Analiza sigurnosti bežične mreže

Skočibušić, Davor

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

ANALIZA SIGURNOSTI BEŽIČNE MREŽE

Završni rad

Davor Skočibušić

Osijek, 2021.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 10.09.2021.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada na preddiplomskom sveučilišnom studiju

Ime i prezime studenta:	Davor Skočibušić
Studij, smjer:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	R4133, 28.07.2017.
OIB studenta:	11905715608
Mentor:	Prof.dr.sc. Goran Martinović
Sumentor:	Izv. prof. dr. sc. Krešimir Grgić
Sumentor iz tvrtke:	
Naslov završnog rada:	Analiza sigurnosti bežične mreže
Znanstvena grana rada:	**Informacijski sustavi (zn. polje računarstvo)**
Predložena ocjena završnog rada:	Vrlo dobar (4)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 3 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 2 razina
Datum prijedloga ocjene mentora:	10.09.2021.
Datum potvrde ocjene Odbora:	22.09.2021.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 24.09.2021.

Ime i prezime studenta:	Davor Skočibušić
Studij:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	R4133, 28.07.2017.
Turnitin podudaranje [%]:	15

Ovom izjavom izjavljujem da je rad pod nazivom**: Analiza sigurnosti bežične mreže**

izrađen pod vodstvom mentora Prof.dr.sc. Goran Martinović

i sumentora Izv. prof. dr. sc. Krešimir Grgić

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

IZJAVA

o odobrenju za pohranu i objavu ocjenskog rada

kojom ja __Davor Skočibušić_____, OIB: __11905715608_____, student/ica Fakulteta elektrotehnike,
računarstva i informacijskih tehnologija Osijek na studiju _Preddiplomski sveučilišni studij Računarstvo_,
kao autor/ica ocjenskog rada pod naslovom: _Analiza sigurnosti bežične mreže**,**

dajem odobrenje da se, bez naknade, trajno pohrani moj ocjenski rad u javno dostupnom digitalnom repozitoriju ustanove Fakulteta elektrotehnike, računarstva i informacijskih tehnologija Osijek i Sveučilišta te u javnoj internetskoj bazi radova Nacionalne i sveučilišne knjižnice u Zagrebu, sukladno obvezi iz odredbe članka 83. stavka 11. *Zakona o znanstvenoj djelatnosti i visokom obrazovanju* (NN 123/03, 198/03, 105/04, 174/04, 02/07, 46/07, 45/09, 63/11, 94/13, 139/13, 101/14, 60/15).

Potvrđujem da je za pohranu dostavljena završna verzija obranjenog i dovršenog ocjenskog rada. Ovom izjavom, kao autor/ica ocjenskog rada dajem odobrenje i da se moj ocjenski rad, bez naknade, trajno javno objavi i besplatno učini dostupnim:

a) široj javnosti

b) studentima/icama i djelatnicima/ama ustanove

c) široj javnosti, ali nakon proteka 6 / 12 / 24 mjeseci (zaokružite odgovarajući broj mjeseci).

**U slučaju potrebe dodatnog ograničavanja pristupa Vašem ocjenskom radu, podnosi se obrazloženi zahtjev nadležnom tijelu Ustanove.*

__Osijek, 24.09.2021._____ _____

(mjesto i datum) (vlastoručni potpis studenta/ice)

SADRŽAJ

1.UVOD

Bežične mreže koriste radio signal za prenošenje podataka stoga su vrlo podložne prisluškivanju za razliku od žičnih mreža. Gotovo svaki čovjek je danas povezan na internetsku mrežu svojim računalom ili pametnim telefonom. Za pristup Wi-Fi mreži s nekim uređajem mora se odabrati naziv mreže i unijeti lozinka. Na nekim mrežama moguće je ostvariti pristup bez potrebe za lozinkom, što znači da se toj mreži može pridružiti bilo tko. Međutim, u većini slučajeva Wi-Fi mreže su sigurne i zahtijevat će lozinku. Trenutno postoji nekoliko različitih protokola koji se koriste za zaštitu Wi-Fi mreže.

Ideja rada je prikazati kompletan proces ostvarivanja neovlaštenog pristupa u bežičnu mrežu ovisno o načinu zaštite koju ista koristi, te pokazati neke prijetnje koje korisnik može očekivati unutar same mreže nakon što napadač ostvari pristup istoj. Na kraju rada dane su preporuke i prakse kojima se može povećati razina sigurnosti bežične mreže. Za napade prema bežičnoj mreži korištena je privatna mreža. Za izradu rada korišten je operacijski sustav Kali linux s kojega se svaki napad odvija korištenjem različitih alata. Također korišteno je računalo sa operacijskim sustavom Windows 10 koje je u jednom od primjera bilo meta za napad čovjek u sredini (engl. *Man-in-the-Middle, MITM)*, kreiranje lažnog DNS poslužitelja, te prisluškivanje prometa. Nadalje unutar virtualne mašine instaliran je sustav Windows XP sa važećom licencom u svrhu prikazivanja eksploatacije sustava, na način da napadač dobije daljinsko izvršavanje koda odnosno daljinski pristup računalu sa svim administratorskim pravima samo zbog toga što je povezan na istu mrežu kao i klijentsko računalo. Kako bi se rad i njegovi modeli napada uspješno izveli potrebno je poznavanje linux komandi, windows powershella, znanje o mrežama te rad s virtualnim mašinama kao i s alatima koji dolaze uz operacijski sustav kali linux ili su za potrebe rada instalirani, a to su aircrack-ng, nmap, metasploit framework, apache, ettercap, whireshark, fluxion, cupp, crunch. Samo instaliranje alata koji su korišteni u radu kao i instaliranje Windows operacijskog sustava, rukovanje s virtualnom mašinom.

Struktura rada je sljedeća: u drugom poglavlju opisano je stanje sigurnosti u bežičnim mrežama, protokoli koji se danas koriste;u trećem poglavlju teoretski su opisani napadi za ostvarivanje pristupa bežičnoj mreži koji su podijeljeni u tri kategorije: napada deautentifikacije, kriptografski napadi te napadi društvenog inženjerstva; u četvrtom poglavlju primjerom je prikazano dobivanje procesa rukovanja osluškivanjem, te ostvarivanje pristupa mreži koja je zaštićena WEP enkripcijom; U petom poglavlju opisana su dva različita alata za kreiranje lista riječi i napad

sirovom snagom korištenjem istih na prethodno uhvaćeni proces rukovanja (engl. captured handshake), te model društvenog inženjerstva; U šestom poglavlju teoretski su opisani protokoli i komunikacija unutar mreže te načini i alati na koji se normalni standardi mogu zloupotrijebiti uz korištenje određenih alata; U sedmom poglavlju napravljen je model napada čovjek u sredini gdje je prikazano trovanje ARP memorije kao i inspekcija paketa te kreiranje lažnog DNS poslužitelja, također je modelom prikazano neovlašteno dobivanje pristupa računalu kao i skeniranje mreže u potrazi za ranjivim uređajima; U osmom poglavlju dane su preporuke zaštite koje se jednostavno mogu implementirati kako bi sigurnost mreže bila nešto veća.

1.1.Zadatak završnog rada

U završnom radu potrebno je opisati i analizirati sigurnosnu okolinu bežične mreže s gledišta ostvarenja pristupa mreži, mogućih prijetnji prema korisnicima mreže, te načina zaštite korisnika. Posebnu pozornost treba posvetiti slanju paketa za deautentificiranje korisnika i društvenom inženjerstvu, neovlaštenom nadziranju korisnika i podvaljivanju korisniku, ostvarivanju neovlaštenog pristupa računalu, te uvođenju preporuka za povećanje razine sigurnosti u bežičnoj mreži. Nadalje, treba razraditi model ostvarenja pristupa, prijetnji i načina zaštite. U praktičnom dijelu rada potrebno je, na temelju predloženog modela, za odgovarajuće primjere ostvarenja pristupa bežičnoj mreži i prijetnje prema korisniku, a koristeći prikladne programe, alate i računalnu okolinu, kvalitativno i kvantitativno analizirati sigurnosnu okolinu i predložiti mjere koje povećavaju razinu sigurnosti u bežičnoj mreži.

2. STANJE U PODRUČJU SIGURNOSTI BEŽIČNIH MREŽA

Kako se cijeli svijet preselio na Internet, tako ga je kriminal i popratio. Tema sigurnosti u kibernetičkom svijetu je vrlo zanimljiva i široko obrađena. Svakim danom otkrivaju se nove prijetnje te se iza kulisa vodi prava utrka između etičnih i ne etičnih hakera. U ovom poglavlju opisano je trenutno stanje u sigurnosti bežičnih mreža, aktualne protokole te ću se osvrnuti na sigurnost koja se analizira u ovom radu [1] .

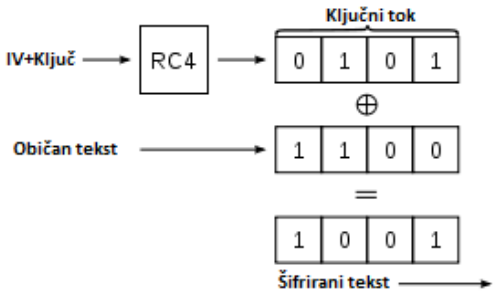
2.1. Trenutna sigurnosna zaštita

Iako se na prvi pogled može pomisliti kako nedostataka i prijetnji koji mogu naštetiti korisnicima bežične mreže ima premalo i da se svaka prijetnja može na vrijeme detektirati, kontrolirati i spriječiti kako bi njen utjecaj na korisnika bio nepostojeći, napadači su pokazali da se jako dobro suprotstavljaju sigurnosnim preprekama koje im se nameću kako bi realizirali svoje prijetnje prema korisnicima bežičnih mreža. U idućem poglavlju opisat ću sigurnosne protokole koji se nalaze u današnjim bežičnim mrežama, a predstavljaju današnji sigurnosni standard. Vatrozid (engl. Firewall) smatra se dodatnim načinom zaštite koji se može implementirati na samu pristupnu točku ili na korisničke uređaje kako bi filtrirali dolazeći promet. Unutar rada opisani su napadi koji zaobilaze vatrozid kao i preporuke konfiguracije istoga u obliku MAC filtriranja [2].

2.2 Sigurnosni protokoli u bežičnoj mreži

2.2.1.WEP - Žična ekvivalentna privatnost

WEP (engl. Wired Equivalent Privacy) je algoritam za sigurnu komunikaciju putem IEEE 802.11 bežičnih mreža te se može reći da predstavlja školski primjer kako se kriptografija ne bi trebala upotrebljavati. Razvijen je 1999. godine i to je najraniji sigurnosni protokol koji je korišten za bežične mreže. Namijenjen je opskrbi bežičnih mreža istom sigurnosti kao i za žičane mreže. Međutim, pokazalo se da to nije slučaj jer je nakon nekog vremena utvrđeno da je 40-bitni ključ za šifriranje koji je WEP koristio ranjiv i nesiguran pa su povećali na 104 bita što još uvijek nije bilo dovoljno [3]. Slika 2.1 prikazuje provjeru cikličke redundancije (CRC) kod je za otkrivanje pogrešaka koji se obično koristi u digitalnim mrežama i uređajima za pohranu radi otkrivanja slučajnih promjena sirovih podataka(u ovom slučaju „data“=lozinka za pristup mreži).



Slika 2.1. Provjera cikličke redundancije [4]

Blokovi podataka koji ulaze u ove sustave dobivaju kratku provjeru vrijednost na temelju ostatka polinomske podjele njihovog sadržaja. Prilikom dohvaćanja, izračun se ponavlja i, u slučaju da se vrijednosti provjere ne podudaraju, mogu se poduzeti korektivne mjere protiv oštećenja podataka. CRC-ovi se koriste za ispravljanje pogrešaka. IV(vektor inicijalizacije) dodaje vrijednost WEP ključu kako ne bi svaki puta isto izgledao. *Za IV može se reći da je ekvivalenti pokušaj „soljenja" hashova u današnjoj kriptografiji*. Oni nakon toga prolaze kroz algoritam šifriranja RC4. Rezultat je šifrirani IV vektor i WEP ključ. Procesom XOR kombinira se 'izvorni podatak'/CRC sa IV i WEP ključem što rezultira šifriranim prijenosom u bežičnoj mreži(Cyphertext=šifrat). Veliki problem ovoga je što se moralo poslati IV sa šifratom zato što je to jedino što se mijenja i primajuća strana treba to da bi mogla dešifrirati šifrat. Vektor inicijalizacije (IV) dodan je kako bi zaštitio ključ za šifriranje. To su dodatna 24 bita koji su dio ključa. Stoga se kod prvotne zaštite od 64 bita veličina ključa sastojala samo od 40 bita (64-24), a kod kasnije proširenih 128 bita veličina ključa je 104 bita(128-24). Problem koji se pojavljuje sa malom veličinom vektora inicijalizacije(24 bita) je taj da ima samo 16,777,216 različitih mogućnosti, nakon čega se vrijednosti vektora inicijalizacije ponavljaju. Neke vrijednosti vektora su mnogo puta slabije od ostalih. Pomoću matematičkog procesa moguće je napraviti ovaj postupak unatrag kako bi se odredila vrijednost ključa enkripcije. Postoje alati koji ovaj proces rješavaju u par minuta na način da se prema mreži pošalje velika količina podataka(paketa) kako bi se prvo otkrio vektor inicijalizacije, a zatim i vrijednost ključa šifriranja. Obično se ključ šifriranja sazna na poslanih 15 do 20 tisuća paketa. Zbog te ranjivosti WEP se danas više ne koristi, a moderni Wi-Fi usmjerivači više ga neće imati ni kao opciju. Danas je dovoljno nekoliko minuta da bi se probila WEP zaštita[4] što je predstavljeno modelom u potpoglavlju 4.2.

2.2.2.WPA/WPA2- Wi-Fi zaštićeni pristup

Prema [4], WPA (engl. Wi-Fi Protected Access) je algoritam za sigurnu komunikaciju putem IEEE 802.11 bežičnih mreža koje su veoma ranjive na prisluškivanje pošto koriste radio signal za

prenošenje podataka. WPA je napravljen i uveden u upotrebu od strane Wi-Fi saveza nakon što je uočena ranjivost starijeg WEP algoritma. Bitna karakteristika WPA algoritma je da radi na uređajima koji mogu koristiti WEP. Poboljšanja koja su uvedena u WPA tiču se enkripcije komunikacije i autentifikacije korisnika. Enkripcija komunikacije je poboljšana korištenjem TKIP protokola (engl. Temporal Key Integrity Protocol). Za autentifikaciju se koristi EAP (Proširivi protokol provjere autentičnosti). WPA je privremeni algoritam koji bi trebao biti zamijenjen kada bude dovršen posao na 802.11i standardu. Prva verzija WPA ima svoje poboljšanje koje se ogleda u WPA2 protokolu čije se poboljšanje ogleda u uvođenju novog algoritma koji se bazira na naprednom standard šifriranja (AES). WPA2 je razvijen kako bi pružio još jaču sigurnost od WPA. I to čini zahtijevajući upotrebu jače metode šifriranja. Iako WPA koristi TKIP za šifriranje za koje se zna da imaju određena ograničenja, WPA2 koristi AES što je skraćenica od Advanced Encryption standard (napredni standard šifriranja). AES koristi simetrični algoritam šifriranja koji ga čini dovoljno snažnim da se odupre Brute-force napadu (napadu sirove snage). AES je toliko siguran da ga je američka vlada usvojila i sada ga koristi za šifriranje osjetljivih državnih podataka. U tablici 1.0 prikazani su nazivi WPA2 ključeva te koja je njihova upotreba.

Naziv ključa	Uporaba ključa
Master Key (MK)	Za izvođenje tajnog PMK ključa
Pairwise Master Key (PMK)	Za razmjenu PTK tajnog ključa
Pairwise Transient Key (PTK)	Za enkripciju, razmjenu GTK ključa, dokazivanje identiteta
Group Temporal Key (GTK)	Za dekripciju *multicast* i *broadcast* prometa

Tablica 1.0. *WPA2 ključevi*

2.2.3. WPA3

Nastao je u 7. mjesecu 2018. godine. Predstavlja poboljšanu verziju WPA2 koji ima poboljšanja za zaštitu nedovoljno kompleksnih lozinki, podržava SAE(Simultaneous Authentication of Equals) što znači da je dijeljenu tajnu teže pogoditi. Konkretan primjer je taj da u WPA2 protokolu napadač može uhvatiti šifrirani podatak u mreži, otići na bilo koju lokaciju i pokušati napad sirove snage na njega, no zbog SAE takav oblik napada je spriječen zbog toga što napadač mora biti u dometu mreže kako bi od nje dobio povratnu informaciju o ispravnosti lozinke što uvelike uvećava vrijeme izvođenja napada jer se mora čekati odgovor pristupne točke. Primjer napada sirovom snagom i vremenske ovisnosti istog detaljno je opisan u poglavlju 5. Uklonjeni su nesigurni kriptografski algoritmi, povećana je duljina ključa koja se koristi u enterprise verziji protokola i dodana je mogućnost jednostavnog spajanja uređaja(IoT uređaji, npr. printera)

upotrebom nekog složenijeg uređaja (npr. laptopa) kao zamjena za WPS koji je potpuno nesiguran [5]. WPA3 tržištu nudi najnovije sigurnosne protokole. Nadovezujući se na široko rasprostranjeni uspjeh i usvajanje Wi-Fi sigurnosti, WPA3 dodaje nove značajke za pojednostavljivanje Wi-Fi sigurnosti, omogućavanje robusnije provjere autentičnosti, isporuku povećane kriptografske snage za visoko osjetljiva tržišta podataka i održavanje otpornosti mreža kritičnih za zadatke. Sve WPA3 mreže koristite najnovije sigurnosne metode, zabranjuju zastarjele naslijeđene protokole, zahtijevaju korištenje zaštićenih okvira za upravljanje. Budući da se Wi-Fi mreže razlikuju po namjeni korištenja i sigurnosnim potrebama, WPA3 uključuje dodatne mogućnosti posebno za osobne i poslovne mreže. Korisnici WPA3-Personal dobivaju povećanu zaštitu od pokušaja pogađanja lozinke, dok korisnici WPA3-Enterprise-a mogu iskoristiti prednosti sigurnosnih protokola više klase za osjetljive podatkovne mreže. Isto kao i WPA2, WPA3 protokol koristi 128-bitnu enkripciju što predstavlja vrlo jak oblik zaštite. Umjesto da se dodatno pojačala enkripcija WPA3 se fokusirao na praktične načine obrane od napada. Sigurnost na javnim mrežama je također pojačana, na prijašnjim protokolima ako se htjelo spriječiti nekoga da nadzire radnje koje klijent obavlja u mreži trebala se koristiti virtualna privatna mreža (engl. VPN - Virtual Private Network) kao i https sigurnostni protokol. WPA3 će šifrirati svaku individualnu vezu koja je usmjerena prema nesigurnom poslužitelju osiguravajući korisničke podatke od krađe ili curenja informacija o pretraživanju. Kućni uređaji koji koriste Wi-Fi također će se lakše povezivati sa mrežom. Iako velik broj današnjih usmjerivača ima opciju WPS (engl. Wi-Fi Protected Setup) koja omogućuje uspostavu sigurnog povezivanja uređaja na mrežu ona ima sigurnosne mane koje je čine ranjivim na napade. WPA3 protokol razvio je noviji sistem koji se zove EasyConnect gdje se uz pomoć pametnog mobilnog uređaja koji je povezan sa mrežom skenira jedan QR kod usmjerivača, a drugi kod uređaja kojeg se želi povezati sa mrežom. Ovo će uvelike olakšati povezivanje IoT uređaja koji se oslanjaju na mobilne aplikacije koje traže ponovno unošenje lozinke mreže kako bi se mogle koristiti. Također kod WPS-a bilo tko može pritisnuti gumb na usmjerivaču i povezati neki uređaj s mrežom dok je kod EasyConnecta takav ishod nemoguć jer je uvjet za spajanje novog uređaja na mrežu povezanost pametnog mobilnog telefona sa mrežom pomoću kojega će se takvi uređaji povezati. Trebati će neko vrijeme da WPA3 usmjerivači, računala te mobilni uređaji zauzmu tržište. Postoji mogućnost da će neki od postojećih uređaja koji ne podržavaju WPA3 protokol dobiti potrebna ažuriranja kako bi omogućila WPA3 sigurnost.

2.3. Osvrt na sigurnost koja se analizira u ovom radu

Rješenje u ovom radu je samostalno te pruža pogled na sveobuhvatni proces ostvarivanja prava neovlaštenog pristupa i traženja slabosti u mreži, nakon čega se prikazuju konkretne prijetnje prema korisnicima mreže. Sve je opisano teoretski i prikazano na modelu. U radu se koriste javno dostupni alati i programi otvorenog koda koji dolaze uz Kali Linux operacijski sustav. Za potrebe rada koristila se virtualna mašina u kojoj je instaliran operacijski sustav koji je ranjiv na daljinsko izvršavanje koda. Osim toga koristi se i računalo koje koristi Windows 10 operacijski sustav koji je aktualiziran na najnoviji sigurnosnu verziju te će se na njemu također pronalaziti i pokazivati ranjivosti. Za razliku od drugih radova koji su posvećeni točno određenom alatu ili sigurnosnom dijelu, ovaj rad kombinira više različitih programa i alata te naglasak stavlja na opisivanje sigurnosnih propusta i prijetnji prema korisnicima bežične mreže.

3. NAPADI ZA OSTVARIVANJE PRISTUPA BEŽIČNOJ MREŽI

U ovome poglavlju teoretski su opisani načini i metode za realizaciju napada ostvarivanja pristupa bežičnoj mreži. Glavni princip je uhvatiti proces rukovanja (engl. Capture handshake) između klijenta i pristupne točke što se postiže napadom deautentifikacije, kako bi kasnije isti dešifrirali ili koristili u svrhe društvenog inženjerstva.

3.1.Napad deautentifikacije

Napad će izbaciti korisnika mreže sa bežične mreže na koju je povezan. Napadač šalje pakete za deautentificiranje prema pristupnoj točki i govori koga da izbaci sa mreže. Ovakvi paketi se nalaze unutar IEEE 802.11 standarda, kako bi se neautorizirani uređaj deautentificiralo s mreže. Loš dizajn je omogućio da bilo tko može izbaciti korisnika neke mreže sa nje same, čak ako napadač i nema pristup toj istoj mreži. Napadač koristi ovakav napad kako bi korisniku uskratio pristup mreži ili kao dio drugog napada kako bi na primjer uhvatio proces rukovanja u tri koraka između klijenta i pristupne točke, kreirao veliku količinu prometa u svrhu pronalaženja WEP ključa ili jednostavno pokušava klijenta prevariti da se spoji na napadačevu mrežu preko lažne pristupne točke. Za ovaj napad koristi se alat Aircrack-ng koji predstavlja cjelovit paket alata za procjenu sigurnosti bežične mreže[6]. Fokusira se na različita područja bežične sigurnosti. Neki od njih su nadgledanje, hvatanje paketa i izvoz podataka u tekstualne datoteke za daljnju obradu pomoću alata nezavisnih proizvođača. napad deautentifikacije, kreiranje lažne pristupne točke. Svi se alati koriste pomoću pozivanja naredbe što omogućuje kreiranje brojnih skripti. Mnogo GUI-ja iskoristilo je ovu značajku. Dizajniran je prvenstveno za Linux, ali može se koristiti i na Windows, OS X, FreeBSD, OpenBSD, NetBSD, kao i Solaris. Za korištenje aircrack-nga potrebno je imati bežičnu karticu koja omogućuje slanje paketa kao i mogućnost rada u načinu osluškivanja[7].

3.2.Kriptografski napadi

Prema [8], kriptografija je znanstvena disciplina o metodama za slanje poruka (informacija) u obliku koji će biti razumljiv samo onima koji ih znaju pročitati, odnosno samo onima kojima su namijenjene. Kriptografija omogućava očuvanje tajnosti poruka između pošiljatelja i primatelja čak i kada se koriste nesigurne veze koje su dostupne trećim osobama. Kriptografija se stoljećima primjenjivala za osiguravanje tajnosti pretežito vojne i diplomatske komunikacije. Ispočetka su se postupci kriptiranja svodili na razmještanje znakova teksta ili na njihovu zamjenu. U današnje vrijeme gdje se razmjene poruka putem globalnih komunikacijskih mreža odvijaju svakodnevno kriptografija nalazi svoju široku upotrebu. Ona se bavi podatcima u digitalnom obliku, a postupci kriptiranja i dekriptiranja matematičke su naravi i provode se uz pomoć računala. Algoritmi koji

iz nešifriranog teksta izračunavaju šifrirani tekst i obrnuto obično se koriste parametarskim matematičkim funkcijama.

3.2.1.Napad rođendana (Birthday attack)

Prema [9], dolazi od paradoksa rođendana koji glasi: „Ukoliko se u jednoj prostoriji nalaze najmanje 23 osobe, vjerovatnost da dvije ili više osoba (bez obzira na godinu rođenja) imaju na isti dan rođendan, je veća od 50%“ Na 70 nasumičnih osoba postotak podudaranja datuma rođendana dvije osobe iznosi 99.9%.

3.2.2.Poznati izvorni tekst i šifrirani tekst

Ako napadač zna izvorni tekst i šifrirani tekst iste riječi ili čitavog teksta može pomoću tih informacija doći do ključa kojim su šifrirani. Ako je izvorna rečenica „FERIT je fakultet u Osijeku.“, a kriptirani tekst „GRTOZ kr gsličzrz i Pdokrli.“, može se zaključiti da je ključ u ovom slučaju pomicanje slova za jedno slovo na tastaturi u desno. F=G, E=R ,R=T, I=O, T=Z… Prema tome napadač može koristiti ovaj ključ kako bi dešifrirao ostale rečenice(pakete) za koje želi saznati izvorno stanje. Postoje alati koji koriste matematičke algoritme kako bi dobili izvorni tekst što uvelike olakšava pronalazak izvornog teksta [10].

3.2.3. Tablice duge

Tablica duge (engl. rainbow table) je unaprijed izračunata tablica za predmemoriranje izlaza kriptografskih hash funkcija, obično za probijanje hasheva lozinki. Hash funkcija je bilo koja funkcija koja se može koristiti za mapiranje podataka proizvoljne veličine u vrijednosti fiksne veličine. Vrijednosti koje vraća hash funkcija nazivaju se hash vrijednosti, hash kodovi, sažetci ili jednostavno hashi. Praktičan primjer je prostorno-vremenskog kompromisa, koji koristi manje vremena za računalnu obradu i više prostora za pohranu od napada sirovom snagom koji izračunava hash za svaki pokušaj, ali više vremena za obradu i manje prostora za pohranu od jednostavne funkcije izvođenja ključa s jednim unosom po hashu. Tablica koja ima hash za svaku lozinku veličine od 1 do 8 znakova gdje se koriste svi mogući znakovi velika i mala slova, brojevi, simboli zauzima oko 550GB prostora [11].

3.2.4.Napad sirovom snagom (engl. brute-force attack)

Napad sirovom snagom jedini je 100% učinkovit, ali ujedno i najsporiji oblik napada. Iz samog imena „sirova snaga“ može se zaključiti da vrijeme napada ovisi o procesorskoj snazi i količini računalnih resursa. Sam napad može se definirati kao metoda pokušaja-pogreške svih mogućih kombinacija znakova kako bi se pronašao hash koji odgovara tim znakovima. Vrijeme i resursi potrebni za rješavanje problema ovom metodom rastu proporcionalno broju mogućih lozinki. Zbog

toga se algoritam napada često optimizira kako bi se smanjio broj mogućih lozinki. Strategija napada bi trebala biti takva da se kao slijedeći pokušaj uzima lozinka za koju je vjerojatnost rješenja najveća, uzevši pritom u obzir neuspjeh prethodnih pokušaja. Drugim riječima, ako su lozinke donekle grupirane, svaki novi pokušaj treba biti što dalje od prethodnih ili obrnuto, ako su rješenja distribuirana jednoliko, onda je optimalna strategija odabira lozinke što bližeg prethodnoj. Ovakva vrsta napada u prošlosti je bila jako neučinkovita zbog vremenske kompleksnosti, no s vremenom došlo je do curenja podataka o velikom broju korisničkih lozinki koje su sada dostupne na internetu u obliku rječnika te ih se upravo ovom metodom može koristiti u svrhu napada. Također razvili su se i pomoćni alati koji uvelike mogu smanjiti vrijeme pronalaska na način da kreiraju posebne liste riječi. Konkretan primjer napada kao i kreiranje personalnih rječnika uz pomoć dva različita alata opisani su i primjerom pokazani u petom poglavlju [12].

3.2.5.Napad rječnikom

Napad rječnikom (eng. dictionary attack) je tehnika za probijanje šifri kod koje se pokušava pronaći tražena zaporka ili tajni ključ uzastopnim isprobavanjem velikog broja riječi ili kombinacija riječi. Napad rječnikom je varijacija napada sirovom snagom kod koje je broj mogućih lozinki smanjen *na način da se ne isprobava svaka moguća kombinacija znakova nego se koriste kombinacije koje imaju određeno značenje na nekom jeziku. Veća vjerojatnost je da lozinka predstavlja neki niz znakova koji ima značenje i samim time je lakše pamtljiva, nego neki drugi niz znakova koji nema nikakvo značenje te je zbog toga težak za zapamtit. Riječi za napad listom riječi se uzimaju iz rječnika koji su dostupni na Internetu i ne predstavljaju rječnike u klasičnom smislu određenog jezika već uključuju velik broj najvjerojatnijih riječi, tj. riječi koje se najčešće koriste u zaporkama [13].

3.3. Društveno inženjerstvo

Društveno inženjerstvo je prema [14] tehnika manipulacije koja iskorištava ljudske pogreške za dobivanje privatnih podataka, pristupa ili dragocjenosti. Kao takvi, napadi socijalnog inženjeringa posebno su korisni za manipuliranje ponašanja korisnika.

3.3.1. Zli blizanac

Zli blizanac (eng. Evil twin) lažna je bežična pristupna točka koja se čini legitimnom, ali je postavljena za prisluškivanje bežičnih komunikacija. Ova vrsta napada može se koristiti za krađu lozinki nepažljivih(naivnih) korisnika, bilo praćenjem njihovih veza ili krađom identiteta, što uključuje postavljanje lažne web stranice i namamljivanje korisnika da ostvare pristup s istom [15]. Na slici 3.1 prikazana je slikovita shema napada u praksi na kojoj je jednostavno shvatiti

kako napad funkcionira. Napadač dolazi u domet signala mreže klijenta kojeg želi nagovoriti na spajanje na njegovu mrežu. Ime lažne pristupne točke identično je onoj sa kojom je klijent trenutno povezan.

Slika 3.1. *Prikaz zli blizanac napada*

Napadom deautentifikacije prekida se povezanost klijenta i mreže na koju je bio spojen. Mreža se i dalje opterećuje velikom količinom paketa te se postaje nemoguće spojiti na istu. Klijent u postavkama za spajanje na mrežu uočava da postoji mreža sa istim imenom i boljim signalom od ove druge vidljive s kojom je prethodno bio povezan(u nekim slučajevima to je jedina mreža koju može vidjeti). Prilikom pokušaja spajanja na lažnu pristupnu točku klijent će morati predati ispravnu lozinku. Jednom predana lozinka uspoređuje se sa prethodno uhvaćenim hashom od prave mreže, te ukoliko je ona ispravna, napad se obustavlja te se klijent spaja na mrežu na kojoj je prethodno bio povezan. Ukoliko je unesena kriva lozinka klijentu se vraća poruka o neispravnom unosu lozinke. Model ovog napada detaljno je razrađen i prikazan u poglavlju 5.

4.MODEL NAPADA NA WPA I WEP MREŽU

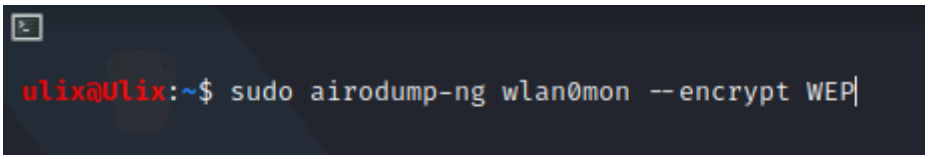
U ovome poglavlju opisan je način hvatanja procesa rukovanja kod WPA/WPA2 mreže te ostvarivanje pristupa WEP mreži uz pomoć alata aircrack-ng koji je detaljno opisan u potpoglavlju 3.2.

4.1.Ostvarivanje pristupa WEP mreži

Kao u navedenom potpoglavlju 4.2 bežično sučelje treba staviti u način rada osluškivanja.

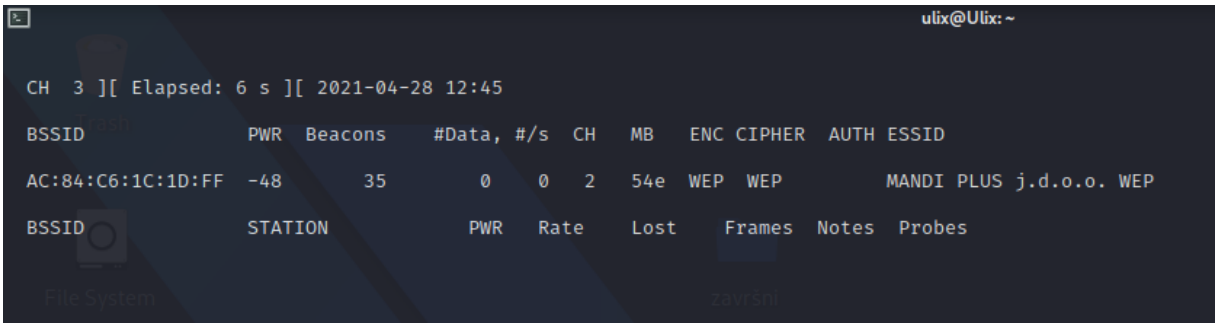
4.1.1. Osluškivanje okoline

Naredbom sudo airodump-ng wlan0mon –encrypt WEP će skenirati okolinu u potrazi za paketima koji su zaštićeni WEP enkripcijom, vraćajući ime i podatke o mreži koja koristi tu vrstu zaštite.



Slika4.1. *Naredba za osluškivanje*

Slika 4.9 prikazuje pronađenu mrežu „MANDI PLUS j.d.o.o. WEP“ koja koristi WEP enkripciju. Iz povratnih rezultata vidljiv je BSSID pristupne točke, kao i kanal na kojemu radi. Pomoću tih informacija u sljedećem koraku specificira se meta.

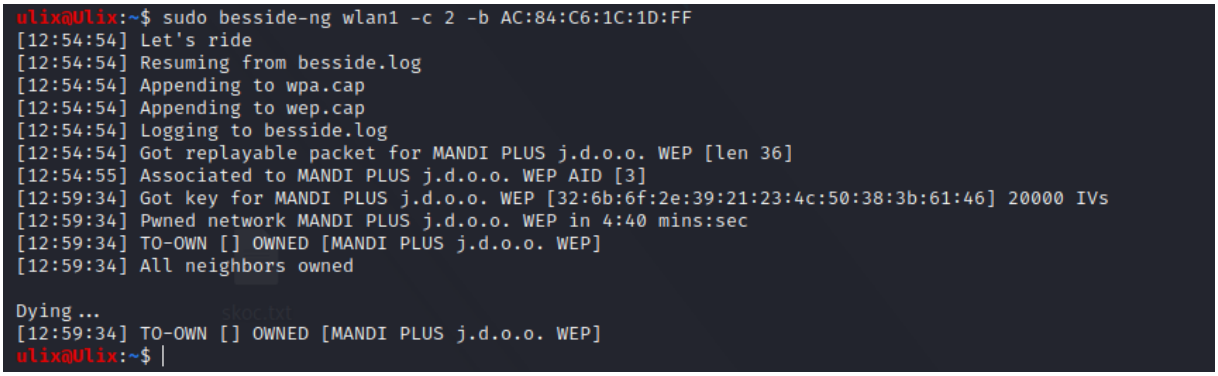


Slika4.2. *Odziv osluškivanja*

4.1.2. Slanje IV paketa

Iz slike 4.10 vidljiva je naredba za napad. Besside-ng wlan 1specificira sučelje koje će se koristiti za napad, -c 2 specificira kanal broj 2, te -b AC:84:C6:1C:1D:FF BSSID koji se napada. Prilikom aktivacije napada IV paketi se šalju samo prema ovoj mreži. Besside-ng će slati velike količine IV paketa kako bi sakupio dovoljnu količinu informacija uz pomoću kojih će dešifrirati lozinku mreže. Na poslanih 20000 IV paketa program je uspio pronaći ključ mreže(detaljnije opisano u

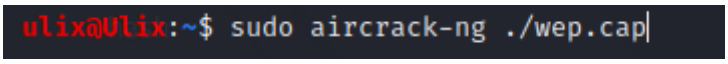
potpoglavlju 2.2.1. Postupak je trajao svega 4 minute i 40 sekundi. Mreža je koristila 128-bitnu zaštitu.



Slika4.3. *Podatci o napadu na WEP mrežu*

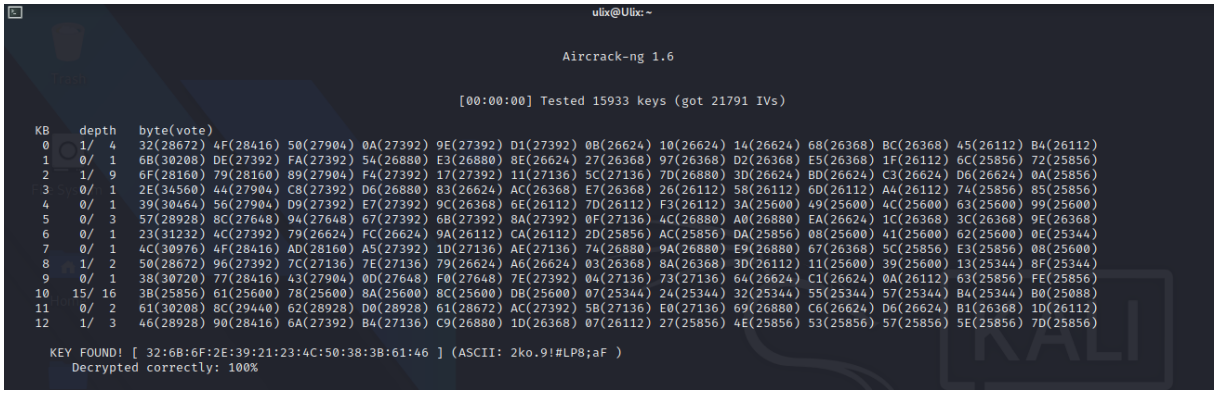
4.1.3. Dobivanje lozinke mreže

Ključ mreže zapisan je u heksadecimalnom obliku. Kako bi se heksadecimalni zapis prebacio u ASCII obliku koristi se alat aircrack-ng.



Slika 4.4. *Naredba za pretvorbu iz heksadekadskog u dekadski*

Naredbom za pretvorbu heksadecimalni rezultat prebacuje se u ASCII zapis. Postupkom dešifriranja iz heksadekadskog oblika dobiven je ASCII zapis lozinke koja je prema današnjim standardima vrlo jaka zbog korištenja velikih i malih slova, brojeva te dijakritičkih znakova i simbola. Na slici 4.12 vidi se koji je pristupni ključ mreži.



Slika 4.5. *Prikaz pretvaranja Naredba za pretvorbu iz heksadekadskog u dekadski*

Lozinka se sastojala od ukupno 13 različitih znakova: 2ko.9!#LP8;aF. Sadržaj lozinke smatra se kao vrlo jak zbog duljine i korištenja svih vrsta znakova, no slabost u ovome slučaju nije lozinka

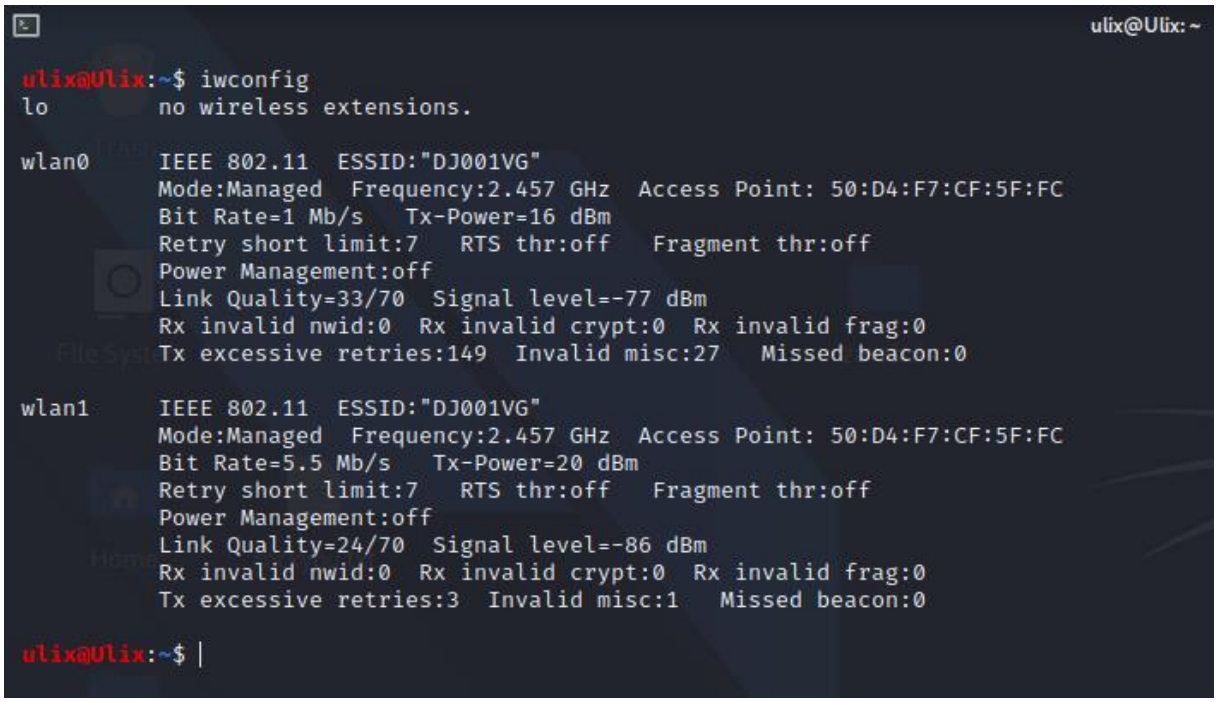
već loše napisan algoritam koji se ovim primjerom eksploatirao i rezultirao dobivanjem lozinke mreže.

4.2. Napad na WPA/WPA2

U nastavku rada prikazan je primjer napada na bežičnu mrežu koja je zaštićena protokolom WPA2. Svrha napada je uhvatiti proces rukovanja između klijenta i pristupne točke kako bi se kasnije nekom od metoda isti iskoristio za ostvarivanje pristupa samoj mreži. Ideja je prekinuti vezu između klijenta i pristupne točke što će rezultirati ponovnim pokušajem povezivanja na mrežu. Pri tom povezivanju između klijenta i pristupne točke trebati će se uspostaviti proces rukovanja koji će se u ovom modelu uhvatiti kao hash datoteka.

4.2.1. Stavljanje sučelja u način rada osluškivanja

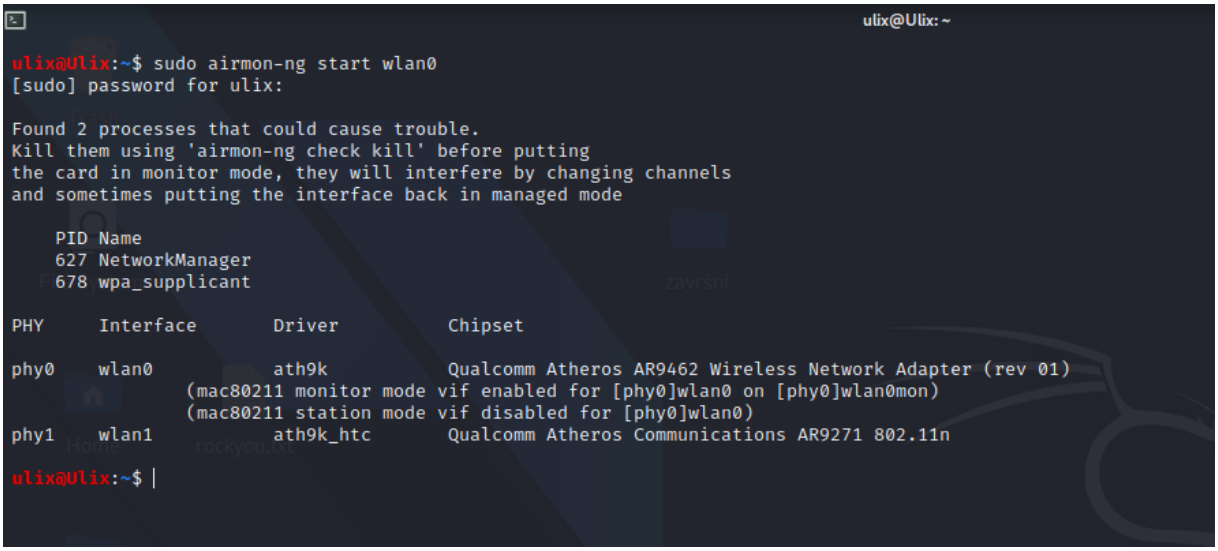
Najprije je potrebno provjeriti koje bežične kartice(sučelja) su dostupne, a to se provjerava naredbom iwconfig Slika 4.1. Iz pretrage je vidljivo da su dostupna dva sučelja. Oba sučelja se nalaze u upravljačkom načinu rada, povezana su sa bežičnom mrežom DJ001VG.



Slika 4.6. *Pretraživanje dostupnih bežičnih sučelja*

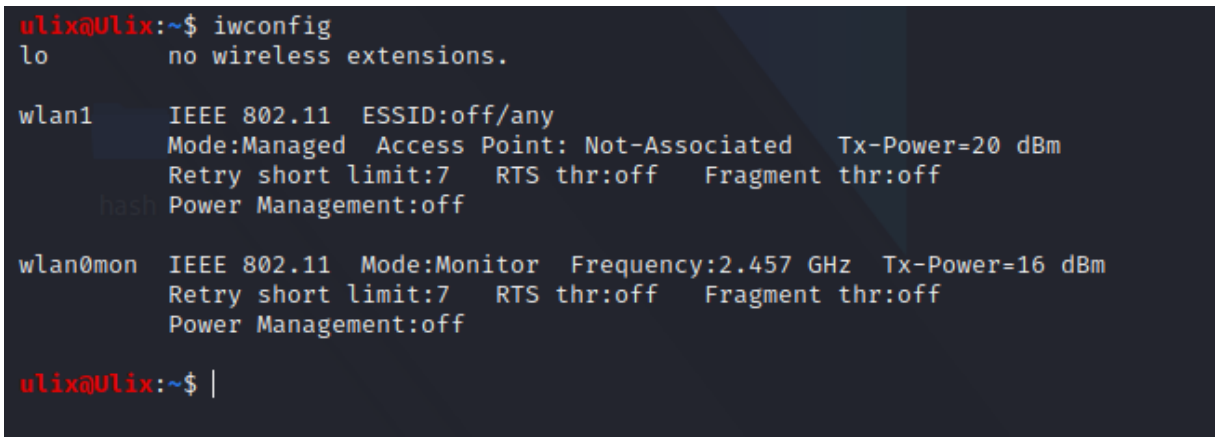
Za pripremu napada potrebno je sučelja staviti u način rada osluškivanja(monitor mode) kako ne bi imala interakciju sa svojim prometom te kako bi bilo u stanju hvatati pakete. Za potrebe ovog napada dovoljno je koristiti jedno sučelje. Naredbom 'airmon-ng start wlan0' sučelje se prebacuje u način rada osluškivanja. Svi procesi koji se odvijaju na bilo kojem od sučelja su prekinuti kako

ne bi došlo do smetnji ili ponovnog povratka u upravljački način rada. Iz slike 4.2 vidljivo je da su svi procesi prekinuti te da je sučelje wlan0 prebačeno u način rada osluškivanja.



Slika 4.7. *Stavljanje bežičnih sučelja u način osluškivanja*

Ponovnim korištenjem naredbe iwconfig slika 4.3 provjerava se jesu li bežična sučelja uspješno prebačena u način rada osluškivanja. Iz slike je vidljivo da više nisu povezana sa bežičnom mrežom te da se nikakvi procesi ne odvijaju. Sučelje wlan0 stavljeno je u način rada osluškivanja (engl. monitor mode), dok je sučelje wlan1 ostalo u upravljačkom (engl. manage mode) ali su mu svi procesi ugašeni.



Slika 4.8. *Provjera stanja bežičnih sučelja*

4.2.2. Osluškivanje okoline

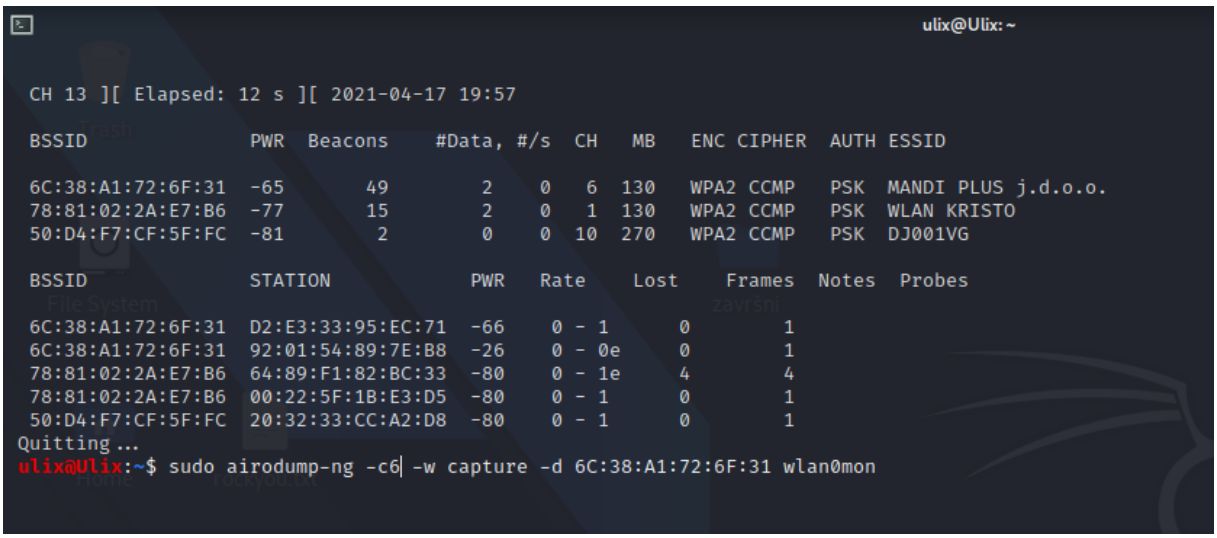
Kada su pripreme za napad završene, potrebno je osluškivati okolinu, kako bi se dobile informacije o dostupnim bežičnim mrežama u blizini. Ovim postupkom konstantnom promjenom kanala pokušavaju se pronaći sve pristupne točke u blizini(svaka mreža koristi drugi kanal). Jednom kada

je ciljana mreža vidljiva postupak osluškivanja može se zaustaviti. U daljnjem toku napada iz ovoga se može očitati informacija o broju kanala na kojem se mreža nalazi, informacije o klijentima, kao i njen BSSID.

```
ulix@Ulix:~$ sudo airodump-ng wlan0mon
```

Slika 4.9. *Naredba za osluškivanje bežičnog prometa u okolici*

Kratkim pregledom iz slike 4.5 vidljive su tri aktivne bežične mreže u dometu bežičnih sučelja. U ovom primjeru mreža koja se koristi za demonstraciju napada je u vlasništvu tvrtke MANDI PLUS j.d.o.o. BSSID označava pristupnu točku. Pristupne točke konstantno emitiraju svjetlosne signale(engl. beacons) kako bi naglasile svoju prisutnost. Stanice (engl. station) su klijenti pristupne točke, te je vidljivo kojoj pristupnoj točki pripadaju. Naredbom „airodump-ng -c6“ se postavlja osluškivanje na kanalu broj 6 jer taj kanal koristi ciljana mreža, „-w capture“ zapisuje proces rukovanja u datoteku imena „capture“. Naredbom „-d BSSID“ filtrira se prikaz podataka koji je bitan za pristupnu točku koja se napada. „wlan0mon“ označava sučelje koje će obavljati zadatak.

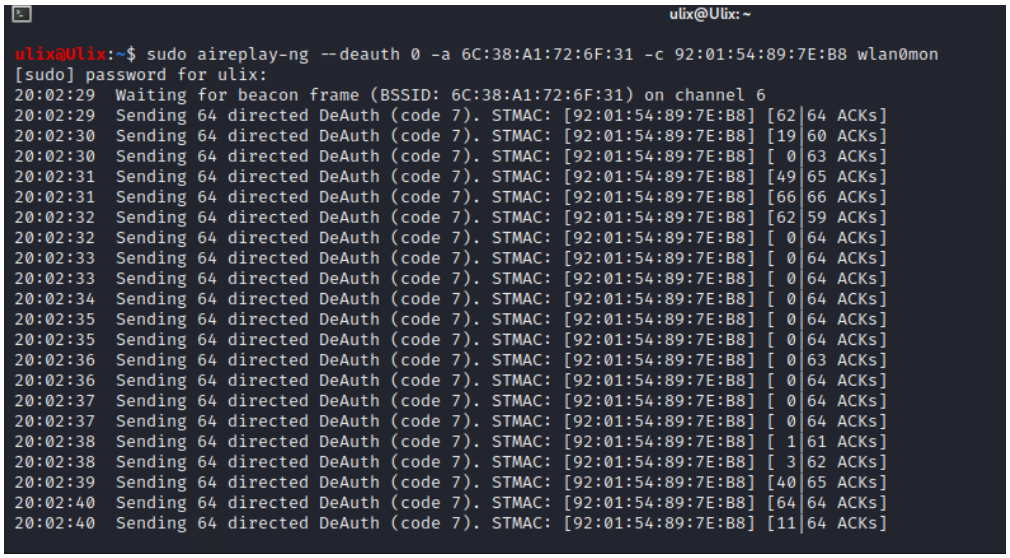


Slika 4.10. *Osluškivanje bežičnog prometa u okolici*

4.2.3. Slanje paketa za deautentifikaciju korisnika

U drugome terminalu pokreće se postupak slanja paketa za deautentificiranje korisnika kao što je prikazano na slici 4.6. Proces deautentificiranja koristi se iz razloga što bi samo osluškivanje mreže trajalo sve dok god se klijent ponovno ne pokuša povezati sa mrežom. Ideja ovoga je ubrzati taj proces slanjem paketa nekom od klijenata kako bi ga se izbacilo sa mreže, pa kada se pokuša ponovno povezati, bežična kartica koja je u načinu osluškivanja mreže može uhvatiti proces

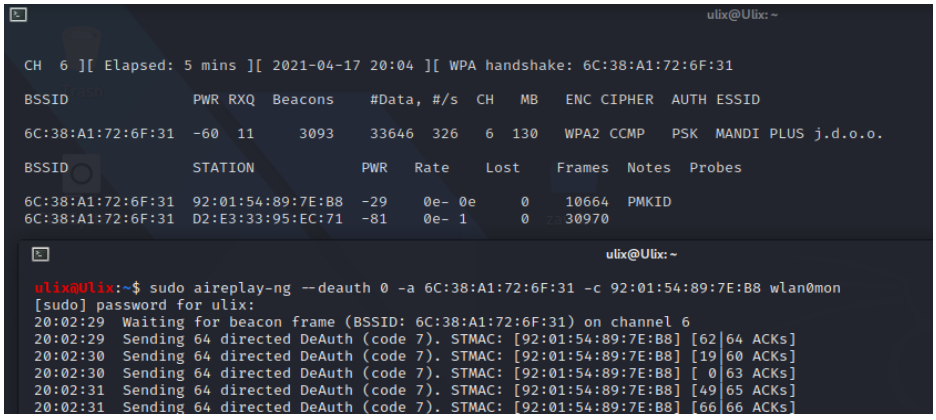
rukovanja i spremiti ga u hash datoteku kako bi kasnije istu bilo moguće iskoristiti za primjenu napad sirovom snagom(ili napada rječnikom). Iz slike 4.6 vidi se da naredbom „aireplay-ng - -deauth 0 -a 6C:38:A1:72:6F:31 -c 92:01:54:89:7E:B8“ konstanto se šalju paketi za deautentifikaciju u skupinama do 64 paketa prema MANDI PLUS j.d.o.o. pristupnoj točki i prema točno određenom klijentu mreže(ako se ne specificira, paketi se šalju svim klijentima koji su trenutno povezani sa mrežom).



Slika 4.11. *Slanje paketa za deautentifikaciju korisnika sa mreže*

4.2.4. Hvatanje procesa rukovanja

Slika 4.7 prikazuje uhvaćeni WPA handshake. Klijent je uspješno izbačen sa mreže i prilikom njegovog ponovnog pokušaja spajanja na mrežu uhvaćen je proces rukovanja koji je pohranjen u capture-02.cap datoteku. Datoteka se kasnije može koristiti u svrhu offline napada sirovom snagom ili napad rječnikom, za koji nije potrebno biti u dometu signala mreže.



Slika 4.12. *Uhvaćeni WPA handshake*

5. UPOTREBA KRIPTOGRAFSKIH MODELA NAPADA I DRUŠTVENOG INŽENJERSTVA NA PRETHODNO UHVAĆENI PROCES RUKOVANJA

U ovome poglavlju prikazat će se kreiranje dva različita rječnika uz pomoć 2 različita alata. Prvi alat Crunch [16] omogućuje kreaciju rječnika prema zadanim parametrima, dok drugi alat Cupp [17] traži unos osobnih podataka mete, te će uz pomoć unesenih riječi generirati rječnik sa više tisuća riječi. Na kraju će se prikazati i primjer društvenog inženjerstva koji će od korisnika tražiti unos ispravne lozinke.

5.1. Izrada rječnika

U ovom primjeru koristi se alat Crunch [16]. Crunch je program koji generira liste riječi prema zadanom skupu ASCII znakova. Može napraviti listu riječi prema kriteriju koji mu je zadan, te istu pohraniti u datoteku ili drugi program. Parametri koje zahtjeva su minimalna dužina niza znakova, maksimalna dužina niza znakova, te skup znakova koji se želi koristiti, ukoliko je skup nedefiniran, koristit će se svi znakovi za taj znak u riječi. Ovaj alat napadaču omogućuje kreiranje liste riječi po njegovom osobnom izboru. Ukoliko je poznat dio lozinke vrlo jednostavno može se saznati preostali dio. Na slici 5.1 prikazan je postupak kreiranja rječnika koji ima točno specificirani dio riječi „skocibusic“ te su preostala 4 znaka nepoznata. Naredbom „crunch 14 14“ specificira se duljina riječi unutar rječnika. Prvi broj označava minimalnu duljinu riječi, a drugi maksimalnu. Ovim postupkom se veličina riječi svela na 14 znakova. Znakom '%' specificiran je skup brojeva {0,1,2,3,4,5,6,7,8,9}. Znakom '^' specificiran je skup svih dijakritičkih znakova {!“#$%&/()=?*+',.-;:_/|\~[]{}@<>,^ }

Naredbom „-o skoc.txt“ kreira se tekstualna datoteka imena „skoc“ oblika .txt u kojoj će se pohraniti svaka kreirana riječ.

```
ulix@Ulix:~$ crunch 14 14 -t 'skocibusic%%%^' -o skoc.txt
Crunch will now generate the following amount of data: 495000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 33000

crunch: 100% completed generating output
ulix@Ulix:~$
```

Slika 5.1. *Korištenje naredbe crunch*

Dakle pomoću naredbe „crunch 14 14 -t 'skocibusic%%%^' -o skoc.txt“ stvorena je lista od 33 000 riječi(svaka riječ veličine je 14 znakova) u par sekundi, a otprilike isto toliko vremena potrebo je da se svaka riječ iz liste usporedi sa uhvaćenim procesom rukovanja. Na slici 5.2 prikazane su neke od riječi koje su kreirane ovom metodom.

Slika 5.2. *Prikaz nekih generiranih riječi unutar liste*

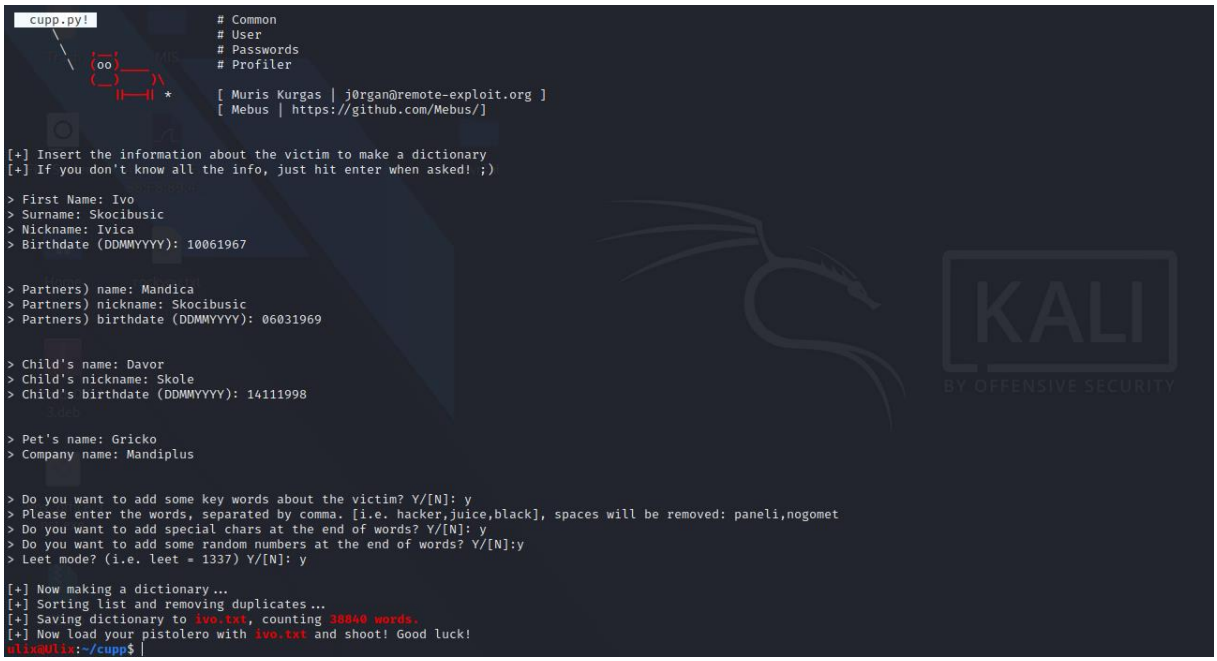
5.1.1. Napad sirovom snagom

Korištenjem aircrack-ng alata zadaje se kao prvi parametar uhvaćeni proces rukovanja, te kao drugi parametar lista riječi. Program će svaku riječ iz rječnika upotrijebiti kako bi pokušao pronašao točan ključ slika 5.3. U ovom slučaju ključ je pronađen za 17 sekundi te je program prije pronalaska točnog ključa imao 33985 pogrešnih pokušaja. Zbog ovakve brzine izvođenja koriste se offline napadi na prethodno uhvaćeni hash. Ako bi napadač išao direktno napasti mrežu putem napada sirove snage, previše vremena bi se gubilo na odgovor pristupne točke. Za 1 pokušaj autentifikacije na mrežu potrebno je 5 sekundi dok se ne dobije povratna informacija od pristupne točke o točnosti pristupnog ključa. Stoga bi ovakva vrsta napada u online obliku trajala minimalno 5*33000 sekundi, što iznosi 45 sati. U offline napadu za proći kroz cijelu listu riječi potrebno je 17 sekundi iz čega se može zaključiti da je ovakva vrsta napada brža otprilike 10 tisuća puta u odnosu na online napad. U prilog ovome ide i činjenica da za offline napad nije potrebno biti u dometu signala mreže, nego se napad može odviti na bilo kojoj lokaciji u bilo koje vrijeme.

Slika 5.3. *Prikaz napada sirovom snagom*

5.2. Izrada personaliziranog rječnika

U ovom primjeru koristi se alat Cupp -Common User Password Profiler **(**Profiler uobičajene korisničke lozinke). Najčešći oblik provjere autentičnosti kombinacija je korisničkog imena i lozinke ili zaporke. Snaga lozinke proporcionalna je poteškoćama u pogađanju ili razbijanju lozinke kriptografskim tehnikama ili automatiziranim testiranjem zamjenskih vrijednosti na temelju liste riječi. Slaba lozinka može biti vrlo kratka ili koristiti samo alfanumeričke znakove, što olakšava dešifriranje. Zbog toga je CUPP nastao i može se koristiti u situacijama poput testova legalne penetracije ili forenzičkih istraga zločina. U slijedećem primjeru kreira se lista riječi na temelju osobnih podataka žrtve poput rođendana, nadimka, adrese, imena kućnog ljubimca ili uobičajene riječi koje stvaraju sumnju kod napadača [17]. Iz slike 5.4 vidljivi su parametri koji su uneseni kako bi se kreirao rječnik.



Slika 5.4. *Unos osobnih informacija žrtve(ključnih riječi) u program.*

Odgovaranjem na pitanja o imenu, prezimenu, povezanim osobama žrtve, te ključnim riječima koje napadač smatra bitnim (nije ograničen broj ključnih riječi) kreira se rječnik od 38 840 riječi u nekoliko sekundi.

0v1!!&	0vI_967610	1v0Iv1c4$*!	Gricko@@	acidnam_606	r0v4D998141
0v1!!'#'	0vI_967667	1v0Iv1c4$*$	Gricko@@!	acidnam_63	r0v4D998144
0v1!!*	0vI_96767	1v0Iv1c4$*%	Gricko@@$	acidnam_669	r0v4D998198
0v1!!@	0vI_967670	1v0Iv1c4$*&	Gricko@@%	acidnam_69	r0v4D9984
0v1!$!	0vI_9676706	1v0Iv1c4$**	Gricko@@&	acidnam_693	r0v4D99841
0v1!$$	0vI_9676710	1v0Iv1c4$*@	Gricko@@'#'	acidnam_696	r0v4D998411
0v1!$%	0vI_967676	1v0Iv1c4$@	Gricko@@*	acidnam_969	r0v4D998414
0v1!$&	1001967	1v0Iv1c4$@!	Gricko@@@	acivI!	r0v4D998498
0v1!$'#'	1001967	1v0Iv1c4$@$	Gricko_1990	acivI!!	r0v4D99898
0v1!$*	10061967	1v0Iv1c4$@%	Gricko_1991	acivI!!!	r0v4D998981

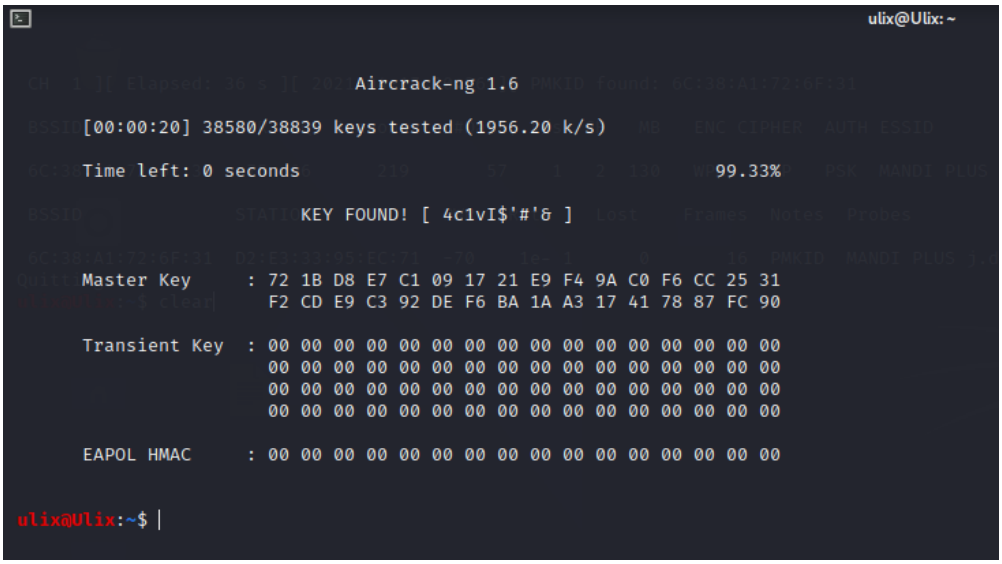
Slika 5.5. *Prikaz nekih generiranih riječi unutar liste rječi*

Čovjek neke brojeve može vidjeti kao slova zbog samog izgleda. Zbog toga se prilikom kreiranja rječnika koristio tako zvani leet(ili „1337“) mode. Naprimjer zamjena za slovo „i“ može biti broj 1, slovo „S“ može biti broj 8 ili znak američkog dolara $. Računalu su to sasvim različiti znakovi prema ASCII tablici i ono samo ne može vidjeti moguću sličnost ali ljudsko oko vidi, što znači da veliki broj ljudi prilikom kreiranja lozinke, kako bi samu učinili kompleksnijom te istovremeno lako pamtljivom koristi simbole slične slovima. U gore prikazanim riječima program je određena slova zamjenjivao odgovarajućim znakovima i brojevima. Primjer riječi acidnam_606, predstavlja obrnutu riječ „mandica“ a 606 datum rođenja, na drugim mjestima u rječniku program koristi leet

mode r0v4D998141, zapravo predstavlja obrnuto napisano ime Davor u leet modu te je na kraju dodan datum rođenja. Ovakva vrsta rječnika daje odlične rezultate prilikom napada na bežičnu mrežu.

5.2.1. Napad sirovom snagom korištenjem personaliziranog rječnika

Korištenjem aircrack-ng alata slika 5.6 zadaje se kao prvi parametar uhvaćeni hash, te kao drugi parametar prethodno kreirana lista riječi. Program će svaku riječ iz rječnika upotrijebiti kako bi pokušao pronašao točan ključ. U ovom slučaju ključ je pronađen za 20 sekundi te je program prije pronalaska točnog ključa imao 38579 pogrešnih pokušaja. Ključ je bio 4c1vI$'#'&. 0brnuto napisano ime Ivica u leet modu plus šest dodatnih znakova.



Slika 5.6. *Prikaz bruteforce napada*

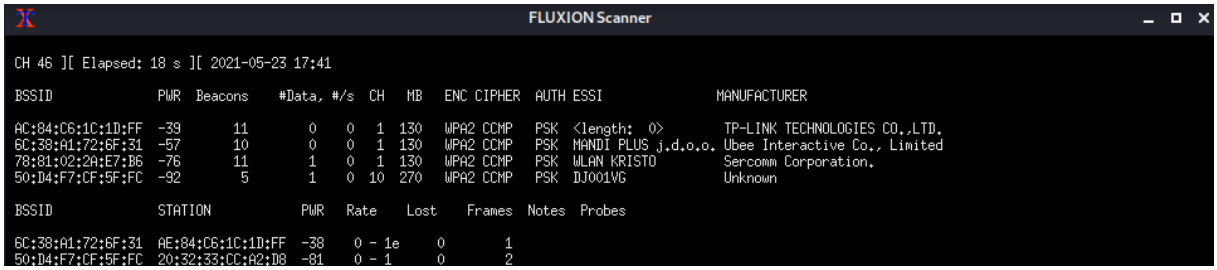
5.3. Model napada društvenog inženjerstva

U prethodna dva poglavlja prikazano je kreiranje različitih tipova rječnika pomoću 2 alata te napad sirovom snagom prethodno uhvaćeni proces rukovanja. Takvi napadi ovisno o težini lozinke mogu biti veoma vremenski zahtjevni. Stoga je lakše pitati korisnika za ispravnu lozinku, jer je on već zna. U donjem primjeru detaljno je prikazana takva vrsta napada.

5.3.1.Zli blizanac (engl. evil twin)

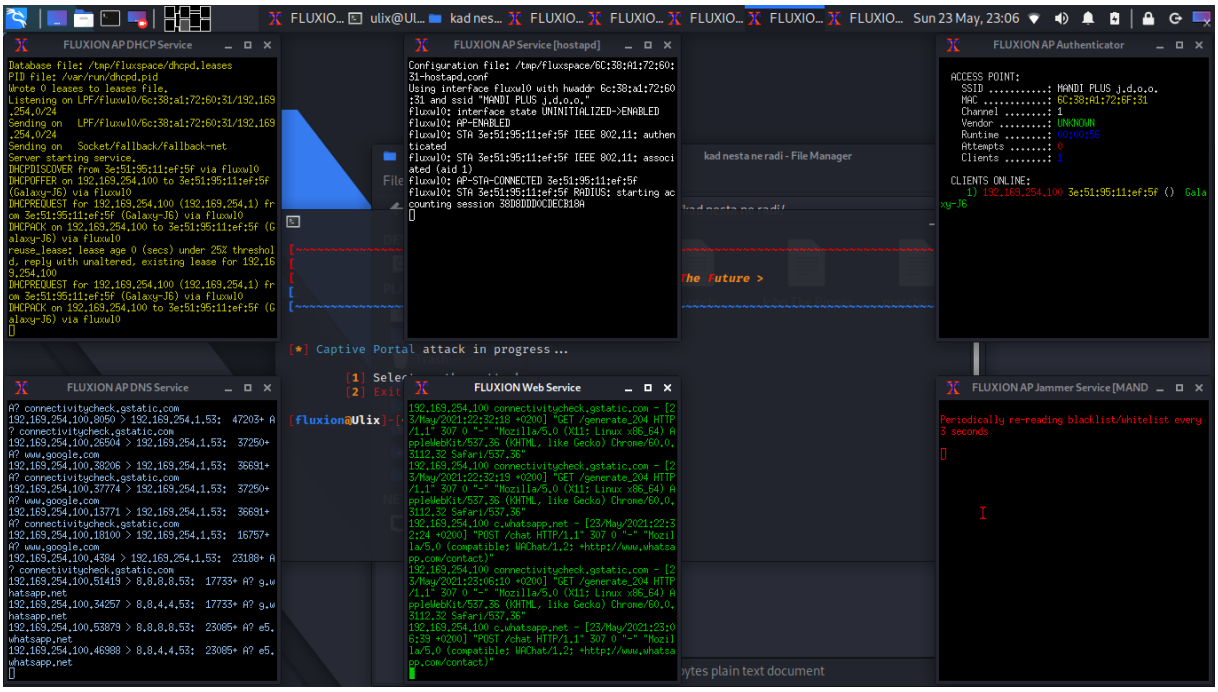
Zli blizanac predstavlja lažnu pristupnu točku koja nosi identično ime kao i pristupna točka sa kojom se želi ostvariti neovlašteni pristup. Za ovaj napad koristi se alat fluxion. Fluxion je alat za sigurnosnu reviziju i istraživanje socijalnog inženjeringa. Skripta pokušava dohvatiti WPA / WPA2 ključ s ciljne pristupne točke pomoću napada socijalnog inženjeringa (phishing-pecanje). Kompatibilan je s kali linuxom. Postavljanje napada Fluxion uglavnom je ručno, ali

eksperimentalni automatski način obrađuje neke od parametara za postavljanje napada[18]. Na slici 5.7 prikazano je skeniranje okoline u potrazi za dostupnim mrežama.



Slika 5.7. *Skeniranje okoline*

Fluxion Scanner koristi aricrack-ng program koji skenira sve mreže u rasponu 2.5 – 5 GHz. Pregledom okoline odabire se mreža MANDIPLUS j.d.o.o. Ukoliko ranije postoji uhvaćeni proces rukovanja ovaj korak u kojem se on hvata može se preskočiti. Proces rukovanja bitan je zbog toga što će se kasnije uhvaćena lozinka uspoređivati s hashom kako bi se potvrdila točnost iste. Captive Portal(zarobljeni portal) prikazan na slici 5.8 predstavlja proces koji istovremeno kreira lažnu pristupnu točku koja ima identično ime kao prava te DNS poslužitelj preusmjeravajući sve zahtjeve prema napadaču. Kreira web stranicu koja traži od korisnika da predaju svoju lozinku(WPA/WPA2 ključ). Također pokreće se napad deautentificiranja svih korisnika mreže, što rezultira uklanjanjem autentičnosti svih klijenata s originalne pristupne točke i privlači ih na spajanje na lažnu pristupnu točku, jer je nemoguće ponovno se spojiti na izvornu mrežu. U prozoru FLUXION AP Authenticator(gore desno), vidljivi su svi klijenti koji se trenutačno pokušavaju spojiti na lažnu pristupnu točku. Tu napadač može vidjeti podatke o uređaju kao što su vrsta uređaja(mobilni uređaj Samsung Galaxy J6), te MAC adresu uređaja.



Slika 5.8. *Pokretanje Captive Portala*

Iz slike 5.9 vidljivo je da klijent u postavkama bežičnog interneta ima vidljive dvije mreže s istim nazivom. Jedna predstavlja originalnu mrežu na koju se vrši napad deautentifikacije stoga klijent konstantno prima poruke o neispravnosti lozinke, a druga dostupna mreža je lažni klon za koju je također potrebna prijava.

Slika 5.9. *Prikaz Klijent se spaja na lažnu pristupnu točku*

Kako bi se povezao s tom lažnom pristupnom točkom klijent mora dati ispravan ključ (lozinku) svoje mreže. Kada klijent preda ključ on se uspoređuje sa prethodno uhvaćenim procesom

rukovanja te ako je on neispravan napad deautentificiranja se nastavlja te klijentu stiže poruka o netočno unesenome ključu. Napad će se automatski završiti nakon što se pošalje ispravan ključ. Ključ će se evidentirati i klijentima će se omogućiti ponovno povezivanje s ciljanom pristupnom točkom. Ovakva vrsta napada u praksi je puno efikasnija od klasičnog bruteforce napada. Kada se korisniku prekine povezanost sa mrežom on će se htjeti što prije povezati sa istom. Zbog emocija često neće ni gledati gdje što upisuje te će dati autentifikacijske podatke. Ovim modelom prikazana je takva realna situacija u kojoj je korisnik u želji da uspostavi vezu odao svoje podatke trećoj osobi. U odnosu na klasičan kriptografski napad bruteforce metodom ovo je puno zahvalnije jer se vrijeme izvođenja drastično smanjuje.

6. PRIJETNJE UNUTAR BEŽIČNE MREŽE

Kada je napadač ostvario pristup mreži, prema klijentu mogu biti usmjerene ozbiljne prijetnje. U ovom poglavlju teoretski ću obradit kako bi se mreža trebala ponašati u normalnim uvjetima te kako u kompromitiranim.

6.1. Alati i protokoli

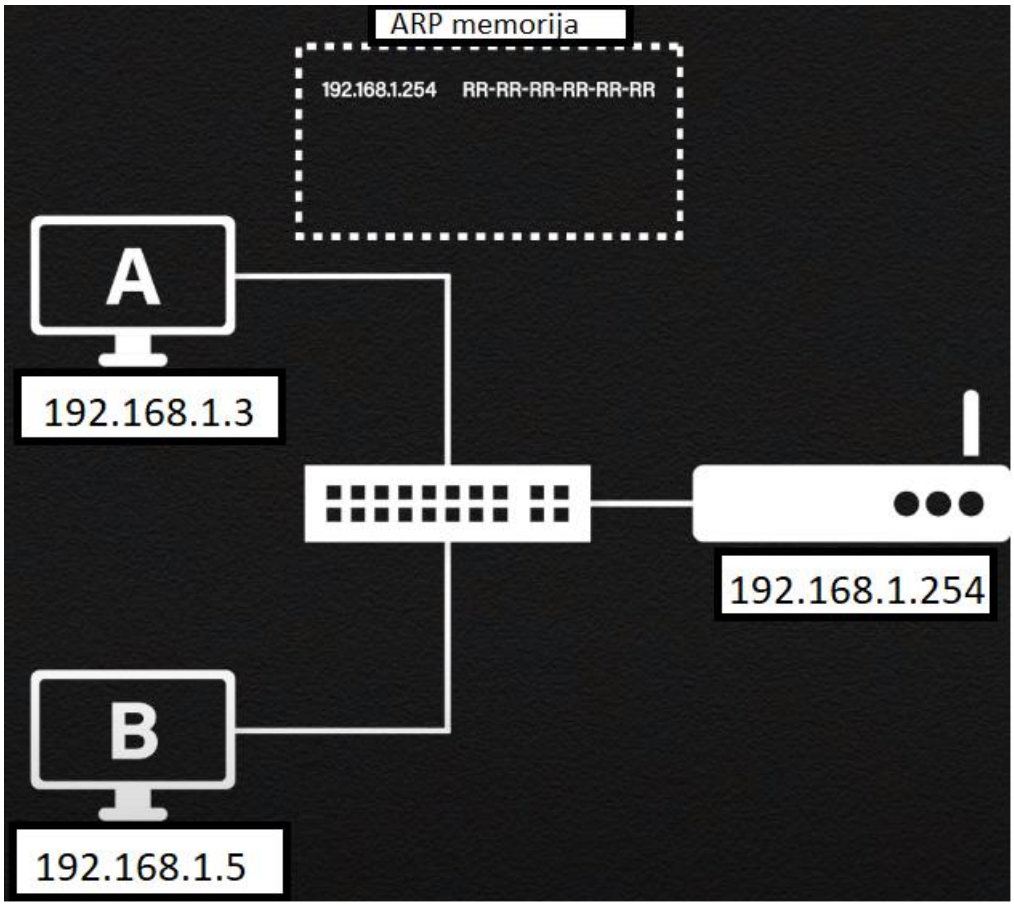
U ovome dijelu opisani su alati koji se koriste za skeniranje mreže i pretragu prometa, te je prikazano kako u teoriji dolazi do trovanja ARP memorije i ubacivanja lažnog DNS poslužitelj.

6.1.1.ARP protokol

ARP (engl. Address Resolution Protocol) je komunikacijski protokol kojim se dobiva fizička adresa na lokalnoj mreži iz poznate mrežne adrese. Najraširenija njegova primjena danas je na Ethernetu gdje se IP adrese povezuju s MAC adresama. ARP je također i naredba kojom se može pregledavati i mijenjati sadržaj tablice u operacijskom sustavu u kojoj se nalaze informacije dobivene ovim protokolom (tzv. ARP cache). ARP naredba omogućava mapiranje fizičke adrese poznate kao IPv4 adrese. Ova metoda uključuje slanje ARP zahtjeva. Uređaj za koji su potrebni podatci upućuje ARP zahtjev na mrežu, a lokalni uređaji odgovarju natrag ARP odgovorom koji sadrži njegovu IP-MAC adresu [19].

6.1.2.Komunikacija unutar mreže

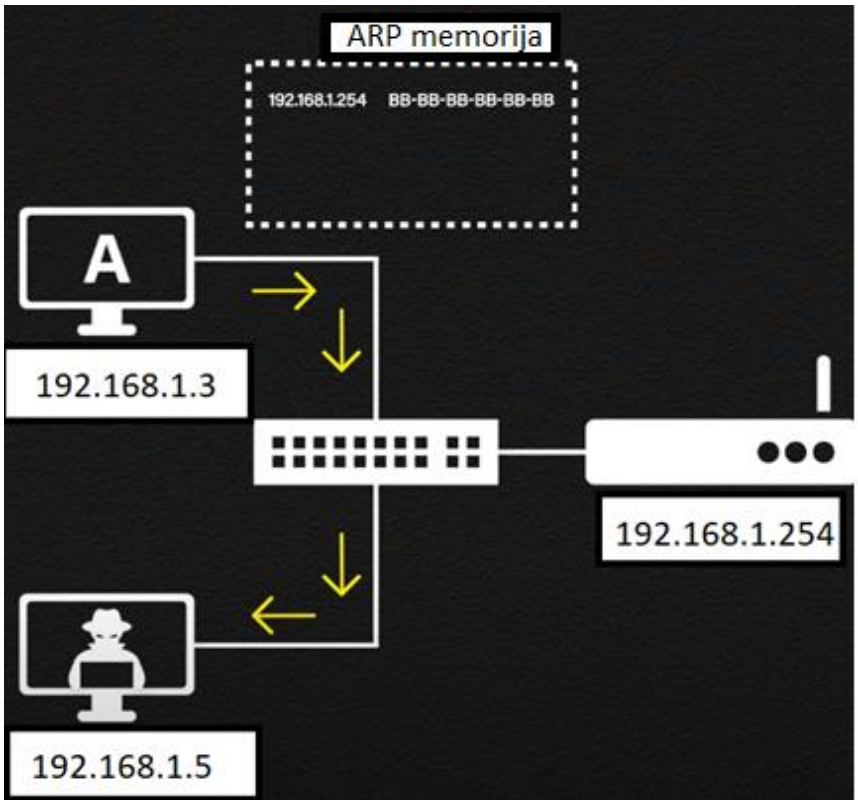
Recimo da u mreži postoje dva klijenta (A i B) te usmjernik kao što je prikazano na slici 6.1. Klijent A želi pronaći MAC adresu od zadane pristupne točke-usmjernika (192.168.1.254). Klijent A će stoga poslati poruku svim korisnicima mreže koja glasi „tko je 192.168.1.254 i koja je tvoja MAC adresa“. Poruka se šalje svim korisnicima mreže, u ovom slučaju klijent B (192.168.1.5) će vidjeti poruku i zaključiti da se ne odnosi na njega te će ju zanemariti. Usmjernik će zaključiti da je to on i poslati će odgovor u obliku svoje MAC adrese prema klijentu A. Klijent tu MAC adresu pohranjuje unutar ARP memorije uz IP adresu usmjerivača kako bi u budućnosti znao tko je usmjernik. Ako klijent A želi komunicirati sa nekim web poslužiteljom X, on će taj zahtjev slati preko usmjernika, odakle će on dalje prenositi poruku.



Slika 6.1. *Pohranjivanje MAC adrese unutar ARP memorije [20]*

6.1.3.Trovanje ARP memorije

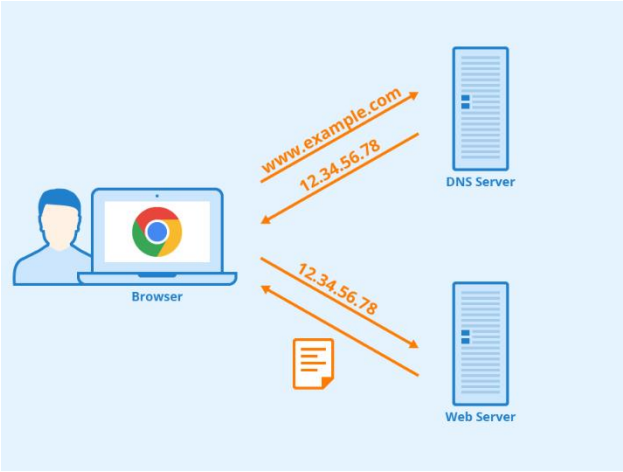
U teoriji komunikacija funkcionira na način kao što je opisano u poglavlju 6.1.2, međutim postoji velika mana u ovom procesu. Ako je u ovoj shemi klijent B napadač koji želi neovlašteno prisluškivati komunikaciju između klijenta i usmjernika on to može lako ostvariti. Napadač šalje specijalno izrađen ARP paket prema klijentu A kako bi se pravio da je on zapravo prava pristupna točka (usmjernik). Ideja je zatrovati klijentovu ARP memoriju, kako bi u sebi pohranila napadačevu MAC adresu kao zadanu pristupnu točku što se može vidjeti na slici 6.2. U ovom slučaju klijent A zamjenjuje MAC adresu usmjernika sa MAC adresom klijenta B(napadača). Sada ako klijent A želi ostvariti komunikaciju sa web poslužiteljom X, opet će pogledati MAC adresu usmjernika koju ima spremljenu u ARP memoriji. Podatke koje želi poslati poslužitelju prvo dolaze do napadača. Napadač s tim podatcima može napraviti bilo što prije nego ih proslijedi dalje do pravog usmjernika. Ovaj napad naziva se čovjek u sredini jer se napadač postavlja između komunikacije klijenta i usmjernika.



Slika 6.2. *Trovanje ARP memorije [20]*

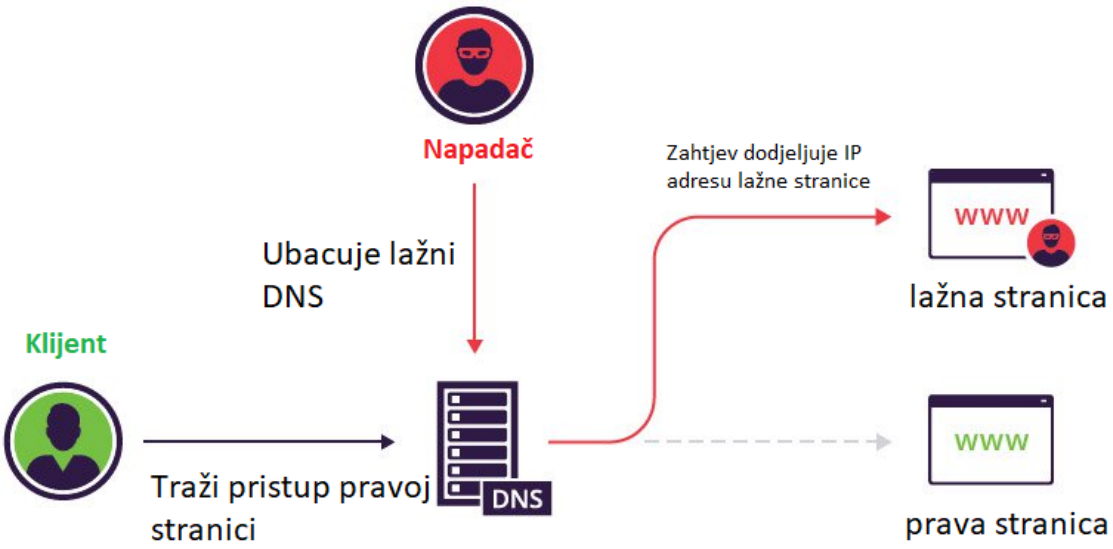
6.1.4. Kreiranje lažnog DNS servisa

DNS(Sustav imena domena) je servis koji primarno služi prevođenju odnosno mapiranju alfa-numeričkih naziva u IP adresu računala (engl. Forward Lookup), ali često i obratno (engl. Reverse Lookup). Njegova svrha je povezivanje ip adrese koja se nalazi u brojčanom obliku sa nečime što je ljudima lako pamtljivo. Lakše je zapamtiti facebook.com, nego IP adresu poslužitelja 69.171.250.35. Na slici 6.1 prikazan je rad DNS-a.



Slika 6.3. *Prikaz rada DNS-a*

Na slici 6.2 prikazana je shema DNS spoofinga koja se vrši zamjenom IP adresa pohranjenih na DNS poslužitelju onima pod nadzorom napadača. Jednom kad to učine, kad god korisnici pokušaju otvoriti određeno web mjesto, usmjeravaju se na lažne web stranice koje je napadač smjestio na lažni DNS poslužitelj.



Slika 6.4. *Shema DNS spoofinga [21]*

6.1.4.Ettercap

Ettercap je sveobuhvatan paket za realizaciju napada čovjek u sredini. Sadrži prisluškivanje živih veza, filtriranje sadržaja u hodu i mnoge druge zanimljive trikove. Podržava aktivno i pasivno seciranje mnogih protokola i uključuje mnoge značajke za analizu mreže i domaćina [22].

6.1.5.Wireshark

Wireshark [23] je najistaknutiji i najčešće korišten analizator mrežnih protokola. Omogućuje prikaz događaja na mreži na mikroskopskoj razini i de facto je standard u mnogim komercijalnim i neprofitnim poduzećima, vladinim agencijama i obrazovnim institucijama. Razvoj Wiresharka konstantno napreduje zahvaljujući dobrovoljnim doprinosima stručnjaka za umrežavanje širom svijeta. Radi na Windowsima, Linuxu, MacOS-u, Solarisu, FreeBSD-u, NetBSD-u i mnogim drugima. Wireshark ima bogat set značajki koji uključuje sljedeće:

Dubinski pregled stotina protokola, s tim da su se stalno dodavali novi, snimanje uživo i izvanmrežna analiza, standardni preglednik paketa s tri okna. Snimljeni mrežni podaci mogu se pregledavati putem GUI-ja ili pomoću uslužnog programa TShark u načinu TTY. Koristi najsnažnije filtre za prikaz u industriji. Datoteke za snimanje komprimirane gzipom mogu se dekomprimirati u hodu. Podaci uživo mogu se čitati s Etherneta, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI i drugih (ovisno o vašoj platformi).

6.2 Skeniranje mreže

Za skeniranje mreže koristi se alat Nmap. Nmap (Network Mapper) je open source alat za istraživanje mreže i sigurnosni reviziju. Prema [24] dizajniran je za efikasno skeniranje mreža. Nmap koristi sirove (engl. raw) IP pakete na nov i originalan način da bi ustanovio koji hostovi su dostupni na mreži, koji servisi (naziv aplikacije i verzija) su pokrenuti na tim hostovima, koji operacijski sustav koristi skenirana meta, koji tip vatrozida te kakvo filtriranje paketa se koristi, te mnogo drugih mogućnosti Nmap je koristan alat za rutinske zadatke poput sastavljanja popisa mrežnog inventara, upravljanja vremenima nadogradnje servisa i nadgledanja uptime-a računala ili usluga. Rezultat pretraživanja Nmap je popis skeniranih meta s dodatnim informacijama o svakoj od njih ovisno o korištenim parametrima. Nmap može dati i dodatne informacije o ciljanom računalu, uključujući reverse DNS imena, pretpostavku o tome koji operativni sustav je s druge strane, tipove uređaja i MAC adrese.

6.3. Testiranje probojnosti mreže

Za testiranje probojnosti mreže (engl. penetration testing) koristi se alat metasploit. Metasploit je modularna platforma za testiranje penetracije zasnovana na Ruby-u koja omogućuje pisanje, testiranje i izvršavanje koda za eksploataciju. Metasploit Framework sadrži paket alata koji se mogu koristiti za testiranje sigurnosnih propusta, izvršavanje napada i izbjegavanje otkrivanja napadača. U svojoj osnovi, Metasploit Framework je zbirka često korištenih alata. Zbog širokog raspona aplikacija i dostupnosti otvorenog koda, Metasploit koriste svi, od evoluirajućeg područja profesionalaca DevSecOps-a do hakera. Korisno je svima kojima je potreban, jednostavan je za instalaciju, pouzdan alat koji obavlja posao bez obzira na platformu ili jezik koji se koristi. Softver je popularan među hakerima i široko je dostupan, što pojačava potrebu da se sigurnosni stručnjaci upoznaju s okvirom (engl. Framework) čak i ako ga ne koriste. Metasploit trenutno uključuje oko 2000 eksploatacija organiziranih na 25 platformi, uključujući Android, PHP, Python, Java, Cisco i druge. Okvir također nosi gotovo 500 korisnih tereta, od kojih neki uključuju: Opterećenje naredbene ljuske koje korisnicima omogućuje pokretanje skripti ili nasumičnih naredbi protiv

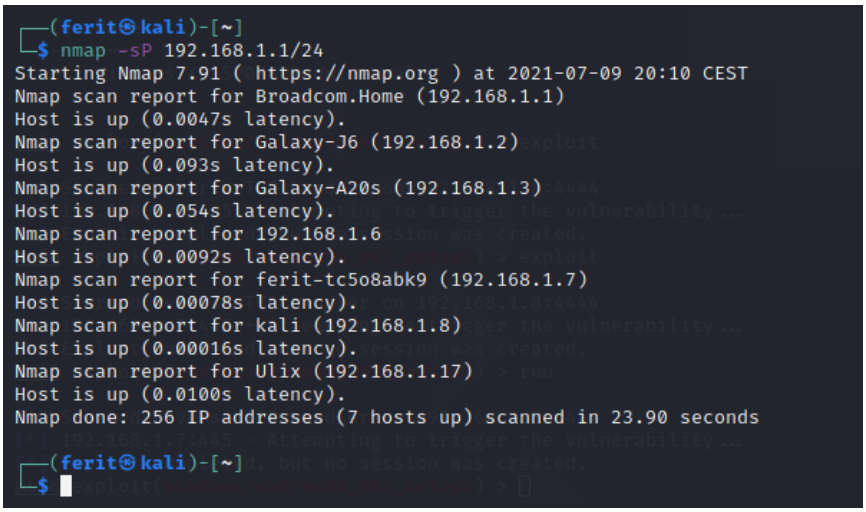
hosta, dinamički korisni tereti koji omogućuju testerima stvaranje jedinstvenih korisnih podataka kako bi izbjegli antivirusni softver, statički teret koji omogućuje prosljeđivanje portova i komunikaciju između mreža.

7. MODEL NAPADA UNUTAR BEŽIČNE MREŽE

U ovom poglavlju prikazani su napadi koji daje neovlašteni pristup računalu, napad čovjek u sredini te napad podvaljivanja lažnog DNS poslužitelja Prvo će se prikazati skeniranje mreže u potrazi za ranjivim uređajima te će se jedan od uređaj eksploatirati pomoću metasploita. Dalje će se prikazati model napada čovjek u sredini na uređaj koji nije ranjiv na dostupne eksploite, u tom napadu će se prikazati proces trovanja ARP memorije kao i inspekcija paketa pomoću programa Whireshark. Za kraj je napravljen lažni DNS poslužitelj koji će korisnika navoditi na napadačevu stranicu.

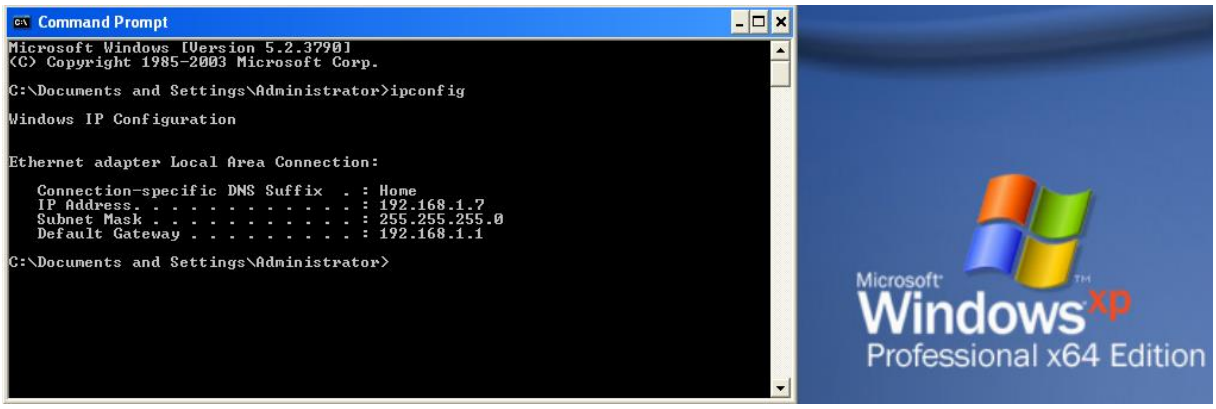
7.1. Traženje mete i ostvarivanje neovlaštenog pristupa računalu

Pomoću programa nmap skenira se mreža u potrazi za njezinim ranjivostima. Naredbom 'nmap -sP 192.168.1.1/24' skenirana je cijela mreža u potrazi za uređajima koji su povezani sa mrežom. Otkrivene su IP adrese uređaja kao i vrste istih, daljnjim skeniranjem traži se ranjivi korisnik. Slika x.x prikazuje…



Slika 7.1. *Korištenje Nmapa za pronalazak uređaja na mreži*

Na slici 7.2 može se vidjeti da je za ovaj napad odabrano je računalo koje koristi Windows XP operacijski sustav te se nalazi na IP adresi 192.168.1.7.

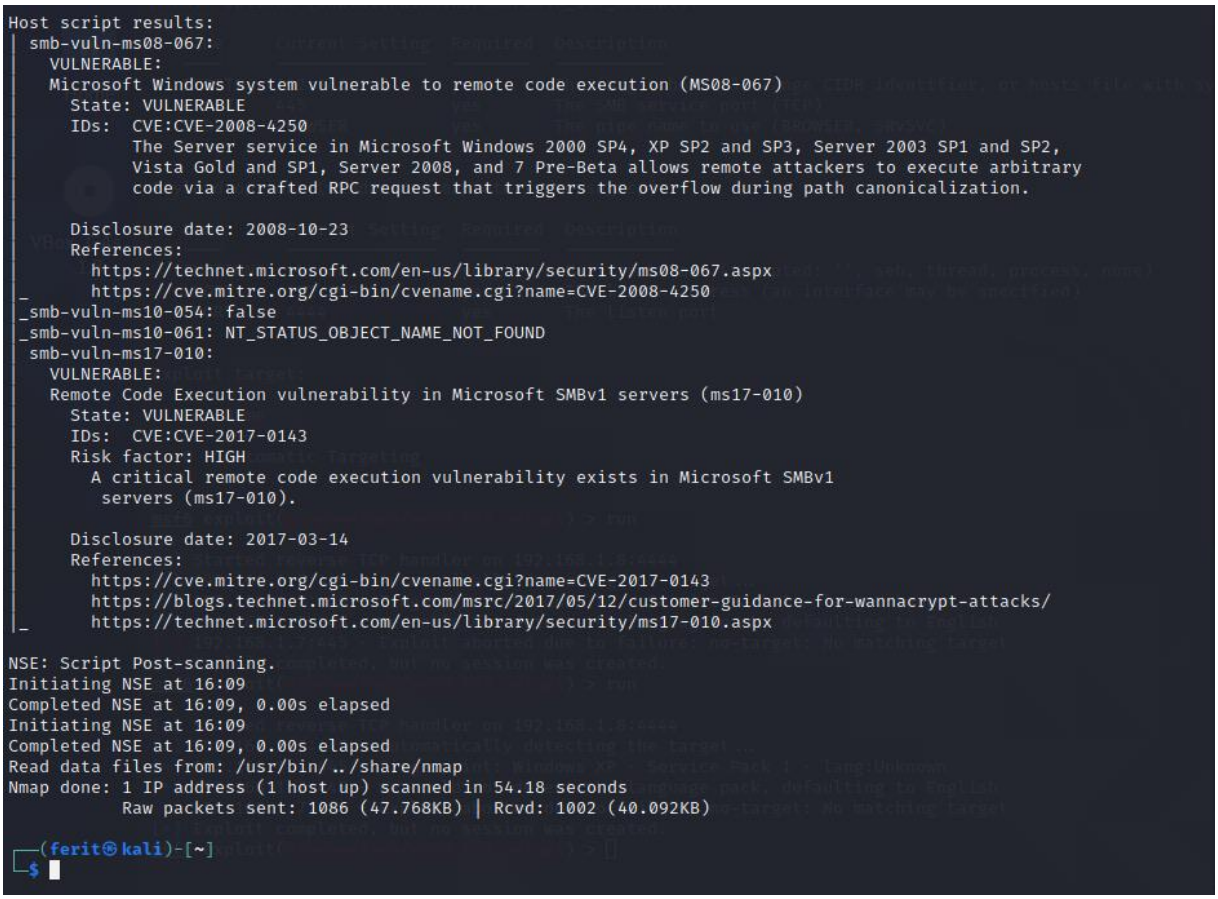


Slika 7.2 *Windows xp*

Naredbom 'nmap -v –script vuln 192.168.1.7' klijent se skenira u potrazi za dostupnim ranjivostima koje su dostupne u napadačevoj bazi. U prvom dijelu dobivene su informacije o otvorenim portovima i MAC adresi uređaja. Rezultati skeniranja prikazani su na slikama 7.3 i 7.4.

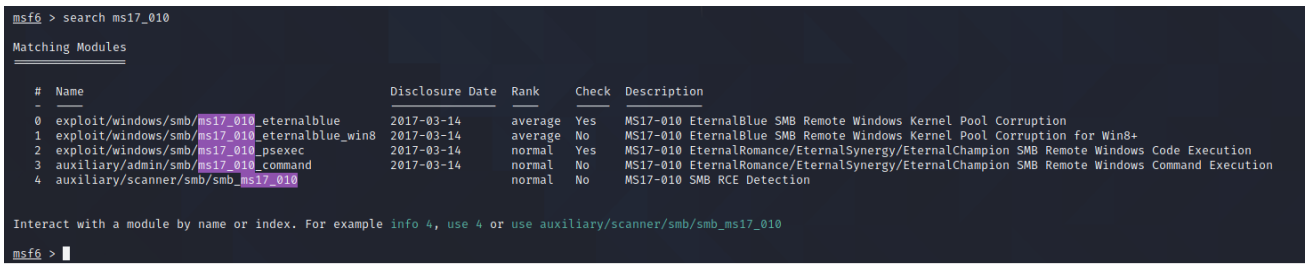
```
┌──(ferit㉿kali)-[~]
└─$ sudo nmap -v --script vuln 192.168.1.7
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-09 16:08 CEST
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:08
Completed NSE at 16:08, 10.00s elapsed
Initiating NSE at 16:08
Completed NSE at 16:08, 0.00s elapsed
Initiating ARP Ping Scan at 16:08
Scanning 192.168.1.7 [1 port]
Completed ARP Ping Scan at 16:08, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:08
Completed Parallel DNS resolution of 1 host. at 16:08, 0.01s elapsed
Initiating SYN Stealth Scan at 16:08
Scanning ferit-tc5o8abk9 (192.168.1.7) [1000 ports]
Discovered open port 139/tcp on 192.168.1.7
Discovered open port 135/tcp on 192.168.1.7
Discovered open port 445/tcp on 192.168.1.7
Discovered open port 1026/tcp on 192.168.1.7
Discovered open port 2869/tcp on 192.168.1.7
Completed SYN Stealth Scan at 16:08, 1.21s elapsed (1000 total ports)
NSE: Script scanning 192.168.1.7.
Initiating NSE at 16:08
Completed NSE at 16:09, 42.11s elapsed
Initiating NSE at 16:09
Completed NSE at 16:09, 0.00s elapsed
Nmap scan report for ferit-tc5o8abk9 (192.168.1.7)
Host is up (0.00021s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1026/tcp open  LSA-or-nterm
2869/tcp open  icslap
MAC Address: 08:00:27:83:53:49 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
```

Slika 7.3. *Prva slika zaslona 'rezultata skeniranja ranjivosti'*



Slika 7.4. *Druga slika zaslona 'rezultata skeniranja ranjivosti'*

Iz slike se može vidjeti da su pronađene kritične ranjivosti sustava. Sustav Microsoft Windows ranjiv je na daljinsko izvršavanje koda (MS08-067). Usluga poslužitelja u sustavima Microsoft Windows 2000 SP4, XP SP2 i SP3, Server 2003 SP1 i SP2, Vista Gold i SP1, Server 2008 i 7 Pre-Beta omogućavaju udaljenim napadačima izvršavanje proizvoljno koda putem izrađenog RPC zahtjeva koji pokreće preljev tijekom kanonizacije puta.[25][26]. Faktor ovakvog rizika je vrlo visok zbog toga što napadač ima mogućnost daljinskog izvođenja koda. U Microsoft SMBv1 postoji kritična ranjivost za izvršavanje daljinskog koda poslužitelji (ms17-010). [27][28][29]

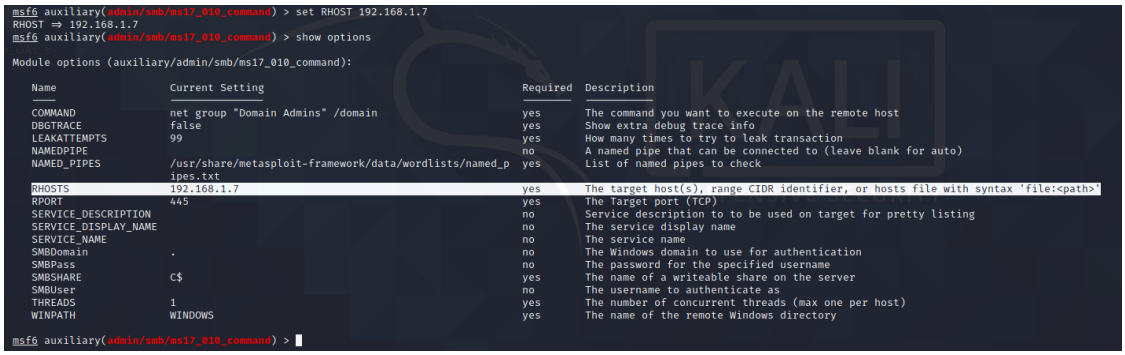


Slika 7.5. *Pretraživanje exploita*

Prethodnim skeniranjem IP adrese 192.168.1.7 pronađena je ranjivost na ms17_010 exploit, poznatiji kao ethernalblue. Naredbom 'search ms17_010' unutar metasploita pretražuju se svi dostupni materijali koji u sebi sadržavaju „ms17_010“. Rezultat pretraživanja dao je 5 modula koji odgovaraju vrsti pretrage. U daljnjem nastavku provjerava se ispravnost modula, odnosno dali je moguće ostvariti neovlašteni pristup računalu kako je navedeno u skeniranju pomoću Nmap programa.

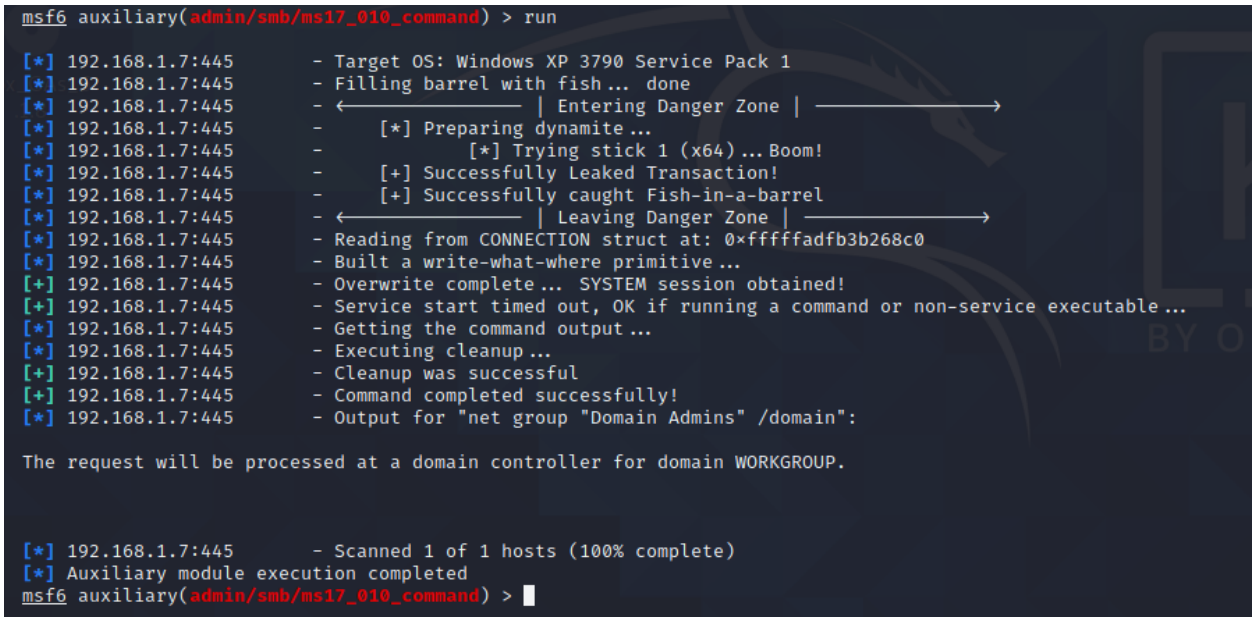
Slika 7.6. *Prikaz opcija modula*

Odabran je modul auxiliary/admin/smb/ms17_010_command koji omogućuje daljinsko izvršavanje koda odnosno konkretno neovlašteni daljinski(bežični) pristup računalu. Napad se odvija preko ranjivog porta 445(TCP). Iz slike 7.8 vidljivo je da se naredbom 'set RHOST 192.168.1.7' postavlja meta prema kojoj ide će se napad izvršiti



Slika 7.8. Provjera IP adrese mete

Naredbom 'run' pokreće se proces po prethodno zadanim parametrima koji će provjeriti ranjivost sustava. Vidljivo je da je uspješno dobivena udaljena sesija nad sustavom. Napadač odavde može raditi bilo što i nanijeti ogromnu štetu korisniku mreže.



Slika 7.9. *Pokretanje procesa eksploatiranja korisničkog računala Windows XP*

Za ovaj primjer korišten je Windows XP zbog toga što njegov ključ posjedujem od ranije. Bitno je naglasiti da je moguće ostvariti ovakav daljinski pristup i prema novijim verzijama Windowsa ako nisu ažurirani na najnovije verzije. Ovime primjerom prikazano je kako je moguće ostvariti daljinski pristup računalu bez da korisnik išta učini, samo je potrebno da je povezan sa mržom.

7.2. Čovjek u sredini

U ovome poglavlju prikazan je proces postavljanja napadača između klijenta i pristupne točke. Meta se otkrila na isti način kao u poglavlju 7.1. korištenjem alata Nmap.

7.2.1. ARP trovanje

Ciljana meta je računalo koje koristi Windows 10 operacijski sustav. Računalo je zaštićeno Windows vatrozidom, te ima dodatan sloj zaštite u obliku malwarebytes antivirusnog programa. Za priliku izvođenja ovog napada nijedna zaštitna mjera nije uklonjena, sve se odvija u realnom vremenu bez ikakvih olakšavajućih čimbenika koji bi išli u prilog samog uspješnog izvođenja napada.

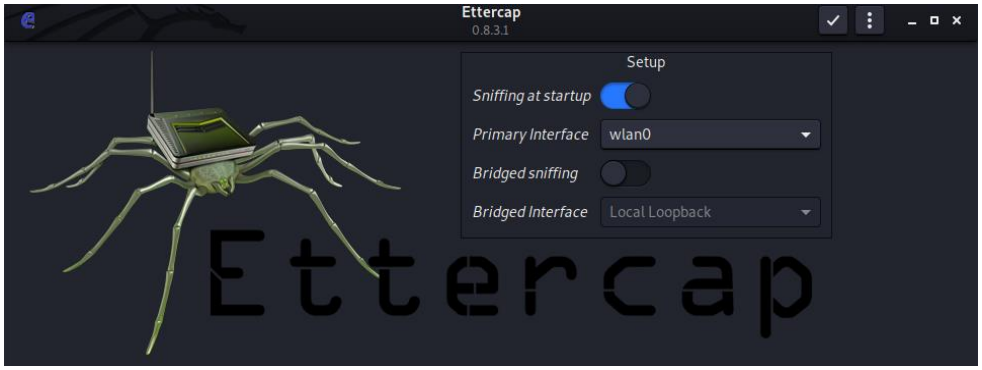
Prije samog napada provjerena je ARP memorija.

Naredbom 'arp -a' unutar Windows naredbenog retka dobivaju se informacije o stanju memorije. Vidljivo je da je IPv4 adresa 192.168.1.16, te da je zadana pristupna točka 192.168.1.1 čija je MAC adresa 6C:38:A1:72:6F:30.

```
Microsoft Windows [Version 10.0.19041.985]
(c) Microsoft Corporation. Sva prava pridržana.

C:\Users\korisnik>arp -a

Interface: 192.168.1.16 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           6c-38-a1-72-6f-30     dynamic
```

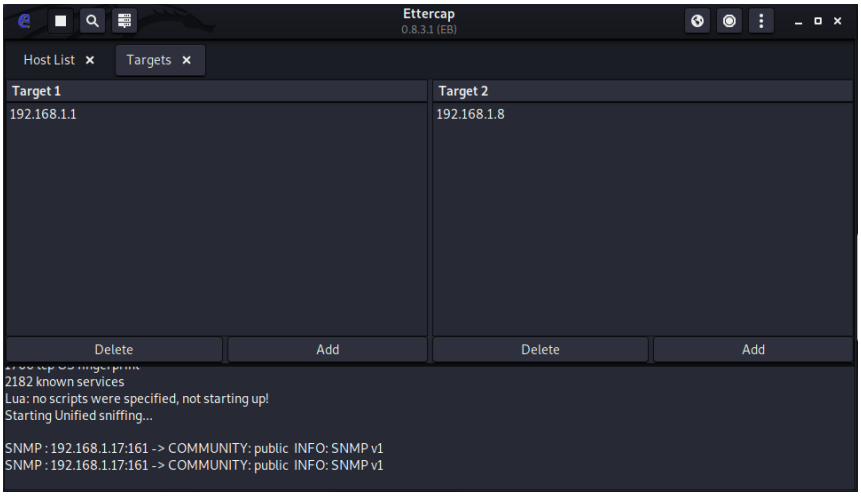
Slika 7.10. *Provjera arp memorije*

Za izvođenje napada koristi se program ettercap u grafičkom obliku. Potrebno je odabrati bežično sučelje koje će osluškivati okolinu.



Slika 7.11. *Prikaz grafičkog sučelja programa ettercap*

Mete u ovom slučaju su usmjernik i računalo, njihove IP adrese unose se u program nakon čega se pokreće proces ARP trovanja[30].

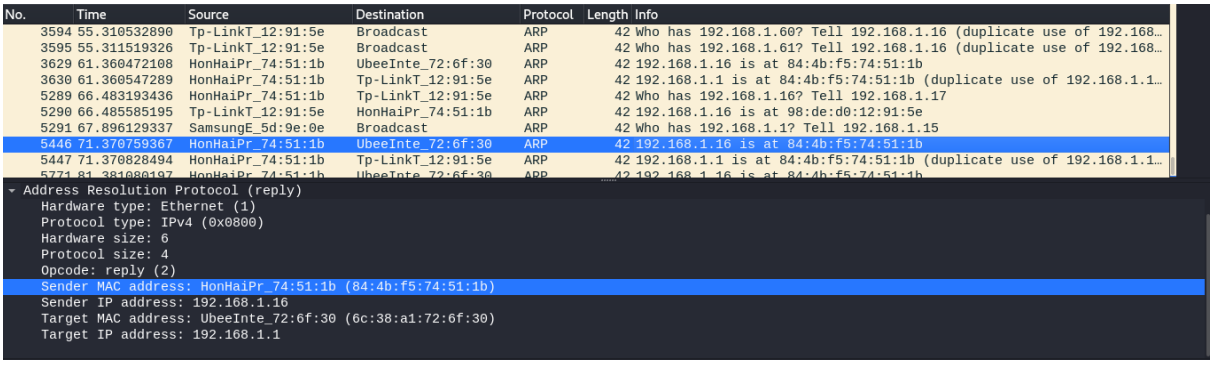


Slika 7.12. *Prikaz odabira meta za ARP trovanje*

7.2.2. Inspekcija paketa

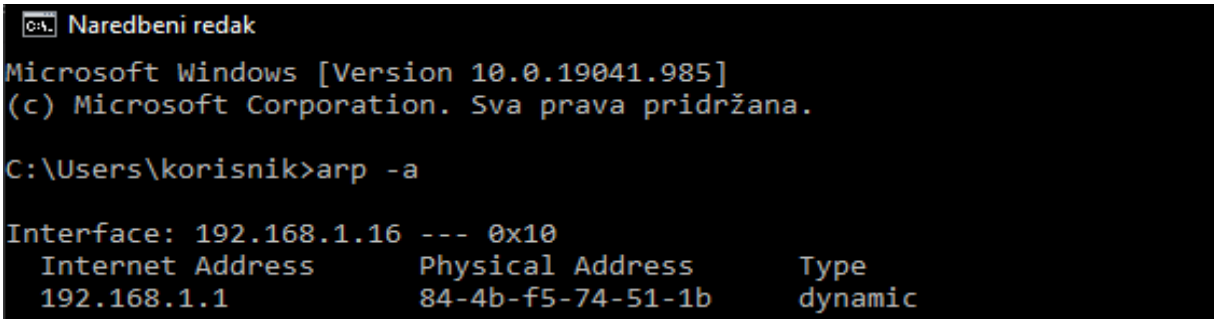
Pomoću programa Wireshark moguće je uhvatiti pakete kako bi se kasnije mogao analizirati sadržaj koji se nalazi unutar istih kao što je prikazano na slici 7.13. Pretragom prometa uočava se

velika količina ARP paketa. Odabrani paket govori da 192.168.1.16 ima MAC adresu 84:4B:F5:74:51:1B, što je zapravo MAC adresa napadača. Ovakav paket će izazvati promjenu unutar ARP memorije.



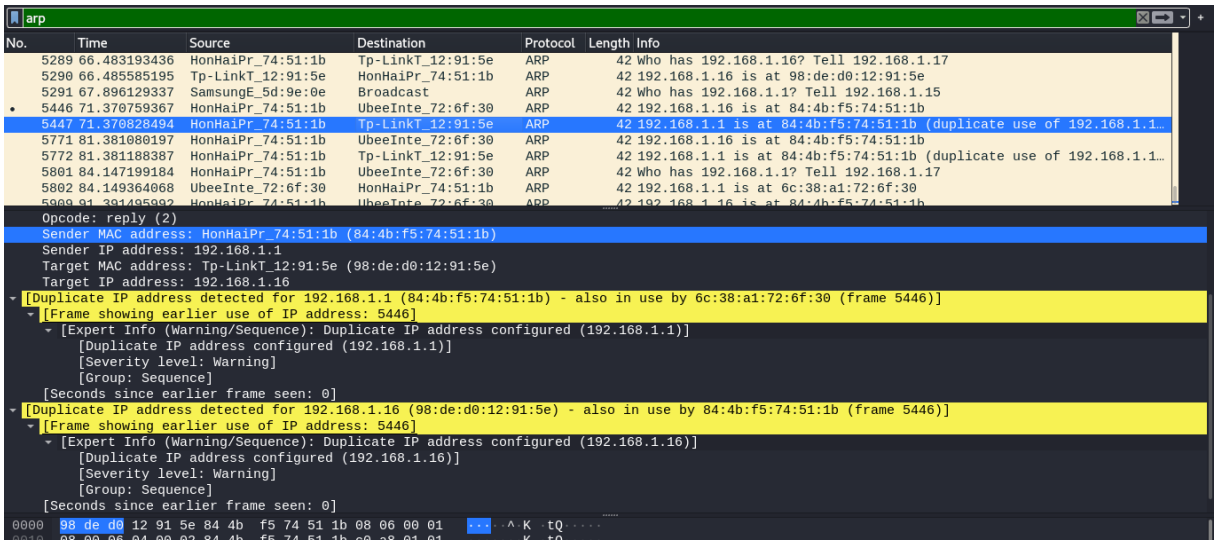
Slika 7.13. *Inspekcija ARP paketa pomoću Wiresharka*

Iz slike 7.14 vidljivo je da je IPv4 adresa 192.168.1.16, te da je zadana pristupna točka 192.168.1.1, ali u odnosu na prethodno stanje u memoriji MAC adresa je promijenjena u napadačevu 84:4B:F5:74:51:1B



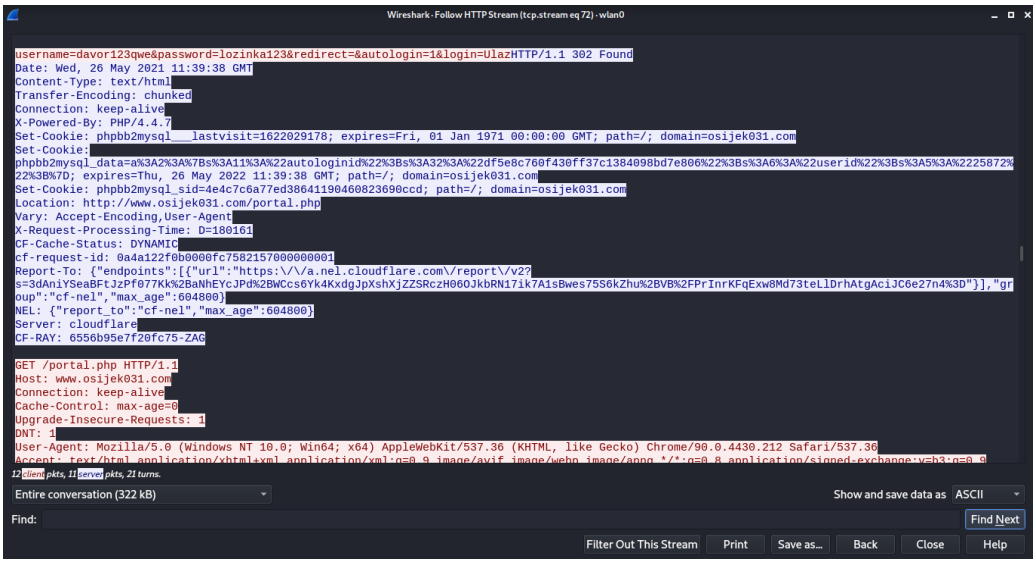
Slika 7.14. *ARP memorija nakon trovanja*

Wireshark je sposoban samostalno uočiti nepravilnosti u paketima. U ovom primjeru iz slike 7.15 pronađena je duplikacija IP adrese među različitim paketima (naznačeno od strane Wiresharka žutom bojom). Napadač koristi IP adresu 192.168.1.1 kako bi se pretvarao da je usmjernik, samo je napravljena izmjena u MAC adresi, međutim pravi usmjernik 192.168.1.1 ostaje aktivan u mreži te njegovi paketi imaju drugačiju MAC adresu u odnosu na pakete koje šalje napadač. Ista stvar detektirana je i na IP adresi klijenta(žrtve).



Slika 7.15. *Uočavanje nepravilnosti među paketima*

Nadalje, napadač može pomoću programa wiresharka detaljnije pregledavati pakete. Filtrirani su paketi koji koriste http protokol. Svaki paket je čitak jer podatci nisu šifrirani. U paketu slika 7.16 se može vidjeti da se klijent pokušao povezati sa web poslužiteljem osječkog portala za novosti, te su njegovi korisnički podatci sadržani u paketu. Tako napadač ima pregled stranica koje klijent pretražuje kao i podatke koje ostavlja na istim. Podatci o korisničkom imenu „davor123qwe“ , lozinki „lozinka123“ , adresi domene „osijek031.com“ dostupni su napadaču.



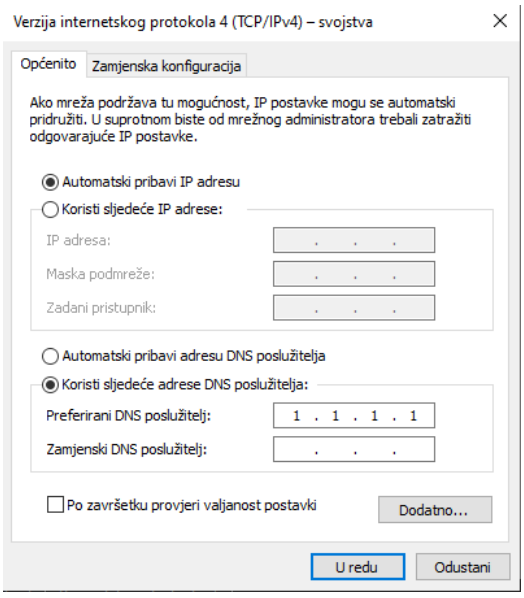
Slika 7.16. *Prikaz praćenja HTTP paketa*

Ovakva vrsta napada više nije opasna kao u vrijeme kada su se koristili nezaštićeni protokoli. Da bi napad funkcionirao klijent mora posjećivati stranice koje koriste zastarjele protokole (ftp, telnet, http) koji podatke prenose u nešifriranom obliku. Ovi protokoli zamijenjeni su puno sigurnijim

metodama i protokolima pa danas ovakva vrsta napada ne daje toliko značajne rezultate. Danas je oko 90% Internet prometa zaštićeno na način da je svaki paket šifriran. Obrana od ove vrste napada je dinamička ARP inspekcija, odnosno kontrola paketa u mreži. Unutar programa wireshark paketi se mogu filtrirati prema vrsti pa ako se primijeti velika količina ARP paketa nešto nije uredu.

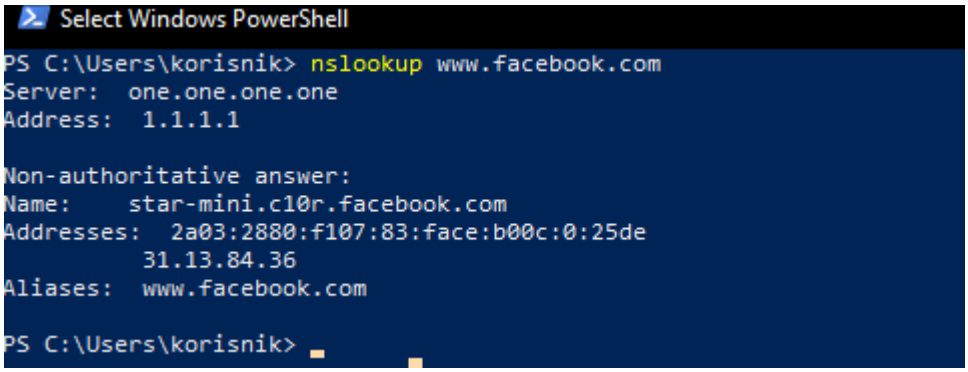
7.2.3. Podvaljivanje lažnog DNS-a

Meta u ovom slučaju je ista kao u gornjem primjeru. Kao otežavajuća okolnost u izvođenju napada je ta da računalo koristi preferirani DNS poslužitelj od cloudflarea (1.1.1.1).



Slika 7.17. *Korištenje preferiranog DNS poslužitelja*

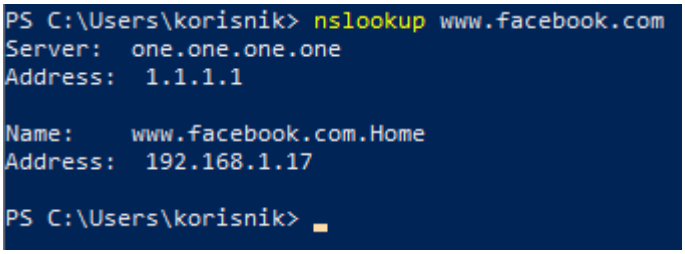
Slika 7.18 prikazuje da se prije samog napada provjerava ip adresa stranice www.facebook.com na računalu mete.



Slika 7.18. *Provjera IP adrese facebooka*

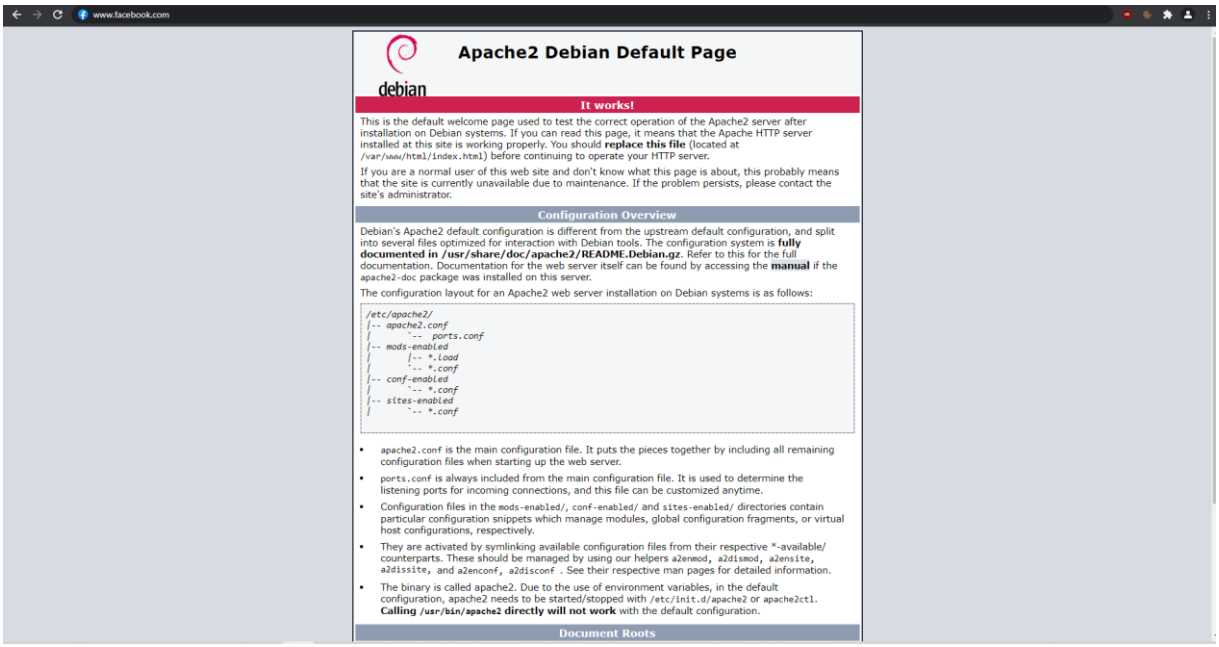
Vidljivo je da se koristi DNS poslužitelj 1.1.1.1 te je pridružena IP adresa 31.13.84.36 stranici www.facebook.com . Pomoću programa ettercap u dodatcima aktivira se DNS spoofing napad.

Prije samog napada potrebno je zatrovati ARP memoriju kao u gore opisanom primjeru kako bi računalo komunikaciju s usmjerivačem vršilo preko napadača i obratno. Za potrebe lažnog DNS servisa koristi se etter.dns tekstualna datoteka u koju je dodana jedna linija teksta '* A 192.168.1.17' što će prilikom izvođenja napada bilo koju domenu povezati sa stranicom koja se nalazi na adresi napadačevog računala koja je 192.168.1.17. Za postizanje tog cilja koristi se tehnologija Apache web poslužitelj. Kako bi sve ispravno radilo, potreban je poslužitelj preko kojega će se moći pristupiti napadačevom računalu. Kao rješenje, potrebno je instalirati Apache web poslužitelj. Moguće je prikazivati jednostavan web sadržaj kojemu se pristupa pomoću lokalne IP adrese napadačevog računala. Moguće je napad prilagoditi i da samo prilikom pretrage IP adrese određene stranice dobije kao rezultat preusmjeravanje na lažnu stranicu. Onda bi na primjer u tekstualnu datoteku bilo potrebno specificirati domenu i IP adresu. ('*.stranica.com A 192.168.1.17, '*.gmail.com A 192.168.1.17). Stranica.com bi korisnika preusmjerila na napadačevo računalo. Isto tako ako bi korisnik pokušao pristupiti gmail.com servisu bio bi preusmjeren na napadačevu stranicu.



Slika 7.19. *Provjera ip adrese www.facebook.com*

Nakon provedenog podvaljivanja DNS-a domenu www.facebook.com DNS poslužitelj povezuje sa adresom napadačevog računala. Vidljivo je da se koristi DNS preferirani DNS poslužitelj 1.1.1.1 te je pridružena IP adresa od domene stranice www.facebook.com ovaj puta 192.168.1.17 što je napadačevo računalo. Ovakva povratna informaciju uzrokovana je time što se napadač postavio između računala i pristupne točke te je lokalni DNS poslužitelj prilikom pretrage stranice facebook.com dobio odgovor koji je bio zapisan u etter.dns tekstualnu datoteku [31].



Slika 7.20. *Žrtva pokušava pristupiti stranici www.facebook.com*

Kao primjer korištena je obična indeks stranica da bi lakše bilo uvidjeti razliku između traženog i isporučenog. Korisnik je želio pristupiti stranici www.facebook.com, a odveden je na napadačevu stranicu. Ovo je mogla biti lažna facebook stranica, te prilikom korištenja takve stranice svi uneseni podatci bili bi kompromitirani. Primjer bi bio takav da klijent prilikom unosa ispravnih korisničkih podataka bude preusmjeren na pravu stranicu servisa kojeg je želio koristiti, a napadač bi bio u posjedu njegovih podataka. Za napraviti izgledom identičnu(lažnu) stranicu potrebno je samo kopirati cijeli izvorni kod od originalne, te po potrebi jednostavno kreirati certifikate kako bi stranica naizgled bila zaštićena https protokolom, kako žrtva nikako ne bi mogla primijetiti razliku. Sličan postupak primjenjuje se u napadima pecanja (engl. phishing) gdje napadač kreira lažne stranice i šalje putem maila ili drugog komunikacijskog sredstva pristupne linkove za naizgled legitimne stranice, no razlika između klasičnog pecanja i DNS podvaljivanja je ogromna iz razloga što se u nazivu same stranice može vidjeti razlika. Ovakav oblik napada gdje korisnik samovoljno želi pristupiti nekoj stranici i sam unosi adresu izaziva veći oblik sigurnosti u validnost iste stranice. Napad se teško primjećuje i u većini slučajeva korisnik gubi svoje podatke zbog toga što se sve odvija na lokalnoj razini bežične mreže. Zbog toga se na javnim bežičnim mrežama npr. kafićima ne bi trebale obavljati radnje koje su osjetljive i bitne za samog korisnika. Pregledom mreže pomoću programa whireshark može se uočiti velika količina ARP paketa te se na taj način može s pravom posumnjati na sumnjive radnje na mreži. Drugi oblik zaštite bi bio provjera samog DNS-a pomoću cmd ili powershella [32].

8. PREPORUKE ZAŠTITE

Na temelju prethodno opisanih napada slijede preporuke zaštite koje će donekle napadaču otežati pristup samoj mreži i njezinim uređajima.

8.1. Izmjena postavki usmjerivača

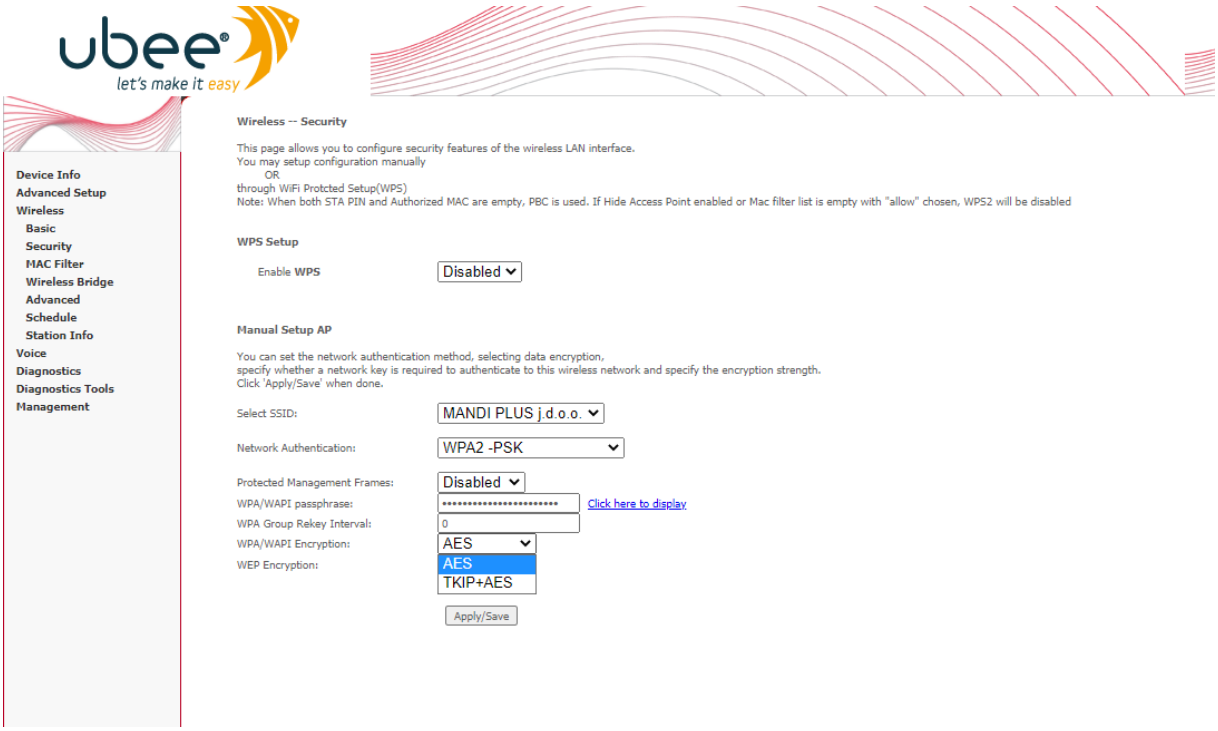
Za pristup postavkama usmjerivača potrebno je u pretraživač unijeti IP adresu na kojoj se usmjerivač nalazi, ona je po zadanom 192.168.1.1.

Nakon toga potrebno je unijeti korisničke podatke kako bi se ostvario pristup postavkama usmjerivača. Korisničke podatke potrebno je zatražiti od davatelja internet usluge. Nakon uspješne autentifikacije u postavkama je moguće puno toga promijeniti. Trenutni najbolji način autentifikacije je WPA3, no ako ga neke starije verzije usmjerivača nemaju preporuka je koristiti WPA2 zajedno sa PSK slika 8.1. WEP ovdje nikako ne dolazi u obzir zbog gore razrađenog modela penetracije u mrežu.

Početno ime BSSID-a treba se promijeniti, iz razloga što napadaču olakšava selekciju mete, nikako se ne bi trebalo koristiti prezime za naziv mreže.

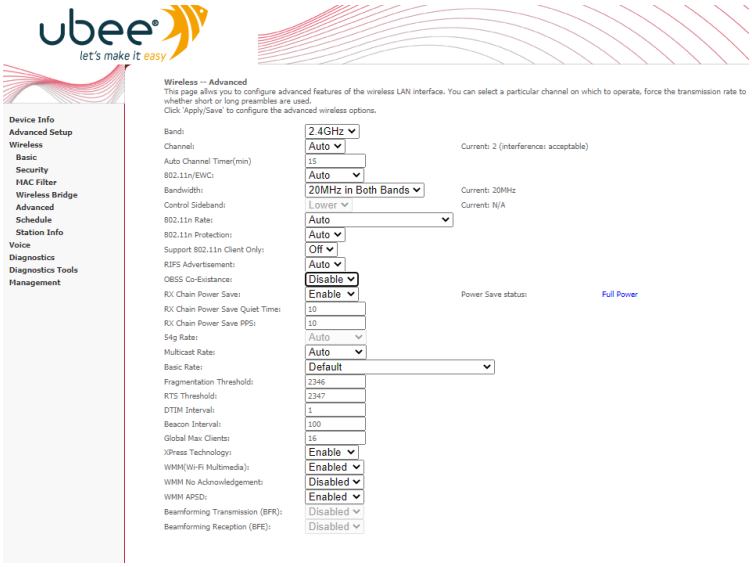
Slika 8.1. *Mijenjanje postavki načina autentifikacije*

Nakon toga enkripciju je potrebno postaviti na AES što predstavlja napredak koji je donio WPA2 u odnosu na WPA(TKIP) kao što je prikazano na slici 8.2.



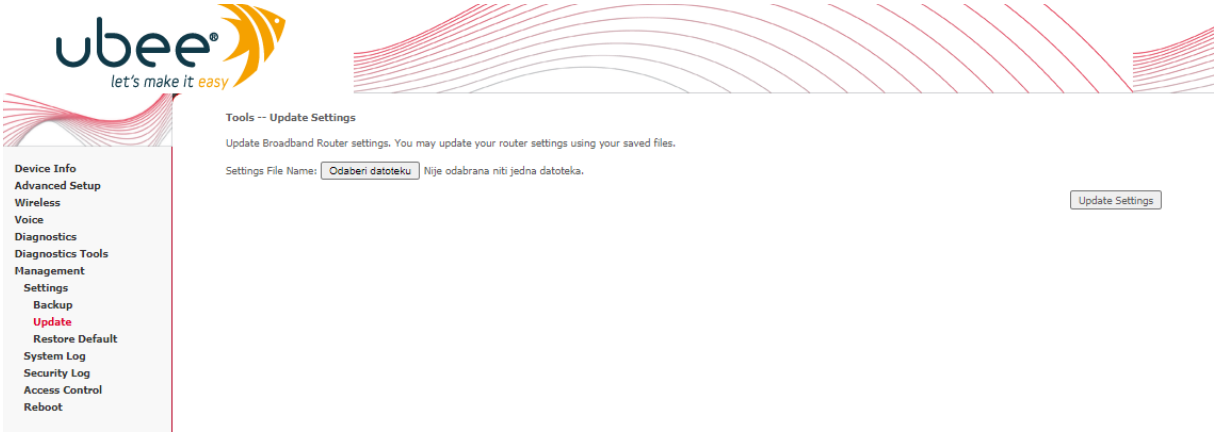
Slika 8.2. Izmjena postavki enkripcije

Iz slike 8.3 vidljive su sve ostale postavke od kojih se treba promjeniti snaga signala kako bi pokrivati točno određeno područje, kako bi se smanjio rizik napada. Moguće je izabrati više različitih postavki za snagu signala. Željeni odabir uobičajeno se samostalno postavlja na kanal s najmanje prometa, no to ne znači da napadač ne može vidjeti mrežu ako se koristi s boljom opremom. Naziv mreže također je moguće promijeniti i po potrebi sakriti. No sakrivanje BSSID-a bi izazvalo nevidljivost mreže samo uređajima koji pretražuju dostupne mreže. Napadač koji gleda promet uvijek će vidjeti takvu sakrivenu mrežu zbog toga što se unutar paketa u zaglavlju nalazi uvijek prikvačeni BSSID.



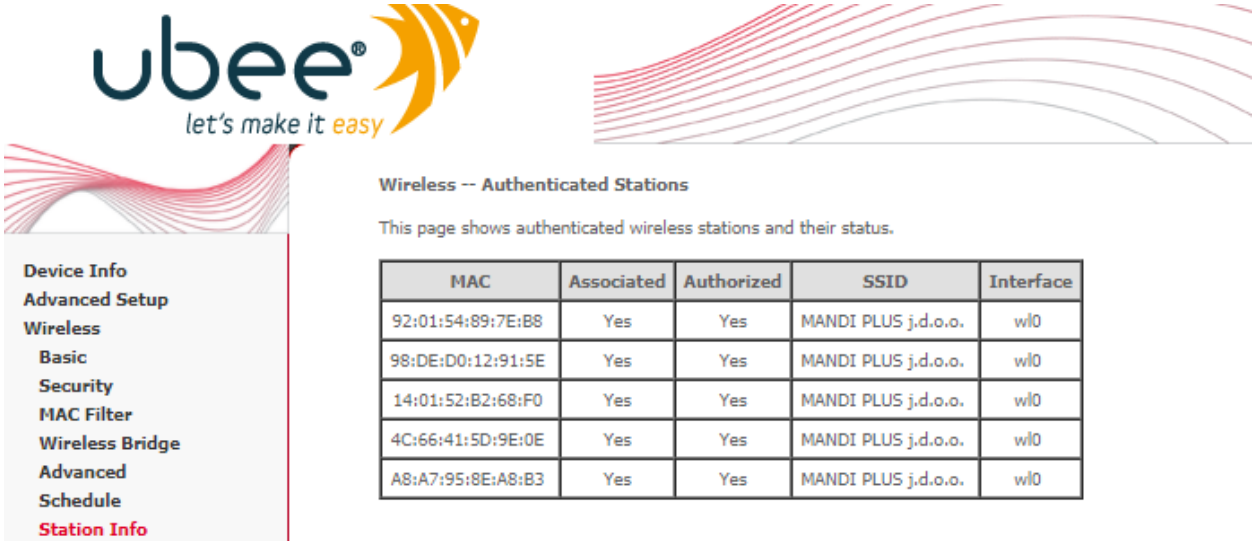
Slika 8.3. Ostale postavke

S vremenom je dobro pretražiti dostupna ažuriranja za usmjerivač iz razloga što svako ažuriranje donosi u pravilu bolje sigurnosne postavke. Slika 8.4 prikazuje izgled stranice na kojoj se obavlja ažuriranje usmjerivača. Noviju verziju je potrebno prethodno skinuti te zatim ažurirati usmjernik.



Slika 8.4. *Ažuriranje usmjernika*

Iz slike 8.5. vidljive su autentificirane MAC adrese kojima je dozvoljen prisutp mreži. MAC filtriranje filtrira pristup bežičnoj mreži prema MAC adresama. Pokušava se osigurati pristup mreži na način da pristup mogu ostvariti samo klijenti čija je MAC adresa prethodno autorizirana, bilo tko drugi neće moći ostvariti pristup zbog toga što vatreni zid (engl, firewall) neće takav zahtjev autorizirati.



Slika 8.5. *MAC filtriranje*

Dodatna zaštita može se postići uključivanjem dodatnog vatrenog zida, ako pristupna točka nudi takvu mogućnost. Neki od trenutno dostupnih uređaja na tržištu dolaze s integriranim vatrenim zidom pa ga je preporučljivo aktivirati.

8.2. Aktualizacija svih uređaja na najnoviju inačicu

Mnogi ljudi mišljenja su da svakim novim ažuriranjem štete svojim uređajima iz razloga što smatraju da ne dobivaju nikakvu korist, a s druge strane gube na performansima uređaja. Ovo naravno nije istina, jer je pretežno svako ažuriranje prije svega iz sigurnosnih razloga. Zbog toga bi se svaki uređaj trebao aktualizirati na najnoviju inačicu programa.

9. ZAKLJUČAK

U ovom radu proučena je sigurnosna okolina WI-FI mreže, odnosno opisana sigurnosna okolina na razini ostvarivanja pristupa mreži te prijetnji koje napadač ostvaruje kada je povezan sa mrežom. U radu se analiziraju i penetracijski testiraju protokoli WEP,WPA,WPA2. Nadalje opisuju se različite vrste napada za ostvarivanje pristupa mreži koji uključuju napade sirovom snagom uz kreiranje lista riječi te napade društvenog inženjeringa. Opisan je detaljan proces deautentifikacije korisnika sa mreže kao i proces hvatanja rukovanja, što je potkrepljeno i konkretnim modelom napada. Prikazan je način pravljenja rječnika kao i dva alata koji se koriste za istu svrhu, a čije korištenje pokriva sve potrebno za pravljenje bilo kakve vrste rječnika. Nadalje, nakon detaljne analize i modela napada za ostvarivanje pristupa mreži u radu se pokazuju konkretne prijetnje koje korisnik može očekivati od napadača kada ostvari pristup istoj. Obrađen je proces čovjek u sredini gdje je teoretski i primjerom pokazano korak po korak, što je sve potrebno kako bi se napadač postavio između pristupne točke i klijenta, na koji način mu truje ARP memoriju, te na koji način pregledava pakete, odnosno promet u mreži. Za tu vrstu inspekcije paketa koristio se program Wireshark u kojem je pokazano na koji način se filtriraju paketi i kako se mogu analizirati, također i za ovo je napravljen teoretski uvod kao i praktičan primjer. Nakon postavljanja čovjeka u sredini, obrađen je teoretski i modelom napada primjer DNS podvaljivanja (engl. DNS spoofing) uz pomoć programa ettercap. Prikazan je alat nmap uz pomoću kojeg se skenira mreža u potrazi za njezinim slabostima i slabim uređajima. Korištenjem Metasploit Frameworka ostvaren je daljinski pristup računalu koje je bilo povezano sa mrežom. Na kraju rada dane su preporuke zaštite koje mogu povećati razinu sigurnosti bežične mreže u vidu otežanja ostvarivanja pristupa neovlaštenim trećim stranama. Prednost ovog rada u odnosu na ostale slične je ta što fokus nije stavljen samo na jedan specifičan dio mrežne sigurnosti nego se pokazuju slabosti sa više različitih strana nakon čega je pokazano zašto je problematično imati treću neovlaštenu stranu unutar mreže.

LITERATURA

[1] N. Pimple, T. Salunke, U. Pawar, J. Sangoi: Wireless Security — An Approach Towards Secured Wi-Fi Connectivity https://ieeexplore.ieee.org/document/9074350 20.8.2021

[2] D. Gollmann, D. Westhoff, G. Tsudik, N. Asokan: Proceedings of the fourth ACM conference on Wireless network security https://dl.acm.org/doi/proceedings/10.1145/1998412 20.8.2021

[3] E. Tews, M. Beck: Practical attacks against WEP and WPA https://dl.acm.org/doi/10.1145/1514274.1514286 20.8.2021

[4] Dajana: Različite metode zaštite wireless mreža https://security.foi.hr/wiki/index.php/Wireless_security.html 15.4.2021

[5] Wi-Fi organization: Discover Wi-Fi Security https://www.wi-fi.org/discover-wi-fi/security 15.4.2021

[6] Aircrack-ng organization: https://www.aircrack-ng.org/ 15.4.2021

[7] Aircrack-ng Main Documentation: https://www.aircrack-ng.org/documentation.html 17.4.2021

[8] Kriptografija. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža: https://www.enciklopedija.hr/natuknica.aspx?ID=33988 17.4.2021

[9] M. Soltanian, I. Amiri: Problem Solving, Investigating Ideas, and Solutions, in Theoretical and Experimental Methods for Defending Against DDOS Attacks, 2016 https://www.sciencedirect.com/topics/computer-science/birthday-attack 17.4.2021

[10] Known plaintext attack of Hill cipher: https://www.nku.edu/~christensen/092mat483%20known%20plaintext%20attack%20of%20Hill%20cipher.pdf 17.4.2021

[11] P. Dutt: Understanding Rainbow Table Attack https://www.geeksforgeeks.org/understanding-rainbow-table-attack/ 17.4.2021

[12] Brute Force Attack: Definition and Examples https://www.kaspersky.com/resource-center/definitions/brute-force-attack 17.4.2021

[13] Hacksplaining: Dictionary attacks https://www.hacksplaining.com/glossary/dictionary-attacks 17.4.2021

[14] What is Social Engineering: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering 20.8.2021

[15] R. Orsi: Russian Wi-Fi Hacking – Evil Twin attacks EXPLAINED https://www.secplicity.org/2018/10/07/russian-wi-fi-hacking-evil-twin-attacks-explained/ 10.5.2021

[16] kali.org: crunch Package Description https://tools.kali.org/password-attacks/crunch 28.4.2021

[17] M. Kurgas; Cupp https://github.com/Mebus/cupp 28.4.2021

[18] Deltaxflux: Fluxion Network https://github.com/FluxionNetwork/fluxion 5.5.2021

[19] PowerCert Animated Videos: ARP Explained - Address Resolution Protocol https://www.youtube.com/watch?v=cn8Zxh9bPio 5.6.2021

[20] ARP Poisoning | Man-in-the-Middle Attack https://www.youtube.com/watch?v=A7nih6SANYs

[21] What is domain name system (DNS) spoofing https://www.imperva.com/learn/application-security/dns-spoofing/ 20.8.2021

[22] Ettercap Organization: https://www.ettercap-project.org/ 5.6.2021

[23] Whireshark Community: https://www.wireshark.org/ 5.6.2021

[24] Nmap Organization: https://nmap.org/ 5.6.2021

[25] Vulnerability in Server Service Could Allow Remote Code Execution https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067 5.6.2021

[26] Vulnerable Software Versions: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250 5.6.2021

[27] The SMBv1 server in Microsoft Windows https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143 5.6.2021

[28] Microsoft Security Bulletin MS17-010 - Critical https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 5.6.2021

[29] Microsoft Security Response Center: Customer Guidance for WannaCrypt attacks https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ 5.6.2021

[30] Poisoned ARP request confirmation while poisoning : https://github.com/Ettercap/ettercap/pull/491 15.6.2021

[31] DNS Spoofing does not work: https://github.com/ettercap/ettercap/issues/889 15.6.2021

[32] Kali 2 How to start and stop Apache server: https://forums.kali.org/showthread.php?26612-Kali-2-How-to-start-and-stop-Apache-server-Command-not-present-in-menu 19.6.2021

SAŽETAK

Cilj ovog rada bio je opisati probleme bežičnog načina rada WI-FI mreže te teoretski i primjerom pokazati slabosti koje ista koristi. Jedan sigurnosni protokol koji se danas još uvijek u ne znanju koristi među širom populacijom predstavlja primjer lošeg načina zaštite. Na druga dva su prikazani mogući napadi kako bi se ostvario pristup mreži u obliku napada sirovom snagom na uhvaćeni proces rukovanja, te oblik napada društvenog inženjerstva gdje se korisnika navodi na otkrivanje pristupnog ključa mreže. Opisani su procesi neovlaštenog nadziranja korisnika i podvaljivanja korisniku, ostvarivanju neovlaštenog pristupa računalu, te uvođenju preporuka za povećanje razine sigurnosti u bežičnoj mreži. Prikazano je korištenje alata Metasploit Framework i nmap kako bi se ostvario daljinski pristup računalu koje se nalazi na istoj mreži kao i napadač. Modelom je prikazan napada čovjek u sredini gdje se pomoću Wiresharka nadzire promet korisnika, te pomoću alata ettercap podvaljuje se lažni sadržaj korisniku u obliku lažnih DNS adresa. Na posljetku su dane preporuke zaštite koje napadačima mogu otežati pristup WI-FI mreži i zlonamjernoj aktivnosti na istoj.

Ključne riječ: bežična mreža, čovjek u sredini, napad sirovom snagom, neovlašteni pristup, sigurnost.

ABSTRACT

The aim of this final work was to describe the problems of wireless operation of the WI-FI network and to show theoretically and by example the weaknesses that it has. One security protocol that is still unknowingly used today among the general population is an example of poor protection. The other two show possible attacks to gain access to the network in the form of a bruteforce attack on the captured handshake process, and a form of social engineering attack where the user is instructed to give the network access key. The processes of unauthorized monitoring of the user and cheating the user, gaining unauthorized access to the computer, and introducing recommendations for increasing the level of security in the wireless network are described. The use of the Metasploit Framework and nmap tools to gain remote access to a computer on the same network as the attacker is shown. The model shows a human attack in the middle where Wireshark monitors user traffic, and uses the ettercap tool to trick fake content into fake user DNS addresses. Finally, protection recommendations were given that could make it difficult for attackers to access the WI-FI network and malicious activity on it.

Key word: brute-force attack, man in the middle, security, unauthorized access, wireless network.

ŽIVOTOPIS

Davor Skočibušić rođen je u Đakovu 14.studenoga 1998. godine, gdje završava *„Osnovnu školu Vladimir Nazor“* sa odličnim uspjehom. Za vrijeme osnovnoškolskih dana pokazuje interes za šahom kojim se još uvijek bavi. Nakon završene osnovne škole upisuje se u srednju školu *„Gimnazija Antuna Gustava Matoša Đakovo“*. 2017. godine završava srednju školu smjera prirodoslovno-matematička gimnazija sa vrlo dobrim uspjehom. Nakon završetka gimnazije 2017. godine upisuje se na preddiplomski studij računarstva na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku gdje se priključuje radu IEEE Studentskog ogranka Sveučilišta u Osijeku. Za Fakultet je nastupao na sportskim natjecanjima STEM-gamesa te esports turnirima. Na trećoj godini prošao je Infrastrukturnu akademiju u Spanu gdje se susreo s networkingom i brojnim rješenjima baziranim na Microsoft tehnologijama, poput Active Directoryja, PowerShella, Group Policyja, DNS-a, Exchangea/Officea 365, Azurea, SCCM-a/SCOM-a. Cilj mu je nakon završetka preddiplomskog studija ostati raditi u IT industriji. Sigurnost mreža, operacijskih sustava i računalnih programa su mu izuzetno zanimljivi. U slobodno vrijeme bavi se sportom, a omiljeni hobi mu je odmaranje u dobrom društvu.

Davor Skočibušić

_____

POPIS SLIKA

PRILOZI

Prilog 1. Završni rad u datoteci docx.

Prilog 2. Završni rad u datoteci pdf