Tallinna Ülikool
Informaatika Instituut

Wifi turvalisus

Seminaritöö

Autor: Ethel Maarits
Juhendaja: Erika Matsak

Tallinn 2011

Sisukord

Sissejuhatus

Järjest rohkem soovivad inimesed mugavust ja lihtsust arvutite kasutamisel. Sülearvuti seda ka pakub. Selle saab lihtsalt kaasa võtta ning kasutada seal, kus vaja. Kuna internet on saanud arvutikasutuse lahutamatuks osaks, siis on tekkinud ka suurem vajadus kaablivaba võrgu järele, mis lubab kodus või tööl vabamalt ringi liikuda. Seetõttu võibki täna paljudest kodudest leida Wi-Fi ruuteri.

Interneti olemasolu igal pool, nii kodudes kui ka avalikes kohtades, on suuremale osale Eesti elanikest saanud loomulikuks igapäevaseks nähtuseks. Selline laialdane Wi-Fi levik on tore, kuid võib tekitada probleeme kõigile, kes seda kasutada soovivad. Selleks, et tänapäeval kodus turvaliselt Wi-Fit kasutada, on vaja teada põhitõdesid traadita arvutivõrgu turvalisuse kohta ning tuleb neid ka rakendada. Tuleb arvestada ohuga, et keegi võib kasutada kaitsmata võrku enda huvides kahjulikel eesmärkidel.

Autori seminaritöö on suunatud arvuti tavakasutajale. Töö autor kajastab töös Wi-Fi olemust ja uurib, kuidas seda turvalisemaks saab muuta. Samuti autor annab ülevaate, milline Wi-Fi krüpteering on kõige turvalisem, milline on aegunud ning milline on kõige lihtsamini lahtimurtav. Autor kajastab oma töös populaarsemaid Wi-Fi jälgimis- ning sissemurdmisrakendusi. Ning katsetab, kuidas ühe sissemurdmisrakendusega Wi-Fi võrku sisse murda saab.

Autor kasutab oma töös teemakohast informatsiooni kogumist ja analüüsi vastavalt püstitatud teema vajadustele. Kogutud materjali ning informatsiooni põhjal jagab autor soovitusi, kuidas kodust Wi-Fi võrku turvalisemaks muuta.

1. Wi-Fi ajalugu

Wi-Fi tehnoloogia tekkis tulenevalt 1985. aasta USA Riikliku Sidekomisjoni otsusest, millega anti vabasse kasutusse raadiote laineala skaalad. Uudse raadiospekteri olemasolu kasutamiseks alustasid tehnoloogiafirmad traadita võrkude ja seadmete loomist. Selleks oli vaja ühist standardit, kuna vastasel juhul oleks liikumine killustunud, sest erinevate tootjate seadmed ei olnud üldiselt kooskõlas.

Tööstuse komitee juhid töötasid 1997.aastal välja ühtse standardi. Wireless Ethernet Compatibility Alliance (WECA) loodi 1999. aastal suuremate firmade poolt. Selle eesmärgiks on edendada uut standardit ning on mittetulunduslik organisatsioon. Uus tehnoloogia nimetati WECA poolt Wi-Fi-ks. Esialgselt ei tähendanudki Wi-Fi midagi, vaid see tekkis brandistrateegia tagajärjel sõnamänguna terminile *Hi-Fi*, et muuta oma teenus kergemini meeldejäävamaks.

Terminit *Wireless Fidelity* kasutati hiljem selleks, et selgitada, mida Wi-Fi tähendab. (WiFi, 2010)

Wi-Fi - Wireless Fidelity - traadita kohtvõrgu seadmete kasutamist propageeriva Wi-Fi Alliance'i kaubamärk. Wi-Fi sertifitseeritud logo seadmel tähendab, et seade vastab nõuetele ning on koostoimiv teiste Wi-Fi logo kandvate seadmetega.

1.1 Wi-Fi ajalugu Eestis

Wi-Fi tuli esimest korda Eestis kasutusele 2000. aasta algul. Siis pakuti juhtmevaba andmesideteenust avalikule sektorile, ettevõtetele ja ka eraisikutele. Juhtmevaba ühendust saab kasutada, kui on olemas vajalikud vastavad seadmed.

2001. aasta keskpaigas avati esimene avalik Wi-Fi leviala Eestis.

2002. aastal avati juhtmeta interneti kodulehekülg wifi.ee. Lehekülg loodi entusiastide poolt ning nende eesmärgiks oli muuta internet vabavaraks. Järgmiseks aastaks oli avalikke Wi-Fi levialade hulk suurenenud seitsmele.

2002. aastal paigaldati Viljandisse esimene traadita interneti liiklusmärk. Projekti eestvedaja mainis, et liiklusmärk ja traadita internet sobivad omavahel kokku, kuna liikuv inimene kasutab traadita võrku.

2002 aastat peetakse traadita interneti alal läbimurdeaastaks Eestis. (Roonemaa, 2002)

2002. aastal avaldas Kalifornia ajakirjanik artikli Eestist, kui Wi-Fi rakendajast Euroopas. Artiklis oli kahjuks sees ka eksimus, Tallinna Lennujaam nimetati bensiinijaamaks. (Biddlecombe, 2002)

Järk-järgult, aasta-aastalt avatakse järjest rohkem avalikke Wi-Fi võrke, nii koolides kui ka bensiinijaamades.

2004. aastal otsustas Tallinna kesklinna valitsus, et tuleb korda teha 6 parki, kuhu luuakse tasuta internetiühendus ja välikohvikud. Wifi.ee portaali toimetaja Veljo Haameri sõnul võiks olla Eestil pargid, kus saaks kuritegevust kartmata internetis surfata. Tema sõnul muudaks see linna nii linnakodanikele kui ka turistidele. Idee tekkis juba aasta varem, aga teostuseni jõuti 2004. aastal. Turvalisuse küsimus jäi välikohvikute omanike lahendada. (Alas, 2004)

2005. aastal Viljandi Folgi raames leidis aset riigi esimene avalik WarDriving ehk traadita interneti orienteerumine. Varasemalt on Wi-Fi orienteerumist korraldatud ainult arvutihuviliste ringis. Ürituse eesmärgiks oli interneti propageerimine. Osalejatele anti raja igas kontrollpunktis ülesanne lahendada. (Ilves, 2005)

2006. aastal saab kolmes elektrirongis kasutada Wi-Fi´t. Traadita internetiühendusega varustatud vagunid on tavaliselt rongikoosseisu 3 esimest. Täpselt ei osata öelda, millistel marsruutidel WiFit kasutada saab, kuna rongid vahetavad marsruute pidevalt. Reisijatele on Wi-Fi kasutamine tasuta. (Pinn, 2006)

2007. aastast alates saab traadita internetiühendust kasutada Pelgulinna sünnitusmajas, olles Euroopa esimene WiFi levialaga sünnitusmaja. (Kuus, 2008)

2007. aastal rajati parvlaevale St.Ola traadita internetiühendus, mida reisijad saavad sõidu ajal kasutada. Arvati, et internetiühendus aitab reisijatel sõiduks kuluvat aega paremini ära kasutada. (Hiiu Maavalitsus, 2007)

2. Wi-Fi turvalisus ja seadistamine

Ruuterit koju osta saavad ja oskavad kõik, ent seda peab ka korralikult seadistama. Paljud inimesed kasutavad Wi-Fi ruuterit vaikeseadetega.

Traadita side seadmed kasutavad kindlat sagedusala. Vabasid sagedusi on aga piiratud arv. Tavapärases Tallinna paneelmajas võib igal korrusel olla 3-4 Wi-Fi võrku, büroohoonete piirkonnas võib see arv aga olla 15-30.

IEEE 802.11b/g Wi-Fi võrguseadmed suhtlevad kõik kitsal, 2,4 GHz sagedusalal. 802.11b/g seadmete juures saab määrata, millist kanalit nad kasutavad. Kanalid on 1-13ni (USA turu seadmetes on kanaleid kuni 11). Eri kanalite sageduskeskme vahe on 5 MHz. Wi-Fi seadmed, mis töötavad kõrvalkanalitel, segavad üksteise tööd. Üldlevinud arvamus on, et kanaleid, mis üksteist ei sega, on kokku kolm. Näiteks 1., 6. ja 11 (vt.tabel 2). Praktikas võib neid olla aga vähemgi. Enamike arvutikasutajate jaoks kõige märgatavamad häired Interneti töös on internetiühenduse kiiruse langemine, võrgu kadumine, katkestused. (Urbas, 2005)

IEEE 802.11n on traadita võrgu standard, mis peaks tõstma 802.11a ja 802.11g andmekiiruse alates 54 Mbit/s kuni 600 Mbit/s. See standard ratifitseeriti 2009. aasta septembris ning avalikustati sama aasta oktoobris. 802.11n on võimeline suhtlema ka 5GHz sagedusalal, mis omakorda laiendab kasutatavate kanalite arvu.

Eestis kolm kõige populaarsemat võrguseadmete firmat on Thomson Telecom Belgium, Linksys ja Buffalo Inc (vt.tabel 4). Nende seadmete puhul on tegemist Elioni poolt pakutavate modem-Wi-Fi-ruuter seadmetega.

Aastaid tagasi osteti kõige rohkem Linksys´i seadmeid. Paljudel on senimaani kodus Linksys´i seadmed kasutusel. Kõik Linksys´i seadmed on tehases seadistatud, et nad vaikimisi kasutaksid 11. kanalit. See teeb kanalite probleemi veel hullemaks. Enamik seadmeomanikke ei arva, et on vajalik seadmel kanal ära vahetada, või siis ei oska seda teha. Seega töötavad nad vaikimisi seadetel. Väga suure tõenäosusega esineb vaikeseadeis seadmetel kanali hõivatuse probleeme sagedamini kui neil seadmetel, millel on kanal ära vahetatud. (Urbas, 2005)

Autoril endal on kodus ka Linksys´i ruuter, mis oli vaikimisi seadistatud 11 kanalile. Kuid kuna lähiringkonnas ei levi teisi traadita ühendusi, ei pidanud autor vajalikuks kanalit vahetada.

Wifikaardistajate andmebaasi kohaselt on 192230 (seisuga detsember 2010) Wi-Fi leviala üle Eesti. 97244 on krüptitud ja 50366 on krüptimata (vt. tabel 3). Krüpteerimata võrk ei tähenda alati, et tegemist oleks turvamata võrguga, need võrgud võivad olla kaitstud MAC-aadressi filtriga, staatilise IP-aadressi, parooli vm lahendusega.

Kindlasti peaks ära muutma SSID ehk võrgu nime. Väga paljud jätavad võrgu nime samaks, mis tehases määratud on (vt.tabel 1). Selle abil saab aga kräkker teada, millise seadmega on tegu ning kuidas sinna paremini sisse murda. Kindlasti ei tohiks ka SSID-nimega kasutada oma aadressi, sest see võib olla reklaamiks varastele, et sel aadressil asub arvuti. Samuti ei tohiks SSID-nimeks panna wpa või wep vms, sest see annab kräkkerile infot, mis krüpteeringuga tegu ning lihtsustab tema tööd kõvasti.

Soovituslik on ka piirata Wi-Fi ruuteri leviala ulatust, et leviraadius ei jõuaks tänavale. Soovitatav on paigutada ruuter kodu keskmesse, mitte akna või välisseina ligidusse, kust ta ka tänavale leviks. Võimalusel võib ka leviala vähendamiseks ruuteril antennid maha keerata.

Inimesed, kes elavad oma majas ning soovivad aeg-ajalt õues arvutiga töötada, ei peaks leviulatust vähendama, kuna siis ei pruugi ühenduse kvaliteedist neile endile piisata.

Soovituslik on aeg-ajalt jälgida oma internetiühendust. Kui veebilehed tulevad aeglaselt lahti ja ühendus on üldiselt aeglane, siis võib arvata, et keegi teine kasutab veel sama võrku. Samuti võib jälgida ruuterit, kui seal vilguvad tuled ajal, mil võrgu omanik ise võrku ei kasuta, siis on üsna tõenäoline, et keegi teine on võrku sisse pääsenud. (Kuus, 2007)

Iga kasutaja peab arvestama sellega, et on olemas kräkkerid. Pahatahtlikud arvutikasutajad, kes murravad võõrasse võrku sisse ning kuritarvitavad võõrast võrku ning andmeid (vt. lisad). Nende eest ei saa ennast kunagi lõplikult kaitsta.

Kindlasti peaks ära muutma SSID nime või vähemalt võtme Thompson ruuteritel. Thompson firma ruuterite puhul on võimalik tuletada võrgu võti lihtsalt allalaetava programmi abil. Programm teeb seda ruuteri mudelinime põhjal, mis vaikimisi seadete puhul on ka SSID nimeks. Seepärast ei tohiks jätta seadmeid vaikimisi seadetega. (Devine, 2008)

3. Wi-Fi krüpteering

Krüpteerides oma raadiovõrku hoiad eemal inimesed (kaasa arvatud naabrid), kes muidu kasutaks seda tasuta internetti pääsemiseks. On ka inimesi, kes meelega jätavad oma võrgu avalikuks. Kuid siis peab arvestama, et enda arvuti on korralikult kaitstud tulemüüri ning viirusetõrjega, sest võrgus olevates arvutites võivad peituda viirused. Krüpteerimine aitab aga takistada sissetungijaid, kes muidu kuulaksid võrguliiklust pealt ning vajalike oskustega tuvastaksid ka nt minu internetipanga paroolid.

Kolm valdavat standardit juhtmevaba krüpteeringu jaoks on järgnevad:

WEP on algupärane kaitse, mis seostati esimeste ruuteritega ning on ühtlasi ka kõige nõrgem. Vastavate vahendite olemasolul saab sissetungija WEP-krüpteeringuga (kaitstud) võrku sisse murda.Seda peetakse peaaegu vananenud tehnoloogiaks, seega on soovitatav kasutada WEP-krüpteeringut ainult siis, kui kasutad vanemat sülearvutit või omad seadmeid, mis ei võimalda uuemate krüpteeringute kasutamist. (bcarigtan, 2009)

Et andmeid krüpteerida kasutab WEP salajasi võtmeid. Nii tugijaam kui ka vastuvõtvad seadmed peavad teadma salajasi võtmeid. Kasutaja peab ära määrama WEP-i kasutamise ning valima võtmetugevuse 64 või 128 bitti. Seejärel tuleb valida võtmesõnad. Võti võib koosneda numbritest (0 .. 9) ja tähtedest (A .. F). 64-bitise võtmetugevusega tekib 10-märgiline võtmesõna. 128-bitilise võtmetugevusega tekib 26-märgiline võtmesõna. (Kuus, 2009)

Internetis on väga palju õpetusi, kuidas on võimalik WEP-krüpteeringuga wifiühendusse sisse murda.

WPA loodi, et parandada turvaaugud WEP-is. WPA on mugavam kui WEP, sest WPA-l sobivad võtmesõnaks kõik tähed ja numbrid. Kasutajal püsib parool paremini meeles, sest kasutaja saab ise valida endale meelepärase tähendusega sõna.

WPA2 – on WPA edasiarendus ning seda peetakse kõige tugevamaks mittekaubanduslikuks krüpteerimise kavaks 802.11x võrkude jaoks. WPA2 rakendab kohustuslikke 802.11i elemente. WPA2 on turvalisem, kui WPA, kuna kasutab AES põhist algoritmi.

On teada juhtumeid, kus mõnda veebilehte ei kuvata korralikult kui kasutaja kasutab AES krüpteeringut, seega peaks kasutama TKIP-i (vt.lisad) ning katsetama, kas see parandab probleemi. (bcarigtan, 2009)

WPA-PSK on wifi kodukasutajale kõige mugavam lahendus. Parool tuleb sisestada kaks korda (Windowsi operatsioonisüsteemi puhul) ning edaspidi pole vaja seda enam sisestada. (Kuus, 2008)

Kõige kindlam ja turvalisem on kasutada WPA2-te koos AES või TKIP krüpteeringuga.

4. Wi-Fi jälgimis- ning sissemurdmisrakendused

Võrguliikluse jälgimise rakendusi on palju. Autori arvates on väärt mainida kahte tarkvara, millest üks kujutab keskkonda erinevatest tarkvara rakendustest ja teine on üks enam levinumatest võrguanalüüsi tarkvaradest. Nende rakenduste kohta leidub internetis küllaldaselt juhendeid, mille abil suudavad võõrast võrku kuritarvitada ka nooremad arvutihuvilised.

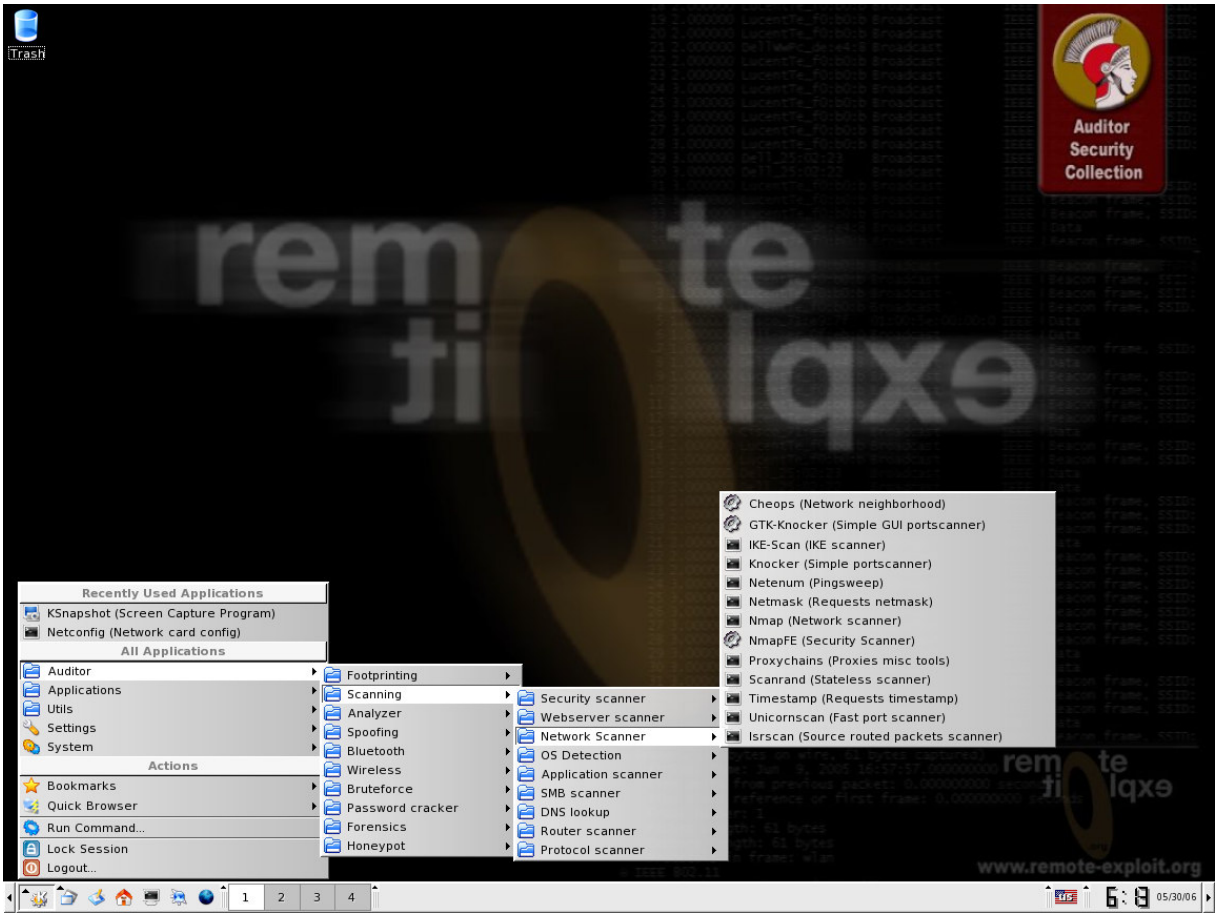
4.1 BackTrack

Backtrack on üks populaarsemaid süsteemide turvalisuse testimiseks mõeldud Linuxi distributsioone. BackTrack on mõeldud nii turvalisuse spetsialistidele kui ka algajatele. BackTracki näol on tegemist LiveCD-ga. See võimaldab kiiremini ükskõik millist arvutit testida, kuna ei pea installima lisaks eraldi programme.

BackTrack hõlmab endas üle 300 turvalisuse tööriista. Teda on nimetatud ka Šveitsi armeenoaks turvalisuse hindamisel.

BackTracki saab kasutada:

- informatsiooni kogumisel
- veebi aplikatsiooni analüüsimisel
- säilitamise testimisel
- digitaalses kriminalistikas
- kõne edastamiseks IP-võrkudes (vt. lisad)



Pilt 1 BackTracki keskkond

Samuti on BackTrack väga hea vahend noorele kräkkerile, kes tahab oma teadmisi naabri võrgu peal proovida.

4.2 Wireshark

Wireshark on avatud lähtekoodiga vaba tarkvara arvutivõrkude vigade otsimiseks, protokollide analüüsiks ja nende tundmaõppimiseks. Wireshark on maailma kõige populaarseim võrguliikluse analüüsimise vahend.

Wireshark kandis varasemalt nime Ethereal, mis avaldati 1998 aastal. 2006 aastal muudeti nimi aga Wireshark´iks, kuna Ethereal´i asutaja vahetas töökohta ning säilitas programmi autoriõigused. (Barr, 2006)

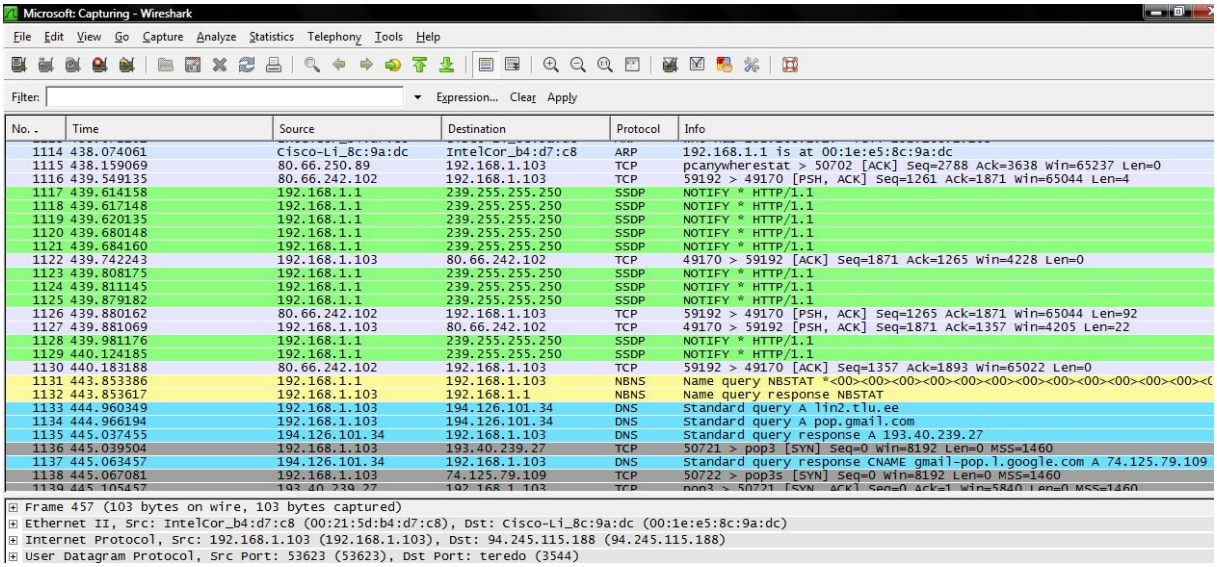
Näited Wiresharki kasutamisest:

- Võrgu administraatorid kasutavad seda võrguprobleemide lahendamiseks.
- Võrgu turvalisuse insenerid kasutavad seda, et uurida turvaprobleeme.

- Arendajad kasutavad seda protokolli töö silumiseks.
- Inimesed kasutavad seda, et õppida võrgu protokolli seespidiselt.
- Kräkker kasutab seda kasutajatunnuste ja paroolide väljasõelumiseks.

Wiresharki funktsioonid:

- Saadaval UNIX-i ja Windows´i jaoks.
- Püüab andmepakette otse võrguliidesest.
- Kuvab pakette väga üksikasjalike protokolli andmetega.
- Avab ja salvestab leitud pakettandmeid.
- Impordib ja ekspordib pakettandmeid.
- Filtreerib pakette mitmete kriteeriumite järgi.
- Otsib pakette mitmete kriteeriumite alusel.
- Kuvab erinevate värvidena pakettidel põhinevad filtrid.

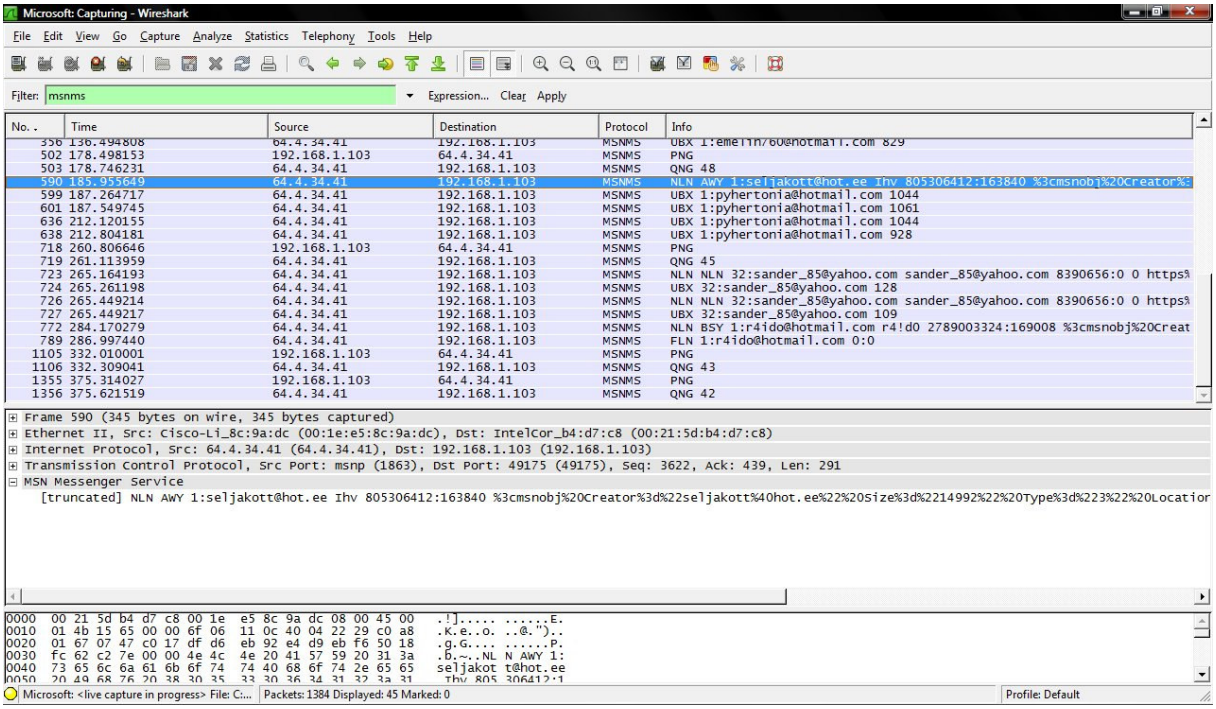


Pilt 2 Võrgupakettide väljund

- Genereerib erinevat statistikat.
- ... ning väga palju muud.

Tavakasutaja jaoks võib Wireshark esialgu väga keeruline olla, kuna ta kuvab väga palju erinevaid pakette ning infot on korraga palju. Kasutaja elu lihtsustamiseks ongi välja mõeldud filtreerimine. Kasutaja saab filtreerida endale huvipakkuvaid pakette vastavalt vajadusele.

Näiteks, kui kasutaja soovib vaadata milline liiklus üle msn´i protokolli käib, peab ta filtri lahtrisse sisse trükkima ’msnms’ ning infot saab vaadata MSN Messenger Service´i alt. Nii pääseb kräkker ligi ka kasutaja privaatsetele vestlustele.



Pilt 3 Võrgupaketid filtreeritud msnms järgi

Wiresharkil on väga põhjalik kasutusjuhend, mida lugedes saab ennast täpsemalt programmi võimalustega kurssi viia.

Mõlemad rakendused on mõeldud pigem ekspertide jaoks, kes päevast päeva tegelevad võrkude ja liikluse jälgimisega. Kuid tänu laiale valikule juhenditele on ka tavakasutajal võimalik nendega nii mõndagi ette võtta. On vaja ainult tahtmist ja järjekindlust.

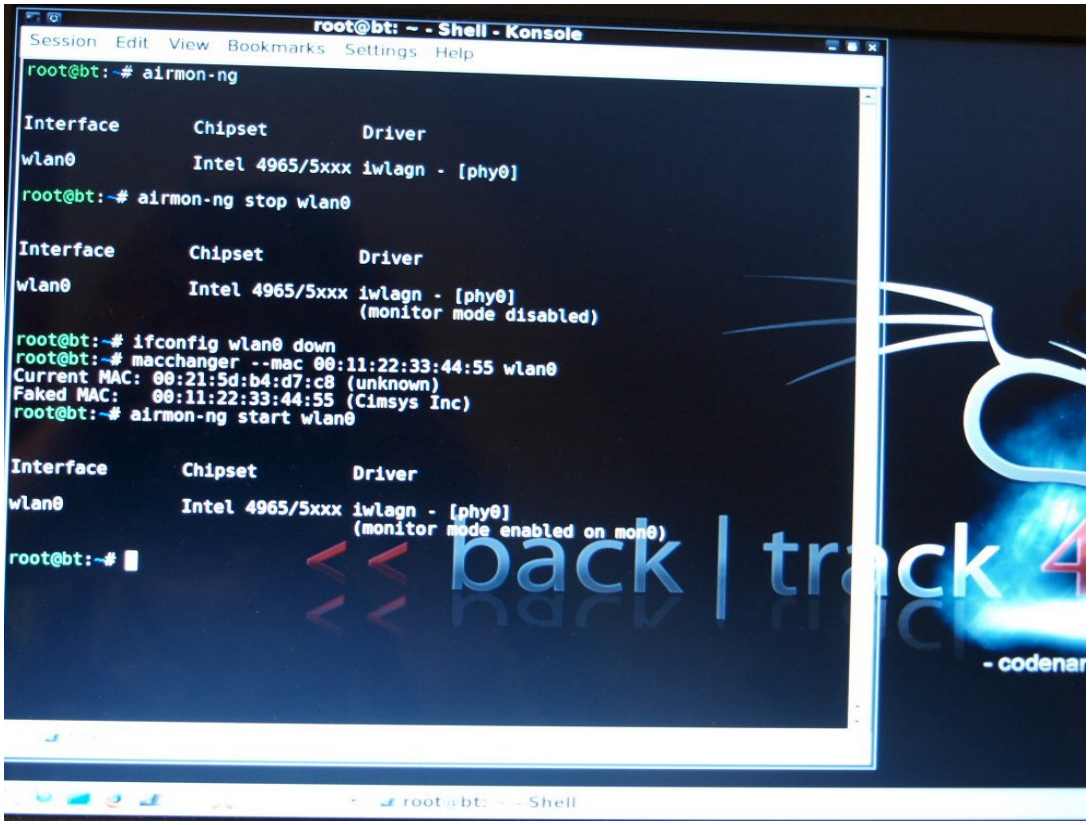
5. Wep võtme murdmine BackTrack´iga.

Autor proovis oma koduses wifi võrgus BackTrackiga murda Wep võtmega turvatud võrku. Kasutasin selleks Linksys WRT54GC ruuterit ning sülearvutiks Lenovo SL400´t, milles BackTrack töötas. Uurides internetist erinevaid õpetusi BackTracki kohta, leidsin paar huvitavat videot, mille abil sain mõningase proovimise järel hakkama wep võtme murdmisega. (Video, 2008).

BackTracki sai väga lihtsalt tasuta internetist alla laadida. Tõmmatud .iso fail tuleb kirjutada plaadi peale ning arvuti selle pealt üles buutida. BackTrack avaneb tekstirežiimis, kuid sisestades käsk 'startx', avaneb graafiline keskkond. Edasised käsklused tuleb sisestada tekstirežiimis konsoolis (Shell Konsole).

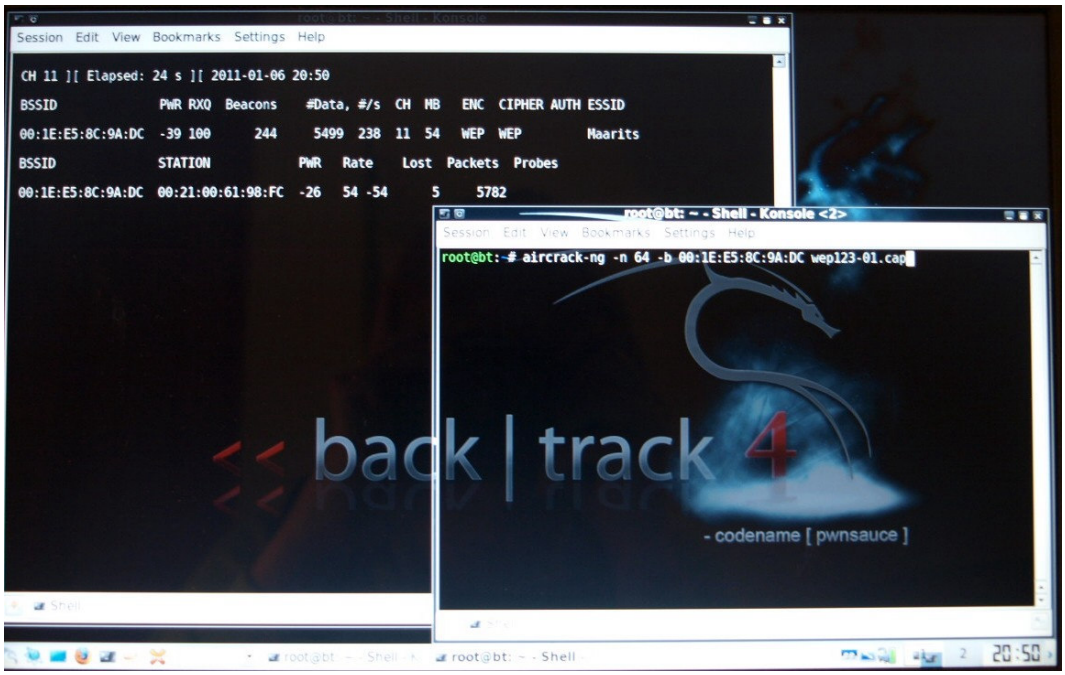
Käsklused on järgnevad:

1. airmon-ng
2. airmon-ng stop wlan0
3. ifconfig wlan0 down
4. macchanger –mac 00:11:22:33:44:55 wlan0
5. airmon-ng start wlan0
6. airodump-ng wlan0 (kui sobilik võrk leitud, ctrl+c ning copy bssid)
7. airodump-ng –c kanal -1 failinimi(nt.wep123) - - bssid ... wlan0

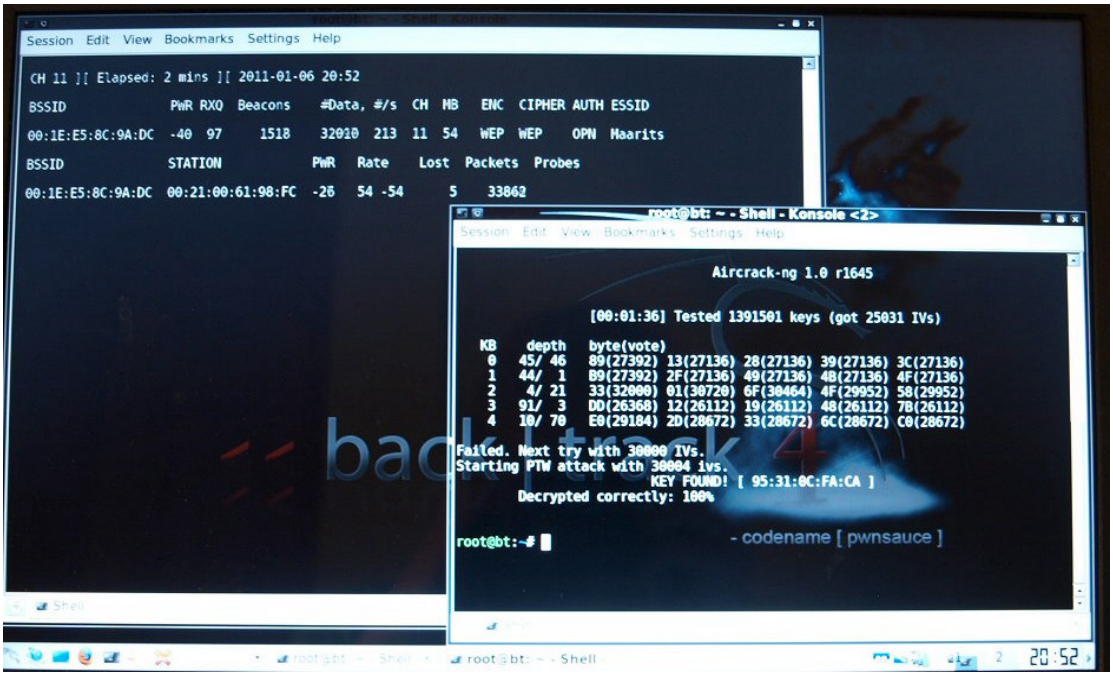


Uus konsooliaken lahti

8. aircrack-ng –n 64(128) –b (bssid) wep123-01.cap (failinimi-01.cap)



Võtme leidmise kiirus sõltub mitmest asjaolust. Kiireks leidmiseks peab wifi võrgus olema pidev liiklus. St kas mingi programmi tõmbamine, pidev interneti lehitsemine, filmifaili tõmbamine vms.



Võrgu võtmed 64-bitise ühenduse puhul mõtlesin ise välja. 128-bitise ühenduse puhul kasutasin enamalt jaolt veebis leiduvat krüptovõtme kalkulaatorit. (Vt.kasutatud kirjandus)

Tulemused on järgmised:

Tulemused

Nr.	Krüpteerimismeetod	Võtme pikkus	Võrgu võti	Aega kulus	Pakette kogutud
1	WEP	64-bit	1234567890	0:01	5474
2	WEP	64-bit	a1b2c3d4e5	0:58	15 021
3	WEP	64-bit	aa58be76cd	1:00	15 003
4	WEP	64-bit	a5b80f41c7	0:53	15 038
5	WEP	64-bit	bcdfe25806	0:55	15 021
6	WEP	64-bit	aa11bb22cc	0:18	10 012
7	WEP	64-bit	95310cfaca	1:36	25 031
8	WEP	64-bit	5c8a6d9f3e	1:16	21 023
9	WEP	64-bit	439baf8146	1:14	15 001
10	WEP	64-bit	f6a1d4b9c7	2:54	26 130
11	WEP	128-bit	34ab67cd89aa00ee123456abcd	17:59	150 893
12	WEP	128-bit	aa11bb22cc33dd44ee55ff66aa	56:33	245 839
13	WEP	128-bit	44495b276642553f5f4f2a7520	2:53:13	585 333
14	WEP	128-bit	22523053587446537220265f70	3:05:43	300 402
15	WEP	128-bit	00000aaaaa111bbb222ccc3333	2:10:20	130 126
16	WEP	128-bit	12345678901234567890123456	20:34	121 091
17	WEP	128-bit	1a2b3c4d5e6f7a8b9c0d1e2f3a	06:44	40 002
18	WEP	128-bit	9a5b80f4150ab5583cd30aa09a	01:08:33	698 610
19	WEP	128-bit	567e20e45e9087456891254865	2:50:10	574 235
20	WEP	128-bit	297b3b70334d61773e2e635b7a693927	2:59:35	481 698

Kõige kiirema tulemuse andis 64-bitine võti, mille BackTrack leidis 0:01 sekundiga. 64-bitistest võtmetest kõige aeglasem tulemus oli 2 minutit ja 54 sekundit.
128-bitistest võtmetest kõige kiirem aeg oli 6 minutit ja 44 sekundit. Ning kõige aeglasem oli 3 tundi, 5 minutit ja 43 sekundit.

Nende katsete puhul võib väita, et võrk, mis on turvatud WEP 64-bitise ühendusega, on väga ebaturvaline ning lihtsasti sissemurtav. Paar minutit oodata pole mingi vaev, kui soovitakse kasutada tasuta teise interneti ühendust.

Küll aga on asjalood teised 128-bitise ühenduse puhul. Lihtsama keerukusega 128-bitise võtme leidis BackTrack 6 kuni 20 minutiga. Seegi pole eriti pikk aeg. Raskema keerukusega võtme leidis BackTrack aga 2 kuni 3 tunniga. Selline aeg võib olla mõnele püsimatule kräkkerile liiga pikk ning loobub katsest võrku sisse saada. Kuid selle peale ei tasu lootma jääda.

6 . WPA/WPA2 krüpteeringu murdmine

WPA ning WPA2 krüpteeringu murdmise õpetusi leiab internetist väga mitmed. Võtan vaatluse alla õpetuse, mis põhineb BackTracki programmil. WPA2 murdmine põhineb brute force attack´il ehk jõhkra jõuga ründel (vt. lisad). Ründeks on vajalik veebist leitav sõnaraamat. Sõnaraamat tuleb BackTrackile ette sööta ning programm hakkab sõnu võtmega võrdlema. See protsess on väga aeganõudev ja pikk. Kui võrgu parooli pole sõnaraamatus, st koosneb tähtede ja numbrite kombinatsioonidest, siis pole võimalik WPA2-ga turvatud võrgu parooli leida.

Õpetuse autor testis WPA2 leidmist, kuid pärast 20 tunnist otsimist loobus, kuna protsess oli liiga aeganõudev ning arvas, et autori eluea jooksul seda võtit ei leita. (Eeckhoutte, 2009)

7. BackTracki ründes kasutatavad mõisted

- BSSID – Basic Service Set Identifier – seadme MAC-aadress
- PWR – signaali tugevus võrgukaardi järgi. Ehk võrgukaardi/sülearvuti kaugus ruuterist.
- RXQ – vastuvõtu kvaliteet mõõdetuna pakettide protsendi põhjal.
- Beacons – tugijaama poolt välja saadetud pakettide hulk.
- #Data – kinnipüütud andmepakettide hulk.
- #/s – andmepakettide hulk sekundis (mõõdetuna viimase 10 sekundi jooksul).
- CH – kanali number.
- MB – tugijaama poolt toetatav maksimumkiirus.
- ENC – kasutuses olev krüpteerimisalgoritm.
- CIPHER – šiffer .
- AUTH – kasutatav autentimisprotokoll.
- ESSID – Extended Service Set Identifier – pääsupunkti nimi.
- Lost – viimase 10 sekundi jooksul kaduma läinud andmepakettide hulk.
- Packets – kliendi poolt saadetud andmepakettide hulk.
- Probes – klient uurib essid.
- (mõistete ning osaliselt ka käskluste allikas: http://riivo320.wordpress.com/2010/01/18/wep-ja-wpa-krpteeringu-murdmine/)

8. Kokkuvõte

Antud seminaritöö eesmärk oli tutvustada lihtsamaid turvaseadistusi, erinevaid krüpteeringuid ning uurida välja, milline hetkel levinud traadita internetiühenduse krüpteering on kõige parem ja turvalisem. Autor soovis kajastada oma töös populaarsemaid Wi-Fi jälgimis- ning sissemurdmisrakendusi.

Tehastest tulevad seadmed vaikimisi häälestusega, mis ei taga piisavat turvalisust. Seetõttu on oluline, et kasutaja oskaks tugijaamade vaikeseadistusi muuta. Soovituslik on muuta SSID võrgunimi, seadistada krüpteering ning muuta vaikimisi seatud krüpteeringuvõti.

WEP on kõige algupärasem ning tänapäeval kõige kiiremini lahtimurtav. Internetis on hulgaliselt õpetusi, kuidas WEP-krüpteeringuga kaitstud Wi-Fi-sse sisse murda. Soovituslik on kasutada WPA2-te, sest seda peetakse praegu kõige turvalisemaks.

Kuid siinkohal võib välja tuua võrdluse: kui uks on kinni ja lukustatud, siis suvaline möödajalutav narkomaan naljalt sisse ei astu. Kui aga tulla soovib K-komando, siis vajadusel see uks ka lõpuks murtakse.

Nii on ka kräkkerite ja tavakasutajatega. Kui kräkker tahab ligi pääseda, siis piisava tahtejõu ja ajakuluga tal see lõpuks tõenäoliselt ka õnnestub. Jääb loota selle peale, et häkkerid loovad uusi Wi-Fi krüpteeringuid, mis kaitsevad kräkkerite eest.

Lisad

1. Mõisted

Järgnevalt toon välja mõned mõisted, mis Wi-Fi-ga seonduvad ning mida Wi-Fi kasutaja teada võiks.

Inglisekeelne mõiste - inglisekeelse mõiste lühend - eestikeelne mõiste

- Access Point – AP - tugijaam
- Ad hoc network – ad hoc
- Brute force attack – jõhkra jõuga rünne
- Cracker – kräkker
- Hacker - häkker
- IEEE 802.11
- Media Access Control address – MAC-address – MAC-aadress
- Rogue Access Point – Rogue AP - võltstugijaam
- Service Set Identifier – SSID – mestiident ehk Wi-Fi võrgunimi
- Temporal Key Integrity Protocol – TKIP – ajutiste võtmete tervikluse protokoll
- Voice over IP – VoIP – IP kõne
- Wi-Fi Protected Access – WPA
- Wired Equivalent Privacy – WEP
- Wireless Fidelity – Wi-Fi – traadita internet
- Wireless Local Area Connection – WLAN – traadita kohtvõrk
- WIPS – Wireless intrusion prevention system – Traadita võrkudesse sissetungi vältimise süsteem

Ad hoc -Ad hoc võrgud sobivad kasutamiseks loodusõnnetuste jt. katastroofide piirkonnas, kus püsiva konfiguratsiooniga võrku ei saa kasutada. Wi-Fi (IEEE 802.11) võimaldab luua ad hoc võrke, kui lähikonnas pole ühtki tugijaama. Kui lähestikku satub mitu Wi-Fi võimelist seadet, siis saavad nad omavahel andmeid vahetada (st. iga seade saadab andmeid välja ja võtab vastu), kuid marsruutimine pole võimalik. Seega ei saa IEEE 802.11 ad hoc võrke tegelikult lugeda mobiilseteks, küll aga on olemas kõrgema taseme protokolle, mille abil saab IEEE 802.11 võrgud muuta mobiilseteks ad hoc võrkudeks.

Jõhkra jõuga rünne - Süstemaatiline ja ammendav kõikvõimalike meetodite äraproovimine turvasüsteemi lahtimuukimiseks. Näit. krüptoanalüüsis kasutatakse krüptogrammi lahtimuukimisel kõiki võtmeruumis leiduvaid võtmeid.

Häkker - Inimene, kes tunneb mõnu programmeeritava süsteemi "hingeelu" süvitsi tundmaõppimisest ja selle võimaluste avardamisest. Sellega erineb häkker ühelt poolt tavakasutajast, kes õpib ära ainult niipalju, kui hädapärast vajalik, ja teiselt poolt kräkkerist, kes kasutab oma teadmisi ja oskusi ebaausatel või lausa kuritegelikel eesmärkidel. Häkkeri tunneb ära eelkõige selle järgi, et tal on sisemine vajadus välja uurida, kuidas asjad töötavad ning see tegevus pakub talle emotsionaalset rahuldust.

IP-kõne - Meetod kõne edastamiseks IP-võrkudes. Oli algselt mõeldud erakõnede edastamiseks üle Interneti, kuid on nüüd kasutusel ka firmavõrkudes. VoIP võimaldab edastada kõnesignaali ja andmeid üle ühe ja sama võrgu infrastruktuuri.

Kräkker - Tehniliselt oskuslik, kuid kuritahtlik arvutientusiast, kes kasutab oma teadmisi ja vahendeid volitamatuks ligipääsuks kaitstud ressurssidele kahju tekitamise, info varastamise või lihtsalt eneseteostuse eesmärgil.

MAC-aadress, meediumipöörduse juhtimise aadress - kohtvõrgus (või mõnes muus võrgus) on MAC-aadress arvuti võrgukaardile tootja poolt omistatud unikaalne riistvaranumber. Etherneti kohtvõrgus on see identne ethernetiaadressiga. Kui arvuti on ühendatud Internetiga, paneb vastavustabel IP aadressi vastavusse arvuti füüsilise MAC-aadressiga kohtvõrgus.

Rogue AP - tugijaam, mille mõni firma töötaja on salaja ühendanud firma kohtvõrguga, et pakkuda võrguühendust kõrvalistele isikutele. Selleks pole vaja teha muud, kui ühendada Wi-Fi tugijaam Ethernet'i pistikupessa. Ilma asjakohaste turvameetmete rakendamiseta avatakse nõnda juurdepääs firma kohtvõrgule igaühele, kes juhtub mööda jalutama.

SSID - traadita võrgu (Wi-Fi võrgu) nimi, mida peavad kasutama kõik antud võrgus tegutsevad seadmed. SSID kujutab endast 32-baidist tõstutundlikku tekststringi, mis tavaliselt sisaldab seadme valmistanud firma nime (linksys, netgear jms) või on mõni lihtne

sõna nagu "wireless" või "default". Mestiident lisatakse kõigile antud võrgus liikuvatele andmepakettidele. Mestiidendi sünonüümiks on võrgunimi (Network Name).

Standard IEEE 802.11 - IEEE traadita kohtvõrgu tehnoloogia standardite perekond. Kasutaja saab kohtvõrguga ühendust pidada raadiokanali (traadita ühenduse) kaudu. 802.11 süsteemide andmekiirus sõltub kaugusest. Mida kaugemal on mobiilseade tugijaamast, seda väiksem on kiirus.

TKIP - ajutiste võtmete tervikluse protokoll - WPA andmeturbeprotokoll, mis kasutab räsialgoritmi võtmete šifreerimiseks ning mille terviklusekontrolli funktsioon võimaldab kindlaks teha, et keegi ei ole võtmeid näppinud. TKIP on üleminekuvariant, mis võeti kasutusele sellepärast, et WEP osutus ebapiisavalt turvaliseks ja see oli vaja kiiresti asendada millegi turvalisemaga juba olemasoleva infrastruktuuri peal. IEEE 802.11i standardiga defineeritud AES'i kasutuselevõtuks varem WEP'i kasutanud süsteemides on vaja teha muudatusi riistvaras ja see võtab aega.

Tugijaam - on seade, mis ühendab traadita WiFi seadmed ühtsesse traadita WiFi võrku. WIFI tugijaamad kasutavad enamasti kokkulepitud standardit IEEE 802.11 (a/b/g/n). Tavaliselt on tugijaam ühendatud traadiga LAN võrku ning ta suudab vahendada infot traadita ja traadiga võrgu vahel.

WEP -"traatsidele vastav privaatsus" - krüptograafiaprotokoll, mis on määratletud traadita kohtvõrgu standardites IEEE 802.11. WEP pakub side krüpteerimist 40- või 104-bitise jaosvõtmega. See võti ühendatakse 24-bitise algväärtustusvektoriga, nii et tulemuseks on 64- või 128-bitine võti. Protokollide teadaolevate nõrkuste tõttu tuleks turbe tugevdamiseks WEP võtmeid tihti vahetada. WEP-i järglane on WPA.

Wi-Fi on WLAN üks tehnoloogiatest, mis originaalselt baseerub IEEE 802.11 standardil. Wifi arendati esialgselt selleks, et ühendada erinevaid mobiilseid arvuteid ühtsesse võrku, kuid tänapäeval kasutatakse Wi-Fi tehnoloogiat juba paljudes teistes teenustes ja seadmetes, nagu näiteks VoIP telefonides, televiisorites, digitaalsetes kaamerates jms.

WLAN on selline kohtvõrk, kus ringiliikuv (mobiilne) kasutaja saab kohtvõrguga ühendust pidada raadiokanali (traadita ühenduse) kaudu. Enim levinud WLAN tüüpi ühendus on Wi-Fi.

WPA ja WPA2 - "kaitstud Wi-Fi " - turbe tugevdamise spetsifikatsioon traadita sidele konfidentsiaalsuse ja tervikluse pakkumiseks on andmeturbe protokoll IEEE 802.11 standardile. WPA arendus oli tingitud eelmise süsteemi WEP puudustest. WPA kasutab ajutise võtme teostuse protokolli TKIP (Temporal Key Integrity Protocol) ning AES algoritmi (WEP kasutas RC4 algoritmi).
WIPS - Traadita võrkudesse sissetungi vältimise süsteem - Wireless sissetungi vältimise süsteem on võrgu seade, mis jälgib raadiospektrit ning sissetungimise avastamise korral võtab automaatselt vastumeetmed kasutusele.

Mõisted võetud järgmistelt aadressidelt: http://viki.digitark.ee/index.php/WIFI ja www.vallaste.ee

2. Tabelid

Tabel 1. SSID nimede esinevuse TOP.

Koht	SSID-de arv	SSID
1	18045	Peidetud
2	7724	linksys
3	3063	default
4	1755	TRENDnet
5	1167	kodu
6	1004	buffalo
7	950	dlink
8	646	Elion
9	586	wifi
10	500	AxessMV400

(allikas: http://kaardistajad.wifi.ee/ssid.php)

Tabel 2. Wi-Fi seadmete kanalite esinevuse TOP.

Koht	AP-de arv	Kanali nr
1	50267	**1** (2.412GHz)
2	45734	**11** (2.462GHz)
3	45282	**6** (2.437GHz)
4	13493	**Tundmatu** (2.437GHz)
5	4953	**10** (2.457GHz)
6	4665	**7** (2.442GHz)
7	4059	**3** (2.422GHz)
8	3900	**2** (2.417GHz)
9	3832	**9** (2.452GHz)
10	3625	**5** (2.432GHz)

(allikas: http://kaardistajad.wifi.ee/kanalid.php)

Tabel 3. Kodeeritud ja mittekodeeritud võrkude esinevus.

Koht	AP-de arv	Kodeering
1	97244	WEP või WPA
2	50366	Ei

(allikas: http://kaardistajad.wifi.ee/kodeeritud.php)

Tabel 4. Wi-Fi AP-de valmistajate esinevuse TOP.

Koht	AP-de arv	% kõigist	Valmistaja (Kiip)
1	44792	23.30	Thomson Telecom Belgium
2	30253	15.73	Linksys
3	13547	7.047	Buffalo Inc
4	7076	3.681	Askey Computer Corp
5	6849	3.562	D-Link

(allikas: http://kaardistajad.wifi.ee/firmad.php)

3. WIPS

WIPS ehk Wireless sissetungi vältimise süsteem on võrguseade, mis jälgib raadiospektrit ning sissetungimise avastamise korral võtab automaatselt vastumeetmed kasutusele.

Sissetungimise avastamine

Wireless sissetungimise avastamise süsteem (Wireless intrusion detection system) jälgib raadiospektri olemasolu võltstugijaamade juures. Süsteem jälgib raadiospektri kasutusala traadita kohtvõrkude juures ning annab administraatorile kohe teada, kui võltstugijaam on avastatud. Pahatahtlikud seadmed võltsivad MAC-aadressi ning jätavad mulje, et ametlik võrguseade on nende oma.

Sissetungimise vältimine

Et saaks sissetungimist vältida, peab täpselt ära määratlema missuguse rünnakuga on tegemist. Järgmisi ohte suudab hea WIPS vältida:

- võltstugijaam
- halvasti seadistatud tugijaam
- kliendi valeühendus
- volitamata ühendus
- MAC-aadressi võltsimine
- Ad hoc võrk (vt.lisad)
- Teenustõkestamise rünne

(allikas: http://en.wikipedia.org/wiki/Wireless_intrusion_detection_system)

Rakendamine

WIPS-i konfigureerimine koosneb kolmest komponendist:

- Sensoritest – seadmed, mis koosnevad antennidest ja raadiotest, mis suudavad skäneerida raadiospektri pakette.
- Serverist – analüüsib pakette, mis sensorid on kinni püüdnud
- Konsoolist – haldab administratsiooni ja aruandlust

WIPS sensorid analüüsivad pakettide liiklust ning saadavad selle informatsiooni WIPS serverisse. Server liigitab info ohtlikuks või ohutuks. Seejärel informeeritakse serveri

administraatorit ohust. Saab ka määratleda, et WIPS võtaks ise ette automaatsed kaitsemeetmed.

WIPS-i on hea kasutada suuremate firmade puhul, kus on eraldi tööl võrgu administraator, kes saab rünnetega vajadusel tegeleda. Tavakasutajale on WIPS tehnoloogia kasutamine küllaltki kulukas.
(allikas: http://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system)

Kasutatud kirjandus

Alas, A (2004) Kesklinn saab kuus wifi-parki. Loetud Internetis 27.detsembril 2010 aadressil http://www.epl.ee/?artikkel=262935

Barr, J (2006) Ethereal changes name to Wireshark. Loetud Internetis 31.detsembril 2010 aadressil http://www.linux.com/archive/feature/54968

Bcarigtan (2009) Which WiFi encryption is best? Loetud Internetis 27.detsembril 2010 aadressil http://helpdeskgeek.com/networking/comparison-of-wifi-encryption-types/

Biddlecombe, E (2002) Estonians pump WiFi with petrol. Loetud Internetis 27.detsembril 2010 aadressil http://www.theinquirer.net/inquirer/news/1017215/estonians-pump-wifi-with-petrol

Devine, Kevin (2008) Hacking Thompson Speedtouch routers with default security settings. Crack wep/wpa keys within minutes. Loetud Internetis 07.jaanuaril 2011 aadressil http://www.kaisersblog.com/2008/07/hacking-thompson-speedtouch-routers-with-default-security-settings-crack-wepwpa-keys-within-minutes/

Eeckhoutte, Van Peter (2009) Cheatsheet: Cracking WPA2 PSK with BackTrack4, aircrack-ng and John the Ripper. Loetud Internetis 07.jaanuaril 2011 aadressil http://www.corelan.be:8800/index.php/2009/02/24/cheatsheet-cracking-wpa2-psk-with-backtrack-4-aircrack-ng-and-john-the-ripper/

Hiiu Maavalitsus (2007) Wifi ühendus parvlaeval St. Ola. Loetud Internetis 27.detsembril 2010 aadressil http://www.mv.hiiumaa.ee/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=43&cntnt01origid=65&cntnt01returnid=65

http://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system Loetud Internetis 28.detsembril 2010

Ilves, H (2005) Wifi orienteerujaid lõpetas seitse. Loetud Internetis 27.detsembril 2010 aadressil http://www.sakala.ajaleht.ee/030805/esileht/artiklid/5017147.php

Krüptovõtme kalkulaator. Wireless Encryption Key Calculator. Kasutatud Internetis 07.jaanuaril 2011 aadressil http://www.csgnetwork.com/wepgeneratorcalc.html

Kuus, J (2008) Mida saad sina ise oma wifi turvalisuse heaks teha. Loetud Internetis 28.detsembril 2010 aadressil http://kaardistajad.wifi.ee/turva.php

Kuus, J (2008) WiFi ajalugu Eestis. Loetud Internetis 27.detsembril 2010 aadressil http://wiki.wifi.ee/index.php?title=Wifi_ajalugu_Eestis

Kuus, J (2008) WPA. Loetud Internetis 28.detsembril 2010 aadressil http://wiki.wifi.ee/index.php?title=WPA

Kuus, J (2009) Wired Equivalent Privacy. Loetud Internetis 28.detsembril 2010 aadressil http://wiki.wifi.ee/index.php?title=WEP

Pinn, M (2006) Kolmes elektrirongis saab WiFit kasutada. Loetud Internetis 27.detsembril 2010 aadressil http://www.ap3.ee/?PublicationId=ed023d14-c8f2-4838-b5f6-278f7a784bf6

Roonemaa, H. (2002) Traadita internetti näitab liiklusmärk. Loetud Internetis 27.detsembril 2010 aadressil http://www.epl.ee/?artikkel=206743

Urbas, A (2005) Internet lekib. Loetud Internetis 26.detsembril 2010 aadressil http://arvutikasutaja.ee/artikkel.php?lk=1&id=207

Video (2008) Crack wep with backtrack3. Vaadatud Internetis 05.jaanuaril 2011 aadressil http://www.youtube.com/watch?v=oHq-cKoYcr8

Wifi (2010) Wireless networking technology. Loetud Internetis 27.detsembril 2010 aadressil http://www.britannica.com/EBchecked/topic/1473553/Wi-Fi