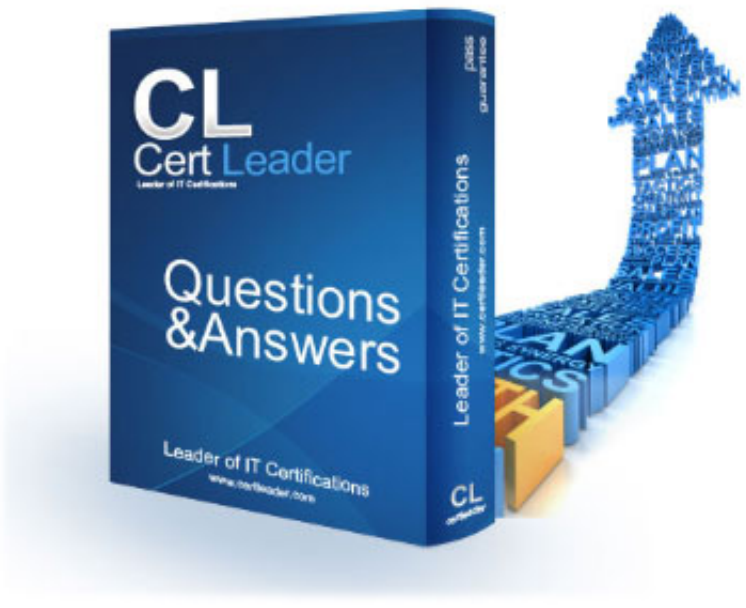
GCCC Dumps

GIAC Critical Controls Certification (GCCC)

https://www.certleader.com/GCCC-dumps.html



NEW QUESTION 1
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 2
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

Answer: B

NEW QUESTION 3
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 4
Which CIS Control includes storing system images on a hardened server, scanning production systems for out-of-date software, and using file integrity assessment tools like tripwire?

A. Inventory of Authorized and Unauthorized Software
B. Continuous Vulnerability Management
C. Secure Configurations for Network Devices such as Firewalls, Routers and Switches
D. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

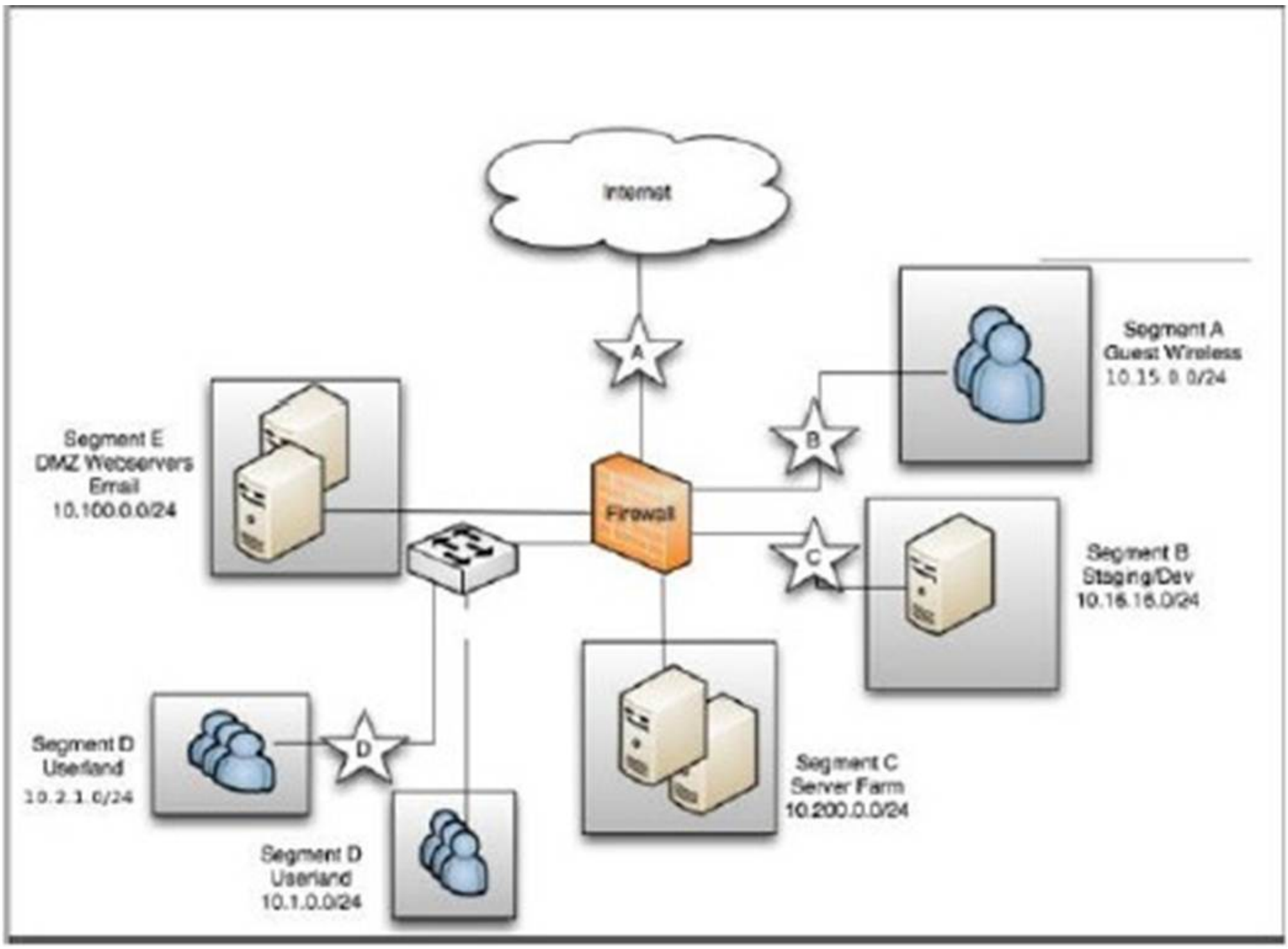
Answer: D

NEW QUESTION 5
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 6
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 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

Answer: D

NEW QUESTION 8
An organization is implementing an application software security control their custom- written code that provides web—based database access to sales partners. Which action will help mitigate the risk of the application being compromised?

A. Providing the source code for their web application to existing sales partners
B. Identifying high-risk assets that are on the same network as the web application server
C. Creating signatures for their IDS to detect attacks specific to their web application
D. Logging the connection requests to the web application server from outside hosts

Answer: C

NEW QUESTION 9
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 10
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 10
Of the options shown below, what is the first step in protecting network devices?

A. Creating standard secure configurations for all devices
B. Scanning the devices for known vulnerabilities
C. Implementing IDS to detect attacks
D. Applying all known security patches

Answer: A

NEW QUESTION 13
Which of the following assigns a number indicating the severity of a discovered software vulnerability?

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

Answer: D

NEW QUESTION 15
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 16
An administrator looking at a web application??s log file found login attempts by the same host over several seconds. Each user ID was attempted with three different passwords. The event took place over 5 seconds.
? ROOT
? TEST
? ADMIN
? SQL
? USER
? NAGIOSGUEST
What is the most likely source of this event?

A. An IT administrator attempting to use outdated credentials to enter the site
B. An attempted Denial of Service attack by locking out administrative accounts
C. An automated tool that attempts to use a dictionary attack to infiltrate a website
D. An attempt to use SQL Injection to gain information from a web-connected database

Answer: C

NEW QUESTION 20
Below is a screenshot from a deployed next-generation firewall. These configuration settings would be a defensive measure for which CIS Control?

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

NEW QUESTION 23
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 27
A global corporation has major data centers in Seattle, New York, London and Tokyo. Which of the following is the correct approach from an intrusion detection and event correlation perspective?

A. Configure all data center systems to use local time
B. Configure all data center systems to use GMT time
C. Configure all systems to use their default time settings
D. Synchronize between Seattle and New York, and use local time for London and Tokyo

Answer: A

NEW QUESTION 28
Which activity increases the risk of a malware infection?

A. Charging a smartphone using a computer USB port
B. Editing webpages with a Linux system
C. Reading email using a plain text email client
D. Online banking in Incognito mode

Answer: A

NEW QUESTION 30
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

Answer: C

NEW QUESTION 31
Which projects enumerates or maps security issues to CVE?

A. SCAP
B. CIS Controls
C. NIST
D. ISO 2700

Answer: A

NEW QUESTION 33
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

Answer: A

NEW QUESTION 35
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 36
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 39
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 c omput er s ys t ems
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

NEW QUESTION 41
Which of the following is a responsibility of a change management board?

A. Reviewing log files for unapproved changes
B. Approving system baseline configurations.
C. Providing recommendations for the changes
D. Reviewing configuration of the documents

Answer: B

NEW QUESTION 45
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

NEW QUESTION 46
What is an organization??s goal in deploying a policy to encrypt all mobile devices?

A. Enabling best practices for the protection of their software licenses
B. Providing their employees, a secure method of connecting to the corporate network
C. Controlling unauthorized access to sensitive information
D. Applying the principle of defense in depth to their mobile devices

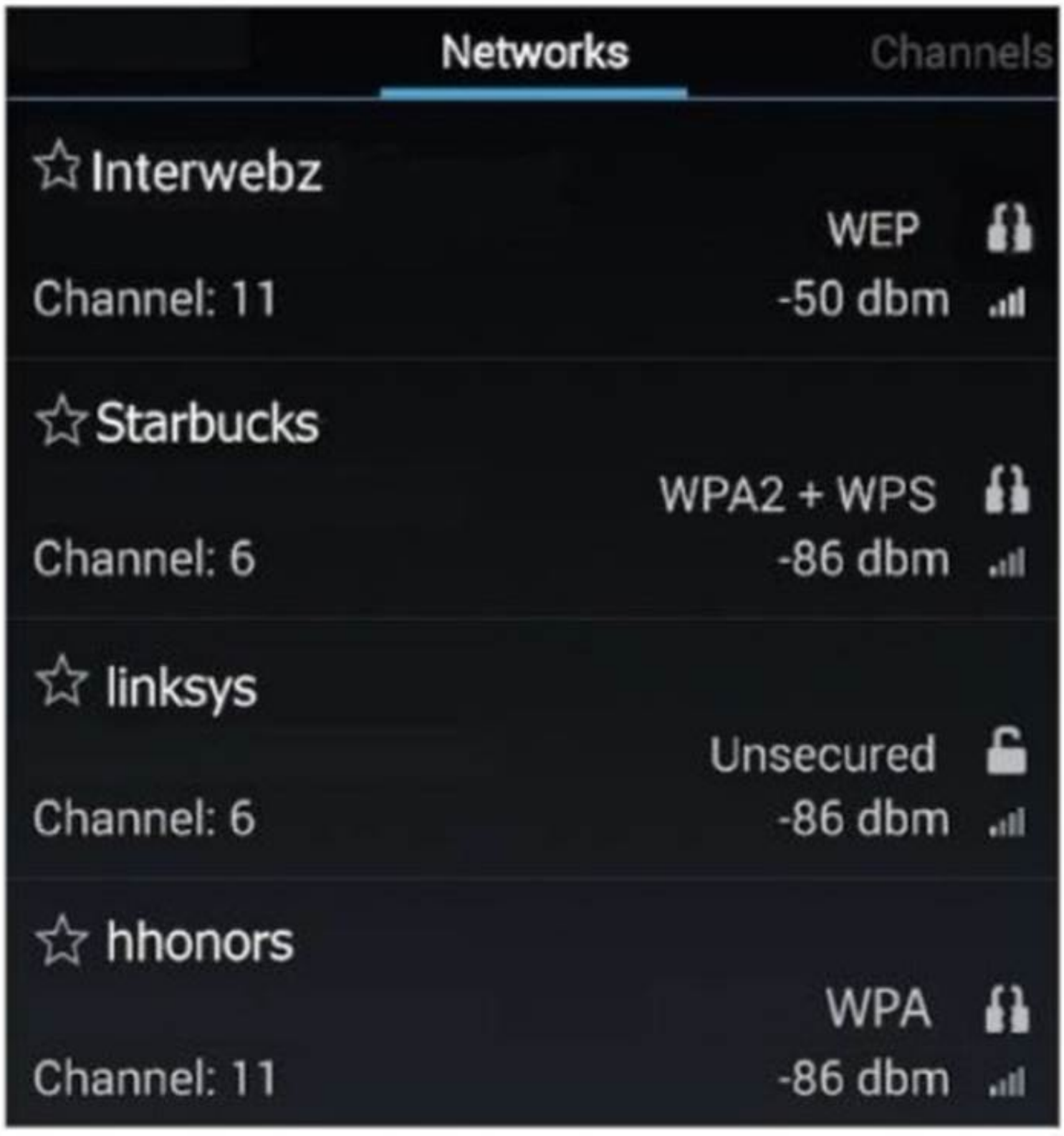
Answer: C

NEW QUESTION 51
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

NEW QUESTION 54
Based on the data shown below.



Which wireless access point has the manufacturer default settings still in place?

A. Starbucks
B. Linksys
C. Hhonors
D. Interwebz

Answer: B

NEW QUESTION 56
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 57
Kenya is a system administrator for SANS. Per the recommendations of the CIS Controls she has a dedicated host (kenya- adminbox / 10.10.10.10) for any administrative tasks. She logs into the dedicated host with her domain admin credentials. Which of the following connections should not exist from kenya-adminbox?

A. 10.10.245.3389
B. Mail.jane.org.25
C. Firewall_charon.jane.org.22
D. 10.10.10.33.443

Answer: B

NEW QUESTION 60
Which of the following baselines is considered necessary to implement the Boundary Defense CIS Control?

A. Multi-Factor Authentication Standard
B. Network Traffic/Service Baseline
C. Network Device Configuration Baselines
D. Network Information Flow

Answer: D

NEW QUESTION 61
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your GCCC Exam with Our Prep Materials Via below:

https://www.certleader.com/GCCC-dumps.html