← Back Managing Safety and Security Risks Quiz
Graded Quiz • 30 min

Due Jul 11, 1:59 PM +07

✓ Congratulations! You passed!

Grade received 100%

Latest Submission Grade 100%

To pass 80% or higher

Go to next item

You have a new skill score!

Great job! Keep learning and making progress in your courses to increase your skill scores.

Probability & Statistics 141

1. What does the acronym SIEM stand for in a cybersecurity context?

1 / 1 point

○ Social, interpersonal, empathic, mental

○ Selective information extrapolation methods

● Security information and event management

○ Serial input to externalized modulation

✓ **Correct**
This is indeed what SIEM represents.

2. Which of the following sources does a SIEM system typically pull data from? (Select two.)

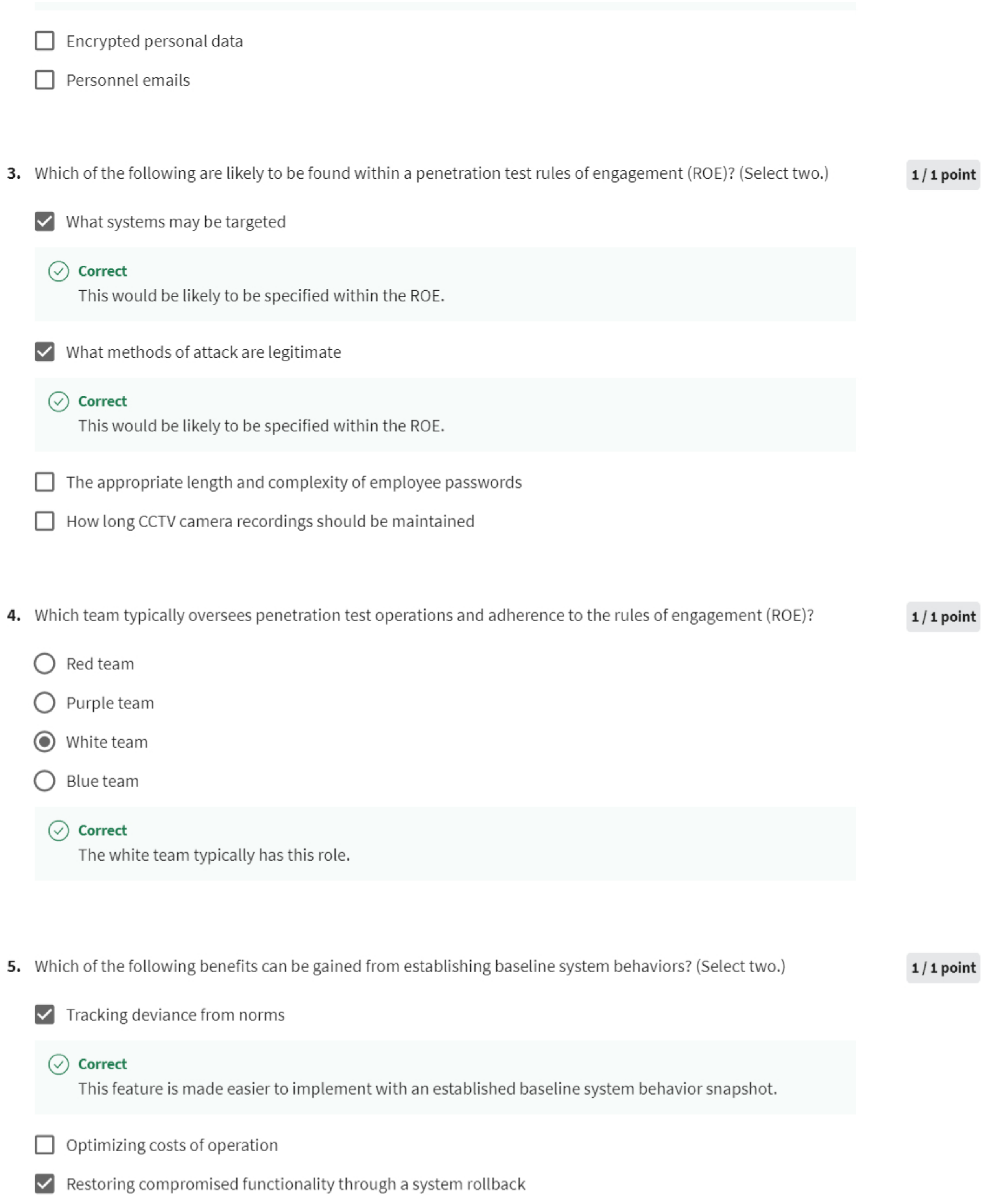
1 / 1 point

☑ System event logs

✓ **Correct**
This would be a likely information source for SIEM.

☑ Network intrusion detection alerts

✓ **Correct**
This would be a likely information source for SIEM.



□ Encrypted personal data

□ Personnel emails

3. Which of the following are likely to be found within a penetration test rules of engagement (ROE)? (Select two.) **1 / 1 point**

☑ What systems may be targeted

✓ **Correct**
This would be likely to be specified within the ROE.

☑ What methods of attack are legitimate

✓ **Correct**
This would be likely to be specified within the ROE.

□ The appropriate length and complexity of employee passwords

□ How long CCTV camera recordings should be maintained

4. Which team typically oversees penetration test operations and adherence to the rules of engagement (ROE)? **1 / 1 point**

○ Red team

○ Purple team

● White team

○ Blue team

✓ **Correct**
The white team typically has this role.

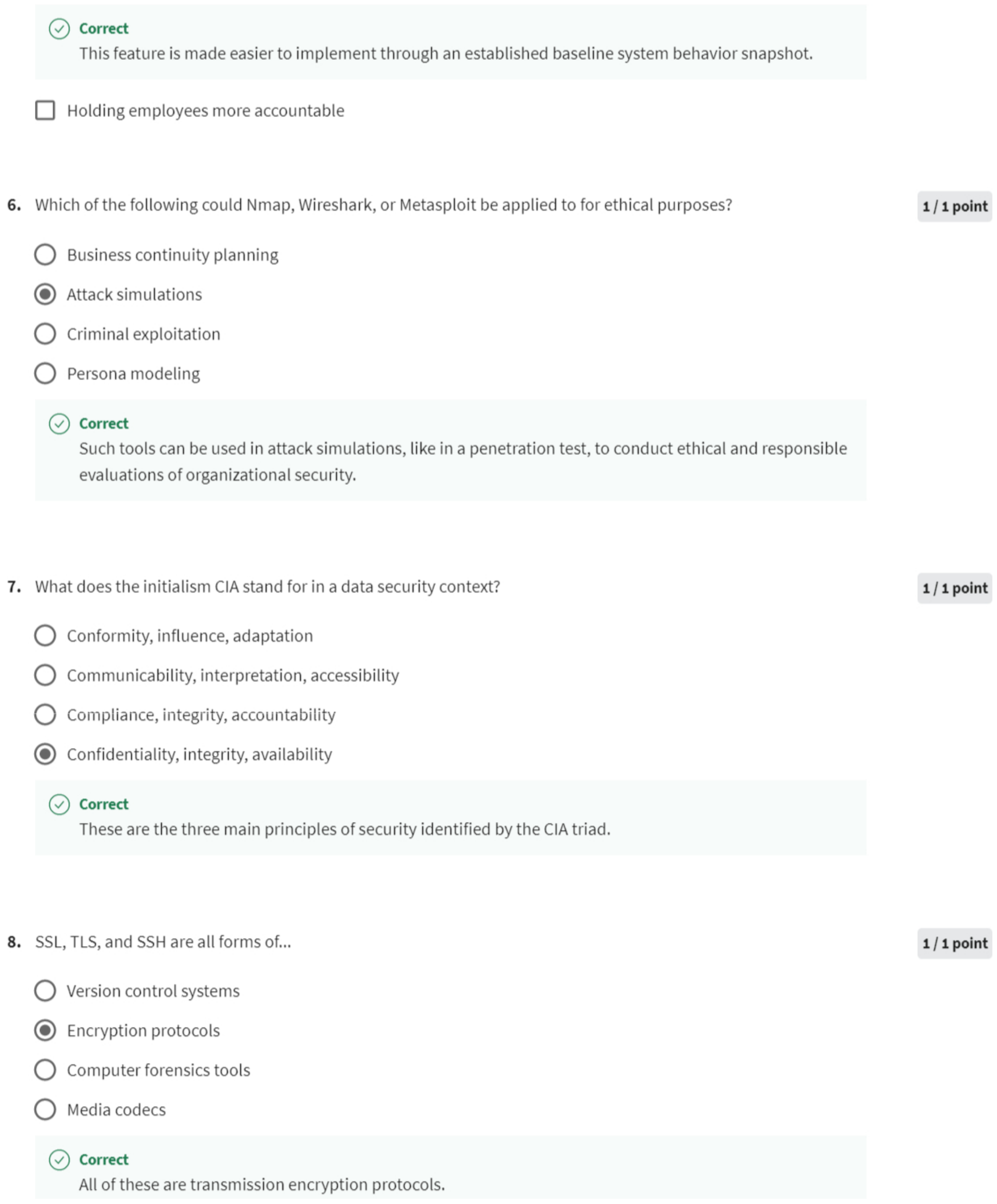
5. Which of the following benefits can be gained from establishing baseline system behaviors? (Select two.) **1 / 1 point**

☑ Tracking deviance from norms

✓ **Correct**
This feature is made easier to implement with an established baseline system behavior snapshot.

□ Optimizing costs of operation

☑ Restoring compromised functionality through a system rollback



✓ **Correct**
This feature is made easier to implement through an established baseline system behavior snapshot.

☐ Holding employees more accountable

6. Which of the following could Nmap, Wireshark, or Metasploit be applied to for ethical purposes?

1 / 1 point

○ Business continuity planning

● Attack simulations

○ Criminal exploitation

○ Persona modeling

✓ **Correct**
Such tools can be used in attack simulations, like in a penetration test, to conduct ethical and responsible evaluations of organizational security.

7. What does the initialism CIA stand for in a data security context?

1 / 1 point

○ Conformity, influence, adaptation

○ Communicability, interpretation, accessibility

○ Compliance, integrity, accountability

● Confidentiality, integrity, availability

✓ **Correct**
These are the three main principles of security identified by the CIA triad.

8. SSL, TLS, and SSH are all forms of...

1 / 1 point

○ Version control systems

● Encryption protocols

○ Computer forensics tools

○ Media codecs

✓ **Correct**
All of these are transmission encryption protocols.

9. What does the acronym CSIRT stand for in a security context?

1 / 1 point

○ Computer security immediate readiness tools

○ Conformance strategy, immutability, reliability, trustworthiness

○ Computer science, Internet, real-time interaction, technology

● Cybersecurity incident response team

✓ **Correct**
This is what CSIRT stands for in a cybersecurity context.

10. In which of the following could STRIDE or VAST classifications be applied?

1 / 1 point

● Threat modeling or analysis tools

○ Black box mitigation methods

○ Bias mitigation techniques

○ Network optimization tools

✓ **Correct**
STRIDE and VAST are techniques used to assess and analyze threats.