QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

SY0-601 Dumps
SY0-601 Braindumps
SY0-601 Real Questions
SY0-601 Practice Test
SY0-601 dumps free

## CompTIA

# SY0-601

*CompTIA Security+ 2021*

Question #145 Section 1

A security incident may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO). A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

- A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag.
- B. Connect a write blocker to the hard drive. Then, leveraging a forensic workstation, utilize the dd command in a live Linux environment to create a duplicate copy.
- C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches.
- D. Refrain from completing a forensic analysis of the CEO's hard drive until after the incident is confirmed; duplicating the hard drive at this stage could destroy evidence.

**Answer:** D

Question #146 Section 1

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer (CIO) believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be BEST to mitigate the CEO's concerns? (Choose two.)

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

**Answer:** AB

Question #147 Section 1

In the middle of a cyberattack, a security engineer removes the infected devices from the network and locks down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

- A. Identification
- B. Preparation
- C. Lessons learned
- D. Eradication
- E. Recovery
- F. Containment

**Answer:** F

Question #148 Section 1

The SOC is reviewing processes and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. This allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

- A. Updating the playbooks with better decision points
- B. Dividing the network into trusted and untrusted zones

- C. Providing additional end-user training on acceptable use
- D. Implementing manual quarantining of infected hosts

**Answer:** A

Question #149 Section 1

A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

- A. Rainbow table
- B. Brute-force
- C. Password-spraying
- D. Dictionary

**Answer:** C

Question #150 Section 1

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate devices using PKI. Which of the following should the administrator configure?

- A. A captive portal
- B. PSK
- C. 802.1X
- D. WPS

**Answer:** C

Question #151 Section 1

Which of the following are the MOST likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Choose two.)

- A. Unsecure protocols
- B. Use of penetration-testing utilities
- C. Weak passwords
- D. Included third-party libraries
- E. Vendors/supply chain
- F. Outdated anti-malware software

**Answer:** AC

Question #152 Section 1

A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers, the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

- A. Physical
- B. Detective
- C. Preventive
- D. Compensating

**Answer:** D

Question #153 Section 1

An organization just experienced a major cyberattack incident. The attack was well coordinated, sophisticated, and highly skilled. Which of the following targeted the organization?

- A. Shadow IT
- B. An insider threat
- C. A hacktivist
- D. An advanced persistent threat

**Answer:** D

Question #154 Section 1

A security analyst has received an alert about PII being sent via email. The analyst's Chief Information Security Officer (CISO) has made it clear that PII must be handled with extreme care. From which of the following did the alert MOST likely originate?

- A. S/MIME
- B. DLP
- C. IMAP
- D. HIDS

**Answer:** B