

Projet d'Audit de Sécurité Technique

Project

General Description and Guidelines

Professor
Abraham Rubinstein

abraham.rubinstein@heig-vd.ch

Professor
Jean-Marc Bost

jean-marc.bost@heig-vd.ch

Teaching Assistant
Lucie Steiner

lucie.steiner@heig-vd.ch

September 2019 – February 2020

Table of Contents

1. Objectives	3
2. Deliverables.....	3
2.1. Deliverables and Deadlines	3
3. Requirements	4
4. Evaluations	4
5. Confidentiality	5
6. Questions and supervision.....	5

1. Objectives

The high-level objective of the present project is to enable you to put what you have learned in class into practice. One of the most important aspects of this project is to be able to structure your information security related work. The structure of this project is as important as its technical contents and will be evaluated accordingly.

In general this project has to be realized in an external organization (e.g. company, non-profit, governmental). The student has to find such an entity among his contacts and network. The estimate of available time to realize this project is 105 hours (or 12 days considering a standard working day of 8.5 hours) per student including the preparation of presentation and report.

The main goals of the project:

- Demonstrate that you are able to structure your security project work
- Ability to work with external parties (your customer)
- Conduct your project according to requirements and within constraints as well as avoid the scope creep
- Efficiently communicate results of your work taking into account the technical level of your customer

2. Deliverables

2.1. Deliverables and Deadlines

Scoping presentation

- The allocated time for the scoping presentations is **Thursday 21st and Friday 22nd of November**:
 - You are free to invite a representative of the customer or to held the meeting at its premises, especially if your work is covered by a signed Non-Disclosure Agreement
- The **customer must have been informed in written** during the scoping that:
 - Deliverables will not be pre-approved by the customer
 - A representative of the customer can participate to the scoping and final presentations and that these meeting can be held at its premises, especially if your work is covered by a signed Non-Disclosure Agreement
- Normally all scoping presentations must be completed before **Friday 22nd of November 16:00**
- Presentation of scoping (pdf and .ppt/.key/.tex or any other source file)

Final deliverables

- The deadline for the final deliverables is **Friday 17th of January at 18:00**.
- **The last week (until 24th of January)** is reserved for the final presentations.
 - You are free to invite a representative of the customer or to held the meeting at its premises, especially if your work is covered by a signed Non-Disclosure Agreement
- Presentation (pdf and .ppt/.key/.tex or any other source file)
- Report (pdf and .doc/.tex or any other source file)

3. Requirements

For the scoping exercise presentation (15 minutes max excluding questions) at least following topics shall be covered :

- Scope of Engagement
 - Goal of the engagement (e.g. for a penetration test, goal based on a threat scenario)
 - Scope
 - Hosts, network ranges and applications
 - What is excluded from the scope (including hosts, network ranges and applications which should not be tested)
 - List of third-party owned systems and applications (if applicable)
- Rules of Engagement
 - Timeline using GANTT chart, Work Break Structure (WBS) or any other method providing a time and effort estimate of every task you have identified
 - Location(s) where the project will be conducted
 - If a penetration test, whether it is a white box or black box pentest
 - Customer-owned data and data viewing policy
 - Status meetings
 - Contact information
- For a penetration test a permission to test memo

For the final presentation and report

- Report
 - Table of contents
 - Executive summary
 - Project summary (scope, goals and methodology)
 - Project results summary
 - Detailed results
 - Next steps and recommendations
 - Appendices (any relevant documents, raw output from vulnerability scans for example)
- Presentation (25 minutes max)
 - Reminder of the scope, goals and the timeline
 - Executive summary of results/findings
 - Most interesting/relevant results with deeper technical details
 - Recommendation and next steps

4. Evaluations

Your project will be evaluated in the following manner:

- 20% of the final project grade – Evaluation of the scoping exercise
- 80% of the final project grade – Evaluation of the report and final presentation

For the scoping exercise presentation (15 minutes max excluding questions) following criteria will be evaluated:

- Scope structure
- Rules of Engagement
- Understanding of customer requirements
- Timeline of the project and its related steps
- Quality of the presentation – structure, spelling/grammar, etc..
- For teams of 2 students – ability to split the work in a coherent and intelligent way

For the final deliverables following criteria will be evaluated:

- Management of the scope along your project
- Fulfillment of project requirements and objectives
- Technical results
- Quality of the deliverables
 - Delivered in time
 - Quality of the report and presentation
 - Structure (executive summary, technical part)
 - Details
 - Spelling and grammar
 - Presentation and communication skills

These criteria are given as an indication. They can be changed (added, removed or modified) and their weight in the final grade calculation adapted.

5. Confidentiality

If your customer requires a Non-Disclosure Agreement (NDA) you shall sign it and take into consideration the points covered. The professor in charge (hereafter, the professor) must be involved in the process as he will also sign the NDA.

In case an NDA is in place, the student can choose to give the scoping and final presentations during a customer's meeting in which case the professor in charge will be present at these meetings. It is the responsibility of the student to schedule these meetings.

In any case the final deliverables has to be submitted before the deadline.

The deliverables do not need to be pre-approved by the customer.

6. Questions and supervision

Unless otherwise specified, the supervision and questions will take place every week on Friday from 13:15 to 15:40 in the usual classroom. Outside these hours, the students are requested to schedule a meeting with the professor or teaching assistant.