Free Cisco 350-201 CBRCOR Practice Questions

Shared by Glover on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The physical security department received a report that an unauthorized person followed an authorized individual to enter a secured premise. The incident was documented and given to a security specialist to analyze. Which step should be taken at this stage?

Options:

A- Determine the assets to which the attacker has access
B- Identify assets the attacker handled or acquired
C- Change access controls to high risk assets in the enterprise
D- Identify movement of the attacker in the enterprise

Answer:

D

Question 2

Question Type: MultipleChoice

Which command does an engineer use to set read/write/execute access on a folder for everyone who reaches the resource?

Options:

A- chmod 666
B- chmod 774
C- chmod 775
D- chmod 777

Answer:

D

Question 3

Question Type: MultipleChoice

What is the difference between process orchestration and automation?

Options:

A- Orchestration combines a set of automated tools, while automation is focused on the tools to automate process flows.
B- Orchestration arranges the tasks, while automation arranges processes.
C- Orchestration minimizes redundancies, while automation decreases the time to recover from redundancies.
D- Automation optimizes the individual tasks to execute the process, while orchestration optimizes frequent and repeatable processes.

Answer:

A

Question 4

Question Type: MultipleChoice

An analyst wants to upload an infected file containing sensitive information to a hybrid-analysis sandbox. According to the NIST.SP 800-150 guide to cyber threat information sharing, what is the analyst required to do before uploading the file to safeguard privacy?

Options:

A- Verify hash integrity.
B- Remove all personally identifiable information.
C- Ensure the online sandbox is GDPR compliant.
D- Lock the file to prevent unauthorized access.

Answer:

B

Question 5

Question Type: MultipleChoice

A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format file was created in the system directory. What is the next step the analyst should take?

Options:

A- Isolate the server and perform forensic analysis of the file to determine the type and vector of a possible attack
B- Identify the server owner through the CMDB and contact the owner to determine if these were planned and identifiable activities
C- Review the server backup and identify server content and data criticality to assess the intrusion risk
D- Perform behavioral analysis of the processes on an isolated workstation and perform cleaning procedures if the file is malicious

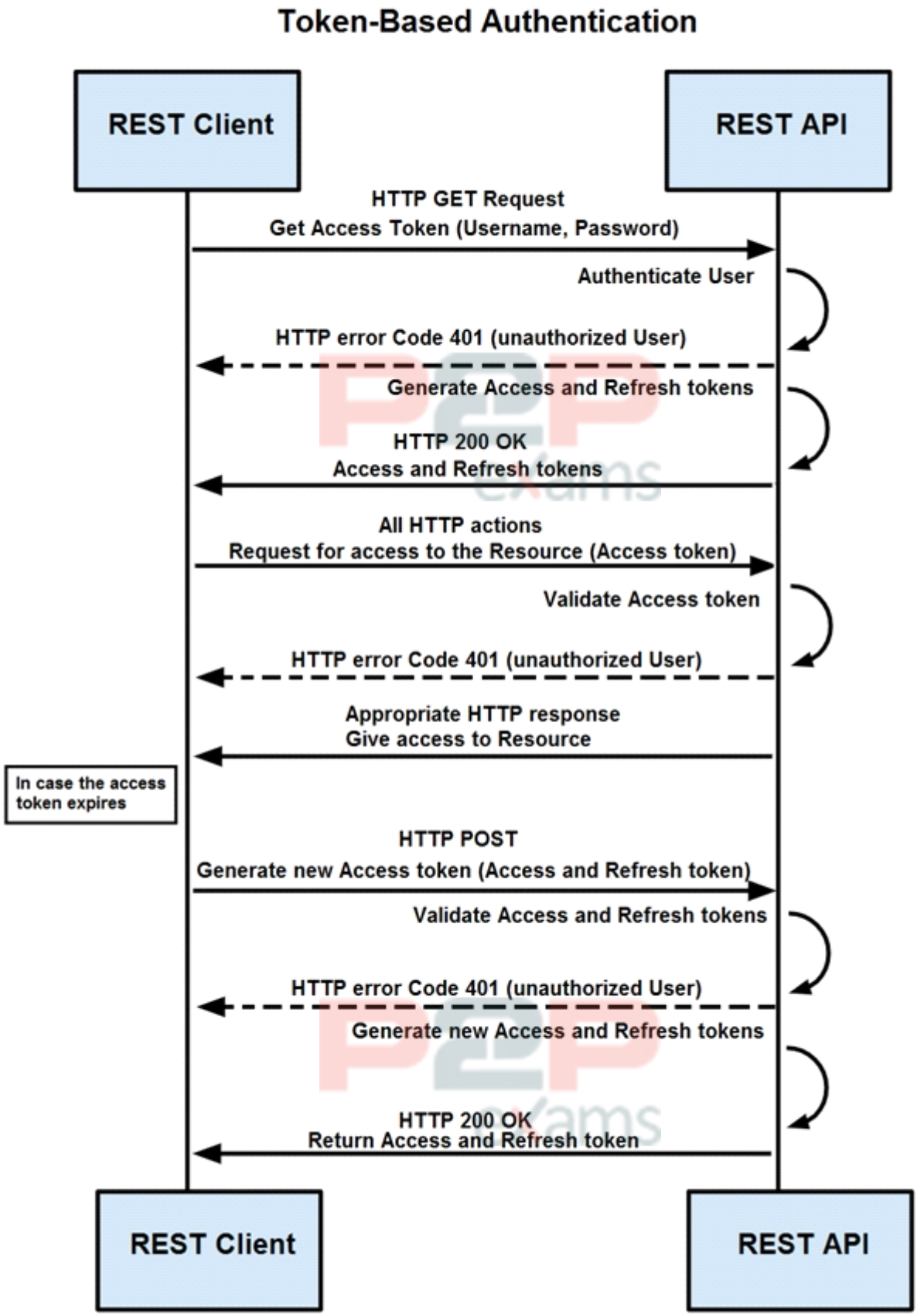
Answer:

C

Question 6

Question Type: MultipleChoice

Refer to the exhibit.



How are tokens authenticated when the REST API on a device is accessed from a REST API client?

Options:

A- The token is obtained by providing a password. The REST client requests access to a resource using the access token. The REST API validates the access token and gives access to the resource.
B- The token is obtained by providing a password. The REST API requests access to a resource using the access token, validates the access token, and gives access to the resource.
C- The token is obtained before providing a password. The REST API provides resource access, refreshes
tokens, and returns them to the REST client. The REST client requests access to a resource using the access token.
D- The token is obtained before providing a password. The REST client provides access to a resource using the access token. The REST API encrypts the access token and gives access to the resource.

Answer:

D

Question 7

Question Type: MultipleChoice

An engineer receives a report that indicates a possible incident of a malicious insider sending company information to outside parties. What is the first action the engineer must take to determine whether an incident has occurred?

Options:

A- Analyze environmental threats and causes
B- Inform the product security incident response team to investigate further
C- Analyze the precursors and indicators
D- Inform the computer security incident response team to investigate further

Answer:

C

Question 8

Question Type: MultipleChoice

What is the HTTP response code when the REST API information requested by the

authenticated user cannot be found?

Options:

A- 401
B- 402
C- 403
D- 404
E- 405

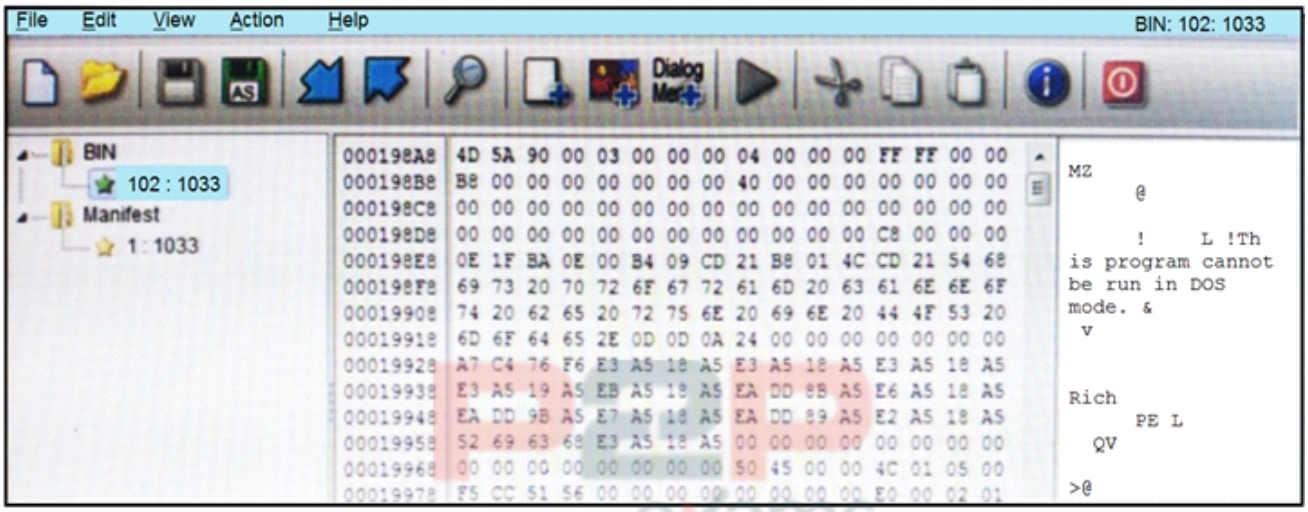
Answer:

A

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

Options:

A- a DOS MZ executable format
B- a MS-DOS executable archive
C- an archived malware
D- a Windows executable file

Answer:

D

Question 10

Question Type: MultipleChoice

An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight. Which type of compromise is indicated?

Options:

A- phishing
B- dumpster diving
C- social engineering
D- privilege escalation

Answer:

C

Question 11

Question Type: MultipleChoice

An engineer receives an incident ticket with hundreds of intrusion alerts that require investigation. An analysis of the incident log shows that the alerts are from trusted IP addresses and internal devices. The final incident report stated that these alerts were false positives and that no intrusions were detected. What action should be taken to harden the network?

Options:

A- Move the IPS to after the firewall facing the internal network
B- Move the IPS to before the firewall facing the outside network
C- Configure the proxy service on the IPS
D- Configure reverse port forwarding on the IPS

Answer:

C

P2P exams