Implementacija sigurne mrežne arhitekture

Rupić, Željka

VELEUČILIŠTE U ŠIBENIKU

ODJEL POSLOVNE INFORMATIKE

PRIJEDIPLOMSKI STRUČNI STUDIJ POSLOVNE INFORMATIKE

Željka Rupić

IMPLEMENTACIJA SIGURNE MREŽNE ARHITEKTURE

Završni rad

Šibenik, 2024.

VELEUČILIŠTE U ŠIBENIKU

ODJEL POSLOVNE INFORMATIKE

PRIJEDIPLOMSKI STRUČNI STUDIJ POSLOVNE INFORMATIKE

Željka Rupić

IMPLEMENTACIJA SIGURNE MREŽNE ARHITEKTURE

Završni rad

Kolegij: Zaštita i sigurnost informacijskih sustava

Mentor: Zvonimir Klarin, mag.ing.comp., pred.

Studentica: Željka Rupić

Matični broj studentice: 1219065093

Šibenik, rujan 2024.

TEMELJNA DOKUMENTACIJSKA KARTICA

Veleučilište u Šibeniku Završni rad

Odjel Poslovne informatike

Stručni prijediplomski studij Poslovne informatike

IMPLEMENTACIJA SIGURNE MREŽNE ARHITEKTURE

ŽELJKA RUPIĆ

Ivana Gundulića 39, Šibenik; zeljka.rupic7@gmail.com

U radu su obrađeni temeljni koncepti računalnog umrežavanja, uključujući topologije, infrastrukturu, mrežne uređaje te sigurnosne politike i rješenja ključna za zaštitu podataka. Pravilnim odabirom mrežnih topologija, uređaja kao što su usmjernici, preklopnici i vatrozidi te pravilnim adresiranjem osigurava se učinkovitost upravljanja mrežnim prometom i kontrola pristupa osjetljivim podacima, što doprinosi stabilnosti i sigurnosti mrežne infrastrukture. Nadalje, rad se fokusira na sigurnosne protokole koji omogućuju enkripciju, autentikaciju i udaljeni pristup kako u žičnim tako i u bežičnim mrežama. Dizajn mreže uključuje i fizičke i logičke elemente koji omogućuju segmentaciju i definiranje sigurnosnih zona, temeljeno na načelima povjerljivosti, integriteta i dostupnosti (CIA trijada) kako bi se postigla optimalna zaštita mrežnog sustava. Praktični dio rada uključuje implementaciju i testiranje *Snort* alata kao sustava za otkrivanje i sprječavanje napada (engl. *Intrusion Detection and Prevention System, IDS/IPS*) u simuliranom okruženju. Rezultati testiranja pokazuju učinkovitost *Snort* alata u detekciji potencijalnih napada i pružaju smjernice za daljnje unaprjeđenje mrežne sigurnosti.

(41 stranica / 19 slika / 3 tablice / 18 literaturnih navoda / jezik izvornika: hrvatski)

Rad je pohranjen u digitalnom repozitoriju Knjižnice Veleučilišta u Šibeniku

Ključne riječi: računalno umrežavanje, mrežna segmentacija, sigurnosni protokoli, sustavi za otkrivanje i sprječavanje napada, sigurnosne zone

Mentor: Zvonimir Klarin, mag.ing.comp., pred.

Rad je prihvaćen za obranu dana: 10.9.2024.

BASIC DOCUMENTATION CARD

Šibenik University of Applied Sciences Bachelor's thesis
Department of Business informatics
Undergraduate professional study of Business informatics

IMPLEMENTATION OF SECURE NETWORK ARCHITECTURE

ŽELJKA RUPIĆ
Ivana Gundulića 39, Šibenik; zeljka.rupic7@gmail.com

The paper discusses the fundamental concepts of computer networking, including topologies, infrastructure, network devices, as well as security policies and solutions crucial for data protection. The proper selection of network topologies, devices such as routers, switches, and firewalls, and appropriate addressing ensures efficient network traffic management and access control to sensitive data, which contributes to the stability and security of network infrastructure. Furthermore, the paper focuses on security protocols that enable encryption, authentication, and remote access for both wired and wireless networks. Network design includes both physical and logical elements that enable segmentation and the definition of security zones, based on the principles of confidentiality, integrity, and availability (CIA triad), to achieve optimal protection of the network system. The practical part of the paper involves the implementation and testing of the Snort tool as an Intrusion Detection and Prevention System (IDS/IPS) in a simulated environment. The test results demonstrate the effectiveness of the Snort tool in detecting potential intrusions and provide guidelines for further improvement of network security.

(41 pages / 19 figures / 3 tables / 18 references / original in Croatian language)
Thesis deposited in Šibenik University of Applied Sciences Library digital repository
Keywords: computer networking, network segmentation, security protocols, intrusion detection and prevention systems, security zones
Supervisor: Zvonimir Klarin, mag.ing.comp., lect.
Paper accepted: 10.9.2024.

SADRŽAJ

1. UVOD

U današnjem digitalnom dobu računalne mreže predstavljaju ključni dio suvremenih informacijskih sustava, omogućujući komunikaciju i razmjenu informacija između računala, uređaja i korisnika širom svijeta. One predstavljaju osnovnu infrastrukturu na kojoj se temelje sve poslovne i obrazovne aktivnosti, zdravstvene usluge te brojni drugi sektori.

S razvojem tehnologije, sigurnost računalnih mreža nameće se kao ključni segment naše svakodnevnice jer napadi na mreže i podatke postaju sve učestaliji i sofisticiraniji. Mrežna sigurnost ima ključnu ulogu u zaštiti osjetljivih podataka i osigurava nesmetan rad informacijskih sustava. Kibernetički kriminal koristi različite tehnike i alate za neovlašteni pristup mrežama, krađu podataka, prekid usluga te nanošenje raznih vrsta štete. Stoga je uvođenje i primjena snažnih sigurnosnih smjernica i alata nužno. Ključne mjere uključuju šifriranje podataka, redovito ažuriranje sustava i, prije svega, kontinuiranu edukaciju krajnjih korisnika.

Ovaj rad analizira osnovne karakteristike računalnih mreža, uključujući topologije, mrežne uređaje i metode adresiranja. Također se istražuju sigurnosni protokoli koji se koriste za zaštitu podataka tijekom prijenosa i čije je poznavanje ključno za dizajniranje i upravljanje mrežama. Rad također naglašava važnost sigurnosti i dizajna mrežne strukture kao ključnih elemenata za zaštitu podataka i pouzdanost mrežnih operacija. Uvođenje sigurnosnih politika, segmentacija mreže i definiranje sigurnosnih zona čine temelj sigurnosnog sustava. Sigurnosna politika računalnih mreža, temeljena na trijadi povjerljivosti (engl. *confidentiality*), integriteta (engl. *integrity*) i dostupnosti (engl. *availability*), pruža smjernice za korisnike i administratore kako bi se spriječio neovlašteni pristup i zloupotreba podataka.

Segmentacija mreže, koja dijeli mrežu na manje, logički odvojene dijelove te definiranje sigurnosnih zona omogućuju primjenu specifičnih sigurnosnih politika u različitim dijelovima mreže. Implementacija sigurnosnih uređaja i softvera, poput vatrozida, sigurnosnih alata i antivirusnih programa, čini prvu liniju obrane, osiguravajući da samo ovlašteni korisnici imaju pristup osjetljivim podacima. Redovito praćenje i održavanje ovih uređaja dodatno osigurava dostupnost sustava i podataka.

Osiguranje računalnih mreža ključno je za ispunjavanje zakonskih zahtjeva i održavanje poslovnog ugleda. Dobro osmišljen dizajn mrežne strukture, koji uključuje segmentaciju i definiranje sigurnosnih zona, postiže optimalnu sigurnost, performanse i skalabilnost mreže. Nadalje, posebna se pažnja posvećuje sustavima za otkrivanje i sprječavanje napada, koji su ključne komponente u zaštiti mreža od kibernetičkih prijetnji (Bace & Mell, 2001). Ovi sustavi

i alati klasificirani su prema metodama detekcije i načinima implementacije. U radu su detaljno opisani popularni alati kao što su *Suricata, Zeek* i *Snort* koji se koriste za otkrivanje prijetnji i zaštitu mreža.

Posljednji dio rada posvećen je alatu *Snort*, uključujući opis njegovih pravila, postupke instalacije na Windows i Ubuntu operacijskim sustavima te praktično testiranje u simuliranom okruženju. Za ispitivanje učinkovitosti *Snorta*, postavljena je virtualna okolina s operacijskim sustavima Linux Kali i Ubuntu. Ubuntu je korišten za implementaciju sigurnosnog sustava, dok je Kali poslužio za izvođenje simuliranih napada.

2. RAČUNALNE MREŽE I UMREŽAVANJE

Računalne mreže predstavljaju temelj moderne komunikacije i informacijskih sustava, omogućujući povezivanje računala i drugih uređaja radi dijeljenja resursa, informacija i usluga. Od kućnih mreža do složenih korporativnih sustava, mreže su postale ključne za poslovanje, obrazovanje i svakodnevni život. Uz stalni napredak tehnologije, mreže se neprestano razvijaju kako bi pružile bolje performanse, sigurnost i skalabilnost, čime podržavaju sve veće zahtjeve korisnika i organizacija. Istovremeno, ovaj rast i sve veća povezanost povećavaju izloženost kibernetičkim prijetnjama, što čini kibernetičku sigurnost ključnim aspektom u dizajnu, implementaciji i održavanju mreža.

2.1. Računalno umrežavanje

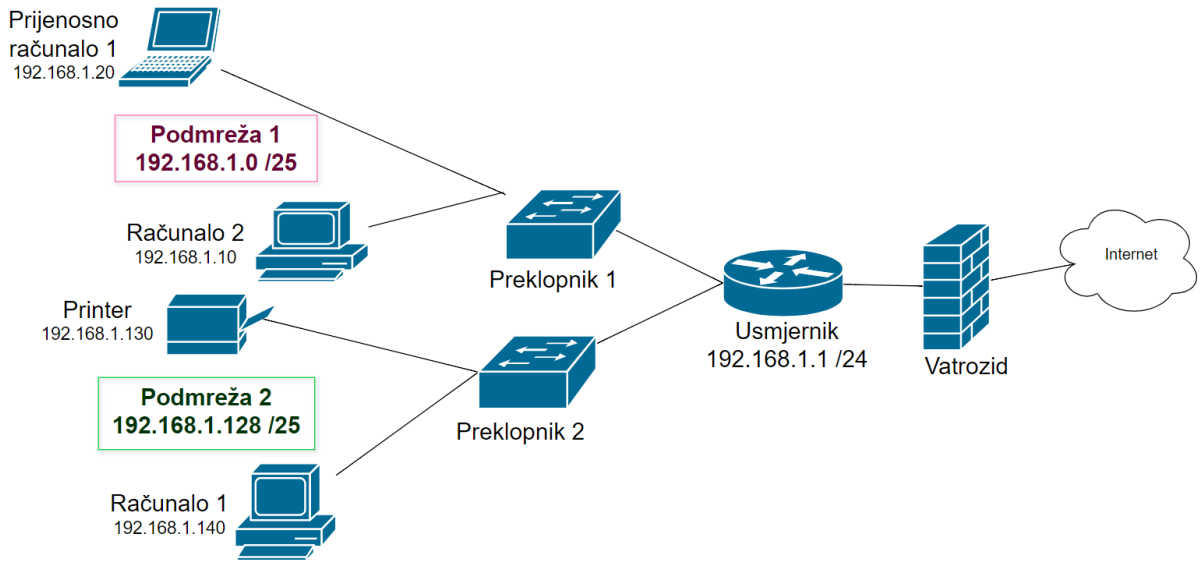
Upoznavanje s pojmom računalnog umrežavanja (Nacional CERT i LS&S, 2009) važno je za razumijevanje i primjenu osnovnih koncepta, tehnologija i praksi vezanih uz mrežne sustave. Računalno umrežavanje (engl. *computer networking*) se odnosi na povezivanje računala i drugih uređaja radi dijeljenja resursa poput podataka, aplikacija i pisača. Ključni pojmovi u ovom kontekstu uključuju IP adrese, podmreže, usmjeravanje (engl. *routing*) i mrežne protokole, s posebnim naglaskom na *Transmission Control Protocol//Internet Protocol* (TCP/IP) skup protokola, koji predstavlja osnovu suvremenih mrežnih komunikacija.

Računalne mreže se mogu klasificirati prema opsegu, topologiji, upravljanju pristupom i mediju za prijenos, dok različiti uređaji kao što su usmjernici (engl. *router*), preklopnici (engl. *switch*) i vatrozidi (engl. *firewall*) igraju ključnu ulogu u funkcioniranju mreža, zajedno s tehnologijama poput virtualnih privatnih mreža (engl. *Virtual Private Network, VPN*). Protokoli iz skupa protokola TCP/IP omogućuju komunikaciju između uređaja, dok standardi poput IEEE 802 LAN/MAN definiraju kompatibilnost između različitih uređaja. Ovi protokoli i standardi su temeljni za uspostavljanje učinkovite i interoperabilne mrežne infrastrukture.

Sigurnost mreža predstavlja ključni aspekt suvremenih informacijskih sustava, u kojem se primjenjuju različite tehnologije kako bi se osigurala zaštita podataka i mrežne infrastrukture. Među najvažnijim alatima i mehanizmima za postizanje ove sigurnosti su vatrozidi, sustavi za otkrivanje napada (engl. *Intrusion Detection Systems, IDS*), sustavi za sprječavanje napada (engl. *Intrusion Prevention Systems, IPS*) te šifriranje (engl. *encryption*). Ove tehnologije zajedno pružaju višeslojni pristup zaštiti, omogućujući pravovremeno otkrivanje prijetnji, sprječavanje napada i očuvanje integriteta mrežnih sustava. Vatrozidi kontroliraju promet na

mreži i sprječavaju neovlašteni pristup, IDS detektira sumnjive aktivnosti, IPS sprječava upade, a šifriranje osigurava privatnost podataka.

Razumijevanje osnovnih elemenata umrežavanja ključno je za stjecanje znanja o mrežnim tehnologijama i procesima, što omogućuje aktivno sudjelovanje u dizajnu, implementaciji i održavanju mrežnih sustava. Primjer takvog umrežavanja prikazan je na slici 1, koja prikazuje jednostavnu strukturu sastavljenu od dvije podmreže.



Slika 1. Struktura računalne mreže, Izvor: izrada autora

Preklopnici 1 i 2 su povezani na usmjernik, iza kojeg je smješten vatrozid, i na taj način omogućuje se siguran pristup Internetu svim prikazanim uređajima. Svaki preklopnik u svojoj podmreži povezuje različite uređaje čime se smanjuje količina emitiranog (engl. *broadcast*) prometa, poboljšavaju mrežne performanse te smanjuje kašnjenje u prijenosu podataka (engl. *latency*).

2.2. Mrežna topologija, uređaji i adresiranje

Računalne mreže omogućuju niz ključnih funkcionalnosti za razmjenu podataka između povezanih uređaja. Dijeljenje resursa i uređaja smanjuje troškove, povećava učinkovitost te olakšava timsku suradnju i razmjenu informacija putem e-pošte, aplikacija za razgovor i mrežnih sastanaka, neovisno o geografskoj udaljenosti. Povezivanje lokalne mreže (engl. *local area network, LAN*) s globalnom Internet mrežom omogućuje korisnicima pristup informacijama, uslugama i aplikacijama na udaljenim poslužiteljima širom svijeta. Centralizirana administracija i upravljanje mrežom pojednostavljuju primjenu sigurnosnih

politika i nadzor mrežnog prometa. Dodatno, skalabilnost i fleksibilnost mreža omogućuju lako dodavanje novih resursa bez značajnih promjena u postojećoj infrastrukturi. Pouzdanost i redundancija mreže osiguravaju kontinuitet poslovanja i povećavaju ukupnu stabilnost sustava.

Mreža može imati nekoliko poznatih topologija, koje se odnose na fizički ili logički raspored uređaja i komunikacijskih linija unutar nje. Fizička topologija prikazuje raspored čvorova u mreži, dok logička topologija prikazuje tok podataka između čvorova. Fizička topologija ne mora nužno odgovarati logičkoj topologiji. Najčešće fizičke topologije koje se koriste u današnjim mrežama prikazane su u tablici 1.

Tablica 1: Prikaz najčešćih fizičkih mrežnih topologija

Vrsta	**Opis**	**Prednosti**	**Nedostaci**
Sabirnička (engl. *bus*)	Članovi se povezuju na jedinstveni zajednički vod (sabirnicu)	Jednostavna instalacija, niska cijena	Ograničena duljina sabirnice, zagušenje
Zvjezdasta (engl. *star*)	Članovi su povezani različitim vodovima na središnji čvor	Lako upravljanje, jednostavno otkrivanje grešaka	Ovisnost o središnjem čvoru
Prstenasta (engl. *ring*)	Svaki čvor je izravno povezan s dva susjedna čvora, čime se formira zatvorena petlja	Predvidiva izvedba, ravnomjerno opterećenje	Prekid u jednoj točki prekida cijelu mrežu
Isprepletena (engl. *mesh*)	Djelomična ili potpuna povezanost svih članova unutar topologije	Visoka otpornost na greške, pouzdanost	Složenost, visoki troškovi postavljanja
Stablasta (engl. *tree*)	Hijerarhijska povezanost centralnog čvora s drugim nižim čvorovima	Skalabilnost, lako održavanje	Ovisnost o glavnim čvorovima, složenija instalacija

Mrežni uređaji omogućuju povezivanje i komunikaciju unutar mreže. Najčešći uređaji su usmjernici, preklopnici, vatrozidi i bežične pristupne točke (engl. *wireless access point*). Usmjernici usmjeravaju promet između različitih mreža koristeći tablice usmjeravanja za pronalaženje najboljih putova za slanje podataka prema odredištu. Preklopnici povezuju uređaje unutar mreže i upravljaju prometom podataka na podatkovnom sloju, prosljeđujući podatke prema odredišnom uređaju. Vatrozidi filtriraju ulazni i izlazni promet na temelju sigurnosnih pravila, stvarajući sigurnu zonu za podatke na mreži. Pristupne točke omogućuju bežični pristup mreži, povezujući bežične uređaje s žičanom mrežom..

Za razlikovanje uređaja na TCP/IP mrežama koristi se sustav adresiranja koji obuhvaća fizičko i logičko adresiranje. U *Ethernet* tehnologiji, fizičko adresiranje provodi se putem *Media Access Control* (MAC) adrese, poznate i kao fizička adresa, koja je pohranjena u memoriji samo za čitanje (engl. *Read Only Memory, ROM*) kartice mrežnog sučelja (engl. *Network Interface Card, NIC*). MAC adresa jedinstveno identificira mrežno sučelje i sastoji se od 48 bitova zapisanih u obliku 12 heksadecimalnih znamenki, pri čemu prvih 24 bita predstavljaju oznaku proizvođača, a preostalih 24 bita su jedinstvena za svaku karticu prema proizvođaču.

Logičko adresiranje odvija se na mrežnom sloju *Open Systems Interconnection* (OSI) referentnog modela pomoću *Internet Protocol* (IP) adresa. IP adrese omogućuju pronalaženje određenog uređaja na mreži i usmjeravanje toka podataka prema njemu. Trenutno su u upotrebi dvije verzije IP protokola. IP verzija 4 (IPv4) sastoji se od 32 bita i prikazuje se u obliku četiri okteta odvojena točkom u tzv. točkasto-decimalnom formatu (engl. *dotted decimal notation*). IP verzija 6 (IPv6), koja ima duljinu od 128 bitova zapisuje se u obliku osam skupina po četiri heksadecimalne znamenke, odvojenih dvotočkom. IPv6 je uveden kako bi se riješio problem nedostatka IP adresa u IPv4 zbog sve većeg broja uređaja koji zahtijevaju jedinstvene adrese na Internetu.

3. SIGURNOSNI PROTOKOLI

U području mrežne sigurnosti protokoli imaju ključnu ulogu u zaštiti podataka i osiguravanju sigurne komunikacije između klijenata na mreži. Protokoli definiraju način komunikacije između računala i drugih uređaja na mreži, a svaki od njih ima svoju specifičnu ulogu u ostvarivanju sigurne komunikacije. Njihova je svrha standardizacija i dosljedna primjena kako među korisnicima, tako i među proizvođačima opreme. S obzirom na sve veću prijetnju kibernetičkih napada i neovlaštenog pristupa, razumijevanje i implementacija odgovarajućih sigurnosnih protokola postali su neizostavni elementi u dizajnu i upravljanju sigurnim mrežama. Među najvažnijim sigurnosnim protokolima su *Secure Sockets Layer* (SSL), *Transport Layer Security* (TLS), *Internet Protocol Security* (IPsec) i *Secure Shell* (SSH).

Svaki od ovih protokola nudi specifične funkcionalnosti, prednosti i ograničenja, što ih čini primjenjivima u različitim segmentima mrežne sigurnosti. Osim spomenutih protokola, važno je naglasiti i sigurnosne protokole za bežične lokalne mreže (engl. *Wireless Local Area Network, WLAN*). Standardi poput *Wired Equivalent Privacy* (WEP) i *Wi-Fi Protected Access* (WPA) osiguravaju zaštitu i privatnost podataka u bežičnim mrežama (Nacionalni CERT, 2018), omogućujući korisnicima siguran pristup Internetu.

Osim pojedinačnih sigurnosnih protokola koji štite komunikaciju i podatke unutar mreža, postoje i tehnologije koje koriste kombinaciju tih protokola za osiguranje sigurnog pristupa i razmjene podataka putem javnih mreža. Jedna od takvih tehnologija je VPN, koja koristi različite sigurnosne protokole kako bi osigurala sigurno povezivanje i razmjenu podataka između korisnika putem javnih mreža. VPN je ključan za osiguranje poslovanja i zaštitu privatnosti, posebno kada se pristupa osjetljivim podacima s udaljenih lokacija.

3.1. SSL i TLS protokoli

Sigurnosni protokol *Secure Sockets Layer* (SSL) prvi put je uveden 1990-ih godina kao protokol za osiguranje komunikacije putem Interneta. Međutim, zbog svojih ranjivosti i sigurnosnih propusta, SSL je postupno zamijenjen modernijim protokolom *Transport Layer Security* (TLS), koji je razvijen kao njegova poboljšana verzija. TLS pruža bolju sigurnost i performanse, te se danas široko koristi za osiguranje mrežne komunikacije, dok je SSL uglavnom napušten zbog zastarjelosti i poznatih sigurnosnih slabosti. Unatoč tome što se SSL više ne koristi, oznaka SSL/TLS i dalje je uobičajena u literaturi i praksi. Razlog za to je

povijesna povezanost ovih protokola i činjenica da je SSL bio prvi široko prihvaćeni standard za siguran prijenos podataka na Internetu. Kada se koristi oznaka SSL/TLS, obično se misli na cijelu obitelj protokola za siguran prijenos podataka, pri čemu se danas TLS koristi kao *de facto* standard.

SSL/TLS (Oppliger, 2009) protokoli omogućuju šifriranje podataka i autentikaciju između komunikacijskih strana, čime se osigurava povjerljivost, integritet i autentičnost informacija. Šifriranje štiti podatke od neovlaštenog pristupa tijekom prijenosa, dok autentikacija putem digitalnih certifikata potvrđuje identitet komunikacijskih strana. Time se smanjuje rizik od napada poput *man-in-the-middle*, pri čemu napadač pokušava presresti ili izmijeniti komunikaciju. Kombinacija enkripcije i autentikacije unutar SSL/TLS protokola osigurava sigurnu i pouzdanu razmjenu informacija na Internetu.

Prednosti SSL/TLS protokola:

- *Enkripcija* – SSL/TLS protokoli omogućuju šifriranje podataka, osiguravajući privatnost i integritet informacija tijekom prijenosa.
- *Autentifikacija* – digitalni certifikati provjeravaju identitet poslužitelja i klijenta, čime se sprječavaju neovlašteni pristupi i lažno predstavljanje.
- *Sigurnost* – SSL/TLS osiguravaju sigurnu komunikaciju na Internetu putem HTTPS-a, koji je postao standard za zaštitu web stranica.

Nedostaci SSL/TLS protokola:

- *Performanse* – proces šifriranja i dešifriranja podataka može biti resursno zahtjevan, što može usporiti rad sustava, posebno na starijim uređajima ili u slučaju velikog broja korisnika.
- *Kompleksnost* – upravljanje SSL/TLS certifikatima, uključujući njihovu instalaciju i redovito obnavljanje, zahtijeva stručno znanje i iskustvo, što može predstavljati izazov za organizacije bez specijaliziranog osoblja.
- *Ranjivosti* – SSL je zastarjeli protokol s poznatim sigurnosnim slabostima, zbog čega se njegova uporaba ne preporučuje. Iako TLS nudi znatno bolju sigurnost i on može biti ranjiv ako se ne implementira i ne konfigurira ispravno.

3.2. IPsec skup protokola

IPsec je skup protokola koji se koriste za osiguranje sigurne komunikacije na mrežnom sloju. Ovi protokoli omogućuju autentikaciju i šifriranje IP paketa unutar komunikacijske sesije, čime se osigurava povjerljivost, integritet i autentičnost podataka.

IPsec se prvenstveno koristi za izgradnju i zaštitu komunikacije unutar VPN-a, čime se omogućuje siguran prijenos podataka preko nesigurnih mreža poput Interneta. Međutim, njegova primjena nije ograničena samo na VPN-ove. IPsec se također koristi za osiguranje komunikacije između različitih mrežnih uređaja, kao što su usmjernici, vatrozidi i hostovi, te je posebno koristan u korporativnim mrežama za zaštitu osjetljivih podataka.

Skup protokola IPsec podržava različite sigurnosne tehnologije i algoritme, uključujući *Encapsulating Security Payload* (ESP) i *Authentication Header* (AH). ESP osigurava šifriranje i opcionalnu autentikaciju podataka, dok AH pruža autentikaciju i integritet, ali ne i šifriranje. Ova modularnost omogućuje prilagodbu IPsec-a specifičnim sigurnosnim potrebama i okruženjima, pružajući visoku fleksibilnost u konfiguraciji i primjeni. Osim toga, IPsec podržava različite algoritme šifriranja, kao što su *Advanced Encryption Standard* (AES) za najnovije sigurnosne standarde i *Triple Data Encryption Standard* (3DES) za kompatibilnost sa starijim sustavima, omogućujući fleksibilnost u zaštiti podataka. Ova fleksibilnost i sveobuhvatnost čine IPsec jednim od najpouzdanijih i najsvestranijih protokola za zaštitu mrežne komunikacije, što ga čini ključnim alatom za osiguranje privatnosti i sigurnosti u modernim mrežnim okruženjima.

Prednosti IPsec-a:

- *Svestranost* – IPsec može osigurati promet između hostova, mreža i gateway uređaja, pružajući fleksibilnost u različitim mrežnim okruženjima.
- *Transparentnost* – budući da radi na mrežnom sloju, IPsec osigurava sav promet bez potrebe za promjenama na aplikacijskom sloju, čime se postiže neprimjetna integracija.
- *Kompatibilnost* – IPsec je kompatibilan s IPv4 i IPv6 protokolima, što omogućuje njegovu široku primjenu u različitim mrežnim infrastrukturama.

Nedostaci IPsec-a:

- *Kompleksnost konfiguracije* – postavljanje i upravljanje IPsec vezama može biti složeno i zahtijeva duboko razumijevanje mrežnih i sigurnosnih postavki.
- *Utjecaj na performanse* – enkripcija i autentikacija mogu negativno utjecati na mrežne

performanse, osobito na uređajima s ograničenim resursima.

- *Interoperabilnost* – postizanje interoperabilnosti između različitih implementacija IPsec-a može biti izazovno za administratore, što može rezultirati poteškoćama u integraciji različitih sustava.

3.3. SSH protokol

SSH je protokol koji omogućuje sigurnu udaljenu administraciju sustava, prijenos datoteka te sigurnu komunikaciju između mrežnih uređaja. Prvotno razvijen kao zamjena za nesigurne metode poput *Telnet*-a i *rlogin*-a, SSH je postao standardni alat za administratore sustava i mreža. Omogućuje šifriranu vezu između klijenta i poslužitelja, pružajući siguran način za izvršavanje naredbi na udaljenim računalima, pristup sustavima, te prijenos datoteka putem protkoola *Secure Copy Protocol* (SCP) i *Secure File Transfer Protocol* (SFTP).

Osnovna prednost SSH-a leži u njegovoj sposobnosti da osigura povjerljivost i integritet komunikacije korištenjem kriptografskih metoda. Osim što omogućuje udaljeni pristup i prijenos datoteka, SSH podržava tuneliranje, što znači da može sigurno prosljeđivati mrežni promet kroz šifrirani kanal. Ova funkcionalnost čini SSH vrlo fleksibilnim alatom koji može osigurati različite vrste mrežnog prometa, uključujući i one koji koriste nesigurne protokole.

Zbog svoje pouzdanosti, sigurnosti i svestranosti, SSH se koristi u mnogim okruženjima, od malih mreža do velikih poduzeća, te je neophodan alat za administratore koji upravljaju udaljenim sustavima ili žele osigurati siguran prijenos podataka putem nesigurnih mreža poput Interneta.

Prednosti SSH protokola:

- *Sigurnost* –koristi snažne metode šifriranja i autentikacije kako bi osigurao povjerljivost i integritet podataka.
- *Fleksibilnost* – može se koristiti za razne svrhe, uključujući daljinsku administraciju, prijenos datoteka i tuneliranje prometa.
- *Jednostavnost* – relativno je jednostavan za postavljanje i korištenje, posebno za korisnike s osnovnim znanjem o mrežama.

Nedostaci SSH protokola:

- *Performanse* – kao i drugi sigurnosni protokoli, enkripcija može utjecati na performanse sustava, osobito kod velikih prijenosa podataka.

- *Administracija* – upravljanje SSH ključevima i autentikacijom može postati složeno kod većih sustava.
- *Ograničenja u funkcionalnosti* – iako je SSH svestran, nije prikladan za sve vrste mrežnog prometa i aplikacija.

3.4. WEP i WPA protokoli

Sigurnost bežičnih lokalnih mreža (Šlekytė, 2023), posebno onih temeljenih na IEEE 802.11 standardu, oslanja se na nekoliko sigurnosnih protokola, uključujući WEP, WPA, WPA2 i WPA3 (Tablica 2).

Tablica 2: Evolucija sigurnosnih protokola za bežične lokalne mreže

Protokol	**Godina uvođenja**	**Glavne karakteristike**
WEP	1997	Osnovna enkripcija, zajednički ključ za sve autorizirane uređaje
WPA	2003	Poboljšana sigurnost u odnosu na prethodnika generiranjem dinamičkih ključeva *Temporal Key Integrity Protocol* (TKIP)
WPA2	2004	Jača enkripcija i sigurnost postignuta pomoću AES šifriranja
WPA3	2018	Poboljšana metoda autentikacije i duži ključevi za šifriranje (osobna i privatna upotreba)

Izvorni protokol IEEE 802.11 standarda bio je WEP, razvijen kako bi omogućio razinu sigurnosti sličnu onoj žičnih mreža. WEP (Stack, 2019) koristi šifriranje podataka za zaštitu bežične komunikacije, pri čemu svaki uređaj na mreži koristi zajednički ključ za šifriranje i dešifriranje podataka, osiguravajući da samo autorizirani uređaji mogu pristupiti mreži. Iako je WEP bio standard za sigurnost bežičnih mreža u ranijim fazama, danas je gotovo u potpunosti napušten zbog svojih značajnih sigurnosnih slabosti.

Prednosti WEP protokola uključuju jednostavnost implementacije i konfiguracije te široku kompatibilnost sa starijom mrežnom opremom. Međutim, WEP ima ozbiljne sigurnosne propuste koji omogućuju napadačima da relativno brzo probiju ključ i pristupe mreži. Zbog ovih slabosti, WEP se više ne preporučuje za upotrebu u modernim mrežama i zamijenjen je sigurnijim WPA protokolima.

WPA protokol i njegove kasnije verzije razvijeni su kako bi poboljšali sigurnost bežičnih lokalnih mreža i pružili znatno veću zaštitu u usporedbi s WEP-om. WPA koristi TKIP za dinamičko generiranje jedinstvenih ključeva za svaku sesiju, dok WPA2 koristi AES koji pruža znatno jače šifriranje i bolju zaštitu podataka. WPA2 trenutno je najkorišteniji protokol za

bežične lokalne mreže. Oba protokola koriste *pre-shared keys* (PSK) za autentikaciju korisnika na mreži. Prednosti WPA i WPA2 protokola uključuju poboljšanu sigurnost, dinamičko generiranje ključeva i naprednu zaštitu putem AES šifriranja. Međutim, ovi protokoli mogu imati problema s kompatibilnošću sa starijim uređajima, zahtijevaju više resursa za AES šifriranje i mogu biti složeniji za postavljanje i upravljanje u usporedbi s WEP-om.

WPA3, uveden 2018. godine kao odgovor na ranjivost *key reinstallation attacks* (KRACK) pronađenu u WPA2, donosi dodatne sigurnosne prednosti. Ove prednosti uključuju bolju zaštitu lozinki putem *Simultaneous Authentication of Equals* (SAE), individualno šifriranje podataka između svakog uređaja i bežične pristupne točke te korištenje duljih i naprednijih ključeva za šifriranje, pri čemu se 192-bitni ključevi koriste za osobnu upotrebu, a 256-bitni ključevi za poslovne svrhe. Ova evolucija sigurnosnih protokola (Tablica 2) omogućuje bolju zaštitu bežičnih mreža, pružajući korisnicima sigurnije iskustvo korištenja bežičnih komunikacija.

4. SIGURNOST I DIZAJN MREŽNE STRUKTURE

Sigurnost i dizajn mrežne strukture ključni su za zaštitu podataka i održavanje pouzdanih mrežnih operacija (Ožegović & Pezelj, 2000). U doba kada su prijetnje poput kibernetičkih napada sve prisutnije, pravilno osmišljen sigurnosni okvir osigurava stabilnost i otpornost mreže na različite sigurnosne izazove. Dobro dizajnirana mrežna arhitektura ne samo da štiti osjetljive informacije, već također omogućuje učinkovito upravljanje resursima i smanjuje rizik od neovlaštenih pristupa. Ključni elementi poput definicije sigurnosnih politika, segmentacije mreže i uspostavljanja sigurnosnih zona čine temelj za stvaranje robusnog i sigurnog sustava prilagođenog specifičnim potrebama svake organizacije.

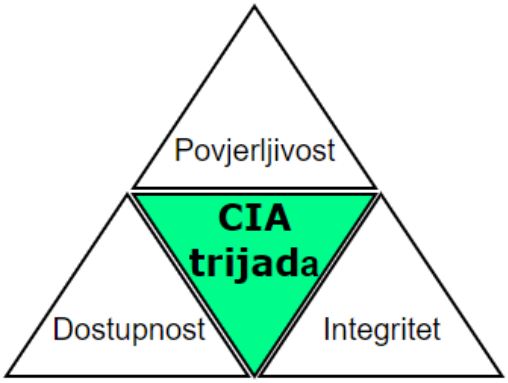
4.1. Sigurnosna politika računalnih mreža

Svi informacijski sustavi sadrže podatke kojima pristupaju korisnici, a ti podaci u većini slučajeva ne smiju biti javno dostupni jer su povjerljivi i u nečijem vlasništvu. Sigurnosna politika je skup pravila, smjernica i postupaka koji definiraju način na koji se mogu koristiti mrežni resursi, s ciljem sprječavanja neovlaštenog pristupa, zloupotrebe, modifikacije, oštećenja ili gubitka podataka (Kovačević, 2006; Scarfone & Mell, 2007). Sigurnosna politika također pruža smjernice za korisnike, administratore i druge relevantne strane, jasno definirajući što smiju, što ne smiju raditi te koje su njihove odgovornosti.

Sigurnosna politika ima tri ključna cilja:

- *Povjerljivost* – osigurava da samo ovlašteni korisnici imaju pristup osjetljivim podacima. To uključuje upravljanje pravima pristupa, enkripciju podataka i zaštitu od neovlaštenog pristupa.
- *Integritet* – štiti podatke i sustave, osiguravajući da se podaci ne mijenjaju ili brišu bez odgovarajuće autorizacije. Integritet se postiže korištenjem digitalnih potpisa, nadzora promjena i redovitih sigurnosnih provjera.
- *Dostupnost* – osigurava da informacijski sustavi budu dostupni korisnicima kad god je to potrebno.

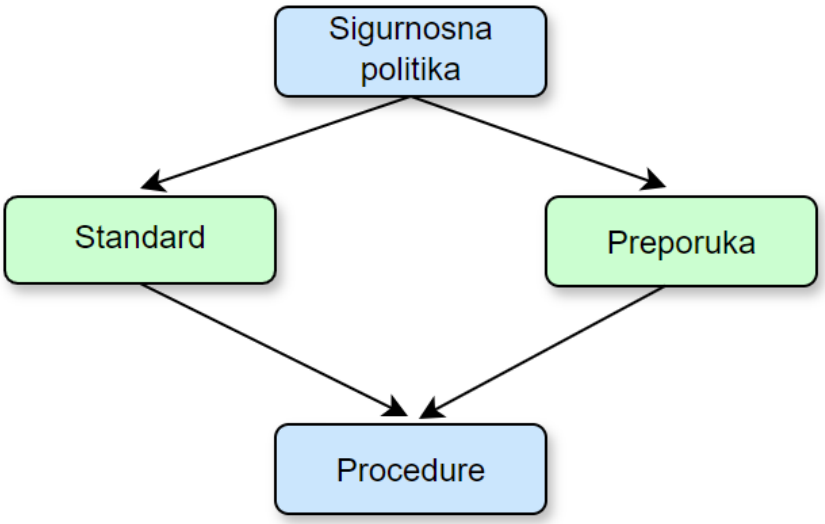
Ova tri cilja čine temelj sigurnosnog modela poznatog kao *Confidentiality, Integrity, and Availability* (CIA) trijada, prikazanog na slici 2. Kada su povjerljivost, integritet i dostupnost zadovoljeni, sustav se smatra dovoljno jakim i opremljenim za rješavanje sigurnosnih prijetnji.



Slika 2. Koncept CIA trijade u kibernetičkoj sigurnosti, Izvor: izrada autora

Ključni elementi sigurnosne politike definiraju razinu pristupa i manipulacije podacima za svakog korisnika, kao i pravila i procedure za zaštitu mrežnih resursa (Fortinet Inc., 2024). Osim toga, sigurnosne politike služe za upravljanje incidentima, obuku korisnika o sigurnosnim prijetnjama i najboljim praksama te osiguravaju kontinuirano praćenje i reviziju kako bi se osigurala njihova učinkovitost i usklađenost s promjenama u okruženju i prijetnjama.

Sigurnosne politike usmjeravaju razvoj informacijske sigurnosti, dok se njihova konkretna primjena temelji na preporukama i procedurama koje detaljno opisuju kako zaštititi svaki element informacijskog sustava prema postojećim standardima. Kako bi se osigurala interoperabilnost, često se definiraju standardi kao temelj za izradu procedura. Procedure su završni korak u implementaciji sigurnosti, precizno opisujući kako provesti standarde i preporuke za svaki ključni element sustava. Svi ovi elementi međusobno su povezani i zajedno čine zatvoreni krug sigurnosnih smjernica (Slika 3).



Slika 3. Povezanost sigurnosnih smjernica; Izvor: izrada autora

Na temelju prikazanih sigurnosnih politika, standarda, preporuka i procedura, jasno je da svaki element igra ključnu ulogu u uspostavljanju i održavanju sigurnosti informacijskih sustava. Samo kroz dosljednu primjenu svih ovih elemenata moguće je izgraditi učinkovit i održiv sustav informacijske sigurnosti koji može odgovoriti na sve složenije prijetnje i izazove modernog digitalnog okruženja.

4.2. Dizajn mrežne strukture i sigurnosne mjere

Dizajn mrežne strukture ključan je korak u stvaranju sigurne i učinkovite mrežne arhitekture. Ovaj proces uključuje detaljno planiranje i organizaciju mrežnih resursa s ciljem osiguravanja optimalne sigurnosti, performansi i skalabilnosti mreže. Ključni elementi dizajna mreže uključuju segmentaciju mreže, definiranje sigurnosnih zona i implementaciju sigurnosnih uređaja.

4.2.1. Segmentacija mreže

Segmentacija mreže je proces podjele mreže na manje, logički odvojene dijelove ili segmente. Svaki segment može imati specifične sigurnosne politike i kontrole pristupa, što pomaže u ograničavanju širenja potencijalnih napada unutar mreže.

Ključne metode segmentacije uključuju:

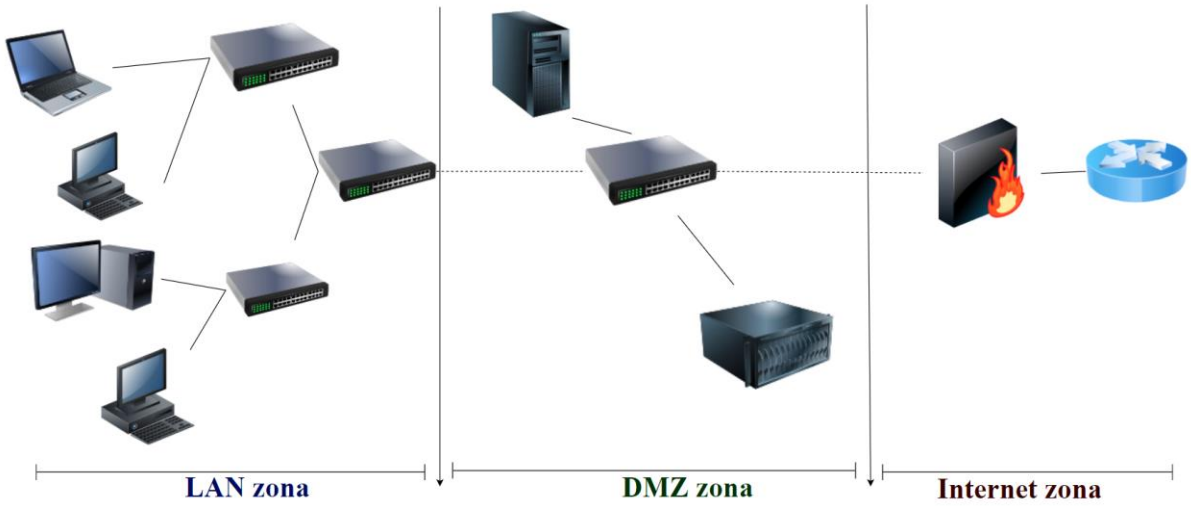
- *Virtualne lokalne mreže* – VLAN-ovi omogućuju kreiranje odvojenih mrežnih segmenata unutar istog fizičkog okruženja, čime se povećava sigurnost i upravljivost mreže.
- *Podmrežavanje* – podjela mreže na manje podmreže temeljem IP adresiranja. Svaka podmreža može imati vlastite sigurnosne politike i upravljačke mjere.
- *Segmentacija prema funkciji* – razdvajanje mreže na segmente prema funkcijama (npr., odvojene mreže za korisnike, administratore, goste, IoT uređaje i sl.) pomaže u boljoj kontroli pristupa i smanjenju sigurnosnih rizika.

4.2.2. Definiranje sigurnosnih zona

Sigurnosne zone su logičke ili fizičke podjele mreže s različitim razinama sigurnosnih kontrola. Definiranjem sigurnosnih zona omogućuje se implementacija specifičnih sigurnosnih politika za različite dijelove mreže.

Ključni aspekti organizacije sigurnosnih zona uključuju:

- *Unutarnja zona (Intranet)* – najsigurnija zona unutar organizacije, koja obično sadrži interni poslovni promet, korisničke uređaje i poslužitelje. Pristup ovoj zoni ograničen je na zaposlenike i ovlaštene korisnike (Slika 4).
- *Demilitarizirana zona (engl. Demilitarized Zone, DMZ)* – zona između unutarnje i vanjske mreže, gdje se nalaze javno dostupni poslužitelji (npr., *web* poslužitelj, poslužitelj e-pošte, *Domain Name System* (DNS) poslužitelj). Pristup ovoj zoni je strogo kontroliran i filtriran (Slika 4).
- *Vanjska zona (Internet)* – najmanje sigurna zona koja obuhvaća sve uređaje i resurse izložene Internetu. Koriste se razne sigurnosne tehnike (npr., firewall, IDS, IPS) kako bi se zaštitili mrežni resursi (Slika 4).
- *Bežična zona (Wi-Fi)* – zona koja obuhvaća bežične uređaje i pristupne točke. Pristup može biti otvoren (za goste) ili zaštićen lozinkom (za interne korisnike).
- *Zona za goste* – posebna zona namijenjena gostima i posjetiteljima, s ograničenim pristupom i bez povezanosti s unutarnjom mrežom.
- *Zona za poslovne partnere* – zona koja omogućava kontroliran pristup poslovnim partnerima i dobavljačima, s ograničenim pristupom resursima.
- *Zona za administraciju* – zona koja sadrži administrativne uređaje i alate za upravljanje mrežom. Pristup je strogo kontroliran i rezerviran za IT osoblje.



Slika 4. Prikaz mrežnih zona, Izvor: izrada autora

4.2.3. Implementacija sigurnosnih uređaja i softvera

Implementacija sigurnosnih uređaja i softvera igra ključnu ulogu u zaštiti mreže. Ovi alati osiguravaju povjerljivost, integritet i dostupnost podataka, što je od vitalnog značaja za poslovanje. Sigurnosni uređaji kao što su vatrozidi, IDS/IPS sustavi i antivirusni softver pružaju prvu liniju obrane protiv zlonamjernih napada, uključujući zlonamjerni softver (engl. *malware*), krađu identiteta (engl. *phishing*), napade uskraćivanjem usluge (engl. *Denial of Service, DoS*) i distribuirane napade uskraćivanjem usluge (engl. *Distributed Denial of Service, DDoS*). Ovi sustavi otkrivaju i blokiraju prijetnje prije nego što mogu prouzročiti štetu.

Šifriranje, autentikacija i kontrola pristupa osiguravaju da samo ovlašteni korisnici imaju pristup osjetljivim podacima. IDS/IPS sustavi i antivirusni softver sprječavaju neovlaštene izmjene i manipulacije podacima, osiguravajući njihovu točnost i pouzdanost. Zaštita od *DDoS* napada i drugih zlonamjernih aktivnosti omogućava neprekidan rad mrežnih usluga. Redovito praćenje i održavanje sigurnosnih uređaja osigurava visoku dostupnost sustava i podataka.

Implementacija sigurnosnih uređaja i softvera također pomaže organizacijama u ispunjavanju zakonskih zahtjeva i izbjegavanju pravnih problema. Sigurnosni sustavi omogućuju redovite sigurnosne kopije i zaštitu od ucjenjivačkog softvera (engl. *ransomware*), osiguravajući obnovu podataka u slučaju kvara sustava ili sigurnosnog incidenta. Vidljiva implementacija sigurnosnih mjera povećava povjerenje korisnika, klijenata i poslovnih partnera, što je ključno za poslovni ugled organizacije.

4.3. Sustavi sigurnosti i zaštite računalnih mreža

Zaštita računalnih mreža ključan je aspekt moderne IT infrastrukture i neophodna je za osiguranje sigurnog i pouzdanog poslovanja. U današnjem povezanom svijetu, računalne mreže čine okosnicu poslovanja, komunikacije i pohrane podataka. S obzirom na sve veći broj sofisticiranih prijetnji, poput zlonamjernog softvera, krađe identiteta, te napada uskraćivanjem usluge, zaštita mreža postaje sve važnija. Njezina je glavna svrha zaštititi osjetljive podatke, uređaje i usluge od neovlaštenog pristupa, zloupotrebe, krađe i raznih oblika napada, čime se osigurava kontinuitet poslovanja, povjerenje korisnika i sukladnost sa zakonskim regulativama.

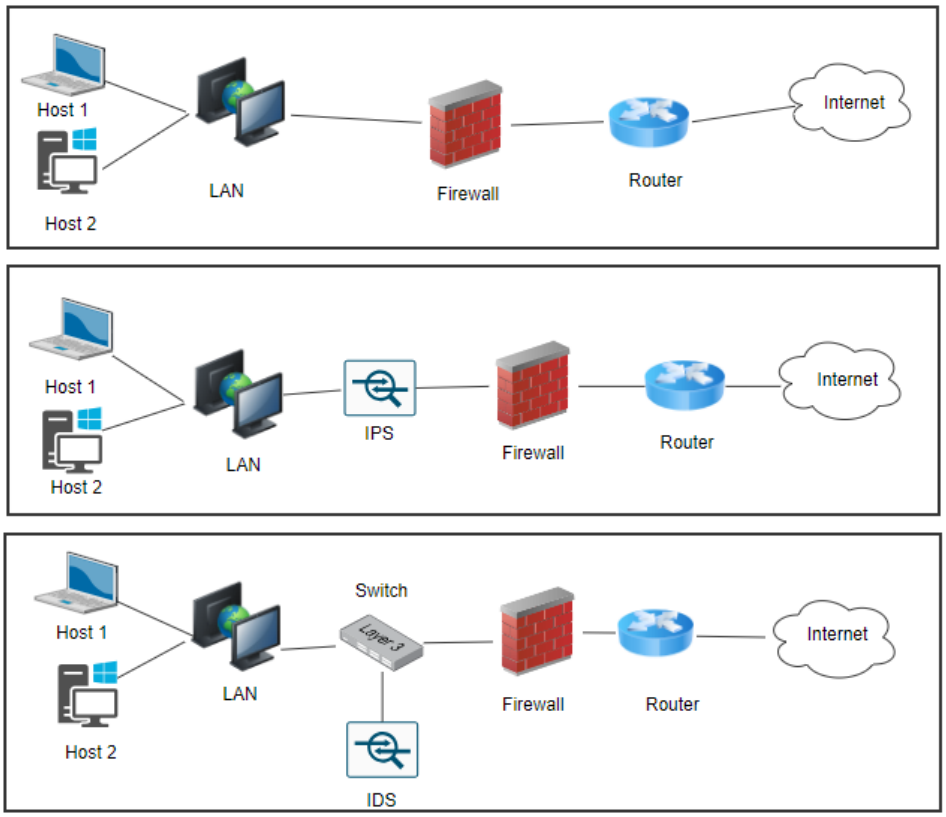
Postoji nekoliko metoda i tehnika za zaštitu računalnih mreža, a one uključuju:

- *Vatrozidi* – predstavljaju prvu liniju obrane, kontrolirajući dolazni i odlazni mrežni promet na temelju unaprijed definiranih sigurnosnih pravila. Postoje različite vrste

vatrozida, npr. mrežni, aplikacijski ili vatrozidi sljedeće generacije (engl. *Next-Generation Firewall, NGFW*). Mrežni vatrozidi filtriraju promet na razini IP adresa i brojeva priključnih točaka (engl. *ports*). Aplikacijski vatrozidi pregledavaju promet na aplikacijskom sloju, dok NGFW kombiniraju tradicionalne funkcije vatrozida s dodatnim mogućnostima, poput inspekcije paketa, antivirusne zaštite i filtriranja sadržaja.

- *IDS/IPS sustavi* – otkrivaju i sprječavaju sumnjive aktivnosti unutar mreže (Hung-Jen Liao;Hung-Jen Liao ;Ying-Chih Lin ; Kuang-Yuan Tung, 2013). IDS sustav otkriva sumnjive aktivnosti i potencijalne napade u mreži, uključujući pokušaje proboja, neovlaštene pristupe i druge anomalije. Analizira mrežni promet i uspoređuje ga s poznatim uzorcima napada. Ako otkrije sumnjivu aktivnost, generira upozorenje ili alarm. IPS sustav, osim što otkriva napade, poduzima i zaštitne mjere, poput promjene pravila vatrozida, kako bi spriječio napade.
- *VPN* – omogućuje sigurnu komunikaciju između udaljenih lokacija putem javne mreže (npr. Internet). Koristi enkripciju kako bi zaštitio podatke tijekom prijenosa, osiguravajući na taj način privatnost i integritet podataka.
- *Ostale sigurnosne komponente* – kao što su antivirusni programi, alati za zaštitu od zlonamjernog softvera (engl. *antimalware tools*), šifriranje podataka i autentikacija, u kombinaciji s prethodno navedenim alatima, osiguravaju cjelovitu sigurnost mreže i štite od napada na mrežne sustave.

Na slici 5 prikazana su tri primjera mrežnih arhitektura koje ilustriraju kako implementirati sigurnosne alate poput vatrozida, IPS-a i IDS-a za zaštitu mreže na različitim razinama. Prvi primjer prikazuje osnovnu mrežnu arhitekturu s vatrozidom postavljenim između LAN-a i usmjernika koji vodi prema Internetu. Ovaj pristup predstavlja osnovnu sigurnosnu mjeru gdje vatrozid djeluje kao prva linija obrane, filtrirajući sav ulazni i izlazni promet na temelju definiranih pravila. Drugi primjer prikazuje napredniju konfiguraciju koja uključuje IPS između LAN-a i vatrozida. IPS sustav omogućuje aktivnu zaštitu mreže tako što ne samo da detektira sumnjive aktivnosti nego ih i blokira u stvarnom vremenu, čime dodatno štiti mrežu od potencijalnih napada prije nego što promet dođe do vatrozida. Treći primjer pokazuje mrežnu arhitekturu s IDS-om koji je povezan putem preklopnika 3. sloja (engl. *layer 3 switch*) za pasivno nadgledanje mrežnog prometa. IDS analizira promet za znakove sumnjivih aktivnosti ili anomalija i generira upozorenja ili alarme, omogućujući administratorima mreže da reagiraju na prijetnje bez izravnog utjecaja na mrežni promet.



Slika 5. Primjeri implementacije sigurnosnih alata, Izvor: izrada autora

Višeslojni pristup, koji koristi kombinaciju vatrozida, IDS-a i IPS-a, osigurava sveobuhvatniji sigurnosni okvir koji može prepoznati, spriječiti i reagirati na razne vrste prijetnji. Ovo slojevito rješenje pruža robusnu obranu mreže, pomaže u osiguravanju kontinuiteta poslovanja i povjerenja korisnika te može doprinijeti usklađenosti sa zakonskim regulativama.

5. SUSTAVI ZA OTKRIVANJE I SPRJEČAVANJA NAPADA NA MREŽI

Jedan od ključnih elemenata sigurne mrežne infrastrukture su IDS/IPS sustavi (Scarfone & Mell, 2007). Ovi sustavi igraju presudnu ulogu u prepoznavanju i neutraliziranju prijetnji koje mogu ugroziti sigurnost mreže i podataka. U današnjem digitalnom okruženju, gdje su kibernetički napadi sve sofisticiraniji i češći, pouzdani sustavi za otkrivanje i sprječavanje napada postali su neophodni za svaku organizaciju. Integracija ovih sustava s drugim sigurnosnim alatima, kao što su vatrozidi, VPN-ovi i antivirusni programi, omogućuje sveobuhvatnu zaštitu koja ne samo da štiti od poznatih prijetnji, već i omogućuje brzo reagiranje na nove, nepoznate napade.

5.1. Otkrivanje i sprječavanje napada

Sustavi za otkrivanje i sprječavanje napada ključni su za zaštitu mreža od raznih kibernetičkih prijetnji. Oni omogućuju napredne metode za identifikaciju, praćenje i blokiranje zlonamjernih aktivnosti prije nego što mogu prouzročiti štetu. Njihova je svrha olakšati nadzor i omogućiti brzu reakciju na sigurnosne prijetnje, smanjujući vrijeme potrebno za njihovo otklanjanje.

IDS sustavi analiziraju mrežni promet uspoređujući ga s bazama podataka poznatih prijetnji ili tražeći anomalije u uobičajenim obrascima ponašanja. Kada otkriju sumnjive aktivnosti, obavještavaju mrežne administratore ili integrirane *Security Information and Event Management* (SIEM) sustave, koji filtriraju dolazne alarme i razlikuju lažne dojave od stvarnih prijetnji. Time se omogućuje pravovremena i precizna reakcija na incidente te minimizira mogućnost oštećenja ili kompromitiranja mrežnih resursa. Za razliku od IDS-a, IPS sustavi imaju proaktivnu ulogu i ne samo da otkrivaju prijetnje, već i automatski blokiraju ili ublažavaju napade, čime se smanjuje rizik od proboja i zlonamjernih aktivnosti.

Kombinirana primjena IDS i IPS sustava u hibridnim sigurnosnim arhitekturama postaje sve češća, jer omogućuje slojevitu obranu koja koristi prednosti oba pristupa. Uz primjenu tehnika poput strojnog učenja (engl. *machine learning*) i analize ponašanja korisnika za otkrivanje novih i nepoznatih prijetnji, moderni IDS/IPS sustavi postaju učinkovitiji u prepoznavanju i neutraliziranju prijetnji, pružajući značajnu zaštitu mrežnim sustavima u dinamičnom kibernetičkom okruženju.

5.2. Klasifikacija IDS i IPS sustava

U području kibernetičke sigurnosti, IDS sustave obično dijelimo u dvije osnovne kategorije, prema metodama detekcije i prema načinu implementacije.

Prema metodama detekcije IDS sustavi se dijele na tri glavne vrste:

- *Sustavi temeljeni na potpisima* – ovi sustavi otkrivaju napade uspoređujući mrežni promet s unaprijed definiranim uzorcima poznatih napada. Učinkoviti su za prepoznavanje poznatih prijetnji, ali im je nedostatak što ne mogu otkriti nove, nepoznate napade.
- *Sustavi temeljeni na anomalijama* – ovi sustavi prate normalno ponašanje mreže i detektiraju odstupanja koja bi mogla ukazati na napad. Njihova prednost je sposobnost otkrivanja novih prijetnji, ali im nedostaje preciznost u razlikovanju normalnih odstupanja od stvarnih prijetnji.
- *Sustavi temeljeni na stanju* – ovi sustavi analiziraju stanje mrežnih veza i prepoznaju nepravilnosti u prometu koje bi mogle ukazivati na napade. Fokusiraju se na prepoznavanje neobičnih ponašanja unutar mreže.

Prema načinu implementacije IDS sustavi se dijele na dvije skupine:

- *Mrežni IDS sustavi* – ovi sustavi postavljeni su na ključne točke unutar mreže kako bi analizirali sav dolazni i odlazni promet. Mogu raditi u *on-line* načinu, gdje djeluju u stvarnom vremenu i omogućuju brzu reakciju na potencijalne prijetnje, ili u *off-line* načinu, gdje analiziraju promet nakon što je spremljen, što smanjuje potrebu za resursima, ali usporava reakciju na napad.
- *Poslužiteljski ili host IDS sustavi* – ovi sustavi postavljeni su na određene uređaje ili poslužitelje kako bi pratili aktivnosti unutar operacijskog sustava, uključujući datoteke i logove, čime štite pojedinačne domaćine od napada.

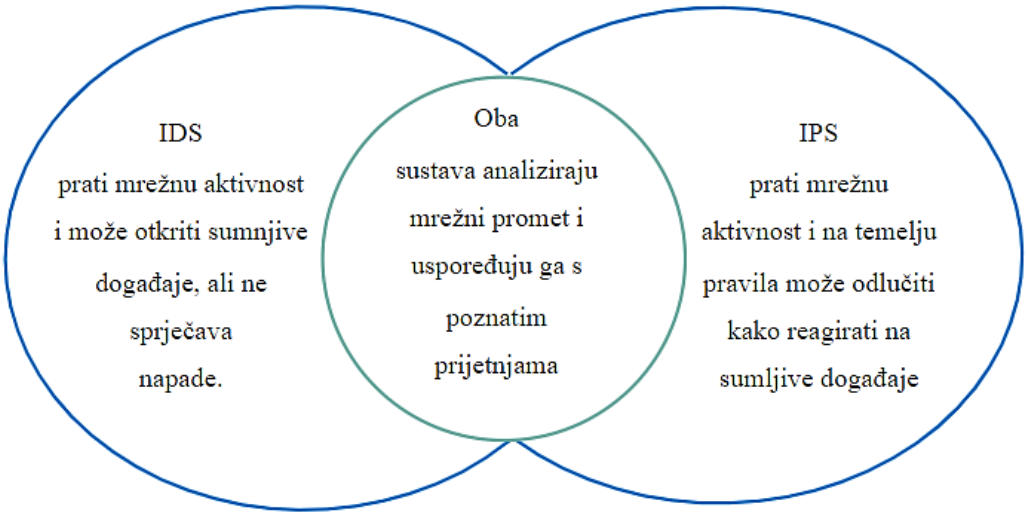
IPS sustavi predstavljaju naprednu verziju IDS sustava, s dodatnom sposobnošću odgovora na otkrivene prijetnje. Poznati su još i kao sustavi za otkrivanje i sprječavanje napada (engl. *Intrusion Detection and Prevention System, IDPS*), a obično su postavljeni na granici između vanjske mreže (Interneta) i unutarnje mreže organizacije. IPS sustavi aktivno blokiraju mrežni promet prije nego što dođe do odredišta, oslanjajući se na pravila koja određuju predstavlja li taj promet sigurnosnu prijetnju. Na taj način mogu zaustaviti napade, mijenjati

sadržaj napada, prilagođavati sigurnosno okruženje te slati alarm blokiranjem ili resetiranjem prometa s upitne IP adrese. Zbog svoje učinkovitosti, IPS sustavi postali su neizostavni dio sigurnosne infrastrukture.

IPS sustavi, kao i IDS sustavi, klasificiraju se prema metodama otkrivanja prijetnji, ali se dodatno dijele na četiri različite vrste prema funkciji:

- *Mrežni sustavi za sprječavanje napada* – analiziraju cijelu mrežu i identificiraju te blokiraju prijetnje unutar mrežnog prometa.
- *Bežični sustavi za sprječavanje napada* – specijalizirani su za analizu i zaštitu bežičnih mreža, detektirajući i sprečavajući napade specifične za bežična okruženja.
- *Sustavi za sprječavanje napada zasnovani na analizi ponašanja na mreži (Network Behavior Analysis, NBA)* – ispituju mrežni promet tražeći neobične događaje ili anomalije koje bi mogle ukazivati na napade.
- *Računalni sustavi za sprječavanje napada* – nadziru aktivnosti unutar pojedinačnih računala i pružaju zaštitu na razini jednog uređaja.

Sustavi za otkrivanje napada i sustavi za sprječavanje napada imaju ključne uloge u mrežnoj sigurnosti. Iako oba sustava dijele određene karakteristike, svaki od njih ima specifične prednosti i mane (Slika 6).



Slika 6. Različitosti i sličnosti IDS i IPS sustava, Izvor: izrada autora

IDS i IPS sustavi ključni su elementi u sigurnosnoj infrastrukturi jer omogućuju otkrivanje i sprječavanje različitih vrsta kibernetičkih napada. Kombinacija oba pristupa, uz pravilnu

implementaciju i optimizaciju, osigurava sveobuhvatnu obranu mreža, prilagodljivu promjenjivim prijetnjama i sigurnosnim izazovima u digitalnom okruženju.

5.3. Vrste i karakteristike IDS i IPS alata

IDS alati su obično softverske aplikacije koje se izvode na hardveru organizacije ili kao mrežna sigurnosna rješenja. Također postoje i IDS rješenja temeljena na oblaku (engl. *cloud IDS*), koja štite podatke, resurse i sustave organizacija unutar njihovih implementacija u oblaku. IDS alati nisu osmišljeni za samostalan rad, već su dizajnirani kao dio šireg sustava kibernetičke sigurnosti. Često su usko integrirani s jednim ili više sigurnosnih rješenja, kao što su SIEM sustavi, koji omogućuju obogaćivanje upozorenja podacima o prijetnjama, filtriranje lažnih alarma i davanje prioriteta kod saniranja štete. Također, često se koriste u kombinaciji s vatrozidima, gdje služe za „hvatanje“ prometa koji uspije proći kroz vatrozid.

S obzirom na sve veću potrebu za sigurnošću osobnih i privatnih podataka, danas postoji mnoštvo različitih IDS sustava koji se mogu integrirati u mrežnu infrastrukturu (Tablica 3). Neki od tih alata dostupni su u trajno besplatnim verzijama, dok se za druge plaća nakon isteka probnog razdoblja. U tablici 3 prikazane su karakteristike nekoliko popularnih alata za detekciju i prevenciju napada. Među najpoznatijima su *Suricata*, *Zeek* i *Snort,* koji su visoko cijenjeni zbog svoje učinkovitosti i široke primjene.

Tablica 3: Karakteristike poznatih sigurnosnih alata

Alat	**Tip**	**Pravila**	**Metode nadzora prometa**	**Integracija**
Suricata	IDS/IPS	Vlastita pravila (kompatibilna sa *Snortom*)	Dubinska inspekcija mrežnih paketa	Dobra, integracija s alatima za analizu mreže
Zeek	IDS	Skriptni jezik za prilagodbu	Analiza mrežnih događaja i protokola	Izvrsna za integraciju sa SIEM alatima
Snort	IDS/IPS	Vlastita pravila	Dubinska inspekcija mrežnih paketa	Dobra, široka podrška unutar sigurnosne zajednice

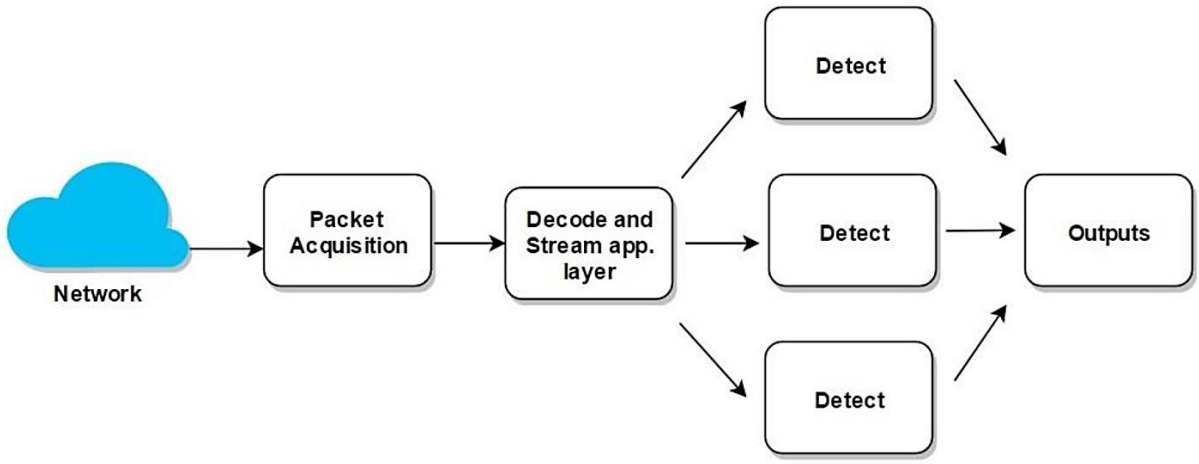
5.3.1. Suricata

Suricata je jedan je od vodećih alata otvorenog koda za otkrivanje i sprječavanje napada na mrežama (Suricata, 2016-2024; Alilović, 2019), a smatra se jednim od glavnih konkurenata *Snortu*, također alatu otvorenog koda. Rad alata temelji se na potpisivanju, otkrivanju

anomalija i pravilima za otkrivanje prijetnji. Jedna od prednosti ovog alata je sposobnost istovremenog rada na više zadataka, što omogućuje bržu analizu mrežnog prometa. Također, koristi grafičke procesore za ubrzanje rada u realnom vremenu i primjenjuje različite metode za analizu anomalija, čime se povećava preciznost u prepoznavanju napada. Alat je kompatibilan sa *Snortovom* strukturom podataka, što omogućuje implementaciju *Snortovih* pravila unutar *Suricate*.

Suricata može analizirati TLS/SSL certifikate, HTTP zahtjeve i DNS transakcije, pružajući sveobuhvatan uvid u mrežnu sigurnost. Ove značajke čine *Suricatu* privlačnim alatom koji nudi visoku učinkovitost i fleksibilnost za suvremene potrebe mrežne sigurnosti.

Slika 7 prikazuje arhitekturu obrade mrežnog prometa u *Suricata* alatu. Prikazan je proces obrade koji započinje prikupljanjem mrežnih paketa (engl. *Packet Acquisition*), dekodiranjem i obradom podataka na sloju aplikacije (engl. *Decode and Stream app. layer*), te prolazi kroz višestruke faze detekcije (engl. *Detect*) kako bi se identificirale potencijalne prijetnje. Završni izlazi (engl. *Outputs*) predstavljaju generirane izvještaje i upozorenja koja mogu biti korisna za mrežne administratore i sigurnosne stručnjake. Ova arhitektura omogućava paralelnu detekciju i pruža fleksibilnost u prilagodbi za različite sigurnosne zahtjeve.



Slika 7. Arhitektura obrade podataka u *Suricata* alatu, Izvor: *(Shah & Issac, 2018)*

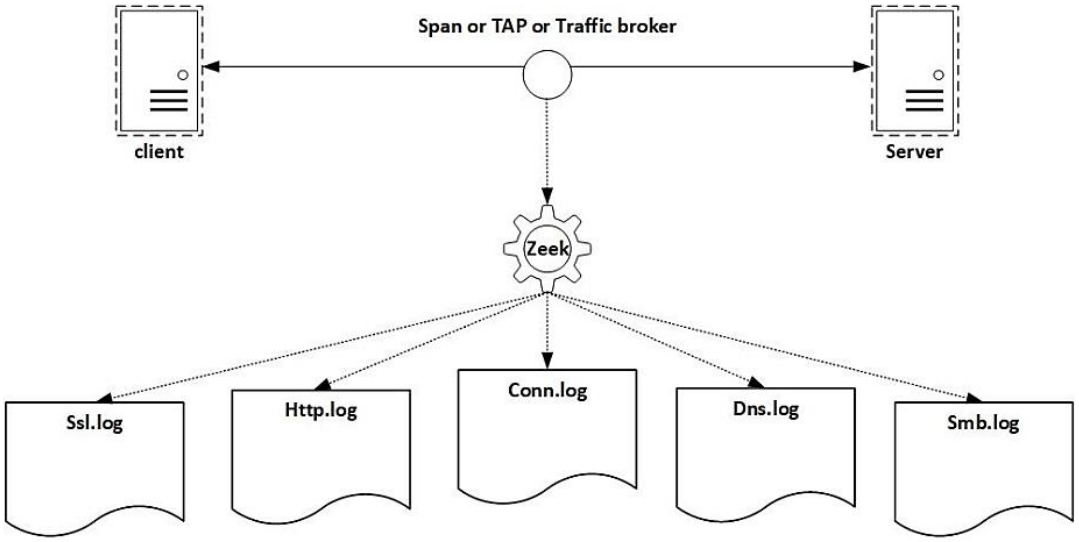
Na temelju ove arhitekture, *Suricata* je sposobna efikasno detektirati različite vrste napada, uključujući *DoS* napade, *Structured Query Language* (SQL) injekcije, *malware* komunikacije i druge prijetnje, sve u realnom vremenu. Mogućnost višeslojne detekcije i prilagodljivost prema specifičnim sigurnosnim politikama čini ovaj alat izuzetno korisnim za organizacije koje žele detaljan uvid i kontrolu nad mrežnim sigurnosnim prijetnjama.

5.3.2. Zeek

Zeek, ranije poznat kao *Bro*, sveobuhvatan je alat otvorenog koda za nadzor mreže koji se koristi za analizu mrežnog prometa s ciljem otkrivanja obrazaca ponašanja i potencijalnih prijetnji. Za razliku od nekih tradicionalnih IDS sustava koji pohranjuju cijele pakete za kasniju analizu, *Zeek* se fokusira na prikupljanje ključnih informacija i generiranje meta podataka iz zaglavlja paketa. Ovaj pristup omogućuje *Zeeku* detaljnu analizu mrežnih događaja i otkrivanje anomalija bez potrebe za pohranjivanjem cijelog mrežnog prometa, čime se smanjuje potrošnja resursa.

Ovaj alat koristi strategiju analize temeljenu na tokovima i otkrivanju anomalija. Detekcija se odvija u dvije faze. U prvoj fazi koristi se *Event Engine*, modul koji analizira podatke na višoj razini apstrakcije, radeći s grupama paketa umjesto s pojedinačnim paketima. Zbog ovakvog načina rada, Zeek je učinkovit u analizi složenih mrežnih događaja, iako može biti sporiji od klasičnog IDS sustava koji analizira promet na razini paketa. Međutim, Zeek omogućava bogatije informacije o mrežnim aktivnostima zbog fokusiranja na kontekstualnu analizu i slojevitu detekciju. Nakon prikupljanja podataka, skripte s politikama koriste se za analizu i procjenu podataka u drugoj fazi detekcije. Ove skripte omogućuju dublje razumijevanje mrežnih aktivnosti i identifikaciju potencijalnih prijetnji, pružajući fleksibilnost u definiranju prilagođenih pravila i politika.

Zeek funkcionira tako da presreće mrežni promet pomoću senzora opremljenog parserima za različite protokole. Ovi parseri raščlanjuju podatke i organiziraju ih u dnevničke (engl. *log*) datoteke specifične za protokole, a svaka je datoteka povezana s jedinstvenim identifikatorom koji predstavlja pojedinačnu mrežnu sesiju (Slika 8). Ovi logovi omogućuju analitičarima da precizno prate sesije i identificiraju sumnjive aktivnosti u mreži.



Slika 8.Zeek arhitektura analize mrežnog prometa, Izvor: *(Cronin, 2023)*

Na slici 8 je prikazan ovaj proces analize mrežnog prometa od klijenta do poslužitelja, pri čemu se promet distribuira putem uređaja kao što su mrežni preklopnik koji koristi funkciju *Switch Port Analyzer* (SPAN), fizički uređaj za presretanje prometa (engl. *Test Access Point, TAP*) ili uređaj za upravljanje prometom (engl. *Traffic Broker*), a zatim obrađuje pomoću *Zeeka*. Kombinirajući pristupe temeljene na tokovima, otkrivanju anomalija i metapodacima, *Zeek* smanjuje potrošnju resursa potrebnu za pohranu podataka, a istovremeno povećava preciznost i učinkovitost u detekciji. Kroz korištenje parsera za različite protokole i strukturiranje podataka u specifične dnevničke datoteke, *Zeek* omogućuje kontinuirano praćenje i analizu mrežnih sesija. Na taj način, *Zeek* postaje ključni alat za organizacije koje trebaju sveobuhvatan i skalabilan sustav za mrežni nadzor i otkrivanje prijetnji.

6. PROGRAMSKI PAKET SNORT

Snort je 1998. godine razvijen unutar organizacije *Sourcefire* kao odgovor na rastuću potrebu za učinkovitim sustavima za detekciju mrežnih napada. Isprva zamišljen kao „lagani“ sustav za detekciju napada, *Snort* se s vremenom razvio u cjeloviti IDS/IPS sustav. Zahvaljujući svojoj fleksibilnosti i mogućnostima prilagodbe, *Snort* je postao *de facto* standard za prevenciju i detekciju napada, s gotovo 4 milijuna preuzimanja godišnje, što potvrđuje njegovu popularnost i pouzdanost u mrežnoj sigurnosti. Definira ga niz pravila koja se koriste za detekciju zlonamjernih mrežnih aktivnosti, identificira pakete koji zadovoljavaju ta pravila i stvara upozorenja za korisnike ovog IDS/IPS sustava.

Snort se najčešće koristi u tri načina rada:

- kao *sniffer* paketa, slično alatu *tcpdump*, koji analizira mrežni promet i prikazuje TCP/IP pakete u stvarnom vremenu,
- kao *logger* paketa, što omogućava korisnicima da rješavaju probleme s mrežnim prometom,
- kao potpuni sustav za sprječavanje napada na mrežu.

Snort se može instalirati i konfigurirati kako za osobnu upotrebu, tako i za poslovne svrhe. Alat je otvoren za povratne informacije, omogućujući korisnicima da sudjeluju u unaprjeđivanju i ispravljanju pogrešaka, što doprinosi stalnom razvoju i napretku sustava. Jedini nedostatak je potreba za vrlo dobrim poznavanjem sintakse pravila i svih mogućnosti pri pisanju novih pravila kako bi se pravila mogla učinkovito kreirati.

6.1. Pravila u programskom paketu

Snort koristi jednostavan i fleksibilan jezik za opisivanje pravila. Prilikom razvijanja pravila, važno je pridržavati se nekoliko smjernica. Pravila moraju biti napisana u jednom retku jer *Snort* ne može obraditi višestruke retke. Pravila su podijeljena na dva dijela, zaglavlje pravila i opcije pravila. Zaglavlje pravila sadrži akciju pravila, protokol, izvorišne i odredišne IP adrese te mrežne maske, kao i informacije o izvorišnim i odredišnim brojevima priključnih točaka. Opcije pravila sadrže poruke upozorenja i informacije o dijelovima paketa koje treba pregledati kako bi se utvrdilo treba li poduzeti akciju.

Pravila u *Snortu* definiraju način na koji će alat prepoznati i reagirati na potencijalne

prijetnje unutar mrežnog prometa. U konfiguracijskom isječku 1 je prikazano pravilo koje detektira pokušaj preplavljivanja (engl. *overflow*) *modification time* (MDTM) zahtjevima u *File Transfer Protocol* (FTP) prometu.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP MDTM
overflow attempt"; flow:to_poslužitelj,established;
content:"MDTM"; nocase; isdataat:100,relative;
pcre:"/^MDTM\s[^\n]{100}/smi"; reference:bugtraq,9751;
reference:cve,2001-1021; reference:cve,2004-0830;
reference:nessus,12080; classtype:attempted-admin; sid:2546;
rev:5;)
```

Konfiguracijski isječak 1. Primjer pavila u *Snortu* za detekciju *FTP MDTM overflow* napada

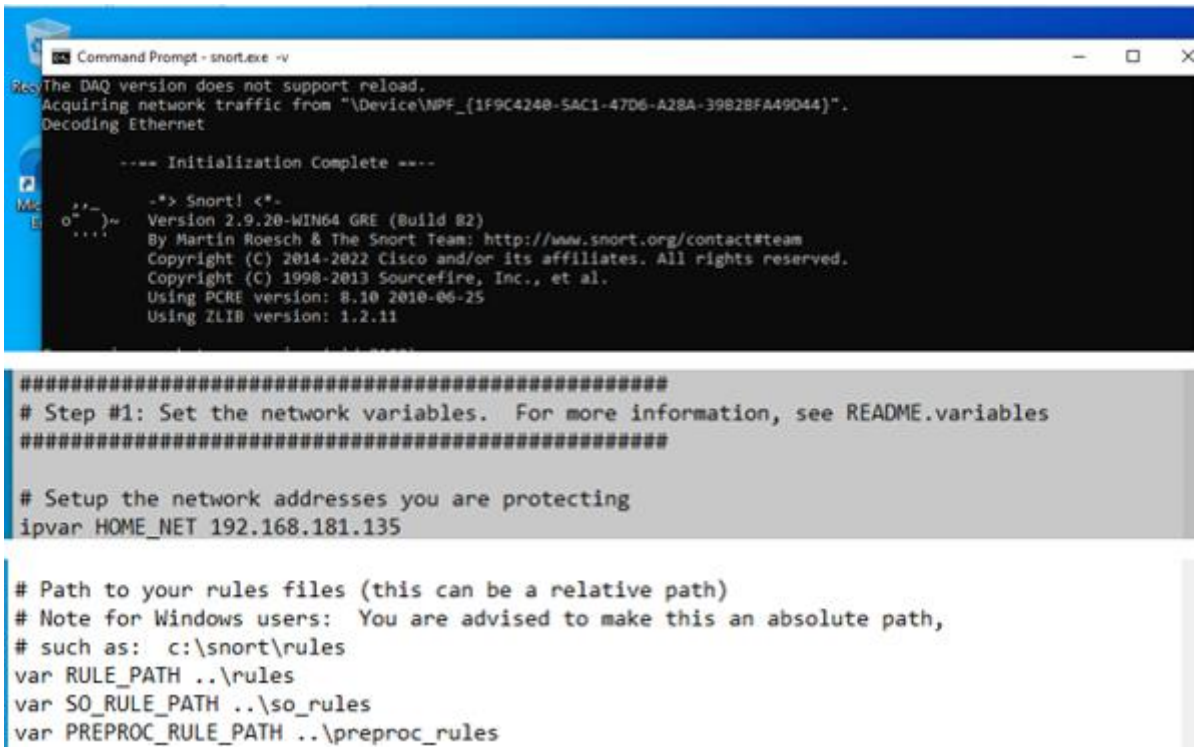
Detaljno objašnjenje prikazanog pravila:

- `alert tcp $EXTERNAL_NET any -> $HOME_NET 21` – definira pravilo za TCP promet koji dolazi s bilo kojeg vanjskog izvora ($EXTERNAL_NET) prema unutarnjoj mreži ($HOME_NET) na broju priključne točke 21 (FTP kontrolna priključna točka).
- `msg:"FTP MDTM overflow attempt"` – poruka koja će se prikazati u upozorenju.
- `flow:to_poslužitelj,established` – primjenjuje se na promet koji ide prema FTP poslužitelju i koji je već uspostavljen.
- `content:"MDTM"; nocase` – traži prisutnost niza "MDTM" (bez obzira na veličinu slova) u paketu.
- `isdataat:100,relative` – provjerava pojavljuje li se niz "MDTM" unutar prvih 100 bajtova podataka u paketu.
- `pcre:"/MDTM\s[\n]{100}/smi"` – koristi Perl-kompatibilan regularni izraz (PCRE) za dodatnu provjeru. Ovaj izraz traži MDTM nakon kojeg slijedi razmak i bilo kojih 100 znakova (osim novog reda).
- `reference:bugtraq,9751; reference:cve,2001-1021; reference:cve,2004-0330; reference:nessus,12080` – referenca na poznate ranjivosti i sigurnosne informacije.
- `classtype:attempted-admin` – klasifikacija napada kao "pokušaj administrativnog pristupa".
- `sid:2546; rev:5` – jedinstveni identifikator pravila i njegova revizija.

6.2. Instalacija i konfiguracija na Windows operacijskom sustavu

Instalacija *Snorta* na Windows operacijskom sustavu započinje preuzimanjem instalacijske datoteke sa službene web stranice *Snorta*. Tijekom instalacije, korisnik će biti upitan da odabere komponente koje želi instalirati i lokaciju za instalaciju *Snorta*. Za ispravno funkcioniranje *Snorta* na Windowsu, potrebno je instalirati *Npcap* upravljački program, koji omogućava „hvatanje“ mrežnog prometa. Nakon završetka instalacije, slijedi konfiguracija *Snorta* prema specifičnom okruženju. Ovo uključuje uređivanje pravila koja se nalaze u direktorijima "rules" i "preproc_rules".

Korisnici trebaju definirati varijable, poput $HOME_NET, u konfiguracijskoj datoteci "snort.conf", kako bi prilagodili postavke specifične za mrežno okruženje. Nakon toga, potrebno je prilagoditi putanje do pravila i postavke globalnih opcija u datoteci "snort.conf". Konfiguriraju se predprocesorski i izlazni moduli te se uključuju potrebni skupovi pravila pomoću ključne riječi *include*. Kada instalirate *Snort* na Windows OS, važno je osigurati da su sve putanje pravilno prilagođene, zamjenjujući znak "/" sa "" kako je prikazano na slici 9.



Slika 9. Prikaz Windows konfiguracije *Snort* alata, Izvor: izrada autora

6.3. Instalacija i konfiguracija na Ubuntu operacijskom sustavu

Instalacija *Snorta* na operacijskom sustavu Ubuntu slična je onoj na Windowsima, a najjednostavnije ju je izvesti putem terminala. Prije same instalacije *Snorta*, potrebno je ažurirati sustav, preuzeti nekoliko potrebnih knjižnica te skup biblioteka pod nazivom *Data Acquisition library* (DAQ), koji je nužan za ispravan rad *Snorta*. Nakon toga, potrebno je stvoriti direktorij u koji će se spremiti i instalirati programski paket *Snort*, te preuzeti pravila koja se potom raspakiraju u novostvorene direktorije.

Sljedeći korak je konfiguracija i dodavanje vlastitih pravila u datoteku "/etc/snort/rules/local.rules". Nakon što su pravila dodana, *Snort* se može pokrenuti i testirati. Ako je instalacija uspješno provedena, prilikom unosa naredbe `snort -version` u terminalu, prikazat će se poruka poput one prikazane na slici 10.

Slika 10. Prikaz Ubuntu instalacije *Snort* alata, Izvor: izrada autora

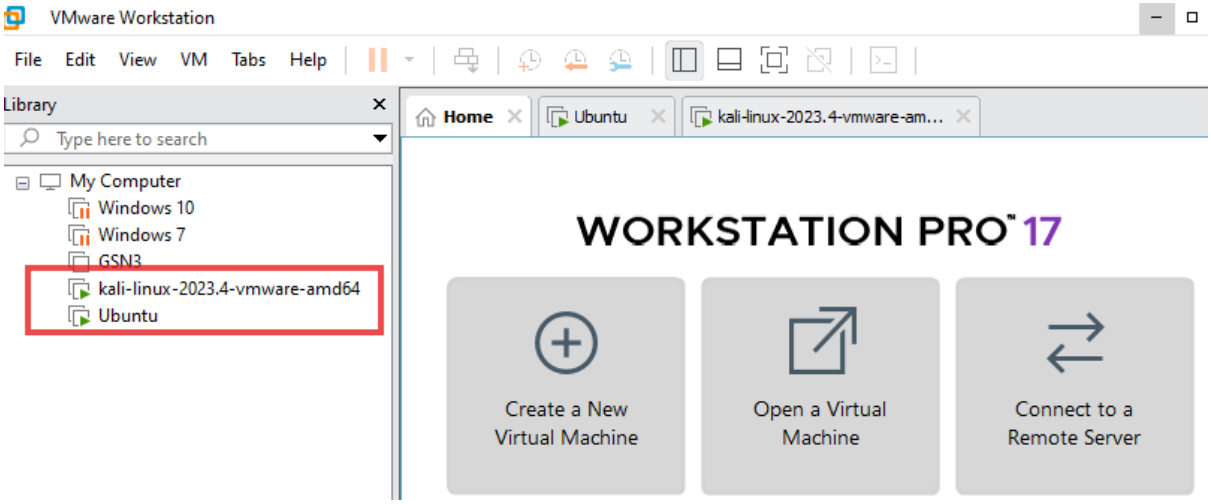
Pravilnom instalacijom i konfiguracijom, *Snort* postaje moćan alat za otkrivanje i prevenciju napada, pružajući mogućnost detaljne analize mrežnog prometa i brze reakcije na sigurnosne prijetnje. Njegova fleksibilnost u prilagodbi pravila i lakoća korištenja čine ga pogodnim za širok raspon korisnika, od malih mreža do velikih organizacija koje zahtijevaju naprednu razinu mrežne sigurnosti.

7. IMPLEMENTACIJA I TESTIRANJE SNORT ALATA U SIMULIRANOM OKRUŽENJU

Za ispitivanje učinkovitosti i rada programskog paketa *Snort* kreirana je virtualna okolina s dva računala na kojima su instalirani Linux sustavi Kali i Ubuntu. Ubuntu virtualni stroj (engl. *virtual machine, VM*) služi kao mjesto implementacije IDS-a, dok se napadi izvode s Kali virtualnog stroja. U edukativne svrhe izvode se *DoS* napadi s Linux Kali virtualnog stroja, dok je *Snort* konfiguriran za rad u *sniffer* modu. Ovakav pristup omogućuje simulaciju stvarnog mrežnog okruženja i procjenu sposobnosti *Snorta* u prepoznavanju i reagiranju na prijetnje. Korištenjem virtualnih strojeva osigurava se sigurno okruženje za testiranje bez rizika za stvarnu mrežnu infrastrukturu. Napadi su izvedeni tri puta s ciljem podizanja kapaciteta preplavljivanja i upoznavanja sa samim alatima koji se koriste u praktičnom dijelu rada.

7.1. Priprema i testiranje virtualnog okruženja

Testiranje i prikaz funkcionalnosti IDS-a zahtijevali su stvaranje virtualnog okruženja. Ovo je postignuto pomoću programskog paketa *VMware Workstation*, koji je namijenjen stvaranju virtualnih okolina. Prvo je instaliran Ubuntu virtualni stroj, koji ima ulogu žrtve i na kojem je implementiran *Snort*. Nakon toga, instaliran je Kali virtualni stroj, zbog svojih performansi i dizajna posebno pogodan za ulogu napadača. Prikaz pripremljenog virtualnog okruženja nalazi se na slici 11.



Slika 11. Prikaz virtualnog okruženja, Izvor: izrada autora

Oba virtualna stroja nalaze se na privatnoj mreži s dodijeljenim IP adresama. Kali Linux

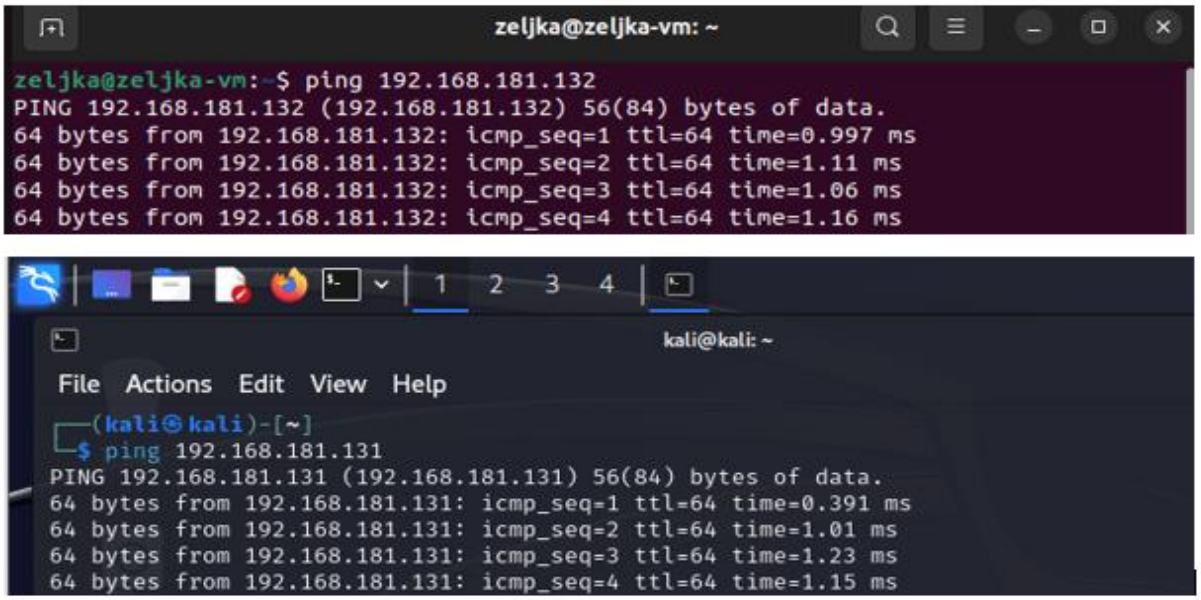
ima IP adresu 192.168.181.132, dok Ubuntu ima IP adresu 192.168.181.131.

Kreiranjem okruženja za izvođenje i testiranje praktičnog dijela rada, te definiranjem IP adresa potrebnih za testiranje povezanosti, postavljena je mrežna varijabla na Ubuntu stroju unutar programskog paketa *Snort*, kao što je prikazano na slici 12.

```
53
54 ##################################################
55 # Step #1: Set the network variables.  For more information, see README.variables
56 ##################################################
57
58 # Setup the network addresses you are protecting
59 #
60 # Note to Debian users: this value is overriden when starting
61 # up the Snort daemon through the init.d script by the
62 # value of DEBIAN_SNORT_HOME_NET s defined in the
63 # /etc/snort/snort.debian.conf configuration file
64 #
65 ipvar HOME_NET 192.168.181.131
66
```

Slika 12. Prikaz izmijenjene varijable u *Snortu*, Izvor: izrada autora

Nakon postavljanja varijable, mrežna povezanost testirana je pomoću `ping` naredbe u terminalu na virtualnim strojevima (Slika 13). Ova naredba omogućava provjeru jesu li oba virtualna stroja ispravno povezana unutar mrežnog okruženja i mogu li međusobno komunicirati. Uspješan odgovor na naredbu `ping` potvrđuje funkcionalnost mrežne konfiguracije i spremnost okruženja za izvođenje daljnjih testova napada (Slika 13).

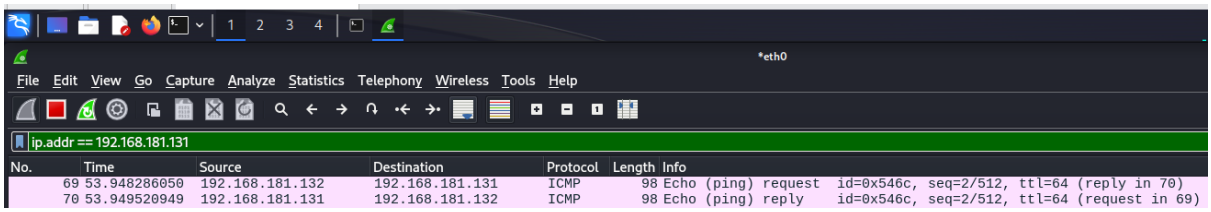


Slika 13. Prikaz rezultata naredbe `ping`, Izvor: izrada autora

7.2. Alati za izvođenje napada i mrežnu analizu

Unutar Kali virtualnog stroja za izvođenje napada pod nazivom *Ping Flood* napad korišteni su alati *Hping3* i *Wireshark*, koji su dostupni među aplikacijama na Kaliju. *Hping3* je alat koji se koristi za izradu i slanje prilagođenih TCP/IP paketa u svrhu testiranja mrežnih performansi, provjere pravila vatrozida, skeniranja priključnih točaka, provjere sigurnosti mreže i analize mrežnog prometa. U ovom praktičnom dijelu rada, *Hping3* će se koristiti za slanje velike količine *Internet Control Message Protocol* (ICMP) zahtjeva prema Ubuntu virtualnom stroju.

S druge strane, *Wireshark* je alat koji se koristi za snimanje i ispitivanje prometa na mreži te za proučavanje mrežne komunikacije. Njegova glavna svrha je „hvatanje“ paketa na mreži i pružanje detaljnog prikaza tih paketa. *Wireshark* prepoznaje više stotina protokola i prikazuje ih u strukturiranom i čitljivom formatu. U ovom slučaju, alat će se koristiti za analizu prometa prema Ubuntu virtualnom stroju, kako je prikazano na slici 14 gdje je vidljiv prikaz rezultata hvatanja za dva paketa na mreži s vremenom slanja paketa, IP adresa izvora i odredišta, korišteni protokol i osnovne informacije o mrežnom paketu.



Slika 14. Prikaz formata u *Wiresharku*, Izvor: izrada autora

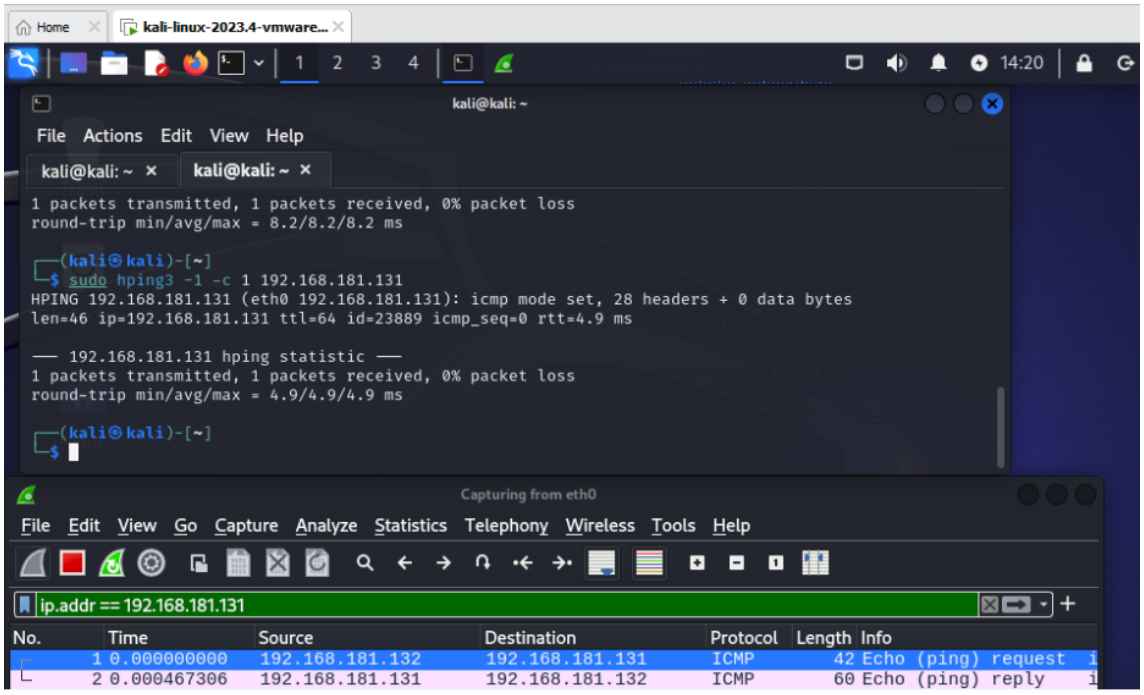
Prikazani promet uključuje dva ICMP paketa između dvije IP adrese, 192.168.181.132 (izvor) i 192.168.181.131 (odredište). Prvi paket je *ICMP Echo* zahtjev koji šalje Kali Linux virtualni stroj prema Ubuntu virtualnom stroju, dok je drugi paket *ICMP Echo* odgovor na taj zahtjev.

7.3. Simulirani napadi

Napad simuliran u ovom dijelu rada naziva se *Ping Flood*, poznat i kao *ICMP Flood*. Radi se o vrsti *DoS* napada u kojem napadač s jednog računala preplavljuje (engl. *flood*) ciljani uređaj `ping` zahtjevima, čime se onemogućava normalan promet i sustav postaje nedostupan. Ovaj napad koristi velik broj ICMP paketa kako bi preopteretio resurse ciljanog uređaja,

otežavajući mu odgovaranje na zahtjeve. Simulirana su tri različita napada kako bi se demonstrirala osnovna provjera detekcije sigurnosnih alata, testirala otpornost mreže na *DoS* napad te procijenila sposobnost sustava za detekciju u uvjetima s lažnim IP adresama koje prikrivaju izvor napada.

Prvi napad, koji je upućen s Kali virtualnog stroja u svrhu testiranja samih alata od strane privilegiranog korisnika sustava, izveden je slanjem jednog paketa pomoću alata *Hping3* naredbom `sudo hping3 -1 -c 1 192.168.181.131`. kao što je prikazano na slici 15, dok je *Wireshark* na istom stroju zabilježio ICMP paket kao odlazni *Echo (ping) request* i povratni *Echo (ping) reply*. Prvi paket prikazuje `ping` zahtjev poslan s Kali stroja, dok drugi paket prikazuje odgovor primljen od strane ciljanog stroja odnosno Ubuntu virtualnog stroja. Sam zapis potvrđuje uspješnu testnu komunikaciju između strojeva i ispravno hvatanje mrežnog prometa unutar *Wiresharka*.

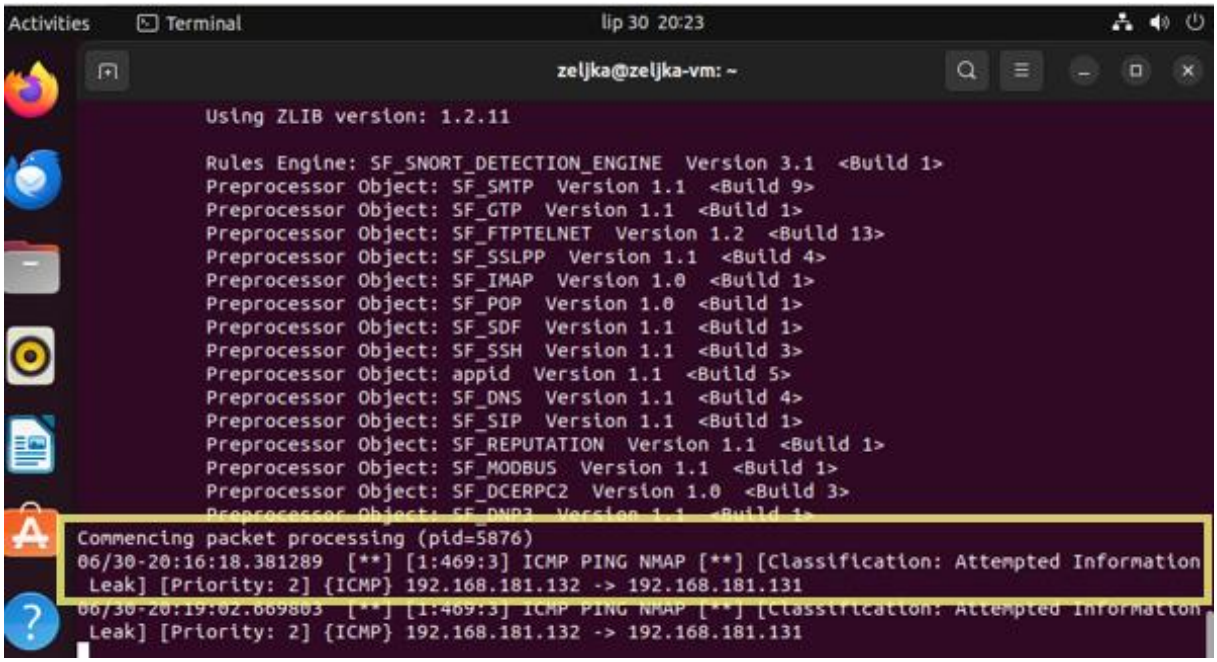


Slika 15. Slanje paketa s Kali virtualnog stroja, Izvor: izrada autora

Odgovor na slanje paketa zabilježen je također i unutar *Snort* alata na Ubuntu virtualnom stroju, gdje je prikazana IP adresa napadača i žrtve, kao što je vidljivo na slici 16.

Detalji prikazani na slici 16 uključuju poruku o započinjanju obrade paketa, koja označava početak analize mrežnog prometa, te vrijeme i datum detekcije sumnjive aktivnosti. *Alert* poruka prikazuje detektirani pokušaj "ICMP PING NMAP", što ukazuje na `ping` skeniranje mreže. Iako *Snort* navodi *Nmap* u opisu, stvarni napad je izveden korištenjem alata *hping3*,

koji može generirati obrasce ICMP prometa slične onima koje koristi *Nmap* za skeniranje, što je *Snort* detektirao i klasificirao kao pokušaj ping skeniranja. Klasifikacija napada je *Attempted Information Leak*, što znači da je *Snort* detektirao pokušaj odavanja informacija putem ICMP prometa. Prioritet upozorenja je 2, gdje manji broj označava veći prioritet za reakciju. Također su prikazane informacije o IP adresama izvora i odredišta, 192.168.181.132 (napadač) i 192.168.181.131 (ciljani uređaj). Administratori mreže mogu koristiti ove informacije za poduzimanje odgovarajućih mjera kako bi osigurali mrežnu infrastrukturu i spriječili daljnje upade ili curenje informacija.

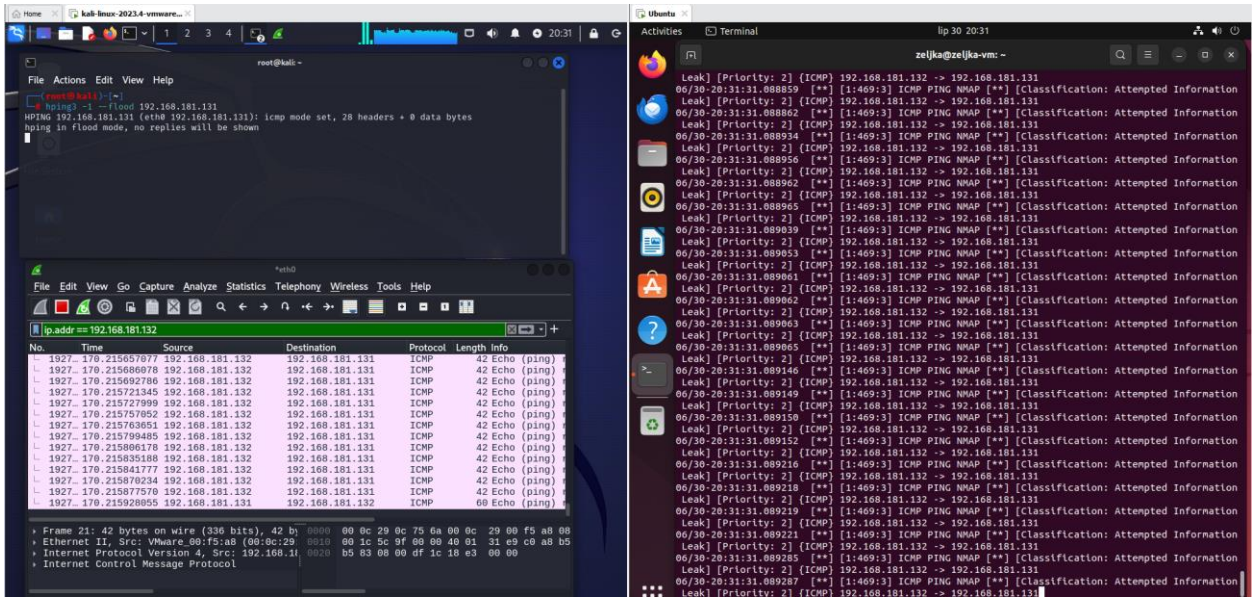


Slika 16. Hvatanje paketa unutar *Snorta*, Izrada: izrada autora

Nakon prvog napada daljnje demonstracije su izvedeni od strane administrativnog korisnika (engl. *root user*) sustava Kali u svrhu jednostavnijeg izvođenja *Dos* napada gdje nema potrebe za korištenjem naredbe `sudo` kod slanja ICMP prometa prema ciljanom uređaju.

Drugi napad na Ubuntu virtualni stroj, pri čemu je pomoću naredbe `hping3 -1 --flood 192.168.181.131` poslana maksimalna količina ICMP paketa. Ovaj napad nastoji preplaviti mrežne resurse ciljanog sustava, što otežava njegovu sposobnost da odgovori na legitimne zahtjeve. Odgovori na taj napad unutar korištenih alata na oba virtualna stroja prikazani su na slici 17. Na lijevoj strani, unutar Kali Linux virtualnog stroja, alat *Wireshark* bilježi veliki broj ICMP *Echo (ping) request* paketa poslanih prema IP adresi 192.168.181.131. Ti paketi, generirani u *flood* načinu rada, pokazuju pokušaj preplavljivanja mrežnog prometa. Na desnoj strani, unutar Ubuntu virtualnog stroja, *Snort* alat neprestano prijavljuje upozorenja

o pokušajima "ICMP PING NMAP" skeniranja, klasificirajući ih kao *Attempted Information Leak*. Ovaj kontinuirani niz upozorenja potvrđuje da je ciljani sustav preopterećen dolaznim prometom. Slika 17 na ovaj način prikazuje dvosmjerni pogled na rezultat *Ping Flood* napada. S jedne strane, masovno generiranje paketa, a s druge strane, detekcija i prijava sigurnosnog događaja, naglašavajući učinkovitost korištenih alata u identifikaciji i analizi ovakvih sigurnosnih prijetnji.



Slika 17. Prikaz *flood* napada, Izvor: izrada autora

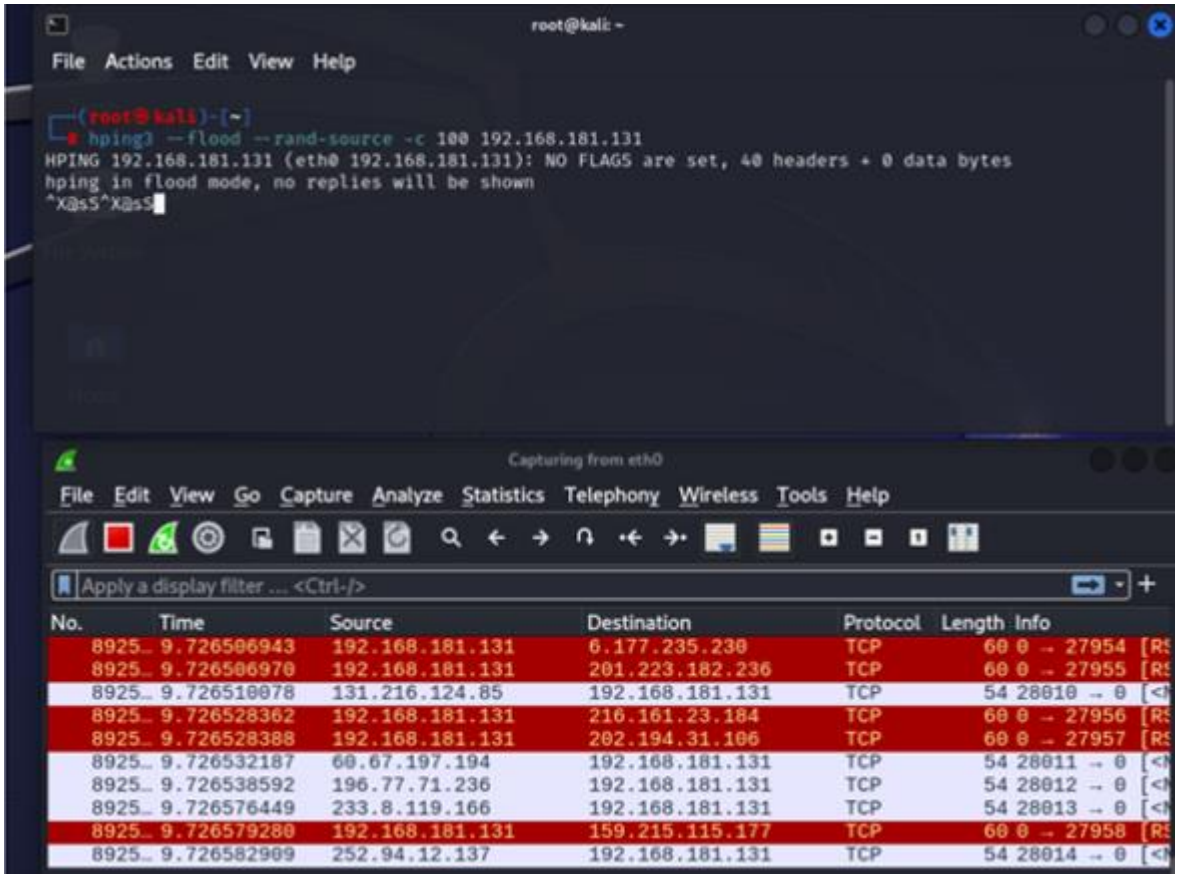
Treći napad izveden je također kao napad preplavljivanjem, ali ovaj put je IP adresa virtualnog stroja s kojeg je napad izvršen bila lažna. Lažiranje (engl. *spoofing*) uključuje manipulaciju IP adresom kako bi se prikrilo stvarno podrijetlo napada, zbog čega su alati na oba virtualna stroja bilježili različitu IP adresu za svaki paket, otežavajući identifikaciju izvora napada čime se učinkovito simulira stvarni scenarij *DoS* napada

Na slici 18 prikazan je rezultat simuliranog napada pomoću alata *hping3* na Kali virtualnom stroju. Administrativni korisnik pomoću naredbe `hping3 --flood --rand-source -c 100 192.168.181.131` uputio je 100 ICMP zahtjeva prema IP adresi 192.168.181.131, pri čemu su korištene nasumično odabrane IP adrese kao izvori napada. Opcija `--flood` omogućuje maksimalnu brzinu slanja paketa bez čekanja na odgovore, dok opcija `--rand-source` generira nasumične IP adrese kao izvore, simulirajući tzv. *IP Spoofing*.

Na gornjem dijelu slike prikazana je naredba u terminalu Kali virtualnog stroja, gdje

vidimo kako je alat postavljen u *flood mode* i ne prikazuje povratne odgovore, što je uobičajeno za ovu vrstu napada kako bi se postigla maksimalna efikasnost preopterećenja ciljanog uređaja.

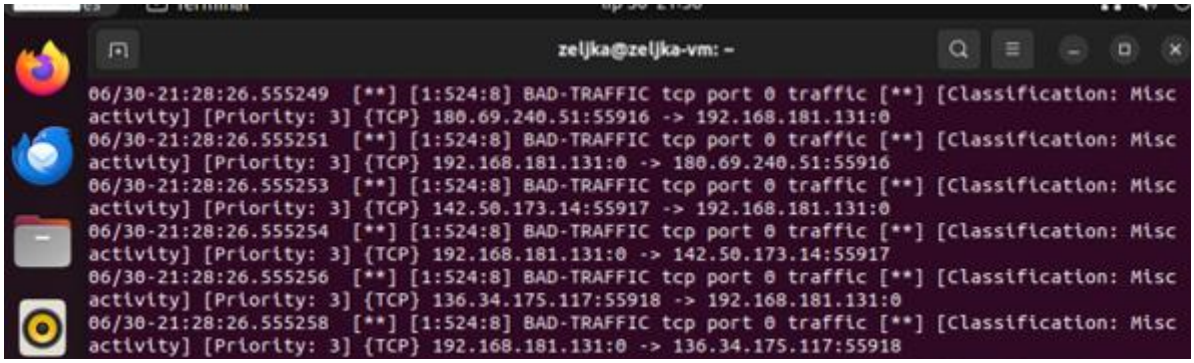
Donji dio slike prikazuje izlaz iz alata *Wireshark* na istom virtualnom stroju. Prikazani su TCP paketi koji su poslani prema ciljanom uređaju (192.168.181.131) s lažiranim IP adresama. Budući da ciljani uređaj prima neželjeni promet, u stupcu *Source* pojavljuje se i njegova IP adresa (192.168.181.131) jer uređaj šalje *TCP RST* pakete kao odgovor na dolazne pakete. Ovi RST paketi označeni su crvenom bojom u Wiresharku, što obično označava potencijalno kritičan ili sumnjiv promet, ukazujući na to da ciljani uređaj pokušava prekinuti veze ili odbiti neželjeni promet. Dakle, IP adrese u stupcu *Source* uključuju lažirane IP adrese generirane napadom, ali i IP adresu ciljanog uređaja koji reagira na dolazni promet, pokušavajući odbiti veze resetiranjem.



Slika 18. Prikaz *flood* napada s lažnim IP adresama unutar *Wiresharka*, Izvor: izrada autora

Ova vrsta napada služi za simuliranje stvarnih napada koji mogu ometati mrežne resurse ili omogućiti napadaču da prikrije svoj stvarni identitet. Snimljeni promet u *Wiresharku* pokazuje karakteristike prometnog preplavljivanja s mnogo različitih izvora, naglašavajući potencijalne izazove za mrežnu sigurnost i potrebu za naprednim tehnikama detekcije.

S druge strane, prikaz odgovora na napad u alatu *Snort* na Ubuntu virtualnom stroju bilježi dolazni promet kao "BAD-TRAFFIC", što ukazuje na veliki broj sumnjivih ili potencijalno opasnih TCP paketa usmjerenih prema ciljanom uređaju (slika 19). Ova klasifikacija "BAD-TRAFFIC" u *Snortu* znači da je detektiran promet koji krši standardne mrežne protokole ili politiku sigurnosti mreže, poput TCP prometa na broju priključne točke 0 koji se ne koristi u legitimnim komunikacijama.



Slika 19. Prikaz odgovora *flood* napada s lažnim IP adresama unutar *Snorta*, Izvor: izrada autora

Na slici 19 možemo vidjeti nekoliko zapisa koji detaljno opisuju ove događaje. *Snort* klasificira svaki paket s oznakom "BAD-TRAFFIC tcp port 0 traffic", a svi dolazni paketi uključuju lažirane IP adrese kao izvore napada, dok je IP adresa ciljanog uređaja (192.168.181.131) navedena kao odredište. To implicira da je ciljani uređaj izložen velikoj količini potencijalno opasnog prometa, čineći ga ranjivim na napade koji mogu iscrpiti resurse ili iskoristiti mrežnu infrastrukturu.

Kao što je prikazano, *Snort* daje informacije o svakom od tih sumnjivih paketa, uključujući vrijeme detekcije, korišteni protokol, IP adrese izvora i odredišta, kao i klasifikaciju i prioritet upozorenja. Ovo omogućava administratorima da brzo identificiraju vrstu prijetnje i poduzmu odgovarajuće mjere za zaštitu mreže i sustava.

8. ZAKLJUČAK

Rad istražuje ključne karakteristike računalnih mreža, njihove topologije, mrežne uređaje i metode adresiranja, kao i sigurnosne protokole koji se koriste za zaštitu podataka. Računalne mreže su temelj suvremenih informacijskih sustava, ali s njihovim širenjem i povećanom povezanošću dolazi do sve većih prijetnji kibernetičke sigurnosti. Zaštita podataka i infrastrukture od kibernetičkih napada je presudna za stabilno i sigurno funkcioniranje mreža u digitalnom dobu.

Jedan od glavnih izazova za računalne mreže je kibernetički kriminal, koji koristi sve sofisticiranije metode za napad na sustave. U tom kontekstu, analizirani sigurnosni protokoli, poput SSL/TLS-a, IPsec-a i SSH-a, pružaju različite razine zaštite i sigurnosne funkcionalnosti za siguran prijenos podataka i zaštitu komunikacijskih kanala. Za bežične mreže, koje su posebno ranjive na napade, protokoli poput WPA2 i WPA3 pokazali su se ključnima za unapređenje mrežne sigurnosti.

Važnost sigurnosti i dizajna mrežne strukture također je istaknuta kao ključni aspekt zaštite mrežnih sustava. Implementacija strategija poput segmentacije mreže, definiranja sigurnosnih zona i uporabe naprednih sigurnosnih uređaja i softvera omogućuje bolje upravljanje pristupom i smanjuju rizik od neovlaštenih upada. Sigurnosna politika temeljena na trijadi povjerljivosti, integriteta i dostupnosti pruža konkretne smjernice za organizacije i korisnike, osiguravajući cjelovitu zaštitu mrežnih resursa.

Ključni doprinos radu je analiza IDS i IPS alata kao što su *Suricata*, *Zeek* i *Snort*, koji koriste različite metode detekcije za prepoznavanje prijetnji i zaštitu mreža. Analiza pokazuje da ovi alati omogućuju višeslojni pristup sigurnosti, kombinirajući preventivne i detekcijske mjere koje značajno povećavaju otpornost mreža na kibernetičke napade. Poseban naglasak je stavljen na *Snort*, koji se pokazao učinkovitim u prepoznavanju različitih vrsta napada, uključujući *DoS* napade. Njegova fleksibilnost i mogućnost prilagodbe pravila čine ga pogodnim za široku primjenu u različitim mrežnim okruženjima, od manjih mreža do velikih organizacija.

Zaključno, rad naglašava da je mrežna sigurnost kontinuiran proces koji zahtijeva proaktivan pristup, stalnu prilagodbu i unapređenje sigurnosnih mjera. Organizacije trebaju ulagati u razvoj naprednih sigurnosnih tehnologija, kontinuiranu edukaciju korisnika te integraciju više sigurnosnih slojeva kako bi osigurale visoku razinu zaštite svojih informacijskih sustava.

LITERATURA

Alilović, A. (2019). *SUSTAVI ZA OTKRIVANJE I SPRJEČAVANJE NAPADA.* Zagreb: Fakultet elektronike i računarstva-FER.

Bace, R., & Mell, P. (2001). *Intrusion Detection Systems.* Gaithersburg: National Institute of Standards and Technology.

Centar Informacijske Sigurnosti (CIS). (2011). *Snort IDS.* Dohvaćeno iz cis.hr: https://www.cis.hr/dokumenti/2852-snortids.html

Cronin, B. (25. rujan 2023). *Network Security Monitoring (NSM) with Zeek.* Dohvaćeno iz Linkedin: https://www.linkedin.com/pulse/network-security-monitoring-nsm-zeek-brendan-cronin/

Fortinet Inc. (2024). *Cyberglossary.* Sunnyvaleu: Fortinet.

Hung-Jen Liao;Hung-Jen Liao ;Ying-Chih Lin ; Kuang-Yuan Tung. (2013). *Kuang-Yuan Tung.* Journal of Network and Computer Applications.

Kalapać, M., Dujmović, M., Jelić, D., Fistonić, M., & Guštin, M. (2012). *Detekcija i Prevencija upada - IDS/IPS.* FOI-OSS otvoreni sustavi i sigurnosti.

Kovačević, D. (2006). *Sigurnosna politika.* Zagreb: Fakultet elektronike i računarstva-FER.

Nacional CERT i LS&S. (2009). *Sigurnosni model mreže računala.* Zagreb: Hrvatska akademska i istraživačka mreža CARNet.

Nacionalni CERT. (2018). *Sigurnost bežičnih mreža.* Zagreb: Hrvatska akademska i istraživačka mreža - CARNET. Dohvaćeno iz https://www.cert.hr/wp-content/uploads/2019/03/Sigurnost-bezicnih-mreza.pdf

Oppliger, R. (04. Apr 2009). *SSL and TLS : theory and practice.* Boston,London: Artech House Publishers. Dohvaćeno iz studenti.rs: https://studenti.rs/skripte/ssl-i-tls-protokoli/

Ožegović, J., & Pezelj, I. (2000). *Projektiranje i upravljanje računalnim mrežama.* Split: Veleučilište u Splitu.

Phillips, G. (2022). *WEP vs. WPA vs. WPA2 vs. WPA3: Wi-Fi Security Types Explained*. Dohvaćeno iz makeuseof.com: https://www.makeuseof.com/tag/wep-wpa-wpa2-wpa3-explained/

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection.* National Institute of Standards and Technology.

Shah, S. A., & Issac, B. (2018). Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System. *Future Generation Computer Systems*, 157-170.

Stack, E. (2019). *Computer netvorking the complete guide.* Independently Published.

Suricata. (2016-2024). *What is Suricata.* Dohvaćeno iz docs.suricata.io: https://docs.suricata.io/en/latest/what-is-suricata.html

Šlekytė, I. (5. Jun 2023). *WEP, WPA, WPA2, and WPA3: Differences explained*. Dohvaćeno iz nordvpn.com: https://nordvpn.com/blog/wep-vs-wpa-vs-wpa2-vs-wpa3/

PRILOZI

Popis tablica

Popis slika