UDC: 004.056:004.087.5 INFO M: str. 46-50

NAPADI NA BEZBEDNOST BEŽIČNIH LOKALNIH MREŽA
ATTACKS ON SECURITY OF WIRELESS LOCAL AREA NETWORKS (WLAN)

Darko Dimitrijević, Snežana Vulović, Slobodan Jovanović
Fakultet informacionih tehnologija, Metropolitan Univerzitet, Beograd, www.metropolitan.edu.rs

REZIME: Razvojem bežične tehnologije i porastom njenog korišćenja raste i potreba da se bezbednost mreže dovede na što viši nivo. Samom komunikacijom u bežičnoj mreži stvara se rizik da se ta komunikacija presretne. Najbolja metoda prisluškivanja i analize paketa kao i ekstrakcije SSID (*Service set ID*) u WLAN mrežama je pomoću Network Sniffer-a. Mrežni prisluškivači (*Network sniffers*) su aplikacije koje mogu da prate protok paketa kroz mrežu i pomoću njih je moguće saznati razne informacije koje zanimaju korisnika, kao što je SSID, šta dati paket sadrži i sl. U ovom radu biće detaljno prikazan konkretan napad na jednu WLAN mrežu, pomoću softvera Aircrack-ng. Takodje, u radu se analizira šta je WEP, metode prisluškivanja, tehnike probijanja lozinke, koji se softveri koriste za napad na bežičnu mrežu, i kako se što bolje zaštititi od takvih napada.
KLJUČNE REČI: Prisluškivanje, Šifriranje, WLAN, WEP
ABSTRACT: Development of wireless technology and its increased use require the network security to be increased to the top level. Any communication in the wireless network represents a risk for it to be intercepted. The best interception and analysis method and SSID (*Service set ID*) extraction in WLAN networks is to use a Network Sniffer. Network sniffers are software applications which are able to follow data flow in the network, and these applications enable extraction of various information, eg. SSID, etc. This paper describes in details a concrete attack on a WLAN network, by using Aircrack-ng software. Also, this paper discusses what is WEP, sniffing methods, attacks on passwords, and software for attacks on WLAN networks, and how WLAN networks can be protected against attacks.
KEY WORDS: Sniffing, Encryption, WLAN, WEP

1. UVOD

Razvojem bežične tehnologije i porastom njenog korišćenja raste i potreba da se bezbednost mreže dovede na što viši nivo. Samom komunikacijom u bežičnoj mreži stvara se rizik da se ta komunikacija presretne. Najbolja metoda prisluškivanja i analize paketa kao i ekstrakcije SSID (Service set ID) u WLAN mrežama je pomoću *Network Sniffer*-a (Slika 1) [1,2]. Mrežni prisluškivači (*Network sniffers*) su aplikacije koje mogu da prate protok paketa kroz mrežu i pomoću njih je moguće saznati razne informacije koje zanimaju korisnika, kao što je SSID.

Paketi u mrežnoj komunikaciji stvoreni su da bi se brzina mreža održala na visokom nivou, jer da se informacije između računara šalju kao jedan tok podataka to bi u bilo kojoj malo većoj mreži stvorilo veliki komunikacijski kolaps. Zato postoje paketi koji celu informaciju koja se šalje podele na manje delove i šalju ih preko mreže do drugog računara. Kada svi ti paketi stignu na drugi računar oni se spoje u jednu celinu. Korisnik vidi kompletnu informaciju kao što je npr. e-mail ili neka internet strana i nema predstavu o tome koliko je paketa poslato i šta su sadržali. Da bi neko mogao da vidi te pakete on mora da ima *network sniffer*. Taj program ili uređaj, može se nazvati i nekom vrstom prisluškivača koji ima mogućnost čitanja i analiziranja paketa koji se kreću kroz računarsku mrežu u kojoj je on prisutan. Oni se mogu koristiti kako za dobre tako i za loše stvari [3-5].

Pozitivan način korišćenja *network sniffer*-a je i ujedno njegov primaran način korišćenja, a koji je održavanje mreža i normalan rad sistema i to su [6,7]:

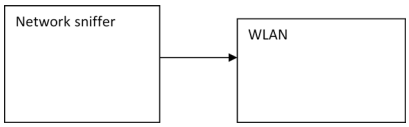
- Hvatanje paketa
- Snimanje i analiziranje saobraćaja
- Dešifrovanje paketa i prikazivanje čistog teksta
- Konvertovanje podataka u čitljiv format
- Pronalazak mogućeg upadača
- Prikazivanje relevantnih informacija kao što je IP, protokol, ime hosta ili servera.

Negativne osobine su:

- Hvatanje lozinke, koji je najčešći razlog za korišćenje *sniffing* alata
- Hvatanje specijalne i privatne informacije ili transakcije, kao što je korisničko ime, ID kreditne kartice, računa i lozinki
- Snimanje email-a ili poruka u chat-u
- Neki sniffer-i imaju mogućnost i modifikacije informacija o ciljnom kompjuteru
- Da bi se dobio neki viši nivo pristupa sistemu.

Da bi *sniffer* mogao da radi kako treba, on mora biti u istoj mreži gde putuju podaci. Nemaju svi *sniffing* programi iste funkcije. Neki *sniffer*-i mogu analizirati na stotine različitih protokola dok neki drugi mogu samo jedan ili dva. Najčešće analizirani protokoli od strane *sniffer*-a su TCP/IP, IPX, DEC-Net. Obično, *sniffer*-i se koriste kao asistenti za menadžment mreža. Njegove sposobnosti monitoring-a i analize nam mogu pomoći oko održavanja mreže, otkrivanja upada, kontrole saobraćaja ili nadgledanje mrežnog sadržaja. Ali te osobine se mogu koristiti i od strane hakera kao alat za upadanje u računar. Sa što većim korišćenjem *sniffer*-a, postaje ironično da on postaje najveća prepreka za sigurnost na mreži, iako je najbolji alat za povećanje sigurnosti na mreži.

U ovom radu biće prikazan konkretan napad na jednu WLAN mrežu, upotrebom programa Aircrack-ng. Ovde se daje detaljan uvid u to kako se ovakav napad može sprovesti u praksi, korak po korak, dok u relevantnoj literaturi se ne daje tako detaljan opis (u praksi je cela procedura napada komplikovanija nego što to izgleda u relevantnoj literaturi). Takodje, u radu se analizira šta je WEP, metode prisluškivanja i analize paketa, tehnike probijanja lozinke, koji se softveri koriste za napad na bežičnu mrežu, i kako se što bolje zaštititi od takvih napada.



Slika 1: *Network sniffer*

2. TEHNIKE PROBIJANJA LOZINKE WLAN MREŽAMA (PREVIOUS WORK)

Probijanje lozinki može biti kako nemoguće tako i veoma lako. Na to najveći uticaj imaju ljudi koji su napravilu tu lozinku (šifru). Što je lozinka komplikovanija to je teže da se probije ili možda čak i nemoguće ako je dovoljno komplikovana. Mnogi obični korisnici prave grešku što stavljaju previše jednostavne šifre kao što su na primer reči koji su napisani samo malim slovima ili prave takođe i proste kombinacije kao što na primer dodaju na kraju reči jedan broj. Statistika pokazuje da izuzetno veliki broj ljudi imaju šifre koje svaki najobičniji napad na njih može da otkrije. Iz tog razloga je pametno da se možda napravi jedna šifra za sve naloge koje korisnik poseduje ali dovoljno komplikovana da bude siguran da je niko ne može probiti.

Postoje razne tehnike probijanja lozinke na bežičnim lokalnim mrežama, a u ovom radu izabrano je pet vrsta tehnika koje se najčešće primenjuju, a to su:

- Dictionary Attack
- Brute Force
- FMS/Korek
- ChopChop
- PTW Attack

Dictionary Attack, ili na srpskom napad rečnikom se smatra jednim od najjednostavnijih napada koji postoje. On se, kao što i sam naziv kaže, bazira na rečniku koji se koristi za napad na lozinku. To funkcioniše tako što se u odgovarajući program ubaci rečnik koji sadrži moguće lozinke i program ide redom kroz taj rečnik sve dok ne nadje pravu lozinku. Naravno, moguće je da rečnik ne sadrži traženu lozinku ali uzimajuću u obzir da većina ljudi pravi jednostavne lozinke to je malo verovatno.

Brute force napad je strategija koja u teoriji može da se primeni na bilo koje kriptovane podatke. Ovakva vrsta napada se obično primenjuje kada nije moguće iskoristiti druge slabosti enkripcionog sistema da bi se olakšao posao. Ovaj napad podrazumeva da se isprobaju svi mogući ključevi, odnosno sve moguće kombinacije slova, broja i znakova sve dok se ne dobije traženi ključ.

FMS Attack [1]: Ovaj napad se zasniva na napadu RC4 algoritma koji se koristi kod WEP-a. Ova vrsta napada je otkrivena 2001. godine od strane Fluhrer-a, tako što su pronađeni *slabi ključevi*, koji se mogu koristiti za određivanje mnogih stanja i izlaznih bitova sa velikom verovatnoćom. FMS napad funkcioniše tako što se obraća pažnja samo na prvi bajt u RC4 nizu ključeva.

KoreK napad opisuje sedamnaest različitih napada na WEP koji mogu da se kategorizuju na sledeći način:

- Otkrivanje ključa zasnovano na prvom bajtu u nizu ključa od PRNG (slično FMS napadu).
- Otkrivanje ključa zasnovano na prvom i drugom bajtu u nizu ključa od PRNG.
- Obrnuti napad - obrnuti metodi zbog smanjivanja prostora traženja.

Chopchop Attack: Umesto da iskoristi ranjivost u RC4 algoritmu, chopchop napada sam WEP protokol i dva njegova propusta u dizajnu, naime njegov nedostatak zaštite od ponavljanja i slabost ICV-a (Integrity Check Value). Iako nije mnogo efikasan, on ima praktičnu primenu sa paketima koji sadrže veliki broj poznatih podataka, kao što su ARP paketi.

PTW Attack: U njihovom izdanju sa naslovom *Razbiti 104-bitni WEP za manje od 60 sekundi,* oni pretstavljaju napad za potpuno otkrivanje ključa koji će uspešno otkriti ključ sa 50% verovatnoće sa manje od 40000 frame-ova.

Pošto je RC4 kriptografski algoritam za simetričnu enkripciju, to znači da ne može da se koristi dva puta isti ključ za prenos podataka [1]. Svrha inicijalizacionog vektora (IV), koji se šalje kao čist tekst, je da spreči bilo kakvo ponavljanje, ali 24-bitni IV nije dovoljno dugačak da bi obezbedio to u opterećenoj mreži. Način na koji je korišćen IV je takođe otvorio WEP za napad srodnih ključeva.

WEP je sigurnosni protokol za IEEE 802.11 bežične mreže, uveden kao deo originalnog 802.11 standarda ratifikovanog 1999, sa namerom da obezbedi poverljivost podataka komparabilnu sa onom kod tradicionalnih žičnih mreža. WEP je bio sigurnosni standard implementiran u prve 802.11 bežične LAN mreže 1999. godine. WEP koristi RC4 algoritam za poverljivost, i CRC-32 za integritet.

2003. godine je dokazano kroz razne eksperimente da je, sa odgovarajućom opremom moguće bez ikakvih problema prisluškivati WEP zaštićene bežične mreže [1]. Pored toga su dokazana dva opšta propusta:

- Korišćenje WEP-a je opcionalno, tako da se kod mnogih instalacija nikad nije koristio;
- WEP nije sadržao protokol za upravljanje ključevima, umesto toga on se oslanjao na jedan deljeni ključ među korisnicima.

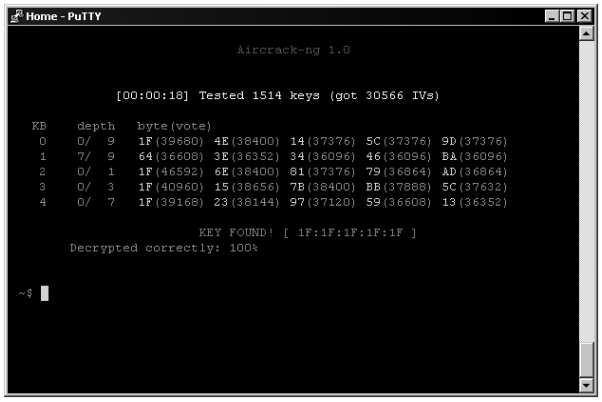
Postoji niz softverskih paketa za napad: Kismet, NetStumbler, Wireshark, Aircracking, itd.. Npr. *Kismet [*2] je detektor mreže, paket sniffer, i sistem za prepoznavanje upada za 802.11 bežične mreže. On je različit od većine drugih detektora mreže zato što radi pasivno. To znači da bez potrebe slanja bilo kakvih paketa kroz mrežu on može da pronađe sve Access Point-ove i klijente u mreži i da ih udruži jedne sa drugima. Kismet takođe sadrži i osnovne bežične IDS (Intrusion Detection System) osobine kao što je detektovanje aktivnog sniffing programa na bežičnoj mreži. *NetStumbler j*e alternativa Kismet-u za ljude koji više vole da koriste Windows operativni sistem pošto je ovaj softver pravljen da se koristi prevashodno na tom operativnom sistemu. Što se tiče samih funkcija NetStumbler-a, one su takoreći iste kao kod Kismet-a.

Wireshark [3] služi za analiziranje mrežnih paketa. On pokušava da uhvati mrežne pakete i da ih prikaže korisniku što je detaljnije moguće. Wireshark ima sledeće mogućnosti:

- Dozvoljava uživo praćenje i analiziranje paketa
- Ima mogućnost analiziranja prethodno snimljenih paketa

- Može da vrši analizu paketa koje je uhvatio neki drugi softver pod uslovom da taj drugi softver ima mogućnost čuvanja tih podataka u formatu koji odgovara wiresharku
- Podržava nekoliko tipova mreža, neke od njih su Ethernet, IEEE 802.11, PPP...
- Uhvaćeni mrežni podaci se mogu pregledati kroz GUI
- Ima mogućnost korišćenja filtera i sortiranja radi lakšeg snalaženja

Aircrack-ng [4] je skup alata za prisluškivanje bežičnih računarskih mreža. Neki od njegovih glavnih alata su airodump-ng, aireplay-ng, aircrack-ng. Svaki od ovih alata ima svoju specifičnu namenu pri prisluškivanju računarskih mreža. *Airodump-ng* je program koji se koristi za prisluškivanje lokalnih bežičnih mreža i sakupljanje paketa iz njih. *Aireplay-ng* služi da bi se lažno predstavili AP-u i za ubacivanje paketa kojima možemo da izazovemo odgovor AP-a tako da time dobijamo još više paketa pomoću kojih posle možemo da otkrijemo šifru. *Aircrack-ng* je program po kome je i paket dobio naziv zato što on predstavlja glavni deo celog paketa. Ovaj program se koristi da bi se saznala šifra i on to radi na dva moguća načina. Prvi je koristeći FMS/Korek napad, a drugi je noviji PTW napad, koji je mnogo brži u odnosu na sve druge napade na WEP.



Slika 2: Prikaz *Aircrack-ing* prozora

Skoro je nemoguće da se primeti da li postoji neki *network sniffer* u mreži. To je pasivna radnja, pošto se pristupa paketima ali se ne menjaju. Postoje neki metodi kako može da se primeti da li postoji neki network sniffer ali oni nisu 100% tačni. Jedan od načina da se vidi da li postoji sniffer je to da se dešavaju dosta DNS pregleda (sniffer pokušava da pretvori IP adrese u *host* imena), međutim to može biti samo neka indikacija pošto se ta situacija može javiti i iz drugih razloga. Drugi, bolji metod da se proveri da li postoji sniffer u mreži je da se pošalje ARP zahtev prema tom uređaju na koji se sumnja da bi se videlo da li je u otvorenom modu. Paket koji nije namenjen vašem računara biće zaustavljen na hardverskom nivou ako otvoreni mod nije uključen. Uređaj koji najčešće pokreće *sniffer* je mrežna kartica.

Kako se zaštititi od napada sniffer-a na vaš sistem? Za sada ne postoji potpuno efikasno sredstvo koje bi sprečilo instaliranje i odbranu od *sniffer-a* na vaš sistem. Mrežni administratori treba dosta da se trude da bi uspeli da smanje štetu koju neki sniffer program može da napravi. Neke od mogućnosti su korišćenje sledećih tehnologija:

- Switch, za razliku od hub-a zna koji su računari povezani preko njega i gde se nalaze.
- Enkripcija vaših podataka može dosta poboljšati bezbednost protiv napada sniffer-ima na vašu mrežu jer iako sniffer može sve pakete u mreži da uhvati on ne može da ih dekodira i pročita.
- WPA2 (WiFi Protected Access 2) koristi za šifrovanje sigurni AES (Advanced Encryption Standard). Pored TKIP protokola je dodat i CCMP (Counter Mode / CBC - MAC Protocol), koji se takođe zasniva na AES. Ovako osiguran WLAN se za sada ne može probiti.

3. PRIMER NAPADA NA MREŽU

Mrežu koju smo napali je AP (*Access point*) u stambenoj zgradi koji se koristi od strane nekoliko komšija. Za napad na bežičnu računarsku mrežu bilo nam je potrebno sledeće:

- Linux distribucija (Koristićemo Ubuntu)
- Bežična mrežna kartica i drajver za nju (mi smo koristili Intel PRO/Wireless 3945ABG sa ipwraw-ng-2.3.4 drajverom)
- *Aircrack-ng* 1.0
- Moramo biti dovoljno blizu *Access Point*-u da bi mogli da primamo i šaljemo pakete. To što možemo da vidimo AP ne znači da i on može nas da vidi zato što je obično signal Access Point-a jači u odnosu na signal koji šalje sama bežična mrežna kartica.
- Mora postojati bar jedan klijent koji je povezan na taj *Access Point.* To je zato što se ova tehnika zasniva na ARP paketima a ako nema nijednog aktivnog klijenta neće biti nijednog ARP paketa.

Da bi bili u mogućnosti da dobijemo WEP šifru i uopšte da krenemo sa radom na tome, treba izvršiti neke pripreme. Prva stvar koju treba uraditi je da se skine odgovarajući drajver za bežičnu mrežnu karticu zato što standardni drajveri koji dolaze uz bežičnu mrežnu karticu odgovarajućeg proizvođača ne podržavaju monitor mode i packet injection. Drajvere koji trebaju moraju da se potraže na internetu i isprobaju zato što postoje različite verzije drajvera za različite bežične mrežne kartice. Za izabranu mrežnu karticu odgovarajući drajver može se naći na Internetu, na sledećem linku: http://homepages.tu-darmstadt.de/~p_larbig/wlan/ [5].

Da bi instalirali drajver bilo je potrebno izvršiti sledeće linije koda:

```
sudo apt-get install build-essential
sudo apt-get install libssl-dev
wget http://dl.aircrack-ng.org/drivers/
ipwraw-ng-2.3.4-04022008.tar.bz2
tar -xjf ipwraw-ng*
cd ipwraw-ng
make
sudo make install
sudo make install_ucode
echo "blacklist ipwraw" | sudo tee /etc/
modprobe.d/ipwraw
sudo depmod -ae
sudo modprobe -r iwl3945
sudo modprobe ipwraw
sudo ifconfig wlan0 up
airmon-ng start wlan0
```

Nakon instaliranja drajvera i potrebnih podešavanja, bežična mrežna kartica se nalazi u Monitor modu. U slučaju da želi-

te da proverite da li se stvarno nalazi u monitor modu a ne kao što je standardno u Managed modu to možete učinite unosom komande *iwconfig (slika 3)*.

Slika 3: *iwconfig prikaz monitor mode-a*

Kada zaključite da je bežična mrežna kartica u monitor modu može se uraditi test ubacivanja paketa u mrežu da bi bili sigurni da naša kartica može da ubaci paket u mrežu. To se može uraditi tako što se izvrše sledeće komande u terminalu:

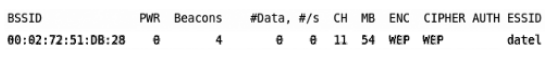
```
aireplay-ng -9 wifi0
aireplay-ng -9 127.0.0.1:666
```

One su dale potvrdnu poruku "Injection is working".

Pronalazak svih* Access Point-*ova pomoću airodump-ng:

Sledeći korak u napadu je pronalazak MAC adrese Access Point-a ili Wireless router-a. Tu informaciju nalazimo izvršavanjem sledeće komande u terminalu:

`sudo airodump-ng wifi0` Rezultat ove komande je sledeći:



Slika 4: *Prikaz airodump-ng rezultata pretrage*

Na Slici 4. možete videti detalje o Access Point-u koji je u našem okruženju i od kog možemo da uhvatimo signal. Sa leve strane se nalazi njegova MAC adresa, dok sa desne strane stoji ime tog AP-a. Ovde možemo i saznati na koji način je zaštićena mreža i koji kanal koristi. Sada kada smo saznali MAC adresu i ostale detalje o Access Point-u možemo nastaviti dalje ka dešifrovanju WEP-a.

Sakupljanje inicijalizacionih vektora:

Postoje dve mogućnosti sakupljanja inicijalizacionih vektora:

- Ubacivanjem paketa, pomoću kojih dobijemo brže odgovore od access point-a i time brže sakupimo potrebnu količinu IV-a
- Prisluškivanje mreže, koje se primenjuje ako nemamo mogućnost da ubacujemo pakete u mrežu

Objasnićemo i jednu i drugu varijantu rada, ali za naš primer koristili smo prisluškivanje mreže.

Pokretanje* airodump-ng *za prikupljanje inicijalizacionih vektora:

Sada kada ste sakupili sve bitne parametre koji su potrebni da bi pokrenuli napad na mrežu (MAC adresa, Kanal, ime...) i podesili bežičnu mrežnu karticu u monitor mode, vreme je da krenemo sa sakupljanjem inicijalizacionih vektora koji se nalaze u paketima koje šalje Access Point. Ovo smo učinili pokretanjem airodump-ng-a podešen na kanal AP-a sa BSSID filterom (MAC adresa AP-a).

Sledeću komandu treba izvršiti:

```
sudo airodump-ng -c 11 --bssid 00:02:72:51:DB:28
-w wepdump -i wifi0
```

Radi lakšeg razumevanja koda objasnićemo ga detaljnije:

- -c označava kanal koji se koristi
- --bssid je MAC adresa AP-a
- -w wepdump je naziv fajla u kome ćemo sačuvati naše inicijalizacione vektore
- -i znači da hoćemo da sačuvamo samo inicijalizacione vektore a ostali podaci da se odbace

Korišćenje *aireplay-ng*-a za lažnu autentifikaciju sa AP-om:

Zatim možemo se povezati na bežičnu mrežu. Da bi AP mogao da prihvati pakete koje šaljete vaša MAC adresa mora biti udružena sa AP-om. Ako to nije slučaj onda AP šalje "DeAuthentication" paket. U tom stanju svi paketi koji šaljete biće ignorisani od strane AP-a. Sada smo se samo povezali sa AP-om i time mu rekli da želimo da komuniciramo sa njim. To smo učinili tako što smo u terminalu ukucali sledeći kod:

```
sudo aireplay-ng -1 0 -e datel -a
00:02:72:51:DB:28 -h 00:13:CE:EC:45:20
wifi0
```

- -1 znači da je lažno prijavljivanje
- 0 pretstavlja vreme ponovnog udruživanja u sekundama
- -e datel je naziv mreže
- -a je MAC adresa AP-a
- -h je vaša MAC adresa, odnosno ona pomoću koje se pretstavljate AP-u

Pokretanje *aireplay-ng*-a u ARP request replay modu za ubacivanje paketa:

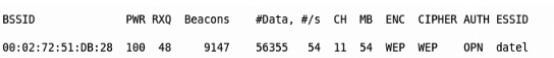
Da bi smo uspeli sa našim napadom na WEP potrebno je da sakupimo dovoljno inicijalizacionih vektora, idealno bi bilo oko 150000. Obično, mrežni protok ne stvara toliku količinu IV-a veoma brzo, zbog čega smo primenili tehniku ubacivanja paketa u mrežu, pomoću koje teramo AP da šalje ARP pakete koji sadrže IV-ove, veoma brzo. Ovo nam dozvoljava da sakupimo dovoljan broj IV-ova za jedan relativno kratak vremenski period. Da bi smo to uspeli pokrenuli smo aireplay-ng u ARP request replay modu, a to smo učinili tako što smo uneli sledeći kod u terminal:

```
sudo aireplay-ng -3 -b 00:02:72:51:DB:28 -h
00:13:CE:EC:45:20 wifi0
```

- -b je MAC adresa AP-a
- -h je MAC adresa pomoću koje se pretstavljamo AP-u

Razbijanje WEP-a bez ubacivanja paketa:

U slučaju da smo u nemogućnosti da se povežemo sa AP-om, ubacivanje paketa nećemo moći da izvedemo. Druga solucija je da prisluškujemo mrežu, odnosno da pratimo kako napreduje sakupljanje IV-ova koje smo pokrenuli ranije. Cilj nam je da prikupimo barem 150000 u #Data koloni.



Slika 5: *Prikaz koliko je trenutno sakupljeno IV-a*

Kada pogledate kolonu RXQ (slika 5) videćete broj 48, koji pretstavlja vrednost koliko je jak signal od AP-a do vašeg računara. Vrednost ispod 80 se smatra previše niskom. Ako ova vrednost dosta talasa to znači da i vi imate slabu vezu. Ovaj način prikupljanja IV-a traje obično oko 2 sata.

Pokretanje *aircrack-ng*-a zbog dešifrovanja WEP ključa pomoću sakupljenih IV-ova:

Kada se sakupi dovoljan broj IV-ova sledeći korak je dešifrovanje WEP ključa. Postoje dve metode pomoću kojih to možemo da uradimo:

- PTW metoda
- FMS/Korek metoda

Da bi dešifrovali WEP ključ otvorili smo nov terminal i izvršili jedan od sledeća dva koda:

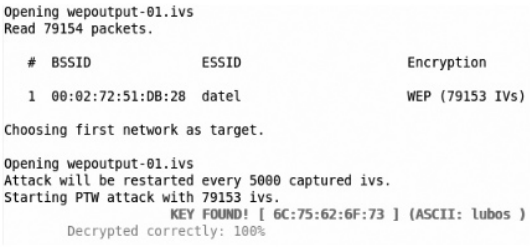
```
sudo aircrack-ng -z -b 00:1A:92:77:BB:D9 wepdump*.ivs
sudo aircrack-ng -a 1 -0 -n 128 wepdump*.ivs
```

Prvi kod se koristi za PTW napad, a drugi za FMS/Korek.

Objašnjenje za prvi kod:
- -z stoji za PTW metod
- -b stoji za AP koji smo izabrali
- wepdump*.ivs selektuje sve fajlove koji počinju sa wepdump a završavaju se sa .ivs

Objašnjenje za drugi kod:
- -a stoji za FMS/Korek metod
- -n selektuje tip WEP ključa, u našem slučaju 128 bita

U napadu koji smo izveli koristili smo FMS/Korek metodu i rezultat bi trebalo da izgleda kao na slici 6. Ovim smo uspešno saznali koji je WEP ključ i time uspešno završili naš napad.



Slika 6: *Rezultat dešifrovanja WEP ključa*

4. ZAKLJUČAK

U ovom radu je prikazan napad na WLAN mrežu pomoću softverskog alata *Aircrack-ng*. U radu je analizirano sledeće:
- Metode prisluškivanja i analize paketa
- Tehnike probijanja lozinke
- Prednosti i mane WEP protokola
- Softver za napad
- Mere zaštite od napada
- Konkretan napad na bežičnu mrežu

Ovde je dat detaljan uvid u to kako se ovakav napad može sprovesti u praksi, a u praksi cela procedura napada je komplikovanija nego što to izgleda u relevantnoj literaturi.

Iz svega se može zaključiti da je WEP protokol prevaziđen i da je potrebno zaštititi bežičnu mrežu novijim i sigurnijim protokolima. Možemo primetiti da je napad na bežičnu mrežu koja je zaštićena WEP protokolom u današnje vreme lako izvesti, odnosno lako je pronaći njegovu šifru (lozinku) ako osoba poseduje barem neka osnovna znanja iz računarskih mreža. Napadom koji je prikazan u radu zapažamo da se veoma lako i što je najbitnije, brzo dolazi do željenog cilja. Ali, takođe, poboljšavanje zaštite nad bežičnom mrežom je lako ostvarivo uzimajući u obzir da su nam novije tehnologije zaštite uglavnom lako dostupne, i da ih današnji router-i i Access Point-i uglavnom imaju integrisane kao standard.

ZAHVALNICA:

Ovaj rad podržan je od strane Ministarstva za nauku i obrazovanje Srbije (Projekat III44006).

LITERATURA:

[1] F. M. Halvorsen, O. Hangen, *Cryptanalysis of IEEE 802.11i TKIP*, NTNU 2009
[2] http://www.kismetwireless.net/ (26. 9. 2012)
[3] www.wireshark.org/docs (26. 9. 2012)
[4] www.aircrack-ng.org (26. 9. 2012)
[5] http://homepages.tu-darmstadt.de/~p_larbig/wlan/ (26. 9. 2012)
[6] M. Gast, 802.11 Wireless Networks: The definitive guide, O'Reilly, 2005
[7] J. Cache, J. Wright, W. Liu, Hacking Exposed Wireless, McGraw-Hill, 2010

Darko Dimitrijević , Inženjer informacionih tehnologija, rodjen je 1986 g. Završio je Fakultet informacionih tehnologija, Metropolitan Univerzitet u Beogradu 2012. g. Bavi se informacionim tehnologijama, i bezbednošću informacionih sistema. Koristi jezike Java, HTML i SQL. Naziv njegovog završnog rada je bio „Analiza saobraćaja i bezbednosti WLAN bežičnih mreža". Kontakt: darkomd@gmail.com

Snežana Vulović, Docent Dr. Inž., predaje na Univerzitetu Metropolitan, Fakultetu za informacione tehnologije, od 2008.g. Njena specijalnost je informaciona bezbednost kompjuterskih sistema, i primena kriptologije. Radila je na nizu naučnih projekata u oblasti računarskih tehnologija, i objavila je niz naučnih radova. Član je Srpskog društva za računsku mehaniku i Srpskog društva za mehaniku. Kontakt: snezana.vulovic@metropolitan.ac.rs

Slobodan Jovanović, Prof. Dr. Inž., predaje na Univerzitetu Metropolitan, Fakultetu za informacione tehnologije, od 2008.g. Bavi se razvojem Web aplikacija, i „pametnim" električnim mrežama (smart electric grids), i veštačkom inteligencijom. Ima veliki broj objavljenih naučnih radova u vodećim internacionalnim časopisima. Predavao je na Strathclyde University, Glasgow, Scotland, u periodu 1993-2008. Učestvovao je u nizu naučnih i razvojnih projekata. Kontakt: slobodan.jovanovic@metropolitan.ac.rs

CIP – Каталогизација у публикацији Народна библиотека Србије, Београд 659.25
INFO M : časopis za informacionu tehnologiju i multimedijalne sisteme = journal of information technology and multimedia systems / glavni i odgovorni urednik Dejan Simić.
– Štampano izd. – God. 1, br. 1 (2002) – . – Beograd : Fakultet organizacionih nauka, 2002 – (Stara Pazova : SAVPO). – 30 cm
Tromesečno. – Je nastavak: Info Science = ISSN 1450-6254. – Drugo izdanje na drugom medijumu: Info M (CD-ROM izd.) = ISSN 1451-4435
ISSN 1451-4397 = Info M (Štampano izd.) COBISS.SR-ID 105690636