Network Security

Project 1: Analyzing logs with ELK

Instructor: Shiuh-pyng Shieh
TA: Su-Xin Chong, Wan-Yu Chen, Tsung-Hung Wu
Pei-Hsuan Hung, Zhong-Hao Liao
Email: TA@dsns.cs.nctu.edu.tw

Due date: 23:55, March 30, 2021

1. Project description:

The goal of this project is to introduce you to logs and how to use logs to analyze the events happening on your computer. After finishing this project, you will be able to analyze logs with ELK.

2. Project guide:

a. Environment:

You need two hosts with interconnection ability to realize the project scenarios.

To let your project go smoothly, we have provided you an open virtualization appliance (.ova) file, `netsec_pj1.ova` that contains two VM templates. One is an Ubuntu 20.04.2 VM with an ELK stack installed, and the other one is a Windows 10 Pro VM acting as an endpoint in an enterprise.

For this project, you will need to produce logs of specified scenarios at the endpoint, upload the logs to logstash, and analyze logs with ELK.

The minimum hardware requirements are as follows:

I. 8GiB of RAM (16GiB recommended)
II. 35GiB of free hard drive space

For more details about the given VMs, please refer to the VM document.

b. Tools you need to install:

i. Winlogbeat:

Winlogbeat is a Windows specific event-log shipping agent installed

as a Windows service. It can be used to collect and send event logs to one or more destinations, including Logstash.

Reference:
https://www.elastic.co/downloads/beats/winlogbeat

ii. Packetbeat:

Packetbeat is a lightweight network packet analyzer that sends data from your hosts and containers to Logstash or Elasticsearch.

Reference:
https://www.elastic.co/beats/packetbeat

c. Implementation and observation:

You are assigned to produce 7 scenarios then find the corresponding logs on ELK. The scenarios you have to reproduce are listed in "**Scenarios.xlsx**".

Scenarios:

1. Logon Success:

   Sign in to your computer with your account name and password.

2. Logoff:

   Sign out.

3. Screensaver invoked:

   Turn on the screensaver setting and invoke a screensaver.

4. Screensaver dismissed:

   Dismiss a screensaver.

5. Open a specific application:

   Open "calc.exe" (Windows built-in calculator)

6. Close a specific application:

Close “calc.exe”.

7. Delete a file:

   Delete an existing file

8. Modify a file:

   Add/Delete some content to/from an existing file

9. DNS query:

   You may use **nslookup** command to trigger a DNS query.

10. Visit website:

    The website is required to be “https://dsns.cs.nctu.edu.tw”

11. Change password:

    Change the user’s password

12. ICMP Echo request:

    Ping an IP address or a domain to generate a request.

13. Modify registry values:

    Keyword: regedit

14. Scheduled task:

    You can use the following command to create a scheduled task:

    “schtasks /create /sc minute /mo 1 /tn HelloFriend /tr notepad”.

3. What to submit?

Part A

a. Show the correspondences between scenarios and logs (including image and description) [35%, 5pts for each]

   i.Image:

Screenshot the logs on Kibana that you feel are associated with the scenarios. (The fields you choose should be able to show the relation between the log and the scenario)

Screenshots are required to contain at least these two fields, <fields.hostname>, <event.code> and the name of fields. <fields.hostname> should be set to your student id with an underscore at the front (_studentID, e.g. _0856568). The example field is shown below.

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

ii. Description:

Tell us how you find those correspondences. (such as the method, the observation...)

b. Following the previous question, wriite down the reason why you choose those fields. If your screenshots don't meet the rules mentioned above and the TAs cannot understand the meaning of the image, you will not get the points. [35%, 5 pts for each]

Part B

- Any interesting observations or problems you encounter while doing this project. [30%]

4. How to submit?

- Upload the PDF file named "<STUDENT ID>.pdf " to E3 platform.
- The penalty for late submission is 10% per day, and 10 points will be deducted for handing in the wrong file format.
- Plagiarism is strictly prohibited. In the case of plagiarism, students will receive zero points and disciplinary actions will be taken.