Primjena Kali Linux distribucije u analizi sigurnosti bežičnih mreža

Petrović, Ivan

Master's thesis / Diplomski rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:200:484983

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

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

Repository / Repozitorij:

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

zir.nsk.hr

Image not found or type unknown

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

PRIMJENA KALI LINUX DISTRIBUCIJE U ANALIZI SIGURNOSTI BEŽIČNIH MREŽA

Diplomski rad

Ivan Petrović

Osijek, 2017.

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

Obrazac D1: Obrazac za imenovanje Povjerenstva za obranu diplomskog rada

Osijek, 15.09.2017.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za obranu diplomskog rada

Ime i prezime studenta:	Ivan Petrović
Studij, smjer:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika'
Mat. br. studenta, godina upisa:	D 965, 12.10.2015.
OIB studenta:	08545373241
Mentor:	Doc.dr.sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	Prof.dr.sc. Drago Žagar
Član Povjerenstva:	Dr.sc. Višnja Križanović-Čik
Naslov diplomskog rada:	Primjena Kali Linux distribucije u analizi sigurnosti bežičnih mreža
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak diplomskog rada:	Kali Linux distribucija uključuje veliki broj aplikacija koje se primjenjuju u postupcima sigurnosne analize i penetraciskog testiranja u različitim vrstama mreža. Potrebno je istražiti mogućnosti primjene Kali Linux distribucije u analizi sigurnosnih karakteristika bežičnih lokalnih mreža,te je primjeniti na različitim primjerima u okruženju bežične lokalne mreže. Prikupljene rezultate potrebno je analitički obraditi,te istaknuti preporuke i smjernice za povećanje razine sigurnosti u bežičnoj lokalnoj mreži.
Prijedlog ocjene pismenog dijela ispita (diplomskog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 3 bod/boda Jasnoća pismenog izražavanja: 3 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene mentora:	15.09.2017.

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, 29.09.2017.

Ime i prezime studenta:	Ivan Petrović
Studij:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika'
Mat. br. studenta, godina upisa:	D 965, 12.10.2015.
Ephorus podudaranje [%]:	1%

Ovom izjavom izjavljujem da je rad pod nazivom**: Primjena Kali Linux distribucije u analizi sigurnosti bežičnih mreža**

izrađen pod vodstvom mentora Doc.dr.sc. Krešimir Grgić

i sumentora

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:

SADRŽAJ

1. UVOD 1

2. KALI LINUX 2

2.1. Instaliranje Kali Linux-a 2

2.2. Upoznavanje s Kali Linux-om 3

2.3. Ažuriranje Kali Linux-a 8

3. IZVIĐANJE I ISKORIŠTAVANJE 10

3.1. Pasivno izviđanje 10

3.2. Aktivno izviđanje 12

3.3. Iskorištavanje 14

3.4. Nakon iskorištavanja - djelovanje na cilj 16

3.5. Nakon iskorištavanja - ustrajnost 17

4. BEŽIČNA MREŽA – WLAN 19

4.1. Nesigurnosti WLAN mreže 19

4.2. Zaobilaženje WLAN ovjere 23

4.3. Nedostatci WLAN enkripcije 28

4.4. Napadi na WLAN infrastrukturu 33

4.5. Napadanje klijenta 39

4.6. Kako se zaštititi? 40

5. ZAKLJUČAK 42

LITERATURA 43

SAŽETAK 44

ŽIVOTOPIS 46

1. UVOD

Gotovo cijeli svijet pokriven je uslugama bežičnih WLAN mreža pa je pitanje sigurnosti korisnika, a i same mreže važan čimbenik. Svakodnevno se mogu pronaći vijesti o raznim oblicima hakiranja i zlouporabe tuđih podataka u razne svrhe. Međutim, to su samo oni oblici napada koji dođu do vijesti. Više od milijun napada godišnje uopće se ne prijavi, a koliko ih onda još ostaje ne primijećeno? Javnost digitalnog svijeta sve manje brine o takvim problemima pa je veća vjerojatnost da će zanemariti neke osnovne mjere zaštite svojih sustava.

Kako bi korisnici izvršili odgovarajuću zaštitu svojih sustava, moraju poznavati koje slabosti i nedostatke sam sustav ima. Upravo je Kali Linux alat koji može znatno pridonijeti u povećanju sigurnosti. Kali je usmjeren na napredno testiranje penetracije računalnih sustava s kojima se mogu pronaći slabosti i nedostatci sustava prije nego to učine napadači. Na taj način se može na vrijeme reagirati i zaštiti od mogućih napada.

Zadatak ovog diplomskog rada je upotrebom Kali-a analizirati sigurnost bežičnih mreža te provođenjem raznih testova ukazati na moguće slabosti računalnih sustava. Rezultati testova ukazati će na moguće načine zaštite od određenih napada. Poznavanjem postupka izvođenja napada stekne se svijest o stvaranju načina obrane ili potrebi promjene određenih postavki sustava kako se napad ne bi mogao ni provesti.

Prema tome, uvodno poglavlje glavnog dijela rada predstavlja upoznavanje sa softverskim okruženjem Kali Linux. Definirano je što je Kali, kako radi i za što se koristi. Također su opisani načini instaliranja za uporabu na vlastitom računalu, kao i izgled radne površine sa svim vidljivim alatima i mogućim opcijama. Zatim slijedi opis kako ažurirati, nadograditi i održavati Kali.

Kako je poznavanje djelovanja napadača jedan od najjačih alata obrane od napada, iduće poglavlje daje uvid u način pristupa samom postupku provođenja napada ili penetracijskog testa. Opisane su faze prikupljanja informacija o ciljanom sustavu te njihovo iskorištavanje kako bi se djelovalo na cilj, a i omogućilo daljnje ili ponovno napadanje.

Na kraju je definirana WLAN mreža i prikazane njene sigurnosne slabosti i nedostatci. Također su opisani razni oblici napada, a isto tako provođeni testovi nad WLAN ovjerom, načinima enkripcije i infrastrukturom. Kao zaključak su istaknute preporuke za povećanje razine sigurnosti u bežičnoj lokalnoj mreži što je i bila uloga provođenja testova.

2. KALI LINUX

Kali Linux predstavlja okruženje temeljeno na *Debian* Linux distribuciji usmjereno na napredno testiranje penetracije računalnih sustava. Penetracijski test pojam je koji označava ovlašteni simulirani napad na računalni sustav. Tako se traže sigurnosne slabosti sustava s mogućnošću dobivanja pristupa značajkama i podacima. Upravo Kali sadrži nekoliko stotina alata usmjerenih prema različitim zadacima informacijske sigurnosti kao što su: penetracijski testovi, sigurnosno istraživanje, računalna forenzika i obrnuti inženjering. Okruženje je razvila tvrtka *Offensive Security*, vodeća tvrtka u obučavanju o informacijskoj sigurnosti. Također ga uzdržava sve do danas.

Prva verzija Kali Linux-a objavljena je 13. ožujka 2013. godine kao cjelovita obrada *BackTrack* Linux-a po razvojnim standardima *Debian*-a. Prema [1] *BackTrack* je objavljen kako bi pružio veliku raznolikost alata za testiranje prodiranja kao i alata za obranu revizorima i mrežnim administratorima koji brinu o sigurnosti svojih mreža. Isti alati su međutim korišteni od ovlaštenih, ali i od neovlaštenih (hakeri) testera prodiranja. Posljednja verzija *BackTrack*-a temeljila se na Linux-ovom okruženju *Ubuntu* koje je bilo široko prihvaćeno od sigurnosne zajednice, ali je sama arhitektura stvarala poteškoće u upravljanju nizom alata. Ubrzo je *BackTrack* zamijenjen Kali Linux-om koji koristi arhitekturu temeljenu na *Debian*-u.

2.1. Instaliranje Kali Linux-a

Postoji nekoliko načina kako instalirati Kali ili ga podići (engl. *Boot*) na računalo kao što su: direktna instalacija na hard disk računala, dvostruko podizanje Kali-a sa Windows-om, dvostruko podizanje Kali-a na Mac hardware-u, samostalno podizanje Kali-a na Mac hardware-u, instalacija preko enkripcijskog diska, Mini ISO instalacija, instalacija preko mreže PXE. Za izradu ovog rada korišten je način instalacije dvostrukog podizanja-a Kali-a sa Windows-om pa će u ovom dijelu biti opisan način instalacije direktno na hard disk i dvostrukog podizanja sa Windows-om. Ostali načini imaju slične korake a detaljne upute mogu se pronaći u službenoj dokumentaciji na web stranici Kali-a.

- Direktna instalacija na hard disk

Prvi korak je skinuti Kali sa službene stranice te ga staviti na DVD, ili pripremiti USB koji ima Kali Linux Live na sebi. U slučaju nemogućnosti korištenja jednog od ova dva medija, moguće je instalirati Kali i preko internet mreže. Za instalaciju je potrebno minimalno 20 GB slobodnog prostora na hard disku, minimalno 1 GB radne memorije, ali se preporučuje 2GB ili više, te potpora

za CD-DVD / USB podizanje sustava. Instalacija započinje kada se računalo stavi u određeni način podizanja sustava sa određenog medija. Ubrzo se pojavljuje Kali pozdravni prozor na kojem su prikazani razni načini instalacije. Nakon što se odabere željeni način potrebno je odabrati jezik, lokaciju kao i jezik tipkovnice. Odabrani medij zatim započinje kopiranje Kali-a na disk računala te zahtijeva postavljanje mrežnog sučelja. Slijedi postavljanje imena za računalo što će stvorit korisnikov ID, postavljanje vremenske zone, a zatim će se ponuditi određene opcije za odabir načina spremanja Kali-a na disk. Nakon toga se postavlja upit želi li korisnik koristiti mrežno ogledalo. Preko njega se instaliraju službeni dodaci sa Kali repozitorija pa je poželjno odabrati „da“. Posljednji korak je instalacija GRUB-a koji omogućava korisniku odabir podizanja jednog od više operacijski sustava sa diska te ponovno pokretanje sustava kako bi se instalacija uspješno završila.

- Dvostruko podizanje Kali sustava sa Windows-om

Ovakav način instalacije smatra se jako korisnim, ali treba postupati s oprezom i sigurnosno pohraniti podatke Windows instalacije na vanjskom mediju. Instalacija je slična kao i direktna instalacija na disk. Razlika je u tome što se prvotno treba podijeliti dio diska na kojem se nalazi Windows u slučaju da on zauzima cjelokupan prostor tog dijela. Postupak podjele diska moguće je obaviti u samom Kali Linux sučelju. Potrebno je postaviti računalo u način podizanja sa određenog medija. Kada se pojavi pozdravni prozor Kali-a potrebno je odabrati opciju „Live“ što će pokrenuti Kali Linux na uređaju. Moguće je i tako koristiti Kali ali bilo kakve promjene i postavke neće ostat spremljene. U aplikacijama Kali-a potrebno je pokrenuti aplikaciju pod nazivom *Gparted*. Unutar nje moguće je podijeliti disk po želji, ali treba imati na umu da kao i u gore navedenom načinu instalacije, potrebno je minimalno 20 GB slobodnog prostora. Dakle, nakon što se disk podijeli tako da jedan dio ima minimalno 20 GB, potrebno je potvrditi napravljene postavke i ponovno pokrenuti uređaj. Nakon ovog koraka instalacijski postupak je jednak kao i u direktnom načinu.

2.2. Upoznavanje s Kali Linux-om

Prema [2] je trenutna verzija Kali-a najlakša za koristiti u usporedbi sa dosadašnjim verzijama Kali-a, ali i *BackTrack*-a. Međutim, proizvođači tvrde kako Kali nije baš za svakoga. Kali je okruženje isključivo usmjereno prema profesionalnom testiranju penetracije i stručnjacima za računalnu sigurnost. Prema tome Kali nije preporučeno okruženje za osobe koje nisu upoznate sa Linux-om. Čak i za iskusne korisnike Linux-a Kali može biti izazov. Iako je Kali *open source* projekt, treba imati na umu da nije *wide-open* projekt iz sigurnosnih razloga. Tim koji radi na

okruženju je malen i pouzdan te su paketi iz repozitorija potpisani od strane članova tima, što znači da bi dodavanje repozitorija na vlastiti sustav, koji nisu bili testirani od razvojnog tima, bio dobar način izazivanja problema. Također, iako je arhitektura Kali-a prilagodljiva na visokoj razini, nije moguće dodavati nepovezane pakete i repozitorije. Važno je spomenuti kako uporaba alata za testiranje penetracije unutar mreže može izazvati nepopravljivu štetu s osobnim i zakonskim posljedicama. Proizvođači navode da, ako se radi o stručnoj osobi za testiranje penetracije ili osobi koja izučava testiranje penetracije s ciljem postizanja certifikata stručnjaka, za te svrhe ne postoji bolji alat od Kali-a.

Kao već spomenuto, Kali obuhvaća velik broj alata za provjeru sigurnosti računalnih mreža. Takvi alati u komercijalnom pogledu imaju visoku cijenu pa Kali samim tim ima prednost u korištenju iz razloga što je besplatan. [2] navodi kako Kali nudi besplatne probne verzije takvih komercijalnih alata koji se mogu nadograditi na potpune plaćene verzije, a iste se mogu zatim koristiti u Kali okruženju.



Sl. 2.1. Prikaz radne površine Kali Linux-a

Radna površina sastoji se od: trake favorita na lijevoj strani, aplikacijskog i mjesnog menija u gornjem lijevom kutu te opcija za pristup drugom radnom prostoru, opcija snimanja, postavki jezika tipkovnice i opcija za prijavu na Internet, odjavu i slično u gornjem desnom kutu. Ikona „Kali Live“ označava da je Kali trenutno pokrenut izravno sa instalacijskog medija.

Traku favorita sa lijeve strane radne površine moguće je preurediti po želji, a općenito se sastoji od najčešće korištenih alata i aplikacija kojim omogućuje brz pristup. Prva tri alata sa slike 2.1. su web pretraživač, Terminal i upravitelj datoteka, a posljednja tri su tekstualni editor, alat za preuređenje izgleda i funkcija Kali-a te ikona za prikaz svih aplikacija i alata (Sl. 2.2.).



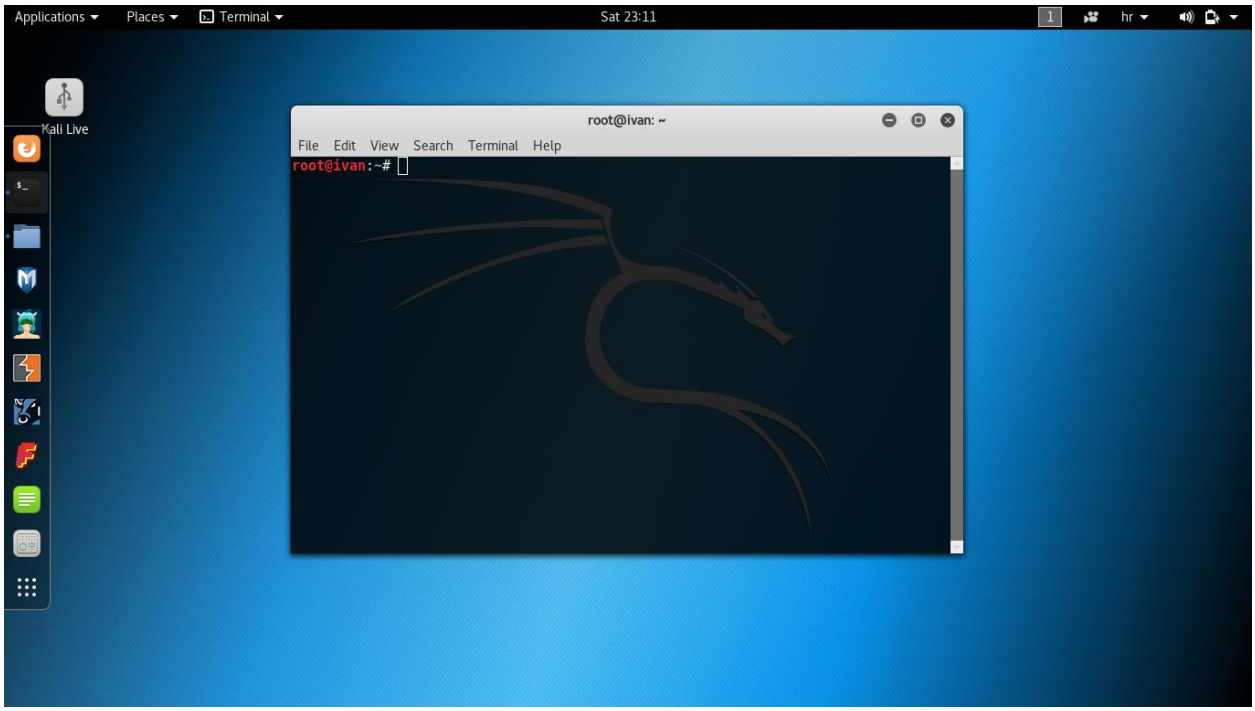
Sl. 2.2. Prikaz nakon pritiska ikone za prikaz svih aplikacija

Aplikacije i alati su organizirani po tipu, a za jednostavnije pretraživanje moguće je upisati traženu aplikaciju u traku za pretraživanje. Raspored aplikacija prema kategorijama moguće je vidjeti pritiskom na aplikacijski meni iz gornjeg lijevog kuta što prikazuje sljedeća slika:

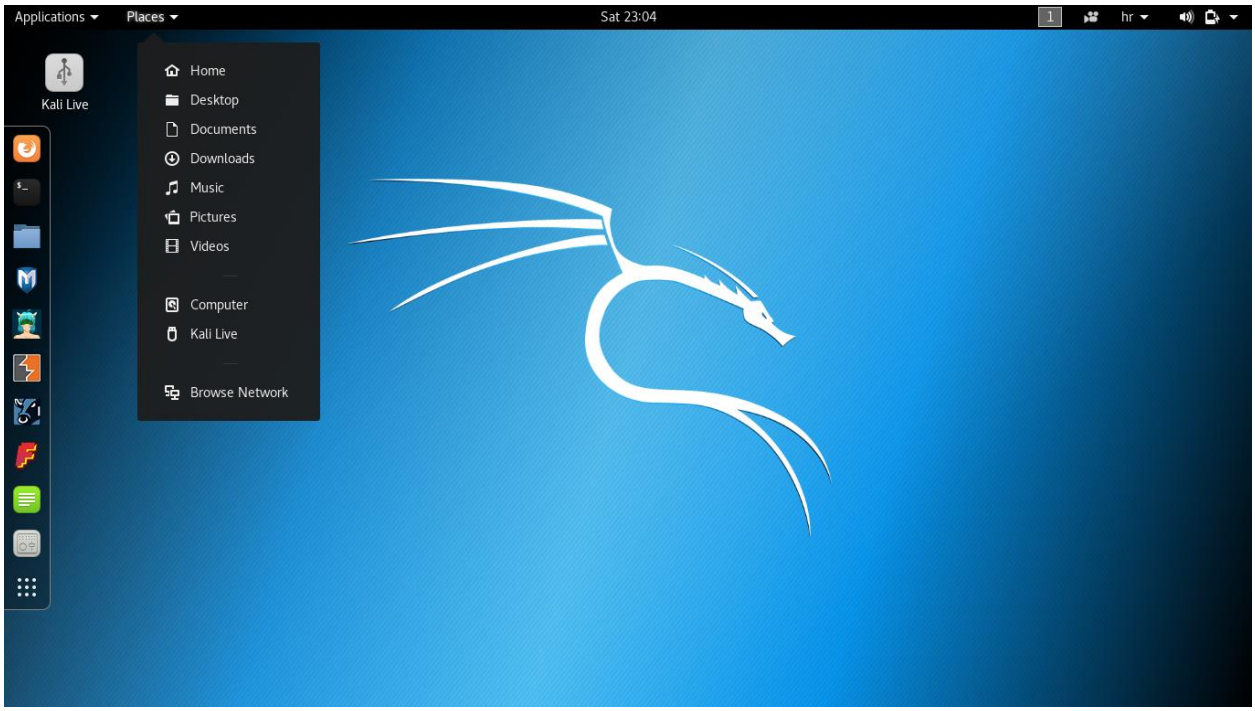


Sl. 2.3. Prikaz aplikacijskog menija

Odabirom određene kategorije ne prikazuju se svi dostupni alati iz te kategorije nego samo najčešće korišteni. Treba imati na umu da je samo dio instaliranih alata vidljiv u aplikacijskom meniju, većina ih je dostupno isključivo preko naredbene linije. Kako bi vidjeli većinu instaliranih alata, u naredbenoj liniji je potrebno tražiti „*usr/share*“ direktorij [2]. Njih je moguće pokrenuti u terminalu (Sl. 2.4.) upisom imena alata. Meni mjesta (engl. *Places)* prikazuje linkove na različite lokacije Kali-a (Sl. 2.5.).



Sl. 2.4. Prikaz pokrenutog terminala



Sl. 2.5. Meni „Places“

2.3. Ažuriranje Kali Linux-a

Kao i svaki sličan sustav, Kali je potrebno redovito ažurirati s ciljem održavanja svih alata u korak sa današnjicom. Budući da se radi o sigurnosti, osobito je važna svaka nadogradnja sigurnosnih alata. Pored toga korisnik može i samostalno uređivati svoj sustav dodavanjem različitih alata pod uvjetom da su iz službenog, testiranog repozitorija. Za sve to postoji APT *Package Handling Utility* (*apt-get*), snažan alat naredbene linije. Koristi se za instaliranje i uklanjanje softverskih paketa, a isto tako prati verzije svega instaliranog te obavještava korisnika u slučaju potrebe za nadogradnjom. Sljedeće osnovne funkcije *apt-get* alata bi, prema [3], svaki korisnik trebao znati:

- Instalacija aplikacija ili paketa: predstavlja najosnovniju funkciju, primjer sintakse: *apt-get install (ime_paketa)*
- Ažuriranje: izvore repozitorija potrebno je povremeno provjeriti, preporuča se provjeriti postoje li ažuriranja uvijek prije instalacije novih paketa, primjer sintakse: *apt-get update*
- Nadogradnja: je funkcija koja će povući i instalirati sve nove verzije prethodno instaliranih softverskih paketa, primjer sintakse: *apt-get upgrade*
- Nadogradnja distribucije: slično funkciji nadogradnje uz dodatne mogućnosti pretrage izvora po posebno označenim paketima, primjer sintakse: *apt-get dist-upgrade*
- Uklanjanje: preporuka je sve pakete koji se ne koriste ukloniti, primjer sintakse: *apt-get remove (ime_paketa)*
- Automatsko uklanjanje: kako se s vremenom softverski paketi zamjenjuju unaprijeđenima, funkcija automatskog uklanjanja će ukloniti stare pakete koji nisu potrebni za trenutne funkcionalnosti sustava. Preporuka je pokrenuti automatsko uklanjanje nakon bilo kakvog oblika nadogradnje, primjer sintakse: *apt-get autoremove*
- Čistka: za razliku od uklanjanja, ova funkcija uklanja sve konfiguracijske datoteke sa uređaja što je nekad potrebno prilikom ponovne instalacije neke aplikacije, primjer sintakse: *apt-get purge (ime_datoteke)*
- Čišćenje: kako se paketi skidaju sa izvora neraspakirani pa zatim instaliraju, ostavljaju višak koji je došao sa izvora u sustavu. Taj višak naravno zauzima prostor na disku pa je ponekad potrebno očistiti ga, primjer sintakse: *apt-get clean*
- Automatsko čišćenje: radi slično kao prethodna funkcija s preporukom pokretanja nakon bilo kakvog oblika nadogradnje. Automatsko čišćenje će ukloniti sve stare pakete koji su zamijenjeni novima prilikom nadogradnje, primjer sintakse: *apt-get autoclean*
- Spajanje više funkcija u jednu: prethodno navedene funkcije moguće je kombinirati u jednu funkciju operatorom && u sintaksi:

apt-get update && apt-get upgrade && apt-get dist-upgrade ili
apt-get autoremove && apt-get autoclean.

Za instalaciju i distribuciju aplikacija i paketa treće strane koristi se *Debian* paket menadžer (*dpkg*). Takve aplikacije, koje se moraju nabaviti preko prodavača, nisu javno dostupne pa *apt-get* neće moći locirati pakete za skidanje i instalaciju. Slično kao i za *apt-get* [3] navodi sljedeće osnovne funkcije:

- Instalacija: nakon skidanja *.deb* paketa biti će potrebno pozvati naredbu *dpkg* kako bi iste instalirali. Takvi paketi obično sadrže sve potrebne informacije za uspješan rad aplikacije, primjer sintakse: *dpkg -i (ime_paketa.deb / ciljani direktorij)*
- Uklanjanje: radi jednako kao i istoimena *apt-get* naredba te na jednak način upravlja paketima, primjer sintakse: *dpkg -r (ime_paketa.deb)*
- Provjera instaliranih paketa: mogućnost trenutnog stanja instaliranog ili uklonjenog softvera.

3. IZVIĐANJE I ISKORIŠTAVANJE

Prilikom testiranja penetracije ili izvršenja napada, potrebno je postupiti nekim određenim pravilima, odnosno pratiti nekakav postupak događanja. Svaki dobar napad ima faze kroz koje prolazi a te faze su faze izviđanja i iskorištavanja. Riječ je o prvobitnom prikupljanju informacija o meti napada i mreži u kojoj se nalazi, a zatim se prikupljene informacije iskorištavaju kako bi se došlo do cilja. Ovo poglavlje obraditi će teorijsku podlogu koja stoji iza postupka napada te dati uvid u djelovanje napadača kada dobiju pristup podacima zbog kojih su napali.

Izviđanje (engl. *Reconnaissance*) je prema [1] prvi korak pri testiranju penetracije ili izvođenja napada na ciljanu računalnu mrežu ili server. Napadači uobičajeno ulože i do 75% cjelokupnog posla na izviđanje, odnosno na definiranje mete napada i istraživanje što će onda dovesti do mogućeg iskorištavanja. Dva su oblika izviđanja koja će biti objašnjena u ovom poglavlju: pasivno i aktivno.

Iskorištavanje (engl. *Exploit*) prema [1] predstavlja stvaranje pristupa za postizanje cilja, bilo to zaustavljanjem pristupa meti napada uskraćivanjem usluga ili uspostavljanjem postojanog pristupa meti od strane napadača. Ono se temelji na rezultatima pasivnog i aktivnog izviđanja.

3.1. Pasivno izviđanje

Pasivno izviđanje predstavlja analizu informacija koje su otvoreno dostupne bilo to od same mete napada ili javnih izvora sa interneta. Kada penetracijski tester ili napadač pristupa tim informacijama ne djeluje na metu na neuobičajeni način. To znači da aktivnost neće biti uhvaćena ili zapisana, tj. neće biti izravno povezana sa napadačem ili penetracijskim testerom. Iz tog razloga se pasivno izviđanje provodi na prvom mjestu kako bi se izbjegla moguća identifikacija napadača ili davanje bilo kakvih signala o mogućem napadu. Gotovo je nemoguće meti napada razlikovati pasivno izviđanje od uobičajenih aktivnosti.

Napadači, a isto tako i penetracijski testeri, uobičajeno prate određeni proces sakupljanja informacija širokog opsega. Kako bi penetracijski testeri bili učinkoviti, moraju znati kakve informacije napadači traže te kako će informacije biti iskorištene prije nego krene sakupljanje. Općenito gledano je prvi korak napada ili penetracijskog testa sakupljanje inteligencije otvorenog izvora (OSINT – engl. *Open-Source Intelligence*) [1]. Ona predstavlja informacije sakupljene sa javnih izvora, odnosno interneta. Kakve se informacije sakupljaju ovisi o početnom cilju penetracijskog testa. Primjerice, ako se želi pristupiti financijskim podacima neke tvrtke, potrebno je prikupiti informacije kao što su imena i biografije od određenih zaposlenika te njihova

korisnička imena i lozinke. Uobičajeno se prikupljanje OSINT-a započinje sa pregledom javne internetske aktivnosti mete kao što su web stranice, društvene mreže i slično. U primjeru poslovne tvrtke informacije koje su od koristi su[1]:

- Geografske lokacije ureda koji dijele poslovne informacije, a nemaju stroge sigurnosne kontrole
- Pregled o matičnoj tvrtki i svim podružnicama, osobito svih novih tvrtki koje su stečene spajanjima jer one često nisu sigurne kao matična tvrtka
- Imena i kontakt informacije zaposlenika, osobito ime, broj telefona te adresa elektroničke pošte
- Informacije o kulturi poslovanja i jeziku tvrtke što će olakšati napade u društvenom smjeru
- Poslovni partneri i dobavljači koji će se moguće spojiti u mrežu tvrtke
- Tehnologije koje se koriste jer u slučaju poznatih slabosti napadači mogu iskoristiti detalje za izvođenje napada

Pored svih navedenih informacija tu naravno postoji još mnogo više, potrebno je samo definirati metu napada te tako razložiti kakve informacije su bitne za izvođenje napada. Jednom kada se identificira meta napada, koja ima određenu online aktivnost, potrebno je spoznati IP adrese i putanje između napadača i krajnje mete napada. Prema tome izvodi se DNS (engl. *Domain Name System*) izviđanje koje pruža spoznaju o tome kome pripada određena domena ili niz IP adresa te o putanji prema meti. Sam DNS predstavlja bazu podataka koja povezuje imena sa njihovim pripadajućim IP adresama. Prikupljanje tih informacija može preko DNS registra stvoriti trag o napadu. Registar može pokupiti informacije o IP adresi i zahtjevima napadača, ali one u pravilu rijetko dođu do krajnjeg cilja. DNS informacije napadači mogu iskoristiti kako bi primjerice našli usluge koje su ranjive ili za pronalazak pogrešno postavljenih servera i slično.

Za spoznaju prostora IP adresa potrebno je prvo povezati adrese sa ciljanom stranicom. Prema [1] se to često postiže naredbom *whois*. Ona dozvoljava pretragu baze podataka koje ima pohranjene informacije o registriranim korisnicima nekog internetskog resursa. Ovisno o tome kakva se baza pretražuje *whois* će dati informacije kao što su: imena, fizičke adrese, brojevi telefona, adrese elektroničke pošte, IP adrese te imena DNS servera. Ove informacije napadači mogu iskoristiti za spoznaju lokacije i planiranje fizičkog napada, ali i za izvođenje raznih drugih napada.

Pitanje određivanja putanje do cilja, predstavlja uglavnom alat kojim se provjerava ruta paketa od jednog uređaja do drugog. Kali za određivanje putanje koristi *traceroute*, a napadači informacije o putanji mogu iskoristiti za spoznaju [1]:

- Točne putanje između napadača i mete napada
- Vanjske topologije mreže
- Informacija o uređajima kontrole pristupa koji filtriraju promet napada
- Unutrašnjeg adresiranja u slučaju pogrešno postavljene mreže

Naredba *traceroute* će većinu skokova paketa pokazati filtrirano pa je potrebno koristiti više alata kao što su: *hping3, intrace* i *trace6*. Uz njihovu pomoć zaobići će se uređaji koji filtriraju pakete i dobiti cijela putanja.

3.2. Aktivno izviđanje

Aktivno izviđanje temelji se na velikim količinama neprimjetno prikupljenih informacija pasivnog izviđanja. Dostavlja više korisnih informacija o napadnutom sustavu, ali poduzete akcije mogu izazvati alarme zaštitnih alata mete što će razotkriti napad. Što je korisnost informacija veća, veći je i rizik otkrivanja napada. Za povećanje učinkovitosti aktivnog izviđanja u dostavljanju što korisnijih informacija koriste se skrivene tehnike ili tehnike koje je teško razotkriti.

Koristeći vremenske oznake napadača, izvornu IP adresu i razne druge informacije meta napada može identificirati izvor dolaznog izviđanja. Penetracijski testeri oponašajući radnje hakera koriste razne načina za poticanje aktivnog izviđanja [1]:

- Koriste alat za kamuflažu kako bi izbjegli otkrivanje i aktiviranje alarma
- Skrivaju napad unutar legitimnog prometa
- Oblikuju napad kako bi sakrili izvor i vrstu prometa
- Koristeći nestandardne načine enkripcije čine napad nevidljivim

Prije nego se krene u penetracijsko testiranje ili napad, potrebno je provjeriti jesu li svi nepotrebni servisi Kali-a onemogućeni ili ugašeni. Ako se to ne učini može doći do međusobne komunikacije između servisa napadača i servisa mete, što će alarmirati administratore mete. Uobičajeno se onemogući IPv6 kako ne bi najavio prisutnost napadača na mreži. Neki alati Kali-a označavaju pakete sa sekvencom za identifikaciju što može biti korisno za analizu nakon testiranja, jer se može vidjeti kako mreža otkriva i reagira na napad. Međutim takvi paketi također mogu aktivirati određene sustave za otkrivanje upada.

Najčešći pristup aktivnom izviđanju je slanje određenih paketa prema meti pa iskoristiti pakete koji su se vratili za dobivanje informacija. Pogodan alat za to je *nmap* koji manipulira paketima, ali za učinkovito korištenje mora se pokrenuti s korijenskim ovlastima što je upravo slučaj u Kali

terminalu. U pokušaju smanjenje mogućeg otkrića, određene tehnike skrivanja prema [1] uključuju sljedeće:

- Prepoznavanje svrhe skeniranja prije testiranja te slanje minimalnog broja paketa potrebnih za utvrđivanje cilja
- Izbjegavanje skeniranja koja bi se mogla povezati sa ciljanim sustavom i izazvati curenje podataka.
- Postavke paketa kao što su izvorni IP i adresa porta te MAC adresa postaviti slučajnim generatorom
- Podešavanje vremena za usporavanje dolaska paketa na stranu mete
- Promjenu veličine paketa fragmentiranjem ili dodavanje slučajnih podataka kako bi zbunili servise sa kontrolu paketa

Kali također sadrži nekoliko alata za prepoznavanje otvorenih portova i operacijskih sustava. Većina funkcija tih alata može se obaviti i preko spomenutog *nmap* alata. Skeniranje porta je proces spajanja na TCP i UDP portove kako bi se odredilo kakve usluge i aplikacije rade na ciljanom uređaju. Korištenje *nmap* alata za otkrivanje porta biti će otkriveno od strane uređaja za mrežnu sigurnost pa treba imati na umu da uspješno skeniranje zahtijeva dobro poznavanje TCP/IP-a i sličnih protokola, a i znanje o radu pojedinih alata. Kako bi napadači ostali neprimjetni, ako već napadanu na portove, napast će samo one koji ih vode ka krajnjem cilju.

Određivanje operacijskog sustava na udaljenom sustavu provodi se prema [1] aktivno i pasivno. Aktivnim načinom napadač šalje normalne i preoblikovane pakete prema meti i snima uzorak odgovora koji se preneseno naziva „otisak prsta“. Pasivan način podrazumijeva osluškivanje, odnosno snimanje i analizu niza paketa kako bi se odredile karakteristike paketa.

Kao konačni postupak aktivnog izviđanja smatra se skeniranje ranjivosti. Skeniranje ranjivosti upotrebljava automatizirane procese i aplikacije kako bi se prepoznale slabosti u računalnoj mreži, operacijskim sustavima ili aplikacijama koje su iskoristive za napad. Ako se provede ispravno, skeniranje ranjivosti daje popis uređaja, poznate ranjivosti dobivene aktivnim skeniranjem i potvrdu o tome koliko su uređaji popustljivi na različite propise. Unatoč tome, skeniranje ranjivosti dostavlja višestruke pakete koji se lako otkriju od strane mrežnih kontrola pa je gotovo nemoguće provesti skeniranje potajno. Autori [1] navode i sljedeća dodatna ograničenja:

- Skeniranje ranjivosti temeljeno je na potpisu pa može otkriti samo poznate ranjivosti i to ako postoji prepoznatljiv potpis koji se može primijeniti na metu.
- Velika je vjerojatnost da učinak skeniranja sadrži lažne pozitivne rezultate

- Skeneri mogu imati negativan utjecaj na mrežu jer mogu prouzrokovati kvar nekih uređaja
- U određenim nadležnostima skeniranje ranjivosti smatra se hakiranjem i može biti nezakonit čin.

3.3. Iskorištavanje

Iskorištavanje slijedi nakon pasivnog i aktivnog izviđanja čija je zadaća bila prepoznati sigurnosne nedostatke, a njih će napadač iskoristiti kako bi došao do cilja. Faza iskorištavanja oslanja se na dva pristupa u postizanju cilja, jedan je sprečavanje pristupa meti uskraćivanjem usluga, a drugi je uspostavljanje postojanog pristupa meti od strane napadača. Prema [1] postoje određena stajališta faze iskorištavanja koje svaka osoba pri testiranju prodiranja mora imati na umu:

- Je li meta potpuno karakterizirana? Ako napadač ne razumije mrežu i arhitekturu sustava, napad neće uspjeti i povećava se opasnost da će napad biti otkriven.
- Jesu li dobro definirane akcije iskorištavanja ciljnog sustava? Neokarakterizirano iskorištavanje može imati neželjene posljedice, a rezultati štete bi mogli imati negativan utjecaj na postupak testiranja. Iz tog razloga bi se pri penetracijskom testu, prije korištenja, trebala potvrditi sva iskorištavanja u poznatim postavkama.
- Provode li se sva iskorištavanja na udaljenoj lokaciji ili lokalno na ciljanom sistemu? Udaljeno iskorištavanje sigurnije je za napadače jer postoji manja opasnost od mogućeg otkrivanja napada. Unatoč tome, lokalno iskorištavanje daje napadaču veću kontrolu nad svim akcijama pa i to smanjuje opasnost od moguće detekcije.
- Koje su potrebne aktivnosti nakon iskorištavanja? Ako napadač treba izvući podatke iz mete onda iskorištavanje mora podržati uspostavljanje interaktivne veze.
- Je li uopće potreban ustrajan pristup ugroženom sustavu ili će ugrožavanje biti kratkotrajno, što bi moglo dovesti ka potrebi za potajnim pristupom.

Kako pasivno i aktivno izviđanje označava mrežu i sustav mete napada, a također identificira slabosti koje bi mogle biti iskorištene za postizanje cilja, penetracijski testeri imaju veliku sklonost poduzeti određene akcije. Želja im je što prije dokazati kako mogu ugroziti metu, ali neplanirani napad nije dobar način za postizanje cilja, a može žrtvovati i tajnost koja je potrebna za uspjeh. Iz tog razloga se primjenjuje postupak oblikovanja prijetnje (engl. *Threat Modeling*) koji je prvobitno uveden od strane mrežnih planera za razvijanje mjere obrane od napada. Napadači i penetracijski testeri su metodologiju obrambenog oblikovanja prijetnje iskoristili u obrnutom smjeru kako bi bili uspješniji u napadu. Napadačko oblikovanje prijetnje pristup je koji povezuje rezultate izviđanja i istraživanje za razvitak strategije napada. Napadač mora razmotriti dostupne

mete i prepoznati njihov tip, a postoje tri vrste meta napada: primarne, sekundarne i tercijarne meta napada. Mete koje, kada su ugrožene, odmah podržavaju postizanje cilja nazivaju se primarnim metama. Sekundarne mete mogu pružiti određene informacije i tako podržati napad ili dopustiti pristup primarnoj meti. Tercijarne mete često nisu uopće povezane sa ciljem napada, ali se lako ugroze i mogu pružiti informacije ili odvratiti pažnju od stvarnog napada [1].

Dakle, pasivno i aktivno izviđanje definira podlogu napada na metu tj. ukupan broj točaka kojim se može pristupiti kao ranjivima. Ako nekakav server ima instaliran samo operacijski sustav može ga se iskoristiti na ranjivosti koje su vezane isključivo za operacijski sustav, međutim količina ranjivosti se povećava sa svakom instaliranom aplikacijom. Prema tome napadači i penetracijski testeri moraju pronaći moguće načine iskorištavanja temeljene na poznatim ranjivostima ili onima koje se daju naslutiti. Prvo mjesto za potragu određenih ranjivosti ili nedostataka nekih uređaja ili aplikacija je na stranicama prodavača jer oni pri objavi novih verzija objave i informacije o ranjivostima. Ako postoji poznato ranjivo mjesto koje se može iskoristiti prodavači će ga naglasiti svojim kupcima. Namjera im je tako dozvoliti kupcima provjeriti postojanost ranjivosti, ali će upravo te informacije iskoristiti i napadači. Postoje tako mnoge online stranice koje prikupljaju, analiziraju i dijele informacije o poznatim ranjivostima. Proizvođači Kali-a, *Offensive Security*, imaju svoju bazu podataka mogućih iskoristivih ranjivosti koju je moguće lokalno spremiti na Kali.

Faza iskorištavanja smatra se najopasnijom kako za napadače tako i za penetracijske testere. Izravno su u interakciji sa računalnom mrežom ili samim sustavom mete pa postoji velika mogućnost da će njihova aktivnost biti zabilježena ili će se otkriti njihov identitet. Iz tog se razloga, kao što je već spomenuto, akcije moraju provoditi skriveno. Koliko god akcije bile skrivene, nijedan alat nije nemoguće otkriti pa se koriste razne promjene postavki koje će otežati detekciju. Računalne mreže tako imaju razne oblike za kontroliranu obranu od napada kao npr. vatrozidi, antivirusni softveri i slično. Većina se antivirusnih softvera oslanja na usporedbu potpisa kako bi locirali virus i druge štetne podatke. Provjeravaju sve izvršne datoteke u potrazi za nizovima koda za koje je poznato da postoje u virusima i onda oglašavaju alarm ako pronađu sumnjive datoteke. Tako se npr. napadi alatom Kali-a pod imenom *Metasploit*, oslanjaju na datoteke čiji su potpisi s vremenom prepoznani od prodavača antivirusnih softvera i tako prijete da će biti otkriveni. *Metasploit* na to reagira omogućavanjem kodiranja samostalnih izvršnih datoteka kako bi se zaobišla detekcija istih kao virus. Ipak je široko testiranje tih izvršnih datoteka na javnim stranicama dovelo do smanjenja učinkovitosti zaobilaženja detekcije antivirusnih softvera.

3.4. Nakon iskorištavanja - djelovanje na cilj

Kako je prethodno opisano, iskorištavanje pretvara pronalaske izviđanja u akcije koje pružaju pristup između testera, odnosno napadača i žrtve napada. Međutim, najvažniji dio napada su akcije nakon iskorištavanja, tj. kada napadači dođu do cilja, a riječ je o krađi i izvlačenju podataka, iskorištavanju slabe provjere pristupa te krađa korisničkih vjerodajnica. Hakeri suvremenog svijeta nisu toliko zaokupljeni iskorištavanjem koliko tim što se može učiniti pristupom tim podacima. Napadači iz ovog dijela izvlače najveću korist, a jednom kada je sustav ugrožen, napadač prema [1] provodi sljedeće aktivnosti:

- Provodi brzo istraživanje lokalnog okruženja (provjera infrastrukture, konekcije, korisničkih računa, postojanost podataka i aplikacija koje mogu olakšati daljnje napade)
- Pronalazi i kopira ili preuređuje datoteke koje ga zanimaju
- Kreira dodatne korisničke račune i preuređuje sustav kako bi podržao akcije nakon iskorištavanja
- Pokušava proširiti razinu povlastica za pristup sustavu hvatanjem administratorskih vjerodajnica
- Pokušava napasti ostale podatkovne sustave provođenjem napada kroz ugroženi sustav ostatkom mreže
- Ugrađuje postojani povratni put u sustav i pretvara kanale kako bi ponovno zadobio kontrolu te imao sigurnu komunikaciju sa ugroženim sustavom
- Uklanja znakove napada sa ugroženog sustava.

Za uspješno djelovanje na cilj nakon iskorištavanja, potrebno je poznavanje operativnog sustava mete kao i podatkovne strukture kako bi se zaobišle zaštitne provjere. Korisnicima Windows-a je poznato kako izvođenje bilo kakvih ovlaštenih aktivnosti zahtijeva administratorsku dozvolu. Prema tome, odmah nakon iskorištavanja napadače zanima tko je korisnik napadnutog sustava i kakve ovlasti ima nad tim sustavom. Njih može dobiti kroz *Metasploit* pa ako su administratorske ovlasti postavljene na uobičajen način, moći će podići vlastite ovlasti.

Kada napadač iskorištavanjem dođe do cilja obično krade ili mijenja vlasničke podatke te se onda okreće idućoj meti, odnosno datotekama sustava. One će pružiti informacije koje će biti korisne za dodatne napade. U slučaju Windows operativnog sustava napadač će napasti: memoriju sustava (pruža velike količine informacija što može iskoristiti za izvlačenje lozinki, enkripcijskih ključeva i slično), registarske datoteke sustava, podatke vezane za elektroničku poštu, a i bilo kakve druge lozinke ili korijenske datoteke korištene za enkripciju.

Kreiranje dodanih korisničkih računa obično se primijeti od strane vlasnika sustava prilikom prijave pa se iz tog razloga zapravo koriste za odvlačenje pažnje od upornijih mehanizama pristupa. Izmjenom određenog registra novo kreirani račun može se sakriti od korisnika sustava, ali naredba se razlikuje ovisno o operacijskom sustavu mete pa je potrebno prvo odrediti vrstu sustava kako bi se moglo dalje postupati.

Često je moguće dobiti pristup sustavu kao gost ili kao korisnik vrlo jednostavno. Mogućnost napadača da dohvati važne informacije ovisi upravo o razinama ovlasti. Prema tome je česta akcija nakon iskorištavanja podići razinu ovlasti od gostujuće i korisničke čak do administratorske sve do sustavne. Kako bi dobio napredne korisnikove vjerodajnice napadač koristi nekoliko metoda kao što su: postavljanje osluškivanja mreže za hvatanje prenesene korisnikove vjerodajnice, pretraživanje lokalno spremljenih lozinki (iz razloga što korisnici često skupljaju lozinke u određenom direktoriju), iniciranje štetnog koda direktno u servise korištenjem sustavne administratorske ovlasti i dr. [1].

Jednom kada napadač dobije pristup određenoj mreži ili sustavu, jako je važno pokriti trag kako bi izbjegao detekciju ili poduzeti mjere kako bi otežao postupak rekonstrukcije svoje aktivnosti. To može učiniti brisanjem zapisničkog dnevnika Windows-a u potpunosti ako se on aktivno vodi na serveru. Brisanje dnevnika ne izaziva nikakve alarme na korisničkoj strani, čak se nedostatak određenih zapisa smatra uobičajeno pa se ne vodi detaljnije istraživanje po tom pitanju.

3.5. Nakon iskorištavanja - ustrajnost

Posljednji korak napada predstavlja faza kada se napadač oslanja na ustrajnu konekciju unutar ugroženog sustava kako bi osigurao mogućnost ponovnog spajanja i održavanja kontrole nad napadnutim sustavom. Često se zato ugrađuju štetni softveri u sustave mete. Napadač mora biti u mogućnosti održati interaktivnu ustrajnost, odnosno dvosmjerni komunikacijski kanal sa napadnutim sustavom koji treba ostati dugo neprimjetan unutar sustava. Razlozi zbog kojih je ovakva konekcija potrebna su prema [1] sljedeći:

- Upade u računalnu mrežu moguće je otkriti pa će doći do identifikacije ugroženog sustava i stvaranja zaštite
- Neka iskorištavanja moguće je provesti samo jednom zbog toga što su ranjivosti isprekidane, iskorištavanja uzrokuju pad sustava ili ga prisiljavaju na promjenu što čini ranjivosti neupotrebljivima.
- Napadači će se možda morati vratiti nekoliko puta na istu metu iz različitih razloga

- Korisnost ugroženog sustava nije uvijek poznata u trenutku kada se dobije pristup.

Štetni softveri, koji su namijenjeni da ostanu u ugroženom sustavu što duži period vremena, pružaju napadačima i penetracijskim testerima velik broj mogućnosti [1]:

- Dozvoljavaju pridruživanje dodatnih alata za podržavanje novih napada osobito na sustave u istoj mreži
- Olakšavaju izvlačenje podataka iz ugroženih sustava i mreža
- Dozvoljavaju napadačima ponovno povezivanje u ugroženi sustav preko kodiranog kanala kako bi izbjegli detekciju. Poznato je da štetni softveri ostaju u sustavu i do godinu dana
- Ugrađuju tehnike kako bi se izbjegla moguća detekcija što uključuje skrivanje unutar sustavnih datoteka ili memoriji sustava koristeći snažnu ovjeru autentičnosti i kodiranje.

Ako se štetni softveri otkriju i uklone potrebno je uložiti dodatne napore kako bi se došlo do ugrožavanja sustava na isti način. Kali se iz tog razloga usredotočuje na štetne softvere koje je teže otkriti ako su ispravno podešeni. Najbolji su oni štetni softveri koje ne treba dodatno skrivati zato što su dio postojeće strukture datoteka ugroženog sustava. Napadač samo mora dodati određenu funkcionalnost kako bi pretvorio uobičajene sustavne datoteke i aplikacije u štetni softver, a takav se pristup gotovo nikako ne može otkriti od strane sigurnosnih kontrolnih sustava.

4. BEŽIČNA MREŽA – WLAN

WLAN (engl. *Wireless Local Area Network)* predstavlja bežičnu računalnu mrežu koja povezuje dva ili više uređaja koristeći bežičnu komunikaciju. Pokriva određeno područje unutar kojeg se korisnici mogu kretati i ostati povezani. Ovakve mreže su izrazito pogodne za kućnu upotrebu zbog jednostavnog postavljanja i korištenja. Također se koriste u komercijalnim prostorima kako bi pružile usluge svojim kupcima. Podaci se razmjenjuju zrakom što predstavlja moguću prijetnju sigurnosti jer su takvi podaci najjednostavniji za presresti. Kasnije će kroz rad biti dani primjeri kako hakeri osluškuju prijenos podataka, odnosno hvataju podatke zračne komunikacije koji dolaze od strane svih usmjerivača koji su u dometu.

Trenutno najraširenij oblik WLAN mreže je WI-FI. Radi na uređajima koji se temelje na IEEE 802.11 standardu. Postoji više verzija tog standarda, ali su najviše rasprostranjeni 802.11a, 802.11b i 802.11g. Verzije *b* i *g* su rasprostranjene u Hrvatskoj, dok se verzija *a* koristi u SAD-u. Jedina razlika između njih je u tome što standardi 802.11b i g rade na radijskoj frekvenciji od 2,4 GHz dok 802.11a radi na 5 GHz.

Po pitanju arhitekture WLAN mreže, važno je imati pristupnu točku te jednog ili više klijenata. Pristupna točka ih povezuje u zajedničku grupu i služi sa spajanje sa žičanom mrežom ili drugim WLAN mrežama. Povezivanje sa drugim mrežama omogućuje bežični usmjerivač čija je glavna zadaća ostvarivanje komunikacije sa WAN mrežom preko spojnih linija kao npr. ISDN, DSL ili drugim WLAN tehnologijama. Kroz ovo poglavlje će biti obrađeni primjeri napada na WLAN mrežu osluškivanjem paketa, probijanjem enkripcijskih zaporki i slično.

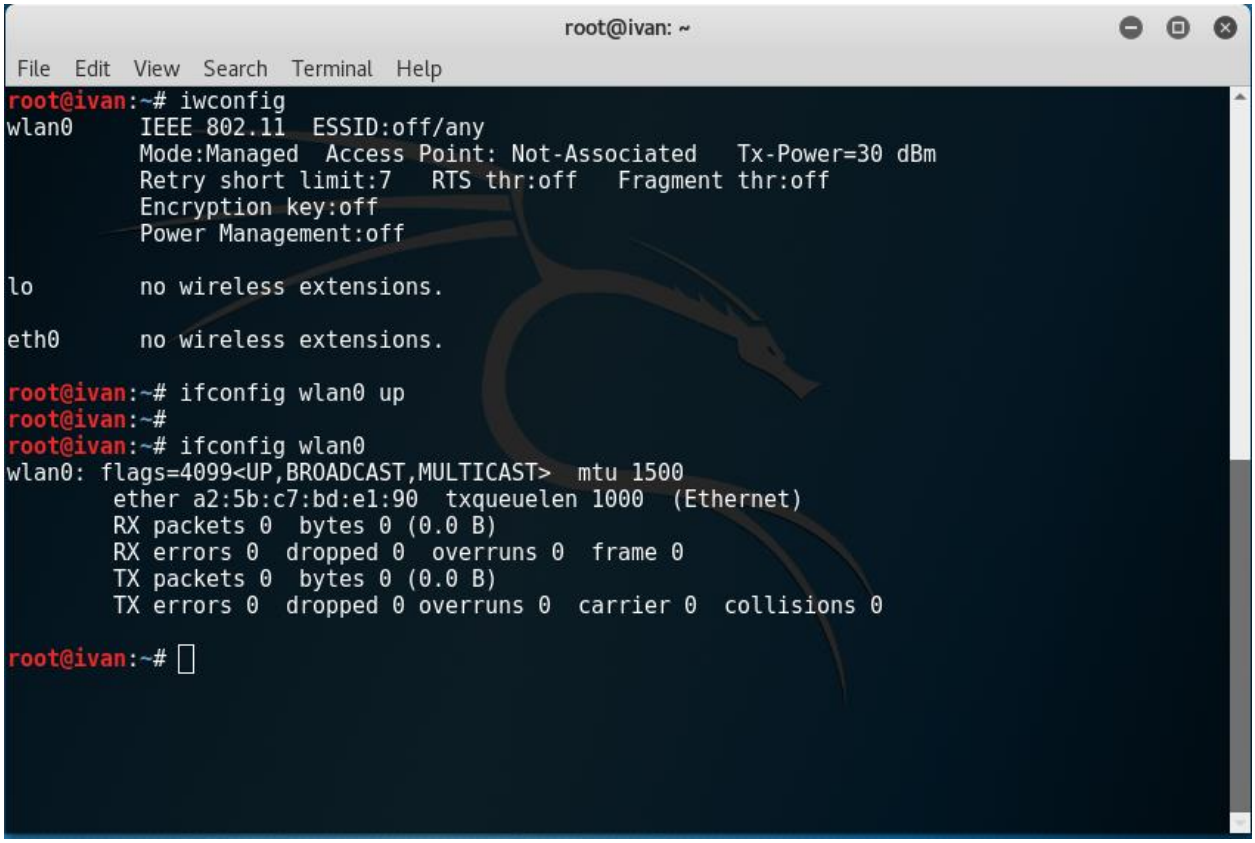
4.1. Nesigurnosti WLAN mreže

Jedna od osnovnih nesigurnosti WLAN mreže predstavlja zračni prijenos podataka jer je moguće osluškivati okvire WLAN paketa bežične mreže. Postoje tri vrste WLAN okvira [4]:

- Upravljački okviri: služe za održavanje komunikacije između pristupne točke i klijenata.
- Kontrolni okviri: osiguravaju odgovarajuću razmjenu podataka između pristupne točke i klijenata
- Podatkovni okviri: prenose stvarne podatke u bežičnoj mreži.

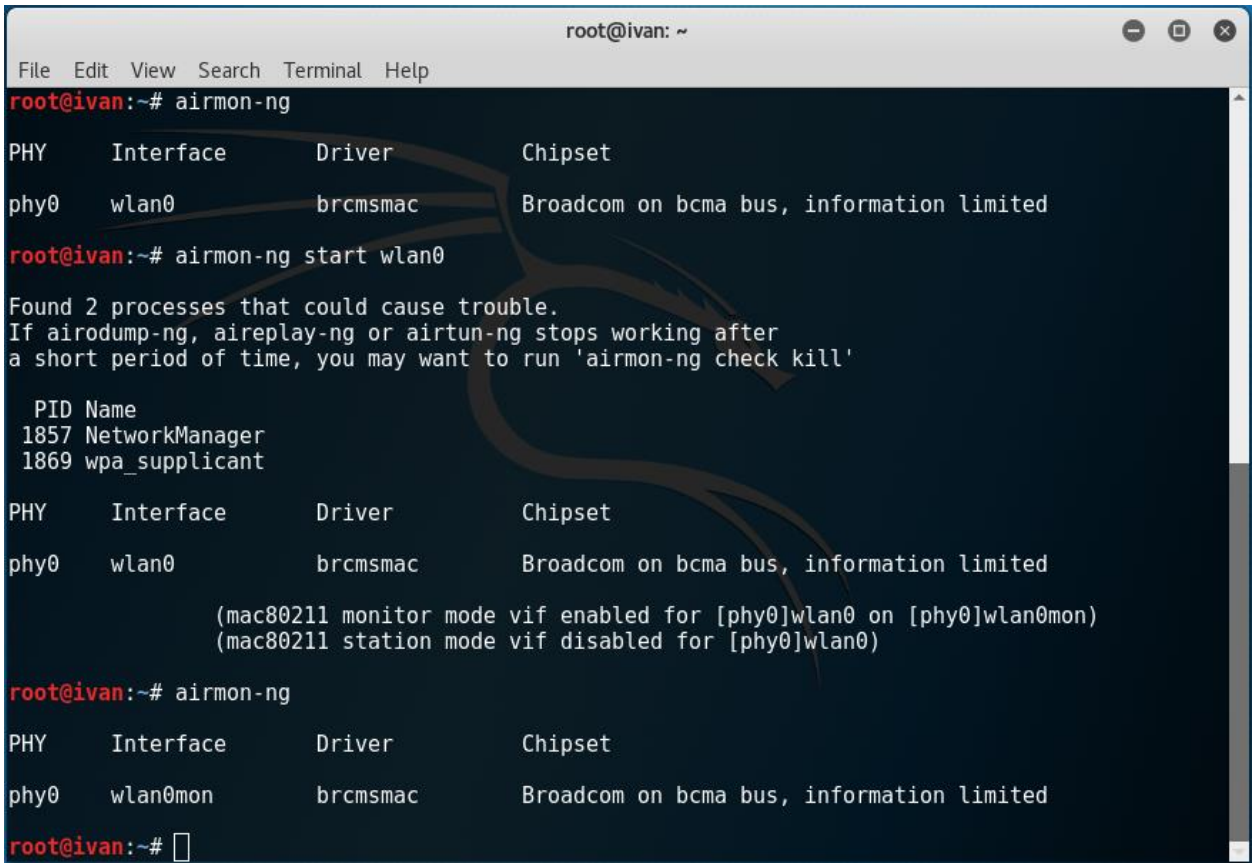
Prva dva oblika imaju i podfiltere, a osluškivanje navedenih okvira moguće je preko alata kao što je *Wireshark,* ali i drugih sa Kali-a kao što su *Airodump-NG, Tcpdump* ili *Tshark*. Prvi korak za osluškivanje je prebaciti mrežnu karticu u način rada osluškivanja. Međutim, kako bi se to moglo

učiniti potrebno je provjeriti i uspostaviti nekoliko postavki. Sve se naredbe unose u terminalu Kali-a. Unosom *iwconfig* moguće je provjeriti je li mrežna kartica aktivna i prepoznana on strane sustava.



Sl. 4.1. Prikaz terminala nakon izvođenja naredbi za provjeru postojanja i podizanja mrežne kartice

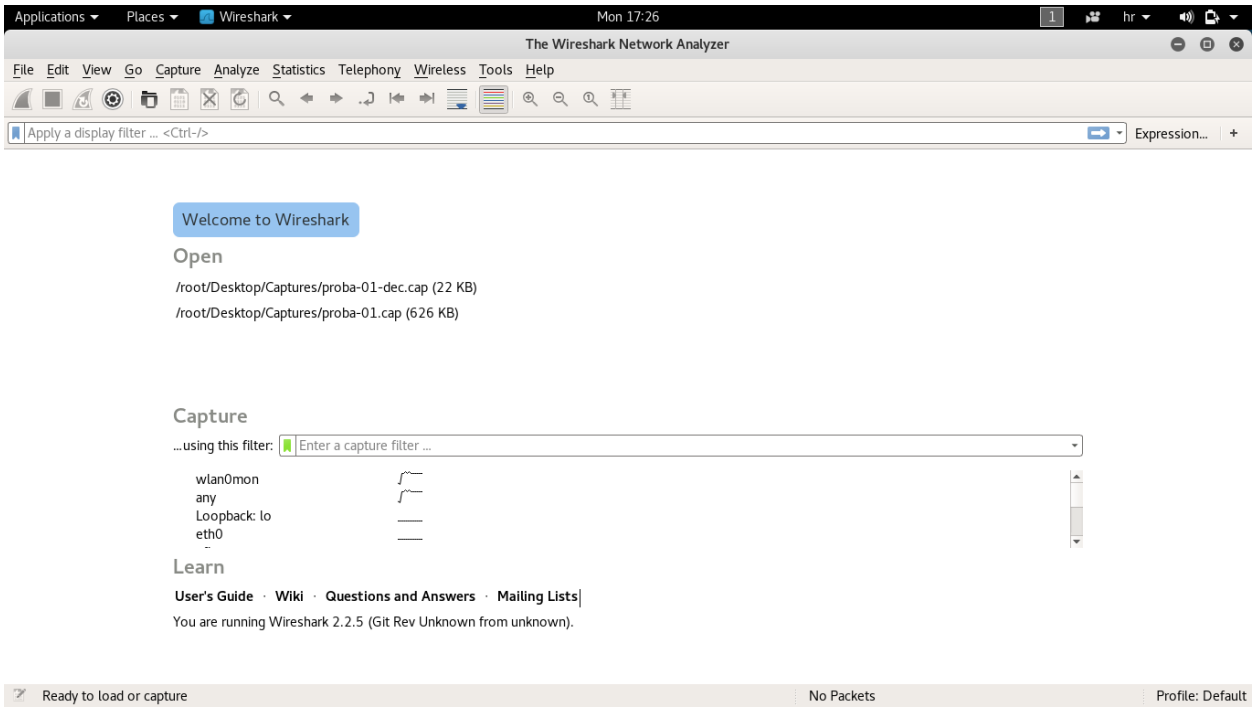
Na slici 4.1. vidimo da sustav prepoznaje mrežnu karticu kao wlan0, zatim ju je potrebno aktivirati naredbom *ifconfig wlan0 up* te provjeriti je li aktivna naredbom *ifconfig wlan0*. U prvom redu koji slijedi nakon posljednje naredbe vidi se ključna riječ *UP* što ukazuje na to da je mrežna kartica uspješno podignuta, odnosno aktivirana. Sada je moguće poduzeti mjere postavljanja načina rada osluškivanja. Slika 4.2. prikazuje naredbu *airmon-ng* kojom se ispituje prepoznaje li dostupne mrežne kartice. Sučelje wlan0 je na popisu pa je iduća naredba *airmon-ng start wlan0* što će sučelje prebaciti u način rada osluškivanja. Zatim je još jednom izvršena provjera novog sučelja naredbom *airmon-ng* te vidimo da se sada naziva *wlan0mon* što označava način rada osluškivanja (engl. *Monitor Mode*).



Sl. 4.2. Postupak prelaska u „Monitor mode“

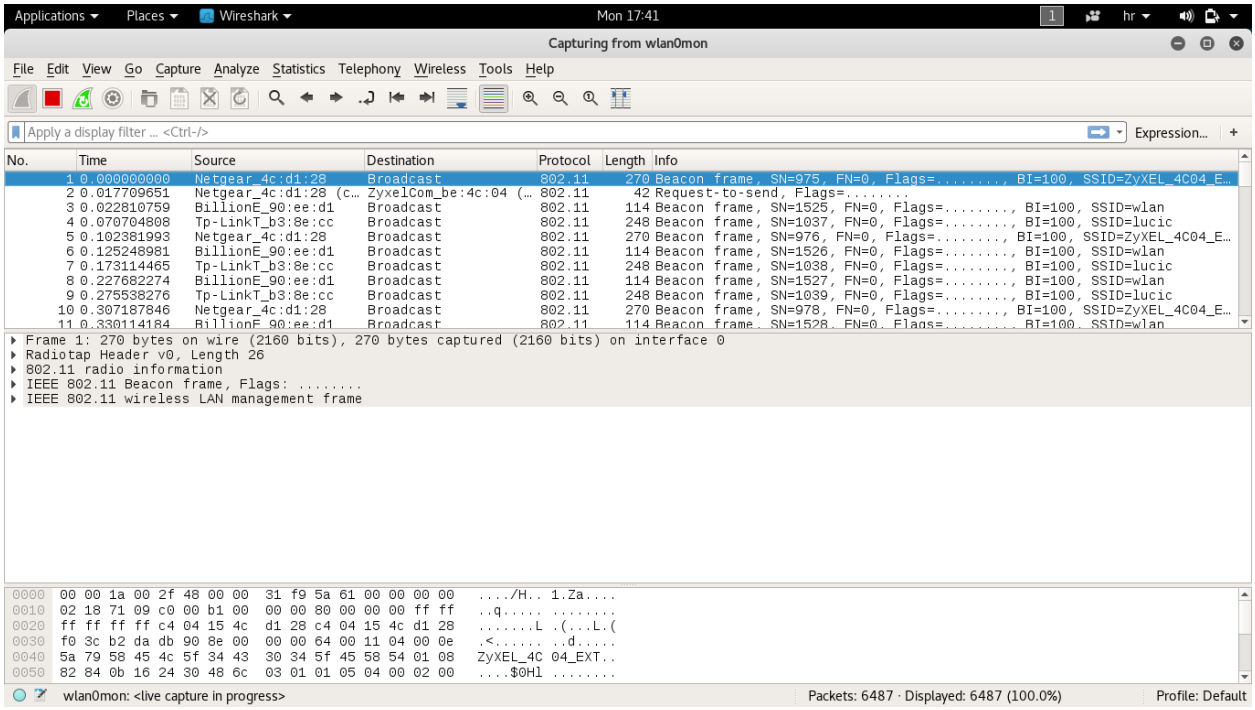
Prikazana su dva procesa koji će nakon određenog vremena isključiti način rada osluškivanja. Kada vide mrežnu karticu u osluškivanju reagiraju zato što znaju da to nije njena uobičajena funkcija i zato će mrežnu karticu vratiti u prvobitno stanje. Da se to ne dogodi, korisnik može isključiti utjecaj procesa naredbom *airmon-ng check kill*. Treba imati na umu, ako se kasnije izađe iz načina rada osluškivanja naredbom *arimon-ng stop wlan0mon,* da ugašene procese treba ponovno pokrenuti naredbom *service network-manager start*. Naredba *ifconfig wlan0mon* bi nakon svega trebala prikazivati postojanje novog sučelja. Na ovaj način uspješno je stvoreno sučelje u načinu rada osluškivanja s kojim će se hvatati, odnosno osluškivati paketi iz zraka.

Sada je potrebno pokrenuti Wireshark istoimenom naredbom u Kali terminalu. Kada se alat pokrene moguće je vidjeti stvoreno sučelje *wlan0mon* koje osluškuje sve pakete koji dolaze sa usmjerivača u dometu računala.



Sl. 4.3. Početni zaslon alata za osluškivanje paketa – *Wireshark*

Odabirom stvorenog sučelja sa slike 4.3. prikazat će se svi paketi koje je uhvatilo iz zraka, a odabirom jednog od paketa prikazuje se više informacija:



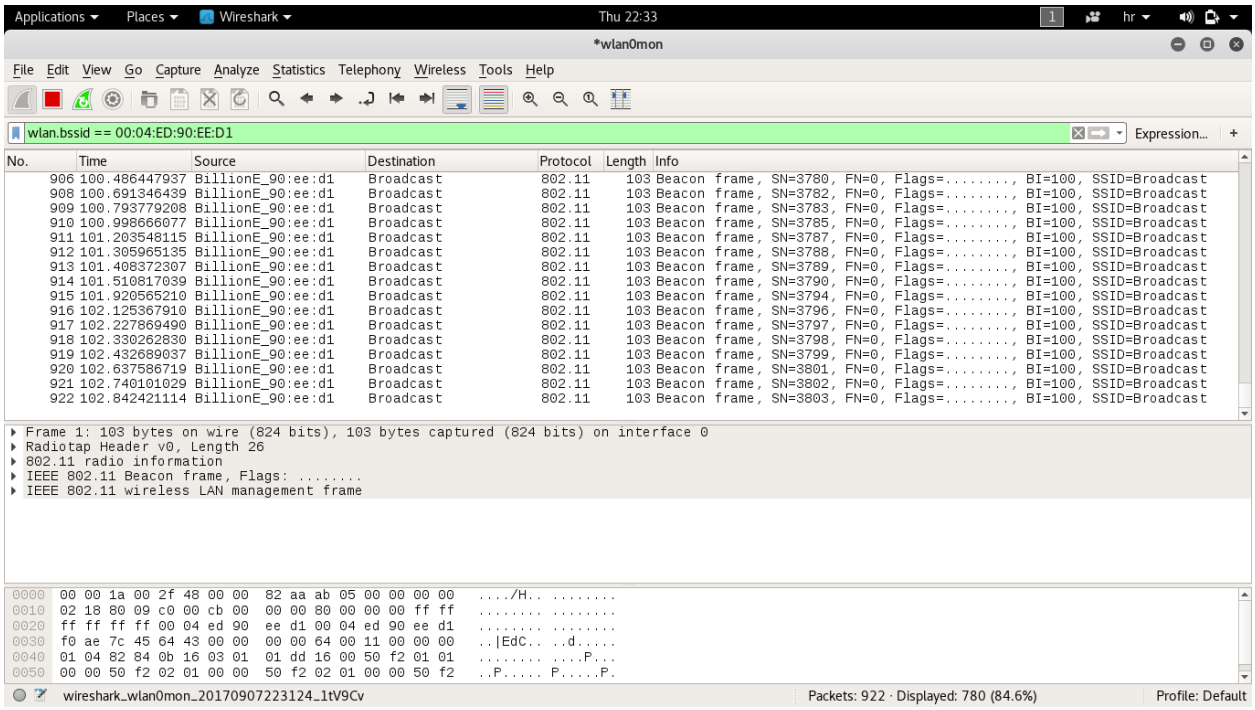
Sl. 4.4. Prikaz uhvaćenih paketa

Za prikaz spomenutih WLAN okvira moguće je unijeti određene filtere u traku za unos. Za upravljačke okvire izraz filtera je *wlan.fc.type == 0*, za kontrolne *wlan.fc.type == 1*, a za podatkovne *wlan.fc.type == 2*. Također je moguće kombinirati izraze za filtriranje operatorom && između njih. Filtere možemo iskoristiti i za prikazivanje prometa sa željenog usmjerivača unosom izraza *wlan.bssid == <MAC>* u polje za unos gdje *<MAC>* predstavlja MAC adresu usmjerivača. MAC adresu bilo kojeg usmjerivača u dometu vrlo je lako pronaći u terminalu Kali-a unosom naredbe *airodump-ng wlan0mon.* Prikazati će se MAC adrese usmjerivača, odnosno BSSID, kanali na kojim rade, način enkripcije koji koriste te naziv koji je dodijeljen usmjerivaču, odnosno ESSID. U drugoj polovici prozora moguće je vidjeti i MAC adrese uređaja koji su trenutno spojeni na usmjerivače i s njima razmjenjuju pakete. Ove informacije se mogu iskoristiti za napad na lozinku za spajanje na usmjerivač, no to će biti objašnjeno kasnije u radu. Trenutno je potrebno kopirati MAC adresu željenog uređaja i pokrenuti ponovno Wireshark. Zatim se u polje za unos filtera unese izraz (*wlan.bssid == <MAC>*) što prikazuje sve pakete koje šalje usmjerivač, a ako se na prethodni izraz doda sljedeći izraz uz operator: *&&* (*wlan.fc.type_subtype == 0x20*) prikazat će se svi paketi usmjereni prema usmjerivaču.

Ako podaci nisu šifrirani, osluškivanje paketa omogućuje vrlo jednostavnu analizu razmijenjenih podataka. Napadači uz ovaj postupak podatke u *Wireshark*-u vide kao čitljivi tekst te se iz tog razloga podaci u bežičnim mrežama moraju šifrirati. Svi korisnici unutar radio frekvencijskog dometa pristupne točke mogu vidjeti sve podatke ako koriste neki način osluškivanja prometa što predstavlja veliki sigurnosni problem.

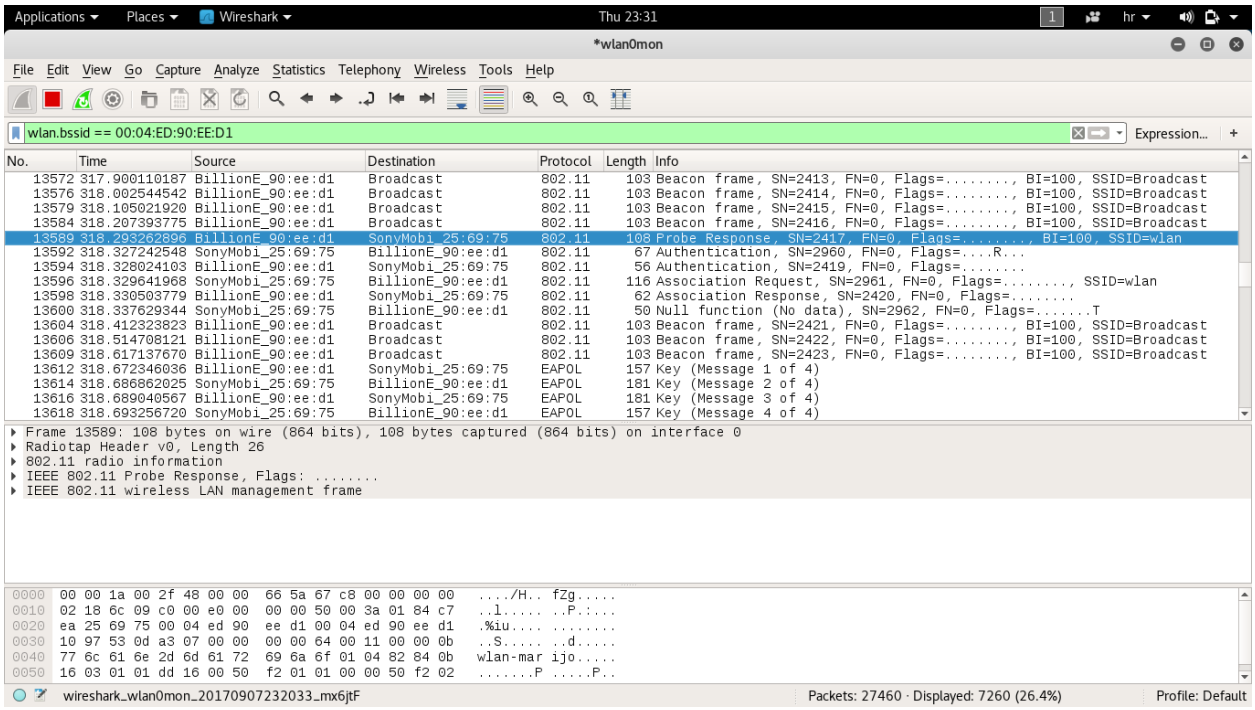
4.2. Zaobilaženje WLAN ovjere

Svakom usmjerivaču dodijeljen je SSID koji predstavlja čovjeku čitljivu identifikacijsku oznaku bežičnog usmjerivača. Drugim riječima, SSID je ime koje je dodijeljeno usmjerivaču te ga se pod tim imenom nalazi kada se želi spojiti na mrežu. Uobičajena postavka svih usmjerivača je da javno šalju svoj SSID. Jedna od mjera zaštite je prema tome u postavkama usmjerivača sakriti SSID, tj. onemogućiti njegovo javno širenje. Na slici 4.4. prikazan je primjer uhvaćenih paketa preko *Wireshark*-a i u trećem retku prikazan je uređaj „Billion“ koji ima SSID „wlan“, a kada se u postavkama SSID onemogući, na istom uređaju SSID je označen kao „Broadast“, odnosno sakriveno je ime usmjerivača.



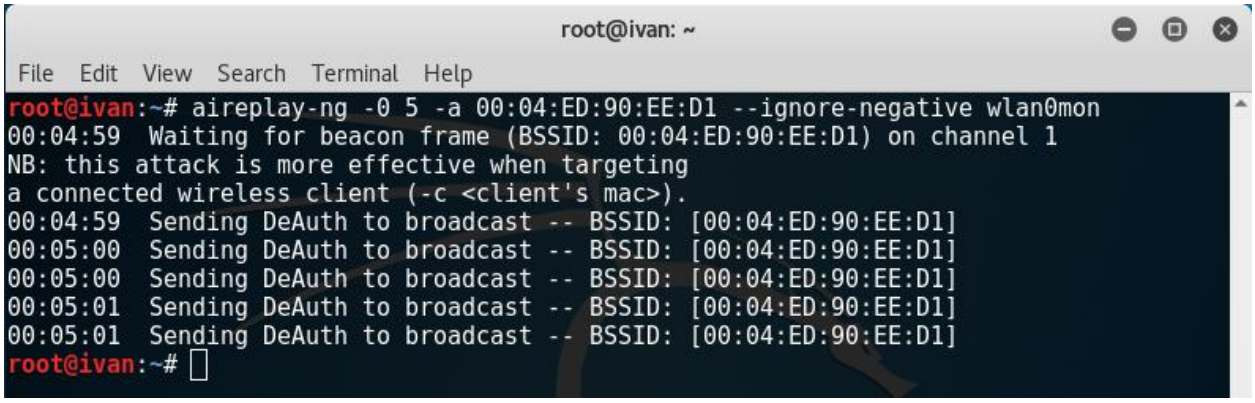
Sl. 4.5. Prikaz uhvaćenih paketa nakon prikrivanja SSID-a

Skriveni SSID znači da se na određeni uređaj mogu spojiti samo korisnici koji znaju za njegovo postojanje. Mnogi mrežni administratori prema tome smatraju kako je skriveni SSID dovoljna mjera zaštite od napada, međutim preko Kali-a ga je lako otkriti. Koristi se pasivna tehnika čekanja prijave nekog korisnika na odgovarajući usmjerivač. Korisnik i usmjerivač izmijenit će pakete u kojima je sadržan SSID mreže te tako otkriti njegovo postojanje što je prikazano na slici 4.6.

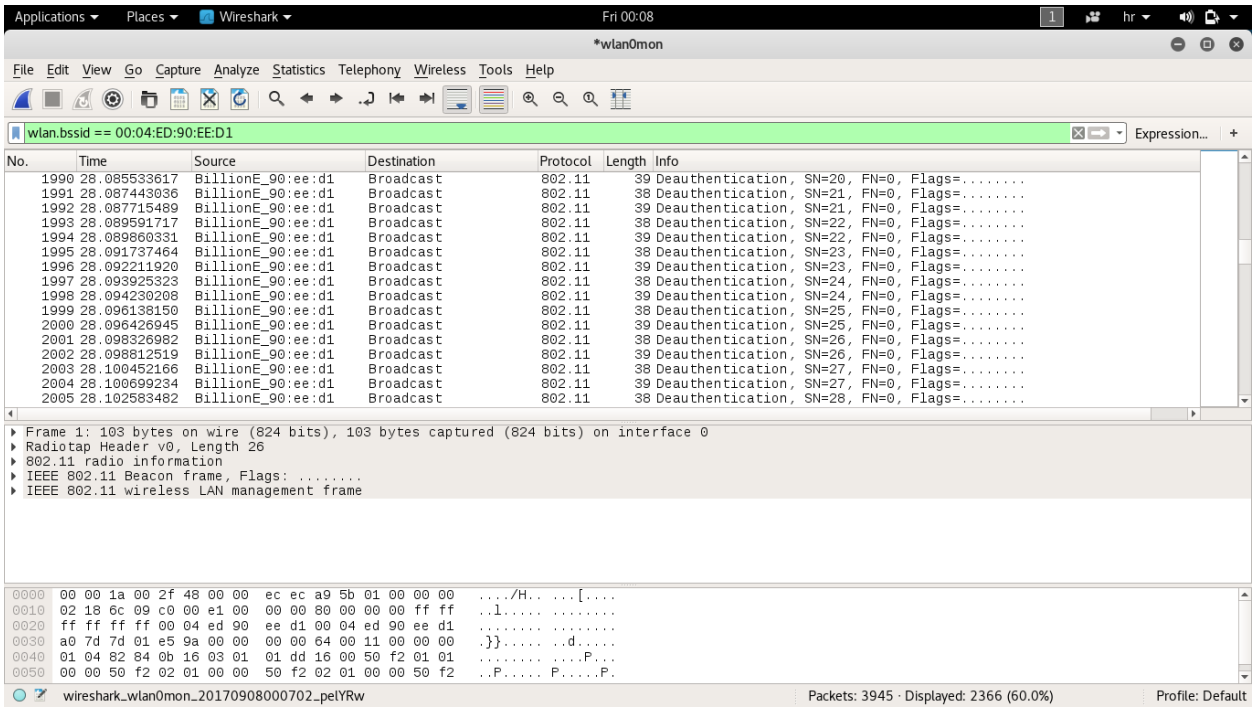


Sl. 4.6. Paketi sa informacijama o SSID-i nakon prijave korisnika

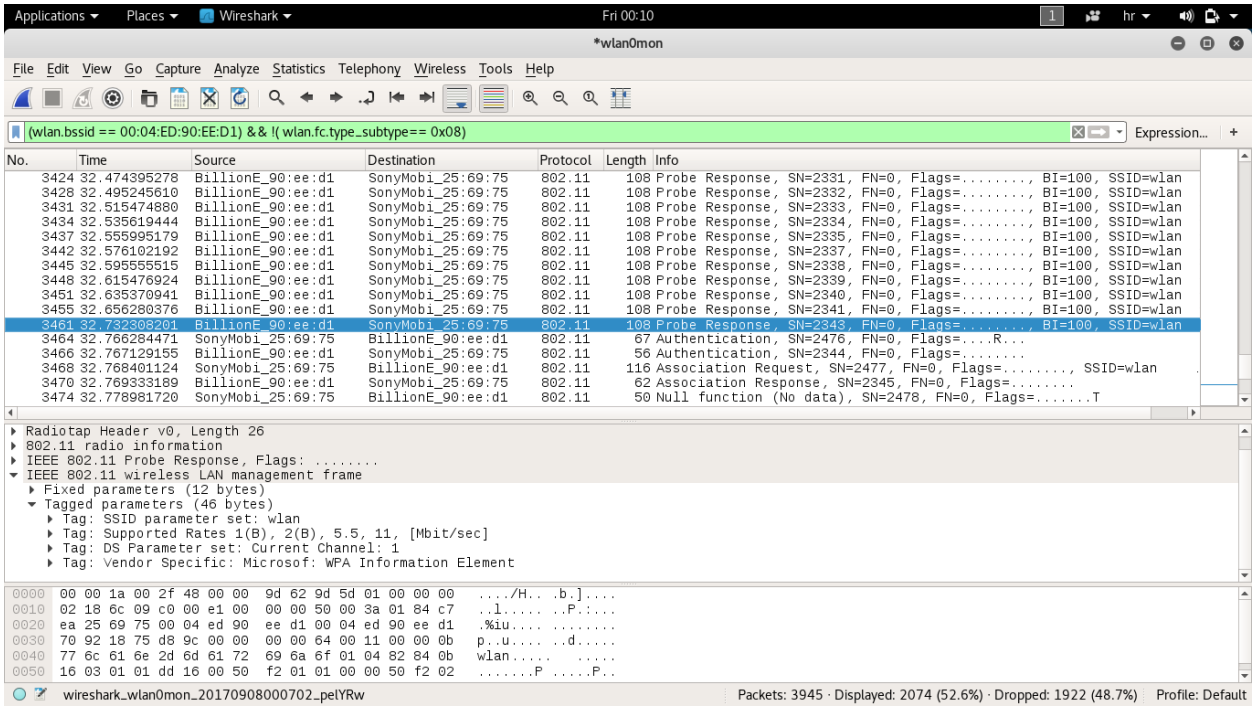
Moguće je i izbjeći tehniku čekanja prisilnim prekidanjem konekcije korisnika na usmjerivač preko Kali terminala naredbom *aireplay-ng -0 5 -a <MAC_usmjerivača> --ignore-negative wlan0mon*, gdje *-0* označava da je riječ o slanju deautentikacijskih poruka pa broj *5* označava koliko ih se šalje. Kada se pošalju sve poruke doći će do ponovnog spajanja korisnika što će u *Wireshark*-u dovesti do prikaza SSID-a kao na slici 4.6.



Sl. 4.7. Prekidanje konekcije svim korisnicima na ciljanom usmjerivaču



Sl. 4.8. Deautentikacijski paketi u Wireshark-u



Sl. 4.9. Uhvaćeni paketi nakon ponovnog spajanja i prikaz SSID-a

Iako je SSID skriven, prilikom svakog pokušaja spajanja korisnika na mrežu izmijeniti će se paketi sa usmjerivačem koji sadrže informacije o SSID-u pristupne točke. Kako takvi paketi nisu kodirani

hvatanjem iz zraka, tj. osluškivanjem se lako dolazi do SSID-a što znači da skriveni SSID nije dovoljno dobra zaštita od napada.

Za zaštitu se često koriste i MAC filteri koji se sastoje od popisa MAC adresa uređaja. Zadaća im je ograničiti pristup svim uređajima koji nemaju na popisu. Pokuša li se spojiti uređaj čija MAC adresa nije na popisu spajanje neće uspjeti što će u *Wireshark*-u prikazati slanje poruka neuspješnog spajanja prema klijentu od strane usmjerivača. MAC filteri se u Kali-u mogu zaobići korištenjem naredbe *airodump-ng* koja je spomenuta u prethodnom dijelu. Ona će ispisati MAC adrese svih usmjerivača u dometu te svih uređaja spojenih na usmjerivače. Kako bi se ograničili informacijama samo jednog ciljanog usmjerivača moguće je specificirati naredbu na sljedeći način: *airodump-ng -c 1 -a --bssid <MAC> wlan0mon*. Na mjestu *<MAC>* ide MAC adresa usmjerivača kojeg se želi promatrati, -c predstavlja definiranje kanala na kojem uređaj radi, -a označava da se prikažu samo oni uređaji koji su spojeni na odgovarajući usmjerivač. Na taj način napadač može saznati MAC adrese koje su dozvoljene za spajanje na ciljani usmjerivač. Zatim u terminalu Kali-a naredbom *macchanger* može postaviti MAC adresu svojeg uređaja na adresu uređaja koji ima pravo pristupa na usmjerivač. To je dokaz kako ni MAC filteri nisu siguran način zaštite od napada.

U slučaju postojanja nezaštićene mreže napadač se u Kali terminalu može spojiti na ciljanu mrežu jednostavnim upisom SSID-a sljedećom naredbom: *iwconfig wlan0 essid <SSID_uređaja>*. Nema potrebe za bilo kakvim korisničkim imenom ili lozinkom, nego odmah može potvrditi da je spajanje uspjelo.

Još jedan način za zaštitu predstavlja ovjera dijeljenim ključem koja koristi dijeljeni tajni ključ za ovjeru korisnika. Kada klijent pristupnoj točki pošalje zahtjev za povezivanjem, pristupna točka uzvraća sa tekstualnom porukom. Klijent zatim treba tu tekstualnu poruku šifrirati sa dijeljenim ključem i poslati nazad prema pristupnoj točki koja dekodira poruku kako bi provjerila može li doći do izvorne poruke. Ako dekodiranje uspije pristupna točka dozvoljava pristup klijentu, u suprotnom odbija pristup. Odmah se može zaključiti kako napadač može cijelu tu komunikaciju osluškivati i tako doći do izvorne poruke kao i šifrirane poruke. Primjenom logičke operacije „isključivo ili“ – XOR dolazi do ključnog niza kojeg može iskoristiti za kodiranje budućih poruka slanih od strane pristupne točke, bez da mu je potreban pravi ključ. Najčešći oblik dijeljenog ključa je WEP (engl. *Wired Equivalent Protocol*) koji je lako probiti, a i kreirano je mnogo alata koji uspješno probijaju WEP način zaštite.

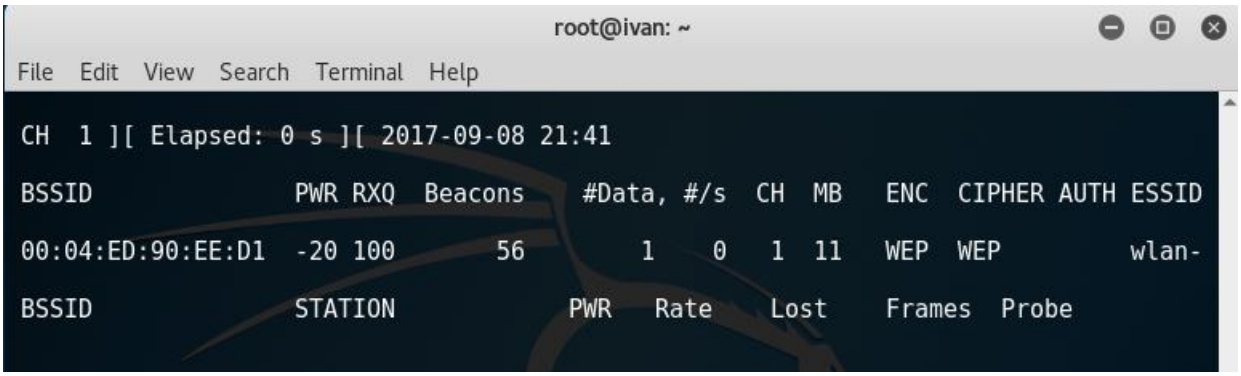
4.3. Nedostatci WLAN enkripcije

Kako se u WLAN mreži podaci prenose zrakom, najbolji način zaštite je nekakav oblik enkripcije. Postoje spomenuti WEP, WPA (engl. *Wi-Fi Protected Access*) i WPAv2 (engl. *Wi-Fi Protection Access v2*) protokoli za zaštitu podataka. U nastavku će biti prikazani nedostaci tih protokola i način njihovog probijanja u Kali-u.

WEP predstavlja sigurnosni algoritam za IEEE 802.11 bežičnu mrežu koji nije izrazito snažan oblik zaštite, čak ni u vrijeme izdavanja. Ograničenja Sjedinjenih Država u izvozu razne kriptografske tehnologije razlog su zbog kojih su proizvođači ograničavali svoje uređaje na 64-bitnu enkripciju. Kada su ograničenja podignuta enkripcija se diže na 128-bitnu, a unatoč uvođenju 256-bitnog WEP-a, ostaje jedna od najčešćih implementacija. Standardni 64-bitni WEP koristi 40-bitni ključ koji je ulančan sa 24-bitnim inicijalizacijskim vektorom kako bi se formirao RC4 ključ. Ključ se obično unosi kao niz od 10 heksadekadskih znakova gdje svaki znak čine 4 bita. 10 znakova po 4 bita zajedno sa 24-bitnim vektorom čini traženih 64 bita WEP ključa. Za razliku od toga, 128-bitni ključ je niz od 26 heksadekadskih znakova.

Nedostatci WEP protokola su poznati već dugo, ali se ipak koristi i dalje te se još uvijek proizvode usmjerivači postavljeni na zaštitu WEP protokolom. U Kali-u se WEP može probiti korištenjem cijele porodice *aircrack-ng* naredbi kao što su npr. do sad poznati *airmon-ng*, ali i *aireplay-ng, airodump-ng* i dr. Glavna slabost WEP protokola je korištenje RC4 algoritma i kratkog inicijalizacijskog vektora koji se reciklira svakih 224 okvira. RC4 predstavlja simetrični kriptografski algoritam toka koji kodira ulazne podatke bit po bit, a kodirani tekst rezultat je logičke operacije XOR između izvornog teksta i pseudo-slučajnih brojeva generiranih na temelju ključa. Inicijalizacijski vektor u kriptografiji predstavlja ulaznu vrijednost stalne veličine koja često treba biti slučajna. Kako je broj 224 velik sam po sebi postoji 50% šanse da će se vektor ponoviti 4 puta u svakih 5000 paketa. To se može iskoristiti generiranjem velikog prometa kako bi se povećala vjerojatnost pojavljivanja ponovljenih inicijalizacijskih vektora. Na taj način moguće je usporediti dva šifrirana teksta kodirana istim inicijalizacijskim vektorom i ključem.

Kako bi testirali probijanje WEP ključa potrebno je prvo u postavkama usmjerivača postaviti WEP kao oblik zaštite. Odabran je 128 bitni WEP ključ i dodijeljena mu je lozinka: 11111222223333344444555556. Idući korak je u terminalu Kali-a postaviti sučelje za osluškivanje koje je spomenuto prije u radu. Naredbama *ifconfig wlan0 up,* i *airmon-ng start wlan0* osigurava se kreiranje sučelja za osluškivanje. Naredbom *airodump-ng wlan0mon* može se vidjeti da je uređaj koji ima SSID „wlan“ šifriran WEP-om.

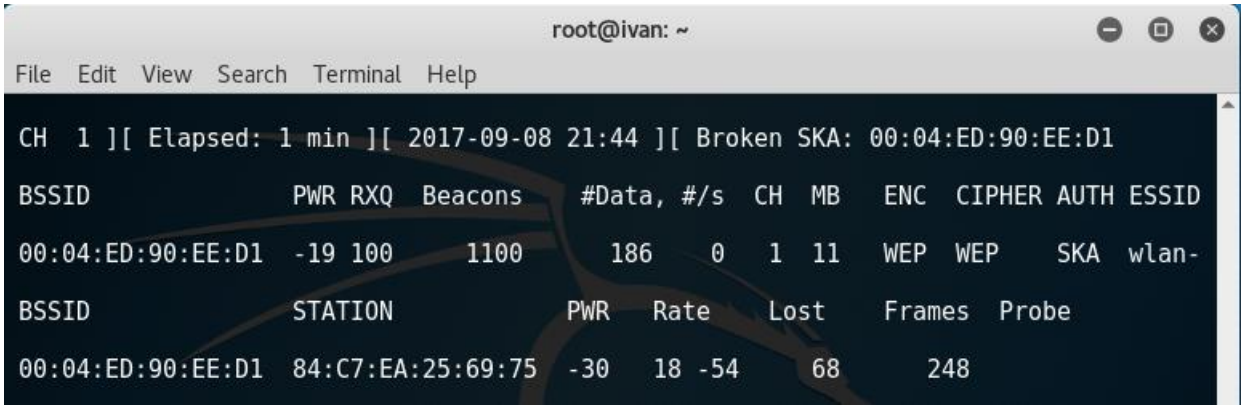


Sl. 4.10. Prikaz usmjerivača postavljen na WEP zaštitu

Od interesa je dakle samo uređaj „wlan“ pa će se njegova MAC adresa upisati u iduću naredbu s kojom se „write“ dijelom dodatno traži od *airodump-ng* da rezultate osluškivanja spremi kao datoteke pod nazivom „WEPPokusajProbijanja“. Izraz je sljedeći:

airodump-ng -bssid <MAC_usmjerivača> --channel 1 --write WEPPokusajProbijanja wlan0mon

Spoji li se sada neki korisnik u mrežu unosom WEP lozinke za spajanje, *airmon-ng* će primijetiti aktivnost.

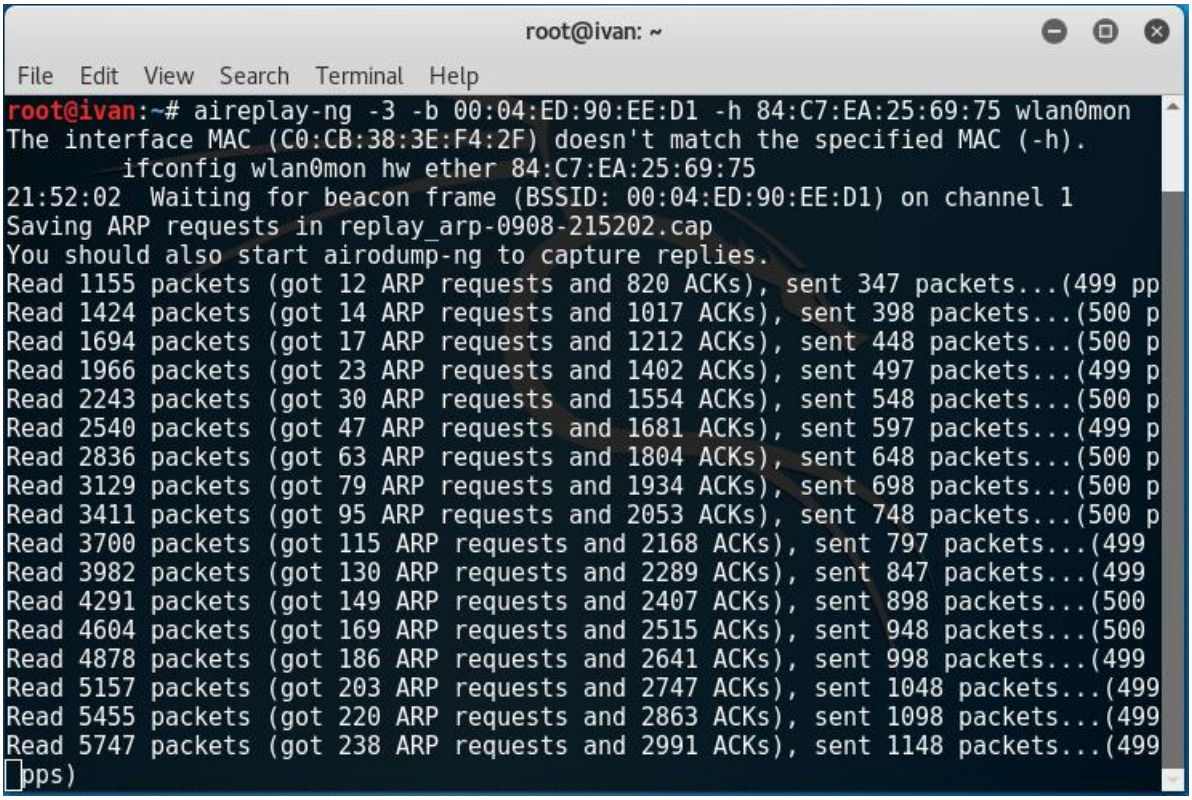


Sl. 4.11. Prikaz nakon spajanja uređaja na usmjerivač

U tom trenutku se kreiraju datoteke „WEPPokusajProbijanja-01“ sa nastavcima *.cap*, *.csv*, *.kismet.csv* i *.kismet.netxml*. Svaka od njih ima drugačiji prikaz uhvaćenih informacija, a za daljnju razradu će se koristiti datoteka sa .cap nastavkom. Na slici 4.11. broj pod stupcem „*#Data*“ označava broj inicijalizacijskih vektora koji su se do sada poslali. Budući da probijanje WEP-a zahtijeva velik promet, odnosno veliku količinu podatkovnih paketa kodiranih istim ključem, potrebno je prisiliti mrežu da proizvodi više paketa. U Kali-u je to moguće učiniti *aireplay-ng* naredbom koja hvata ARP pakete bežične mreže i ponovno ih vraća u mrežu kako bi se simulirali ARP odgovori. U novom prozoru terminala koristi se naredba:

aireplay-ng -3 -b <MAC_usmjerivača> -h <MAC_spojenog_uređaja> wlan0mon,

gdje *-3* označava ARP odgovore, *-b* je BSSID ciljane mreže, a *-h* predstavlja MAC adresu klijenta kojeg se osluškuje.

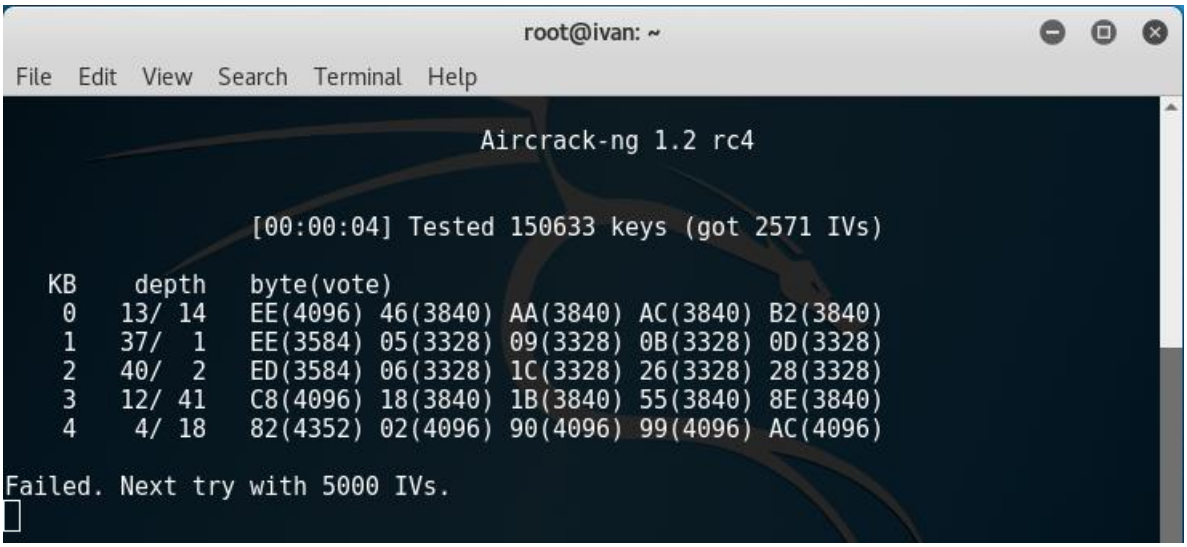


Sl. 4.12. Popunjavanje mreže paketima naredbom *aireplay-ng*

Od ovog trenutka *airmon-ng* počinje prikazivati velik broj paketa, a svi oni se spremaju u kreirane datoteke koje su nazvane „WEPPokusajProbijanja“. Sada se može započeti sa stvarnim pokušajem probijanja. U novom prozoru terminala koristi se naredba:

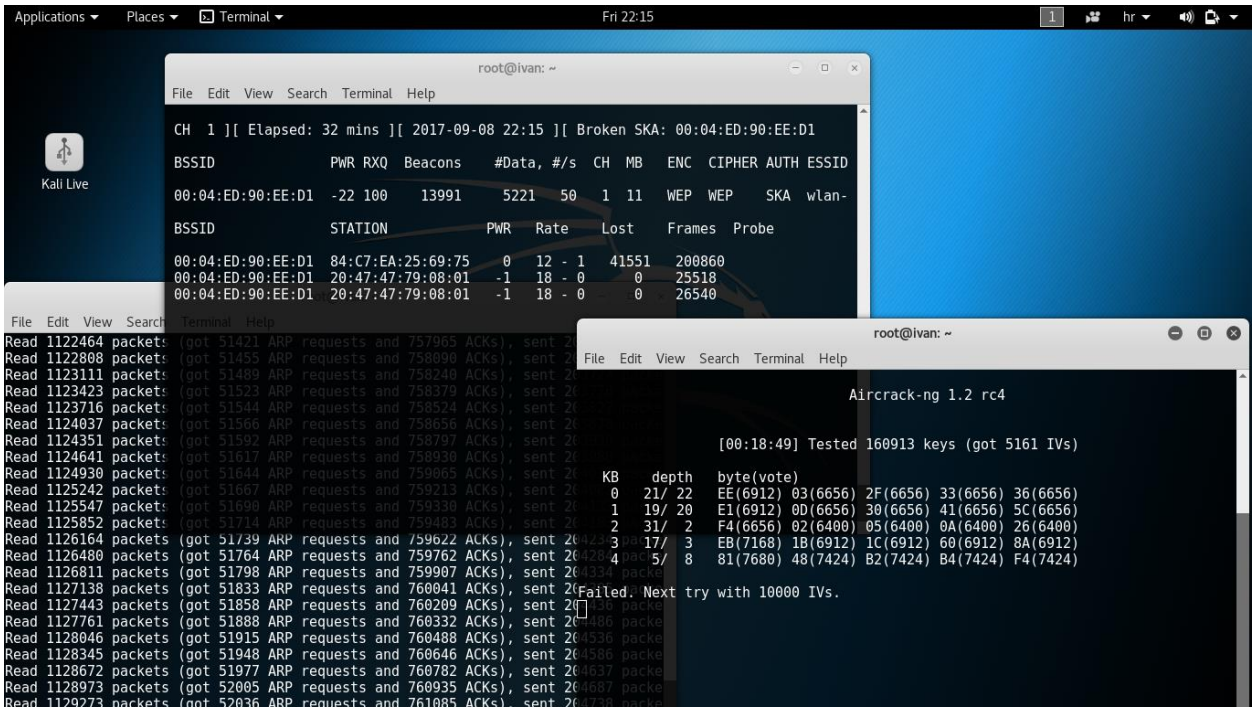
aircrack-ng WEPPokusajProbijanja-01.cap,

što će započeti postupak probijanja WEP lozinke koristeći podatkovne pakete iz kreirane datoteke.



Sl. 4.13 Prvi pokušaj probijanja WEP lozinke

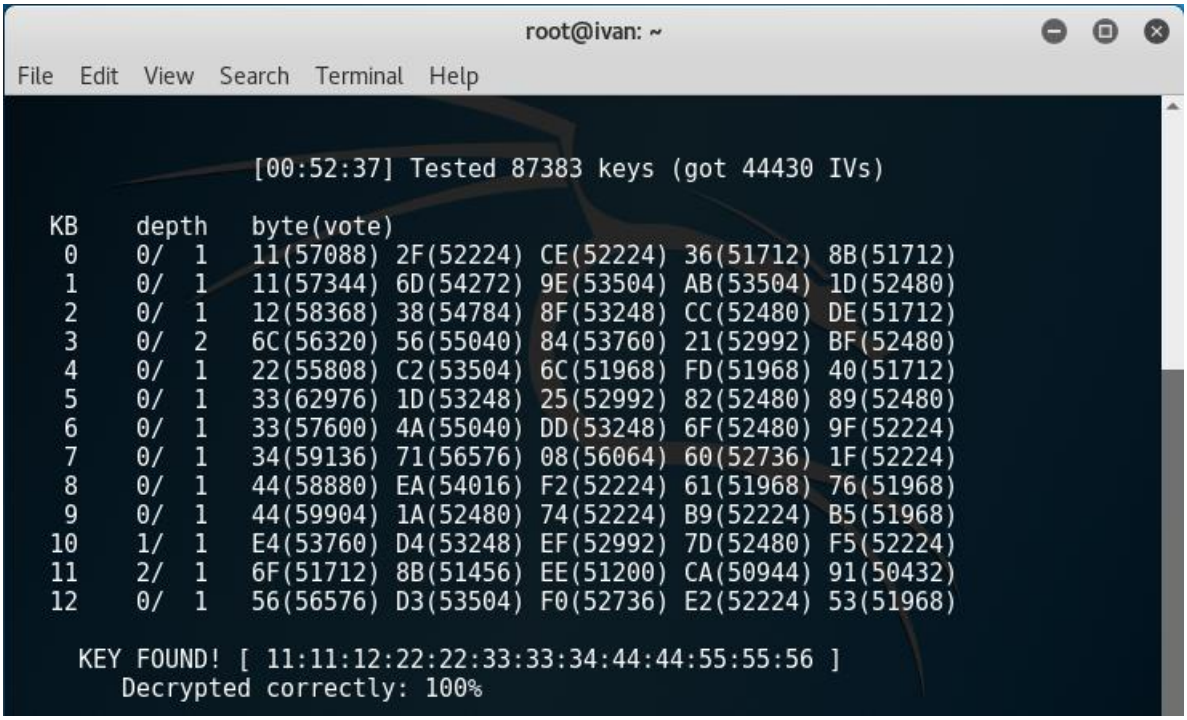
Airodump-ng kupi WEP pakete, *aireplay-ng* ponavlja slanje paketa, a *aircrack-ng* pokušava probiti WEP na osnovu uhvaćenih paketa. Rade u isto vrijeme u odvojenim prozorima terminala:



Sl. 4.14. Rad svih alata zajedno

Postupak obrade paketa *aircrack-ng* alata prikazan je na slici 4.13. U vrlo kratkom roku obradi sve do sad dostupne inicijalizacijske vektore, a u slučaju neuspjeha se zaustavlja i čeka hvatanje više paketa. Ponovni pokušaj započinje nakon svakih 5000 uhvaćenih vektora.

Trajanje postupka probijanja ovisi o brzini mreže, te se nakon uspjeha u terminalu ispisuje jasna poruka o pronalasku ključa uz ispis njegovog izgleda. U vlastitom pokušaju testiranje je trajalo 52 minute i 37 sekundi, a uspjelo je nakon 44430 uhvaćenih inicijalizacijskih vektora i ispisana je lozinka 11:11:12:22:22:33:33:34:44:45:55:55:56 koja je i postavljena u postavkama usmjerivača prije testiranja. Koliko god ključ bio složen, navedenim postupkom uvijek će biti probijen.



Sl. 4.15. Prikaz uspješno provedenog napada

WPA je bio izravan odgovor na sve ranjivosti WEP protokola, a time i njegova zamjena. Koristi 256-bitni ključ, te uvodi provjeru integriteta poruka kako bi se utvrdilo je li napadač uhvatio ili izmijenio pakete koji su prošli između pristupne točke i klijenta. Uvodi se i TKIP (engl. *Temporal Key Integrity Protocol*) koji koristi sustav ključa po paketu, što se pokazalo znatno sigurnijim od fiksnog ključa koji koristi WEP. TKIP kasnije zamjenjuje mnogo snažniji AES (engl. *Advanced Encryption Standard*). Unatoč tome što je značajno poboljšanje u odnosu na WEP dokazane su osjetljivosti na upad. TKIP je dizajniran tako da nadogradnjom reciklira određene elemente koji se koriste u WEP sustavima, a oni se mogu iskoristiti za probijanje ključa. Čest napad na WPA je preko WPS-a (engl. *Wi-Fi Protected Setup*) koji omogućava jednostavno povezivanje uređaja na suvremene pristupne točke.

Za razliku od WPA, WPA2 zahtijeva obavezno korištenje AES algoritma, a predstavljen je i CCMP (engl. *Counter Cipher Mode Protocol*) kao zamjena za TKIP. Međutim, TKIP se i dalje

koristi u WPA2 enkripciji kao sustav za suradnju sa WPA-om. Trenutna sigurnosna ranjivost WPA2 zahtijeva da je napadač spojen na bežičnu mrežu kako bi dobio pristup određenim ključevima i bio u mogućnosti provesti napad nad drugim uređajima u mreži. Prema tome se može zaključiti kako je ranjivost unutar kućne mreže gotovo nepostojana. Međutim, ostaje jednaka ranjivost kao i za WPA preko WPS-a. Probijanje zahtijeva od 2 do 14 sati neprekidnog napora modernog računala pa je preporuka onemogućiti WPS i nadograditi uređaj na takav način da ga uopće ne podržava što će u potpunosti ukloniti mogućnost napada.

U Kali-u je test probijanja sličan kao i za WEP, jedina je razlika u tome što su WPA/WPA2 PSK ranjivi na napade uz pomoć rječnika. Ulazne vrijednosti koje su potrebne za napad su četverostruko rukovanje između pristupne točke i klijenta i popis čestih lozinki. WPA/WPA2 PSK po sjednici izvlače ključ PTK (engl. *Pairwise Transient Key*) koristeći PSK i dodatnih pet parametara: SSID mreže, ANounce, SNounce, MAC adresu pristupne točke i MAC adresu klijenta. Taj se ključ potom koristi za kodiranje svih podataka između pristupne točke i klijenta [4]. Napadač koji osluškuje cijelu komunikaciju hvatanjem paketa iz zraka može doći do svih pet parametara. Jedina stvar koja mu nedostaje je PSK.

Postupak testiranja napada sličan je kao i za WEP. Postavlja se sučelje za osluškivanje i čeka se prijava korisnika na mrežu. Kako bi se ubrzao postupak moguće je prisilno odjaviti sve korisnike te izazvati njihovo ponovno spajanje deautentikacijskim porukama što je već prikazano prije u radu. Kada dođe do prijave *airodump-ng* će uhvatiti i prikazati postojanje rukovanja (engl. *Handshake*). Za pokušaj probijanja moguće je koristiti popise čestih lozinki sa Kali-a, ali treba imati na umu kako postoji mogućnost da to neće biti dovoljno za uspjeh. U *aircrack-ng* naredbi se poziva datoteka koja je spremala uhvaćene pakete uz poziv na datoteku koja sadrži popis lozinki koja, ovisno o jačini, može biti veličine i do jednog TB. Lozinke korisnika ovise o mnogo čimbenika, a neki od njih su država u kojoj žive, česta imena i fraze vezane za to područje, sigurnosna shvaćanja i slično. Potrebno je prema tome koristiti popise koji su odgovarajući, a tražena lozinka mora biti unutar popisa. Iz toga se može zaključiti da je uspjeh probijanja ovisan od jačine popisa lozinki koji se pri probijanju koristi. Za razliku od WEP-a koji se može probiti uvijek, WPA/WPA2 PSK se smatraju, kriptografski gledano, neprobojnim. Jedini način je u slučaju slabe lozinke kada napad može uspjeti korištenjem popisa čestih lozinki.

4.4. Napadi na WLAN infrastrukturu

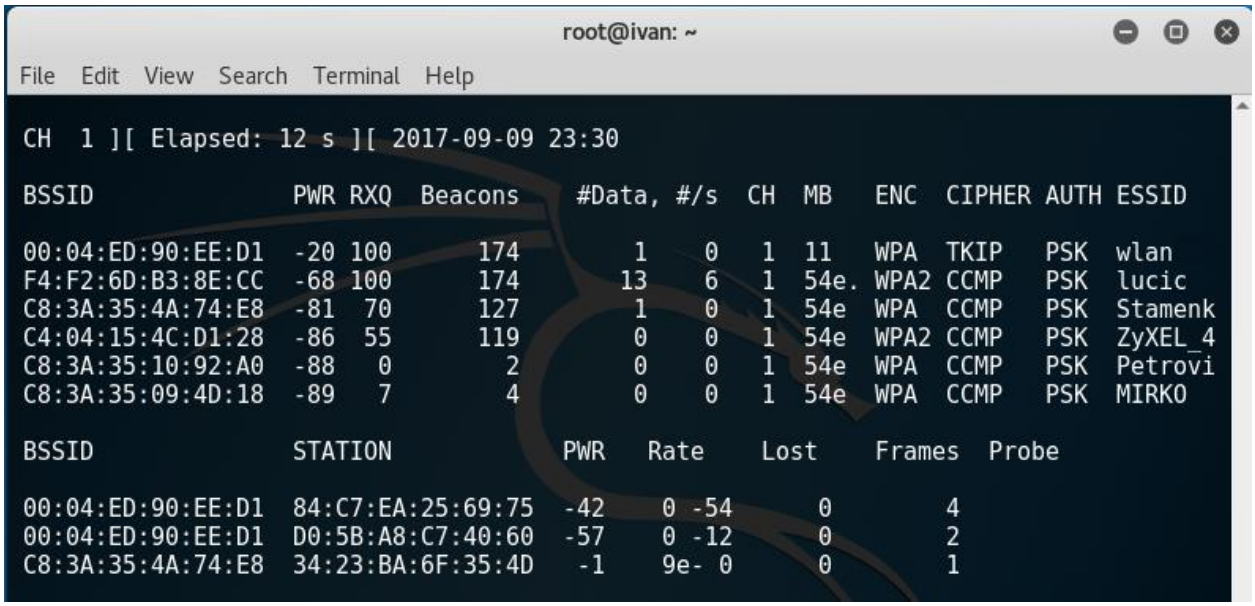
WLAN infrastruktura pruža bežične usluge svim korisnicima WLAN mreže u nekom sustavu i postoje različiti načini napada na nju. Jedna od čestih mjesta napada su korisničko ime i lozinka

samog usmjerivača, odnosno pristupne točke. Pristupna točka predstavlja osnovni element infrastrukture. Usprkos tome često se zanemari važnost promjene uobičajenih postavki. Korisničko ime i lozinka spajanja za ulaz u postavke usmjerivača mogu se pronaći na stranicama proizvođača uređaja pa je preporuka promijeniti ih kako se ne bi izgubila potpuna kontrola nad uređajem.

Još jedan oblika napada je uskraćivanje usluga spomenut prije u radu. Slanjem poruka deautentikacijskih poruka prisiljavaju se korisnici na odjavu i tako sprečava njihov pristup mreži. Moguće je jednostavno nastaviti uskraćivati uslugu korisnicima, ili iskoristiti ponovnu prijavu za druge oblike napada.

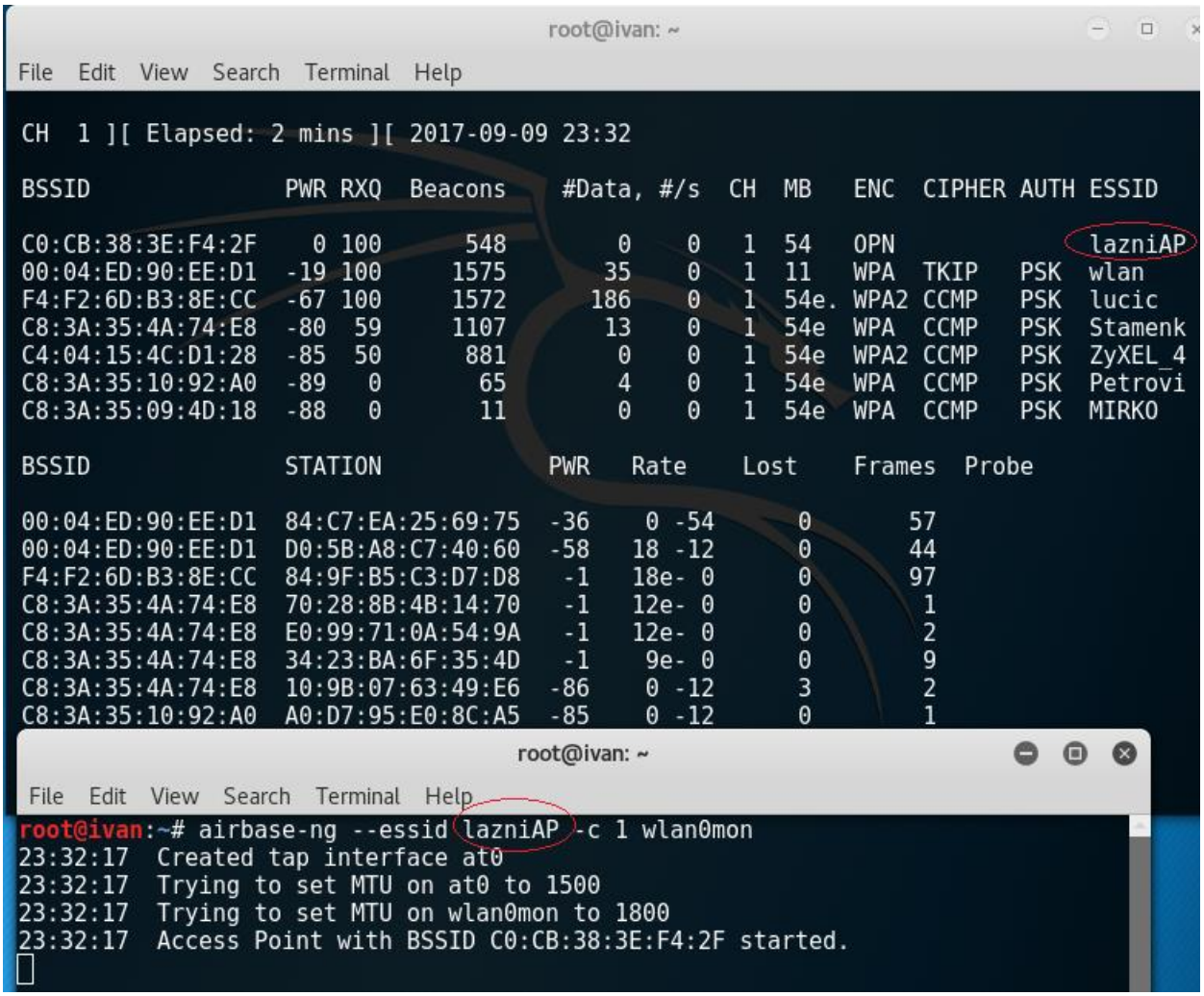
Najmoćnijim napadom na infrastrukturu smatra se stvaranje kopije pristupne točke. Riječ je o stvaranju pristupne točke u blizini ciljane WLAN mreže koja je upravljanja od strane napadača. Ta pristupna točka će se predstavljati istim SSID-em kao i pravi ovlašteni uređaj. Ovakav oblik napada provodi se u blizini ciljane mreže kako bi se korisnici zabunom spojili na zlonamjernu točku smatrajući da je dio ovlaštene mreže. Za stvaranje dodatne zbunjenosti i uspjeha napada, zlonamjerna se pristupna točka postavi sa jednakom MAC adresom kao i prava. Kada se uspostavi komunikacija napadač može provoditi razne oblike napada, a istovremeno slati podatke dok osluškuje cijelu komunikaciju.

Prvi korak u stvaranju zlonamjerne pristupne točke je naredbom *airodump-ng* provjeriti BSSID i ESSID mreže koja je cilj napada.



Sl. 4.16. Sve uhvaćene mreže naredbom *airodump-ng*

Čeka se prijava korisnika pa je dobivene informacije moguće iskoristiti za stvaranje nove pristupne točke u terminalu Kali-a naredbom *airbase-ng* što će stvoriti pristupnu točku sa istim ESSID-em, ali drugom MAC adresom. Naredba je sljedeća: *airbase-ng --essid <neko_ime> -c 1 wlan0mon*. Ponovnim upisom *airodump-ng* naredbe na popisu će biti i nova zlonamjerna pristupna točka.

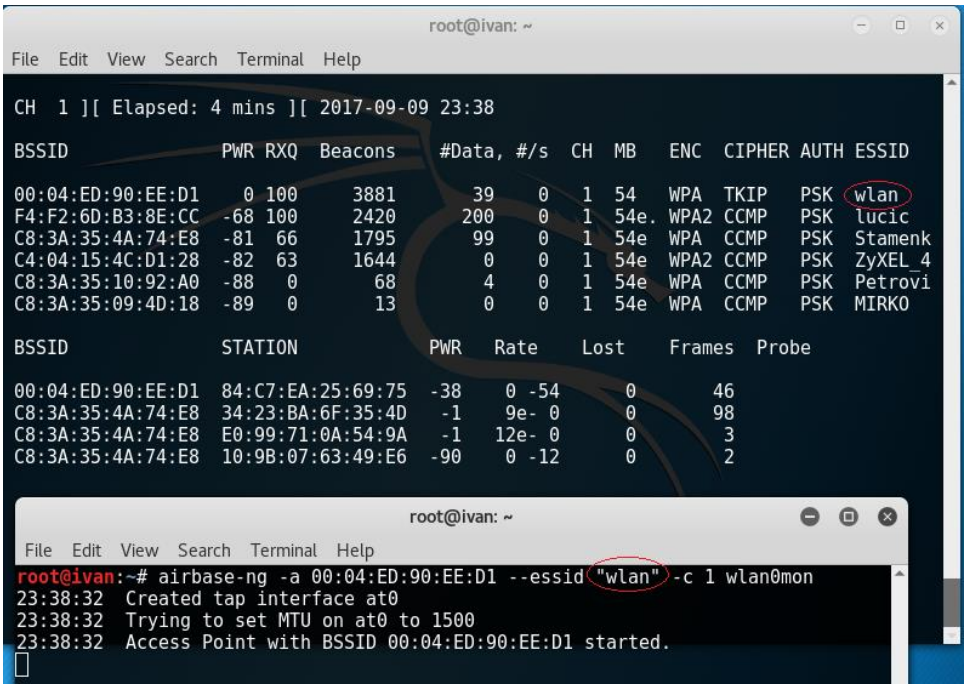


Sl. 4.17. Prikaz kreirane lažne pristupne točke

Idući korak je prisiliti korisnika na odjavu. Ubrzo će krenuti ponovna prijava korisnika, međutim zlonamjerna pristupna točka ima jači signal pa će se izvršit prijava na nju. Kako bi postavili jednak SSID i jednaku MAC adresu na zlonamjernu pristupnu točku, potrebno je u izrazu naredbe dodati određene parametre:

Airbase-ng -a <MAC_usmjerivača> --essid „<SSID_mreže>“ -c 1 wlan0mon.

Sada ni *airodump-ng* ne može razlikovati da se radi o dvije različite fizičke pristupne točke što je najjači oblik ovakvog napada.

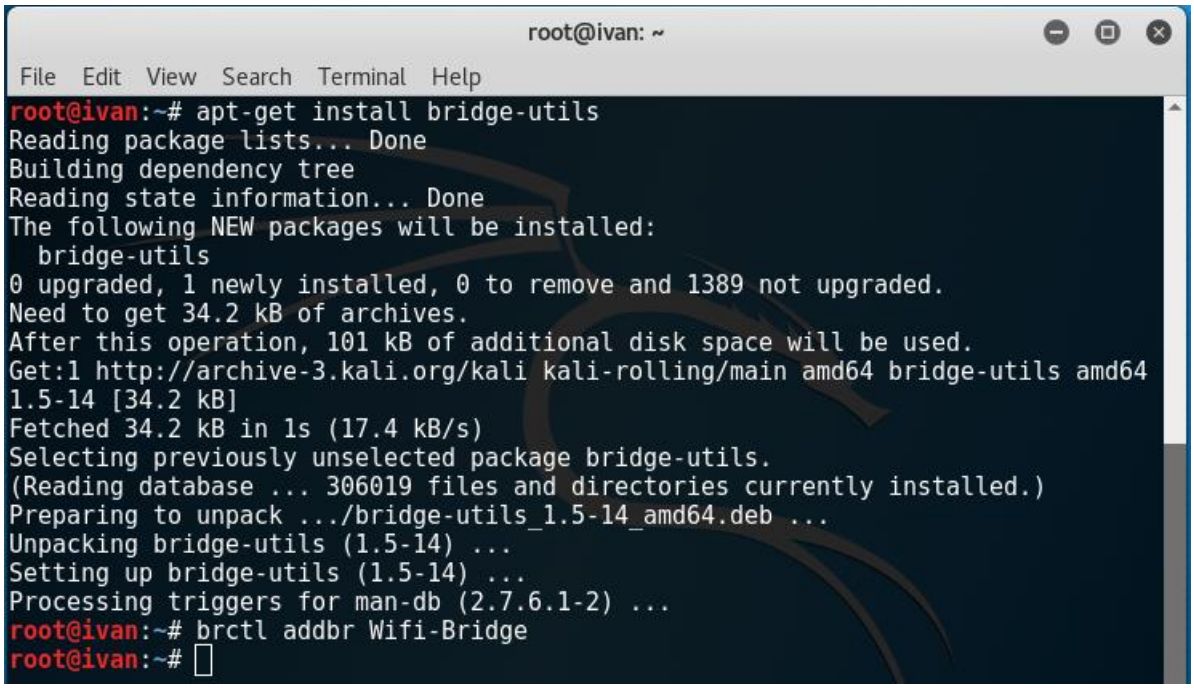


Sl. 4.18. Lažna pristupna točka sa istom MAC adresom

Još jedan oblik napada predstavlja stvaranje neovlaštene pristupne točke koja je spojena na ovlaštenu mrežu. Obično se koristi kako bi napadači imali ponovan ulaz u ugroženi sustav zaobilazeći sve sigurnosne kontrole. Postavlja se na način rada bez zaštite i enkripcije, a prema [4] se takva vrsta pristupne točke može stvoriti na jedan od sljedećih načina:

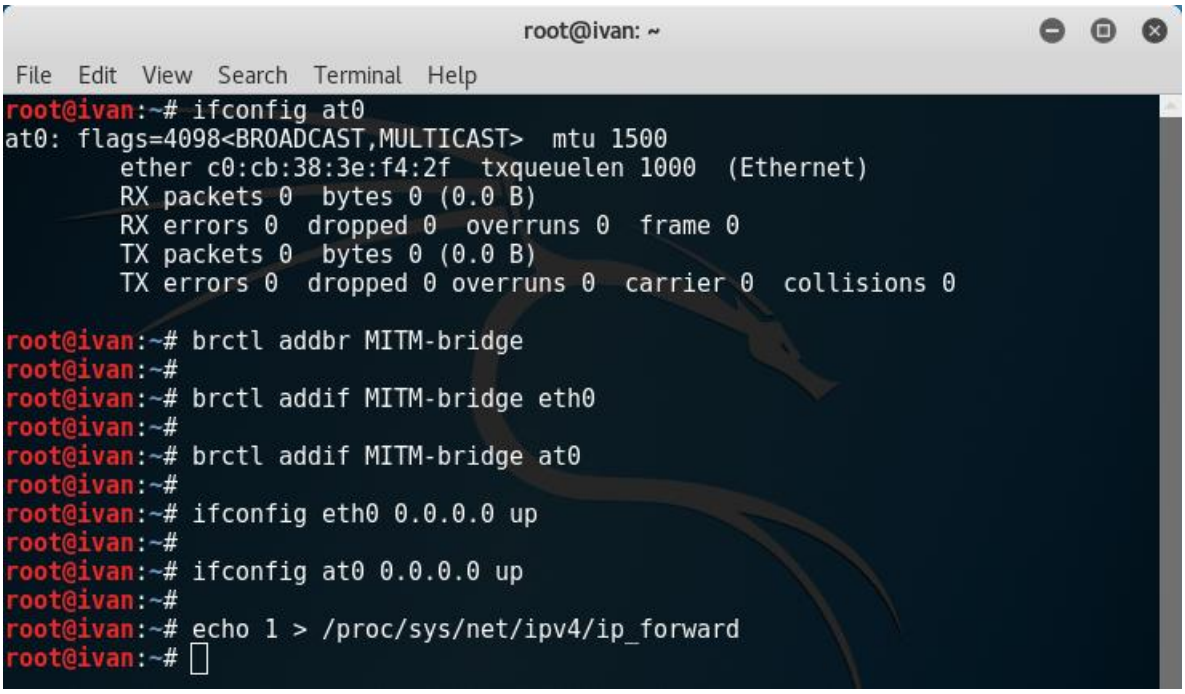
- Instaliranjem stvarnog fizičkog uređaja na ovlaštenu mrežu kao zla pristupna točka
- Stvaranje zle pristupne točke u softveru i premošćivanje sa ovlaštenom Ethernet mrežom, što zapravo dozvoljava svakom računalu, koje je spojeno na ovlaštenu mrežu, mogućnost rada kao zla pristupna točka.

Stvaranje zle pristupne točke započinje stvaranjem pristupne točke sa nekim imenom naredbom *airebase-ng --essid <neko_ime> -c 1 wlan0mon*. Nakon toga potrebno je postaviti most Ethernet sučelja prema ovlaštenoj mreži. Za to je potrebno instalirati *bridge-utils* datoteke i nazvati sučelje nekim imenom. Naredbe su: *apt-get install bridge-utills* i *brctl addbr <neko_ime>*.

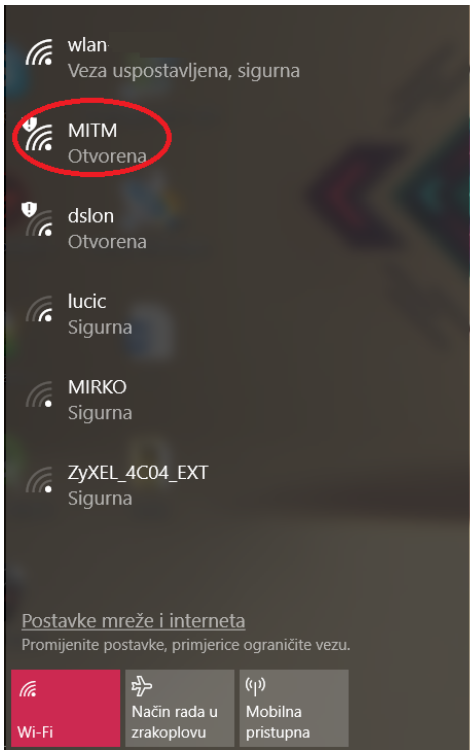


SL. 4.19. Prikaz instalacije *bridge-utils* sučelja

Idući korak je postavka sučelja *brctl addif <neko_ime> eth0* i *brctl addif <neko_ime> at0,* te podizanje istih *ifconfig eth0 0.0.0.0 up* i *ifconfig at0 0.0.0.0 up*. Na kraju je još potrebno osigurati prosljeđivanje IP paketa: *echo 1 > /proc/sys/net/ipv4/ip_forward*. Nakon toga kreirana je zla pristupna točka sa koje će svaki spojeni korisnik imati potpuni pristup ovlaštenoj mreži zahvaljujući kreiranom mostu što se koristi za provođenje jednih od naprednih napada odnosno, napad čovjek u sredini (engl. *Man in the Middle Attack*).



Sl. 4.20. Stvaranje i podešavanje mosta za upravljanje zlom pristupnom točkom



Sl. 4.21. Prikaz pronađene zle pristupne točke

4.5. Napadanje klijenta

Kao što postoje napadi na infrastrukturu WLAN mreže, tako postoje i napadi na samog klijenta. Zbog teškog prijevoda na hrvatski jezik korišteni su engleski izrazi za ove napade, a napadi na klijenta slični su do sada opisanim napadima. Jedan od napada na klijenta zove se *Honeypot and Mis-Association* napad, odnosno napad prilikom kojeg se vrši slučajno spajanje na pristupnu točku koju je stvorio napadač. Temelji se na činjenici da uređaji prilikom uključivanja traže prisutnost mreža na koje su do sada bili spojeni. Napadač ima nekoliko opcija kako pristupiti napadu:

- Može osluškivati uređaje i stvoriti lažnu pristupnu točku sa istim imenom koju klijent traži, što će uzrokovati njegovo spajanje na napadačev uređaj umjesto na ovlaštenu mrežu
- Može stvoriti pristupnu točku sa istim imenom kao susjedne mreže kako bi uvjerio korisnika u spajanje na njegov uređaj. Takvi se napadi lako provode na javnim mjestima gdje se klijenti pokušavaju spojiti na bilo kakvu bežičnu mrežu
- Može koristiti informacije kako bi naučio ponašanje i kretanje mete.

Postupak provođenja *Honeypot* napada zapravo se temelji na stvaranju zlonamjerne pristupne točke. Osluškivanjem se dobiju potrebne informacije za napad, stvori se istoimena pristupna točka kako bi trag bio teže uočljiv, vrši se prisilna odjava korisnika sa mreže te pri ponovnoj uspostavi konekcije korisnik se spaja na zlonamjernu pristupnu točku.

Još jedan napad na klijenta je *Caffe Latte* napad koji vrši probijanje WEP ključa. *Honeypot* napad kod WEP ključa neće uspjeti iz razloga što operacijski sustav Windows spremi WEP ključ kada se korisnik spoji na mrežu. Idući puta kada se korisnik spaja na istu mrežu, Windows-ov upravitelj bežičnih postavki automatski iskorištava spremljeni ključ. Prema tome *Caffe Latte* napad omogućava napadaču spoznaju WEP ključa ovjerene mreže korištenjem samo klijenta. Napad ne zahtijeva spojenost klijenta na mrežu, probiti će WEP uspješno i sa izoliranim klijentom. Postupak započinje ponovno osluškivanjem prometa, zatim se stvara pristupna točke sa istim imenom kao što ima ovjerena mreža. Nakon toga je postupak jednak kao pri probijanju WEP ključa. Može se zaključiti kako WEP pristupna točka ne mora dokazati klijentu poznavanje WEP ključa kako bi dobila šifrirane podatke. Prva informacija prilikom komunikacije uvijek će biti ARP zahtjev koji traži IP adresu uređaja. Napad je uspješan zbog ponavljanja paketa ARP zahtjeva koje šalje pristupna točka stvorena od strane napadača. ARP zahtjevi uvjetovat će ARP odgovore od strane klijenta što znači da se stvaraju velike količine podataka koje su potrebne za dešifriranje WEP ključa. Svi su paketi šifrirani WEP ključem koji dolazi za klijenta što je razlog zašto je ovakav napad uspješan.

Napad deautentikacije korisnika jednak je kao i do sada objašnjeni, razlika je u tome što se može definiranjem MAC adrese uređaja izvršiti prisilna odjava samo jednog korisnika. Izraz za to je sljedeći: *aireplay-ng --deauth 0 -a <MAC_klijenta> --ignore-negative-one wlan0mon.*

AP-less WPA-Personal napad predstavlja probijanje WPA šifre bez prisutnosti pristupne točke. Temelji se na hvatanju rukovanja klijenta i lažne kreirane pristupne točke od strane napadača. Dobivene informacije su dovoljne kako bi se mogao provesti pokušaj probijanja uz pomoć popisa čestih lozinki.

Spomenuti *Man-in-the-Middle* napad predstavlja jedan od najuspješnijih napada na bežičnu mrežu. Postoje različiti načini kako provesti ovakvu vrstu napada, a najčešći je kada je napadač povezan žičano na pristupnu točku te podešava svoje računalo kao zlonamjernu pristupnu točku i premošćuje promet. Tako se sva komunikacija između pristupne točke i korisnika odvija preko napadačevog računala, a on ima pristup svim podacima.

4.6. Kako se zaštititi?

Nakon spoznaje raznih oblika napada na bežičnu mrežu postavlja se pitanje kako se zapravo zaštitit. Kao što to rade penetracijski testeri, treba iskoristiti znanje o mogućim napadima kako bi se iste moglo spriječiti. Prvi korak je uvijek postojanje nekakvog oblika zaštitnog mehanizma, odnosno enkripcije. U slučaju postavke pristupne točke kao otvorene razina zaštite jednaka je nuli. Podaci i sav promet čitljivi su iz bilo kojeg softvera koji osluškuje i prati komunikacije iz zraka te ih napadač može iskoristiti za svoje potrebe. Mnogi proizvođači usmjerivača su u početku smatrali kako su skriveni SSID i filteri MAC adresa siguran način zaštite od napada. Međutim dokazano je suprotno uz pomoć *Wireshark*-a i terminala Kali-a gdje se ti podaci mogu dobiti vrlo jednostavno.

Zaštita dijeljenim ključem napredovala je kroz godine razvitkom složenijih algoritama za kodiranje podataka. Prvi oblik ključa, WEP, se u današnjici rijetko koristi ali ipak pronalazi svoju primjenu. Međutim, primjenom određenih naredbi uspjeh njegovog probijanja je sigurna što ukazuje na nesigurnost takvog ključa. Za razliku od WEP-a, WPA i WPA2 su složeni i smatraju se kriptografski neprobojnima. Provode se pokušaji probijanja uz pomoć velikih popisa često korištenih lozinki, a postotak uspješnosti ovisi o složenosti korištene lozinke. Preporuka je lozinku učiniti što više jedinstvenom, dakle, koristiti što dužu riječ koja po mogućnosti nema nikakvog smisla uz dodavanje brojeva i posebnih znakova.

Osim pokušaja dešifriranja ključeva za zaštitu, postoje razni napadi na infrastrukturu bežične mreže. Napadači stvaraju lažne pristupne točke i prisilnom odjavom korisnika sa ovlaštene mreže

uspiju ga prevariti u spajanju na pogrešnu mrežu. To mogu iskoristiti kako bi zadobili pristup određenim podacima i izvedbu raznih napada kao što je i *Man in the Middle* napad. Preporuka zaštite od ovakve vrste napada temelji se na oprezu i znanju samog korisnika. Nikada ne koristiti otvorene javne mreže jer se nikad ne zna tko upravlja njom sa druge strane. Ako se pak mora koristiti, izbjegavati upisivanje važnih vjerodajnica kao što su korisničko ime i lozinka. Uvijek provjeriti radi li se o sigurnoj web stranici tražeći https oznaku. Napadači mogu kopirati web stranice što može prevariti korisnika. Smatrajući da se radi o sigurnoj stranici neće primijetiti razliku pa moguće unijeti važne informacije prijavom na, primjerice, bankovni račun. U vlastitom domu obavezno koristiti WPA zaštitu uz jak ključ te ne dozvoliti povezivanje nepovjerljivim osobama u mrežu.

Jedan oblik zaštite je i korištenje virtualne privatne mreže. Ona pruža sigurnost čak i od osluškivanja prometa iako se radi o zračnoj komunikaciji jer šifrira podatke. Čak i da dođe do osluškivanja podataka oni napadaču neće puno pomoći.

Općenite preporuke koje mogu pridonijeti sigurnosti sustava i računalne mreže su: nikada ne kliknuti na sumnjive linkove, koristiti i redovno osvježavati antivirusne softvere i koristiti jako dobar vatrozid, Također osvježavati sustav i aplikacije jer često starije verzije su sklone pronalasku ranjivosti. Koristiti dvostruki faktor autentikacije, tj. pored korisničkog imena i lozinke, uređaj dodatno zaštititi nekim oblikom biometrije, kao što je otisak prsta primjerice na pametnim telefonima i sl.

5. ZAKLJUČAK

Cilj ovog diplomskog rada bio je analizirati sigurnost bežičnih mreža primjenom Kali Linux distribucije te je primijeniti na različitim primjerima u okruženju bežičnih mreža, a prikupljene rezultate iskoristiti kako bi se istaknule preporuke i smjernice za povećanje razine sigurnosti.

Definirano je što je i kako izgleda Kali, opisana njegova uloga i način kako se ažurira i održava. Zatim je navedena teorijska podloga u postupku provođenja napada ili penetracijskog testiranja s radnjama i razmišljanjima napadača ili penetracijski testera.

Vršeni su testovi penetracije nad različitim parametrima WLAN mreže. Osnovna metoda svakog napada je osluškivanje budući da se komunikacija i prijenos podataka odvija zrakom. Dokazano je kako skrivanje SSID-a i filtriranje MAC adresa nije siguran način zaštite od napada jer se uporabom programa za osluškivanje prometa i unosom par naredbi u Kali terminalu lako dolazi do traženih informacija. Testirana je uspješnost probijanja ključeva za prijavu na WLAN mrežu kao što su WEP, WPA i WPA2. WEP se temelji na algoritmu koji koristi inicijalizacijske vektore. Inicijalizacijski vektori se ponavljaju nakon određenog broja okvira pa se probijanje vrši prikupljanjem velikog broja paketa i usporedbom šifriranih tekstova. Na taj način će se WEP ključ probiti uvijek uz dovoljan broj paketa što je znak kako WEP zaštita nije sigurna. WPA i WPA2 zaštita se trenutno smatra kriptografski neprobojnom uz prisustvo dovoljno jakog ključa. Uz uvjet slabog ključa, probijanje je moguće na sličan način kao i WEP, ali je potreban rječnik, odnosno ogroman popis često korištenih lozinki. Ako se lozinka nalazi na popisu probijanje WPA ili WPA2 ključa će uspjeti pa je preporuka koristiti što dužu jedinstvenu lozinku uporabom brojeva i posebnih znakova.

Opasni su još i napadi na infrastrukturu WLAN mreže koji se temelj na stvaranju lažne pristupne točke i prisiljavanje korisnika na njihovo spajanje. Od njih se može zaštititi opreznim rukovanjem i pristupanju samo sigurnih internet stranica sa oznakom https. Kako se komunikacija odvija zrakom osluškivanje je neizbježno, ali se od njega može zaštitit korištenjem virtualne privatne mreže koja šifrira sav promet između korisnika i usmjerivača. Preporuka je dakako i obvezna korištenja antivirusnih softvera i dobrog vatrozida, kao i izbjegavanje korištenja važnih vjerodajnica ako je korisnik spojen na javnim mrežama.

LITERATURA

[1] R. W. Beggs, Mastering Kali Linux for Advanced Penetration Testing, Packt Publishing, Birmingam – Mumbai, 2014.

[2] D. W. Dieterle, Basic Security Testing With Kali Linux 2, D. W. Dieterle, 2016

[3] J. Broad, A. Bindner, Hacking with Kali, Elsevier Inc., Amsterdam, 2014.

[4] V. Ramachandran, C. Buchanan, Kali Linux Wireless Penetration Testing: Beginner's Guide, Packt Publishing, Birmingham – Mumbai, 2015.

[5] Offensive Security, Penetration Testing with Kali Linux, Offensive Security Ltd., 2014

SAŽETAK

Kali Linux okruženje je temeljeno na Debian Linux distribuciji usmjereno na napredno testiranje penetracije računalnih sustava. Koristi se za spoznaju slabosti i nedostataka računalnih sustava prije nego to učine hakeri i iskoriste pristup podacima u svoje svrhe. Svaki napad prati određena pravila i postupke. Drugim riječima, prikupljaju se informacije i vrši njihovo iskorištavanje kako bi se djelovalo na cilj ili omogućilo dodatne napade. WLAN predstavlja bežičnu računalnu mrežu koja povezuje dva ili više uređaja bežičnom komunikacijom. Upravo iz tog razloga postoje razne sigurnosne slabosti takvih mreža. Kako bi se povećala razina sigurnosti provedeni su testovi s Kali Linux-om nad raznim parametrima bežične mreže. Kada klijent zna područje djelovanja napada može se primjereno prilagoditi i postupati kako bi napad spriječio. Korištenjem terminala Kali-a i *Wireshark*-a dokazani su nedostaci skrivanja SSID-a, MAC filtriranja, te WEP/WPA/WPA2 enkripcije. WEP se može probiti uvijek pa se smatra ne sigurnim, a WPA/WPA2 se trenutno smatraju kriptografski neprobojnim uz postojanje jakog jedinstvenog ključa. Općenito treba pažljivo rukovati mrežom, osobito ako se koriste javne mreže, a isto tako preporučljivo je koristiti antivirusne sustave i vatrozide.

Ključne riječi: Kali Linux, napadači, penetracijski testeri, izviđanje, iskorištavanje, bežična mreža, sigurnost, ovjera, šifriranje, vjerodajnice, pristupna točka, klijent, zaštita.

The Application of Kali Linux for Security Analysis of Wireless Networks

The Kali Linux environment is based on the Debian Linux distribution focused on advanced computer network penetration testing. It is used to detect weaknesses and disadvantages of computer systems before hackers do it and exploit the access to data for their purposes. Each attack follows certain rules and procedures. With other words, information is collected and exploited to influence the target or to allow additional attacks. WLAN represents a wireless computer network that connects two or more devices with wireless communication. That is why there are various security weaknesses of such networks. To increase the security level, tests with Kali Linux have been carried out over various wireless network parameters. When a client knows the scope of the attack, he can adapt and act appropriately to prevent it. Using the Kali terminal and Wireshark has shown the lack of a hidden SSID, MAC filtering and WEP/WPA/WPA2 encryption. WEP can always be cracked, so it is considered unsafe, and WPA/WPA2 are currently considered cryptographically impenetrable with the existence of a strong unique key. In general, care should be taken when handling in a network, especially if public networks are used, and it is also advisable to use antivirus systems and firewalls.

Key words: Kali Linux, hackers, penetration testers, scanning/reconnaissance, exploitation, wireless network, security, authentication, encryption, credentials, access point, client, protection.

ŽIVOTOPIS

Ivan Petrović rođen je 12. siječnja 1994. godine u gradu Frankfurt am Main, Njemačka, kao drugo dijete u obitelji. Tu je proveo šest godina života nakon kojih zajedno sa obitelji seli u selo Domaljevac (BiH) gdje potom živi do odlaska na fakultet. Godine 2000. upisao je osnovnu školu u Osnovnoj školi Braće Radić u Domaljevcu te završava osam godina školovanja sa odličnim uspjehom. Za vrijeme osnovnog školovanja sudjelovao je tri godine za redom na državnom ekološkom kvizu „Lijepa naša“ u Hrvatskoj (2006., 2007., 2008.). Također je na kraju školovanja proglašen učenikom generacije. 2008. godine upisao je opću gimnaziju u Srednjoj školi fra. Martina Nedića u Orašju (BiH), koju također završava odličnim uspjehom. U tom razdoblju sudjelovao je na internacionalnoj olimpijadi njemačkog jezika u Sarajevu te dobio certifikat za odlično poznavanje jezika na C1 razini Goethe instituta.

Akademske godine 2012/2013 upisao se na sveučilišni preddiplomski studij elektrotehnike na Elektrotehničkom fakultetu u Osijeku kao redoviti student. Pri upisu u drugu godinu opredjeljuje se za smjer komunikacije i informatika. 10. rujna 2015. godine završio je preddiplomski studij i stekao zvanje: sveučilišni prvostupnik (baccalaureus), inženjer elektrotehnike. Iste godine upisao se na sveučilišni diplomski studij elektrotehnike, smjer komunikacije i informatika, modul mrežne tehnologije.

Potpis: _____