Network Security Project 1

Analyzing logs with ELK

Instructor: Shiuhpyng Shieh

TA: Su-Xin Chong, Wan-Yu Chen, Tsung-Hung Wu,

Pei-Hsuan Hung, Zhong-Hao Liao

Outline

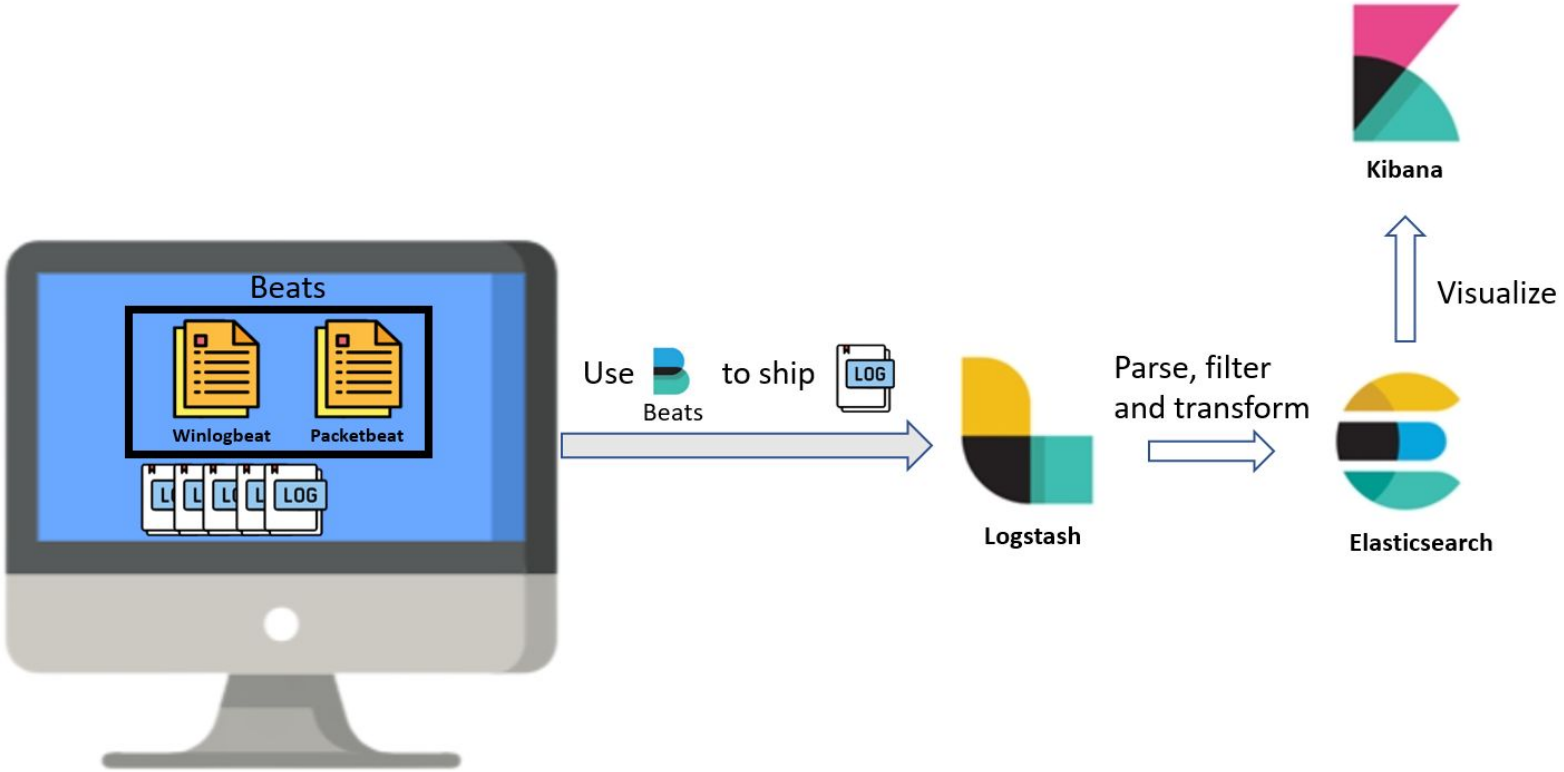
- Introduction to ELK Stack, Beats and other tools
- Goal of this project
- Project description
  - Scenarios
  - Tools & Environment requirements
  - Submission rules

ELK Stack & Beats

- Acronym for Elasticsearch, Logstash, Kibana

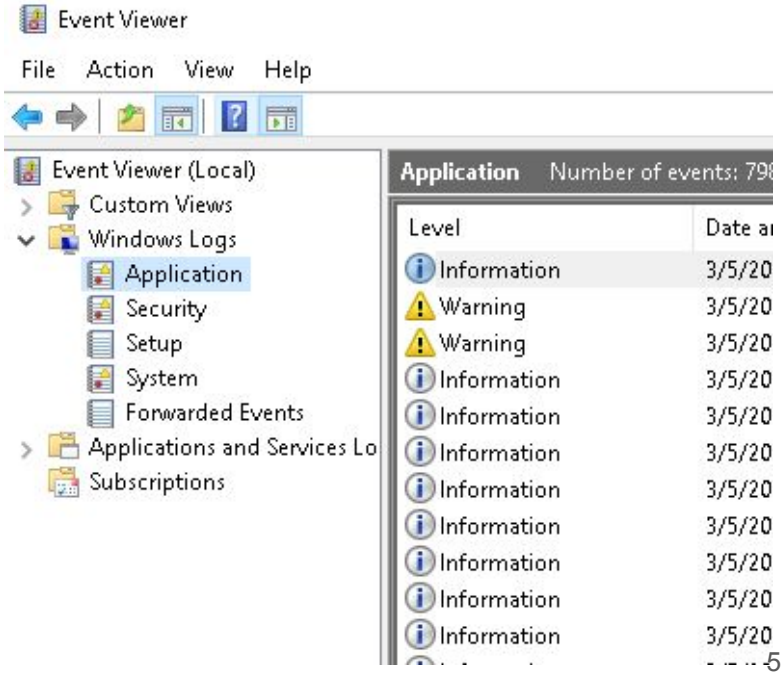
- Elasticsearch: RESTful, JSON-based **search engine**
- Logstash: **Processing pipeline** that ingests data from multiple sources
- Kibana: Flexible **visualization** tool
- Beats: **Data shipper** installed on machines
  - Winlogbeat: Ships Windows event logs
  - Packetbeat: Ships network data

ELK Workflow



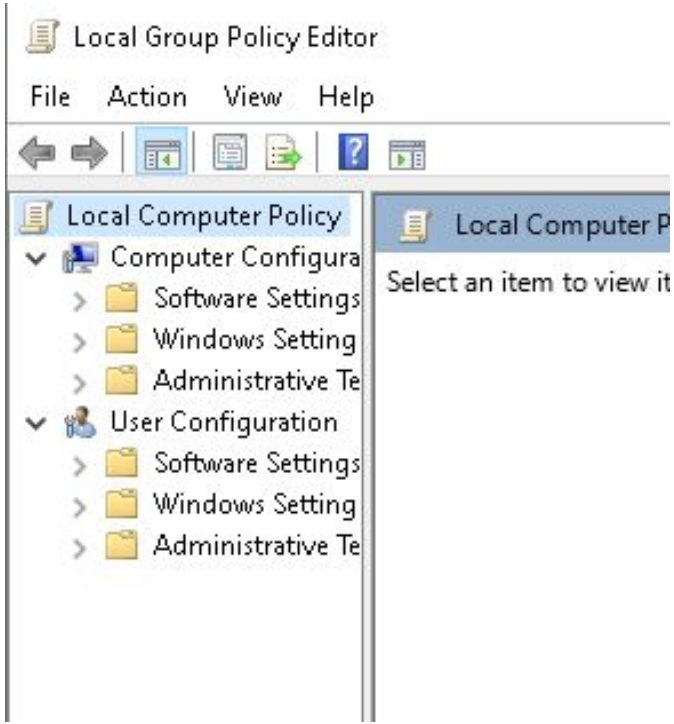
Event Viewer

- A tool to inspect Windows Logs locally (Not on Kibana!)
- Events are identified by Event IDs



Group Policy Editor

- What is Group Policy
  - Centralized management and configuration for operating systems
- Why do we need to edit group policy
  - Some events may not be recorded by default



Goal of this project

- Know how to configure Beats on your Windows machine
- Know how to upload and inspect logs on Kibana/Windows Event Viewer
- Be able to find out the correspondence between user’s behavior and the generated logs

Scenarios

- 7 scenarios (See Scenarios.xlsx)
- Reproduce the scenarios on the Windows machine and find out the corresponding logs on Kibana

Tools & Environment requirements

- Virtualbox (on host machine)
- Winlogbeat (on Windows VM)
- Packetbeat (on Windows VM)
- Minimum hardware requirements
  - 8 GiB of RAM (16GiB recommended)
  - 35 GiB of free hard drive space

Please refer to NS_Project1_vm.md for further details

Report

- Part A (70%)
  - The correspondences between the scenarios and the logs (including screenshots and descriptions) (35%)
  - The reason you connect the logs with the scenarios (35%)
- Part B (30%)
  - Any interesting things you've found or problems you've encountered while doing this project (30%)

Example Scenario

- Logon Fail

Every screenshot should contain **fields.hostname** and **event.code**

(Modify the configuration file to add this field)

Submission

- Upload a PDF file named "**<STUDENT ID>.pdf**" to E3 platform
- Deadline: 2021/3/30 23:55
- The penalty for late submission is 10% per day, and 10 points will be deducted for handing in wrong file format.
- Plagiarism is prohibited!

Steps to work on this project

1. Download **VirtualBox** and import the provided VMs
2. Download and configure **Winlogbeat** and **Packetbeat** on your Windows VM. Make sure logs are successfully uploaded to ELK stack.
3. Trigger the given scenarios and observe the logs that belong to the corresponding scenario.

Q&A

- Questions and answers for Project 1 from last semester
  - https://github.com/dsnslab/NetworkSecurity/issues?q=label%3A109-1-pj1
- Feel free to contact us via email or Github issue if you have any questions. (You are encouraged to discuss with other classmates in issues)
- Email: TA@dsns.cs.nctu.edu.tw
- TA Hour:
  - Mon. 13:00~15:00 @EC622
  - Tue. 13:00~15:00 @EC622