Exercise 1 (E1)

Attack Taxonomy and Cybercrime Organization

Part 1: Autonomous Research Activity

Objectives

The objectives of part 1 of E1 are:

- Create teams and know each other (background, skills, interests or the different members of the team).
- Organize working team: choose a representative, identify available assets (laptops, OSs), define other requirements/constraints that might affect collaborative work.
- Find available documents, resources, and tools providing an attack taxonomy (classification), i.e. enumerating and describing the characteristics of attacks and classifying them by dimensions such as impact, target, source, vulnerability, and vector of attacks for better understanding and analysis.
- Identify and describe the main characteristics of cybercrime actors: cybercriminals and organizations against cybercrime.

Statement

1. Create **teams of 3 or 4, following lecturer instructions and constraints.** For the sake of a simpler organization, designate a **representative** that will be doing specific tasks on behalf of the group, such as submit deliverables and reports.
2. Send an email to marc.ruiz-ramirez@upc.edu and marc.catrisse@upc.edu. indicating:
    a. The number of lab group: 11, 12, or 13
    b. The list of team members (name and surname/s)
    c. The name of the representative
3. Take some time to know each other and identify the strong and weak points of each member (background, skills, interests). Focus on cybersecurity background and skills.

4. Do exploratory research to find an **attack(threat) taxonomy**. Explore several available alternatives and choose the one that you thing is clear, exhaustive, and well-organized and structured. Combine inputs from different sources.

   Hint: a good taxonomy should be first organized into categories, and for each category, the different attacks should be enumerated and several attributes listed, such as:

   a. Brief description
   b. Are well-known attacks or emergent ones?
   c. Identify targets, sources, vectors
   d. Which pillar/s they aim at affecting: confidentiality, availability, integrity?
   e. Which vulnerability they aim at exploiting?
   f. Additional characteristics such as risk, impact
   g. Did you know this attack/threat before this doing this activity?

5. Investigate about **cybercrime landscape**, facing the topic from the two main sides of the story. On the one hand, try to find **how cybercriminals are organized**, what are their main targets, and motivations, what are the most common “modus operandi”. On the other hand, identify and enumerate the main **organizations fighting against cybercrime**, in a word-wide and/or national scope. Are they specific to cybercrime or are part of generic security bodies? Are they fighting against any potential threat or are specific to protect some specific targets from some specific attacks?
6. Decide the best way to collect and organize the obtained information in the form of a report. Use supporting resources such as figures and/or tables to improve readability and presentation. Name this file **E1_Part1.** Include in the final page/s, the list of sources (citations, URL links) you used.

Delivery

E1_Part1 report will be delivered after finishing part 2 of E1, jointly with **E1_Part2** report. So, save the file and keep it for upcoming delivery.

Aspects that will be positively evaluated during correction of **E1_Part1** are: capacity of summarizing and processing information from different sources. Critical analysis on the provided contents (disparity among team members, if any, can be reported). Use of high impact sources (high-quality articles from well-known institutions/bodies). Clarity in the organization and presentation of the report.

Supporting Material

N/A