

PRACTICE QUESTIONS

GIAC / SANS

GOAA

GIAC Offensive AI Analyst

SHARED BY [u/Kind-Cluster-8056](#) on aiexamcerts

EDITION Free Set 2

QUESTIONS 10

SHARED October 18, 2026

EXAM GIAC / SANS GOAA, GIAC Offensive AI Analyst

Shared by u/Kind-Cluster-8056 on aiexamcerts

10 practice questions for the GIAC / SANS G0AA 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 G0AA and the question number.

1. Which two statements about AI-assisted malware work in an authorized assessment are accurate? (Choose two.)

- A The engagement rules should define how generated samples are contained, tracked and destroyed
- B A model's refusal to produce code always proves that no malicious code could be written
- C Generated samples can be shared with unrelated third parties once the test is over
- D Sample analysis should be done in an isolated lab rather than on production systems
- E Guardrail refusals are a reliable measure of how secure a model is against all misuse

Answer: A, D

Samples must be governed by the engagement rules, including containment and destruction, and analysis belongs in an isolated lab rather than on production systems. The refusal claim is the tempting distractor because refusals are often treated as proof of safety, but they are not a complete measure. Sharing samples with third parties breaks confidentiality and containment.

2. Does the principle of defense in depth mean that a single control, such as an email filter, is sufficient on its own?

- A True
- B False

Answer: B (False)

False. Defense in depth layers multiple independent controls so that the failure of one does not expose the environment. A single filter is a point of failure, which is why it is combined with authentication, endpoint protection and user training.

3. In the context of web application testing, what is command injection?

- A A flaw where untrusted input is passed to an operating system shell and interpreted as commands
- B A method for loading a browser extension into a page's document object model
- C A certificate error that occurs when the server presents an expired TLS certificate that the browser has already pinned
- D A technique for slowing a site's responses so that users give up on a checkout

Answer: A

Command injection occurs when input is concatenated into a shell command and the operating system executes the injected text. Browser extensions are the tempting distractor because they also run code in the page, but they are not command execution on the server. Certificate errors and deliberate slowdowns are unrelated.

4. Which speech element is essential for a convincing audio deepfake of a specific person?
- A The file format of the audio, which must be lossless WAV and sampled at a studio rate for any model to work
 - B A fixed background image that is shown while the audio is playing
 - C A large, consistent sample of that person's voice recordings, which a model can learn from
 - D The exact number of words in the script, which must match the target's average

Answer: C

Voice cloning depends on enough representative recordings of the target's speech to model timbre, cadence and accent. File format is the tempting distractor because audio quality matters, but it is not what makes the voice convincing. Background images and word counts do not determine voice identity.

5. Pretexting is a social engineering technique in which an attacker creates a fabricated _____ to justify a request for information or access.

Answer: scenario (also accepted: story, pretext, identity)

A pretext is the invented scenario or identity that makes a request seem legitimate to the target. It is distinct from phishing, which is a delivery method, although the two are often combined. The accepted answers cover the common nouns used in training material.

6. Which open-source tool is widely used to run authorized phishing simulations with tracking of clicks and submitted data?
- A Wireshark
 - B GoPhish
 - C Nessus
 - D BloodHound

Answer: B

GoPhish is an open-source framework for building and tracking phishing simulation campaigns. Wireshark is the tempting distractor because it is a common security tool, but it captures and analyzes network packets rather than running campaigns. Nessus is a vulnerability scanner and BloodHound maps Active Directory relationships.

7. What does a vulnerability scanner primarily produce?

- A A new firewall ruleset that blocks every service on the network automatically
- B A list of user passwords extracted from the directory service database for every account in the domain
- C A record of every email message sent by the organization during the day
- D A map of checks run against detected services, with findings matched to known weaknesses

Answer: D

A vulnerability scanner identifies services and version details, checks them against known vulnerability data, and reports matched findings for triage. A firewall ruleset is the tempting distractor because scan results often drive hardening decisions, but the scanner does not write rules itself. Extracting passwords and mail logs are not scanner outputs.

8. Which mechanism describes a malware technique for surviving a reboot?

- A Persistence through registry run keys, scheduled tasks or service entries
- B Compression of the executable to reduce its size on disk
- C Encryption of the file so that antivirus cannot read the file header
- D Propagation through an unpatched service to a neighboring host, which spreads the code across the segment

Answer: A

Persistence means the malware re-establishes itself after restarts, often through autostart locations, scheduled tasks or services. Propagation is the tempting distractor because it is a separate phase in which malware spreads to other hosts, not a way to survive a reboot. Compression and encryption affect storage and detection rather than persistence.

9. Does an effective social engineering awareness program reduce risk by teaching staff to verify unexpected requests through a known channel?

- A True
- B False

Answer: A (True)

True. Verification through a known, separately sourced channel defeats most pretext-based requests, whether they arrive by email, phone or message. Awareness training that reinforces this habit is widely recommended because it addresses the human decision the attacker depends on.

10. Which term describes a fluent answer from a generative AI system that is unsupported by its sources?
- A A refusal produced when a safety classifier blocks a prompt
 - B A timeout caused by sending a request larger than the context window
 - C A confident output that is not supported by the training data or the supplied context
 - D A lower-quality response produced when the temperature setting is set very low and the prompt is very short

Answer: C

A hallucination is fluent, confident content that is not grounded in reliable sources, which is why RAG and verification are used to reduce it. A safety refusal is the tempting distractor because it is also an unexpected output, but it is a deliberate control response. Timeouts and low-temperature outputs have different causes.