Tietoliikenteen harjoitustyö, ohjeistus

Timo Karvi

21.1.2016

Sisältö

- Yleiskuvaus
- Dokumentointiohjeet
- Viikkoaikataulu
- Loppuraportointi ja posteri
- Wireshark

Yleiskuvaus

- 3. periodi.
- Oma tutkimusaihe.
- Itsenäinen tutkimus ja sen raportointi.

Dokumentointiohjeet

- Kirjalliset työselostukset kaikista vaiheista:
  - Mitä tehty, miksi,
  - mitä vaiheita liittyi, yms.
  - Tuntikirjanpito.
- Palautetaan heti vaiheen päätyttyä.
- Yleisohje: kirjoita muistiinpanot itselle tulevaa tarvetta varten.
  - Pituus ei ole tärkeä.
  - Toimenpiteiden dokumentointi sen sijaan on.

Viikkoaikataulu

Viikko 1: Analysointityökalun peruskäyttö ja oman tutkimusprojektin suunnittelua

Viikko 2 : Klusterissa toimivan virtuaalikoneen liikenteen analysointi ja lyhyt suullinen esitys (2-5 min) ajatuksista omaksi tutkimusprojektiksi

Viikko 3: Oman tutkimusprojektin (analysointitehtävän) kirjallinen kuvaus: Mitä tutkitaan ja miten

Viikko 4 : Oman tutkimusprojektin datan keruu, ensimmäisiä ideoita posteriin laitettavaksi

Viikko 5 : Oman tutkimusprojektin kerätyn datan analyysi, posterin ensimmäinen luonnos

Viikko 6 : Oman analysointitehtävän viimeistelyä ja dokumentointi, posterin viimeinen versio

Viikko 7 : Posteritilaisuus to 3.3. klo 14-16. KAIKKI PAIKALLA VIIMEISTÄÄN 12:00!!!

Loppuraportti ja posteri

- Mikä on posteri?
- Posterin ulkoasu?
- Posteripohjia voi etsiä yliopiston logodomainista, linkki tänne on mm. laitoksen hallinnon lomakkeet-sivulla.
- Millä teen: Taitto-ohjelma tai vaikkapa powerpoint.
- Miten tulostan: Adobe Reader (windowsissa) osaa tulostaa paloina A3 arkeille.

1. viikon tehtävä: Wireshark

- Kertaa TilPen sisältö protokollien ja kerrosrakenteen osalta.
- Opettele käyttämään wireshark –ohjelmaa.
- Mieti/kehitä oma tutkimusongelma!
- Analysoi vaikka esimerkkidata smtp.pcap (tai mikä tahansa muu): Mitä sanomia? Mitä tietojen viestin kentissä on? Mitä niistä voi päätellä?
- Käytä suodattimia, laadi graafeja: Tee ainakin yksi oma suodatin ja kokeile erilaisia visualisointivälineitä

1. viikon raportti

- Wireshark asennus (jos joudut tekemään sen)
- Wireshark peruskäyttö (jos opettelet sitä)
- Wireshark tehokäyttö
- Wireshark näyttösuodattimet (display filter): Dokumentoi kokeilut ja tee yksi oma ja dokumentoi sekin.
- Wireshark graafit: Kokeile niistä kahta erilaista. Mitä niistä näkee?
- Palautus sähköpostitse su 31.1. klo 24.00 mennessä!

Oma tutkimus ja sen sunnittelu

Hyvä aihe: Mitataan liikennettä jotain tarkoitusta varten

- Mitä halutaan selvittää?
- Mitä protokollia tutkitaan?
- Millainen analyysi: Aikasarja, sanomien lkm, data määrä, jotain muuta.
- Taustatietoja posteriin ja analyyseihin, myös lähdeluettelo ja viittaukset lähteisiin.

On myös mahdollista kokeilla jotain hyökkäystä omassa kotiverkossa ja testata erilaisia tapoja torjua hyökkäys.

Viikko 2: Klusterikoneen tai pilven virtuaalikoneen liikenteen analysointi

- Tehtävän vaiheet:
  1. Kerää liikennettä annetulta koneelta. Joudut itse tuottamaan analysoitavan liikenteen.
  2. Siirrä analysoitavaksi muualle ja tee analyysi.
  3. Toista tarvittaessa, jos yllätyksiä.
- Raportti: Toimintaohje
  - Yksityiskohtainen toimintaohje jollekin muulle, joka voi toistaa tehtävän.
  - Kirjaa siis komennot ja niiden selitykset.