Exam frontmatter

CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering

Examination in Computer Security EDA263 (DIT641) for the International Master's Program in Computer Systems and Networks, Monday June 8 2020, 14:00—18:00

Examiner:

Associate professor Magnus Almgren, Ph.031-772 1702,
email: magnus.almgren@chalmers.se

Teacher available during exam:

Magnus Almgren, Ph.031-772 1702
(remote exam, so email your questions)

***Language*:** Answers and solutions must be given in English.

Grades: will be posted before July 1 2020.

An exam review will then be scheduled and announced on Canvas.

Normally, you are **not** allowed to use any means of aid. However, Chalmers centrally has declared that since this will be a remote exam all aids are allowed but the exam needs to be done individually.

The exam consists of the different "quizzes" in Canvas

- Exam Part A: on a timer, short answers
- Exam Part B: In-depth questions

Please write the answer to each question (question 1, question 2, etc) directly in canvas.

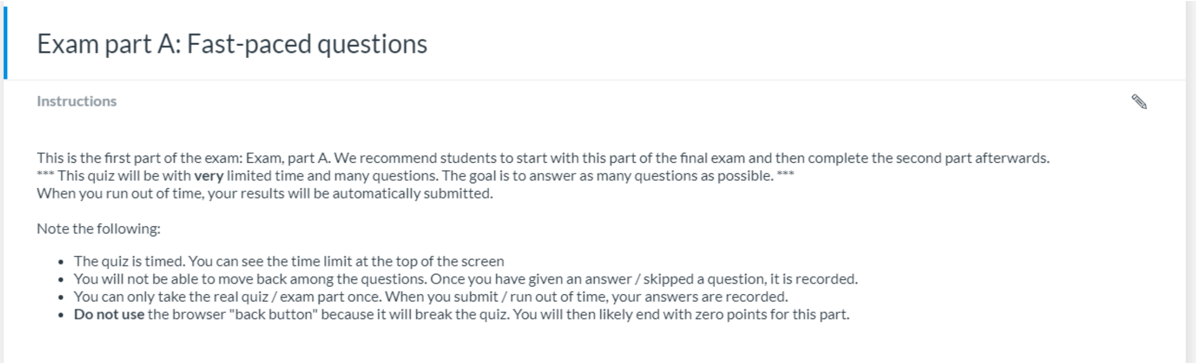
For previous exams, the has been determined as follows:

30 p ≤ grade 3 < 38 p ≤ grade 4 < 46 p ≤ grade 5 (EDA263)

30 p ≤ pass < 46 p ≤ pass with distinction (DIT641)

Given that this is a remote exam, the answers will be judged holistically to see how well the learning goals are fulfilled. Please see a longer discussion in Canvas.

Some questions contain two parts: a short answer and a longer motivation for that answer. For these questions, the motivation will only be considered if the short answer is correct.



Exam part A: Fast-paced questions

Instructions

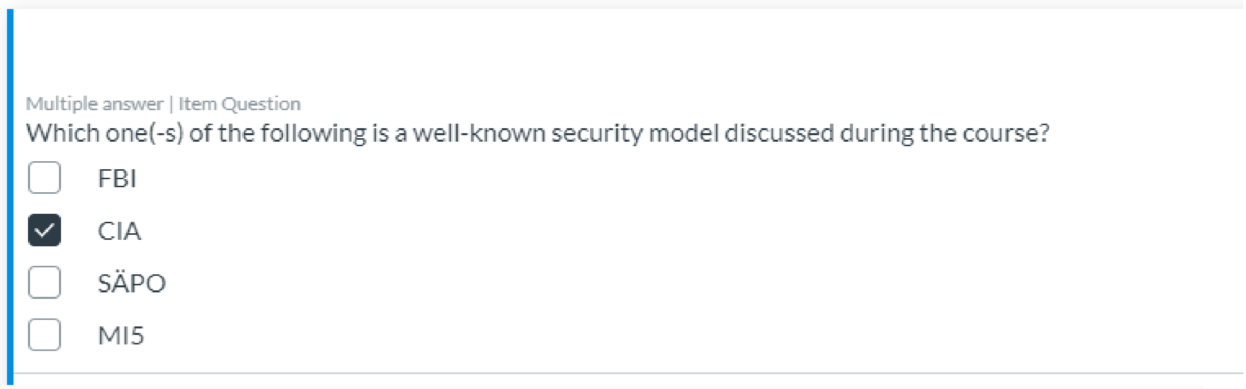
This is the first part of the exam: Exam, part A. We recommend students to start with this part of the final exam and then complete the second part afterwards.
*** This quiz will be with **very** limited time and many questions. The goal is to answer as many questions as possible. ***
When you run out of time, your results will be automatically submitted.

Note the following:

- The quiz is timed. You can see the time limit at the top of the screen
- You will not be able to move back among the questions. Once you have given an answer / skipped a question, it is recorded.
- You can only take the real quiz / exam part once. When you submit / run out of time, your answers are recorded.
- **Do not use** the browser "back button" because it will break the quiz. You will then likely end with zero points for this part.

(note: you need to answer fully correctly and for most question in A you do not get partial credits)

Fast Recall, 10 questions, 1 point per question



Multiple answer | Item Question

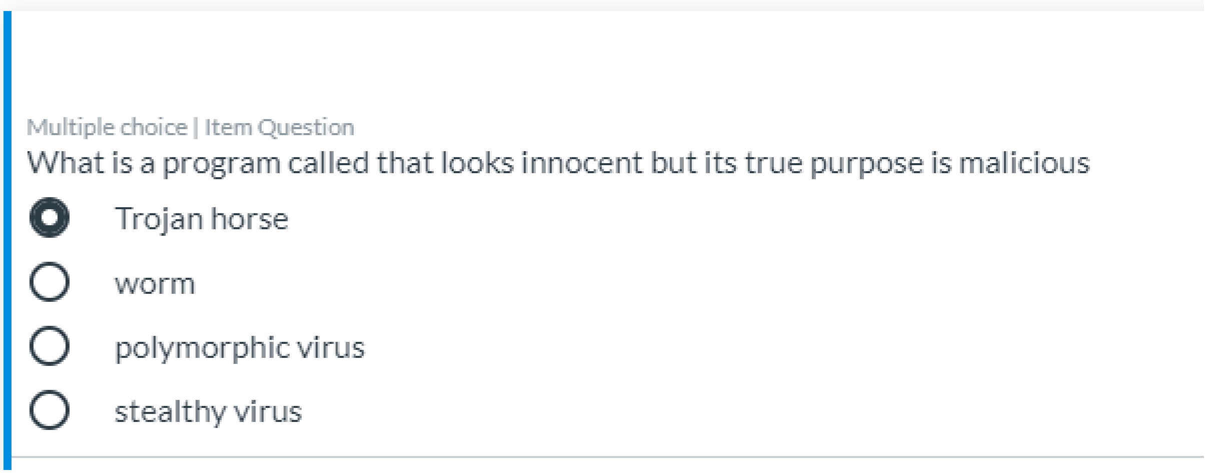
Which one(-s) of the following is a well-known security model discussed during the course?

□ FBI

☑ CIA

□ SÄPO

□ MI5



Multiple choice | Item Question

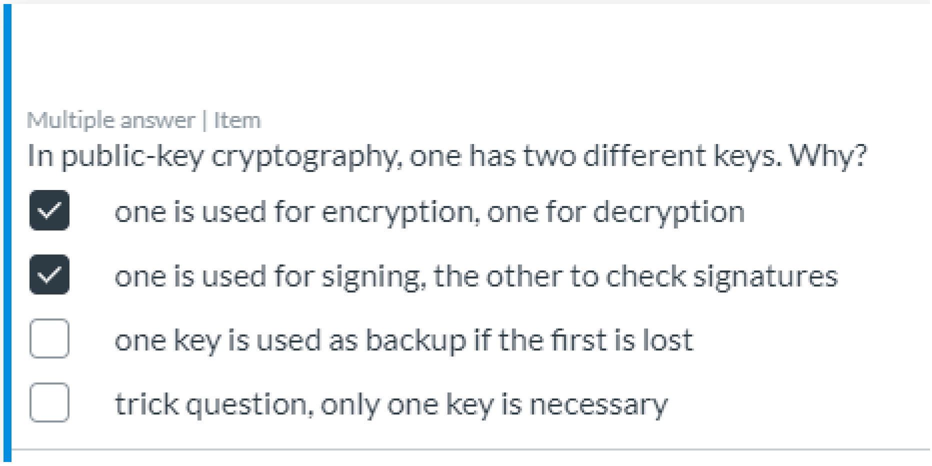
What is a program called that looks innocent but its true purpose is malicious

● Trojan horse

○ worm

○ polymorphic virus

○ stealthy virus



Multiple answer | Item

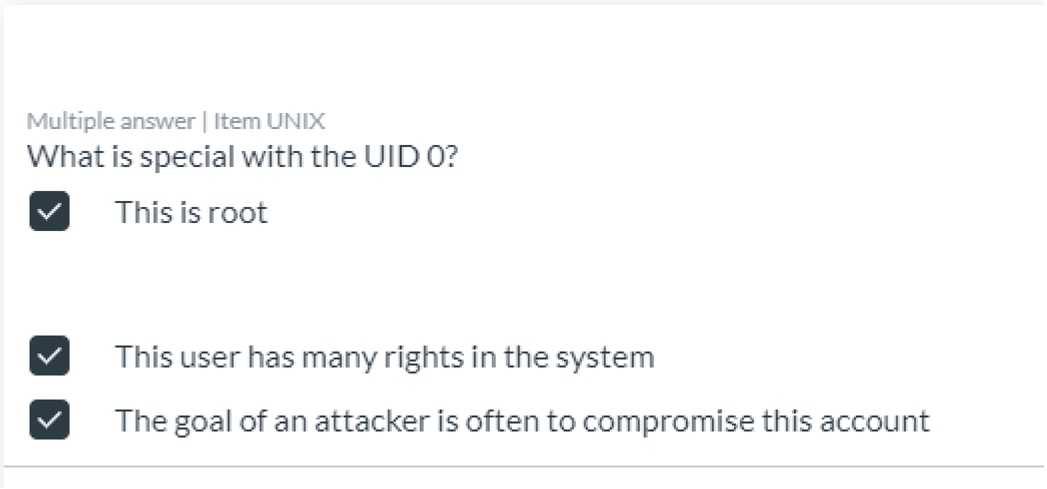
In public-key cryptography, one has two different keys. Why?

☑ one is used for encryption, one for decryption

☑ one is used for signing, the other to check signatures

□ one key is used as backup if the first is lost

□ trick question, only one key is necessary



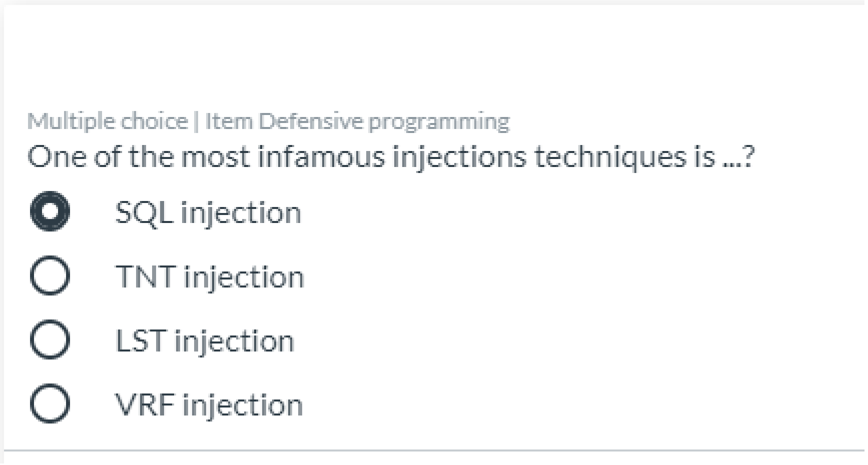
Multiple answer | Item UNIX

What is special with the UID 0?

☑ This is root

☑ This user has many rights in the system

☑ The goal of an attacker is often to compromise this account



Multiple choice | Item Defensive programming

One of the most infamous injections techniques is ...?

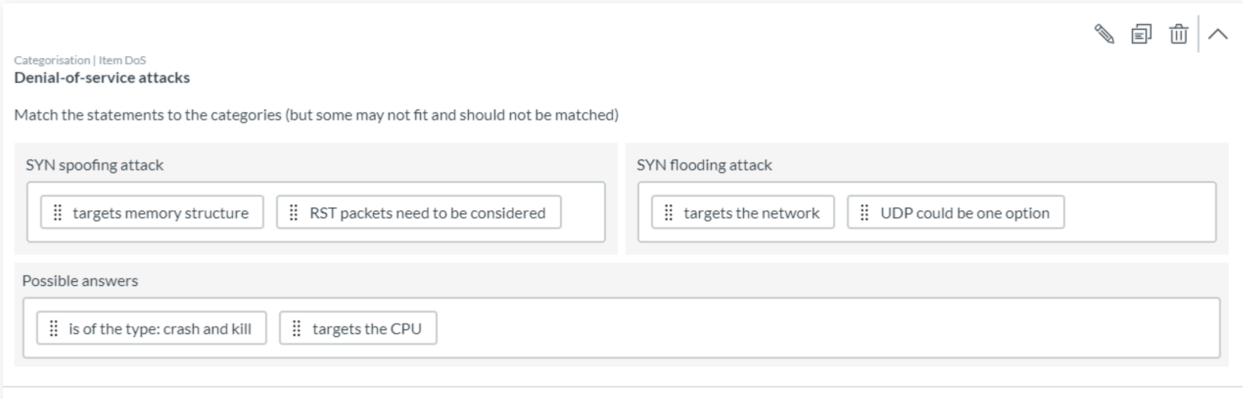
● SQL injection

○ TNT injection

○ LST injection

○ VRF injection

Medium Recall, 4 questions, 2 points per question



Categorisation | Item DoS

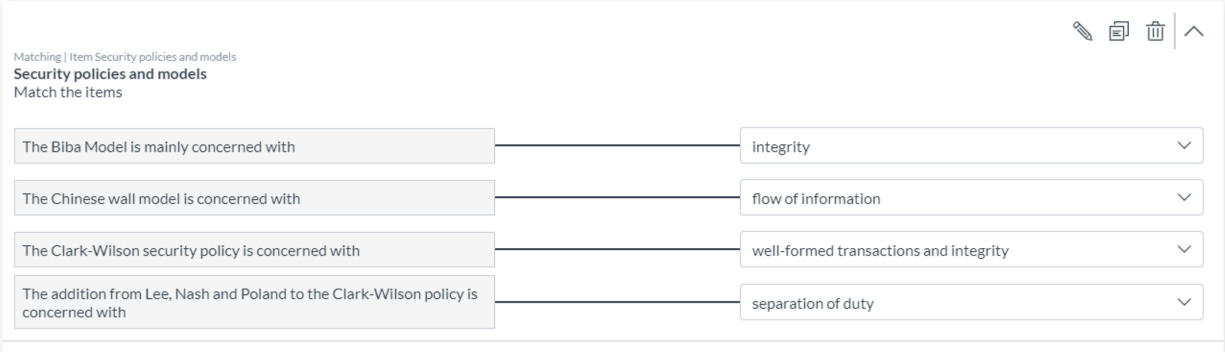
Denial-of-service attacks

Match the statements to the categories (but some may not fit and should not be matched)

SYN spoofing attack: targets memory structure; RST packets need to be considered

SYN flooding attack: targets the network; UDP could be one option

Possible answers: is of the type: crash and kill; targets the CPU

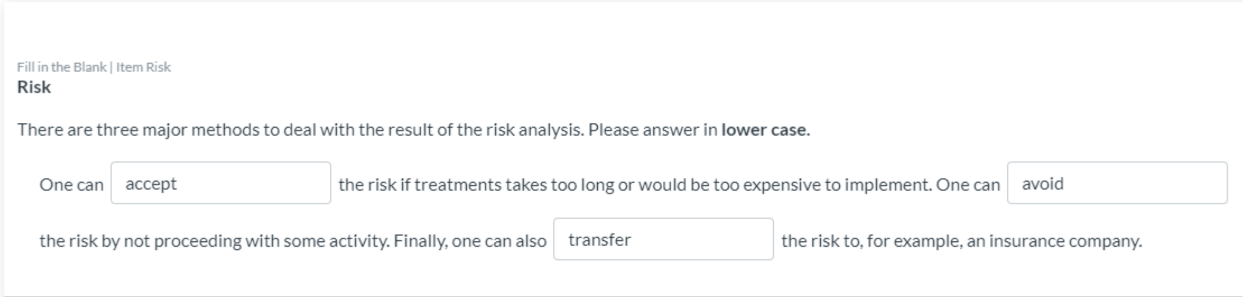


Matching | Item Security policies and models

Security policies and models

Match the items

The Biba Model is mainly concerned with	integrity
The Chinese wall model is concerned with	flow of information
The Clark-Wilson security policy is concerned with	well-formed transactions and integrity
The addition from Lee, Nash and Poland to the Clark-Wilson policy is concerned with	separation of duty

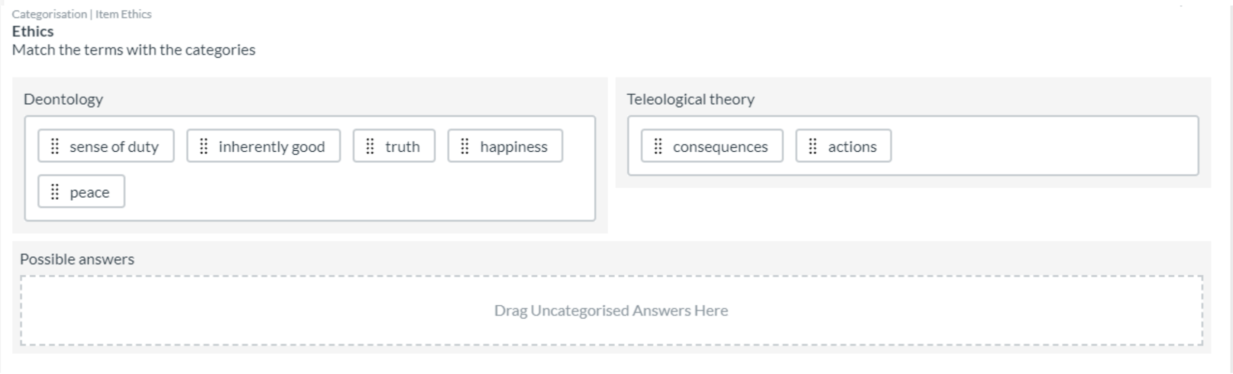


Fill in the Blank | Item Risk

Risk

There are three major methods to deal with the result of the risk analysis. Please answer in **lower case.**

One can accept the risk if treatments takes too long or would be too expensive to implement. One can avoid the risk by not proceeding with some activity. Finally, one can also transfer the risk to, for example, an insurance company.



Categorisation | Item Ethics

Ethics

Match the terms with the categories

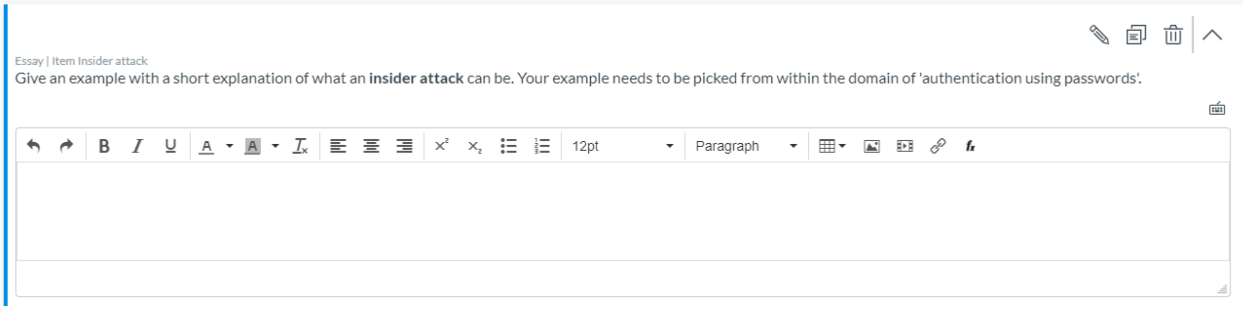
Deontology: sense of duty; inherently good; truth; happiness; peace

Teleological theory: consequences; actions

Possible answers

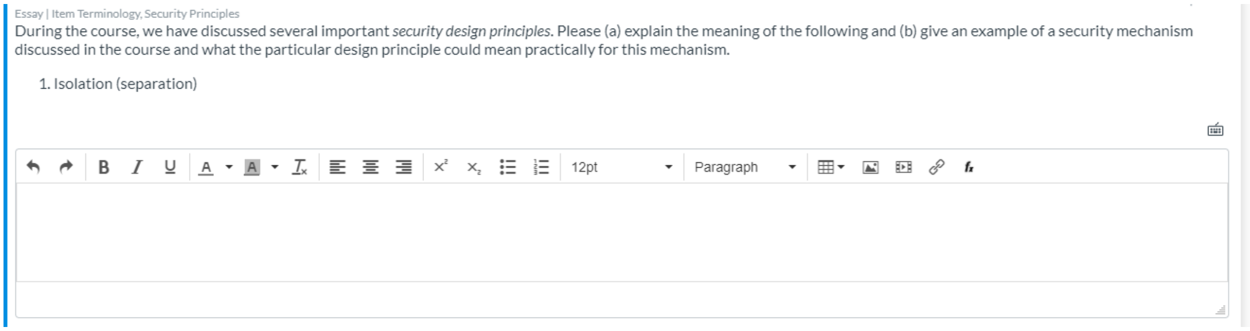
Drag Uncategorised Answers Here

Slow Recall, 3 questions, 5 points per question



Essay | Item Insider attack

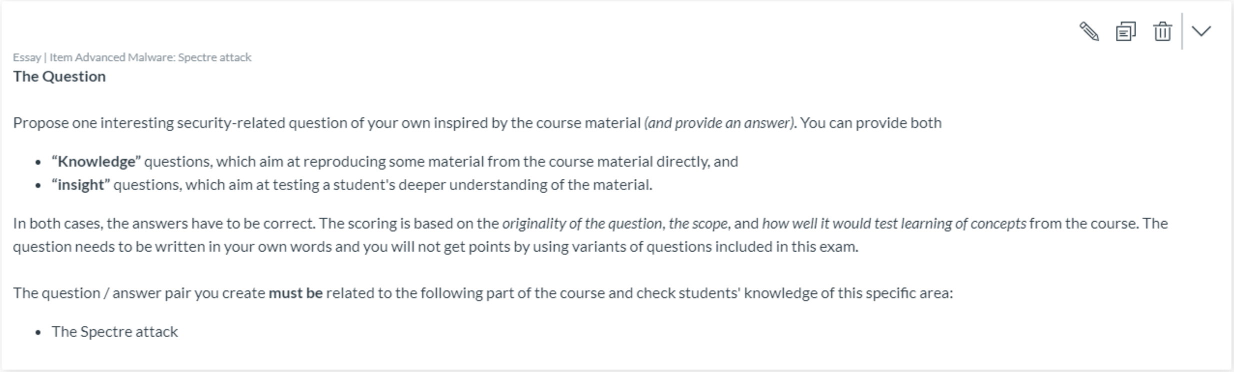
Give an example with a short explanation of what an **insider attack** can be. Your example needs to be picked from within the domain of 'authentication using passwords'.



Essay | Item Terminology, Security Principles

During the course, we have discussed several important *security design principles*. Please (a) explain the meaning of the following and (b) give an example of a security mechanism discussed in the course and what the particular design principle could mean practically for this mechanism.

1. Isolation (separation)



Essay | Item Advanced Malware: Spectre attack

The Question

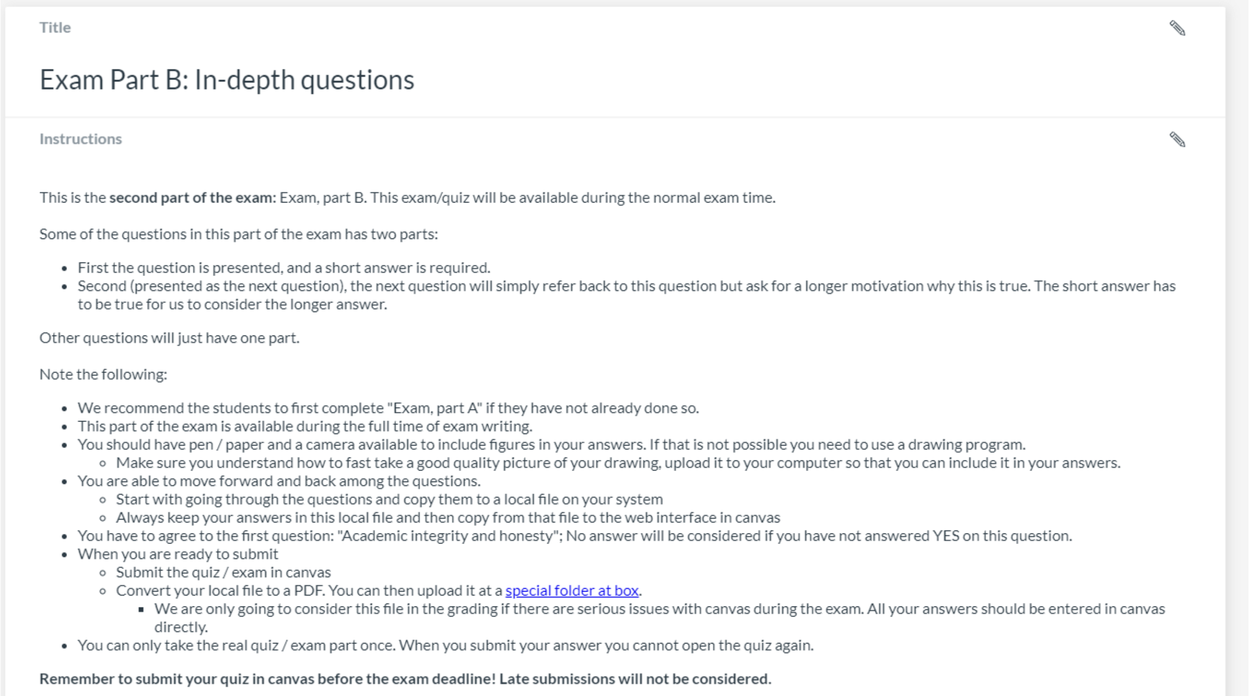
Propose one interesting security-related question of your own inspired by the course material *(and provide an answer)*. You can provide both

- **"Knowledge"** questions, which aim at reproducing some material from the course material directly, and
- **"insight"** questions, which aim at testing a student's deeper understanding of the material.

In both cases, the answers have to be correct. The scoring is based on the *originality of the question*, *the scope*, and *how well it would test learning of concepts* from the course. The question needs to be written in your own words and you will not get points by using variants of questions included in this exam.

The question / answer pair you create **must be** related to the following part of the course and check students' knowledge of this specific area:

- The Spectre attack



Title

Exam Part B: In-depth questions

Instructions

This is the **second part of the exam:** Exam, part B. This exam/quiz will be available during the normal exam time.

Some of the questions in this part of the exam has two parts:

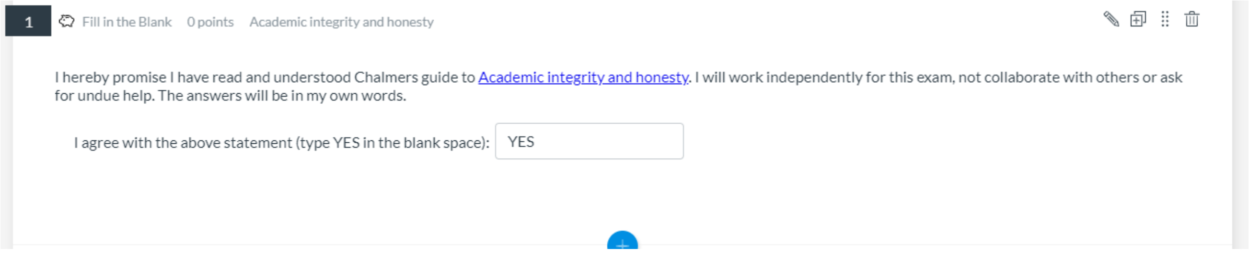
- First the question is presented, and a short answer is required.
- Second (presented as the next question), the next question will simply refer back to this question but ask for a longer motivation why this is true. The short answer has to be true for us to consider the longer answer.

Other questions will just have one part.

Note the following:

- We recommend the students to first complete "Exam, part A" if they have not already done so.
- This part of the exam is available during the full time of exam writing.
- You should have pen / paper and a camera available to include figures in your answers. If that is not possible you need to use a drawing program.
  - Make sure you understand how to fast take a good quality picture of your drawing, upload it to your computer so that you can include it in your answers.
- You are able to move forward and back among the questions.
  - Start with going through the questions and copy them to a local file on your system
  - Always keep your answers in this local file and then copy from that file to the web interface in canvas
- You have to agree to the first question: "Academic integrity and honesty"; No answer will be considered if you have not answered YES on this question.
- When you are ready to submit
  - Submit the quiz / exam in canvas
  - Convert your local file to a PDF. You can then upload it at a special folder at box.
    - We are only going to consider this file in the grading if there are serious issues with canvas during the exam. All your answers should be entered in canvas directly.
- You can only take the real quiz / exam part once. When you submit your answer you cannot open the quiz again.

Remember to submit your quiz in canvas before the exam deadline! Late submissions will not be considered.

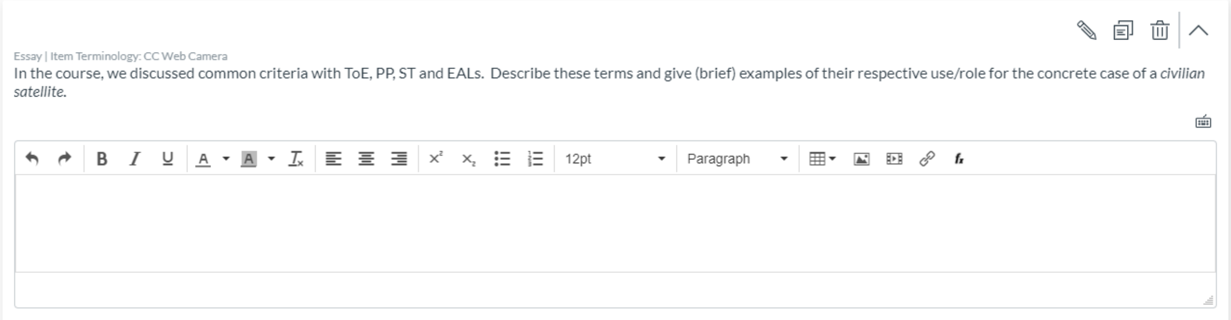


1 Fill in the Blank 0 points Academic integrity and honesty

I hereby promise I have read and understood Chalmers guide to Academic integrity and honesty. I will work independently for this exam, not collaborate with others or ask for undue help. The answers will be in my own words.

I agree with the above statement (type YES in the blank space): YES

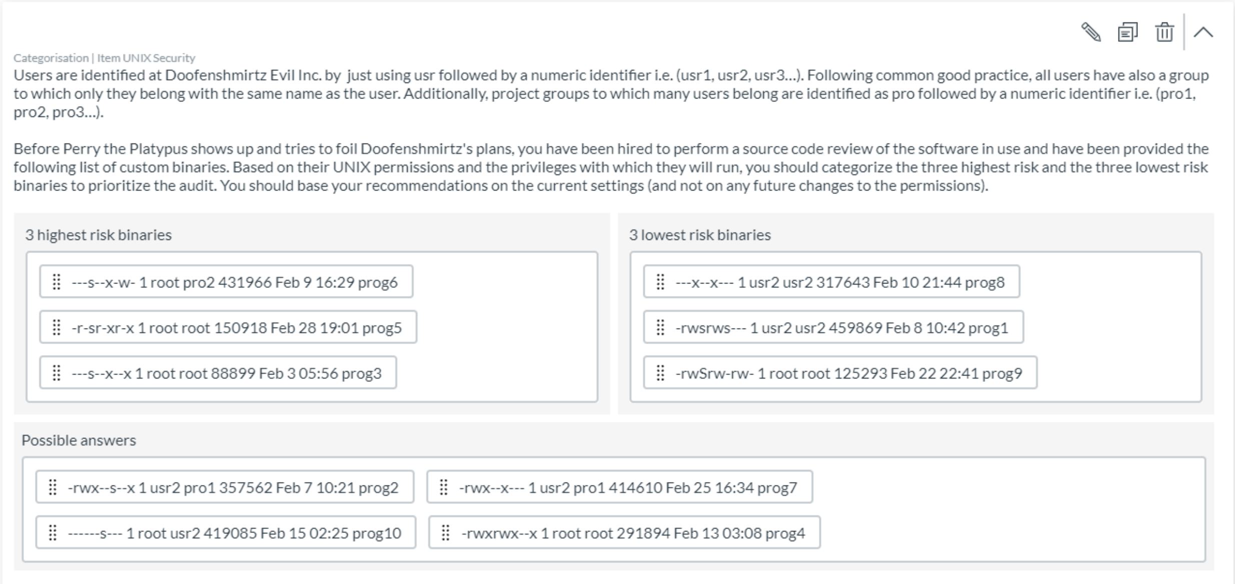
Question 2: 6 points



Essay | Item Terminology: CC Web Camera

In the course, we discussed common criteria with ToE, PP, ST and EALs. Describe these terms and give (brief) examples of their respective use/role for the concrete case of a *civilian satellite.*

Question 3: 10 points



Categorisation | Item UNIX Security

Users are identified at Doofenshmirtz Evil Inc. by just using usr followed by a numeric identifier i.e. (usr1, usr2, usr3...). Following common good practice, all users have also a group to which only they belong with the same name as the user. Additionally, project groups to which many users belong are identified as pro followed by a numeric identifier i.e. (pro1, pro2, pro3...).

Before Perry the Platypus shows up and tries to foil Doofenshmirtz's plans, you have been hired to perform a source code review of the software in use and have been provided the following list of custom binaries. Based on their UNIX permissions and the privileges with which they will run, you should categorize the three highest risk and the three lowest risk binaries to prioritize the audit. You should base your recommendations on the current settings (and not on any future changes to the permissions).

3 highest risk binaries

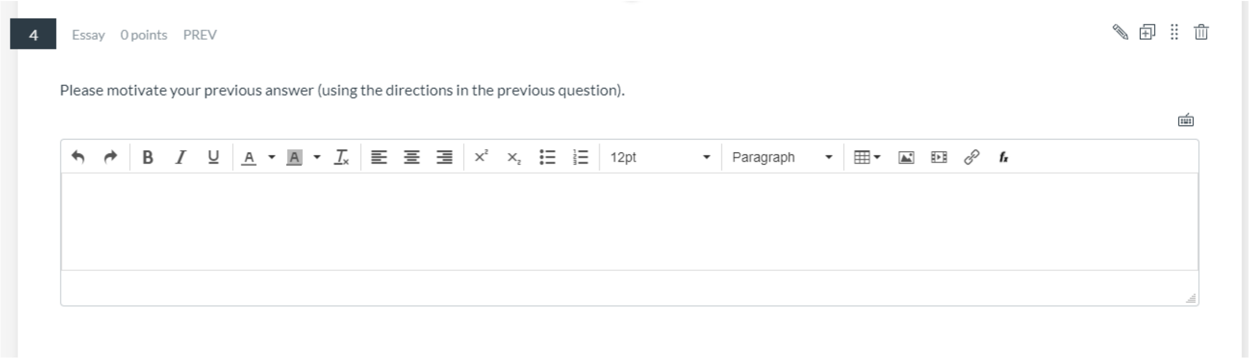
```
---s--x-w- 1 root pro2 431966 Feb 9 16:29 prog6
-r-sr-xr-x 1 root root 150918 Feb 28 19:01 prog5
---s--x--x 1 root root 88899 Feb 3 05:56 prog3
```

3 lowest risk binaries

```
---x--x--- 1 usr2 usr2 317643 Feb 10 21:44 prog8
-rwsrws--- 1 usr2 usr2 459869 Feb 8 10:42 prog1
-rwSrw-rw- 1 root root 125293 Feb 22 22:41 prog9
```

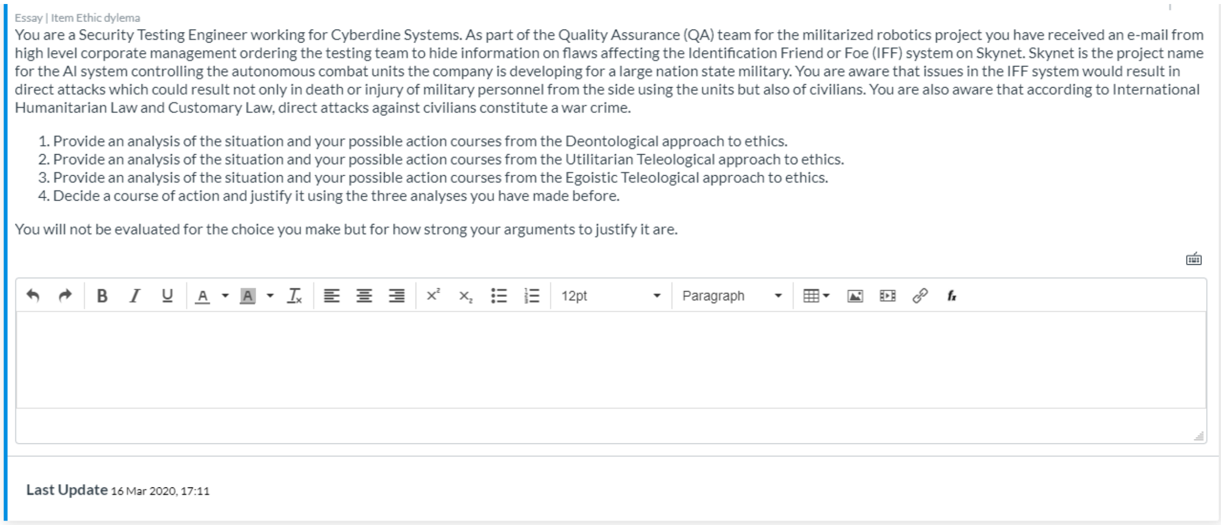
Possible answers

```
-rwx--s--x 1 usr2 pro1 357562 Feb 7 10:21 prog2
-rwx--x--- 1 usr2 pro1 414610 Feb 25 16:34 prog7
------s--- 1 root usr2 419085 Feb 15 02:25 prog10
-rwxrwx--x 1 root root 291894 Feb 13 03:08 prog4
```



Please motivate your previous answer (using the directions in the previous question).

Question 5: 5 points



Essay | Item Ethic dylema

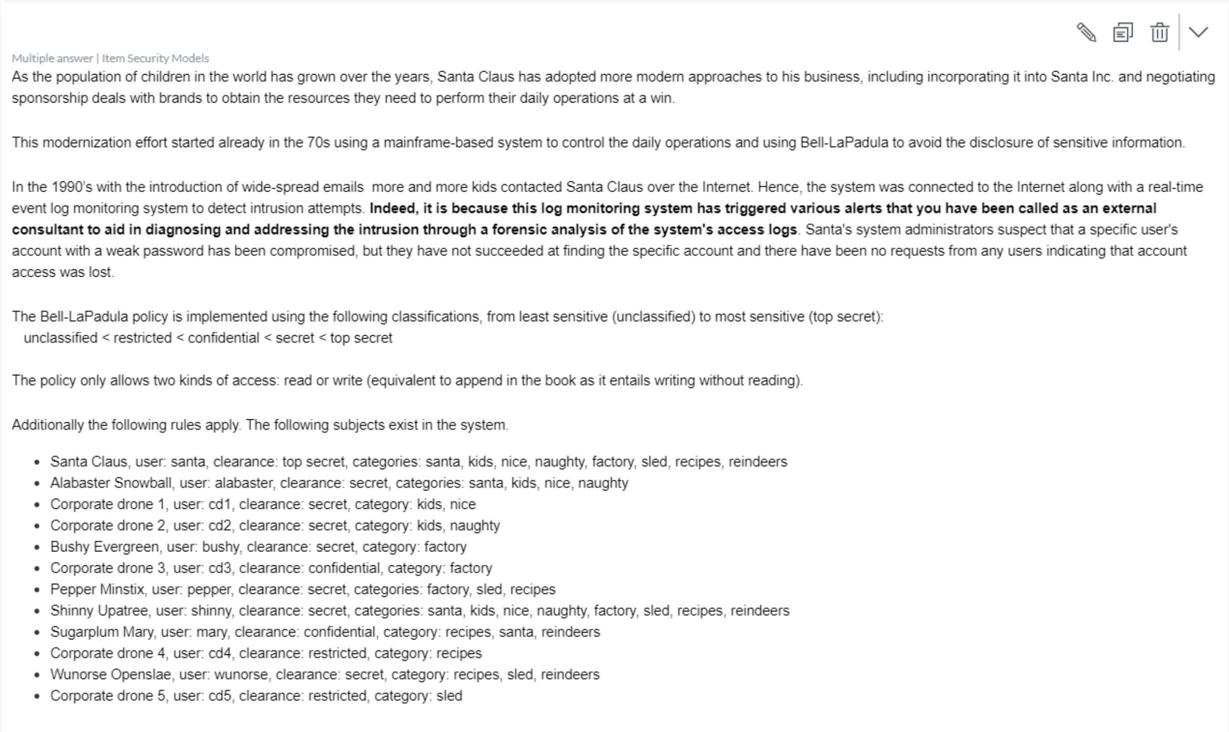
You are a Security Testing Engineer working for Cyberdine Systems. As part of the Quality Assurance (QA) team for the militarized robotics project you have received an e-mail from high level corporate management ordering the testing team to hide information on flaws affecting the Identification Friend or Foe (IFF) system on Skynet. Skynet is the project name for the AI system controlling the autonomous combat units the company is developing for a large nation state military. You are aware that issues in the IFF system would result in direct attacks which could result not only in death or injury of military personnel from the side using the units but also of civilians. You are also aware that according to International Humanitarian Law and Customary Law, direct attacks against civilians constitute a war crime.

1. Provide an analysis of the situation and your possible action courses from the Deontological approach to ethics.
2. Provide an analysis of the situation and your possible action courses from the Utilitarian Teleological approach to ethics.
3. Provide an analysis of the situation and your possible action courses from the Egoistic Teleological approach to ethics.
4. Decide a course of action and justify it using the three analyses you have made before.

You will not be evaluated for the choice you make but for how strong your arguments to justify it are.

Last Update 16 Mar 2020, 17:11

Question 6: 14 points



Multiple answer | Item Security Models

As the population of children in the world has grown over the years, Santa Claus has adopted more modern approaches to his business, including incorporating it into Santa Inc. and negotiating sponsorship deals with brands to obtain the resources they need to perform their daily operations at a win.

This modernization effort started already in the 70s using a mainframe-based system to control the daily operations and using Bell-LaPadula to avoid the disclosure of sensitive information.

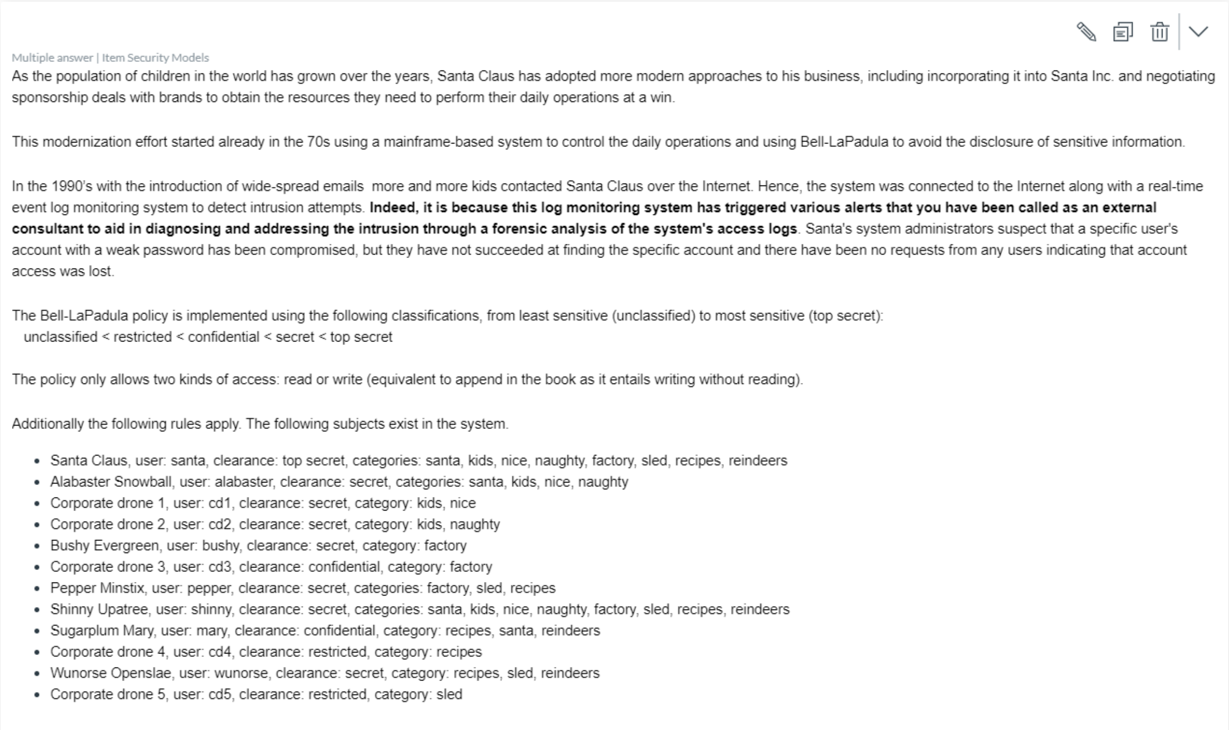
In the 1990's with the introduction of wide-spread emails more and more kids contacted Santa Claus over the Internet. Hence, the system was connected to the Internet along with a real-time event log monitoring system to detect intrusion attempts. **Indeed, it is because this log monitoring system has triggered various alerts that you have been called as an external consultant to aid in diagnosing and addressing the intrusion through a forensic analysis of the system's access logs**. Santa's system administrators suspect that a specific user's account with a weak password has been compromised, but they have not succeeded at finding the specific account and there have been no requests from any users indicating that account access was lost.

The Bell-LaPadula policy is implemented using the following classifications, from least sensitive (unclassified) to most sensitive (top secret):
unclassified < restricted < confidential < secret < top secret

The policy only allows two kinds of access: read or write (equivalent to append in the book as it entails writing without reading).

Additionally the following rules apply. The following subjects exist in the system.

- Santa Claus, user: santa, clearance: top secret, categories: santa, kids, nice, naughty, factory, sled, recipes, reindeers
- Alabaster Snowball, user: alabaster, clearance: secret, categories: santa, kids, nice, naughty
- Corporate drone 1, user: cd1, clearance: secret, category: kids, nice
- Corporate drone 2, user: cd2, clearance: secret, category: kids, naughty
- Bushy Evergreen, user: bushy, clearance: secret, category: factory
- Corporate drone 3, user: cd3, clearance: confidential, category: factory
- Pepper Minstix, user: pepper, clearance: secret, categories: factory, sled, recipes
- Shinny Upatree, user: shinny, clearance: secret, categories: santa, kids, nice, naughty, factory, sled, recipes, reindeers
- Sugarplum Mary, user: mary, clearance: confidential, category: recipes, santa, reindeers
- Corporate drone 4, user: cd4, clearance: restricted, category: recipes
- Wunorse Openslae, user: wunorse, clearance: secret, category: recipes, sled, reindeers
- Corporate drone 5, user: cd5, clearance: restricted, category: sled



Multiple answer | Item Security Models

As the population of children in the world has grown over the years, Santa Claus has adopted more modern approaches to his business, including incorporating it into Santa Inc. and negotiating sponsorship deals with brands to obtain the resources they need to perform their daily operations at a win.

This modernization effort started already in the 70s using a mainframe-based system to control the daily operations and using Bell-LaPadula to avoid the disclosure of sensitive information.

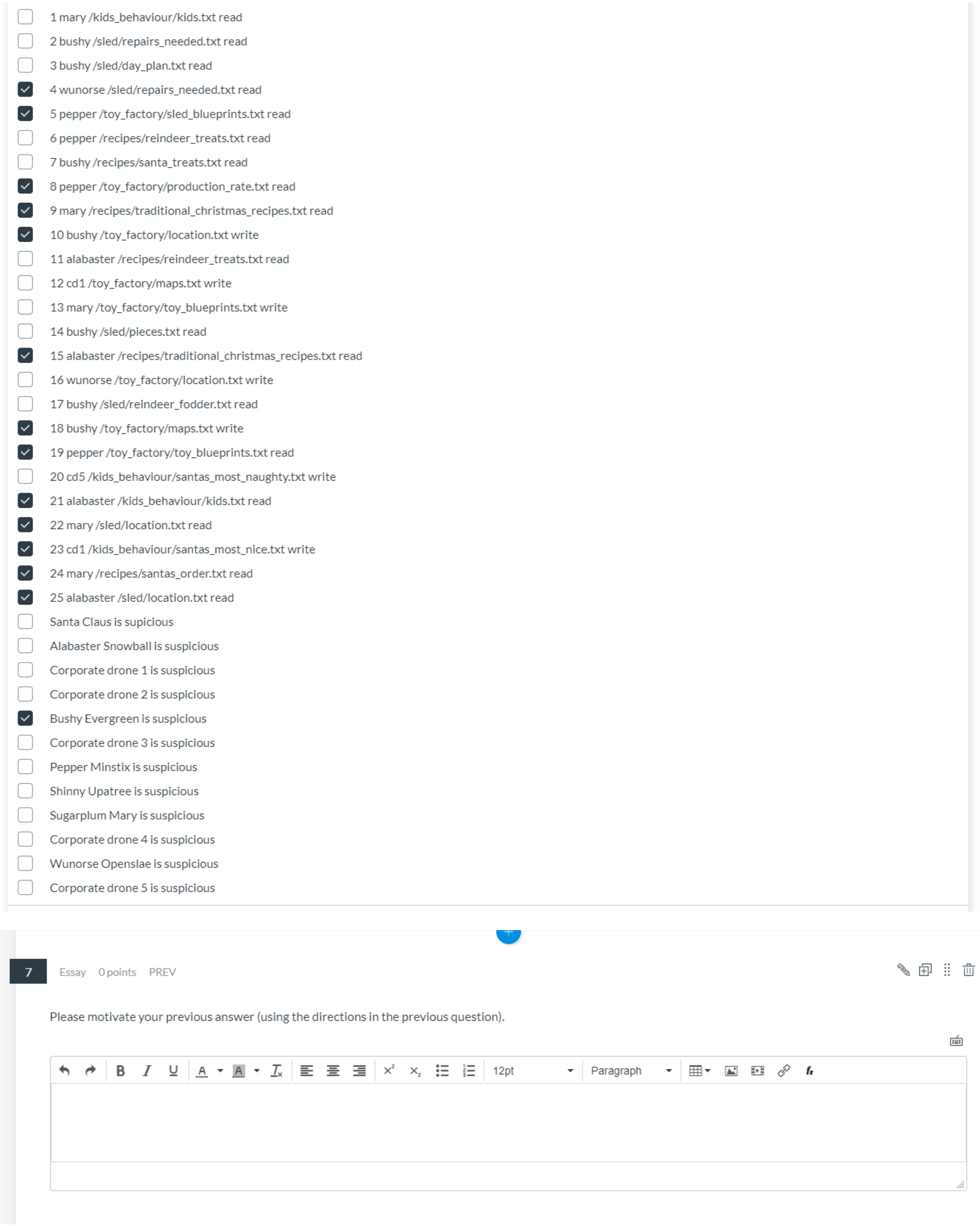
In the 1990's with the introduction of wide-spread emails more and more kids contacted Santa Claus over the Internet. Hence, the system was connected to the Internet along with a real-time event log monitoring system to detect intrusion attempts. **Indeed, it is because this log monitoring system has triggered various alerts that you have been called as an external consultant to aid in diagnosing and addressing the intrusion through a forensic analysis of the system's access logs**. Santa's system administrators suspect that a specific user's account with a weak password has been compromised, but they have not succeeded at finding the specific account and there have been no requests from any users indicating that account access was lost.

The Bell-LaPadula policy is implemented using the following classifications, from least sensitive (unclassified) to most sensitive (top secret):
unclassified < restricted < confidential < secret < top secret

The policy only allows two kinds of access: read or write (equivalent to append in the book as it entails writing without reading).

Additionally the following rules apply. The following subjects exist in the system.

- Santa Claus, user: santa, clearance: top secret, categories: santa, kids, nice, naughty, factory, sled, recipes, reindeers
- Alabaster Snowball, user: alabaster, clearance: secret, categories: santa, kids, nice, naughty
- Corporate drone 1, user: cd1, clearance: secret, category: kids, nice
- Corporate drone 2, user: cd2, clearance: secret, category: kids, naughty
- Bushy Evergreen, user: bushy, clearance: secret, category: factory
- Corporate drone 3, user: cd3, clearance: confidential, category: factory
- Pepper Minstix, user: pepper, clearance: secret, categories: factory, sled, recipes
- Shinny Upatree, user: shinny, clearance: secret, categories: santa, kids, nice, naughty, factory, sled, recipes, reindeers
- Sugarplum Mary, user: mary, clearance: confidential, category: recipes, santa, reindeers
- Corporate drone 4, user: cd4, clearance: restricted, category: recipes
- Wunorse Openslae, user: wunorse, clearance: secret, category: recipes, sled, reindeers
- Corporate drone 5, user: cd5, clearance: restricted, category: sled

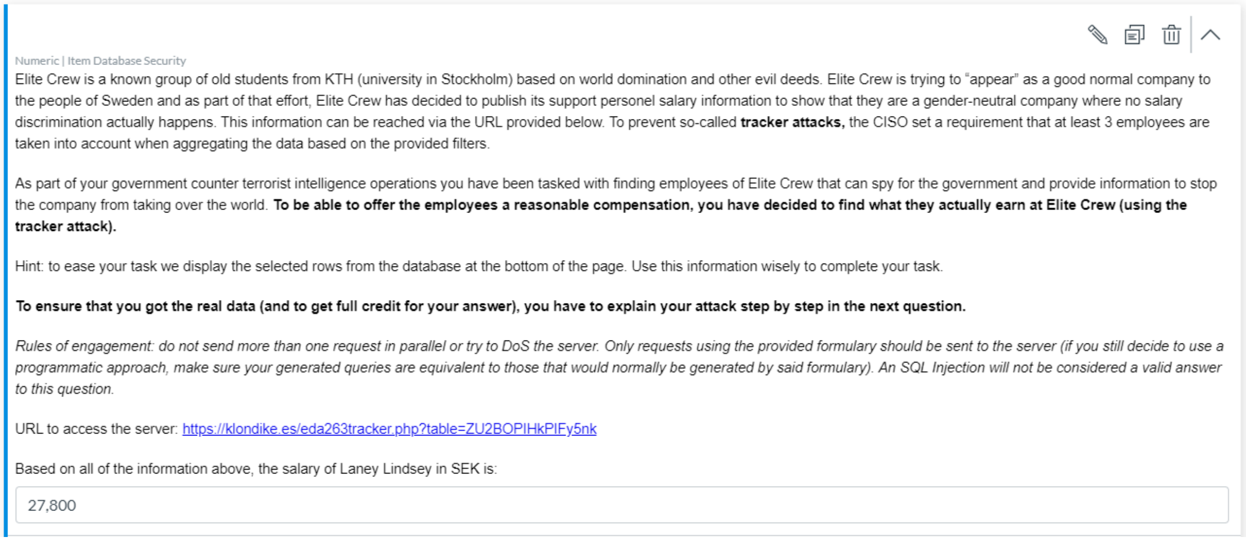


☐ 1 mary /kids_behaviour/kids.txt read
☐ 2 bushy /sled/repairs_needed.txt read
☐ 3 bushy /sled/day_plan.txt read
☑ 4 wunorse /sled/repairs_needed.txt read
☑ 5 pepper /toy_factory/sled_blueprints.txt read
☐ 6 pepper /recipes/reindeer_treats.txt read
☐ 7 bushy /recipes/santa_treats.txt read
☑ 8 pepper /toy_factory/production_rate.txt read
☑ 9 mary /recipes/traditional_christmas_recipes.txt read
☑ 10 bushy /toy_factory/location.txt write
☐ 11 alabaster /recipes/reindeer_treats.txt read
☐ 12 cd1 /toy_factory/maps.txt write
☐ 13 mary /toy_factory/toy_blueprints.txt write
☐ 14 bushy /sled/pieces.txt read
☑ 15 alabaster /recipes/traditional_christmas_recipes.txt read
☐ 16 wunorse /toy_factory/location.txt write
☐ 17 bushy /sled/reindeer_fodder.txt read
☑ 18 bushy /toy_factory/maps.txt write
☑ 19 pepper /toy_factory/toy_blueprints.txt read
☐ 20 cd5 /kids_behaviour/santas_most_naughty.txt write
☑ 21 alabaster /kids_behaviour/kids.txt read
☑ 22 mary /sled/location.txt read
☑ 23 cd1 /kids_behaviour/santas_most_nice.txt write
☑ 24 mary /recipes/santas_order.txt read
☑ 25 alabaster /sled/location.txt read
☐ Santa Claus is supicious
☐ Alabaster Snowball is suspicious
☐ Corporate drone 1 is suspicious
☐ Corporate drone 2 is suspicious
☑ Bushy Evergreen is suspicious
☐ Corporate drone 3 is suspicious
☐ Pepper Minstix is suspicious
☐ Shinny Upatree is suspicious
☐ Sugarplum Mary is suspicious
☐ Corporate drone 4 is suspicious
☐ Wunorse Openslae is suspicious
☐ Corporate drone 5 is suspicious

7 Essay 0 points PREV

Please motivate your previous answer (using the directions in the previous question).

Question 8: 15 points



Numeric | Item Database Security

Elite Crew is a known group of old students from KTH (university in Stockholm) based on world domination and other evil deeds. Elite Crew is trying to "appear" as a good normal company to the people of Sweden and as part of that effort, Elite Crew has decided to publish its support personel salary information to show that they are a gender-neutral company where no salary discrimination actually happens. This information can be reached via the URL provided below. To prevent so-called **tracker attacks,** the CISO set a requirement that at least 3 employees are taken into account when aggregating the data based on the provided filters.

As part of your government counter terrorist intelligence operations you have been tasked with finding employees of Elite Crew that can spy for the government and provide information to stop the company from taking over the world. **To be able to offer the employees a reasonable compensation, you have decided to find what they actually earn at Elite Crew (using the tracker attack).**

Hint: to ease your task we display the selected rows from the database at the bottom of the page. Use this information wisely to complete your task.

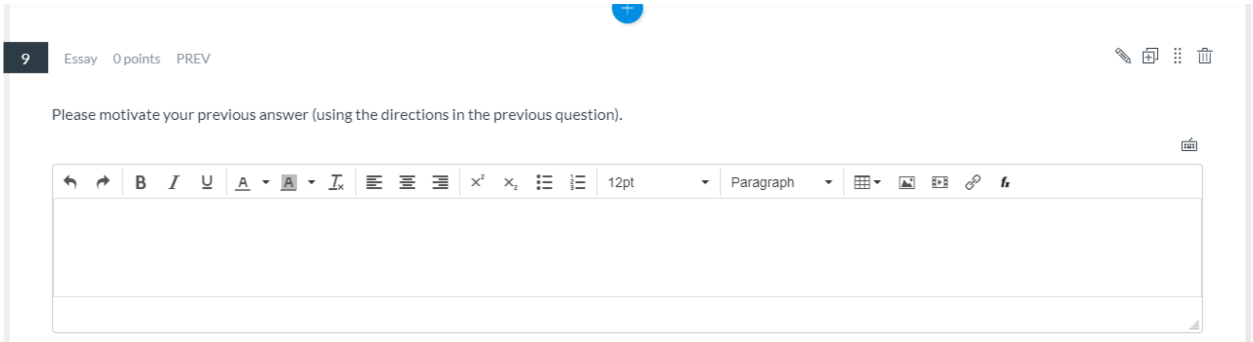
To ensure that you got the real data (and to get full credit for your answer), you have to explain your attack step by step in the next question.

Rules of engagement: do not send more than one request in parallel or try to DoS the server. Only requests using the provided formulary should be sent to the server (if you still decide to use a programmatic approach, make sure your generated queries are equivalent to those that would normally be generated by said formulary). An SQL Injection will not be considered a valid answer to this question.

URL to access the server: https://klondike.es/eda263tracker.php?table=ZU2BOPIHkPIFy5nk

Based on all of the information above, the salary of Laney Lindsey in SEK is:

27,800



9 Essay 0 points PREV

Please motivate your previous answer (using the directions in the previous question).