- **Vendor: CompTIA**
- **Exam Code: CS0-002**
- **Exam Name: CompTIA CSA+ Certification Exam**
- **New Updated Questions from Braindump2go (Updated in July/2020)**

QUESTION 34
A small electronics company decides to use a contractor to assist with the development of a new FPGA- based device. Several of the development phases will occur off-site at the contractor's labs. Which of the following is the main concern a security analyst should have with this arrangement?

A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.
B. Moving the FPGAs between development sites will lessen the time that is available for security testing.
C. Development phases occurring at multiple sites may produce change management issues.
D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Answer: D

QUESTION 35
A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

```
$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4): 56 data bytes
--- 192.168.1.4 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

The analyst runs the following command next:

```
$ sudo hping3 -c 4 -n -i 192.168.1.4
HPING 192.168.1.4 (en1 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 id=32101 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32102 sport=0 flags=RA seq=1 win=0 rtt=0.3ms
len=46 ip=192.168.1.4 ttl=64 id=22103 sport=0 flags=RA seq=2 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32104 sport=0 flags=RA seq=3 win=0 rtt=0.4ms
--- 10.0.1.33 hpaing statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

Which of the following would explain the difference in results?

A. ICMP is being blocked by a firewall.
B. The routing tables for ping and hping3 were different.
C. The original ping command needed root permission to execute.
D. hping3 is returning a false positive.

Answer: A

QUESTION 36
A cybersecurity analyst is contributing to a team hunt on an organization's endpoints.

Which of the following should the analyst do FIRST?

A. Write detection logic.
B. Establish a hypothesis.
C. Profile the threat actors and activities.
D. Perform a process analysis.

Answer: B

QUESTION 37
A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system. After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources.
Which of the following BEST describes this attack?

A. Injection attack
B. Memory corruption
C. Denial of service
D. Array attack

Answer: B

QUESTION 38
Which of the following BEST describes why vulnerabilities found in ICS and SCADA can be difficult to remediate?

A. ICS/SCADA systems are not supported by the CVE publications.
B. ICS/SCADA systems rarely have full security functionality.
C. ICS/SCADA systems do not allow remote connections.
D. ICS/SCADA systems use encrypted traffic to communicate between devices.

Answer: A

QUESTION 39
An organization has been conducting penetration testing to identify possible network vulnerabilities. One of the security policies states that web servers and database servers must not be co-located on the same server unless one of them runs on a non-standard. The penetration tester has received the following outputs from the latest set of scans:

```
Starting Nmap 4.11 (http://nmap.org) at 2011-11-03 18:32 EDT

Interesting ports on host orgServer (192.168.1.13)
PORT              STATE         SERVICE
22/tcp            open          ssh
80/tcp            open          http
139/tcp           open          netbios-ssn
3306/tcp          open          mysql
Service detection performed.

Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds

Starting Nmap 4.11 ((http://nmap.org) at 2011-11-03 18:33 EDT

Interesting ports on host finServer (192.168.1.14):
PORT              STATE         SERVICE
22/tcp            open          ssh
80/tcp            open          http
139/tcp           open          netbios-ssn
Service detection performed.

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

Which of the following servers is out of compliance?

A. finServer
B. adminServer
C. orgServer
D. opsServer

Answer: C

QUESTION 40
The security team for a large, international organization is developing a vulnerability management program. The development staff has expressed concern that the new program will cause service interruptions and downtime as vulnerabilities are remedied.
Which of the following should the security team implement FIRST as a core component of the remediation process to address this concern?

A. Automated patch management
B. Change control procedures
C. Security regression testing
D. Isolation of vulnerable servers

Answer: C

QUESTION 41
A company is developing its first mobile application, which will be distributed via the official application stores of the two major mobile platforms.
Which of the following is a prerequisite to making the applications available in the application stores?

A. Distribute user certificates.
B. Deploy machine/computer certificates.
C. Obtain a code-signing certificate.
D. Implement a CRL.

Answer: B

QUESTION 42
A security analyst's daily review of system logs and SIEM showed fluctuating patterns of latency. During the analysis, the analyst discovered recent attempts of intrusion related to malware that overwrites the MBR. The facilities manager informed the analyst that a nearby construction project damaged the primary power lines, impacting the analyst's support systems. The electric company has temporarily restored power, but the area may experience temporary outages.
Which of the following issues the analyst focus on to continue operations?

A. Updating the ACL
B. Conducting backups
C. Virus scanning
D. Additional log analysis

Answer: C

QUESTION 43
A company has a popular shopping cart website hosted geographically diverse locations. The company has started hosting static content on a content delivery network (CDN) to improve performance. The CDN provider has reported the company is occasionally sending attack traffic to other CDN-hosted targets.
Which of the following has MOST likely occurred?

A. The CDN provider has mistakenly performed a GeoIP mapping to the company.
B. The CDN provider has misclassified the network traffic as hostile.
C. A vulnerability scan has tuned to exclude web assets hosted by the CDN.
D. The company has been breached, and customer PII is being exfiltrated to the CDN.

Answer: D

QUESTION 44
During a recent breach, an attacker was able to use tcpdump on a compromised Linux server to capture the password of a network administrator that logged into a switch using telnet. Which of the following compensating controls could be implemented to address this going forward?

A. Whitelist tcpdump of Linux servers.
B. Change the network administrator password to a more complex one.
C. Implement separation of duties.
D. Require SSH on network devices.

Answer: D

QUESTION 45
A company uses a managed IDS system, and a security analyst has noticed a large volume of brute force password attacks originating from a single IP address. The analyst put in a ticket with the IDS provider, but no action was taken for 24 hours, and the attacks continued. Which of the following would be the BEST approach for the scenario described?

A. Draft a new MOU to include response incentive fees.
B. Reengineer the BPA to meet the organization's needs.

C. Modify the SLA to support organizational requirements.
D. Implement an MOA to improve vendor responsiveness.

Answer: C