



GCCCC^{Q&As}

GCCC - GIAC Critical Controls Certification (GCCC)

Pass GIAC GCCC Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/gcccc.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

During a security audit which test should result in a source packet failing to reach its intended destination?

- A. A new connection request from the Internet is sent to a host on the company \\s internal net work
- B. A packet originating from the company\\s DMZ is sent to a host on the company\\s internal network
- C. A new connection request from the internet is sent to the company\\s DNS server
- D. A packet originating from the company\\s internal network is sent to the company\\s DNS server

Correct Answer: A

QUESTION 2

An organization has implemented a control for Controlled Use of Administrative Privilege. The control requires users to enter a password from their own user account before being allowed elevated privileges, and that no client applications (e.g. web browsers, e-mail clients) can be run with elevated privileges. Which of the following actions will validate this control is implemented properly?

- A. Check the log entries to match privilege use with access from authorized users.
- B. Run a script at intervals to identify processes running with administrative privilege.
- C. Force the root account to only be accessible from the system console.

Correct Answer: B

QUESTION 3

Which of the following assigns a number indicating the severity of a discovered software vulnerability?

- A. CPE
- B. CVE
- C. CCE
- D. CVSS

Correct Answer: D

QUESTION 4

A security incident investigation identified the following modified version of a legitimate system file on a compromised client:

C:\Windows\System32\winxml.dll Addition Jan. 16, 2014 4:53:11 PM



The infection vector was determined to be a vulnerable browser plug-in installed by the user. Which of the organization's CIS Controls failed?

- A. Application Software Security
- B. Inventory and Control of Software Assets
- C. Maintenance, Monitoring, and Analysis of Audit Logs
- D. Inventory and Control of Hardware Assets

Correct Answer: B

QUESTION 5

Review the below results of an audit on a server. Based on these results, which document would you recommend be reviewed for training or updates?

```
Output
Target Passwords Tuning Specific Start
Output:
Hydra v2.9 (c)2013 by van Hauser/THC & David Meeblek - For legal purposes only
Hydra (http://www.thc.org/thc-hydra) starting at 2014-04-22 17:04:21
[WARNING] Restorefile (c:\hydra.restore) from a previous session found, to prevent overwriting, you have 10 se
[DATA] 5 tasks, 1 server, 48 login tries (16/pw), 3 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host 192.168.80.151 login: dave password: Spring2014
[22][ssh] host 192.168.80.151 login: sandy password: Fall2013
[22][ssh] host 192.168.80.151 login: ted password: Spring2014
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-04-22 17:04:47
$finished$

Start Stop Save Output Clear Output
hydra -s 22 -L /root/daemon.txt -P /root/daemon.txt -t 1 192.168.80.151 ssh
```

- A. Procedure for authorizing remote server access
- B. Procedure for modifying file permissions
- C. Procedure for adjusting network share permissions
- D. Procedure for setting and resetting user passwords

Correct Answer: D