

PRACTICE QUESTIONS

GIAC / SANS

GMLE

GIAC Machine Learning Engineer

SHARED BY [u/Cosmic-Lantern-9540](#) on aiexamcerts

EDITION Free Set 2

QUESTIONS 10

SHARED October 15, 2026

EXAM GIAC / SANS GMLE, GIAC Machine Learning Engineer

Shared by [u/Cosmic-Lantern-9540](#) on aiexamcerts

10 practice questions for the GIAC / SANS GMLE exam, GIAC Machine Learning Engineer, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/giac-sans/gmle. Spotted a mistake? Email support@aiexamcerts.com with the exam code GMLE and the question number.

1. Which knowledge base catalogs adversarial tactics and techniques against machine learning systems, in a structure modeled on ATT&CK?

- A OWASP Top 10 for web applications
- B ISO 27001 Annex A controls
- C MITRE ATLAS
- D CIS Benchmarks for operating systems

Answer: C

MITRE ATLAS maps attacker tactics and techniques against AI and ML systems in a knowledge base modeled on ATT&CK. The OWASP Top 10 is tempting because it also lists common risks, but it targets web applications rather than ML models. ISO 27001 and the CIS Benchmarks are management and configuration standards.

2. Because the fraud model was trained on a full year of transactions, it is protected from distribution shift when it is deployed in new regions.

- A True
- B False

Answer: B (False)

Customers and payment patterns in new regions can differ from the training year, which can degrade accuracy without warning. A large training window does not guarantee coverage of a new population. The statement is false.

3. Which split strategy is most appropriate for time-ordered transaction data?

- A Random shuffling of all transactions before splitting them into folds
- B Splitting the records by alphabetical customer name
- C Using all data for both training and testing the model
- D Chronological split with the most recent data held out for testing

Answer: D

A time-based split tests on data that comes after the training period, which matches how the model will be used. Random shuffling is tempting because it gives balanced folds, but it lets the model see future patterns. Alphabetical splits and testing on training data do not reflect deployment.

4. Features must be computed from only the information that existed at prediction time, a rule known as point-in-_____ correctness.

Answer: time

Point-in-time correctness keeps offline results honest by excluding records that would not have been known when the prediction was made. Snapshot correctness is tempting as a similar phrase, but a snapshot describes a stored copy of data rather than the time-based rule. Full-dataset aggregation violates the rule by pulling in future records.

5. Which two risks come from a labeling vendor that is paid per label with no quality review? (Choose two.)
- A Label noise that degrades model accuracy
 - B Deliberate manipulation of labels that can implant hidden behavior
 - C Excessive GPU utilization on the training cluster
 - D Slow rendering of the labeling dashboard
 - E Expired TLS certificates on the vendor website

Answer: A, B

Without review, honest errors and deliberate manipulation can both enter the labels unnoticed, so the model learns the wrong patterns. GPU load is tempting as a cost concern, but it is an operational matter rather than a labeling risk. The dashboard and certificate issues are real operational problems, but neither describes label quality.

6. Which format is safer for distributing model weights because it stores tensors without executable code?
- A Python pickle (.pkl)
 - B safetensors
 - C Python source file with embedded weight arrays
 - D Compressed archive of Python bytecode

Answer: B

safetensors stores raw tensor data and metadata without executing code during loading, which is why it is preferred for shared weights. Pickle is tempting because it is the default in many workflows, but its loader can run arbitrary code. A source file and a bytecode archive also run code when loaded.

7. Which evaluation method estimates generalization by repeatedly training and validating on different partitions of the data?
- A Timing a single batch of inference requests
 - B Permutation importance computed on training data only
 - C Visual inspection of a monitoring dashboard
 - D K-fold cross-validation

Answer: D

K-fold cross-validation trains on k minus one folds and validates on the remaining one, rotating so every record is validated once and the scores are averaged. Permutation importance is tempting because it is a validation-adjacent technique, but computed on training data it measures fit rather than generalization. Timing and dashboards do not estimate predictive performance.

8. A model that scores well on a standard benchmark is guaranteed to resist adversarial inputs in production.
- A True
 - B False

Answer: B (False)

Benchmark accuracy measures performance on typical inputs and says little about deliberately crafted ones. Robustness must be tested separately with adversarial evaluation. The statement is false.

9. Which statement about adversarial transferability is correct?
- A Adversarial examples built against one model can often fool another
 - B Adversarial examples never transfer between models
 - C Transfer attacks require the victim's source code and training data
 - D Transferability only applies to audio models

Answer: A

Models trained on similar data often learn similar decision boundaries, which lets an attacker craft examples on a surrogate and apply them to a target. The claim that examples never transfer is tempting, but it is false. Source code access is not required for transfer, and the effect is not limited to audio.

10. Which property best describes a certified defense against adversarial examples?
- A A promise that the model was trained on more data than any competing model of its kind
 - B A mathematical guarantee of unchanged predictions within a perturbation bound
 - C A rule that the model is never updated after release
 - D A requirement that the model runs only on a CPU

Answer: B

Certified defenses prove a prediction cannot change for perturbations inside a norm ball of a given radius, which is a stronger claim than empirical testing. More training data is tempting as a robustness remedy, but it provides no proof. Freezing updates and CPU execution do not bound how predictions can change.