Jarno Kari

TIETOKONEEN TIETOTURVA

Opinnäytetyö
CENTRIA AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Huhtikuu 2014

Yksikkö Ylivieska	**Aika** Huhtikuu 2014	**Tekijä/tekijät** Jarno Kari
Koulutusohjelma Tietotekniikan koulutusohjelma		
Työn nimi Tietokoneen tietoturva.		
Työn ohjaaja Ritva Saviluoto		**Sivumäärä** 15 + 17
Työelämäohjaaja		

Opinnäytetyön aiheena oli tietokoneen tietoturva yleisesti ja siihen liittyen WLAN-salausta käsittelevän harjoituksen tekeminen ammattikorkeakoululle opetuskäyttöön.
Työlle oli tarvetta tietoturvan jatkuvasti kasvavan merkityksen takia. Opinnäytetyötä aloittaessa tutkittiin tietoturvaan liittyviä materiaaleja ja näiden pohjalta luotiin runko työlle. Seuraavaksi suunniteltiin harjoitustyö tekemällä WLAN-verkko koulun tiloihin jossa suoritettiin mittauksia ja näiden pohjalta luotiin harjoitukset.
Työtä varten hankittiin AirPcap Tx usb-tikku jolla WLAN-salaukseen liittyvät testaukset suoritettiin. Tämä opinnäytetyö on jaettu kahteen osaan. Ensimmäinen osa käsittelee tietokoneen tietoturvaa yleisesti ja toinen osa AirPcap Tx-harjoitusta, jossa tutkittiin WLAN-salausta. Liitteissä ovat harjoitustyö ja vastaukset annettuihin kysymyksiin.

Asiasanat
AirPcap Tx, tietoturva, WLAN-salaus

Unit	Date	Author/s
CENTRIA UNIVERSITY OF APPLIED SCIENCES Ylivieska	April 2014	Jarno Kari
Degree programme Information technology degree		
Name of thesis Computer information security		
Instructor Ritva Saviluoto		**Pages** 15 + 17
Supervisor		

The topic of this thesis was computer security in general and related to the wireless local area network encryption project that was made for the University of Applied Sciences for education purposes. As the importance of information security is increasing all the time, there was demand for the study. The thesis started with an investigation of information security-related materials which created the framework for the work. The next phase included planning the WLAN network at the school premises where the measurements that formed the basis of the exercises were made. The AirPcap Tx usb stick for testing the WLAN encryption was acquired to carry out the work. This thesis is divided into two parts. The first part discusses the computer security in general, and the second part focuses on the AirPcap Tx exercise that examined the WLAN encryption. The description of the created exercises and the key to the specific questions are annexed.

Key words
AirPcap Tx, information security, WLAN encryption

TIIVISTELMÄ
ABSTRACT
SISÄLLYS

1 JOHDANTO **1**

2 TIETOTURVA **2**
2.1 Mihin tietoturvaa tarvitaan **2**
2.2 Mitä tietoturva on **2**

3 TIETOKONEEN TIETOTURVAUHAT **4**
3.1 Haittaohjelmat **4**
3.1.1 Virukset **4**
3.1.2 Madot **4**
3.1.3 Troijan hevoset **5**
3.1.4 Vakoiluohjelmat **5**
3.1.5 Rootkit-ohjelma **5**
3.1.6 Kiristys-ohjelma **5**
3.2 Haittaohjelmien torjunta **7**
3.2.1 Viruksilta suojautuminen **7**
3.2.2 Virusohjelmat **7**
3.2.3 Palomuuri **8**
3.2.4 Salasanat **8**
3.2.5 Haittaohjelmien poistotyökalu **9**
3.2.6 Salaukset **9**
3.2.7 Langattoman lähiverkon salaukset **10**

4 AirPcap Tx HARJOITUS-TYÖ **12**

5 YHTEENVETO **14**

LÄHTEET **15**

1 JOHDANTO

Tietoturvallisuudesta on tullut tärkeämpi asia kuluttajille ja yrityksille internet-yhteyksien myötä. Moni käyttää tietokonettaan tajuamatta, miten ne toimivat. Tavallinen käyttäjä unohtaa usein, että suojaamaton tietokone on usein kuin avoin ovi haittaohjelmille ja tietomurtautujille. Yleensä käyttäjä huomaa vasta ongelmien ilmettyä kuinka tärkeää suojautuminen on.

Opinnäytetyön aiheeseen oli tarvetta tietoturvan jatkuvasti kasvavan merkityksen takia. Työhön kuului kaksi eri osa-aluetta.

Opinnäytetyön ensimmäisessä osassa käydään läpi mitä tietoturva on, tietoturvan uhat ja annetaan vinkkejä kuinka suojautua uhilta. Salasanat, salaukset ja langattoman lähiverkon asetuksia on myös tarjolla, jotka mielestäni tulee painaa mieleen hyvin. Pääasiallisena lähteenä työssä käytettiin erilaisia tietoturva sivustoja ja oppaita. Näistä tiedoista kirjoitettiin tiiviimmin tietoa lukijalle.

Toisessa osassa käsitellään tehty laboratorio-työ, siinä opiskelija pääsee testaamaan ja pohtimaan miten WLAN-salaus toimii ja auttaa tietoturvassa. Harjoituksessa päästään myös tutkimaan esimerkiksi koulun vapaassa käytössä olevaa WLAN-verkkoja ja kirjaamaan tuloksia ylös.
Liitteisiin on liitetty harjoitustyö ja vastaukset.

2 TIETOTURVA

Tietoturva tarkoittaa tietojen, palveluiden, järjestelmien sekä tietoliikenteen suojaamista erilaisilla toimilla. Tietoturva uhkina pidetään tiedon luvatonta käyttöä, tietokoneviruksia, piratismia, roskapostia, verkkoterrorismia ja uutena uhkana elektroninen sodankäynti.

2.1 Mihin tietoturvaa tarvitaan

Tietokonetta ja sen käyttäjää uhkaavat monet vaarat verkkoon kytkeytyessä. Suojaamaton tietokone on alttiina melkein kaikille tietoturvauhille, esimerkiksi verkkohyökkäys, virukset, madot ja kiristys-ohjelmat.

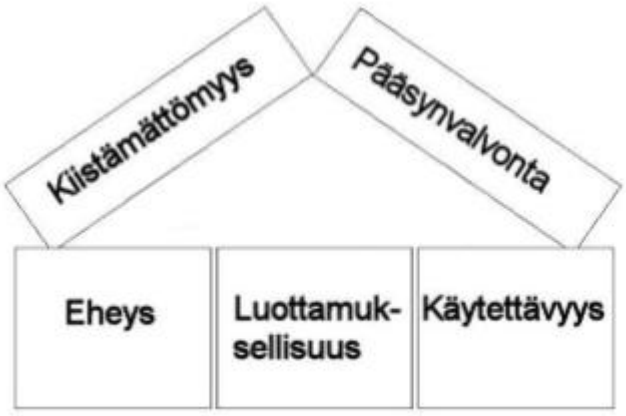
Tietoturvaa tarvitaan suojaamaan konetta mahdollisimman monelta riskiltä. Sitä myös tarvitaan varmistamaan järjestelmän suojeltavat tiedot, jotka ovat vain niiden käyttäjien käytössä, joille ne on ainoastaan tarkoitettu.

2.2 Mitä tietoturva on

Tietoturvaa on se, että koneen tietoihin ei pääse käsiksi sellaiset henkilöt, joilla ei niihin ole oikeuksia. Tietoturva ei ole vain dokumenttien ja viestien turvausta, vaan se on kokonaisuus, johon liittyvät tiedonkäsittelylaitteiden fyysinen turvallisuus että tiedonkäsittelijöiden osaaminen.

Internet avoimena järjestelmänä antaa mahdollisuuden hyökkäyksiin. Henkilöitä, jotka yrittävät saada arkaluontoista tietoa koneilta kutsutaan hakkereiksi.

Tietoturvallisuus voidaan yleensä selvittää viidellä eri tavalla. Näitä ovat kiistämättömyys, pääsyvalvonta, eheys, luottamuksellisuus ja käytettävyys.



KUVIO 1 Tietoturvallisuuden osa-alueet (Hakala, Vainio & Vuorinen 2006, 3-6)

Luottamuksellisuudessa tietoja käsittelevät vain ne, joilla on siihen oikeus. Tiedot ja laitteet pyritään suojaamaan salasanoilla, käyttäjätunnuksilla ja erilaisilla salakirjoitusmenetelmillä.

Pääsyvalvonnalla rajoitetaan käyttäjien pääsyä tietoihin. Luvattomat käytöt yleensä kuormittavat tietoliikenneverkkoja. Pääsyvalvontaan kuuluu myös käytön seuranta.

Kiistämättömyydessä järjestelmä tunnistaa ja tallentaa käyttäjien tietoja, joilla pyritään varmistamaan tiedon alkuperä. Tällä tavalla varmistetaan, ettei käsiteltyjä tietoja voi käsitellä tai muokata huomaamatta.

Eheys eli oikeellisuus (integrity) tarkoittaa, että tiedon käsittely taataan virheettömäksi ja tieto ei sisällä tahallisia tai tahattomia virheitä.

Käytettävyys tarkoittaa sitä, että oikeuksien haltijoilla on kaikki saatavilla helposti ja viiveettömästi.

Internetin tietoturva voidaan myös jakaa kahteen eri luokkaan. Nämä ovat tietojen suojaaminen ja palvelukoneen suojaaminen. (Tirronen H. 2003)

Tietoliikenteen suojaamisella estetään kahden tietokoneen välisen liikenteen kuunteleminen esimerkiksi pankkipalvelut ja sähköposti.

Palvelukoneen suojaamisella estetään ulkopuolisilta pääsy koneelle. Kone eristetään verkosta esimerkiksi palomuurilla. Käyttäjien tunnistamiseen tehdään salasanoja ja käyttötunnuksia.

3 TIETOKONEEN TIETOTURVAUHAT

3.1 Haittaohjelmat

Tietokoneelle asennetut ohjelmat auttavat käyttäjiä työtehtävissä, viihdekäytössä ja viestinnän parissa. Jotkin ohjelmat eivät ole turvallisia vaan voivat avata käytävän tunkeutujalle tiedostoihin. Haittaohjelmiin kuuluvat virukset, madot, Troijan hevoset, erilaiset vakoiluohjelmat ja kiristys-ohjelmat. Haittaohjelmat yleensä toimivat samalla tavalla kuin tavalliset ohjelmat, mutta niiden tarkoituksena on vahingoittaa tietokonetta ja sen käyttäjää erilaisilla toiminnoilla. Haittaohjelmat yleensä leviävät koneesta toiseen verkon kautta. Leviämistapoja ovat Internet, sähköposti tai tiedostot. Haittaohjelmat on tehty ja piilotettu yleensä niin, että käyttäjä ei edes huomaa niiden toimintaa. Langattomien Internet-yhteyksien lisääntyminen on vaikuttanut haittaongelmien lisääntymiseen ja nopeuden kehitys on vaikuttanut taas leviämisnopeuteen.

3.1.1 Virukset

Virus on haittaohjelma joka yleensä monistaa itseään ja levittää tietokoneesta toiseen itseään. Viruksen aiheuttama data-liikenne voi jopa tukkia verkon heikoimpia kohtia tai lukita järjestelmien Internet-sivuja. Yleisin syy viruksen päätymiseen tietokoneelle on sähköpostin liitetiedosto tai Internetissä ladattu tiedosto. Virus ei kykene itsenäiseen leviämiseen vaan se tarvitsee isäntätiedoston, jonka avulla se leviää ja aktivoituu. Osa viruksista tuhoaa tiedostoja ja osa voi muuttua roskapostin lähettäjäksi.
Microsoft Security Intelligencen mukaan viruksien määrä haittaohjelmista oli yli 57 prosenttia vuonna 2013 (Gaille, B. 2013).

3.1.2 Madot

Mato on samantapainen kuin virus, mutta se on suunniteltu leviämään tietokoneesta toiseen ilman isäntäohjelmaa tai käyttäjän toimenpiteitä. Mato käyttää leviämisessä hyväkseen Internetiä sekä erilaisia tietoturva-aukkoja. Leviäminen tapahtuu nopeammin kuin viruksilla, jotka käyttäjä huomaa siitä, että hänen verkkosiirtonopeus koneelta verkkoon on huomattavasti alhaisempi kuin verkosta koneelle. Verkkomadot saattavat kantaa mukanaan myös vaarallisia troijalaisia. Microsoft Security Intelligencen mukaan matojen määrä haittaohjelmista oli vain 2 prosenttia vuonna 2013 (Gaille, B. 2013).

3.1.3 Troijan hevoset

Troijan hevonen on ohjelma, joka on viattomaksi naamioitu haittaohjelma tai ohjelman pätkä, joka tekee jonkin hyödyllisen toiminnon, mutta samalla käynnistää viruksen, madon tai jotenkin muuten vahingoittaa tietokonetta avaamalla takaportteja järjestelmään. Näiden takaporttien kautta pyritään hankkimaan tietoa jättämättä jälkiä. Troijalainen ei pyri leviämään kuten mato hallitsemattomasti vaan se pyrkii asentumaan näkymättömästi. Troijan hevonen voi toimia itsenäisesti kuten virus ja se voi toimia kuin esimerkiksi kirjoitusohjelma, joka poistaa tietokoneesta tietoja, kun ohjelma on päällä. Microsoft Security Intelligencen mukaan troijalaisten määrä haittaohjelmista oli noin 7 prosenttia vuonna 2013 (Gaille, B. 2013).

3.1.4 Vakoiluohjelmat

Vakoiluohjelma eli spyware on haittaohjelma, joka kerää tietoa käyttäjän toimista ja lähettää ne Internetin kautta esimerkiksi hakkerille. Vakoiluohjelma voi esimerkiksi tallentaa kaikki näppäin painallukset, joiden kautta saadaan käyttäjätunnuksia eri ohjelmiin ja niiden kautta pyritään aiheuttamaan vahinkoa.

3.1.5 Rootkit-ohjelma

Rootkit on ohjelmisto, joka asentuu järjestelmään hyökkääjän saatua sen hallintaansa. Rootkitit pyrkivät asentumalla käyttöjärjestelmään tietoturva-aukon avulla, sekä tuhoamalla kaikki jäljet tartunnasta ja piilottamalla tietokoneella olevat vieraat prosessit tai verkkoyhteydet (Rootkit-ohjelma. www.dokumentti. http://fi.wikipedia.org/wiki/Haittaohjelma).

3.1.6 Kiristys-ohjelma

Kiristysohjelmasta esimerkkinä on Suomessa oleva poliisivirus, vuodesta 2012 alkaen levinnyt kiristysohjelma joka estää tietokoneen käytön poliisin nimissä väittäen tietokoneen sisältävän lapsipornografiaa, eläinpornoa ja lasten pahoinpitelyä esittäviä videoita lukiten koneen kaikki tiedostot. Avatakseen lukituksen käyttäjän pitäisi maksaa 100 euron sakko. Lokakuussa 2013 uutisoitiin, että haittaohjelmaa levittää usea samalla konseptilla toimiva rikollisryhmä. Suomessa uhreja noin 30 000 ja maailmanlaajuisesti viitisen miljoonaa. (Hakala, P. 2013. Helsingin sanomat 17.10.2013).

Tämän kiristysohjelman seurauksena perustettiin sivusto, joka tiedottaa ja avustaa rikoksen uhreja haittaohjelman poistossa. Sivusto sijaitsee osoitteessa www.ramsonware.fi

3.2 Haittaohjelmien torjunta

3.2.1 Viruksilta suojautuminen

Paras keino viruksiin on ennaltaehkäisy, että se saadaan tuhottua ennen, kuin se edes pääsee koneeseen aiheuttamaan vahinkoa. Kun virus pääsee varatoimista huolimatta koneelle, pitäisi vahingot minimoida mahdollisimman nopeasti.

Yleisesti tiedossa olevia tietokoneen käyttäjän muistilista ohjeita:

- Palomuuri on asennettu ja asetettu aktiiviseksi.
- Muista poistua verkkokaupasta tai muusta sivustosta asianmukaisesti sen omalla poistumistoiminnolla.
- Koneessa on virustorjuntaohjelma ja automaatti-päivitys aktiivisena.
- Tuntemattomia tai vähänkin epäilyttäviä tiedostoja/ohjelmia ei pidä asentaa tai käyttää. Älä klikkaa Ok-nappia, minkä tarkoitusta et tiedä.
- Varmuuskopioiden ottaminen talteen ennen kuin vahinko sattuu, suurin osa tietojen häviämisestä johtuu ihmisestä.
- Tuhoa tuntemattomat vieraskieliset sähköpostiviestit ja älä klikkaa näissä olevia linkkejä.
- Lähettäessäsi liitetiedostoja olisi hyvä ilmoittaa sen sisältö ja ohjelma, jolla se aukeaa.
- Päivitä käyttöjärjestelmä säännöllisesti.
- Salattu (tai suojattu) yhteys Internettiin.

3.2.2 Virusohjelmat

Virustorjuntaan on virustorjunta-ohjelmia, joilla voidaan etsiä ja poistaa viruksia sekä estää viruksen leviäminen muille tietokoneille verkossa. Näitä ohjelmia voidaan suorittaa paikallisesti ja etähallinnalla. Virustorjuntaohjelma poistaa sen tuntemat virukset automaattisesti parhaimmalla vaihtoehdolla.
Virustorjuntaohjelmissa on kaksi tilaa. Ohjelma joko tarkastaa tiedostot määrättynä aikana tai käyttää reaaliaikaista tarkastusta, jolloin jokainen Web-sivu ja toiminto tarkastetaan. Hyvä virusohjelma toimii tietokoneella jatkuvasti, mutta huomaamattomasti taustalla ja näkyy koneen käyttäjälle heti ongelmien ilmettyä.

Virusohjelmat ovat suurimmaksi osaksi siirtyneet ennalta ehkäisemään verkkopalveluissa haittaohjelmien leviämistä, esimerkkinä tästä sähköpostiliikenteen suodattimet. Joskus virus on torjuntaohjelmaa parempi ja ainoana vaihtoehtona on täydellinen tietokoneen alustaminen.

Viisi suosituinta ilmaista virustorjunta-ohjelmaa ovat, Avast Free Antivirus, Panda Cloud Antivirus Free, Zonealarm Free Antivirus + Firewall, Avira Free Antivirus ja Bitdefender Antivirus Free Edition.

Ja muutamia maksullia virustorjunta-ohjelmia ovat, F-Secure, Norton Antivirus, McAfee Antivirus ja Panda Internet Security.

F-Secure on Suomalaisen yrityksen valmistama ohjelma. Ohjelma sisältää virustorjunnan, palomuurin, roskapostin suodatuksen, lapsilukon ja vakoiluohjelmien tunnistajan. F-Securen tutkimuspäällikkö Mikko Hyppönen esiintyy usein uutisissa kun tietoturvauhista uutisoidaan.

3.2.3 Palomuuri

Palomuuri on tietokoneesi tietoturvan perusta. Sen tehtävänä on valvoa liikennettä ja pysäyttää ei-toivottu liikenne tietokoneellesi ja siltä ulospäin. Palomuuri toimii sille tehtyjen sääntöjen mukaan esimerkiksi niin, että vanhemmat voivat määrittää ettei k-18 tietokonepeli saa liikennöidä sisään ja ulos, vain vanhempien määräämät peliportit ovat auki. Useissa palomuureissa on lisäksi STOP-nappi, jolla voidaan katkaista kaikki liikenne ulos ja sisään. Tätä kutsutaan hätänapiksi, joka voi auttaa silloin, kun huomaat, että jotakin tietoturvareikää koneessasi hyödynnetään, esimerkiksi madon välityksellä.
Suosituimpia ilmaisia palomuuri-ohjelmia ovat, Hardrware firewalls, Comodo Firewall, ZoneAlarm Free Firewall ja Private firewall.

3.2.4 Salasanat

Salasana on keino tunnistaa henkilö, jolle pääsy tietoihin sallitaan. Mitä monimutkaisempi salasana on, sitä vaikeampi se on murtaa. Salasanojen murtamiseen on kehitetty ohjelmia, jotka toimivat periaatteessa siten, että ne kokeilevat kaikki mahdollisuudet. Hyvä salasana

ei ole helposti arvattavissa, vaan sen kokeilemiseen menee nykytietokoneiden laskentateholla kymmeniä vuosia, joten salasanan murtaminen ei ole todennäköistä. Hyvä salasana täyttää seuraavat tunnusmerkit:

- Sisältää isoja ja pieniä kirjaimia sekä numeroita.
- On tarpeeksi pitkä, vähintään kymmenen kirjainta.
- Ei ole mistään sanakirjasta löytyvä sana eikä ole kenenkään nimi.
- Ei ole yhdistettävissä käyttäjään (oma nimi, hääpäivä yms. ovat huonoja).
- Hyvää salasanaa ei ole kierrätetty muissa palveluissa.

Kun riittävän monimutkainen salasana on valittu, se täytyy opetella riittävän hyvin. Eräs tapa on näppäillä salasanaansa tekstinkäsittelyohjelmalla niin kauan, että se sujuu hyvin. The New York Times listasi 2010 suosituimpia salasanoja maailmalla:

1. **123456**	17. **michael**
2. **12345**	18. **ashley**
3. **123456789**	19. **654321**
4. **password**	20. **qwerty**
5. **iloveyou**	21. **iloveu**
6. **princess**	22. **michelle**
7. **rockyou**	23. **111111**
8. **1234567**	24. **0**
9. **12345678**	25. **tigger**
10. **abc123**	26. **password1**
11. **nicole**	27. **sunshine**
12. **daniel**	28. **chocolate**
13. **babygirl**	29. **anthony**
14. **monkey**	30. **angel**
15. **jessica**	31. **FRIENDS**
16. **lovely**	32. **soccer**

KUVIO 2. Suosituimpia salasanoja 2010 (Vance, A. 2010.)

3.2.5 Haittaohjelmien poistotyökalu

Microsoft Windows haittaohjelmien poistotyökalu tarkistaa, ettei tietokoneissa ole tiettyjä yleisiä haittaohjelmia, kuten esimerkiksi Blaster, Sasser tai Mydoom ja auttaa poistamaan mahdollisesti löytyvät haitat. Tarkastuksen ja poiston jälkeen tulee raportti, jossa kerrotaan, mitä haittaohjelmia mahdollisesti löydettiin ja on poistettu (http://www.microsoft.com/fi-fi/download/malicious-software-removal-tool-details.aspx)

3.2.6 Salaukset

Salattu yhteys tarkoittaa yhteyttä tietokoneelta Internettiin. Lähtevä ja tuleva tieto salataan, jottei sitä voida lukea suoraan. Salattu tieto ei ole ulkopuolisen luettavissa, mikäli tieto

joutuisikin hänen haltuunsa ja mikäli hän ei osaa purkaa salausta. Salauksen purkaminen vaatii avaimen. Salattua yhteyttä ei tarvita, jos katselet esimerkiksi Internetin julkisia sivuja, tai siirrät Internettiin julkiseksi tarkoitettua materiaalia. Salausta suositellaan silloin, kun lähetät salaiseksi tarkoitettua tietoa, esimerkiksi pankkikortin tietoja tai muita salaisia tietoja.

Salausmenetelmiä on useita riippuen siitä, missä niitä käytetään. Internet-sivujen salausmetodit ovat yleensä SSL-salauksia (Secure Sockets Layer). Palvelimissa käytetään SSH-salausta (Secure Shell) ja nykyään SSH2-salausta (Secure Shell version 2) enemmän, koska ykkösversiossa on haavoittuvuuksia ilmennyt. Tiedonsiirroissa käytetään SCP (Secure copy) sekä SFTP – protokollia (Secure File Transfer Program). Arkaluontoisissa sähköposteissa käytetään PGP-salausta ((Pretty Good Privacy) (http://www.internetopas.com/yleistietoa/tietoturva/tekninensuojaus/.)

SSL on salausprotokolla, jolla voidaan salata tunnistus käyttäjän ja palvelimen välillä. SSL on yleisin pankkipääteyhteyksien suojausmenetelmä.

SSH on suomalaista alkuperää. SSH turvaa tiedonsiirron Unix-koneiden sekä Unix-palvelimien välillä. SSH suojaa liikenteen vain Unix-palvelinten käytössä, mutta ei Windows-verkon liikennettä.

SFTP on SSH-protokollaa hyväksi käyttävä tiedonsiirtomenetelmä, joka salaa sekä käyttäjätunnuksen, salasanan että siirrettävän tiedon.

PGP on yleisin sähköpostin salaamiseen käytetty menetelmä ja monet sähköpostiohjelmat tukevat sitä. Käyttäjä voi suojata tiedostojaan sekä lähettää ja vastaanottaa luottamuksellisia sähköpostiviestejä ja niiden liitteitä. Tiedostot voidaan halutessa varmentaa sähköisellä allekirjoituksella (http://www.internetopas.com/yleistietoa/tietoturva/tekninensuojaus/.)

3.2.7 Langattoman lähiverkon salaukset

Langaton lähiverkko eli WLAN (Wireless Local Area Network) mahdollistaa tietokoneiden ja lisälaitteiden kytkemisen langattomasti tietoverkkoon. WLAN on maailmanlaajuinen standardi, joka toimii eri puolilla maailmaa käytännössä katsoen

samoilla 2,4 GHz ja 5,6Ghz taajuusalueilla. WLAN-verkot ovat yleistymässä koti- ja yrityskäytössä sekä julkisissa tiloissa. Myös mobiililaitteet käyttävät paljon WLAN-yhteyttä. Tämä on lisännyt tietoturvallisuuden tarvetta runsaasti. Yleisin syy tietovuotoihin ja väärinkäyttöihin löytyy salaamattomista verkoista. Naapurisi WLAN-verkko saattaa ylettyä jopa sadan metrin päähän ja salaamatonta nettiyhteyttä pystyy käyttämään kaikki tuon sadan metrin alueelle osuvat esimerkiksi väärinkäytöksiin. Salaamatonta liikennettä myös pystytään kuuntelemaan helposti.

WLAN-salausmenetelmiä ovat WEP-, WPA- ja EPA2-salaus.
WEP-salaus (Wired Equivalent Privacy) on aikaisemmin yleisesti käytetty salaus. Se sisältää heikkouksia, joiden takia se on helposti murrettavissa. Jos WEP-salaus murretaan, voi ulkopuolinen paitsi kuunnella verkon liikennettä, myös käyttää verkkoa omiin tarkoituksiinsa. WEP-salauksesta on olemassa 40-bittinen ja 128-bittinen avain versio, mutta kumpaakaan ei suositella käytettäväksi, sillä suojauksien heikkoudet eivät liity pelkästään salausavaimenpituuteen. WEP-salauksen murtavia ohjelmia ovat esimerkiksi Airsnort, Kismet, KisMAC.

WPA-salaus (Wi-Fi Protected Access) kehitettiin WEP-salauksen ongelmien paljastuttua. Se käyttää dynaamista avainta, jolloin avain vaihtuu jatkuvasti. Verkkoon murtautuminen on vaikeampaa kuin WEP-salauksessa.

WPA2-salaus (Wi-Fi Protected Access 2) on uudempi WPA-salaus, jota suositellaan käytettävän, jos laitteet ja ohjelmistot sitä tukevat.

WLAN- suojautumisessa kannattaa muistaa nämä asiat:

- käytä WPA2-salausta jos mahdollista.
- Kytke pois SSID (SSID broadcast) mainostaminen.
- Hallinnoi WLAN-verkkoa vain kiinteän kaapelin kautta.
- Jos WLAN-verkossa siirretään arkaluontoista tietoa, kannattaa WEP:in tai WPA lisäksi käyttää aina (riittävän) vahvaa salausta.
- Jos tunnistautumiseen käytetään salasanoja, älä käytä helposti arvattavia salasanoja. Ota lisäksi käyttöön MAC (Media Access Control) -osoitteisiin pohjautuva tunnistautuminen.

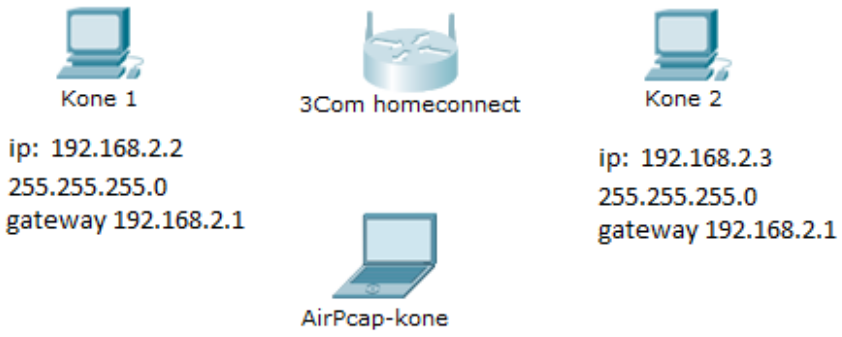
4 AirPcap Tx HARJOITUS-TYÖ

Opinnäytetyön toisessa osassa opiskelijalle tehtiin WLAN-harjoitustehtäviä. Tehtävät luotiin AirPcap Tx ympärille. Työn suunnittelussa tutustuin AirPcap ohjelmistoon ja sen pohjalta lähdin rakentamaan harjoitus-työtä opiskelijalle.

AirPcap Tx on edullinen ja helppokäyttöinen WLAN (802.11b/g) – standardille tarkoitettu laitteisto. 802.11 on yleisin standardi langattomille WLAN-lähiverkoille.
Laitteistoon kuuluu Wireshark ohjelmisto ja USB tikkumainen AirPcap Tx laite.

Kuvio 2. AirPcap Tx

AirPcap Tx:llä pystyy vastaanottamaan ja lähettämään tietoa Windows-ympäristössä. Laitteen avulla voidaan tutkia verkkojen tietoturva-aukkoja. Langattoman liikenteen tulkitsemiseen tarvitaan Wireshark ohjelmisto, joka tulee ”tikun” mukana. Yhdessä nämä tuotteet ovat todella hyvä työkalu tietoturva-aukkojen tutkimiseen langattomissa verkoissa. Työn alussa rakennettiin verkko, johon kuului 3 konetta ja yksi WLAN-tukiasema. Yksi näistä koneista kytkettiin AirPcap Tx USB-tikkuun. AirPcap-koneeseen asennettiin myös Wireshark ohjelmisto (LIITE1/5).



Kuvio 4. Laboratorion WLAN-testiverkko

Tämän jälkeen tehtiin WLAN-tukiasemalle oikeat asetukset, jotta tukiasema keskustelisi oikein siihen kytkeytyvien koneiden kanssa. Tässä kohtaan myös tukiaseman salaus laitettiin pois päältä, jotta harjoituksissa pystytään tutkimaan myös salaamatonta liikennettä (LIITE 1/2 – LIITE 1/4).

Tukiaseman asetuksien jälkeen koneet tunnistivat verkon ja näkyivät toisilleen. Siirryttiin Wireshark-ohjelmaan ja sieltä aloitettiin verkon liikenteen tutkiminen annetuilla ohjeilla ja tehtävillä (LIITE1/5 – LIITE1/7).

Tehtävänä oli irrottaa molemmat WLAN-koneet verkosta irti ja tämän jälkeen kytkeä toinen kone takaisin verkkoon. Wireshark-ohjelmalla tutkittiin ja kirjattiin kyseiset tapahtumat ylös (LIITE2/2). Tämä toiminto toteutettiin myös toisella irti otetulla koneella kirjaamalla tiedot. Wiresharkista pitäisi tulkita, kuinka koneet liittyvät verkkoon. Ongelmia tässä kohtaan voi tulla monelle, jos ei laita Wireshark-ohjelmaa tutkimaan signaalia paria sekuntia ennen koneen kytkemistä verkkoon. Ohjelma tulostaa tuhansia rivejä tietoa ja sitä voi olla vaikea tulkita, ellei tiedä mitä tietoa hakee.

Yhtenä tehtävänä avattiin kone1- tai kone2:lta Internet sivuja ja jaettiin notepadilla tehtyjä tiedostoja (LIITE1/8 ja LIITE1/10).
Näitä tutkittiin Wireshark:lla ja kirjattiin ylös tapahtumia. Testi.txt tiedostot ja avatut Internet-sivut näkyivät ruudulla selvästi ilman salausta ja jopa Internet-sivutkin näkyivät www-osoitteineen (LIITE2/5).
Tämän jälkeen kytkettiin salaukset päälle tukiasemasta ja suoritettiin samat tiedosto- ja Internet-sivu-testit (LIITE1/10).
Salatussa liikenteessä ei pitäisi näkyä mitään liikennettä ulospäin, koska salaus WEP2 on käytössä. Tämä todistaa hyvin miksi salaus on tarpeellista WLAN-verkoissa.

Viimeisenä tehtävänä oli tutkia muita WLAN-taajuus kanavia ja niiden tapahtumia (LIITE1/10). Tätä tehdessä huomaa kuinka paljon salaamatonta liikennettä kulkee eri kanavilla. Wireshark näytti kannettavia tietokoneita, kännyköitä ja jopa langattomia musiikkisoittimien tietoja. Tiedoissa näkyivät käyttäjien nimet ja asiat, joita he tekivät koneella salaamattomassa verkossa. Olin itsekin yllättänyt, että näinkin moni laite on salaamaton. Etenkin hämmästyttivät kännykät joissa näkyi käyttäjien oikeat nimet. Tämän harjoituksen tarkoituksena oli näyttää sen tekijälle, mitä hyötyä on salatulla WLAN-yhteydellä ja sen se mielestäni tekee hyvin.

5 YHTEENVETO

Työtä kootessani huomasin, että materiaalia saa todella paljon tietoturva aiheeseen, joten ongelmana oli sen kerääminen yhteen nippuun ja kertoa siitä lyhyesti ja ytimekkäästi. Opinnäytetyön tarkoituksena oli kertominen miksi tietoturva on tärkeää ja kertoa tietoturvauhista, jotka koskevat jokaista tietokonetta, joka on liitetty verkkoon langallisesti tai langattomasti. Luettelin haittaohjelmia, jotka verkossa vaanivat käyttäjää ja kerroin myös miten niitä torjutaan. Olemalla askeleen edellä haittaohjelmia turvaa itsensä ja ei samalla saastuta muita koneita verkossa. Tärkeimpiä tietoturva suojia olivat mielestäni hyvä virustorjunta-ohjelma, palomuuri ja jos käytät WLAN-yhteyttä niin siihen laittamalla WPA/WPA2-salaus päälle ja täytyy myös muistaa vaihtaa se vakio salasana sieltä lähettimestä.

Etsimällä tietoa tietoturvaan internetissä törmäsin hauskoihin asioihin kuten esimerkiksi yleisimmät salasanat. Aika moni käyttää omaa nimeään tai sanakirjan sanoja. Toivottavasti tämän työn tuloksena jokainen vaihtaa sen vähän hankalampaan kuin oma nimi.

Opinnäytetyön toisessa osassa tein koululle laboratoriotyön, jota opiskelijat voivat käyttää havainnollistaakseen, miten tietoturva toimii WLAN-yhteyksissä salauksien kera ja ilman niitä. Laboratoriotyön kasaamisen ja tekemieni testien aikana huomasin, kuinka monta kännykkää ja kannettavaa tietokonetta koulun alueella on salaamattomana. Mielestäni tämä AirPcap-harjoitus viimeistään todistaa oppilaille, miksi on tärkeää salata kaikkia langatonta verkkoliikennettä jopa niitä kännyköitä. Vaikka tietoturvaohjelmat ovat erittäin tärkeä osa tietokoneen turvaamista, vastaa viimekädessä tietoturvatasosta kuitenkin käyttäjä itse. Täytyy muistaa, että vaikka kuinka varautuisit kaikkiin uhkiin, niin absoluuttista pistettä tietoturvassa ei ole olemassa koskaan.

LÄHTEET

Gaille, B. 2013. 36 shocking computer virus Statistics. Www-dokumentti. Saatavissa: http://brandongaille.com/36-shocking-computer-virus-statistics/. Luettu 21.2.2014.

Hakala, P. 2013. Valepoliisit kiristäneet netissä tuhansia suomalaisia. Helsingin-sanomat 17.10.2013. Www-dokumentti. Saatavissa: http://www.hs.fi/kotimaa/Valepoliisit+kirist%C3%A4neet+netiss%C3%A4+tuhansia+suomalaisia/a1381976746244. Luettu 14.4.2014.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. 1. painos. Jyväskylä: Docendo.

Suomen Internetopas. Www-dokumentti saatavissa: http://www.internetopas.com/yleistietoa/tietoturva/tekninensuojaus/. Luettu 12.4.2014.

Rootkit-ohjelma. Www-dokumentti. Saatavissa: http://fi.wikipedia.org/wiki/Haittaohjelma Luettu 20.5.2014.

Tirronen, H. 2003 Www-dokumentti. Saatavissa http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva.html. Luettu 21.2.2014.

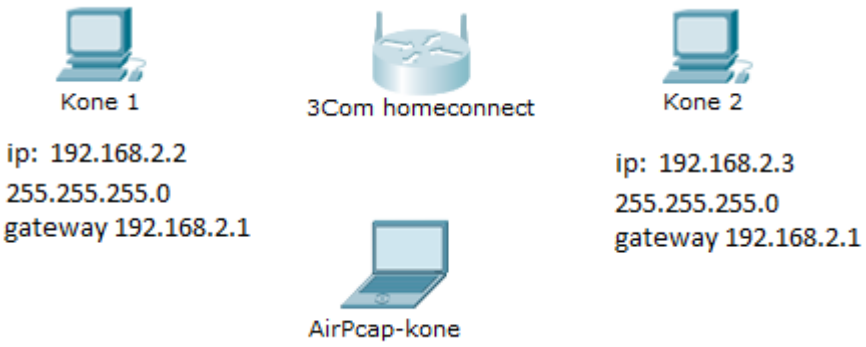
Vance, A. 2010. If your password is 123456, Just Make It HackMe. 20.1.2010. Www-dokumentti. Saatavissa: http://www.nytimes.com/2010/01/21/technology/21password.html?ref=technology&_r=0 Luettu 26.4.2014.

Keskipohjanmaan AMK, Ylivieska Jarno Kari 2014
Tietoliikennetekniikan laboraatiot

AirPcap Tx

Työn kuvaus	Tämän laboratoriotyön tarkoituksena on perehtyä AirPcap Tx laitteen käyttöönottoon, konfigurointiin ja toimintaan.
Tarvittavat laitteet	- 1x 3Com home connect-tukiasema - 2x WLAN-kortteja - 1x RJ45 Ethernet kaapeli - 1x AirPcap Tx

Esitehtävä	Tutki ja kerro miten AirPcap laitteet toimivat http://www.riverbed.com/products-solutions/products/network-performance-management/wireshark-enhancement-products/Wireless-Traffic-Packet-Capture.html#How_It_Works
Työn suorittaminen	Asetetaan WLAN-tukiasemalle asetukset, konfiguroidaan WLAN-korttien asetukset. Asennetaan AirPcap ja tehdään annettuja harjoitteita joista raportoidaan havainnot ja tulokset.



1. Asenna kahteen koneeseen WLAN-kortit kyseisillä asetuksilla:

   kone1 ip: 192.168.2.2 255.255.255.0 gateway 192.168.2.1

   kone2 ip: 192.168.2.3 255.255.255.0 gateway 192.168.2.1

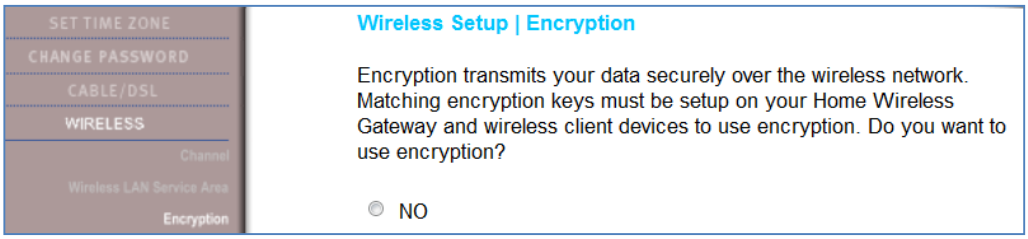
2. Ota yhteys 3Com homeconnect-tukiasemaan (tukiaseman osoite http://192.168.2.1/) R45-johdolla ja tee seuraavat asetukset:

   Kyseinen aloitusruutu pitäisi olla näkyvissä. Paina Setup ->

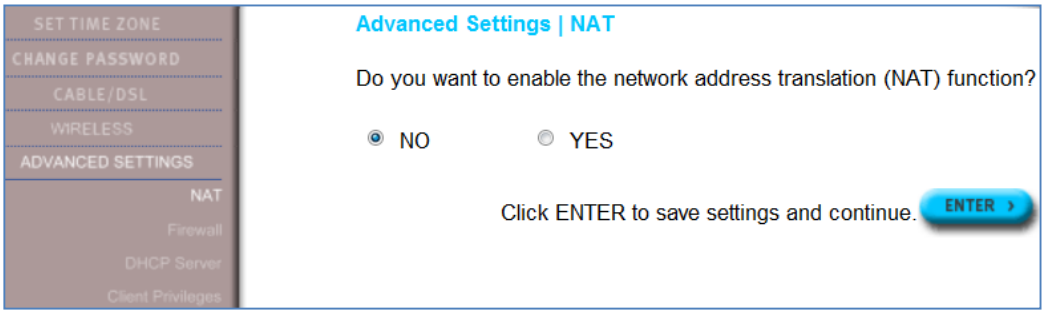
Olet nyt Setup valikossa ja sieltä valitset Wireless channel -> manually -> ja kanavaksi 11

Wireless LAN service access -> Labra1 alueeksi

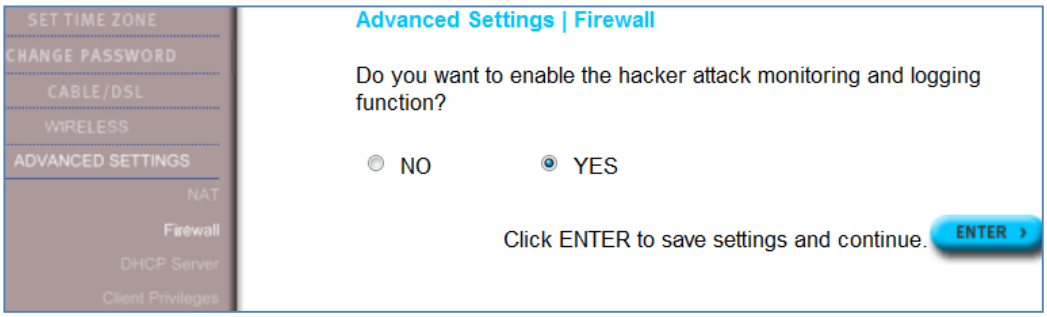
Encryptionista saat salaukset päälle joita emme tarvitse vielä joten joten laita siihen -> NO



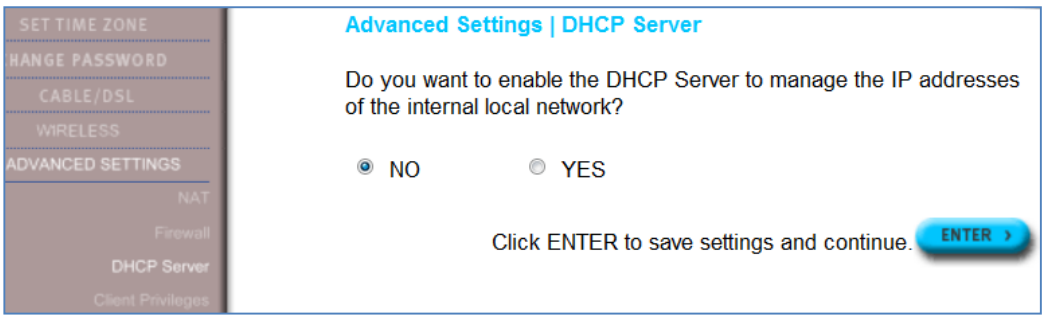
Advanced settings -> NAT -> NO



Advanced settings -> Firewall -> YES



Advanced settings -> DHCP Server -> NO



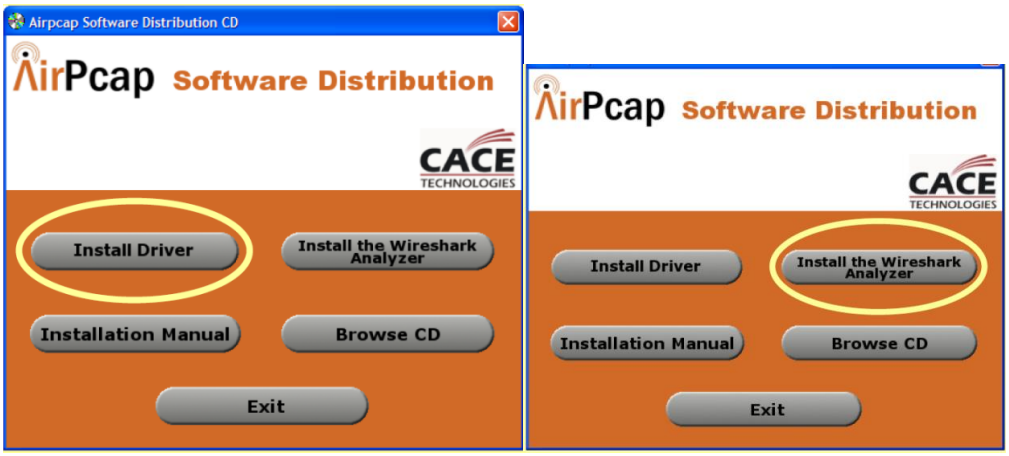
Tämän jälkeen tukiasema varmaan haluaa bootata itsensä.

Tarkista tämän jälkeen että kone 1 ja 2 löytävät kyseisen labra1 verkon ja yhdistä koneet verkkoon

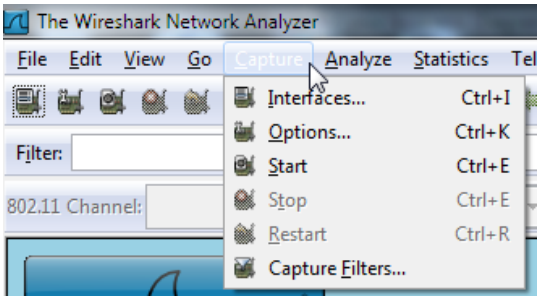
3.

AirPcap ajureiden ja Wireshark-ohjelman asennus (ohjeet ja installeri cd:llä)

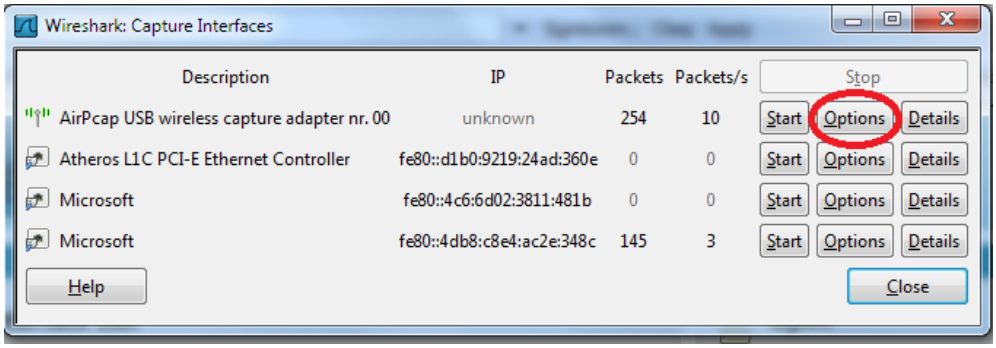
Asenna ensin ajurit ja vasta sitten ohjelma.



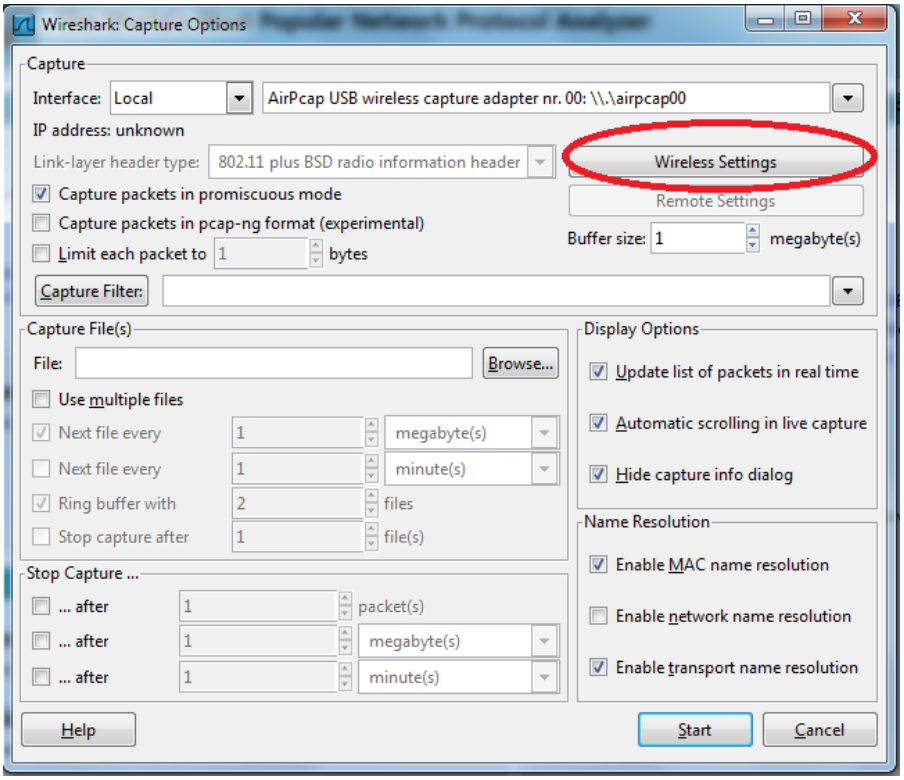
Käynnistä wireshark ja avaa Capture -> Interfaces



AirPcap USB wireless capture adapter kohdasta painat -> options

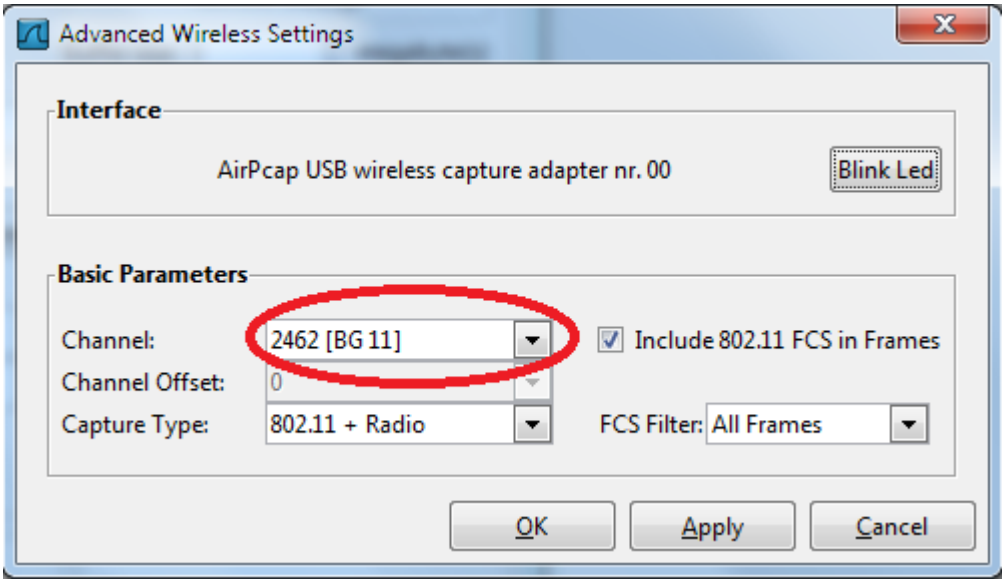


Wireless settings ->

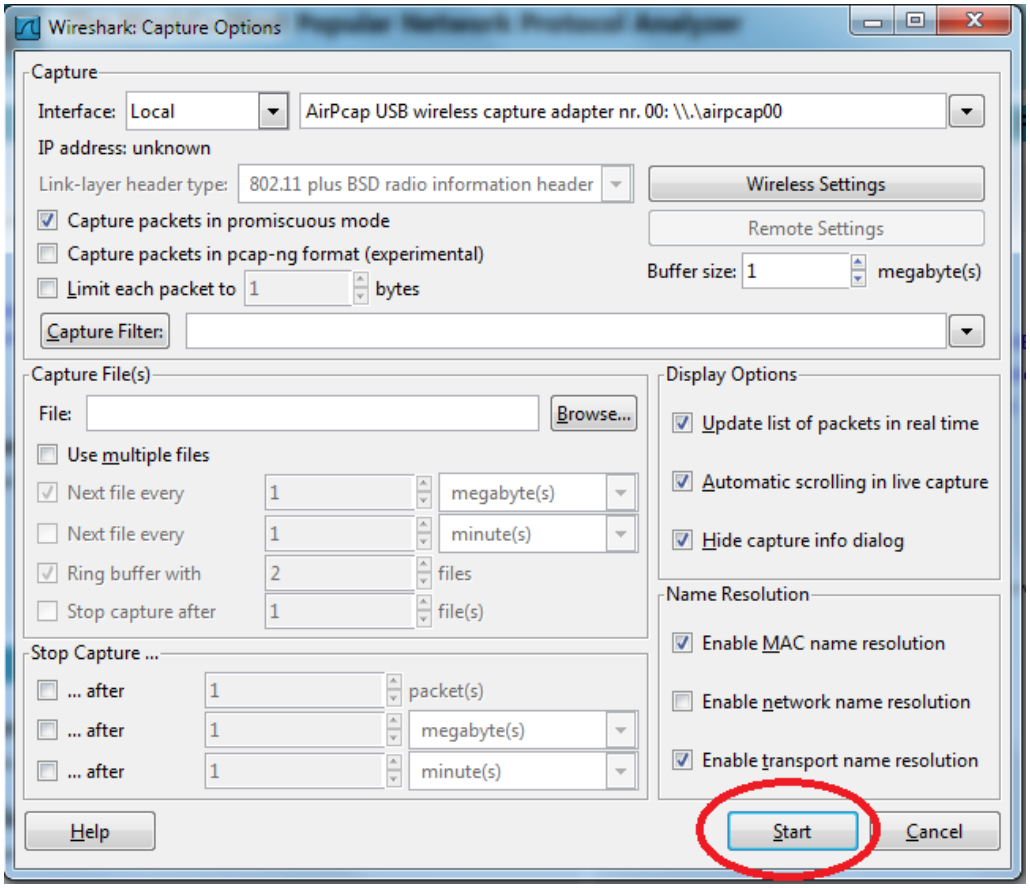


Valitaan kanava 11 joka tukiasemalle asetettiin aiemmin,

capture type 802.11 + Radio -> OK

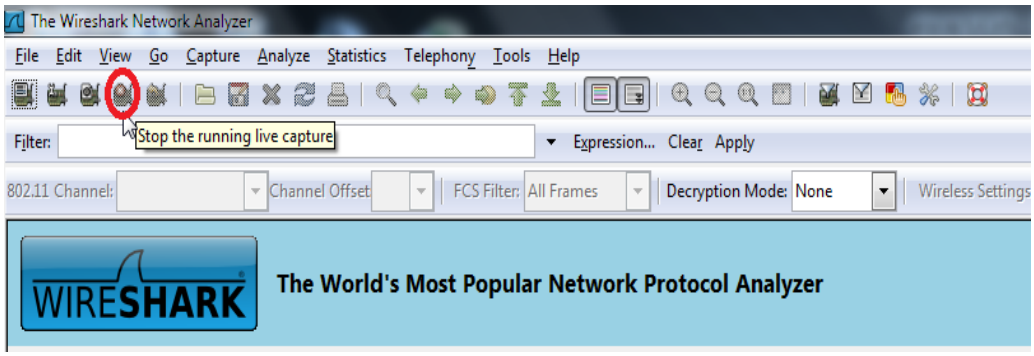


Paina start käynnistääksesi scannauksen



4.Tehtävät.

Anna kyseisen testin jatkua hetken ja sitten paina "stop the running live capture" jota suositellaan aina käytettäväksi kun aloitetaan tutkimaan tapahtumia. HUOM! napin vasemmalla puolella on uuden testin aloitus pikanäppäin jota suositellaan käytettäväksi kun asetukset on sisäänajettu ajan säästämiseksi."



Tehtävä 1. Minkälaisia tapahtumia erotat taulukosta kanavalta 11?

Kirjattuasi tapahtumat talteen kokeile irroittaa molemmat WLAN-koneet verkosta ja tutki, mitä tapahtuu wiresharkin ruudulla? (Suljet labra1 yhteydet koneilta)

Kirjattuasi tiedot ylös kokeile liittää toinen koneista verkkoon takaisin ja tutki, mitä ruudulla tapahtuu kyseisellä hetkellä. Tee sama myös toiselle koneelle. On suositeltavaa, että ohjelma laitetaan scannaamaan paria sekunttia ennen koneen kytkemistä labra1 verkkoon, ettei tarvitse koluta tuhansia rivejä tietoa.

Kirjaa tärkeimmät tiedot ylös, kun kone liittyy verkkoon ja kommentoi tapahtumia suuripiirtein. HUOM. Muista tehdä taulukko molemmille koneille.

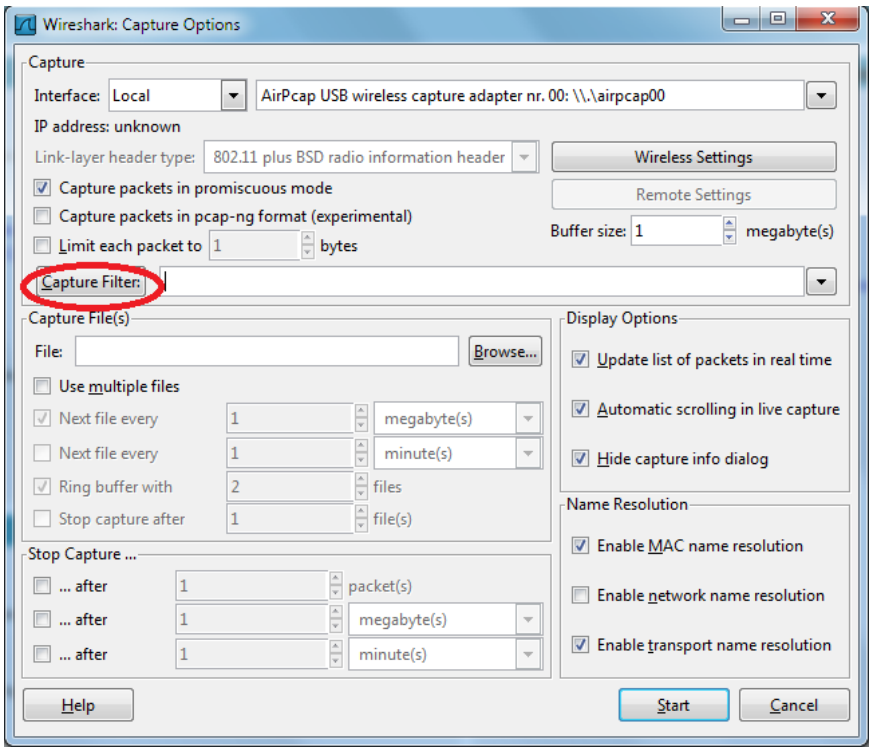
No.	*Time*	*Source*	*Destination*	*Protocol*	*Info*

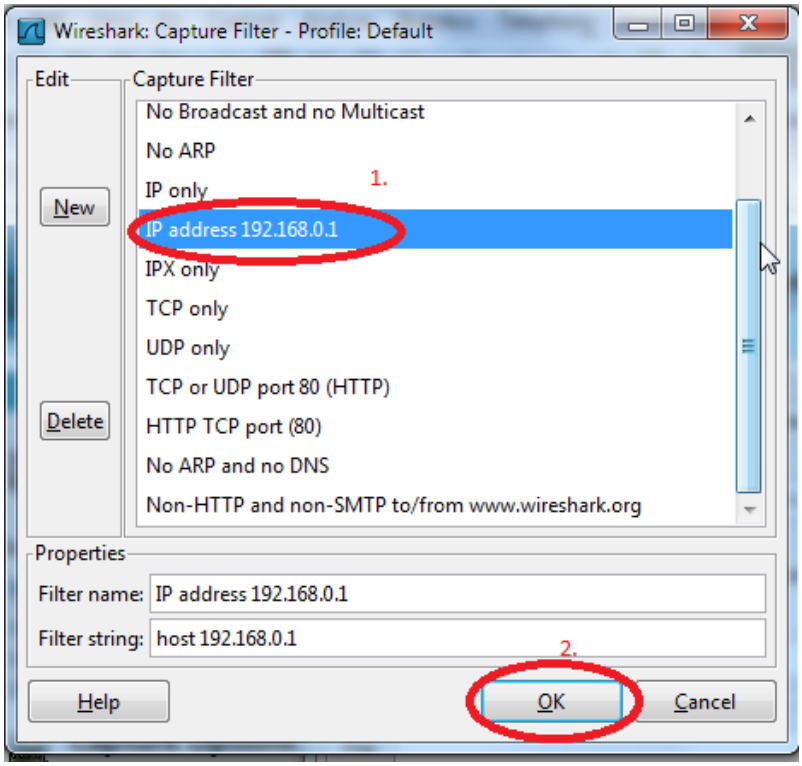
Tehtävä 2. Tiedosto verkon yli.

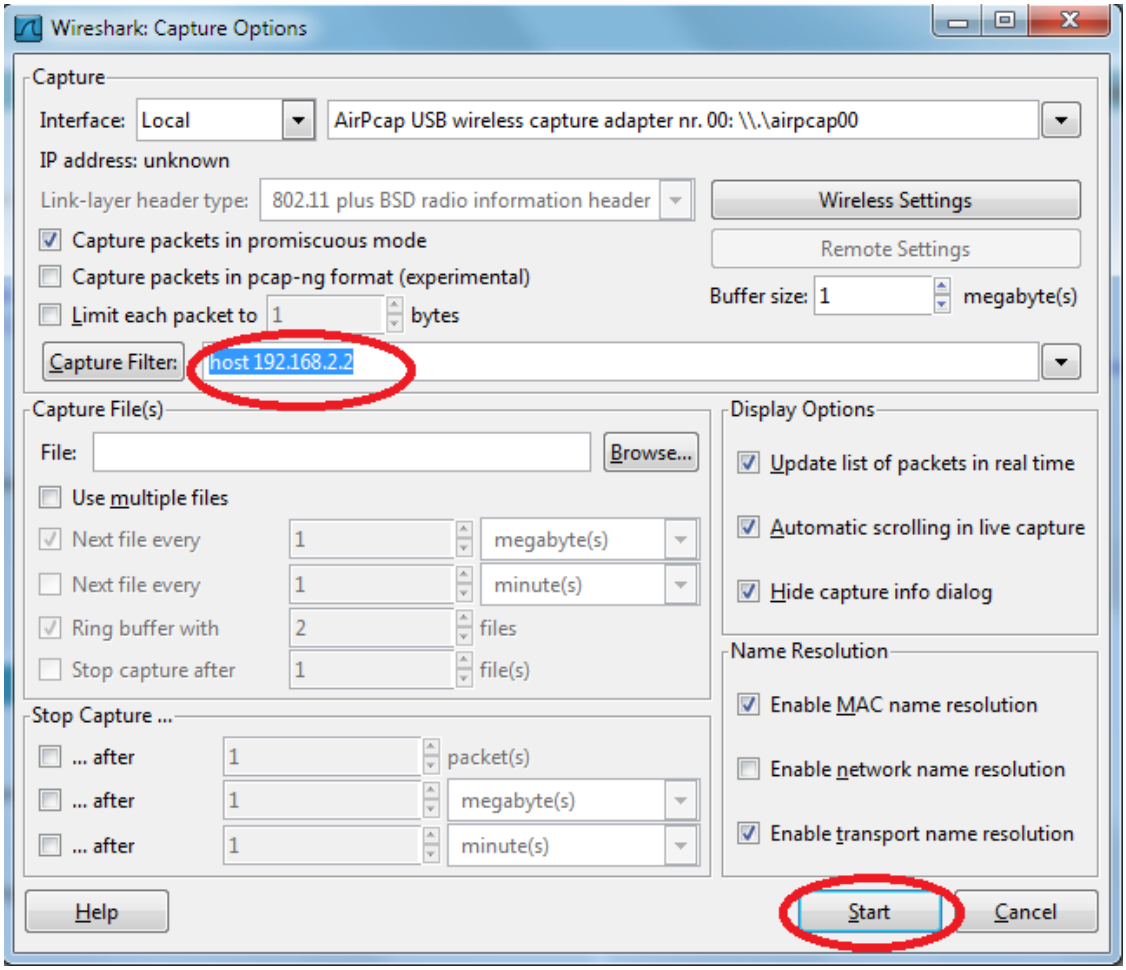
Tee toiselle koneelle kansio, jossa on jokin tiedosto esim notepadilla testi.txt ja jaa se koko verkolle. Toiselta koneelta avaa kyseinen tiedosto verkon yli. Tutki, miltä se näyttää ja kirjaa ylös joitakin wiresharkin antamia tietoja.

Vinkki. Laita wiresharkin filtereistä vain scannaamaan kyseisen koneen tietoja joka toimintoja tekee niin näet selvemmin. esim jos kone 192.168.2.2 avaa kansion koneelta 192.168.2.3 laitat filetereistä ip address 168.192.2.2

Capture -> Interface.. -> options -> capture filter




Wireshark: Capture Filter - Profile: Default
Edit
Capture Filter
No Broadcast and no Multicast
No ARP
IP only
1.
New
IP address 192.168.0.1
IPX only
TCP only
UDP only
TCP or UDP port 80 (HTTP)
Delete
HTTP TCP port (80)
No ARP and no DNS
Non-HTTP and non-SMTP to/from www.wireshark.org
Properties
Filter name: IP address 192.168.0.1
Filter string: host 192.168.0.1
2.
Help
OK
Cancel


Wireshark: Capture Options
Capture
Interface: Local
AirPcap USB wireless capture adapter nr. 00: \\.\airpcap00
IP address: unknown
Link-layer header type: 802.11 plus BSD radio information header
Wireless Settings
Capture packets in promiscuous mode
Remote Settings
Capture packets in pcap-ng format (experimental)
Buffer size: 1 megabyte(s)
Limit each packet to 1 bytes
Capture Filter: host 192.168.2.2
Capture File(s)
File:
Browse...
Use multiple files
Next file every 1 megabyte(s)
Next file every 1 minute(s)
Ring buffer with 2 files
Stop capture after 1 file(s)
Display Options
Update list of packets in real time
Automatic scrolling in live capture
Hide capture info dialog
Name Resolution
Enable MAC name resolution
Enable network name resolution
Enable transport name resolution
Stop Capture ...
... after 1 packet(s)
... after 1 megabyte(s)
... after 1 minute(s)
Help
Start
Cancel

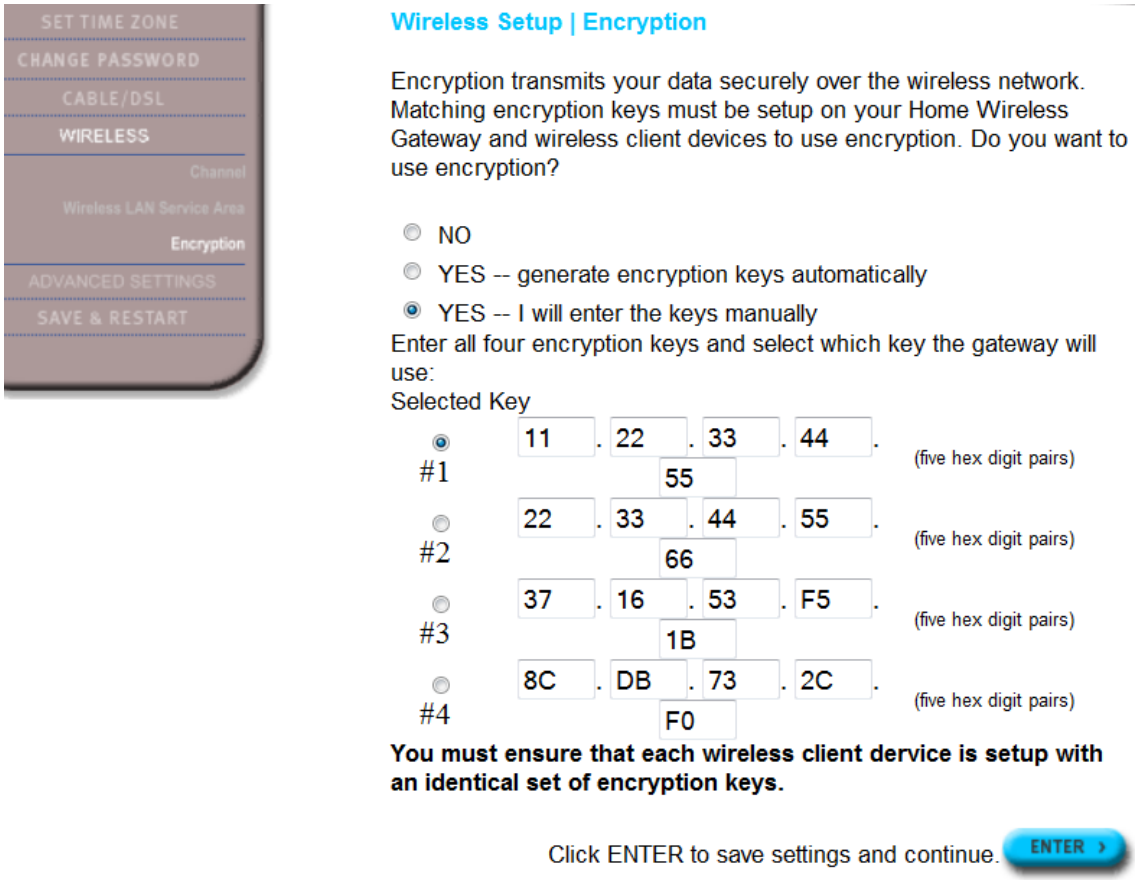
Tehtävä 3. Internet-sivu

Poista filtterit ja avaa netti-selain toiselta koneelta ja kirjoita esim www.mtv3.fi ,tutki wiresharkin antamia tietoja ja kirjaa ylös.

Kokeile eri ohjelmia, esimerkiksi telnet ja tulkitse niitä wiresharkista....

Tehtävä 4. Salaukset päälle

Seuraavaksi otetaan yhteys tukiaseman asetuksiin ja muutetaan wireless-> encryption -> ja suojaukset päälle, suosittelen määrittelemään itse 2 ensimmäistä avainta molemmille wlan korteille. Huom! muistathan kun yhdistyt kone1 ja 2 verkkoon ja laitat avaimia pisteet jäävät väleistä pois esim 11223344.



Tutki nyt wiresharkilla koko 11 kanavaa. Kokeile tiedosto,www jne toimintoja ja raportoi tulokset.

Tehtävä 5. Muiden kanavien liikenne.

Tämän jälkeen kokeile wiresharkista scannata muita kanavia, esim 5 tai 6. Minkälaista liikennettä huomaat koulun verkossa liikkuvan salaamattomana?

Työselostus:

- Tehtävistä saatuja taulukoita kommenttien kera.
- Miksi salaus on tärkeää? Kerro jokin esimerkkitapaus.
- Pohdi missä voisit käyttää AirPcap Tx:tä hyödyksi?

Suuntaa antavia vastauksia tehtäviin:

Esitehtävä: Tutki AirPcapin sivuilta kyseisen laitteen toimintaa:
http://www.riverbed.com/products-solutions/products/network-performance-management/wireshark-enhancement-products/Wireless-Traffic-Packet-Capture.html#How_It_Works

Captures wireless traffic on a single channel

Each AirPcap adapter captures traffic on a single channel at a time; the channel setting for the AirPcap adapter can be changed using the AirPcap Control Panel, or from the "Advanced Wireless Settings" dialog in Wireshark or other tools. Depending on the model of your AirPcap adapter, it can be set to any valid 802.11a/b/g/n channel for packet capture.

Operate in completely passive mode

AirPcap adapters operate in a completely passive mode. This means that they capture the traffic on a channel without associating with an access point or interacting with any other wireless device. Unless you are transmitting with either AirPcap Tx , Ex or Nx, the adapters are not detectable by any other wireless station.

Can also work in monitor mode

The AirPcap adapters can work in Monitor Mode. In this mode, the AirPcap adapter will capture all of the frames that are transferred on a channel, not just frames that are addressed to it. This includes data frames, control frames and management frames.

Can be configured to decrypt WEP-encrypted frames

The AirPcap software can optionally be configured to decrypt WEP-encrypted frames. An arbitrary number of keys can be configured in the driver at the same time, so that the driver can decrypt the traffic of more than one access point at the same time. WPA and WPA2 support is handled by applications such as Wireshark and Aircrack-ng.

Use multiple AirPcap adapters for multi-channel aggregation

When more than one AirPcap adapter is plugged in, the AirPcap Control Panel will show one additional interface: the Multi-Channel Aggregator. The Multi-Channel Aggregator is a virtual capture interface that can be used from Wireshark or any other supported application. Using this capture interface, the application will receive the traffic from all installed USB AirPcap adapters as if it was coming from a single device.

The Multi-Channel Aggregator has its own FCS, Capture Type and FCS Filter settings. These settings, and not those of the physical adapter, will be used when capturing from the Aggregator. Note that it's not possible to set the channel of the Multi-Channel Aggregator; instead, the *channel* drop-down box will show a list of aggregated channels. To change the channel of any individual adapter, select the Capture adapter from the *Interface* drop-down list and set the desired value in the *channel* drop-down box.

Tehtävä 1. Minkälaisia tapahtumia erotat taulukosta kanavalta 11?

3com_7c:13:21 tukiasema broadcastaa omaa asemaansa.
linksysG_1b:c1:56 wlan-kortti broadcastaa itseään.
aironet_38_90:6d wlan-kortti broadcastaa itseään.

Kirjattuasi tapahtumat talteen kokeile irroittaa molemmat WLAN-koneet verkosta ja tutki mitä tapahtuu wiresharkin ruudulla ? Kirjaa ylös

3com_7c:13:21 tukiasema broadcastaa omaa asemaansa.
linksysG_1b:c1:56 WLAN-kortti broadcastaa itseään.
aironet_38_90:6d wlan-kortti broadcastaa itseään.

Kirjattuasi tiedot ylös nyt kokeile liittää toinen koneista verkkoon takaisin ja tutki mitä ruudulla tapahtuu kyseisellä hetkellä, tee sama myös toiselle koneelle. On suositeltavaa että ohjelma laitetaan scannaamaan paria sekunttia ennen koneen kytkemistä labra1 verkkoon ettei tarvitse koluta tuhansia rivejä tietoa.
Kirjaa tiedot ylös ja kommentoi

No.	*Time*	*Source*	*Destination*	*Protocol*	*Info*
		Linksys WLAN-kortti (vasemmanpuoleinen kone)			
5674	375.671033	LinksysG_1b:c1:56	Broadcast	ARP	Gratuitous ARP for 192.168.2.3 (Request)
5675	375.671298		LinksysG_1b:c1:56 (RA)	IEEE 802.11	Acknowledgement, Flags=........C
5676	375.672168	LinksysG_1b:c1:56	Broadcast	ARP	Gratuitous ARP for 192.168.2.3 (Request)
5680	375.928673	LinksysG_1b:c1:56	Broadcast	ARP	Gratuitous ARP for 192.168.2.3 (Request)
5681	375.928797		LinksysG_1b:c1:56 (RA)	IEEE 802.11	Acknowledgement, Flags=........C
5682	375.929794	LinksysG_1b:c1:56	Broadcast	ARP	Gratuitous ARP for 192.168.2.3 (Request)
5709	377.946801	192.168.2.3	224.0.0.22	IGMP	V3 Membership Report / Join group 239.255.255.250 for any sources
5710	377.947027		LinksysG_1b:c1:56 (RA)	IEEE 802.11	Acknowledgement, Flags=........C
5711	377.947795	192.168.2.3	224.0.0.22	IGMP	V3 Membership Report / Join group 239.255.255.250 for any sources
5712	377.948395	192.168.2.3	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
5713	377.948545		LinksysG_1b:c1:56 (RA)	IEEE 802.11	Acknowledgement, Flags=........C
5714	377.949170	192.168.2.3	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
5716	378.006923	192.168.2.3	192.168.2.255	NBNS	Registration NB YKAY-TIETOL5<00>
5717	378.007169		LinksysG_1b:c1:56 (RA)	IEEE 802.11	Acknowledgement, Flags=........C
5718	378.007669	192.168.2.3	192.168.2.255	NBNS	Registration NB YKAY-TIETOL5<00>

	Time	***Source***		***Destination***	***Protocol***
		(cisco) Aironet Wlan-kortti (oikeanpuoleinen kone)			
575	31.245635	Aironet_38:90:6d	Broadcast	ARP	Gratuitous ARP for 192.168.2.2 (Request)
576	31.245879		Aironet_38:90:6d (RA)	IEEE 802.11	Acknowledgement, Flags=........C
604	33.326878	192.168.2.2	224.0.0.22	IGMP	V3 Membership Report / Join group 239.255.255.250 for any sources
605	33.327127		Aironet_38:90:6d (RA)	IEEE 802.11	Acknowledgement, Flags=........C
606	33.327500	192.168.2.2	224.0.0.22	IGMP	V3 Membership Report / Join group 239.255.255.250 for any sources
607	33.332999	192.168.2.2	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
608	33.333122		Aironet_38:90:6d (RA)	IEEE 802.11	Acknowledgement, Flags=........C
609	33.333624	192.168.2.2	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
610	33.382880	3com_7c:13:21	Broadcast	IEEE 802.11	Beacon frame, SN=1507, FN=0, Flags=........C, BI=100, SSID="Labra1"
611	33.385752	192.168.2.2	192.168.2.255	NBNS	Registration NB YKAY-TIETOL1<00>
612	33.385998		Aironet_38:90:6d (RA)	IEEE 802.11	Acknowledgement, Flags=........C

Pitäisi osata tulkita koneen liittyminen verkkoon.

Tehtävä 2. Tiedosto verkon yli.

Tee toiselle koneelle kansio jossa on jokin notepad tiedosto esim testi.txt ja jaa se koko verkolle. Toiselta koneelta avaa kyseinen tiedosto verkon yli. Tutki miltä se näyttää ja kirjaa ylös joitakin wiresharkin antamia tietoja.

Vinkki. Laita wiresharkin filtereistä vain scannaamaan kyseisen koneen tietoja joka toimintoja tekee niin näet selvemmin. esim jos kone 192.168.2.2 avaa kansion koneelta 192.168.2.3 laitat filetereistä ip address 168.192.2.2

No.	*Time*	*Source*	*Destination*	*Protocol*	*Info*
325	10.718392	192.168.2.3	192.168.2.2	SMB	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: \testi.txt
326	10.718998	192.168.2.3	192.168.2.2	SMB	[TCP Out-Of-Order] Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: \testi.txt
327	10.719872	192.168.2.2	192.168.2.3	SMB	Trans2 Response, QUERY_PATH_INFO
487	250.651027	192.168.2.3	192.168.2.2	SMB	NT Create AndX Request, Path: \testi.txt

Tehtävä 3. Internet-sivu

Poista filtterit ja avaa netti-selain toiselta koneelta ja kirjoita esim www.mtv3.fi ,tutki wiresharkin antamia tietoja ja kirjaa ylös.

Kokeile eriohjelmia, esim telnet ja tulkitse niitä wiresharkista....

No.	*Time*	*Source*	*Destination*	*Protocol*	*Info*
19	89.883879	192.168.2.3	192.168.2.255	NBNS	Name query NB WWW.MTV3.FI<00>
23	91.183024	192.168.2.3	192.168.2.2	SMB	Echo Request

Tehtävä 4. Salaukset päälle

Seuraavaksi otetaan yhteys tukiaseman asetuksiin ja muutetaan wireless-> encryption -> ja suojaukset päälle, suosittelen määrittelemään itse 2 ensimmäistä avainta molemmille wlan korteille. Huom! muistathan kun yhdistyt kone1 ja 2 verkkoon ja laitat avaimia pisteet jäävät väleistä pois esim 11223344.

Tutki nyt wiresharkilla koko 11 kanavaa. Kokeile telnet,www jne toimintoja ja raportoi tulokset.

Ei pitäisi näkyä mitään liikennettä koneiden välillä koska salaukset ovat päällä. Ainoastaan 3com broadcast pitäisi pystyä näkemään.

Tehtävä 5. Muiden kanavien liikenne.
Tämän jälkeen kokeile wiresharkista scannata muita kanavia, esim 5 tai 6. Minkälaista liikennettä huomaat koulun verkossa liikkuvan salaamattomana?
Jos hyvä tuuri käy siellä pitäisi näkyä iphone/ipodeja nimien kera + joitakin kannettavia tietokoneita nimien kera + www sivuja joita muut katselevat kännyköillään jne.....

Pohdi missä voisit käyttää AirPcap Tx:tä hyödyksi.

Esimerkiksi tutkimaan WLAN-verkkojen aukot ja yrityksissä scannaamaan suojaamattomat yhteydet helposti.