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, Friday 20 March 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 Wednesday 15 April 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.

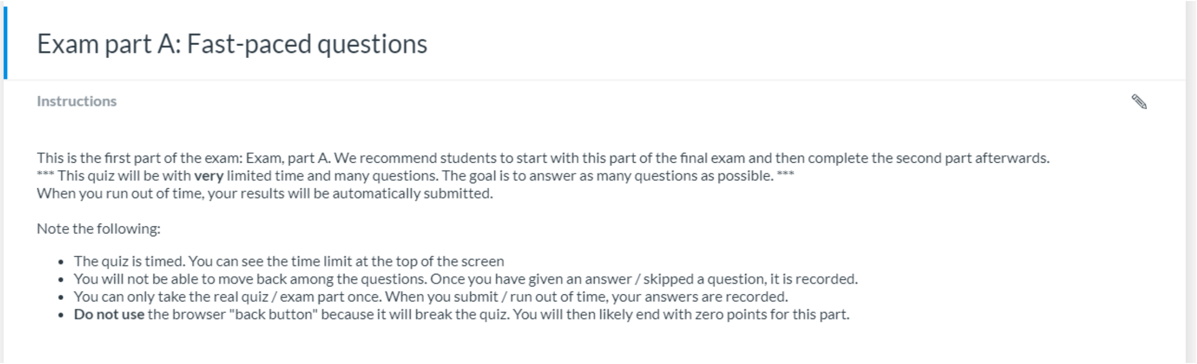
For previous exams, the has been determined as follows:

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

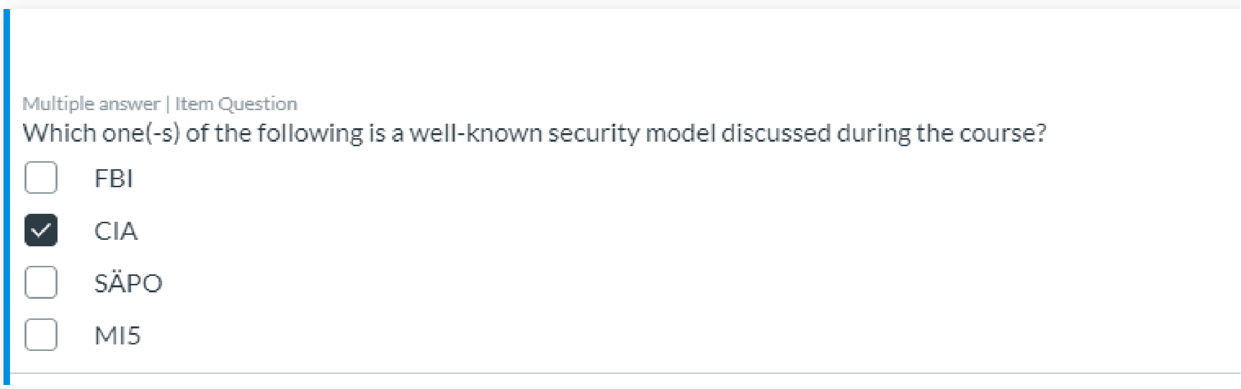
This is the first part of the exam: Exam, part A. We recommend students to start with this part of the final exam and then complete the second part afterwards.
*** This quiz will be with **very** limited time and many questions. The goal is to answer as many questions as possible. ***
When you run out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

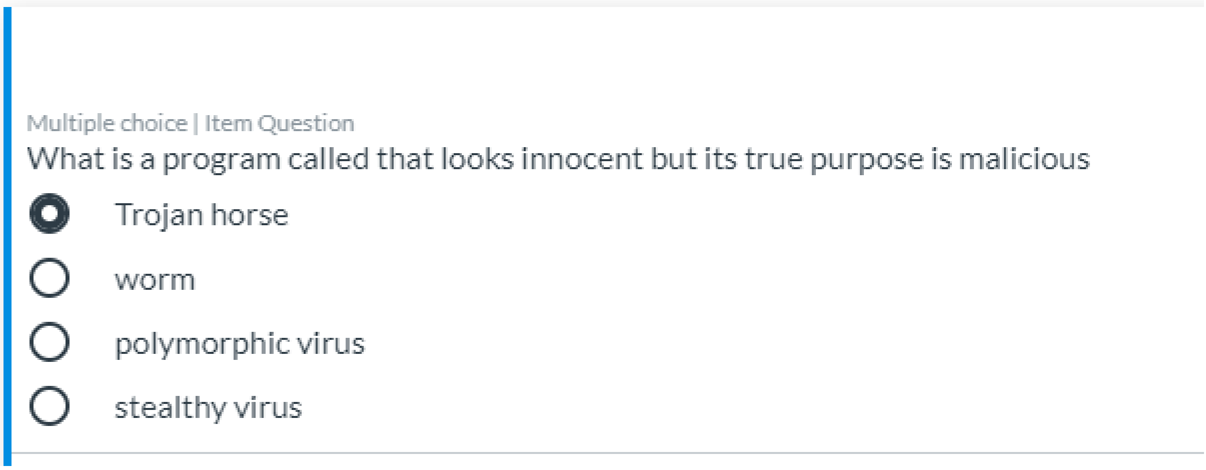
Which one(-s) of the following is a well-known security model discussed during the course?

□ FBI

☑ CIA

□ SÄPO

□ MI5



Multiple choice | Item Question

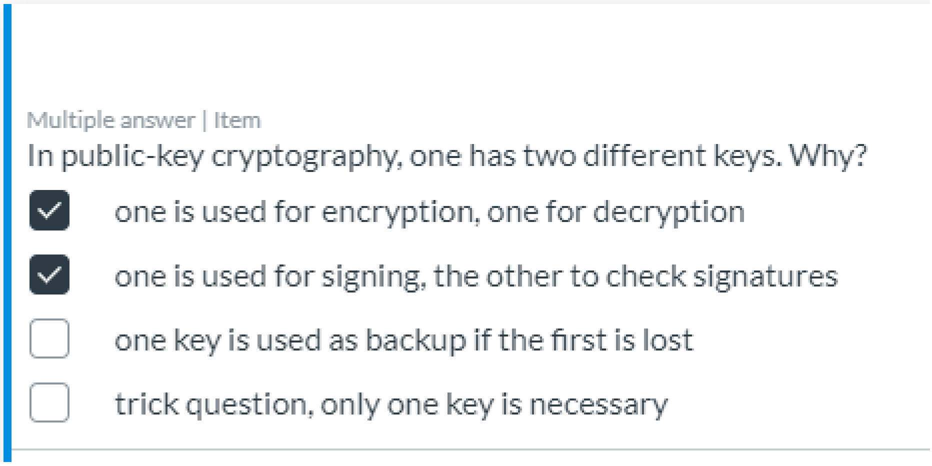
What is a program called that looks innocent but its true purpose is malicious

● Trojan horse

○ worm

○ polymorphic virus

○ stealthy virus



Multiple answer | Item

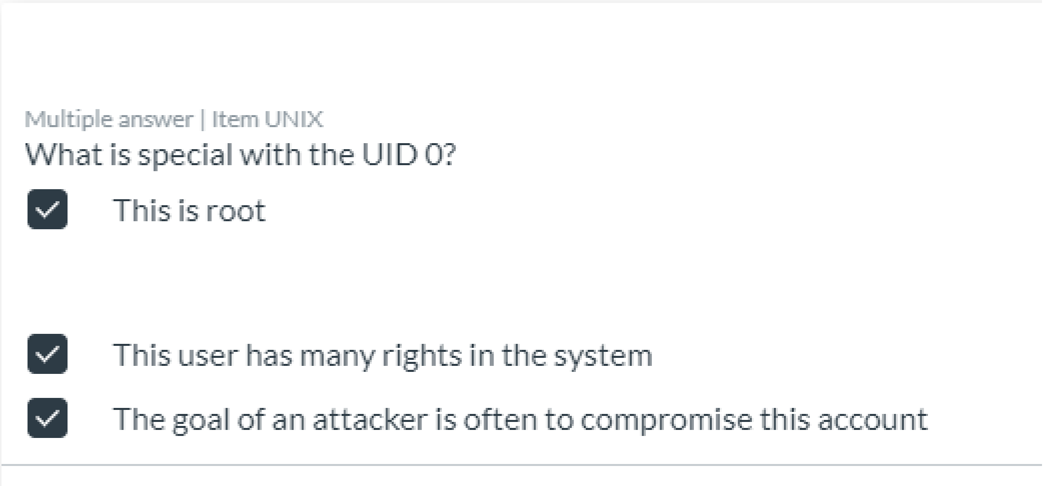
In public-key cryptography, one has two different keys. Why?

☑ 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



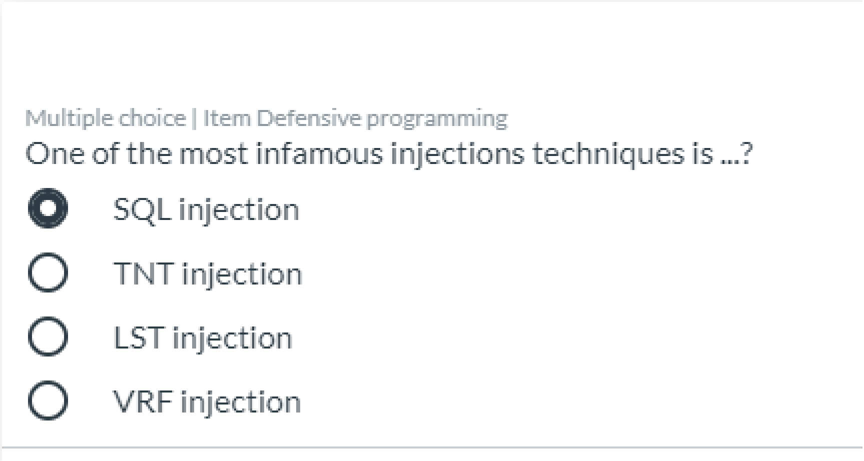
Multiple answer | Item UNIX

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 ...?

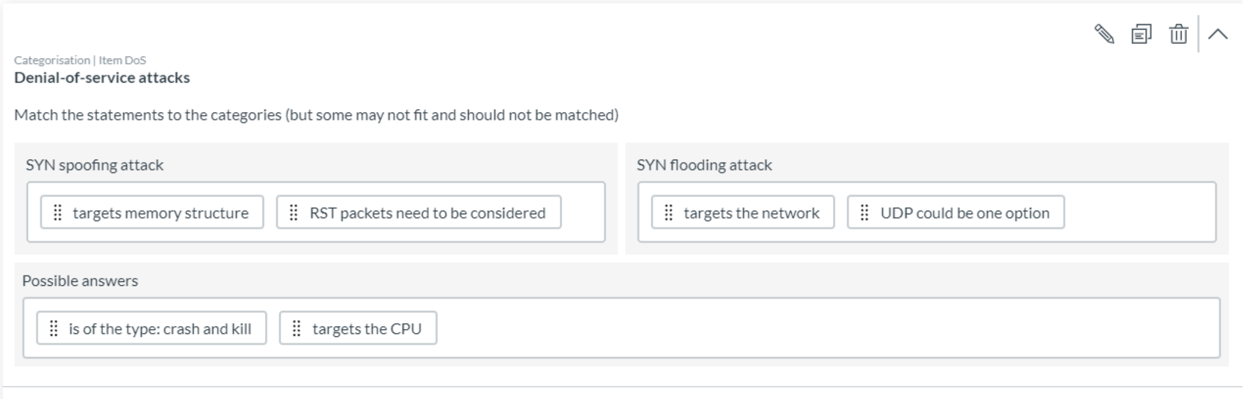
● SQL injection

○ 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

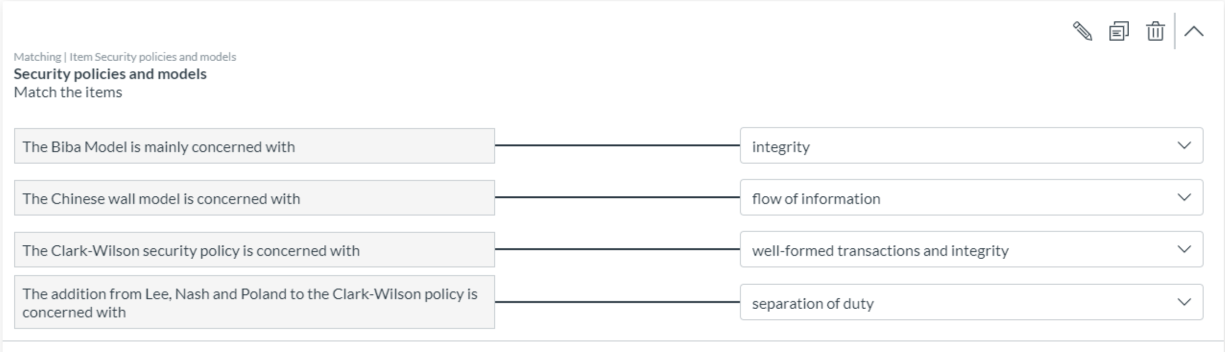
- targets memory structure
- RST packets need to be considered

SYN flooding attack

- targets the network
- UDP could be one option

Possible answers

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

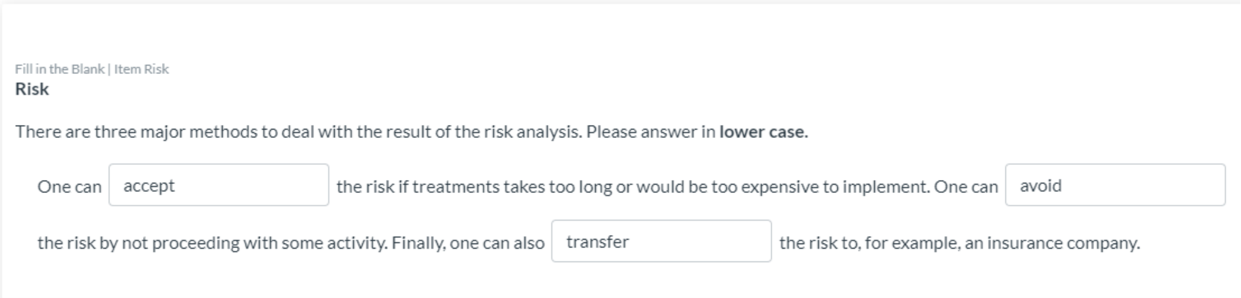


Matching | Item Security policies and models

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

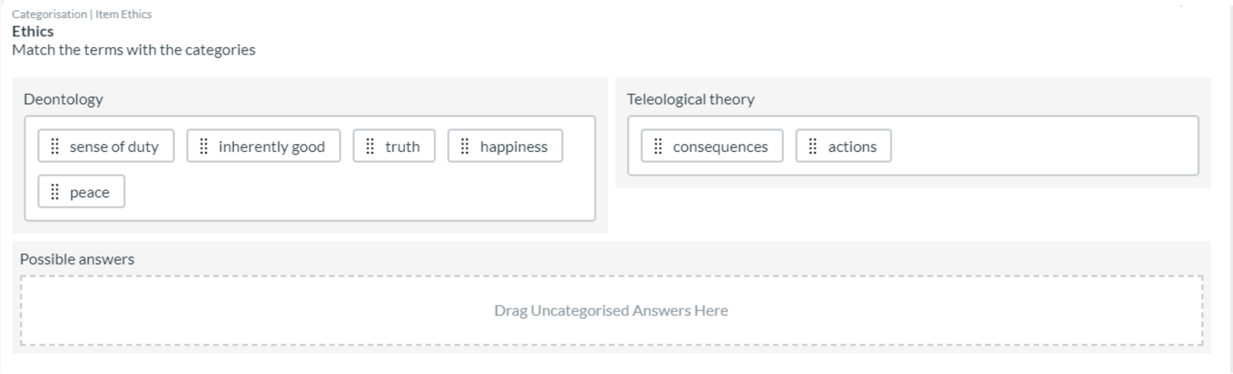


Fill in the Blank | Item Risk

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

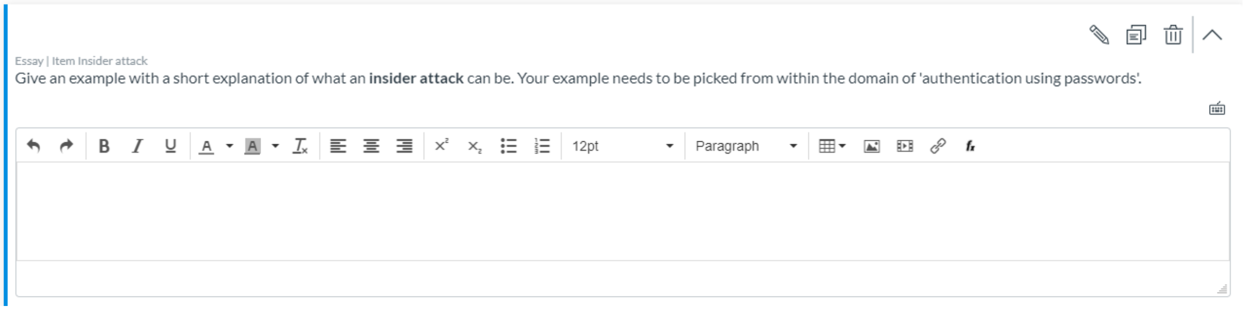
Teleological theory

- consequences
- actions

Possible answers

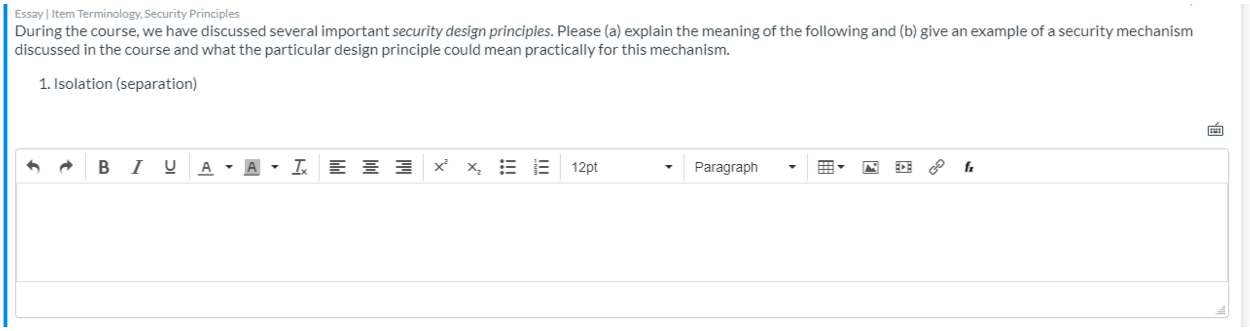
Drag Uncategorised Answers Here

Slow Recall, 3 questions, 5 points per question



Essay | Item Insider attack

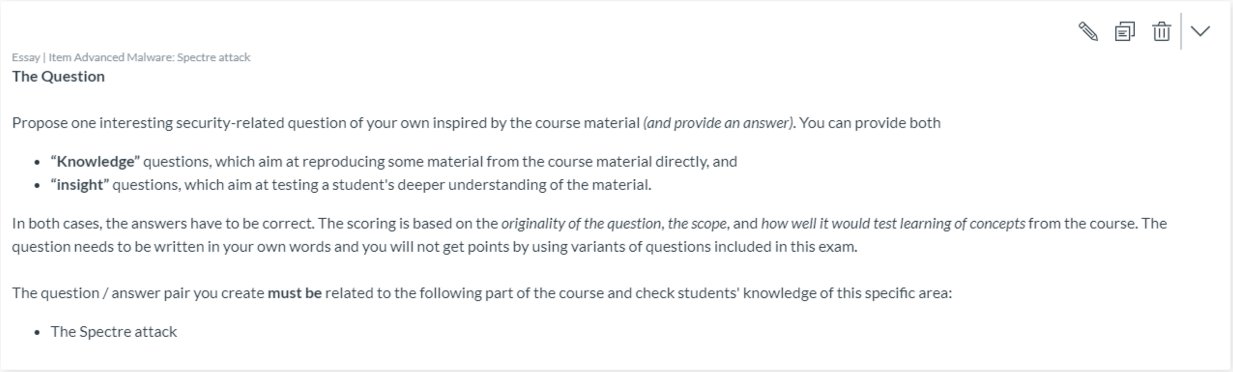
Give an example with a short explanation of what an **insider attack** can be. Your example needs to be picked from within the domain of 'authentication using passwords'.



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

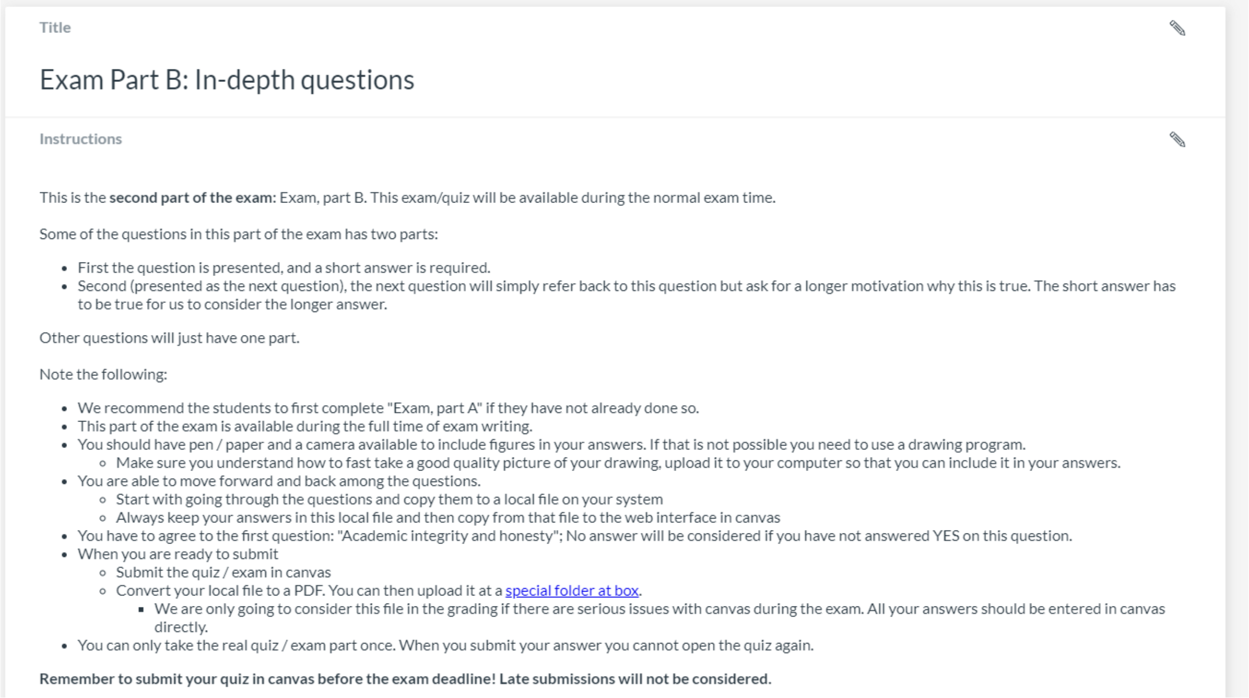
Propose one interesting security-related question of your own inspired by the course material *(and provide an answer)*. You can provide both

- **"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:

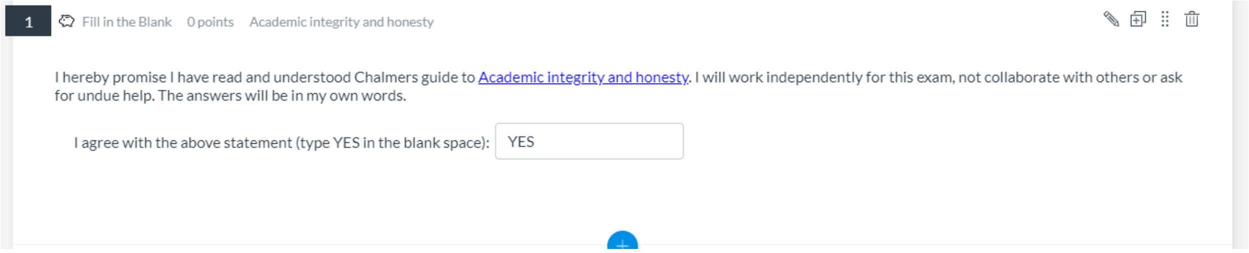
- First the question is presented, and a short answer is required.
- Second (presented as the next question), the next question will simply refer back to this question but ask for a longer motivation why this is true. The short answer has to be true for us to consider the longer answer.

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.

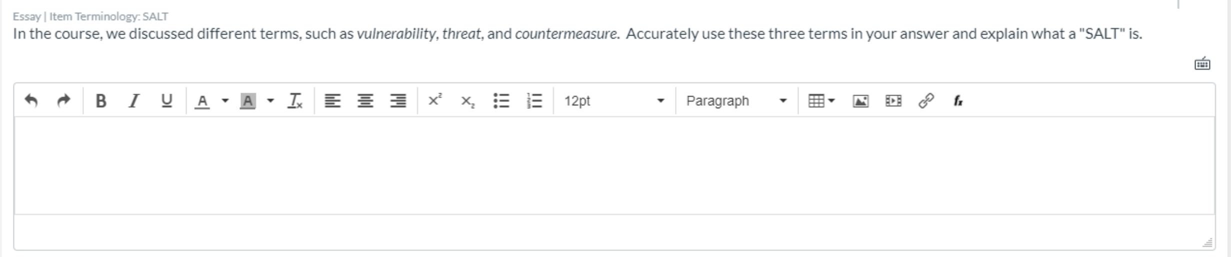


1 Fill in the Blank 0 points Academic integrity and honesty

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

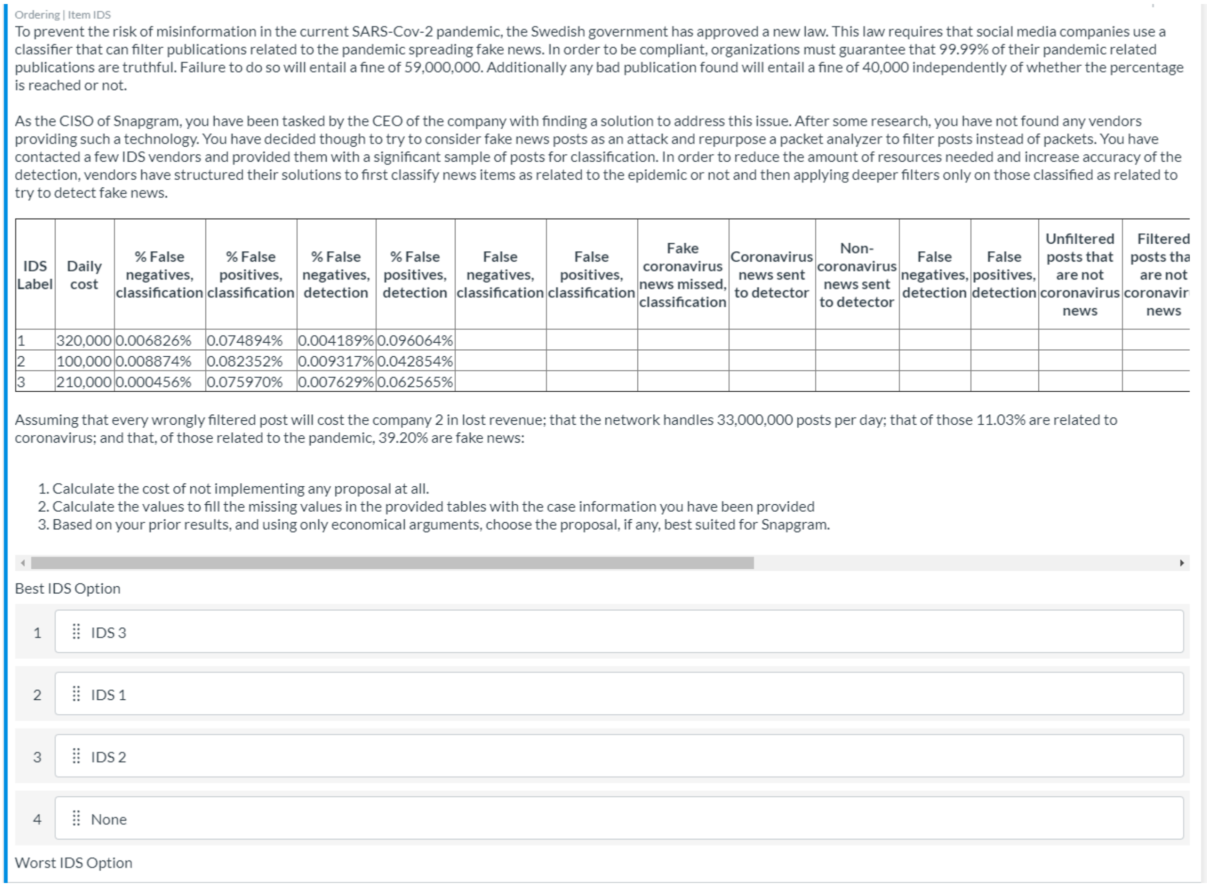
Question 2: 6 points



Essay | Item Terminology: SALT

In the course, we discussed different terms, such as *vulnerability*, *threat*, and *countermeasure*. Accurately use these three terms in your answer and explain what a "SALT" is.

Question 3: 1 point



Ordering | Item IDS

To prevent the risk of misinformation in the current SARS-Cov-2 pandemic, the Swedish government has approved a new law. This law requires that social media companies use a classifier that can filter publications related to the pandemic spreading fake news. In order to be compliant, organizations must guarantee that 99.99% of their pandemic related publications are truthful. Failure to do so will entail a fine of 59,000,000. Additionally any bad publication found will entail a fine of 40,000 independently of whether the percentage is reached or not.

As the CISO of Snapgram, you have been tasked by the CEO of the company with finding a solution to address this issue. After some research, you have not found any vendors providing such a technology. You have decided though to try to consider fake news posts as an attack and repurpose a packet analyzer to filter posts instead of packets. You have contacted a few IDS vendors and provided them with a significant sample of posts for classification. In order to reduce the amount of resources needed and increase accuracy of the detection, vendors have structured their solutions to first classify news items as related to the epidemic or not and then applying deeper filters only on those classified as related to try to detect fake news.

IDS Label	Daily cost	% False negatives, classification	% False positives, classification	% False negatives, detection	% False positives, detection	False negatives, classification	False positives, classification	Fake coronavirus news missed, classification	Coronavirus news sent to detector	Non-coronavirus news sent to detector	False negatives, detection	False positives, detection	Unfiltered posts that are not coronavirus news	Filtered posts tha are not coronavir news
1	320,000	0.006826%	0.074894%	0.004189%	0.096064%									
2	100,000	0.008874%	0.082352%	0.009317%	0.042854%									
3	210,000	0.000456%	0.075970%	0.007629%	0.062565%									

Assuming that every wrongly filtered post will cost the company 2 in lost revenue; that the network handles 33,000,000 posts per day; that of those 11.03% are related to coronavirus; and that, of those related to the pandemic, 39.20% are fake news:

1. Calculate the cost of not implementing any proposal at all.
2. Calculate the values to fill the missing values in the provided tables with the case information you have been provided
3. Based on your prior results, and using only economical arguments, choose the proposal, if any, best suited for Snapgram.

Best IDS Option

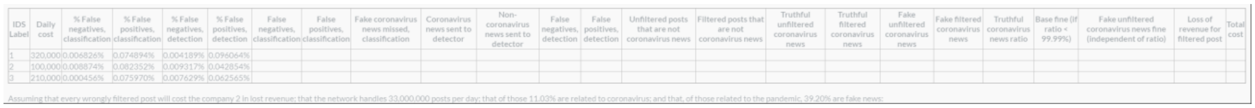
1 IDS 3

2 IDS 1

3 IDS 2

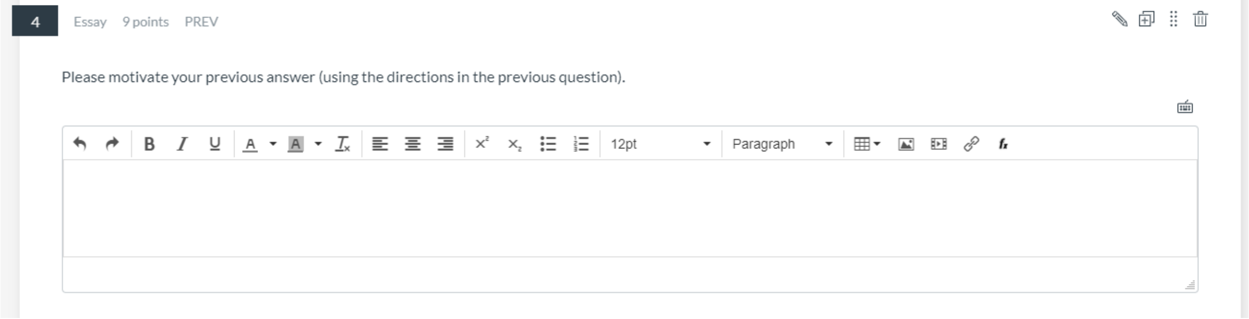
4 None

Worst IDS Option



IDS Label	Daily cost	% False negatives, classification	% False positives, classification	% False negatives, detection	% False positives, detection	False negatives, classification	False positives, classification	Fake coronavirus news missed, classification	Coronavirus news sent to detector	Non-coronavirus news sent to detector	False negatives, detection	False positives, detection	Unfiltered posts that are not coronavirus news	Filtered posts that are not coronavirus news	Truthful unfiltered coronavirus news	Truthful filtered coronavirus news	Fake unfiltered coronavirus news	Fake filtered coronavirus news	Truthful coronavirus news ratio	Base fine (if ratio < 99.99%)	Fake unfiltered coronavirus news fine (independent of ratio)	Loss of revenue for filtered post	Total cost
1	320,000	0.006826%	0.074894%	0.004189%	0.096064%																		
2	100,000	0.008874%	0.082352%	0.009317%	0.042854%																		
3	210,000	0.000456%	0.075970%	0.007629%	0.062565%																		

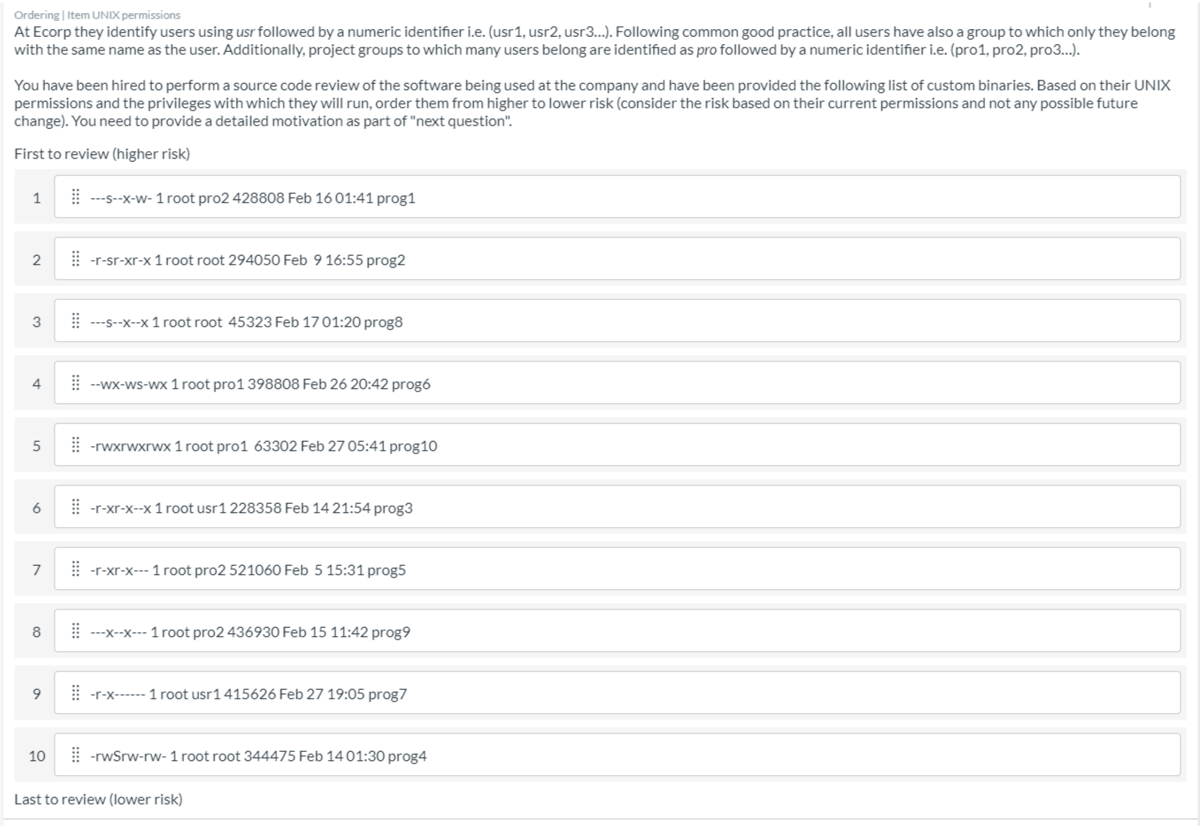
Assuming that every wrongly filtered post will cost the company 2 in lost revenue; that the network handles 33,000,000 posts per day; that of those 11.03% are related to coronavirus; and that, of those related to the pandemic, 39.20% are fake news:



4 Essay 9 points PREV

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

Question 5: 14 points



Ordering | Item UNIX permissions

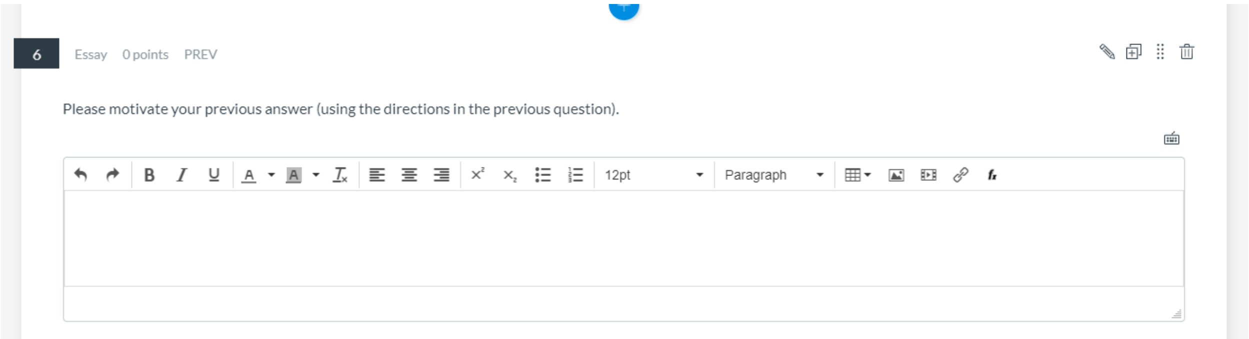
At Ecorp they identify users using *usr* followed by a numeric identifier i.e. (usr1, usr2, usr3...). Following common good practice, all users have also a group to which only they belong with the same name as the user. Additionally, project groups to which many users belong are identified as *pro* followed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

You have been hired to perform a source code review of the software being used at the company and have been provided the following list of custom binaries. Based on their UNIX permissions and the privileges with which they will run, order them from higher to lower risk (consider the risk based on their current permissions and not any possible future change). You need to provide a detailed motivation as part of "next question".

First to review (higher risk)

1. ---s--x-w- 1 root pro2 428808 Feb 16 01:41 prog1
2. -r-sr-xr-x 1 root root 294050 Feb 9 16:55 prog2
3. ---s--x--x 1 root root 45323 Feb 17 01:20 prog8
4. --wx-ws-wx 1 root pro1 398808 Feb 26 20:42 prog6
5. -rwxrwxrwx 1 root pro1 63302 Feb 27 05:41 prog10
6. -r-xr-x--x 1 root usr1 228358 Feb 14 21:54 prog3
7. -r-xr-x--- 1 root pro2 521060 Feb 5 15:31 prog5
8. ---x--x--- 1 root pro2 436930 Feb 15 11:42 prog9
9. -r-x------ 1 root usr1 415626 Feb 27 19:05 prog7
10. -rwSrw-rw- 1 root root 344475 Feb 14 01:30 prog4

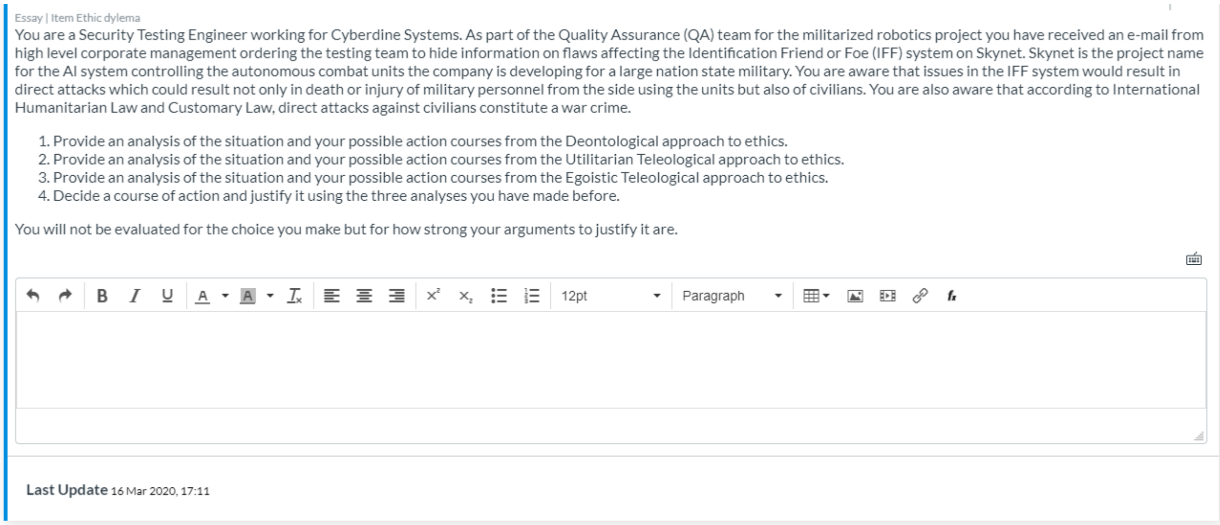
Last to review (lower risk)



6 Essay 0 points PREV

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

Question 7: 5 points



Essay | Item Ethic dylema

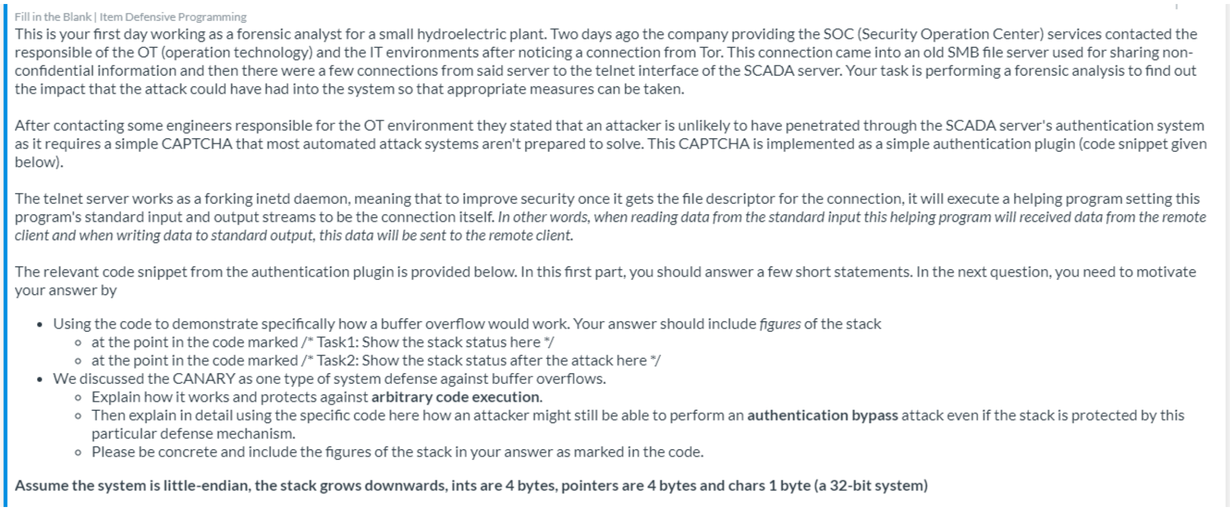
You are a Security Testing Engineer working for Cyberdine Systems. As part of the Quality Assurance (QA) team for the militarized robotics project you have received an e-mail from high level corporate management ordering the testing team to hide information on flaws affecting the Identification Friend 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 8: 1 point



Fill in the Blank | Item Defensive Programming

This is your first day working as a forensic analyst for a small hydroelectric plant. Two days ago the company providing the SOC (Security Operation Center) services contacted the responsible of the OT (operation technology) and the IT environments after noticing a connection from Tor. This connection came into an old SMB file server used for sharing non-confidential information and then there were a few connections from said server to the telnet interface of the SCADA server. Your task is performing a forensic analysis to find out the impact that the attack could have had into the system so that appropriate measures can be taken.

After contacting some engineers responsible for the OT environment they stated that an attacker is unlikely to have penetrated through the SCADA server's authentication system as it requires a simple CAPTCHA that most automated attack systems aren't prepared to solve. This CAPTCHA is implemented as a simple authentication plugin (code snippet given below).

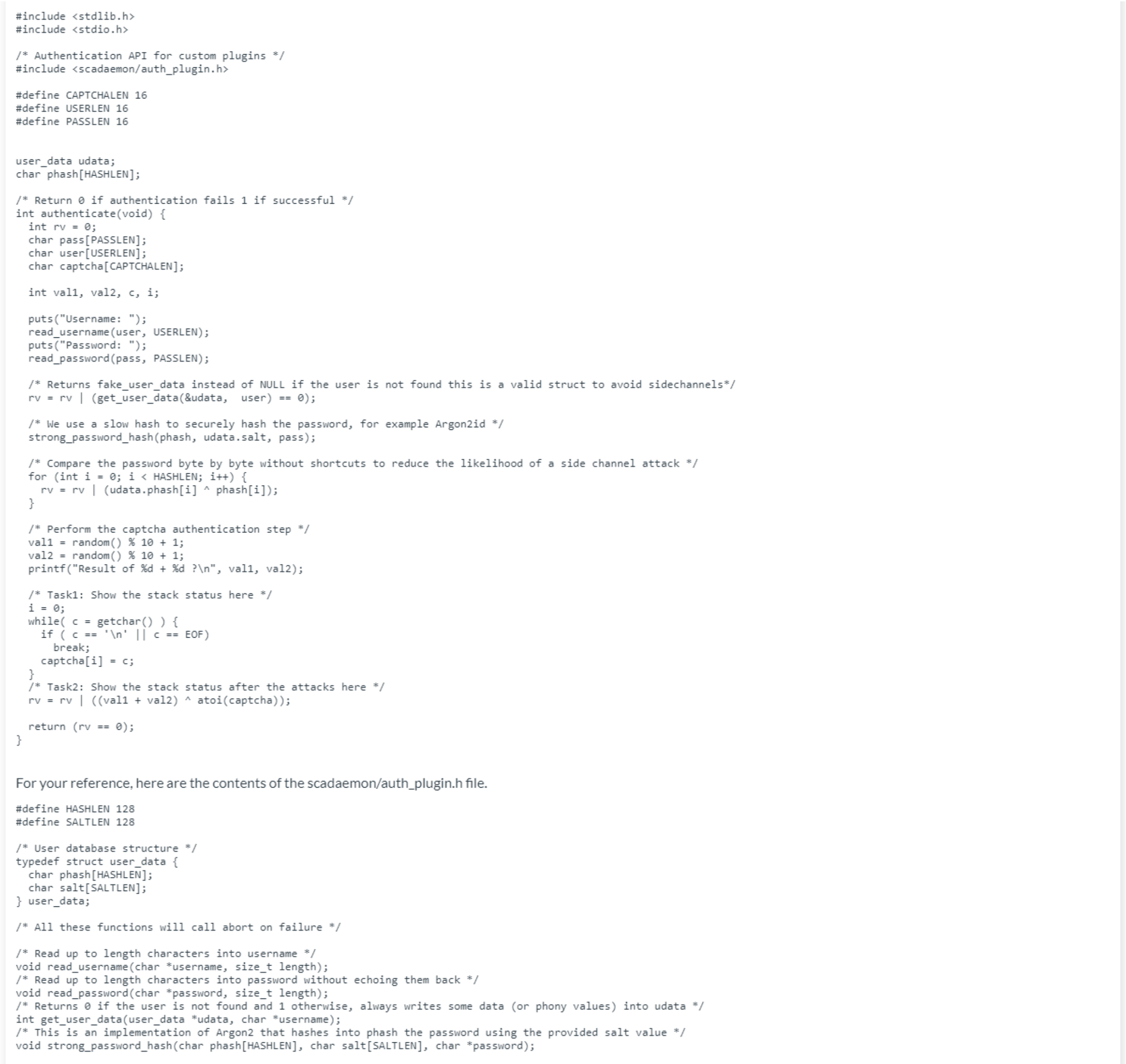
The telnet server works as a forking inetd daemon, meaning that to improve security once it gets the file descriptor for the connection, it will execute a helping program setting this program's standard input and output streams to be the connection itself. *In other words, when reading data from the standard input this helping program will received data from the remote client and when writing data to standard output, this data will be sent to the remote client.*

The relevant code snippet from the authentication plugin is provided below. In this first part, you should answer a few short statements. In the next question, you need to motivate your answer by

- Using the code to demonstrate specifically how a buffer overflow would work. Your answer should include *figures* of the stack
  - at the point in the code marked /* Task1: Show the stack status here */
  - at the point in the code marked /* Task2: Show the stack status after the attack here */
- We discussed the CANARY as one type of system defense against buffer overflows.
  - Explain how it works and protects against **arbitrary code execution.**
  - Then explain in detail using the specific code here how an attacker might still be able to perform an **authentication bypass** attack even if the stack is protected by this particular defense mechanism.
  - Please be concrete and include the figures of the stack in your answer as marked in the code.

Assume the system is little-endian, the stack grows downwards, ints are 4 bytes, pointers are 4 bytes and chars 1 byte (a 32-bit system)

(continuation on the next page)



```
#include <stdlib.h>
#include <stdio.h>

/* Authentication API for custom plugins */
#include <scadaemon/auth_plugin.h>

#define CAPTCHALEN 16
#define USERLEN 16
#define PASSLEN 16


user_data udata;
char phash[HASHLEN];

/* Return 0 if authentication fails 1 if successful */
int authenticate(void) {
  int rv = 0;
  char pass[PASSLEN];
  char user[USERLEN];
  char captcha[CAPTCHALEN];

  int val1, val2, c, i;

  puts("Username: ");
  read_username(user, USERLEN);
  puts("Password: ");
  read_password(pass, PASSLEN);

  /* Returns fake_user_data instead of NULL if the user is not found this is a valid struct to avoid sidechannels*/
  rv = rv | (get_user_data(&udata,  user) == 0);

  /* We use a slow hash to securely hash the password, for example Argon2id */
  strong_password_hash(phash, udata.salt, pass);

  /* Compare the password byte by byte without shortcuts to reduce the likelihood of a side channel attack */
  for (int i = 0; i < HASHLEN; i++) {
    rv = rv | (udata.phash[i] ^ phash[i]);
  }

  /* Perform the captcha authentication step */
  val1 = random() % 10 + 1;
  val2 = random() % 10 + 1;
  printf("Result of %d + %d ?\n", val1, val2);

  /* Task1: Show the stack status here */
  i = 0;
  while( c = getchar() ) {
    if ( c == '\n' || c == EOF)
      break;
    captcha[i] = c;
  }
  /* Task2: Show the stack status after the attacks here */
  rv = rv | ((val1 + val2) ^ atoi(captcha));

  return (rv == 0);
}
```

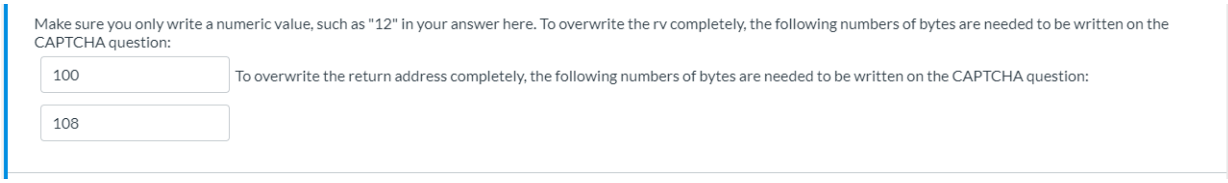
For your reference, here are the contents of the scadaemon/auth_plugin.h file.

```
#define HASHLEN 128
#define SALTLEN 128

/* User database structure */
typedef struct user_data {
  char phash[HASHLEN];
  char salt[SALTLEN];
} user_data;

/* All these functions will call abort on failure */

/* Read up to length characters into username */
void read_username(char *username, size_t length);
/* Read up to length characters into password without echoing them back */
void read_password(char *password, size_t length);
/* Returns 0 if the user is not found and 1 otherwise, always writes some data (or phony values) into udata */
int get_user_data(user_data *udata, char *username);
/* This is an implementation of Argon2 that hashes into phash the password using the provided salt value */
void strong_password_hash(char phash[HASHLEN], char salt[SALTLEN], char *password);
```

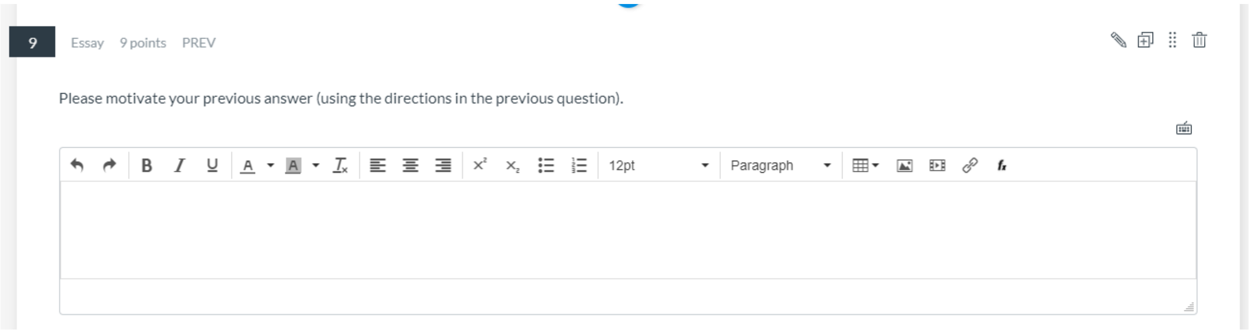


Make sure you only write a numeric value, such as "12" in your answer here. To overwrite the rv completely, the following numbers of bytes are needed to be written on the CAPTCHA question:

100

To overwrite the return address completely, the following numbers of bytes are needed to be written on the CAPTCHA question:

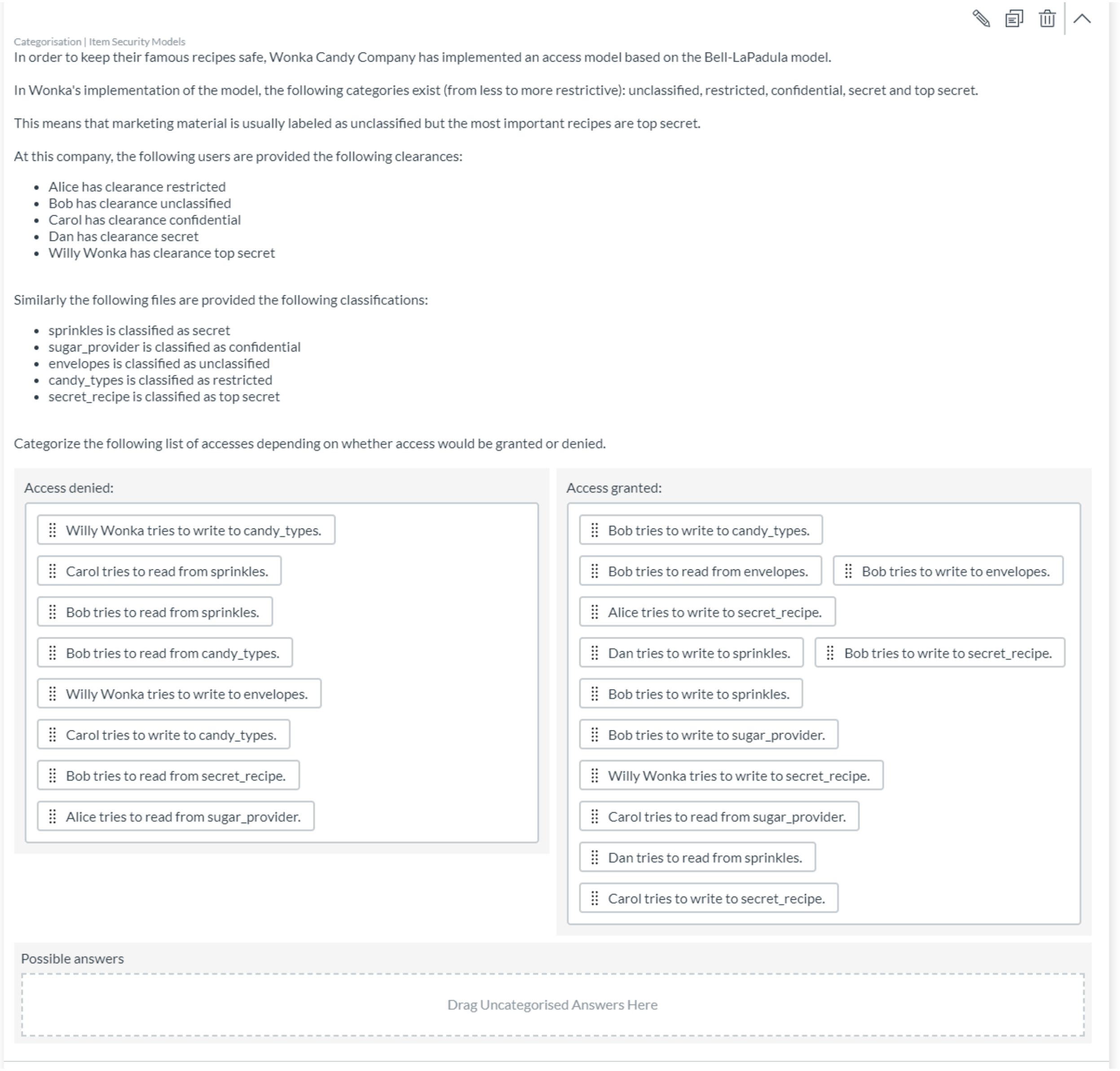
108



9 Essay 9 points PREV

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

Question 10: 5 points



Categorisation | Item Security Models

In order to keep their famous recipes safe, Wonka Candy Company has implemented an access model based on the Bell-LaPadula model.

In Wonka's implementation of the model, the following categories exist (from less to more restrictive): unclassified, restricted, confidential, secret and top secret.

This means that marketing material is usually labeled as unclassified but the most important recipes are top secret.

At this company, the following users are provided the following clearances:

- Alice has clearance restricted
- Bob has clearance unclassified
- Carol has clearance confidential
- Dan has clearance secret
- Willy Wonka has clearance top secret

Similarly the following files are provided the following classifications:

- sprinkles is classified as secret
- sugar_provider is classified as confidential
- envelopes is classified as unclassified
- candy_types is classified as restricted
- secret_recipe is classified as top secret

Categorize the following list of accesses depending on whether access would be granted or denied.

Access denied:

- Willy Wonka tries to write to candy_types.
- Carol tries to read from sprinkles.
- Bob tries to read from sprinkles.
- Bob tries to read from candy_types.
- Willy Wonka tries to write to envelopes.
- Carol tries to write to candy_types.
- Bob tries to read from secret_recipe.
- Alice tries to read from sugar_provider.

Access granted:

- Bob tries to write to candy_types.
- Bob tries to read from envelopes.
- Bob tries to write to envelopes.
- Alice tries to write to secret_recipe.
- Dan tries to write to sprinkles.
- Bob tries to write to secret_recipe.
- Bob tries to write to sprinkles.
- Bob tries to write to sugar_provider.
- Willy Wonka tries to write to secret_recipe.
- Carol tries to read from sugar_provider.
- Dan tries to read from sprinkles.
- Carol tries to write to secret_recipe.

Possible answers

Drag Uncategorised Answers Here