DUMPSCOLLECTION
Build a Successful Future

CompTIA

SY0-601

CompTIA Security+ Exam 2023

Version: Demo

[Total Questions: 10]

Web: www.dumpscollection.com

Email: support@dumpscollection.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@dumpscollection.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@dumpscollection.com and our technical experts will provide support within 24 hours.

Copyright

Exam Topic Breakdown

Exam Topic	Number of Questions
Topic 1 : Exam Set 1	3
Topic 3 : Exam Set 3	3
Topic 4 : Exam Set 4	3
Topic 2 : Exam Set 2	1
TOTAL	10

Topic 1, Exam Set 1

Question #:1 - (Exam Topic 1)

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

Answer: D

Explanation

Reviewing the email event logs can support an investigation for fraudulent submission, as these logs can provide details about the history of emails, including the message content, timestamps, and sender/receiver information. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 3.2 Given a scenario, implement appropriate data security and privacy controls.

Question #:2 - (Exam Topic 1)

Which of the following disaster recovery tests is the LEAST time consuming for the disaster recovery team?

A. Tabletop

B. Parallel

C. Full interruption

D. Simulation

Answer: A

Explanation

A tabletop exercise is a type of disaster recovery test that simulates a disaster scenario in a discussion-based format, without actually disrupting operations or requiring physical testing of recovery procedures. It is the least time-consuming type of test for the disaster recovery team.

Question #:3 - (Exam Topic 1)

A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears.

The task list shows the following results

Name	CPU %	Memory	Network %
Calculator	0%	4.1MB	0Mbps
Chrome	0.2%	207.1MB	0.1Mbps
Explorer	99.7%	2.15GB	0.1Mbps
Notepad	0%	3.9MB	0Mbps

Which of the following is MOST likely the issue?

A. RAT

B. PUP

C. Spyware

D. Keylogger

Answer: C

Explanation

Spyware is malicious software that can cause a computer to slow down or freeze. It can also cause the mouse pointer to disappear. The task list shows an application named "spyware.exe" running, indicating that spyware is likely the issue. References:

- CompTIA Security+ Certification Exam Objectives 6.0: Given a scenario, analyze indicators of compromise and determine the type of malware.
- CompTIA Security+ Study Guide, Sixth Edition, pages 125-126

Topic 3, Exam Set 3

Question #:4 - (Exam Topic 3)

Which of the following describes the exploitation of an interactive process to gain access to restricted areas?

A. Persistence

B. Port scanning

C. Privilege escalation

D. Pharming

Answer: C

Explanation

Privilege escalation describes the exploitation of an interactive process to gain access to restricted areas. It is a type of attack that allows a normal user to obtain higher privileges or access rights on a system or network, such as administrative or root access. Privilege escalation can be achieved by exploiting a vulnerability, design flaw, or misconfiguration in the system or application. Privilege escalation can allow an attacker to perform unauthorized actions, such as accessing sensitive data, installing malware, or compromising other systems.
References:

- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/privilege-escalation-3/
- https://www.linkedin.com/learning/comptia-security-plus-sy0-601-cert-prep-2-secure-code-design-and-im

Question #:5 - (Exam Topic 3)

A user downloaded an extension for a browser, and the user's device later became infected. The analyst who Is Investigating the Incident saw various logs where the attacker was hiding activity by deleting data. The following was observed running:

New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter C| Format-Volume -Driveletter C -FileSystemLabel "New"-FileSystem NTFS - Full -Force -Confirm:$false

Which of the following is the malware using to execute the attack?

A. PowerShell

B. Python

C. Bash

D. Macros

Answer: A

Explanation

PowerShell is a scripting language and command-line shell that can be used to automate tasks and manage systems. PowerShell can also be used by malware to execute malicious commands and evade detection. The code snippet in the question is a PowerShell command that creates a new partition on disk 2, formats it with NTFS file system, and assigns it a drive letter C. This could be part of an attack that wipes out the original data on the disk or creates a hidden partition for storing malware or stolen data. References:

- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/scripting-and-automation/
- https://learn.microsoft.com/en-us/powershell/module/storage/new-partition?view=windowsserver2022-ps

Question #:6 - (Exam Topic 3)

Which of the following are common VoIP-associated vulnerabilities? (Select two).

A. SPIM

B. Vishing

C. VLAN hopping

D. Phishing

E. DHCP snooping

F. Tailgating

Answer: A B

Explanation

SPIM (Spam over Internet Messaging) is a type of VoIP-associated vulnerability that involves sending unsolicited or fraudulent messages over an internet messaging service, such as Skype or WhatsApp. It can trick users into clicking on malicious links, downloading malware, providing personal or financial information, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity. Vishing (Voice Phishing) is a type of VoIP-associated vulnerability that involves making unsolicited or fraudulent phone calls over an internet telephony service, such as Google Voice or Vonage. It can trick users into disclosing personal or financial information, following malicious instructions, transferring money, etc., by using voice spoofing, caller ID spoofing, or interactive voice response systems.

Topic 4, Exam Set 4

Question #:7 - (Exam Topic 4)

An organization relies on third-party videoconferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources Which of the following would best maintain high-quality videoconferencing while minimizing latency when connected to the VPN?

A. Using geographic diversity lo have VPN terminators closer to end users

B. Utilizing split tunneling so only traffic for corporate resources is encrypted

C. Purchasing higher bandwidth connections to meet the increased demand

D. Configuring OoS properly on the VPN accelerators

Answer: B

Explanation

Utilizing split tunneling so only traffic for corporate resources is encrypted would best maintain high-quality videoconferencing while minimizing latency when connected to the VPN. Split tunneling is a technique that allows a VPN user to access both the public internet and the private network simultaneously, without routing all traffic through the VPN. This can improve the performance and quality of videoconferencing applications that rely on low latency and high bandwidth, as well as reduce the load on the VPN server.

Question #:8 - (Exam Topic 4)

A security analyst receives a SIEM alert that someone logged in to the app admin 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. A replay attack is being conducted against the application.

B. An injection attack is being conducted against a user authentication system.

C. A service account password may have been changed, resulting in continuous failed logins within the application.

D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Answer: A

Explanation

A replay attack is a type of network attack where an attacker captures and retransmits a valid data transmission, such as a login request, to gain unauthorized access or impersonate a legitimate user. In this case, the attacker may have captured the credentials of the app admin test account and used them to log in to the application. The application log shows multiple failed login attempts from different IP addresses, which indicates a replay attack.

Question #:9 - (Exam Topic 4)

A security analyst has been reading about a newly discovered cyberattack from a known threat actor Which of the following would best support the analyst's review of the tactics, techniques, and protocols the throat actor was observed using in previous campaigns?

A. Security research publications

B. The MITRE ATT4CK framework

C. The Diamond Model of Intrusion Analysis

D. The Cyber Kill Cham

Answer: B

Explanation

The MITRE ATT&CK framework would best support the analyst's review of the tactics, techniques, and procedures (TTPs) the threat actor was observed using in previous campaigns. The MITRE ATT&CK framework is a knowledge base that describes the common TTPs used by various threat actors across different stages of an attack lifecycle. The framework can help security analysts understand how adversaries operate, what tools they use, what vulnerabilities they exploit, what indicators they leave behind, etc. The framework can also help security analysts improve their detection and response capabilities by providing recommendations and best practices.

Topic 2, Exam Set 2

Question #:10 - (Exam Topic 2)

A security engineer updated an application on company workstations. The application was running before the update, but it is no longer launching successfully. Which of the following most likely needs to be updated?

A. Blocklist

B. Deny list

C. Quarantine list

D. Approved fist

Answer: D

Explanation

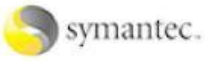
Approved list is a list of applications or programs that are allowed to run on a system or network. An approved list can prevent unauthorized or malicious software from running and compromising the security of the system or network. An approved list can also help with patch management and compatibility issues. If the security engineer updated an application on the company workstations, the application may need to be added or updated on the approved list to be able to launch successfully. References: **1** CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security **2** CompTIA Security+ Certification Exam Objectives, page 12, Domain 3.0: Implementation, Objective 3.1: Implement secure network architecture concepts **3** https://www.comptia.org/blog/what-is-application-whitelisting

About dumpscollection.com

dumpscollection.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- Sales: sales@dumpscollection.com
- Feedback: feedback@dumpscollection.com
- Support: support@dumpscollection.com
- Skype ID: crack4sure@gmail.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.

15% Discount Coupon Code:

DC15disc