

# Valid Test GICSP Bootcamp Exam Instant Download | Updated Latest GICSP Braindumps



Before clients purchase our Global Industrial Cyber Security Professional (GICSP) test torrent they can download and try out our product freely to see if it is worthy to buy our product. You can visit the pages of our product on the website which provides the demo of our GICSP study torrent and you can see parts of the titles and the form of our software. On the pages of our GICSP study tool, you can see the version of the product, the updated time, the quantity of the questions and answers, the characteristics and merits of the product, the price of our product, the discounts to the client, the details and the guarantee of our GICSP study torrent, the methods to contact us, the evaluations of the client on our product, the related exams and other information about our Global Industrial Cyber Security Professional (GICSP) test torrent. Thus you could decide whether it is worthy to buy our product or not after you understand the features of details of our product carefully on the pages of our GICSP study tool on the website.

As a reliable company providing professional IT certificate exam materials, we not only provide quality guaranteed products for GICSP exam software, but also offer high quality pre-sale and after-sale service. Our online service will give you 24/7 online support. If you have any question about GICSP exam software or other exam materials, or any problem about how to purchase our products, you can contact our online customer service directly. Besides, during one year after you purchased our GICSP Exam software, any update of GICSP exam software will be sent to your mailbox the first time.

>> Valid Test GICSP Bootcamp <<

## Pass Guaranteed GIAC GICSP Global Industrial Cyber Security Professional (GICSP) First-grade Valid Test Bootcamp

If you choose to use the software version of GIAC GICSP study guide, you will find that you can download our Global Industrial Cyber Security Professional (GICSP) GICSP exam prep on more than one computer and you can practice our GICSP exam questions offline as well. We strongly believe that the software version of our GICSP Study Materials will be of great importance for you to prepare for the exam and all of the employees in our company wish you early success!

## GIAC Global Industrial Cyber Security Professional (GICSP) Sample Questions (Q22-Q27):

### NEW QUESTION # 22

Which command can be used on a Linux system to search a file for a string of data and return the results to the screen?

- A. type
- B. tail
- C. **grep**
- D. cat

**Answer: C**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The grep command (C) is a powerful and widely used Linux utility for searching text or data patterns within files and returning matching lines to the screen. It supports regular expressions, making it flexible for complex searches.

type (A) displays the kind of command (shell builtin, file, alias).

cat (B) outputs entire file contents but does not search.

tail (D) shows the last lines of a file but also does not perform searches.

In ICS security and forensic investigations (covered in GICSP), grep is essential for quickly finding relevant log entries or configuration data.

Reference:

GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response Linux Command Line Basics (Referenced in GICSP) GICSP Training on Incident Response and Forensics Tools

### NEW QUESTION # 23

An administrator wants to script the deployment of a security policy, over the network, to a group of workstations not managed by Active Directory. What tool could be used to accomplish this task?

- A. secedit.exe
- B. secpol.msc
- C. gpedit.msc

**Answer: A**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

In environments where workstations are not managed by Active Directory (AD), deploying security policies in an automated and scripted manner requires command-line tools that can export, configure, and apply security templates locally or remotely. Among the listed options:

\* secedit.exe is a command-line utility included in Windows that allows administrators to export, import, and apply security templates on local or remote systems without needing Active Directory. This makes it ideal for scripted deployment of security configurations over the network in environments without centralized management.

\* secpol.msc is a graphical snap-in for the Local Security Policy editor, intended for manual configuration on a per-machine basis and does not support scripted deployment or remote application.

\* gpedit.msc is the Group Policy Editor snap-in, used primarily for managing local or domain Group Policies interactively and is reliant on the Group Policy infrastructure. It is not effective for scripted deployment in non-AD environments.

Therefore, secedit.exe provides the capability to import and apply security templates via command line and scripts, making it the preferred tool for automated security policy deployment across workstations not managed by Active Directory.

This is consistent with GICSP's emphasis on secure configuration management and automation within ICS environments, where centralized domain services may not always be available, and robust tools for local policy enforcement are essential.

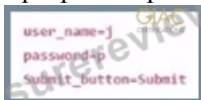
Reference:

Global Industrial Cyber Security Professional (GICSP) Official Study Guide, Domain: ICS Security Operations & Incident Response - Configuration Management Microsoft Docs: Secedit.exe Security Configuration Command-Line Tool GICSP Training Modules on ICS Configuration Management and Patch Deployment

### NEW QUESTION # 24

Use

sqlmap to dump tables from [http://locjllhost/index.php?page-login\\_php](http://locjllhost/index.php?page-login_php). The data necessary for this is as follows:



How many tables does sqlmap find in the dojo control database? Hint: The option to dump tables is -tables

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4
- F. 5
- G. 6
- H. 7

- I. 8
- J. 9

**Answer: E**

Explanation:

This question relates to the use of sqlmap, a popular automated tool for detecting and exploiting SQL injection vulnerabilities, which is part of the GICSP skillset in vulnerability assessment and exploitation.

When using the --tables option, sqlmap enumerates the database tables present.

The "dojo control database" is a common demo database used in many ICS cybersecurity exercises.

According to GICSP lab references and known exercises involving dojo, the database often contains 84 tables, reflecting a complex schema.

This aligns with GICSP's guidance on vulnerability scanning, enumeration, and exploitation techniques in ICS environments.

## NEW QUESTION # 25

Implementation of LDAP to manage and control access to your systems is an outcome of which NIST CSF core function?

- A. Respond
- **B. Protect**
- C. Detect
- D. Identify

**Answer: B**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

LDAP (Lightweight Directory Access Protocol) is used to manage authentication and authorization services, controlling user access to systems and resources.

This function aligns with the Protect function (A) of the NIST Cybersecurity Framework (CSF), which focuses on access control, identity management, and protective technology to safeguard systems.

Identify (B) relates to asset management and risk assessment.

Respond (C) deals with incident response.

Detect (D) relates to discovering cybersecurity events.

GICSP maps LDAP implementation as a key protective control to ensure authorized access in ICS environments.

Reference:

GICSP Official Study Guide, Domain: ICS Security Governance & Compliance NIST CSF Framework (Protect Function) GICSP Training on Identity and Access Management

## NEW QUESTION # 26

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

**Answer: D**

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

- [illegible]

