

PRACTICE QUESTIONS

GIAC / SANS

GOAA

GIAC Offensive AI Analyst

SHARED BY [u/cosmic_widget_66](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 18, 2026

EXAM GIAC / SANS GOAA, GIAC Offensive AI Analyst

Shared by [u/cosmic_widget_66](#) on aiexamcerts

10 practice questions for the GIAC / SANS GOAA exam, GIAC Offensive AI Analyst, each followed by its answer and a short explanation. More free sets and the full practice exam: aiexamcerts.com/giac-sans/goaa. Spotted a mistake? Email support@aiexamcerts.com with the exam code GOAA and the question number.

1. Is it appropriate to use an AI tool during OSINT work to summarize public records without checking that the output is accurate?

- A True
- B False

Answer: B (False)

False. Language models can state unsupported facts, so an analyst must verify summarized information against the original sources before relying on it. Treating AI output as verified is a common error that can lead to wrong conclusions and reputational harm.

2. Which description best distinguishes an agent from a single prompt-and-response model call?

- A An agent is a model that is always trained from scratch on each new task, so it cannot use any tools at all
- B An agent is a model with a larger parameter count than a standard chat model
- C An agent loops through planning, tool calls and observations until a goal is met or it stops
- D An agent stores every answer in a static document that no one can later update

Answer: C

An agent decides on actions, invokes tools, observes results and repeats until its goal is complete or it halts, which is what makes its behavior harder to predict. A larger parameter count is the tempting distractor because it describes capacity rather than control flow. Training from scratch and static document storage are not defining features.

3. In an authorized penetration test, what is the main reason to generate a malware sample with an AI model?

- A To release the sample publicly so other researchers can study it
- B To test whether the client's detection stack identifies the sample's behavior in a controlled environment
- C To sell the sample on underground markets once the engagement is complete
- D To avoid writing the engagement report by letting the model describe the results to the client in a summary

Answer: B

Authorized generation is justified only as a controlled test of detection and response, with the sample contained and destroyed under the engagement rules. Public release is the tempting distractor because research sharing sounds legitimate, but it puts a working artifact in circulation. Selling samples and avoiding reporting are clearly out of scope.

4. Which defense is the most reliable protection against SQL injection in an application?
- A Hiding the database error messages from the browser while leaving the queries unchanged
 - B Relying only on a web application firewall rule that blocks the word SELECT in requests
 - C Renaming the database tables on a regular schedule to confuse automated tools that scan for injection points
 - D Using parameterized queries or prepared statements so user input is never executed as SQL

Answer: D

Parameterized queries keep the query structure separate from the data, so injected input cannot change the SQL statement. Hiding error messages is the tempting distractor because it reduces information leakage, but it does not stop the injection itself. A keyword block rule is easily bypassed, and renaming tables provides no real protection.

5. Which objective is most typical of a social engineering assessment in penetration testing?
- A Measuring whether employees follow a defined verification process when a sensitive request arrives
 - B Installing a permanent backdoor on every workstation in the building so that access survives future audits
 - C Collecting personal passwords from employees for a public leak list
 - D Disrupting the company's email service during the business day

Answer: A

A social engineering assessment tests whether people and processes resist manipulation, which gives the client actionable findings on verification gaps. Installing a backdoor exceeds the usual scope and is a different objective. Collecting passwords for leak lists and disrupting service are harmful acts that no authorized assessment would pursue.

6. Do SPF and DKIM help a receiving server check whether a message was authorized by the sending domain?
- A True
 - B False

Answer: A (True)

True. SPF checks that the sending IP is authorized in the domain's DNS record, and DKIM verifies a cryptographic signature on the message. Together with DMARC they let receivers judge whether a claimed sender is legitimate.

7. A scan that checks which TCP ports on a host accept connections is called a _____ scan.

Answer: port (also accepted: TCP port, port scan)

Port scanning identifies open services by testing ports, which is the step after host discovery in network enumeration. Vulnerability scanning is a separate activity that checks services against known weaknesses. The accepted answers cover the common wording of the term.

8. What is a payload in the context of malware analysis?

- A The file-format container that carries a document to a mail server
- B The network address to which a host sends its heartbeat messages
- C The function that a malicious program performs after it has been executed on a system
- D The schedule that determines when an updater checks for new versions and downloads them to every machine

Answer: C

The payload is the part of malware that carries out the intended action, such as data theft, encryption or remote control, once it has run. The container is the tempting distractor because a file format can hold malicious content, but the container is not the action. Network addresses and update schedules are unrelated to the payload concept.

9. Which practice keeps an AI-assisted OSINT workflow ethical and within legal limits?

- A Collecting personal data from private accounts because it is available to the AI through a shared login
- B Limiting collection to public sources within the authorized scope and minimizing personal data stored
- C Feeding every collected record into a public model for faster analysis without reviewing it
- D Building a dossier on every employee's family members to test the social engineering surface

Answer: B

Keeping collection to public sources within scope, and minimizing the personal data retained, respects legal and ethical boundaries that apply to OSINT. Using private accounts is the tempting distractor when access appears easy, but it is unauthorized access. Sending data to public models and profiling family members both create privacy and legal exposure.

10. What does fine-tuning a language model involve?

- A Adding retrieved documents to the prompt at query time without changing the weights, using a vector index of the corpus
- B Lowering the temperature setting so that outputs become more deterministic
- C Splitting the input text into tokens before the model reads it
- D Continuing training on additional examples so that the model's weights are updated for a task

Answer: D

Fine-tuning continues training on task-specific examples so the weights change, which can shape style or behavior for a domain. Retrieval at query time is the tempting distractor because it is a common customization method, but it leaves the weights untouched. Temperature and tokenization are separate settings and steps.