

PRACTICE QUESTIONS

GIAC / SANS

GMLE

GIAC Machine Learning Engineer

SHARED BY [u/Eager-Compass-2440](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 15, 2026

EXAM GIAC / SANS GMLE, GIAC Machine Learning Engineer

Shared by [u/Eager-Compass-2440](#) 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 threat model question should be answered first when scoping the security of an ML system?

- A Which GPU type gives the best training throughput for the largest planned model
- B Who can write to the training data and who can query the deployed model
- C Which Python version the team prefers to use for the training code
- D How many epochs to train the model for before it stops improving

Answer: B

The attack surface depends on who can influence the training data and who can query the model, and that determines poisoning and extraction risk. GPU selection is tempting because it is a major early decision, but it does not define threats. The Python version and epoch count are implementation details.

2. When scoping ML threats, the first question is the attacker's _____ level: whether they can write training data, query the model or read its parameters.

Answer: access (also accepted: access level)

Access level determines which attacks are feasible, from poisoning with write access to extraction with query access alone. Capability is tempting as a related idea, but it describes the attacker's skills rather than what they can reach. Objective describes the goal of the attack, not the access needed to carry it out.

3. Which practice reduces the impact of a single poisoned source in a crowdsourced dataset?

- A Averaging all labels from every contributor without checking their history
- B Deleting the source identifiers from each record before training
- C Requiring multiple independent annotators and agreement thresholds
- D Training only on the newest records in the dataset

Answer: C

Requiring agreement among independent annotators makes it harder for one contributor to push false labels into the dataset. Averaging labels is tempting because it sounds robust, but averaging does not stop a coordinated set of bad labels. Deleting source identifiers removes the ability to trace and block bad contributors.

4. Dataset provenance records the source, license and transformations of each dataset, which supports audit and incident response.
- A True
 - B False

Answer: A (True)

Provenance tells reviewers where data came from, what rights apply, and how it was processed, which is what an audit or a poisoning investigation needs. The statement is true. Provenance is sometimes confused with access logs, but it describes the data's history rather than who opened it.

5. Which two statements about robustness and evaluation are correct? (Choose two.)
- A A single aggregate accuracy number can hide poor performance on subgroups.
 - B Subgroup metrics should be reported alongside overall metrics.
 - C Test data should be reused repeatedly to tune hyperparameters.
 - D Standard k-fold cross-validation gives unbiased estimates for time series.
 - E Adversarial testing is unnecessary if the model passes unit tests.

Answer: A, B

Overall accuracy can mask failures on minority groups, so per-subgroup results belong next to the headline number. Reusing test data to tune is tempting as a shortcut, but it leaks information into the model choice. Standard k-fold cross-validation shuffles away time order, which is why it is wrong for forecasting, and unit tests check code paths rather than adversarial behavior.

6. Which hyperparameter search method samples combinations at random rather than exhaustively, often finding good settings faster in high-dimensional spaces?
- A Grid search
 - B Exhaustive enumeration of every combination with no time budget
 - C Manual trial of one setting at a time by an engineer
 - D Random search

Answer: D

Random search spends a fixed budget across the space, and it often covers the important dimensions better than a fixed grid. Grid search is tempting because it is systematic, but it spends most of its budget on unimportant dimensions. Exhaustive enumeration and one-at-a-time trials are slower or less informative.

7. Which risk matters most when loading a model file from an untrusted source in Python pickle format?
- A Pickle deserialization can execute arbitrary code during loading
 - B Pickle files cannot store numeric arrays
 - C Pickle files are always encrypted by default when saved through the standard library
 - D Pickle only supports image models

Answer: A

Python pickle can run code while deserializing, so loading an untrusted file can compromise the host. The claim that pickle cannot store arrays is tempting as a limitation, but pickle stores arrays without difficulty. Encryption and model type are not properties of the format.

8. A holdout set that is touched only once gives an unbiased _____ of performance after all model choices are made.

Answer: estimate (also accepted: final estimate)

Using the holdout only at the end prevents selection bias from leaking into the reported figure. Tuning the learning rate interactively is tempting because it is part of development, but repeated looks at the holdout bias the final number. Replacing the training data or storing logs are unrelated to this purpose.

9. What is the typical goal of a model extraction attack?
- A Delete the victim's training data from storage
 - B Encrypt the victim's API traffic with a new key
 - C Obtain a surrogate model that approximates the victim's behavior
 - D Increase the victim's response latency until legitimate users get timeouts

Answer: C

Extraction queries the target repeatedly and trains a substitute on the answers, which can then be used offline or to craft transferable attacks. Deleting data is tempting because it would also harm the victim, but it is not what extraction does. Traffic encryption and latency have nothing to do with copying behavior.

10. Which control helps detect adversarial or probing inputs at a model API?
- A Larger display fonts in the admin console for the on-call operators of the API
 - B Disabling request logs to lower storage costs
 - C Sharing the model weights publicly for community review
 - D Input validation plus anomaly scoring on request distributions

Answer: D

Validating formats and monitoring request statistics can flag probing and out-of-range inputs before they reach the model. Font size is tempting as a usability change, but it has no security effect. Disabling logs removes detection, and public weights make attacks easier.