2. A school district wants to ensure that only the school principal (**kmurray**) can edit faculty evaluation reports and to limit permissions for everyone else. The district's system administrator wants to set the following permission for the file **Oak_Park_HS**, which contains the faculty evaluations.

```
-rw-r----- kmurray staff 2048 Sep 18 10:45 Oak_Park_HS
```

Which of the following commands can be used to set the permissions shown?

(A) `chmod 444 Oak_Park_HS`
(B) `chmod 640 Oak_Park_HS`
(C) `chmod 740 Oak_Park_HS`
(D) `chmod 777 Oak_Park_HS`

3. Consider the following email.

From: Management
To: Security Manager

Subject: New Access Rules for Transaction System

Thank you for implementing access restrictions on our internal applications.

We are now interested in applying additional security rules that automatically limit user access based on specific conditions. For example, access to the transaction system should only be allowed during business hours and from devices connected to the corporate network.

Thanks!

Which of the following access control models best meets the request in the email?

(A) DAC
(B) MAC
(C) RBAC
(D) RuBAC

9. How does the email's claim that "Over 92% of employees have already completed the verification" attempt to pressure the recipient into responding to the email?

(A) By framing the request as routine HR communication that seems safe, showing the use of familiarity
(B) By implying that the opportunity to comply is limited and may soon be lost, showing the use of scarcity
(C) By presenting the request as coming from those in power and intimidating the recipient, showing the use of authority
(D) By applying social pressure and making the recipient believe most coworkers have already acted, showing the use of consensus

10. Which of the following is the most likely impact if the recipient responds to this email with the requested information?

(A) An adversary could use the recipient's personal details to impersonate them.
(B) An adversary could use the recipient's device as a foothold and move laterally on the network compromising other devices.
(C) An adversary could infect the recipient's device with malicious code hidden in the reply email.
(D) An adversary could disrupt the entire payroll system by disabling access for all employees.

11. A natural gas company's help desk receives reports from employees that the company's website is intermittently crashing when they try to log in. The cybersecurity analyst reviews the server's access logs and finds the following entries.

```
[22/Oct/2025:10:11:02] "GET /index.html HTTP/1.1" 200 4521
[22/Oct/2025:10:11:07] "GET /about.html HTTP/1.1" 200 3890
[22/Oct/2025:10:11:10] "GET ../../../../etc/passwd HTTP/1.1" 403 721
[22/Oct/2025:10:11:12] "GET ../../../../etc/shadow HTTP/1.1" 403 654
```

Which of the following application attacks is indicated in the log file?

(A) Buffer overflow attack
(B) Cross site scripting attack
(C) Directory traversal attack
(D) SQL injection attack

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.