CS5321 Network Security Mini-Project

Daisuke MASHIMA

2022/23 Sem 2

Type 1 Mini-Project

- Includes 2 tasks. Please complete **BOTH**.
- **Individual** project
- 18 point max

- Deadline
  - Project report: **16 April 2023** (Sunday before Reading Week)
  - Project report (5-10 page) should include:
    - Procedure (including description about tool, code, packet filter conditions, etc.)
    - Summary of findings (including figures and/or tables)

Task 1: Honeypot traffic analysis

- Study real-world honeypot data (network traces same as Globecom 2019 paper)
  - Can use Wireshark (and any other tool, such as Zeek, Snort)
  - https://www.illinois.adsc.com.sg/softgrid/honeypot
- Sub-Task 1 **[2pt]**: Pick 1 country dataset (1-month or longer duration) and show summary statistics
    - Histogram or table of each field (source, target service, protocol, etc.)
    - Also briefly discuss the findings in one paragraph.
- Sub-Task 2 **[2pt]**: Pick 2 country dataset (1-month or longer duration) and show statistics related to correlation and dynamics, for instance:
    - Correlation in terms of daily/hourly packet count, data size, etc.
    - The number of source IPs that appear both, and changes over time
    - Also briefly discuss the findings in one paragraph.
- Sub-Task 3 **[3pt]**: Find attack attempts for one (or more) country dataset(s) and explain details (can use open-source IDS etc.)
- Sub-Task 4 **[3pt]**: Discuss how the findings can be used for tuning/configuring cybersecurity tools (no implementation is needed)

Task 2: APT Network Trace Analysis

- Study a synthetic network trace including APT (advanced persistent threat).
  - https://uillinoisedu-my.sharepoint.com/:f:/g/personal/dmashima_illinois_edu/EnaegzQJWytBu9UiMBHKLZAB9MmDCiE9TxEKAWuFA6WnVw?e=y7wD6F
- Assume this network trace is captured in a small-scale office network. The network involves 4 machines (192.168.x.x). The trace includes legitimate, normal activities too. Your analysis does NOT need to decrypt TLS communication.
- Sub-Task 1 **[2pt]**: Please list external servers that the office machines communicated. Please collect information who they are. You can use external services or tools.
- Sub-Task 2 **[3pt]**: Please identify which machine was compromised by a malware. Also briefly explain why you think so.
- Sub-Task 3 **[3pt]**: Please explain what malware did after compromising a machine. Your discussion can be focused only on what is visible in the network trace.