# Case 3. Analyzing a data breach

The material and files of ENISA's course on cyberforensics have been used with permission to complete this assignment. They have been modified to a more suitable format, extracts from files have been made, and self-made information and files have been added to complement the task.

All names, companies, systems, etc. presented in the position. are a figment of the imagination.

# Task

**The task is to analyze a data breach. Based on the analysis, you should make a description of what happened, prepare a timeline, as well as a few instructions on what to do first now after a data breach.**

Read through the scenario below, and then perform an analysis based on the scenario and the information provided. To do the task, you need Wireshark software to analyze the pcap files. Other necessary information can be found in this assignment (images, links, text, files, etc.). In addition, you can and should search for more information, for example, by google.

At the end of the assignment, a number of questions are asked. Answering them is not necessary for the performance of the task, but it can help in doing so. In any case, the assignment does not present the information in any particular reasonable order, but it is good to analyse it as a whole.

1. *Note1. The analysis does not have to be completely watertight. Now we are not doing a police-level investigation, but trying to get an idea of what has happened = the best possible "guess"*

1. *Note2. The absolute traffic volumes in the assignment do not correspond to the correct situation, but their changes have been made to illustrate such a thing.*

## Task in a nutshell, instructions

1. Study the scenario carefully and get an overview of the situation
2. **Create a timeline** of  **events**
3. Make a brief description of the cyber threat: what has happened?
4. Give two recommendations for action: what should be done immediately?

## Files used

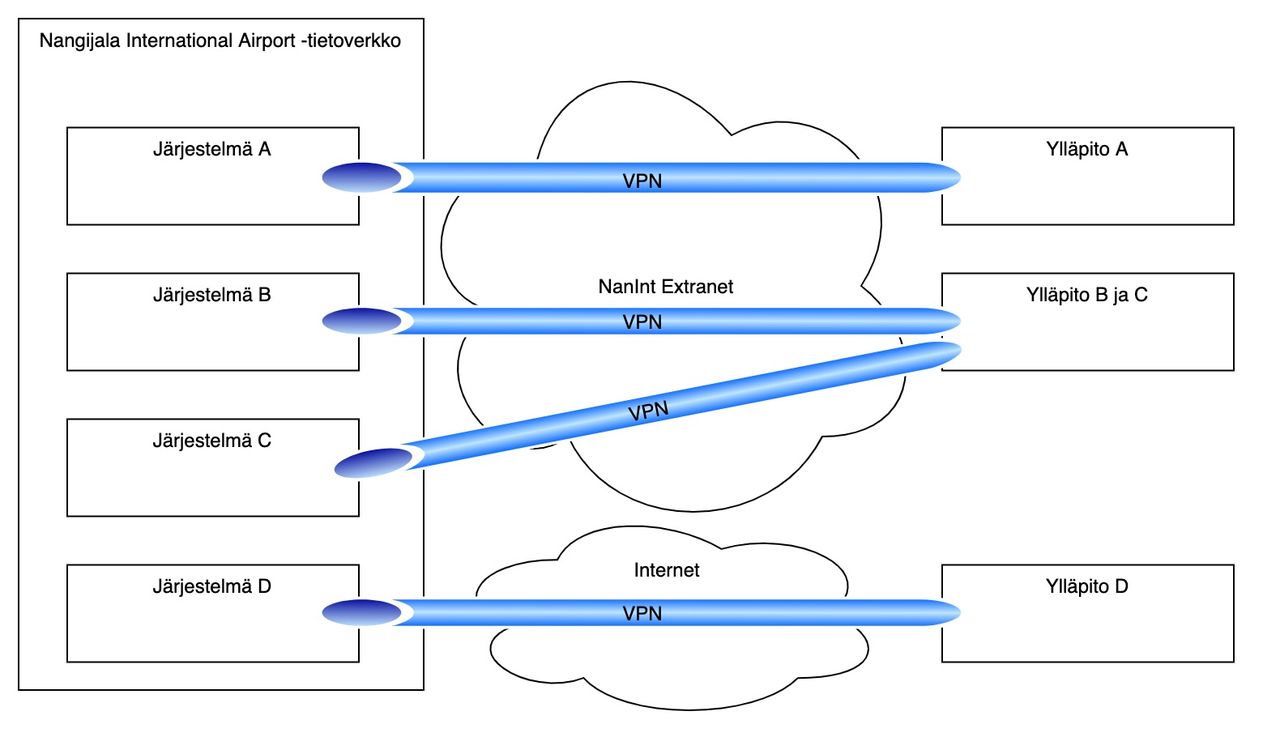
The following zip file contains all the files mentioned and needed for the task:

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

# Scenario

## Nangijala International Airport (NanInt)

Nangijala International Airport is an international airport, a reasonably busy although rather compact airport. The field has its own IT department, which is responsible for the operation of the field data network. There are numerous different services in the field network, which are mainly maintained by the suppliers of the systems through encrypted remote connections. Below is a rough-level architectural image of the maintenance of third-party systems:



The remote connections of the external maintenance systems have been implemented with VPN tunneling so that the maintenance connections are always encrypted traffic and the maintenance connections to the systems can only be obtained from specified devices/networks.

1. *VPN = Virtual Private Network, a technology used to create an encrypted data transfer connection between two devices or networks.*

**One such externally maintained system is AirPortSys, the airport bulletin board control/management system.**

## Cyber threat materializes

One Friday, at Nangijala Airport, we notice that the electronic bulletin board system is working strangely, outwardly maybe okay but the content is little what hurts:



The CIO of NanInt Airport has hired you as a consultant to find out the big picture of what has happened.

## Background information on the bulletin board system

The bulletin board control system (AirPortSys) is from **an external supplier and is maintained by HaiTek Ltd**. HaiTek has announced that the AirPortSys system has been updated the previous working day, but the update **should not have affected the content but only the presentation of the monitors' data**. HaiTek is not entirely sure which of the administrators (**Peter Sunshine, Vicky Lily or Tahvo Terävä**) has taken the measures, but the only connections to AirPortSys are from the machines on their premises and they observe office hours **from 9 am to 5 pm**.

HaiTek has a monitoring system in its own network that monitors network traffic and an IDS system that generates alerts about abnormal traffic. Unfortunately, they haven't had the resource to maintain/monitor their IDS system in real-time.

1. *IDS = Intrusion Detection System, a system that detects and reports known nuisances from network traffic.*

The company has also collected log data on logins to the system to its own log server.

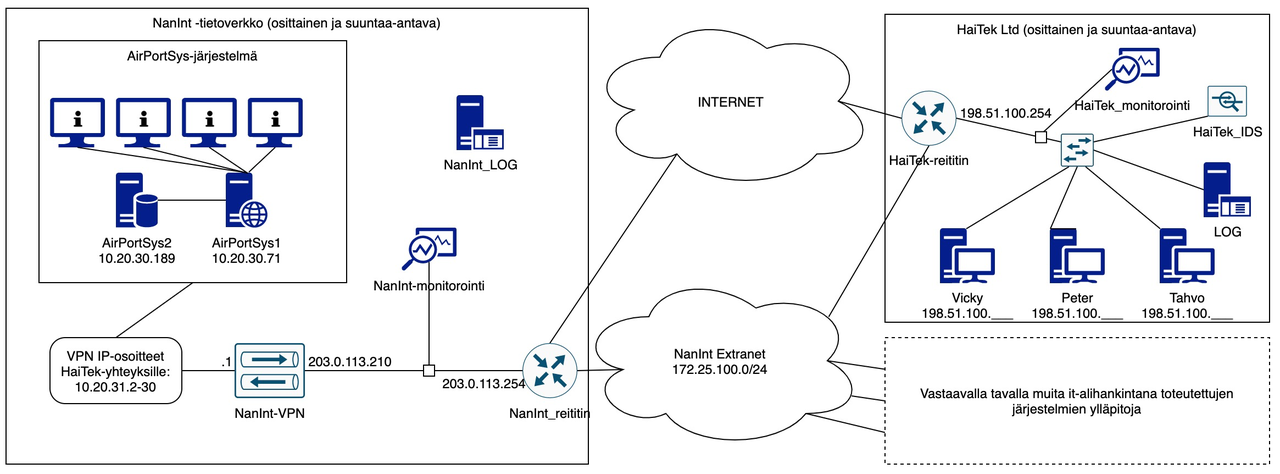
HaiTek has made available to you the monitoring data of the previous day (HaiTek....pcap(, IDS system alerts (snort....jpg) and AirPortSys system log files (access\_log....txt).

## Learn more about NanInt

Nangijala Airport's network also has its own monitoring system and log data has been collected from the VPN connection point. This information has been made available to you (NanInt....pcap and vpn\_log\_NanInt....txt)

## More detailed topology

Based on discussions with business experts, you have been able to create a more accurate picture of how the network works below. The figure shows all those components of the network and the connections between them that are relevant for this task (click to get a larger picture):



## Tips and considerations

1. There is no guarantee that all information obtained will be comprehensive or that the images will be in order.
2. There is no guarantee that the time will be correct, let alone synchronized.
3. It is worth chewing on the problem in smaller pieces (not immediately trying an all-encompassing solution). Through details towards the understanding of the whole.
4. There are quite a lot of packages in the capture files. Appropriate filtering is an essential factor. What other information could Wireshark give... In the Statistics menu, you can again find keys.

## Questions

Below are a few questions to make the task easier to do, as well as to bring a little more information. Answering them (reverting) is not necessary, but you can use them to help you complete the task (by looking for information in response to a question, you can find out many other things):

1. In what period of time do all events take place (date, at)? 26 July 2018
2. Who has managed to log in, where and when? Tahvo from 10.20.31.2 (first checked for root then admin) 22:38 via ssh
3. Who has tried to log in without success, where and when? Root and admin 22:37
4. What ip addresses appear in the data and why?
5. From which device (IP address) has maintenance work been done on the HaiTek network?
6. When have VPNs been opened, when have they closed?
7. What connections have all the devices had?
8. What information has been transferred between the systems (can you even find out)? When? Quantities and direction?
9. Are there major quantitative changes in data transfer between different devices?
10. What does the term "Supply Chain Attack" mean? Is it related to this scenario?
11. Extras:
    1. What is the source of the attack?
    2. How does the exploitation method related to the vulnerability in question work?
    3. What operating system does HaiTek use on its workstations (this can be found in pcap files but can also be guessed from the scenario)?

# Return

Return the analysis you have made through the course recovery folder:

* Brief description of the realized cyber threat - remember in its description a sufficiently general level
* A more detailed timeline of events
* Two measures that should be taken immediately
* If you did the work in a group, be sure to write the names of the group members in the restoration

1. *Tip: The timeline is easy to get with office tools when you select SmartArt → Process → Simple Timeline - of course, you can use other tools as well.*

END