SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.geekcert.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

A. Semi-authorized hackers

B. State actors

C. Script kiddies

D. Advanced persistent threats

Correct Answer: B

APT=An attacker\\'s ability to obtain, maintain, and diversify access to network systems using exploits and malware.

Stateactor=A type of threat actor that is supported by the resources of its host country\\'s military and security services.

QUESTION 2

A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

A. Establish chain of custody.

B. Inspect the file metadata.

C. Reference the data retention policy.

D. Review the email event logs

Correct Answer: D

inspecting the file meta data isn\\'t going to do anything because the file\\'s creation or modified date isn\\'t in question. The question is if they sent the file at all. In this case they didn\\'t which can be proven via email event log.

QUESTION 3

A cybersecurity analyst needs to adopt controls to properly track and log user actions to an individual. Which of the following should the analyst implement?

A. Non-repudiation

B. Baseline configurations

C. MFA

D. DLP

Correct Answer: A

Non-repudiation is the process of ensuring that a party involved in a transaction or communication cannot deny their involvement. By implementing non-repudiation controls, a cybersecurity analyst can properly track and log user actions, attributing them to a specific individual. This can be achieved through methods such as digital signatures, timestamps, and secure logging mechanisms.

References:

1. CompTIA Security+ Certification Exam Objectives (SY0-601): https://www.comptia.jp/pdf/CompTIA%20Security%2B%20SY0- 601%20Exam%20Objectives.pdf

QUESTION 4

A company wants to improve end users experiences when they tog in to a trusted partner website The company does not want the users to be issued separate credentials for the partner website Which of the following should be implemented to allow users to authenticate using their own credentials to log in to the trusted partner\\'s website?

A. Directory service

B. AAA server

C. Federation

D. Multifactor authentication

Correct Answer: C

Federation means the company trusts accounts created and managed by a different network. It connects the identity management services of multiple systems

QUESTION 5

An end user reports a computer has been acting slower than normal for a few weeks, During an investigation, an analyst determines the system 3 sending the users email address and a ten-digit number ta an IP address once a day. The only resent log entry regarding the user\\'s computer is the following:

```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdftodocx.msi
Connection Details: 35.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

A. The end user purchased and installed a PUP from a web browser

B. A bot on the computer is brute forcing passwords against a website

C. A hacker is attempting to exfiltrate sensitive data

D. Ransomware is communicating with a command-and-control server.

Correct Answer: A