TIEA222 Tietoturva, laboratoriotyö 1

Joel Lehtonen et al.

23.9.2010, v1.11

1 Johdanto

WLAN-verkkoja löytyy nykyään lähes kaikkialta – kouluista, työpaikoilta, kodeista ja avoimiakin WLAN-verkkoja on tarjolla. Usein WLAN-verkot ovat heikosti suojattuja tai jopa täysin suojaamattomia. Työssä on tarkoitus tutustua muutamaan WLAN-verkon suojaukseen ja tutustua niiden toimivuuteen. Työssä ei ole tarkoituskaan käydä kaikkia mahdollisia suojaustapoja läpi.

Tietoliikennelaboratoriossa toimii vahvasti myös Jyväskylän yliopiston langaton verkko. Pidä huoli, että et työskentele yleisessä verkossa, kuten jyu-student tai agora-open!

Tietoverkkojen ja tietojärjestelmien yleistyessä myös sosiaalinen tiedustelu on yleistynyt. Tietojärjestelmissä on yhä enemmän ja enemmän arkaluonteista (esim. yrityssalaisuuksia) tietoa, joista jotkut henkilöt ovat kiinnostuneita. Työssä pääset itse kokeilemaan sosiaalista tiedustelua.

Tässä harjoituksessa esitettyjä asioita saa kokeilla vapaasti vain omaan verkon langattomaan verkkoonsa. Salauksen murtamista ei saa kokeilla toisten ihmisten langattomissa verkoissa ilman verkon ylläpitäjän lupaa.

2 Esitehtävät

Lue tämä työohje huolellisesti läpi ja vastaa näihin kysymyksiin ennen laboratorioon tuloasi. Näytä vastaukset assistentille ennen työn aloittamista. Lähetä näidenkin kysymysten vastaukset muiden kysymysten vastausten kanssa ohjeen lopussa olevien ohjeiden mukaisesti.

Q1: Katso laboratoriotyön kuvausta ja selvitä mitä Suomen laki sanoo työn eri vaiheista. Onko käytetyt keinot tai tavoitteet sallittuja vai kiellettyjä? Perustele vastauksesi viitaamalla ao. lakipykälään.

Q2: Miten WLAN-verkon WEP-salaus toimii?

Q3: Mitä on sosiaalinen tiedustelu? Mihin se perustuu? Etsi muutama tositapaus, joissa on käytetty sosiaalista tiedustelua.

Q4: Miten sinä voisit saada käyttäjän paljastamaan sinulle tunnuksensa ja salasanansa? Voit miettiä toimintatapaa, jota käyttäisit puhelimessa ja tapaa, jota käyttäisit kasvotusten kohdehenkilön kanssa.

3 Laboratoriotyön kuvaus

Laboratoriotyössä on tarkoituksena murtautua Web-palvelimelle WLAN-verkon kautta ja muokata palvelimella olevaa Web-sivua. Haasteina matkan varrella on WEP-salattu WLAN-verkko, jonka salaus tulee murtaa ja käyttäjätunnusten kalasteleminen palvelinkoneen käyttäjältä.

3.1 Murra WLAN-verkon WEP-salaus

Aivan aluksi kytke NetworkManager pois käytöstä, jotta se ei tekisi automaattisesti verkkoasetuksia löydettyään langattomia verkkoja. Se tapahtuu painamalla hiiren kakkosnäppäintä ruudun oikeassa ylälaidassa olevasta langattoman verkon kuvakkeesta ja poistamalla valinta kohdasta *Enable Networking*.

Kannettavalle tietokoneelle on asennettu aircrack-ng -ohjelmisto, jonka avulla WLAN-verkon WEP-avain voidaan selvittää.

Katso iwconfig-komennolla minkä niminen koneen WLAN-liitäntä on (esim. wlan0 tai eth1). Käynnistä WLAN-kortti monitorointitilaan. Vaihda alla olevista komennoista tarvittaessa WLAN-liitännän nimi (oletuksena wlan0). Kaikki alla olevat komennot tulee ajaa **ylläpitäjän oikeuksilla**.

\# **airmon-ng start wlan0**

On mahdollista (riippuu käytetystä WLAN-kortista ja sen ajurista), että edellinen komento luo erillisen monitorointiverkkoliitännän (esim. mon0), joten katso tarkasti edellisen komennon tulosteita. Varmista mahdollisen monitorointiliitännän olemassaolo iwconfig tai ifconfig -komennoilla. Jos edellinen komento loi erillisen monitorointiliitännän, käytä sen nimeä alla olevissa komennoissa wlan0 sijasta.

Käynnistä WLAN-verkon monitorointiohjelma.

\# **airodump-ng wlan0**

Monitorointiohjelmassa pitäisi näkyä ainakin yksi verkko, jonka ESSID on piilotettu. Tukiasemaan pitäisi olla käyttäjä liittyneenä ja heidän välillään pitäisi liikkua paketteja. Katso, mitä kanavaa kyseinen verkko käyttää. Sammuta monitorointi, painamalla Ctrl+C, ja käynnistä monitorointi uudelleen, mutta vain löytämälläsi kanavalla.

Huom! Komentoihin on merkitty kulmasulkeisiin (<, >) tieto, joka sinun tulee itse lisätä. Kulmasulkeita ei kirjoiteta komentoihin. Esimerkiksi alla olevaan komentoon sinun tulee korvata <kanava> -kohta löytämälläsi kanavan numerolla (1-13).

\# **airodump-ng -c <kanava> wlan0**

ESSID lähetetään WLAN-verkossa suojaamattomana, kun käyttäjä ottaa yhteyden WLAN-verkon tukiasemaan. Verkossa on jo käyttäjä, joten tämä käyttäjä pitää saada ottamaan yhteys tukiasemaan uudelleen. Sopivalla menetelmällä olisi mahdollista saada tukiaseman (bssid) purkamaan yhteyden verkossa olevan käyttäjän (station) kanssa. Toinen vaihtoehto on odottaa, kunnes jokin tietokone yhdistetään verkkoon, jolloin saadaan kaapattua verkon ESSID.

Pyynnöstä ohjaaja hiukan nopeuttaa ESSID:n paljastumista.

Ennen WLAN-liikenteen kaappauksen aloittamista varmista assistentilta, että olet löytänyt oikean, työssä käytettävän WLAN-verkon. Sammuta monitorointiohjelma (Ctrl+C) ja käynnistä WLAN-liikenteen kaappaus.

\# **airodump-ng -c <kanava> −−bssid <bssid> -w <tiedoston nimi> wlan0**

Komennossa <kanava> tarkoittaa seuratun WLAN-verkon kanavaa ja <bssid> tukiaseman MAC-osoitetta. Nämä tiedot löytyvät edellisen kohdan monitorointiohjelmasta.

Monitorointiohjelma näyttää, että WLAN-verkko käyttää WEP-salausta. WEP-salauksen murtamiseen tarvitaan noin 300000 pakettia, jos kyseessä on 40-bittinen avain ja noin miljoona pakettia, jos kyseessä on 128-bittinen avain. Kerää kaappausohjelmalla haluamasi määrä paketteja (lopettaa Ctrl+C) ja kokeile murtaa WEP-salaus. Jos pakettien määrä ei ole riittävä, voit jatkaa kaappausta aloittamalla uuden kaappauksen toiseen tiedostoon. Käytä mergecap -ohjelmaa kaappaustiedostojen yhdistämiseen.

Pura WEP-salaus ja selvitä WLAN-verkossa käytetty WEP-avain.

\# **aircrack-ng <tiedoston nimi>.cap**

Kun olet onnistunut selvittämään WEP-avaimen, sammuta WLAN-kortin monitorointitila. Jos sinulla oli käytössä erillinen monitorointiliitäntä, sammuta sekä monitorointiliitäntä että varsinainen verkkokortin

liitäntä.

airmon-ng stop wlan0

Q5: Mitkä ovat WLAN-verkon tukiaseman ESSID ja BSSID?

Q6: Mitä kanavaa WLAN-verkko käyttää?

Q7: Mikä WEP-avain WLAN-verkossa on käytössä?

Q8: Mikä on WLAN-verkossa olevan tietokoneen MAC-osoite?

Q9: Kuinka paljon paketteja keräsit, että onnistuit selvittämään WEP-avaimen?

3.2 Liity WLAN-verkkoon

Konfiguroikaa WLAN-yhteys koneelle. Muista vaihtaa komennoista wlan0 vastaamaan WLAN-verkkoliitännän nimeä, jonka aikaisemmin selvitit.

Kytke NetworkManger takaisin käyttöön ja yhdistä sillä löytämääsi langattomaan verkkoon. NetworkManager asettaa langattoman verkon parametrit ja pyytää IP-osoitetta DHCP-palvelimelta.

Mikäli pääsit verkkoon, avaa verkkoselain ja varmista, että pääset myös Web-palvelimelle (http://192.168.0.10).

Q10: Saitko DHCP-palvelimelta IP-osoitteen? Entä pääsitkö Web-palvelimelle? Jos et, niin minkä arvelet olevan ongelmana?

Kokeile muuttaa kannettavan tietokoneen, langattoman verkkokortin MAC-osoite vastaamaan selvittämääsi, toisen koneen MAC-osoitetta (esimerkissä 01:23:45:ab:cd:ef). **Ota alkuperäinen MAC-osoite talteen (käytä ifconfig-komentoa)!**

ifconfig wlan0 down
ifconfig wlan0 hw ether 01:23:45:ab:cd:ef
ifconfig wlan0 up

Kokeile tämän jälkeen yhdistää verkkoon uudelleen käyttäen NetworkMangeria.

Q11: Saitko nyt DHCP-palvelimelta IP-osoitteen? Ja pääsitkö Web-palvelimelle?

3.3 Kirjaudu Web-palvelimelle

Kirjautuaksesi Web-palvelimelle tarvitset käyttäjätunnuksen ja salasanan. Käytä sosiaalista tiedustelua selvittääksesi tarvittavat tunnukset ja salasanat. Laboratoriotyön assistentti kertoo kohdehenkilösi.

Kirjaudu Web-palvelimelle SSH-yhteydellä käyttäen saamiasi tunnuksia.

$ ssh *käyttäjätunnus*@192.168.0.10

Q12: Miten sait selvitettyä käyttäjätunnuksen ja salasanan? Mitkä ne olivat?

Q13: Epäonnistuiko joku yrityksesi? Mitä tapaa yritit ja miksi luulet sen epäonnistuneen?

3.4 Muokkaa Web-sivua

Mene Web-palvelimen kotisivuhakemistoon (/**var**/**www**/) ja muokkaa sieltä löytyvää **hacked.txt** -sivua. Lisää sivulle ryhmän jäsenten nimet ja päivämäärä ja kellon aika (esim. 01.10.2009 12:24 Matti Meikäläinen, Mikko Mallikas).

Käy kurkkaamassa Web-selaimella, näkyykö nimesi listassa.

3.5 Siivoa jälkesi

Poista Web-palvelimelta komentotulkin historia seuraavalla komennolla:

rm ~/.bash_history
history -c

Poista kannettavalta tietokoneelta kaikki tekemäsi kaappaustiedostot. Jos muutit kannettavan tietokoneen WLAN-kortin MAC-osoitetta, palauta se alkuperäiseksi. Lisäksi siivoa komentohistoria seuraavilla komennoilla:

rm ~/.bash_history
history -c

Kytke lopuksi NetworkManager takaisin käyttöön samalla tavalla, kuin alussa se kytkettiin pois käytöstä. Poista sen asetuksista löytämäsi Wlan-verkon tiedot.

4 Kysymyksiä

Vastaa työssä esitettyjen kysymysten lisäksi alla oleviin kysymyksiin ja palauta vastauksesi viikon kuluessa sähköpostitse osoitteeseen tietoturva@zouppen.iki.fi .

Q14: Mikä oli käyttämäsi työohjeen versionumero?

Q15: Mitkä asiat tai puutteet mahdollistivat ulkopuolisen henkilön tekemän Web-palvelimen sivuston muokkaamisen?

Q16: Mitä ja miten korjaisit työssä esiintulleet tietoturvaongelmat?

Q17: Miten työssä käytetty WLAN-verkko oli suojattu?

Q18: Laboratoriotyössä murretulle WEP-salaukselle on vaihtoehtoina WPA ja WPA2. Vertaile näitä eri vaihtoehtoja keskenään tietoturvallisuus näkökulmasta. Miten eri vaihtoehtojen perustoiminnallisuudet eroavat toisistaan? Kuinka tietoturvallisia vaihtoehdot ovat? Onko WPA tai WPA2 jo murrettu?