Network Security

Log Analysis

Instructor: Shiuh-Pyng Shieh
TA: Su-Xin Chong, Tsung-Hung Wu, Pei-Hsuan Hung
Email: TA@dsns.cs.nycu.edu.tw

Due date: 23:55, December 28, 2021

1. Project description

The goal of this project is to let you be familiar with log analysis with a hands-on exercise. 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 Scenario.xlsx for your assigned scenario), 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).

You can refer to the description of your scenario @ p.10-13 in the slides.

All logs are uploaded to the Kibana 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

Your submission should include a report in PDF format with the following contents:

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. Insider

- IoC
  1. IP address (victim's IP, insider's IP)
  2. Filename of sensitive resources (at least 3 files)
  3. Target filename of compressed sensitive data
- Timeline
  1. Start/End timestamp of anomalous RDP connection (e.g. Oct 10, 2021 @ 17:44)
  2. Time range when the insider collects sensitive data

b. Watering Hole

- IoC
  1. Attacker's IP address
  2. Compromised website URL
  3. C2 agent launcher
  4. Registry run key added for persistence
  5. Tools used for credential dumping, RDP and discovery
- Timeline
  1. Time range when the victim visits the compromised website till the C2 agent is installed in the victim's computer
  2. Timestamps of when persistence registry run key is added, and credential dumping
  3. Time range when the attacker is dumping credentials, performing lateral movement, discovery and data exfiltration

c. Phishing

- IoC
  1. Attacker's IP address
  2. Victim's IP address
  3. Filename of the attachment
  4. Filename of the downloader
  5. Filename of the ransomware
- Timeline
  1. Timestamp of the phishing attachment was downloaded.
  2. Timestamp of the ransomware was executed.

d. Exposed RDP with weak password
    - IoC
        1. Attacker's IP address
        2. Victim's IP address
        3. Filename of the ransomware
    - Timeline
        1. Start/End timestamp of port scan
        2. Start/End timestamp of rdp brute-forcing
        3. Timestamp of the ransomware was executed.

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.

========== Congratulations, you have found the Easter Egg! ==========

Tips

- Can refer to Event ID to look for specific action.
    - E.g. Event ID: 3, network connection detected.
    - Event ID: 4663, an attempt was made to access an object
    - Sysmon Events ID
- Keep track of the process that is used to compress sensitive data. (Insider)
- The compromised website is udn.com. (Watering hole)
- Credentials are dumped from memory. (Watering hole)
- Discovery is done with a command line Active Directory query tool. (Watering hole)
- Lateral movement is accomplished with a headless (non-GUI) RDP tool. (Watering hole)
- Attachment is a compressed file to evade detection and was extracted via Windows built-in function. (Phishing)
- The ransomware leverages a Windows built-in program to hide real parent process relationships. (Phishing & Exposed RDP with weak password)