



Vendor: GIAC

Exam Code: GCCC

Exam Name: GIAC Critical Controls Certification

Version: DEMO

QUESTION 1

Which of the following CIS Controls is used to manage the security lifecycle by validating that the documented controls are in place?

- A. Controlled Use of Administrative Privilege
- B. Account Monitoring and Control
- C. Data Protection
- D. Penetration Tests and Red Team Exercises

Answer: D

QUESTION 2

When evaluating the Wireless Access Control CIS Control, which of the following systems needs to be tested?

- A. Log management system
- B. 802.1x authentication systems
- C. Data classification and access baselines
- D. PII data scanner

Answer: B

QUESTION 3

As part of an effort to implement a control on E-mail and Web Protections, an organization is monitoring their webserver traffic. Which event should they receive an alert on?

- A. The number of website hits is higher than the daily average
- B. The logfiles of the webserver are rotated and archived
- C. The website does not respond to a SYN packet for 30 minutes
- D. The website issues a RST to a client after the connection is idle

Answer: C

QUESTION 4

Which of the following items would be used reactively for incident response?

- A. A schedule for creating and storing backup
- B. A phone tree used to contact necessary personnel
- C. A script used to verify patches are installed on systems
- D. An IPS rule that prevents web access from international locations

Answer: B

QUESTION 5

Below is a screenshot from a deployed next-generation firewall. These configuration settings would be a defensive measure for which CIS Control?

URI List Configuration

Allowed URI List:	None
Forbidden URI List:	None
URI List Searching Order:	Allowed URI List First
Operation for Forbidden URI List:	Block

Category Configuration

#. Category	Operation
11. Gambling	Block
12. Alcohol/Tobacco	Block
13. Chat/Instant Messaging (IM)	Allow
14. Arts/Entertainment	Block
15. Business and Economy	Allow

- A. Controlled Access Based on the Need to Know
- B. Limitation and Control of Network Ports, Protocols and Services
- C. Email and Web Browser Protections
- D. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches.

Answer: C

QUESTION 6

What is a recommended defense for the CIS Control for Application Software Security?

- A. Keep debugging code in production web applications for quick troubleshooting
- B. Limit access to the web application production environment to just the developers
- C. Run a dedicated vulnerability scanner against backend databases
- D. Display system error messages for only non-kernel related events

Answer: C

QUESTION 7

How does an organization's hardware inventory support the control for secure configurations?

- A. It provides a list of managed devices that should be secured
- B. It provides a list of unauthorized devices on the network
- C. It provides the MAC addresses for insecure network adapters

D. It identifies the life cycle of manufacturer support for hardware devices

Answer: A

QUESTION 8

Which of the following is a reliable way to test backed up data?

- A. Verify the file size of the backup
- B. Confirm the backup service is running at the proper time
- C. Compare data hashes of backed up data to original systems
- D. Restore the data to a system

Answer: D

QUESTION 9

As part of a scheduled network discovery scan, what function should the automated scanning tool perform?

- A. Uninstall listening services that have not been used since the last scheduled scan
- B. Compare discovered ports and services to a known baseline to report deviations
- C. Alert the incident response team on ports and services added since the last scan
- D. Automatically close ports and services not included in the current baseline

Answer: B

QUESTION 10

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?



```
Quit
Target Passwords Tuning Specifics Start
Output:
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - For legal purposes only
Hydra (http://www.thc.org/thc-hydra) starting at 2014-04-22 17:04:21
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 se
[DATA] 5 tasks, 1 server, 18 login tries (l:b/p:l), ~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: Fat12013
[22][ssh] host 192.168.80.151 login: ted password: Spring2014
1 of 1 target successfully completed, 3 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-04-22 17:04:47
xfinishedx
Start Stop Save Output Clear Output
hydra -e 22 -L /root/dossier.txt -P /root/dates.txt -t 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

Answer: D

QUESTION 11

How can the results of automated network configuration scans be used to improve the security of the network?

- A. Reports can be sent to the CIO for performance benchmarks
- B. Results can be provided to network engineers as actionable feedback
- C. Scanners can correct network configurations issues
- D. Results can be included in audit evidence failures

Answer: B

QUESTION 12

An organization wants to test its procedure for data recovery. Which of the following will be most effective?

- A. Verifying a file can be recovered from backup media
- B. Verifying that backup process is running when it should
- C. Verifying that network backups can't be read in transit
- D. Verifying there are no errors in the backup server logs

Answer: A

QUESTION 13

What is the business goal of the Inventory and Control of Software Assets Control?

- A. Only authorized software should be installed on the agency's computer systems
- B. All software conforms to licensing requirements for the business
- C. Accurate software versions are captured to enable patching
- D. Accurate software versions and counts are documented for licensing updates

Answer: A

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14