# Network Security

## Project 1: Get to know log and ELK Stack

Instructor: Shiuhpyng Shieh
TA: Wei-Tung Tai, Li-Ren Zhang, Wei-Gang Sun
Email: TA@dsns.cs.nctu.edu.tw

**Due date: 23:59, October 20, 2020**

## 1 Project Description

The goal of this project is to introduce you to logs and ELK Stack environment. ELK Stack is an platform used to collect and analyze logs. By the end of this semester, you should be more familiar with logs and ELK Stack environment. In this project, you'll practice how to set up and use ELK to observe and analyze the logs.

## 2 Project Guide

1. **Environment:** Use Ubuntu Server 18.04LTS 64bit and Windows 10 operating system for this project. Ubuntu is for setting up ELK environment and Windows is using to reproduce logs of the scenarios and upload it to your Logstash. You can use your own computers or install new VMs, yet setting up a new VM is recommended since the logs will be fewer and easier to observe later. (You can find Ubuntu image at *https://www.ubuntu-tw.org/modules/tinyd0/* and Windows 10 image at university's FTP server : *ca.nctu.edu.tw.*)

   The minimum hardware requirements for Ubuntu,

   (a) Memory 4G (Recommend 8G for better fluency)

   (b) Hard disk 40G

   (c) Swap space 4G

2. **Tools you need to install:**

   (a) Ubuntu

      i. Docker:
      *Docker* is a tool which provides the way to create, manage, and deliver container applications.

      ii. ELK Stack:
      "ELK" is the acronym for three open source projects: Elasticsearch, Logstash, and Kibana, and it is used to collect, search, analyze logs. We will provide the docker files for you to set up your ELK stack more easily. The link of the files is
      *https://drive.google.com/uc?id=1i8d_sqoEe226EjuxkSKnzOh8Xc5Hmt-b&export=download*

   (b) Windows

      i. Winlogbeat:
      *Winlogbeat* is a Windows specific event-log shipping agent installed as Windows service. It can be used to collect and send event logs to one or more destinations, including Logstash.
      *https://www.elastic.co/downloads/beats/winlogbeat*

   ii. PACKETBEAT:
   *Packetbeat* is lightweight network packet analyzer that sends data from your hosts and containers to Logstash or Elasticsearch. *https://www.elastic.co/beats/packetbeat*

3. **Implement events and observe:** For this part, you are asked to reproduce 5 of the following scenarios and find the corresponding logs on ELK. Everyone's set of events is different, find your set in *NS_project1_sets.xlsx* which has been uploaded on the new e3 platform. Scenarios:

   (a) *Logon Success:*
   Sign in to your computer with your account name and password.

   (b) *Logoff:*
   Sign out.

   (c) *Screensaver invoked:*
   Turn on screen saver setting and invoke a screen saver.

   (d) *Screensaver dismissed:*
   Dismiss a screen saver.

   (e) *Open the specific application:*
   Open the calculator.exe.

   (f) *Close the specific application:*
   Close the calculator.exe.

   (g) *Create file:*
   Create a new file.

   (h) *Change file name:*
   Change a existed file's name.

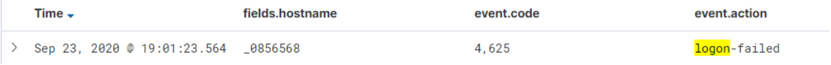
   (i) *DNS query:* You may use `nslookup` command to create the log. The domain is required to be *youtube.com.*

   (j) *Visit http website:* The website is require to be *http://www.fybus.com.tw/*

## 3 What to Submit?

A report in PDF format, contains:

1. Part A
   - (a) The correspondences between scenarios and logs(images and descriptions).
     - i. Image: Screenshot the fields of the log which can show its correspondences with the scenario(The fields you choose should be able to show the relation between the log and the scenario.)**on the Kibana interface**. The screenshot is required to contain the two fields, <fields.hostname>and <event.code>, and the name of fields.
       In addition, set the <fields.hostname>to your student id with a underscore at the front(ex. _studentID) when you upload your log. There is a example of how to screenshot a log below.

       | Time | fields.hostname | event.code | event.action |
       |---|---|---|---|
       | Sep 23, 2020 @ 19:01:23.564 | _0856568 | 4,625 | logon-failed |

     - ii. Description: Write down why you choose those fields, as detailed as possible.

     If your screenshots don't meet the rules mentioned above and the TAs can't understand the meaning of the image, you will not get the points.
   - (b) Continuing the last question, tell us how you find those correspondences. (such as the method, the observation...)
2. Part B
   - (a) Anything interesting you find or problems you encounter while you're using the ELK Stack. (This part will affect 30% of your score , so please don't leave it blank.)

## 4 How to Submit?

- Upload the PDF file named by "<STUDENT_ID>.pdf" to the E3 platform.

**The penalty for late submission is 10% per day, and 10 points will be deducted for handing in wrong file format.**