

Harjoitustehtäväkierros 3: Tietoturva ja televerkot

T-110.1100 kurssihenkilökunta

DL: Torstai 31.3.2011 18:00

Johdanto

Tällä tehtäväkierroksella pääset tutustumaan tietoturvaan ja televerkkoihin.

Tehtävässä 1 opit yhden mahdollisen tavan kiertää sovellustason liikenteen suodatus.

Toinen tehtävä on tarkoitettu syventämään ymmärrystäsi tietoturvasta. Järjestelmien tietoturvallisuutta on usein mielekästä arvioida tunnettuja tietoturvahyökkäyksiä vastaan. Tässä tehtävässä tutustut erääseen yleiseen tietoturvahyökkäysten luokkaan.

Kolmannessa tehtävässä joudut selventämään itsellesi mobiiliverkkojen toimintaa.

Neljännessä tehtävässä hypätään pois tietoturvan ja televerkkojen maailmasta. Tehtävässä pääset kurkistamaan tietokoneen konepellin alle.

Tehtävä palautetaan Rubyrin-järjestelmään kurssin Noppa-sivuilta löytyvien ohjeiden mukaisesti. *Kiinnitä huomiota palautuksen formatointiohjeisiin. Väärästä tiedostoformaattista tai merkistöstä sakotetaan pisteitä!*

1 SSH-putkitus (5p)

Kaverisi Ruohomutahevonen¹ on lähtenyt vaihtoon Gobin autiomaahan. Haluatte kaverisi kanssa Facebuukata keskenänne, mutta paha Jokirapu suodattaa Facebookin IP-alueet pois Gobin Internetistä. Jokirapu on kekseliäs ja tarkastelee liikennettä myös sovellustasolla, joten et voi käyttää yksinkertaista HTTP-välityspalvelinta (proxya). Olette Ruohomutahevosen kanssa molemmat Aallon opiskelijoita, joten päätät jeesata Ruohista valmistelemalla tälle ohjeet SSH:n yli tunneloidun SOCKS-proxyn tunneloimiseksi koneelleen.

¹http://en.wikipedia.org/wiki/Grass_Mud_Horse

- A Esittele kuinka konfiguroit SSH-klienttisi ottamaan yhteyden koulun palvelimelle (kosh, vipunen, kekkonen) ja samalla toimimaan SOCKS-proxyyna ja tunneloimaan liikennettä koulun palvelimen kautta. Esittele myös kuinka konfiguroit selaimesi käyttämään kyseistä yhteyttä. (3p)
Vinkkejä: asiasta löytyy monia ohjeita netistä. Selaimena kannattaa käyttää Firefoxia, koska sen välityspalvelinasetukset ovat helpompia asettaa kuin esim. IE:n tai Chromen.
- B Mikä on SOCKS? Voisitko ohjata muitakin ohjelmia (vaikkapa ftp-klientin tai Spotify-klientin) käyttämään samaa tunnelia. (2p)

2 MITM (4p)

Yksi yleisimmistä tietoturvahyökkäyksistä on niin kutsuttu Man in the Middle (MITM)-hyökkäys, jossa Mallory on Alicen ja Bobin välissä ja teeskentelee Alicelle olevansa Bob ja Bobille olevansa Alice.

- A Miten voisit hyökätä verkkopankissa olevaa tietoa kohtaan Man in the Middle-hyökkäyksellä? Hyökkäyksen ei tarvitse olla tekninen. (2p)
- B Avaa verkkopankkisi kotisivu. Miten voit varmistua olevasi yhteydessä suoraan pankkiin etkä johonkin välikäteen? (2p)

3 Puhelinverkko (6p)

Haluat soittaa VoIP-puhelun kaverillesi kännykkääsi asennetulla Skype-ohjelmalla. Kaverillasi ei kuitenkaan ole kännykässään asennettuna Skypeä, joten hänen päähänsä Skype-puhelu välittyy normaalina puheluna. Kaverisi asuu ulkomailla, joten sinun ja kaverisi puhelimet ovat eri UMTS-verkkojen alueella.

Selosta minkä UMTS-verkon osien kautta puhelu välittyy kummassakin päässä. Voit olettaa, että puhelu muuttuu IP-datasta normaaliksi puheluksi jossain puhelinverkkojen välissä. (6p)

4 Komponentit ja liittimet (5p)

- A Hae kuva osoitteesta <http://www.niksula.hut.fi/~pakoivis/T-110.1100/komponentit.png> ja tunnista kuvasta numeroidut komponentit.

- B Hae kuva osoitteesta <http://www.niksula.hut.fi/~pakoivis/T-110.1100/liittimet.png>. Kuva on otettu tavallisen PC-koneen takaa. Tunista kuvasta numeroidut liittimet. Mainitse jokaisen liittimen yhteydessä muutama esimerkki liittimiin tyypillisesti kiinnitettävistä laitteista. Mikäli liitin on tarkoitettu täsmälleen yhdelle laitetypille, yksi esimerkki riittää.

Materiaalia

- <https://noppa.tkk.fi/noppa/kurssi/t-110.1100/etusivu> Kurssin kotisivut
- <http://www.cse.tkk.fi/Tietoliikenne/Opinnot/Ohjeet/> T-110 -kurssien yleisiä ohjeita
- <http://opetuki2.tkk.fi/p/top/> Teekkarin ohjauspakki
- Internetin hakupalvelut (jos et löydä, googlaa)