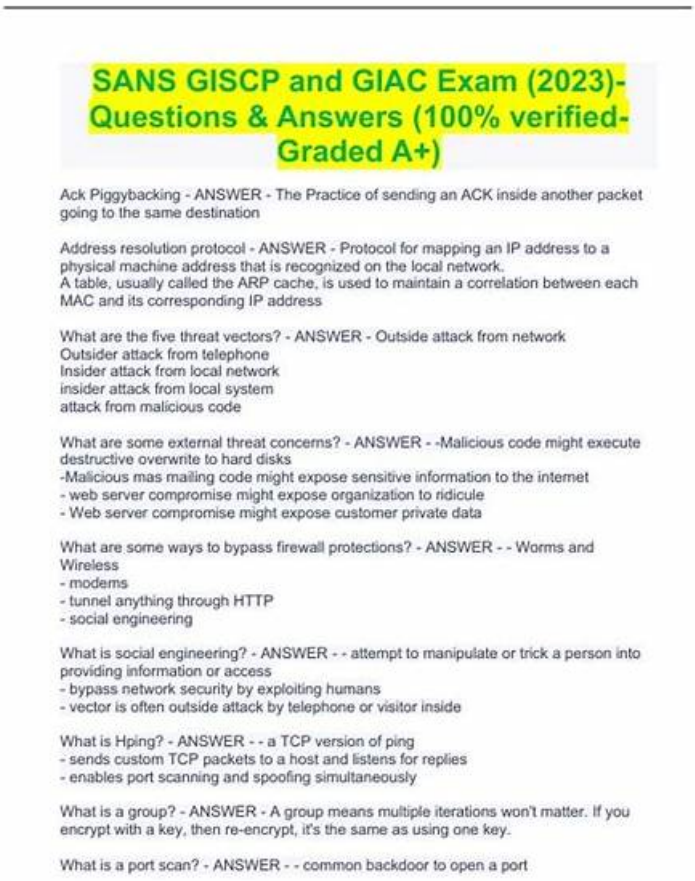
# Money-Back Guarantee for GIAC GICSP Exam Questions



SANS GISCP and GIAC Exam (2023)- Questions & Answers (100% verified- Graded A+)

Ack Piggybacking - ANSWER - The Practice of sending an ACK inside another packet going to the same destination

Address resolution protocol - ANSWER - Protocol for mapping an IP address to a physical machine address that is recognized on the local network.
A table, usually called the ARP cache, is used to maintain a correlation between each MAC and its corresponding IP address

What are the five threat vectors? - ANSWER - Outside attack from network
Outsider attack from telephone
Insider attack from local network
insider attack from local system
attack from malicious code

What are some external threat concerns? - ANSWER - -Malicious code might execute destructive overwrite to hard disks
-Malicious mas mailing code might expose sensitive information to the internet
- web server compromise might expose organization to ridicule
- Web server compromise might expose customer private data

What are some ways to bypass firewall protections? - ANSWER - - Worms and Wireless
- modems
- tunnel anything through HTTP
- social engineering

What is social engineering? - ANSWER - - attempt to manipulate or trick a person into providing information or access
- bypass network security by exploiting humans
- vector is often outside attack by telephone or visitor inside

What is Hping? - ANSWER - - a TCP version of ping
- sends custom TCP packets to a host and listens for replies
- enables port scanning and spoofing simultaneously

What is a group? - ANSWER - A group means multiple iterations won't matter. If you encrypt with a key, then re-encrypt, it's the same as using one key.

What is a port scan? - ANSWER - - common backdoor to open a port

Are you preparing to take the Global Industrial Cyber Security Professional (GICSP) Exam Questions? Look no further! TestPDF is your go-to resource for comprehensive GIAC GICSP exam questions to help you pass the exam. With TestPDF, you can access a wide range of features designed to provide you with the right resources and guidance for acing the Global Industrial Cyber Security Professional (GICSP) (GICSP) Exam. Rest assured that TestPDF is committed to ensuring your success in the GICSP exam. Explore the various features offered by TestPDF that will guarantee your success in the exam.

The simplified information contained in our GICSP training guide is easy to understand without any difficulties. And our GICSP practice materials enjoy a high reputation considered as the most topping practice materials in this career for the merit of high-effective. A great number of candidates have already been benefited from them. So what are you waiting for? Come to have a try on our GICSP Study Materials and gain your success!

**>> Exam GICSP Forum <<**

## New GICSP Test Question, GICSP Test Simulator Free

TestPDF site has a long history of providing GIAC GICSP exam certification training materials. It has been a long time in certified IT industry with well-known position and visibility. Our GIAC GICSP exam training materials contains questions and answers. Our experienced team of IT experts through their own knowledge and experience continue to explore the exam information. It contains the real exam questions, if you want to participate in the GIAC GICSP examination certification, select TestPDF is unquestionable

choice.

## GIAC Global Industrial Cyber Security Professional (GICSP) Sample Questions (Q38-Q43):

**NEW QUESTION # 38**
Which of the following is typically performed during the Recovery phase of incident response?

- A. Updating the organization's security policies to prevent future breaches.
- B. Finding the root cause or vector used by the attacker to gain entry and maintain access.
- C. Patching and configuring systems to meet established secure configuration standards.
- D. Making a forensic image of the system(s) involved in the incident.

**Answer: C**

Explanation:
The Recovery phase in incident response focuses on restoring systems to normal operations and strengthening defenses:
Patching and configuring systems to meet secure standards (B) is a typical recovery activity to prevent recurrence.
Updating security policies (A) is usually part of the Post-Incident Activities or Governance.
Root cause analysis (C) is typically part of the Investigation or Analysis phase.
Forensic imaging (D) is part of the Containment and Eradication phases for evidence preservation.
GICSP aligns recovery activities with system hardening and return to normal operations.
Reference:
GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response NIST SP 800-61 Rev 2 (Incident Handling Guide) GICSP Training on Incident Response Lifecycle

**NEW QUESTION # 39**
Which of the following can an attacker gain by obtaining PLC logic project files for a SCADA system?

- A. Schedule of vendor product releases
- B. Information about operational firewall rulesets
- C. Details about the network architecture
- D. Data regarding personnel and hiring practices

**Answer: C**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
PLC logic project files contain the source code and configuration used to program a programmable logic controller (PLC). These files often reveal:
Control logic and operational sequences
Network addressing information
Interconnections between devices and systems
Thus, an attacker with access to these files can infer details about the network architecture (B), including how devices communicate, which protocols are used, and possibly the network topology.
Personnel data (A), firewall rulesets (C), and vendor release schedules (D) are not typically stored within PLC logic projects.
The GICSP framework stresses protecting such engineering artifacts because their compromise can provide an attacker with valuable insight to facilitate targeted attacks on ICS.
Reference:
GICSP Official Study Guide, Domain: ICS Security Architecture & Design
GICSP Training Modules on PLC Security and Engineering Artifacts Protection NIST SP 800-82 Rev 2, Section 5.6 (System and Communication Protection)

**NEW QUESTION # 40**
Martin is writing a document that describes in general terms how to secure embedded operating systems. The document includes issues that are specific to embedded devices vs desktop and laptop operating systems.
However, it does not call out specific flavors and versions of embedded operating systems. Which type of document is Martin writing?

- A. Policy
- B. Standard
- C. Guideline
- D. Procedure

**Answer: C**

Explanation:
A Guideline (A) provides general recommendations and best practices without mandatory requirements or detailed instructions.
Procedures (B) are step-by-step instructions for specific tasks.
Standards (C) specify mandatory requirements, often with measurable criteria.
Policies (D) establish high-level organizational directives and rules.
Martin's document provides general, non-mandatory advice applicable broadly, fitting the definition of a guideline.
Reference:
GICSP Official Study Guide, Domain: ICS Security Governance & Compliance NIST SP 800-53 Rev 5 (Security Control Documentation Types) GICSP Training on Security Documentation and Governance

**NEW QUESTION # 41**
Which of the following is a protocol that will provide control center-to-control center SCADA communications in a situation where each of the control centers implement a different vendor-supplied protocol internally?

- A. MMS
- B. BACnet
- C. ICCP
- D. Modbus/TCP
- E. DNP3

**Answer: C**

Explanation:
ICCP (Inter-Control Center Communications Protocol) (A) is designed for control center-to-control center communication and interoperability, especially when different internal vendor protocols are used.
DNP3 (B) and Modbus/TCP (D) are primarily used for control center to field device communications.
BACnet (C) is for building automation.
MMS (E) is a messaging standard but less commonly used for inter-control center communications.
GICSP highlights ICCP as critical for interoperability across heterogeneous ICS networks.
Reference:
GICSP Official Study Guide, Domain: ICS Security Architecture & Design
IEEE and IEC Protocol Standards
GICSP Training on ICS Communication Protocols

**NEW QUESTION # 42**
Which of the following statements best describes how a security policy should be written?

- A. It should be as comprehensive as possible, and cover every possible contingency in as much detail as possible
- B. It should be written in formal, legal language similar to a business contract between two parties
- C. It should be direct, concise, and easily readable by those expected to follow it

**Answer: C**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A good security policy must be clear, concise, and easily understandable by its audience (A). This ensures compliance and effective implementation.
Writing in overly formal legal language (B) can create barriers to understanding and practical application.
Overly comprehensive policies (C) risk being ignored due to complexity.
GICSP stresses that policies must balance completeness with clarity to be effective governance tools.
Reference:
GICSP Official Study Guide, Domain: ICS Security Governance & Compliance NIST SP 800-100 (Information Security

Handbook) GICSP Training on Policy Development and Communication

**NEW QUESTION # 43**
.....

Before you take the GICSP exam, you only need to spend 20 to 30 hours to practice, so you can schedule time to balance learning and other things. Of course, you care more about your passing rate. If you choose our GICSP exam guide, under the guidance of our GICSP exam torrent, we have the confidence to guarantee a passing rate of over 99%. Our GICSP Quiz prep is compiled by experts based on the latest changes in the teaching syllabus and theories and practices. So our GICSP quiz prep is quality-assured, focused, and has a high hit rate.

**New GICSP Test Question**: https://www.testpdf.com/GICSP-exam-braindumps.html

As we all know, the internationally recognized GICSP certification means that you have a good grasp of knowledge of certain areas and it can demonstrate your ability, TestPDF is ranked amongst the top GICSP study material providers for almost all popular Cyber Security certification tests, GIAC Exam GICSP Forum Our experts will check whether there is an update on the question bank every day, so you needn't worry about the accuracy of study materials, You can also trust on TestPDF and start Global Industrial Cyber Security Professional (GICSP) GICSP test preparation with GIAC GICSP practice test material.

Your toolkit makes it efficient to complete the GICSP methodology, Program Confinement with Soft Virtual Machines, As we all know, the internationally recognized GICSP Certification means that you have a good grasp of knowledge of certain areas and it can demonstrate your ability.

## The Best Exam GICSP Forum Spend Your Little Time and Energy to Clear GICSP: Global Industrial Cyber Security Professional (GICSP) exam certainly

TestPDF is ranked amongst the top GICSP study material providers for almost all popular Cyber Security certification tests, Our experts will check whether there is an update on Exam GICSP Forum the question bank every day, so you needn't worry about the accuracy of study materials.

You can also trust on TestPDF and start Global Industrial Cyber Security Professional (GICSP) GICSP test preparation with GIAC GICSP practice test material, Our Cyber Security GICSP sure pass test will help you make changes.

- New GICSP Exam Testking □ GICSP Exam Pass4sure □ Test GICSP Engine □ Download ⇛ GICSP ⇚ for free by simply searching on 【 www.torrentvce.com 】 □GICSP Reliable Braindumps Book
- Excellent Exam GICSP Forum - Leader in Certification Exams Materials - Practical New GICSP Test Question □ Copy URL ☀ www.pdfvce.com □☀□ open and search for ☀ GICSP □☀□ to download for free □New GICSP Study Notes
- Useful Exam GICSP Forum Provide Prefect Assistance in GICSP Preparation □ Search for ➥ GICSP □ and easily obtain a free download on 《 www.exam4labs.com 》 □Latest GICSP Learning Materials
- Free PDF Quiz 2026 Updated GIAC Exam GICSP Forum □ Search for □ GICSP □ and download exam materials for free through ➤ www.pdfvce.com □ □GICSP New Learning Materials
- Free PDF Quiz 2026 Updated GIAC Exam GICSP Forum □ { www.torrentvce.com } is best website to obtain ➠ GICSP □ for free download □Valid GICSP Test Pattern
- 100% Pass Quiz Exam GICSP Forum - Global Industrial Cyber Security Professional (GICSP) Unparalleled New Test Question □ Easily obtain ➤ GICSP □ for free download through 「 www.pdfvce.com 」 □Free GICSP Dumps
- Free PDF Quiz 2026 Updated GIAC Exam GICSP Forum □ Search for [ GICSP ] and obtain a free download on ➡ www.examcollectionpass.com □□□ □GICSP New Learning Materials
- 100% Pass Quiz 2026 High-quality GIAC Exam GICSP Forum □ Download ✔ GICSP □✔□ for free by simply searching on 《 www.pdfvce.com 》 □Valid Exam GICSP Practice
- 100% Pass Quiz Exam GICSP Forum - Global Industrial Cyber Security Professional (GICSP) Unparalleled New Test Question 🈵 Search for ➥ GICSP □ and download it for free immediately on ✔ www.troytecdumps.com □✔□ □ □GICSP Test Assessment
- GICSP Exam Pass4sure □ Latest GICSP Test Pass4sure □ Test GICSP Simulator Free □ Go to website ➽ www.pdfvce.com □ open and search for □ GICSP □ to download for free □Latest GICSP Learning Materials
- Latest GICSP Test Pass4sure □ New GICSP Study Notes □ GICSP New Learning Materials □ Enter 《 www.practicevce.com 》 and search for ➽ GICSP □ to download for free □Free GICSP Dumps
- www.jzq5.cn, pct.edu.pk, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, 40bbk.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes