Question 1

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

Options:

A- Application Software Security

B- Inventory and Control of Hardware Assets

C- Account Monitoring and Control

D- Controlled Use of Administrative Privileges

Answer:

B

Question 2

Question Type: MultipleChoice

Which of the following will decrease the likelihood of eavesdropping on a wireless network?

Options:

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

Question 3

Question Type: MultipleChoice

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?

Options:

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

Question 4

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

Options:

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

Question 5

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?

Options:

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

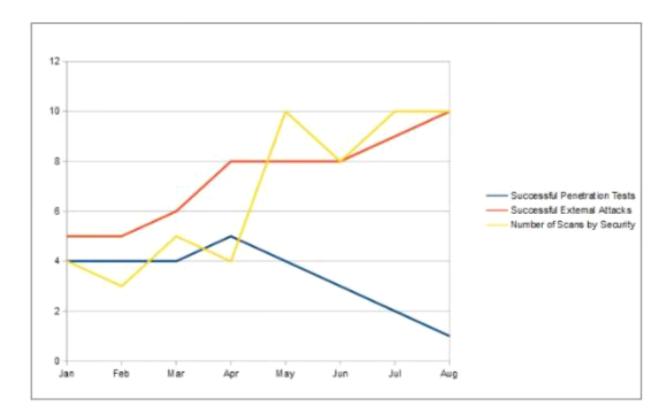**D-** Logging the connection requests to the web application server from outside hosts

Answer:

C

Question 6

Question Type: **MultipleChoice**

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.

Options:

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

Question 7

Question Type: MultipleChoice

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

Options:

A- CPE

B- CVE

C- CCE

D- CVSS

Answer:

D

Question 8

Question Type: MultipleChoice

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

Options:

A- Mimikatz

B- OpenVAS

C- Metasploit

Answer:

C

Question 9

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?

Options:

A- Input Validation

B- Output Sanitization

C- URL Encoding

D- Account Management

Answer:

A

Question 10

Question Type: **MultipleChoice**

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?

Options:

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

Question 11

Question Type: MultipleChoice

What is the relationship between a service and its associated port?

Options:

A- A service closes a port after a period of inactivity

B- A service relies on the port to select the protocol

C- A service sets limits on the volume of traffic sent through the port

D- A service opens the port and listens for network traffic

Answer:

D