CS0-002Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

QUESTION 1

A company provides wireless connectivity to the internal network from all physical locations for company-owned devices. Users were able to connect the day before, but now all users have reported that when they connect to an access point in the conference room, they cannot access company resources. Which of the following BEST describes the cause of the problem?

A. The access point is blocking access by MAC address. Disable MAC address filtering.

B. The network is not available. Escalate the issue to network support.

C. Expired DNS entries on users\\' devices. Request the affected users perform a DNS flush.

D. The access point is a rogue device. Follow incident response procedures.

Correct Answer: D

QUESTION 2

A suite of three production servers that were originally configured identically underwent the same vulnerability scans. However, recent results revealed the three servers has different critical vulnerabilities. The servers are not accessible by the Internet, and AV programs have not detected any malware. The servers\\' syslog files do not show any unusual traffic since they were installed and are physically isolated in an off-site datacenter. Checksum testing of random executables does not reveal tampering. Which of the following scenarios is MOST likely?

A. Servers have not been scanned with the latest vulnerability signature

B. Servers have been attacked by outsiders using zero-day vulnerabilities

C. Servers were made by different manufacturers

D. Servers have received different levels of attention during previous patch management events

Correct Answer: D

QUESTION 3

A cyber-security analyst is implementing a new network configuration on an existing network access layer to prevent possible physical attacks. Which of the following BEST describes a solution that would apply and cause fewer issues during the deployment phase?

A. Implement port security with one MAC address per network port of the switch.

B. Deploy network address protection with DHCP and dynamic VLANs.

C. Configure 802.1X and EAPOL across the network

D. Implement software-defined networking and security groups for isolation

Correct Answer: A

QUESTION 4

In order to meet regulatory compliance objectives for the storage of PHI, vulnerability scans must be conducted on a continuous basis. The last completed scan of the network returned 5,682 possible vulnerabilities. The Chief Information Officer (CIO) would like to establish a remediation plan to resolve all known issues. Which of the following is the BEST way to proceed?

A. Attempt to identify all false positives and exceptions, and then resolve all remaining items.

B. Hold off on additional scanning until the current list of vulnerabilities have been resolved.

C. Place assets that handle PHI in a sandbox environment, and then resolve all vulnerabilities.

D. Reduce the scan to items identified as critical in the asset inventory, and resolve these issues first.

Correct Answer: D

QUESTION 5

An analyst needs to forensically examine a Windows machine that was compromised by a threat actor. Intelligence reports state this specific threat actor is characterized by hiding malicious artifacts, especially with alternate data streams. Based on this intelligence, which of the following BEST explains alternate data streams?

A. A different way data can be streamlined if the user wants to use less memory on a Windows system for forking resources.

B. A way to store data on an external drive attached to a Windows machine that is not readily accessible to users.

C. A Windows attribute that provides for forking resources and is potentially used to hide the presence of secret or malicious files inside the file records of a benign file.

D. A Windows attribute that can be used by attackers to hide malicious files within system memory.

Correct Answer: C

QUESTION 6

A technician recently fixed a computer with several viruses and spyware programs on it and notices the Internet settings were set to redirect all traffic through an unknown proxy. This type of attack is known as which of the following?

A. Phishing

B. Social engineering

C. Man-in-the-middle

D. Shoulder surfing

Correct Answer: C

QUESTION 7

A security analyst was asked to join an outage call for a critical web application. The web middleware support team determined the web server is running and having no trouble processing requests; however, some investigation has revealed firewall denies to the web server that began around 1.00 a.m. that morning. An emergency change was made to enable the access, but management has asked for a root cause determination. Which of the following would be the BEST next step?

A. Install a packet analyzer near the web server to capture sample traffic to find anomalies.

B. Block all traffic to the web server with an ACL.

C. Use a port scanner to determine all listening ports on the web server.

D. Search the logging servers for any rule changes.

Correct Answer: D

QUESTION 8

A company frequently expenences issues with credential stuffing attacks.

Which of the following is the BEST control to help prevent these attacks from being successful?

A. SIEM

B. IDS

C. MFA

D. TLS

Correct Answer: C

QUESTION 9

A cybersecurity analyst develops a regular expression to find data within traffic that will alarm on a hit.

```
^(?:4[0-9]{12}(?:[0-9]{3})(?:5[1-5][0-9]{2})$
```

The SIEM alarms on seeing this data in cleartext between the web server and the database server.

```
'4554-8795-1596-7948'
'3723-159786-57984'
```

Which of the following types of data would the analyst MOST likely to be concerned with, and to which type of data classification does it belong?

A. Credit card numbers that are PCI

B. Social security numbers that are PHI

C. Credit card numbers that are PII

D. Social security numbers that are PII

Correct Answer: A

QUESTION 10

Given the following output from a Linux machine:

file2cable eth0 -f file.pcap

Which of the following BEST describes what a security analyst is trying to accomplish?

A. The analyst is attempting to measure bandwidth utilization on interface eth0.

B. The analyst is attempting to capture traffic on interface eth0.

C. The analyst is attempting to replay captured data from a PCAP file.

D. The analyst is attempting to capture traffic for a PCAP file.

E. The analyst is attempting to use a protocol analyzer to monitor network traffic.

Correct Answer: E

QUESTION 11

A threat hurting team received a new IoC from an ISAC that follows a threat actor\\'s profile and activities. Which of the following should be updated NEXT?

A. The whitelist

B. The DNS

C. The blocklist

D. The IDS signature

Correct Answer: D

QUESTION 12

While reviewing firewall logs, a security analyst at a military contractor notices a sharp rise in activity from a foreign domain known to have well-funded groups that specifically target the company\\'s RandD department. Historical data reveals other corporate assets were previously targeted. This evidence MOST likely describes:

A. an APT.

B. DNS harvesting.

C. a zero-day exploit.

D. corporate espionage.

Correct Answer: A

QUESTION 13

During a review of the vulnerability scan results on a server, an information security analyst notices the following:

```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH 3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

The MOST appropriate action for the analyst to recommend to developers is to change the web server so:

A. It only accepts TLSvl 2

B. It only accepts cipher suites using AES and SHA

C. It no longer accepts the vulnerable cipher suites

D. SSL/TLS is offloaded to a WAF and load balancer

Correct Answer: C

QUESTION 14

An administrator has been investigating the way in which an actor had been exfiltrating confidential data from a web server to a foreign host. After a thorough forensic review, the administrator determined the server\\'s BIOS had been modified by rootkit installation. After removing the rootkit and flashing the BIOS to a known good state, which of the following would BEST protect against future adversary access to the BIOS, in case another rootkit is installed?

A. Anti-malware application

B. Host-based IDS

C. TPM data sealing

D. File integrity monitoring

Correct Answer: C

QUESTION 15

Which of the following technologies can be used to house the entropy keys for task encryption on desktops and laptops?

A. Self-encrypting drive

B. Bus encryption

C. TPM

D. HSM

Correct Answer: A