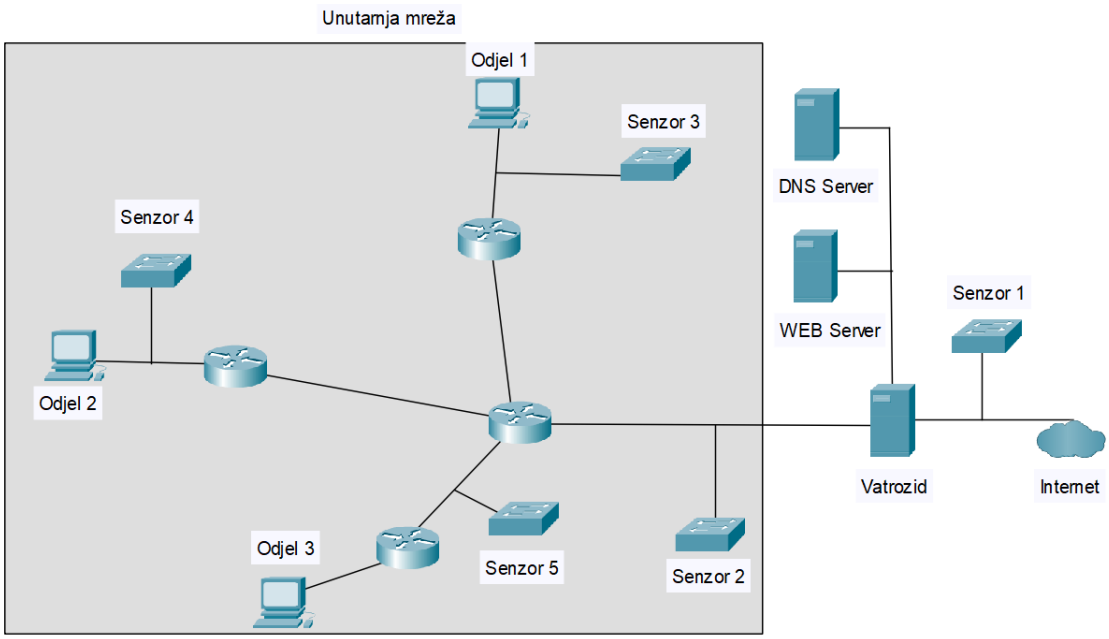
Dok IDS sustav prati mrežni promet on to radi pasivno što znači da ako dođe do napada ili neovlaštene aktivnosti, IDS sustav ništa ne poduzima u vezi toga osim slanja obavijesti administratorima da je došlo do napada. Za razliku od IDS sustava IPS sustav aktivno poduzima mjere ako dođe do napada. To se može sastojati od blokiranja mrežnog prometa, prekidanja veza ili primjenom pravila na vatrozidu.

Ukratko IDS i IPS imaju gotovo iste funkcionalnosti uz dodatak da IPS ima dodatne mogućnosti u blokiranju napada.

# 5. Smještaj IDS u mrežnoj topologiji

Smještaj IDS sustava u mrežno okruženje predstavlja ključnu odluku koja ovisi o nekoliko faktora. Prvenstveno, topologija mreže igra važnu ulogu jer određuje kako će se promet kretati unutar sustava. Ukoliko se mrežni IDS koristi, on će analizirati sav promet na mreži, no u situacijama gdje postoji velika količina prometa, može se javiti potreba za više IDS sustava kako bi se osigurala potpuna analiza prometa.

S druge strane, potrebe korisnika također igraju ključnu ulogu pri smještaju IDS sustava. Ovisno o vrsti napadačeve aktivnosti koju treba otkriti, kao što su unutarnji ili vanjski napadi, IDS će se postaviti na odgovarajuće pozicije unutar mreže. Važno je napomenuti da je zaštita pristupnih veza prema Internetu od izuzetnog značaja, jer su često mete napada. IDS bi stoga trebao pokrivati sve pristupne veze prema Internetu u sustavu kako bi detektirao potencijalne prijetnje. Položaj IDS sustava u odnosu na vatrozid jedan je od prvih koraka u uspostavi cjelovite mrežne sigurnosti. Postavljanje IDS sustava nakon vatrozida omogućuje analizu samo podataka koje vatrozid propusti, čime se smanjuje količina analiziranog prometa. S druge strane, postavljanje IDS sustava izvan vatrozida omogućuje i detekciju neuspjelih napada, ali može rezultirati većim prometom za analizu, što može dovesti do pada performansi sustava.




*Slika 1. Smještaj IDS sustava u mrežnoj topologiji [2]*

Slika 1. pokazuje jedan od mogućih rasporeda IDS sustava u mrežnoj topologiji. Senzor 1 nadgleda sav mrežni promet koji dolazi izvana. Senzor 2 nadgleda promet koji je propušten kroz vatrozid. Senzor 3, Senzor 4 i Senzor 5 nadgledaju promet između različitih odjela unutar tvrtke [2].

# 6. Model procesa za detekciju upada

Većinu IDS sustava možemo opisati sa tri funkcionalne komponente:

- *Izvor informacija* - Različiti izvori informacija se koriste za utvrđivanje je li došlo do upada. Ovi izvori se razlikuju sa djelom sustava koji se prati. Ovdje se najčešće govori o mrežnom, host ili aplikacijskom nadziranju [1].
- *Analiza* - Komponenta sustava IDS-a koja organizira i tumači događaje prikupljene iz izvora informacija, određujući kada takvi događaji sugeriraju da su u tijeku provale ili su se već prije dogodile. Otkrivanje zloupotrebe (engl. *misuse detection*) i otkrivanje nepravilnosti (engl. *anomaly detection*) su dvije najčešće korištene tehnike analize [1].
- *Reakcija* - Skup radnji koje sustav poduzima nakon što otkrije upada. Ovdje se svrstavaju aktivne i pasivne radnje. Aktivne radnje uključuju neke automatske intervencije dok pasivne samo prijavljuju upad odgovornim osobama [1].

Sustav analizira informacije dobivene iz izvora informacija te po njima generira odgovore koji mogu varirati od slanja obavijesti administratorima te ako je riječ o IPS sustavima oni mogu poduzeti neke aktivne mjere poput pokretanja skripti, onemogućivanja korisničkog računa i slično.

# 7. Vrste IDS-a

S obzirom na različite načine analize i nadzora mrežnog prometa moguće je razlikovati nekoliko osnovnih kategorija IDS sustava. Spomenuti ćemo sve pristupe iako svi nisu jednako zastupljeni u praksi.

Postoji sedam pristupa klasifikaciji IDS sustava:

1. Arhitektura
2. Ciljevi
3. Kontrolna strategija
4. Vrijeme
5. Informacijski izvori
6. IDS analiza
7. Reakcija IDS sustava

Svaki od navedenih operativnih modela moguće je opisati tzv. Generičkim procesnim modelom koji razlikuje tri temeljne funkcionalne komponente:

Izvori informacija - povlačenje informacija o događajima iz različitih izvora pomažu pri odlučivanju o prisutnosti sigurnosnih proboja. Informacije se prikupljaju s različitih razina sustava, poput krajnjih uređaja, mrežne opreme te aplikacija za nadzor i kontrolu mreža i pratećih usluga.

Analiza - organizacija prikupljenih podataka u smislene indikatore događaja. Realizira se kroz dva pristupa: detekcija zlouporabe te detekcija nesukladnosti, tj. anomalija.

Odaziv - skup radnji koje se poduzimaju na temelju detektiranih upada. Ovisno o načinu donošenja konačnih mjera, uobičajeno se grupiraju u aktivne i pasivne. Kod aktivnih mjera sustav automatski poduzima potrebne intervencije, dok se kod pasivnih mjera očekuje ljudska analiza primljenih IDS izvještaja prije donošenja konačnih akcija.

## 7.1. Arhitektura

Arhitektura IDS sustava odnosi se na organizaciju i poredak funkcionalnih komponenti ovog sustava u cilju efikasne detekcije potencijalnih prijetnji. Ključne

komponente arhitekture IDS sustava su sustav na kojem je IDS pokrenut (engl. Host), te sustav koji se nadzire radi otkrivanja problema (engl. Target).

Host komponenta IDS sustava predstavlja središte sustava. To je sustav na kojem se instalira i izvodi sam IDS softver. Host ima ključnu ulogu u obradi i analizi podataka kako bi identificirao neobične i potencijalno opasne aktivnosti unutar mreže. S obzirom na složenost ovog zadatka, važno je da Host komponenta bude dovoljno resursno snažna kako bi mogla obrađivati veliku količinu podataka u realnom vremenu.

S druge strane, Target komponenta IDS sustava je sustav koji se nadzire. Ova komponenta je odgovorna za prikupljanje podataka i komunikaciju s Hostom kako bi omogućila analizu prometa i identifikaciju potencijalnih prijetnji. Važno je napomenuti da Target može biti pojedinačni uređaj, mreža uređaja ili cijela mreža, ovisno o opsegu nadzora koji IDS treba pokriti.

### 7.1.1. Host-Target kolokacija

Ovaj pristup koji uključuje IDS koji se izvodi na istom računalu koje štiti predstavlja staromodnu arhitekturu koja se koristila u vremenima kada su računala bila centralna i ogromna, a ne individualni i distribuirani sustavi kao što su danas. Ideja je bila jednostavna - koristiti računalo koje već postoji na mreži kako bi se nadgledao promet i otkrile prijetnje.

Međutim, ova arhitektura ima svoje ozbiljne mane. Prvenstveno, kada napadač uspije provaliti u ciljani sustav, postoji visok rizik da će on moći vrlo lako onesposobiti IDS koji se izvodi na istom računalu. To znači da napadač, jednom kada pristupi sustavu, može deaktivirati IDS kako bi ostao neotkriven ili manipulirao svoje aktivnosti.

Zbog ovog ozbiljnog nedostatka, ovakva arhitektura se sve manje koristi u suvremenim informacijskim sustavima. Umjesto toga, IDS se često izvodi na posebnim uređajima ili računalima koja su odvojena od ciljnog sustava koji se štiti. Ovo omogućuje bolju izolaciju IDS sustava od potencijalnih napadačkih aktivnosti i povećava vjerojatnost otkrivanja neovlaštenih pristupa i prijetnji.

### 7.1.2. Host-Target separacija

Kako je vrijeme odmicalo, a tehnologija osobnih računala postajala sve dostupnija, promatrano je kontinuirano smanjenje cijene računalnih resursa. Ovaj tehnološki napredak omogućio je inženjerima i arhitektima IDS sustava da razvijaju sofisticiranije i efikasnije arhitekture.

Jedna od ključnih promjena bila je sposobnost odvajanja sustava na kojem se IDS izvodi od sustava koji IDS promatra. Ovaj pristup omogućio je veću fleksibilnost u postavljanju i upravljanju IDS sustavom. Umjesto da se IDS izvodi na samom ciljnom sustavu, sada se može izvoditi na odvojenom računalu ili uređaju posvećenom analizi prometa. To je znatno povećalo sposobnost otkrivanja i reagiranja na potencijalne prijetnje.

No, važno je napomenuti da je s ovom promjenom došlo i do izazova. S obzirom na odvojeni IDS sustav, postoji potreba za zaštitom samog IDS sustava od mogućih napadača. U suprotnom, napadači bi mogli pokušati onesposobiti ili degradirati performanse IDS sustava kako bi izbjegli otkrivanje.

## 7.2. Ciljevi

Kada se govori o ciljevima u kontekstu IDS sustava, tada se obično misli na odgovornost (engl. accountability) i reakciju (engl. response).

Odgovornost podrazumijeva sposobnost povezivanja konkretnih aktivnosti i događaja, poput napada ili neovlaštenog pristupa, s osobama ili entitetima koji su odgovorni za te događaje. Međutim, postizanje te povezanosti često je izrazito teško u TCP/IP mrežama, s obzirom na karakteristike samih protokola.

TCP/IP mreže omogućavaju napadačima da izvode različite oblike obmane, uključujući krivotvorenje izvora paketa ili prometa. Ova tehnika, poznata kao "spoofing," omogućava napadačima da manipuliraju svojim izvorima ili identifikatorima kako bi prikrili svoje stvarne identitete. Ovaj pristup čini izazovnijim povezivanje događaja s odgovornim osobama, jer se pravi izvor ili entitet može lako zamaskirati, otežavajući identifikaciju i praćenje prijetnji.

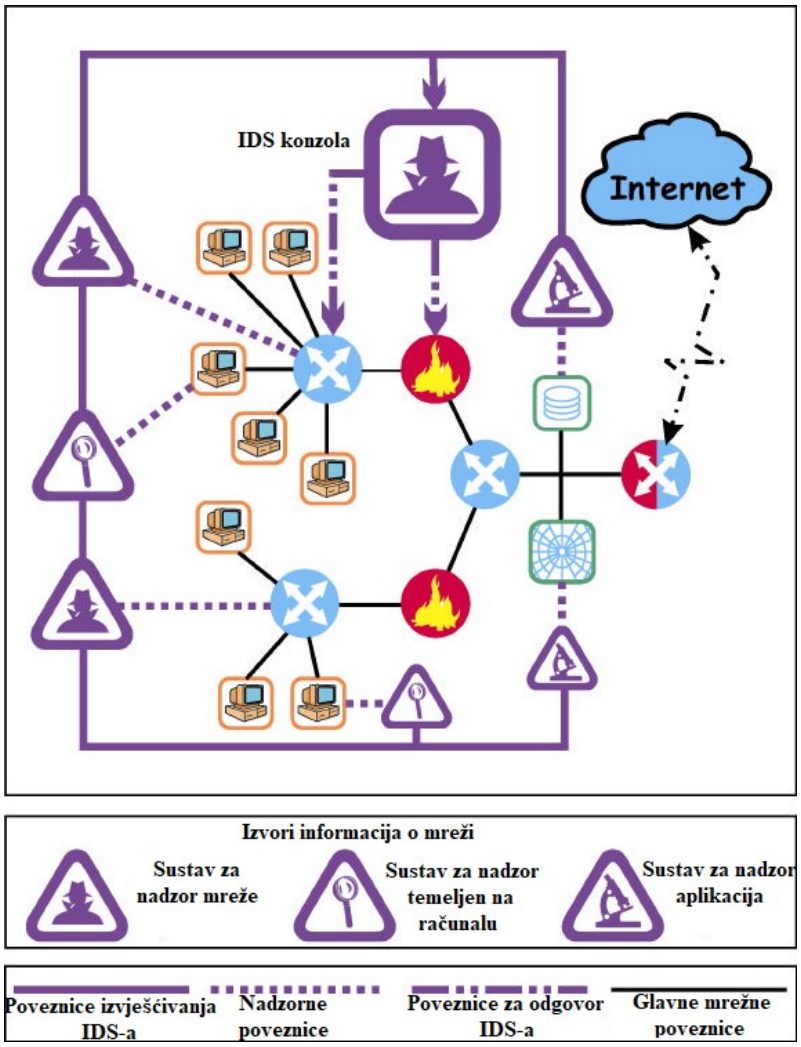
Reakcija u kontekstu sigurnosti informacijskih sustava odnosi se na ključni aspekt nakon što je otkriven određeni događaj, uključujući napade ili druge prijetnje. Ovaj korak zahtijeva sposobnost brzog i učinkovitog prepoznavanja potencijalno štetnih aktivnosti u sustavu nakon što su detektirane, a zatim poduzimanje odgovarajućih akcija kako bi se zaštitio sustav od daljnjih posljedica.

## 7.3. Kontrolna strategija

Kontrolna strategija objašnjava kako se rukuje komponentama IDS sustava i kako se kontroliraju njegov ulaz i izlaz.

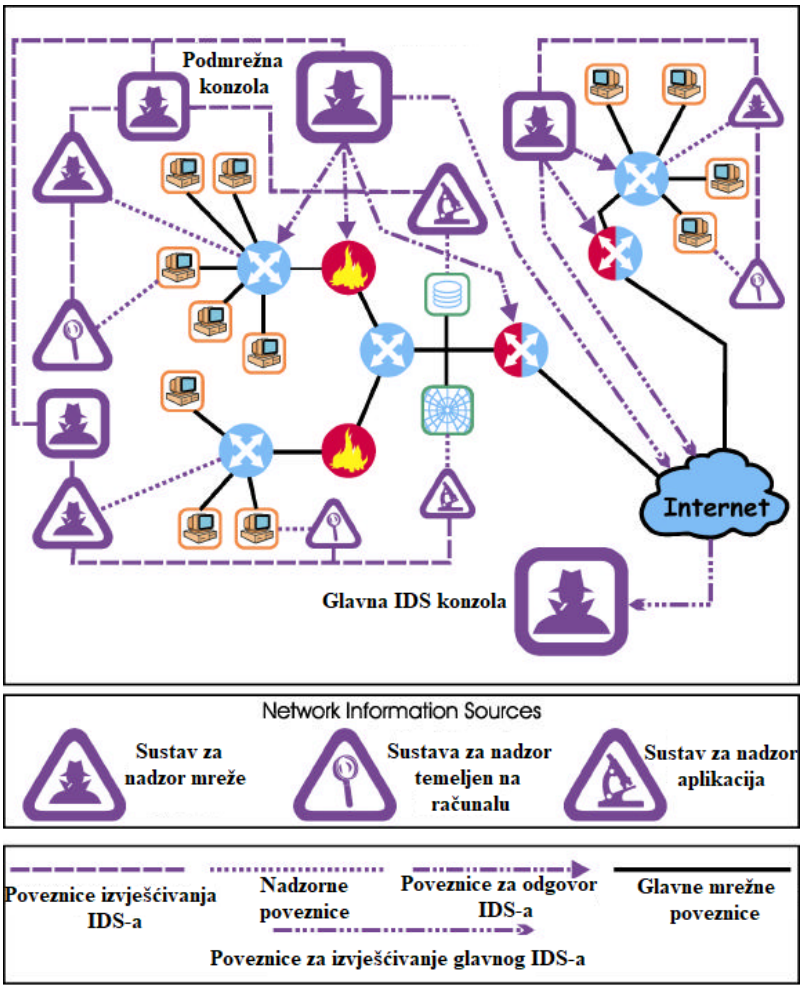
Kontrolna strategija može biti:

- *Centralizirana* - Svo praćenje, otkrivanje i izvještavanje upravlja se izravno s jednog središnjeg mjesta, drugim riječima sa centralne lokacije [1]. Primjer toga je prikazan slikom 2.



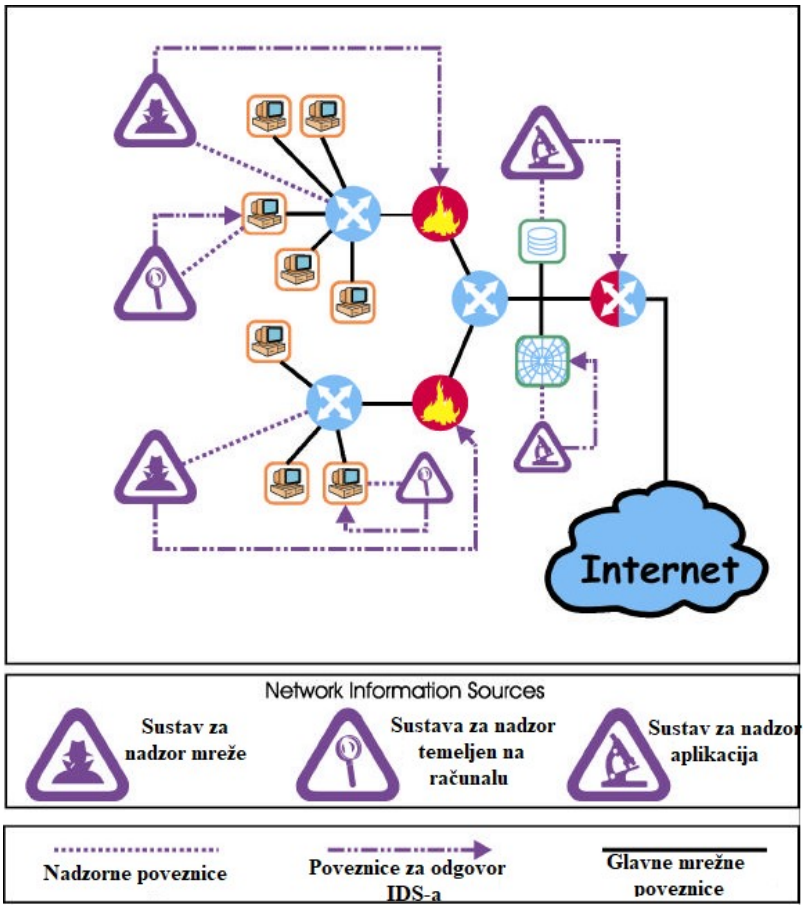

*Slika 2. Centralizirana kontrolna strategija [1]*

- *Djelomično distribuirana* - Nadgledanje i detekcija se odvijaju u lokalnim čvorovima koji to hijerarhijski prijavljuju jednoj centralnoj jedinici [1]. Primjer je prikazan slikom 3.




*Slika 3. Djelomično distribuirana kontrolna strategija[1]*

- *Potpuno distribuirana* - Koristi se strategija temeljena na agentima za praćenje i otkrivanje, a donošenje odluka o odgovorima odvija se u trenutku analize [1]. Primjer je prikazan slikom 4.




*Slika 4. Potpuno distribuirana kontrolna strategija[1]*

## 7.4. Vrijeme

Pod vrijeme se misli na vrijeme koje je prošlo između detekcije nekog događaja i njegove analize. Ovdje se razlikuju IDS sustavi zasnovani na vremenskim fragmentima (engl.. Interval-based IDS) te oni zasnovani na kontinuiranom radu u realnom vremenu (engl. Real-time IDS).

### 7.4.1. Vremenski fragmentirani IDS

U prošlim vremenima, operacijski sustavi često su koristili tehniku zapisivanja kontrolnih zapisa u datoteke kako bi dokumentirali aktivnosti u sustavu. Međutim, ovaj pristup je brzo pokazao svoje ograničenje u današnjem sve kompleksnijem i dinamičnijem digitalnom okruženju. Analiza takvih datoteka zahtijevala je znatno vrijeme i resurse, što je rezultiralo sporom reakcijom na potencijalne prijetnje

### 7.4.2. Vremenski kontinuirani IDS

Vremenski kontinuirani IDS sustavi predstavljaju ključnu komponentu suvremene sigurnosne arhitekture, jer omogućuju analizu i detekciju potencijalnih prijetnji u stvarnom vremenu. Ova sposobnost znači da se informacije o prometu i događajima analiziraju u trenutku kada se događaju, što rezultira puno bržom i dinamičnijom reakcijom IDS sustava na moguće napade.

Vremenski fragmentirani IDS, s druge strane, temelji se na sakupljanju podataka tijekom određenih vremenskih intervala. Ovakav pristup može značiti da se relevantni događaji neće otkriti sve dok se ne provede intervalna analiza, što može rezultirati značajnim vremenom kašnjenja u detekciji i reakciji na prijetnje.

## 7.5. Informacijski izvori

Najčešći način klasifikacije IDS sustava je po informacijskom izvoru. Informacijski izvor IDS sustava je zapravo onaj dio sustava koji IDS nadzire. S obzirom na to, razlikuju se mrežno bazirani *IDS (*engl. *network based-IDS),* host bazirani *IDS (*engl. *host-based IDS)* te aplikacijski bazirani IDS *(*engl. *application-based IDS)* koji je zapravo podvrsta host baziranog IDS sustava.

### 7.5.1. Mrežno bazirani IDS

Najčešća vrsta IDS sustava dostupna su mrežno bazirani IDS koji djeluju na načelu dohvaćanja i analiziranja mrežnih paketa. Mrežno bazirani IDS sustavi imaju senzore koji su postavljeni po određenim dijelovima mreže koji analiziraju promet lokalno te napade prijavljuju centralnoj jedinici. Dobro postavljen mrežni IDS može pokrivati veliki dio mreže na kojem se nalazi više hostova.

***Prednosti mrežno baziranog IDS-a:***

- Par dobro raspoređenih IDS sustava mogu pokriti cijelu mrežu.
- Vrlo laka implementacija u postojeću mrežu. IDS radi pasivno, što znači da samo osluškuje mrežu te nije potrebno uvelike mijenjati topologiju mreže.
- Lagano ih je osigurati od napada te su nevidljivi napadačima [1].

***Nedostatci mrežno baziranog IDS-a:***

- Mrežno bazirani IDS sustavi imaju poteškoće detektiranja napada u velikim mrežama i mrežama s puno mrežnog prometa. Pošto IDS analizira mrežne pakete u mreži s puno paketa IDS nije u stanju ih sve analizirati te su veće šanse da dođe do napada u velikim mrežama. Ovaj problem se može ublažiti ako je IDS implementiran hardverski a ne softverski pošto hardverski IDS je puno brži.
- Mnoge prednosti se ne odnose u modernim komutatorski-orijentiranim mrežama. Komutatori dijele mreže u manje segmente, ali većinom ne osiguravaju univerzalne portove zbog čega se nadzor na senzoru ograničava na samo jedan host.
- Mrežno bazirani IDS sustavi ne mogu analizirati kriptirane informacije. Ovo je problem u virtualnim privatnim mrežama jer u njima su sve informacije kriptirane.
- Većina mrežnih IDS sustava ne mogu razaznati je li napad bio uspješan. Ako dođe do napada administratori moraju pregledati svakog hosta ako se na njemu dogodio napad.
- Kod nekih IDS sustava dolazi do problema ako se pojavi napad s fragmentiranim paketima. Takvi paketi uzrokuju nestabilnost i cjelokupno rušenje IDS sustava [1].

### 7.5.2. Host bazirani IDS

Host bazirani IDS sustavi nadziru promet na pojedinim hostovima. Mogu biti instalirani na svakom hostu u sustavu. Host bazirani IDS sustavi se još mogu razlikovati s obzirom na korišteni izvor informacija. Ovdje se ubrajaju revizijski tragovi operacijskog sustava te sistemski logovi. Revizijski tragovi se generiraju u jezgri operacijskog sustava te su detaljniji i sigurniji od sistemskih logova, no sistemski logovi su kraći od zapisa operacijskog sustava te ih je ujedno i lakše za shvatiti.

***Prednosti Host baziranog IDS-a:***

- Host bazirani IDS sustavi mogu detektirati napade koje mrežno bazirani IDS sustavi ne mogu zahvaljujući praćenju događaja na lokalnom računalu na lokalnom računalu.

- Pošto imaju pristup podatkovnim datotekama i procesima sustava mogu otkriti ako je napada bio uspješan.
- Mogu djelovati u okruženju u kojem je mrežni promet kriptiran. To postižu sa analizom prometa prije nego što host kriptira ili nakon dekriptiranja nakon što paket dostigne na host.
- Host bazirani IDS sustavi nemaju problema u komutatorski orijentiranim mrežama.
- S provjerom integriteta softvera mogu se otkriti određeni tipovi malicioznih napada. Ovi se napadi pojavljuju kao neusklađenosti u izvršavanju procesa [1].

***Nedostatci Host baziranog IDS-a:***

- Teže upravljati s njim, pošto ga je potrebno konfigurirati na svakom hostu zasebno.
- Pošto se izvor informacija nalazi na samome hostu u slučaju napada i sam IDS može biti onesposobljen.
- Nemaju sliku cijele mreže pošto vide samo pakete koji dostignu i koje pošalje sam host.
- Mogu biti onesposobljeni sa DOS (engl. *denial of service*) napadima.
- Može doći do pada performansi na samom hostu pošto IDS koristi resurse tog hosta [1].

### 7.5.3. Aplikacijski bazirani IDS

Aplikacijski bazirani IDS predstavlja specifičnu podvrstu host baziranog IDS sustava koja se fokusira na analizu događaja unutar pojedinih programskih aplikacija. Ovaj pristup omogućuje dublju i precizniju analizu sigurnosnih aspekata unutar aplikacija te identifikaciju potencijalnih prijetnji ili nepravilnosti koje se mogu pojaviti unutar njih.

Ključna komponenta aplikacijskog baziranog IDS sustava su aplikacijske transakcijske log datoteke koje služe kao izvor informacija za analizu. Ove log datoteke sadrže zapis o svakoj transakciji ili aktivnosti unutar aplikacije, uključujući pristup podacima, upite baze podataka, komunikaciju s drugim aplikacijama i korisničke interakcije.

Analizom ovih logova IDS može identificirati neobične ili sumnjive aktivnosti, što može ukazivati na pokušaj neovlaštenog pristupa ili druge sigurnosne prijetnje.

***Prednosti aplikacijski baziranog IDS-a:***

- Mogu pratiti interakciju između korisnika i aplikacije, što im često omogućuje praćenje neovlaštene aktivnosti do pojedinih korisnika.
- Često mogu raditi u kriptiranim okruženjima, budući da se povezuju s aplikacijom na krajevima transakcija, gdje se informacije prikazuju korisnicima u ne kriptiranim oblicima [1].

***Nedostatci aplikacijski baziranog IDS-a:***

- Mogu biti ranjiviji od host baziranih IDS sustava na napade jer zapisi aplikacija nisu jednako dobro zaštićeni zapisi operacijskog sustava.
- Ne mogu detektirati maliciozne skripte ili druge napade koji uključuju mijenjanje softvera [1].

## 7.6. IDS Analiza

IDS analiza predstavlja način na koji IDS sustavi analiziraju prikupljene informacije. Pri tome se razlikuju dvije osnovne kategorije pristupa: Detekcija zlouporabe (engl. *misuse detection*) i Otkrivanje nepravilnosti (engl. *anomaly detection*).

### 7.6.1. Detekcija zlouporabe

Svaki napad je specifičan po svom cilju i načinu izvršavanja. Jednom kada je napad izvršen, ostavlja se specifičan trag u obliku tzv. potpisa. Potpisi se pohranjuju u liste IDS sustava, koji se potom koriste pri analizi paketa te se usporednom metodom traženja sličnosti utvrđuje postojanja napada. Ovaj način detekcije se još naziva detekcija bazirana na potpisu (engl. *signature-based detection*).

***Prednosti detekcije zloupotrebe:***

- Velika efikasnost pri otkrivanju napada.

- Brzo i pouzdano dijagnosticiranje korištenja određenog alata ili tehnike izvršavanja napada. Ovo može pomoći administratorima da prioritiziraju korektivne mjere.
- Omogućava administratorima praćenje sigurnosnih problema na njihovim sustavima te pokretanje postupaka rješavanja incidenata [1].

***Nedostatci detekcije zloupotrebe:***

- Mogu detektirati samo one napade čiji su potpisi na listi potpisa.
- Detektori zlouporabe dizajnirani su tako da koriste čvrsto definirane potpise koji ih sprječavaju da otkriju varijante uobičajenih napada [1].

### 7.6.2. Otkrivanje nepravilnosti

Kod otkrivanja nepravilnosti u informacijskim sustavima, detektori se usmjeravaju na identifikaciju tragova ili aktivnosti koje se razlikuju od očekivanog normalnog ponašanja. Ovaj pristup koristi se kako bi se otkrile potencijalne prijetnje, napadi ili nepravilnosti u radu sustava. Detektori za otkrivanje nepravilnosti, dok sustav normalno funkcionira, prikupljaju informacije o aktivnostima korisnika i konstruiraju profile koji se temelje na njihovom uobičajenom ponašanju u okruženju mreže. Ovi profili uključuju obrasce pristupa podacima, učestalost aktivnosti, vremenske obrasce, i druge karakteristike koje se smatraju normalnima za svakog korisnika. Međutim, ovaj način rada može generirati lažne uzbune, odnosno detekcije koje nisu povezane s prijetnjama. Na primjer, korisnici mogu povremeno promijeniti svoje radne obrasce, eksperimentirati s novim aplikacijama ili promijeniti način pristupa sustavu. Ovi nesavršeni aspekti ljudskog ponašanja mogu rezultirati lažnim alarmima jer se korisnici ponekad ponašaju nepredvidljivo. Da bi se smanjio broj lažnih pozitivnih alarmi, detektori za otkrivanje nepravilnosti često koriste napredne tehnike strojnog učenja kako bi bolje razumjeli kontekst i promjene u ponašanju korisnika

***Prednosti otkrivanja nepravilnosti:***

- Mogućnost detektiranja novih tipova napada bez posjedovanja specifičnog znanja o tim napadima.
- Detektori nepravilnosti mogu proizvesti informacije koje se zatim mogu koristiti za definiranje potpisa za detekciju zlouporabe [1].

***Nedostatci otkrivanja nepravilnosti:***

- Detektori nepravilnosti obično proizvode veliki broj lažnih alarma zbog nepredvidivih ponašanja korisnika i mreže.
- Detektori nepravilnosti zahtijevaju puno vremena za „trening“ tijekom normalnog rada mreže da karakteriziraju normalno ponašanje korisnika i mreže [1].

## 7.7. Reakcija IDS-a

Kada se IDS konfrontira s potencijalnim napadom, generira odgovor kako bi reagirao na prijetnju. Ti odgovori mogu biti pasivni, u obliku obavijesti ili zabilježenih informacija te aktivni, uključujući automatske korake za zaustavljanje ili suzbijanje napada radi zaštite sustava.

### 7.7.1. Pasivni odgovori

Kod pasivnih odgovora IDS šalje obavijest te ne poduzima nikakve druge mjere protiv napada.

- *Alarmi i obavijesti* - Šalje obavijest administratorima da je napad u tijeku ili se već dogodio. Najčešći oblik alarma je prikaz upozorenja na ekranu ili skočnog prozora. Informacije koje se pružaju u poruci alarma mogu uključivati jednostavne informativne poruke poput obavijesti da je došlo do provale, sve do detaljnih izvještaja koji opisuju IP adrese izvora i specifičan alat za napad koji je korišten za dobivanje pristupa te ishod napada.
- *SNMP zamke i dodaci* - Neki IDS sustavi imaju mogućnost slanja SNMP poruka centralnim konzolama [1].

### 7.7.2. Aktivni odgovori

Aktivni odgovori IDS sustava su automatske radnje poduzete kada se otkriju određene vrste napada. Ovdje se misli o IPS-ovima te postoje tri kategorije aktivnih odgovora.

*Prikup dodatnih informacija:*

Podizanjem osjetljivosti informacijskih izvora mogu se otkriti informacije poput otkrivanja ako je napad u tijeku ili je već završen. Ova opcija također omogućuje organizaciji prikupljanje informacija koje se mogu koristiti za podršku istrazi i uhićenju napadača [1].

*Promjena napadnutog okruženja:*

Ovdje je cilj zaustavljanje napada u tijeku. To se može postići blokiranjem izvorišnih IP adresa napadača, blokiranjem mrežnih portova, protokola ili servisa koje koristi napadač te u ekstremnim slučajevima prekidanje veza koje koristi određeno mrežno sučelje [1].

*Djelovanje protiv uljeza:*

Ovdje se uključuje pokretanje protunapada na napadača ili prikupljanje informacija o okruženju i opremi s kojom se napadaš koristi[1].

### 7.7.3. Izvještavanje i sposobnost arhiviranja

Većina, ako ne i svi komercijalni IDS sustavi nude opciju stvaranja redovitih izvješća i drugih detaljnih informativnih dokumenata. Određeni od njih mogu proizvesti izvješća o događajima u sustavu i otkrivenim upadima tijekom određenog razdoblja izvješćivanja, poput tjedna ili mjeseca. Drugi pružaju statistike ili dnevnike generirane od strane IDS-a u formatima koji su prikladni za integraciju u baze podataka ili za uporabu u softverskim alatima za generiranje izvješća.[1]

# 8. Napadi i ranjivosti

Iako IDS sustavi pružaju važnu razinu zaštite za informacijske sustave, njihova učinkovitost ovisi o kompetentnim osobama koje su u stanju upravljati njima. To uključuje poznavanje ne samo samog sustava koji se štiti, već i razumijevanje različitih vrsta napada, napadačkih tehnika i metoda kako bi se adekvatno osigurala zaštita sustava od potencijalnih prijetnji.

## 8.1. Vrste napada

Unatoč raznolikim sposobnostima računalnih napada, obično rezultiraju kršenjem samo četiri različita sigurnosna svojstva:

- *Povjerljivost* - Napad uzrokuje narušavanje povjerljivosti ako omogućuje napadačima pristup podacima bez odobrenja vlasnika informacija.
- *Integritet* - Napad uzrokuje narušavanje integriteta ako omogućuje napadaču promjenu stanja sustava ili bilo kojih podataka koji se nalaze na ili prolaze kroz sustav.
- *Dostupnost* - Napad uzrokuje narušavanje dostupnosti ako sprječava ovlaštenog korisnika da pristupi određenom resursu sustava kada, gdje i u obliku u kojem im je potreban.
- *Kontrola* - Napad uzrokuje narušavanje kontrole ako dodjeljuje napadaču privilegiju koja krši politiku kontrole pristupa sustava. Ta privilegija omogućuje kasnije narušavanje povjerljivosti, integriteta ili dostupnosti [1].

## 8.2. Vrste napada koje IDS otkriva

Postoje tri vrste napada koje IDS najčešće otkriva. To su: skeniranje sustava (engl. *System scanning*), uskraćivanje usluge (engl. *Denial of service*) i prodor u sustav (engl. *System penetration*).

### 8.2.1. Skeniranje sustava

Skenirajući napad se događa kada napadač istražuje ciljnu mrežu ili sustav slanjem različitih vrsta paketa. Koristeći primljene odgovore od sustava koji se skenira napadač može saznati mnoge karakteristike i ranjivosti sustava. Ovim napadom mogu se otkriti određene

informacije o ciljnom sustavu poput: topologije mreže, vrste mrežnog prometa koji su dopušteni kroz vatrozid, broj aktivnih hostova u mreži, operativne sustave na hostovima, serverski softver pokrenut na hostovima, brojevi verzija softvera za sve otkrivene softvere [3].

### 8.2.2. Uskraćivanje usluge

Cilj napada uskraćivanja usluge ili DOS napada je usporavanje i rušenje mrežnih sustava. Ovdje raspoznajemo dvije vrste DOS napada.

- *DOS napadi iskorištavanjem slabosti* - Ovi napadi iskorištavaju slabost u ciljanom sustavu te uzrokuju neuspjeh obrade ili iscrpljivanje sistemskih resursa. Najčešći primjer je „Ping of death“. Ovaj napad uključuje slanje velikog broja paketa određenim Windows sustavima. Ciljani sustav nije u mogućnosti obraditi ovoliki ogromni broj paketa što uzrokuje rušenje sustava. Jednostavno ažuriranje softvera može zaobići ovu vrstu napada.
- *DOS napadi preplavljivanjem* - Ova vrsta napada radi tako da ciljni sustav preplavi ogromnom količinom podataka, većom nego što sustav može podnijeti. Kod ovih napada, ne postoji mana u ciljnom sustavu koja se može zakrpati. DDOS napadi koriste više od jednog računala za lansiranje napada [1].

### 8.2.3. Prodor u sustav

Napadi prodora u sustav ili penetracijski napadi uključuju neovlašteno stjecanje i/ili promjenu privilegija, resursa ili podataka sustava.

Najčešće vrste penetracijskih napada su:

- *User to root* - Lokalni korisnik na hostu dobiva potpunu kontrolu nad tim hostom.
- *Remote to user* - Napadač na mreži dobiva pristup korisničkom računu na ciljnom hostu.
- *Remote to Root* - Napadač na mreži dobiva potpunu kontrolu nad ciljnim hostom.

- *Remote Disk Read* - Napadač na mreži dobiva sposobnost čitanja privatnih datoteka s podacima na ciljnom hostu bez odobrenja vlasnika.
- *Remote Disk Write* - Napadač na mreži dobiva sposobnost pisanja u privatne datoteke s podacima na ciljnom hostu bez odobrenja vlasnika [1].

## 8.3. Vrste računalnih ranjivosti

Mnogi IDS sustavi pružaju detaljne opise detektiranih napada, uključujući informacije o vrsti ranjivosti koju napadač iskorištava. Ova dodatna informacija omogućuje administratorima da nakon napada istraže i poprave iskorištene ranjivosti, čime se povećava razina sigurnosti sustava.

### 8.3.1. Ulazne validacijske pogreške

Ulazne validacijske pogreške predstavljaju ozbiljnu ranjivost u aplikacijama i sustavima jer omogućavaju potencijalnim napadačima da iskoriste neispravno provjerene unose kako bi izazvali neželjene posljedice. To znači da se sustav neadekvatno nosi s unosima koji nisu u skladu s očekivanim ili sigurnosnim standardima, otvarajući vrata za potencijalne napade ili neovlašten pristup podacima ili funkcionalnostima. Poznate su dvije vrste ulaznih validacijskih pogrešaka.

#### 8.3.1.1. Preljev međuspremnika

Preljev međuspremnika (engl. *Buffer overflow*) predstavlja ozbiljnu ranjivost u softveru gdje sustav ne provjerava duljinu unosa, što omogućava napadačima da prelijevanjem spremnika (engl. *buffer*) za unos u memoriji izvrše zlonamjerne naredbe. Ova ranjivost se može iskoristiti pametnom manipulacijom unosa kako bi se izazvalo neželjeno izvršavanje koda ili izvođenje zlonamjernih operacija, što može ozbiljno ugroziti sigurnost sustava.

#### 8.3.1.2. Pogreške rubnih uvjeta

Pogreške rubnih uvjeta predstavljaju ranjivosti koje se javljaju kada uneseni podaci uzrokuju prekoračenje pretpostavljene granice ili ograničenja, što može rezultirati ozbiljnim problemima za sustav. Na primjer, takvi greške mogu dovesti do iscrpljivanja resursa poput memorije, prostora na disku ili propusnosti mreže, što može uzrokovati disfunkcionalnost sustava i potencijalne posljedice po njegovu sigurnost i stabilnost.

### 8.3.2. Pogreške kontrole pristupa

Pogreške kontrole pristupa (engl. *Access validation error*) predstavljaju ranjivosti koje se pojavljuju kada je mehanizam kontrole pristupa u sustavu neispravan i ne uspijeva pravilno provjeriti ovlasti korisnika ili entiteta koji pokušavaju pristupiti određenim resursima ili funkcionalnostima. Ova vrsta ranjivosti ne ovisi o konfiguraciji koju korisnik može kontrolirati, već je povezana s temeljnim mehanizmom samog sustava, što znači da je nasljedna i potencijalno ozbiljna. Pogreške kontrole pristupa mogu omogućiti neovlaštenim korisnicima ili entitetima pristup osjetljivim podacima, sistemskim resursima ili funkcionalnostima koje bi inače trebali biti zaštićeni. To može dovesti do ozbiljnih sigurnosnih incidenata i potencijalnih gubitaka povjerljivosti, integriteta i dostupnosti podataka. Stoga je od velike važnosti da se takve ranjivosti prepoznaju i isprave kako bi se osigurala adekvatna kontrola pristupa i očuvanje sigurnosti sustava.

### 8.3.3. Pogreške upravljanja iznimkama

Pogreške upravljanja iznimkama predstavljaju ranjivosti koje se pojavljuju kada sustav nepravilno ili neadekvatno obrađuje iznimne situacije ili pogreške koje se dogode tijekom izvršavanja. Ovakve greške mogu otvoriti potencijalne sigurnosne rupe jer napadači mogu zlonamjerno iskoristiti taj neispravni postupak obrade iznimnih stanja kako bi izazvali neželjene posljedice ili pokušali izvesti napade. Stoga je ključno da sustavi adekvatno i sigurno upravljaju iznimnim stanjima kako bi se minimalizirala ranjivost i očuvala integritet i sigurnost sustava.

### 8.3.4. Pogreške okoline

Pogreške okoline (engl. *Environmetal error*) predstavljaju ranjivosti koje proizlaze iz neočekivanih ili nepredvidljivih interakcija između sustava, aplikacija ili komponenti u određenoj okolini. Ovakve greške mogu rezultirati nepravilnim ponašanjem sustava ili aplikacija, otvarajući mogućnost za različite vrste napada ili sigurnosnih problema. Važno je prepoznati i upravljati takvim pogreškama kako bi se osigurala stabilnost i sigurnost sustava u različitim okruženjima.

### 8.3.5. Konfiguracijske pogreške

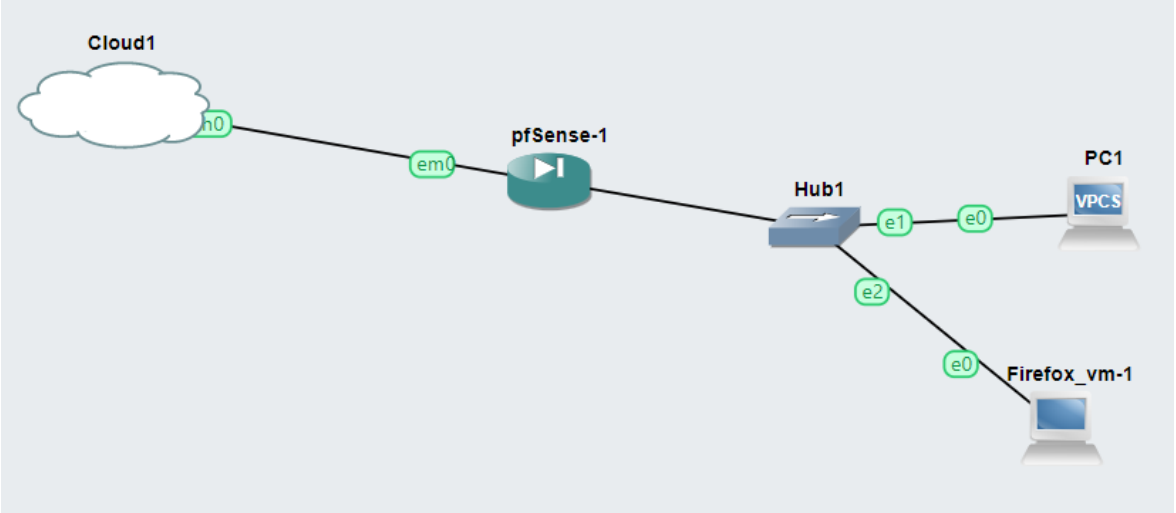
Konfiguracijske pogreške (engl. *Configuration error*) predstavljaju ozbiljnu prijetnju sigurnosti informacijskog sustava, a javljaju se kada korisnici ili administratori nepravilno konfiguriraju sustav, postavke ili aplikacije. Ova vrsta ranjivosti ne proizlazi iz samog dizajna sustava, već iz ljudske greške u procesu postavljanja i konfiguracije. Takve greške u konfiguraciji mogu omogućiti potencijalnim napadačima neovlašteni pristup sustavu, izazvati nesigurnosti u postavkama pristupa podacima ili drugim osjetljivim resursima te rezultirati ozbiljnim sigurnosnim incidentima. Stoga je ključno provesti detaljnu i točnu konfiguraciju sustava kako bi se minimalizirala mogućnost takvih pogrešaka i osigurala sigurnost informacijskog okruženja.

### 8.3.6. Race Condition

Race condition predstavlja ranjivost koja se javlja kada postoji odgoda između trenutka kada sustav provjerava dopuštenost operacije prema sigurnosnom modelu i trenutka kada sustav stvarno izvršava tu operaciju. Pravi problem nastaje kada se okolina ili kontekst promijeni između ta dva trenutka, što rezultira situacijom u kojoj sigurnosni model više ne dopušta operaciju koja se izvršava. Napadači često iskorištavaju ovu malu priliku kako bi manipulirali sustavima i prisilili ih da izvrše nedopuštene operacije, poput pisanja u osjetljive datoteke, dok su u visoko privilegiranom stanju. Ova vrsta ranjivosti zahtijeva posebnu pažnju i pravilno upravljanje kako bi se spriječila mogućnost zloupotrebe i očuvala sigurnost sustava.

# 9. Primjer implementacije Snort IDS sustava

Pomoću GNS3 poslužitelja je moguće implementirati Snort IDS sustav. Primjer arhitekture koja će se koristiti je prikazana na slici 1.




*Slika 5. Arhitektura GNS3 sustava [3]*

Cloud je mrežno sučelje koje omogućuje pristup lokalnim računalnim resursima na Veleučilištu.

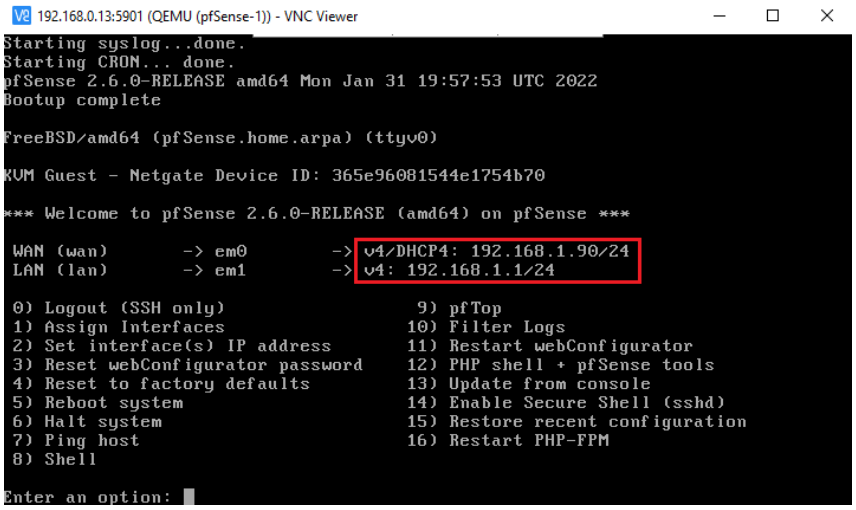
Pfsense je usmjeritelj s postavljenim WAN i LAN sučeljima, opremljen sustavom Snort za otkrivanje i prevenciju napada pomoću kojega će se detektirati napad.

PC1 je generičko računalo za kontrolu DHCP usluge.

Ethernet hub se koristi za stvaranje virtualne kopije mrežnog prometa koji se generira na drugim računalima unutar iste mrežne podmreže kako bi se omogućila njegova analiza i inspekcija.

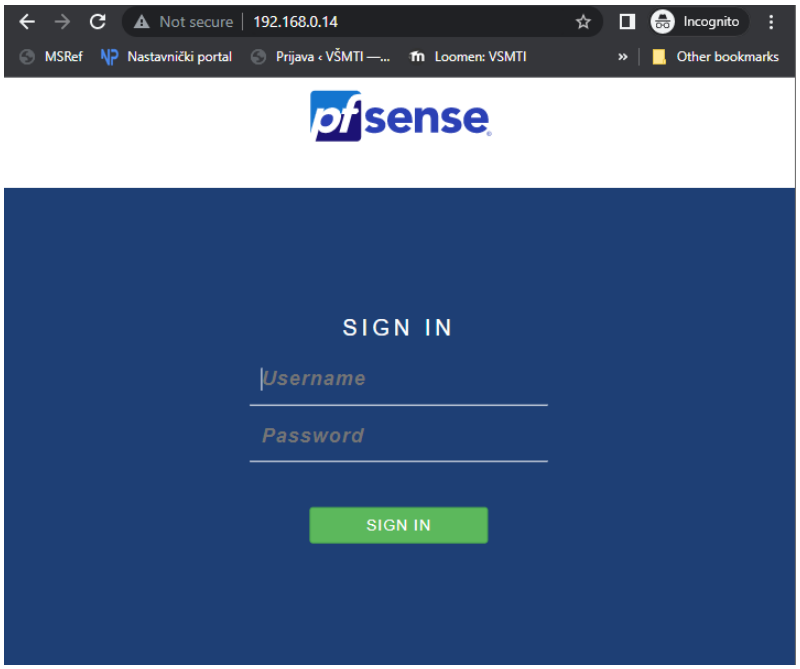
Firefox_vm-1 je virtualizirana instanca sustava TinyCore Linux operacijskog sustava s unaprijed instaliranim preglednikom Firefox.

Slika 2. pokazuje aplikaciju VNC Viewer pomoću koje se može povezati na element pfSense pomoću IP adrese i porta prikazanog na aplikaciji GNS3.




*Slika 6. VNC Viewer [3]*

Na temelju očitane IP adrese uz pomoć aplikacije VNC Viewer ostvaren je pristup grafičkom sučelju pfSense kao na sljedećoj slici.



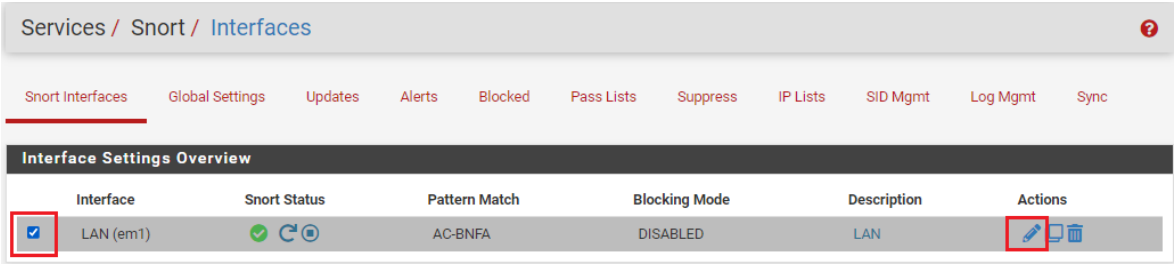

*Slika 7. pfSense grafičko sučelje [3]*

Unutar sustava pfSense vatrozida prethodno je instaliran i podešen Snort IDS sustav.

Za primjer napada koristitio se program zvan Nmap. Nmap je alat za skeniranje mreže otvorenog koda koji se koristi za otkrivanje uređaja, otvorenih portova i prikupljanje informacija o mrežama. Pomaže mrežnim administratorima i stručnjacima za sigurnost ocijeniti sigurnost mreže, identificirati potencijalne ranjivosti i mapirati resurse mreže.

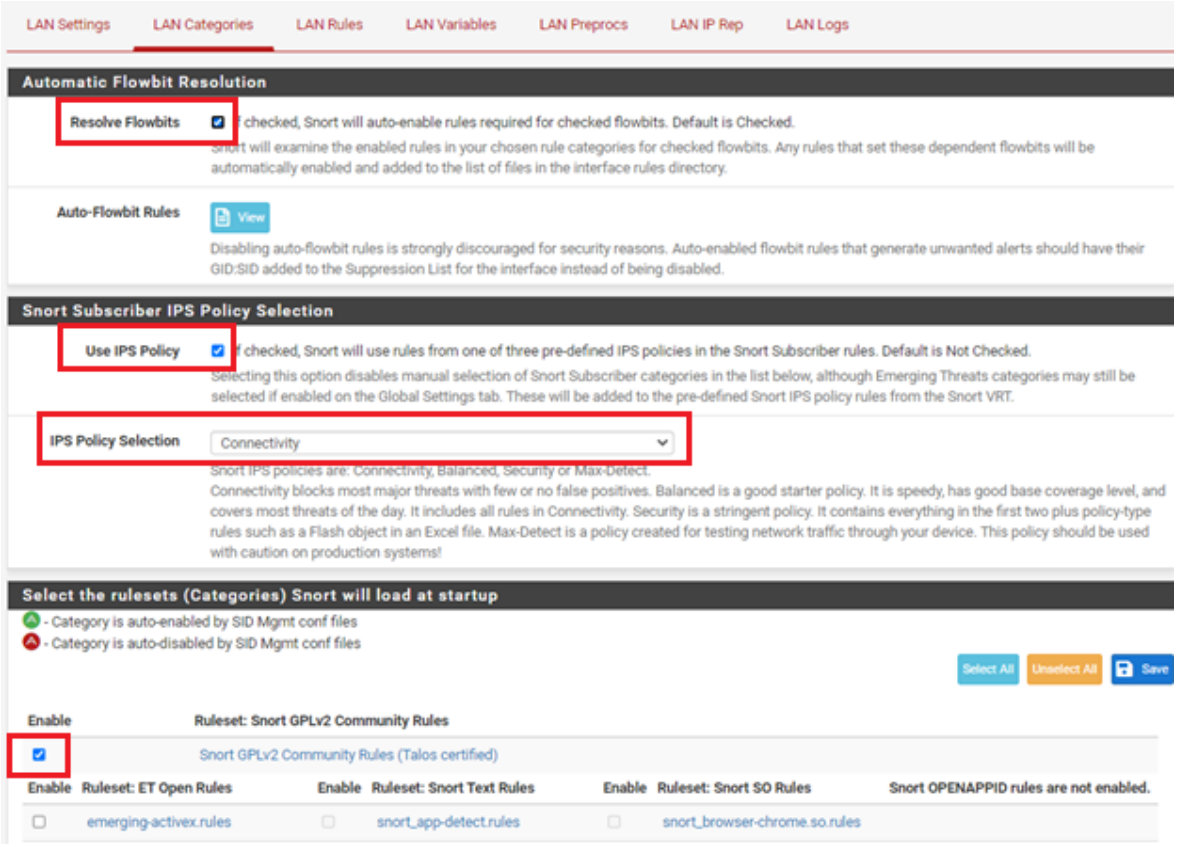
Snort je IDS alat koji omogućuje nadzor mrežnog prometa u stvarnom vremenu radi identifikacije potencijalnih napada i zlonamjernih aktivnosti. Ovaj alat koristi se za analizu mrežnih paketa i usporedbu njihovog sadržaja s pravilima ili potpisima koji definiraju poznate prijetnje. To ga čini učinkovitim u otkrivanju napada poput napada za uskraćivanje usluge ili napada s potpisima. Sniffer način rada omogućuje Snortu da pasivno "promatra" ili "osluškuje" promet na mreži, ali ne djeluje na njega. U ovom načinu rada Snort analizira dolazne mrežne pakete i provjerava ih protiv definiranih pravila i potpisa kako bi identificirao potencijalne prijetnje. Međutim, ne poduzima aktivne akcije za sprječavanje tih prijetnji. Sniffer mod koristan je za pasivno praćenje i analizu mrežnog prometa radi uočavanja potencijalnih problema i izvještavanja o njima, ali ne štiti mrežu odmah. Packet Logger način rada omogućuje Snortu da bilježi informacije o mrežnim paketima koji prolaze kroz mrežu. Umjesto aktivne analize i otkrivanja prijetnji, ovaj način rada fokusira se na pohranu informacija o svakom paketu, uključujući izvor, odredište, vrijeme i druge metapodatke. Ova vrsta rada korisna je za vođenje evidencije o mrežnom prometu radi kasnije analize ili za pridržavanje zakonskih zahtjeva o zadržavanju podataka [4].

U zaglavlju grafičkog sučelja pfsense potrebno je kliknuti na Services kategoriju, a zatim na opciju Snort. Nakon toga, sučelje LAN treba označiti potvrdnom kvačicom i kliknuti na dugme Edit, kako je prikazano na sljedećoj slici.




*Slika 8. Sučelje [3]*

U izborniku koji je prikazan, odabrati potkategoriju LAN Categories. Aktivirati IPS pravilo nazvano Connectivity, koje uključuje pravila za blokiranje u najčešćim scenarijima upotrebe. Označiti opcije koje su prikazane na priloženoj slici i potvrditi promjene klikom na dugme za spremanje.

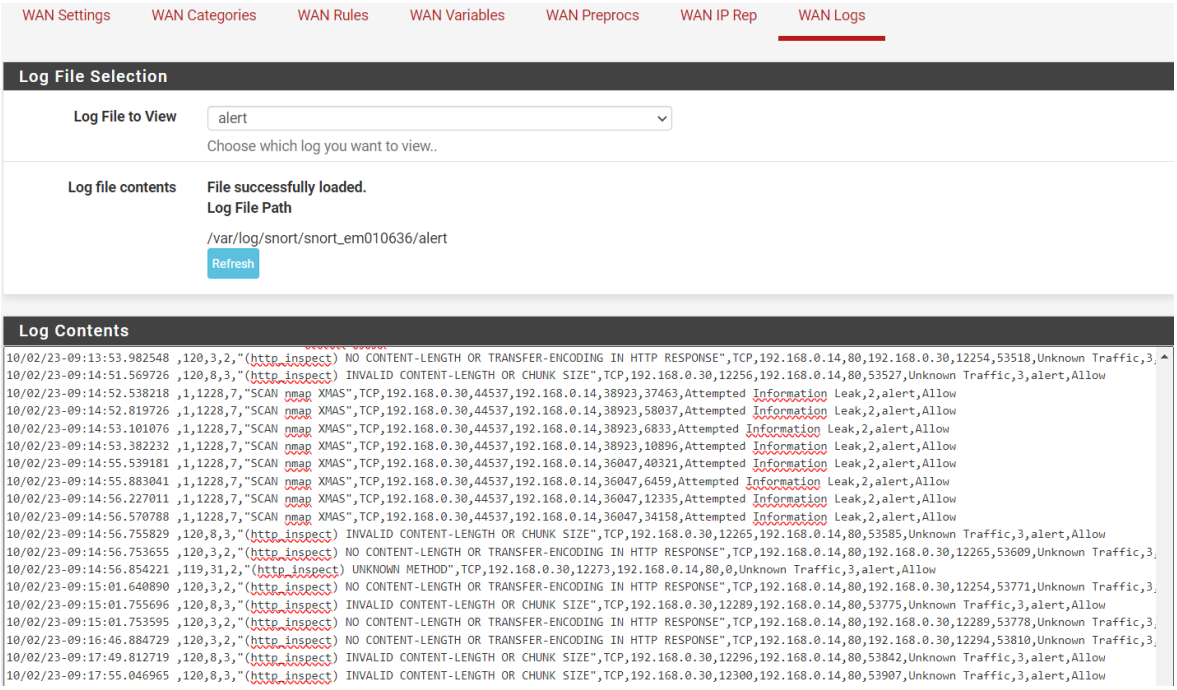



*Slika 9. Konfiguracija pravila [3]*

Pošto Snort sustav već ima podešena pravila potrebno je samo pokrenuti skeniranje iz aplikacije Nmap kao što je prikazano na slici 6.


*Slika 10. Nmap skeniranje*

Kada se naredba izvrši pod kategorijom WAN Logs može se vidjeti obavijest za mogući napad kao što je prikazano na slici 7.




*Slika 11. Obavijest o napadu*

# 10. Zaključak

Sustavi za detekciju i prevenciju upada predstavljaju nezaobilazan dio mrežne sigurnosti. Njihova uloga u prepoznavanju ranjivosti i suzbijanju potencijalno štetnih aktivnosti ključna je za očuvanje sigurnosti. Ubrzan tehnološki razvoj zahtijeva kontinuiranu evoluciju ovih sustava kako bi se adekvatno odgovorilo izazovima sve sofisticiranijih prijetnji. Opisom arhitekture i različitih načina na koji su IDS sustavi izvedeni, dobiveno je znanje o njihovim razlikama i sličnostima te prednostima i nedostatcima. Kroz praktični primjer preko Snort IDS sustava je pokazano kako IDS sustav analizira pakete u mrežnom sustavu te po unaprijed određenim pravilima generira obavijesti ako dođe do podudaranja između pravila i sadržaja paketa. Preko ovog primjera može se dobiti uvid u važnost IDS sustava u sprječavanju napada u složenijim mrežnim sustavima i protiv složenijih napada.

# Literatura

[1] Intrusion Detection Systems Rebecca Bace and Peter Mell, Pristupljeno 3.11.2023 [Online]. Dostupno na: https://www.researchgate.net/publication/2943853_Intrusion_Detection_Systems

[2] Detekcija upada u sustav Nikolina Pavković (2007) Pristupljeno 3.11.2023 [Online]. Dostupno na: http://sigurnost.zemris.fer.hr/ns/2007_pavkovic/IDS.html

[3] Sustavi za detekciju sigurnosnih proboja (SNORT IDS) Enes Ciriković

[4] CIS-DOC-2011-10-028 Snort IDS Pristupljeno 3.11.2023 [Online]. Dostupno na: https://www.cis.hr/files/dokumenti/CIS-DOC-2011-10-028.pdf

# Popis slika

Veleučilište u Virovitici

**OBRAZAC 5**

**IZJAVA O AUTORSTVU**

Ja, Dorian Mlinar

izjavljujem da sam autor/ica završnog/diplomskog rada pod nazivom

Sustavi za detekciju i prevenciju upada

Svojim vlastoručnim potpisom jamčim sljedeće:

- da je predani završni/diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija,
- da su radovi i mišljenja drugih autora/ica, koje sam u svom radu koristio/la, jasno navedeni i označeni u tekstu te u popisu literature,
- da sam u radu poštivao/la pravila znanstvenog i akademskog rada.

**Potpis studenta/ice**

Dorian Mlinar

Veleučilište u Virovitici

**OBRAZAC 6**

**ODOBRENJE ZA OBJAVLJIVANJE ZAVRŠNOG/DIPLOMSKOG RADA U DIGITALNOM REPOZITORIJU**

Ja, Dorian Mlinar
dajem odobrenje za objavljivanje mog autorskog završnog/diplomskog rada u nacionalnom repozitoriju odnosno repozitoriju Veleučilišta u Virovitici u roku od 30 dana od dana obrane.

Potvrđujem da je za pohranu dostavljena završna verzija obranjenog završnog/diplomskog rada.

Ovom izjavom, kao autor navedenog rada dajem odobrenje i da se moj rad, bez naknade, trajno javno objavi i besplatno učini dostupnim na sljedeći način (zaokružiti):

a) Rad u otvorenom pristupu
b) Rad dostupan nakon: _____ (upisati datum)
c) Pristup svim korisnicima iz sustava znanosti i visokog obrazovanja RH
d) Pristup korisnicima matične ustanove
e) Rad nije dostupan (*u slučaju potrebe dodatnog ograničavanja pristupa Vašem završnom/diplomskom radu, podnosi se pisani obrazloženi zahtjev*).

U slučaju dostupnosti rada prethodno označeno od a) do d), ovom izjavom dajem pravo iskorištavanja mog ocjenskog rada kao autorskog djela pod uvjetima Creative Commons licencije (zaokružiti):

1) CC BY (Imenovanje)
2) CC BY-SA (Imenovanje – Dijeli pod istim uvjetima)
3) CC BY-ND (Imenovanje – Bez prerada)
4) CC BY-NC (Imenovanje – Nekomercijalno)
5) CC BY-NC-SA (Imenovanje – Nekomercijalno – Dijeli pod istim uvjetima)
6) CC BY-NC-ND (Imenovanje – Nekomercijalno – Bez prerada)

Ovime potvrđujem da mi je prilikom potpisivanja ove izjave pravni tekst licencija bio dostupan te da sam upoznat s uvjetima pod kojim dajem pravo iskorištavanja navedenog djela.

**Potpis studenta/ice**

Dorian Mlinar