ANALIZA SIGURNOSTI I SIMULACIJA NAPADA NA BEŽIČNE MREŽE

Leko, Ivan

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Stručni diplomski studij Elektrotehnika

IVAN LEKO

ZAVRŠNI RAD

Analiza sigurnosti i simulacija napada na bežične mreže

Split, kolovoz 2024.

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Stručni diplomski studij Elektrotehnika

Predmet: Sigurnost mreža i usluga

ZAVRŠNI RAD

Kandidat: Ivan Leko

Naslov rada: Analiza sigurnosti i simulacija napada na bežične mreže

Mentor: Tonko Kovačević

Split, kolovoz 2024.

Sadržaj

Analiza sigurnosti i simulacija napada na bežične mreže

Sažetak:

U ovom radu analizirana je sigurnost bežičnih mreža i ključne metode zaštite od potencijalnih prijetnji. Fokus je bio na razumijevanju glavnih sigurnosnih protokola kao što su WPA, WPA2, SSID, 802.1x, CCMP i TKIP, te njihovih prednosti i nedostataka. Poseban naglasak stavljen je na moguće napade poput presretanja podataka, neovlaštenog pristupa i DoS napada. Također, istražene su najbolje prakse za osiguranje bežičnih mreža u privatnim i poslovnim okruženjima. Na kraju je odrađen i praktični dio simuliranja napada kako bi se demonstrirale stvarne prijetnje i učinkovitost obrambenih mjera.

Ključne riječi: sigurnost, WPA,SSID, 802.1x ,napadi

Security Analysis and Simulation of Attacks on Wireless Network

Summary:

This paper analyzed the security of wireless networks and key protection methods against potential threats. The focus was on understanding major security protocols such as WPA, WPA2, SSID, 802.1x, CCMP, and TKIP, along with their advantages and disadvantages. Special emphasis was placed on possible attacks such as data interception, unauthorized access, and DoS attacks. Best practices for securing wireless networks in both private and business environments were also explored. Finally, a practical simulation of attacks was conducted to demonstrate real-world threats and the effectiveness of defensive measures.

Keywords: security, WPA, SSID, 802.1x, attacks

1. UVOD

Razvoj tehnologije bežičnih komunikacija značajno je promijenio način na koji pristupamo informacijama i komuniciramo. Bežične mreže, poznate kao WLAN (eng. Wireless Local Area Network), postale su neizostavni dio suvremenog života, omogućujući korisnicima povezivanje na mrežu bez potrebe za fizičkom vezom. Ova praktičnost omogućava korisnicima slobodno kretanje i neometan pristup internetu s gotovo bilo koje lokacije unutar dosega mreže. Međutim, s povećanjem korištenja bežičnih mreža, povećala se i izloženost sigurnosnim prijetnjama, što čini pitanje sigurnosti ključnim aspektom njihove implementacije i uporabe. Potreba za sigurnošću bežičnih mreža proizlazi iz inherentnih karakteristika ove tehnologije. Za razliku od žičanih mreža, koje koriste fizičke veze za prijenos podataka, bežične mreže koriste radio valove koji se šire kroz zrak, što ih čini dostupnima ne samo legitimnim korisnicima nego i potencijalnim napadačima. Ova otvorenost prijenosa podataka povećava rizik od presretanja komunikacija, neovlaštenog pristupa i različitih oblika napada, uključujući prisluškivanje ('eavesdropping'), krivotvorenje podataka i Denial-of-Service (DoS) napade. U ranim fazama razvoja bežičnih mreža, sigurnosni mehanizmi bili su ograničeni i često nedovoljno učinkoviti. Primarni sigurnosni protokol, WEP (eng. Wired Equivalent Privacy), pokazao se ranjivim na brojne napade, što je dovelo do razvoja naprednijih protokola kao što su WPA (eng. Wi-Fi Protected Access) i WPA2. Ovi protokoli donijeli su značajna poboljšanja u pogledu enkripcije i autentifikacije, ali sigurnost bežičnih mreža i dalje ostaje dinamično područje koje zahtijeva kontinuirano unaprjeđenje zbog evolucije prijetnji i napadačkih metoda. Osim tehničkih izazova, sigurnost bežičnih mreža uključuje i niz organizacijskih i proceduralnih mjera. Implementacija sigurnosnih protokola zahtijeva pravilnu konfiguraciju mrežne opreme, redovito ažuriranje softvera i edukaciju korisnika o sigurnosnim prijetnjama i najboljim praksama. Upravo kombinacija tehničkih i organizacijskih mjera može osigurati cjelovitu zaštitu bežičnih mreža. Cilj ovog rada je detaljno analizirati sigurnosne aspekte bežičnih mreža, pregledati postojeće sigurnosne protokole i tehnologije, te identificirati najbolje prakse za zaštitu mreža od suvremenih prijetnji. Posebna pažnja bit će posvećena novim tehnologijama i standardima koji obećavaju povećanje sigurnosti bežičnih komunikacija u budućnosti. Kroz ovu analizu, rad će pružiti sveobuhvatan pregled trenutnog stanja sigurnosti bežičnih mreža i smjernice za njihovu daljnju zaštitu [1].

2. BEŽIČNE MREŽE

Skup računala, povezanih prijenosnim medijem, čini računalnu mrežu, koja može obuhvatiti bliže ili udaljenije lokacije. Danas su računala i računalne mreže najučinkovitiji način prijenosa velikih količina informacija u kratkom vremenu i na velike udaljenosti. Razvojem informatičke opreme, posebice radnih stanica i osobnih računala, otvara se mogućnost stvaranja raznovrsnih informatičkih mreža. Informatičke mreže omogućuju pristup najvećim nacionalnim instalacijama s mnogih međusobno udaljenih lokacija.

Koristeći radiofrekvencije, bežična mreža omogućuje komunikaciju između računala i drugih mrežnih uređaja. Često nazivane Wi-Fi mrežama ili WLAN-om (Wireless Local Area Network), ove mreže postaju sve popularnije zbog jednostavne instalacije bez potrebe za kablovima. Računala se mogu povezati bilo gdje u domu bez korištenja LAN kabela. Bežične mreže nude veliku fleksibilnost, omogućujući brzo postavljanje. Koristeći niz baznih stanica, spajaju korisnike na postojeću mrežu. Infrastruktura bežične mreže je visokokvalitetna, bez obzira na broj korisnika. Prvi uređaji temeljeni na danas široko korištenom IEEE 802.11b standardu pojavili su se sredinom 1999. godine. S rastom broja proizvođača i interesa kupaca, bilo je potrebno standardizirati koncept. U tu svrhu osnovana je 'Wireless Ethernet Compatibility Alliance', koja se bavi standardizacijom opreme za bežične mreže. Zahvaljujući ovoj udruzi, različiti standardi dobili su zajedničko ime. Danas mnoge mreže koriste metodu "spread spectrum", koja upravlja frekvencijom signala tako da paketi podataka putuju na različitim frekvencijama između odašiljača i prijemnika. Postoje dvije vrste "spread spectrum" sustava: 'frequency hopping' i 'direct sequence'. U 'frequency hopping spread spectrum' sustavu (FHSS) uređaji prelaze između različitih frekvencija, osiguravajući sigurniju i pouzdaniju komunikaciju. 'Direct sequence' sustavi osiguravaju pouzdanost emitiranjem u različitim, nasumično generiranim intervalima na jednoj frekvenciji.

Tehnologije koje zajednički nazivamo WLAN tehnologije definirane su skupom IEEE 802.11 standarda. Preciznije, WLAN tehnologije označene su kao 802.11b, 802.11a i 802.11g. U usporedbi s Ethernetom, brzine ovih mreža nisu velike. Naime, teoretska brzina najpopularnije bežične tehnologije – 802.11b – od 11 Mbps gotovo je deset puta manja od najpopularnijeg 100 Mbps Etherneta [2].

2.1 Primjene bežičnih mreža u poslovnom i privatnom okruženju

Bežične mreže danas igraju ključnu ulogu kako u poslovnom tako i u privatnom okruženju, omogućujući brzu, fleksibilnu i efikasnu povezanost među korisnicima i uređajima. U poslovnom svijetu, bežične mreže omogućuju radnicima da budu mobilni i produktivni bez obzira na njihovu fizičku lokaciju, što je naročito korisno u okruženjima poput ureda otvorenog tipa, skladišta, bolnica i obrazovnih ustanova. Mnoge organizacije danas koriste bežične mreže za pristup 'cloud' uslugama, daljinsko upravljanje resursima, kao i za podršku Internetu stvari (IoT), što dodatno unapređuje operativnu efikasnost. Primjerice, bežične mreže omogućuju zaposlenicima u velikim kompanijama brzi pristup informacijama i aplikacijama u realnom vremenu, olakšavajući komunikaciju i saradnju među timovima bez fizičkih ograničenja.

U privatnom okruženju, bežične mreže su osnova za kućne internet mreže, povezivanje mobilnih uređaja, laptopa, pametnih televizora, igraćih konzola i brojnih drugih uređaja. S obzirom na rastuću popularnost pametnih domova, bežične mreže igraju važnu ulogu u povezivanju uređaja poput pametnih termostata, sigurnosnih kamera, svjetala i glasovnih asistenata. Ovo omogućuje korisnicima kontrolu nad svojim domovima putem aplikacija, čak i kada su daleko.

Osim toga, bežične mreže omogućuju jednostavan pristup internetu u javnim prostorima poput kafića, aerodroma, hotela i trgovačkih centara, pružajući korisnicima slobodu da rade ili se zabavljaju dok su u pokretu. Ovo je posebno korisno za putnike i digitalne nomade, koji se oslanjaju na stabilne bežične mreže kako bi ostali povezani.

Iako bežične mreže pružaju mnoge prednosti u smislu fleksibilnosti i produktivnosti, njihova upotreba također nosi i određene sigurnosne izazove, posebno kada se koriste u okruženjima s velikim brojem korisnika ili kada se povezuje veliki broj uređaja. Stoga je važno osigurati visoku razinu sigurnosti kako bi se spriječili neovlašteni pristupi i zaštitili podaci u privatnom i poslovnom okruženju [2].

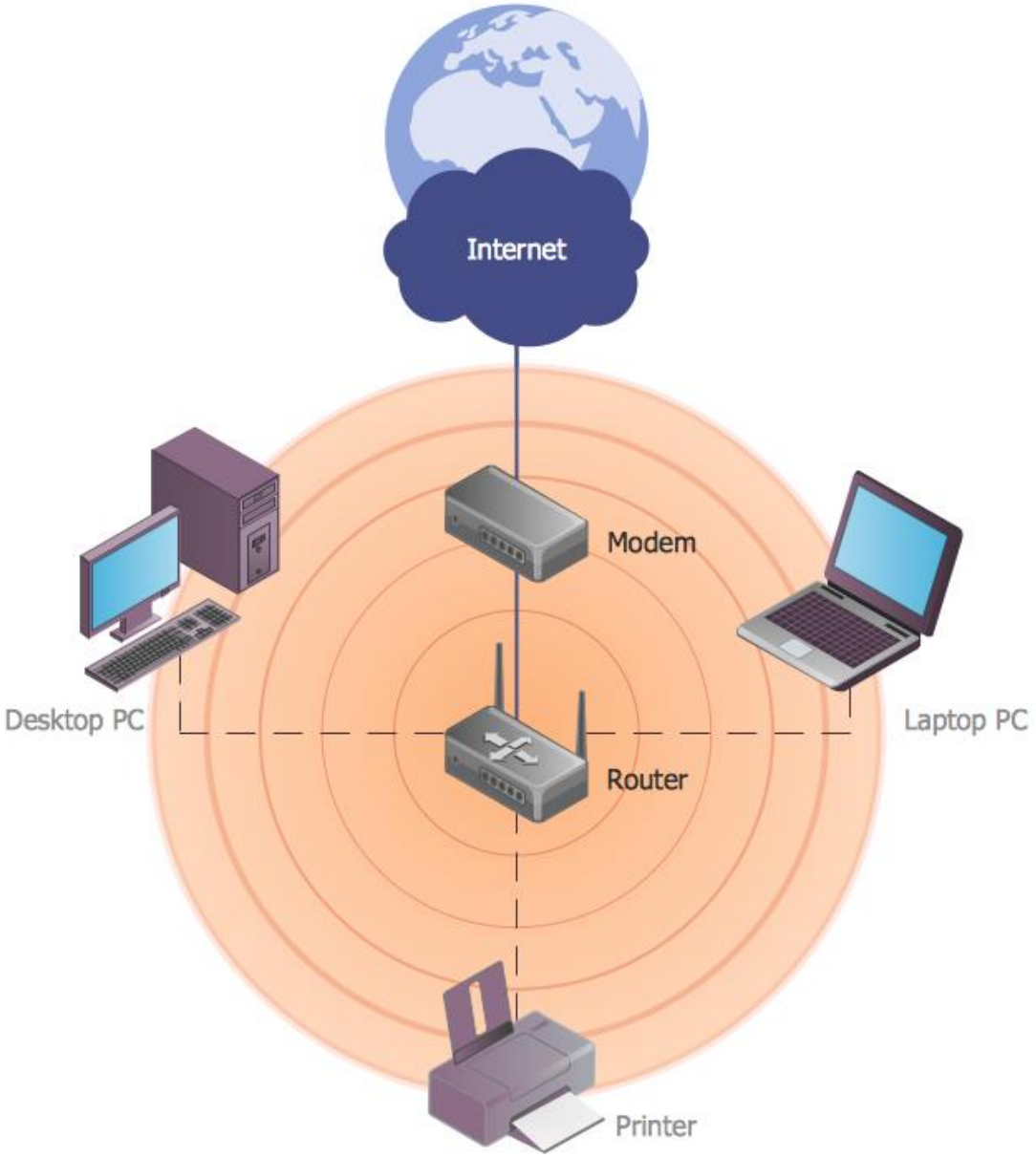
2.2 Prilagodljivost i učinkovitost bežičnih mreža

Bežične mreže pružaju brojne prednosti u odnosu na klasične žične mreže. Prva prednost koja se može navesti je bolja pokretljivost korisnika jer nisu ograničeni na kabel .Korisnici se mogu slobodno kretati ili biti bilo gdje unutar prostora pokrivenog radio signalom emitiranim od strane pristupne točke. Druga prednost je jednostavnija instalacija bežične mreže, jer je potrebna samo jedna pristupna točka koja može povezati više računala bez potrebe za dodatnim priključcima i kablovima. Ostale prednosti uključuju povećanu produktivnost, jednostavnu proširivost mreže i niže troškove.

No, unatoč ovim prednostima, bežične mreže imaju i određene tehničke nedostatke. Glavni nedostatak je sigurnost, jer antene odašilju signal unutar određenog radijusa, što može omogućiti neautoriziranim korisnicima da registriraju signal i pokušaju neovlašteno pristupiti mreži. Domet bežičnih mreža također može biti ograničen, što zahtijeva postavljanje više pristupnih točaka za pokrivanje većih područja. Pouzdanost bežičnog sustava može biti narušena smetnjama, interferencijama i drugim poremećajima uzrokovanim prijenosom signala putem radio valova. Brzina prijenosa podataka je još jedan značajan nedostatak, ali se stalno razvijaju nove tehnologije i sustavi koji omogućuju veću brzinu prijenosa.

Osim tehničkih aspekata, treba uzeti u obzir i praktične koristi bežičnih mreža. Na primjer, u poslovnom okruženju, bežične mreže omogućuju fleksibilnije radne prostore i olakšavaju timski rad jer se zaposlenici mogu slobodno kretati i povezivati s mrežom s bilo koje lokacije unutar ureda. U kućnom okruženju, bežične mreže omogućuju jednostavnije spajanje raznih uređaja poput pametnih telefona, tableta, pametnih televizora i drugih ″IoT″ uređaja, čime se stvara integriran i povezan dom.

Sveukupno, dok WLAN mreže imaju svoje izazove, njihove prednosti u smislu fleksibilnosti, mobilnosti i jednostavnosti postavljanja čine ih neizostavnim dijelom modernog umreženog svijeta [3].



Slika 2.1. Način rada bežične mreže [23]

2.3 Standardi bežičnih mreža

Standard IEEE 802.11 definira bežične mreže, a donio ga je IEEE. Ovaj standard pokriva najniža dva sloja OSI modela: fizički sloj i podatkovni sloj veze. Prva verzija standarda IEEE 802.11 formirana je sredinom 1997. godine, pri čemu je radna frekvencija za bežične Ethernet sustave određena na 2,4 GHz, uz dvije brzine prijenosa podataka – 1 Mb/s i 2 Mb/s. Standard je također ponudio dvije tehnologije prijenosa radio-signala: FHSS (Frequency Hopping Spread Spectrum) i DSSS (Direct Sequence Spread Spectrum). FHSS označava skakanje po

frekvencijama, dok DSSS označava niz skokova, a SS na kraju ovih skraćenica predstavlja razmazani spektar, tehnologiju prijenosa signala ispod razine šuma.

Razvoj bežičnih mreža kroz standard IEEE 802.11 značajno je doprinio povećanju njihove upotrebe i funkcionalnosti. Kroz godine, poboljšanja i nove verzije ovog standarda omogućile su veće brzine prijenosa podataka, bolju sigurnost i širu primjenu u različitim okruženjima. Na primjer, kasnije verzije kao što su 802.11n, 802.11ac i 802.11ax (Wi-Fi 6) donijele su znatna poboljšanja u pogledu brzine, kapaciteta i efikasnosti mreža.

Nisu svi stariji Wi-Fi standardi potpuno zastarjeli. Evo kratke povijesti Wi-Fi standarda i informacija o tome jesu li standardi još uvijek aktivni.

IEEE 802.11: Originalni standard stvoren 1997. godine, podržavao je maksimalnu brzinu veze od 54 Mbps. Uređaji koji koriste ovaj standard nisu proizvedeni već više od desetljeća i nisu kompatibilni s današnjom opremom.

IEEE 802.11a: Stvoren 1999. godine, ovaj standard radi na 5 GHz frekvencijskom pojasu s ciljem smanjenja interferencije jer mnogi uređaji koriste 2.4 GHz pojas. 802.11a postiže maksimalnu brzinu prijenosa podataka od 54 Mbps, ali 5 GHz frekvencija ima problema s preprekama u putu signala, pa je domet često loš.

IEEE 802.11b: Također stvoren 1999. godine, ovaj standard koristi 2.4 GHz pojas i može postići maksimalnu brzinu od 11 Mbps. 802.11b je standard koji je potaknuo popularnost Wi-Fi-ja.

IEEE 802.11g: Dizajniran 2003. godine, ovaj standard povećao je maksimalnu brzinu prijenosa podataka na 54 Mbps, zadržavajući pouzdani 2.4 GHz pojas, što je rezultiralo širokim usvajanjem.

IEEE 802.11n: Predstavljen 2009. godine, ovaj standard radi na 2.4 GHz i 5 GHz, podržava višekanalnu upotrebu i nudi maksimalnu brzinu prijenosa podataka od 150 Mbps po kanalu, što ukupno može dosegnuti 600 Mbps.

IEEE 802.11ac: Izdan 2014. godine, ovaj standard značajno povećava propusnost podataka za Wi-Fi uređaje do maksimalnih 1.300 Mbps. Također dodaje podršku za MU-MIMO, dodatne Wi-Fi kanale za 5 GHz pojas i više antena na jednom usmjerivaču.

IEEE 802.11ax: Ovaj standard, također poznat kao Wi-Fi 6, pruža teoretsku propusnost mreže do 10 Gbps, što je 30-40 posto poboljšanje u odnosu na prethodni standard. Povećava kapacitet

mreže dodavanjem pod-kanala za emitiranje, nadogradnjom MU-MIMO i omogućavanjem više istovremenih tokova podataka.

IEEE 802.11be: Specifikacije za ovaj standard još nisu konačne, ali je vrlo vjerojatno da će naslijediti 802.11ax. Prema IEEE 'Xplore' dokumentaciji, 802.11be će omogućiti udvostručenu propusnost i povećan broj prostornih tokova, što će omogućiti brzine prijenosa podataka do 40 Gbps.

Wi-Fi 8: U razvoju je novi standard Wi-Fi 8, čije je službeno ime trenutno IEEE 802.11bn.

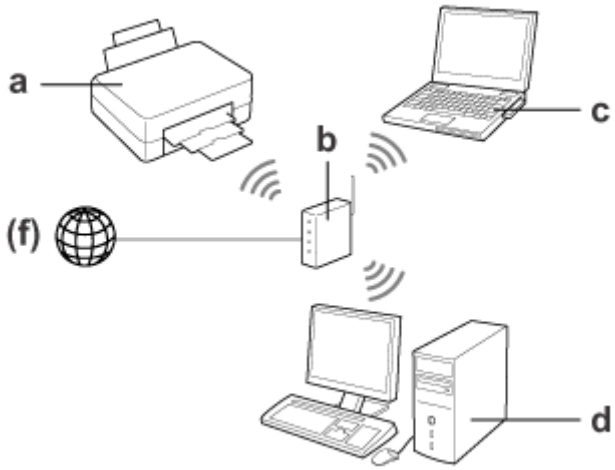
Dok su stariji standardi, poput IEEE 802.11 i 802.11a, uglavnom zastarjeli i ne koriste se u današnjim uređajima, noviji standardi poput 802.11ac i 802.11ax donose značajna poboljšanja u brzini, kapacitetu i pouzdanosti mreža. S obzirom na brzi tehnološki napredak, očekujemo da će novi standardi nastaviti unapređivati performanse bežičnih mreža, omogućujući bržu i pouzdaniju povezanost u različitim okruženjima [3].

2.4 Arhitektura bežičnih mreža

Dva glavna načina ostvarivanja bežičnih mreža, između kojih korisnik bira u skladu sa svojim potrebama i mogućnostima, su infrastrukturni i ad-hoc režim rada.

2.4.1 Infrastrukturni način rada

Kada govorimo o računalnim mrežama, infrastrukturni način rada se ostvaruje spajanjem uređaja putem pristupne točke, poput usmjerivača, bilo žičnim ili bežičnim putem. Ova karakteristika razlikuje infrastrukturni način rada od ad-hoc načina. Za postavljanje infrastrukturne mreže potrebna je najmanje jedna bežična pristupna točka (AP) te je neophodno da pristupna točka i svi klijenti budu konfigurirani za korištenje istog imena mreže (SSID). Pristupna točka je povezana na žičnu mrežu kako bi bežični klijenti mogli pristupiti mrežnim resursima. Dodatne pristupne točke mogu se povezati na mrežu radi povećanja dometa signala i podrške za više bežičnih klijenata [4].

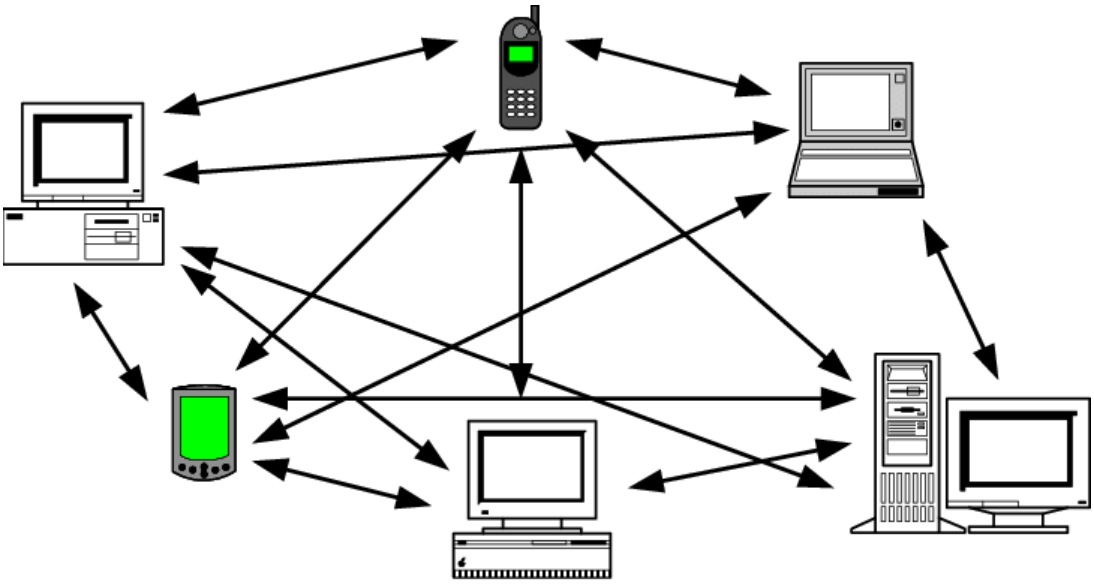


Slika 2.2. Infrastrukturni način rada [24]

2.4.2 Ad-Hoc način rada

Ad-hoc mreže, također poznate kao P2P (engl. peer-to-peer) mreže, omogućuju uređajima direktnu komunikaciju bez potrebe za centralnim uređajem. Ove mreže se obično sastoje od male skupine uređaja koji su u neposrednoj blizini. Bežična ad-hoc mreža povezuje više uređaja bez korištenja centralnog čvora, omogućujući svakom uređaju da prosljeđuje podatke drugim uređajima u mreži.

Zbog minimalne konfiguracije i brzog postavljanja, ad-hoc mreže su idealne za situacije koje zahtijevaju privremenu i jeftinu bežičnu lokalnu mrežu (WLAN). Također, ad-hoc mreže su korisne kao privremena zamjena u slučaju kvara opreme infrastrukturne mreže. Njihova fleksibilnost čini ih pogodnima za hitne situacije i privremena okupljanja, poput konferencija ili terenskih istraživanja. Nadalje, ad-hoc mreže omogućuju brz i jednostavan način povezivanja uređaja u okruženjima gdje nije moguće postaviti stalnu mrežnu infrastrukturu [4].



Slika 2.3. Ad-hoc način rada [25]

2.4.3 Usporedba infrastrukturnog i ad-hoc načina rada

U usporedbi s ad-hoc bežičnim mrežama, infrastrukturni način rada omogućuje centralizirano upravljanje mrežom i veći domet. Bežični uređaji mogu se povezati s resursima na žičanoj lokalnoj mreži, što je često u poslovnim okruženjima. Dodavanjem više pristupnih točaka može se smanjiti prometna zagušenost i proširiti domet mreže. Međutim, implementacija bežične infrastrukturne mreže je skuplja.

Ad-hoc mreže koriste P2P metodu povezivanja, što znači da su potrebni samo krajnji uređaji, a pristupna točka nije potrebna za međusobno povezivanje uređaja. Ukratko, infrastrukturni način rada omogućuje stabilnu topologiju. Javne ustanove i poslovni prostori rijetko koriste P2P mreže jer su previše decentralizirane i stoga neprikladne za njihove potrebe. Ad-hoc mreže koriste se za kratkotrajne svrhe kada je potrebno prenijeti podatke između uređaja koji su previše udaljeni za povezivanje putem infrastrukturne mreže.

Ad-hoc mreža je korisna za komunikaciju između nekoliko uređaja, ali nije prikladna za sve prometne zahtjeve, pa je tada potrebna infrastrukturna mreža. Mnogi bežični uređaji mogu raditi samo u infrastrukturnom načinu rada, što znači da moraju biti povezani putem pristupne točke [4].

3. SIGURNOST BEŽIČNIH MREŽA

Bežična mreža zahtijeva posebnu pažnju kada je riječ o sigurnosti. Mnogi korisnici nisu svjesni razine sigurnosti ili nesigurnosti svojih mreža. Nedovoljna zaštita i nepažnja mogu izložiti vaše podatke ozbiljnoj opasnosti. Najveći problem u vezi sa sigurnošću danas je nedostatak informiranosti. Mnogi korisnici vjeruju da su zaštićeni samo zato što posjeduju potrebne uređaje i osnovne postavke. Međutim, sigurnost zahtijeva više od postavljanja jedne lozinke.

Zaštita bežičnih mreža je složenija u usporedbi s žičanim mrežama i ne može se postići istim metodama. Svaki uređaj koji ima nezaštićen ili slabo zaštićen pristup internetu izložen je riziku. Virusi i neželjene poruke su postali uobičajeni problemi, no postoje i ozbiljnije prijetnje poput računalnih prijevara, napada uskraćivanjem pristupa i drugih oblika cyber napada.

Svaki put kada koristimo računalo i pristupamo internetu, izlažemo se određenim rizicima kao što su krađa identiteta, virusi, spam i spyware. Čak i naizgled bezopasne web stranice, poput onih za e-trgovinu ili online zabavu, mogu instalirati softver koji generira oglase (što usporava rad računala) ili prati naše aktivnosti na internetu. Mnogi korisnici, međutim, koriste internet bez ikakvih sigurnosnih mjera: nemaju vatrozid, antivirusni softver, niti su svjesni da prevaranti i hakeri stalno pretražuju internet u potrazi za novim žrtvama.

Wi-Fi mreže pružaju veliku praktičnost, ali narušavaju privatnost i sigurnost. Bežične kartice ili čipovi u našim računalima i pristupne točke zapravo su radio prijemnici, iako mali, koji koriste različite frekvencije od tradicionalnih AM/FM radija. Napadači mogu uhvatiti bilo koji uređaj unutar dometa zbog signala koji šalju naši uređaji ,oni to znaju i koriste softverske programe zvane prisluškivači koji im omogućuju praćenje nešifrirane bežične komunikacije. Ovi prisluškivači su bežični ekvivalenti uređajima za prisluškivanje telefonskih razgovora, s tom razlikom što mogu presresti e-poštu, te sve lozinke ili brojeve računa koji se prenose bežičnim putem.

Projektiranje bežične mreže na određenom području zahtijeva temeljit pregled prostora kako bi se odabrala optimalna vrsta antena i odgovarajuća snaga, uzimajući u obzir sva moguća ograničenja. Frekvencije koje koriste mreže prema standardima 802.11b i 802.11g, na 2,4 GHz, nelicencirane su, što može uzrokovati smetnje od drugih uređaja koji koriste istu frekvenciju, što može rezultirati prekidima u usluzi.

3.1 Sigurnosni standardi

Od 1990. godine, kada su bežične mreže postale popularne, javila su se brojna pitanja i sumnje u vezi s njihovom sigurnošću. Zbog tih problema i rizika, mnogi su smatrali da bežične mreže uopće ne bi trebale biti korištene. Međutim, zbog njihove jednostavnosti i praktičnosti, jasno je da bežične mreže moraju ostati, što znači da ih moramo zaštititi kako bismo osigurali sigurnost. Postoje tri glavna mehanizma, odnosno standarda, za zaštitu WLAN prometa,a opisat ćemo i još neke koji se koriste: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) i WPA2 (ažurirana verzija WPA koja koristi jači algoritam za zaštitu i teško je probiti).

3.1.1 WEP

Protokol koji je definiran u standardu 802.11 nastoji ispuniti osnovne funkcije :

- Povjerljivost: Primarna svrha WEP-a je spriječiti prisluškivanje mrežnog prometa.
- Kontrola pristupa: WEP također služi za kontrolu pristupa jer pristupne točke mogu zabraniti promet klijentima koji ne prođu uspješno proces autentifikacije.
- Integritet: Dodatno polje u svakom okviru koristi se za provjeru integriteta okvira.

U sva tri slučaja snaga WEP-a temelji se na poteškoći otkrivanja tajnog ključa pomoću napada čistom silom ('brute force attack'), ali postoje brži i učinkovitiji načini napada na WEP, o čemu ćemo kasnije govoriti [5].

WEP se primjenjuje na podatkovnom sloju OSI modela kako bi zaštitio podatke tijekom prijenosa. Oslanja se na tajnost ključa koji se koristi između pristupne točke i klijenta te pomoću njega enkriptira tijela okvira poruke. Proces enkripcije se odvija u sljedećim koracima:

1.Zaštitno kodiranje (checksumming)

Kako bi se očuvao integritet poruke, nad njom se primjenjuje zaštitno kodiranje koristeći CRC32 polinom. Ova zaštita se dodaje na kraj podataka koje želimo zaštititi. Rezultat je čisti tekst P koji se može izraziti kao P={M, c(M)}, gdje je M izvorni podatak. Važno je napomenuti da c(M), a samim tim i P, ne ovise o dijeljenom ključu k. Čisti tekst P tada služi kao ulaz za sljedeći korak.

2. Enkripcija

U drugom koraku, čisti tekst iz prethodnog koraka enkriptira se pomoću algoritma RC4. Odabiremo inicijalizacijski vektor (IV) na neki način (npr. slučajnim odabirom), koji zajedno s ključem k služi kao ulaz u RC4 algoritam. Kreira se niz bitova koji generira algoritam koristeći funkciju ključa k i inicijalizacijskog vektora. Ovaj niz bitova označava se kao RC(IV, k). Nakon

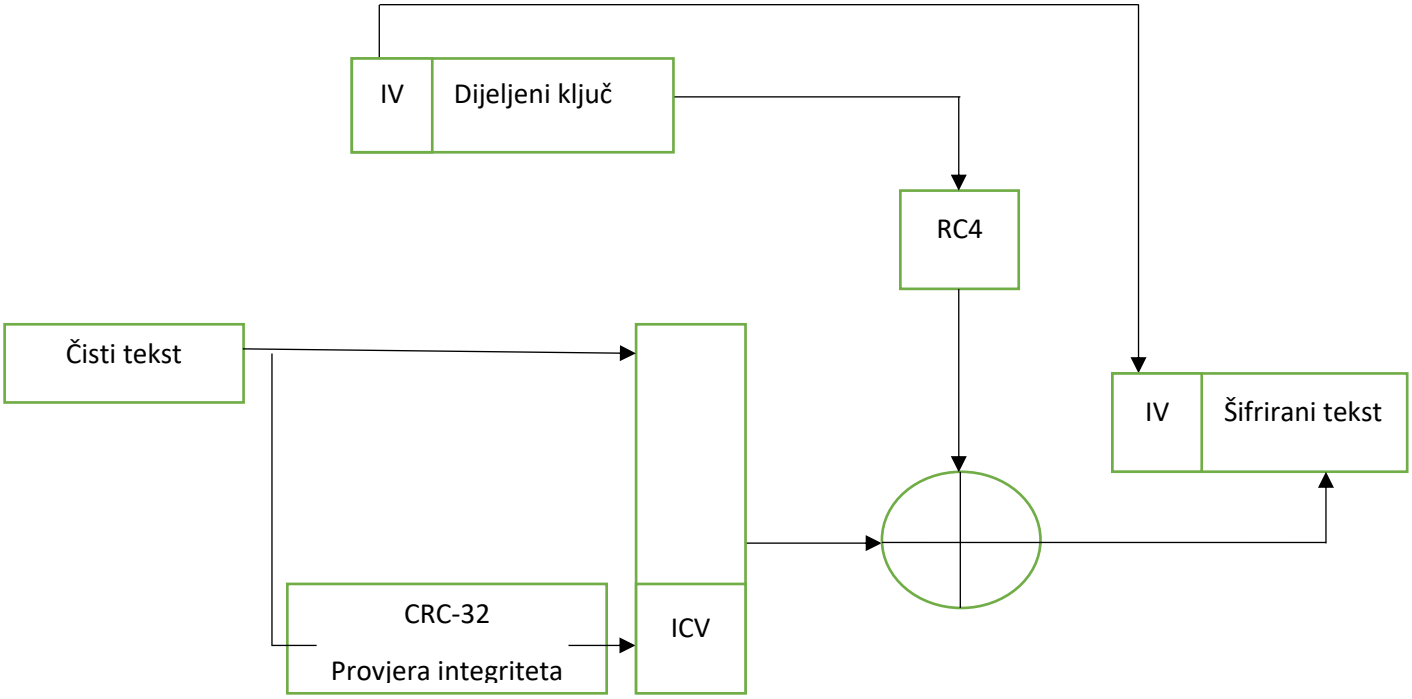
toga, nad bitovima čistog teksta i dobivenim nizom pseudo-slučajnih bitova primjenjuje se operacija ekskluzivno-ili (XOR) kako bi se dobio šifrirani tekst [6].

$$C = P \oplus RC\ (IV, k)$$

Jednadžba 3.1. WEP enkripcija

Završni korak je odašiljanje paketa koji se sastoji od IV vektora i šifriranog teksta preko bežične mreže.

Proces enkripcije prikazan je na sljedećoj slici:



Slika 3.1. Proces enkripcije teksta

3.1.2 WPA

WPA je predstavila organizacija 'Wi-Fi Alliance', koja okuplja proizvođače mrežne opreme, u suradnji s IEEE. WPA je razvijen kao odgovor na probleme uočenima kod WEP-a, s ciljem uklanjanja nedostataka uz zadržavanje kompatibilnosti s postojećom mrežnom opremom. WPA koristi TKIP (Temporal Key Integrity Protocol) za enkripciju i 802.1X standard s nekim od uobičajenih EAP protokola za autentifikaciju. Novost je i uvođenje MIC-a (Message Integrity

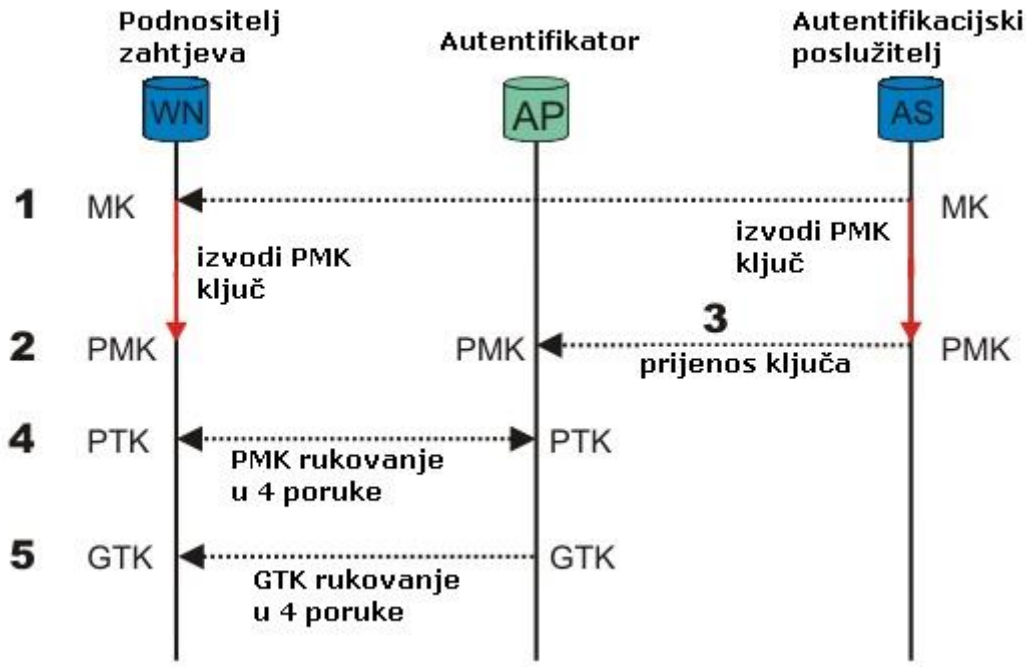
Check, poznatog i kao "Michael") kako bi se spriječilo krivotvorenje paketa. TKIP će biti detaljnije opisan u sljedećem poglavlju. Enkripcija se, zbog kompatibilnosti, provodi pomoću RC4 algoritma.

Prednost WPA je mogućnost jednostavne integracije u postojeću mrežnu opremu bez većih troškova. Dovoljno je instalirati nove upravljačke programe u pristupnim točkama i klijentskim mrežnim karticama kako bi se prešlo na novi standard. Prilikom kupovine nove opreme važno je osigurati da podržava WPA. Za velike korporativne mreže potrebno je dopuniti sustav s RADIUS poslužiteljem kako bi se autentifikacija mogla provoditi pomoću 802.1X standarda. Također, potrebno je odabrati tip EAP-a koji će se koristiti. Kako velike mreže imaju mnogo klijenata, neki proizvođači omogućuju rad u tzv. miješanom načinu, gdje se koriste i WEP (za klijente koji nisu instalirali nove upravljačke programe) i WPA. No, preporučuje se da prijelazna faza bude što kraća kako bi se postigla najbolja sigurnost. Za male kućne i uredske mreže predviđeno je da se autentifikacija provodi putem dijeljenih ključeva, kako bi se izbjegla potreba za RADIUS poslužiteljem.

Može se zaključiti da je WPA korak naprijed prema boljem i potpunijem standardu koji osigurava bežične mreže. Donosi mnoga poboljšanja uz prihvatljive troškove. Mnogo je isplativiji od današnjih IPsec rješenja i bolji jer djeluje na drugom sloju OSI modela.[7]

3.1.3 WPA2

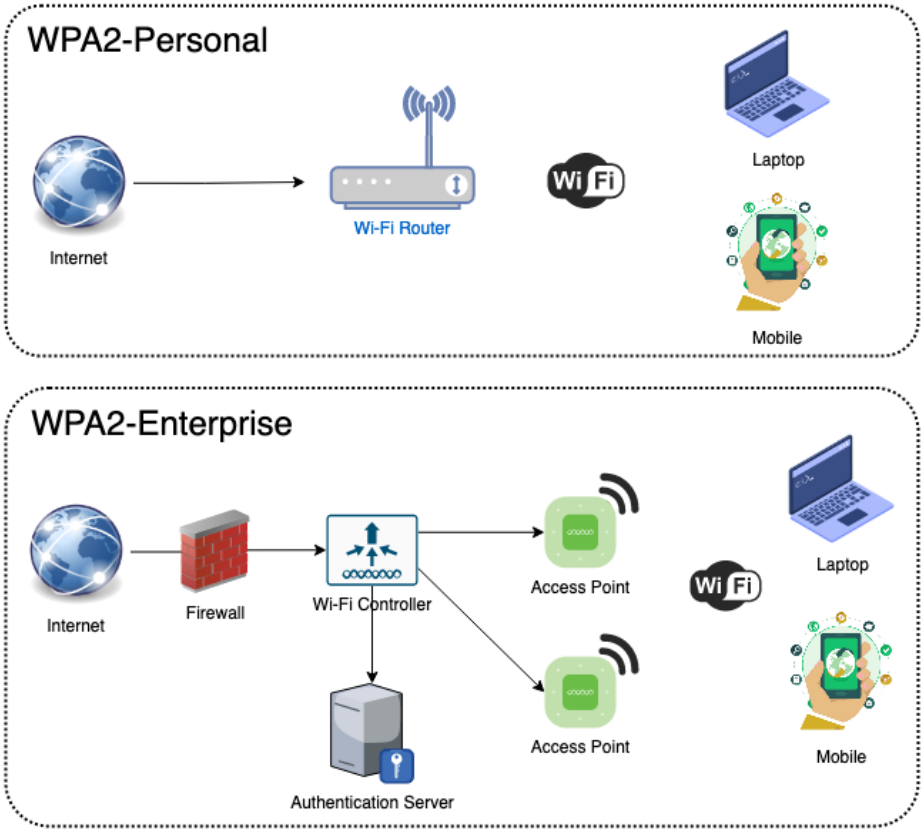
WPA2 je sustav za zaštitu bežičnih lokalnih mreža (WLAN – eng. Wireless LAN), razvijen kao odgovor na ranjivosti i nedostatke prethodnih WLAN sigurnosnih protokola, WEP i WPA. WPA2 osigurava korisničku autentifikaciju i enkripciju podataka. Autentifikacija se može provoditi u poslovnom načinu – između svakog uređaja u mreži i pristupne točke pojedinačno, ili u privatnom načinu – korištenjem zajedničkog ključa za sve uređaje (eng. 'Pre-shared Key'). Enkripcija u WPA2 sustavu koristi CCMP (eng. 'Counter Mode with Cipher Block Chaining Message Authentication Code Protocol') protokol, koji se temelji na AES simetričnom kriptografskom algoritmu. Ovaj dokument pruža pregled osnovnih karakteristika WPA2 zaštite, uključujući korištene algoritme i sigurnosne protokole koji su prethodili WPA2. Osim toga, opisane su arhitektura i specifičnosti bežičnih lokalnih mreža kako bi se bolje razumjela potreba i značaj korištenja WPA2 zaštite [8].



Slika 3.2. WPA2 autentifikacija [26]

Djelovanje WPA2 protokola može se opisati kroz dva načina a to su WPA2-Enterprise i WPA-2 Personal. Upotreba ovisi o zahtjevima mreže.

WPA2-Personal i WPA2-Enterprise su dvije varijante sigurnosnog protokola WPA2 dizajnirane za različite potrebe mreža. WPA2-Personal, poznat i kao WPA2-PSK (Pre-Shared Key), koristi zajednički ključ za autentifikaciju svih uređaja na mreži, što ga čini idealnim za kućne mreže i manje urede zbog jednostavnosti postavljanja i nepostojanja potrebe za dodatnom infrastrukturom. S druge strane, WPA2-Enterprise je namijenjen većim organizacijama i koristi RADIUS server za autentifikaciju, omogućujući individualne vjerodajnice za svakog korisnika i bolju kontrolu pristupa. WPA2-Enterprise pruža napredniju sigurnost kroz protokole poput EAP (Extensible Authentication Protocol), što smanjuje rizik od neovlaštenog pristupa i poboljšava upravljanje mrežom. Obje varijante koriste AES enkripciju putem CCMP protokola, ali WPA2-Enterprise nudi veću skalabilnost i fleksibilnost u upravljanju korisnicima. Glavna razlika između njih je u načinu autentifikacije: WPA2-Personal koristi statički ključ, dok WPA2-Enterprise koristi dinamičke ključeve i centraliziranu autentifikaciju [8].



Slika 3.3. Prikaz rada WPA2Personal i WPA2Enterprise [27]

3.1.4 SSID

Identifikator seta usluga (SSID) je niz znakova koji jedinstveno imenuje Wi-Fi mrežu. Ponekad se SSID naziva i nazivom mreže. Ovaj naziv omogućuje uređajima da se povežu s željenom mrežom kada više nezavisnih mreža radi u istom fizičkom području.

SSID-ovi se koriste u kućnim i poslovnim Wi-Fi mrežama, a najčešće ih se vidi prilikom povezivanja mobilnih uređaja poput prijenosnih računala ili pametnih telefona na bežičnu mrežu.

SSID može imati do 32 znaka. Bežični usmjerivači i pristupne točke emitiraju SSID-ove kako bi ih korisnici mogli pronaći i povezati se na bežičnu mrežu. Proizvođači usmjerivača često kreiraju zadane SSID-ove koristeći ime proizvođača uz dodatak nasumičnih brojeva i slova. Kako bi se smanjila zbrka u području s više bežičnih mreža, uobičajeno je mijenjati zadani SSID u neki drugi niz znakova.

Neke mreže mogu zahtijevati lozinku prije povezivanja, dok druge bežične mreže mogu prvo tražiti od korisnika da pročitaju i prihvate uvjete korištenja na internetu prije nego se povežu.

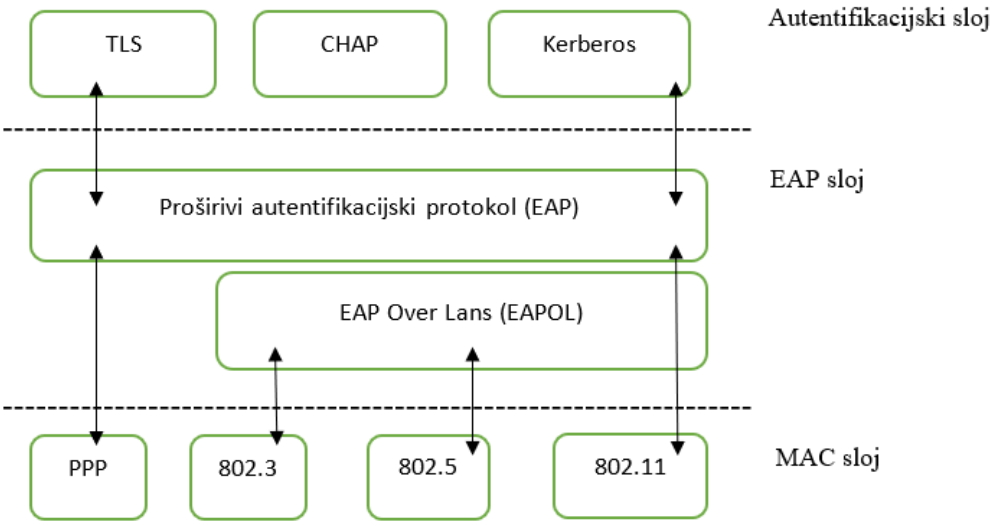
Skup bežičnih uređaja koji međusobno komuniciraju izravno naziva se osnovni skup usluga (BSS). Više BSS-ova može se spojiti kako bi formirali jedan logički segment bežične lokalne mreže (WLAN), poznat kao prošireni skup usluga (ESS). SSID je naziv od 1 do 32 bajta koji se dodjeljuje svakom ESS-u. Svaka pristupna točka oglašava svoju prisutnost nekoliko puta u sekundi emitiranjem signala koji nose naziv ESS-a.

Standardi arhitekture WLAN-a Instituta inženjera elektrotehnike i elektronike (IEEE) 802.11 propisuju da SSID treba biti priložen zaglavljima paketa kada se šalju putem WLAN-a. Ovo osigurava da su podaci poslani i primljeni u pravoj mreži.[9]

3.1.5 802.1x standard

Standard 802.1X pruža arhitekturu koja omogućuje korisnicima razne metode autentifikacije, kao što su autentifikacija certifikatima, pametnim karticama i jednokratnim lozinkama. Ovaj standard omogućuje pristup mreži temeljen na portovima za mrežne tehnologije kao što su Token Ring, FDDI, 802.11 i 802.3 LAN. 802.1X osigurava sigurnost apstrahiranjem tri osnovna entiteta: klijent ('supplicant'), autentifikator (obično mrežni port) i autentifikacijski poslužitelj. Klijent koristi usluge koje autentifikator nudi preko svojih portova. Autentifikator može biti mrežni preklopnik ili pristupna točka. Klijent se autentificira putem autentifikatora kod autentifikacijskog poslužitelja, koji tada autentifikatoru nalaže da dozvoli pristup klijentu u mreži. Pretpostavlja se da svi autentifikatori komuniciraju s istim centralnim autentifikacijskim poslužiteljem. U praksi, taj poslužitelj može biti fizički raspoređen na više lokacija radi rasterećenja, ali se logički smatra jedinstvenim.

Standard 802.1X koristi EAP (Extensible Authentication Protocol) kao temelj za razne autentifikacijske mehanizme. EAP je izgrađen na paradigmi izazov-odgovor ('challenge-response'). Iako je EAP prvotno razvijen za korištenje u žičanim mrežama, kasnije je prilagođen i za bežične mreže. Struktura EAP-a može se prikazati slijedećom slikom:[10]



Slika 3.4. Struktura EAP-a

Imamo 4 osnovna tipa poruka u protokolu:

- EAP zahtjev (EAP Request)
- EAP odgovor (EAP Response)
- EAP uspjeh (EAP Success)
- EAP neuspjeh (EAP Failure)

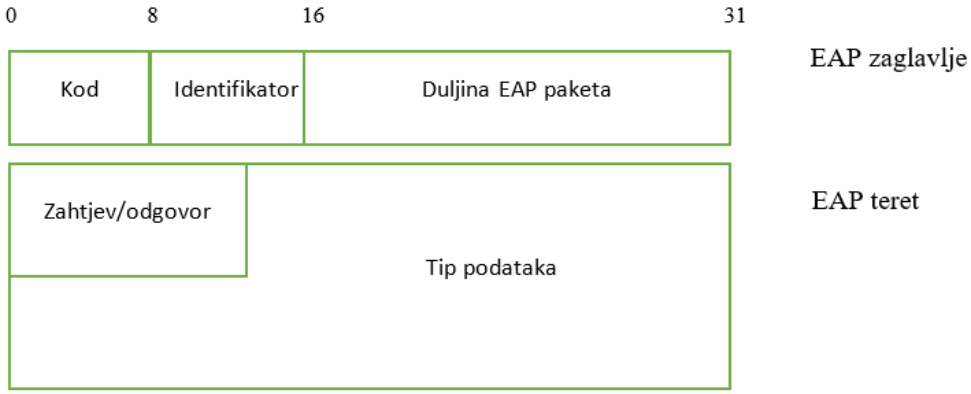
EAP zahtjev je izazov koji supplicant šalje autentifikatoru, dok je EAP odgovor supplicanta na izazov autentifikatora. Ostale dvije poruke, EAP uspjeh i EAP neuspjeh, obavještavaju supplicanta o ishodu autentifikacije.

Kada se EAP koristi u bežičnoj mreži, sam EAP paket se enkapsulira unutar EAPoL (EAP over LAN) paketa. EAPoL paketi omogućuju komunikaciju između supplicanta i autentifikatora preko mreže.

Postoje tri vrste EAPoL paketa:

- EAPoL Start: Inicira autentifikacijski proces kod autentifikatora.
- EAPoL Logoff: Šalje obavijest autentifikatoru o odjavljivanju korisnika s mreže
- EAPoL Key: Prevozi informaciju o dijeljenom WEP ključu.

EAP paket unutar EAPoL paketa prikazan je na sljedećoj slici:



Slika 3.5. EAPOL paket

EAP je protokol koji omogućuje proširivost jer može enkapsulirati različite metode autentifikacije unutar EAP zahtjeva/odgovora. On operira na drugom (podatkovnom) sloju OSI modela. Centralizacija autentifikacije preko RADIUS poslužitelja je preferirano rješenje jer omogućuje efikasno upravljanje autentifikacijom svih korisnika, za razliku od pristupa gdje bi svaki port bio odgovoran za autentifikaciju pojedinog korisnika. Za pristup mreži, pristupna točka mora propuštati EAP pakete prema poslužitelju. Autentifikator koristi dualni način rada portova: nekontrolirane portove koji dopuštaju samo EAP promet i kontrolirane portove koji omogućuju normalan promet nakon uspješne autentifikacije. Ovaj model je kompatibilan s klijentima koji ne podržavaju 802.1X standard, omogućujući administratorima da usmjeravaju njihov promet na nekontrolirane portove kako bi im omogućili pristup mreži.[10]

3.1.6 CCMP i TKIP protokol

CCMP se smatra boljim i trajnim rješenjem za zaštitu podataka u bežičnim računalnim mrežama. Temelji se na AES (Advanced Encryption Standard) algoritmu u CCM (Counter Mode Encryption with CBC-MAC Data Origin Authenticity) načinu rada. CCM koristi jedan ključ za enkripciju i zaštitu integriteta podataka, što znači da se paket enkriptira i autentificira istovremeno. CCM je specijalno dizajniran za 802.11i standard i predviđen je za rad isključivo s blokovima podataka, bez planova za prilagodbu tokovima podataka. CCM radi s 128-bitnim blokovima podataka. U CBC-MAC načinu rada, prvi blok podataka se enkriptira pomoću AES-a, zatim se provodi operacija ekskluzivno-ili s drugim blokom podataka i ponovo enkriptira, te se taj proces ponavlja sve do posljednjeg bloka. Rezultat je 64-bitni kod koji se dodaje na kraj paketa podataka i služi za zaštitu integriteta.

TKIP je razvijen kao nadogradnja postojećeg WEP-a kako bi se otklonile njegove sigurnosne slabosti. IEEE je prepoznao sve nedostatke u dizajnu WEP-a i odlučio ih ukloniti uz zadržavanje kompatibilnosti s postojećom mrežnom opremom. Cilj je bio omogućiti nadogradnju trenutne mrežne opreme putem softverske promjene, bez značajnog opterećenja za hardver koji se uglavnom sastoji od ARM7 ili i386/486 računala. TKIP koristi dijelove sklopovlja koje WEP nije koristio, čime se izbjegava značajno smanjenje performansi mreže.

TKIP je otklonio probleme WEP-a kroz sljedeće promjene:

- Inicijalizacijski vektor je povećan s 24 na 48 bita, čime se sprječava enkripcija dva paketa istim vektorom.
- Dinamička raspodjela ključeva, miješanje ključeva i bolja zaštita integriteta paketa. U TKIP-u je velika pažnja posvećena složenom problemu raspodjele ključeva, za razliku od WEP-a.
- Izbjegavanje kriptografski slabih ključeva koji su se pojavljivali u WEP-u.

Proces dobivanja ključeva u TKIP-u se sastoji od dvije faze:

- Vremenski ključ ('temporal key') veličine 128 bita miješa se s klijentskom MAC adresom ('transmitter address') veličine 48 bita i s najznačajnijih 32 bita inicijalizacijskog vektora, čime se dobiva privremeni ključ veličine 80 bita. Vremenski ključ poznaju i pošiljatelj i primatelj paketa.
- Privremeni ključ dobiven u prvoj fazi ponovo se miješa s vremenskim ključem i preostalih 16 bita inicijalizacijskog vektora.[11]

4. NAPADI NA BEŽIČNE MREŽE

Prije nego što se upustimo u analizu sigurnosnih propusta u standardu, ključno je razmotriti koliko je napad na bežičnu računalnu mrežu izvodiv u praksi. Prvi korak svakog napada je pristupiti signalu mreže, što omogućava provođenje aktivnog ili pasivnog napada. Za pasivan napad napadač mora imati opremu koja može presretati promet između pristupne točke i klijenta te mora dobro poznavati fizički sloj definiran standardom 802.11. Aktivni napad zahtijeva dodatno opremu koja može odašiljati podatke na mrežu. Pouzdana oprema za ove svrhe može biti značajno skupa.

Proizvođači bežične opreme često zanemaruju napade na podatkovnom sloju, smatrajući ih nepraktičnima i teško izvedivima. Ovo je pogrešno iz dva razloga. Prvo, postoje napadači koji imaju dovoljno resursa i vremena da ulože značajna sredstva i trud kako bi dobili pristup podacima. Industrijska špijunaža je dobar primjer, s obzirom na njezinu profitabilnost. Na primjer, procurio je dio izvornog koda Windowsa 2000, a nedavno je Cisco prijavio krađu najnovijeg operativnog sustava za novu generaciju usmjerivača.

Drugo, oprema potrebna za praćenje i aktivni napad je široko dostupna u obliku bežičnih kartica za stolna ili prijenosna računala. Praktični pasivni napadi su izvedeni s takvim karticama putem modificiranih upravljačkih programa. Na primjer, PCMCIA kartica Orinoco tvrtke Lucent omogućuje izmjenu upravljačkih programa (reverznim inženjerstvom) kako bi se mogao ubaciti proizvoljan promet u mrežu, čime se može izvesti aktivan napad. Iako je vrijeme potrebno za takav zadatak značajno, to se mora napraviti samo jednom, jer se gotovi upravljački programi mogu objaviti na internetu i tako postati dostupni svima.

Dakle, razumno je zaključiti da dovoljno motiviran napadač može dobiti puni pristup podatkovnom sloju i provoditi pasivne ili aktivne napade [12].

4.1 Provjera identiteta korisnika

U bežičnim mrežama, autentifikacija je ključna za osiguravanje pristupa mreži samo ovlaštenim korisnicima. Dva najčešća tipa autentifikacije su Open System Authentication (OSA) i Shared Key Authentication (SKA). Ovi sistemi imaju različite mehanizme provjere identiteta, što utječe na sigurnost mreže.

Open System Authentication (OSA):

'Open System Authentication' je osnovni i najjednostavniji oblik autentifikacije u bežičnim mrežama. U ovom sistemu, korisnik ili uređaj jednostavno šalje zahtjev za autentifikaciju pristupnoj točki (AP). AP uvijek prihvaća ovaj zahtjev bez provjere identiteta korisnika. Proces uključuje sljedeće korake:

- Zahtjev za autentifikaciju: Klijent šalje zahtjev za autentifikaciju AP-u.
- Odobrenje: AP odgovara s odobrenjem zahtjeva.

Zbog svoje jednostavnosti, OSA je ranjiva na neovlaštene pristupe jer ne koristi nikakvu enkripciju ili provjeru identiteta. To znači da se bilo koji uređaj unutar dometa AP-a može povezati s mrežom, što predstavlja sigurnosni rizik, posebno u otvorenim ili javnim mrežama [13].

Shared Key Authentication (SKA):

'Shared Key Authentication' koristi unaprijed dogovoreni ključ za provjeru identiteta korisnika, što osigurava viši nivo sigurnosti u odnosu na OSA. Proces autentifikacije uključuje nekoliko koraka:

- Zahtjev za autentifikaciju: Klijent šalje zahtjev za autentifikaciju AP-u.
- Izazovni tekst: AP odgovara slanjem izazovnog teksta klijentu.
- Šifrirani izazov: Klijent koristi unaprijed dogovoreni ključ za šifriranje izazovnog teksta i šalje ga natrag AP-u.
- Provjera odgovora: AP dešifrira primljeni odgovor i uspoređuje ga s originalnim izazovnim tekstom. Ako se podaci podudaraju, AP odobrava autentifikaciju; ako ne, pristup se odbija.

SKA pruža veću sigurnost jer zahtijeva korištenje šifriranog ključa, što otežava neovlaštenim korisnicima da pristupe mreži. Međutim, ovaj sistem također ima svoje nedostatke. Ako napadač dobije pristup unaprijed dogovorenom ključu, može presretati i dešifrirati mrežni promet. Također, proces distribucije i upravljanja ključevima može biti složen i podložan sigurnosnim rizicima.

Nakon razmatranja sigurnosnih propusta pri provjeri identiteta korisnika te različitih metoda autentifikacije u bežičnim mrežama, važno je osvrnuti se na jedan od najopasnijih napada koji može ugroziti mrežnu sigurnost – "Man in the Middle" (MitM) napad. Ovaj napad omogućava napadaču da presreće i potencijalno mijenja komunikaciju između dvaju krajnjih uređaja, bez njihovog znanja [14].

4.2 Propusti u WEP standardu

U ranim danima bežičnih mreža, WEP (Wired Equivalent Privacy) standard bio je prvi sigurnosni protokol osmišljen za zaštitu bežičnih komunikacija. Cilj WEP-a bio je pružiti sigurnost na razini žičane mreže, omogućavajući korisnicima prijenos podataka bez straha od presretanja ili manipulacije. Međutim, ubrzo je postalo jasno da WEP ima značajne sigurnosne propuste koji ga čine ranjivim na različite napade.

Jedan od glavnih problema WEP-a je korištenje statičkih enkripcijskih ključeva. Ključevi se rijetko mijenjaju, što napadačima olakšava njihovo presretanje i analizu. Dodatno, WEP koristi RC4 algoritam za enkripciju, koji se pokazao slabim zbog svoje predvidljivosti. Zbog ovih nedostataka, napadači mogu koristiti alate za analizu prometa i brzo dešifrirati WEP ključeve.

Još jedan ozbiljan problem je inicijalizacijski vektor (IV) koji WEP koristi za šifriranje. IV je prekratak, samo 24 bita, što znači da se ponavlja relativno često. To ponavljanje omogućava napadačima prikupljanje dovoljno podataka za izvođenje statističkih napada, koji im omogućuju rekonstruiranje enkripcijskih ključeva.

Zbog ovih nedostataka, WEP je vrlo ranjiv na različite vrste napada, kao što su korelacija ključeva i napadi s ponavljanjem. Čak i uz minimalno tehničko znanje, napadači mogu koristiti dostupne alate za brzo kompromitiranje WEP zaštićenih mreža.

Osim tehničkih nedostataka, WEP pati i od slabih upravljačkih mehanizama. Ključevi se često dijele među velikim brojem korisnika, što povećava vjerojatnost njihovog otkrivanja ili zloupotrebe. Također, mnogi korisnici nisu svjesni sigurnosnih prijetnji i ne mijenjaju zadane postavke, što dodatno povećava ranjivost mreža zaštićenih WEP-om.

Zbog ovih ozbiljnih sigurnosnih propusta, WEP je zamijenjen naprednijim protokolima kao što su WPA (Wi-Fi Protected Access) i WPA2, koji pružaju mnogo bolju zaštitu. WPA i WPA2 koriste dinamičke ključeve i naprednije enkripcijske algoritme, čime se značajno smanjuje rizik od presretanja i dešifriranja podataka.

Iako se WEP još uvijek može pronaći u nekim starijim sustavima, njegovo korištenje se snažno ne preporučuje. Organizacije i pojedinci trebaju nadograditi svoje mreže na modernije sigurnosne protokole kako bi zaštitili svoje podatke od napadača.

Razumijevanje propusta u WEP standardu je važno kako bi se izbjegle slične greške u budućim sigurnosnim protokolima i kako bi se podigla svijest o važnosti sigurnosti u bežičnim mrežama.

WEP je dobar primjer kako se sigurnosne tehnologije razvijaju i kako je potrebno kontinuirano unapređivati sigurnosne mjere kako bi se zaštitili podaci u digitalnom dobu [15].

4.3 WEP Napadi

WEP (Wired Equivalent Privacy) protokol, usmjeren na zaštitu bežičnih mreža, ima ozbiljne sigurnosne slabosti koje omogućavaju različite vrste napada. Ti napadi mogu biti klasificirani kao pasivni ili aktivni, svaki sa svojim specifičnim tehnikama i ciljevima. Ovdje su detaljni opisi pasivnih i aktivnih napada na WEP.

4.3.1 Pasivni napadi

Pasivni napadi uključuju presretanje i analiziranje mrežnog prometa bez aktivnog sudjelovanja ili mijenjanja podataka od strane napadača. Cilj pasivnih napada je prikupljanje informacija koje mogu pomoći u kasnijem izvođenju aktivnih napada ili dešifriranju komunikacije. Neki od najpoznatijih pasivnih napada na WEP su:

1.Presretanje prometa ('Traffic Sniffing'):

- Napadač koristi bežični adapter u promiskuitetnom načinu rada kako bi presreo sve pakete koji prolaze kroz mrežu.
- Analizom snimljenih paketa napadač može prikupiti dovoljno podataka za kasniju analizu i eventualno dešifriranje komunikacije.

2.Prikupljanje inicijalizacijskih vektora (+IV Collection+):

- Napadač prikuplja pakete kako bi analizirao inicijalizacijske vektore (IV-ove).
- Zbog kratke dužine IV-a (24 bita), oni se često ponavljaju, što omogućava napadaču da prikupi dovoljno IV-ova za izvođenje statističkih analiza.

3.Korištenje statističke analize ('Statistical Analysis'):

- Nakon prikupljanja velikog broja IV-ova, napadač koristi statističke metode za rekonstruiranje enkripcijskog ključa.
- Korištenjem alata kao što su Aircrack-ng, napadač može brzo dešifrirati WEP ključ nakon prikupljanja dovoljno podataka.

Pasivni napadi su teški za otkrivanje jer napadač ne mijenja ili šalje pakete, već samo prisluškuje mrežni promet [16].

4.3.2 Aktivni napadi

Aktivni napadi uključuju aktivno sudjelovanje napadača u mrežnoj komunikaciji s ciljem izmjene, ometanja ili preuzimanja kontrole nad komunikacijom. Ovi napadi su opasniji jer omogućuju napadaču da izvrši direktne akcije na mreži. Neki od najpoznatijih aktivnih napada na WEP su:

1. Napad s ponavljanjem ('Replay Attack'):
    - Napadač presreće legitimni paket podataka, mijenja ga i ponovno šalje pristupnoj točki.
    - Ovaj napad koristi ranjivosti u WEP-ovoj enkripciji kako bi stvorio lažne pakete koji izgledaju legitimno.
2. Napad deautentifikacijom ('Deauthentication Attack'):
    - Napadač šalje deautentifikacijske okvire pristupnoj točki ili klijentu, prisiljavajući ih na prekid veze.
    - Kada se klijent ponovno poveže, napadač može presresti inicijalizacijske vektore i podatke potrebne za analizu i dešifriranje ključeva.[17]
3. Napad s injektiranjem paketa ('Packet Injection Attack'):
    - Napadač šalje lažne pakete podataka u mrežu kako bi ometao normalan rad mreže ili ubacio zlonamjerni kod.
    - Ovaj napad koristi slabosti u WEP-u koje omogućuju napadaču da šalje pakete koji izgledaju kao legitimni.[17]
4. Napad lažnim pristupnim točkama ('Evil Twin Attack'):
    - Napadač stvara lažnu pristupnu točku koja izgleda kao legitimna mreža.
    - Korisnici se nesvjesno povezuju na lažnu mrežu, omogućujući napadaču da presreće sav njihov promet i potencijalno krade osjetljive informacije poput lozinki i osobnih podataka.
5. Napad fragmentacijom ('Fragmentation Attack'):
    - Napadač šalje male, fragmentirane pakete podataka i presreće odgovore koje pristupna točka šalje.
    - Korištenjem fragmentiranih paketa, napadač može rekonstruirati cijele pakete podataka i dešifrirati WEP ključ [17].

6. Man in the Middle' napad:

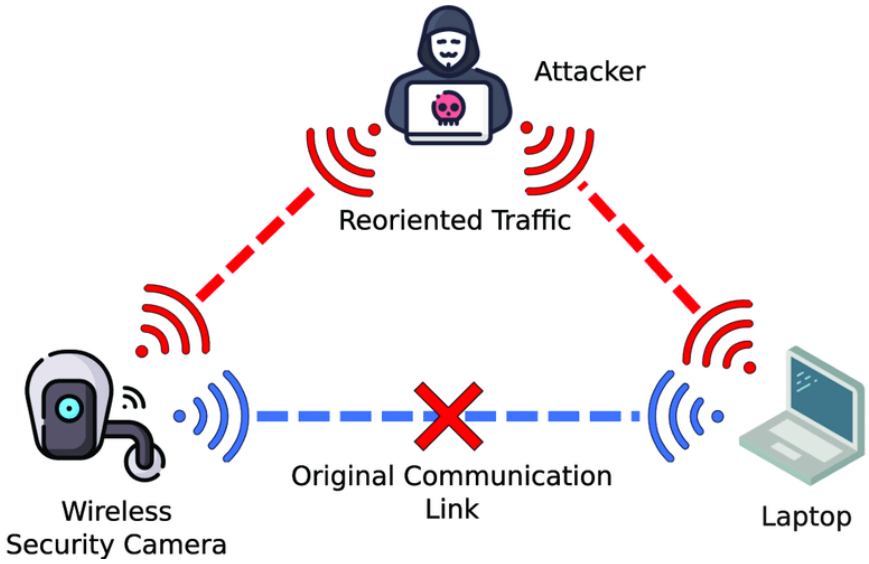
"Man in the Middle" napad je vrsta kibernetičkog napada gdje napadač tajno presreće i potencijalno mijenja komunikaciju između dviju strana koje vjeruju da izravno komuniciraju jedna s drugom. U kontekstu bežičnih mreža, napadač može koristiti različite tehnike kako bi se pozicionirao između pristupne točke i korisnika.

Napad obično započinje presretanjem signala između korisnika i pristupne točke. Napadač može koristiti lažnu pristupnu točku koja se ponaša kao legitimna, privlačeći korisnike da se na nju povežu. Kada se korisnik poveže, sav promet prolazi kroz napadačev uređaj, omogućujući mu da prati, snima ili mijenja podatke.

Napadač može koristiti MitM napad za krađu osjetljivih informacija poput lozinki, brojeva kreditnih kartica i drugih osobnih podataka. Također može injektirati zlonamjerni kod u preuzimanja ili web stranice koje korisnik posjećuje, dodatno kompromitirajući sigurnost uređaja.

MitM napadi se često koriste u kombinaciji s drugim vrstama napada, kao što su phishing ili DNS spoofing, kako bi se povećala njihova učinkovitost. Da bi se zaštitili od MitM napada, korisnici bi trebali koristiti enkripciju (kao što je HTTPS) i višefaktorsku autentifikaciju. Također, važno je biti oprezan pri povezivanju na javne bežične mreže i koristiti VPN za dodatnu sigurnost.

MitM napadi predstavljaju ozbiljnu prijetnju mrežnoj sigurnosti, posebno u bežičnim okruženjima gdje je lako presresti komunikaciju. Svjesnost o postojanju ovakvih napada i poduzimanje preventivnih mjera ključni su za zaštitu osjetljivih informacija i održavanje sigurnosti mreže [18].



Slika 4.1. Man in the Middle Napad [28]

4.4 Zaštita mreže

Zaštita bežičnih mreža postala je ključno pitanje u svijetu umreženih tehnologija zbog sve veće učestalosti napada na mreže. S obzirom na ranjivosti starijih protokola poput WEP-a, neophodno je koristiti naprednije sigurnosne mjere kako bi se osigurala pouzdanost i sigurnost podataka. WPA3, najnoviji sigurnosni standard, nudi značajna poboljšanja u odnosu na svoje prethodnike, uključujući jaču enkripciju i bolju zaštitu od brute-force napada. Također, implementacija dodatnih sigurnosnih mjera kao što su složene lozinke, redovito ažuriranje softvera i korištenje VPN-a može značajno smanjiti rizik od neovlaštenog pristupa. Osiguravanje bežičnih mreža ključ je za zaštitu osobnih i poslovnih podataka u današnjem digitalnom okruženju.

4.4.1 Statičko IP adresiranje

Statičko IP adresiranje uključuje ručno dodjeljivanje stalne IP adrese svakom uređaju u mreži, što olakšava upravljanje mrežnim resursima. Ovaj način adresiranja omogućava pouzdaniju komunikaciju između uređaja, jer IP adrese ostaju nepromijenjene. U smislu sigurnosti, statičke IP adrese mogu pojednostaviti praćenje i kontrolu mrežnog prometa, što olakšava identifikaciju i rješavanje sigurnosnih prijetnji. Međutim, stalne IP adrese također mogu biti meta napada, jer napadači mogu lakše pratiti i ciljati specifične uređaje. Za dodatnu zaštitu, statičko IP

adresiranje treba kombinirati s drugim sigurnosnim mjerama poput vatrozida i enkripcije podataka [19]

4.4.2 MAC filtriranje

MAC filtriranje uključuje kontrolu pristupa mreži na temelju jedinstvenih MAC adresa uređaja. Ova metoda omogućava administratorima da definiraju popis dopuštenih uređaja, čime se sprječava povezivanje neovlaštenih uređaja. MAC filtriranje pomaže u povećanju sigurnosti mreže, jer samo uređaji s prepoznatim MAC adresama mogu pristupiti mrežnim resursima. Međutim, ova metoda nije nepogrešiva, jer napadači mogu lažirati (spoofati) MAC adrese ovlaštenih uređaja kako bi zaobišli filtriranje. Unatoč tome, kada se MAC filtriranje koristi zajedno s drugim sigurnosnim mjerama, poput WPA3 enkripcije i jakih lozinki, može značajno otežati neovlašteni pristup. Osim toga, MAC filtriranje može pomoći u praćenju i upravljanju mrežnim prometom, olakšavajući identifikaciju sumnjivih aktivnosti. Sveukupno, MAC filtriranje pruža dodatni sloj zaštite, ali se ne bi trebalo koristiti kao jedina sigurnosna mjera [20].

4.4.3 Vatrozid

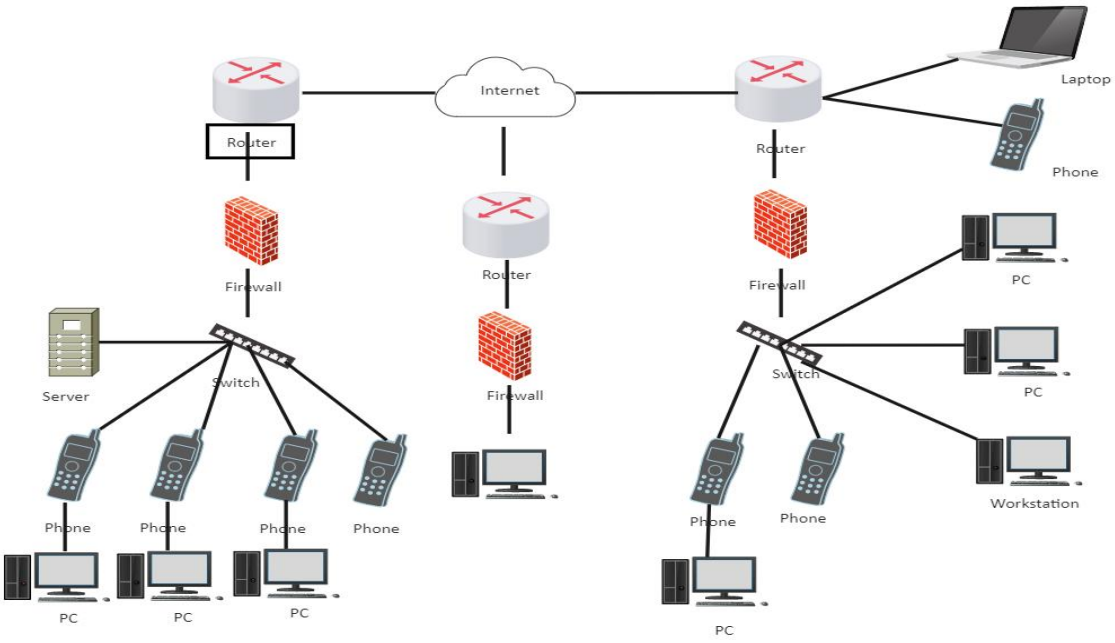
Vatrozid, ili firewall, predstavlja ključni element u zaštiti mreža od neovlaštenih pristupa i cyber napada. Vatrozid djeluje kao barijera između sigurne interne mreže i nesigurne vanjske mreže, filtrirajući promet na temelju unaprijed definiranih sigurnosnih pravila. Ova tehnologija može biti implementirana u obliku hardvera, softvera ili kombinacije oba, pružajući višeslojnu zaštitu.

Prvi korak u funkciji vatrozida je kontrola pristupa, koja uključuje praćenje ulaznog i izlaznog prometa. Vatrozid koristi pravila koja definiraju koji promet je dopušten, a koji je blokiran. Ova pravila mogu biti postavljena na temelju IP adresa, brojeva portova, protokola i drugih kriterija. Na primjer, vatrozid može blokirati sav promet koji dolazi s određenih IP adresa za koje je poznato da su izvori napada ili sumnjivih aktivnosti.

Osim kontrole pristupa, vatrozid može analizirati sadržaj mrežnog prometa kako bi otkrio i spriječio prijetnje. Napredni vatrozidi, poznati kao vatrozidi nove generacije (NGFW), integriraju tehnologije poput dubinske inspekcije paketa (DPI), prevencije upada (IPS) i antivirusne zaštite. DPI omogućava vatrozidu da analizira sadržaj paketa podataka u stvarnom vremenu, prepoznajući zlonamjerne aktivnosti poput pokušaja upada ili širenja malvera.

Važno je napomenuti da vatrozid ne štiti samo od vanjskih prijetnji, već također može spriječiti interno curenje podataka. Interni vatrozidi mogu ograničiti pristup određenim resursima unutar mreže na temelju uloga i privilegija korisnika. Ovo je posebno korisno u velikim organizacijama gdje različiti odjeli trebaju različite razine pristupa podacima i aplikacijama.

Implementacija vatrozida značajno poboljšava sigurnost mreže, no važno je napomenuti da sama tehnologija nije dovoljna. Vatrozid se mora redovito ažurirati kako bi bio učinkovit protiv novih prijetnji. Pravila i politike vatrozida trebaju se revidirati i prilagođavati kako bi odgovarale promjenjivim sigurnosnim zahtjevima organizacije [21].



Slika 4.2. Implementacija vatrozida [29]

Jedna od ključnih prednosti vatrozida je mogućnost praćenja i evidentiranja mrežnog prometa. Ove evidencije mogu biti neprocjenjive za timove za sigurnost informacijskih sustava prilikom istraživanja incidenata i analiziranja sigurnosnih prijetnji. Također, mogu poslužiti kao dokazni materijal u slučaju pravnih postupaka povezanih s cyber incidentima.

Međutim, unatoč brojnim prednostima, vatrozid ima i svoja ograničenja. Primjerice, vatrozid ne može zaštititi mrežu od napada koji se odvijaju putem enkriptiranih kanala, ako nije konfiguriran za dešifriranje i analizu tih podataka. Također, ne može spriječiti napade iznutra ako korisnici imaju valjane ovlasti za pristup mrežnim resursima.

Zaključno, vatrozid predstavlja osnovnu komponentu mrežne sigurnosti koja značajno doprinosi zaštiti od neovlaštenih pristupa i cyber napada. Njegova učinkovitost ovisi o pravilnoj implementaciji, redovitom ažuriranju i integraciji s drugim sigurnosnim tehnologijama. U kombinaciji s dobrim praksama upravljanja mrežom, vatrozid može pružiti snažnu zaštitu i osigurati integritet, povjerljivost i dostupnost mrežnih resursa [22].

7. SIMULACIJA NAPADA NA BEŽIČNE MREŽE

5.1 Sniffing i deautentifikacijski napad (probijanje WEP zaštite)

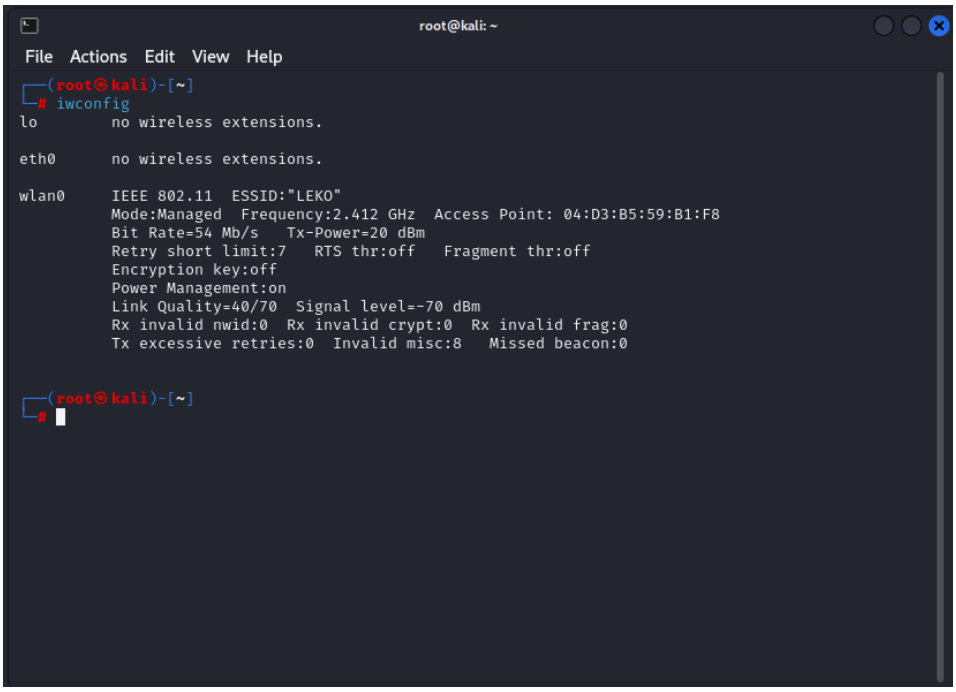
Bežične mreže su postale osnovna komponenta modernih informacijskih sustava, omogućujući korisnicima povezivanje na internet bez potrebe za fizičkim kablovima. Međutim, kao i kod svih tehnologija, bežične mreže su ranjive na različite vrste napada. Jedan od najučinkovitijih napada je sniffing, odnosno presretanje podataka koji se prenose kroz mrežu, dok deautentifikacijski napad prisiljava korisnike da se isključe s mreže.

Kali Linux, kao vodeći operacijski sustav za penetracijsko testiranje, nudi niz alata za izvođenje ovakvih napada. Neki od tih alata su „airmon-ng“, „airodump-ng“, „aireplay-ng“ i „aircrack-ng“. Ovi alati omogućuju korisnicima da identificiraju mreže, presretnu pakete i eventualno probiju mrežnu enkripciju. Ovaj rad se fokusira na demonstraciju kako se koristi „sniffing“ i deautentifikacijski napad na bežičnu mrežu.

Napomena: Ovaj napad, zajedno s opisanim tehnikama i alatima, isključivo je namijenjen za edukativne i znanstvene svrhe, kao i za penetracijsko testiranje na mrežama za koje imate izričitu dozvolu vlasnika. Neovlašteno presretanje podataka ili napadi na bežične mreže predstavljaju ozbiljno kršenje zakona i mogu rezultirati pravnim sankcijama. Svi alati i metode opisani u ovom radu trebaju se koristiti odgovorno, u okviru zakonskih propisa, te u svrhu poboljšanja mrežne sigurnosti, a ne u svrhu nanošenja štete.

1. Postavke bežične mreže

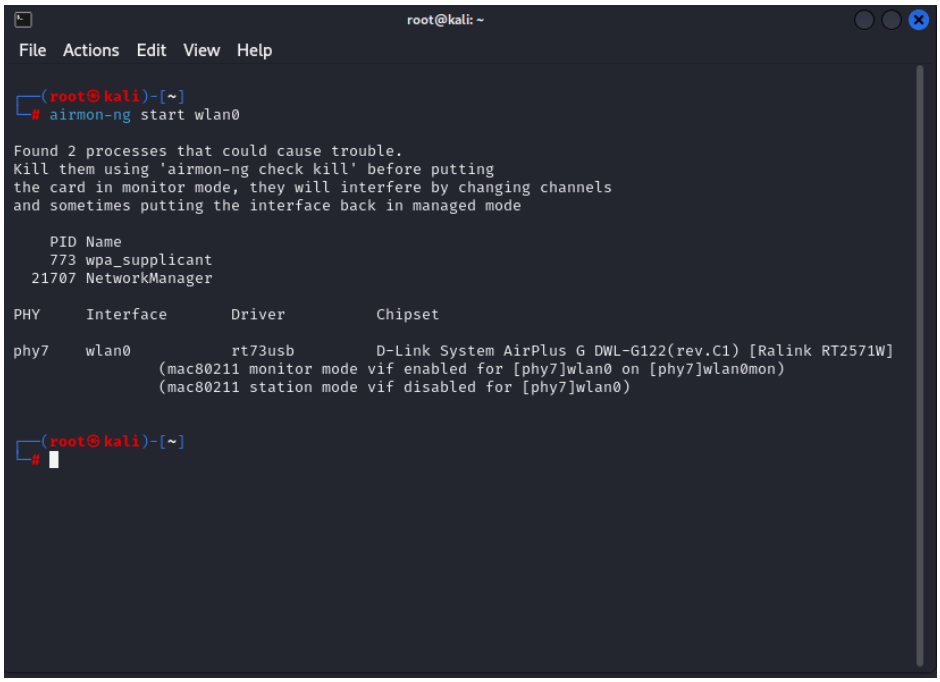
Kako bismo uspješno provodili penetracijsko testiranje bežičnih mreža, prvo koristimo naredbu 'iwconfig' kako bismo pregledali i konfigurirali bežične mrežne sučelja. Ova naredba omogućuje korisniku provjeru postavki bežičnih mrežnih adaptera, kao što su ESSID (naziv mreže), frekvencija, način rada, snaga signala i druge relevantne informacije o bežičnim sučeljima. 'iwconfig' je slična naredbi 'ifconfig', ali specijalizirana za rad s bežičnim mrežnim karticama.



Slika 7.1. Stanje bežične mreže

Naša bežična mreža nalazi se 'managed' modu a da bi mogli presretati promet i raditi razna testiranja našu mrežu moramo prebaciti u 'monitor' mode .

To radimo naredbom 'airmon-ng start wlan0'

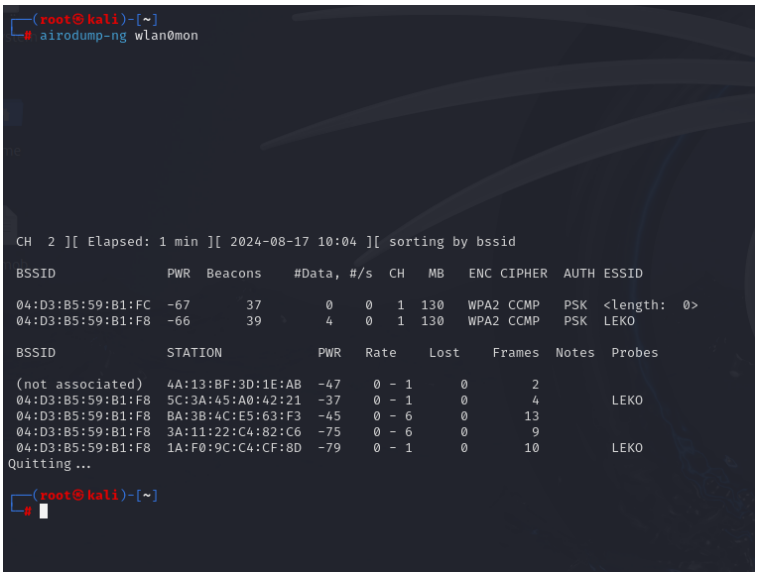


Slika 7.2. wlan0 mreža prebačena u 'monitor' mod

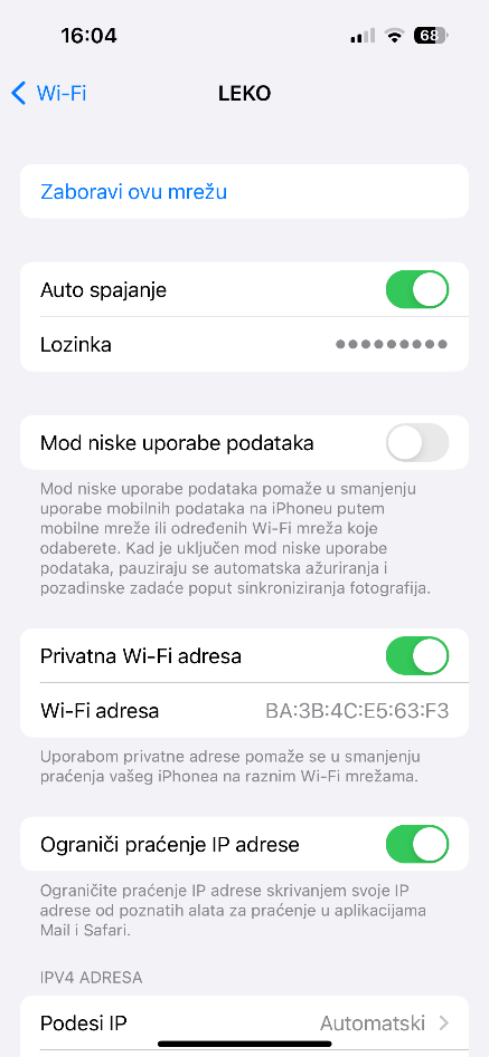
1. Skeniranje mreža koristeći 'airodump-ng' naredbu

Kada je mrežni adapter u monitor modu, koristimo airodump-ng za skeniranje dostupnih mreža. Ova naredba omogućuje pregled svih dostupnih bežičnih mreža i prikazuje relevantne informacije kao što su SSID (naziv mreže), BSSID (MAC adresa pristupne točke), signal, korištena enkripcija itd.

Naredba glasi 'airodump-ng wlan0mon'.



Slika 7.3. Prikaz dostupnih mreža i stanica spojenih na mrežu

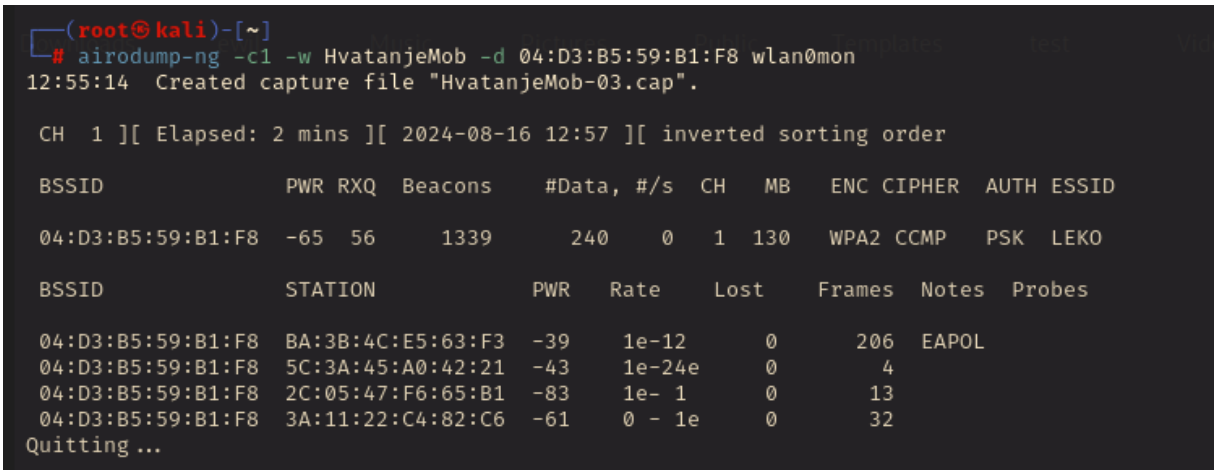


Slika 7.4. MAC adresa uređaja na kojeg se vrši napad

Pomoću ove naredbe na slici vidimo dvije mreže koje su dostupne a jedna od njih je i moja kućna mreža na koju sam spojen a to je mreža sa „04:D3:B5:59:B1:F8“ MAC adresom . Donja lista je lista uređaja koji su spojeni na mrežu „LEKO“ .
Uređaj koji ću ja u ovom slučaju pratiti je i na kojeg ću raditi napad je moj mobitel sa MAC adresom „BA:3B:4C:E5:63:F3“ .

3. Presretanje paketa

Nakon što je ciljna mreža odabrana, koristimo 'airodump-ng' kako bismo presretali pakete koji se šalju unutar mreže.



Slika 7.5. Presretanje paketa

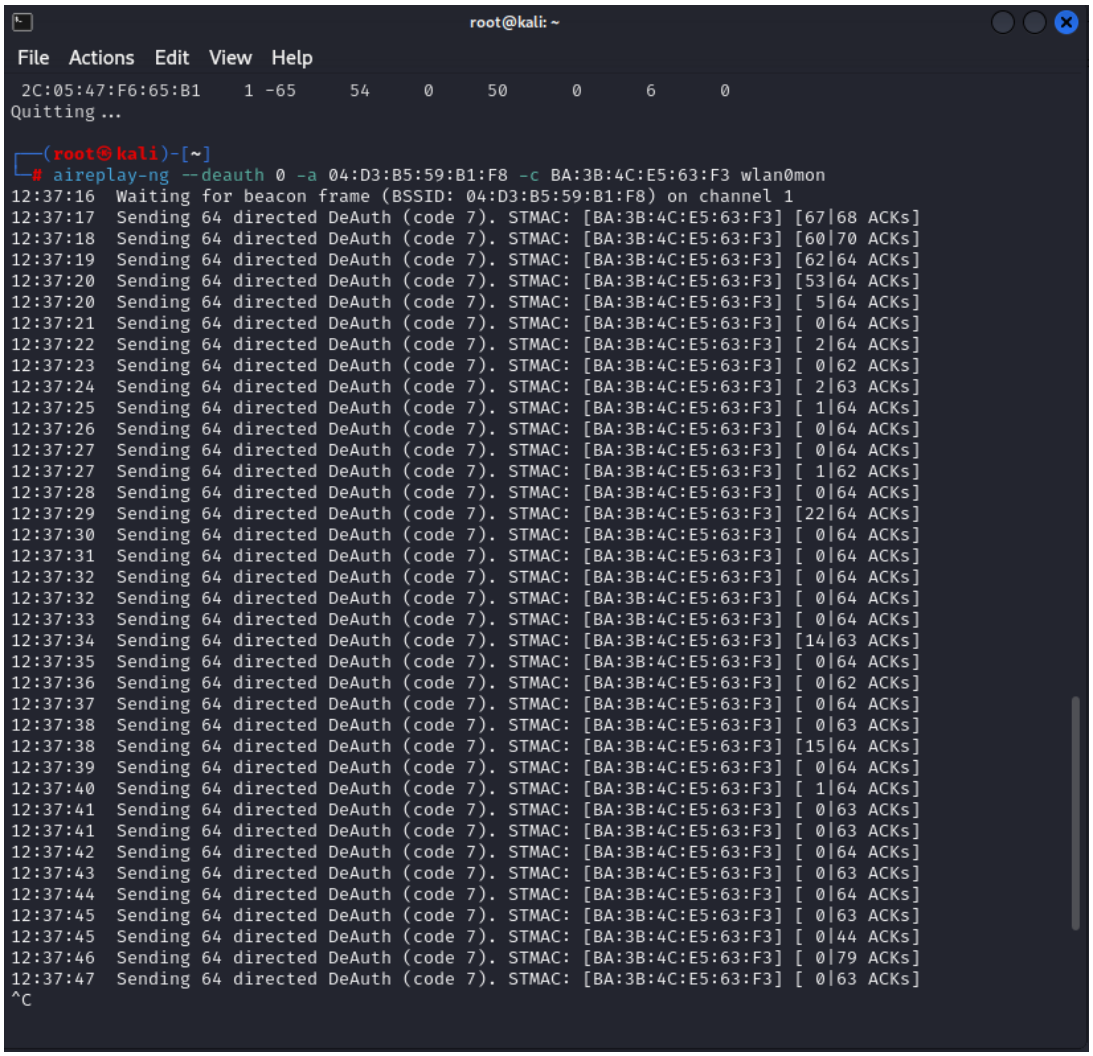
- c – označava broj kanala na kojem se naša mreža nalazi ,možemo vidjeti iz slike na mjestu „CH“ je broj 1.
- w- stvaranje tekstualne datoteke u koju će se spremati paketi (ja sam tu datoteku nazvao 'HvatanjeMob')
- d- izdvajanje samo jedne određene mreže

Program će sam stvoriti datoteku 'HvatanjeMob-03.cap' i u nju spremati pakete koje ćemo kasnije gledati preko 'Wireshark' programa .

4. Deautentifikacija korisnika pomoću aireplay-ng:

Deautentifikacijski napad ima za cilj prisiliti korisnike da se odjave s mreže, kako bi se ponovno povezali. Ovaj proces može pomoći u generiranju 'handshake-a' (rukovanja) koji se može kasnije koristiti za probijanje WPA/WPA2 lozinke.

Naredba za deautentifikaciju : 'sudo aireplay-ng --deauth 0 -a [BSSID_mreze] wlan0mon'



Slika 7.6. Deautentifikacijski napad

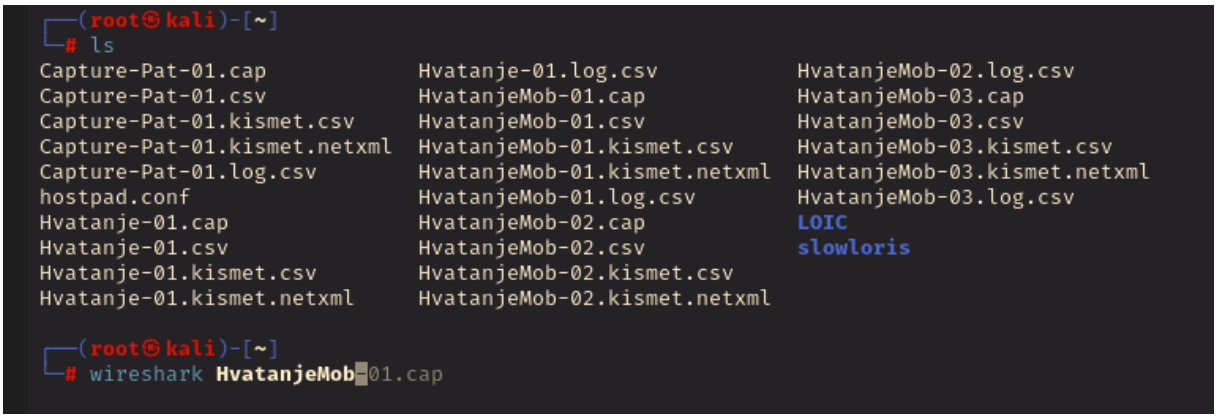
-aireplay-ng – naredba za aktivaciju napada

--deauth – znak da se radi o deautentifikaciji

-a- označava mrežu našu na koju smo spojeni

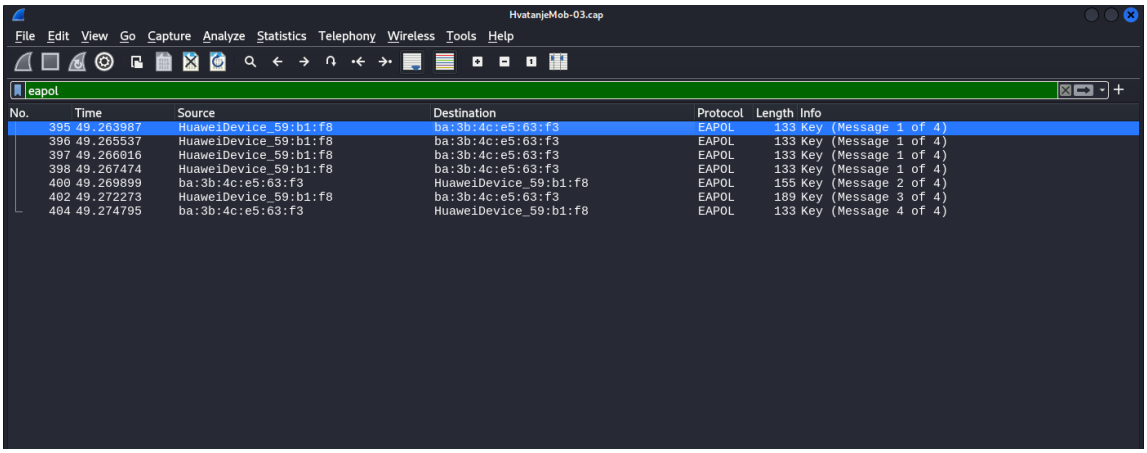
-c – označava klijenta kojeg napadamo (u ovom slučaju moj mobilni uređaj)

Proces hvatanja podataka je završen .Sljedeći korak je naredbom ' –ls 'ako želimo provjeriti koje datoteke su nam se stvorile i preko 'wiresharka' otvoriti ciljanu datoteku . (U mom slučaju datoteka koja se stvorila i koja nam je potrebna je HvatanjeMob-03.cap).



Slika 7.7. Direktorij stvaranja datoteka

Nakon toga nam se otvara 'Wirehark' gdje vidimo pakete koji su uhvaćeni. Za filter unutar koristimo EAPOL datoteke. EAPOL datoteke su potrebne kako bi se uhvatio tzv. '4-way handshake', koji se koristi u WPA/WPA2 protokolima za autentifikaciju uređaja na mreži. Ovaj 'handshake' sadrži informacije koje omogućavaju analizu i potencijalno probijanje lozinke mreže. Kada se izvrši uspešan 4-way 'handshake' između uređaja i Access Point-a, razmenjuju se EAPOL paketi.

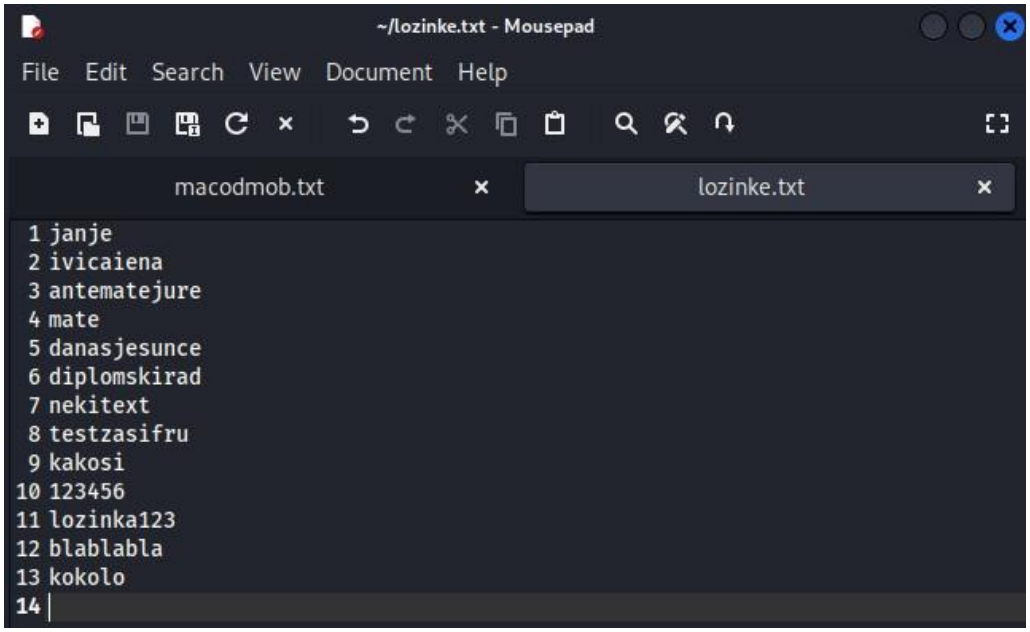


Slika 7.8. Prikaz paketa unutar 'wireshark-a'

5. Probijanje lozinke s 'aircrack-ng'

Koristimo 'aircrack-ng' alat i datoteku s prikupljenim paketima kako bismo probili lozinku, često koristeći 'dictionary attack' (napad s riječnikom).

Slika 7.9. Probijanje lozinke koristeći 'aircrack' alat



Slika 7.10. Primjer navedenih lozinki od kojih je jedna točna

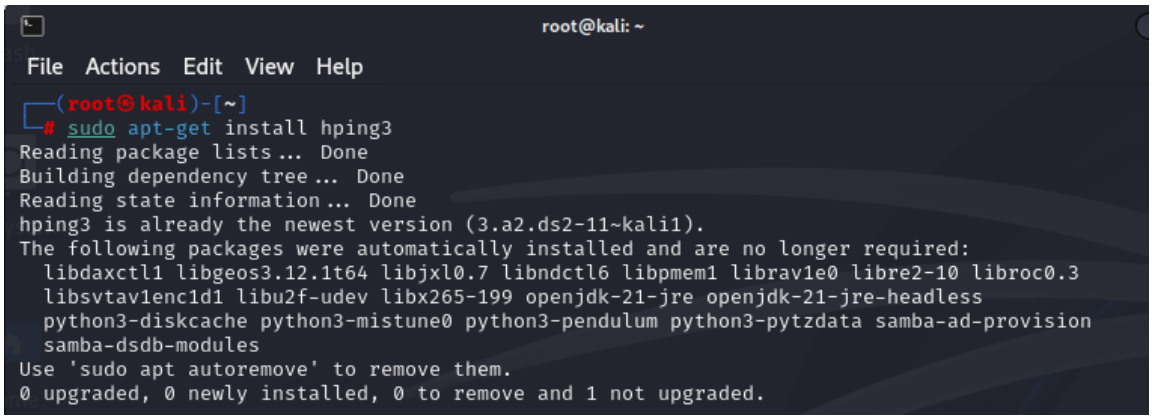
Alat je uspješno pronašao koja je od navedenih lozinki unutar tekstualne datoteke točno lozinka mreže na koju je spojen bio uređaj.

5.2 DOS napad

Simulacija DoS (Denial of Service) napada na Kali Linuxu može se izvesti pomoću različitih alata, uključujući hping3, koji je jedan od popularnijih alata za ovakve aktivnosti. Imaj na umu da izvođenje DoS napada bez eksplicitnog dopuštenja na tuđe mreže ili sisteme može biti ilegalno i protivno zakonima o cyber sigurnosti.

1. Instalacija alata 'hping3'

Ako 'hping3' nije instaliran , možeš ga instalirati jednostavnom komandom :
sudo apt-get install hping3



Slika 7.11. Instalacija 'hping3' alata

2. Izvršavanje DoS napada pomoću 'hping3'

Jedan od najčešćih oblika DoS napada je slanje ogromnog broja ICMP (Ping) paketa, TCP SYN paketa ili UDP paketa ciljnom sistemu. To može preopteretiti mrežne resurse cilja, što može dovesti do toga da sistem postane nefunkcionalan.

TCN SYN Flood Napad

'TCP SYN flood' napad pokušava preplaviti mrežni resurs lažnim zahtjevima za uspostavljanje veze. Možeš koristiti hping3 za ovakav napad:

```
┌──(root㉿kali)-[~]
└─# sudo hping3 -S --flood -p 80 192.168.8.145
HPING 192.168.8.145 (wlan0 192.168.8.145): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.8.145 hping statistic ---
46703 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Slika 7.12. Aktivacija SYN flood napada

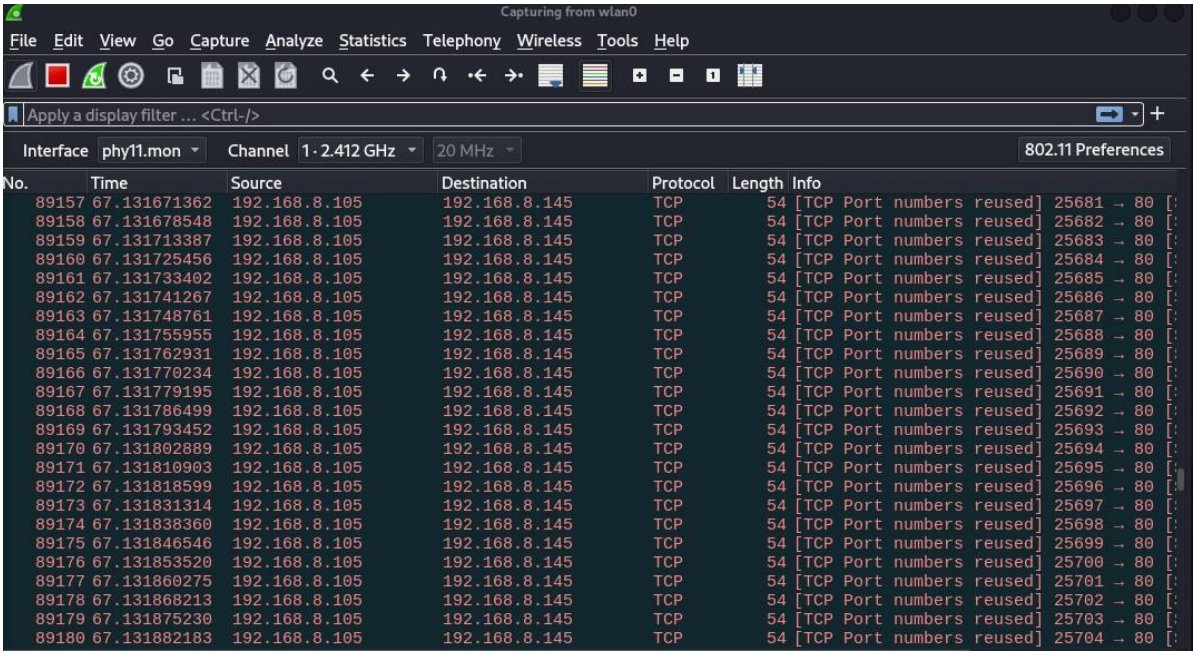
-'s': Postavlja TCP SYN flag

'--flood': Šalje pakete što je brže moguće bez čekanja odogovora

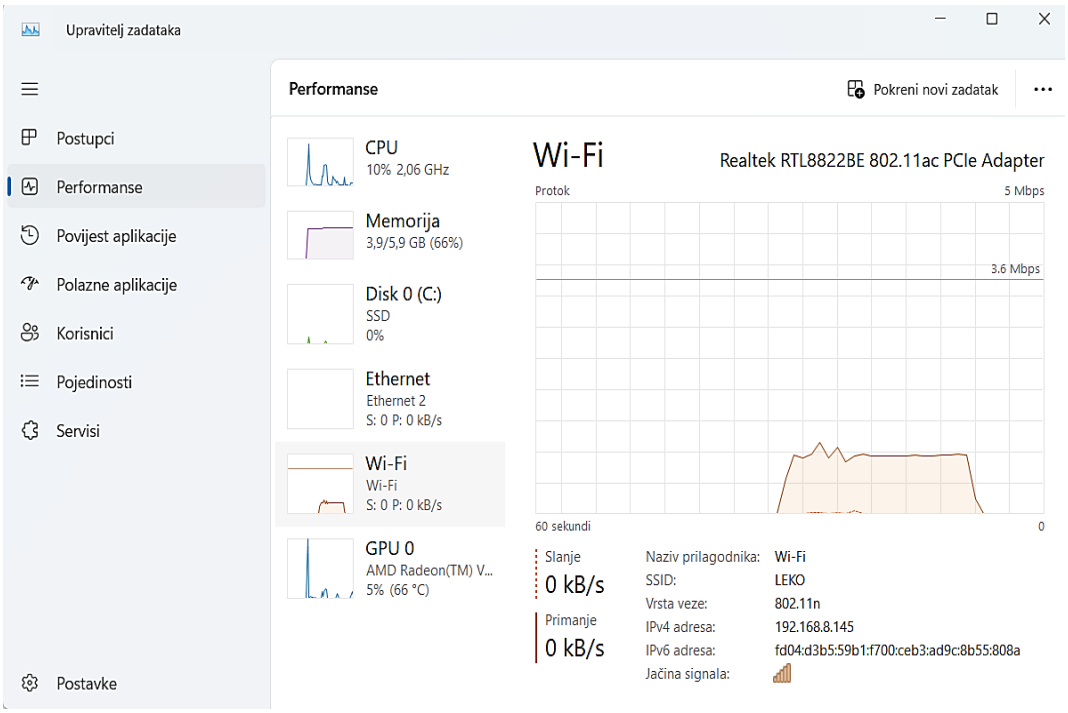
'-v': Omogućava verbosni način rada

'-p ': Ciljni port i nakon njega ip adresa koju napadamo

Na sljedećim slikama je prikazano opterećenje mreže pod SYN napadom:



Slika 7.13. Prikaz poslanih paketa unutar 'wireshark-a'



Slika 7.14. Opterećenje mreže tijekom napada

UDP Flood Napad

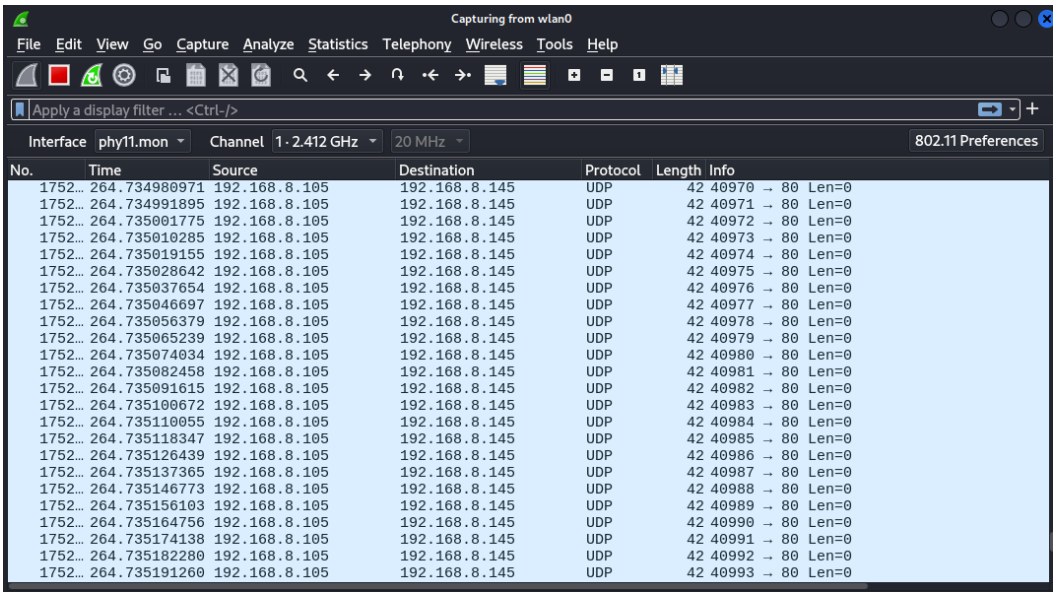
UDP Flood napad je vrsta DoS napada u kojem napadač šalje veliki broj UDP paketa ciljanom serveru ili mreži. Cilj je preopteretiti resurse servera, što može dovesti do usporavanja ili potpune nedostupnosti usluga. UDP protokol ne koristi mehanizam potvrde prijema, što omogućava napadaču da lako generira ogroman broj paketa. Ovi napadi se često koriste za ometanje mrežnih servisa poput DNS-a ili VoIP aplikacija

Pokretanje napada prikazano je na sljedećoj slici :

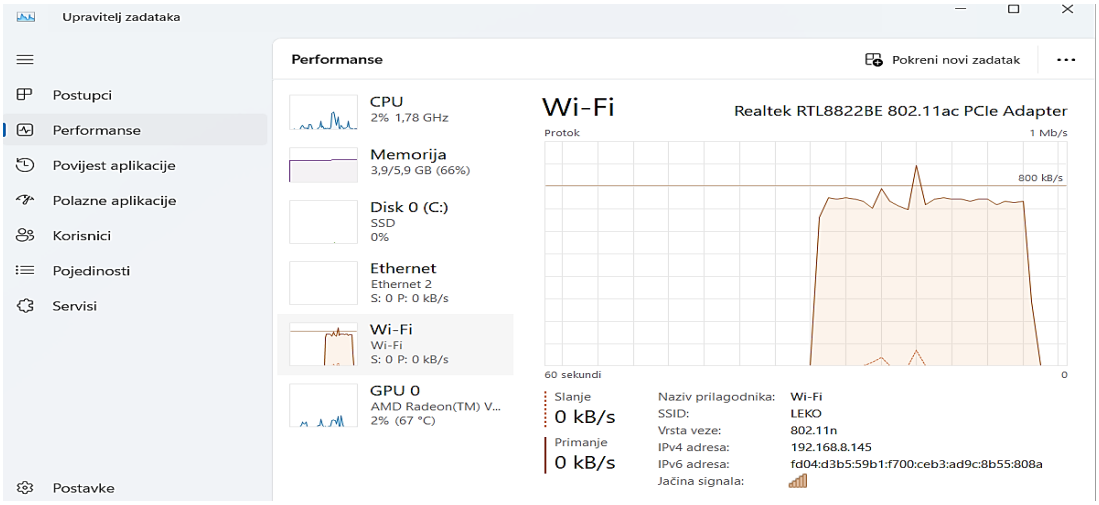
```
┌──(root㉿kali)-[~]
└─# sudo hping3 --udp --flood -p 80 192.168.8.145
HPING 192.168.8.145 (wlan0 192.168.8.145): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.8.145 hping statistic ---
53089 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Slika 7.15. Pokretanje UDP flood napada

Nakon ovog napada mreža je bila neiskoristiva tj. nijedna Web stranica se nije mogla učitati .



Slika 7.16. Prikaz UDP paketa unutar 'wireshark-a'



Slika 7.17. Opterećenje mreže tijekom UDP flood napda

8. ZAKLJUČAK

Bežične mreže su izuzetno važan segment modernih komunikacija, nudeći praktičnost i širok raspon primjena u svakodnevnom životu. Njihova prilagodljivost i učinkovitost omogućuju jednostavno skaliranje i prilagođavanje različitim korisničkim potrebama, čime se značajno povećava produktivnost i mobilnost. Međutim, sigurnost bežičnih mreža ostaje izazov zbog inherentnih rizika koji proizlaze iz otvorene prirode prijenosa podataka. Različiti standardi bežičnih mreža, kao što su WPA3 i druge napredne metode enkripcije, postavljaju čvrste temelje za osiguranje mrežnih resursa i zaštitu podataka. Arhitektura bežičnih mreža, u kombinaciji s odgovarajućim sigurnosnim mjerama, pruža mogućnost za balansiranje između performansi i sigurnosti. Usprkos napretku u sigurnosnim protokolima, bežične mreže su i dalje ranjive na napade poput neovlaštenog pristupa, presretanja podataka i DoS napada. Stoga je ključno stalno nadograđivati sigurnosne prakse i alate kako bi se spriječili potencijalni sigurnosni incidenti. Istraživanje provedeno u ovom radu pokazalo je da je edukacija korisnika o sigurnosnim prijetnjama jednako važna kao i tehničke mjere zaštite.

U konačnici, sigurnost bežičnih mreža mora ostati prioritet kako bi se omogućilo sigurno i pouzdano korištenje ovih tehnologija u budućnosti. Pored tehničkih mjera, važno je implementirati i redovite sigurnosne audite i monitoring sustave kako bi se brzo otkrile i neutralizirale potencijalne prijetnje. Unatoč snažnim protokolima poput WPA3, slabosti u konfiguraciji mreža i nemarni korisnički postupci često otvaraju prostor za napade. Stoga je neophodno da sigurnosne politike budu jasno definirane i redovito ažurirane kako bi odgovarale najnovijim prijetnjama. Također, rastuća upotreba IoT uređaja stvara nove izazove jer se mnogi od tih uređaja oslanjaju na bežične mreže, ali dolaze s ograničenim sigurnosnim mogućnostima. Zaključno, sveobuhvatan pristup sigurnosti bežičnih mreža, uključujući tehničke, organizacijske i edukativne mjere, ključan je za osiguranje njihove dugoročne otpornosti i pouzdanosti u svakodnevnoj upotrebi.

LITERATURA

[1] Fortinet: What Is A Wireless Network? Types of Wireless Networks, https://www.fortinet.com/resources/cyberglossary/wireless-network (pristupljeno 20.1.2024.)

[2] Cert: Wireless forenzika CCERT-PUBDOC-2008-03-225, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-04-225.pdf (pristupljeno 10.2.2024.)

[3] Vanet: Introduction to Vanet Basics, https://ebrary.net/183102/computer_science/introduction_vanet (pristupljeno 12.2.2024.)

[4] Vanet: Ad Hoc Network Features, https://ebrary.net/183102/computer_science/introduction_vanet (pristupljeno 12.2.2024)

[5] Okta: Wired Equivalent Privacy , https://www.okta.com/identity-101/wep/ (pristupljeno 14.2.2024.)

[6] Logsign: What is Wire Equivalent Privacy Encryption? , https://www.logsign.com/blog/what-is-wired-equivalent-privacy-wep-encryption/ (pristupljeno 15.2.2024.)

[7] SecureW2: What is WPA authentication?, https://www.securew2.com/blog/what-is-wpa-authentication (pristupljeno 1.3.2024.)

[8] AVG: What is WPA2?, https://www.avg.com/en/signal/what-is-wpa2 (pristupljeno 2.3.2024.)

[9] Kaspersky : What i san SSID?, https://www.kaspersky.com/resource-center/definitions/what-is-an-ssid (pristupljeno 10.3.2024)

[10] Intel: 802.1x Overview and EAP Types, https://www.intel.com/content/www/us/en/support/articles/000006999/wireless/legacy-intel-wireless-products.html (pristupljeno 11.3.2024.)

[11] ProfessorMesser:TKIP and CCMP, https://www.professormesser.com/security-plus/sy0-401/tkip-and-ccmp/#google_vignette (pristupljeno 12.3.2024.)

[12] Kaspersky:How to avoid public WIFI safety risks, https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks (pristupljeno 20.3.2024.)

[13] HP :Open system authentication, https://support.hpe.com/techhub/eginfolib/networking/docs/routers/msrv7/cg/5200-3028_wlan_cg/content/466576910.htm (pristupljeno 1.4.2024.)

[14] Tech Target: Shared key Authentication,
https://www.techtarget.com/searchsecurity/definition/Shared-Key-Authentication-SKA
(pristupljeno 3.4.2024.)
[15] FER: Sigurnosni propusti u standardima,
http://sigurnost.zemris.fer.hr/ns/wireless/2004_maric/wep_flaw.htm (pristupljeno 4.4.2024.)
[16] FER: Pasivni napadi ,
http://sigurnost.zemris.fer.hr/ns/wireless/2004_maric/pasivni.htm (pristupljeno 10.4.2024.)
[17] FER: Aktivni napadi,

http://sigurnost.zemris.fer.hr/ns/wireless/2004_maric/aktivni.htm (pristupljeno 10.4.2024.)

[18] IBM: What is a man-in-the-middle attack?,

https://www.ibm.com/think/topics/man-in-the-middle (pristupljeno 15.4.2024.)

[19] Tech Target: Static IP address,

https://www.techtarget.com/whatis/definition/static-IP-address (pristupljeno 21.4.2024.)

[20] Lifewire: MAC address fitlering,
https://www.lifewire.com/enabling-mac-address-filtering-wireless-router-816571
(pristupljeno 23.4.2024.)
[21] Cloudflare: What is a firewall?,
https://www.cloudflare.com/learning/security/what-is-a-firewall/ (pristupljeno 12.5.2024.)
[22] NordLayer: What is a firewall?,

https://nordlayer.com/learn/firewall/what-is-firewall/ (pristupljeno 20.5.2024.)

[23] ConceptDraw: Wireless Network WLAN,

https://www.conceptdraw.com/examples/wireless-wlan (pristupljeno 3.6.2024.)

[24] EPSON: Bežična mreža,

https://support.epson-europe.com/onlineguides/hr/bx310tx510/html_z/intro_5.htm
(pristupljeno 15.6.2024.)

[25] ResearchGate: Peer to Peer,

https://www.researchgate.net/figure/Illustration-of-a-peer-to-peer-network_fig1_2605250

(pristupljeno 1.7.2024.)

[26] FOI:Wirelles security,

https://security.foi.hr/wiki/index.php/Wireless_security.html (pristupljeno 5.7.2024)

[27] SOT: WPA2 Enterprise,

https://sysopstechnix.com/wpa2-enterprise-secure-your-organization-wi-fi-network/ (pristupljeno 5.7.2024.)

[28]ResearchGate: MITM,

https://www.researchgate.net/figure/Illustration-of-a-Man-in-the-Middle-attack_fig4_353723022 (pristupljeno 6.7.2024.)

[29] EdrawMax: Firewall network diagram ,

https://edrawmax.wondershare.com/for-it-service/network-diagram-tips.html

(pristupljeno (10.7.2024.)

POPIS SLIKA