CSUS, College of Engineering and Computer Science

Department of Computer Science
CSC 154 – Computer System Attacks and Countermeasures

Group Projects
(Mid-term report due date: week 7's Friday 11:59pm)
(Final report due date: last week's Friday 11:59pm)
(PPT due date: class presentation time)

Purpose:

1. To offer the students opportunities to gain beyond-class experience in exploring some incidents of network intrusions and cyber security defense.
2. The students are expected to practice more knowledge, experience or skills that are covered or not covered in class.

Topics: Each group will be responsible for **hands-on** investigation and exploration on any cybersecurity topic. The following is just a growing list for your reference.

1. Blockchain and cybersecurity/privacy
2. Drones and cybersecurity;
3. Smart city and cybersecurity;
4. Internet of things;
5. Intelligent transportation (such as autonomous driving) and cybersecurity;
6. Smart grid communication protocols, vulnerabilities, hacking tools;
7. Intrusion detection system;
8. Intrusion prevention system;
9. Virtualization and cybersecurity;
10. Bank security, ATM hacks;
11. Attack graph techniques;
12. How to discover and kill a botnet?
13. Honeypot, honey-net, honey-farm;
14. Mobile security;
15. Malware detection/categorization/analysis in Android-based systems;
16. Data/Privacy concerns or leakages in social networks;

Requirement/Expectation/Policy:

1. Mid-term report;
2. **Video** (around 10-minute);
3. Final presentation;
4. Final report.

Requirement/Expectation/Policy:

1. Write your report like a **professional** paper **concisely**. Writing and presentation skills are more than important and demanded for your future career. You are encouraged to

use a professional format like the LNCS template for computer science publications or IEEE template for conference proceedings. Both Latex and Word version are welcome. They can be found in the following links.
(http://www.springer.com/computer/lncs?SGWID=0-164-6-793341-0);
(http://www.ieee.org/conferences_events/conferences/publishing/templates.html);

2. Give reference when you need to cite others' work. **DO NOT** just copy and paste. **No** plagiarism;
3. Present your outcome in a professional manner. If it is a thorough case study, an oral presentation is required in class. If you have a simulation/implementation (with programming/configuration/exploit work), a demonstration or proof-of-concept with essential explanation is required in class;
4. Always keep the **legal policy** in mind;
5. **Do not** use your personal account in any projects, in case your personal information is revealed;
6. **No** work (including any form of outcomes and results) from other places (like others' papers or your own reports from courses projects/labs) can be used here in this course; duplicate work will directly lead to your failure in this course and a report will be sent to the department;

Grading:

1. The project report and oral presentation are supposed to document **what you analyzed**, **what you did** and **what you got**. Please use the concepts and mechanisms from this class to make descriptions and judgments.

2. One suggested way is to tell the security incidents like several "stories", draw security take-away messages from the stories, and then propose potential solutions based on what you learn from this class. Or, you can build an experimental environment to "reproduce" the incidence and test your proposed solution to mitigate the security issue.

3. The report and presentation will all be evaluated based on the following grading criteria.

Correctness	25%
Completeness	25%
Clarity	25%
Quality of English writing	25%