Network Security

Log Analysis

Instructor: Shiuh-Pyng Shieh
TA: Yung-Hao Li, Pin-Ching Chen, Tsung-Sheng Wang
Email: TA@dsns.cs.nycu.edu.tw

Due date: 23:55, May 31, 2022

1. Project Description

The goal of this project is to let you be familiar with log analysis with a hands-on exercise, and know what will really happen in a real world attack scenario. After this project, you should be able to inspect the network/system logs and figure out possible incidents that happened on your computer.

In this project, you are assigned with one scenario (see the homework description on E3), your task is to figure out the detailed incidents (e.g. IoC, timeline) and possible detection method (acceptable if you only describe the thoughts, thoughts with Proof of Concept is very welcomed).

All logs are uploaded to the Woodpecker platform for your convenience. Some basic usage is illustrated during the demo and in the slides, though you can still inspect the logs through text editor or other tools to your favor.

2. What to submit

1. Indicator of Compromise (IoC) (50%)

   Indicator of Compromise can be the IP of the attacker, filename, hash, e.t.c. For the minimum IoCs you need to figure out in different scenarios, please refer to Section 3.

2. Detailed timeline of the attack (20%)

   Plot the timeline of the attack, some necessary information is needed to get basic points (please refer to Section 3). Additional information related to the attack will result in a higher score.

3. Possible detection method (20%)

   Describe your findings related to the scenario, your answer can be some of (but not limited to) the topics stated below:

   - Your detection method
   - Which system/network behavior implies the attack
   - Which normal (benign) usage leads to false positives in your method
   - Proof of Concept (PoC) of your detection method

4. Feedback (10%)

3. Scenario information

a. Phishing

   In this scenario, the attacker sent an email with a malicious link. The victim then clicked the link, downloaded a malicious file and executed it. The malicious file then opens the RDP service.

   - IoC
     - Attacker’s IP and port
     - Malicious filename

        - Command that the malicious file executed
    - Timeline
        - Timestamp of the malicious file was downloaded.
        - Timestamp of when RDP was opened.

b. Exposed RDP with weak password and Discovery

   In this scenario, the attacker used brute force to try to login the victim’s computer through RDP services. After success, the attacker used some commands to discover some information about the computer.

    - IoC
        - Attacker’s IP address
        - Port of RDP Service
        - Command that execute for information discovery
    - Timeline
        - Start/End timestamp of RDP brute-forcing.
        - Timestamp of login.
        - Start/End timestamp of information discovery.

c. File Collection and Exfiltration

   In this scenario, the attacker discovered some sensitive data in the victim’s computer. The attacker then collected and stole them from the victim’s computer.

    - IoC
        - Attacker’s IP address
        - Filename of file being stolen
        - Port that attacker used to exfiltrate data
    - Timeline
        - Start/End timestamp of collection information that will be exfiltrated later.
        - Start/End timestamp of exfiltration.

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 hand in the wrong file format.
- Plagiarism is strictly prohibited. In the case of plagiarism, students will receive zero points and disciplinary action will be taken.