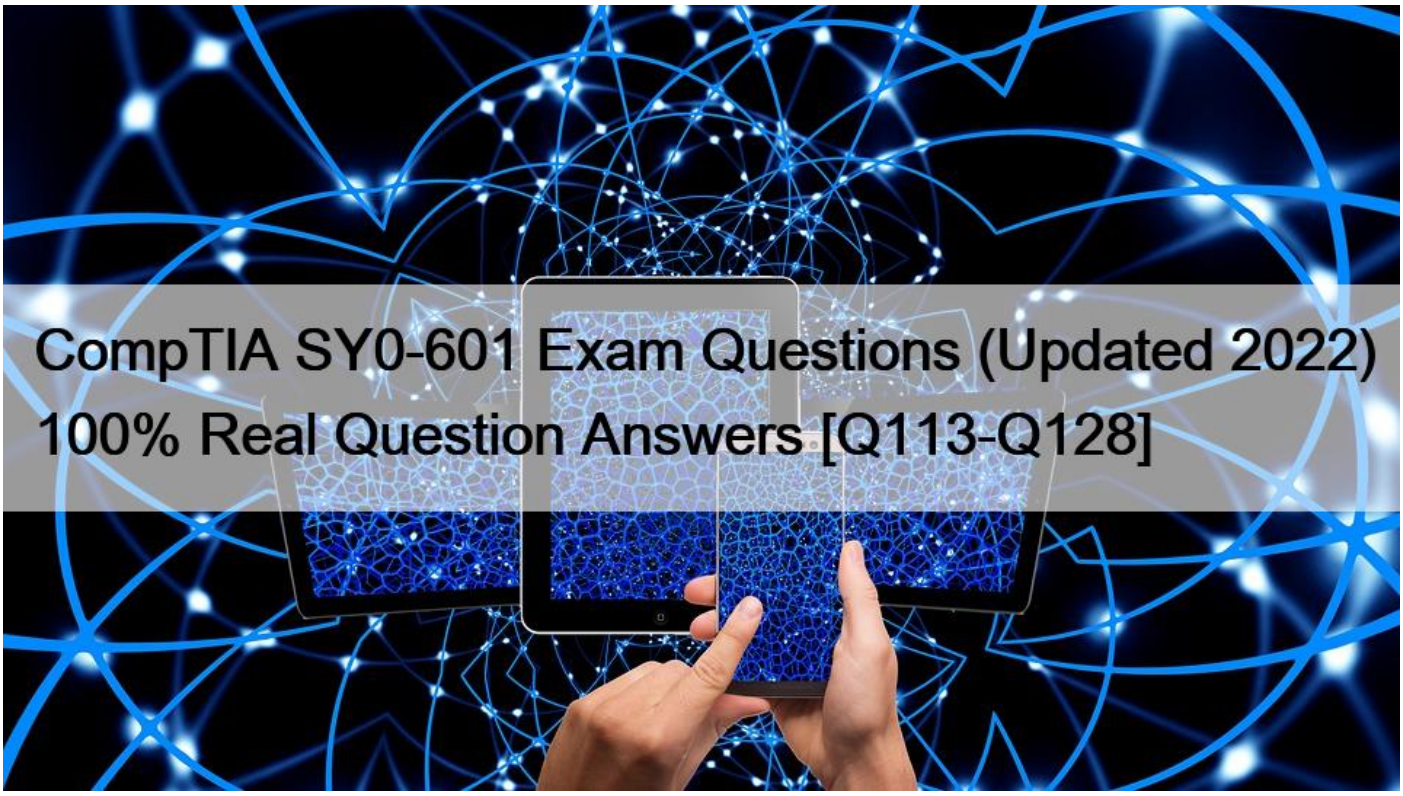
CompTIA SY0-601 Exam Questions (Updated 2022) 100% Real Question Answers [Q113-Q128



CompTIA SY0-601 Exam Questions (Updated 2022) 100% Real Question Answers
Pass CompTIA SY0-601 Exam Quickly With Test4Engine

Audience Profile

If you are getting ready to explore what the world of cybersecurity offers with this Security+ SY0-601 exam, then you should have some hands-on experience in security concepts. Overall, Junior Security Engineers, Help Desk Technicians, or entry-level Security Analysts can level-up their careers with the aforementioned certification.

CompTIA SY0-601: Prerequisites

The CompTIA SY0-601 exam is intended for those individuals who want to establish a career in the cybersecurity domain. The biggest advantage of this certification test is that there are no prior requirements for it. There is no need to undertake any training or have any experience. The students just have to take a single exam whenever they are prepared. However, possessing working experience of two years in the IT administration field will be beneficial, but it is not necessary.

Architecture & Design (21%) - Summarize secure automation, deployment, and development of application concepts;- Describe the significance of physical security controls;- Given a specific scenario, execute cybersecurity resilience;- Describe the significance of security concepts within an enterprise environment;- Describe security implications of specialized and embedded systems;- Summarize the fundamentals of cryptographic concepts. **NO.113** A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers.

Which of the following frameworks should the management team follow?
* Payment Card Industry Data Security Standard
* Cloud Security Alliance Best Practices
* ISO/IEC 27032 Cybersecurity Guidelines
* General Data Protection Regulation

NO.114 An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions.

Which of the following sources of information would BEST support this solution?
* Web log files
* Browser cache
* DNS query logs
* Antivirus

NO.115 A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```

Which of the following can the security analyst conclude?
* A replay attack is being conducted against the application.
* An injection attack is being conducted against a user authentication system.
* A service account password may have been changed, resulting in continuous failed logins within the application.
* A credentialed vulnerability scanner attack is testing several CVEs against the application.

NO.116 A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

```
User account 'JHDoe' does not exist...
User account 'VMAdmin' does not exist...
User account 'tomcat' wrong password...
User account 'Admin' does not exist...
```

Which of the following MOST likely would have prevented the attacker from learning the service account name?
* Race condition testing
* Proper error handling
* Forward web server logs to a SIEM
* Input sanitization

NO.117 Which of the following BEST explains the difference between a data owner and a data custodian?
* The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
* The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
* The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
* The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

NO.118 Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a “cloud-first” adoption strategy?
* Risk matrix
* Risk tolerance
* Risk register
* Risk appetite

NO.119 A large enterprise has moved all Hs data to the cloud behind strong authentication and encryption A sales director recently had a laptop stolen and later, enterprise data was round to have been compromised database. Which of the following was the MOST likely cause?
* Shadow IT
* Credential stuffing
* SQL injection
* Man-in-the-browser
E .Bluejacking

NO.120 A global pandemic is forcing a private organization to close some business units and reduce staffing at others.

Which of the following would be BEST to help the organization’s executives determine the next course of action?
* An incident response plan
* A communications plan
* A disaster recovery plan
* A business continuity plan

NO.121 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?
* Updating the playbooks with better decision points
* Dividing the network into trusted and untrusted zones
* Providing additional end-user training on acceptable use
* Implementing manual quarantining of infected hosts

NO.122 A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?
* SIEM
* DLP
* CASB
* SWG

Explanation

A cloud access security broker is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies

NO.123 A company uses specially configured workstations tor any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery.

Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?
* Fileless malware
* A downgrade attack
* A supply-chain attack
* A logic bomb
* Misconfigured BIOS

NO.124 A network administrator was provided the following output from a vulnerability scan:

Plugin ID	Severity	Count	Description	Risk Score
10	Critical	1	CentOS 7 : rpm (CTSA-2014:1980)	3.4
11	Low	178	Microsoft Windows Update	1.3
12	Medium	120	openSUSE Security Update: python3 / rpm	1.8
13	High	15	Microsoft Windows Update Reboot Required	3.6
14	Low	1389	RHEL 4 : RPM (RHSA-2016:0678)	2.1

The network administrator has been instructed to prioritize remediation efforts based on overall risk to the enterprise. Which of the following plugin IDs should be remediated FIRST?
* 10
* 11
* 12
* 13
* 14

NO.125 An analyst is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services. Given this output from Nmap.

```
PORT     STATE
21/tcp   filtered
22/tcp   open
23/tcp   open
443/tcp  open
```

Which of the following should the analyst recommend to disable?
* 21/tcp
* 22/tcp
* 23/tcp
* 443/tcp

NO.126 A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multicloud provider environment.

The security architect is looking for a solution with reduced latency to allow the incorporation of the organization’s existing keys and to maintain consistent, centralized control and management regardless of the data location.

Which of the following would BEST meet the architect’s objectives?
* Trusted Platform Module
* laaS
* HSMaaS
* PaaS
* Key Management Service

NO.127 Employees are having issues accessing the company’s website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?
* DDoS
* Man-in-the-middle
* MAC flooding
* Domain hijacking

NO.128 The chief compliance officer from a bank has approved a background check policy for all new hires. Which of the following is the policy MOST likely protecting against?
* Preventing any current employees’ siblings from working at the bank to prevent nepotism
* Hiring an employee who has been convicted of theft to adhere to industry compliance
* Filtering applicants who have added false information to resumes so they appear better qualified
* Ensuring no new hires have worked at other banks that may be trying to steal customer information