GIAC

Exam Questions GCCC

GIAC Critical Controls Certification (GCCC)

NEW QUESTION 1
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

Answer: D

NEW QUESTION 2
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 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

Answer: B

NEW QUESTION 4
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 5
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 6
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 7
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

NEW QUESTION 8
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 9
What tool creates visual network topology output and results that can be analyzed by Ndiff to determine if a service or network asset has changed?

A. Ngrep
B. CIS-CAT
C. Netscreen
D. Zenmap

Answer: D

NEW QUESTION 10
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.

Answer: B

NEW QUESTION 10
An auditor is validating the policies and procedures for an organization with respect to a control for Data Recovery. The organization??s control states they will completely back up critical servers weekly, with incremental backups every four hours. Which action will best verify success of the policy?

A. Verify that the backup media cannot be read without the encryption key
B. Check the backup logs from the critical servers and verify there are no errors
C. Select a random file from a critical server and verify it is present in a backup set
D. Restore the critical server data from backup and see if data is missing

Answer: D

NEW QUESTION 13
IDS alerts at Service Industries are received by email. A typical day process over 300 emails with fewer than 50 requiring action. A recent attack was successful and went unnoticed due to the number of generated alerts. What should be done to prevent this from recurring?

A. Tune the IDS rules to decrease false positives.
B. Increase the number of staff responsible for processing IDS alerts.
C. Change the alert method from email to text message.
D. Configure the IDS alerts to only alert on high priority systems.

Answer: A

NEW QUESTION 18
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 21
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 26
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 27
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

NEW QUESTION 29
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 33
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 34
An analyst investigated unused organizational accounts. The investigation found that:
-10% of accounts still have their initial login password, indicating they were never used
-10% of accounts have not been used in over six months
Which change in policy would mitigate the security risk associated with both findings?

A. Users are required to change their password at the next login after three months
B. Accounts must have passwords of at least 8 characters, with one number or symbol
C. Accounts without login activity for 15 days are automatically locked

Answer: C

NEW QUESTION 38
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 42
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 46
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 49
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 53
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

Answer: B

NEW QUESTION 58
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

Answer: B

NEW QUESTION 59
Which type of scan is best able to determine if user workstations are missing any important patches?

A. A network vulnerability scan using aggressive scanning
B. A source code scan
C. A port scan using banner grabbing
D. A web application/database scan
E. A vulnerability scan using valid credentials

Answer: E

NEW QUESTION 60
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

NEW QUESTION 65
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 66
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 68
After installing a software package on several workstations, an administrator discovered the software opened network port TCP 23456 on each workstation. The port is part of a software management function that is not needed on corporate workstations. Which actions would best protect the computers with the software package installed?

A. Document the port number and request approval from a change control group
B. Redirect traffic to and from the software management port to a non-default port
C. Block TCP 23456 at the network perimeter firewall
D. Determine which service controls the software management function and opens the port, and disable it

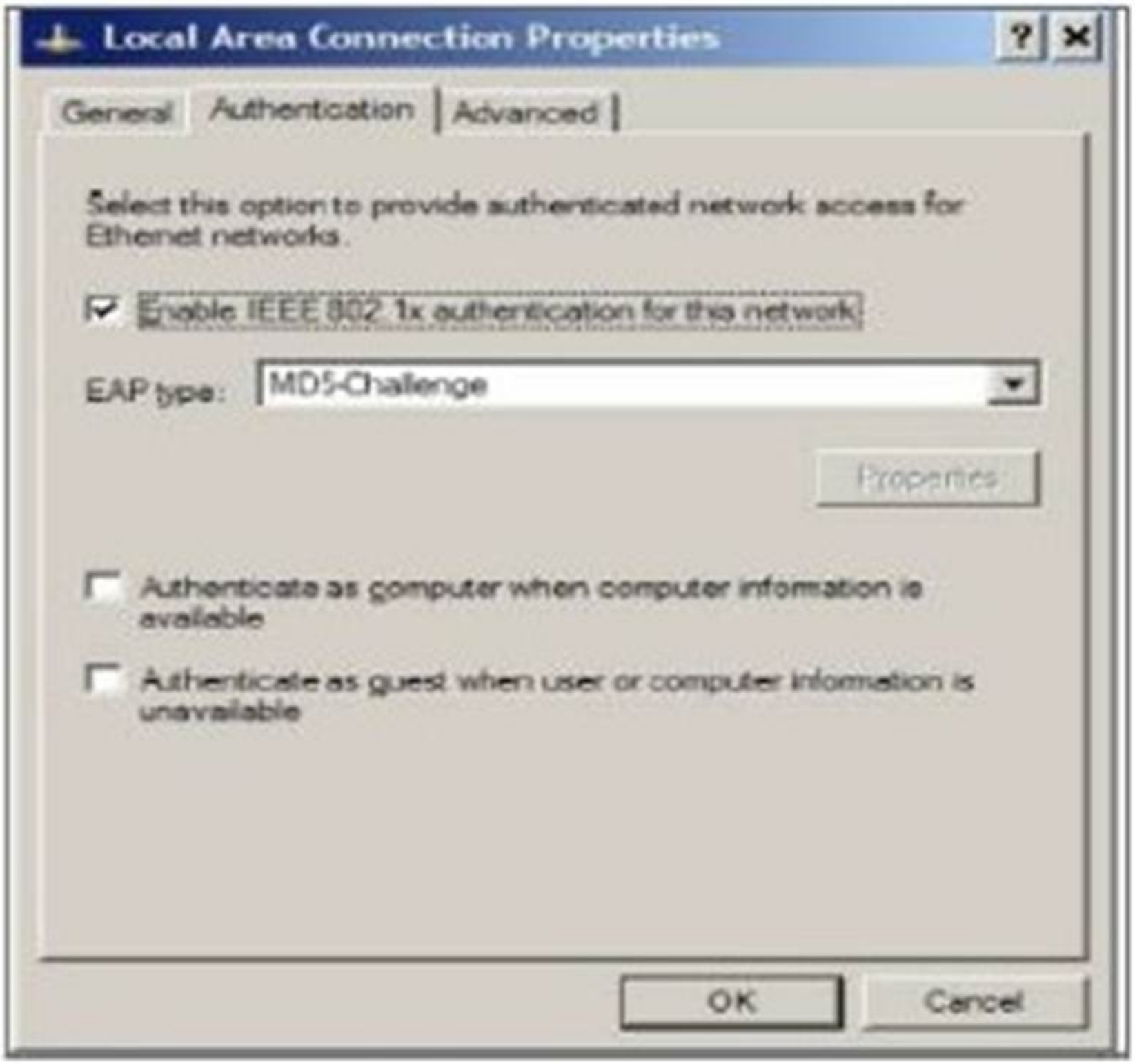
Answer: D

NEW QUESTION 71
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 76
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 81
Which of the following statements is appropriate in an incident response report?

A. There had been a storm on September 27th that may have caused a power surge
B. The registry entry was modified on September 29th at 22:37
C. The attacker may have been able to access the systems due to missing KB2965111
D. The backup process may have failed at 2345 due to lack of available bandwidth

Answer: B

NEW QUESTION 86
Implementing which of the following will decrease spoofed e-mail messages?

A. Finger Protocol
B. Sender Policy Framework
C. Network Address Translation
D. Internet Message Access Protocol

Answer: B

NEW QUESTION 91
Which of the following should be used to test antivirus software?

A. FIPS 140-2
B. Code Red

C. Heartbleed
D. EICAR

Answer: D

NEW QUESTION 96
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 100
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

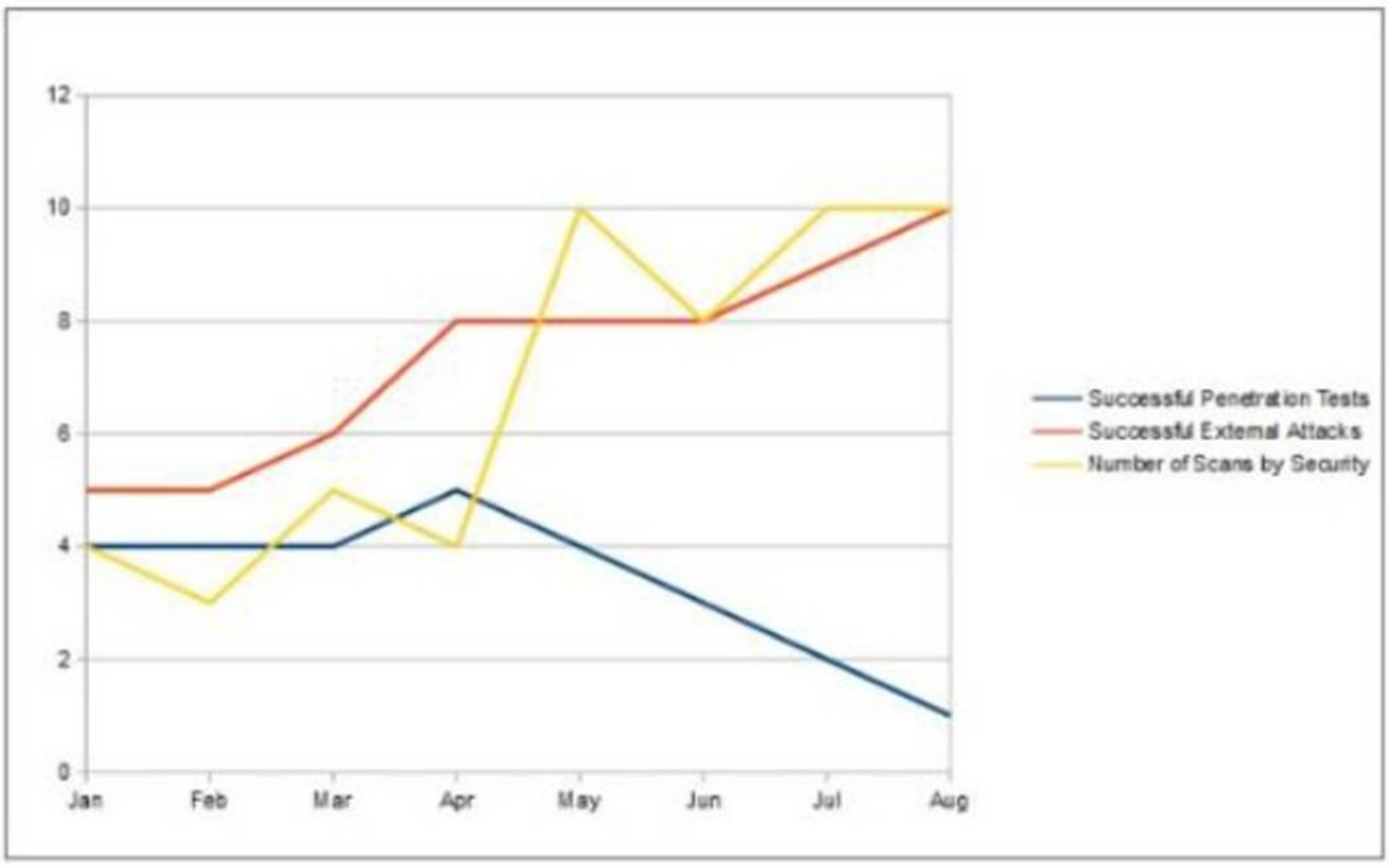
Answer: D

NEW QUESTION 103
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 104
An organization has implemented a control for penetration testing and red team exercises conducted on their network. They have compiled metrics showing the success of the penetration testing (Penetration Tests), as well as the number of actual adversary attacks they have sustained (External Attacks). Assess the metrics below and determine the appropriate interpretation with respect to this control.

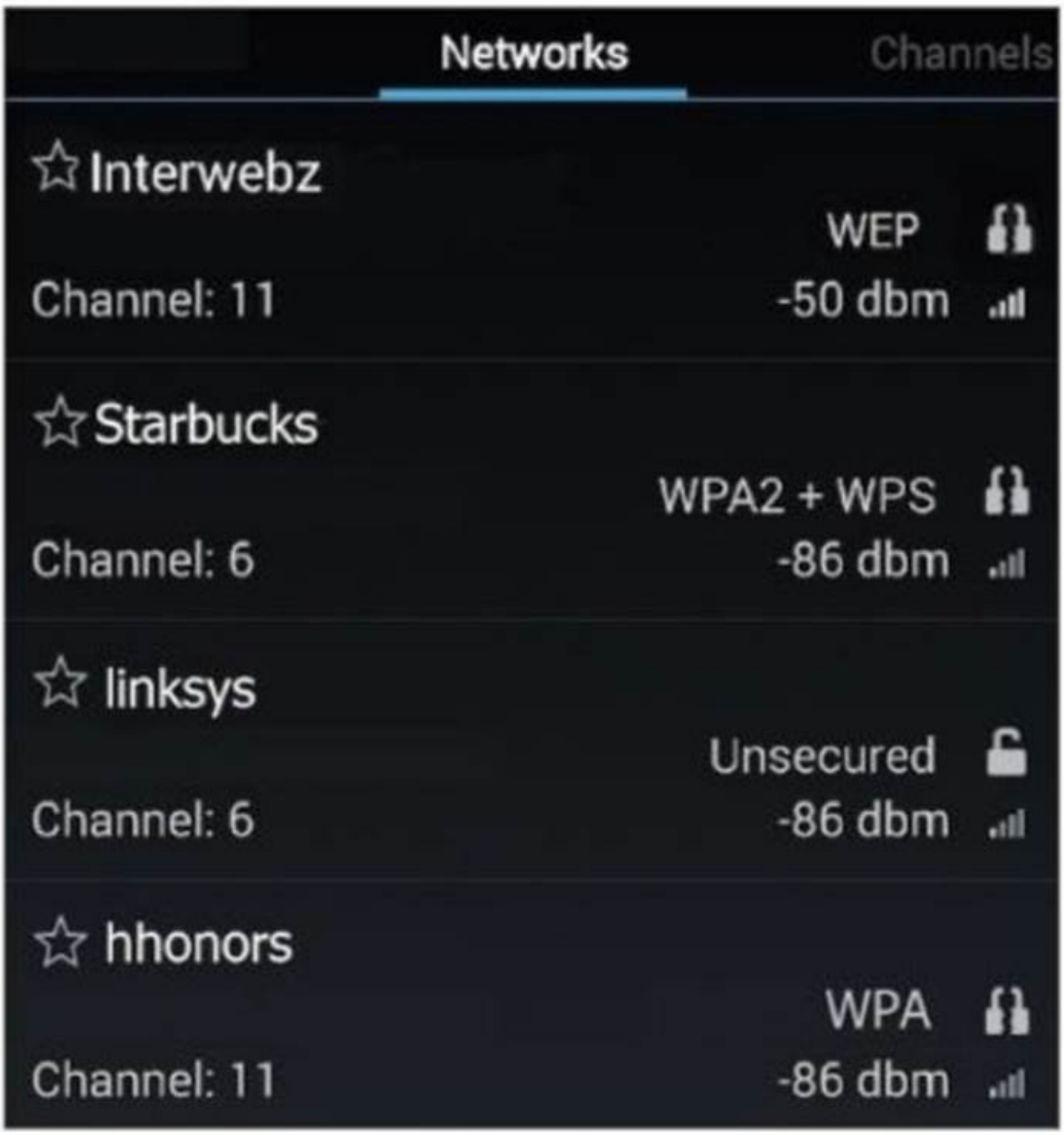


A. The blue team is adequately protecting the network
B. There are too many internal penetration tests being conducted

C. The methods the red team is using are not effectively testing the network
D. The red team is improving their capability to measure network security

Answer: C

NEW QUESTION 108
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 113
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 115
Which of the following will decrease the likelihood of eavesdropping on a wireless network?

A. Broadcasting in the 5Ghz frequency
B. Using Wired Equivalent Protocol (WEP)
C. Using EAP/TLS authentication and WPA2 with AES encryption

D. Putting the wireless network on a separate VLAN

Answer: C

NEW QUESTION 120
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 125
.....

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