GCCC 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/gccc.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

Correct Answer: A

QUESTION 2

An attacker is able to successfully access a web application as root using ` or 1 = 1 . as the password. The successful access indicates a failure of what process?

A. Input Validation

B. Output Sanitization

C. URL Encoding

D. Account Management

Correct Answer: A

QUESTION 3

An auditor is focusing on potential vulnerabilities. Which of the following should cause an alert?

A. Workstation on which a domain admin has never logged in

B. Windows host with an uptime of 382 days

C. Server that has zero browser plug-ins

D. Fully patched guest machine that is not in the asset inventory

Correct Answer: B

QUESTION 4

What is a zero-day attack?

A. An attack that has a known attack signature but no available patch

B. An attack that utilizes a vulnerability unknown to the software developer

C. An attack that deploys at the end of a countdown sequence

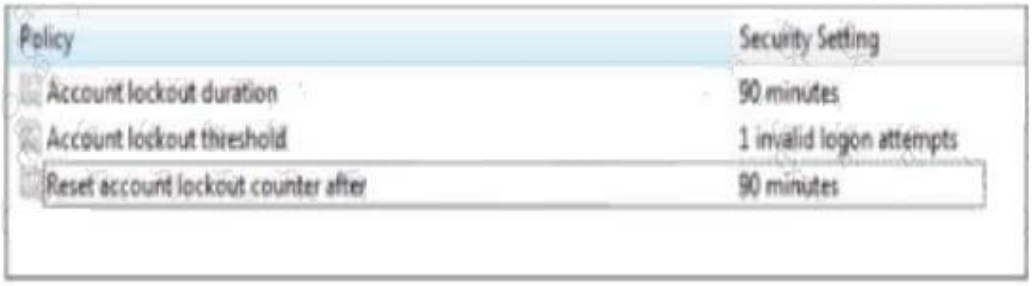
D. An attack that is launched the day the patch is released

Correct Answer: B

QUESTION 5

An organization is implementing a control for the Account Monitoring and Control CIS Control, and have set the Account Lockout Policy as shown below. What is the risk presented by these settings?

(Image)



A. Brute-force password attacks could be more effective.

B. Legitimate users could be unable to access resources.

C. Password length and complexity will be automatically reduced.

D. Once accounts are locked, they cannot be unlocked.

Correct Answer: B

QUESTION 6

Which of the options below will do the most to reduce an organization\\'s attack surface on the internet?

A. Deploy an access control list on the perimeter router and limit inbound ICMP messages to echo requests only

B. Deploy antivirus software on internet-facing hosts, and ensure that the signatures are updated regularly

C. Ensure that rotation of duties is used with employees in order to compartmentalize the most important tasks

D. Ensure only necessary services are running on Internet-facing hosts, and that they are hardened according to best practices

Correct Answer: D

QUESTION 7

Which of the following actions will assist an organization specifically with implementing web application software security?

A. Making sure that all hosts are patched during regularly scheduled maintenance

B. Providing end-user security training to both internal staff and vendors

C. Establishing network activity baselines among public-facing servers

D. Having a plan to scan vulnerabilities of an application prior to deployment

Correct Answer: D

QUESTION 8

According to attack lifecycle models, what is the attacker\\'s first step in compromising an organization?

A. Privilege Escalation

B. Exploitation

C. Initial Compromise

D. Reconnaissance

Correct Answer: D

QUESTION 9

Executive management approved the storage of sensitive data on smartphones and tablets as long as they were encrypted. Later a vulnerability was announced at an information security conference that allowed attackers to bypass the device\\'s authentication process, making the data accessible. The smartphone manufacturer said it would take six months for the vulnerability to be fixed and distributed through the cellular carriers. Four months after the vulnerability was announced, an employee lost his tablet and the sensitive information became public.

What was the failure that led to the information being lost?

A. There was no risk acceptance review after the risk changed

B. The employees failed to maintain their devices at the most current software version

C. Vulnerability scans were not done to identify the devices that we at risk

D. Management had not insured against the possibility of the information being lost

Correct Answer: A

QUESTION 10

A breach was discovered after several customers reported fraudulent charges on their accounts. The attacker had exported customer logins and cracked passwords that were hashed but not salted. Customers were made to reset their passwords.

Shortly after the systems were cleaned and restored to service, it was discovered that a compromised system administrator\\'s account was being used to give the attacker continued access to the network. Which CIS Control failed in the continued access to the network?

A. Maintenance, Monitoring, and Analysis of Audit Logs

B. Controlled Use of Administrative Privilege

C. Incident Response and Management

D. Account Monitoring and Control

Correct Answer: C

QUESTION 11

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

Correct Answer: C

QUESTION 12

A need has been identified to organize and control access to different classifications of information stored on a fileserver. Which of the following approaches will meet this need?

A. Organize files according to the user that created them and allow the user to determine permissions

B. Divide the documents into confidential, internal, and public folders, and ser permissions on each folder

C. Set user roles by job or position, and create permission by role for each file

D. Divide the documents by department and set permissions on each departmental folder

Correct Answer: B

QUESTION 13

What documentation should be gathered and reviewed for evaluating an Incident Response program?

A. Staff member interviews

B. NIST Cybersecurity Framework

C. Policy and Procedures

D. Results from security training assessments

Correct Answer: C

QUESTION 14

Which of the following actions produced the output seen below?

```
C3PO:Documents student$ diff firewallrules.txt firewallrules2.txt

< access-list inbound permit tcp 8.8.0.0 0.0.0.255 10.10.12.252 eq 8080
---
> access-list inbound permit tcp 8.8.0.0 0.0.0.255 10.10.12.252 eq 8080
> access-list inbound permit tcp host 209.7.159.53 any 3389
```

A. An access rule was removed from firewallrules.txt

B. An access rule was added to firewallrules2.txt

C. An access rule was added to firewallrules.txt

D. An access rule was removed from firewallrules2.txt

Correct Answer: B

QUESTION 15

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

Correct Answer: B