CS0-003Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.pass2lead.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

HOTSPOT

The developers recently deployed new code to three web servers. A daily automated external device scan report shows server vulnerabilities that are failing items according to PCI DSS.

If the vulnerability is not valid, the analyst must take the proper steps to get the scan clean.

If the vulnerability is valid, the analyst must remediate the finding.

After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

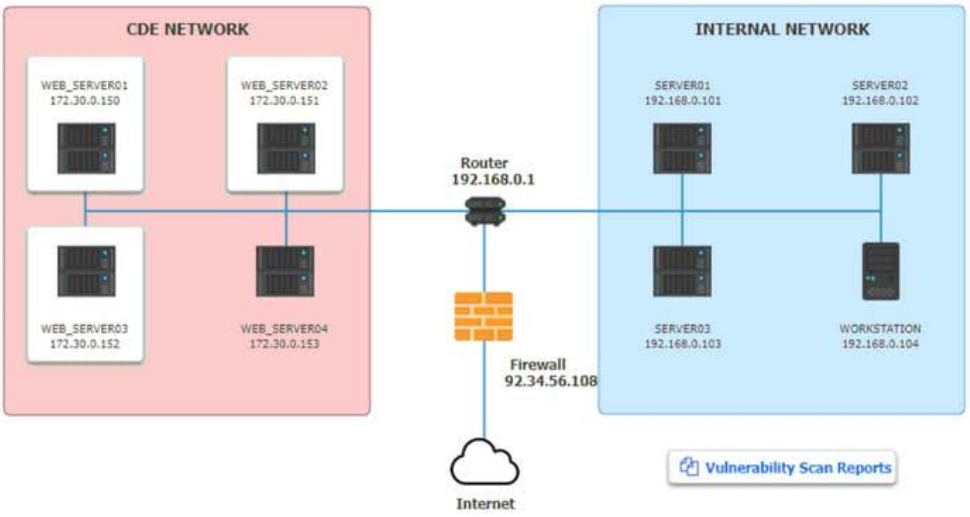
INSTRUCTIONS

STEP 1: Review the information provided in the network diagram.

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

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

Step 1



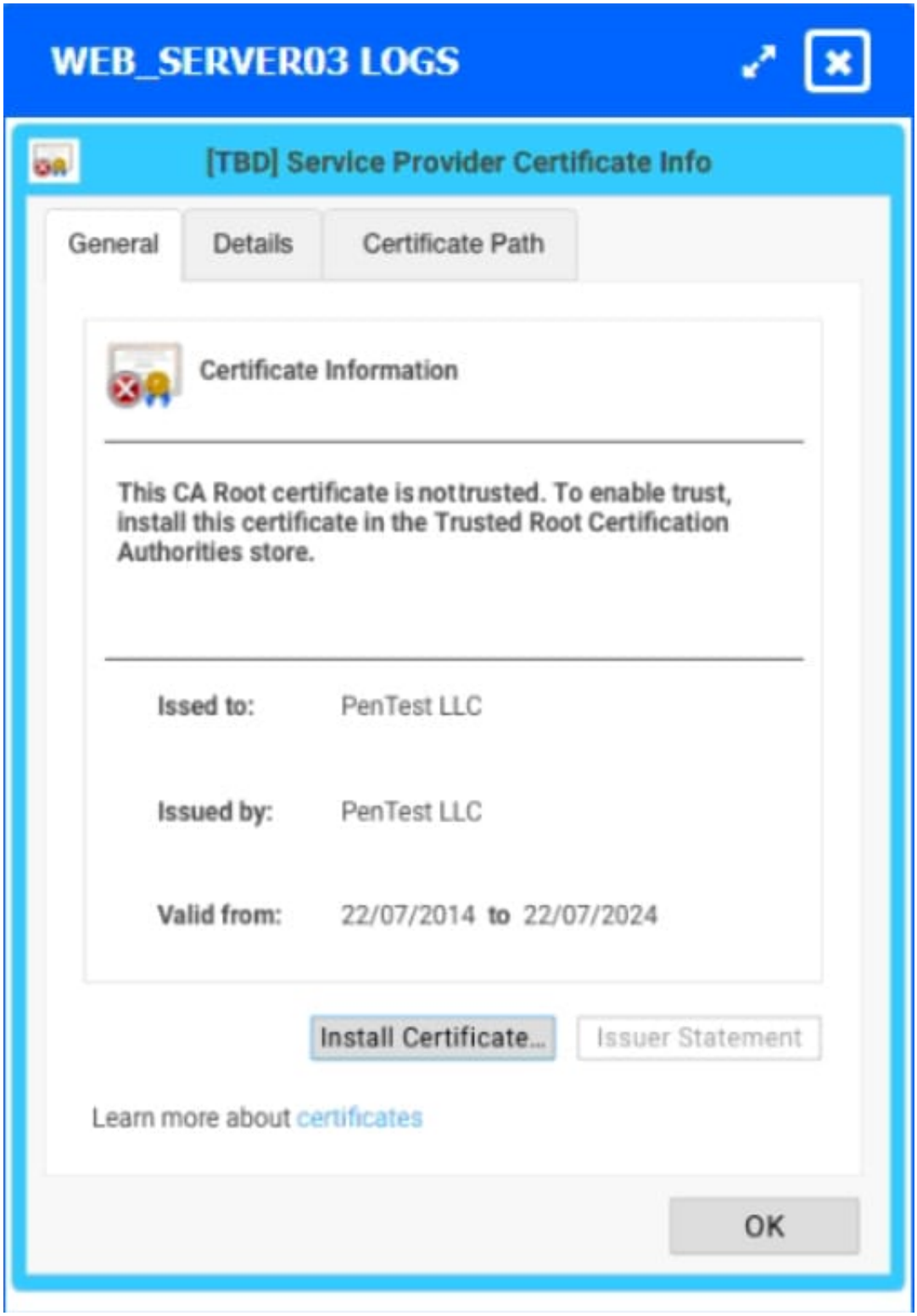
WEB_SERVER01 LOGS

```
While logged in to the web portal (172.30.0.150) from the workstation (192.168.0.104), perform an account
password change.  This process requires you to reenter the original password and enter a new password
twice.


192.168.0.104    172.30.0.151    TLSv1     733    Application Data
172.30.0.151     192.168.0.104   TLSv1    1107    Application Data
192.168.0.104    172.30.0.151    TCP        66    44088 > https   [ACK]  Seq=1510 Ack=12723  Win=42368
192.168.0.104    172.30.0.150    HTTP      608    GET  /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
172.30.0.151     192.168.0.104   TCP        66    http > 60928  [ACK]  Seq=622  Ack=847  Win=5154  Len=…


Frame  4021:  114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src:  Vmware 00:03:22  (00:50:56:00:03:22),  Dst:  PaloAlto_39:1c:30  (00:1b:17:39:1c:30)
Internet Protocol Version 4, Src:  192.168.0.104 (192.168.0.104), Dst:  172.30.0.150 (172.30.0.150)
[2 Reassembled  TCP  Segments  (1496 bytes):  #4820(1448), #4821(48)]
Hypertext  Transfer  Protocol
    GET  /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
    Host:  XXXXX
    User - Agent:  Mozilla/5.0  (x11;  Linux  x86_64;  rv:18.0)  Gecko/20100101  Firefox/18.0
Iceweasel/18.0.1
    Accept:  text/html, application/xhtml+xml,application/xml;q=0.9,*/*;q=0
    Accept-Language:  en=US,en;q=0.5
    Accept-Encoding:  gzip,  deflate
    Referer:  http:/XXXXX/Shared/Portal/CustomProfiles/A_Profile.real
    [truncated]  Cookie:  ASPSESSIONIDQABRBT BC=HEJCAHEDJPK08CEP; ZZZ; ECUSERPROPS=
    Connection:  keep alive
    Content-Type:  application/x-www-form-urlendcoded
    Content-Length:  121

    [Full  request  URI:  http//XXX/Shared/Portal/CustomProfiles/PostProfile.real?47=25378158]
Line-based   text  data:  application/x-www-form-urlencoded
    EMAIL=someone@cloud.org m&PASSold=PassWord1  m&PASSnew1=PassWord2  m&PASSnewv=PassWord2
```

WEB_SERVER02 LOGS

Cookies

Name	Value	Domain	...	Expires / Max Age	...	Http	Secure
_utma	250288278.1028202552.1383963...	yourcompany.com	...	Thu, 05 Nov 2015 23:21:28 GMT	...		X
_utmb	250288278.2.10.1383693377	yourcompany.com	...	Tue, 05 Nov 2013 23:51:28 GMT	...		X
_utmc	250288278	yourcompany.com	...	Session	...		X
_utmz	250288278.1383693377.1.1.utmcs	yourcompany.com	...	Thu, 08 May 2014 11:21:28 GMT	...		X



Hot Area:

Correct Answer:

Validate Result	Remediation Action
WEB_SERVER01	WEB_SERVER01
False Positive	Encrypt Entire Session
False Negative	Encrypt All Session Cookies
True Negative	Implement Input Validation
True Positive	Submit as Non-Issue
	Employ Unique Token in Hidden Field
	Avoid Using Redirects and Forwards
	Disable HTTP
	Request Certificate from a Public CA
	Renew the Current Certificate
WEB_SERVER02	WEB_SERVER02
False Positive	Encrypt Entire Session
False Negative	Encrypt All Session Cookies
True Negative	Implement Input Validation
True Positive	Submit as Non-Issue
	Employ Unique Token in Hidden Field
	Avoid Using Redirects and Forwards
	Disable HTTP
	Request Certificate from a Public CA
	Renew the Current Certificate
WEB_SERVER03	WEB_SERVER03
False Positive	Encrypt Entire Session
False Negative	Encrypt All Session Cookies
True Negative	Implement Input Validation
True Positive	Submit as Non-Issue
	Employ Unique Token in Hidden Field
	Avoid Using Redirects and Forwards
	Disable HTTP
	Request Certificate from a Public CA
	Renew the Current Certificate

Validate Result	Remediation Action
WEB_SERVER01	WEB_SERVER01
False Positive	Encrypt Entire Session
False Negative	Encrypt All Session Cookies
True Negative	Implement Input Validation
True Positive	Submit as Non-Issue
	Employ Unique Token in Hidden Field
	Avoid Using Redirects and Forwards
	Disable HTTP
	Request Certificate from a Public CA
	Renew the Current Certificate
WEB_SERVER02	WEB_SERVER02
False Positive	Encrypt Entire Session
False Negative	Encrypt All Session Cookies
True Negative	Implement Input Validation
True Positive	Submit as Non-Issue
	Employ Unique Token in Hidden Field
	Avoid Using Redirects and Forwards
	Disable HTTP
	Request Certificate from a Public CA
	Renew the Current Certificate
WEB_SERVER03	WEB_SERVER03
False Positive	Encrypt Entire Session
False Negative	Encrypt All Session Cookies
True Negative	Implement Input Validation
True Positive	Submit as Non-Issue
	Employ Unique Token in Hidden Field
	Avoid Using Redirects and Forwards
	Disable HTTP
	Request Certificate from a Public CA
	Renew the Current Certificate

QUESTION 2

A security team is struggling with alert fatigue, and the Chief Information Security Officer has decided to purchase a SOAR platform to alleviate this issue. Which of the following BEST describes how a SOAR platform will help the security team?

A. SOAR will integrate threat intelligence into the alerts, which will help the security team decide which events should be investigated first.

B. A SOAR platform connects the SOC with the asset database, enabling the security team to make informed decisions immediately based on asset criticality.

C. The security team will be able to use the SOAR framework to integrate the SIEM with a TAXII server, which has an automated intelligence feed that will enhance the alert data.

D. Logic can now be created that will allow the SOAR platform to block specific traffic at the firewall according to predefined event triggers and actions.

Correct Answer: A

QUESTION 3

A security analyst must preserve a system hard drive that was involved in a litigation request

Which of the following is the best method to ensure the data on the device is not modified?

A. Generate a hash value and make a backup image.

B. Encrypt the device to ensure confidentiality of the data.

C. Protect the device with a complex password.

D. Perform a memory scan dump to collect residual data.

Correct Answer: A

Generating a hash value and making a backup image is the best method to ensure the data on the device is not modified, as it creates a verifiable copy of the original data that can be used for forensic analysis. Encrypting the device, protecting it with a password, or performing a memory scan dump do not prevent the data from being altered or deleted. Verified References: CompTIA CySA+ CS0-002 Certification Study Guide, page 3291

QUESTION 4

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

A. Uncredentialed scan

B. Discovery scan

C. Vulnerability scan

D. Credentialed scan

Correct Answer: B

A discovery scan is typically used to identify the scope of a web application and understand where the scan will go. This type of scan is often the first step in assessing a web application\\'s security and helps the analyst determine which areas

should be further examined or tested in-depth.

Reference: https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/scans/scanning_basics.htm

QUESTION 5

A security analyst who works in the SOC receives a new requirement to monitor for indicators of compromise. Which of the following is the first action the analyst should take in this situation?

A. Develop a dashboard to track the indicators of compromise.

B. Develop a query to search for the indicators of compromise.

C. Develop a new signature to alert on the indicators of compromise.

D. Develop a new signature to block the indicators of compromise.

Correct Answer: B