**CS440 - Group Project**

**Table of Contents**

[**Synopsis**](#_heading=h.1fob9te)

[**Deliverables**](#_heading=h.3znysh7)

[**Project Topics**](#_heading=h.tyjcwt)

[**Requirements & Deadlines**](#_heading=h.3dy6vkm)

[**Presentation Structure**](#_heading=h.1t3h5sf)

[**Evaluation Rubrics**](#_heading=h.26in1rg)

[**Frequently Asked Questions (FAQs)**](#_heading=h.lnxbz9)

**Synopsis**

You are to create a team of 4 and choose a leader. Each team chooses a topic from the given list and conducts an open-ended investigation on the topic. The key learning outcome will be

* Understanding of how security concepts learnt in CS440 are applied in practice
* Deep understanding of a particular security topic
* Ability to learn new concepts, techniques and technologies independently

**Deliverables**

1. Slides deck to present the topic -- submit in **eLearn -> Assignments -> Project**
2. 12 mins presentation in Week 13 Lecture Period
3. All team members must participate in the presentation
4. All team members must be present during Week 13 class and answer the questions if asked by the instructor and the fellow students -- Q&A will be conducted in the class (or Zoom/Slack in case the classes are to be conducted online)

**Project Topics**

* No two teams in the same section can select the same topic unless approved by the instructor. That is, each team in the same section selects a distinct topic.
* Select a topic and **team leaders report their choice to TA via email**
* First come first serve.

**Requirements & Deadlines**

1. Report team information by Week 3
2. Presentation

* Presentation slides are to be submitted to **elearn-> Assignments -> Project**
* The deadline of submitting slides is by **Week 12 Friday 5pm**
  + 10% penalty for late submission < 1 hr
  + 100% penalty for late submission > 1 hr or no submission
* The oral presentation must be delivered within **12 minutes (excludes Q&A)**
* **In week 13**, there is no lecture. But all the teams must be available for Presentation and Q&A

**Presentation Structure**

1. Introduction: title, team member, who did what
2. Background: provide background regarding the topic
3. Approach: explain how the investigated protocol/method/malware works
4. Conclusion: Draw your own conclusion based on your research and findings

**Introduction: title, team member, who did what**

* Introduce title of the project
* Introduce team members
* Briefly describe the contribution of each member

For example,

|  |  |
| --- | --- |
| **Member** | **Contribution** |
| Dettol | Conducted literature study  Investigated strengths and weaknesses of the approach |
| Sephora | Investigated step1 and step2 of the approach |
| Bath & Body | Investigated step3 and 4 of the approach |
| Unity | Setup tools for running demo |

**Background: provide background regarding the topic**

* E.g. for Kerberos authentication, explain what authentication is, types of authentication methods, applications of authentications, the ingredients, the issues (weaknesses of other authentication methods compared to NTLM; open problems)
* For a Malware topic, explain what this specific malware is and consequences; give a generic concept/example of how it works
* This basically defines the context you are dealing with

**Approach: explain how the investigated protocol/method/malware works**

* Overview --- Give an overview of how it works; explain the concepts and steps involved with a diagram if possible
* Give technical details --- Deep dive
  + Explain how the protocol/method/malware works in detail using technical terms/notations/formula where applicable
  + Strengths & weaknesses, attacks & defenses, where applicable
* Demo --- not compulsory but it may be the differentiator for getting A+ --- e.g.
  + Demonstrate how Kerberos authentication works
  + Demonstrate how malware attacks programs/files/browser/etc.
  + (Demonstrate in a way similar to what we do in the workshops or you can be creative)

**Conclusion: Draw your own conclusion based on your research and findings**

* Summarize your presentation
* Highlight any important findings (on your own or according to the findings you read/understood from literature)
  + e.g. one important finding from the study of Mirai botnet attack is that IoT devices, despite their usefulness, opened the door for new ways of conducting massive denial of service attacks…
* Lessons learnt
  + e.g. based on the observations of past security attacks, we learn that many of those arise from insiders…
* Any open problem?
  + e.g. Kerberos authentication solves the problem of (….) weaknesses of NTLM authentication but on the other hand, (….) weaknesses remain to be addressed…

**Evaluation Rubrics**

|  |  |
| --- | --- |
| **Component (weightage)** | **Grade** |
| **Presentation (5%)** | A/A+ :   * Very clear, organized, and coherent slides * Effective use of presentation tools (e.g. animation, impressive layout, etc.) * Great clarity and articulation in presentation |
| A-/B+ :   * Clear, organized, and coherent slides * Good use of presentation tools * Good clarity and articulation in presentation |
| B/B- :   * Slides lack clarity, organization, and/or cohesion * Lack of use of presentation tools * Lack of clarity and articulation in presentation |
| C+ & below :   * Slides severely lack clarity, organization, and/or cohesion * Severe lack of use of presentation tools * Severe lack of clarity and articulation in presentation |
| **Background content (3%)** | A/A+ :   * Comprehensive background information |
| A-/B+ :   * Sufficient background information |
| B/B- :   * Some background information |
| C+ & below :   * Little or no background information |
| **Approach content (10%)** | A/A+ :   * Demonstrate excellent understanding of the concepts * Demonstrate excellent knowledge of technical details * Provide excellent demonstration of the security topic being investigated |
| A-/B+ :   * Demonstrate good understanding of the concepts * Demonstrate good knowledge of technical details * Provide good demonstration of the security topic being investigated |
| B/B- :   * Lack understanding of the concepts * Lack knowledge of technical details * No demonstration or demonstration given is not good enough |
| C+ & below :   * Little or no understanding of the concepts * Little or no knowledge of technical details * No demonstration provided |
| **Conclusion content (2%)** | A/A+ :   * Excellent summary of the presentation * Great ability to draw lessons, highlight important findings, and identify open problems |
| A-/B+ :   * Good summary of the presentation * Good ability to draw lessons, highlight important findings, and identify open problems |
| B/B- :   * Lack ability to draw lessons, highlight important findings, and identify open problems |
| C+ & below :   * Severely lack ability to draw lessons, highlight important findings, and identify open problems |

**Frequently Asked Questions (FAQs)**

*Last updated:* ***14th August 2022***

* **Are all members of a group receiving the same group project grade?**

Yes. One grade for the whole team. Extreme cases of non-participation will be handled on a case-by-case basis. Please let me know if a group member is not participating as early as possible.

* **Are all members of a group required to present?**

Yes. This is to ensure that every member contributes to the project.

* **Can the presentation exceed 12 minutes?**

No. Up to 2% penalty may be imposed.

* **For my project, background section seems unnecessary. Will it be fine without presenting the background?**

Absolutely NOT. Every project and presentation needs to provide background information so that the audience can understand the context.

* **Any tips for drawing conclusions?**

See the above Evaluation Rubrics -> Conclusion content -> A/A+

* **Will answering questions from the instructor and the fellow students (Q&A) be graded?**

Yes. Q&A will be graded as part of Background, Approach, or Conclusion component, with respect to the type of questions asked.

* **Is asking questions during/after other teams’ presentation encouraged?**

Asking questions is encouraged as it will be considered as Class Participation. In general, if you have a question, please wait till the presentation is over and then ask, unless there is an urgent need to clarify.