# CS0-003$^{\text{Q\&As}}$

CompTIA Cybersecurity Analyst (CySA+)

## Pass CompTIA CS0-003 Exam with 100% Guarantee

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

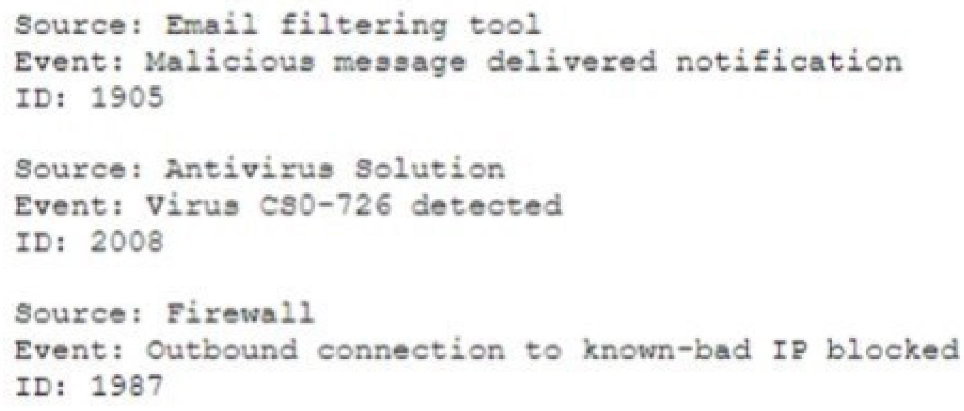
**https://www.passapply.com/cs0-003.html**

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 needs to automate the incident response process for malware infections. When the following logs are generated, an alert email should automatically be sent within 30 minutes:



```
Source: Email filtering tool
Event: Malicious message delivered notification
ID: 1905

Source: Antivirus Solution
Event: Virus CS0-726 detected
ID: 2008

Source: Firewall
Event: Outbound connection to known-bad IP blocked
ID: 1987
```

Which of the following is the best way for the analyst to automate alert generation?

A. Deploy a signature-based IDS

B. Install a UEBA-capable antivirus

C. Implement email protection with SPF

D. Create a custom rule on a SIEM

Correct Answer: D

A security information and event management (SIEM) system is a tool that collects and analyzes log data from various sources and provides alerts and reports on security incidents and events. A security analyst can create a custom rule on a SIEM system to automate the incident response process for malware infections. For example, the analyst can create a rule that triggers an alert email when the SIEM system detects logs that match the criteria of malware infection, such as process name, file name, file hash, etc. The alert email can be sent within 30 minutes or any other desired time frame. The other options are not suitable or sufficient for this purpose. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15; https://www.sans.org/reading-room/whitepapers/analyst/security-information-event-managementsiem-implementation-33969

**QUESTION 2**

Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

A. Business continuity plan

B. Vulnerability management plan

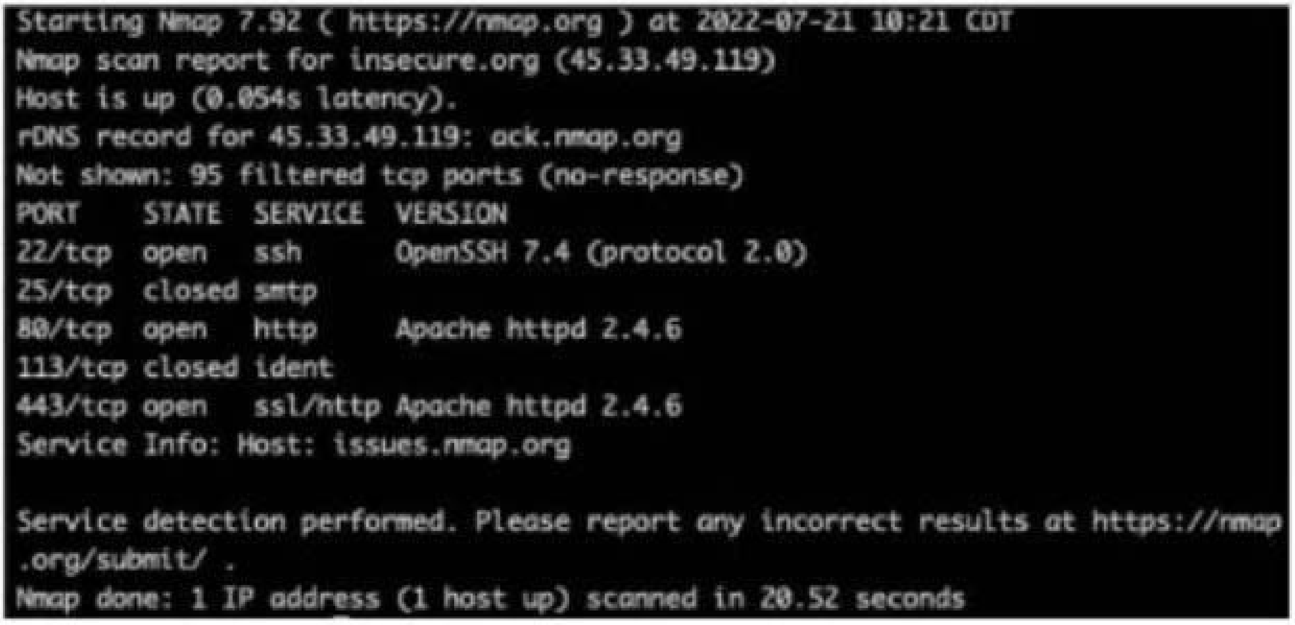
C. Disaster recovery plan

D. Asset management plan

Correct Answer: C

**QUESTION 3**

An analyst investigated a website and produced the following:



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 10:21 CDT
Nmap scan report for insecure.org (45.33.49.119)
Host is up (0.054s latency).
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 95 filtered tcp ports (no-response)
PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 7.4 (protocol 2.0)
25/tcp   closed smtp
80/tcp   open   http     Apache httpd 2.4.6
113/tcp closed ident
443/tcp open   ssl/http Apache httpd 2.4.6
Service Info: Host: issues.nmap.org

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.52 seconds
```

Which of the following syntaxes did the analyst use to discover the application versions on this vulnerable website?

A. nmap -sS -T4 -F insecure.org

B. nmap -o insecure.org

C. nmap -sV -T4 -F insecure.org

D. nmap -A insecure.org

Correct Answer: C

**QUESTION 4**

Which of the following ICS network protocols has no inherent security functions on TCP port 502?

A. CIP

B. DHCP

C. SSH

D. Modbus

Correct Answer: D

**QUESTION 5**

A security analyst is reviewing the findings of the latest vulnerability report for a company\\'s web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability with the fewest changes to the current script and infrastructure?

A. Deploy a WAF to the front of the application.

B. Replace the current MD5 with SHA-256.

C. Deploy an antivirus application on the hosting system.

D. Replace the MD5 with digital signatures.

Correct Answer: B

This option involves changing the hash algorithm from the vulnerable MD5 to the more secure SHA-256. It addresses the hash collision vulnerability directly and doesn\\'t require major changes to the existing infrastructure or script logic.

Latest CS0-003 Dumps    CS0-003 PDF Dumps    CS0-003 VCE Dumps