Final Project Description-Ethical Hacking and Penetration Testing - COMP6210001

Ardimas Andi Purwita

March 9, 2022

1 Descriptions

This final project description aims to detail the flow and requirements of the final project and final exam for COMP6210001.

2 Workflow

Please see Figure 1 to see the workflow. Basically, you can choose to do a full written exam, a hands-on exam, or a self-defined project.

In the full written exam, it is mandatory for you to write a short academic/-scientific paper where the topic will be defined at least 3 weeks before the final exam week starts. In addition, there will be a few questions that you need to answer, and the questions will be published on the final exam day. In the hands-on exam, you choose one of topics that I have selected and build application on your choice of topic. If you can't deliver it well, then you need to participate in the written exam. However, you can choose some of the questions to be answered. If you can successfully deliver it, then I'll give you an A grade for your final exam. For the self-defined project, I'll let you define the topics yourself. If you're not sure whether the complexity is sufficient or not, you can write a project proposal and send it to me. There is no template for this project proposal.

3 Grouping

This grouping only applies for the hands-on and self-defined projects. You can decide how many team members you want to have. You can also mix your team members from different class. The main requirement is that all team members must be students from Binus International. Furthermore, the size of your team should justify the complexity of your project. That is, having more people implies more complexities.

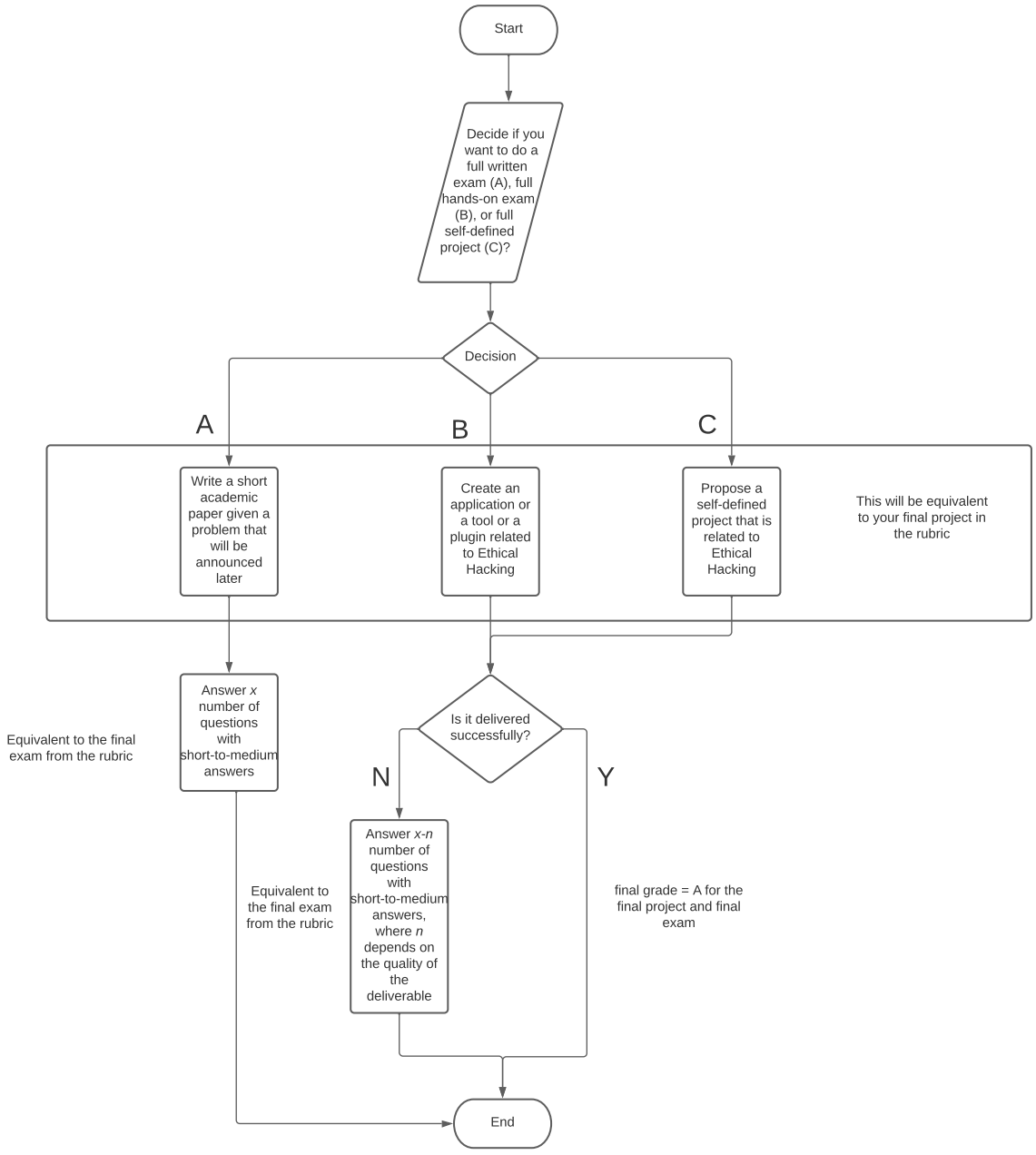

Figure 1: Decision Flow.

4 Submission

1. The short scientific paper will be submitted along side your answers for the questions that require short-to-medium answers.

2. For the hands-on and self-defined projects, a live presentation is required. During the presentation, I will judge your understanding for this course. In addition, I also demand a git repo of the project having a complete documentation explaining how to install, software/library dependencies, and documentation about your application. If you don't want your git goes public, you can invite 'focm-binus' (Github) to your private repo, and you can kick me out after you receive your grade later.

5 Timetable

The deadline for the written exam is the same as the final for the final exam. Meanwhile, the deadline for the hands-on and self-defined projects are your team's presentations schedule, which will be held at least a week before the final exam for this course.

6 Scoring and Assessment

The goal of this exercise is a medium for you to show off your understanding of most of topics in ethical hacking. Therefore, please make sure to cover most of topics in ethical hacking that we are discussing throughout this semester. As you can earn a grade A upon succefully delivering this project, you need to show that you understand at least 90% of the topic. You can argue later what this 90% means. For example, 90% of topics can be based on the number of session titles from my slides. Alternatively, you can interpret it such that your application covers 90% of general topics in ethical hacking, for example information gathering, vulnerability scanning, exploitation deployment, maintaining access, reporting, etc.

7 Topics for the Hands-on Exam

In this section, topics for the hands-on exam are detailed.

7.1 Create A New Exploit

For this particular topic, as long as it is a **novel** exploit, and it works, I'll give you an A for this course. Being able to develop your own exploit, you must have understood about a system under attack, which is part of information gathering as well as detecting vulnerabilities. If this sounds very advanced, I'll give a very simple example, which is a new google dork entry. With regards to this, I'll double check if your google dork is significantly different compared

to the existing google dorks in, for example, exploit-db. Significant difference means that you cannot only change, for example, the domain name in an existing google dork entry.

7.2 Penetration Testing Lab Demonstrations

An example of this project is a pentest lab where you need to deploy a victim machine and an attacker machine. In the victim machine, you can install a vulnerable application where the attacker can gain a root access. For this particular topic, I will only accept a lab with respect to modern application frameworks. The main reason for this is that you can easily find a vulnerable box where you can perform a very simple attack such as SQL injection. This kind of box is quite old; therefore, I demand a vulnerable application that uses modern framework, for example, the MERN or MEAN stacks. You can ask a confirmation to me if a framework is considered modern or not.

7.3 CTF Documentations from Hacktrace-Range Boxes

We are under a discussion with Spentera. They own a service like HackTheBox where you can practice penetration testing. Therefore, if you can demonstrate that you can capture the flags from the Hacktrace-range boxes, I would accept it as a final project as well. With this regard, the number of people should reflect the difficulty level of vulnerable boxes that you try to hack. Similarly, you can confirm it to me if your choice of boxes are sufficient.