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.leads4pass.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

The security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted files

The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again.

Which of the following is MOST capable of accomplishing both tasks?

A. HIDS

B. Allow list

C. TPM

D. NGFW

Correct Answer: C

QUESTION 2

A security proposal was set up to track requests for remote access by creating a baseline of the users\\' common sign-in properties. When a baseline deviation is detected, an Iv1FA challenge will be triggered. Which of the following should be configured in order to deploy the proposal?

A. Context-aware authentication

B. Simultaneous authentication of equals

C. Extensive authentication protocol

D. Agentless network access control

Correct Answer: A

An access control scheme that verifies an object\\'s identity based on various environmental factors, like time, location, and behavior.

QUESTION 3

A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive\\'s accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement

B. Least privilege

C. An acceptable use policy

D. Ofboarding

Correct Answer: D

QUESTION 4

A user attempts to load a web-based application, but the expected login screen does not appear A help desk analyst troubleshoots the issue by running the following command and reviewing the output on the user\'s PC

```
user> nslookup software-solution.com
        Server: rogue.comptia.com
        Address: 172.16.1.250
        Non-authoritative answer:
        Name: software-solution.com
        Address: 10.20.10.10
```

The help desk analyst then runs the same command on the local PC

```
helpdesk> nslookup software-solution.com
        Server: dns.comptia.com
        Address: 172.16.1.1
        Non-authoritative answer:
        Name: software-solution.com
        Address: 172.16.1.10
```

Which of the following BEST describes the attack that is being detected?

A. Domain hijacking

B. DNS poisoning

C. MAC flooding

D. Evil twin

Correct Answer: B

QUESTION 5

A customer called a company\'s security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following

1.

 The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.

2.

 One of the websites the manager used recently experienced a data breach

3.

The manager\\'s corporate email account was successfully accessed in the last five days by an IP address located in a foreign country Which of the following attacks has MOST likely been used to compromise the manager\\'s corporate account?

A. Remote access Trojan

B. Brute-force

C. Dictionary

D. Credential stuffing

E. Password spraying

Correct Answer: D

"Credential stuffing is a type of cyberattack in which the attacker collects stolen account credentials, typically consisting of lists of usernames or email addresses and the corresponding passwords (often from a data breach), and then uses the credentials to gain unauthorized access to user accounts"

[SY0-601 VCE Dumps](#)   [SY0-601 Study Guide](#)   [SY0-601 Exam Questions](#)