Vendor:GIAC

Exam Code:GCCC

Exam Name:GCCC - GIAC Critical Controls Certification (GCCC)

Version: Demo

QUESTION 1

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

Correct Answer: B

QUESTION 2

An organization has implemented a policy to detect and remove malicious software from its network. Which of the following actions is focused on correcting rather than preventing attack?

A. Configuring a firewall to only allow communication to whitelisted hosts and ports

B. Using Network access control to disable communication by hosts with viruses

C. Disabling autorun features on all workstations on the network

D. Training users to recognize potential phishing attempts

Correct Answer: B

QUESTION 3

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

Correct Answer: C

QUESTION 4

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

Correct Answer: A

QUESTION 5

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

Correct Answer: D

QUESTION 6

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.

Correct Answer: C

QUESTION 7

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

Correct Answer: B

QUESTION 8

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

Correct Answer: D

QUESTION 9

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

Correct Answer: A

QUESTION 10

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

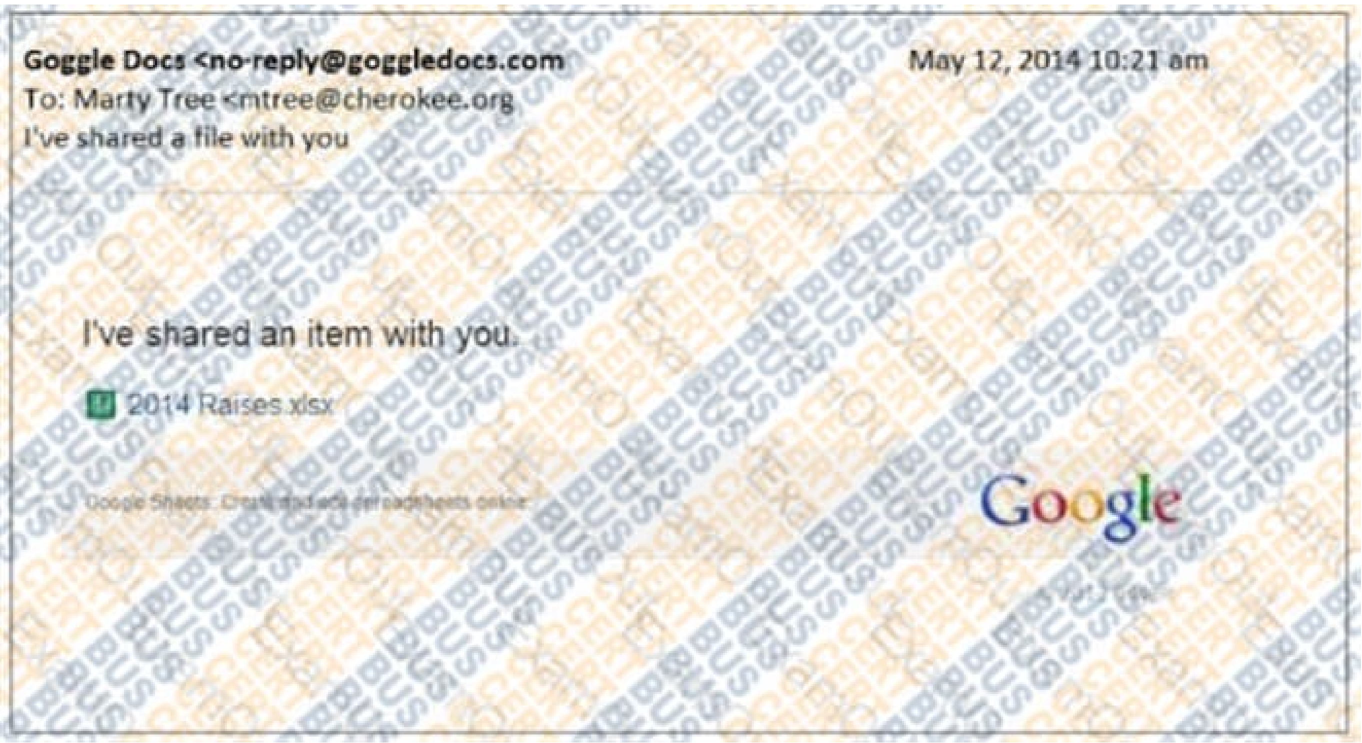
C. Reading email using a plain text email client

D. Online banking in Incognito mode

Correct Answer: A

QUESTION 11

Which of the following actions would best mitigate against phishing attempts such as the example below?



Goggle Docs <no-reply@goggledocs.com May 12, 2014 10:21 am

To: Marty Tree <mtree@cherokee.org

I've shared a file with you

I've shared an item with you.

2014 Raises.xlsx

Google Sheets: Create and edit spreadsheets online.

A. Establishing email filters to block no-reply address emails

B. Making web filters to prevent accessing Google Docs

C. Having employee\\'s complete user awareness training

D. Recommending against the use of Google Docs

Correct Answer: C

QUESTION 12

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

Correct Answer: B