# Case 3. Tietomurron analysoiminen

Tämän tehtävän tekemisessä on käytetty luvallisesti ENISAn Tietoverkkoforensiikkaa käsittelevän kurssin materiaalia ja tiedostoja. Niitä on muokattu sopivampaan muotoon, tehty tiedostoista otteita ja lisätty tehtävää täydentäviä itse tehtyjä tietoja sekä tiedostoja.

Kaikki tehtävässä esitetyt nimet, yritykset, järjestelmät, jne. ovat mielikuvituksen tuotetta.

# Tehtävä

**Tehtävänä on analysoida eräs tietomurto. Analyysin perusteella sinun tulee tehdä kuvaus tapahtuneesta, laatia aikajana sekä muutama ohje, mitä toimia tulisi ensimmäiseksi nyt tietomurron jälkeen.**

Lue läpi alla oleva skenaario ja tee sen jälkeen analyysi pohjautuen skenaarioon ja siihen liittyviin annettuihin tietoihin. Tehtävän tekemiseen tarvitaan Wireshark-ohjelmisto pcap-tiedostojen analysointiin. Muu tarvittava tieto on tässä tehtävänannossa (kuvina, linkkeinä, tekstinä, tiedostoina jne). Lisäksi lisätietoja voi ja kannattaa hakea vaikka googlettamalla.

Tehtävänannon lopussa esitetään useita kysymyksiä. Niihin vastaaminen ei ole välttämätöntä tehtävän suorittamisen kannalta mutta se voi auttaa tekemisessä. Muutoinkaan tehtävänannossa tietoja ei esitetä missään tietyssä järkevässä järjestyksessä vaan niitä on hyvä analysoida kokonaisuutena.

1. *Huom1. Analyysin ei tarvitse olla täydellisen aukoton. Nyt ei tehdä poliisitason tutkintaa vaan yritetään saada käsitys siitä mitä on tapahtunut = mahdollisimman hyvä “arvaus”*

1. *Huom2. Tehtävänannon absoluuttiset liikennemäärät eivät vastaa oikeata tilannetta mutta niiden muutokset on tehty sellaista havainnollistamaan.*

## Tehtävä tiivistetysti, ohjeet

1. Tutustu skenaarioon huolella ja muodosta yleiskuva tilanteesta
2. **Luo aikajana tapahtumista**
3. Tee lyhyt kuvauskyberuhkasta: mitä on tapahtunut?
4. Anna kaksi toimenpidesuositusta: mitä tulisi välittömästi tehdä?

## Käytetyt tiedostot

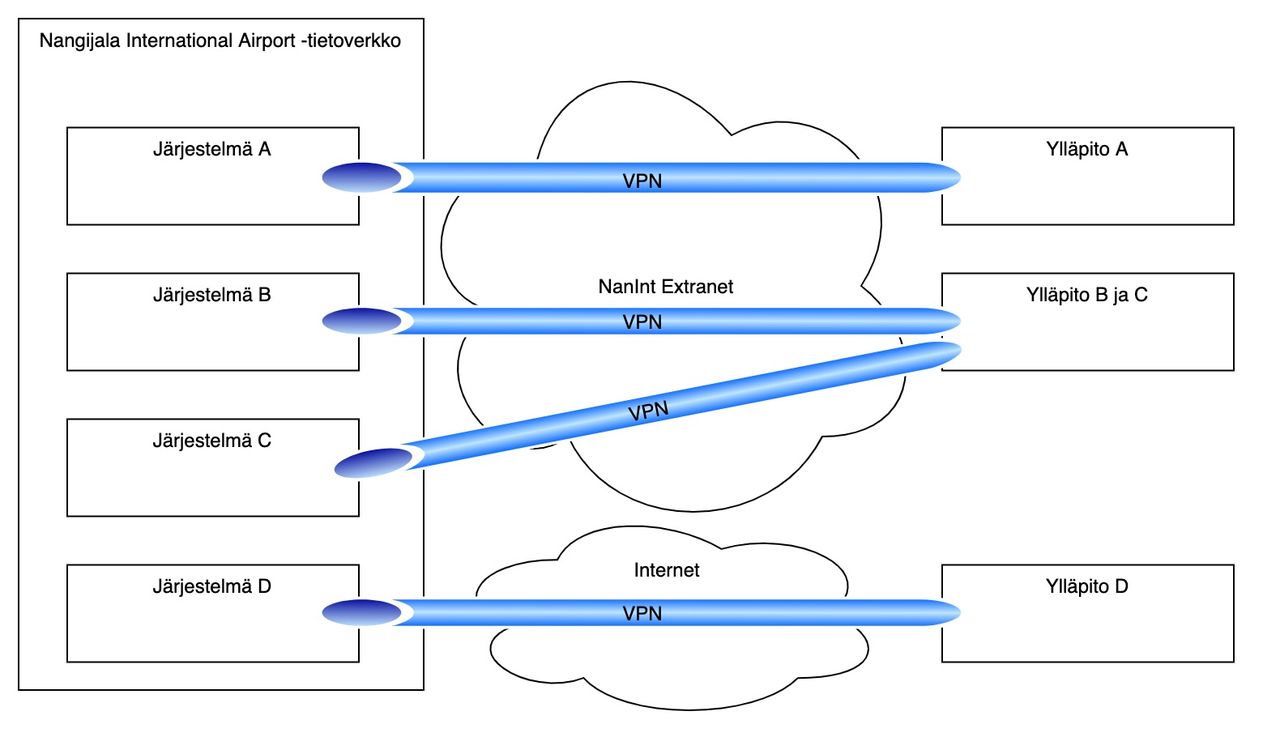
Oheisessa zip-tiedostossa on kaikki tehtävässä mainitut ja tarvittavast tiedostot:

<https://www.dropbox.com/s/x3wjmlt6cv2slyl/Case3_files.zip?dl=0>

# Skenaario

## Nangijala International Airport (NanInt)

Nangijala International Airport on kansainvälinen lentokenttä, kohtuullisen vilkas vaikkakin melko pienikokoinen kenttä. Kentällä on oma IT-osasto, joka vastaa kentän tietoverkon toiminnasta. Kentän verkossa on lukuisia erilaisia palveluita, joita ylläpitävät pääsääntöisesti järjestelmien toimittajat salattujen etäyhteyksien kautta. Alla on karkean tason arkkitehtuurikuva kolmansien osapuolten järjestelmien ylläpidosta:



Ulkoisessa ylläpidossa olevien järjestelmien etäyhteydet on toteutettu VPN-tunneloinneilla niin, että ylläpitoyhteydet ovat aina salattua liikennettä ja järjestelmiin saa ylläpitoyhteydet ainoastaan määritellyiltä laitteilta/verkoista.

1. *VPN = Virtual Private Network, tekniikka, jolla luodaan salattua datansiirtoyhteys kahden laitteen tai verkon välille.*

**Yksi tällainen ulkopuolisten toimesta ylläpidetty järjestelmä on lentokentän ilmoitustaulujen ohjaus-/hallintajärjestelmä  AirPortSys.**

## Kyberuhka realisoituu

Eräänä perjantaina, Nangijalan lentokentällä havaitaan sähköisen ilmoitustaulujärjestelmän toimivan omituisesti, ulkoisesti ehkä kunnossa mutta sisältö on vähän mitä sattuu:



NanInt-lentokentän tietohallintojohtaja on palkannut sinut konsultiksi selvittämään kokonaiskuva siitä mitä on tapahtunut.

## Taustatietoja ilmoitustaulujärjestelmästä

Ilmoitustaulujen ohjausjärjestelmä (AirPortSys) on ulkoiselta toimittajalta ja sen ylläpidosta vastaa HaiTek Ltd. HaiTek on ilmoittanut, että AirPortSys-järjestelmää on päivitetty edellisenä työpäivänä mutta päivityksen ei olisi pitänyt vaikuttaa sisältöön vaan ainoastaan monitorien tiedon esitysasuun. HaiTekilla ei ole täyttä varmuutta siitä, kuka ylläpitäjistä (Peter Sunshine, Vicky Lily vai Tahvo Terävä) on toimenpiteet tehnyt mutta ainoat yhteyden AirPortSys-järjestelmään on heidän toimitilojen koneilta ja heillä noudatetaan virastotyöaikaa 9-17.

HaiTekilla on omassa verkossaan monitorointijärjestelmä, joka seuraa verkon liikennettä sekä IDS-järjestelmä, josta generoituu hälytyksiä epänormaalista liikenteestä. Valitettavasti heillä ei ole ollut resurssia ylläpitää/seurata IDS-järjestelmäänsä reaaliajassa.

1. *IDS = Intrusion Detection System, järjestelmä, joka havaitsee verkkoliikenteestä tunnettuja haitakkeita  ja ilmoittaa niistä.*

Yritys on myös kerännyt lokitietoja järjestelmään tapahtuneista kirjautumisista omalle lokipalvelimelleen.

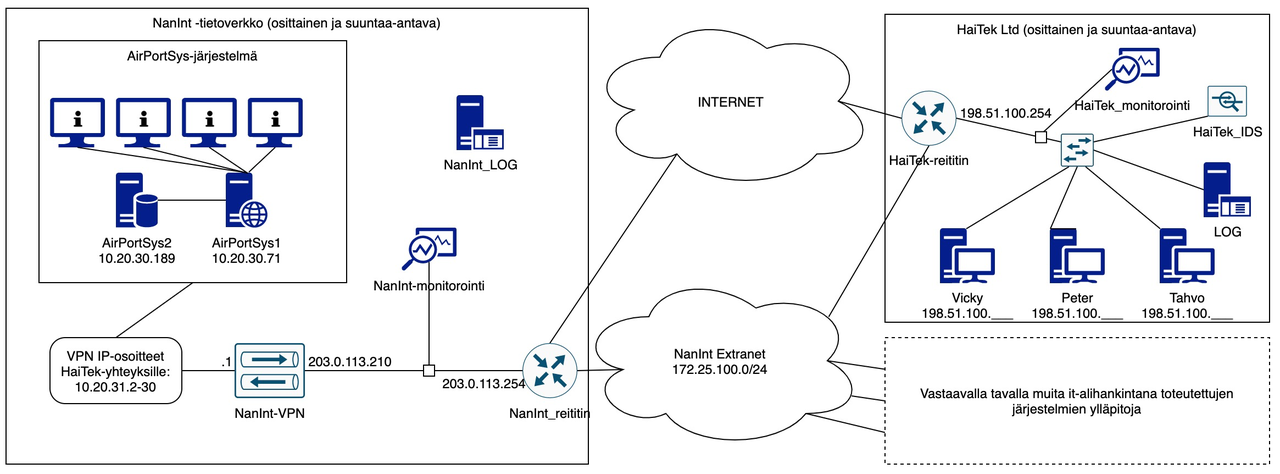
Sinun käyttöösi HaiTek on luovuttanut edellisen päivän monitorointidatan (HaiTek….pcap(, IDS-järjestelmän hälytykset (snort….jpg) ja AirPortSys-järjestelmän lokitiedostot (access\_log….txt).

## Lisätietoja NanInt -tietoverkosta

Nangijalan lentokentän verkossa on myös oma monitorointijärjestelmänsä ja lokitietoja on kerätty VPN-yhteyspisteeltä. Nämä tiedot on luovutettu käyttöösi (NanInt….pcap ja vpn\_log\_NanInt….txt)

## Tarkempi topologia

Yritysten asiantuntijoiden kanssa käytyjen keskustelujen pohjalta olette kyenneet luomaan alla olevan tarkemman kuvan verkon toiminnasta. Kuvasta käy selville kaikki ne verkon komponentit ja niiden väliset yhteydet, joilla on merkitystä tämän tehtävän kannalta (klikkaamalla saa kuvan suuremmaksi):



## Vinkkejä ja huomioita

1. Mitään taetta ei ole sille, että kaikki saadut tiedot on kattavia tai kuvat kunnossa.
2. Mitään taetta ei ole sillekään, että kellonajata on oikein saatikka synkronoidut.
3. Kannattaa pureskella ongelmaa pienempinä paloina (ei heti yrittää kaikenkattavaa ratkaisua). Yksityiskohtien kautta kohti kokonaisuuden ymmärtämistä.
4. Kaappaustiedostoissa on aika paljon paketteja. Sopiva suodattaminen on oleellinen tekijä. Mitä muuta tietoa Wireshark voisi antaa… Statistics-valikosta löytyy jälleen avaimia.

## Kysymyksiä

Alla on muutamia kysymyksiä helpottamaan tehtävän tekemistä sekä tuomaan vähän lisätietoja. Niihin vastaaminen (palauttaminen) ei ole välttämätöntä mutta tehtävän suorittamisessa voi käyttää niitä apuna (etsimällä tietoa vastauksena kysymykseen, voi saada selville monia muitakin asioita):

1. Millä ajanjaksolle kaikki tapahtumat sijoittuvat (pvm, klo)?
2. Kuka on onnistunut kirjautumaan, minne ja milloin?
3. Kuka on yrittänyt kirjautua onnistumatta, minne ja milloin?
4. Mitä ip-osoitteita tiedoissa esiintyy ja miksi?
5. Miltä laitteelta (IP-osoite) HaiTekin verkosta on ylläpitotöitä tehty?
6. Milloin VPN-yhteyksiä on auottu, milloin ne ovat menneet kiinni?
7. Mitä kaikki yhteyksiä laitteilla on ollut?
8. Mitä tietoa on järjestelmien välillä siirretty (saako sitä edes selville)? Milloin? Määrät ja suunta?
9. Tapahtuuko tiedonsiirrossa eri laitteiden välillä suuria määrällisiä muutoksia?
10. Mitä tarkoittaa termi “Supply Chain Attack”? Liittyykö se tähän skenaarioon?
11. Extrat:
    1. Mitä haavoittuvuutta hyödyntämällä on hyökkäys saanut alkunsa?
    2. Miten kyseiseen haavoituvuuteen liittyvä hyväksikäyttömenetelmä toimii?
    3. Mitä käyttöjärjestelmää HaiTek käyttää työasemissaan (tämän löytää pcap-tiedostoista mutta voi myös hyvin arvata skenaarion pohjalta)?

# Palautus

Palauta tekemäsi analyysi opintojakson palautuskansion kautta:

* Lyhyt kuvaus realisoituneesta kyberuhasta - muista kuvaukseesa riittävän yleinen taso
* Tarkempi aikajana tapahtumista
* Kaksi toimenpidettä, joihin kannattaisi välittömästi ryhtyä
* Jos teit työn ryhmässä, niin muista kirjoiuttaa palautukseen ryhmäläisten nimet

1. *Vinkki: aikajanan saa helposti office-työkaluilla, kun valitsee SmartArt → Process → Simple Timeline - toki muitakin työvälineitä saa käyttää.*

LOPPU