Network Security Project1

Get to know log and ELK

Instructor: Shiuhpyng Shieh

TA: 13m0n, Tori, Liren

What is Log?

- Log is the automatically produced and time-stamped record of events from applications.
- Log is the source for finding things that happens behind the scenes.
- Types of log:
  - System log
  - Network log
  - Application log

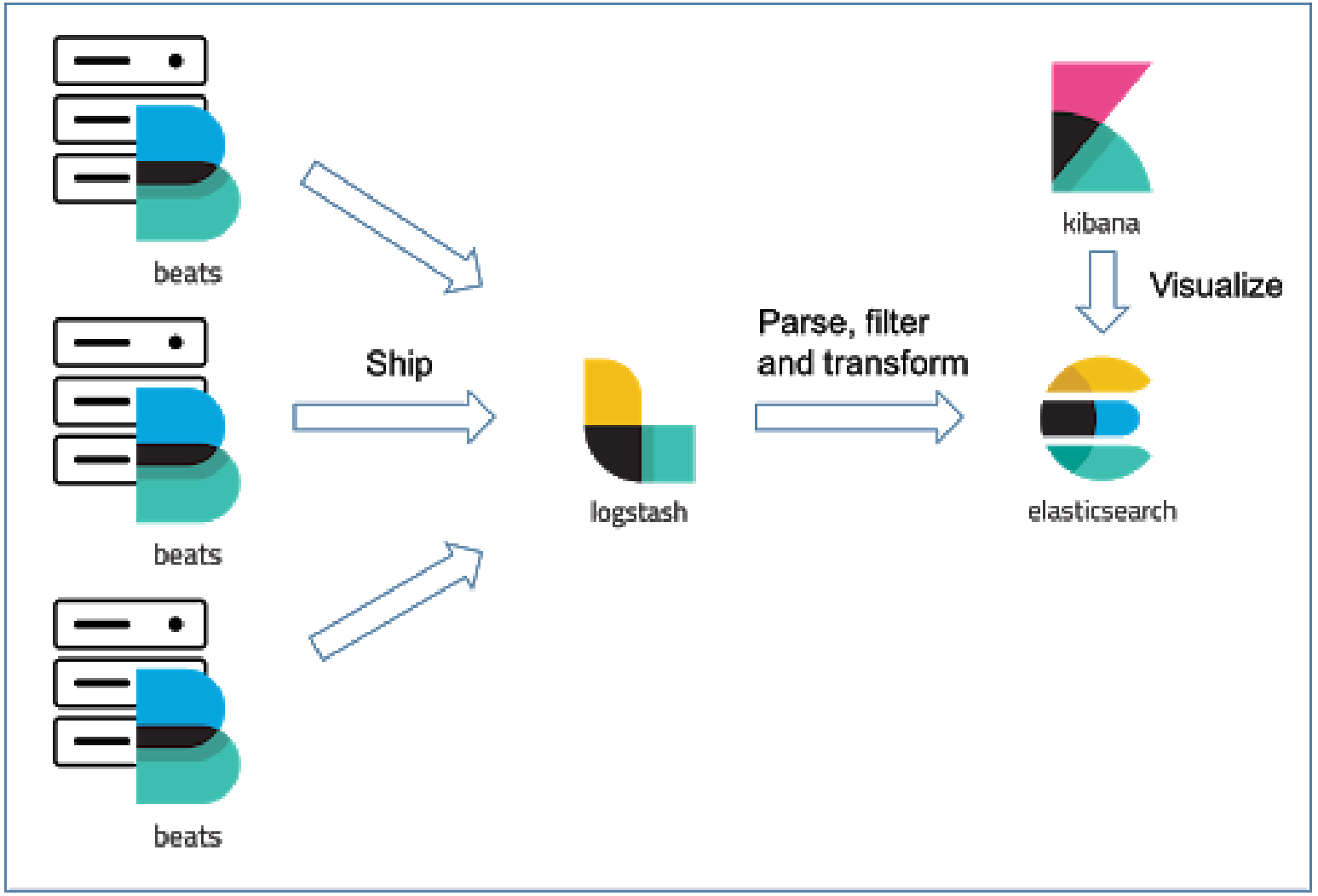
Why do we need Log?

- We need logs for that they hold information that can’t be found anywhere else.
- Things we can do with log data:
  - Alarm System
  - Forensic
  - User Behavior Analytics

What is ELK Stack?

- ELK is the acronym for three open source projects:
  - Elasticsearch
  - Logstash
  - Kibana
- Beats is a platform for single-purpose data shippers.
  - Winlogbeat
  - Filebeat
  - Packetbeat

ELK Workflow



The Goal of the project

- To get to know log and ELK stack
- What you will have to do:
  - Set up your own ELK environment.
  - Upload logs to ELK.
  - Observe logs.

Scenarios

- You will be given 5 scenarios which are randomly picked out of 10 scenarios.
- Reproduce the scenarios on your Windows 10 and upload logs to your ELK. Find the log that fit your given scenarios and screenshot it in the form as specified in the spec.

Environment

- An Ubuntu Server 18.04 LTS 64bits for setting up your ELK.
- A Windows 10 for reproducing the scenarios and upload the logs to your ELK.

Ubuntu

- Version: Ubuntu Server 18.04 LTS 64bits.
- Minimum hardware requirements:
  - Memory 4G (Recommend 8G for better experience)
  - Hard disk 40G
  - Swap space 4G
- Tools you need to install
  - Docker
  - ELK Stack

Set up ELK with our docker files

- Get the docker files

```
$ wget --no-check-certificate 'https://drive.google.com/uc?id=1i8d_sqoEe226EjuxkSKnzOh8Xc5Hmt-b&export=download' -O elastic.zip
```

- Increase the virtual memory limit(You should run this command every time after rebooting)
  - `$ sudo sysctl -w vm.max_map_count=262144`
- Run the docker files (run in the folder elastic)
  - `$ sudo docker-compose up`
- When the 4 nodes are ready, you should be able to connect to your Kibana with a browser. Address: your_Ubuntu_IP:5601.

Windows

- Version: Windows 10
- Tools you need to install
  - Winlogbeat
  - Packetbeat

Report

A part:

- The correspondences between the scenarios and the logs(images and descriptions).
- How you find those correspondences.

B part:

- Anything interesting things you find or problems you encounter while you're using the ELK Stack.

Example of correspondence image

- Logon Fail

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

Submit

- Upload the PDF file named by “<STUDENT ID>.pdf” to the E3 platform.
- Deadline: 2020/9/29 ~ 2020/10/20 23:55
- The penalty for late submission is 10% per day, and 10 points will be deducted for handing in wrong file format.

Score

- Point distribution
  - 35 points for “The correspondences between logs and events”
  - 35 points for “How you find those correspondences”
  - 30 points for “Anything interesting you find or problems you encounter in setting up the environment”

Q&A

- Feel free to contact up if you have any question. You can post an issue on the github below.
  - **https://github.com/dsnslab/NetworkSecurity**
- Email: TA@dsns.cs.nctu.edu.tw
- Lab: EC622