Sample Exam Questions

The sample exam questions that follow illustrate the relationship between the course framework and the AP Cybersecurity Exam and serve as examples of the types of questions that appear on the exam. After the sample questions is a table that shows which skill(s) and learning objective(s) each question assesses. The table also provides the answers to the multiple-choice questions.

Section I: Multiple-Choice Questions

The following are examples of the kinds of multiple-choice questions found on the exam.

1. A cybersecurity analyst recently completed a review of a hotel's security. Consider the following information from their report.
   - The hotel's Wi-Fi extends to the parking area, allowing outsiders potential access to the network.
   - Open network ports in the conference center connect to the hotel's internal network and could enable spoofing of a legitimate device.
   - Guest feedback tablets in the lobby use a shared Wi-Fi network, exposing nonsensitive customer satisfaction data.
   - Model numbers of printers and the firmware versions the printers are running are visible on the internal network, revealing some information about devices on the network.

   Which of the following risks would the cybersecurity analyst most likely document as a high risk?

   (A) The hotel's Wi-Fi extending to the parking area

   (B) Open network ports in the conference center

   (C) Guest feedback tablets using a shared Wi-Fi network

   (D) The model numbers of printers and the firmware versions the printers are running being visible

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

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.

Questions 8 through 10 refer to the following.

Consider the following email that was identified and reported as a phishing attempt.

From: Human Resources
To: All Employees

Subject: Final Reminder — Deadline Today!

Our records indicate that your employee profile is incomplete. In order to remain in compliance with company-wide HR standards, all staff must confirm their personal information by the end of the day. Failure to respond by this deadline may result in suspension of payroll access until your profile is verified.

Please note: Over 92% of employees have already completed this verification, and you are among the last to finalize your record.

To confirm your employee file, reply to this email with the following details:

1. Personal phone number
2. Pet's name (for verification)
3. Date of birth

We appreciate your cooperation in keeping our records accurate and ensuring continued access to employee services.

Thank you,

Human Resources

8. Which of the following shows how the email uses urgency to pressure the recipient into responding?
   (A) The recipient is warned that they must confirm their personal information by the end of the day.
   (B) The recipient is warned that failure to comply could result in payroll suspension.
   (C) The recipient is encouraged to help human resources keep their records accurate.
   (D) The recipient is told that the message comes from a trusted internal department.

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

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.

16. A state's National Guard base is documenting cybersecurity risks from physical vulnerabilities. Which of the following would be classified as a moderate risk?
    (A) An unlocked trailer containing non-networked office equipment that cannot be used to access sensitive systems
    (B) A locked warehouse with noncritical computers that could be a foothold to access other network resources
    (C) A publicly accessible touchscreen directory for visitors that contains no sensitive data and is unlikely to be exploited
    (D) A main server room that contains sensitive systems and information and does not have sufficiently restricted or controlled access

Questions 17 through 20 refer to the following.

Consider the following article.

> *Small Town Bank Disrupts Attempted Cyber Attack on Customer Database*
>
> Fairgrove Community Bank, a local financial institution serving residents of central Kentucky, reported that it successfully stopped a cyber intrusion attempt earlier this week aimed at its customer database.
>
> The attack was detected on Tuesday afternoon when automated security systems flagged unusual database queries originating from the bank's online loan application form. Investigators determined that the form was being used to input malicious code.
>
> "One of the strings the adversary submitted included `' OR '1'='1';--`," said James Holloway, a network administrator at Fairgrove Community Bank. "That's a common trick pulled from online tutorials."
>
> Holloway said the attacker did not succeed in accessing any customer data, but the attempt revealed a flaw in the bank's web application.
>
> Fairgrove Community Bank's security team has since patched the vulnerability. No data was compromised, and banking operations continued without interruption.
>
> "This wasn't some advanced adversary," Holloway added. "They were copying code from the internet and testing to see if anything would work. But even simple attacks like this can work if we don't implement best practices."
>
> Fairgrove Community Bank says it is conducting a full audit of its customer-facing applications to ensure proper protections are in place.

17. Which of the following best describes the adversary in this scenario?
    (A) Cyberterrorist
    (B) Script kiddie
    (C) State actor
    (D) Insider

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

22. A hospital's security manager has implemented an automated network security tool with the following functions.
    - The tool analyzes network traffic for signs of malicious activity so the security team can quickly spot potential threats.
    - The tool generates an alert when suspicious or malicious traffic is detected because the hospital wants to be notified right away if an attack is attempted.
    - The tool does not take direct action to block or stop the traffic itself because the hospital wants administrators to decide how to respond to threats.

    Which of the following security systems did the security manager implement?

    (A) Data loss prevention system

    (B) Network intrusion prevention system

    (C) Network intrusion detection system

    (D) Security information and event management system

Section II: Free-Response Question

The following is an example of the free-response question found on the exam.

Device Security Analysis

The following sources all come from the same device and are captured in a risk assessment for this device.

Source 1

The device's IP address is 192.168.1.10.

Device Firewall Settings

Rule Number	Action	Source	Destination	Direction	Port Number	Protocol
1	Deny	172.45.66.184	192.168.1.10	Inbound	22	SSH
2	Allow	ALL	192.168.1.10	Inbound	21	FTP
3	Allow	ALL	192.168.1.10	Inbound	80	HTTP
4	Allow	ALL	192.168.1.10	Inbound	445	SMB
5	Allow	ALL	192.168.1.10	Inbound	443	HTTPS
6	Allow	ALL	192.168.1.10	Inbound	22	SSH
7	Allow	172.45.66.184	192.168.1.10	Inbound	3306	MySQL
8	Allow	ALL	192.168.1.10	Inbound	3389	RDP
9	Allow	192.168.1.50	192.168.1.10	Inbound	5900	VNC
10	Deny	ALL	ALL	Inbound	ALL	ALL

Source 2

```
sudo tail -n 30 /var/log/app/network_app.log

1 - Nov 10 09:00:11 ubuntu sudo: jprice : TTY=pts/0 ;
PWD=/home/jprice ; USER=root ; COMMAND=/usr/bin/
less/var/log/syslog

2 - Nov 10 09:00:15 ubuntu sudo: pam_unix(sudo:
session): session opened for user root by
jprice(uid=1000)

3 - Nov 10 09:00:35 ubuntu apt-get[1345]: Get:1
http://archive.ubuntu.com jammy InRelease [265 kB]

4 - Nov 10 09:00:46 ubuntu apt-get[1345]: Get:2
http://security.ubuntu.com jammy-security InRelease
[110 kB]

5 - Nov 10 09:00:55 ubuntu apt-get[1345]: Fetched
375 kB in 19s (19.7 kB/s)

6 - Nov 10 09:01:00 ubuntu apt-get[1345]: Reading
package lists... Done

7 - Nov 10 09:01:01 ubuntu sudo: pam_unix(sudo:
session):
session closed for user root

8 - Nov 10 09:02:14 ubuntu jprice: executed command:
'ufw status verbose'

9 - Nov 10 09:02:14 ubuntu jprice: executed command:
'systemctl status apache2'

10- Nov 10 09:02:16 ubuntu jprice: executed command:
'tail –n /var/log/auth.log'

11 - Nov 10 09:03:10 ubuntu jprice: executed
command: 'systemctl status apache2'

12 - Nov 10 09:03:35 ubuntu systemd[1]: Starting
Daily apt download activities...

13 - Nov 10 09:03:36 ubuntu systemd[1]: Finished
Daily apt download activities.

14 - Nov 10 09:04:00 ubuntu jprice: executed
command: 'ss -tuln'

15 - Nov 10 09:04:01 ubuntu jprice: executed
command: 'cat/etc/ufw/user.rules'

16 - Nov 10 09:05:11 ubuntu jprice: executed
command: 'journalctl -xe'

17 - Nov 10 09:05:32 ubuntu jprice: executed
command: 'df -h'

18 - Nov 10 09:05:50 ubuntu jprice: executed
command: 'du -sh/var/log'
```

```
19 - Nov 10 09:06:02 ubuntu jprice: executed
command: 'top -n 1'

20 - Nov 10 09:06:33 ubuntu jprice: executed
command: 'curl -I http://localhost'

21 - Nov 10 09:06:33 ubuntu sudo:
pam_unix(sudo:session): session opened for user root
by jprice(uid=1000)

22 - Nov 10 09:06:34 ubuntu sudo:
pam_unix(sudo:session): session closed for user root

23 - Nov 10 09:07:01 ubuntu CRON[1773]:
pam_unix(cron:session): session opened for user root
by (uid=0)

24 - Nov 10 09:07:01 ubuntu CRON[1773]:
pam_unix(cron:session): session closed for user root

25 - Nov 10 09:07:45 ubuntu jprice: executed
command: 'ip addr'

26 - Nov 10 09:07:47 ubuntu jprice: executed
command: 'netstat - tulnp'

27 - Nov 10 09:08:10 ubuntu jprice: executed
command: 'ufw status verbose'

28 - Nov 10 09:08:11 ubuntu systemd[1]: Reloading
firewall rules (ufw.service)...

29 - Nov 10 09:08:11 ubuntu systemd[1]: Reloaded
firewall rules (ufw.service).

30 - Nov 10 09:08:20 ubuntu jprice: executed
command: 'exit'
```

Source 3

```
sudo tail -n 30 /var/log/auth.log

1 - Nov 10 14:11:43 ubuntu sshd[1123]: Server
listening on 0.0.0.0 port 22.

2 - Nov 10 14:11:43 ubuntu sshd[1123]: Server
listening on :: port 22.

3 - Nov 10 14:21:01 ubuntu vsftpd[2184]: Failed login
for invalid user admin from 203.0.113.25 port 21 ftp

4 - Nov 10 14:21:02 ubuntu vsftpd[2186]: Failed login
for invalid user root from 203.0.113.25 port 21 ftp

5 - Nov 10 14:21:03 ubuntu vsftpd[2188]: Failed login
for invalid user test from 203.0.113.25 port 21 ftp

6 - Nov 10 14:21:04 ubuntu vsftpd[2190]: Failed login
for invalid user guest from 203.0.113.25 port 21 ftp

7 - Nov 10 14:21:05 ubuntu vsftpd[2192]: Failed login
for invalid user ubuntu from 203.0.113.25 port 21 ftp
```

```
8 - Nov 10 14:21:06 ubuntu vsftpd[2194]: Failed login
for invalid user deploy from 203.0.113.25 port 21 ftp

9 - Nov 10 14:21:07 ubuntu vsftpd[2196]: Failed
login for invalid user support from 203.0.113.25
port 21 ftp

10 - Nov 10 14:21:08 ubuntu vsftpd[2198]: Failed
login for invalid user admin1 from 203.0.113.25 port
21 ftp

11 - Nov 10 14:21:09 ubuntu vsftpd[2200]: Failed
login for invalid user oracle from 203.0.113.25 port
21 ftp

12 - Nov 10 14:21:10 ubuntu vsftpd[2202]: Failed
login for invalid user ftp from 203.0.113.25 port 21
ftp

13 - Nov 10 14:22:14 ubuntu sshd[2234]: Connection
closed by authenticating user jprice 192.168.1.50
port 22 [preauth]

14 - Nov 10 14:22:15 ubuntu sshd[2234]: Accepted
password for jprice from 192.168.1.50 port 22 ssh2

15 - Nov 10 14:22:15 ubuntu sshd[2234]:
pam_unix(sshd:session): session opened for user
jprice by (uid=0)

16 - Nov 10 14:25:47 ubuntu sudo: jprice : TTY=pts/0 ;
PWD=/home/jprice ; USER=root ; COMMAND=/usr/bin/apt
update

17 - Nov 10 14:25:47 ubuntu sudo:
pam_unix(sudo:session): session opened for user root
by jprice(uid=1000)

18 - Nov 10 14:25:48 ubuntu sudo:
pam_unix(sudo:session):session closed for user root

19 - Nov 10 14:28:02 ubuntu sshd[2331]: Connection
closed by 203.0.113.25 [preauth]

20 - Nov 10 14:29:01 ubuntu CRON[2345]:
pam_unix(cron:session): session opened for user root
by (uid=0)

21 - Nov 10 14:29:01 ubuntu CRON[2345]:
pam_unix(cron:session): session closed for user root

22 - Nov 10 14:30:17 ubuntu kernel: [UFW BLOCK]
IN=eth0 OUT= SRC=203.0.113.25 DST=192.168.1.10
PROTO=TCP PORT=25 SYN

23 - Nov 10 14:30:18 ubuntu sshd[2369]: Failed
password for invalid user user from 203.0.113.25
port 22 ssh2

24 - Nov 10 14:30:18 ubuntu sshd[2370]: Received
disconnect from 203.0.113.25 port 49151:11: Bye Bye
[preauth]
```

```
25 - Nov 10 14:30:18 ubuntu kernel: [UFW BLOCK]
IN=eth0 OUT= SRC=203.0.113.25 DST=192.168.1.10
PROTO=TCP PORT=77 SYN

26 - Nov 10 14:31:55 ubuntu systemd-logind[99]: New
session 7 of user jprice.

27 - Nov 10 14:31:55 ubuntu systemd: Started Session
7 of user jprice.

28 - Nov 10 14:31:55 ubuntu sudo: jprice : TTY=pts/0 ;
PWD=/home/jprice ; USER=root ; COMMAND=/usr/bin/
journalctl -xe

29 - Nov 10 14:31:55 ubuntu sudo:
pam_unix(sudo:session): session opened for user root
by jprice(uid=1000)

30 - Nov 10 14:31:56 ubuntu sudo:
pam_unix(sudo:session): session closed for user root
```

Source 4

```
sudo tail -n 30 /var/log/nginx/access_log

1 - 192.168.1.50 - jprice [10/Nov/2025:09:02:14
-0500] "GET/index.html HTTP/1.1" 200 4212 "-"
"Mozilla/5.0 (Ubuntu)"

2 - 192.168.1.50 - jprice [10/Nov/2025:09:02:15
-0500] "GET /assets/css/style.css HTTP/1.1" 200 1024
"-" "Mozilla/5.0 (Ubuntu)"

3 - 192.168.1.50 - jprice [10/Nov/2025:09:02:15
-0500] "GET /assets/js/main.js HTTP/1.1" 200 2876
"-" "Mozilla/5.0 (Ubuntu)"

4 - 192.168.1.50 - jprice [10/Nov/2025:09:02:16
-0500] "GET /images/logo.png HTTP/1.1" 200 2048 "-"
"Mozilla/5.0 (Ubuntu)"

5 - 192.168.1.50 - jprice [10/Nov/2025:09:02:17
-0500] "GET /about.html HTTP/1.1" 200 3198 "-"
"Mozilla/5.0 (Ubuntu)"

6 - 192.168.1.50 - jprice [10/Nov/2025:09:02:18
-0500] "GET /contact.html HTTP/1.1" 200 2951 "-"
"Mozilla/5.0 (Ubuntu)"

7 - 192.168.1.50 - jprice [10/Nov/2025:09:02:20
-0500] "POST /contact_form HTTP/1.1" 200 87
"https://example.local/contact.html" "Mozilla/5.0
(Ubuntu)"

8 - 192.168.1.50 - jprice [10/Nov/2025:09:02:21
-0500] "GET /dashboard HTTP/1.1" 200 4981 "-"
"Mozilla/5.0 (Ubuntu)"
```

```
9 - 192.168.1.55 - - [10/Nov/2025:09:03:10 -0500]
"GET /api/user/profile?id=12 HTTP/1.1" 200 614 "-"
"curl/7.81.0"

10 - 192.168.1.55 - - [10/Nov/2025:09:03:11
-0500] "GET /api/data/list HTTP/1.1" 200 1187 "-"
"curl/7.81.0"

11 - 192.168.1.55 - - [10/Nov/2025:09:03:12 -0500]
"POST /api/user/update HTTP/1.1" 200 152 "-"
"curl/7.81.0"

12 - 10.0.0.5 - admin [10/Nov/2025:09:04:01
-0500] "GET /admin/login HTTP/1.1" 200 4329 "-"
"Mozilla/5.0 (Windows NT 10.0)"

13 - 10.0.0.5 - admin [10/Nov/2025:09:04:02 -0500]
"POST /admin/login HTTP/1.1" 302 112 "https://
example.local/admin/login" "Mozilla/5.0 (Windows NT
10.0)"

14 - 10.0.0.5 - admin [10/Nov/2025:09:04:03 -0500]
"GET /admin/dashboard HTTP/1.1" 200 6275 "-"
"Mozilla/5.0 (Windows NT 10.0)"

15 - 203.0.113.45 - - [10/Nov/2025:09:04:11 -0500]
"GET ../../../../etc/passwd HTTP/1.1" 400 234 "-"
"curl/7.68.0"

16 - 203.0.113.45 - - [10/Nov/2025:09:04:12 -0500]
"GET ../../../etc/shadow HTTP/1.1" 403 312 "-"
"curl/7.68.0"

17 - 203.0.113.45 - - [10/Nov/2025:09:04:13 -0500]
"GET ../../../var/www/html/config.php.bak HTTP/1.1"
404 198 "-" "curl/7.68.0"

18 - 192.168.1.55 - - [10/Nov/2025:09:04:15 -0500]
"GET /api/status HTTP/1.1" 200 94 "-" "curl/7.81.0"

19 - 192.168.1.50 - jprice [10/Nov/2025:09:04:16
-0500] "GET /logout HTTP/1.1" 302 51 "-"
"Mozilla/5.0 (Ubuntu)"

20 - 192.168.1.50 - jprice [10/Nov/2025:09:04:17
-0500] "GET /login.html HTTP/1.1" 200 3811 "-"
"Mozilla/5.0 (Ubuntu)"

21 - 192.168.1.50 - jprice [10/Nov/2025:09:05:00
-0500] "GET /favicon.ico HTTP/1.1" 200 428 "-"
"Mozilla/5.0 (Ubuntu)"

22 - 192.168.1.50 - jprice [10/Nov/2025:09:05:22
-0500] "GET /docs/index.html HTTP/1.1" 200 2491 "-"
"Mozilla/5.0 (Ubuntu)"

23 - 192.168.1.55 - - [10/Nov/2025:09:05:23 -0500]
"GET /api/docs HTTP/1.1" 200 682 "-" "curl/7.81.0"

24 - 192.168.1.50 - jprice [10/Nov/2025:09:05:25
-0500] "GET /help HTTP/1.1" 200 4122 "-"
"Mozilla/5.0 (Ubuntu)"
```

```
25 - 192.168.1.55 - - [10/Nov/2025:09:05:26 -0500]
"GET /api/user/profile?id=14 HTTP/1.1" 200 637 "-"
"curl/7.81.0"

26 - 10.0.0.5 - admin [10/Nov/2025:09:05:27 -0500]
"GET /admin/settings HTTP/1.1" 200 5214 "-"
"Mozilla/5.0 (Windows NT 10.0)"

27 - 10.0.0.5 - admin [10/Nov/2025:09:05:28
-0500] "POST /admin/update HTTP/1.1" 200 164 "-"
"Mozilla/5.0 (Windows NT 10.0)"

28 - 192.168.1.50 - jprice [10/Nov/2025:09:05:29
-0500] "GET /assets/js/analytics.js HTTP/1.1" 200
1193 "-" "Mozilla/5.0 (Ubuntu)"

29 - 192.168.1.50 - jprice [10/Nov/2025:09:05:30
-0500] "GET / HTTP/1.1" 200 4231 "-" "Mozilla/5.0
(Ubuntu)"

30 - 192.168.1.50 - jprice [10/Nov/2025:09:05:31
-0500] "GET /images/banner.jpg HTTP/1.1" 200 3087
"-" "Mozilla/5.0 (Ubuntu)"
```

Source 5

```
ls -l /home/jprice/Documents

-rw-r--r--  1 jprice  jprice   2143 Nov  08  09:15  report.txt

-rw-------  1 jprice  jprice   1024 Nov  02  09:01  secrets.key

-rwxr-xr-x  1 jprice  jprice   8576 Nov  10  11:02  backup.sh

-r--r-----  1 jprice  admin    3421 Nov  06  11:53  config.cfg

-rw-rw-r--  1 jprice  devteam  5012 Nov  10  09:04  notes.md

-rwx------  1 jprice  jprice   7744 Nov  10  06:17  deploy_script

-rw-r-----  1 jprice  admin    2088 Nov  09  09:36  database.ini

-rwxrwx---  1 jprice  devteam  9281 Nov  04  01:27  run_tests.sh

-rw-r--rw-  1 jprice  shared   3999 Nov  01  12:08  public_data.csv
```

Source 6

Acceptable Use Policy

Required Activities:

- Users must keep the operating system and installed software up to date.

Permitted Activities:

- Users may connect peripheral devices such as keyboards, mice, monitors, and printers as needed for daily work.

Prohibited Activities:

- Users may not connect external drives, USB storage devices, or other removable media unless explicitly authorized.
- Users may not modify system configurations, security settings, or access controls without authorization.
- Users may not access social media websites on this device.

Device Security Analysis

Use the given information to respond to parts A, B, C, D, and E. Label any subparts (e.g., i and ii) that may be present.

Part A

Consider the policy for the device in Source 6.

i. **Explain** how one part of the policy helps protect the device.

ii. **Explain** how one rule in the current policy could be modified to make the device more secure. Include a specific example in your response.

Part B

In the authorization log, there is evidence of a password attack in rows 3–12.

i. **Describe** the evidence in the log file that indicates a password attack. Include specific entries from the log file in your response.

ii. **Identify** the IP address of the adversary.

Part C

Consider all the sources from the device.

i. **Explain** how the permission settings for one file in the `/home/jprice/Documents` directory determine the level of access for that file for the owner, group, and all other users on the system. Include the name of the file in your response.

ii. Other than removing all permissions from all users, **describe** one way the permission settings for one file on the system could be configured to restrict access for some users on the device. Include the name of the file in your response.

iii. Using the explanation from part C (ii), **write** one or more `chmod` commands that set the permissions described.

Part D

Consider all the sources from the device.

i. **Explain** how one connection attempt on the device was blocked by the device's firewall. Include evidence from a log file in your response.

ii. Other than allowing all traffic for all services, **describe** a modification to one firewall rule that would allow the connection attempt identified in part D (i).

iii. Other than allowing the connection attempt identified in part D (i), **describe** one impact of your modification from part D (ii) on incoming or outgoing network traffic on the device.

Part E

Apart from the password attack identified in part B, there is evidence of another attack on the device. Consider all the sources from the device.

i. **Determine** the type of attack evidenced in a log file.

ii. **Describe** specific information in the log file that indicates the attack named in part E (i).

iii. **Describe** one way an automated system could halt this type of attack in real time.

iv. This attack could be mitigated by an automated system, such as a firewall, IDS, IPS, or AI. **Identify** a different countermeasure that could mitigate, prevent, or deter the attack.