Sigurnost lokalnih bežičnih mreža

Tomičić, Ivan

Undergraduate thesis / Završni rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:139183

Rights / Prava: Attribution-NonCommercial-NoDerivs 3.0 Unported/Imenovanje-Nekomercijalno-Bez prerada 3.0

Download date / Datum preuzimanja: **2024-03-29**

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

Repository / Repozitorij:

Faculty of Organization and Informatics - Digital Repository

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Ivan Tomičić

SIGURNOST LOKALNIH BEŽIČNIH MREŽA

ZAVRŠNI RAD

Varaždin, 2020.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Ivan Tomičić

Matični broj: 44031/15-R

Studij: Poslovni sustavi

SIGURNOST LOKALNIH BEŽIČNIH MREŽA

ZAVRŠNI RAD

Mentor:

Prof. dr.sc. Ivan Magdalenić

Varaždin, lipanj 2020.

Ivan Tomičić

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor potvrdio prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

U radu će se opisati i definirati lokalne bežične mreže klasificirane prema IEEE 802.11 standardu. Prvi dio rada namijenjen je opisu sigurnosnih protokola i njihove propusnosti na određene napade korištenih u bežičnoj mrežnoj sigurnosti. Nadalje, glavni fokus ovog završnog rada usmjeren je na sigurnost bežičnih lokalnih mreža gdje korištenjem suvremenih metoda detaljno prikazujemo načine penetracijskih napada na bežične lokalne mreže korištenjem Linux operativnog sustava i potrebnih alata za otkrivanje slabosti bežičnih mreža. Praktični dio rada prikazat će nam na koje načine i kako uspješno obaviti različite vrste napada na bežične mreže. Dokazati ćemo da bežične mreže nije preporučljivo koristiti u važnim poslovnim okruženjima koja zahtijevaju sigurnost i pouzdanost podataka.

Ključne riječi: Mrežna sigurnost; bežične lokalne mreže; prevencija napada; Wi-Fi; IEEE 802.11; Linux alati; napadi; autentifikacija; enkripcija

Sadržaj

Sadržaj iii
1. Uvod 1
2. Sigurnosni protokoli bežičnih mreža 2
2.1. Wired Equivalent Privacy protokol 3
2.1.1. Algoritam 3
2.1.2. Sigurnosni propusti WEP protokola 5
2.1.3. Načini penetracije WEP protokola 6
2.2. WPA protokol 7
2.2.1. TKIP protokol 7
2.2.2. MIC algoritam 8
2.2.3. WPA autentifikacije 9
2.2.4. Načini penetracije WPA protokola 10
2.3. WPA version 2 protokol 11
2.3.1. Četverostruko rukovanje 11
2.3.2. CCMP enkripcijski protokol 13
2.3.3. Advanced Encryption Standard (AES) 16
2.3.4. EAP autentifikacijski protokol 18
2.3.5. Načini penetracije WPA2 protokola 20
2.4. WPA3 Protokol 21
2.5. Wi-Fi Protected Setup (WPS) 21
3. Vrste penetracijskih napada na lokalne bežične mreže 23
3.1. Prikupljanje informacija 23
3.1.1. Socijalni inženjering 24
3.2. Pasivni penetracijski napadi na bežične mreže 25
3.2.1. Prisluškivanje 25
3.2.2. Analiza i nadgledanje prometa podataka mreže 26
3.3. Aktivni penetracijski napadi na bežične lokalne mreže 26
3.3.1. Lažno predstavljanje 26
3.3.2. Preusmjeravanje i izmjena komunikacije unutar mreže 27
3.3.3. Slanje lažnih poruka 28
3.3.4. Prekidanje usluga 29
4. Alati potrebni za penetracijsko testiranje 31
4.1. Paket alata Aircrack-ng 31
4.2. Nmap alat za mapiranje mreže 32
4.3. Alat za penetracijsko testiranje Bettercap 33

4.4. Alat za penetracijsko testiranje MANA Toolkit 34
4.5. Alat za penetracijsko testiranje Pixiewps 34
4.6. Alat za probijanje zaporaka Hashcat 34
5. Praktični primjeri penetracijskog napada 36
5.1. Potreban hardver i softver za penetracijski napad 36
5.2. Postavljanje mrežnog adaptera za penetracijsko testiranje 37
5.3. Penetracijsko testiranje WEP protokola bežične mreže 38
5.4. Penetracijsko testiranje WPA/WPA2 protokola bežične mreže 41
5.5. Napad „Čovjek u sredini“ 43
5.6. Kreiranje lažne pristupne točke 45
5.7. Deautentifikacija uređaja s lokalne bežične mreže 46
6. Zaključak 48
Popis literature 49
Popis slika 51

1. Uvod

Svakodnevno koristimo svoje uređaje kako bi smo se mogli spojiti na Internet i uživali u beskrajnom sadržaju kojeg nam Internet nudi. S obzirom na sve veći porast IoT (*eng. Internet of Things*) uređaja potreba za korištenjem bežične tehnologije eksponencijalno je u porastu. Procjenjuje se da trenutno preko 700 milijuna uređaja poput pametnih telefona koriste Internet u svrhu komunikacije, interakcije i unaprjeđenja životnog standarda. Većina povezanih uređaja koristi bežične tehnologije za umrežavanje i komunikaciju na Internetu. Korisnici se svakodnevno povezuju na Internet uz pomoć bežičnih mreža bez slutnje kakve informacije i podatke mogu nenamjerno izložiti čitavoj okolini u kojoj se nalaze. Uz sve prednosti poput mobilnosti, brzine, pokrivenosti, bežične lokalne mreže imaju slabosti u aspektima sigurnosti podataka koji se odašilju signalom u zraku.

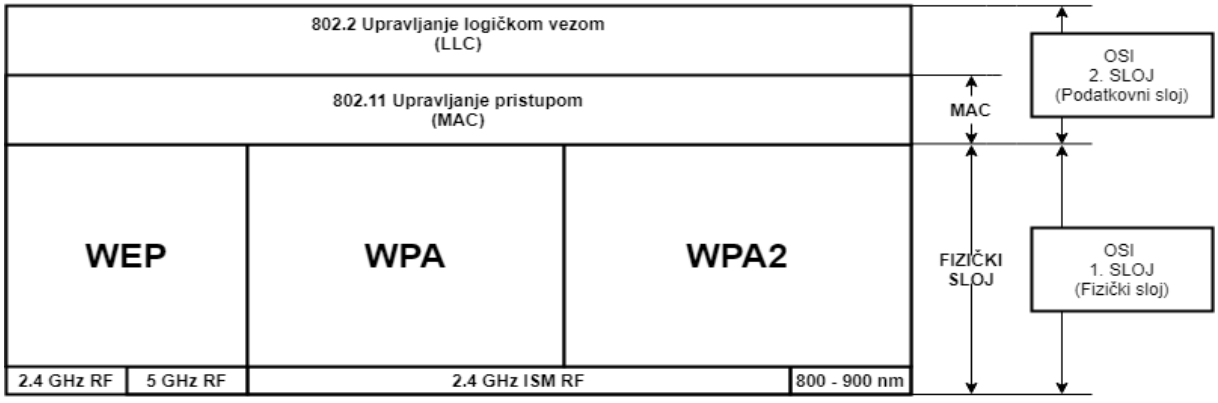
Kako bismo detaljno opisali opširnu temu u mrežnoj sigurnosti, rad je podijeljen na više dijelova. Prvi dio nas ukratko upoznaje s najkorištenijim sigurnosnim protokolima unutar IEEE 802.11 standarda. Opisat ćemo način rada protokola i mehanizme koje protokoli sadrže te opisati sve slabosti podložne napadima na mrežu. Drugi dio rada opisuje sve vektore napada korištenih u penetracijskom testiranju bežične lokalne mreže koji direktno ili indirektno napadaju bežične mreže. Napadi kao i alati korišteni pri testiranju biti će objašnjeni u praktičnom dijelu rada. Penetracijsko testiranje obavljat će se na Kali Linux operativnom sustavu pokrenutog u virtualnom stroju. Testirat će se sigurnosni mehanizmi bežičnih mreža poput WEP, WPA/WPA2 i WPS protokola. Zajedno uz sigurnosne mehanizme, rad će sadržavat napade unutar same bežične mreže poput presretanja podataka, lažnog predstavljanja i preusmjeravanja podataka unutar bežične lokalne mreže.

Svrha ovog rada je prikazati jasnu sliku ranjivosti bežičnih mreža koje uz pomoć različitih pristupa napada mogu ozbiljno povrijediti korisnikovu sigurnost i privatnost na Internetu. Rad pobliže opisuje metode rješavanja sigurnosnih nedostataka u bežičnoj sigurnosti koji uvelike mogu otežati rad napadača, te pogled u trenutnu situaciju svijeta mrežne sigurnosti bežičnih mreža.

2. Sigurnosni protokoli bežičnih mreža

Prijenos podataka ovisi o načinu prijenosa. Prijenos se može odvijati zrakom ili pomoću žice to jest vodiča. S obzirom da postoje dvije različite vrste prenošenja podataka, svaka vrsta medija ima svoje određene sigurnosne protokole ili mehanizme kako bi poruka nesmetano došla do krajnjeg korisnika. U bežičnoj mreži podaci putuju zrakom pomoću elektromagnetskih valova na određenoj frekvenciji stoga promet podataka zrakom treba biti na neki način zaštićen kako bi ostalim uređajima koji nisu dio mreže bilo onemogućeno prepoznavanje sadržaja poslane poruke bežičnim putem. Takve protokole čine algoritmi koju enkriptiraju sadržaj poruke stvarajući poseban specifični ključ uz pomoć kojeg se poruka može dešifrirati i pročitati. Sigurnost uz enkriptirani sadržaj čini i autentifikacija uređaja na bežične pristupne točke uređaja (eng. *access point*).

Početni su protokoli u početku pružali osnovnu zaštitu kontrolu pristupa i privatnosti. Prvi takav sigurnosni protokol zove se WEP (eng. Wired Equivalent Privacy) protokol, dio IEEE 802.11 standarda, s principom rada enkriptiranja poruke u unikatne ključeve. WEP se ubrzo nakon toga pokazao jako nesigurnim i propusnim na mrežne napade zbog slabog algoritma enkripcije i autentifikacije pristupnih uređaja. Sljedeća nadogradnja sigurnosti dolazi u obliku novog protokola nazvanog WPA (eng. Wi-Fi Protected Access). WPA protokol donosi nova poboljšanja u enkripcijskom algoritmu te nove protokole autentifikacije. WPA je nedugo zatim nadograđen novijim WPAv2 (eng. Wi-Fi Protected Access version 2) protokolom koji je danas najraširenij sustav sigurnosti lokalnih bežičnih mreža. WEP, WPA i WPA2 smješteni su na fizičkom sloju OSI modela vidljivo na slici 1.



Slika 1: Položaj sigurnosnih protokola u OSI modelu. Vlastita izrada prema (Poddar,Choudhary, 2014.)

2.1. Wired Equivalent Privacy protokol

Nakon službenog objavljivanja IEEE 802.11 standarda, početne bežične mreže uspostavljale su konekciju s korisnikom pomoću otvorenog tipa autentifikacije i uz jednostavnu enkripciju. Takav protokol naziva se WEP (eng. Wired Equivalent Privacy) protokol. Službeno predstavljen 1997. godine, WEP protokol spada unutar IEEE 802.11 standarda i kao takav je prvi protokol osmišljen u zaštiti sigurnosti bežičnih mreža.

Prema Hucabyu (2016.) protokol je zamišljen kako bi se sigurnost bežičnih mreža približila sigurnosti fizičkim mrežama to jest Ethernetu. U to vrijeme WEP protokol je bio jedini protokol bežične lokalne mreže koji je pružao metodu dijeljenja ključeva za enkripciju sadržaja. Dijeljenje ključeva radi tako da uređaj korisnika koji se želi priključiti bežičnoj lokalnoj mreži mora imati isti ključ kao i pristupna točka uređaja. Takvo dijeljenje ključeva mora se izvesti u unaprijed određeno vrijeme kako bi obje strane mogle potvrditi proizvoljne ključeve. Zbog međusobnog dijeljenja ključeva WEP protokol vrši ulogu autentifikacije i enkripcije gdje se korisnik može priključiti bežičnoj mreži jedino ako upiše pravilan WEP ključ postavljen od pristupne točke. Pristupna točka učestalo provjerava točnost WEP ključa korisnika tako da korisniku šalje slučajne fraze koje korisnik enkriptira i šalje rezultate pristupnoj točki koja tada provjerava točnost primljene fraze i identičnost ključa. Ključevi su prvotno sadržavali 40-bitni enkripcijski ključ, a kasnije i 104-bitni enkripcijski ključ prikazani u nizu od 10 ili 26 heksadekadskih znamenaka.

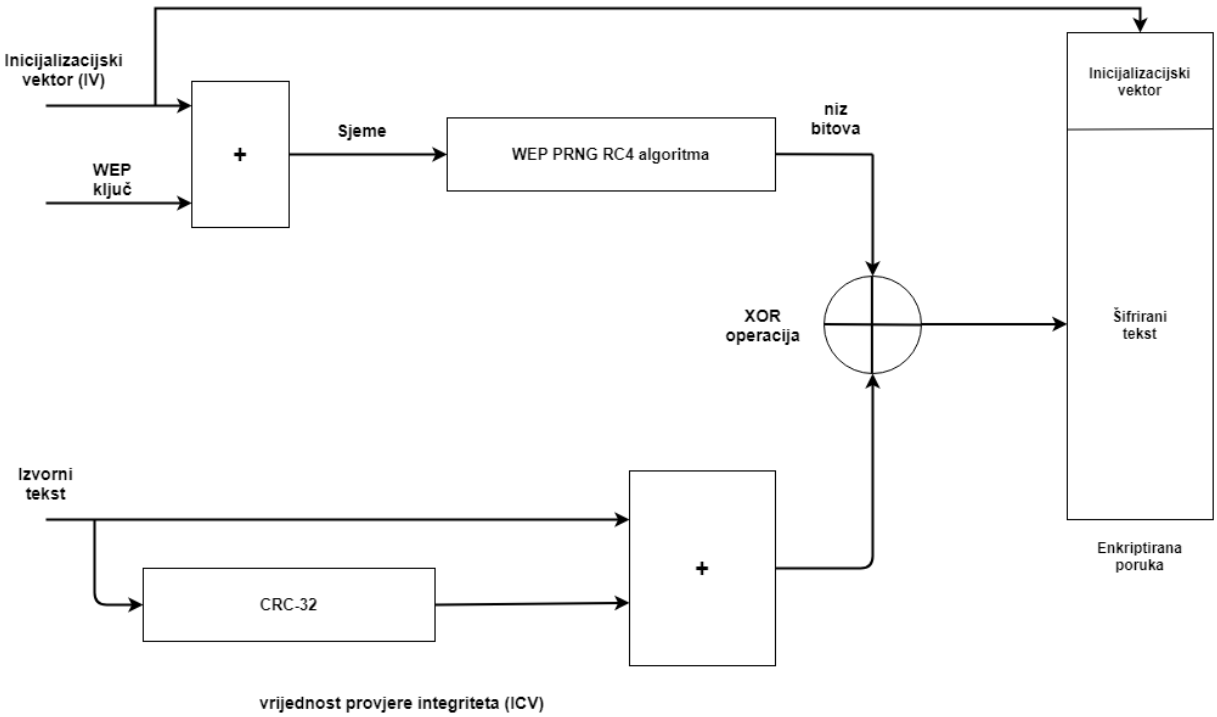
WEP se već 2001. godine pokazao kao protokol s ranjivim enkripcijskim algoritmom te je 2004. godine zamijenjen s novijim složenijim protokolom koji je pružao bolju sigurnost i manju ranjivost u bežičnim mrežama.

2.1.1. Algoritam

Za zaštićen prijenos podataka WEP protokol koristi RC4 enkripcijski algoritam koji se sastoji od dvije ključne komponente: KSA algoritma za pripremu ključa (eng. *Key Scheduling Algorithm*) i PRGA i algoritma pseudo nasumičnog generiranja (eng. *Pseudo-random Generation Algorithm*). KSA algoritma potreban je kako bi promiješao početne elemente zadane permutacije dok PRGA algoritam koristi promiješane elemente kako bi generirao pseudoslučajne ključeve koji se koriste u enkripciji podataka.

Enkripcijski proces WEP protokola zasnovan je na 40-bitnom i 104-bitnoj enkripciji gdje zajedno s inicijalizacijskim vektorom čini 64 bitnu i 128 bitnu enkripciju. Yao, Chong, Xingwei (2010.) objašnjavaju kako proces enkripcije započinje spajanjem inicijalizacijskog vektora (IV)

koji čini 24 bitni broj zajedno s WEP enkripcijskim ključem. Inicijalizacijski vektor tada generira ključ „sjeme“ to jest početni ključ koji se tada prosljeđuje PRNG komponenti RC4 algoritma. PRNG algoritam enkriptira izvorni nezaštićeni tekst koristeći pseudo-slučajne sekvence u niz bitova ključa. Niz bitova ključeva prolazi kroz XOR operaciju nakon koje dobijemo poruku koja sadrži šifrirani tekst zajedno s inicijalizacijskim vektorom. Drugi dio enkripcije sadržaja odnosi se na izvorni tekst kojeg enkriptiramo. Kako bi bili sigurni da poruka ne može biti modificirana prilikom slanja IV-a, nešifriranog teksta i ICV vrijednosti provjere integriteta (eng. *Integrity Check Value*) sustav koristi CRC32 cikličnu 32-bitnu provjeru redundancije (eng. *Cyclic Redundancy Check*). ICV računa kontrolnu sumu u okviru koja služi kao zaštita od promijene podataka u prijenosu. Opis procesa enkripcije vidljiv je na slici 2.



Slika 2: Prikaz procesa enkripcije WEP protokola. Vlastita izrada prema (Yao, Chong, Xingwei, 2010.)

2.1.2. Sigurnosni propusti WEP protokola

U današnje vrijeme korištenje WEP protokola pri autentifikaciji u bežičnim mrežama gotovo smanjena na minimum zbog velikih sigurnosnih propusta otkrivenih početkom 21. stoljeća. Iako se kriptografski RC4 algoritam koristi i u nekim današnjim softverima, zbog njegove jednostavnosti takav način enkripcije je podložan laganom probijanju zaštite kako bi se otkrio izvorni tekst.

Prodanović i Simić (2007.) navode kako postoje nekoliko sigurnosnih propusta WEP protokola:

Opasnost od ponovnog korištenja niza bitova ključeva korištenih u WEP autentifikaciji. Glavni sigurnosni problem polazi od inicijalizacijskog ključa koji zajedno s WEP ključem čini enkriptiranu poruku. Problem nastaje u tome što se paketi mogu ponavljati s istim IV-om. Kada takve poruke dođu do napadača on može iskoristiti XOR operaciju nad dva paketa s istim vektorom kako bi dobio izvorni tekst. Rezultati jednog paketa nakon XOR operacije mogu se iskoristiti za dekriptiranje drugog paketa WEP protokola. Mane inicijalizacijskog vektora su rijetka promjena ključa gdje postoji mogućnost generiranja istog ključa inicijalizacijskog vektora. Taj problem je najviše ranjiv zbog toga što poruka IV-a nema enkripciju stoga napadač može lagano pročitati vrijednosti IV-a i tako otkriti cijeli sadržaj poruke. S obzirom da IV ima samo dužinu od 24 bita njegova veličina se ne može mijenjati stoga postoji mali broj permutacija unutar WEP standarda.

Drugi najveći problem sigurnosti korištenja WEP protokola je upravljanje ključevima. WEP protokol nije imao točno definirana pravila distribucije ključeva u mreži. Gledajući da bežične mreže za autentifikaciju koriste jedan ključ, više osoba s istim ključem povećavaju mogućnosti brze dekripcije ključa bežične lokalne mreže. Učestala promjena ključeva iziskuje veliku potrošnju vremena rekonfiguracije hardvera s promjenama stoga više korisnika koristi jedan ključ čime povećavaju mogućnosti dohvaćanja inicijalizacijskog vektora od strane napadača.

Sigurnosni mehanizmi WEP protokola, uz današnju tehnologiju, mogu biti dekriptirani u roku nekoliko minuta. Današnji usmjernici koji imaju mogućnost bežične pristupne točke ne nude opciju postavljanja WEP protokola kao protokola za autentifikaciju na bežičnu mrežu.

2.1.3. Načini penetracije WEP protokola

Beck i Tews (2008) objašnjavaju nekoliko vrsta penetracijskih napada na WEP protokol:

- FMS napad (Fluhrer, Mantin i Shamir) prvi je oblik penetracijskog napada na WEP protokol u bežičnom mrežama. Napad na WEP odvija se pomoću pasivnog prisluškivanja prometa bežične lokalne mreže gdje uz pomoć WEP protokola možemo snimiti velik broj poslanih enkriptiranih podataka u kojima se nalaze i inicijalizacijski vektori paketa. Napadač tada iskorištava sigurnosne mane WEP algoritma te jednadžbom dobiva moguće rezultate ključa. Ovakav napad prvi je napad na bežične lokalne mreže s autentifikacijom. Iako postoji 5% šanse točnosti rezultata uz korištenje jednadžbe, da bi napad bio uspješan potrebno je snimiti i analizirati od 4 do 6 milijuna paketa kako bi uspješnost napada premašivala 50%.
- „KoreK“ napad poboljšana je verzija FMS napada u kojem se jednadžba za dobivanje ključa dodatno poboljšala kako bi smanjio potrebni broj uhvaćenih paketa na 700 tisuća uz moguću 50%-nu uspješnost.
- PTW ili Pyshkin, Tews, Weinmann napad je nadopuna prošlih napada s boljim korelacijskim jednadžbama koje smanjuju vrijeme izračuna mogućnosti ključa. Drugi novi nadopunjeni koncept napada mijenja pristup izračuna nakon uhvaćenih paketa. Ovakav napad smanjuje potrebni broj uhvaćenih paketa na 35 do 40 tisuća uz 50%-nu uspješnost.
- „Chopchop“ napad je napad koji omogućava napadaču da iz snimljenih paketa dekriptira zadnji n broj bajtova izvornog teksta u enkriptiranoj poruci gdje u mrežu odašilje n puta 128 paketa. Ovakav napad nije usmjeren prema propustima RC4 algoritma, nego napad je zamišljen da matematički izračuna i pogodi kontrolnu sumu paketa koji se šalje pristupnoj točki bežične mreže. Ako je kontrolna suma točna napadač saznaje zadnji bajt izvorne poruke. Ovakav proces zahtjeva najmanje 128 pokušaja do najviše 256 pokušaja da bi dobili zadnji bajt izvorne poruke.

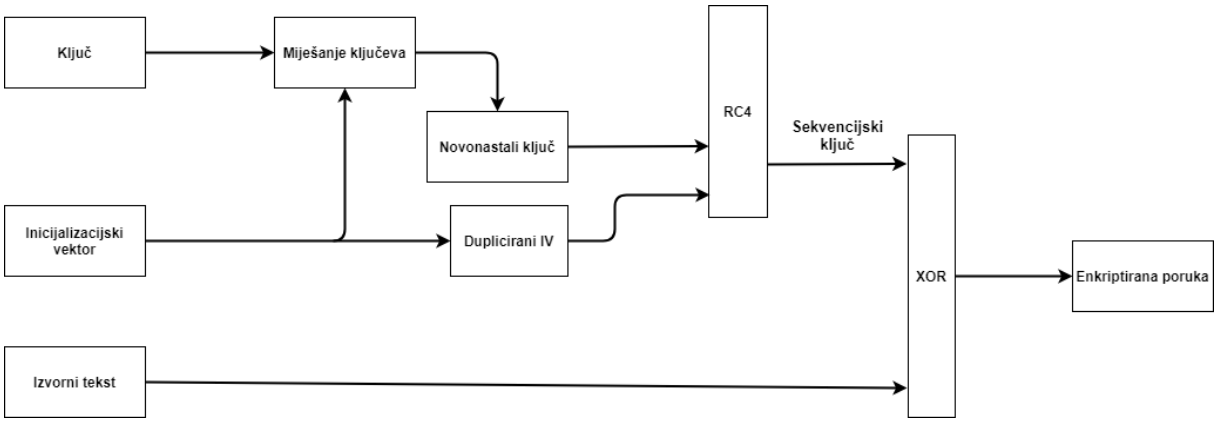
2.2. WPA protokol

Kako bi zamijenili i poboljšali nedostatke WEP protokola, 2004. godine IEEE institut objavljuje novi protokol za bežičnu mrežnu sigurnost zvan WPA (eng. *Wi-Fi Protected Access*) pod standardom IEEE 802.11i koji će svojom strukturom i novim algoritmima zamijeniti ranjive WEP mehanizme enkripcije. WPA donosi novi enkripcijski protokol zvan TKIP (eng. *Temporal Key Integrity Protocol*) te novi algoritam MIC (eng. *Message Integrity Check*) za provjeru integriteta paketa. Takav protokol specifično je dizajniran kao nadogradnja na prošle sustave mrežne bežične opreme. Ciljevi WPA protokola usmjereni su na poboljšanje mehanizama bežične mreže pružajući potpunu sigurnost, korištenje u poslovnom i kućnom okruženju te jednostavnu nadogradnju na već postojeće uređaje. Protokol koristi RC4 algoritam za kriptiranje poruka koristeći nadograđeni 128-bitni ključ zajedno s 48-bitnim inicijalizacijskim vektorom.

2.2.1. TKIP protokol

Temporal Key Integrity Protokol ili TKIP podrazumijeva skupinu različitih algoritama koji zajednički sudjeluju u procesu enkripcije podataka bežične mreže. TKIP protokol karakterističan je po povećanim 48-bitnim inicijalizacijskim vektorom u odnosu na IV WEP protokola, nudi mogućnost korištenja mehanizama ponavljajućih ključeva te provjeru integriteta paketa ili (MIC). Kako je prijašnji algoritam RC4 već uveliko implementiran na uređaje bežične mreže, TKIP koristi RC4 algoritam za potpuno drugačiji pristup dijeljenju ključeva. (Prodanović, Simić, 2007.)

Glavna razlika između načina rada WPA i WEP protokola je u procesu enkripcije TKIP algoritma WPA protokola. Inicijalizacijski vektor spaja se s tajnim ključem nakon čega se izmiješa (eng. *hash*) te nastaje novo pomiješani ključ. IV se duplicira i ponovno spaja s izmiješanim ključevima koji ulaze u RC4 algoritam nakon čega se XOR operacijom spaja s izvornim tekstom kojeg je potrebno enkriptirati (slika 3).



Slika 3: Princip rada TKIP protokola u WPA. Vlastita izrada prema (Khasawneh, Kajman, Alkhudaidy, Althubyani, 2014.)

Zadatak TKIP protokola je generacija posebnog ključa za svaki različiti poslani paket u mreži. Svaki paket zahtjeva novi ključ generiran miješanjem TKIP ključa i sekvence inicijalizacijskog vektora. Generacija ključa odvija se u dvije faze. U prvoj fazi se izračunava funkcija miješanja ili hash, funkcija ovisno o MAC (eng. *Media Access Control*) adresi korisnika koja zahtjeva ključ, privremeni ključ te 32-bitni incijalizacijski vektor. Izvršavanje ove faze ovisi o promjeni privremenog ključa, ako je privremeni ključ promijenjen faza se izvršava. Drugi dio generiranja ključa ovisi o izvršenju prve faze. Izlazni produkt prve faze spaja se s 16-bitnim IV koji zajedno u zbroju čine 128-bitnu enkripciju. Druga faza događa se pri miješanju ključeva kako potencijalni napadač ne može direktno odrediti pripadnost IV-a i ključeva za svaki poslani paket. (Prodanović, Simić, 2007.)

2.2.2. MIC algoritam

Algoritam za provjeru integriteta ili MIC (eng. *Message Integrity Check*) spada u skupinu algoritama napravljenih unutar TKIP protokola. MIC još nazivamo i „Michael“ algoritam koji je dizajniran prvenstveno kao enkripcijski algoritam koji služi kao brojač okvira koji se prenose u paketima između korisnika i pristupne točke bežične lokalne mreže. Okvir dobiven TKIP protokolom veže vrijednost MIC-a na poruku koja se tada enkriptira RC4 algoritmom i šalje primatelju poruke. Primatelj ponovno izračunava MIC vrijednost i uspoređuje rezultat s vrijednošću dobivene poruke. Ako se vrijednosti podudaraju poruka se prikazuje primatelju, a ako su vrijednosti različite poruka se odbacuje. Takvim načinom verifikacije MIC zaštićuje poruku u prijenosu od izmjenjivanja sadržaja poruke tijekom komunikacije korisnika s poslužiteljem.

Prodanović i Simić (2007.) vrše podjelu MIC algoritma na tri važne komponente:

- Autentifikacijski ključ koji se sastoji od „Michael“ ključa, ključ kojeg moraju imati oba smjera u kojem se komunikacija održava.
- Funkciju označavanja.
- Verifikaciju.

Autentifikacijski ključevi ili „Michael“ ključevi nazivamo ključevima generiranih unutar TKIP protokola koji nastaju uz pomoć hash funkcije. Tijekom komunikacije primatelj i pošiljatelj poruke koriste 64-bitne ključeve.

Funkcija označavanja koristi se pri verifikaciji poslanog ključa i poruke. MIC oznaka spaja se s originalnom porukom te se šalje primatelju. Ako oba smjera komunikacije imaju jednake oznake poruka se dostavlja primatelju.

Verifikacija djeluje tako da TKIP protokol provjerava broj lažnih ili pogrešnih poruka. Ako u intervalu od jedne sekunde TKIP poprimi dvije ili više lažnih poruka od MIC-a, protokol pretpostavlja da je razlog lažnih poruka vanjski napad. U takvoj situaciji ključevi se brišu te se uspostavlja blokada sesije od jedne minute nakon što MIC i TKIP generiraju nove ključeve.

2.2.3. WPA autentifikacije

Gledajući da WEP protokol nema nikakav oblik autentifikacije to jest sadrži otvoreni tip autentifikacije, da bi riješili sigurnosne mane WEP protokola, WPA i nadograđeni WPAv2 protokol koriste dvije vrste autentifikacijskih mehanizama, WPA Personal i WPA Enterprise. WPA Personal autentifikacija je namijenjena privatnim osobama to jest u SOHO (eng. Small Office Home Office) okruženju, a WPA Enterprise u poslovnom svijetu i robusnijim mrežama gdje je očekivana razina sigurnosti mreža znatno veća u odnosu na osobne bežične mreže.

- WPA Personal vrsta autentifikacije sastoji se od već unaprijed podijeljenog ključa (eng. Pre-Shared Key) te se zbog toga još naziva i WPA-PSK autentifikacija. PSK autentifikacija ne koristi serversku podršku autentifikacije kao Enterprise autentifikacija. Princip rada zasniva se na razmjenu ključeva između korisnika koji se želi priključiti na bežičnu mrežu i pristupne točke mreže. Obje strane komunikacije moraju znati vrijednosti ključeva izvora i primatelja. Bežični uređaji koriste 256-bitne ključeve za autentifikaciju s pristupnim točkama. Prednost ovakve vrste autentifikacije je nemogućnost brzog izračuna vrijednosti ključeva u razumnom vremenu što povećava vrijeme dobivanja hash vrijednosti ključeva. (Khasawneh, Kajman, Alkhudaidy, Althubyani, 2014.)
- WPA Enterprise predstavlja robusniji način zaštite bežičnih lokalnih mreža koji koristi server pomoću kojeg korisnik dobavlja potrebne autentifikacijske podatke za povezivanje na mrežu. Enterprise vrsta autentifikacije najčešće se koristi u poslovnim

okruženjima jer pruža visoku razinu sigurnosti. Ovakav način autentifikacije vrši se uz pomoć EAP (eng. *Extensible Authentication Protocol*) protokola (detaljnije objašnjenog u 2.3. WPAv2 odlomku rada) te servera za autentifikaciju zvanog RADIUS (eng. *Remote Authentication Dial In User Service*). Autentifikacija se odvija na način da korisnik ima jedinstveni autentifikacijski ključ zapisan na serveru pomoću kojeg se povezuje na bežičnu mrežu. (Rumale, Chaudhari 2011.)

2.2.4. Načini penetracije WPA protokola

S obzirom na mehanizme zaštite, WPA protokol je i dalje ranjiv na određene penetracijske napade. Slabost ovog protokola nalazi se u TKIP protokolu u kojem se iz kratkog enkriptiranog paketa može dobaviti vrijednost MIC ključa zajedno s nekriptiranim tekstom koristeći metodu lažiranja paketa u mreži.

Najpoznatiji pristup napada na WPA protokol zove se „Chopchop“ napad autora Becka i Tewsa. „Chopchop“ napad koristi sličan vektor napada kao i u WEP protokolu koristeći mehanizme kvalitete usluge (eng. Quality of Service – QoS). Kvaliteta usluge pruža bežičnim mrežama komunikaciju kroz različite kanale između korisnika i bežične mreže kroz koju se odvija promet paketa. Kvaliteta usluge sastoji se od brojača vremena (eng. *Time Stamp Counter* – TCS) koji je specifičan za pojedini kanal kvalitete usluga. Napad se izvodi na način da napadač hvata enkriptirani inicijalizacijski vektor na određenom kanalu bežične mreže nakon kojeg se, zbog brojača vremena, napad vrši na različitom kanalu nego uhvaćeni paket u kojem je vrijednost brojača vremena manja nego na početnom kanalu napada. Nekriptirani tekst se dohvaća pomoću adresnog rezolucijskog protokola (eng. *Address Resolution Protocol* – ARP) gdje se izračunavaju bajtovi i nakon toga uspoređuju s dohvaćenim vrijednostima MIC ključa i kontrolne sume koristeći „chopchop“ napad. Ako kontrolne sume nisu identične sumama uhvaćenih vrijednosti ARP-a, paket se odbacuje. Proces se ponavlja dok svi kandidati ARP paketa nisu smanjeni na posljednju vrijednost koja dekriptira cijeli sadržaj poruke. Nakon dekriptiranog paketa, napadač šalje lažno stvoreni paket korisniku koji takav paket interpretira kao stvarni paket. Napad „chopchop“ se mora dogoditi u $x - 1$ minuta gdje x označava broj pokušaja radi zaštitnog mehanizma MIC ključeva gdje se ključevi mijenjaju ako se pojave minimalno dvije pogreške unutar jedne minute. (Ohigashi, Morii, 2009.)

2.3. WPA version 2 protokol

Ubrzo nakon službenog izlaska WPA protokola unutar IEEE 802.11i standarda, u bežičnoj sigurnosti pojavljuje se nova, poboljšana inačica WPA protokola koja danas čini najpopularniju i najrašireniju metodu enkripcije i autentifikacije podataka bežične lokalne mreže. Novi protokol zadržao je mehanizme prethodnog WPA protokola poput EAP protokola za autentifikaciju i četverostrukog rukovanja. WPA version 2 ili WPA2 protokol donosi velik broj poboljšanja u odnosu na prošlu generaciju WPA protokola poput nove vrste unaprijeđenog standarda enkripcije (eng. *Advanced Encryption Standard* – AES) te CCMP (eng. *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) algoritam zaštite podataka.

2.3.1. Četverostruko rukovanje

Proces četverostrukog rukovanja pojavljuje se u WPA protokolu unutar WPA Enterprise i WPA-PSK načina autentifikacije. Četverostruko rukovanje pridonosi sigurnosti novog WPA2 protokola jer u kombinaciji s novim enkripcijskim algoritmom i CCMP zaštitom podataka nudi autentifikaciju između pristupne točke i korisnika bežične mreže pomoću koje mogu međusobno potvrditi identitet bez otkrivanja vrijednosti ključa za autentifikaciju. Komunikacija između korisnika i pristupne točke odvija se enkripcijskim porukama koristeći proširivi autentifikacijski protokol na lokalnoj mreži (eng. *Extensible Authentication Protocol over LAN* – EAPOL). Enkripcijske poruke jedino mogu dekriptirati sudionici komunikacije uz pomoću uparenog glavnog ključa (eng. *Pairwise Master Key* – PMK). Ako se pri komunikaciji poruke uspješno dekriptiraju, tada se uspostavlja autentifikacija između korisnika i pristupne točke. Princip rada četverostrukog rukovanja zasniva se na izmjeni četiri poruka između pristupne točke, poznatog imenom „autentifikator“ i korisnika bežične mreže ili „suplikantom“ u svrhu generiranja enkripcijskih ključeva potrebnih za enkripciju prijenosa podataka preko bežične mreže. Proces četverostrukog rukovanja sastoji se od pet različitih ključeva i dva različita slučajno generiranih brojeva.

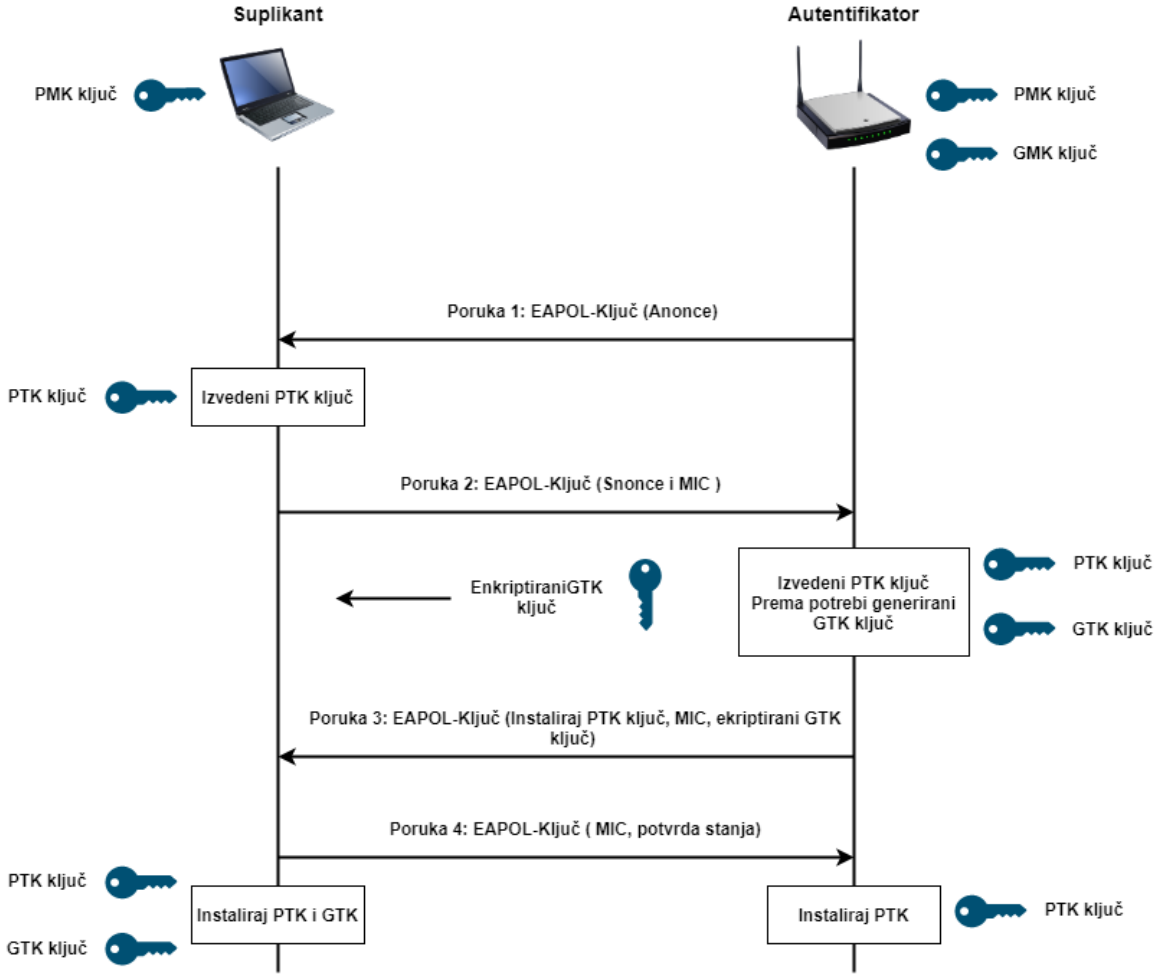
Četverostruko rukovanje započinje prijenosom prve poruke koja prenosi slučajno generiran broj od strane pristupne točke (eng. *Anonce*) koja uz pomoć EAPOL protokola dolazi do povezanog uređaja te generira upareni sjednički ključ (eng. *Pairwise Transit Key*- PTK). Svježe generirani PTK ključ izveden je pomoću glavnog uparenog ključa PMK koristeći matematičke pseudoslučajne funkcije. Oba uređaja međusobno znaju svoje jedinstvene MAC adrese kako bi generirali PMK ključeve. Uz PMK ključeve dolazi i identifikacijski broj PMK ključa zvan PMKID. PMKID će se kasnije pokazati kao najveća slabost četverostrukog rukovanja jer napadač može uhvatiti identifikacijski broj PMK ključa te probiti zaštitu WPA2

protokola bez direktnog povezivanja i deautentifikacije korisnika na bežičnoj mreži. Pseudoslučajne funkcije koriste glavni ključ, MAC adrese oba uređaja te slučajno generiran broj od strane autentifikatora i suplementa kao „recept“ za dobivanje uparenog sjedničkog ključa. Poruka se provjerava algoritmom za provjeru integriteta (MIC) koji, ako sadrži poruku s pogreškom ili nepoznatim sekvencijskim slijedom odbacuje poruku i prisiljava korisnika na deautentifikaciju.

Nakon generiranja PTK ključa rukovanje se nastavlja povratnom porukom suplikanta usmjerenom prema pristupnoj točki bežične mreže. U drugoj poruci rukovanja suplikant šalje svoj vlastiti generirani slučajni broj (eng. *Snonce*) pristupnoj točki kako bi ona također mogla generirati PTK ključ. Poruka se prenosi pomoću EAPOL protokola koristeći MIC kako bi se zaštitio integritet i sadržaj poruke tijekom prijenosa. Autentifikator može generirati PTK ključ nakon uspješnog prijenosa Snonce vrijednosti.

Autentifikator prihvaća prethodno poslanu poruku koristeći MIC algoritam te započinje slanje treće poruke koja šalje poruku suplementu. U poslanoj poruci autentifikator generira grupni privremeni ključ (eng. Group Temporal Key- GTK) koji nastaje uz pomoć grupnog glavnog ključa (eng. Group Master Key – GMK), specifičan za svaki uređaj s mogućnošću bežičnog povezivanja. GTK ključ koristi se pri enkriptiranju i zaštite prijenosa podataka između povezanog uređaja i pristupne točke. Svaki GTK ključ predstavlja jedinstvenu vrijednost za pojedinu pristupnu točku u bežičnoj mreži, koju autentifikator u trećoj poruci šalje svim uređajima koji zahtijevaju autentifikaciju s pristupnom točkom.

Zadnju poruku četverostrukog rukovanja šalje suplikant kojom potvrđuje stanje primljenog GTK ključa poslanog u prethodnoj poruci. Proces autentifikacije pomoću četverostrukog rukovanja vidljiv je na slici 4. („4-way handshake“, 2019; He, Mitchell 2004.)



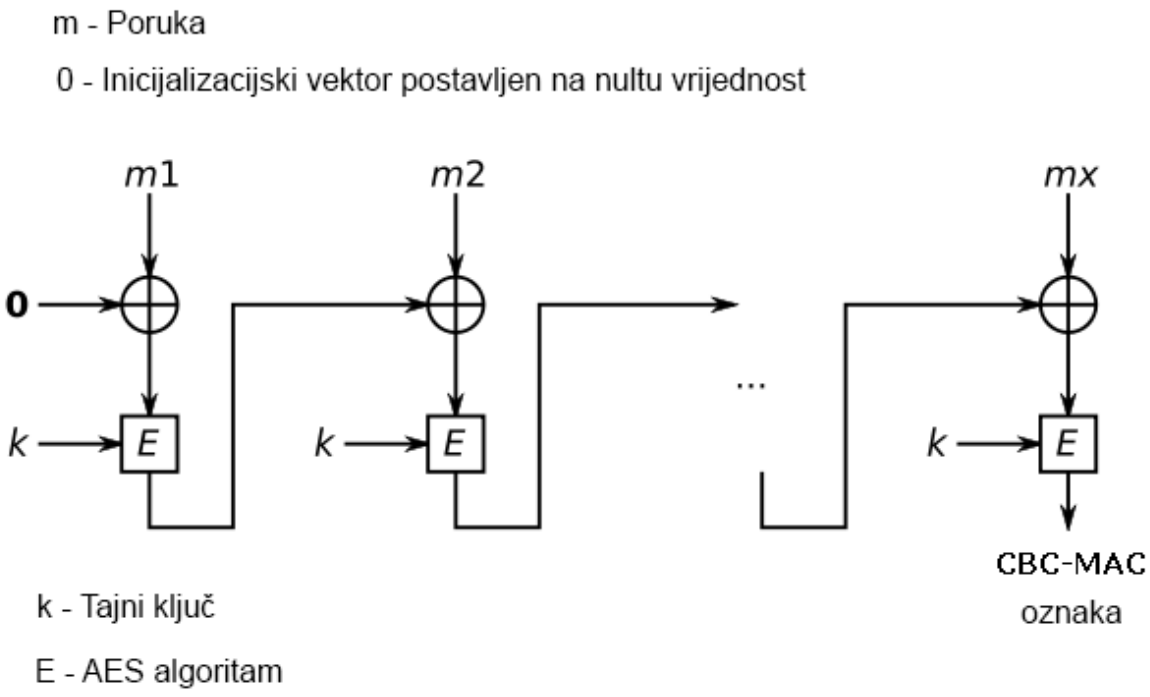
Slika 4: Prikaz procesa četverostrukog rukovanja. Vlastita izrada prema: („4-way handshake“, 2019.)

2.3.2. CCMP enkripcijski protokol

Uz nadograđenu verziju WPA2 protokola dolaze i nove vrste enkripcijskih algoritama koji rješavaju mane i slabosti prethodno korištenog TKIP algoritma u WPA protokolu. Tako WPA2 uvodi novi algoritam CCMP (eng. *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) unutar IEEE 802.11i standarda koji u usporedbi s TKIP algoritmom donosi novi napredni enkripcijski standard (eng. *Advanced Encription Standard.-AES*) (poglavlje 2.3.3.), ulančani način kriptiranja blokova te brojač. Ovakav način enkripcije, poput CCMP enkripcije, smatran je najpouzdanijim i trajnijim rješenjem zaštite podataka bežičnih lokalnih mreža.

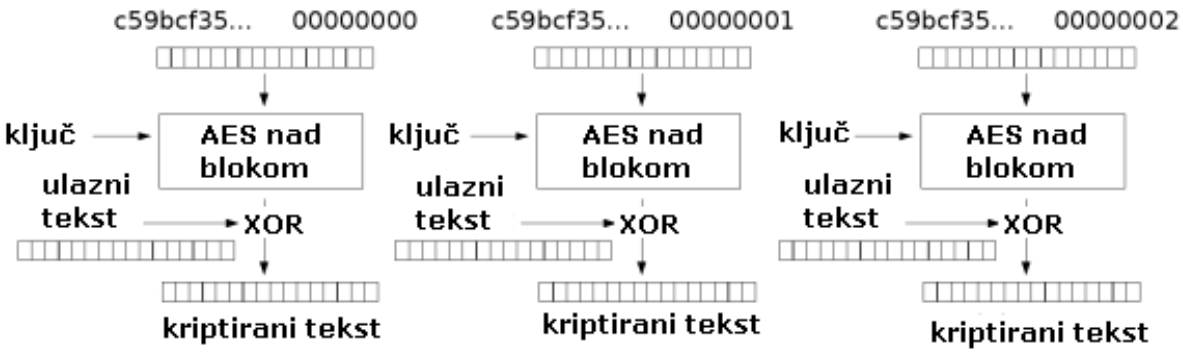
Princip rada CCMP protokola temelji se na AES kriptosustavu koji koristi CCM (eng. *Conter Mode Encryption with CBC-MAC Data Origin Autenticity*) enkripciju i autentifikaciju. CCM algoritam specifičan je po tome što se pri kriptiranju blokova podataka koristi kombinaciju

dviju različitih metoda AES enkripcije, CBC-MAC (eng. *Cipher Block Chaining Message Authentication Code*) i CTR (eng. *Counter mode*) algoritam. CCM način enkriptira poruku korištenjem jednog jedinog ključa koji ima dvostruku ulogu enkripcijskog ključa i autentifikatora unutar CCMP enkripcije. Zbog dvostruke uloge CCM je zamišljen kao algoritam koji radi na blokovima podataka dobivenih pseudoslučajnim permutacijama AES kriptosustava veličine 128 bita. CCM algoritam u svojem načinu rada prvo koristi CBC-MAC tehniku zaštite integriteta poruka tijekom enkripcije. Princip rada CBC-MAC algoritma započinje postavljanjem inicijalizacijskog vektora na nultu vrijednost koji se miješa s blokovima poruka. Pomiješani blok podataka tada koristi AES enkripciju nakon koje se primjenjuje XOR funkcija sa sljedećim blokom podataka gdje se proces ponavlja za svaki sljedeći blok podataka sve do posljednjeg bloka. Rezultat posljednjeg bloka CBC-MAC algoritma daje konačnu vrijednost MAC. Prikaz CBC-MAC procesa autentifikacije vidimo na slici 5. („Croatian Academic and Research network“ [CARNet], 2009.; Whiting, Housley, Ferguson, 2003.)



Slika 5: Prikaz CBC-MAC algoritma za izradu MAC oznake. Vlastita izreda prema (CARNet, 2009.)

Nakon dobivene MAC oznake koja čini autentifikacijski dio CCM mehanizma, dobiveni integritet ponovno prolazi kroz AES enkripciju u CTR algoritmu koji čini enkripcijski dio CCM mehanizma. CTR proces započinje postavljanjem vrijednosti brojača koji se koristi u enkripciji MIC-a i poruke. Prilikom enkripcije MIC-a vrijednost brojača postavlja se na nulu, a pri enkripciji poruke brojač sadrži vrijednost 1. Blokovi podataka se tada enkriptiraju pomoću XOR operacije nakon koje se povećavaju vrijednosti brojača za jedan. Princip rada i enkripcije CTR algoritma vidljiv je na slici 6. („Croatian Academic and Research network“ [CARNet], 2009.; Whiting, Housley, Ferguson, 2003.)



Slika 6: Proces CTR enkripcije poruke i MIC-a (CARNet, 2009.)

CCMP koristi CCM mehanizme enkripcije i autentifikacije kako bi zaštitila integritet poruke u bežičnoj mreži i MPDU (eng. *Media Access Control Protocol Data Unit*) poruka koje služe u izmjeni komunikacije između uređaja u bežičnoj mreži unutar MAC sloja OSI (eng. *Open Systems Interconnection*) modela. Prema objašnjenom načinu rada CCMP mehanizama zaštite podataka, vidljivo je kako CCMP pruža dominantnu zaštitu u usporedbi s prošlim mehanizmima WEP i WPA protokola. Najveći nedostatak ovog mehanizma predstavlja složenost integracije mehanizma u već postojeće sustave bežične zaštite.

2.3.3. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) predstavlja grupu novih enkripcijskih standarda koji su zamišljeni u svrhu zamijene starijeg DES (eng. Dana Encryption Standard- DES) algoritma. AES algoritam osmišljen je 2001. godine kao algoritam koji koristi ulančano kriptiranje blokova podataka. Iako je autor algoritma AES osmislio da podržava 128-bitne, 192-bitne i 256-bitne blokove podataka, standard koristi samo 128-bitne blokove podataka. 128-bitni blokovi podataka mogu koristiti 128-bitne, 192-bitne ili 256-bitne kriptografske ključeve. AES algoritam za enkripciju koristi matricu bajtova kojoj veličina stupaca i redova ovisi u broju bajtova, a najčešće čini matricu reda 4 x 4.

Kako bi kriptirali ili dekriptirali podatke pomoću AES algoritma, proces je potrebno razdijeliti na određeni broj koraka. Koraci i njihov broj ovise o veličini bloka podataka, s obzirom da bežične mreže unutar WPA2 protokola koriste 192-bitne blokove podataka potrebno je obaviti 10 koraka AES enkripcije. U ostalim inačicama s 192-bitnim i 256-bitnim blokovima podataka koristimo 12 i 14 koraka enkripcije. (Mahajan, Sachdeva, 2013.)

Svaki korak unutar enkripcije sastoji se od četiri različite razine koje sadrže četiri transformacije matrica:

1. Zamjena znakova – Bajtovi matrice se zamjenjuju sa supstitucijskom matricom zvanom Rijndaelova S kutija veličine 8 bitova.
2. Posmak redova – Svi redovi matrice osim prvog reda bivaju pomaknuti. Svaki bajt se pomiče ulijevo u odnosu na početnu poziciju na matrici.
3. Miješanje stupaca – Stupac bloka matrice množi se s fiksnim polinomom $c(x)$.
4. Dodavanje potključa – potključevi se kombiniraju pomoću XOR operacije s matricom bajtova.

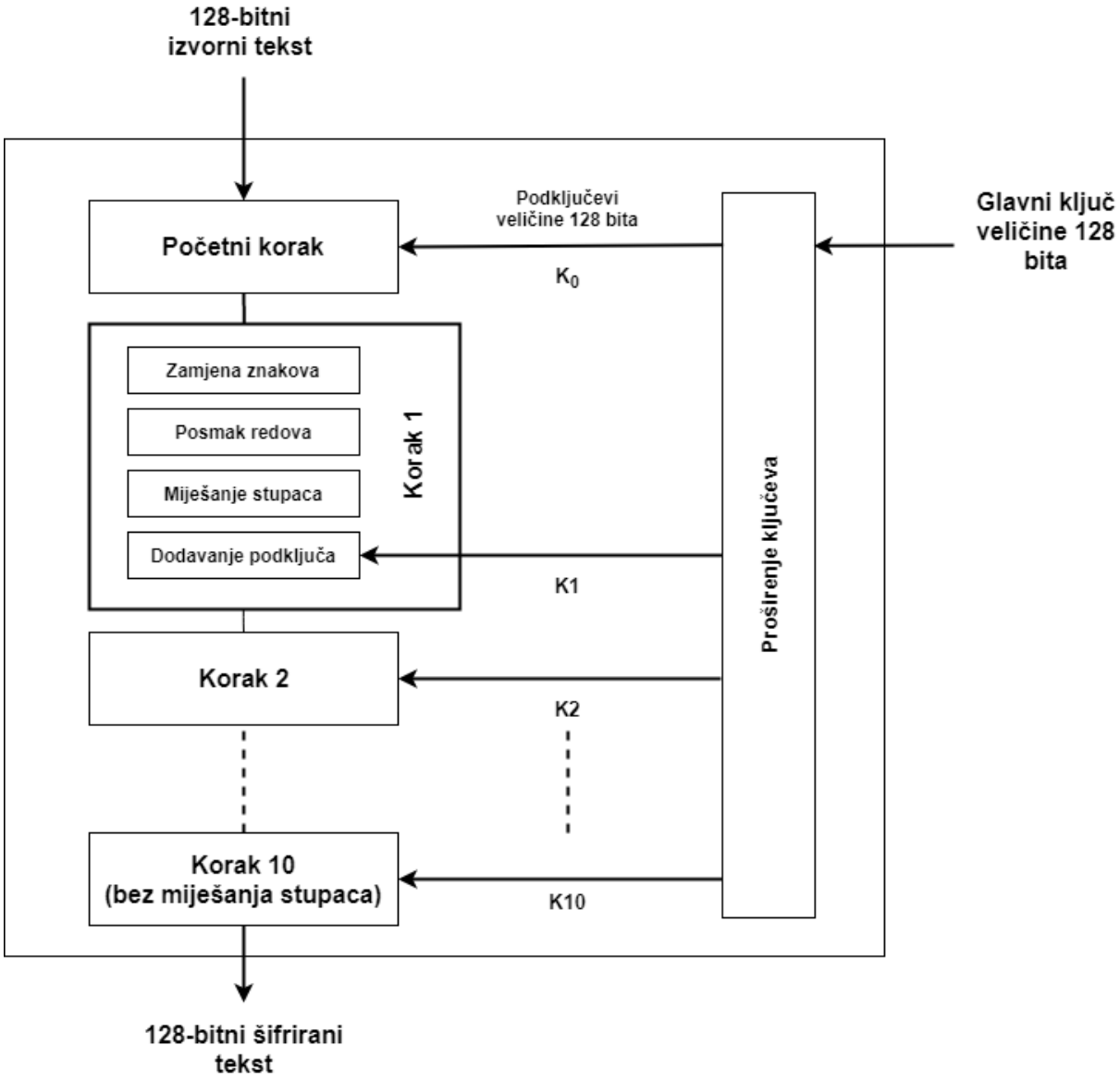
Prva faza odnosi se na generiranje potključeva koji se izvode od glavnog ključa u enkripciji. Prošireni ključ će imati jednak broj bitova kao i veličina bloka podataka pomnožena s brojem koraka gdje se veličini potključa dodaje još jedan bit jer je enkripciji potreban jedan ključ za početnu fazu transformacije.

Druga faza obuhvaća kombiniranja generiranog potključa glavnog ključa s matricom bajtova. Potključevi se dodaju matrici pomoću XOR operacije gdje je veličina potključa jednaka veličini bloku podataka potrebnog za enkripciju.

Treća faza sastoji se od enkripcije koraka za 128-bitni blok podataka u kojem se primjenjuju sve četiri transformacije matrica. Na svaki korak primjenjuje se sve četiri operacije te se postupak ponavlja za sve ostale korake.

Posljednja faza opisuje posljednji korak enkripcije u kojem se primjenjuju sve transformacije osim miješanja stupaca. Sadržajno posljednji korak ima istu strukturu kao i

koraci treće faze. Proces AES strukture i transformacija u koracima vidljiv je na slici 7. (Daemen, Rijmen, 2002.)



Slika 7: Shematski prikaz AES strukture i transformacija u koracima. Vlastita izrada prema (AES structure, bez dat.)

2.3.4. EAP autentifikacijski protokol

Proširivi autentifikacijski protokol (eng. *Extensible Authentication Protocol* – EAP) spada pod IEEE 802.1X standard koji omogućuje noviji, robusniji način autentifikacije. Prvotno zamišljen za Ethernet mreže, EAP se danas najčešće koristi u bežičnim mrežama. Prednosti EAP protokola je široka prilagodljivost različitim metodama autentifikacije u bežičnim mrežama.

Način rada EAP protokola razlikuje se od svih prošlo navedenih autentifikacijskih metoda bežičnih mreža. Kada se korisnik želi povezati na bežičnu mrežu, EAP protokol ne pokušava uspostaviti vezu s određenim autentifikacijskim mehanizmom, kao što je WEP ili WPA-PSK protokol činio, nego korisnik odabire EAP metodu autentifikacije nakon koje se slijedi razmjenjivanje autentifikacijskih poruka. EAP autentifikacijska struktura sastoji se od tri glavne komponente, EAP klijenata (eng. *Peer*) to jest korisnika koji se povezuje na određenu bežičnu mrežu, EAP autentifikatora kojeg nazivamo pristupnom točkom koji čini posrednika između korisnika i pristupa bežičnoj mreži te autentifikacijskog poslužitelja koji dogovara uvjete autentifikacije s korisnikom poput metode koje korisnik želi koristiti, jesu li autentifikacijski paketi ispravni. Poslužitelj nakon provjerene poruke omogućava ili onemogućava pristup bežičnoj mreži. Komunikaciju između autentifikacijskog poslužitelja i EAP autentifikatora održava RADIUS (eng. *Remote Authetication Dial-In User Service*) poslužitelj. (CARNet, 2008.)

Prema CARNetu (2008) EAP komunikacija između korisnika i autentifkatora sastoji se od četiri tipa poruka:

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

Komunikacija započinje autentifikator slanjem EAP paketa zahtjeva korisniku u kojem se nalazi određena EAP metoda autentifikacije zajedno sa zahtjevom za identitetom uređaja koji se želi povezati na bežičnu mrežu. U povratnoj poruci korisnik šalje EAP odgovor autentifikatoru u kojem se korisnik predstavlja autentifikatoru i određuje metodu autentifikacije. Treći korak autentifikacije je komunikacija između korisnika i autentifikatora pomoću Request/Response poruka koje ne moraju očekivati odgovor u određenom vremenu. Autentifikator nakon poslane poruke zahtjeva ne šalje novi zahtjev ukoliko nije dobio odgovor na prethodni. Ponovno slanje zahtjeva događa se samo ukoliko korisnik ne odgovara neko vrijeme autentifikatoru. Nakon ponovnog slanja zahtjeva u kojima korisnik ne odgovara,

autentifikator prekida postupak EAP autentifikacije s korisnikom. Zadnji korak autenfikacije događa se nakon uspješno primljenih zahtjeva i odgovora autentifikatora i korisnika. Ako u toj razmjeni autentifikator utvrdi da korisnik nije ispunio zahtjeve autentifikacije, on šalje poruku neuspjeha u suprotnom autentifikator usred ispunjenih zahtjeva autentifikacije šalje potvrdnu poruku uspjeha. Važno je napomenuti da se komunikacija između korisnika i autentifikatora u EAP metodi autentifikacije bežične lokalne mreže vrši pomoću EAPOL paketa. EAP paket enkapsulira se u EAPOL paket koji se prenosi korisniku te sadrži tri vrste poruka: Početak autentifikacije, Odjava korisnika s mreže te informacije o dijeljenju ključeva.

CARNet (2006) navodi sljedeće najčešće korištene EAP metode autentifikacije u poslovnim okruženjima kao i u okruženjima koja iziskuju visoku razinu zaštite:

- LEAP (eng. Lightweight EAP) metoda,
- EAP-TLS (eng. EAP Transport Layer Security) metoda,
- EAP-TTLS (eng. EAP-Tunnelled Transport Layer Seurity) metoda,
- PEAP (eng. Protected Extensible Authenthication Protocol) metoda,
- SPEKE (eng. Strong Password Exponential Key Exchange) metoda.

LEAP metoda autentifikacije koristi zaporku i korisničko ime kao način autentifikacije. Autentifikacija između korisnika i bežične pristupne mreže odvija se pomoću dijeljene tajne. Metoda sadrži i zaštitne ključeve kojima je svrha očuvanje integriteta komunikacije. U PEAP metodi zaštitni ključevi se mijenjaju tijekom svake novonastale komunikacije s bežičnom pristupnom točkom.

EAP-TLS metoda autentifikacije smatra se najsigurnijom metodom komunikacije koja radi na principu dodjele certifikata korisnicima koji pomoću javnog ključa (eng. *Public Key Infrastructure* - PKI) ključa osigurava komunikaciju korisnika i autentifikacijskog poslužitelja. Prednost ove metode je korištenje certifikata bez kojeg se korisnik ne može autentificirati na bežičnu mrežu čak i s odgovarajućom lozinkom i korisničkim imenom.

EAP-TTLS metoda nadograđuje EAP TLS metode gdje se prije dijeljenja korisničkog imena i lozinke uspostavlja siguran tunel pomoću certifikata poslužitelja kojeg korisnik ne mora posjedovati za autentifikaciju.

PEAP metoda koristi jednake mehanizme poput EAP-TLS i EAP-TTLS metoda autentifikacije gdje se uspostavlja sigurna komunikacija pomoću tunela. Razlika PEAP metode je u tome što prilikom PEAP autentifikacije PEAP ne zaštićuje sve podatke tijekom komunikacije poput korisničkog imena.

SPEKE metoda temeljena je na principu rada LEAP metode koja koristi korisničko ime i zaporku kao način autentifikacije s bežičnom mrežom. Razlika između ovih metoda autentifikacije je u dodatnoj sigurnosti koju SPEKE pruža pri komunikaciji. Izmjene poruka koje sadrže korisničko ime i lozinku gotovo je nemoguće uhvatiti jer poruke sadrže niz slučajnih brojeva koji mogu biti dešifrirani samo na strani korisnika i poslužitelja.

2.3.5. Načini penetracije WPA2 protokola

Postoje dva različita vektora napada na WPA2 protokol, prvi i stariji način penetracijskog napada na WPA2 protokol odvija se uz pomoć hvatanja dijelova četverostrukog rukovanja prilikom autentifikacije uređaja na bežičnu mrežu. Kao što je objašnjeno u odlomku 2.3.1 rada pri četverostrukim rukovanjem koji koristi glavni upareni ključ ili PMK ključ za komunikaciju. Slabost ove vrste autentifikacije je u PMK ključu iz kojeg se možemo vidjeti važne podatke poput lozinke SSID (eng. *Service Set Identifier*) identiteta bežične mreže, duljinu SSID vrijednosti, broj miješanja (hash) teksta i veličinu vrijednosti. Svi podaci vidljivi su prilikom hvatanja četverostrukog rukovanja korisnikova uređaja i pristupne točke. Kako bi otkrio lozinku bežične pristupne točke, napadač jednostavno može prisilno deautentificirati uređaj s mreže kako bi prilikom ponovnog spajanja uređaja mogao uhvatiti podatke četverostrukog rukovanja. Takve podatke koristi u napadu gdje pomoću rječnika traži moguće kombinacije lozinke. Takav napad sadrži mane gdje za hvatanje rukovanja na bežičnu mrežu mora biti povezan uređaj. Druga velika mana je izloženost napadača za vrijeme prisilnog deautentificiranja uređaja čime otkriva napad na bežičnu mreža koja koristi WPA2 protokol. (Kumkar, Tiwari, Tiwari, Gupta, Shrawne, 2012.)

Noviji način napada zaobilazi mane napada hvatanja četverostrukog rukovanja koristeći novu tehniku napada na RSN IE (eng. *Robust Security Network Information Element*) elementa unutar EAPOL okvira kako bi uhvatio PMKID PMK ključa koji se izračunava pomoću hash operacija. Napadač tako može izvršiti napad na bežičnu pristupnu točku bez deautentificiranja korisnika koji komunicira s bežičnom mrežom. PMKID vrijednost u sebi zapisuje vrijednosti PMK ključa, ime PMK ključa te MAC adrese pristupnog uređaja. Napadač jednostavno uhvati PMKID te na tu vrijednost primjenjuje kriptografsku hash funkciju za dobivanje spomenutih vrijednosti. („New attack on WPA/WPA2 using PMKID“ 2018.)

2.4. WPA3 Protokol

Kao odgovor na sigurnosne nedostatke WPA2 protokola krajem lipnja 2018. godine predstavljen je WPA3 protokol kao budući standard sigurnosne zaštite bežičnih lokalnih mreža. Cilj WPA3 protokola je poboljšati sigurnosnu zaštitu komunikacije između korisnika i pristupne točke i onemogućiti sve poznate napade na bežične mreže u bilo kojem trenutku. Da bi riješili većinu mogućih napada na bežičnu mrežu, WPA3 uvodi SAE (eng. *Simultaneous Authetication of Equals*) način autentifikacije. SAE algoritam koristi dijeljene lozinke za autentifikaciju umjesto PMK ključa čime tjera napadača na fizičku prisutnost napada na pristupne točke. Na takav način probijanje i jednostavne lozinke zahtjeva više vremena nego u prijašnjim napadima na WPA/WPA2 protokole. SAE autentifikacija odvija se pomoću nove vrste rukovanja između korisnika i bežične pristupne točke zvanog „dragonfly“ rukovanje. „Dragonfly“ način rukovanja onemogućuje napadačima izvanmrežni napad grubom silom (eng. *Brute Force*) na hash vrijednosti ključeva viđeni unutar WPA2 protokola. SAE ili „dragonfly“ rukovanje djeluje slično SPEKE načinu EAP autentifikacije koji pruža potpunu sigurnost i tajnost izmjene podataka. (Kohlios, Hayajneh 2018.)

2.5. Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup ili WPS je protokol osmišljen s ciljem brzog i olakšanog povezivanja korisnika s bežičnom pristupnom točkom. Klasična autentifikacija korisnika na bežičnu mrežu vrši se pomoću imena mreže ili SSID *(eng. Service Set Identifier)* i lozinke koristeći autentifikacijski protokol (WPS-PSK, WEP itd.), u WPS protokolu takva autentifikacija je pojednostavljena na pritisak jednog dugmeta ili upisa brojčanog koda. Postoje tri različita načina povezivanja na bežičnu mrežu pomoću WPS protokola:

1. Metoda pritiska WPS tipke na pristupnoj točki poznatija kao PBC *(eng. Push Button Connect)* u kojem korisnik mora pritisnuti tipku na pristupnoj točki ili uređaju s kojim se želi povezati na bežičnu mrežu. Tipka za povezivanje može biti u fizičkom obliku ili virtualna. Nakon pritiska tipke, pristupna točka otvara konekciju za autentifikaciju pomoću PBC-a sve dok ista ne bude uspješna u protivnom zatvara konekciju u vremenskom roku od dvije minute od prvotne interakcije.

2. Metoda autentifikacije pomoću osobnog identifikacijskog broja PIN *(eng. Personal Identification Number)* je autentifikacija u kojoj korisnik upisuje brojčani kod bežičnog adaptera uređaja u web sučelje pristupne točke. Brojčani kod može biti već unaprijed označen od strane proizvođača ili generiran od strane softvera.

3. Metoda autentifikacije pomoću PIN-a u kojem korisnik upisuje brojčani kod pristupne točke u zadani obrazac uređaja klijenta.

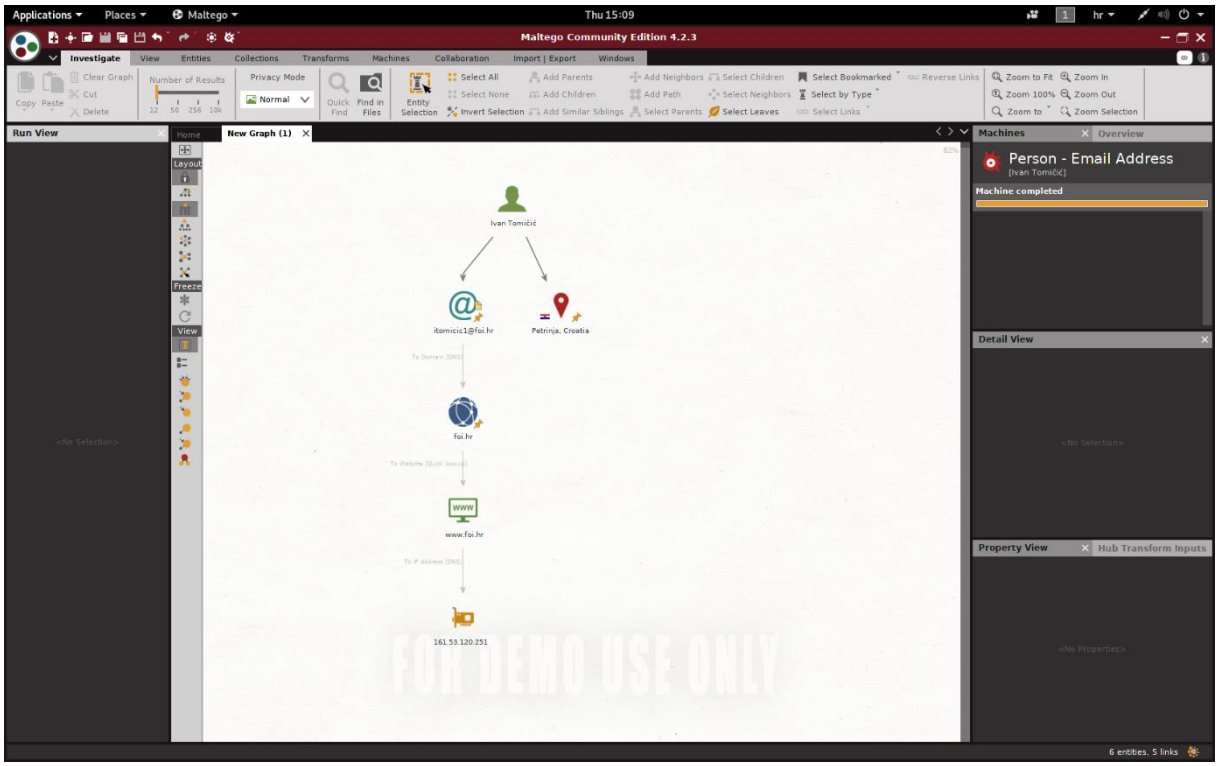
Iako osmišljen u svrhu brzog povezivanja, već u ranijoj fazi djelovanja protokol je sadržavao velike sigurnosne propuste gdje napadač koristeći WPS protokol lagano zaobilazi zaštitu WPA2 sigurnosnog protokola koristeći napad grubom silom na WPS PIN. Nakon 2011. godine većina proizvođača koristi PBC metodu uspostavljanja konekcije kako bi otklonili mogućnost napada na bežičnu mrežu pomoću WPS PIN metode autentifikacije korisnika s pristupnom točkom.

3. Vrste penetracijskih napada na lokalne bežične mreže

Proces penetracijskog napada na lokalnu bežičnu mrežu nužno ne započinje direktnim napadom na samu mrežu. Kako bi napad bio efektivan i uspješan u svakom pogledu, potrebno je poduzeti određene pripreme kao što je skupljanje informacija o meti napada. Informacije ne predstavljaju samo tehničke specifikacije poput modela usmjernika ili IP adrese *(eng. Internet Protocol address)* nad kojim se vrši napad, nego obuhvaćaju sveopće informacije poput navika vlasnika uređaja, njegovu informatičku pismenost i osobne podatke. Ovakve podatke moguće je dohvatiti koristeći dvije tehnike: socijalni inženjering i obrada otvorenih izvora (eng. Open-source intelligence – OSINT). Nakon prikupljanja informacija korištenjem određenih metoda napadač vrši penetracijski napad na određenu metu. Penetracijski napadi dijele se na aktivne i pasivne koji će biti pobliže opisani u sljedećim odlomcima.

3.1. Prikupljanje informacija

Prilikom aktivnog ili pasivnog penetracijskog napada, najvažnije je znati određene podatke o meti poput adrese elektroničke pošte ili datuma rođenje i slične osobne podatke koje napadač ne bi dobio direktno od svoje mete. Kako bi došao do takvih informacija, napadač može koristiti otvorene izvore ili skraćeno OSINT metode dobavljanja informacija. Takve informacije su javno dostupne na različitim medijima poput novina, javnih državnih registara i najvažnijeg medija Interneta. Koristeći razne OSINT programe korisnik preko Interneta može saznati sve informacije o osobi koju želi napasti. Napadnuta osoba je svjesno javno objavila svoje podatke na Internetu stoga dostupni podaci vidljivi su svim korisnicima Interneta. Ova metoda omogućuje napadaču da prikupi dodatne informacije o osobi koju napada kako bi odredio sve moguće vektore napada poput lažnog predstavljanja, kreiranja rječnika za Brute-force napad i slično. Primjer osnovnog OSINT istraživanja vidljiv je na slici 8.



Slika 8: Primjer osnovnog OSINT istraživanja u programu Maltego (autorski rad)

3.1.1. Socijalni inženjering

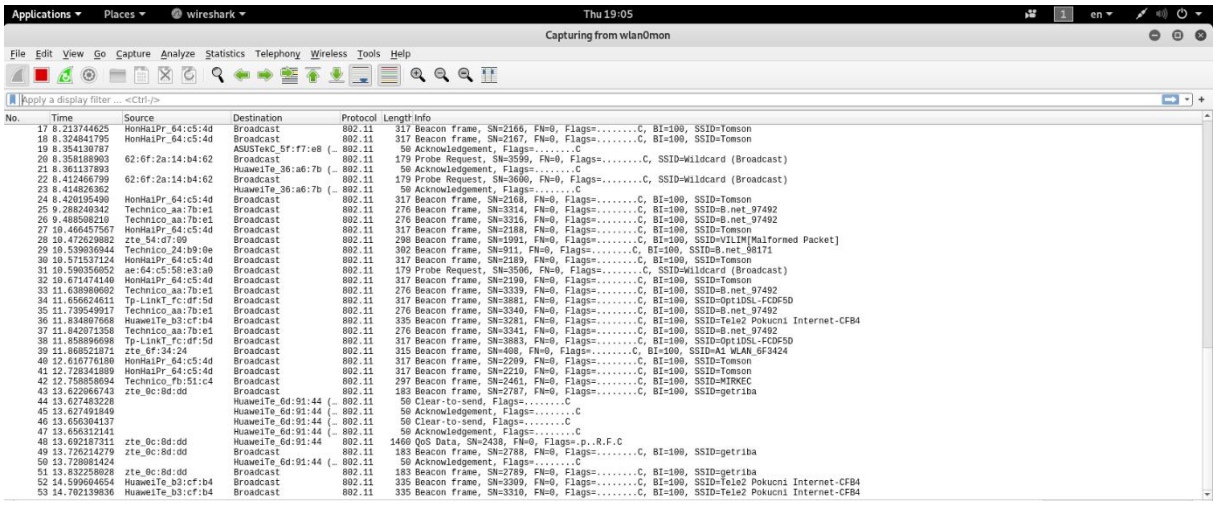
Socijalni inženjering obuhvaća niz različitih tehnika koje napadač može koristiti nad određenim pojedincem iskorištavanjem njegovih slabosti i ljudskih pogrešaka u svrhu dobivanja povjerljivih informacija ili dobivanja pristupa nad određenim resursima do kojih napadač ne može samostalno doći. Socijalni inženjering u informacijskoj sigurnosti koristi se primarno za probijanja sigurnosne zaštite postavljene od čovjeka. Čovjek kao biće je u informacijskoj sigurnosti najranjiviji dio zaštite i sigurnosti određenog sustava u informacijskoj tehnologiji. Socijalni inženjering vrši se u tri različita pristupa pojedincu: Lažno predstavljanje s pouzdanih izvora *(eng. Phishing)*, Lažno predstavljanje pomoću telefona *(eng. Vishing)* te fizičko predstavljanje korištenjem lažnog identiteta. Svrha svih pristupa je dobivanje osobnih informacija i korištenje lažnog utjecaja na pojedinca za pristup neovlaštenim podacima ili radnog mjesta. Svaka osoba emocionalno različito reagira na različite pojave ili događaje, stoga se je teško zaštiti od ovakvih načina prikupljanja informacija.(CERT.hr, bez dat.)

3.2. Pasivni penetracijski napadi na bežične mreže

Pasivni penetracijski napadi su napadi koji direktno ne utječu na rad mreže koje napadamo. Napadač tijekom pasivnog napada samo prikuplja podatke u mreži ne mijenjajući joj sadržaj i autentičnost. Tijekom pasivnog napada napadač dobiva informacije u uređajima, IP adresi, protokolima u korištenju lokaciji i ostalih parametara bežične mreže. Korištenjem pasivnog napada narušava se povjerljivost podataka tijekom izmjene informacija bežičnom mrežom, stoga je ovakve napade jako teško uočiti i spriječiti. Pod pasivne napade ubraja se metoda prisluškivanja bežične mreže te analiza i nadgledanje prometa podataka mreže. (Jawandhiya, Ghonge, Ali, Deshpande, 2010.)

3.2.1. Prisluškivanje

Najjednostavniji oblik pasivnog penetracijskog napada naziva se prisluškivanje. Napadač tijekom prisluškivanja može hvatati pakete unutar mreže ili izvan mreže. Pomoću prisluškivanja napadač može saznati informacije poput IP adrese, MAC adrese usmjerivača ili pristupne točke, enkripcije koju mreža koristi i slično. Prisluškivanje ne mijenja informacije koje se šalju između komunikacijskog kanala prisluškivanog uređaja i njegovog odredišta. Paketi poslani pomoću bežične mreže i dalje stižu na svoje odredište neizmijenjeni, samo se tijekom komunikacijskog kanala paketi hvataju pomoću mrežnog adaptera napadačevog uređaja. Primjer prisluškivanja paketa bežičnih mreža bez direktnog povezivanja na istu vidljiv je na slici 9.



Slika 9: Prikaz prisluškivanja paketa okolnih pristupnih točaka pomoću Wiresharka (autorski rad)

3.2.2. Analiza i nadgledanje prometa podataka mreže

Analiza i nadgledanje prometa podataka podrazumijeva detaljno iščitavanje uhvaćenih paketa pomoću metode prisluškivanja gdje se uhvaćeni paketi detaljno ispituju kako bi napadač saznao primjerice odredište i izvorište uhvaćenog paketa, vrstu paketa u koji može sadržavati osobne podatke poput lozinki, korisničkih imena i slično. Iako današnji protokoli znatno otežavaju dohvaćanja takvih podataka u kombinaciji s aktivnim penetracijskim napadima, napadač može nesvjesno „natjerati“ korisnika da se izmjena komunikacije vrši preko protokola sa slabom sigurnošću.

3.3. Aktivni penetracijski napadi na bežične lokalne mreže

Aktivni penetracijski napadi na bežične lokalne mreže definirani su kao pokušaji napada koji svojim djelovanjem direktno utječu na tok podataka unutar komunikacijskog kanala. Podaci tijekom aktivnog penetracijskog napada bivaju izmijenjeni ili uništeni od strane napadača. Ovakvi napadi izvršavaju se na gotovo sve slojeve OSI modela arhitektura mreža te tako narušava integritet i raspoloživost podataka. Aktivni napadi prema strukturi podijeljeni su na unutarnje i vanjske napade. Unutarnji napadi su oni napadi koji se izvršavaju unutar same strukture i arhitekture mreže. Napadač za takvu vrstu napada koristi resurse poput računala, usmjernika, prespojnika i ostalih mrežnih uređaja koji čine arhitekturu napadnute mreže. Unutarnje penetracijske napade teško je prepoznati upravo zbog napada koji se odvija s uređaja koji pripada mreži. Za razliku od unutarnjeg napada, vanjski napad događa se uz pomoć uređaja izvan strukture napadnute mreže koji zahtjeva pristup mreži pomoću podataka za prijavu u sustav. Posljedice aktivnog penetracijskog napada obuhvaćaju oštećenje napadnutog sustava i ometani rad usluga unutar sustava. Postoji velik broj metoda aktivnog penetracijskog napada na mrežu, a neke od najpoznatijih metoda korištenih u penetracijskom napadu na lokalne bežične mreže biti će objašnjenje u sljedećim odlomcima.(Jawandhiya, Ghonge, Ali, Deshpande, 2010.)

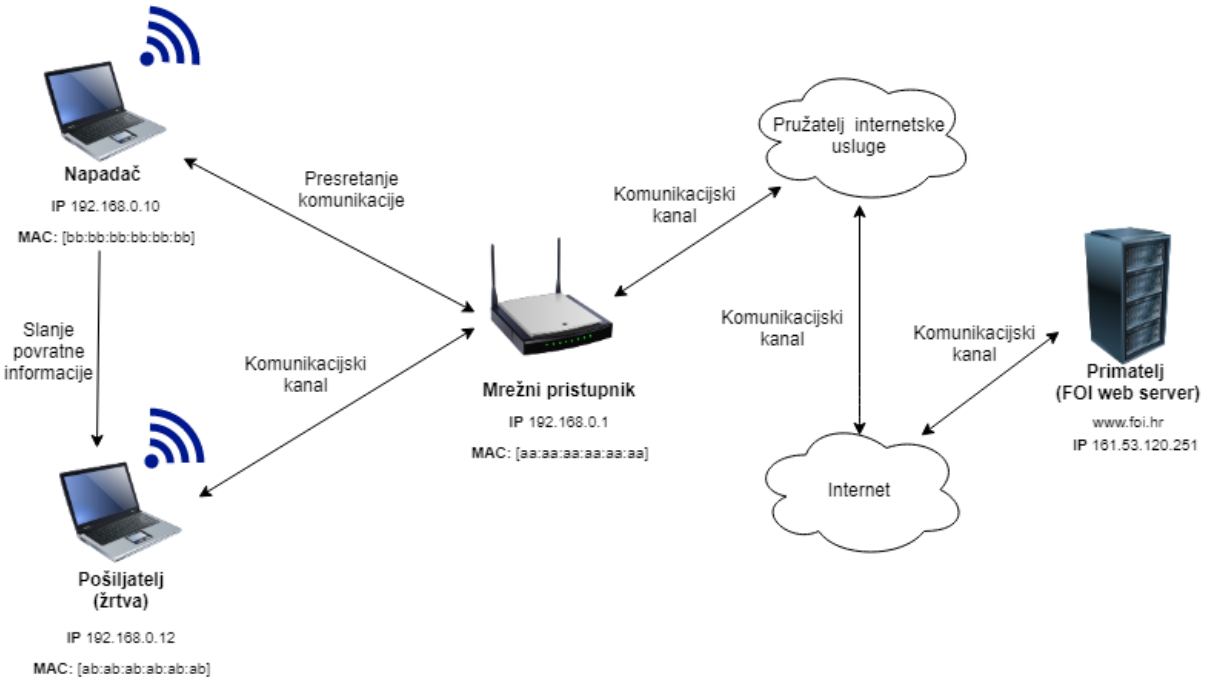
3.3.1. Lažno predstavljanje

Lažno predstavljanje poznato u terminologiji kao i „Spoofing“ predstavlja metodu aktivnog penetracijskog napada u kojem se napadač predstavlja kao neka druga osoba ili uređaj u mreži koju želi napasti s ciljem primanja podataka koje su namijenjeni osobi za koju se napadač lažno predstavlja. Pri penetracijskom napadu na bežične mreže napadač prvotno lažira IP i MAC adrese dobivene pasivnim izviđanjem žrtve kako bi ih modificirao i maskirao u lažni uređaj. S obzirom da u bežičnim mrežama postoje sigurnosni 802.11 protokoli, oni mogu samo zaštiti integritet podataka poslanih zrakom ali ne mogu provjeriti identitet MAC adrese

pošiljatelja. Metode lažnog predstavljanja stoga čine početni korak pri penetracijskom napadu na lokalne bežične mreže te su dio složenijih napada na mreže. Osim lažnog predstavljanja pomoću IP i MAC adrese, napadač može maskirati ostale protokole slojeva OSI modela poput domenskog sustava *imena (eng. Domain Name System – DNS)*, adresnog rezolucijskog protokola *(eng. Address Resolution Protocol- ARP)*, protokola za kontrolu prijenosa podataka *(eng. Transmission Control Protocol – TCP)* te datagram protokol korisnika *(eng. User Datagram Protocol-UDP)*.

3.3.2. Preusmjeravanje i izmjena komunikacije unutar mreže

Preusmjeravanje komunikacije paketa unutar mreže poznat kao i napad „Čovjek u sredini“ *(eng. Man in The Middle – MiTM)* je aktivni napad u kojem se napadač unutar mreže stavlja u „sredinu“ komunikacije između pošiljatelja to jest napadnutog računala i primatelja s ciljem presretanja paketa poslanih od strane žrtve. Ova metoda radi na principu da napadač već ima pristup bežičnoj ili žičanoj Ethernet konekciji. Shematski prikaz napada unutar bežične mreže vidljiv je na slici 10.



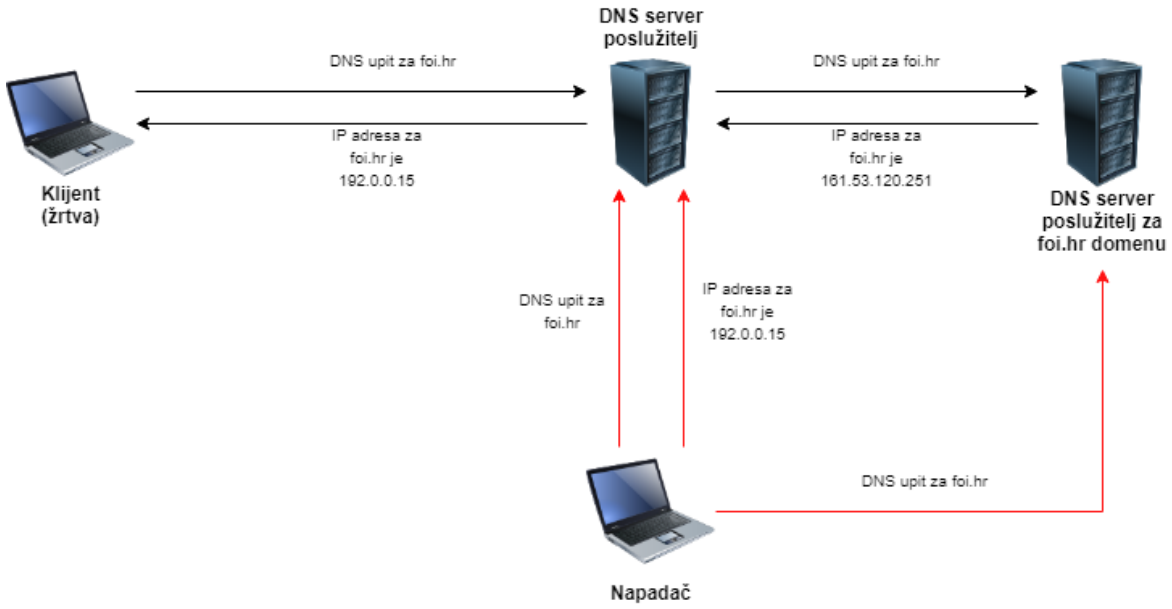
Slika 10: shematski prikaz napada „Čovjek u sredini“ (autorski rad)

Na slici 10 vidljiv je prikaz penetracijskog napada MiTM na lokalnu bežičnu mrežu. Kako bi uspješno napravio penetracijski napad, napadač prvo mora biti spojen na mrežu koju napada. Kada je spojen na mrežu, napadač vrši ARP trovanje *(eng. ARP Poisoning)* nad mrežnim pristupnikom na kojem je spojen. ARP trovanje podrazumijeva napad na ARP protokol koji sadrži manu nedovoljnog provjeravanja primljenih ARP poruka. ARP protokol

nema definiran način provjere valjanosti ARP poruka u komunikaciji. Napadač tu manu može iskoristiti tako da izmjeni sadržaj ARP poruke te takvu poruku pošalje žrtvi to jest napadnutom računalu. Napadnuto računalo ne može provjeriti integritet poruke stoga tu ARP poruku prihvaća kao istinitu. Korak prije ARP trovanja može činiti metoda lažnog predstavljanja kako bi napadač zavarao mrežnog pristupnika da je on jedan od uređaja s kojim pristupnik mora komunicirati. Nakon što napadač izvrši ARP trovanje nad mrežnim pristupnikom, on trenutno preusmjerava svu komunikaciju koju žrtva pošalje do mrežnog pristupnika. Pretpostavimo da žrtva želi pristupiti FOI web serveru na Internetu. Žrtva ili pošiljatelj prvo šalje zahtjev mrežnom pristupniku (u ovom slučaju bežičnom usmjerniku) za dohvaćanje adrese FOI web stranice. Umjesto da pristupnik preusmjeri zahtjev direktno prema web serveru FOI stranice, on poruku preusmjerava napadaču. Napadač sada ima informaciju o zahtjevu informacija o pristupu FOI web stranici. Napadač u tom trenutku poruku može izmijeniti, uništiti ili samo proslijediti ovisno o napadu kojeg želi izvršiti. Komunikacijski kanal se vraća od napadača pristupniku koji tu poruku dalje prosljeđuje sve do FOI web servera. Žrtva kao odgovor dobiva odgovor od web servera koji je poslan od strane napadača te ga tretira kao valjanog odgovora. Ovim pristupom presretanja poruka napadač može izvoditi napade uskraćivanja usluga, čitati ili izmjenjivati podatke koje žrtva proslijedi pristupniku.

3.3.3. Slanje lažnih poruka

Slanje lažnih poruka naziva se još i trovanje DNS priručne memorije *(eng. DNS cache poisoning)* djeluje slično MiTM napadu gdje je cilj zavarati žrtvino računalo da je dobiven odgovor poslanog zahtjeva legitiman i originalan te ga spremiti u priručnu memoriju. Princip djelovanja slanja lažnih poruka zasniva se na slanju lažnog DNS odgovora koji će žrtvino računalo pročitati kao valjan DNS odgovor poslužitelja. Prednost ovakvog načina slanja lažnih poruka je u tome što napadač ne mora biti direktno spojen na lokalnu bežičnu mrežu da bi izveo napad. Napadanje priručne memorije DNS poslužitelja omogućuje napadaču širenje lažnih poruka svim računalima što su poslali DNS upit za napadnuti DNS poslužitelj. Napadač može postaviti lažnu IP adresu na DNS poslužitelj čime omogućuje izvršavanje različitih napada na žrtve poput prisluškivanja, izmjena komunikacije, postavljanje stražnjih *ulaza (eng. Backdoor)* na žrtve i slične napade. („Centar informacijske sigurnosti [CIS], 2011.) Pojednostavljeni prikaz trovanja DNS priručne memorije vidljiv je na slici 11.



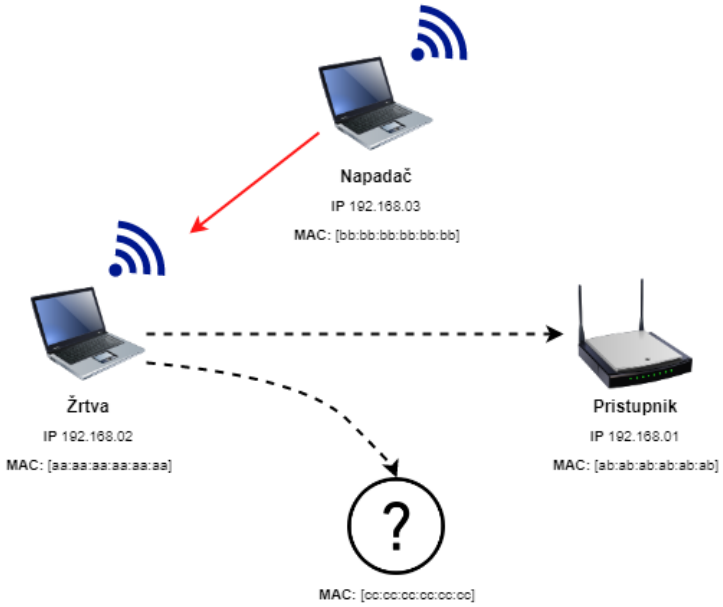
Slika 11: Primjer trovanja DNS priručne memorije (autorski rad)

Prema slici 11 vidljivo je da na DNS upit klijenta za IP adresom web stranice foi.hr DNS poslužitelj nema u priručnoj memoriji zapisanu IP adresu za traženu web stranicu, stoga prosljeđuje zahtjev sljedećim autoritativnim DNS poslužiteljima. Za vrijeme slanja DNS upita sljedećim DNS poslužiteljima, napadač vrši trovanje DNS poslužitelja tako da na početku šalje upit za web stranicu foi.hr i nakon toga u priručnu memoriju smjesti lažnu IP adresu za web stranicu foi.hr. Cilj napadača je poslati zahtjev za IP adresom prije stvarnog odgovora autoritativnog DNS poslužitelja, a to radi na način tako da napadač šalje jako velik broj DNS upita *(eng. DNS flooding)* prema autoritativnom DNS poslužitelju kako bi ga držao „zaposlenog“ u obradi svih upita. Kada klijent zatraži DNS upit za stranicu foi.hr DNS poslužitelj mu vraća odgovor s IP adresom koju je postavio napadač. Žrtvino računalo takav zahtjev prihvaća kao legitiman DNS odgovor i IP adresu zapisuje u svoju DNS priručnu memoriju.

3.3.4. Prekidanje usluga

Napad prekidanja usluga poznat u informacijskoj sigurnost još kao i napad uskraćivanja usluga *(eng. Denial od Service- DoS)* obilježava napad u kojem napadač sprječava komunikaciju žrtve s drugim uređajima ili pristupnika. DoS napadi dijele se na tri osnovne skupine: napad iskorištavanja ranjivosti, napad poplavljivanja *(eng. Flooding)* te lokalni DoS napad. Napad iskorištavanja ranjivosti *(eng. Vulnerability attack)* oblik je napada u kojem napadač pronalazi manu ili ranjivost u aplikacijskom sloju programa ili softvera koji mu omogućuje da dovede cijeli sustav u stanje prekidanja davanja usluga. Flooding napad bazira se na slanje velikog broja poruka prema sustavu s ciljem da ga opterete i zauzmu njegove

kritične resurse poput memorije, mrežni protok i sličnih resursa. Da bi takav DoS napad bio efektivan, napadač mora slati veći broj poruka nego što ga pristupnik može obraditi stoga ovakva vrsta napada zahtjeva veći broj napadačkih računala usmjerena prema žrtvi. U ovakvom napadu korištenje tuđih računala pod napadačevom kontrolom *(eng. Botnet)* naziva se još i distribuirani napad uskraćivanjem sigurnosti *(eng. Distributed Denial of Service – DDoS)*. Posljednja skupina napada uskraćivanja usluga je lokalni DoS napad. Lokalni DoS napad zasniva se na trovanju ARP protokola gdje će napadnuto računalo biti onemogućeno komunicirati s vanjskim Internetom te napad deautentifikacije bežičnih uređaja. Prikaz DoS napada pomoću ARP trovanja vidljiv je na slici 12.



Slika 12: Prikaz lokalnog DoS napada. Vlastita izrada prema: („CIS“, 2011.)

Slika 12 prikazuje lokalni DoS napad koji započinje tako da napadač šalje napadnutom računalu ARP odgovore u kojima se predstavlja kao pristupnik s IP adresom od 192.168.0.1 i lažnom MAC adresom od cc:cc:cc:cc:cc:cc . Žrtvino računalo ne može provjeriti da li je poslana poruka lažna stoga svaku takvu poruku tretira kao istinitu te zapisuje par adresa u svoju ARP tablicu. Kada žrtvino računalo želi komunicirati s bilo kojim uređajem izvan svoje lokalne mreže, paketi poslani prema pristupniku neće biti dostavljeni na željenu destinaciju. Paketi će biti odbačeni onoliko dugo sve dok žrtvino računalo ima lažnu MAC adresu pristupnika. („CIS“,2011.; „DoS napadi“, bez dat.)

4. Alati potrebni za penetracijsko testiranje

Kako bi se penetracijsko testiranje moglo uspješno sprovesti, potrebno je koristiti razne alate stvorene posebno za izvođenje penetracijskog testiranja. Postoji širok spektar alata dizajniranih za različite upotrebe u penetracijskom testiranju. Većina alata dizajnirana je za Linux operacijske sustave upravo zbog visoke razine sigurnosti koju Linux pruža nasuprot konkurentog Windows OS-a. Penetracijski programi u Linuxu najčešće su napisani Python programskim jezikom koji imaju mogućnost iskorištavati slabosti i mane unutar različitih sustava i softvera. Pri penetracijskom testiranju lokalnih bežičnih mreža postoji velik broj penetracijskih alata, a neki od najvažnijih biti će spomenuti u sljedećim odlomcima.

4.1. Paket alata Aircrack-ng

Aircrack-ng naziv je za skup besplatnih alata koji se koriste pri penetracijskom testiranju bežičnih mreža u mrežnoj sigurnosti. Skup alata primarno je zamišljen za Linux OS ali kompatibilan je i s ostalim operacijskim sustavima. Aircrack-ng službeno je predstavljen 2006. godine kao sljedeća generacija alata za penetracijsko testiranje bežičnih mreža. Prema aircrack-ng.org glavna područja mrežne sigurnosti na koje se Aircrack-ng orijentira su:

- Nadgledanje koje se sastoji od hvatanja paketa i izvoza uhvaćenih podataka u tekstualnu datoteku dostupnu za sve ostale penetracijske alate.
- Napadanje deautentifikacijom, kreiranje lažnih pristupnih točki, injekcija paketa i slično.
- Testiranje mogućnosti WiFi adaptera i upravljačkih programa za hvatanje i injekciju paketa.
- Penetracijsko probijanje WEP i WPA PSK/WPA2 sigurnosnih protokola.

Aircrack-ng čini paket alata s 18 različitih programa za penetracijsko testiranje bežičnih mreža. Neki od najvažnijih su:

- Airmon-ng – Osnovni alat koji omogućuje upravljanje načina rada bežičnog adaptera u modu za nadgledanje *(eng. Monitor mode)* ili upravljački način rada *(eng. Managed mode)*. Program također nudi izbor sučelja rada bežičnog adaptera te pronalazak programa koji ometaju rad istog.
- Airodump-ng – Alat koji se koristi u svrhu hvatanja paketa bežičnih 802.11 mreža. Alat je zamišljen u svrhu izviđanja lokalnih bežičnih mreža hvatajući pakete koje emitiraju pristupne točke. Pomoću ovog alata napadač može saznati informacije poput MAC adrese pristupne točke, kanal na kojem se odašilje signal, jakost signala bežične mreže, broj uhvaćenih paketa, način sigurnosne enkripcije, naziv pristupne točke te

način autentifikacije. Uz navedene informacije o pristupnim točkama, napadač može vidjeti i MAC adrese povezanih uređaja unutar uhvaćenih pristupnih točaka.

- Aireplay-ng – Alat potreban za izvršavanje napada deautentifikacije, lažnih autentifikacija te injektiranja modificiranih ARP zahtjeva prema bežičnoj pristupnoj točki.
- Aircrack-ng – Alat za penetracijski proboj WEP i WPA/WPA2-PSK ključeva. Pri napadu na WEP protokol aircrack-ng koristi PTW metodu napada dok za WPA i WPA2 protokole koristi metodu napada rječnikom na uhvaćene pakete četverostrukog rukovanja.
- Besside-ng – Automatizirani alat za penetracijski napad WEP i WPA protokola s mogućnošću automatskog probijanja zaštite WEP protokola u radijusu djelovanja bežičnog adaptera. Alat sadrži mogućnost spremanja podataka o WPA rukovanju.

4.2. Nmap alat za mapiranje mreže

Network Mapper ili Nmap je besplatni softver otvorenog koda koji se koristi u mrežnoj sigurnosti i istraživanju mreža. Nmap je osmišljen kako bi prvotno bio koristan sistemskim administratorima u obavljanju zadataka održavanja i praćenja mrežnih uređaja i mrežnog usmjeravanja. Nmap se također može koristiti pri penetracijskom testiranju mreža pomoću kojeg napadač može skenirati više broj mreža ili samo jedan uređaj unutar mreže. Princip rada nmap-a zasniva se na korištenju neobrađenih IP paketa pomoću kojih može otkriti dostupnost uređaja unutar mreže i sve informacije koje se nalaze u uhvaćenih paketima poput operacijskog sustava koji koristi, vrste pružanja usluge, vrste vatrozida *(eng. Firewall)* i desetak ostalih karakteristika. U penetracijskom testiranju nmap se najčešće koristi za otkrivanje portova unutar uhvaćenih uređaja na mreži. Prilikom pretraživanja nmap izbacuje listu portova koja sadrži broj porta, ime usluge i njegov status pomoću kojih napadač određuje smjer budućeg napada. Alat ima mogućnost skeniranja portova unutar TCP, UDP, SCTP *(eng. Stream Control Transmission Protocol)* i ICMP *(eng. Internet Control Message Protocol)* protokola. („Chapter 15. Nmap Reference Guide“, bez dat.)

Uz ključnu značajku otkrivanja portova nmap pruža ostale mogućnosti poput:

- Mapiranje mreže pri kojem nmap može otkriti povezane uređaje na mreži, koji mogu biti serveri, usmjerivači, mrežnog preklopnika, te odrediti način njihovog fizičkog povezivanja.
- Otkrivanje Operacijskih sustava koji upravljaju povezanim uređajima u mreži s ciljem pružanja informacija poput imena proizvođača, verziju operativnog sustava te aktivno vrijeme rada sustava.

- Otkrivanje usluga koje podrazumijevaju otkrivanje web servera, servera elektroničke pošte i drugih te aplikacije i verzije softvera koji koriste serveri.
- Mrežne sigurnosti sustava gdje skeniranjem različitih informacija poput portova i aktivnih usluga omogućuje sistemskom administratoru prikaz stanja cijelog mrežnog sustava i detaljne informacije o najranjivijoj točki sustava. S takvom informacijom administrator može brzo locirati i pokrpati ranjivosti unutar sustava. Prednost korištenja nmap softvera je automatizacija pozivajućih funkcija programa.

4.3. Alat za penetracijsko testiranje Bettercap

Bettercap je alat za penetracijsko testiranje čiju primjenu najčešće koristimo u mrežnoj sigurnosti za otkrivanje ili testiranje slabosti mreža. Prednost Bettercapa je ujedinjavanje mogućnosti rada više alata u jedan univerzalan alat koji nudi rad s bežičnim mrežama, Bluetooth uređajima, niskoenergetskim uređajima te Ethernet mrežama.

Prema bettercap.org glavne značajke alata čine:

- Skeniranje bežičnih mreža te izvršavanje različitih napada poput deautentifikacije uređaja, PMKID napad te automatsko dohvaćanje WPA/WPA2 paketa četverostrukog rukovanja.
- Skeniranje Bluetooth niskoenergetskih uređaja s pripadajućim informacijama o uređaju.
- ARP, DNS i DHCPv6 *(eng. Dynamic Host Configuration Protocol version 6)* krivotvorenje za napade „Čovjek u sredini“.
- Proxy poslužitelj za pakete pomoću TCP, HTTP *(eng. HyperText Transfer Protocol)* i HTTPS *(eng. HyperText Transfer Protocol Secure)* protokola uz pomoć javascript dodataka.
- Prikupljanje informacija o mrežama i podataka za online prijavu koristeći MiTM napade.
- Skeniranje 2.4 GHz bežične mreže s ciljem preotimanja rada miša *(eng. MouseJacking).*

4.4. Alat za penetracijsko testiranje MANA Toolkit

Alat MANA Toolkit pripada skupini alata za napade simuliranja različitih servisa s ciljem zaobilaženja određene sigurnosne značajke sustava koju napadač napada, poznat u mrežnoj sigurnosti pod nazivom *HoneyPot*. MANA Toolkit alat zamišljen je u svrhu napada na bežične lokalne mreže uz pomoć lažne divlje pristupne točke *(eng. Rogue Access Point)* ili kreiranja napada „Zli Blizanac“ *(eng. Evil Twin Attack)*. Alat nudi postavke implementacije MiTM napada s alatom „Bettercap“. Uz postavke za kreiranje lažnih pristupnih točaka, MANA Toolkit nudi mogućnost degradiranja SSL-a *(eng. Secure Socket Layer)* ili skidanja HSTS *(eng. HTTP Strict Transport Security)* zaštite, razbijanje EAP autentifikacije i mogućnost spremanja podataka u različitim formatima za ostale penetracijske programe. (The MANA Toolkit, bez dat.)

4.5. Alat za penetracijsko testiranje Pixiewps

Pixiewps je alat za penetracijsko testiranje WPS protokola s ciljem dobivanja WPS PIN-a. Pixiewps vrši napad grubom silom na WPS protokole pristupnih točki pomoću metode napada vilinske prašine *(eng. Pixie dust)*. Prilikom napada na WPS protokol napadač ne mora biti spojen na Internet. U usporedbi s konkurencijskim programima, prednost Pixiewps-a je u brzini otkrivanja PIN-a od nekoliko sekundi do nekoliko minuta ovisno o uređaju i ranjivosti. Napad ovim alatom jedino je uspješan ukoliko korisnik ne koristi metodu WPS povezivanja pomoću tipke. Uz probijanje WPS zaštite, Pixiewps nudi hvatanje svih poruka unutar četverostrukog rukovanja pristupne točke i napadača.(Pixiewps, bez dat.)

4.6. Alat za probijanje zaporaka Hashcat

Hashcat, spada u jednih od najboljih alata za probijanje i otkrivanje zaporki. Alat se prvenstveno koristi za penetracijski napad svih vrsta enkriptiranih podataka. Hashcat koristi razne vrste dekripcijskih metoda kako bi u što bržem vremenu otkrio i probio bilo koju lozinku ili enkriptirani sadržaj. Hashcat dekriptira sadržaj u dva različita načina rada, enkriptiranje pomoću centralne procesorske jedinice *(eng. Central Processing Unit – CPU)* ili pomoću grafičke procesorske jedinice *(eng. Graphical Processing Unit- GPU)*. Brzina probijanja enkripcija ili zaporki ovisi o načinu rada alata i načinu napada kojeg napadač vrši. Danas se najčešće koristi snaga grafičkih kartica u probijanju enkripcija. U usporedbi s CPU načinom, GPU način dekripcije nudi veću brzinu izvedenih komputacija po sekundi *(eng. Hash rate)* nego procesorski način rada. (Hashcat, bez dat.)

Postoje nekoliko načina napada unutar Hashcat programa:

- Napad rječnikom jedna je od najčešćih napada na WPA i WPA2 autentifikacije zbog jednostavnosti i brzine pronalaženja potrebne autorizacije za prijavu na bežičnu mrežu. Napadač može kreirati ili koristiti već dostupne rječnike koje sadrže riječi ili fraze koje se koriste pri autorizaciji bežičnih mreža. Hashcat provjerava uhvaćeni hash sa svakom riječju u rječniku. Rječnik može sadržavati nekoliko riječi ili nekoliko stotina tisuća riječi.
- Napad grubom silom u kojem Hashcat provjerava sve moguće kombinacije slova i brojeva. Uz brojeve i slova pri otkrivanju lozinke mogu se koristit i posebni znakovi poput razmaka, točke i ostalih znakova. Ovaj napad iziskuje veliku procesorsku i grafičko-procesorsku snagu čija duljina enkripcije ovisi o veličini lozinke i složenosti tražene fraze. Napad grubom silom iziskuje puno vremena koje može varirati od nekoliko sati do nekoliko mjeseci ovisno o složenosti lozinke. Ovakva vrsta napada kombinira se s socijalnih inženjeringom gdje napadač zna dio fraze ili određene kombinacije slova koje koristi pri enkripciji.
- Kombinirani napad je napad u kojem se koristi kombinacija rječnika i napada grubom silom. Takav postupak je dugotrajan i rijetko korišten u praktičnoj upotrebi.
- Maskirani napad naziv je za napad sličan napadu grubom silom, ali u ovom napadu za vrijeme enkripcije koriste se samo određena slova abecede dobivena pomoću socijalnog inženjeringa koja predstavljaju sve moguće permutacije pri enkripciji. Ovakva vrsta napada je brža od napada grubom silom, ali iziskuje točnost odabira slova pri enkripciji.
- Napad uz zadana pravila predstavlja način napada u kojem napadač može odabrati različita pravila prilikom dekriptiranja lozinke poput korištenja velikih slova, dupliciranja određenih znakova, memoriziranja znakova i sličnih funkcija.

5. Praktični primjeri penetracijskog napada

U sljedećim odlomcima prikazati ćemo nekoliko najčešćih praktičnih načina penetracijskih napada na lokalne bežične mreže te postupke napada zajedno s objašnjenjima funkcija koristenih u istim. Praktični dio prikazuje koji je softver i hardver potrebno koristiti, različite napade na protokole bežične mreže, napade unutar same mreže te nekih od napada korištenih u metodi socijalnog inženjeringa. U praktičnom prikazu penetracijskog testiranja koristit će se dva različita usmjernika. Jedan usmjernik će simulirati WEP protokol bežične mreže te on neće imati internetsku vezu. Drugi usmjernik s internetskom vezom simulirati će WPA/WPA2 protokole bežične mreže. Svi operacijski sustavi korišteni u praktičnim primjerima biti će postavljeni u virtualnoj mašini pomoću VirtualBox softvera.

5.1. Potreban hardver i softver za penetracijski napad

Kako bi uopće penetracijsko testiranje moglo biti izvršeno, potrebno je posjedovati nekoliko hardverskih uređaja i softverskih programa specifično dizajniranih za penetracijska testiranja u mrežnoj sigurnosti. Pri penetracijskom testiranju najčešće se koriste različite Linux distribucije operacijskog sustava koji omogućuju instaliranje i korištenje potrebnih penetracijskih alata. U praktičnom radu penetracijskog testiranja korišten je Linux OS s Kali distribucijom verzije 5.4.0 zbog već unaprijed instaliranih alata korištenih u testiranju. Moguće je koristit ostale Linux distribucije poput BackBoxa, Parrot OS-a, BlackArcha, Pentoo Linuxa i sličnih distribucija specifično dizajniranih za penetracijsko testiranje mreža. Hardver potreban za testiranje bežičnih mreža podrazumijeva korištenje bežičnih adaptera koji imaju mogućnost injektiranja paketa i nadgledanja prometa. U praktičnom radu korišteni su dva različita adaptera, TP-Link TL-WN722Nv2 i ALFA AWUS036NHA adapter (Slika 13). Važno je napomenuti da samo određeni adapteri imaju mogućnost injektiranja paketa i nadgledanja prometa s određenim čipsetom. Najpopularniji čipseti korišteni u penetracijskim testiranjima su Atheros AR9271, Realtek RTL8812AU i Ralink RT3070.

Slika 13: Mrežni adapteri korišteni u praktičnom dijelu penetracijskog testiranja (autorski rad)

5.2. Postavljanje mrežnog adaptera za penetracijsko testiranje

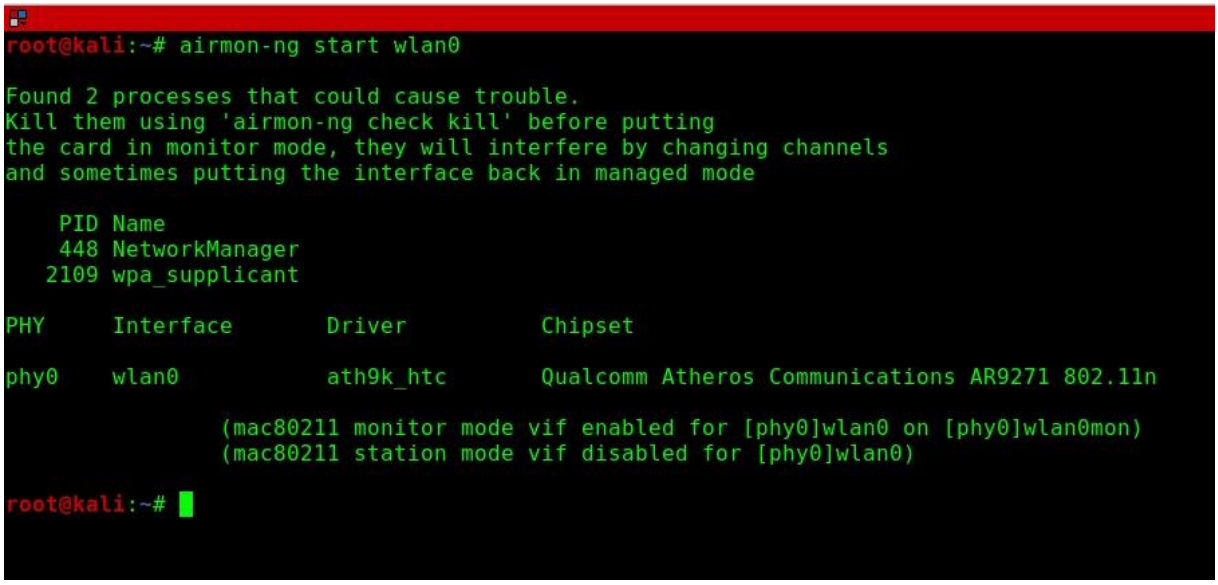
Kako bi izvršili penetracijski napad na WEP protokol lokalne bežične mreže i općenito na bežične mreže potrebno je obaviti nekoliko koraka pripreme koji obuhvaćaju uspostavljanje mrežnog adaptera u način nadgledanja te, kako bi praktičan primjer bio stvaran, maskirati i lažirati MAC adresu mrežnog adaptera.

Prvi korak predstavlja lažiranje MAC adrese mrežnog adaptera. U terminal Kali Linuxa upisuje se naredba za gašenje mrežnog adaptera *ifconfig wlan0 down*. Ifconfig predstavlja naredbu konfiguracije mrežnih prilagodnika, dok wlan0 predstavlja naziv mrežnog adaptera, a s argumentom down onemogućuje se rad mrežnog adaptera. Nakon toga u terminal upisujemo naredbu za promjenu MAC adrese – *macchanger -r wlan0* (Slika 14)

Slika 14: Promjena MAC adrese mrežnog adaptera (autorski rad)

Na slici 14. vidimo promjenu originalne MAC adrese 00:C0:CA:98:9C:E9 u novu adresu 66:C2:1B:18:C3:DE. U naredbi argument -r predstavlja slučajnu kombinaciju MAC adrese dok wlan0 predstavlja mrežni adapter. Moguće je koristiti i argument -m kojom možemo samostalno napisati novu željenu MAC adresu adaptera.

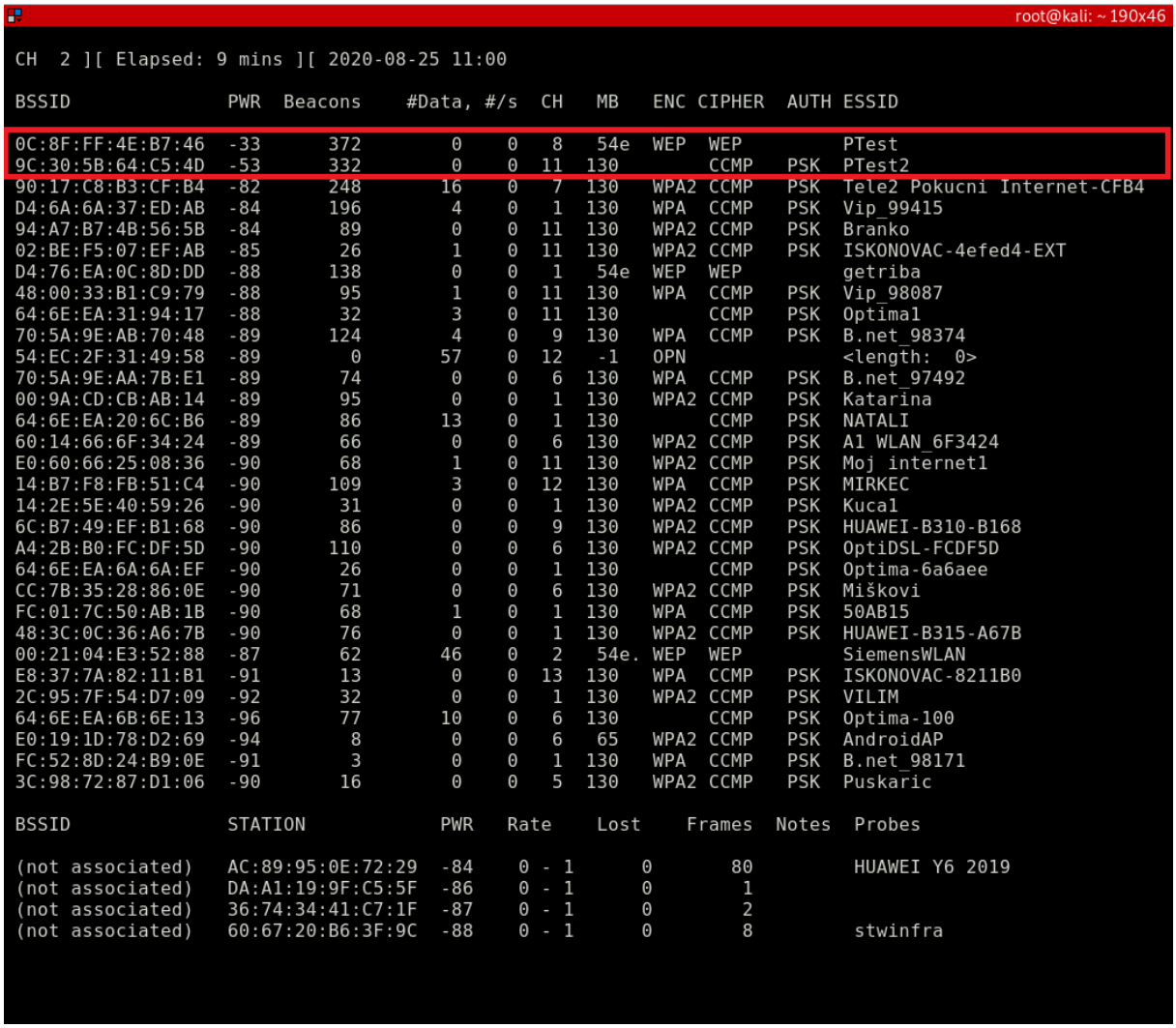
Sljedeći korak je pokretanje načina za nadziranje *(eng. Monitor mode)* mrežnog adaptera. Pokretanje načina za nadziranje vrši se pomoću naredbe *airmon-ng start wlan0* alata aircrack-ng. (Slika 15). Nakon uspješnog postavljanja mrežnog adaptera u način za nadziranje, ime adaptera se mijenja u wlan0mon te smo spremni izvršavati penetracijsko testiranje lokalne bežične mreže.



Slika 15: Pokretanje načina za nadziranje mrežnog adaptera (autorski rad)

5.3. Penetracijsko testiranje WEP protokola bežične mreže

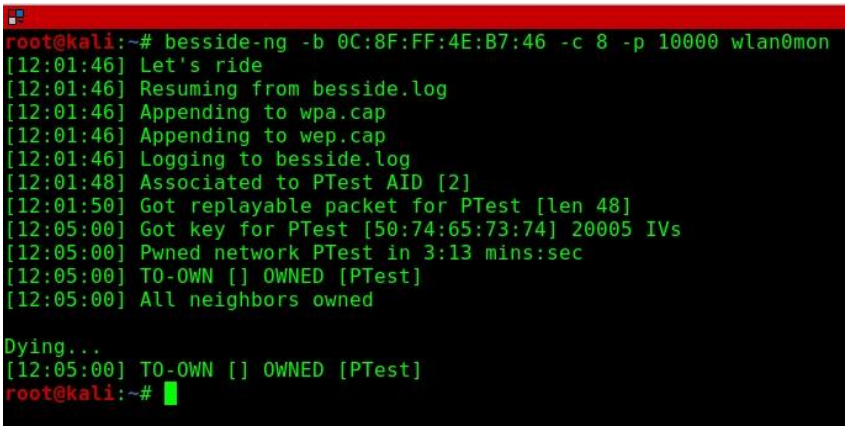
Prvi korak pri penetracijskom testiranju WEP protokola je odabir mreže koju želimo testirati. Kako bismo dobili informacije o željenoj mreži potrebno je provesti skeniranje i snimanje lokalnih bežičnih mreža. Za skeniranje i snimanje lokalnih bežičnih mreža koristimo naredbu *airodump-ng wlan0mon*. (Slika 16)



Slika 16: Skeniranje lokalnih bežičnih mreža pomoću airodump-ng alata (autorski rad)

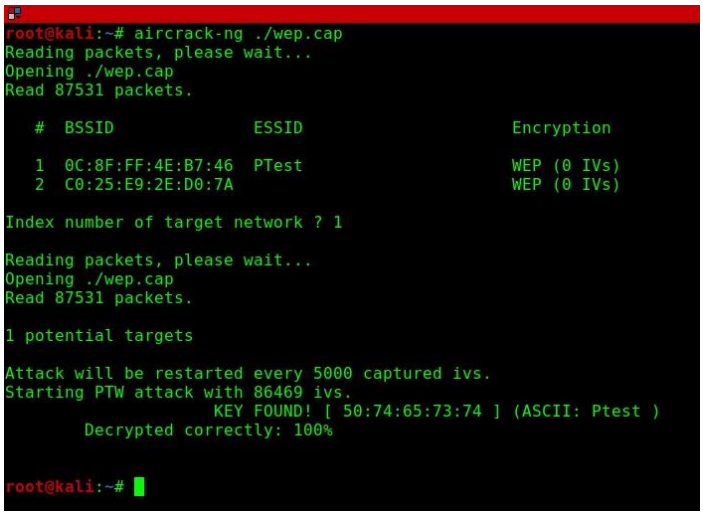
Na slici 16. vidljiv je prikaz skeniranja lokalnih bežičnih mreža pomoću airodump-ng alata. Tražene mreže za penetracijsko testiranje označene su crvenim kvadratom na slici. Skeniranjem saznajemo informacije o bežičnoj mreži poput MAC adrese pristupne točke, jačinu signala, kanale na kojima mreže emitiraju te načine enkripcije i autentifikacije zajedno s nazivima bežičnih mreža. U donjem dijelu slike prikazane su MAC adrese uređaja zajedno s MAC adresama pristupnih točaka na koje su povezani. Naša bežična mreža naziva se „PTest“ i vidimo da koristi WEP protokol kao enkripciju s MAC adresom 0C:8F:FF:4E:B7:46 i da se nalazi na kanalu 8. Sljedeći korak je izvršavanje samog napada na WEP protokol „PTest“ pristupne točke pomoću naredbe *besside-ng -b 0C:8F:FF:4E:B7:46 -c 8 -p 10000 wlan0mon*. Besside-ng koristimo za poplavljivanje bežične mreže s inicijalizacijskim vektorima kako bi dobili hash ključ s potrebnom lozinkom. U naredbi smo koristili argument -b koji označava MAC adresu bežične pristupne točke koje napadamo, -c kanal na kojem emitira pristupna točka, -p

koji predstavlja količinu IV-a kojima poplavljujemo mrežu i adapter wlan0mon koji koristimo pri napadu. Rezultat korištenja ove funkcije vidljiv je na slici 17.



Slika 17: Poplavljivanje WEP protokola inicijalizacijskim vektorima (autorski rad)

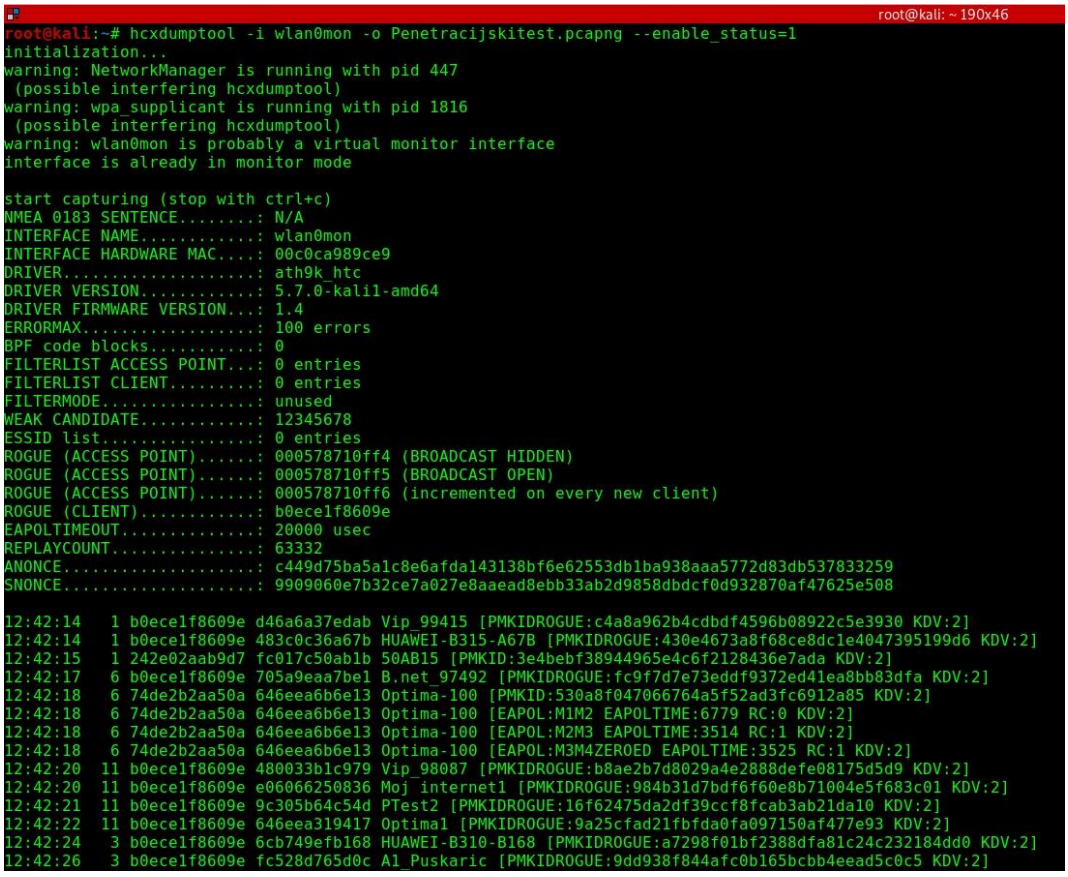
Na slici 17 vidimo kako je bilo potrebno malo više od 20 tisuća inicijalizacijskih vektora kako bismo pronašli ključ. Dobiveni podaci se automatski spremaju za sljedeći korak, a to je dobivanje same lozinke pomoću aircrack-ng alata. Za dobivanje lozinke koristimo naredbu *aircrack-ng ./wep.cap* gdje pomoću Linux naredbe govorimo alatu aircrack-ng da otvori i dekriptira datoteku pod nazivom wep.cap. Rezultati naredbe daju heksadekadsku vrijednost ključa i vidljivi su na slici 18 gdje zajedno s ostalim uhvaćenim IV-ovima dobivamo lozinku u ASCII vrijednosti „PTest“.



Slika 18: Dekriptiranje heksadekadske vrijednosti ključa WEP-a u ASCII (autorski rad)

5.4. Penetracijsko testiranje WPA/WPA2 protokola bežične mreže

Prilikom testiranja WPA i WPA2 protokola bežične mreže, koristimo paket alata Hcxtools i Hashcat. Za otkrivanje lozinke unutar hasha s uhvaćenim podacima koristit ćemo napad rječnikom radi bržeg otkrivanja lozinke i jednostavnosti prikaza penetracijskog testiranja. Penetracijski napad vrši se na bežičnu pristupnu mrežu pod nazivom „PTest2“. Pri napadu pretpostavljamo da se fraza za lozinku nalazi u rječniku te ćemo koristiti rječnik s 10000 riječi i radi demonstracijskog primjera „umjetno“ postavljenom riječju koja čini vrijednost lozinke pristupne točke. Kako bismo uopće mogli izvršiti napad potrebno je obaviti izviđanje lokalnih bežičnih mreža pomoću airodump-ng alata. Informacije za traženu bežičnu mrežu već smo dobili prethodnim skeniranjem lokalnih bežičnih mreža prikazane na slici 16. poglavlja 5.3.. Sljedeći korak pri testiranju je hvatanje PMKID ključa tako da ćemo „osluškivati“ emitiranje pristupne točke. Traženje i hvatanje PMKID ključa vršimo pomoću alata hcxdumptool i naredbe *hcxdumptool -i wlan0mon -o Penetracijskitest.pcapng –enable_status=1*.

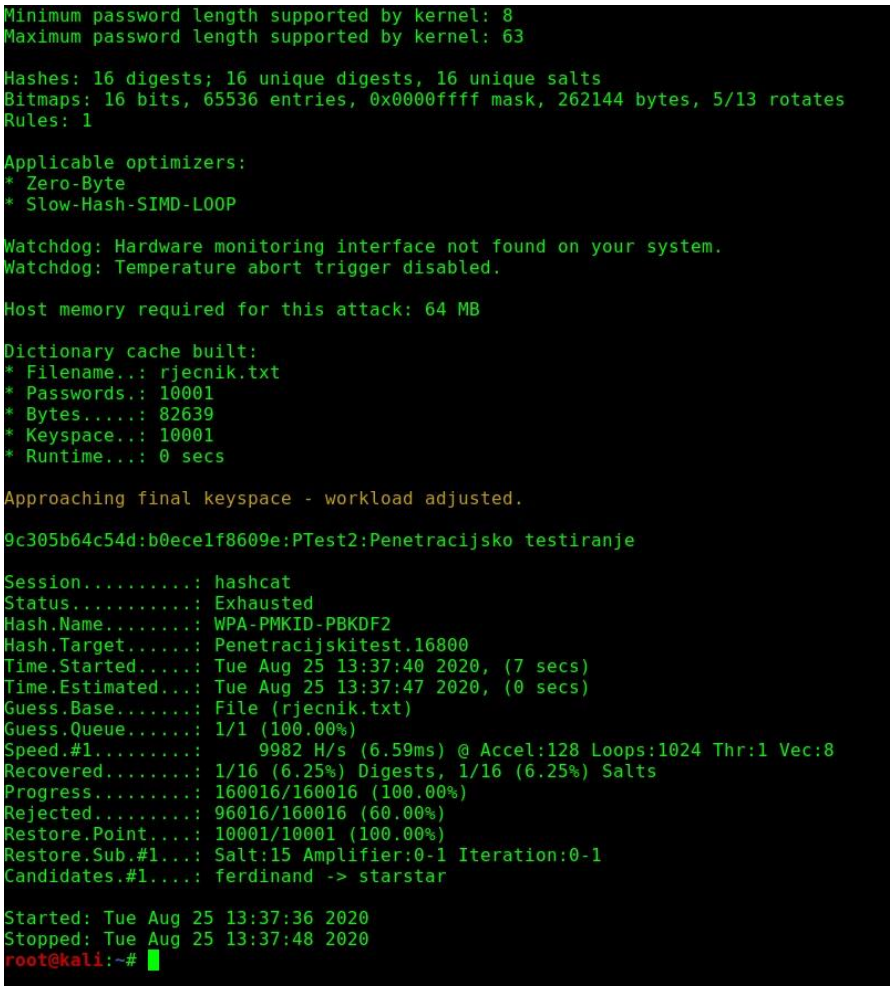


Slika 19: Hvatanje PMKID vrijednosti pomoću hcxdumptool-a (autorski rad)

Ovom funkcijom skeniramo sva lokalna emitiranja te hvatamo PMKID ključeve lokalnih bežičnih pristupnih točaka u obliku hasha kojeg ćemo kasnije koristiti u napadu s rječnikom. U naredbi koristili smo argument -i koji označava mrežni adapter s kojim hvatamo ključeve (wlan0mon), -o ime datoteke u koju spremamo uhvaćene podatke i –enable_status=1 koji označava EAP i EAPOL okvir koje hvatamo prilikom skeniranja mreža. (Slika 19)

Nakon dobivene datoteke formata .pcapng, tu datoteku konvertiramo u format .16800 kako bismo u Hashcatu mogli dekriptirati uhvaćene PMKID-ove u obliku hasha. Format 16800 označava format koji Hashcat prepoznaje kao PMKID dekripciju. Konvertiranje datoteke vrši se pomoću naredbe *hcxpcaptool -E -I -U -z Penetracijskitest.16800 Penetracijskitest.pcapng* gdje -E označava listu uhvaćenih MAC adresa, -I listu identiteta, -U listu korisničkih imena i -z ime novokreirane datoteke s 16800 formatom. Posljednji korak u dobivanju lozinke je korištenje Hashcat alata koji dekriptira novostvorenu datoteku i pomoću napada rječnikom izbacuje moguće rezultate uhvaćenih paketa.

Za dobivanje krajnje vrijednosti lozinke koristimo naredbu *hashcat -m 16800 Penetracijskitest.16800 -a 0 –force –self-test-disabled rjecnik.txt.* Argument -m predstavlja način enkripcije hash vrijednosti (u ovom slučaju 16800), -a način napada gdje 0 označava napad rječnikom, --force argument otklanja moguća upozorenja kako bismo nastavili s radom programa, --self-test-disabled označava argument kojim otklanjamo moguće greške prilikom dekripcije te rjecnik.txt predstavlja naziv datoteke koja sadrži riječi. Rezultati nakon obrade vidljivi su na slici 20. Slika 20 prikazuje postupak pretraživanja riječi u rječniku i uspoređivanja riječi sa svim uhvaćenim vrijednostima. Vidimo da za hash „9c305b64c54d:b0ece1f8609e“ s nazivom pristupne točke „PTest2“ postoji lozinka „Penetracijsko testiranje“. Važno je napomenuti da je u realnim slučajevima napada na ovakvu frazu lozinke s razmakom i velikim slovima potrebno puno vremena i procesorske snage, te da je ova lozinka samo primjer kako i koje lozinke Hashcat može otkriti. U donjem dijelu slike vidimo proces uspoređivanja i pretraživanja riječi. Bitne vrijednosti koje možemo promatrati su vrijednost „Speed.#1“ prikazuje već spomenuti Hash Rate obrade te vrijednost „Candidates.#1“ koja označava trenutnu uspoređenu riječ. U ovom slučaju cijeli proces je trajao 12 sekundi zbog malog rječnika s 10 tisuća riječi, ali pri stvarnim penetracijskih testiranjima vrijeme obrade može trajati danima.

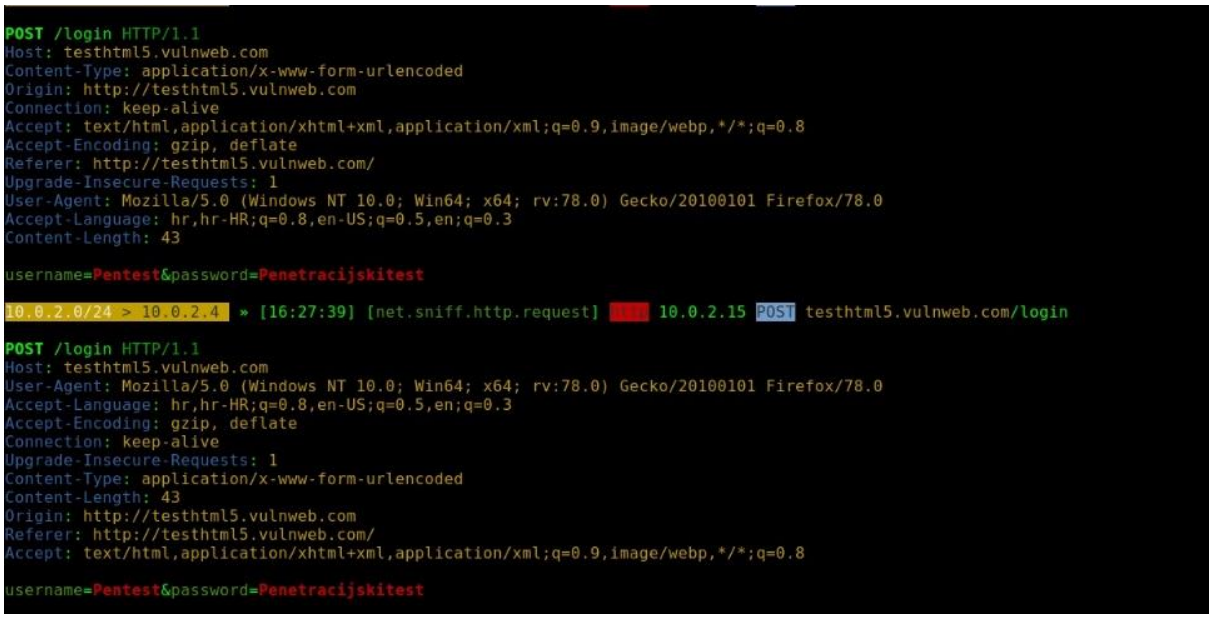


Slika 20: Rezultati obrade Hash vrijednosti s dobivenom lozinkom (autorski rad)

5.5. Napad „Čovjek u sredini“

Nakon uspješnog penetracijskog napada nad nekim od sigurnosnih protokola i dobivanja lozinke za autentifikaciju, sljedeći korak je izvršavanje unutarnjeg napada na lokalnu bežičnu mrežu pomoću MiTM napada ili napada „Čovjek u sredini“. Kako bi saznali IP adresu povezanog uređaja potrebno je prvo izvršiti unutarnje izviđanje bežične mreže pomoću nmap alata. U primjeru za penetracijsko testiranje koristimo dva uređaja, napadača i napadnuti uređaj. Napadnuti uređaj i napadač spojeni su pomoću preraspodjele adresnog prostora odnosno pomoću NAT *(eng. Network Address Translation)* mreže. Skeniranjem uređaja pomoću nmap alata saznajemo IP adresu napadnutog uređaja koji ima IP adresu vrijednosti 10.0.2.6. dok uređaj s kojeg vršimo napad ima IP adresu vrijednosti 10.0.2.4. Nakon što smo saznali IP adresu, možemo vršiti napad „Čovjek u sredini“ između uređaja i pristupne točke pomoću alata bettercap. Prvo što moramo napraviti u bettercapu je pokrenuti napad trovanja ARP protokola pomoću naredbe *set arp.spoof.fullduplex true*. Ova naredba omogućuje napad

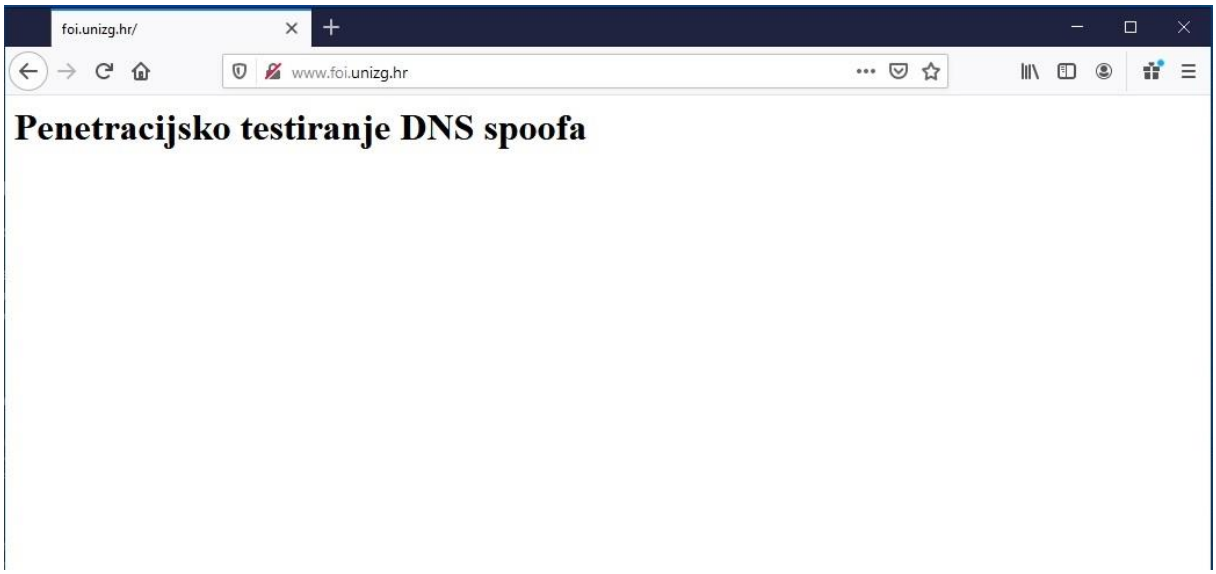
u dva smjera, prema napadnutom računalu i prema mrežnom pristupniku. Sljedeći korak je određivanje IP adrese koju napadamo pomoću naredbe *set arp.spoof.targets 10.0.2.15* te posljednji korak u trovanju ARP protokola je omogućivanje rada programa pomoću naredbe *arp.spoof on*. Trovanje ARP protokola omogućuje nam presretanje podataka koje napadnuto računalo pretražuje na Internetu. Pokretanje presretanja podataka vršimo naredbom *net.sniff on*. Nakon upisane naredbe računalo presreće sve zahtjeve koje napadnuto računalo šalje mrežnom pristupniku. Pomoću napada „Čovjek u sredini“ napadač može vidjeti sve podatke koje kruže od napadnutog uređaja prema Internetu poput učitanih slika, posjećenih stranica i slično. Ovaj napad može ozbiljno povrijediti privatnost podataka napadnute osobe ukoliko osoba posjeti web stranicu s nezaštićenim HTTP protokolom gdje napadač može vidjeti osobe podatke poput lozinke i korisničkog imena prilikom prijave na HTTP web stranici (Slika 21).



Slika 21: Prikaz napada „Čovjek u sredini“ i dohvaćanja osobnih podataka (autorski rad)

Napad „Čovjek u sredini“ možemo koristiti i za DNS napade u kojima možemo preusmjeriti određenu web stranicu na vlastitu web stranicu. Za takozvani DNS spoofing potrebno je pokrenuti vlastiti server s web stranicom koju želimo da napadnuta osoba vidi koristeći naredbu ugrađenu unutar Linux operativnog sustava *service apache2 start*. Navedenom funkcijom pokrećemo Apache HTTP poslužitelj s lokalnom web stranicom kojom možemo pristupiti pomoću IP adrese uređaja, u ovom slučaju 10.0.2.4. U ovom primjeru zamijenit ćemo početnu web stranicu foi.unizg.hr s vlastitom stranicom pomoću bettercap alata. Kako bismo izmijenili putanju DNS servera u bettercap upisujemo naredbu *set*

dns.spoof.all true u svrhu odgovora na bilo koji DNS zahtjev poslan napadačevom računalu. Sljedeća naredba *set dns.spoof.domains foi.unizg.hr,*.foi.unizg.hr* opisuje koju ćemo web stranicu i njezine domene zamijeniti s vlastitom stranicom. Argument *.foi.unizg.hr predstavlja sve subdomene koje se mogu pojavljivati prilikom pristupa na početnu web stranicu. Potrebno je samo pokrenuti DNS spoof pomoću naredbe *dns.spoof on*. Kada korisnik želi pristupiti početnoj stranici domene foi.unizg.hr, on će biti preusmjeren na napadačevu stranicu kao što vidimo na slici 22.

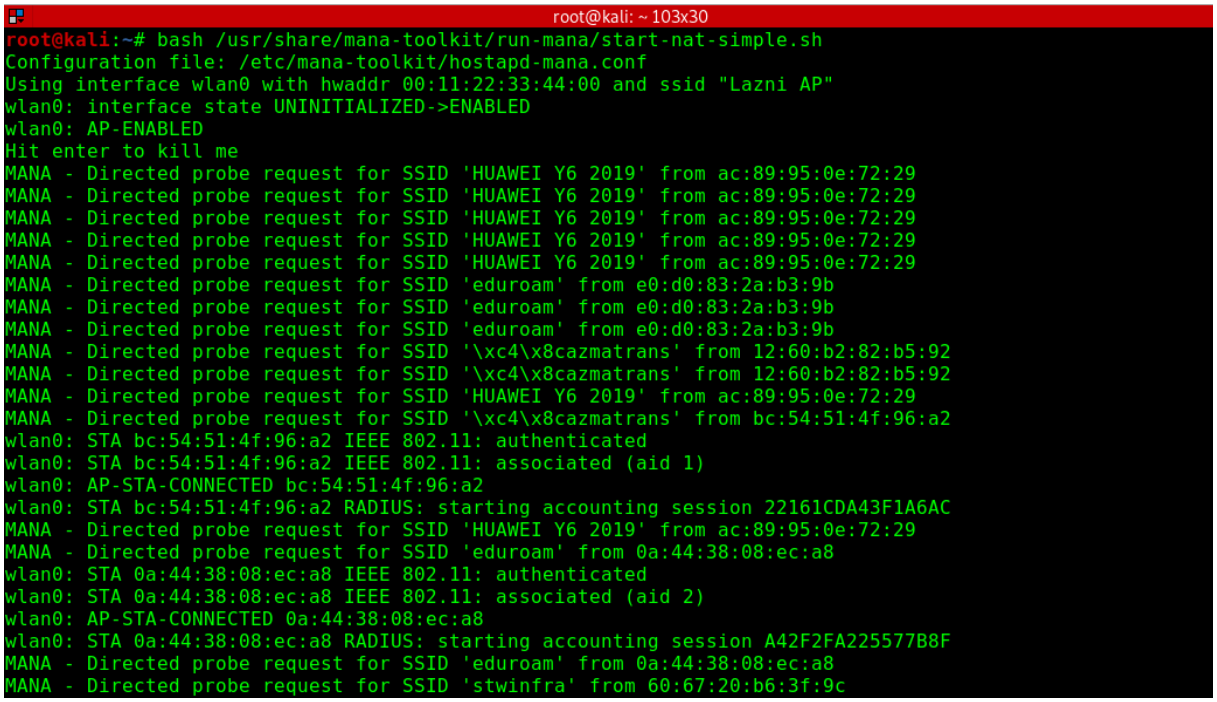


Slika 22: Prikaz DNS spoof foi.unizg.hr domene (autorski rad)

5.6. Kreiranje lažne pristupne točke

Lažne pristupne točke mogu biti kreirane u dvije različite svrhe, kreiranjem divlje pristupne točke ili kreiranja „Zla Blizanca“. Ovaj primjer biti će usmjeren na kreiranje divlje pristupne točke. Karakteristike divlje pristupne točke je otvorena internetska veza bez upotrebe autentifikacije. Ovakav napad najčešće se odvija na javnim mjestima kako bi privukao što više ljudi. Krajnji cilj ovog napada je korištenje napada „Čovjek u sredini“ nad priključenim uređajem. U ovom primjeru koristiti ćemo alat mana toolkit koji sadrži automatske programske i funkcijske vrijednosti za uspostavu divlje pristupne točke. Alat nije preinstaliran unutar Kali operacijskog sustava stoga koristimo osnovne Linux naredbe. Prvo otvaramo tekstni dokument s postavkama lažne pristupne točke tako da u terminal upišemo naredbu *leafpad /etc/mana-toolkit/hostapd-mana.conf* pomoću tekstualnog editora leafpada. U konfiguracijskoj datoteci možemo odrediti mrežni adapter pomoću kojeg emitiramo bežičnu mrežu, MAC adresu i naziv

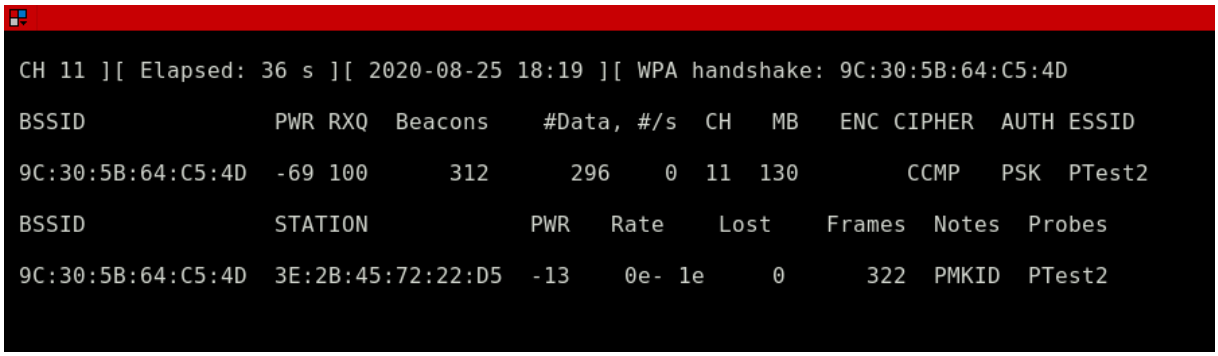
lažne pristupne točke te kanal na kojem će se mreža emitirati. Sljedeći korak je aktiviranje lažne pristupne točke pomoću bash naredbe. Nakon pokretanja u terminalu vidimo aktiviranu lažnu pristupnu točku s internetskom vezom. (Slika 23)



Slika 23: Prikaz aktiviranja i djelovanja lažne pristupne točke (autorski rad)

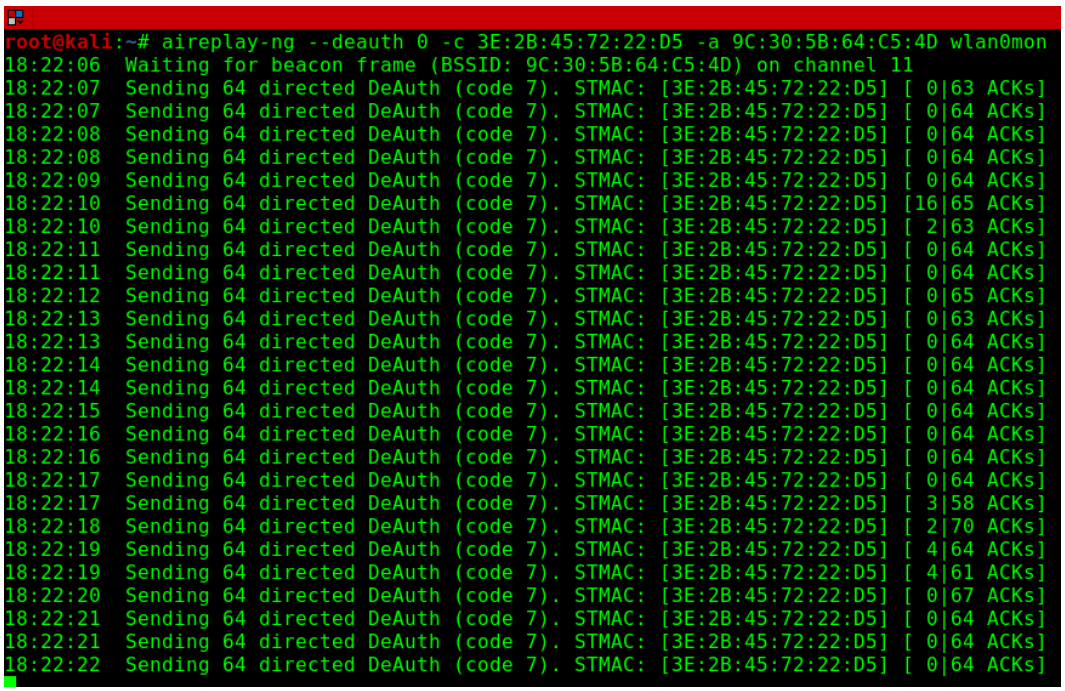
5.7. Deautentifikacija uređaja s lokalne bežične mreže

Deautentifikacija uređaja s lokalne bežične mreže dio je DoS napada koji je detaljnije objašnjen u odlomku 3.3.4.. Deautentifikacija uređaja izvršava se u slučajevima kada napadač želi namjerno isključiti korisnika s njegove bežične mreže kako bi korisnik ponovno zatražio autentifikaciju s mrežom, ali ovog puta lažnom mrežom to jest stvorenog „Zla Blizanca“ s ciljem da dođe do lozinke duplicirane bežične pristupne točke. Kako bi vidjeli uređaje povezane na lokalnu bežičnu mrežu, potrebno je izvršiti naredbu *airodump-ng –bssid 9C:30:5B:64:C5:4D –channel 11 wlan0mon* u kojoj argument --bssid predstavlja MAC adresu pristupne točke, --channel broj kanala emitiranja mreže i wlan0mon naziv mrežnog adaptera. Nakon izvršavanje naredbe dobijemo popis povezanih uređaja na mreži vidljiv na slici 24.



Slika 24: Prikaz traženja uređaja povezanih na specifičnu bežičnu mrežu (autorski rad)

Sljedeći korak je izvršavanje DoS napada na uređaj pomoću alata aireplay-ng. U aireplay-ng alatu koristimo naredbu *aireplay-ng –deauth 0 -c 3E:2B:45:72:22:D5 -a 9C:30:5B:64:C5:4D wlan0mon.* Argument –deauth predstavlja napad deautentifikacije, broj 0 predstavlja neograničenu količinu injektiranih paketa koji vrše napad deautentifikacije, -c MAC adresu uređaja kojeg napadamo, -a MAC adresu pristupne točke koju napadamo i wlan0mon mrežni adapter kojeg koristimo. Nakon izvršenog napada u terminalu vidimo broj poslanih ACK *(eng. Acknowledgment)* signala.(Slika 25)



Slika 25: Prikaz napada deautentifikacije uređaja unutar bežične mreže (autorski rad)

6. Zaključak

Sadašnjost bez Interneta je nezamisliv pojam. Svakim danom povećava se broj korisnika Interneta koji nesvjesno ostavljaju svoj trag u virtualnoj mreži dostupnoj većini populacije. Većina tih korisnika nije svjesno opasnosti koje Internet predstavlja njihovoj sigurnosti i privatnosti. Živimo u dobu gdje se prodaju informacije korisnika Interneta za vlastiti dobitak i prihod te svakodnevno u svijetu virtualno napadne osoba ili korporacija koristeći Internet. Cilj ovog rada je prikazati kako Internet nije savršeno i sigurno mjesto te kako postojeće sigurnosne zaštite nisu dovoljne da osoba bude potpuno sigurna od virtualnih napada. U današnjem vremenu posvećeno je jako malo pažnje mrežnoj sigurnosti koja će u budućnosti biti sve potrebnija i traženija informatička disciplina kako bi se sigurnost i privatnost korisnika potpuno zaštitila u „Online“ svijetu.

Praktični dio rada prikazuje kako ranjivost bežične mreže te koliko su određeni sigurnosni protokoli jednostavno probijeni u roku od nekoliko minuta. Većina korištenih alata i Linux distribucija besplatni su na Internetu čime se svakodnevno povećava broj novih većih napada u svijetu.

Popis literature

Poddar, V., & Choudhary, H. (2014). A Comparitive Analysis of Wireless Security Protocols (WEP And WPA2). *International Journal On Adhoc Networking Systems*, *4*(3), 1-7. doi: 10.5121/ijans.2014.4301

Hucaby, D. (2016). *CCNA wireless 200-355 official cert guide*. Indianapolis, IN: Cisco Press.

Yao Yao, Jiang Chong and Wang Xingwei, "Enhancing RC4 algorithm for WLAN WEP protocol," 2010 Chinese Control and Decision Conference, Xuzhou, 2010, pp. 3623-3627, doi: 10.1109/CCDC.2010.5498536.

Prodanović, R., & Simić, D. (2007). A Survey of Wireless Security. Journal Of Computing And Information Technology, 15(3), 237. doi: 10.2498/cit.1000877

Tews, E., & Beck, M. (2009). Practical attacks against WEP and WPA. Proceedings of the Second ACM Conference on Wireless Network Security - WiSec '09. doi:10.1145/1514274.1514286

Khasawneh, Mahmoud & Kajman, Izadeen & Alkhudaidy, Rashed & Althubyani, Anwar. (2014). A Survey on Wi-Fi Protocols: WPA and WPA2. 420. 496-511. 10.1007/978-3-642-54525-2_44.

Rumale, A.S., & Chaudhari, D.D. (2011). IEEE 802 . 11 x , and WEP , EAP , WPA /

WPA 2. Ohigashi, T., & Morii, M. (2009). A Practical Message Falsification Attack on WPA.

4-way handshake (2019). Preuzeto 15.6.2020. s https://www.wifi-professionals.com/2019/01/4-way-handshake

C He, J C Mitchell (2004). - In Proceedings of the 3rd ACM workshop on Wireless security,

Croatian Academic and Research network [CARNet] (2009). *WPA2 zaštita.*

Preuzeto 16.06.2020. s https://www.cert.hr/wp-content/uploads/2009/06/CCERT-PUBDOC-2009-06-267.pdf

O socijalnom inženjeringu (bez dat.). U CERT.hr. Preuzeto 15.07.2020. s https://www.cert.hr/socijalni_inzenjering/#

D. Whiting, R. Housley, and N. Ferguson. (2003.) RFC3610: Counter with CBC-MAC (CCM). RFC Editor, USA.

Mahajan, P., & Sachdeva, A. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. Global journal of computer science and technology, 13.

Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard.

AES structure [Slika] (bez dat.) Preuzeto 16.06.2020. sa https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

Croatian Academic and Research network [CARNet] (2008). EAP protokol. Preuzeto 16.06.2020. s https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2008-01-216.pdf

Croatian Academic and Research network [CARNet] (2006). Autentifikacija u bežičnim mrežama. Preuzeto 16.06.2020. s https://www.cert.hr/wp-content/uploads/2006/10/CCERT-PUBDOC-2006-10-170.pdf

Kumkar, Vishal & Tiwari, Akhil & Tiwari, Pawan & Gupta, Ashish & Shrawne, Seema. (2012). Vulnerabilities of Wireless Security protocols (WEP and WPA2). International Journal of Advanced Research in Computer Engineering & Technology. 1.

„New attack on WPA/WPA2 using PMKID“ (2018.) Preuzeto 17.06.2020. s https://hashcat.net/forum/thread-7717.html

Kohlios, C.P., & Hayajneh, T. (2018). A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. Electronics, 7, 284.

Jawandhiya, Pradip & Ghonge, Mangesh & DR, M.S.ALI & DESHPANDE, PROF. (2010). A Survey of Mobile Ad Hoc Network Attacks. International Journal of Engineering Science and Technology. 2. 4063-4071. 10.2139/ssrn.3451027.

Centar informacijske sigurnosti [CIS] (2011.) *Zaštita od prisluškivanja mrežnog prometa*. Preuzeto 16.07.2020. s https://www.cis.hr/files/dokumenti/CIS-DOC-2011-10-029.pdf

DoS Napadi (bez dat.). U Wiki Informacijske Sigurnosti. Preuzeto 17.07.2020. s https://www.cis.hr/WikiIS/doku.php?id=dos_attacks

Introduction. (bez dat.) U aircrack-ng wiki. Preuzeto 19.07.2020. s https://www.aircrack-ng.org/doku.php

Chapter 15. Nmap Reference Guide. (bez dat.) U nmap.org. Preuzeto 21.07.2020. s https://nmap.org/book/man.html#man-description

Introduction (bez dat.). U bettercap.org. Preuzeto 21.07.2020. s https://www.bettercap.org/intro/

The MANA Toolkit. (bez dat.) U github.com. Preuzeto 21.07.2020. s https://github.com/sensepost/mana

Pixiewps. (bez dat.) U github.com. Preuzeto 21.07.2020. s https://github.com/wiire-a/pixiewps

Hashcat (bez dat.) U hashcat.com/wiki Preuzeto 21.07.2020. s https://hashcat.net/wiki/

Popis slika

Slika 1: Položaj sigurnosnih protokola u OSI modelu. 2
Slika 2: Prikaz procesa enkripcije WEP protokola. 4
Slika 3: Princip rada TKIP protokola u WPA. 8
Slika 4: Prikaz procesa četverostrukog rukovanja. 12
Slika 5: Prikaz CBC-MAC algoritma za izradu MAC oznake. 14
Slika 6: Proces CTR enkripcije poruke i MIC-a 15
Slika 7: Shematski prikaz AES strukture i transformacija u koracima. 17
Slika 8: Primjer osnovnog OSINT istraživanja u programu Maltego 24
Slika 9: Prikaz prisluškivanja paketa okolnih pristupnih točaka pomoću Wiresharka 25
Slika 10: shematski prikaz napada „Čovjek u sredini“ 27
Slika 11: Primjer trovanja DNS priručne memorije 29
Slika 12: Prikaz lokalnog DoS napada. 30
Slika 13: Mrežni adapteri korišteni u praktičnom dijelu penetracijskog testiranja 37
Slika 14: Promjena MAC adrese mrežnog adaptera 37
Slika 15: Pokretanje načina za nadziranje mrežnog adaptera 38
Slika 16: Skeniranje lokalnih bežičnih mreža pomoću airodump-ng alata 39
Slika 17: Poplavljivanje WEP protokola inicijalizacijskim vektorima 40
Slika 18: Dekriptiranje heksadekadske vrijednosti ključa WEP-a u ASCII 40
Slika 19: Hvatanje PMKID vrijednosti pomoću hcxdumptool-a 41
Slika 20: Rezultati obrade Hash vrijednosti s dobivenom lozinkom 43
Slika 21: Prikaz napada „Čovjek u sredini“ i dohvaćanja osobnih podataka 44
Slika 22: Prikaz DNS spoof foi.unizg.hr domene 45
Slika 23: Prikaz aktiviranja i djelovanja lažne pristupne točke 46
Slika 24: Prikaz traženja uređaja povezanih na specifičnu bežičnu mrežu 47
Slika 25: Prikaz napada deautentifikacije uređaja unutar bežične mreže 47