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.certbus.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An application owner has requested access for an external application to upload data from the central internal website without providing credentials at any point. Which of the following authentication methods should be configured to allow this type of integration access?

A. OAuth

B. SSO

C. TACACS+

D. Kerberos

Correct Answer: B

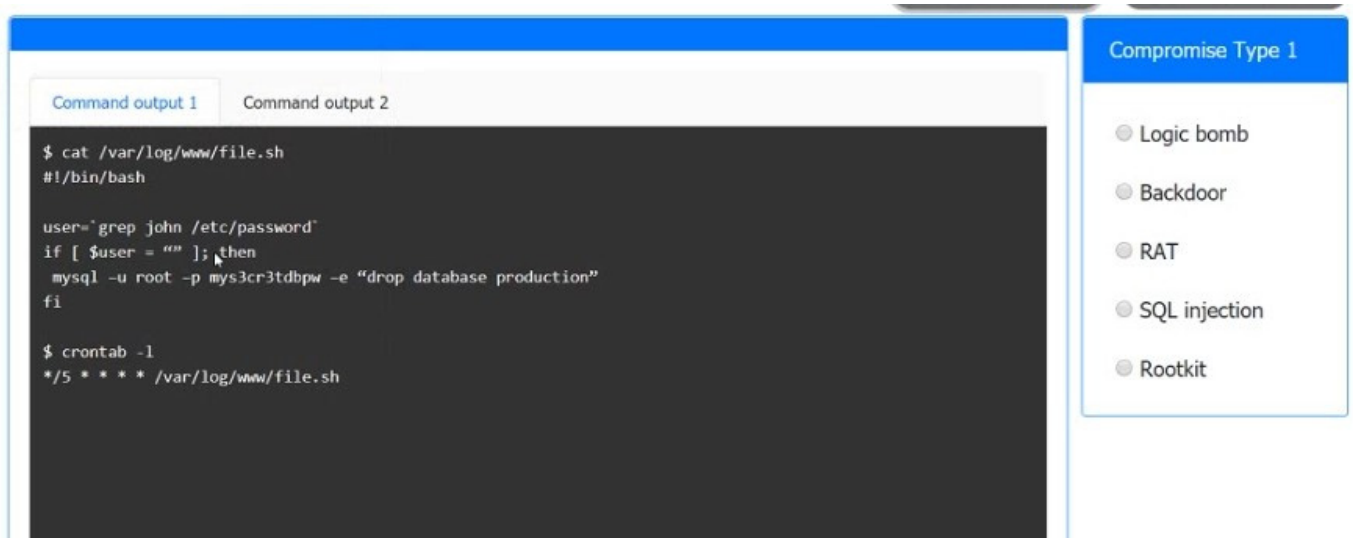
QUESTION 2

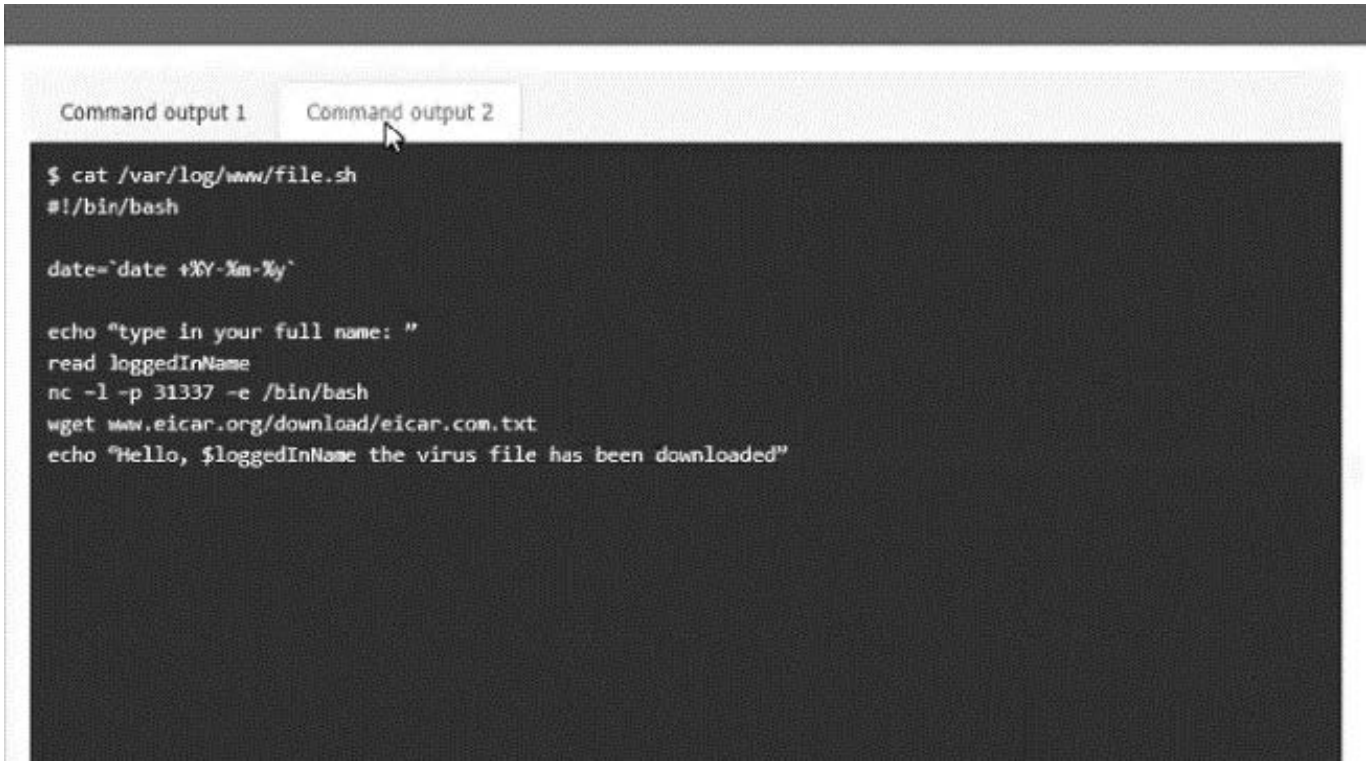
CORRECT TEXT

An incident has occurred in the production environment.

Analyze the command outputs and identify the type of compromise.

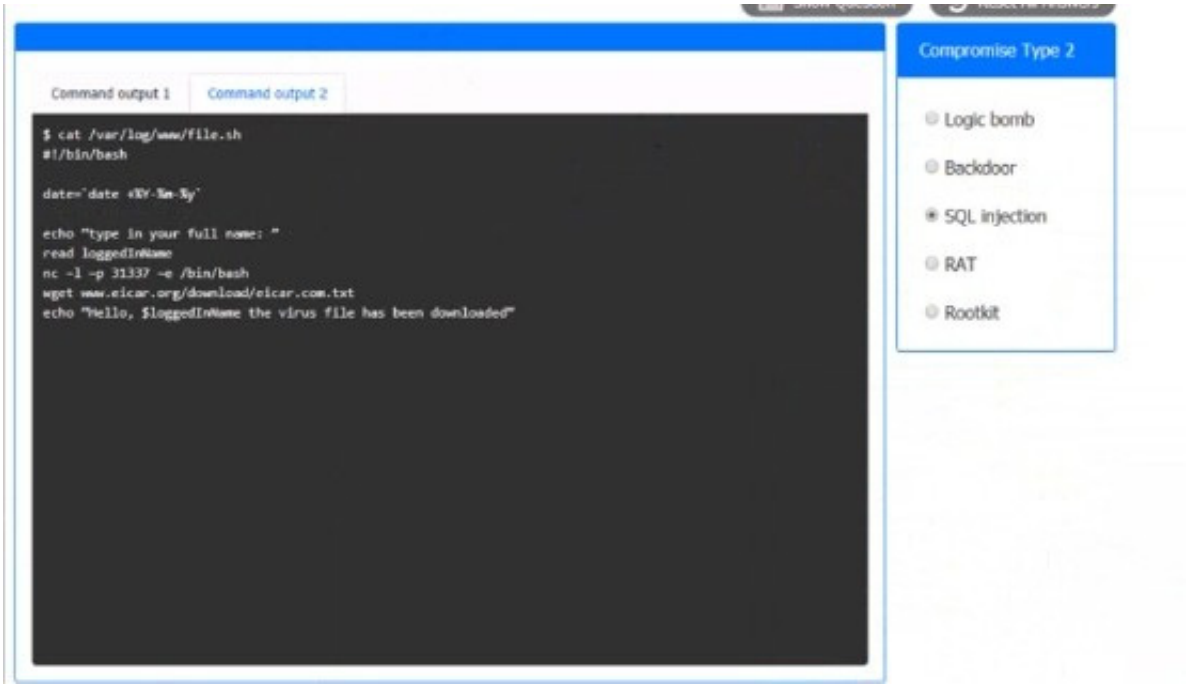
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Correct Answer:

Answer as SQL injection



QUESTION 3

Business partners are working on a secunty mechanism lo validate transactions securely. The requirement is for one company to be responsible for deploying a trusted solution that will register and issue artifacts used to sign encrypt, and decrypt transaction files.

Which of the following is the BEST solution to adopt?

A. PKI

B. Blockchain

C. SAML

D. OAuth

Correct Answer: A

Ref the following: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786417(v=ws.11)

QUESTION 4

Which of the following best describes the process of adding a secret value to extend the length of stored passwords?

A. Hashing

B. Quantum communications

C. Salting

D. Perfect forward secrecy

Correct Answer: C

QUESTION 5

A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which f the following configuration should an analysis enable To improve security? (Select TWO.)

A. RADIUS

B. PEAP

C. WPS

D. WEP-EKIP

E. SSL

F. WPA2-PSK

Correct Answer: AF

WPA2-PSK: WPA works using discrete modes for enterprise and personal use.

The most recent enterprise mode, WPA-EAP, uses a stringent 802.1x authentication.

The latest personal mode, WPA-PSK, uses Simultaneous Authentication of Equals (SAE) to create a secure handshake.

QUESTION 6

Which of the following risk management strategies would an organization use to maintain a legacy system with known risks for operational purposes?

A. Acceptance

B. Transference

C. Avoidance

D. Mitigation

Correct Answer: A

The key word in the question is "Legacy". Legacy equipment is no longer supported by the vendor, which means no new patches will ever be released for this equipment again, there is no mitigation here. If a company is using legacy equipment with known risks, they have accepted those risks.

QUESTION 7

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

A. Insurance

B. Patching

C. Segmentation

D. Replacement

Correct Answer: C

If support from the manufacturer is not available, and the vulnerability is in the OS of legacy IoT devices, the best option to quickly mitigate the vulnerability is C. Segmentation. Since patching may not be feasible without manufacturer support, segmentation can help isolate the vulnerable devices from the rest of the network. This can limit the potential attack surface and reduce the risk of exploitation, even if the devices themselves cannot be patched or updated. Segmentation can be an effective short-term strategy to enhance security when dealing with unsupported legacy IoT devices.If support from the manufacturer is not available, and the vulnerability is in the OS of legacy IoT devices, the best option to quickly mitigate the vulnerability is C. Segmentation.

Since patching may not be feasible without manufacturer support, segmentation can help isolate the vulnerable devices from the rest of the network. This can limit the potential attack surface and reduce the risk of exploitation, even if the devices themselves cannot be patched or updated.

QUESTION 8

A company wants to begin taking online orders for products but has decided to outsource payment processing to limit risk. Which of the following best describes what the company should request from the payment processor?

A. ISO 27001 certification documents

B. Proof of PCI DSS compliance

C. A third-party SOC 2 Type 2 report

D. Audited GDPR policies

Correct Answer: B

QUESTION 9

A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO).

A. The order of volatility

B. A CRC32 checksum

C. The provenance of the artifacts

D. The vendor\\'s name

E. The date time

F. A warning banner

Correct Answer: CE

Date and time of collection Location of collection Name of investigator(s) Name or owner of the media or computer Reason for collection Matter name or case number Type of media Serial number of media if available Make and model of hard drive or other media Storage capacity of device or hard drive Method of capture (tools used) Physical description of computer and whether it was on or off Name of the image file or resulting files that were collected Hash value(s) of source hard drive or files Hash value(s) of resulting image files for verification Any comments or issues encountered Signature(s) of persons giving and taking possession of evidence

QUESTION 10

An analyst is reviewing an incident in which a user clicked on a link in a phishing email. Which of the following log sources would the analyst utilize to determine whether the connection was successful?

A. Network

B. System

C. Application

D. Authentication

Correct Answer: A

Network log sources can show the traffic between the user\\'s device and the phishing website, such as DNS queries, the IP addresses, the port, and the protocols. Network logs can also reveal if the connection was blocked by a firewall or other security tools

QUESTION 11

Which of the following procedures would be performed after the root cause of a security incident has been identified to help avoid future incidents from occurring?

A. Walk-throughs

B. Lessons learned

C. Attack framework alignment

D. Containment

Correct Answer: B

After the root cause of a security incident has been identified, it is important to take the time to analyze what went wrong and how it could have been prevented. This process is known as "lessons learned" and allows organizations to identify potential improvements to their security processes and protocols. Lessons learned typically involve a review of the incident and the steps taken to address it, a review of the security systems and procedures in place, and an analysis of

any potential changes that can be made to prevent similar incidents from occurring in the future.

QUESTION 12

Recent changes to a company\\'s BYOD policy require all personal mobile devices to use a two-factor authentication method that is not something you know or have. Which of the following will meet this requirement?

A. Facial recognition

B. Six-digit PIN

C. PKI certificate

D. Smart card

Correct Answer: A

Facial recognition is a form of biometric authentication, which falls under the "something you are" factor. It uses unique facial features to authenticate a user, making it a form of authentication that is based on physical characteristics rather than something you know (like a password) or have (like a smart card).

QUESTION 13

A company is setting up a web server on the Internet that will utilize both encrypted and unencrypted web-browsing protocols. A security engineer runs a port scan against the server from the Internet and sees the following output:

Port	Protocol	State	Service
22	tcp	open	ssh
25	tcp	filtered	smtp
53	tcp	filtered	domain
80	tcp	open	http
443	tcp	open	https

Which of the following steps would be best for the security engineer to take NEXT?

A. Allow DNS access from the internet.

B. Block SMTP access from the Internet

C. Block HTTPS access from the Internet

D. Block SSH access from the Internet.

Correct Answer: D

The reason for D is because you want to block the SSH as it will be a vulnerability.

QUESTION 14

An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the incident could have been prevented?

A. The vulnerability scan output

B. The security logs

C. The baseline report

D. The correlation of events

Correct Answer: B

QUESTION 15

A security analyst needs to propose a remediation plan for each item in a risk register. The item with the highest priority requires employees to have separate logins for SaaS solutions and different password complexity requirements for each solution. Which of the following implementation plans will most likely resolve this security issue?

A. Creating a unified password complexity standard

B. Integrating each SaaS solution with the identity provider

C. Securing access to each SaaS by using a single wildcard certificate

D. Configuring geofencing on each SaaS solution

Correct Answer: B