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
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 3
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 4
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 5
Which of the following can be enabled on a Linux based system in order to make it more difficult for an attacker to execute malicious code after launching a buffer overflow attack?

A. ASLR
B. Tripwire
C. SUID
D. Iptables
E. TCP Wrappers

Answer: A

NEW QUESTION 6
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 7
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

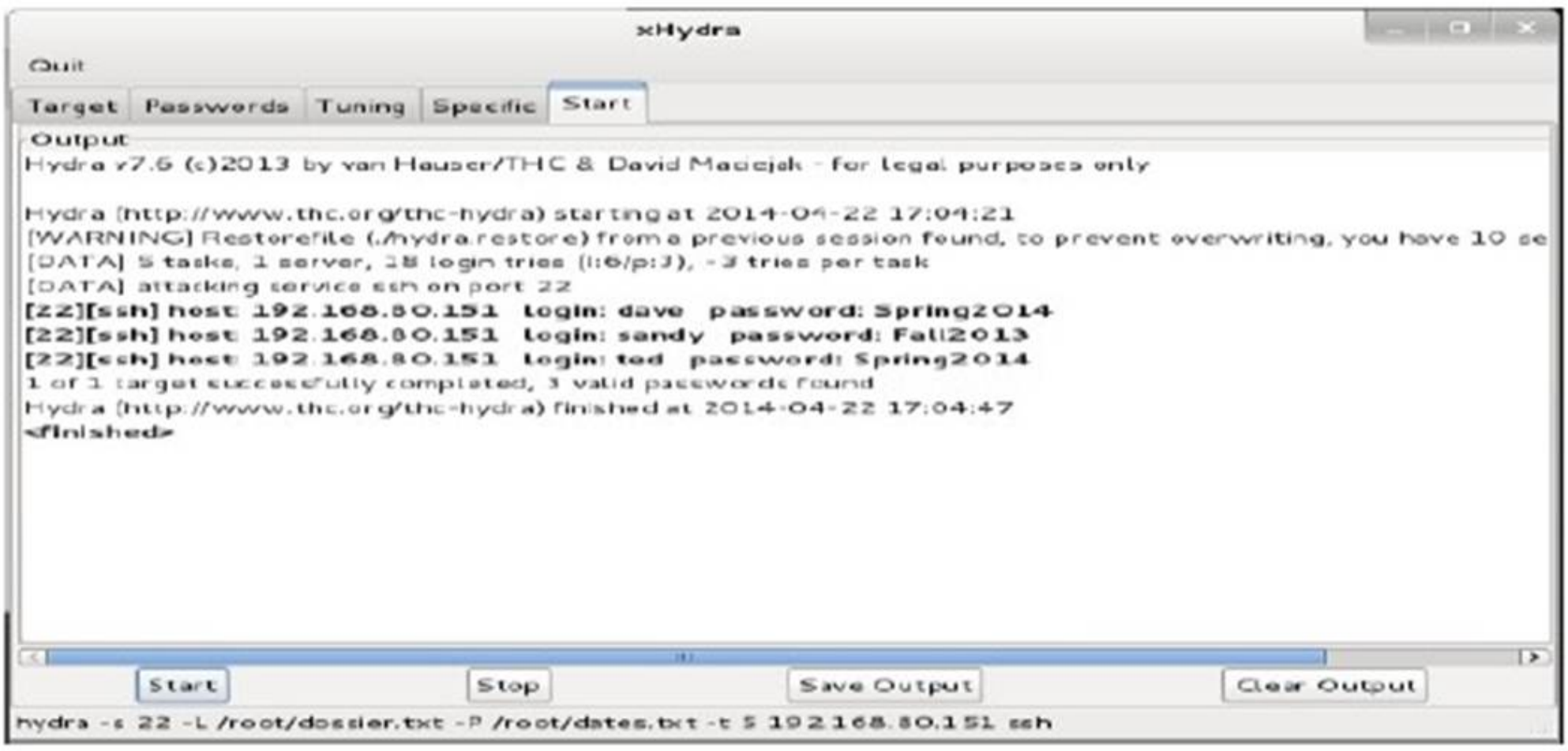
Answer: C

NEW QUESTION 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
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 10
Which of the following should be measured and analyzed regularly when implementing the Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers CIS Control?

A. How long does it take to identify new unauthorized listening ports on the network systems
B. How long does it take to remove unauthorized software from the organization??s systems
C. What percentage of the organization??s applications are using sandboxing products
D. What percentage of assets will have their settings enforced and redeployed
E. What percentage of systems in the organization are using Network Level Authentication (NLA)

Answer: D

NEW QUESTION 10
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 that 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

NEW QUESTION 13
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 17
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 18
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 19
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 20
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 25
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 27
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 31
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 33
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 35
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 38
Scan 1 was taken on Monday. Scan 2 was taken of the same network on Wednesday. Which of the following findings is accurate based on the information contained in the scans?

Scan 1

```
Nmap scan report for 192.168.177.7
Host is up (0.00090s latency).
Not shown: 94 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
5357/tcp  open  wsdapi
49155/tcp open  unknown
MAC Address: D8:50:E6:9F:EE:60 (Unknown)

Nmap scan report for 192.168.177.9
Host is up (0.00014s latency).
Not shown: 98 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
5357/tcp  open  wsdapi
MAC Address: D4:BE:D9:37:D1:7A (Dell)

Nmap scan report for 192.168.177.10
Host is up (0.00039s latency).
Not shown: 98 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3000/tcp  open  ppp
MAC Address: 00:0C:29:2E:3C:F9 (VMware)

Nmap scan report for 192.168.177.11
Host is up (0.0000050s latency).
Not shown: 99 closed ports
PORT    STATE SERVICE
80/tcp  open  http
```

Scan 2

```
Nmap scan report for 192.168.177.9
Host is up (0.00011s latency).
Not shown: 98 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
5357/tcp  open  wsdapi
MAC Address: D4:BE:D9:37:D1:7A (Dell)

Nmap scan report for 192.168.177.11
Host is up (0.0000050s latency).
Not shown: 99 closed ports
PORT    STATE SERVICE
80/tcp  open  http

Nmap scan report for 192.168.177.12
Host is up (0.011s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
80/tcp  open  http
515/tcp open  printer
MAC Address: 2C:9E:FC:2F:E0:83 (Canon)

Nmap scan report for 192.168.177.21
Host is up (0.00091s latency).
Not shown: 94 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
5357/tcp  open  wsdapi
49155/tcp open  unknown
MAC Address: D8:50:E6:9F:EE:60 (Unknown)
```

A. The host located at 192.168.177.7 is no longer on the network
B. The host with MAC Address D8:50:E6:9F:EE:60 is no longer on the network
C. The host located at 192.168.177.21 is a new host on the network
D. The host with MAC Address D8:50:E6:9F:EE:60 had an IP address change

Answer: D

NEW QUESTION 39
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 42
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 46
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

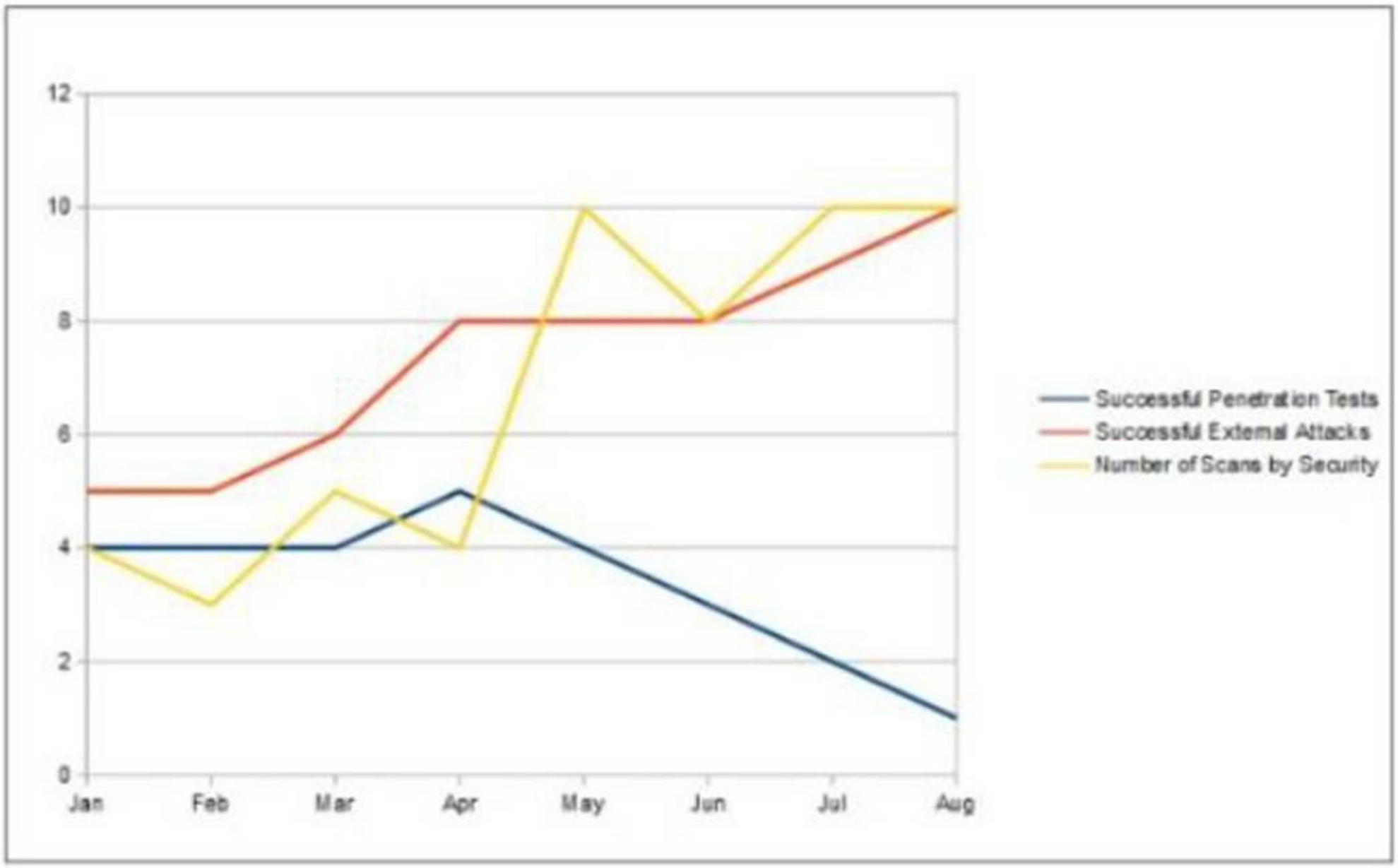
Answer: D

NEW QUESTION 47
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

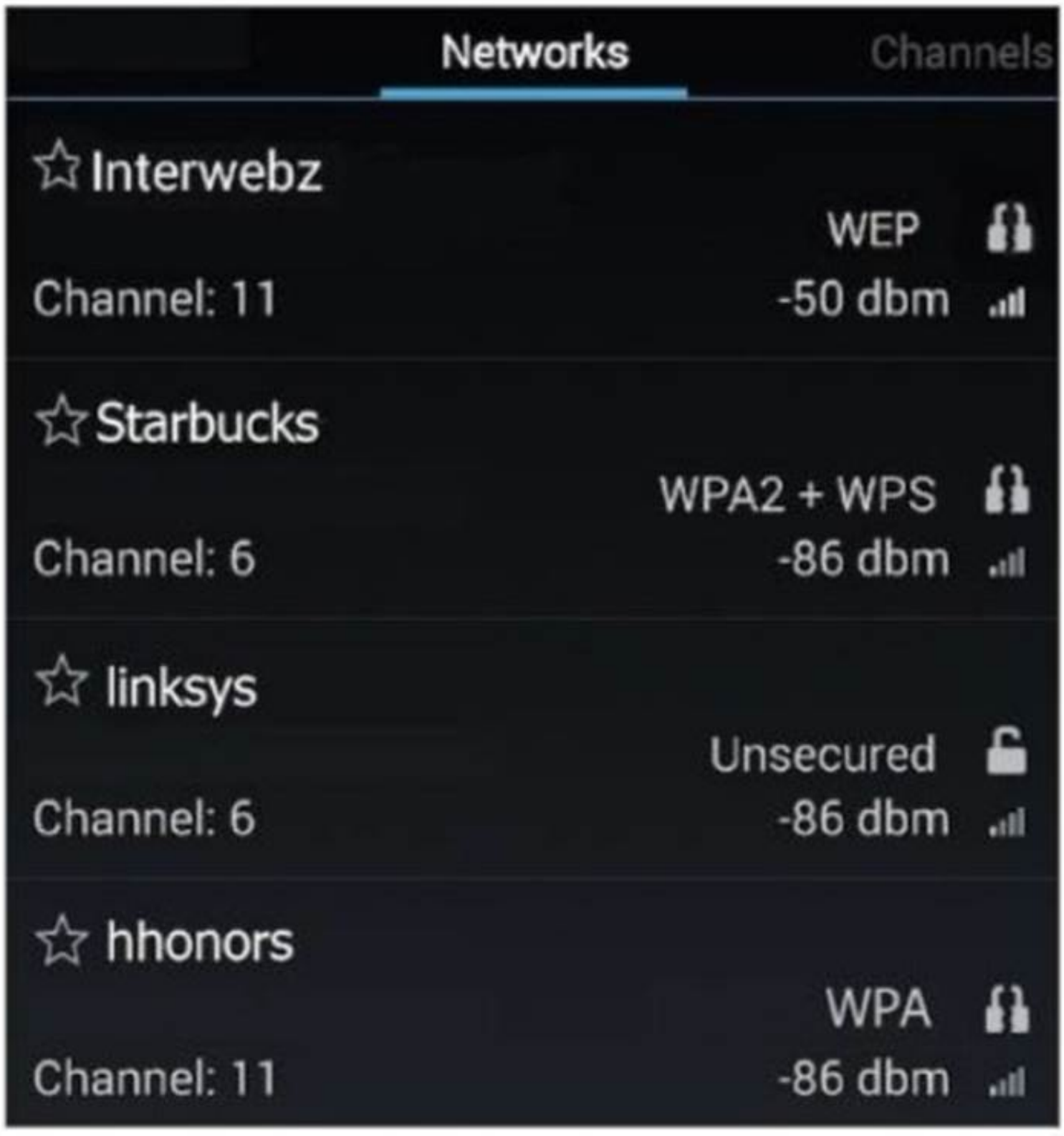
NEW QUESTION 52
An organization has implemented a control for penetration testing and red team exercises conducted on their network. They have compiled metrics showing the success of the penetration testing (Penetration Tests), as well as the number of actual adversary attacks they have sustained (External 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 55
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 58
.....

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