NAPADI NA IEEE802.11 BEŽIČNE MREŽE

Dejan M. Tepšić, *Mladen* Đ. Veinović,
Univerzitet Singidunum, Beograd

DOI: 10.5937/vojtehg61-2301

OBLAST: računarske nauke, telekomunikacije
VRSTA ČLANKA: stručni članak

Sažetak:

U radu su prikazani nedostaci današnjih IEEE 802.11 bežičnih mreža u situacijama kada se nađu na meti napadača. U meri u kojoj su namena i obim ovog rada to dozvoljavali, obrađene su savremene metode napada na bežične računarske mreže. Uprkos napretku i razvoju sigurnosnih protokola i dalje postoje slabosti u IEEE 802.11 bežičnim mrežama. Mogući su brojni netehnički, mrežni i softverski napadi. Za sada, bežične mreže nije preporučljivo koristiti u okruženjima gde se ne toleriše nepouzdanost ili nedostupnost.

Ključne reči: *WLAN, IEEE 802.11, bežične mreže, napadi.*

Uvod

U celokupnoj istoriji umrežavanja, nikada nije bilo lakše prodreti u mrežu. IEEE 802.11 bežična mrežna tehnologija omogućuje napadačima i mrežnim administratorima jeftine, čak i besplatne alate za rad. Bilo da su u pitanju strastveni korisnici Linux ili Windows operativnih sistema, alati su dostupni svuda. Zbog postojanja sveprisutne piraterije i hakerskih zajednica, napadači mogu dobiti čak i skupe softvere za analizu i upad na mrežu bez finansijskih ulaganja. Ovaj rad prikazuje najvažnije alate i način njihovog efikasnog korišćenja za prodiranje u bežične mreže i otkrivanje korisnih informacija.

Jedan od najvećih problema današnjih bežičnih mreža je nedostatak efikasnih sistema za detekciju upada. Banke, osiguravajuća društva, kao i druge organizacije koje poseduju osetljive informacije, imaju korporativne politike koje ne dozvoljavaju upotrebu bežičnih mreža. Oni misle da takva politika obezbeđuje sigurnost njihovih ožičenih mreža, ali tu ozbiljno greše. Zlonamernu bežičnu pristupnu tačku mogu postaviti na mrežu napadači ili zaposleni. Tada, bez sistema za detekciju upada, ne bi ni na koji način znali da su svi njihovi sigurnosni mehanizmi zaobiđeni, dajući pun pristup napadaču u opsegu od nekoliko stotina metara od objekta. Mrežni administratori trebalo bi da znaju da koriste alate za pronalaženje

dejan.tepsic.10@singimail.rs

bežičnih pristupnih tačaka, da onemoguće neovlašćene bežične pristupne tačke i da poznaju sve ranjivosti bežičnih mreža. Jedan od najtežih zadataka predstavlja upoznavanje korisnika sa bežičnim mrežnim tehnologijama. Korisnici često ne razumeju tehnologiju, niti rizike povezane sa njom. IEEE 802.11 bežične mreže imaju značajan udeo u nekim organizacijama, ali istovremeno stvaraju ogromnu sigurnosnu rupu. Kompanije moraju pažljivo razmotriti da li su bežične mreže pogodne za njih i mogu li biti adekvatno zaštićene. Brojni faktori utiču na sigurnost bežičnih mreža, od planske instalacije do obuke IT osoblja.

Zaboravljanje pokrivanja nedostataka u bežičnoj mrežnoj sigurnosti može dovesti do upada napadača u mrežu. Rizici mogu uveliko prevagnuti dobit korišćenja bežičnih tehnologija, tako da se neke kompanije odlučuju da ih uopšte ne koriste. Ipak, čak i takve kompanije moraju se zaštititi od bežičnih napada. Poželjno im je demonstrirati alate za napad. Ukoliko imaju bežične mreže osigurane WEP sigurnosnim mehanizmom, otkrivanje WEP ključa brzo će im otvoriti oči. Svakako, ove demonstracije uvek treba izvoditi uz dozvolu klijenta, u zatvorenom okruženju. U suprotnom, to može dovesti do pravnog spora i drugih neželjenih rezultata.

Vreme nikada nije prijatelj IT stručnjaka. Praćenje razvoja novih alata i tehnika zahteva dosta rada i vremena. Tako i ovaj rad predstavlja presek trenutnog stanja u svetu sigurnosti IEEE 802.11 bežičnih mreža.

Bezbednost u IEEE 802.11 bežičnim mrežama

Sigurnost IEEE 802.11 bežičnih mreža prvobitno je bila osigurana WEP sigurnosnim protokolom koji se oslanja na RC4 algoritam za šifrovanje i CRC algoritam za proveru integriteta (Milovanović, 2009). Osnovni problemi WEP-a su kratki inicijalizacioni vektor, nesigurna provera integriteta podataka, korišćenje zajedničkog ključa, nepostojanje mehanizma za upravljanje i zamenu ključeva, nedostatak zaštite od beskonačnog umetanja istog paketa u mrežu, nepostojanje autentifikacije bežične pristupne tačke i sl. Posledice navedenih propusta su laki napadi na WEP mreže, odnosno njihova potpuna nesigurnost.

Zbog toga je započeo rad na IEEE 802.11i protokolu koji je trebalo radikalno da poboljša sigurnost bežičnih mreža. Budući da je razvoj protokola potrajao, izdat je WPA standard, kako bi nadomestio sigurnosnu prazninu koju je izazvao WEP. Takođe, WPA se oslanja na RC4 i CRC algoritme, ali donosi privremene ključeve i MIC algoritam za očuvanje integriteta podataka. Uvedena je 802.1X autentifikacija, odnosno više nisu potrebni zajednički ključevi već je moguće koristiti autentifikacione servere. Povećana je dužina inicijalizacionog vektora koji se dobija na osnovu serijskog broja paketa, kako bi se sprečilo umetanje istog paketa u bežičnu mrežu. Slabost WPA sigurnosnog mehanizma je korišćenje zajedničkog ključa.

Kasnije se pojavio i WPA2 (IEEE 802.11i). Za razliku od WPA mehanizma koji je radio na starim uređajima uz zamenu softvera, WPA2 zahteva nove mrežne uređaje koji mogu obavljati AES šifrovanje. AES zamenjuje RC4 algoritam i donosi znatno veću sigurnost. Integritet podataka kriptografski je zaštićen.

Prvobitni WEP sigurnosni protokol danas je gotovo nezaštićen od brojnih, dokazano izvodljivih napada. WPA, iako noviji sigurnosni protokol, takođe poseduje sigurnosne propuste, te se kao takav ne preporučuje za upotrebu u okruženjima gde se zahteva visok stepen sigurnosti. Sa druge strane, WPA2 sigurnosni protokol, iako dokazano ranjiv, predstavlja sasvim solidno rešenje za kriptografsku zaštitu podataka prilikom prenosa putem IEEE 802.11 bežičnih mreža.

Iako su IEEE 802.11 protokolom definisani sigurnosni standardi, bežične mreže predstavljaju jednu od najslabijih karika u lancu računarskih mreža. Osnovni sigurnosni zahtevi svake računarske mreže su pouzdana provera identiteta korisnika, zaštita privatnosti i autorizacija korisnika. Pomenuti zaštitni mehanizmi poseduju niz sigurnosnih propusta. Međutim, zbog nedovoljne upućenosti u značaj same sigurnosti, veliki broj korisnika ne koristi nikakvu vrstu zaštite, što njihovu mrežu ostavlja otvorenu za napadače. Za uspešnu autentifikaciju korisnika neophodno je korišćenje pouzdanog sistema provere identiteta korisnika.

Neophodno je razmotriti koliko je napad na bežičnu računarsku mrežu izvodljiv u praksi. Početni problem svakog napada je doći do signala same mreže i tako izvesti aktivan ili pasivan napad. Da bi napadač bio u mogućnosti da izvede pasivan napad mora imati opremu koja može da osluškuje i presreće saobraćaj između bežične pristupne tačke i klijenta, što znači da napadač mora poznavati fizički sloj definisan standardom IEEE 802.11. Za aktivan napad potrebno je posedovati opremu koja je sposobna da šalje podatke na mrežu (Evseev, et al, 2011, pp.15–39),a ona nije jeftina. Treba uzeti u obzir i činjenicu da proizvođači bežične mrežne opreme često zanemaruju napade na sloju veze, smatrajući ih nepraktičnim i neizvodljivim, što je pogrešno iz dva razloga:

1. Mogućnost postojanja napadača koji nije ograničen materijalnim resursima i vremenom, tj. napadač može uložiti velika sredstva i svoje vreme kako bi pristupio podacima. Kao primer može poslužiti industrijska špijunaža, koja je prilično profitabilan posao.

2. Hardver potreban za pasivan i aktivan napad dostupan je svima u obliku bežičnih mrežnih kartica ili adaptera za računare. Modifikacija drajvera na takvim karticama omogućuje izvođenje pasivnih i aktivnih napada. Vreme uloženo u takav posao nije kratko, ali je izmena drajvera posao koji se obavlja samo jednom. Ukoliko se gotovi izmenjeni drajveri objave na internetu postaju dostupni svima.

Zbog toga je razumno pretpostaviti da dovoljno motivisan napadač može ostvariti pun pristup sloju podataka i da je u mogućnosti da izvede pasivne i aktivne napade na bežične mreže.

U bežičnim mrežama koriste se različite antene. Prilikom projektovanja bežične mreže u nekom području potrebno je detaljno pregledati to područje i utvrditi optimalnu vrstu antena koje će se koristiti i njihovu snagu zračenja, vodeći računa o svim ograničenjima. Takođe, mora se uzeti u obzir da je frekvencija koju koriste bežične mreže po standardima IEEE 802.11 b, g i n od 2,4 GHz nelicencirana, što znači da može doći do interferencije sa bežičnim uređajima koji rade na istoj ili sličnoj frekvenciji, pa čak i do potpunog uskraćivanja servisa do kojeg uglavnom dolazi usled nepažnje projektanta bežične mreže. Osim toga, potrebno je pretpostaviti da napadač može imati bolju i osetljiviju opremu od one koja je propisana standardima, što praktično proširuje domet mreže van fizičkih granica organizacije kojoj mreža pripada i omogućuje brojne napade među kojima „napad sa parkirališta“ (parking lot attack) i „ratnu vožnju“ (wardriving).

Sigurnosni napadi na IEEE 802.11 bežične mreže

Bežične lokalne računarske mreže definisane IEEE 802.11 standardom nude praktičnost, pokretljivost, a u mnogim slučajevima mogu biti jeftinije i jednostavnije za implementaciju od ožičenih mreža. Kao posledica potražnje i novih industrijskih standarda bežična mrežna tehnologija je prihvaćena i ostaće prisutna. Svakako, postavlja se pitanje sigurnosti bežične mrežne tehnologije.

Bežične mreže definisane su na Institutu inženjera elektrotehnike i elektronike (Institute of Electrical and Electronics Engineers, IEEE) 802.11 skupom standarda (Tanenbaum, Wetherall, 2010). IEEE 802 standard dobio je ime na osnovu godine i meseca kada je ova grupa formirana – februar 1980 godine. Broj 11 u nazivu standarda odnosi se na bežične LAN mreže. Postoji čitav niz industrijskih grupa za bežično umrežavanje, ali dve glavne, opšteprihvaćene su IEEE 802.11 radna grupa i Wi-Fi Alliance.

Uz bežične mreže dolaze novi sigurnosni rizici (Earle, 2006).

Netehnički napadi

Ove vrste napada koriste različite ljudske slabosti, kao što su nedostatak savesti, nehat i preterana poverljivost prema strancima. Tu su, takođe, fizičke ranjivosti koje napadaču daju direktan pristup na bežične uređaje. To su često najlakše vrste napada koji uključuju:

– upad na bežične uređaje koje su korisnici samostalno instalirali i ostavili nezaštićene,

– socijalni inženjering, napadi gde se napadač predstavlja kao neka druga osoba i navodi korisnike na odavanje informacija o sopstvenoj mreži,
– fizički pristup na pristupne tačke, antene i ostalu bežičnu opremu.

Mrežni napadi

Kada je reč o mrežnim napadima, postoje brojne tehnike koje napadači mogu koristiti kako bi provalili unutar bežične mreže ili je bar onesposobili. Ovi napadi uključuju:
– instaliranje zlonamernih bežičnih pristupnih tačaka i varanje bežičnih klijenata koji se povezuju na njih,
– snimanje mrežnog saobraćaja sa udaljenosti: šetnjom, vožnjom ili letom iznad mreže,
– napadanje mrežnog saobraćaja lažiranjem MAC adrese (napadač se maskira kao legitiman korisnik), napad „čoveka u sredini“ (umetanje bežičnog sistema između bežične pristupne tačke i bežičnih klijenata) i slično,
– korišćenje mrežnog protokola poput SNMP-a,
– napad uskraćivanja servisa (Denial of Service, DoS),
– ometanje RF signala.

Softverski napadi

Pored sigurnosnih problema sa IEEE 802.11 protokolom, prisutne su softverske ranjivosti operativnih sistema i programa na bežičnim klijentima. Navodimo neke primere softverskih napada:
– napadanje operativnih sistema i drugih aplikacija na bežičnim klijentima,
– upadi putem podrazumevanih parametara, kao što su lozinke i SSID-ijevi koji se mogu lako odrediti,
razbijanje WEP ključeva i prisluškivanje unutar mrežnog sistema šifrovanja,
– ostvarivanje pristupa iskorišćavanjem slabe mrežne autentifikacije.

Metodologija napada

Pre nego što započne testiranje bežične mreže na sigurnosne propuste važno je definisati formalnu metodologiju testiranja (Graves, 2010). Postoje formalne procedure koje bi trebalo uključiti u testiranje da bi ono bilo ispravno i da bi se optimalno iskoristilo:
– prikupljanje javnih informacija, kao što su imena domena i IP adrese koje mogu poslužiti kao dobro polazište,
– mapiranje mreže da bi se dobila opšta ideja o njenom izgledu,

– skeniranje sistema da bi se videlo koji uređaji su aktivni i komuniciraju,
– utvrđivanje servisa koji se koriste,
– pretraga za specifičnim ranjivostima,
– napad na sistem.

Napadači započinju napad na bežične mreže posmatranjem sistema kako bi pronašli njegove slabosti. Za početak potrebno je pretražiti sledeće parametre bežične mreže:

– jačinu radio-signala,
– specifične SSID-ijeve koji se emituju,
– IP adresni plan,
– zaštitne mehanizme, kao što su WEP, WPA, WPA2 ili VPN saobraćaj,
– hardverske modele uređaja,
– softversku verziju uređaja.

Snimanje sistema

Prvi korak pre samog napada je snimanje sistema (footprinting), odnosno sakupljanje informacija o mreži koje su dostupne svima. Većina podataka otkriva se pomoću pretraživača kao što je Google (www.google.com). Zapravo, Google je jedan od omiljenih alata za obavljanje procene sigurnosti u celini. Iznenađujuće je šta se sve može učiniti sa njim. Moguće je tražiti informacije o bežičnim sistemima, njihovoj konfiguraciji, pretraživati ključne reči i informacije koje su slučajno ili namerno objavljene na internetu. Budući da su bežične mreže uglavnom lokalizovane, javno dostupne informacije možda neće biti rasprostranjene u onoj meri kao što je to slučaj kod ožičenih mrežnih sistema.

Sledeća područja u potrazi za informacijama o bežičnim sistemima su internet baze podataka bežičnih mreža, koje sadrže podatke kao što su SSID-ijevi, MAC adrese i GPS koordinate bežičnih pristupnih tačaka koje su otkrili znatiželjni napadači.

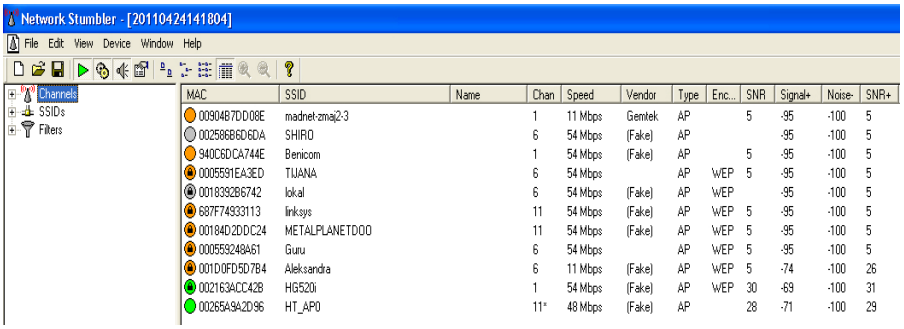
Mapiranje mreže

Drugi korak je stvaranje mrežne karte koja pokazuje kako bežični sistem izgleda. Mapiranje bi trebalo učiniti iz oba smera, unutar i izvan mreže, jer bežične mreže poseduju radio-talasnu karakteristiku. Emitovanje radio-talasa omogućuje njihovo otkrivanje sa obe strane.

Network Stumbler

Network Stumbler (www.netstumbler.com) najbolji je alat za mapiranje bežičnih mreža, odnosno za stvaranje unutrašnjeg i spoljašnjeg izgleda bežične mreže. Ovaj besplatni Windows alat omogućuje napadaču skeniranje radio-talasa izvan zgrade, dok sedi u automobilu na parkiralištu ili tokom „ratne vo-

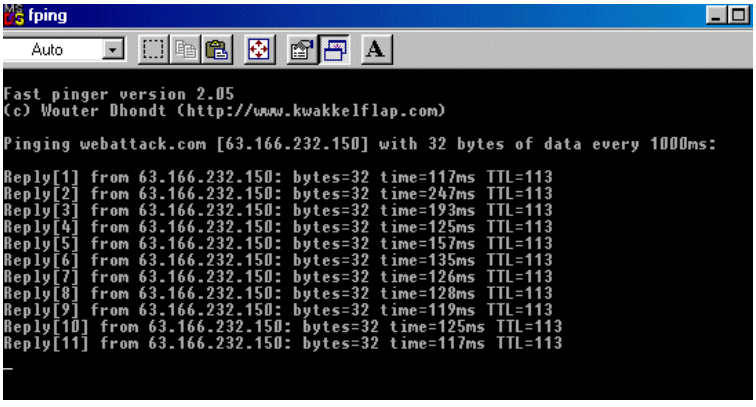
žnje“. Može se pokrenuti i unutar zgrade kako bi pronašao sve bežične pristupne tačke, među kojima i zlonamerne koje ne pripadaju toj mreži. Slika 1 prikazuje informacije koje Network Stumbler može prikupiti o bežičnoj mreži, bez obzira na to da li je zaštićena WEP, WPA ili WPA2 sigurnosnim protokolom.



Slika 1 – Network Stumbler
Figure 1 – Network Stumbler

Nmap i Fping

Ovi alati koriste protokol za upravljanje porukama na internetu (Internet Control Message Protocol, ICMP), kako bi se utvrdilo koji klijenti su prisutni na bežičnoj mreži, bez obzira na to da li je mreža zaštićena WEP, WPA ili WPA2 sigurnosnim protokolom. Nmap (http://nmap.org) i Fping (http://fping.sourceforge.net) jesu alati napisani za Windows, UNIX i Linux platforme. Razlikuju se od običnog *ping*-a koji pokušava dobiti odgovor samo od jednog klijenta, u tome što oni šalju ping paket na jednog klijenta i momentalno prelaze na sledećeg u round-robin algoritmu. Ako klijent odgovori, to se beleži i uklanja sa spiska klijenata za proveru. Ako klijent ne odgovori u određenom roku, smatra se nedostupnim. Na slici 2 prikazan je alat Fping.



Slika 2 – Fping
Figure 2 – Fping

Skeniranje sistema

Kada se prikupe osnovne informacije o bežičnoj mreži, kao što su SSID i IP adrese, više informacija moguće je saznati kroz proces skeniranja sistema koji se zove nabrojiva lista (enumeration). Nabrojiva lista je ispitivanje sistema i pravljenje liste sa svim detaljima koje je moguće otkriti o tome šta i kako radi. Procesom nabrojive liste moguće je otkriti:

– žive bežične mrežne uređaje (pristupne tačke i bežične klijente),
– jačinu radio-signala,
– koji sigurnosni mehanizmi se koriste,
– koji mrežni portovi su otvoreni na bežičnim pristupnim tačkama i klijentima.

Network Stumbler ne samo da može otkriti žive bežične mrežne uređaje, već i detaljnije informacije o jačini radio-signala i sigurnosni mehanizam koji se koristi. Stoga je Network Stumbler dobar alat za skeniranje sistema.

Korišćenjem alata za skeniranje portova kao što je Nmap moguće je videti koji mrežni portovi su otvoreni na bežičnim mrežnim uređajima. Skeniranje portova pomaže napadačima u stvaranju detaljnije slike o servisima koji su dostupni na bežičnoj mreži. Te informacije im pružaju polaznu tačku da pokušaju iskoristiti potencijalne ranjivosti sistema. Tabela 1 prikazuje portove koji se često mogu pronaći otvoreni i koji su osetljivi na napade.

Tabela 1

Često napadani mrežni portovi

Table 1

Often attacked network ports

Broj porta	***Servis***	***Protokol***
20	FTP data (File Transfer Protocol)	TCP
21	FTP control	TCP
22	SSH (Secure Shell)	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
53	DNS (Domain Name System)	UDP
80	HTTP (HyperText Transfer Protocol)	TCP
110	POP3 (Post Office Protocol version 3)	TCP
135	DCE/RPC Endpoint Mapper for Microsoft networks	TCP, UDP
137,138,139	NetBIOS over TCP/IP	TCP, UDP
161	SNMP (Simple Network Management Protocol)	TCP, UDP
443	HTTPS (HTTP over SSL)	TCP
512,512,514	Berkeley remote commands (rsh, rexec and rlogin)	TCP
1433	Microsoft SQL Server	TCP, UDP
1434	Microsoft SQL Monitor	TCP, UDP
3389	Windows Terminal Server	TCP

Napadi na IEEE 802.11 bežične mreže

Socijalni inženjering

Socijalni inženjering (Beaver, Davis, 2005) jeste tehnika napadača kojom se iskorišćava prirodno poverenje većine ljudi. Napadači se često predstavljaju kao zaposleni radnici unutar kompanije ili kao neke druge osobe, kako bi dobili informacije kojima inače ne bi mogli pristupiti. Zatim koristite dobijene informacije kako bi dublje prodrli u računarsku mrežu.

Socijalni inženjering se lakše izvodi u većim kompanijama, ali to se može dogoditi svakome. Napadač može tvrditi da je kupac, poslovni partner, konsultant, administrator i sl.

Najlakši način za početak prikupljanja informacija tokom socijalnog inženjeringa je jednostavno pretraživanje interneta putem Googla. Napadač može koristiti Google kako bi pronašao telefonski imenik kompanije, organizacione dijagrame, mrežne dijagrame i sl. Te informacije mogu se koristiti kao osnova za socijalni inženjering i konačan prodor u mrežu.

Napadač može koristiti razne metode za prikupljanja informacija od zaposlenih. Dve jednostavne i manje zahtevne metode su telefon i elektronska pošta. Napadač može jednostavno pozvati slučajanog zaposlenog i početi postavljati pitanja. Pritom koristi telefon na kojem neće odati svoj identitet. Isto može učiniti i sa elektronskom poštom, pri čemu će promeniti svoj nalog u e-mail klijentu ili će koristiti Web poštu (webmail).

Fizička sigurnost IEEE bežičnih mreža

Neovlašćena oprema

Vrlo čest problem je naivno uvođenje bežične opreme na mrežu. Naime, neki korisnici samostalno instaliraju bežičnu opremu u kancelariji, ne razumejući sigurnosne probleme povezane sa njihovom radnjom.

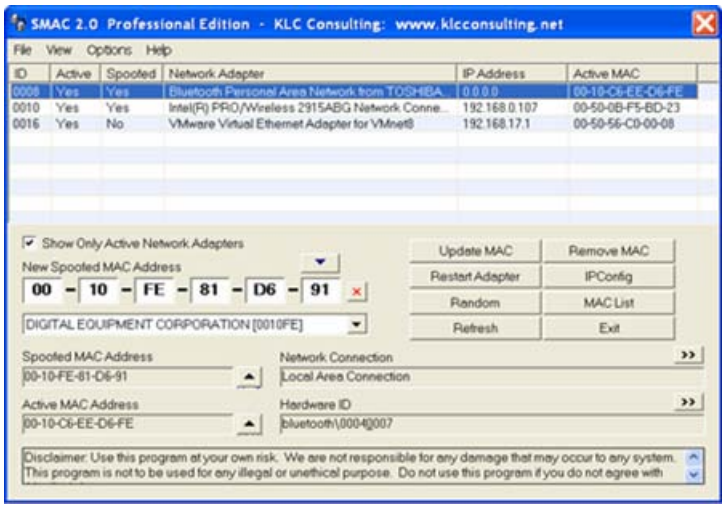
Podešavanje snage zračenja bežične pristupne tačke

Radio-talasi putuju, što znači da napadačima nije potrebna fizička konekcija na bežičnoj mreži. Prvi korak za testiranje bezbednosti bežične računarske mreže jeste da se utvrde njene granice. Radio-talasi ne poštuju definisane granice, pa je na mestima gde se ne želi emitovanje signala neophodno smanjiti snagu zračenja bežične pristupne tačke, tako da signali putuju na kraćim udaljenostima. Ukoliko se signali i dalje prostiru van definisanih granica mreže može se uneti dodatno slabljenje upotrebom atenuatora. Konačno, moguće je jednostavno premestiti bežičnu pristupnu tačku.

Provera mreže za neželjenim klijentima

Većina bežičnih pristupnih tačaka omogućuje da se vide IP adrese asociranih klijenata ili keš svih MAC adresa. Za male mreže dovoljno je povremeno pregledati keš MAC adresa, kako bi bili sigurni da su samo legitimni klijenti asocirani na bežičnu pristupnu tačku. Ukoliko se pronađe klijent koji tu ne pripada, može se koristiti MAC filtriranje za blokiranje tog klijenta.

Za velike mreže praćenje svih MAC adresa unutar kompanije je isuviše teško. Pritom, napadač bi mogao koristiti alat za nadgledanje protoka podataka i otkriti legitimne MAC adrese klijenata. Tada bi mogao koristiti alat za menjanje MAC adrese, kao što je SMAC (Spoof MAC) koji mu omogućava da promeni hardversku ili MAC adresu na bilo kom interfejsu na Windows operativnom sistemu. Slika 3 prikazuje SMAC (www.klcconsulting.net/smac) korisnički interfejs. Ovaj napad podjednako je efikasan na bežičnim mrežama zaštićenim WEP, WPA ili WPA2 sigurnosnim protokolom.



Slika 3 – SMAC
Figure 3 – SMAC

Antene

Antene su sastavni deo bežičnih računarskih mreža. Prilikom postavljanja bežične pristupne tačke mora se razmotriti oblast zračenja različitih tipova antena. Tip izabrane antene utiče na performanse i domet bežične mreže, kao i njenu sigurnost.

U bežičnim računarskim mrežama koriste se četiri osnovna tipa antena:
– parabolična,
– yagi,
– dipol,
– omnidirekciona.

Parabolična antena

Parabolična antena prvenstveno se koristi za konekcije tipa tačka na tačku. Može biti u obliku tanjira ili kao žičana rešetkasta mreža. Parabolična antena je usmerena, što znači da zrači u jednom određenom pravcu.

Yagi antena

Yagi antena fokusira zrake, ali u manjoj meri nego parabolična antena. Pogodna je za konekcije tipa tačka na tačku na manjim udaljenostima. Poput parabolične antene, yagi antena je, takođe, direkciona.

Napadači mogu koristiti modifikovane yagi antene, kako bi znatno povećali razdaljinu sa koje mogu pristupiti bežičnoj mreži. Ovakve antene osiguravaju dobit od 16 dBi. Usmerene antene su dobre za ciljanje u susedne zgrade. Na slici 4 prikazana je modifikovana yagi antena, Cantenna (www.cantenna.com).

Slika 4 – Cantenna (usmerena, direkciona antena)
Figure 4 – Cantenna (focused, directional antenna)

Dipol antena

Dipol antena je dvosmerna, a prvenstveno se koristi za povezivanje klijenata na bežičnu pristupnu tačku.

Omnidirekciona antena

Omnidirekciona antena zrači u svim smerovima, uz gubitak snage zračenja sa povećanjem udaljenosti. Slika 5 prikazuje omnidirekcionu antenu. Većina bežičnih pristupnih tačaka isporučuje se sa malom omnidirekcionom antenom.

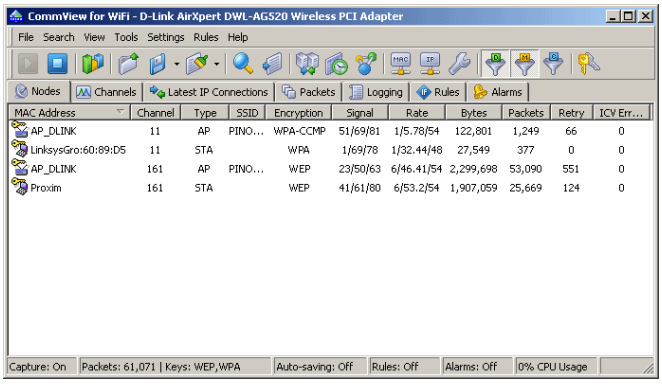
Slika 5 – Omnidirekciona antena
Figure 5 – Omnidirectional antenna

Otkrivanje podrazumevanih vrednosti

Nadgledanje protoka podataka

CommView for WiFi

CommView for WiFi je alat za nadgledanje protoka podataka (sniffer), specifičan za bežične mreže (Cache, Wright, Liu, 2010). Pored toga, nudi statističke analize na osnovu kojih se mogu prepoznati oblici neovlašćenog korišćenja mreže. CommView sakuplja pakete, čuva ih i analizira. Da bi snimio sve pakete na mreži postavlja bežični adapter u mod za monitorisanje. CommView for WiFi (slika 6) ne može prikupiti podatke sa bežične pristupne tačke zaštićene WEP, WPA ili WPA2 sigurnosnim protokolom, osim ako se ne unesu odgovarajući ključevi. CommView for WiFi je komercijalni proizvod napisan za Windows operativne sisteme, dostupan za preuzimanje sa internet adrese www.tamos.com/products/commview.

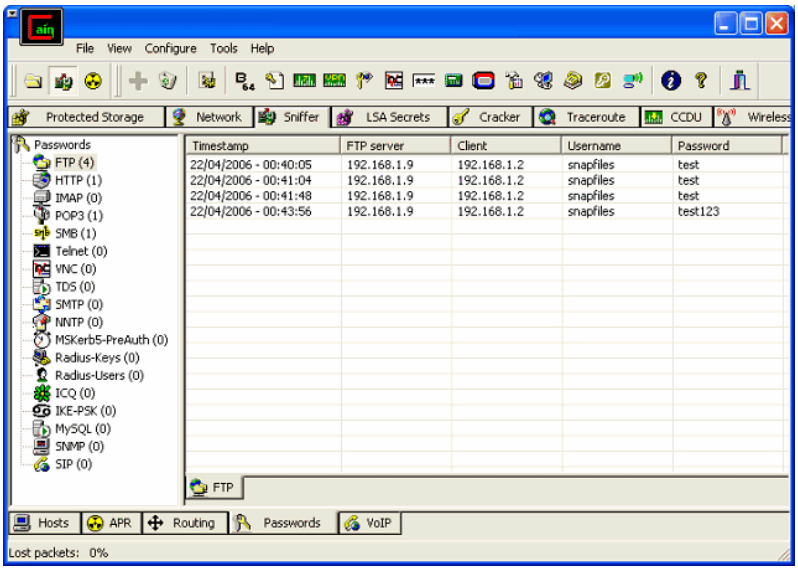


Slika 6 – CommView for WiFi
Figure 6 – CommView for WiFi

Otkrivanje lozinki

Cain & Abel

Cain & Abel je besplatan alat za otkrivanje lozinki (password recovery) napisan za Windows platformu. Sastavljen je od dva programa, Cain i Abel (slika 7), koji zajedno omogućuju pronalaženje raznih vrsta lozinki njuškanjem po mreži, razbijanje šifrovanih lozinki koristeći rečnike, napade grubom silom, dešifrovanje šifrovanih lozinki, otkrivanje lozinki unutar polja, otkrivanje keširanih lozinki i dr. Ovaj alat koristi sigurnosne slabosti unutar nekih protokola, metoda autentifikacije i mehanizama za keširanje. Cain & Abel može analizirati šifrovane protokole, kao što su SSH i HTTPS, i hvatati ovlašćenja na mehanizmima za autentifikaciju. Cain & Abel (www.oxid.it/cain.html) predstavlja univerzalni alat za otkrivanje svih vrsta lozinki. Zahvaljujući sigurnosnim propustima u okviru WEP i WPA sigurnosnog protokola, Cain & Abel može uspešno otkriti tajni ključ.



Slika 7 – Cain & Abel
Figure 7 – Cain & Abel

Prikupljanje IP adresa

Arping

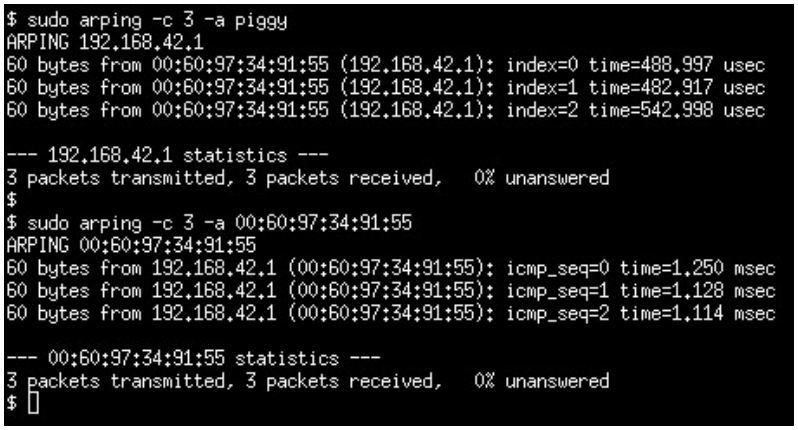
Napadači traže mete – IP adrese. Ako se na bežičnoj mreži koristi zaštitni mehanizam filtriranja MAC adresa, tada napadač mora prikupiti IP adrese. To može uraditi jednostavnim slanjem probnog signala *ping*

na svakog klijenta na mreži da bi dobio tabelu translacija MAC adresa u IP adrese. Ali, to je neefikasno, pa umesto toga napadač može *ping*-ovati opštu adresu mreže (broadcast), što će zauzvrat poslati probni signal *ping* na sve klijente na lokalnoj podmreži. To je ono što alat Arping radi.

Na Windows operativnim sistemima *arp* naredba pruža pristup lokalnom ARP kešu. Upisivanje komande *arp-a* u komandnom odzivniku (command prompt) prikazaće sve stavke ARP keša tog računara, koji čuva sve prethodno razrešene hardverske ili MAC adrese.

Alat Arping (www.habets.pp.se/synscan/programs.php?prog=arping) sličan je probnom signalu *ping*, ali razlikuje se po tome što radi na mrežnom sloju. Dok probni signal *ping* testira dostupnost IP adrese, Arping prikazuje IP adresu cilja, njegovu MAC adresu, kao i vreme koje je proteklo između ARP zahteva i ARP odgovora. Korišćenje opcije *U* šalje ARP zahtev na opštu adresu mreže i kao rezultat dobijaju se sve IP adrese na tom mrežnom opegu.

Na slici 8 prikazan je primer korišćenja alata Arping.



Slika 8 – Arping
Figure 8 – Arping

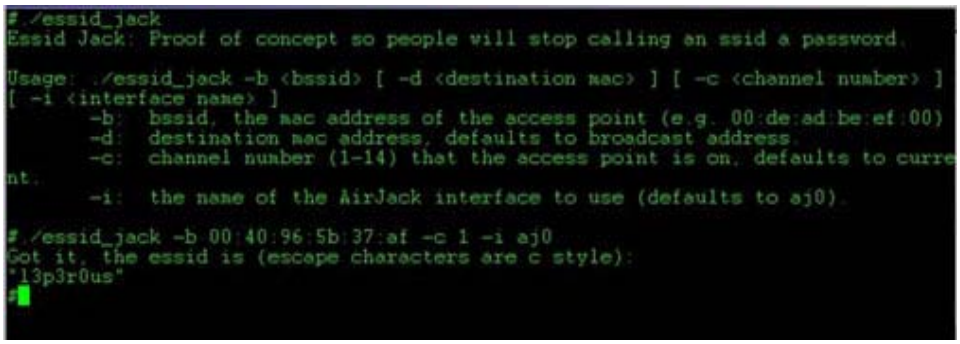
Prikupljanje SSID-ijeva

AirJack

Za spajanje na bežičnu pristupnu tačku neophodno je znati njen SSID. Nasuprot onome što neki misle, SSID nije lozinka i ne treba ga posmatrati kao takvog.

Essid_jack je deo paketa alata otvorenog koda AirJack, i može se preuzeti sa Web adrese http://sourceforge.net/projects/airjack. Es-

sid_jack otkriva čak i skrivene SSID-ijeve. Razlog tome je što bežična pristupna tačka šalje SSID kao otvoreni tekst kada se legitiman bežični klijent pokušava spojiti. Međutim, većina napadača su nestrpljivi i ne žele da čekaju da se neko od legitimnih korisnika pokuša povezati. U stvari, Essid_jack se predstavlja kao bežična pristupna tačka, na taj način što lažira svoju MAC adresu. Zatim, šalje disasocijacionu poruku klijentima, forsirajući ih da se disasociraju sa legitimne bežične pristupne tačke. Klijenti potom pokušavaju da urade reasocijaciju na bežičnu pristupnu tačku i, čineći to, šalju zahtev za asocijaciju koji sadrži SSID pristupne tačke kao otvoreni tekst. Tada Essid_jack snima SSID. Na slici 9 prikazan je alat Essid_jack, kao i primer zadavanja lažne MAC adrese i praćenja saobraćaja na kanalu 1. Napad je uspešan i otkriven je SSID legitimne bežične pristupne tačke „l3p3r0us". Alat Essid_jack delotvoran je za napade na bežične mreže zaštićene WEP sigurnosnim protokolom.



Slika 9 – Essid_jack
Figure 9 – Essid_jack

Ratna vožnja

Kada se razmatraju mogući napadi na bežične mreže, prvo što se pomisli jeste da neko vozi svoj automobil po komšiluku sa prenosnim računarom i otkriva bežične pristupne tačke na koje se kasnije pokušava spojiti (Hurley, Rogers, Thornton, 2007). Ta aktivnost otkrivanja bežičnih računarskih mreža naziva se „ratna vožnja" (wardriving). Isti napad moguće je izvesti i bez automobila, šetajući po komšiluku sa ručnim računarom (Pocket PC). Tada se napad naziva „ratna šetnja" (warwalking). Napad je moguće izvesti i u vožnji biciklom (warcycling), kao i letom iz aviona (warflying).

Sve što je potrebno za „ratnu vožnju" jeste softver i bežična mrežna kartica ili adapter, na koje je moguće dodati eksternu antenu za poveća-

nje jačine signala do bilo koje pronađene bežične pristupne tačke. To napadaču omogućuje da otkrije bežične pristupne tačke na većim udaljenostima nego kada se koristi ugrađena antena unutar bežične mrežne kartice. Takođe, moguće je koristiti uređaj za globalno pozicioniranje (Global Positioning System, GPS) kako bi se na karti odredile koordinate otkrivenih bežičnih pristupnih tačaka.

Network Stumbler

Network Stumbler je najkorišćeniji alat za „ratnu vožnju" napisan za Windows platformu. On koristi aktivni metod skeniranja opisan IEEE 802.11 standardom za otkrivanje bežičnih pristupnih tačaka. Tvorci ovog standarda kreirali su opciju aktivnog skeniranja kako bi klijenti sa višestrukim jedinstvenim mrežama mogli naći sve njihove dostupne mreže. Network Stumbler šalje brojne ispitne poruke (probe request) i evidentira odgovore na njih (probe response). Nakon što bežična pristupna tačka dobije ispitnu poruku, odgovara sa upravljačkim okvirom koji sadrži mrežni BSSID, odnosno jedinstvenu MAC adresu pristupne tačke, i SSID pristupne tačke. Sigurnosno rešenje koje se nameće jeste korišćenje bežičnih pristupnih tačaka koje mogu maskirati svoj SSID, prisiljavajući klijente da prethodno znaju SSID mreže kojoj pristupaju. Network Stumbler može otkriti bežične mreže zaštićene WEP, WPA ili WPA2 sigurnosnim protokolom, ali ne može prijaviti bežične pristupne tačke koje maskiraju svoj SSID. U tom slučaju napadač mora koristiti napredniji alat Kismet.

Kada Network Stumbler locira bežičnu mrežu, beleži sledeće informacije:

– signal, šum i odnos signal/šum (SNR) otkrivene bežične pristupne tačke, što napadaču daje informaciju koliko je udaljen od nje,

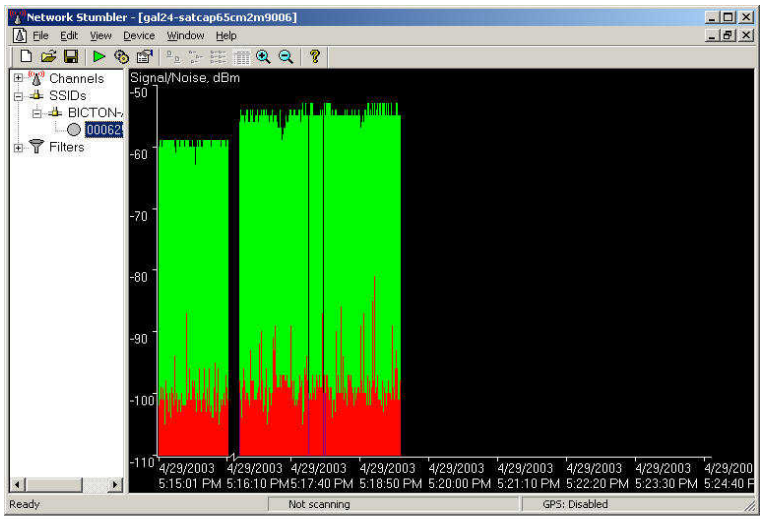
– operativni kanal (između 1 i 11),

– osnovni SSID (BSSID), zapravo MAC adresu pristupne tačke,

– Service Set Identifier (SSID), jedinstveni identifikator bežične računarske mreže maksimalne dužine do 32 karaktera, ugrađen u zaglavlje svih poslatih paketa preko bežične mreže,

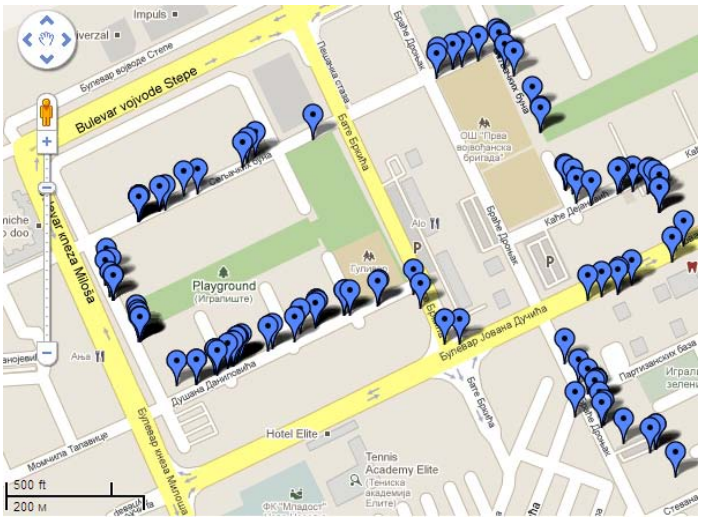
– naziv bežične pristupne tačke.

Network Stumbler poseduje grafički prikaz jačine signala i odnosa signal/šum (slika 10) primljenih sa bežičnih pristupnih tačaka ili drugih bežičnih klijenata u okruženju. Ovi parametri omogućuju da se sa usmerenom antenom otkrije lokacija izvorišta signala. Kada je opremljen GPS uređajem, Network Stumbler beleži koordinate otkrivenih bežičnih pristupnih tačaka.



Slika 10 – Network Stumbler – Odnos signal/šum
Figure 10 – Network Stumbler – Signal/Noise ratio

Po završetku „ratne vožnje“ potrebno je sačuvati podatke iz Network Stumbler-a u vidu *txt* datoteke. Takvu *txt* datoteku moguće je menjati i uneti koordinate u internet alatku GPS Visualizer (www.gpsvisualizer.com) koji će zadate koordinate ucrtati na Google mapama (slika 11). Takvu mapu (www.personalmag.rs) moguće je sačuvati u različitim grafičkim formatima.



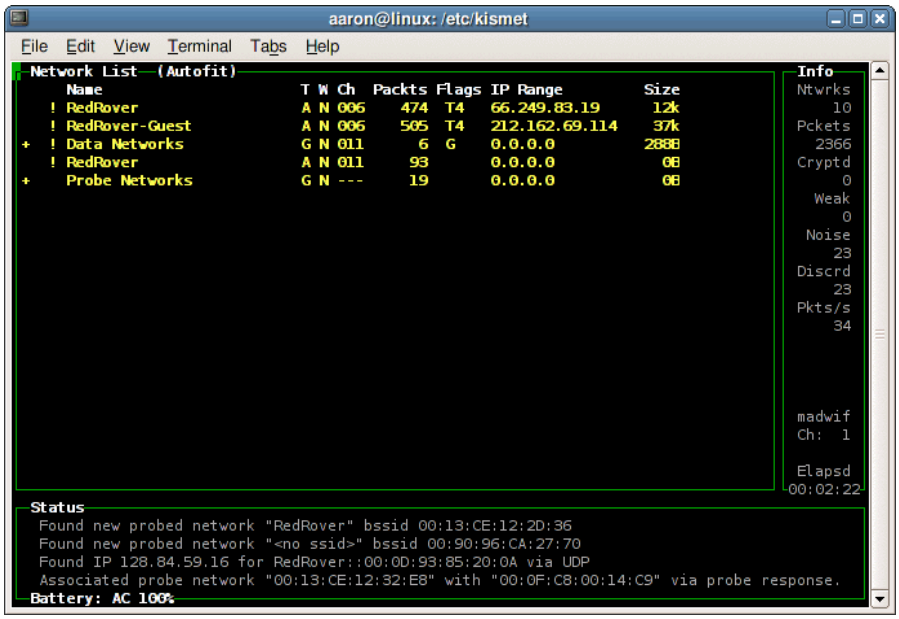
Slika 11 – GPS Visualizer – Mapa skenirane oblasti ucrtana u Google mapama
Figure 11 – GPS Visualizer – Map of the scanned area marked in Google Maps

Kismet

Network Stumbler ne pronalazi mreže koje ne odašilju svoj SSID, te ga je potrebno dopuniti drugim alatima. Kismet je pasivni mrežni skener, alat za nadgledanje protoka podataka i sistem detekcije upada. Sposoban je za otkrivanje saobraćaja sa bežične pristupne tačke i bežičnih klijenata na standardnim i skrivenim bežičnim mrežama zaštićenim WEP ili WPA sigurnosnim protokolom sa tajnim ključem. Funkcioniše na svim bežičnim mrežnim adapterima koji mogu raditi u režimu za monitorisanje.

Kismet je napisan za Linux, te kao takav zahteva odgovarajuću proceduru pri instalaciji. Prvi korak pri instalaciji Kismet-a (http://kismetwireless.net) jeste konfigurisanje pomoću skripte, zadavanjem komande *./configure* iz komandnog okruženja (command shell)**.** Zatim je potrebno ulogovati se sa *root* korisničkim nalogom. Da bi se kompajlirao Kismet potrebno je zadati komandu *make* i zatim *make install* da bi se instalirao Kismet. Potom treba instalirati besplatan alat Global Positioning System Daemon (http://prdownload.berlios.de/gpsd/gpsd-2.38.tar.gz) koji daje prostornu informaciju dobijenu sa GPS-a. To je korisno za „ratnu vožnju" kako bi otkrivene bežične mreže bilo moguće ponovo pronaći.

Instalacija je završena i komandom *kismet* startuje se program koji će automatski prepoznati bežičnu mrežnu karticu ili adapter.



Slika 12 – Kismet
Figure 12 – Kismet

Na slici 12 prikazane su informacije koje su dostupne kada Kismet radi. Vidi se da Kismet ima tri okvira:

– listu mreža (Network List),

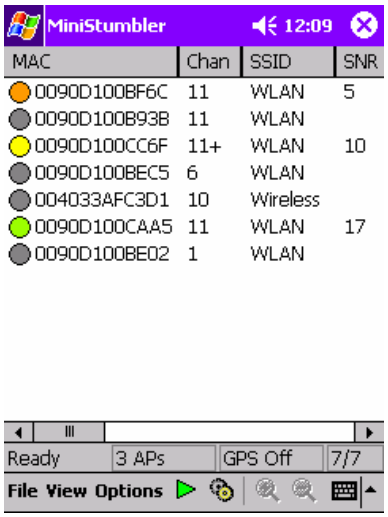
– statističke informacije (Info),

– status (prikazuje glavne događaje, kao što su pronađene bežične mreže i stanje baterije na prenosivom računaru).

Kismet prikazuje spisak pronađenih bežičnih mreža bez određenog redosleda. Za sortiranje po različitim kriterijumima koristi se taster *s*. Pritiskom na taster *i* dobijaju se detaljne informacije o određenoj bežičnoj mreži. Kismet automatski snima sve podatke u datoteke za evidenciju (log file) dok je pokrenut. Kada se završi rad sa Kismet-om, pritiskom na taster *q* zatvara se aplikacija.

MiniStumbler

MiniStumbler (slika 13) jeste kompaktno izadanje Network Stumblera za ručni računar (Pocket PC) i mobilne uređaje sa Windows Mobile platformom. Obično se koristi za „ratnu šetnju“, jer nudi slične mogućnosti kao i Network Stumbler, jednostavan je za upotrebu i mobilan. Zbog manjeg ekrana prikazuje manje informacija i nema mogućnost grafičkog prikaza odnosa signal/šum za pojedinačne mreže, ali u log fajlovima čuva iste podatke kao i veći brat Network Stumbler. Dostupan je besplatno za preuzimanje sa internet adrese www.netstumbler.com/downloads.



Slika 13 – MiniStumbler
Figure 13 – MiniStumbler

Mrežni napadi

Lažiranje MAC adrese

Uobičajen napad za zaobilaženje osnovne kontrole pristupa u bežičnim mrežama je maskiranje sopstvene MAC adrese MAC adresom nekog od legitimnih klijenata na mreži (MAC address spoofing). Napadači to čine krađom identiteta, odnosno predstavljaju se kao da imaju identitet drugog klijenta. Svi mrežni uređaji, ožičeni ili bežični, moraju imati mrežni identifikator, MAC (Media Access Control) adresu. MAC adresa svakog uređaja je jedinstveni broj od 48 bita (šest bajtova) koji dodeljuje proizvođač mrežnog uređaja. Prva 24 bita (tri bajta) MAC ili hardverske adrese čine broj jedinstven za svakog proizvođača mrežne opreme. Te vrednosti dodeljuje IEEE, pod nazivom organizacijski jedinstveni identifikator (Organizationally Unique Identifier, OUI). Javno dostupna internet baza jedinstvenih identifikatora svih proizvođača nalazi se na adresi: http://standards.ieee.org/develop/regauth/oui/public.html.

Preostala 24 bita (tri bajta) MAC adrese stvaraju jedinstveni identifikator za svaku mrežnu karticu. Ideja je da se uređaj identifikuje na mreži bez izazivanja konflikata sa drugim sistemima, pa napadač koji koristi lažnu MAC adresu može napraviti velike nevolje. Ovaj napad je podjednako poguban za bežične mreže zaštićene WEP, WPA ili WPA2 sigurnosnim protokolom.

Za promenu MAC adrese na Linux-u moguće je koristiti besplatnu alatku GNU MAC Changer (www.alobbs.com/macchanger).

Demonstracija jednostavnosti lažiranja MAC adrese

1. Prvi korak je pronalaženje bežične pristupne tačke. Najjednostavnije skeniranje bežičnih mreža je putem alata Network Stumbler. Pomoću ovog alata napadač pronalazi SSID i MAC adresu željene bežične pristupne tačke.

2. Drugi korak je korišćenje analizatora bežične mreže, poput Omni-Peek-a za traženje bežičnih klijenata koji šalju ispitne poruke na opštu adresu mreže ili za traženje bežične pristupne tačke koja odgovara na ispitne poruke,

3. Kada se otkrije MAC adresa legitimnog klijenta na mreži potrebno je promeniti MAC adresu na napadačevom računaru, tako da bude istovetna sa MAC adresom legitimnog klijenta. Treba imati na umu da pristupne tačke, ruteri, svičevi i drugi mrežni uređaji uglavnom poseduju mogućnost da otkriju kada više od jednog klijenta na mreži koristi istu MAC adresu. U tom slučaju potrebno je sačekati da se drugi klijent raskači sa mreže ili je potrebno poslati paket za deautentifikaciju legitimnog klijenta,

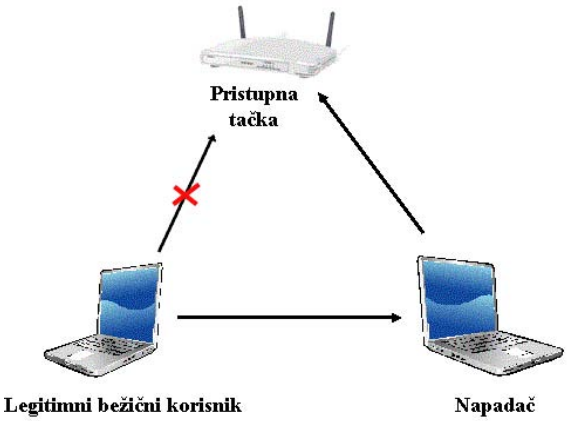
4. Bežični mrežni interfejs na napadačevom računaru potrebno je podesiti sa odgovarajućim SSID-ijem mreže na koju se želi zakačiti. Ukoliko se na mreži koristi WEP zaštita potrebno je uneti odgovarajuće ključeve. Ovo je korak gde napadač mora koristiti odgovarajuće alate za njihovo pronalaženje.

5. Sledeći korak je dobijanje IP adrese na napadačevom računaru, bilo dinamički, putem DHCP-a, ili njenim statičkim zadavanjem.

6. Konačno, potebno je utvrditi da je ostvaren pristup na odgovarajućoj mreži, jednostavnim *ping*-om poznatih klijenata. Tada se napadač uspešno infiltrirao na sistem i dalje može činiti šta mu je volja.

Napad „čoveka u sredini“

Napadom „čoveka u sredini“ (Man-in-the-Middle, MITM) napadač umeće svoj sistem u sredinu komunikacije između bežičnih klijenata i bežične pristupne tačke (Bobar, 2009, pp.80–87). Napad „čoveka u sredini” izvodljiv je u bežičnim mrežama bez obzira na to da li se u njima koristi WEP, WPA ili WPA2 sigurnosni protokol.



Slika 14 – Napad „čoveka u sredini“
Figure 14 – Man-in-the-Middle attack

Legitimni bežični korisnik biće prevaren pri povezivanju, tako što će biti asociran na napadačev sistem umesto na legitimnu bežičnu pristupnu tačku (slika 14). Tada će napadač moći prisluškivati mrežni saobraćaj, ubacivati nove pakete, menjati njihov sadržaj, preusmeravati saobraćaj, pa čak i u potpunosti obustaviti komunikaciju između klijenata i bežične pristupne tačke. Tok napada „čoveka u sredini“:

1. Napadač pronalazi bežičnog klijenta koji je povezan i koji komunicira sa bežičnom pristupnom tačkom, saznaje njegovu MAC adresu i radio-kanal.

2. Napadač šalje deautentifikacionu ili disasocijativnu poruku klijentu, prisiljavajući ga da se raskači sa pristupne tačke.

3. Napadač aktivira lažnu bežičnu pristupnu tačku, predstavljajući je kao legitimnu, koristeći isti SSID i MAC adresu kao na legitimnoj pristupnoj tački, sa jedinom razlikom što napadačev sistem mora raditi na različitom bežičnom kanalu.

4. Bežični klijent se automatski pokušava povezati sa originalnom bežičnom pristupnom tačkom, samo što će se ovog puta najverovatnije spojiti na napadačev sistem umesto na legitimnu pristupnu tačku.

5. Napadač se povezuje na originalnu bežičnu pristupnu tačku, tako da sada celokupan saobraćaj između bežičnog klijenta i pristupne tačke ide preko napadačevog sistema.

Jedan od alata za ostvarivanje ovakve vrste napada je AirJack (http://sourceforge.net/projects/airjack). Pokreće se na Linux platformi izvršavanjem komande *./monkey_jack.* Tako, na primer, ako napadač želi da ubaci svoj sistem između bežičnog klijenta sa MAC adresom *00:0C:AA:BB:CC:DD* i bežične pristupne tačke *00:0C:11:22:33:44* sa SSID-ijem *„Wireless"* zadaće sledeću komandu:

./monkey_jack –b 00:0C:AA:BB:CC:DD –v 00:0C:11:22:33:44 –C 6 –c 1 –I eth0 –e „Wireless" (1)

pri čemu menja bežični kanal sa 6 na 1.

Napad trovanja ARP-a

Napadi trovanja ARP-a (ARP poisoning) takođe predstavljaju napade gde se napadač umeće u sredinu komunikacije između legitimnih klijenata i bežične pristupne tačke. Napadači mogu iskoristiti protokol za razrešenje adresa (Address Resolution Protocol, ARP) ako je pokrenut na mreži. Cilj je da se napadačev sistem predstavi kao legitimni korisnik na mreži. Korišćenjem alata kao što su Dsniff ili Ettercap NG napadač može promeniti ARP tabele na bežičnoj pristupnoj tački i napadnutom klijentu. ARP tabele preslikavaju IP adrese na MAC adrese klijenata. To uzrokuje da napadnuti klijent šalje podatke ka napadaču umesto na pravu destinaciju. Tok napada:

1. Napadač truje ARP tabelu na napadnutom klijentu i na bežičnoj pristupnoj tački, koristeći pomenute alate.

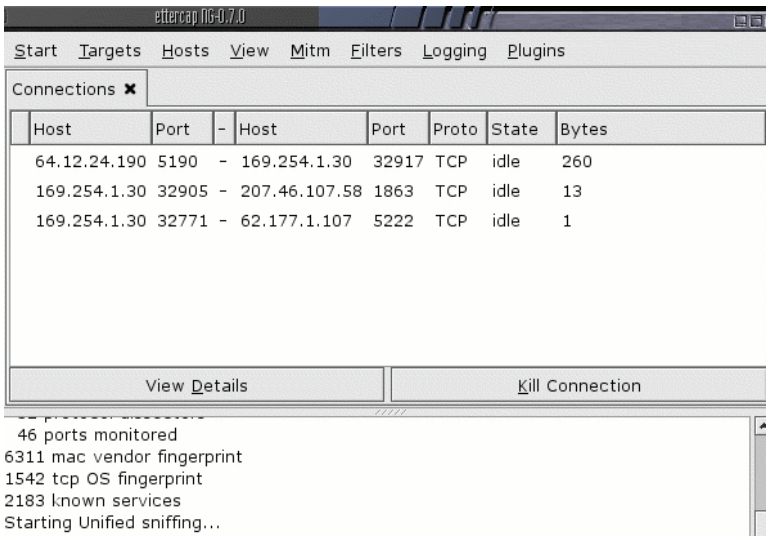
2. Napadnuti klijent asocira MAC adresu napadača sa IP adresom bežične pristupne tačke.

3. Bežična pristupna tačka asocira MAC adresu napadača sa IP adresom napadnutog klijenta.

4. Saobraćaj između napadnutog računara i bežične pristupne tačke šalje se na IP adresu napadača.

5. Napadač snima sav saobraćaj između, a ako je podešen da radi kao ruter šalje podatke na originalnu destinaciju tako da napadnuti klijent i bežična pristupna tačka ne primećuju nikakvu razliku, iako komuniciraju preko napadača.

Jedan od alata za ostvarivanje ARP napada je Ettercap NG (http://ettercap.sourceforge.net). Alat je besplatan i pokreće se na Windows ili Linux platformi (slika 15). Tok napada je automatizovan i svodi se na izbor mrežnog interfejsa na kojem će se ostvariti napad. Ettercap NG efikasan je za napade na bežične mreže zaštićene WEP sigurnosnim protokolom.



Slika 15 – Ettercap NG – Lista konekcija
Figure 15 – Ettercap NG – Connections

SNMP

Protokol za upravljanje mrežom (Simple Network Management Protocol, SNMP) koristi se za monitorisanje i upravljanje mrežnim uređajima na ožičenim i bežičnim mrežama. SNMP verzije 1 i 2 ne poseduje sigurnosne mehanizme prilikom upravljanja klijentima. Autentifikacija, šifrovanje i kontrola pristupa dodati su tek u SNMP verziji 3. Da bi napadač utvrdio da li je SNMP pokrenut na nekom mrežnom uređaju dovoljno je da utvrdi da li je na uređaju otvoren UDP port 161. Ukoliko jeste, napadač je u mogućnosti da dobije detaljne informacije o tom sistemu.

Napadi uskraćivanja servisa

Napad uskraćivanja servisa (Denial of Service, DoS) šalje gomilu zlonamernih mrežnih zahteva ili preklapa radio-talase na bežičnom sistemu sa bespotrebnim saobraćajem, sprečavajući adresiranje legitimnih zahteva. Napadi uskraćivanja servisa mogu imati za cilj uskraćivanje mrežnih usluga legitimnim korisnicima ili dalje probijanje unutar mreže.

Napad uskraćivanja servisa na koji su bežične mreže najosetljivije je ometanje radio-frekvencija. Bežični mrežni signali mogu biti poremećeni i zaglavljeni kada se pojavi drugi radio-signal koji radi u istom ili bliskom frekventnom opsegu. Normalni radio-frekventni opsezi kod IEEE 802.11 mreža su 2,4 GHz (za 802.11 b i g standarde), odnosno 5 GHz (za 802.11a standard). Noviji 802.11n standard može raditi na oba (2,4 GHz i na manje korišćenom 5 GHz) radio-frekventna opsega. Snažan radio- signal može omesti ili u potpunosti nadvladati postojeće radio-signale unutar bežične mreže.

Bežične mreže su osetljive na ometanje zbog niske snage rada i relativno uskih radio-kanala (22 MHz po kanalu) koji se koristite za komunikaciju. U zavisnosti od snage dolaznog ometajućeg signala, radio-frekventne smetnje mogu uzrokovati gubitak nekoliko paketa u prenosu ili stvoriti potpuni prekid komunikacije. Radio-frekventno ometanje može biti izazvano nenamerno sa radio-uređaja u okolini ili zlonamerno od strane napadača, čak i sa većih udaljenosti.

Radio-frekventno ometanje može prisiliti bežične klijente da tumaraju raspoloživim frekvencijama tražeći alternativnu bežičnu pristupnu tačku za komunikaciju. Pri tome, oni mogu pronaći i asocirati se na tuđu bežičnu mrežu ili, još gore, na zlonamernu bežičnu pristupnu tačku koju je postavio napadač.

IEEE 802.11 b, g i n bežični mrežni sistemi rade na nelicencnom delu spektra na 2,4 GHz koji je širom sveta namenski rezervisan za industrijske, naučne i medicinske potrebe. Za emitovanje na ovom delu spektra nije potrebna ekskluzivna licenca, pa na njemu, pored uređaja, za bežično umrežavanje funkcionišu brojni elektronski uređaji, kao što su bežični telefoni, bežične kamere za video-nadzor, bluetooth sistemi, teledirigovane igračke, mikrotalasne rerne, generatori radio signala i sl. Svi ovi uređaji mogu izazvati ometanje radio-signala unutar bežinih mreža. U najgorem slučaju njihovom upotrebom možemo izazvati napad uskraćivanja servisa.

Napad uskraćivanja servisa moguć je usled činjenice da bežične pristupne tačke mogu adresirati saobraćaj sve dok im se radna memorija ili procesori ne preopterete. Iako se donedavno smatralo da je novi sigurnosni protokol WPA2 otporan na napade uskraćivanja servisa, hakerska zajednica je objavila novootkrivene propuste u okviru ovog standarda koji im omogućuju efikasno izvođenje ovih napada na bežičnim mrežama zaštićenim bilo kojim sigurnosnim protkolom.

Asocijacioni i autentifikacioni napadi

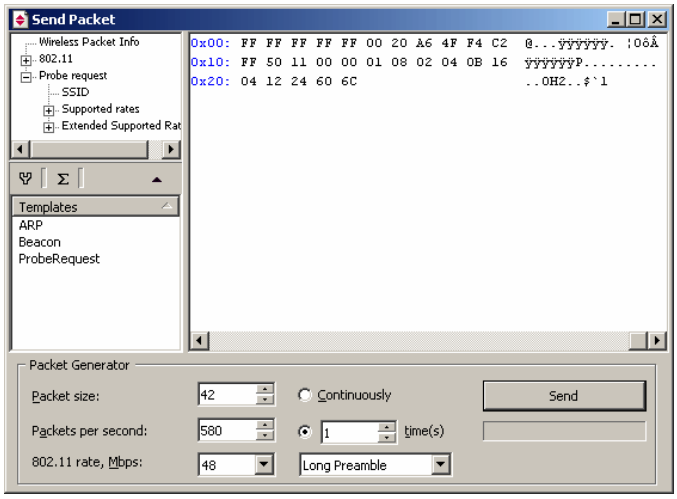
Napadači mogu iskoristiti slabost u načinu na koji bežične pristupne tačke obrađuju dolazne zahteve klijenata, počevši od tabele asocijacionih identifikatora klijenata (Association Identifier, AID). AID tabela je deo memorije na bežičnoj pristupnoj tački koja čuva podatke o povezivanju klijenata. Ona ima na raspolaganju ograničenu količinu memorije, pa može sačuvati samo ograničen broj bežičnih klijentskih konekcija. Nakon što se ova memorija napuni, bežične pristupne tačke više ne prihvataju dolazne zahteve, a moguće je i da potpuno otkažu. Ove vrste napada uskraćivanja servisa koriste jedan od dva metoda:

– asocijacionu poplavu (association flooding),
– autentifikacionu poplavu (authentication flooding).

Oba metoda napada su efikasnija ukoliko je bežična pristupna tačka otvorena za sve konekcije, od strane legitimnih i nelegitimnih klijenata.

CommView for WiFi Packet Generator Tool

Jedan od Windows alata za kreiranje asocijacionih i autentifikacionih napada je CommView for WiFi Packet Generator Tool (www.tamos.com/products/commwifi). CommView for WiFi je generator paketa koji omogućava ponavljanje bilo kog snimljenog paketa, uključujući asocijacione i autentifikacione zahteve, koje je napadač snimio pomoću mrežnog analizatora paketa. Nakon što je napadač snimio saobraćaj, dovoljno je da izabere jedan od paketa za asocijaciju ili autentifikaciju na bežičnu pristupnu tačku i izgeneriše ogroman broj istovetnih paketa (slika 16).



Slika 16 – CommView for WiFi Packet Generator Tool
Figure 16 – CommView for WiFi Packet Generator Tool

Disasocijacioni i deautentifikacioni napadi

Ova vrsta napada pogubnija je od asocijacionih i autentifikacionih napada, jer bežični klijenti za celokupan saobraćaj koji dolazi sa bežične pristupne tačke veruju da je validan. Ovi napadi mogu trajati tokom dužeg perioda, odnosno sve dok napadač ne prekine napad.

Disasocijacioni napad je situacija u kojoj bežična pristupna tačka govori klijentima da ne želi dalju komunikaciju sa njima. Slično može biti inicirano i od bežičnog klijenta ka bežičnoj pristupnoj tački. Prvo napadač pronalazi MAC adresu klijenta ili bežične pristupne tačke koji komuniciraju, i, koristeći jednu od otkrivenih validnih MAC adresa sa svog sistema, šalje disasocijacioni paket ka drugom sistemu. Nakon napada klijent se vraća u stanje u kojem je još uvek autentifikovan na bežičnu pristupnu tačku, ali nije povezan. To ga ostavlja isključenog sa mreže.

Deautentifikacioni napad je efikasniji, jer klijenta stavlja u stanje potpune isključenosti sa mreže. Kod deautentifikacionog napada bežična pristupna tačka govori klijentima da njihova konekcija više nije validna. Kao i kod disasocijacionog napada, deautentifikacioni napad može biti iniciran sa klijentske strane. Napadač prvo snima saobraćaj koristeći bežični mrežni analizator, pronalazi jedan od legitimnih deautentifikacionih paketa, i unosi ga u CommView for WiFi-a Packet Generator Tool. Zatim modifikuje snimljeni paket i menja mu izvorišnu i odredišnu adresu, koja može biti opšta adresa za celokupni mrežni opseg, i pokreće generator paketa. Ova vrsta napada izvodljiva je na bežičnim mrežama zaštićenim WEP ili WPA sigurnosnim protokolom sa tajnim ključem.

Zaključak

U ovom radu analizirani su i obrađeni savremeni metodi napada na IEEE 802.11 bežične mreže. Prikazani su najvažniji alati za napad i način njihovog efikasnog korišćenja za prodiranje u bežične mreže i otkrivanje korisnih informacija.

Metode zaštite podataka pri bežičnom prenosu znatno su napredovale od prvobitne WEP specifikacije. Šifrovanje podataka znatno je jače, a provera integriteta izvodi se kriptografskim algoritmima. Takođe, porasla je procesorska moć mrežne opreme, kao i kompatibilnost među uređajima različitih proizvođača. Korisnici su svesniji o neophodnosti implementacije sigurnosnih mehanizama za zaštitu bežičnih mreža. Algoritmi za generisanje ključeva više nisu statički i predvidljivi. Zahvaljujući snažnom AES šifarskom algoritmu, WPA2 trenutno predstavlja sasvim solidno rešenje za kriptografsku zaštitu podataka u IEEE 802.11 bežičnim mrežama.

Uprkos napretku i dalje postoje slabosti u IEEE 802.11 bežičnim mrežama. Prenošenje podataka radio-talasima u prostoru osetljivo je na smetnje i

interferenciju. Bežični radio-spektar na 2,4 GHz dostupan je svima i svako u njemu može odašiljati signal. Napadi uskraćivanja servisa isuviše se lako izvode. Širenjem signala na neplanirana područja otvaraju se vrata napadačima koji snimanjem mrežnog saobraćaja dolaze do podataka sa mreže.

IEEE 802.11 bežične mreže predstavljaju rešenje za sve korisnike koji žele jednostavno, jeftino i mobilno umreženje na kojem će pokretati servise za koje mogu dozvoliti blagu nepouzdanost i povremenu nedostupnost. Korišćenje bežičnih mreža u okruženjima gde su sigurnost i dostupnost mreže imperativ ipak nije preporučljiva.

Literatura

Beaver, K., Davis, P., 2005, *Hacking wireless networks for dummies,* Wiley Publishing, Inc., Indianapolis, Indiana, USA,

Bobar, Z., 2009, *Zaštita računarskih mreža Ministarstva odbrane i Vojske Srbije primenom virtuelnog honeyneta*, Vojnotehnički glasnik/Military Technical Courier, Vol. 57, No. 3, pp.80–87.

Cache, J., Wright, J., Liu, V., 2010, *Hacking Exposed Wireless,* Second Edition, The McGraw-Hill Companies, New York, USA,

Earle, A., 2006, *Wireless Security Handbook,* Taylor & Francis Group, New York, USA,

Evseev, S.P., Dorohov, A.V., Korolj, O.G., 2011, *Mehanizmi zaštite informacija u kompjuterskim mrežama i sistemima*, Vojnotehnički glasnik/Military Technical Courier, Vol. 59, No. 4, pp.15–39,

Graves, K., 2010, *CEH: Certified Ethical Hacker Study Guide,* Wiley Publishing, Inc., Indianapolis, Indiana, USA,

Hurley, C., Rogers, R., Thornton, F., 2007, *WarDriving and Wireless Penetration Testing,* Syngress Publishing, Inc.,

Milovanović, I., 2009, *Master rad: Bežične MESH mreže,* Fakultet za informatiku i menadžment, Univerzitet Singidunum, Niš,

Tanenbaum, A., Wetherall, D., 2010, *Computer Networks*, 5th Edition, Prentice Hall, USA,

www.personalmag.rs/blog/ns-wardriving-mapa, posećeno: 25.05.2012.

ATTACKS ON IEEE WIRELESS NETWORKS

FIELD: Computer Sciences, Telecommunications
ARTICLE TYPE: Professional Paper

Summary:

Security of wireless computer networks was initially secured with the WEP security protocol, which relies on the RC4 encryption algorithm and the CRC algorithm to check the integrity. The basic problems of the

WEP are a short initialization vector, unsafe data integrity checking, using a common key, the lack of mechanisms for management and exchange of keys, the lack of protection from the endless insertion of the same package into the network, the lack of authentication of access points and the like. The consequences of these failures are easy attacks against the WEP network, namely their complete insecurity.

Therefore, the work began on the IEEE 802.11i protocol, which should radically improve the security of wireless networks. Since the development of a protocol lasted, the WPA standard was released to offset the security gap caused by the WEP. The WPA also relies on RC4 and CRC algorithms, but brings temporary keys and the MIC algorithm for data integrity. The 802.1X authentication was introduced and common keys are no longer needed, since it is possible to use an authentication server. The length of the initialization vector was increased and the vector is obtained based on the packet serial number, in order to prevent the insertion of the same packet into the network. The weakness of the WPA security mechanism is the use of a common key.

WPA2 (802.11i) later appeared. Unlike the WPA mechanism that worked on old devices with the replacement of software, WPA2 requires new network devices that can perform AES encryption. AES replaces the RC4 algorithm and delivers much greater security. Data integrity is protected by encryption.

Despite progress, there are still weaknesses in wireless networks. Attacks for denial of service are possible as well as spoofing package headers attacks. For now, it is not advisable to use wireless networks in environments where unreliability and unavailability are not tolerated.

Introduction

In the entire history of networking it has never been easier to penetrate the network. One of the biggest problems of today's wireless networks is the lack of effective systems for intrusion detection. Forgetting to cover gaps in wireless network security may result in intrusion into the network by an attacker.

Security in IEEE 802.11 wireless networks

Although the IEEE 802.11 protocol defines security standards, wireless networks are one of the weakest links in the chain of computer networks. The basic security requirements of each computer network are reliable user authentication, privacy protection and user authentication.

Security attacks on IEEE 802.11 wireless networks

Non-technical attacks include a variety of human weaknesses, such as lack of conscience, negligence or over-confidence towards the strangers. Network attacks include a number of techniques that enable attackers to penetrate into the wireless network, or at least to disable it. Apart from the security problems with the IEEE 802.11 protocol, there are vulnerabilities in operating systems and applications on wireless clients.

The methodology of attack

Before testing wireless network security vulnerabilities, it is important to define a formal testing methodology. The first step before the actual attack is footprinting. The second step is the creation of a network map that shows how the wireless system looks. For this purpose, hackers are using specific tools, such as Network Stumbler, Nmap and Fping. When basic information about the wireless network is gathered, more information can be found out through the process of system scanning (enumeration).

Attacks on IEEE 802.11 wireless networks

Social engineering is a technique by which attackers exploit the natural trust of most people.

Radio waves do not respect defined boundaries. If radio waves are broadcasted outside of the boundaries of the defined area, then it is necessary to reduce signal strength on wireless access points. In that way, radio waves travel over shorter distances. Antennas are an integral part of wireless networks. A selected antenna type affects performance, network availability and safety of wireless networks.

Finding default values

CommView for WiFi is a tool for monitoring data flow (sniffer) especially written for wireless networks.

Cain & Abel is a universal tool for the detection of all types of passwords.

If a wireless network uses a protective mechanism of MAC address filtering, then the attacker must collect the IP addresses. To connect to a wireless access point, it is necessary to know its SSID. Contrary to what some people think, SSID is not a password.

Wardriving

Driving a car with a portable computer aimed at the detection of wireless computer networks, onto which connection is later possible, is called wardriving. For wardriving, it is necessary to have an appropriate software tool and a wireless network card or an adapter, on which an external antenna can be added to increase signal strength. It is also possible to use a global positioning device (GPS) to determine the coordinates of the detected wireless access points on a map. The most widely used software tools for wardriving are Network Stumbler, Kismet and MiniStumbler.

Network attacks

Hackers' most usual attack to circumvent the basic access control in wireless networks is masking their own MAC address with an MAC address of a legitimate client on the network (MAC address spoofing).

Man-in-the-Middle attack inserts the attacker's system in the middle between wireless clients and the wireless access point. Legitimate wireless users will be fooled when they try to connect, by being associated to the attacker's system instead of the legitimate wireless access point.

The ARP table poisoning attack inserts the attacker's system in the middle of communication between legitimate clients and the wireless access point. Attackers could use the address resolution protocol if it is running on the network. The aim of this attack is to introduce an attacker as a legitimate user on the network.

The Simple Network Management Protocol (SNMP) is used to monitor and manage network devices. SNMP versions 1 and 2 do not possess security mechanisms when managing clients.

Denial of service attack sends a bunch of malicious network requests which overlap radio waves on a wireless network system with unnecessary traffic, preventing addressing of the legitimate demands. Denial of service attack may be aimed to deny legitimate network services and to allow an attacker further penetration into the network.

Conclusion

In this paper, modern methods of attacks on IEEE 802.11 wireless networks are analyzed and processed. The most important tools for the attacks are presented as well as their effective usage for intrusion into wireless networks and discovery of useful information. The usage of wireless computer networks in environments where security and network availability are imperative is not recommended.

Key words: *WLAN, IEEE 802.11, wireless networks, attacks.*

Datum prijema članka/Paper received on: 22. 07. 2012.

Datum dostavljanja ispravki rukopisa/Manuscript corrections submitted on: 03. 08. 2012.

Datum konačnog prihvatanja članka za objavljivanje/ Paper accepted for publishing on: 05. 08. 2012.