GIAC

Exam Questions GCCC

GIAC Critical Controls Certification (GCCC)

NEW QUESTION 1
Why is it important to enable event log storage on a system immediately after it is installed?

A. To allow system to be restored to a known good state if it is compromised
B. To create the ability to separate abnormal behavior from normal behavior during an incident
C. To compare it performance with other systems already on the network
D. To identify root kits included on the system out of the box

Answer: B

NEW QUESTION 2
Janice is auditing the perimeter of the network at Sugar Water InC. According to documentation, external SMTP traffic is only allowed to and from 10.10.10.25. Which of the following actions would demonstrate the rules are configured incorrectly?

A. Receive spam from a known bad domain
B. Receive mail at Sugar Water In
C. account using Outlook as a mail client
D. Successfully deliver mail from another host inside the network directly to an external contact
E. Successfully deliver mail from web client using another host inside the network to an external contact.

Answer: C

NEW QUESTION 3
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

Answer: C

NEW QUESTION 4
Dragonfly Industries requires firewall rules to go through a change management system before they are configured. Review the change management log. Which of the following lines in your firewall ruleset has expired and should be removed from the configuration?

Line	Date	Port	Internal Host(s)	External Host(s)	In/Out/Both	Length rule is needed	Reason
1	1/15/2013	22	8.8.207.97	10.10.12.100	in	6 weeks	software set-up
2	5/12/2013	25	10.1.1.7	any	out	indefinite	marketing mail delivery
3	6/17/2013	8080	10.10.12.252	8.8.0.0/24	in	indefinite	network backup transfers
4	10/21/2013	80	any	74.125.228.2	out	indefinite	prevent video browsing
5	4/4/2014	443	10.10.12.17	any	in	indefinite	enable secure access

A. access-list outbound permit tcp host 10.1.1.7 any eq smtp
B. access-list outbound deny tcp any host 74.125.228.2 eq www
C. access-list inbound permit tcp 8.8.0.0 0.0.0.255 10.10.12.252 eq 8080
D. access-list inbound permit tcp host 8.8.207.97 host 10.10.12.100 eq ssh

Answer: D

NEW 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)

Policy	Security Setting
Account lockout duration	90 minutes
Account lockout threshold	1 invalid logon attempts
Reset account lockout counter after	90 minutes

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.

Answer: B

NEW QUESTION 6
Acme Corporation is doing a core evaluation of its centralized logging capabilities. Which of the following scenarios indicates a failure in more than one CIS Control?

A. The loghost is missing logs from 3 servers in the inventory
B. The loghost is receiving logs from hosts with different timezone values
C. The loghost time is out-of-sync with an external host
D. The loghost is receiving out-of-sync logs from undocumented servers

Answer: D

NEW QUESTION 7
Which approach is recommended by the CIS Controls for performing penetration tests?

A. Document a single vulnerability per system
B. Utilize a single attack vector at a time
C. Complete intrusive tests on test systems
D. Execute all tests during network maintenance windows

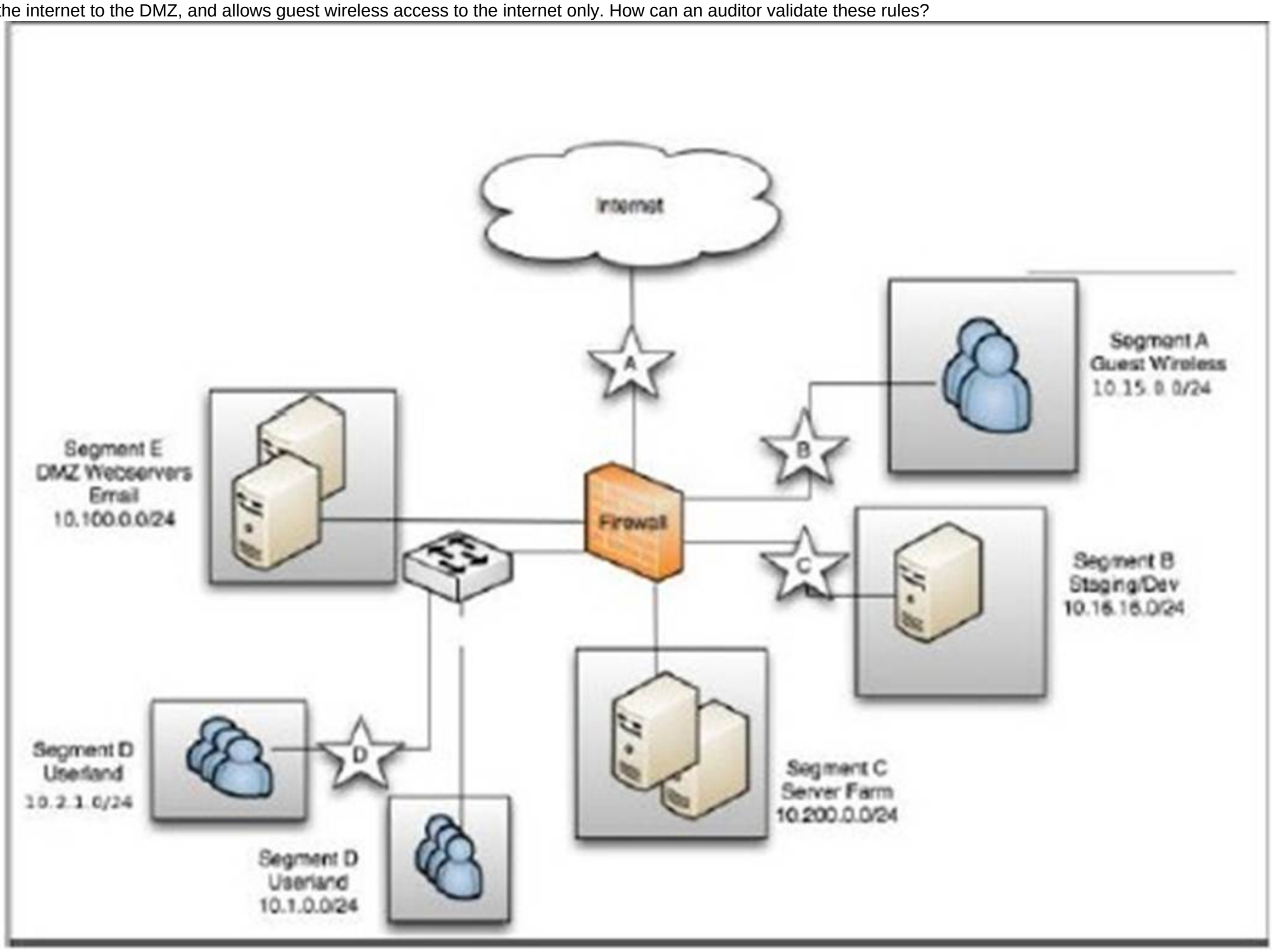
Answer: C

NEW QUESTION 8
Which of the following is used to prevent spoofing of e-mail addresses?

A. Sender Policy Framework
B. DNS Security Extensions
C. Public-Key Cryptography
D. Simple Mail Transfer Protocol

Answer: A

NEW QUESTION 9
An organization has installed a firewall for Boundary Defense. It allows only outbound traffic from internal workstations for web and SSH, allows connections from the internet to the DMZ, and allows guest wireless access to the internet only. How can an auditor validate these rules?



A. Check for packets going from the Internet to the Web server
B. Try to send email from a wireless guest account
C. Check for packages going from the web server to the user workstations
D. Try to access the internal network from the wireless router

Answer: D

NEW QUESTION 10
John is implementing a commercial backup solution for his organization. Which of the following steps should be on the configuration checklist?

A. Enable encryption if it ??s not enabled by default
B. Disable software-level encryption to increase speed of transfer
C. Develop a unique encryption scheme

Answer: A

NEW QUESTION 10
If an attacker wanted to dump hashes or run wmic commands on a target machine, which of the following tools would he use?

A. Mimikatz
B. OpenVAS
C. Metasploit

Answer: C

NEW QUESTION 11
An organization has implemented a control for Controlled Use of Administrative Privileges. They are collecting audit data for each login, logout, and location for the root account of their MySQL server, but they are unable to attribute each of these logins to a specific user. What action can they take to rectify this?

A. Force the root account to only be accessible from the system console.
B. Turn on SELinux and user process accounting for the MySQL server.
C. Force user accounts to use ??sudo?? f or privileged use.
D. Blacklist client applications from being run in privileged mode.

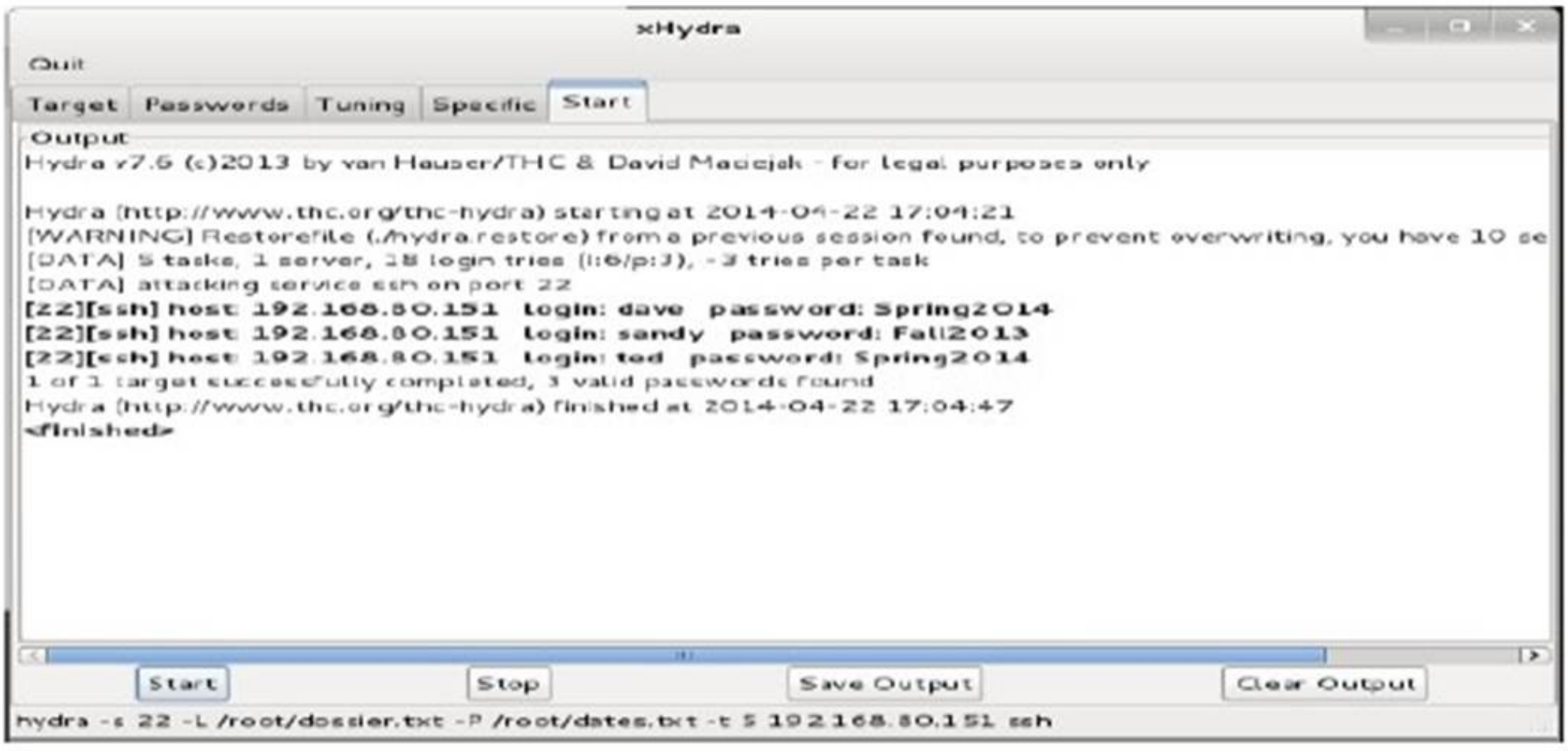
Answer: C

NEW QUESTION 16
Which of the following best describes the CIS Controls?

A. Technical, administrative, and policy controls based on research provided by the SANS Institute
B. Technical controls designed to provide protection from the most damaging attacks based on current threat data
C. Technical controls designed to augment the NIST 800 series
D. Technical, administrative, and policy controls based on current regulations and security best practices

Answer: B

NEW QUESTION 21
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?



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

NEW QUESTION 22
Which of the following archiving methods would maximize log integrity?

A. DVD-R
B. USB flash drive
C. Magnetic Tape
D. CD-RW

Answer: A

NEW QUESTION 24
An organization is implementing a control within the Application Software Security CIS Control. How can they best protect against injection attacks against their custom web application and database applications?

A. Ensure the web application server logs are going to a central log host
B. Filter input to only allow safe characters and strings
C. Configure the web server to use Unicode characters only
D. Check user input against a list of reserved database terms

Answer: B

NEW QUESTION 29
John a network administrator at Northeast High School. Faculty have been complaining that although they can detect and authenticate to the faculty wireless network, they are unable to connect. While troubleshooting, John discovers that the wireless network server is out of DHCP addresses due to a large number of unauthorized student devices connecting to the network. Which course of action would be an effective temporary stopgap to secure the network until a permanent solution can be found?

A. Limit access to allowed MAC addresses
B. Increase the size of the DHCP pool
C. Change the password immediately
D. Shorten the DHCP lease time

Answer: C

NEW QUESTION 31
Which of the following is necessary to automate a control for Inventory and Control of Hardware Assets?

A. A method of device scanning
B. A centralized time server
C. An up-to-date hardening guide
D. An inventory of unauthorized assets

Answer: A

NEW QUESTION 35
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

Answer: D

NEW QUESTION 36
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

Answer: B

NEW QUESTION 41
An organization is implementing a control for the Limitation and Control of Network Ports,
Protocols, and Services CIS Control. Which action should they take when they discover that an application running on a web server is no longer needed?

A. Uninstall the application providing the service
B. Turn the service off in the host configuration files
C. Block the protocol for the unneeded service at the firewall
D. Create an access list on the router to filter traffic to the host

Answer: A

NEW QUESTION 45
Given the audit finding below, which CIS Control was being measured?

- 58% percent of system assets do not require multi-factor authentication for elevated account access
- 9% percent of system assets do not enforce encrypted channels for elevated account activity

A. Controlled Access Based on the Need to Know
B. Controlled Use of Administrative Privilege
C. Limitation and Control of Network Ports, Protocols and Services
D. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
E. Inventory and Control of Hardware Assets

Answer: B

NEW QUESTION 47
Which of the following is necessary for implementing and automating the Continuous Vulnerability Assessment and Remediation CIS Control?

A. Software Whitelisting System
B. System Configuration Enforcement System
C. Patch Management System
D. Penetration Testing System

Answer: C

NEW QUESTION 49
What is the first step suggested before implementing any single CIS Control?

A. Develop an effectiveness test
B. Perform a gap analysis
C. Perform a vulnerability scan
D. Develop a roll-out schedule

Answer: B

NEW QUESTION 52
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

NEW QUESTION 53
An organization has failed a test for compliance with a policy of continual detection and removal of malicious software on its network. Which of the following errors is the root cause?

A. A host ran malicious software that exploited a vulnerability for which there was no patch
B. The security console alerted when a host anti-virus ran whitelisted software
C. The intrusion prevention system failed to update to the newest signature list
D. A newly discovered vulnerability was not detected by the intrusion detection system

Answer: C

NEW QUESTION 55
An organization has created a policy that allows software from an approved list of applications to be installed on workstations. Programs not on the list should not be installed. How can the organization best monitor compliance with the policy?

A. Performing regular port scans of workstations on the network
B. Auditing Active Directory and alerting when new accounts are created
C. Creating an IDS signature to alert based on unknown ??User-Agent ?? strings
D. Comparing system snapshots and alerting when changes are made

Answer: C

NEW QUESTION 56
Which of the following is a requirement in order to implement the principle of least privilege?

A. Mandatory Access Control (MAC)
B. Data normalization
C. Data classification
D. Discretionary Access Control (DAC)

Answer: C

NEW QUESTION 59
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

Answer: A

NEW QUESTION 64
Which of the following is a benefit of stress-testing a network?

A. To determine device behavior in a DoS condition.
B. To determine bandwidth needs for the network.
C. To determine the connectivity of the network
D. To determine the security configurations of the network

Answer: A

NEW QUESTION 66
The settings in the screenshot would be configured as part of which CIS Control?

A. Application Software Security
B. Inventory and Control of Hardware Assets
C. Account Monitoring and Control
D. Controlled Use of Administrative Privileges

Answer: B

NEW QUESTION 69
Acme Corporation performed an investigation of its centralized logging capabilities. It found that the central server is missing several types of logs from three servers in Acme's inventory. Given these findings, what is the most appropriate next step?

A. Define processes to manually review logs for the problem servers
B. Restart or reinstall the logging service on each of the problem servers
C. Perform analysis to identify the source of the logging problems
D. Document the missing logs in the core evaluation report as a minor issue

Answer: C

NEW QUESTION 70
An organization has implemented a policy to continually detect and remove malware from its network. Which of the following is a detective control needed for this?

A. Host-based firewall sends alerts when packets are sent to a closed port
B. Network Intrusion Prevention sends alerts when RST packets are received
C. Network Intrusion Detection devices sends alerts when signatures are updated
D. Host-based anti-virus sends alerts to a central security console

Answer: D

NEW QUESTION 73
To effectively implement the Data Protection CIS Control, which task needs to be implemented first?

A. The organization??s proprietary data needs to be encrypted

B. Employees need to be notified that proprietary data should be protected
C. The organization??s proprietary data needs to be identified
D. Appropriate file content matching needs to be configured

Answer: C

NEW QUESTION 76
An Internet retailer's database was recently exploited by a foreign criminal organization via a remote attack. The initial exploit resulted in immediate root-level access. What could have been done to prevent this level of access being given to the intruder upon successful exploitation?

A. Configure the DMZ firewall to block unnecessary service
B. Install host integrity monitoring software
C. Install updated anti-virus software
D. Configure the database to run with lower privileges

Answer: D

NEW QUESTION 79
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

NEW QUESTION 81
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

GCCC Practice Exam Features:

* GCCC Questions and Answers Updated Frequently

* GCCC Practice Questions Verified by Expert Senior Certified Staff

* GCCC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* GCCC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year