

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

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.