CARDIFF UNIVERSITY

SCHOOL OF INFORMATICS

Cyber Incident-Response Smart Grid Tool

Initial Plan

Module: CM3203 – One Semester Individual Project

Author: Jorge Correa Merlino
Supervisor: Neetesh Saxena
Moderator: Angelika Kimmig

Project Description

As our world becomes more digitalised with new technology, it is important to be able to defend against cyber-attacks. With the rapid increase of cyber-crime [1], an attack can come at any moment without any notice. Therefore, the first person to respond to an incident like this can determine whether an attack is successful or not. These people are called first responders, and they need a plan and tools to act in case of an incident.

The aim of the project is to design and create a tool that could help first responders to respond to the cyber-attacks in order to mitigate their impact onto the smart grid. In order to achieve this, the incidents must be analysed and classified. First, I will look at finding the indicators of compromise. Indicators include, if an element has had many DNS changes as the attacker may be trying to hide their location, or if a malicious URL is detected in the system that can lead to a security breach.

To analyse all the information that has been happening in the system, we need to review logs. However, the number of logs generated to store information nowadays far exceed human analysing capabilities. Therefore, we need a log analyser that flags relevant logs for inspection, such as logs close to the incident time or that point to dubious resources.

The tool that is been made in this project will get all of this information so that I can then develop capabilities to counter the attacks. The final tool will meet all of these requirements and will be helpful for first responders to act in a cyber incident.

Project Aims and Objectives

- Implement an Indicator of Compromise detector.
    - Must be able to find and classify indicators.

- Implement a log analyser.
    - Must find and analyse logs related to a cyber incident.

- Implement capabilities for response.
    - Must be able to help against certain common incidents.

Ethics

Since dummy data will be used when testing, this project does not require consideration on the ethics of the data. If a need to use real information arises, this will be discussed with my supervisor in order to take appropriate steps.

Work Plan

The total time allocated for the project is 15 weeks beginning from the week starting the 27th January. During weeks 1 and 2, aside from this initial plan that will be completed by week 1, I will research information related to project to gain a better understanding of the task at hand. During weeks 3 to 9, I will work on the implementation of the separate subproblems mentioned in the Project Objectives section. I anticipate that developing capabilities for response will be more challenging than finding indicators of compromise or log analysis, therefore I allocated more time to it. After all the implementations are done, I will have a review meeting with my supervisor to discuss whether the program is good enough to meet the criteria. After the implementation has been approved, I will integrate the three parts together to create the final tool during week 10. Then for the remaining weeks I will continue to test the tool and possibly try to add some additional features. At the same time, I will start writing the final report. The week after Easter (week 13), I will review the test results with my supervisor to make the final changes before presenting.

If the implementations are not good enough for integration (week 10), changes will be made during weeks 10 to 12 which is the Easter holiday. In this case, testing will begin once the changes are made. The review meeting for the test results may be pushed back one week to allow sufficient time to produce test results given the delay.

Weekly meetings have been scheduled with my supervisor to review progress made each week and as an opportunity for me to ask for advice in any issues that should arise.

Week 1 (27th January) – Complete Initial Plan. Start research on indicators of compromise. **Deliverable: Complete Initial Plan.**

Week 2 (3rd February) – Research on existing tools. Understand how they work and how they are implemented.

Week 3 (10th February) – Start on implementation to find indicators of compromise. Select most common indicators to implement.

Week 4 (17th February) – Finish implementation on indicators of compromise. Test implementation.

Week 5 (24th February) – Start on implementation of log analysis. Explore methods of implementing log analysis.

Week 6 (2nd March) – Finish implementation of log analysis. Test implementation.

Week 7 (9th March) – Start developing capabilities to respond to the indicators and log analysis. Refer to previous tools to contrast what has been done before.

Week 8 (16th March) – Continue working on developing capabilities for response.

Week 9 (23rd March) – Finish development. Test implantation. **Review Meeting: Review three produced parts before integration.**

Week 10 (30th March) – Assemble previous three parts together. Test tool. **Deliverable: Complete Project Code.**

Week 11 (6th April) – Report writing. More testing if needed.

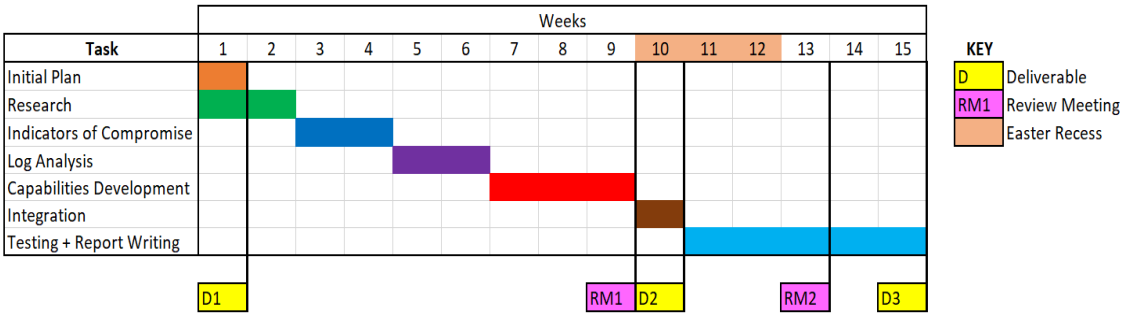
Week 12 (13th April) – Report writing. More testing if needed.

Week 13 (20th April) – Report writing. More testing if needed. **Review Meeting: Testing Results.**

Week 14 (27th April) – Report writing. More testing if needed.

Week 15 (4th May) – Report writing. More testing if needed. **Deliverable: Complete Final Report**

Gantt Chart



References

[1] Ismail, N. 2017. The rise of cybercrime continues to accelerate. Available at: https://www.information-age.com/rise-cyber-crime-continues-accelerate-123467629/ [Accessed: 3rd February 2020]