DUMPSARENA

CompTIA CSA+ Certification Exam

CompTIA CS0-001

Version Demo

Total Demo Questions: 20

Total Premium Questions: 416

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

As part of an upcoming engagement for a client, an analyst is configuring a penetration testing application to ensure the scan complies with information defined in the SOW. Which of the following types of information should be considered based on information traditionally found in the SOW? (Choose two.)

A. Timing of the scan

B. Contents of the executive summary report

C. Excluded hosts

D. Maintenance windows

E. IPS configuration

F. Incident response policies

ANSWER: A C

QUESTION NO: 2

Creating a lessons learned report following an incident will help an analyst to communicate which of the following information? (Choose two.)

A. Root cause analysis of the incident and the impact it had on the organization

B. Outline of the detailed reverse engineering steps for management to review

C. Performance data from the impacted servers and endpoints to report to management

D. Enhancements to the policies and practices that will improve business responses

E. List of IP addresses, applications, and assets

ANSWER: A D

QUESTION NO: 3

A red team actor observes it is common practice to allow cell phones to charge on company computers, but access to the memory storage is blocked. Which of the following are common attack techniques that take advantage of this practice? (Choose two.)

A. A USB attack that tricks the computer into thinking the connected device is a keyboard, and then sends characters one at a time as a keyboard to launch the attack (a prerecorded series of keystrokes)

B. A USB attack that turns the connected device into a rogue access point that spoofs the configured wireless SSIDs

C. A Bluetooth attack that modifies the device registry (Windows PCs only) to allow the flash drive to mount, and then launches a Java applet attack

D. A Bluetooth peering attack called “Snarfing” that allows Bluetooth connections on blocked device types if physically connected to a USB port

E. A USB attack that tricks the system into thinking it is a network adapter, then runs a user password hash gathering utility for offline password cracking

ANSWER: C D

QUESTION NO: 4

Given the following code:

```
<SCRIPT type="text/javascript">
var adr = "../evil.php?breadmonster=" +escape{document.cookie};
var query = "SELECT * FROM users WHERE name='smith';
</SCRIPT>
```

Which of the following types of attacks is occurring?

A. MITM

B. Session hijacking

C. XSS

D. Privilege escalation

E. SQL injection

ANSWER: E

QUESTION NO: 5

An analyst was tasked with providing recommendations of technologies that are PKI X.509 compliant for a variety of secure functions. Which of the following technologies meet the compatibility requirement? (Choose three.)

A. 3DES

B. AES

C. IDEA

D. PKCS

E. PGP

F. SSL/TLS

G. TEMPEST

ANSWER: B D F

QUESTION NO: 6

A system administrator is doing network reconnaissance of a company's external network to determine the vulnerability of various services that are running. Sending some sample traffic to the external host, the administrator obtains the following packet capture:

```
18 17.646496 67.53.200.1 67.53.200.12 TCP 58 47669 -> 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19 17.646944 67.53.200.1 67.53.200.12 TCP 58 47669 -> 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20 17.648631 67.53.200.12 67.53.200.1 TCP 58 22 -> 47669 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
21 17.648646 67.53.200.1 67.53.200.12 TCP 58 47669 -> 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22 17.648887 67.53.200.12 67.53.200.1 TCP 54 445 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 17.649763 67.53.200.12 67.53.200.1 TCP 54 80 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Based on the output, which of the following services should be further tested for vulnerabilities?

A. SSH

B. HTTP

C. SMB

D. HTTPS

ANSWER: C

QUESTION NO: 7 - (HOTSPOT)

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.

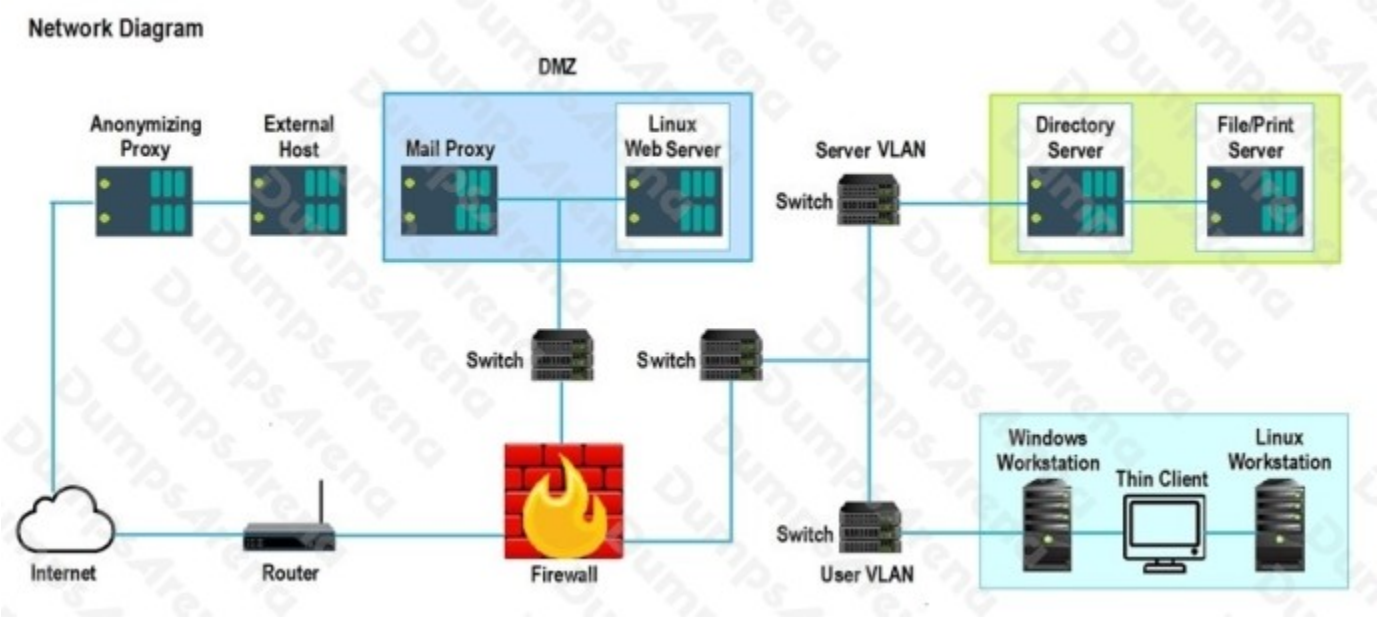
Instructions:

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.

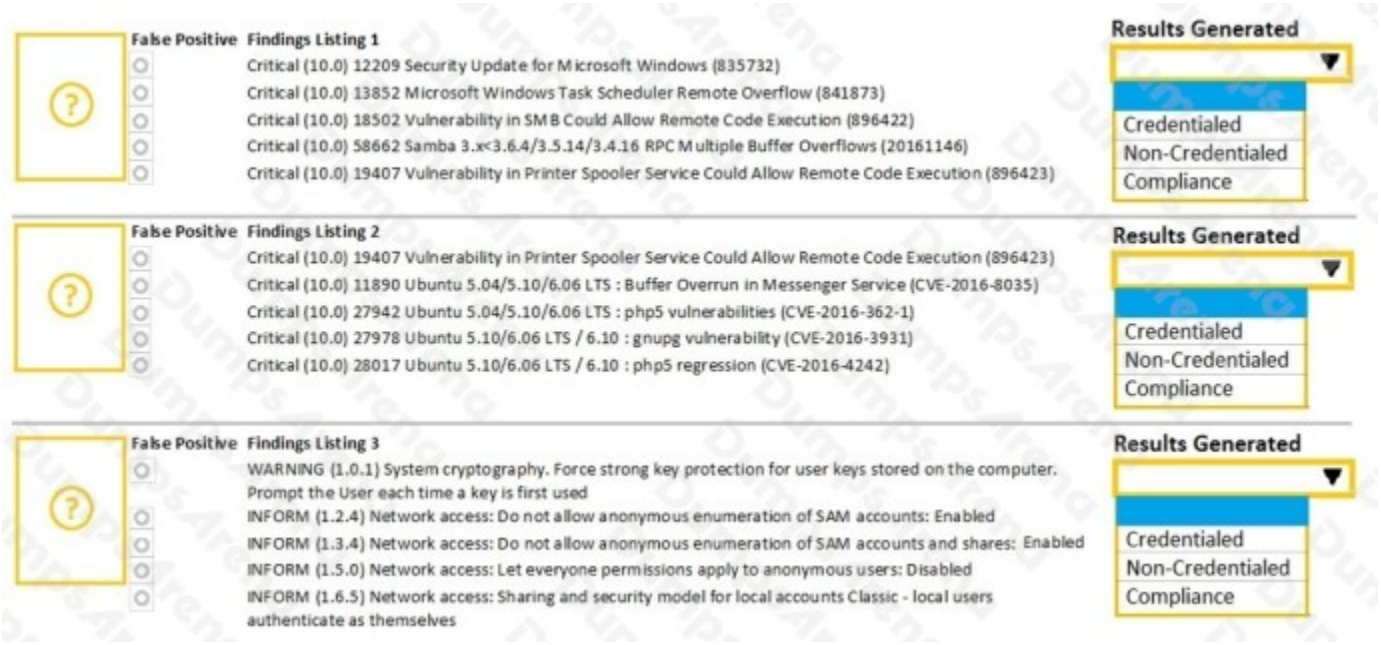
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

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.

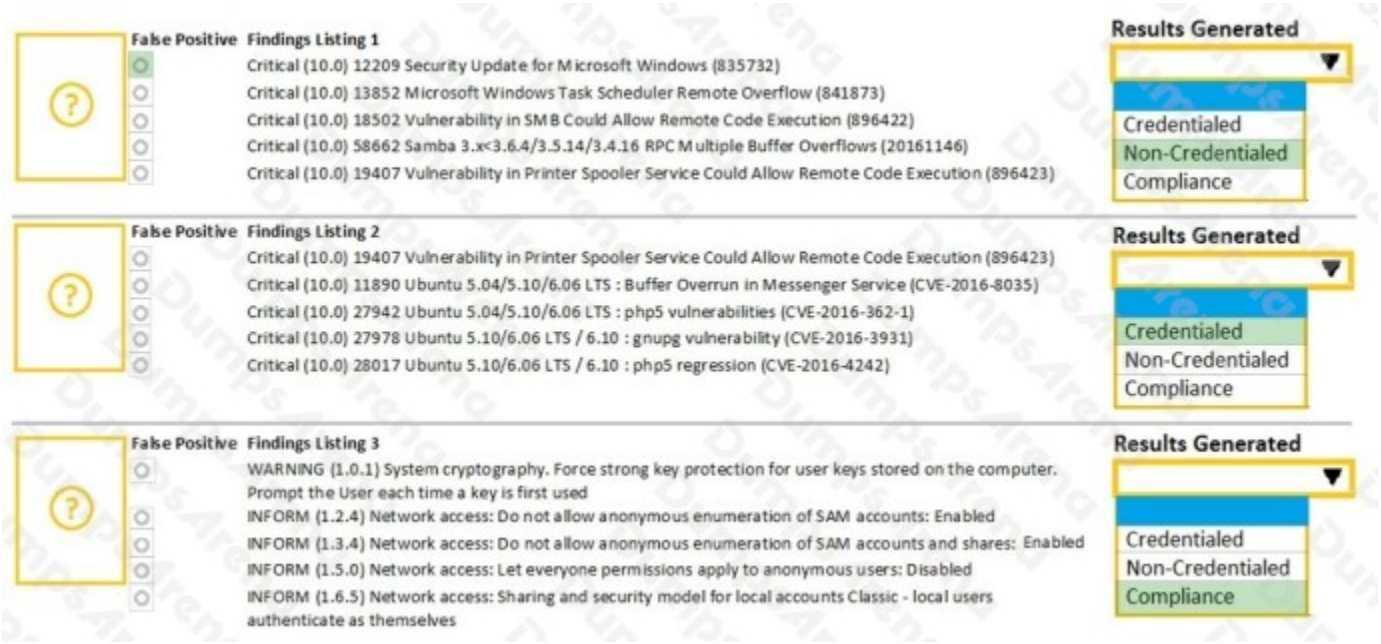
If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Hot Area:



ANSWER:



Explanation:

1. non-credentialed scan - File Print Server: False positive is first bullet point.

2. credentialed scan – Linux Web Server: No False positives.

3. Compliance scan - Directory Server

QUESTION NO: 8

A cybersecurity analyst was asked to review several results of web vulnerability scan logs.

Given the following snippet of code:

```
Iframe src="http://65.240.22.1" width="0" height="0" frmeborder="0"
tabindex="-1" title="empty" style=visibility:hidden;display:none
/iframe
```

Which of the following BEST describes the situation and recommendations to be made?

A. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. The code should include the domain name. Recommend the entry be updated with the domain name.

B. The security analyst has discovered an embedded iframe that is hidden from users accessing the web page. This code is correct. This is a design preference, and no vulnerabilities are present.

C. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. The link is hidden and suspicious. Recommend the entry be removed from the web page.

D. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. Recommend making the iframe visible. Fixing the code will correct the issue.

ANSWER: B

QUESTION NO: 9

A security administrator determines several months after the first instance that a local privileged user has been routinely logging into a server interactively as “root” and browsing the Internet. The administrator determines this by performing an annual review of the security logs on that server. For which of the following security architecture areas should the administrator recommend review and modification? (Choose two.)

A. Log aggregation and analysis

B. Software assurance

C. Encryption

D. Acceptable use policies

E. Password complexity

F. Network isolation and separation

ANSWER: A D

QUESTION NO: 10

Malicious users utilized brute force to access a system. An analyst is investigating these attacks and recommends methods to management that would help secure the system. Which of the following controls should the analyst recommend? (Choose three.)

A. Multifactor authentication

B. Network segmentation

C. Single sign-on

D. Encryption

E. Complexity policy

F. Biometrics

G. Obfuscation

ANSWER: A E F

QUESTION NO: 11

A security analyst is conducting a vulnerability assessment of older SCADA devices on the corporate network. Which of the following compensating controls is likely to prevent the scans from providing value?

A. Access control list network segmentation that prevents access to the SCADA devices inside the network.

B. Detailed and tested firewall rules that effectively prevent outside access of the SCADA devices.

C. Implementation of a VLAN that allows all devices on the network to see all SCADA devices on the network.

D. SCADA systems configured with 'SCADA SUPPORT'=ENABLE

ANSWER: B

QUESTION NO: 12

A technician is troubleshooting a desktop computer with low disk space. The technician reviews the following information snippets:

Disk Allocation Report
350Gb – C:\Users\user1\movies\movies

Network Stats

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:8080	0.0.0.0:0	LISTENING movieDB
TCP	192.168.1.10:8080	172.16.34.77:1200	TIME_WAIT

Which of the following should the technician do to BEST resolve the issue based on the above information? (Choose two.)

A. Delete the movies/movies directory

B. Disable the movieDB service

C. Enable OS auto updates

D. Install a file integrity tool

E. Defragment the disk

ANSWER: B E

QUESTION NO: 13

Considering confidentiality and integrity, which of the following make servers more secure than desktops? (Choose three.)

A. VLANs

B. OS

C. Trained operators

D. Physical access restriction

E. Processing power

F. Hard drive capacity

ANSWER: B C D

QUESTION NO: 14

A security analyst has created an image of a drive from an incident. Which of the following describes what the analyst should do NEXT?

A. The analyst should create a backup of the drive and then hash the drive.

B. The analyst should begin analyzing the image and begin to report findings.

C. The analyst should create a hash of the image and compare it to the original drive's hash.

D. The analyst should create a chain of custody document and notify stakeholders.

ANSWER: C

QUESTION NO: 15

A security analyst notices PII has been copied from the customer database to an anonymous FTP server in the DMZ. Firewall logs indicate the customer database has not been accessed from anonymous FTP server. Which of the following departments should make a decision about pursuing further investigation? (Choose two.)

A. Human resources

B. Public relations

C. Legal

D. Executive management

E. IT management

ANSWER: D

QUESTION NO: 16

An organization has recently experienced a data breach. A forensic analysis confirmed the attacker found a legacy web server that had not been used in over a year and was not regularly patched. After a discussion with the security team, management decided to initiate a program of network reconnaissance and penetration testing. They want to start the process by scanning the network for active hosts and open ports. Which of the following tools is BEST suited for this job?

A. Ping

B. Nmap

C. Netstat

D. ifconfig

E. Wireshark

F. L0phtCrack

ANSWER: B

QUESTION NO: 17

A security analyst is running a routine vulnerability scan against a web farm. The farm consists of a single server acting as a load-balancing reverse proxy and offloads cryptographic processes to the backend servers. The backend servers consist of four servers that process the inquiries for the front end.

Vulnerability	Risk	Time	Host
SSL Expiration Less Than 90 days	Low	12:45	farm.company.com
SSL Certificate Hostname Mismatch	Medium	12:58	backend1.local
SSL Certificate Hostname Mismatch	Medium	13:11	backend2.local
SSL Certificate Hostname Mismatch	Medium	13:24	backend3.local
SSL Certificate Hostname Mismatch	Medium	13:37	backend4.local

A web service SSL query of each server responds with the same output:

Connected (0x000003)

depth=0 /0=farm.company.com/CN=farm.company.com/OU=Domain Control Validated

Which of the following results BEST addresses these findings?

A. Advise the application development team that the SSL certificates on the backend servers should be revoked and reissued to match their hostnames

B. Notify the application development team of the findings and advise management of the results

C. Create an exception in the vulnerability scanner, as the results and false positives and can be ignored safely

D. Require that the application development team renews the farm certificate and includes a wildcard for the 'local' domain in the certificate SAN field

ANSWER: C

QUESTION NO: 18

Which of the following is the BEST way to share incident-related artifacts to provide non-repudiation?

A. Secure email

B. Encrypted USB drives

C. Cloud containers

D. Network folders

ANSWER: B

QUESTION NO: 19

An employee at an insurance company is processing claims that include patient addresses, clinic visits, diagnosis information, and prescription. While forwarding documentation to the supervisor, the employee accidentally sends the data to a personal email address outside of the company due to a typo. Which of the following types of data has been compromised?

A. PCI

B. Proprietary information

C. Intellectual property

D. PHI

ANSWER: D

QUESTION NO: 20

An analyst was investigating an attack that took place on the network. A user was able to access the system without proper authentication. Which of the following will the analyst recommend, related to management approaches, in order to control access? (Choose three.)

A. RBAC

B. LEAP

C. DAC

D. PEAP

E. MAC

F. SCAP

G. BCP

ANSWER: A C E