4. A network technician is unable to access a server using port 443 from a machine with an IP address of 192.168.45.37.

   Consider the following access control list (ACL) for the server's firewall.

Rule Number	Allow/Deny	Direction	Protocol	Port	Source
1	Allow	Inbound	TCP	22	ALL
2	Allow	Inbound	TCP	80	ALL
3	Deny	Inbound	TCP	443	192.168.0.0 - 192.168.255.255
4	Allow	Inbound	ICMP	ALL	ALL
5	Allow	Inbound	TCP	3306	ALL
6	Deny	Inbound	TCP	3389	ALL
7	Allow	Inbound	TCP	443	ALL
8	Allow	Inbound	TCP	587	ALL
9	Deny	Inbound	TCP	8140	192.168.45.0 - 192.168.45.255
10	Deny	Inbound	ALL	ALL	ALL

   Which of the following changes to the firewall would allow the network technician to access the server?

   (A) Swap firewall rule 1 with firewall rule 10

   (B) Swap firewall rule 3 with firewall rule 4

   (C) Swap firewall rule 3 with firewall rule 7

   (D) Swap firewall rule 4 with firewall rule 7

5. A system administrator runs two hashing functions on four files. Consider the following outputs for the two hashing functions.

Function 1 outputs

```
file1.txt - 8d8e115e5ebc50c8e03930beac6802a94ef4f36ab
file2.txt - 79a7d08081d12ecf123d63845e38c14c09956ee79
file3.txt - 02db6aefd093c317f8cf78a2fbe52a31b58a6bc5e
file4.txt - bcd3cf9d8527f711031d0d908d84cbb0df97ce90b
```


Function 2 outputs

```
file1.txt - 804537a7adfa4e1bce4d72d0b212a80af2dae3a5e
file2.txt - ba429665c8b95d05a963ee89fded2c7f18892d13e
file3.txt - 804537a7adfa4e1bce4d72d0b212a80af2dae3a5e
file4.txt - 7fa2901ebbb731eb283487afc033e45dae210a89e
```

   Which of the following statements is supported by the file hashes?

   (A) The files **`file1.txt`** and **`file3.txt`** are exact copies of each other.

   (B) Function 1 is more secure than Function 2.

   (C) Function 1 and Function 2 are the same hashing function.

   (D) The files **`file1.txt`** and **`file3.txt`** have a collision in one hashing function.

6. The security manager at a hospital is planning to upgrade the hospital's physical security system to ensure that only authorized personnel can access areas containing sensitive medical equipment and patient records. Because these areas require a high level of security, the manager wants an authentication method that is unique to each individual and extremely difficult for an adversary to duplicate or spoof. Which of the following authentication methods is best suited for these areas?

   (A) Authentication token

   (B) Password

   (C) Retina scan

   (D) Access card

7. Which of the following best describes how offline password attacks work?

   (A) Adversaries attempt user:password combinations in an active authentication portal.

   (B) Adversaries intercept communication as it travels across a network and read the password in transit.

   (C) Adversaries exploit weak access controls to directly retrieve plaintext passwords stored in a database.

   (D) Adversaries use automated tools to hash many potential passwords and compare them to a captured hash.

12. The system administrator at a high school receives an alert that there may have been multiple unauthorized login attempts to the school's online grading system. To investigate, the administrator decides to review the authentication logs. Which of the following best describes how authentication logs can be used to determine whether unauthorized login attempts have occurred?
    (A) The logs record which password was used in each login attempt, which allows the administrator to verify account ownership.
    (B) The logs record all login activity, which allows the administrator to reconstruct when and how login attempts occurred.
    (C) The logs record the location of each user attempting to log in, which allows the administrator to identify login attempts from other geographic regions.
    (D) The logs record the type of device attempting to log in, which allows the administrator to block unauthorized devices.

13. The network administrator for a manufacturing facility has implemented a signature-based network detection system. Which of the following is a potential impact of using this network detection method instead of anomaly-based detection?
    (A) More false negative alerts
    (B) Higher operating costs
    (C) Slower detection time
    (D) More alert fatigue

14. Consider the following lines from a log file.

```
2025-09-25 08:01:14 ARP Reply: 192.168.1.13 is-at 00:01:5e:00:fc:16
2025-09-25 09:14:15 ARP Reply: 192.168.1.13 is-at 00:3b:cc:5e:ee:01
```

    Which of the following attack types is indicated in the log file?
    (A) ARP poisoning attack
    (B) DNS poisoning attack
    (C) Evil-twin attack
    (D) MAC flooding attack

15. Which of the following best describes the length of a cryptographic hash function output?
    (A) The length of the output is longer than the input due to the hashing process.
    (B) The length of the output is fixed regardless of the length of the input.
    (C) The length of the output varies based on the length of the input.
    (D) The length of the output is shorter than the length of the input.

18. Which of the following types of attacks occurred when the adversary submitted a string that included `' OR '1'='1';--`?
    (A) SQL injection attack
    (B) Buffer overflow attack
    (C) Cross site scripting attack
    (D) Directory traversal attack

19. Which of the following security controls would most likely prevent an attack like this in the future?
    (A) Encryption
    (B) Stateful firewall
    (C) Input sanitization
    (D) Access control list

20. Which of the following best explains how the adversary attempted to manipulate the bank's customer database through the online loan application form?
    (A) When user input is fed into a server's file system, HTTP requests can access sensitive data.
    (B) When user input contains executable scripts, those scripts can run in the user's browser and access sensitive data.
    (C) When user input exceeds the size of the designated memory, it can allow the adversary to access, modify, and delete files.
    (D) When user input from a web form is fed directly into a database query, an adversary can inject control characters that can allow an adversary to view or modify the contents of a database.

21. An organization only allows their users to log into a system if they are physically in one of the following time zones (a time zone is a region where everyone uses the same clock time).
    - Eastern time zone
    - Central time zone
    - Mountain time zone
    - Pacific time zone

    Which of the following authentication factors is being used to verify the identity of the users?
    (A) Biometric factor
    (B) Knowledge factor
    (C) Location factor
    (D) Possession factor