Answer Key and Question Alignment to Course Framework

Multiple-Choice Question	Answer	Skill	Learning Objective
1	B	1.C	3.1.C
2	B	2.D	5.2.D
3	D	2.B	5.2.C
4	C	2.C	3.4.B
5	D	1.A	4.2.A
6	C	2.B	4.2.C
7	D	1.B	4.2.B
8	A	1.A	1.1.A
9	D	1.B	2.1.A
10	A	1.C	1.1.C
11	C	3.D	5.6.E
12	B	3.A	4.4.A
13	A	3.C	3.5.D
14	A	3.D	3.5.E
15	B	2.A	4.2.A
16	B	1.D	2.2.C
17	B	1.A	2.1.B
18	A	3.D	5.6.E
19	C	2.B	5.5.B
20	D	1.B	5.1.B
21	C	2.A	4.2.C
22	C	3.A	3.5.A

Free-Response Question	Skills	Learning Objectives
Device Security Analysis	2.A, 2.B, 2.C, 2.D, 3.B, 3.D	3.1.A, 3.4.B, 3.4.D, 3.5.A, 3.5.E, 4.1.C, 4.2.D, 4.3.A, 4.3.C, 4.4.A, 4.4.D, 5.1.B, 5.2.D, 5.5.B, 5.6.E

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

Scoring Guidelines

Device Security Analysis — 14 points

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.

Model Responses

Part A

i. Not allowing users to connect removable media devices helps protect the device against malware that could be installed on it. Because the organization does not have control over external devices, they cannot guarantee that no malware will automatically be installed when they are plugged into the device.

ii. The AUP could require the system to check for updates within a certain time frame, such as weekly. If they force the system to check for updates weekly, this will ensure that all patches are installed in a timely fashion.

Part B

i. There are multiple failed login attempts within seconds of each other all from the same device. Row 3 is the first failed login at 14:21:01, and 9 seconds later there are 10 failed login attempts ending on row 12 at 14:21:10.

ii. 203.0.113.25

Part C

i. In the run_tests.sh file, the owner of the file and the group devteam have all permissions (read, write, and execute) for the file because the first and second groupings have rwx, while all other users on the system have no permissions for the file because the last grouping has ---.

ii. To harden the report.txt file, they could remove the read permission from both the group and all other users for this system.

iii. "chmod g-r report.txt" and then "chmod o-r report.txt"

Part D

i. Since firewall rule 10 denies all traffic to port 25 due to the absence of an allow rule, when the connection attempt from IP 203.0.113.25 occurs on line 22 in the auth log, the attempt to access port 25 is blocked.

ii. Rule 2 of the firewall could change the port number from 21 to 25.

iii. Changing the port in rule 2 to 25 from 21 would stop all inbound FTP/port 21 traffic to the device.

Part E

i. Directory traversal attack

ii. In lines 15–17 of the web application log (source 4), there are attempts of "../..", which is the classic sign of a directory traversal attack. They are attempting to go back in the file structure of the system where the web application is hosted—where they could try to access parts of the system that they should not have access to.

iii. An automated system could notice the malicious signs of a directory traversal attack and shut down the IP address from accessing the machine. So, in this case, it would stop the IP address of 203.0.113.45 from accessing the device when it recognizes the "../.." in the URL.

iv. The system could sanitize the user inputs to not allow any "../.." in the URL submitted by the user.

Scoring Guidelines for Question: Device Security Analysis

<table>
<tr><th>Reporting Category</th><th colspan="2">Scoring Criteria</th></tr>
<tr><td rowspan="5">Part A (i)
(0–1 points)
Point 1</td><td>0 points
Does not explain how any part of the policy helps protect the device.</td><td>1 point
Accurately explains how one part of the policy helps protect the device.</td></tr>
<tr><td colspan="2">Decision Rules and Scoring Notes</td></tr>
<tr><td>Responses that do not earn this point:
Are vague or unrelated to the policy.
Describe something not in the policy.
Do not clearly connect the policy to improved security.
Identify something in the policy without explaining how it protects the device.</td><td>Responses that earn this point:
Explain how a part of the acceptable use policy protects the device.</td></tr>
<tr><td>Examples that do not earn this point:
“Long passwords are good.”
“Users should avoid downloading games.”
“The policy keeps the device safe.”</td><td>Examples that earn this point:
“Users need to keep their operating system and software up to date because this ensures all known vulnerabilities are patched, preventing adversaries from exploiting them on the device.”
“Keeping the operating system and software up to date ensures known vulnerabilities are patched, reducing the risk of adversaries exploiting those vulnerabilities on the device.”</td></tr>
</table>

Reporting Category	Scoring Criteria	
Part A (ii) **(0–1 points)** **Point 2**	**0 points** Does not explain a modification to the current policy or describes a modification that would not improve security.	**1 point** Accurately **explains** how one rule in the current policy could be modified to make the device more secure, including a specific example in the response.
	Decision Rules and Scoring Notes	
	Responses that do not earn this point: ▪ Suggest adding a new rule instead of modifying an existing rule. ▪ Suggest a modification that would not enhance security. ▪ Do not provide evidence from a log file. ▪ Identify or describe without explaining.	**Responses that earn this point:** ▪ Propose a modification to a policy rule and accurately explain how this helps make the device more secure.
	Examples that do not earn this point: ▪ "Allow social media during lunch breaks." ▪ "Let users plug in USB devices if they think it's safe."	**Examples that earn this point:** ▪ "Modifying the removable media rule to include blocking wireless external storage, such as Bluetooth file transfers, would help prevent wireless Bluetooth attacks because it eliminates an additional attack vector." ▪ "Requiring automatic OS updates instead of manual updates ensures updates are applied without user intervention, helping keep the system up to date and reducing exposure to known vulnerabilities."

Reporting Category	Scoring Criteria	
Part B (i) **(0–1 points)** **Point 3**	**0 points** Does not describe evidence of a password attack in the authorization log or identifies the attack but does not include evidence from a log file.	**1 point** Accurately **describes** valid evidence in the log file that indicates a password attack, including specific entries from a log file in the response.
	Decision Rules and Scoring Notes	
	Responses that do not earn this point: ▪ Mention entries unrelated to failed authentication attempts. ▪ Describe normal logins.	**Responses that earn this point:** ▪ Describe multiple failed password attempts from the same IP address in quick succession.
	Examples that do not earn this point: ▪ "Row 14 shows a successful login." ▪ "There was a CRON job run at 14:29."	**Examples that earn this point:** ▪ "Rows 3–12 show repeated failed FTP login attempts for many usernames within seconds."

Reporting Category	Scoring Criteria	
Part B (ii) **(0–1 points)** **Point 4**	**0 points** Does not identify the correct IP address or port in the password attack.	**1 point** Accurately **identifies** the indicated IP address or port in the password attack.
	Decision Rules and Scoring Notes	
	Responses that do not earn this point: ▪ Provide any IP address other than 203.0.113.25. ▪ Identify multiple IP addresses. ▪ Provide a port.	**Responses that earn this point:** ▪ Identify IP address 203.0.113.25 as the adversary in the attack.
	Examples that do not earn this point: ▪ "113.25" ▪ "203.0.113.25 and 6.117.89.203"	**Examples that earn this point:** ▪ "203.0.113.25" ▪ "IP address 203.0.113.25"

Reporting Category	Scoring Criteria	
Part C (i) **(0–1 points)** **Point 5**	**0 points** Does not accurately explain file permissions or identifies incorrect user or group permissions.	**1 point** Accurately **explains** how the permission settings for one file in the indicated directory determine the level of access for that file for the owner, group, and all other users on the system, including the name of the file in the response.
	Decision Rules and Scoring Notes	
	Responses that do not earn this point: ▪ Misread the permission bits. ▪ Describe permissions for a file not in the stimulus. ▪ Do not list the name of the file. ▪ Identify or describe without explaining.	**Responses that earn this point:** ▪ Explain the correct permissions for owner, group, and others for a chosen file and identify the file.
	Examples that do not earn this point: ▪ "Everyone can read notes.md." ▪ "deploy_script is open to all users." ▪ "The owner can read and write, the group can read, and all other users have no permissions."	**Examples that earn this point:** ▪ "For backup.sh, the owner has read, write, and execute permissions because the permissions are rwx, while the group and others have read and execute permissions indicated by r-x." ▪ "For secrets.key, only the owner has read and write permissions, as shown by rw-, while the group and others have no permissions since no permission bits are set." ▪ "File: report.txt Owner: read and write since the first group is rw- Group: read only since the second group is r-- Others: read only since the last group is r--"

<table>
<tr><th>Reporting Category</th><th colspan="2">Scoring Criteria</th></tr>
<tr><td rowspan="5">Part C (ii)
(0–1 points)
Point 6</td><td>0 points
Does not describe a valid configuration change to the permissions of one file to modify access for users on this device.</td><td>1 point
Accurately describes one way the permission settings for one file on the system could be configured to appropriately modify access (by granting or removing permissions) for some users on the device, including the name of the file in the response.</td></tr>
<tr><td colspan="2">Decision Rules and Scoring Notes</td></tr>
<tr><td>Responses that do not earn this point:
Suggest removing all permissions for a file on this system.
Suggest removing all access for the owner.
Do not identify the file name.</td><td>Responses that earn this point:
Suggest removing one or more permissions from a file that it currently has.
Suggest removing read, write, or execute access appropriately.</td></tr>
<tr><td>Examples that do not earn this point:
“Remove execute permission from report.txt for owner.”
“Remove all permissions so no one can access it.”
“Give write permissions to all users on secrets.key.”</td><td>Examples that earn this point:
“Remove read access for the group and others on report.txt to keep it private to the owner.”
“Remove execute permission for the owner on deploy_script.”</td></tr>
<tr><td colspan="2">Additional notes:
The file explained in part C (i) does not have to be the same file discussed in part C (ii) to earn the point.</td></tr>
</table>

<table>
<tr><th>Reporting Category</th><th colspan="2">Scoring Criteria</th></tr>
<tr><td rowspan="5">Part C (iii)
(0–1 points)
Point 7</td><td>0 points
Does not write a valid chmod command or the command does not match the permissions described in part C (ii).</td><td>1 point
Accurately writes one or more chmod commands that would set the permissions described in part C (ii).</td></tr>
<tr><td colspan="2">Decision Rules and Scoring Notes</td></tr>
<tr><td>Responses that do not earn this point:
Have incorrect command syntax.
Have permissions that do not match the configuration to restrict access described in part C (ii).</td><td>Responses that earn this point:
Use correct syntax, such as <code>chmod 600 filename</code>, or symbolic modes matching the response in part C (ii).</td></tr>
<tr><td>Examples that do not earn this point:
“chmod -rw------- deploy.sh”
“chmod 777 secrets.key”</td><td>Examples that earn this point:
“chmod 200 run_tests.sh”
“sudo chmod go-r report.txt”</td></tr>
<tr><td colspan="2">Additional notes:
Correct responses may begin with <code>sudo</code>, but <code>sudo</code> is not required to earn the point.
The response may still earn the point for part C (iii) if it did not earn the point for part C (ii) as long as the chmod command accurately sets the permissions described in part C (ii).</td></tr>
</table>

<table>
<tr><th>Reporting Category</th><th colspan="2">Scoring Criteria</th></tr>
<tr><td rowspan="5">Part D (i)
(0–1 points)
Point 8</td><td>0 points
Does not explain how a connection attempt was blocked or identifies an event unrelated to the firewall.</td><td>1 point
Accurately explains how one connection attempt on the device was blocked by the device's firewall, including evidence from a log file in the response.</td></tr>
<tr><td colspan="2">Decision Rules and Scoring Notes</td></tr>
<tr><td>Responses that do not earn this point:
Reference a login failure not caused by the firewall.
Indicate a successful login attempt.
Indicate multiple attempts being blocked where at least one attempt is incorrect.
Do not provide evidence from a log file.
Identify or describe without explaining.</td><td>Responses that earn this point:
Correctly identify a line from a log file and a firewall rule that would prevent the attempt in the log file, and explain why it would be prevented.
Indicate how more than one connection attempt is being blocked by the firewall.</td></tr>
<tr><td>Examples that do not earn this point:
"User admin failed login because of a wrong password."
"SSH from 192.168.1.50 was blocked."</td><td>Examples that earn this point:
"Source 3 line 22 shows a blocked TCP SYN packet to port 25 from 203.0.113.25 because no firewall rule allows traffic on port 25."
"In line 25 of the auth log, a connection attempt to port 77 is blocked by the firewall, as access to port 77 is not permitted."</td></tr>
</table>

<table>
<tr><th>Reporting Category</th><th colspan="2">Scoring Criteria</th></tr>
<tr><td rowspan="5">Part D (ii)
(0–1 points)
Point 9</td><td>0 points
Does not describe a valid change to a firewall rule or suggests a modification that does not allow the connection attempt identified in part D (i).</td><td>1 point
Accurately describes a modification to one firewall rule that would allow the connection attempt identified in part D (i).</td></tr>
<tr><td colspan="2">Decision Rules and Scoring Notes</td></tr>
<tr><td>Responses that do not earn this point:
Suggest adding another deny rule to the firewall.
Suggest altering an unrelated firewall rule.
Suggest allowing a modification that would allow all traffic for all services.</td><td>Responses that earn this point:
Suggest a change that would allow the connection attempt from part D (i).</td></tr>
<tr><td>Examples that do not earn this point:
“Change rule 3 from allow to deny.”
“Disable the firewall.”</td><td>Examples that earn this point:
“Modify rule 8 to allow port 25 before the final deny-all rule.”</td></tr>
<tr><td colspan="2">Additional notes:
The response may still earn the point for part D (ii) if it did not earn the point for part D (i).</td></tr>
</table>

Reporting Category	Scoring Criteria	
Part D (iii) **(0–1 points)** **Point 10**	**0 points** Does not describe the impact of the modification suggested in part D (ii).	**1 point** Correctly **describes** one impact of the modification suggested in part D (ii) on incoming or outgoing network traffic on the device.
	Decision Rules and Scoring Notes	
	Responses that do not earn this point: ▪ Do not include an accurate impact of the firewall change. ▪ Include an incorrect impact of the firewall change. ▪ Only references the connections in part D (i) or part D (ii) being impacted. ▪ Reference a different change than was recommended in part D (ii).	**Responses that earn this point:** ▪ Describe an impact of implementing the modification to the firewall as described in part D (ii).
	Examples that do not earn this point: ▪ "It would block all adversaries." ▪ "It would stop brute force attempts." ▪ "It would allow the connection that was blocked originally by the firewall."	**Examples that earn this point:** ▪ "Allowing port 25 would permit email traffic into the device but could expose the system to SMTP-based attacks."

Reporting Category	Scoring Criteria	
Part E (i) **(0–1 points)** **Point 11**	**0 points** Does not determine the type of attack.	**1 point** Accurately **determines** the type of attack evidenced in a log file.
	Decision Rules and Scoring Notes	
	Responses that do not earn this point: ▪ Identify a type of attack not supported by the evidence. ▪ Indicate multiple attack types where at least one attack is incorrect. ▪ Indicate a password attack.	**Responses that earn this point:** ▪ Identify directory traversal as the type of attack.
	Examples that do not earn this point: ▪ "Ping flood attack" ▪ "DDoS attack" ▪ "ARP poisoning and directory traversal"	**Examples that earn this point:** ▪ "There is evidence of a directory traversal attack." ▪ "Directory traversal"

Reporting Category	Scoring Criteria	
Part E (ii) **(0–1 points)** **Point 12**	**0 points** Does not describe how specific entries indicate the attack using evidence from the log or gives a description unrelated to the log.	**1 point** Accurately **describes** specific information in the log file that indicates the attack named in part E (i).
	Decision Rules and Scoring Notes	
	Responses that do not earn this point: ▪ Do not include evidence from the log. ▪ Incorrectly interpret a directory traversal attack.	**Responses that earn this point:** ▪ Describe how the attack is indicated using evidence from source 4 lines 15–17 that show attempts, like "../../../../etc/passwd".
	Examples that do not earn this point: ▪ "The attacker sent a POST request, which shows they were trying to hack the server." ▪ "There is a lot of traffic, which indicates an attack." ▪ "The system blocked port 25, which indicates a traversal attack."	**Examples that earn this point:** ▪ "In source 4 line 15, the request includes '../../../../etc/passwd', which is a path traversal sequence attempting to reach system files outside the web root." ▪ "Lines 15–17 show attempts to access sensitive files like '/etc/passwd' and '/etc/shadow' using repeated '../', which is a signature of directory traversal attacks."

Reporting Category	Scoring Criteria	
Part E (iii) **(0–1 points)** **Point 13**	**0 points** Does not describe how an automated system could halt this type of attack.	**1 point** Accurately **describes** one way an automated system could halt this type of attack in real time.
	Decision Rules and Scoring Notes	
	Responses that do not earn this point: ▪ Reference making changes to the system prior to the attack. ▪ Indicate an action that would not stop the attack.	**Responses that earn this point:** ▪ Correctly state that an automated system would notice the malicious traffic and give a way to stop this traffic. ▪ Correctly state more than one way an automated system would stop this attack immediately.
	Examples that do not earn this point: ▪ "The device could install updates to stop the attack." ▪ "The system should deny social media so attackers can't get in."	**Examples that earn this point:** ▪ "An IPS could detect repeated '../' patterns and block 203.0.113.45 immediately." ▪ "An intrusion prevention system could monitor for attempts to access protected files, like /etc/passwd, and immediately drop the connection and blacklist the IP."

<table>
<tr><th>Reporting Category</th><th colspan="2">Scoring Criteria</th></tr>
<tr><td rowspan="5">Part E (iv)
(0–1 points)
Point 14</td><td>0 points
Does not identify a valid countermeasure or provides one already listed in the prompt.</td><td>1 point
Accurately identifies a countermeasure other than firewall, IDS, IPS, or AI that could mitigate, prevent, or deter the attack.</td></tr>
<tr><td colspan="2">Decision Rules and Scoring Notes</td></tr>
<tr><td>Responses that do not earn this point:
Identify a firewall, IDS, IPS, or AI-based countermeasure.
Do not identify a countermeasure that would stop this type of attack.</td><td>Responses that earn this point:
Identify sanitizing inputs.
Indicate not allowing "../.." patterns as a way to stop this type of attack.</td></tr>
<tr><td>Examples that do not earn this point:
"Install an IDS."
"Disable Telnet from the device as it is outdated."</td><td>Examples that earn this point:
"The application could sanitize user input to remove all '../' sequences before processing."</td></tr>
</table>