# CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

## Pass CompTIA CS0-002 Exam with 100% Guarantee

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

**https://www.geekcert.com/cs0-002.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

A security analyst is conducting traffic analysis and observes an HTTP POST to the company\\'s main web server. The POST header is approximately 1000 bytes in length. During transmission, one byte is delivered every ten seconds. Which of the following attacks is the traffic indicative of?

A. Exfiltration

B. DoS

C. Buffer overflow

D. SQL injection

Correct Answer: A

**QUESTION 2**

An organization is conducting penetration testing to identify possible network vulnerabilities. The penetration tester has already identified active hosts in the network and is now scanning individual hosts to determine if any are running a web server. The output from the latest scan is shown below:

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Interesting ports on host 192.168.1.13:

PORT      STATE     SERVICE
80/tcp    open      http

Service detection performed:
Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds
```

Which of the following commands would have generated the output above?

A. map V 192.168.1.13 80

B. map P 192.168.1.0/24 ALL

C. map V 192.168.1.1 80

D. map P 192.168.1.13 ALL

Correct Answer: A

**QUESTION 3**

An insurance company employs quick-response team drivers that carry corporate-issued mobile devices with the

insurance company\\'s app installed on them. Devices are configuration-hardened by an MDM and kept up to date. The employees use the app to collect insurance claim information and process payments. Recently, a number of customers have filed complaints of credit card fraud against the insurance company, which occurred shortly after their payments were processed via the mobile app. The cyber-incident response team has been asked to investigate. Which of the following is MOST likely the cause?

A. The MDM server is misconfigured.

B. The app does not employ TLS.

C. USB tethering is enabled.

D. 3G and less secure cellular technologies are not restricted.

Correct Answer: B

**QUESTION 4**

During a cyber incident, which of the following is the BEST course of action?

A. Switch to using a pre-approved, secure, third-party communication system.

B. Keep the entire company informed to ensure transparency and integrity during the incident.

C. Restrict customer communication until the severity of the breach is confirmed.

D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

Correct Answer: D

**QUESTION 5**

Management is concerned with administrator access from outside the network to a key server in the company. Specifically, firewall rules allow access to the server from anywhere in the company. Which of the following would be an effective solution?

A. Honeypot

B. Jump box

C. Server hardening

D. Anti-malware

Correct Answer: B