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, Wednesday August 26 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 Sep 17, 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.

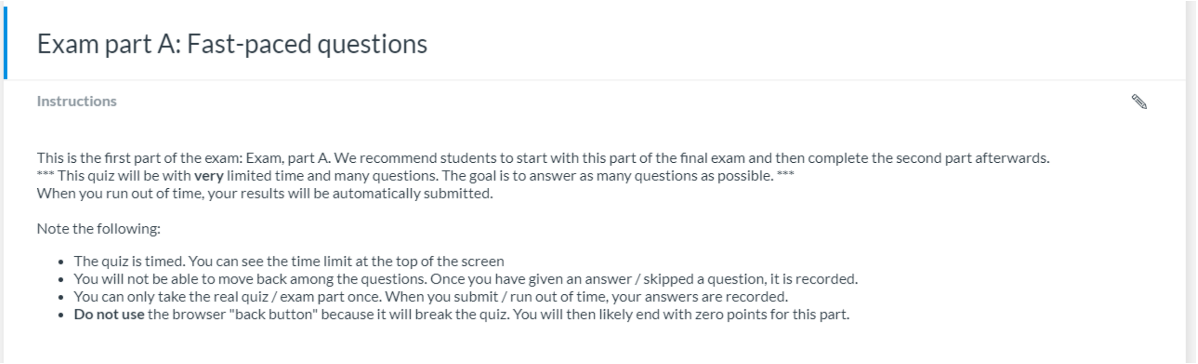
For previous exams, the has been determined as follows:

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

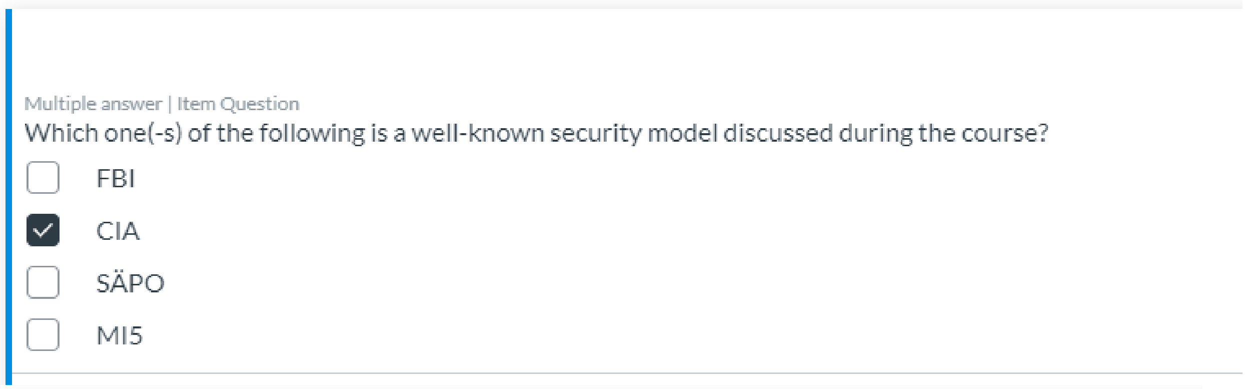
This is the first part of the exam: Exam, part A. We recommend students to start with this part of the final exam and then complete the second part afterwards.
*** This quiz will be with **very** limited time and many questions. The goal is to answer as many questions as possible. ***
When you run out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

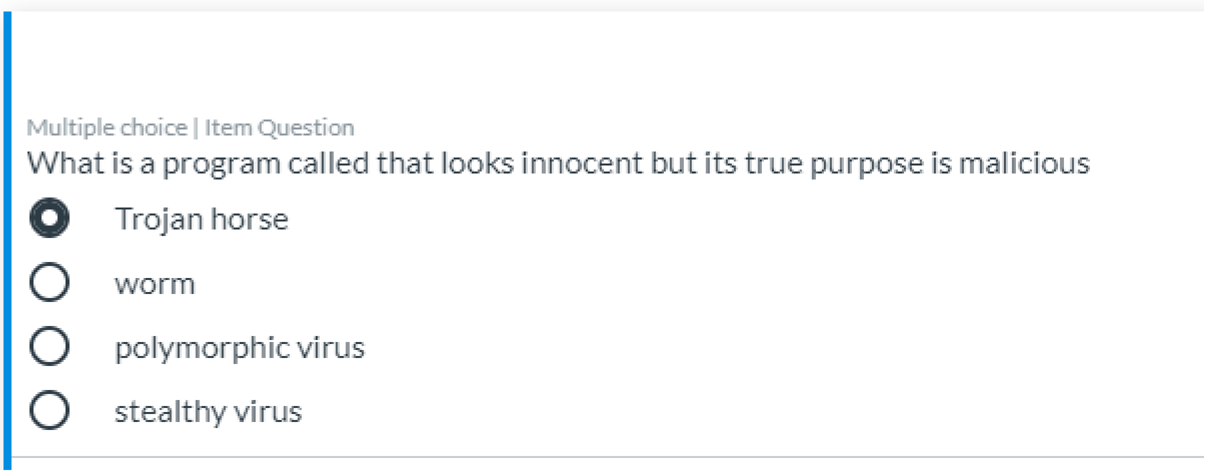
Which one(-s) of the following is a well-known security model discussed during the course?

□ FBI

☑ CIA

□ SÄPO

□ MI5



Multiple choice | Item Question

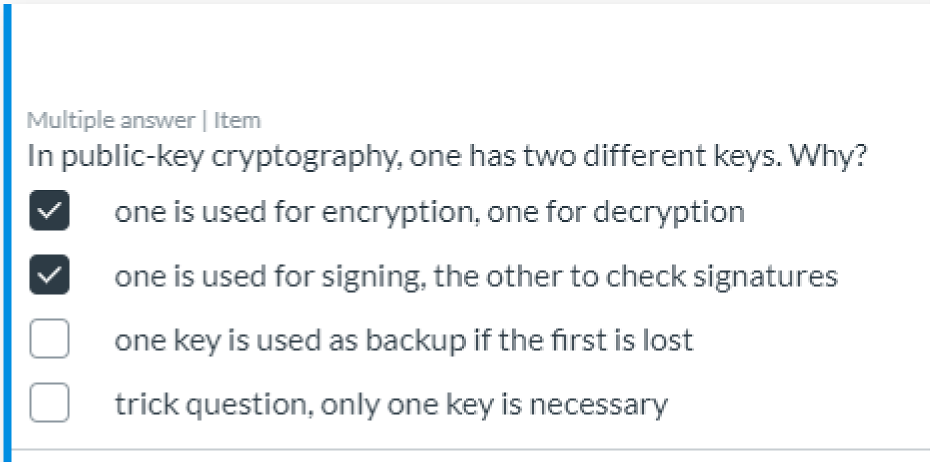
What is a program called that looks innocent but its true purpose is malicious

● Trojan horse

○ worm

○ polymorphic virus

○ stealthy virus



Multiple answer | Item

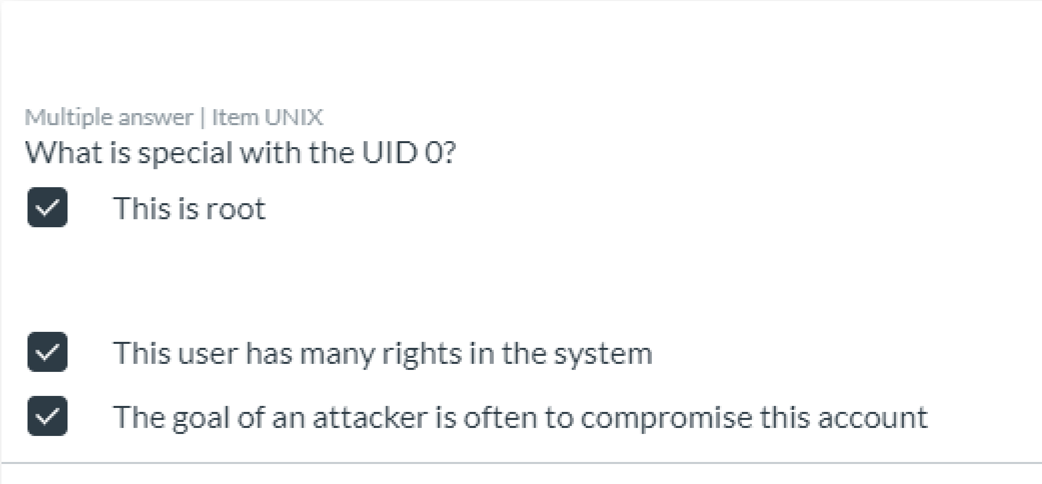
In public-key cryptography, one has two different keys. Why?

☑ 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



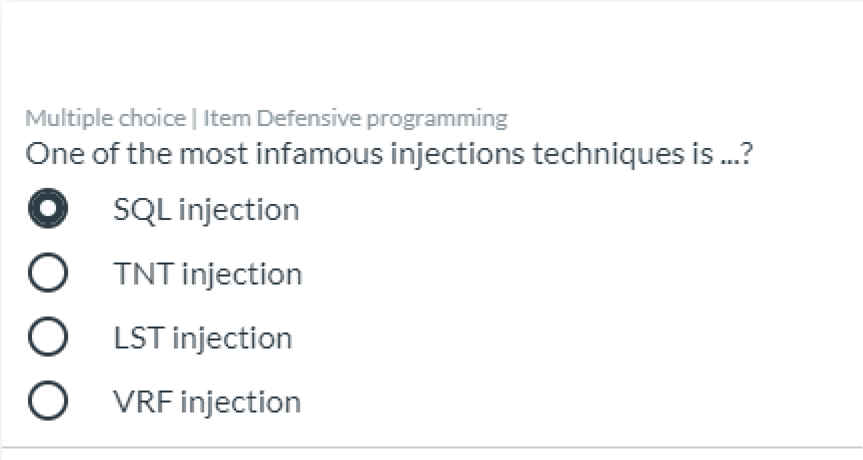
Multiple answer | Item UNIX

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 ...?

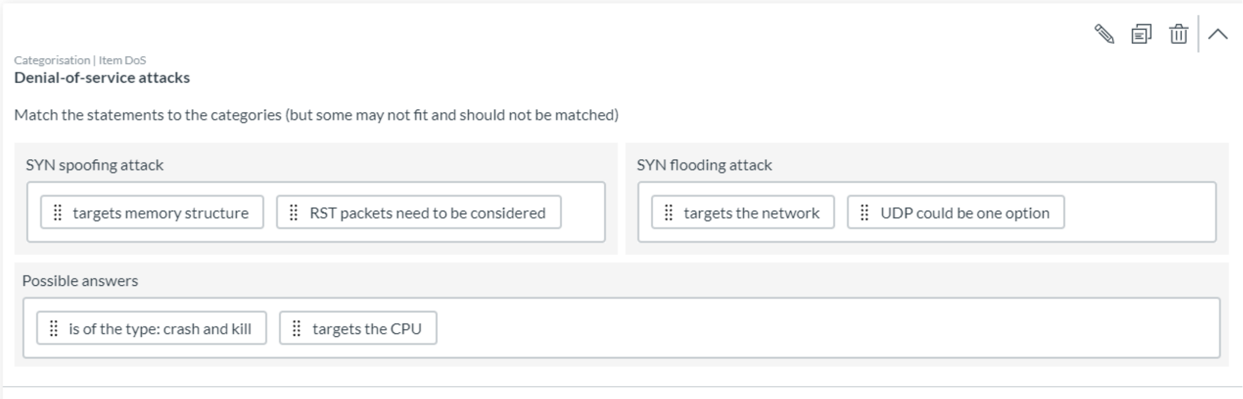
● SQL injection

○ 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

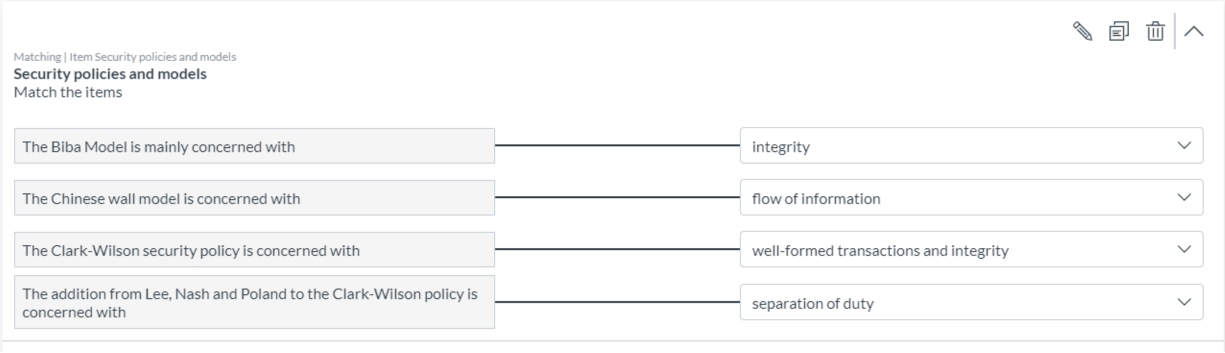
- targets memory structure
- RST packets need to be considered

SYN flooding attack

- targets the network
- UDP could be one option

Possible answers

- is of the type: crash and kill
- targets the CPU

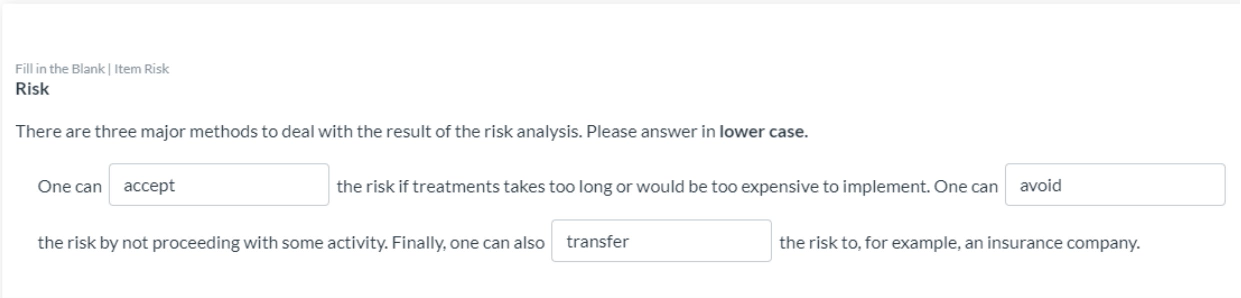


Matching | Item Security policies and models

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

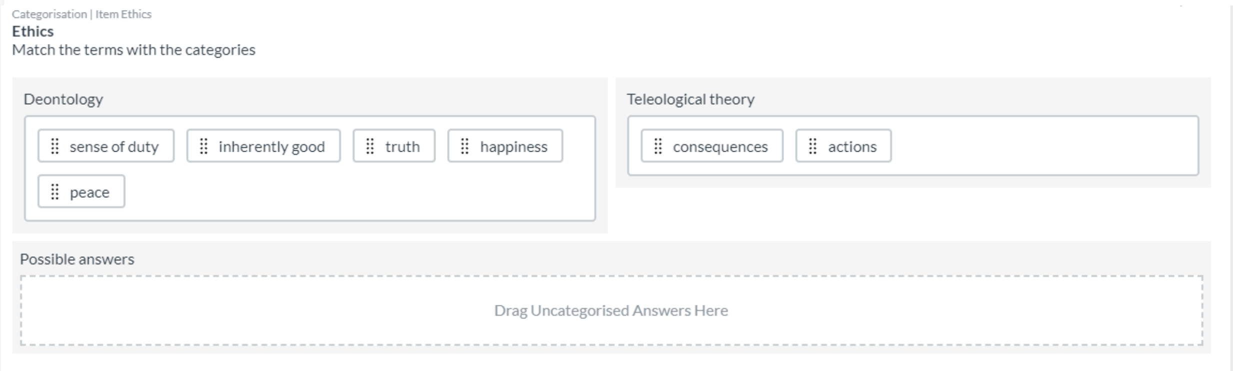


Fill in the Blank | Item Risk

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

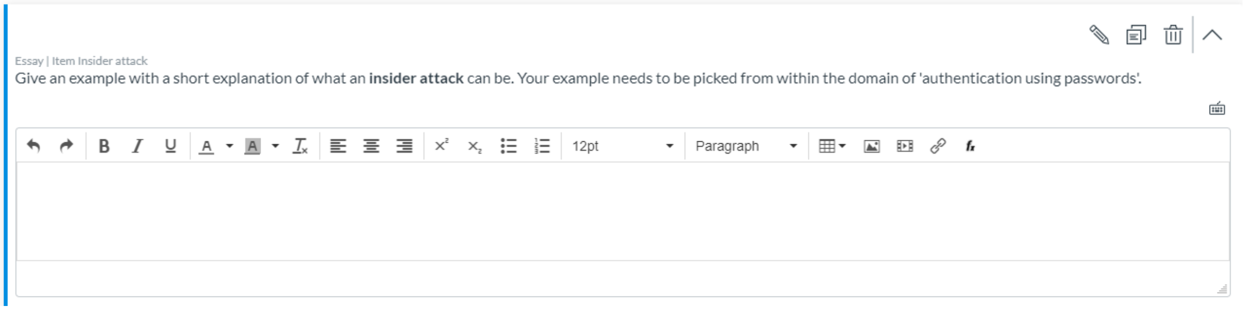
Teleological theory

- consequences
- actions

Possible answers

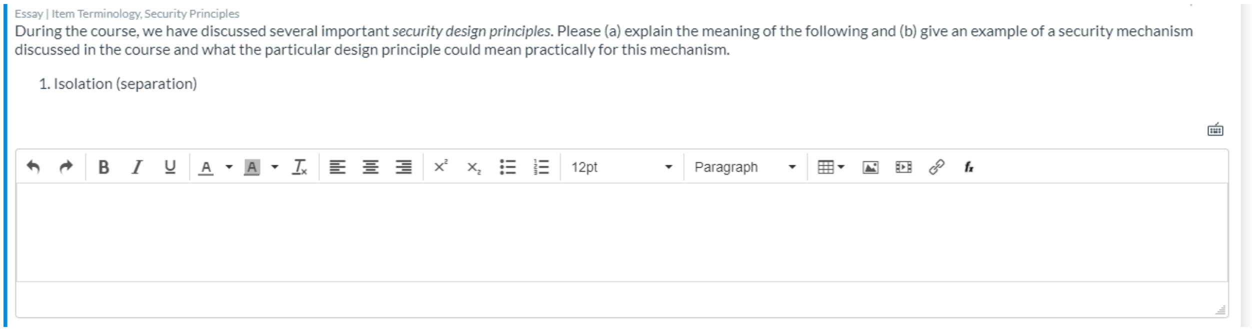
Drag Uncategorised Answers Here

Slow Recall, 3 questions, 5 points per question



Essay | Item Insider attack

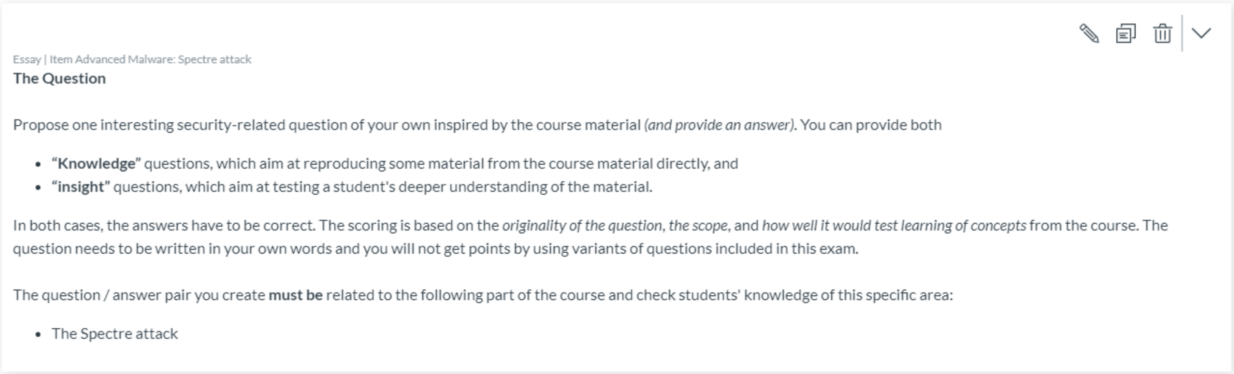
Give an example with a short explanation of what an **insider attack** can be. Your example needs to be picked from within the domain of 'authentication using passwords'.



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

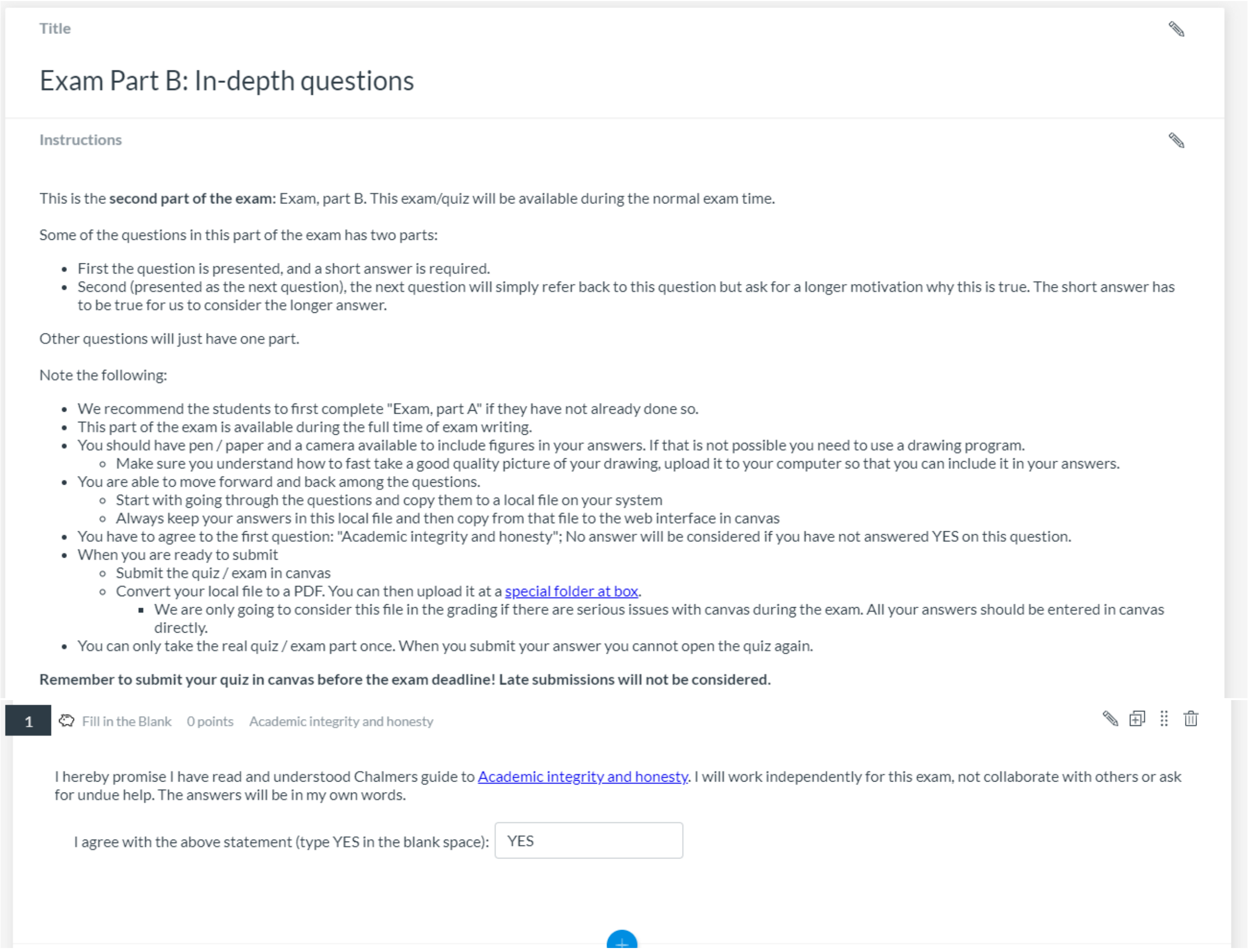
Propose one interesting security-related question of your own inspired by the course material *(and provide an answer)*. You can provide both

- **“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.

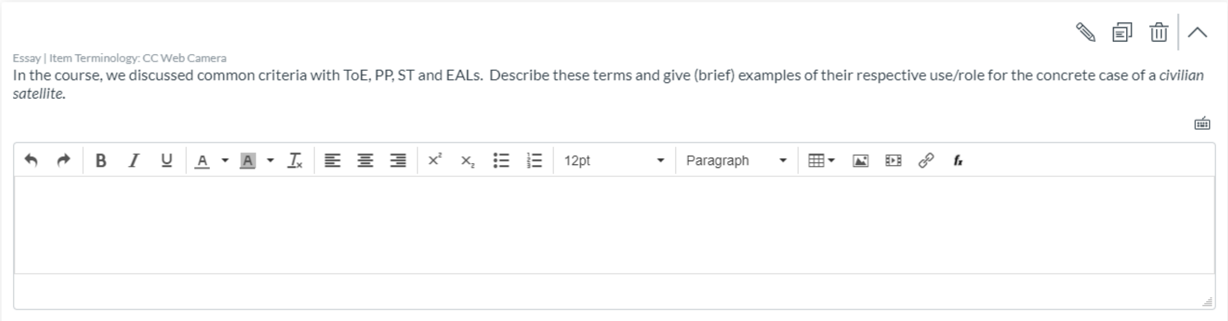
Remember to submit your quiz in canvas before the exam deadline! Late submissions will not be considered.

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

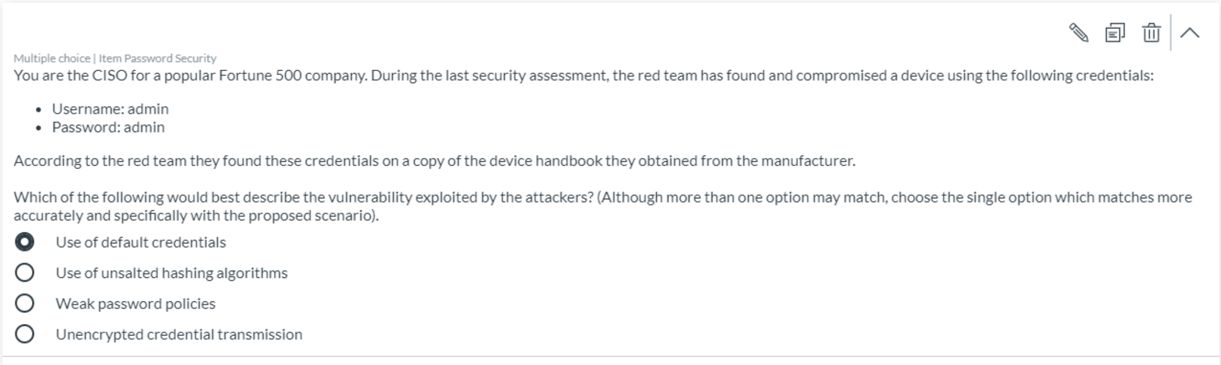
Question 2: 6 points



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: 1 point



Multiple choice | Item Password Security

You are the CISO for a popular Fortune 500 company. During the last security assessment, the red team has found and compromised a device using the following credentials:

- Username: admin
- Password: admin

According to the red team they found these credentials on a copy of the device handbook they obtained from the manufacturer.

Which of the following would best describe the vulnerability exploited by the attackers? (Although more than one option may match, choose the single option which matches more accurately and specifically with the proposed scenario).

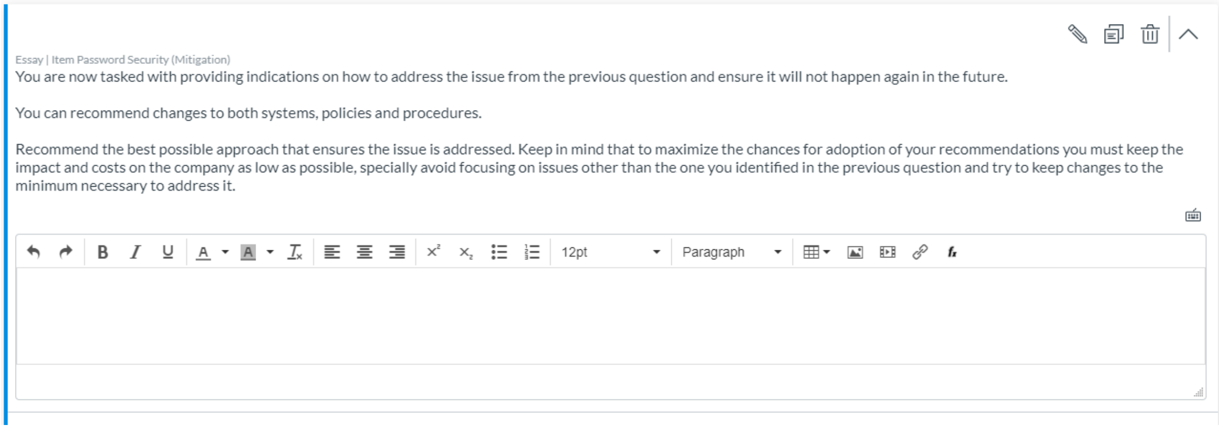
● Use of default credentials

○ Use of unsalted hashing algorithms

○ Weak password policies

○ Unencrypted credential transmission

Question 4: 9 points



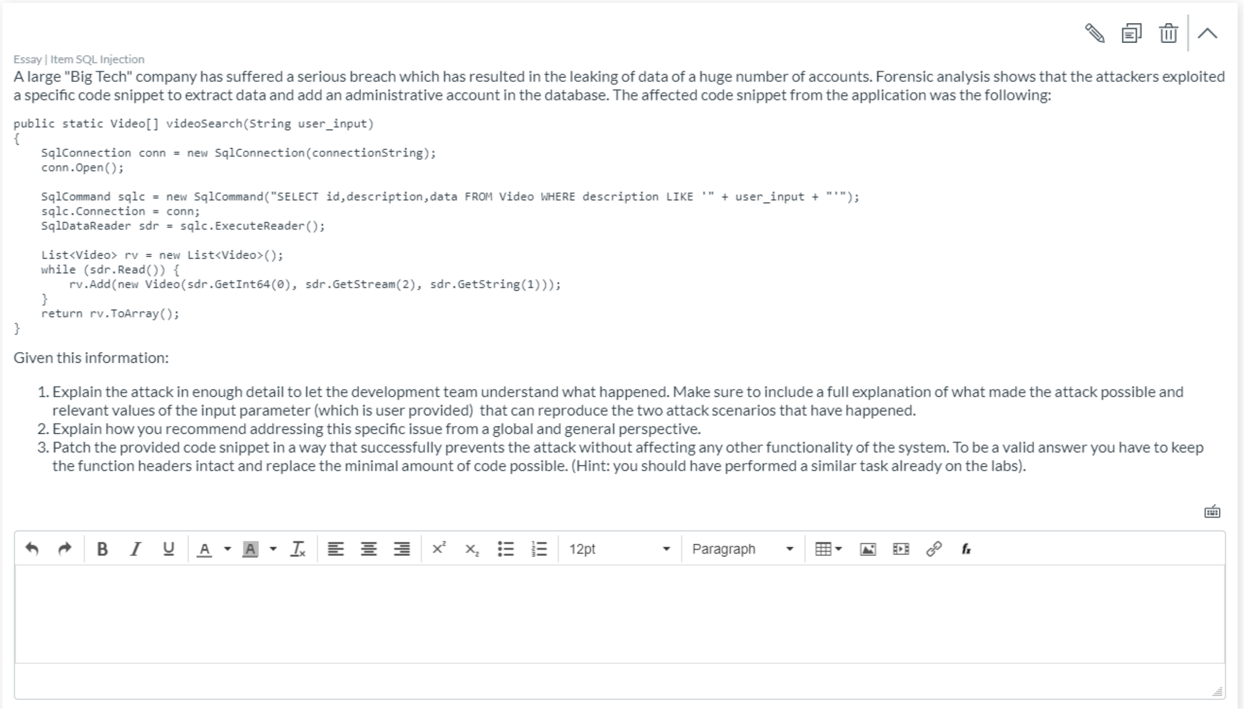
Essay | Item Password Security (Mitigation)

You are now tasked with providing indications on how to address the issue from the previous question and ensure it will not happen again in the future.

You can recommend changes to both systems, policies and procedures.

Recommend the best possible approach that ensures the issue is addressed. Keep in mind that to maximize the chances for adoption of your recommendations you must keep the impact and costs on the company as low as possible, specially avoid focusing on issues other than the one you identified in the previous question and try to keep changes to the minimum necessary to address it.

Question 5: 10 points



Essay | Item SQL Injection

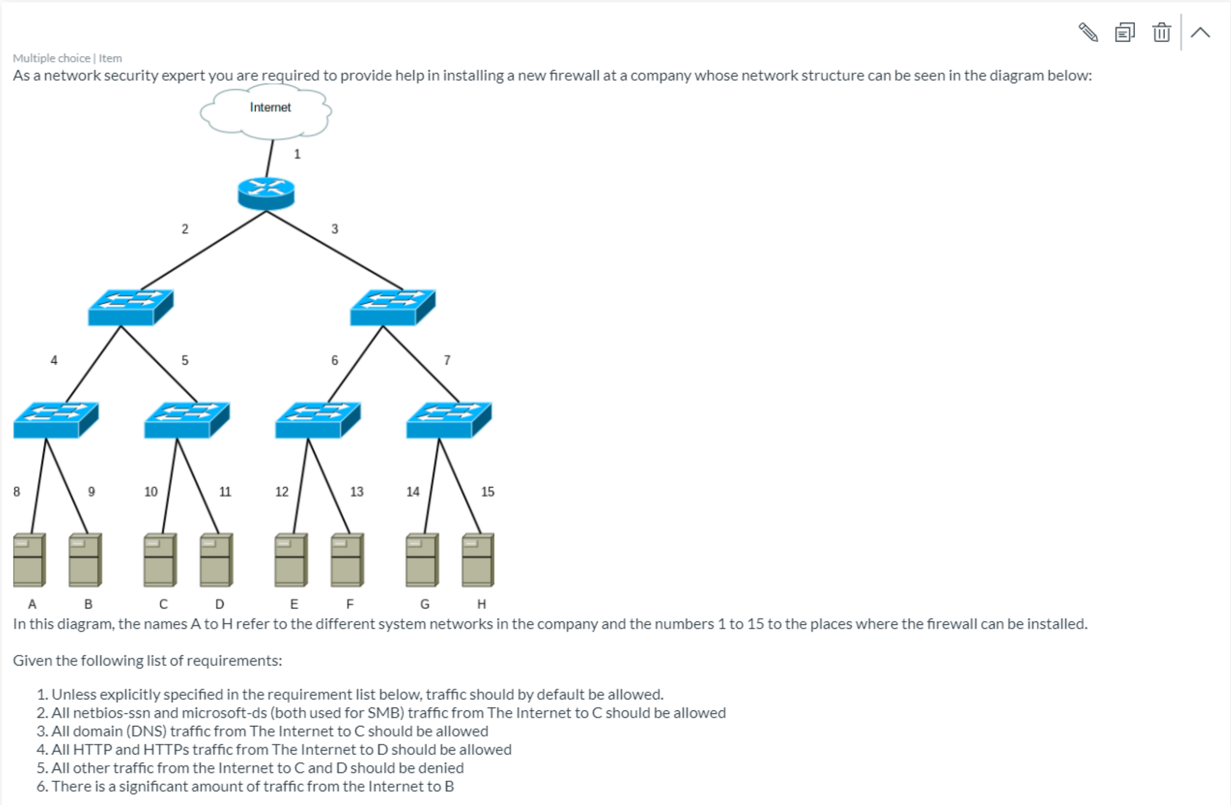
A large "Big Tech" company has suffered a serious breach which has resulted in the leaking of data of a huge number of accounts. Forensic analysis shows that the attackers exploited a specific code snippet to extract data and add an administrative account in the database. The affected code snippet from the application was the following:

```
public static Video[] videoSearch(String user_input)
{
    SqlConnection conn = new SqlConnection(connectionString);
    conn.Open();

    SqlCommand sqlc = new SqlCommand("SELECT id,description,data FROM Video WHERE description LIKE '" + user_input + "'");
    sqlc.Connection = conn;
    SqlDataReader sdr = sqlc.ExecuteReader();

    List<Video> rv = new List<Video>();
    while (sdr.Read()) {
        rv.Add(new Video(sdr.GetInt64(0), sdr.GetStream(2), sdr.GetString(1)));
    }
    return rv.ToArray();
}
```

Given this information:

1. Explain the attack in enough detail to let the development team understand what happened. Make sure to include a full explanation of what made the attack possible and relevant values of the input parameter (which is user provided) that can reproduce the two attack scenarios that have happened.
2. Explain how you recommend addressing this specific issue from a global and general perspective.
3. Patch the provided code snippet in a way that successfully prevents the attack without affecting any other functionality of the system. To be a valid answer you have to keep the function headers intact and replace the minimal amount of code possible. (Hint: you should have performed a similar task already on the labs).

Question 6: 1 point



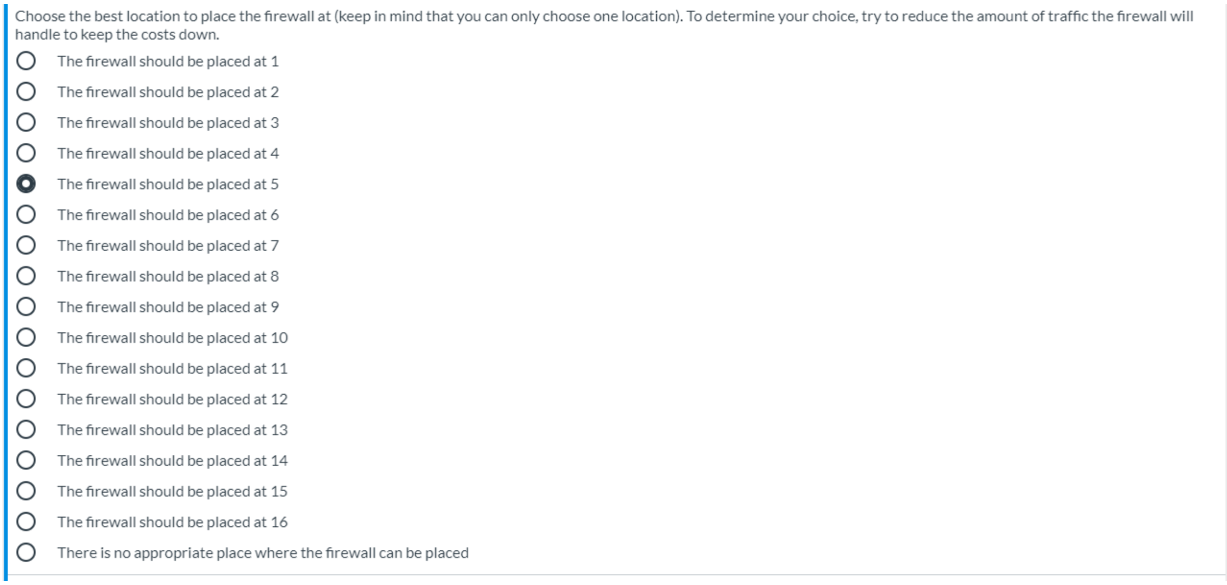
Multiple choice | Item

As a network security expert you are required to provide help in installing a new firewall at a company whose network structure can be seen in the diagram below:

In this diagram, the names A to H refer to the different system networks in the company and the numbers 1 to 15 to the places where the firewall can be installed.

Given the following list of requirements:

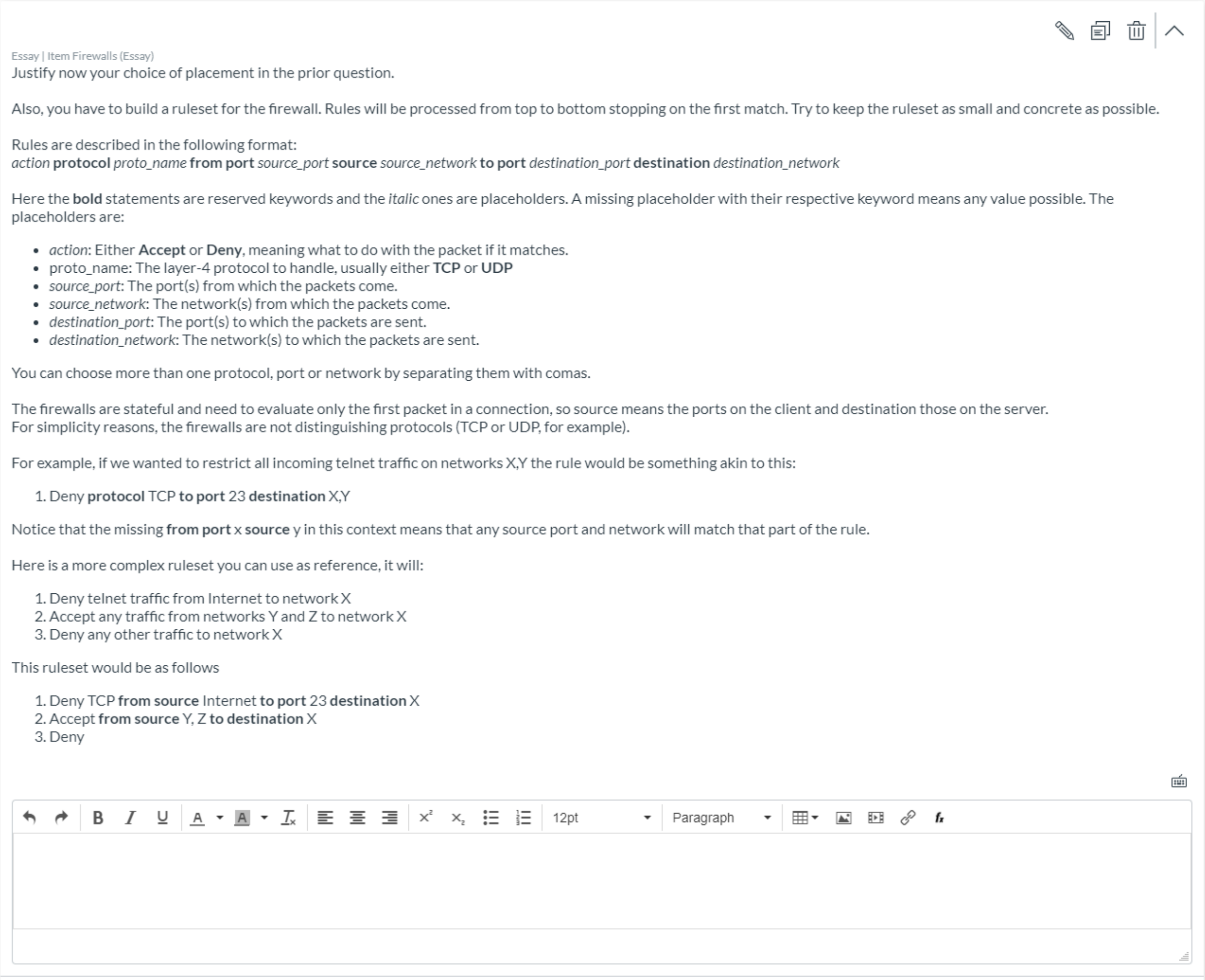
1. Unless explicitly specified in the requirement list below, traffic should by default be allowed.
2. All netbios-ssn and microsoft-ds (both used for SMB) traffic from The Internet to C should be allowed
3. All domain (DNS) traffic from The Internet to C should be allowed
4. All HTTP and HTTPs traffic from The Internet to D should be allowed
5. All other traffic from the Internet to C and D should be denied
6. There is a significant amount of traffic from the Internet to B



Choose the best location to place the firewall at (keep in mind that you can only choose one location). To determine your choice, try to reduce the amount of traffic the firewall will handle to keep the costs down.

○ The firewall should be placed at 1
○ The firewall should be placed at 2
○ The firewall should be placed at 3
○ The firewall should be placed at 4
● The firewall should be placed at 5
○ The firewall should be placed at 6
○ The firewall should be placed at 7
○ The firewall should be placed at 8
○ The firewall should be placed at 9
○ The firewall should be placed at 10
○ The firewall should be placed at 11
○ The firewall should be placed at 12
○ The firewall should be placed at 13
○ The firewall should be placed at 14
○ The firewall should be placed at 15
○ The firewall should be placed at 16
○ There is no appropriate place where the firewall can be placed

Question 7: 9 points



Essay | Item Firewalls (Essay)

Justify now your choice of placement in the prior question.

Also, you have to build a ruleset for the firewall. Rules will be processed from top to bottom stopping on the first match. Try to keep the ruleset as small and concrete as possible.

Rules are described in the following format:
action **protocol** *proto_name* **from port** *source_port* **source** *source_network* **to port** *destination_port* **destination** *destination_network*

Here the **bold** statements are reserved keywords and the *italic* ones are placeholders. A missing placeholder with their respective keyword means any value possible. The placeholders are:

- *action*: Either **Accept** or **Deny**, meaning what to do with the packet if it matches.
- proto_name: The layer-4 protocol to handle, usually either **TCP** or **UDP**
- *source_port*: The port(s) from which the packets come.
- *source_network*: The network(s) from which the packets come.
- *destination_port*: The port(s) to which the packets are sent.
- *destination_network*: The network(s) to which the packets are sent.

You can choose more than one protocol, port or network by separating them with comas.

The firewalls are stateful and need to evaluate only the first packet in a connection, so source means the ports on the client and destination those on the server.
For simplicity reasons, the firewalls are not distinguishing protocols (TCP or UDP, for example).

For example, if we wanted to restrict all incoming telnet traffic on networks X,Y the rule would be something akin to this:

1. Deny **protocol** TCP **to port** 23 **destination** X,Y

Notice that the missing **from port** x **source** y in this context means that any source port and network will match that part of the rule.

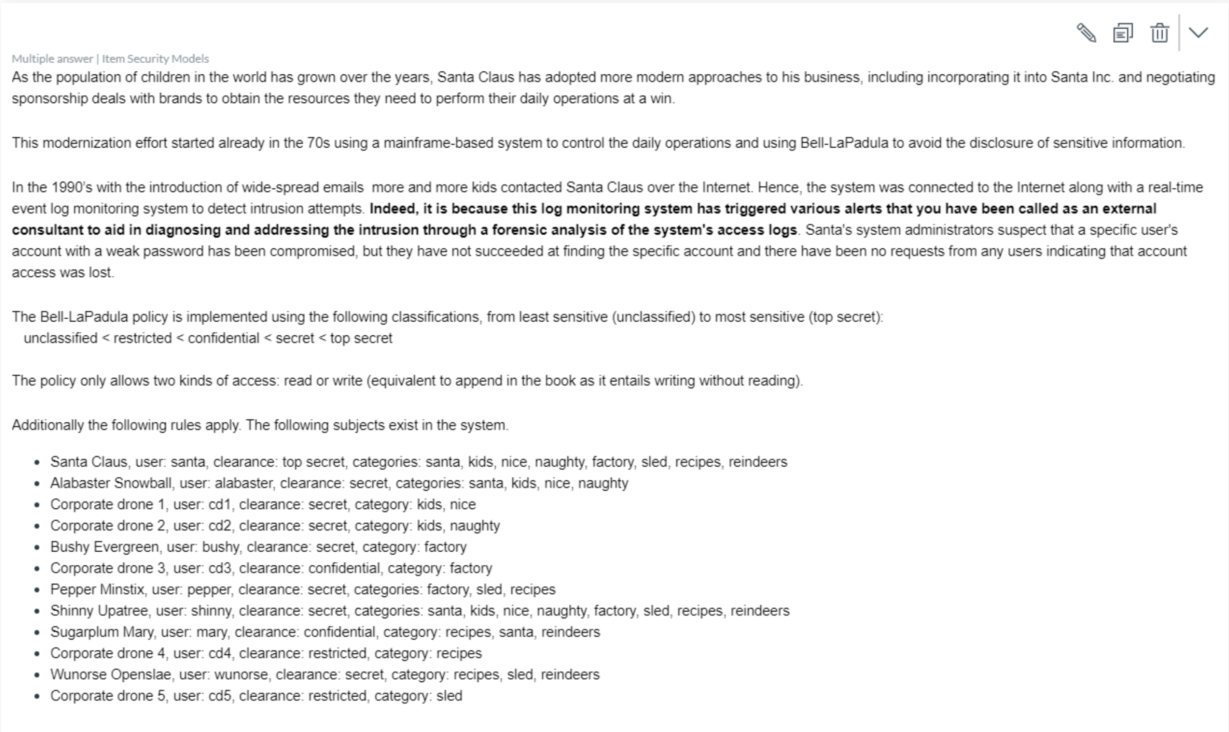
Here is a more complex ruleset you can use as reference, it will:

1. Deny telnet traffic from Internet to network X
2. Accept any traffic from networks Y and Z to network X
3. Deny any other traffic to network X

This ruleset would be as follows

1. Deny TCP **from source** Internet **to port** 23 **destination** X
2. Accept **from source** Y, Z **to destination** X
3. Deny

Question 8: 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.

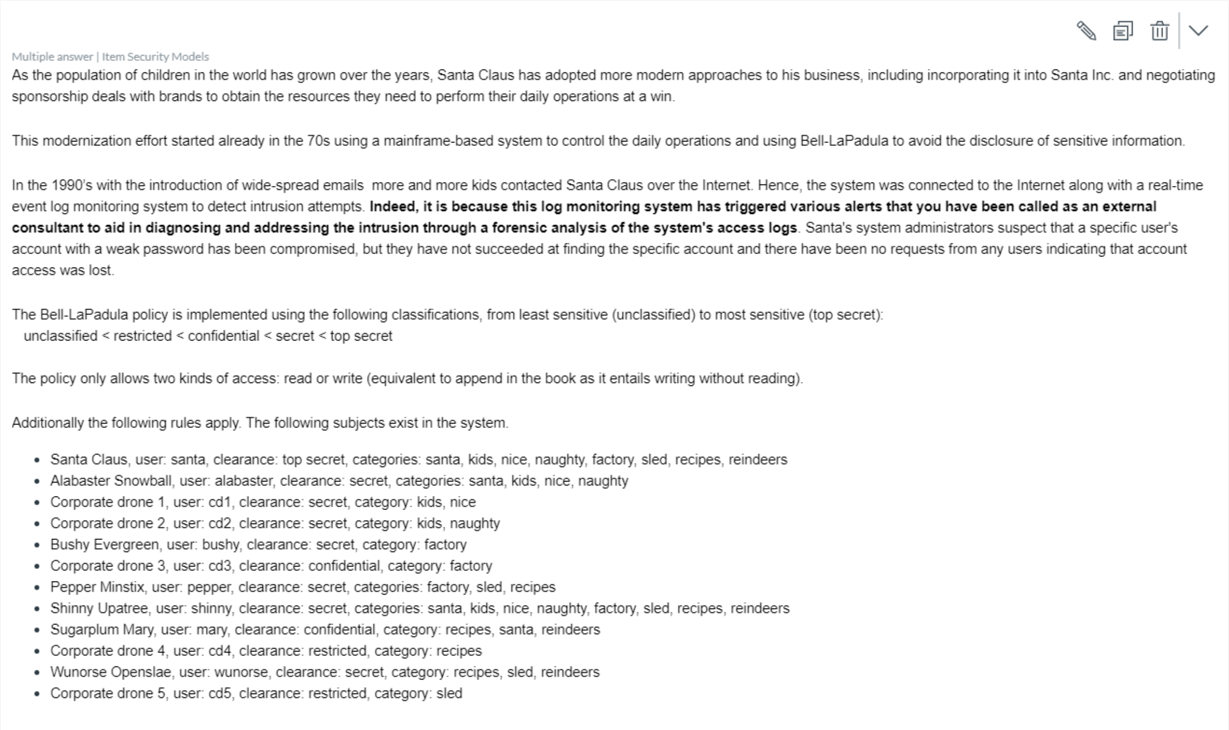
In the 1990's with the introduction of wide-spread emails more and more kids contacted Santa Claus over the Internet. Hence, the system was connected to the Internet along with a real-time event log monitoring system to detect intrusion attempts. **Indeed, it is because this log monitoring system has 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.

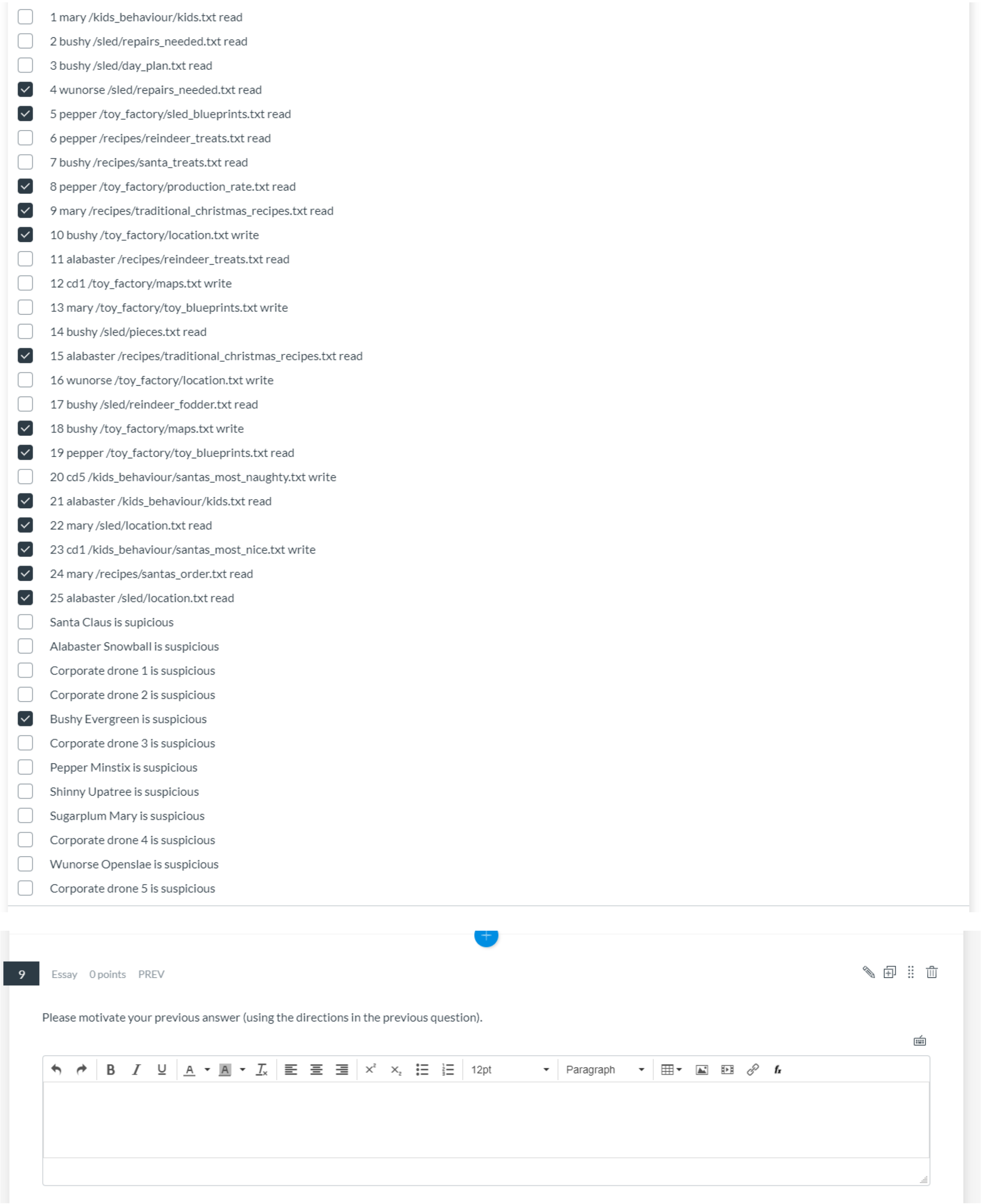
In the 1990's with the introduction of wide-spread emails more and more kids contacted Santa Claus over the Internet. Hence, the system was connected to the Internet along with a real-time event log monitoring system to detect intrusion attempts. **Indeed, it is because this log monitoring system has 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

9 Essay 0 points PREV

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