Introduction to Information Security

December 2021

Lab Assignment II: Introduction to information security

1 Task choice phase

First register your group in the Assignment Two Groups activity in iLearn. Many of you will no doubt choose to stay in the same group as assignment 1, but you must nevertheless register anew in this activity, and may like to try to grab the same group number as you had for assignment 1. If you find that you have different ambitions for assignment 2, or have found that your cooperation in assignment 1 has not worked well, this is an opportunity to now find another partner. If you do so we expect you to keep your assignment 1 partner fully informed of your actions, so as to avoid confusion about who they can work with on assignment 2.

For this project you are to complete one out of three tasks as described below. First view the task descriptions and by all means do preliminary investigations into what kind of documentation you can find to help you complete the task. If you have previous experience with any of the tasks mentioned in this document, you are encouraged to choose something outside of your comfort zone. Make a choice for which task your group prefers to complete.

1.1 Task completion phase

Task completion is expected to take three days of study for each group member. This entails that group members shall collaborate closely on all tasks. Only minor practical elements of the projects may be delegated between group members, and then only where all the members are assumed to be equally able to complete and to report the delegated tasks. Besides minimal advice, groups are not permitted to assist other groups in the completion of these tasks. Each

group is to document their task in Portable Document Format (pdf). All group members' names must be included on a separate header page at the front of the hand-in document. If you were originally registered for the course before the Autumn term 2021 then make it clear on this header page which term you were originally registered. Do not waste author, or examiner time on filling out with descriptions of things that can readily be found in other sources, such as on the Internet. Document what is needed in order for the reader to understand what is required to complete your experiment and the actions you have taken. Include a Time Summary section a general estimation of what parts of your task took how long to complete in terms of person hours. The report must also contain a Conclusions section where the group discusses what security lessons may be learned by completing this experiment. The report is to be written as concisely as possible and with correct and appropriate language. The report must include proper academic referencing, meaning that statements and quotations not directly attributable to the authors themselves must be supported by an indexed reference list that clearly shows the source. If there are any signs that the authors have included ideas, text or illustrations that are derived from other sources than their own mental processes without proper attribution, their work will be subject to investigation according to the university disciplinary proceedings. To avoid any doubt in what such referencing entails students are encouraged to review the Wikipedia page: `https://en.wikipedia.org/wiki/Citation`

In summary, your document will contain a header page, then a body with sub-headings.

1. Design (for tasks Anonymisation, AppArmor and Social Engineering)

2. Experiment results – where your steps are discussed, not just stated.

3. Time Summary

4. The group's reflections on what has been learned from the experiment as a whole

5. References – A list a sources that have been cited in the main body of the text.

In iLearn2 any additional files that are needed by the examiner in order to verify that your work meets the assignment requirements must also be a part of your hand-in. Submit such files separately, not as e.g. compressed packages. All group members must confirm the group's submission in the relevant iLearn2 submission activity. Only confirm once you are sure that the submitted files are those that the group agrees are a true representation of the group's work. Submit the group's assignment solution to Assignment 2 Hand-in in the course page in iLearn2. Any additional files that are needed by the examiner in order to verify that your work meets the assignment requirements must also be a part of your hand-in. Submit such files separately, not as e.g. compressed packages.

All group members must confirm the group's submission in the relevant iLearn2 submission activity. Only confirm once you are sure that the submitted files are those that the group agrees are a true representation of the group's work.

1.2 Laboratory Environment

During this lab assignment you will be working with VMware for those of you who choose Task 1, AppArmor. You need to use VMware that you used for assignment one. You just need to use the same credentials, and you have the option to work on Kali Linux VM (Kali 2021.3) and Linux VM (Xubuntu 20.04.3 LTS).

You have also another alternative to work with Virtualbox. In order to do so, you have to use a computer with administrative rights, so that you can import the DiFo _ Kali.ova virtual machine. You can download the Kali machine from:`http://ftp.cs2lab.dsv.su.se/DIFO/DiFo_Kali.ova`

To import the Kali machine, just open up VirtualBox and click File/Import appliance and then select the kali.ova file and click OK. Disable the sound card and USB if that gives you an error when trying to import it.

There are several tools that might be useful when completing this assignment's exercises. Feel free to use any other tool that you find sufficient. On the Kali machine, most of the programs are command line based - that means that you have to launch them in a terminal.

1.3 Grading criteria

The general grading criteria as specified in the "Course Goals and Criteria" document apply to this assignment. Students are advised to re-read the section "Assignments" before commencing work and before submitting. Pass: a pass mark is awarded if the work is

Pass:a pass mark is awarded if the work is

- Completed and documented independently of other groups.
- That both the group's own task fulfil the written requirements
- Clearly presented and easy to read.

Fail: fail grade will be given if:

- The group has clearly failed to reach the requirements for at least an

insufficient grade.

- An attempt to mislead the staff is evident, such as documenting so as to make it appear that more work has been done that in reality, or such as submitting as a group although students have not properly shared the tasks.
- Plagiarism is evident

A fail grade entails that the students in that group will not be given further opportunities to complete an equivalent assignment before the next time the course is held.

Past Deadline Hand-ins Due to the time dependencies between phases on this assignment, hand-ins that are not properly submitted by deadline will in general be regarded as automatic fails.

1.4 Task 1: AppArmor

Profile: Task will require reading of some dry documentation and coding of a configuration file in order to test what a mandatory access control system can look like. We assume it will primarily attract those students who have some coding experience, and good linux experience. You will have to find your own way around the sources of AppArmor documentation on the net that best suit your level of ability. [1] For this task you are to write an AppArmor profile for either vi, vim, nano, or (advanced) gedit.

Using comments on each line in your profile code explain what each line in your rule set does and why you included it. In your documentation include a description of how you arrived at your solution, including sources referred to and tools used. Include an excerpt of a system log that shows how an attempt to use the editor to write outside of its permitted directory has been refused.

Evaluation of your security understanding Based on understanding gained from this exercise include a short report that describes how the behaviour that you have seen in AppArmor's mandatory access control can be used to improve system security in a real-life situation. Include also a discussion on what strengths and weaknesses the group perceives in its use. Include your AppArmor profile code within your report but also include it as a separate file in your submission in case the staff wish to use it for testing purposes.

[1] https://wiki.ubuntu.com/AppArmor

1.5 Task 2: Anonymisation Tools: Keeping Your Information to Yourself

Profile: *Though there are technical aspects to this assignment it allows you to find tools for the operating system environment that you prefer.*

Your task is to find 3 different anonymisation tools that you are able to motivate are especially interesting to work with and compare them in a written report. If you do not already know which tools you are most interested in you may find useful links starting with the Wikipedia web page on Anonymizer. You do not have to limit yourselves to only Web anonymisation.

You must first set up, motivate and document - under a document subheading Design - a test protocol for the aspects of the tools that you regard are the most interesting to test. The test protocol is to be designed based on aspects of the tools that you chosen and to give a reasonable investigation for the time available. Factors that you should consider comparing include:

- How easy is it for a user to install and use the system securely? E.g

  1) Are there parts that would be difficult for a naïve user to complete, or complete securely? 2) Are there any kinds of delay involved that might make users too impatient to use the tool? 3) Is it possible to demonstrate where poor handling of the tool may contribute to a breach of anonymity?

- Compared to the other tools you are looking at?
- What might the tools not protect against? How helpful is the documentation for different user profiles?
- What does each tool protect against
- What common misconceptions might exist about the tool?
- Is it possible to uncover the anonymised data if the user does not use the tool properly?
- A short discussion on the cost/benefit ratio of the tool's benefits versus the potential loss of availability involved in installing, configuring and using the tool.

Wherever possible and reasonable, prove identified problems with practical demonstrations.

1.6 Task 3: Social Engineering

Profile: This is an experiment and investigation that does not assume much technical prowess, but does require careful thought, strict ethical behaviour, and finesse when dealing with interview subjects

Your task is to find and document - under a document sub-heading Design - two true to life situations where deliberate and malicious social engineering could be used to break, bypass or exploit an IT security policy. You are also to first design and then perform and document at least 3 interviews per social engineering scenario with potential victims of such a scenario in order to assess the likelihood of success, the potential damage caused and the potential victims' awareness of the exploit-ability of the situation.

your task is to find and document- Under document sub heading design- two true to life situations where deliberate and malicious social engineering could be used to break.

Your overall goal with this task is to gain insight into, and to document, the public's understanding of the risks involved with IT connected social engineering attacks. You should therefore ensure that the subjects that you interview are good representatives of the potential targets of the attack. Interviewing friends and family may be suspected of giving less reliable results than interviewing members of the general public (assuming they are potential targets for your chosen scenarios).

You are not trying to find experts on social engineering (as some previous students have mistakenly assumed). You are trying to find ordinary people and then finding a safe and objective way to interrogate them about how they are likely to act to thereby draw assumptions on the public's understanding of social engineering. This in turn should give an indication of how serious a threat your specific scenarios are likely to be

In your report you are to describe how the situation could be exploited, if any artefacts are used for the exploit, how a victim can protect from it, your interviewed potential victims awareness of the situation, and the expected gains from a successful exploit. Also document how the dangers from your scenarios could be mitigated by a security manager's measures.

WARNING! Previous years a few groups have erroneously interpreted this task as being about directly executing social engineering attacks on unsuspecting individuals. This would be regarded as a transgression of course and university ethical principles. The very trick is to investigate social engineering without causing even the least amount of possible danger or discomfort to others. If you are in any doubt about the limits of ethical research you are encouraged to

browse[2]. If there is any indication that any subject may have suffered the least discomfort at your hands due to poorly devised method, your project may be summarily terminated and failed. If in doubt, check with the course staff before conducting any practical stages.

1.7 Supervision

Supervision will be available online on primarily using the forum.

[2] http://www.codex.vr.se/en/index.shtml