CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.geekcert.com/cs0-002.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

A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

Antivirus is installed on the remote host:

Installation path: C:\Program Files\AVProduct\Win32\

Product Engine: 14.12.101

Engine Version: 3.5.71

Scanner does not currently have information about AVProduct version 3.5.71.

It may no longer be supported.

The engine version is out of date. The oldest supported version from the vendor is 4.2.11.

The analyst uses the vendor\\'s website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

A. This is a false positive and the scanning plugin needs to be updated by the vendor

B. This is a true negative and the new computers have the correct version of the software

C. This is a true positive and the new computers were imaged with an old version of the software

D. This is a false negative and the new computers need to be updated by the desktop team

Correct Answer: C

QUESTION 2

HOTSPOT

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

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

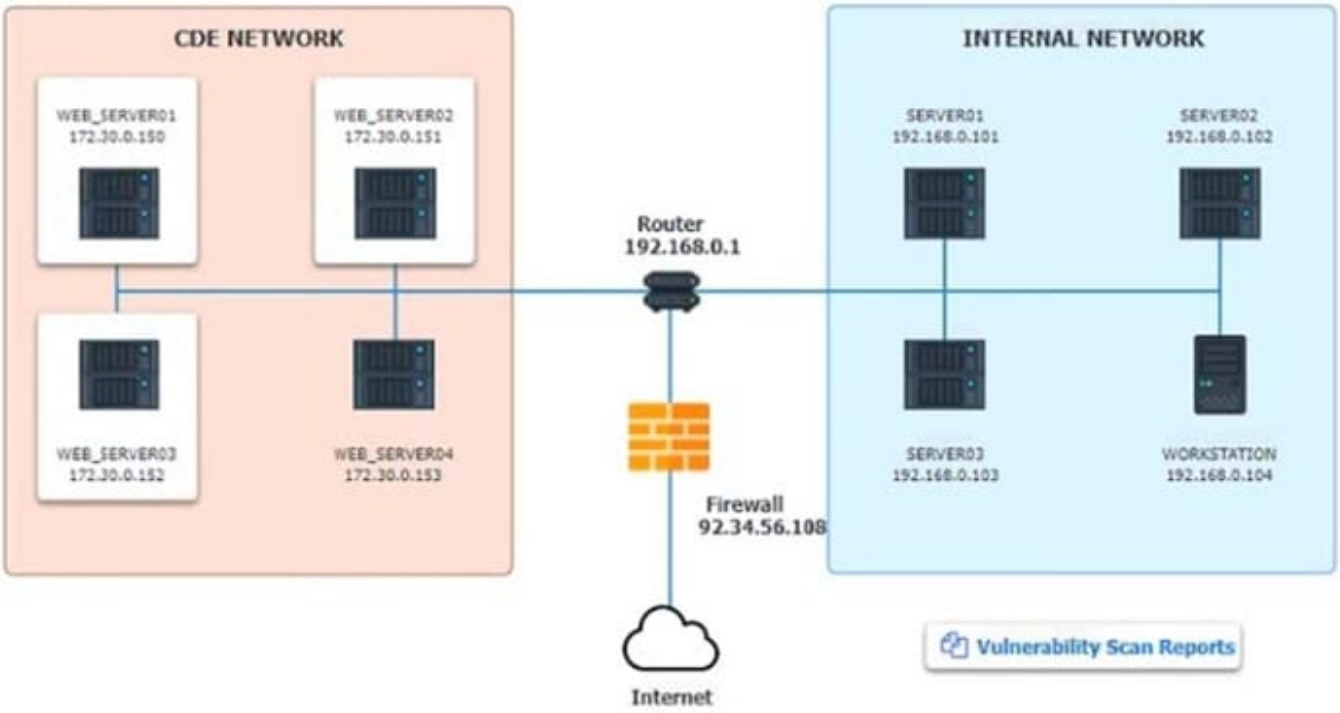
If the venerability is valid, the analyst must remediate the finding.

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.

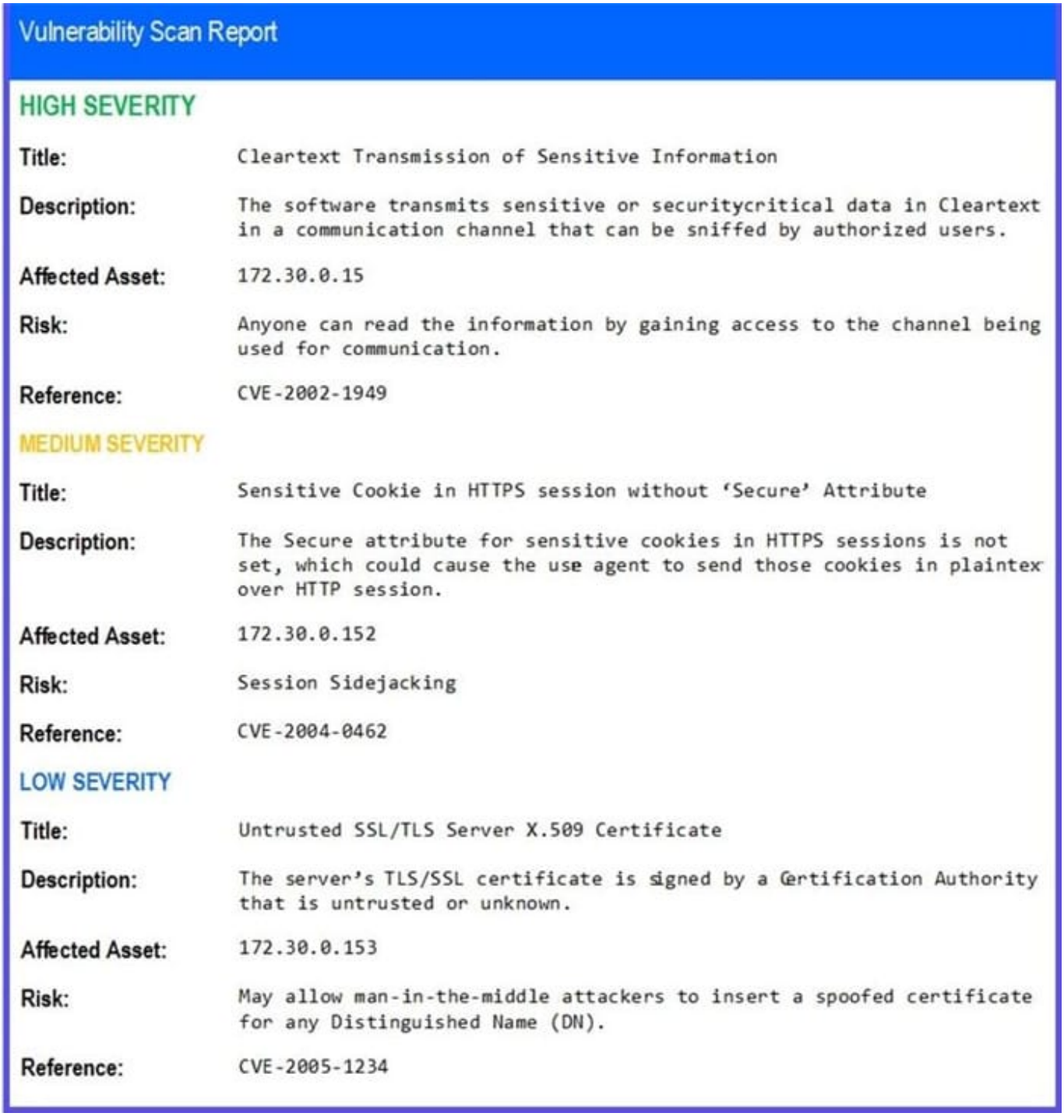
INTRUCTIONS:

The simulation includes 2 steps.

Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.



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



Vulnerability Scan Report

HIGH SEVERITY

Title:	Cleartext Transmission of Sensitive Information
Description:	The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected Asset:	172.30.0.15
Risk:	Anyone can read the information by gaining access to the channel being used for communication.
Reference:	CVE-2002-1949

MEDIUM SEVERITY

Title:	Sensitive Cookie in HTTPS session without 'Secure' Attribute
Description:	The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the use agent to send those cookies in plaintex over HTTP session.
Affected Asset:	172.30.0.152
Risk:	Session Sidejacking
Reference:	CVE-2004-0462

LOW SEVERITY

Title:	Untrusted SSL/TLS Server X.509 Certificate
Description:	The server's TLS/SSL certificate is signed by a Certification Authority that is untrusted or unknown.
Affected Asset:	172.30.0.153
Risk:	May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).
Reference:	CVE-2005-1234

Hot Area:

Network Diagram

INSTRUCTIONS

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

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation 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	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation 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	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation 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

Correct Answer:

Network Diagram

INSTRUCTIONS

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

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative **True Positive** True Negative	**Encrypt Entire Session** Encrypt All Session Cookies Implement Input Validation 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	False Positive False Negative **True Positive** True Negative	Encrypt Entire Session **Encrypt All Session Cookies** Implement Input Validation 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	False Positive False Negative **True Positive** True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation 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 3

A cyber incident response team finds a vulnerability on a company website that allowed an attacker to inject malicious code into its web application. There have been numerous unsuspecting users visiting the infected page, and the malicious code executed on the victim\\'s browser has led to stolen cookies, hijacked sessions, malware execution, and bypassed access control. Which of the following exploits is the attacker conducting on the company\\'s website?

A. Logic bomb

B. Rootkit

C. Privilege escalation

D. Cross-site scripting

Correct Answer: D

QUESTION 4

A security analyst is required to stay current with the most recent threat data and intelligence reports. When gathering data, it is MOST important for the data to be:

A. proprietary and timely

B. proprietary and accurate

C. relevant and deep

D. relevant and accurate

Correct Answer: D

QUESTION 5

A product security analyst has been assigned to evaluate and validate a new products security capabilities Part ot the evaluation involves reviewing design changes at specific intervals tor security deficiencies recommending changes and checking for changes at the next checkpoint.

Which of the following BEST defines the activity being conducted?

A. User acceptance testing

B. Stress testing

C. Code review

D. Security regression testing

Correct Answer: C

Once the SDLC reached the development phase, code starts to be generated. That means that the ability to control the version of the software or component that your team is working on, combined with check-in/check-out functionality and

revision histories, is a necessary and powerful tool when developing software.

The question refers to a "new" product so I believe that is key. However, it also makes it seem that it is about the development of a product that could be in production.

Regression testing focuses on testing to ensure that changes that have been made do not create new issues, and ensure that no new vulnerabilities, misconfigurations, or other issues have been introduced.