First part: multiple choice questions

For each question, mark the box corresponding to the correct answer. Each question has **exactly one** correct answer.

Question 1 : Authentication
Assume Barbie and Ken have established a secure TLS connection. They use this connection for the following authentication exchange in which Barbie uses her password `'Il0veP1nk'` to prove her identity to Ken:

```
Barbie -- (Barbie, 'I want to login') --> Ken
Barbie <-- Hash(Ken) -- Ken
Barbie -- Enc('Il0veP1nk'|Hash(Ken), k) --> Ken
```

- `Hash()` is a secure cryptographic hash function that is second pre-image resistant.
- `str1|str2` is the concatenation of two strings `str1` and `str2`.
- `Enc(m,k)` is the symmetric encryption of message m with key k that Barbie and Ken have securely exchanged before.
- `'-->'` indicates communication via the secure TLS connection.

Which of the following statements is correct?

- ☐ This authentication exchange is secure against replay attacks because `Hash(Ken)` is second pre-image resistant.
- ☐ This authentication exchange is not secure against replay attacks because Barbie has chosen a weak password that is easily guessable.
- ☐ This authentication exchange is not secure against replay attacks because `Hash(Ken)` is not collision resistant.
- ■ This authentication exchange is secure against replay attacks because Barbie and Ken use a secure TLS channel.

Question 2 : Network
A professor decides that the final exams of their course must be taken online. To ensure fairness, all students must sit in the same classroom during the exam and connect to the server hosting the exam questions using the classroom LAN. The teaching team creates a website with the exam questions and hosts it on the only lab server with IP `107.18.90.101` that all students in the course have interacted with in the past. The teaching team hears that some lazy students who have not studied want to stop the exam from happening through a denial of service (DoS) attack. To reduce the risk of a successful DoS attack, the teaching team keeps the domain name of the exam hidden until the start of the exam.

Which of the following statements is incorrect?

- ☐ Keeping the domain name secret cannot prevent the lazy students from using a ping message with a spoofed origin IP address to launch a distributed Denial of Service attack.
- ■ Keeping the domain name secret prevents the lazy students from launching a DNS hijacking-based Denial of Service attack.
- ☐ Keeping the domain name secret prevents the lazy students from launching a DNS poisoning-based Denial of Service attack.
- ☐ Keeping the domain name secret cannot prevent the lazy students from launching a Denial of Service attack on the classroom LAN gateway.

Question 3 : Cryptography
During the TLS handshake, the client can propose to the server two methods to decide on the session key k that will be used for encryption:

(a) **Key transport** in which the client will generate a fresh symmetric session key k and send it to the server encrypted with the server's public key pk. Thus, only the server can decrypt the session key with the server's secret key sk. The session key k is deleted at the end of the session.

(b) **Key exchange** in which client and server will exchange cryptographic material to derive a fresh symmetric session key k only known to them to be used during the session. The session key k is deleted at the end of the session.

- k is a symmetric session key known to both sender and client
- pk is the public key of the server known to everyone
- sk is the secret key of the server known only to the server

Which of the following statements is correct?

- ☐ None of the options provide forward secrecy because the session key k is deleted at the end of the session.
- ☐ Both options provide forward secrecy because in both cases the session key k is freshly generated at the start of each session.
- ■ Only key exchange provides forward secrecy because there is no long-term secret involved in the process to decide on the session key k.
- ☐ Only key transport provides forward secrecy because only the server knows sk that enables to decrypt the session key k.

Question 4 : Software
Oppenheimer's team wrote a program that can answer queries about statistics on the atomic bombs in storage, e.g., how many atomic bombs are currently in status `'ready to launch'`. The members of the Oppenheimer team ask queries to this program from the lab computer. The team worries that if one of the team members is a spy they could exploit potential bugs in the program to perform a code injection attack to maliciously trigger the launch of a bomb from the lab computer.

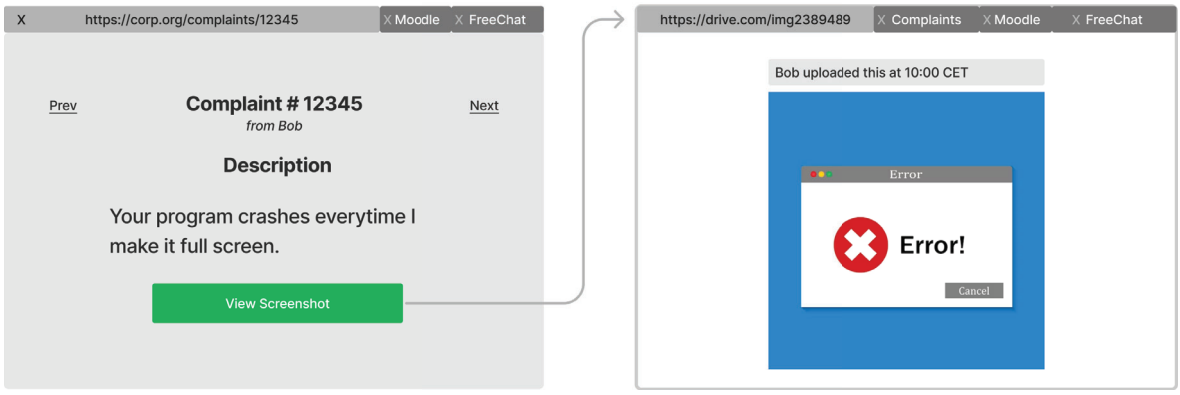
Which mitigation guarantees that such an attack cannot be launched?

- ☐ Add a canary to the stack of the lab computer.
- ☐ Implement address space layout randomization at the OS level on the lab computer.
- ■ Implement data execution prevention through the X^W policy on the lab computer.
- ☐ Use mutation-based fuzzing on the program before loading it to the lab computer.

Question 5 : Access Control
Which of the following statements is correct?

- ☐ Capabilities are more efficient than access control lists to remove access rights to a particular object.
- ■ In role-based access control, increasing the number of roles of a principal can never reduce the number of permissions of this principal.
- ☐ Encrypting part of a message so that the ciphertext can only be decrypted by the intended receiver is an example of a covert channel.
- ☐ BIBA's goal of maintaining integrity is consistent with ensuring that information from low clearance levels is available to authorised users with high clearance.

Question 6 : Web Security



Maurice uses a browser on his personal computer to answer complaints from clients. On the complaints website `bigCorp.org/complaints`, each complaint is reachable at `bigCorp.org/complaints/<complaint-id>` and contains a description text box and a button "View Screenshot". This button redirects Maurice to a **media server** chosen by the writer of the complaint that hosts an image of the problem that they encountered. The URL of this image is not visible on the complaints webpage.
Maurice uses the same web browser to fill out assignments on Foodle, and chat on FreeChat.com. Both Foodle and FreeChat use a session cookie stored in the browser for authentication.

Given his setup and the actions he has to perform to review complaints, which of the following attacks is Maurice vulnerable to?

- ☐ Cross-site scripting; because when returning a webpage to Maurice, the media servers might have `src` URLs that trigger malicious server-side scripts to track him.
- ☐ Cross-site scripting; because malicious media servers might add JavaScript code to the "FreeChat.com" tab to send messages to Maurice's friends using the existing session cookie.
- ■ Cross-site request forgery; because clients might give any URL for the "View Screenshot" button including `foodle.com/user/set-password?pwd=pwned`, which uses existing session cookies for authentication, to change Maurice's password for Foodle.
- ☐ Cross-site request forgery; because malicious media servers might include JavaScript in the displayed webpage to hijack Maurice's Foodle tab and drop him from his courses.

Question 7 : Malware

You receive an envelope which contains a USB flash drive and a note "Connect it to a computer and open the files". Which of the following is the best way to minimize the risks caused by malware that could be on the flash drive?

- ☐ Connect the flash drive to two computers connected to the Internet such that you can compare the effect of opening the files to learn if there is malware.
- ☐ Connect the flash drive to a computer connected to the Internet that has just been updated to install the latest patches for all installed programs, and open the files.
- ■ Connect the flash drive to a new computer that is still in factory state and not connected to the Internet or other devices, and open the files.
- ☐ Connect the flash drive to a computer disconnected from the Internet, open the files in a sandbox and scan for any virus using a signature-based antivirus program. If there is no matched signature, connect the computer to the Internet, re-attach the flash drive, and open the files outside the sandbox.

Question 8 : Network Security

Which of the following statements is true?

- ☐ Using static hard-coded ARP tables stored on the communicating devices to determine mappings from MAC to IP addresses does not defend against ARP spoofing.
- ☐ If a user visits "vaud.ch" through a VPN, they are more likely to be able to access the page during a Denial of Service attack targeted against the "vaud.ch" server than users not using a VPN.
- ☐ A stateful firewall can block HTTPS packets based on its payload.
- ☒ The establishment of session keys using the Diffie-Hellman protocol does not prevent man-in-the-middle attacks.