F21AN/F20AN Coursework Description

The coursework is to be completed by groups of **THREE** students. All students must equally contribute to all components of the coursework, including the demo.

Avoiding Plagiarism and Other Forms of Academic Misconduct

This is a reminder that you need to complete your coursework on your own with your group partner. Here are some further points to take into consideration, where "you" refers to either or both group members depending on the CW component. Both student members should contribute to all components of the coursework except individual reports.

- The usage of AI-generated content (such as text from ChatGPT) is forbidden and might result in voiding the course, resitting the course, and up to exclusion from the university, depending on your case and as per our disciplinary guidelines.
- Coursework reports must be written in your own words and any code in your coursework must be your own code. If some text or code in the coursework has been taken from other sources, these sources must be properly referenced.
- Failure to reference work that has been obtained from other sources or to copy the words and/or code of another student is plagiarism and if detected, this will be reported to the School's Discipline Committee. If a student is found guilty of plagiarism, the penalty could involve voiding the course.
- Students must never give hard or soft copies of their coursework reports or code to another student. Students must always refuse any request from another student for a copy of their report and/or code.
- Sharing a coursework report and/or code with another student is collusion, and if detected, this will be reported to the School's Discipline Committee. If found guilty of collusion, the penalty could involve voiding the course.
- And remember: the consequences of taking dishonnest shortcuts in coursework are much worse than getting a bad mark (or even no marks) on a piece of coursework. There has been one case this year where a student was awarded on Ordinary degree (rather than an Honours degree) because of the sanction imposed by the University's Discipline Committee. The offence was plagiarism of coursework.
- Further information on academic misconduct can be found at Student-Academic-Misconduct-Policy

Your coursework submissions will be automatically checked for plagiarism.

Coursework Components and Assessment

The coursework is worth 25% of the course. For students registered in F20AN, the coursework will be marked out of 40 marks; for students registered in F21AN, the coursework will be marked out of 50 marks.

The coursework has three components:

1. A single, group report: worth 20 marks, about 1,500 words in length (excluding figures, such as screenshots).

2. A presentation of your work: worth 20 marks. The recorded presentation should include a demo appropriate for the selected topic in addition to your slides. The presentation (including demo) should be done in 5-6 minutes and should show a good understanding of the topic by both students. The presentation might include slides if needed.

3. [F21AN students only]) An individual report worth 10 marks. Each F21AN student in a group should prepare a short report (about 500 words) that critically reflects on the use and the impact of the chosen tool/attack on industry, end-users, and society as well possible countermeasures. **The individual report must be prepared separately by each student, on their own.**

These components must be about the same topic. Each group will choose one topic, write a report, and make a presentation (including demo) about it.

The report and presentation should provide a short introduction and conclusion to the chosen topic, describe the tool/attack and explain how it works. Demo screenshots should be included in the report and presentation.

Coursework Topics

Topics could be security tools or attacks. In general, a study of “tools” should involve a broad exploration of a tool’s functionality (e.g., purpose, how it works with some example attacks), while a study of “attacks” should involve a detailed exploration of a particular attack (e.g., how/why it works) using scripts and hosts created/built by the students. Some examples are provided below:

- Tools: rootkits, nessus, binders, w3af, metasploitable 2 (vulnerable OS), Social Engineering Tool (SET).

- Attacks: SQL injection, cross site scripting, buffer overflow, NetBIOS (DoS) attacks.

You cannot choose a topic that is already taken.

You need to contact your Professor (Hani in Dubai and Mehran in Edinburgh) by the 20th of February) to have agreement on the topic **before** you start working on it.

Environment

For demo purposes, you can use either two (or more) computers, or one computer with one or more virtual machines or dockers running on top of it. You should be careful if the demo is running against your (host) OS as it could cause data loss/OS crash. (If you are using a university computer, you should only use VMs, and take care to not communicate with the host computer or Internet).

In addition to the option of using the VMs on the university computers, possible scenarios for the demo infrastructure using your personal computers are:

1- One computer with one virtual machine/docker on top of it: ideally, the attacker should be the host, the target being obviously the guest (virtual machine). In this case it is enough to switch off your physical network cards to avoid attacking the university's infrastructure by mistake.

2- Two computers: an attacker + a target, in this case you MUST be sure that they are directly connected to each other using a network other than the university network (e.g., your own wireless access point, to avoid attacking/causing IDS alarms on the university's infrastructure).

If you are using the University VMs, you will need to consider how you will demo your solution in a classroom as part of your presentation.

Submission

The submission deadline for soft copies of the individual **report**, the presentation **slides** and a recorded **video** for your presentation is **Monday the 18th of March at 23:59GMT.**

Late Coursework Submission.

Coursework that is submitted within a maximum of 5 days late will receive a standard **30%** deduction. Coursework submitted more than 5 days late will **not** receive a mark, nor any formative feedback.

A coursework is considered late until all components have been submitted, i.e., the group report, presentation video, presentation slides, and individual report (F21AN students only).

ETHICAL REMINDER/WARNING: ONLY RUN YOUR HACKS ON AN INFRASTRUCTURE THAT BELONGS TO YOU.