Enterprise Cybersecurity
Project

Instructor: Shiu-Pyng Shieh
TA: Yung-Shiu Chen, Chen Lien
Email: t0856124.cs08g@nctu.edu.tw, s61176193388.iie08g@nctu.edu.tw

1. Project Description

The goal of this project is to reproduce the provided attack scenario and inspect logs generated by the actions of the attack then propose a possible detection method or algorithm to detect such an attack scenario.

2. Project Guide

I. **Attack Scenario**: Select an attack scenario from the list we provided on E3 platform (the "Spec" file). Each attack scenario is used by at least one attack group, and you need to reproduce the attack scenario according to the requirements that list under each attack scenario.

II. **Environment**: For some attack scenarios we will provide Virtual Machine. For the rest of scenarios, you need to use either Virtual Machine on your computer or AWS cloud platform to create the environment.

III. **Tools you need**:

(a) On victim's host (Windows)

i. Wireshark (For monitoring network activities):
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

ii. Windows event viewer (For monitoring system activities):
Event Viewer is a component of Microsoft's Windows NT operating system that lets administrators and users view the event logs on a local or remote machine.

(b) On attacker's host

i. Attack tools like C&C server depend on the attack scenario (feel free to use any open source tools or implemented by yourself).

3. What to submit

I. A ppt for presentation

- The content of the ppt needs to include:
  1. Attack scenario introduction.
  2. How you reproduced the attack scenario. (tools, how it works or how you implemented)
  3. Observed activities. (according to Wireshark and Windows event viewer)
  4. Possible solutions to detect such an attack scenario.

II. A report

- A detail report containing:
  1. Attack scenario introduction.

2. How you reproduced the attack scenario. (tools, how it works or how you implemented)
3. Observed activities. (according to Wireshark and Windows event viewer)
4. Possible solutions to detect such an attack scenario.

III. The code for reproduction

- The code that you implemented or open source code for reproducing the attack scenario.

IV. (Bonus) The code for detecting the attack scenario

- The code that you implemented to detect the attack scenario

4. How to Submit

- **The ppt**
  - Due date: Midterm Exam
  - Upload the ppt to the new E3 platform
- **The report and code**
  - Due date: Final Exam
  - Upload the "<Student ID>.zip" file containing the report and code
    - The structure needs to be:

```
<Student ID>
 |-<Report>
   |-report.pdf
 |-<Code>
   |-code
```