CS0-003 Q&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.passapply.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

A security analyst performs various types of vulnerability scans.

Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

INSTRUCTIONS

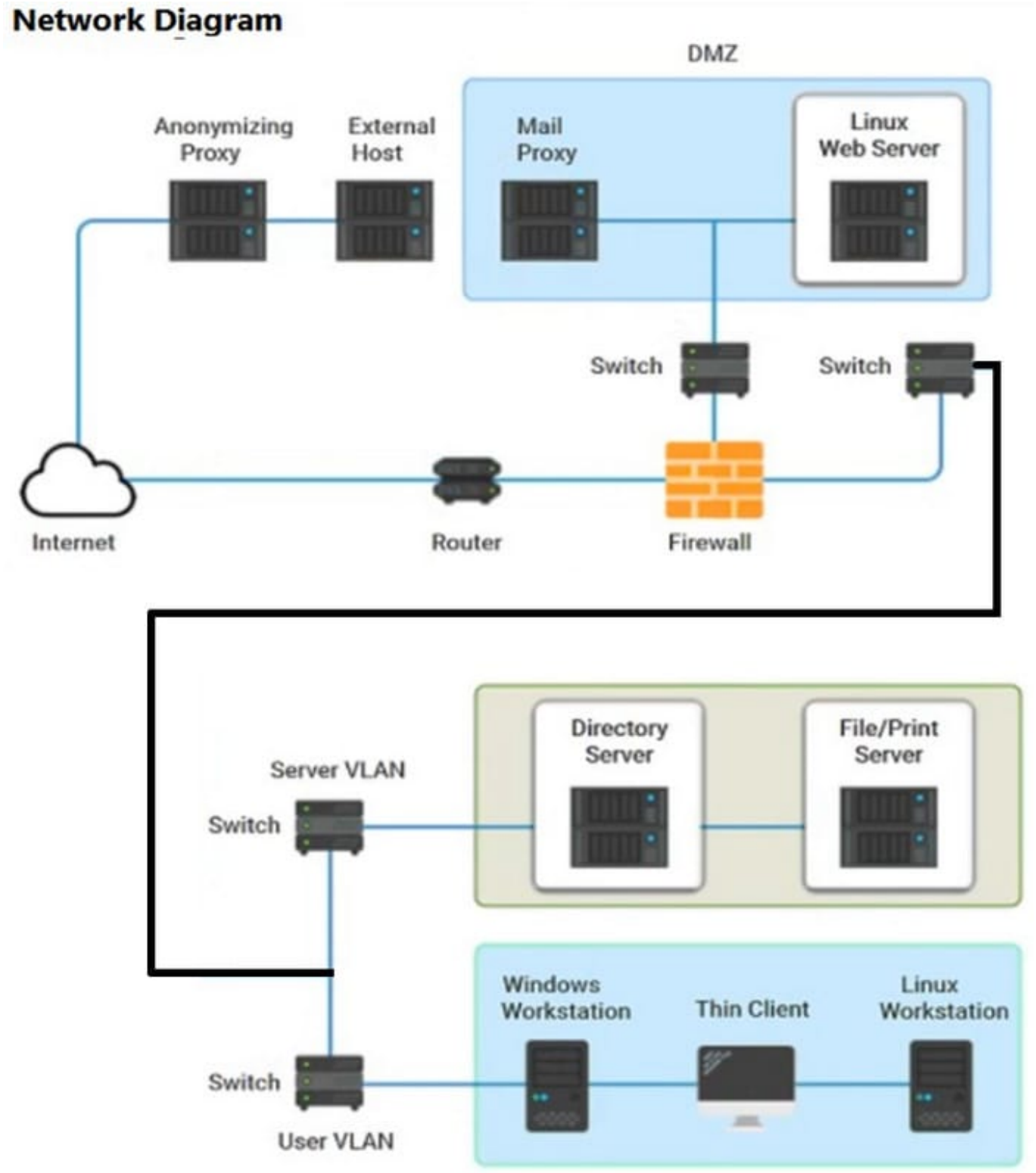
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

For ONLY the credentialed and non-credentialed scans, evaluate the results for False Positives and check the Findings that display false positives.

NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server, and Directory Server are draggable.

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


Network Diagram
DMZ
Anonymizing Proxy
External Host
Mail Proxy
Linux Web Server
Switch
Switch
Internet
Router
Firewall
Server VLAN
Switch
Directory Server
File/Print Server
Windows Workstation
Thin Client
Linux Workstation
Switch
User VLAN

Hot Area:

Findings Listing 1

Critical (10.0) 12209 Security Update for Microsoft Windows (835732)
Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
Critical (10.0) 58662 Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows (20161146)
Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated

- Credentialed
- Non-Credentialed
- Compliance

Findings Listing 2

Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
Critical (9.3) 08955 Ubuntu 5.04 / 5.10 / 6.06 LTS : Buffer overrun in enscript before 1.6.4 (CVE-2008-4306)
Critical (10.0) 27942 Ubuntu 5.04 / 5.10 / 6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
Critical (10.0) 27978 Ubuntu 5.10 / 6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
Critical (10.0) 28017 Ubuntu 5.10 / 6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated

- Credentialed
- Non-Credentialed
- Compliance

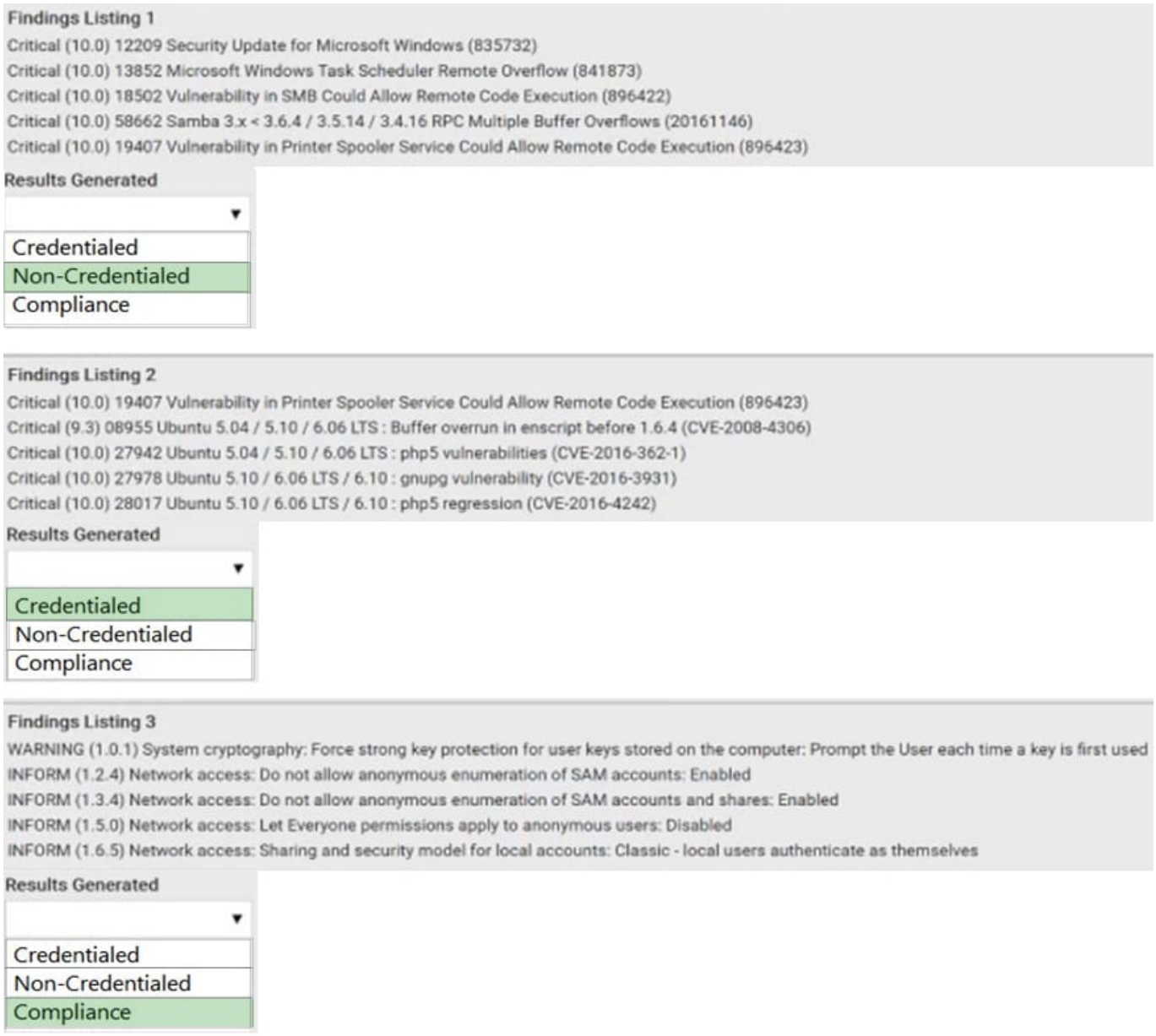
Findings Listing 3

WARNING (1.0.1) System cryptography: Force strong key protection for user keys stored on the computer: Prompt the User each time a key is first used
INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
INFORM (1.5.0) Network access: Let Everyone permissions apply to anonymous users: Disabled
INFORM (1.6.5) Network access: Sharing and security model for local accounts: Classic - local users authenticate as themselves

Results Generated

- Credentialed
- Non-Credentialed
- Compliance

Correct Answer:



QUESTION 2

Which of the following is a reason to take a DevSecOps approach to a software assurance program?

A. To find and fix security vulnerabilities earlier in the development process

B. To speed up user acceptance testing in order to deliver the code to production faster

C. To separate continuous integration from continuous development in the SDLC

D. To increase the number of security-related bug fixes worked on by developers

Correct Answer: A

QUESTION 3

A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is taking place?

A. Data exfiltration

B. Rogue device

C. Scanning

D. Beaconing

Correct Answer: D

Beaconing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

QUESTION 4

A company\\'s threat team has been reviewing recent security incidents and looking for a common theme. The team discovered the incidents were caused by incorrect configurations on the impacted systems. The issues were reported to support teams, but no action was taken. Which of the following is the next step the company should take to ensure any future issues are remediated?

A. Require support teams to develop a corrective control that ensures security failures are addressed once they are identified.

B. Require support teams to develop a preventive control that ensures new systems are built with the required security configurations.

C. Require support teams to develop a detective control that ensures they continuously assess systems for configuration errors.

D. Require support teams to develop a managerial control that ensures systems have a documented configuration baseline.

Correct Answer: A

Requiring support teams to develop a corrective control that ensures security failures are addressed once they are identified is the best step to prevent future issues from being remediated. Corrective controls are actions or mechanisms that are implemented after a security incident or failure has occurred to fix or restore the normal state of the system or network. Corrective controls can include patching, updating, repairing, restoring, or reconfiguring systems or

components that were affected by the incident or failure . https://www.techopedia.com/definition39/memory-dump

QUESTION 5

A security analyst wants to capture large amounts of network data that will be analyzed at a later time. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called "packetCapture." The capture must be as efficient as possible, and the analyst wants to minimize the likelihood that packets will be missed. Which of the following commands will best accomplish the analyst\\'s objectives?

A. tcpdump -w packetCapture

B. tcpdump -a packetCapture

C. tcpdump -n packetCapture

D. nmap -v > packetCapture

E. nmap -oA > packetCapture

Correct Answer: A

The tcpdump command is a network packet analyzer tool that can capture and display network traffic. The -w option specifies a file name to write the captured packets to, in a binary format that can be read by tcpdump or other tools later. This option is useful for capturing large amounts of network data that will be analyzed at a later time, as the question requires. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called " . The capture must be as efficient as possible, and the -w option minimizes the processing and output overhead of tcpdump, reducing the likelihood that packets will be missed.