DUMPSARENA

CompTIA CySA+ Certification Exam (CS0-002)

CompTIA CS0-002

Version Demo

Total Demo Questions: 15

Total Premium Questions: 275

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

A security analyst observes a large amount of scanning activity coming from an IP address outside the organization's environment. Which of the following should the analyst do to block this activity?

A. Create an IPS rule to block the subnet.

B. Sinkhole the IP address.

C. Create a firewall rule to block the IP address.

D. Close all unnecessary open ports.

ANSWER: C

Explanation:

A firewall is a device or software that controls the incoming and outgoing network traffic based on predefined rules. Creating a firewall rule to block the IP address that is scanning the organization’s environment is an effective way to stop this activity and prevent potential attacks. Creating an IPS rule to block the subnet, sinkholing the IP address, or closing all unnecessary open ports are other possible actions, but they are not as specific or efficient as creating a firewall rule to block the IP address. Reference: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/firewall.html

QUESTION NO: 2

Which of the following factors would determine the regulations placed on data under data sovereignty laws?

A. What the company intends to do with the data it owns

B. The company's data security policy

C. The type of data the company stores

D. The data laws of the country in which the company is located

ANSWER: D

Explanation:

The data laws of the country in which the company is located would determine the regulations placed on data under data sovereignty laws. Data sovereignty laws are laws that govern how data is collected, stored, processed, and transferred within a country’s jurisdiction. Data sovereignty laws can vary from country to country, depending on their legal system, political system, culture, and values. Data sovereignty laws can affect how companies handle their data, especially when they operate across borders or use cloud services. For example, some countries may have strict data protection or privacy laws that require companies to obtain consent from data subjects before collecting or processing their data. Some countries may also have data localization or data residency laws that require companies to store their data within the country’s borders or limit cross-border data transfers.

QUESTION NO: 3

An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issued mobile device while connected to the network. Which of the following actions would help during the forensic analysis of the mobile device? (Select TWO).

A. Resetting the phone to factory settings

B. Rebooting the phone and installing the latest security updates

C. Documenting the respective chain of custody

D. Uninstalling any potentially unwanted programs

E. Performing a memory dump of the mobile device for analysis

F. Unlocking the device by browsing the eFuse

ANSWER: C E

Explanation:

Documenting the chain of custody is an important step in the forensic analysis of any device, as it helps to ensure that all evidence is collected and preserved correctly. A memory dump is also essential, as it can provide information about the state of the device when the attack occurred and can be used for further analysis.

Documenting the respective chain of custody can help to preserve the integrity and admissibility of the evidence collected from the mobile device during the forensic analysis. Chain of custody is a record of who handled, accessed or modified the evidence, when, where, how and why . Performing a memory dump of the mobile device for analysis can help to extract volatile data from the mobile device that may contain valuable information about the ransomware attack, such as processes, network connections or encryption keys. Memory dump is a process of copying the contents of the memory (RAM) to a file or storage device .

References: https://www.techopedia.com/definition/23371/chain-of-custody
https://www.techopedia.com/definition/10339/memory-dump

QUESTION NO: 4 - (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.

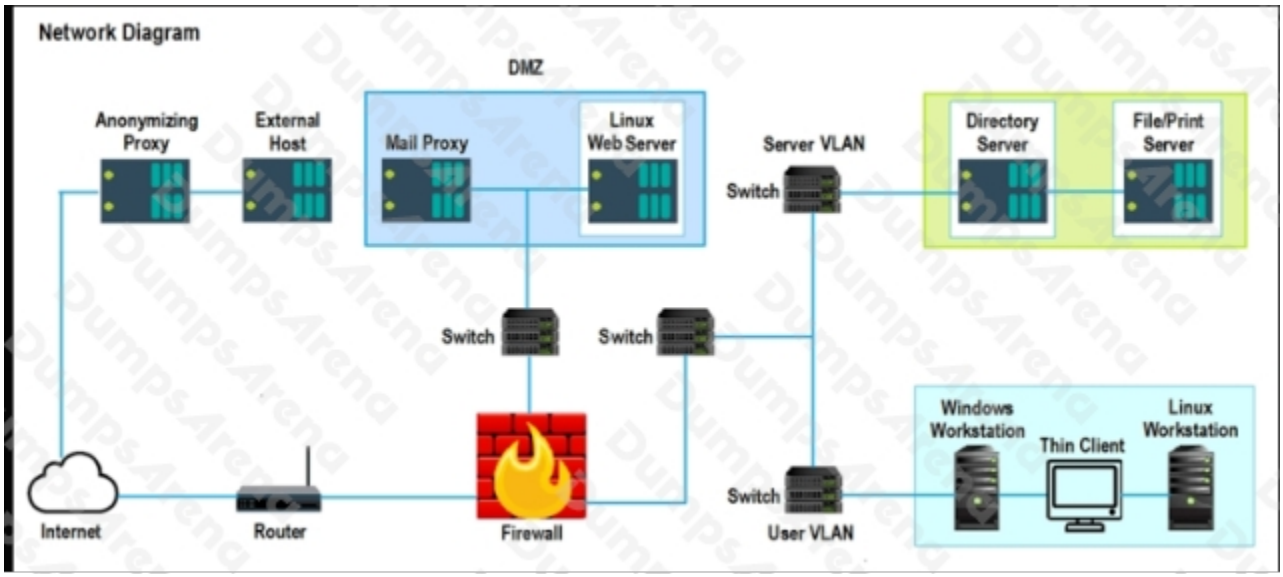
Instructions:

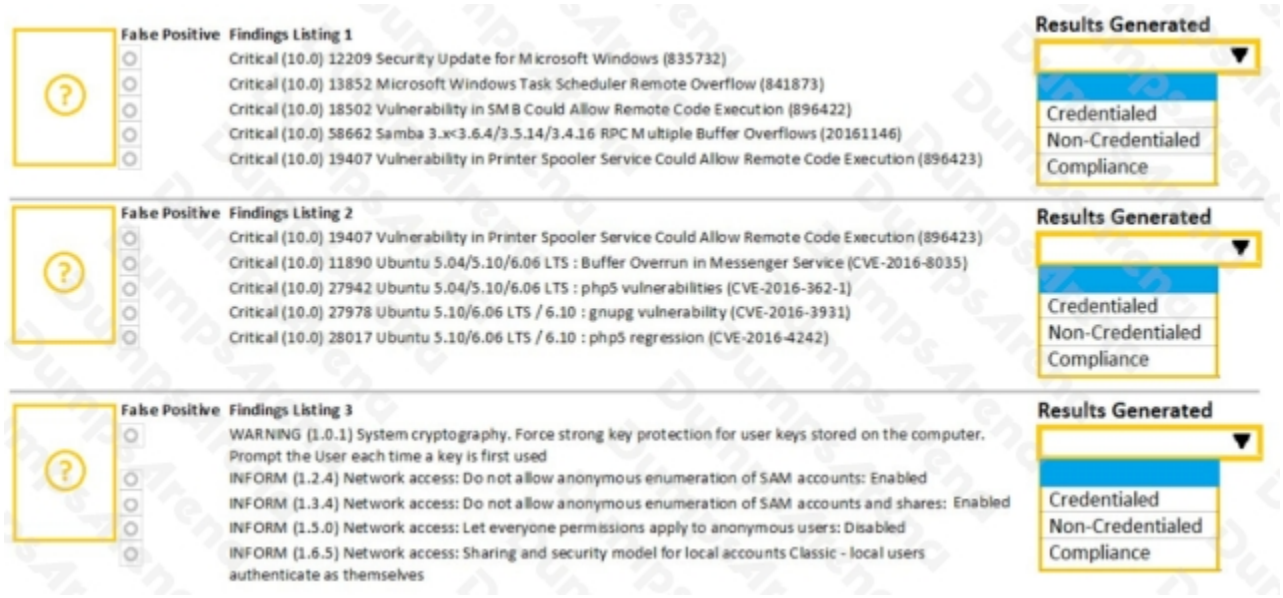
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

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.


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


False Positive
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
False Positive
Findings Listing 2
Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
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
False Positive
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

ANSWER:


False Positive
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
False Positive
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
Non-Credentialed
False Positive
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
Compliance

QUESTION NO: 5

Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

A. Message queuing telemetry transport does not support encryption.

B. The devices may have weak or known passwords.

C. The devices may cause a dramatic Increase in wireless network traffic.

D. The devices may utilize unsecure network protocols.

E. Multiple devices may interface with the functions of other loT devices.

F. The devices are not compatible with TLS 12.

ANSWER: B D

Explanation:

Consumer IoT devices are devices that connect to the internet and provide various functions or services for personal or home use, such as smart speakers, cameras, thermostats, etc. Consumer IoT devices should be avoided in an enterprise environment because they may pose security risks or challenges for the organization’s network and data. Some of the reasons why consumer IoT devices should be avoided are:

Reference: Why Consumer IoT Devices Should Be Avoided In Enterprise Environments | Security Boulevard

QUESTION NO: 6

A company creates digitally signed packages for its devices. Which of the following best describes the method by which the security packages are delivered to the company's customers?

A. Antitamper mechanism

B. SELinux

C. Trusted firmware updates

D. eFuse

ANSWER: C

Explanation:

Trusted firmware updates are a method by which security packages are delivered to the company’s customers. Trusted firmware updates are digitally signed packages that contain software updates or patches for devices, such as routers, switches, or firewalls. Trusted firmware updates can help to ensure the authenticity and integrity of the packages by verifying the digital signature of the sender and preventing unauthorized or malicious modifications to the packages .

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_trustsec/configuration/xe-16/sec-usr-trustsec-xe-16-book/sec-trust-firm-upd.html

QUESTION NO: 7

A development team recently released a new version of a public-facing website for testing prior to production. The development team is soliciting the help of various teams to validate the functionality of the website due to its high visibility. Which of the following activities best describes the process the development team is initiating?

A. Static analysis

B. Stress testing

C. Code review

D. User acceptance testing

ANSWER: D

Explanation:

User acceptance testing is a process of verifying that a software application meets the requirements and expectations of the end users before it is released to production. User acceptance testing can help to validate the functionality, usability, performance and compatibility of the software application with real-world scenarios and feedback . User acceptance testing can involve various teams, such as developers, testers, customers and stakeholders.

Reference: https://www.techopedia.com/definition/3887/user-acceptance-testing-uat

QUESTION NO: 8

Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)

A. Kitten

B. Panda

C. Tiger

D. Jackal

E. Bear

F. Spider

ANSWER: A D

Explanation:

Kitten and Jackal are two APT (Advanced Persistent Threat) adversary archetypes that represent non-nation-state threat actors. APT adversary archetypes are categories of threat actors that share common characteristics, such as motivation, objectives, capabilities, or tactics. APT adversary archetypes can help security analysts understand and prioritize the threats they face2. Kitten is a term used to describe Iranian-based threat actors that are typically not backed by the Iranian government. They are motivated by ideological or religious beliefs and target political or regional adversaries3. Jackal is a term used to describe cybercriminal groups that operate as mercenaries or proxies for other threat actors. They are motivated by financial gain and target various sectors and regions.

QUESTION NO: 9

A Chief Information Security Officer has asked for a list of hosts that have critical and high-severity findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?

A. Nessus

B. Nikto

C. Fuzzer

D. Wireshark

E. Prowler

ANSWER: A

Explanation:

Nessus is a vulnerability scanning and assessment tool that can be used to scan systems for potential vulnerabilities and weaknesses. It provides detailed reports on any critical and high-severity findings as referenced in the CVE database, making it the ideal tool for fulfilling the Chief Information Security Officer's request. Nikto, fuzzer, wireshark, and prowler are all security tools, but they are not applicable for the scenario described in the question. Here is a link to an article from CompTIA's website about Nessus for your reference: https://www.comptia.org/content/nessus-vulnerability-scanning-and-assessment-tool.

QUESTION NO: 10

During an audit, several customer order forms were found to contain inconsistencies between the actual price of an item and the amount charged to the customer. Further investigation narrowed the cause of the issue to manipulation of the public-facing web form used by customers to order products. Which of the following would be the best way to locate this issue?

A. Reduce the session timeout threshold

B. Deploy MFA for access to the web server.

C. Implement input validation.

D. Run a dynamic code analysis.

ANSWER: C

Explanation:

Implementing input validation is the best way to locate and prevent the issue of manipulation of the public-facing web form used by customers to order products. Input validation is a technique that checks and filters any user input that is sent to an application before processing it. Input validation can help to ensure that the user input conforms to the expected format, length and type, and does not contain any malicious characters or syntax that may alter the logic or behavior of the application. Input validation can also reject or sanitize any input that does not meet the validation criteria .

Reference: https://portswigger.net/web-security/input-validation

QUESTION NO: 11

A cybersecunty analyst needs to harden a server that is currently being used as a web server The server needs to be accessible when entenng www company com into the browser Additionally web pages require frequent updates which are performed by a remote contractor Given the following output:

```
Starting Nmap 7.12 ( https://nmap.org ) at 2020-08-25 11:44
Nmap scan report for finance-server (72.56.70.94)
Host is up (0.000060s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
```

Which of the following should the cybersecunty analyst recommend to harden the server? (Select TWO).

A. Uninstall the DNS service

B. Perform a vulnerability scan

C. Change the server's IP to a private IP address

D. Disable the Telnet service

E. Block port 80 with the host-based firewall

F. Change the SSH port to a non-standard port

ANSWER: D F

Explanation:

Disabling the Telnet service would harden the server by removing an insecure protocol that transmits data in cleartext and could allow unauthorized access to the server. Changing the SSH port to a non-standard port would harden the server by reducing the exposure to brute-force attacks or port scans that target the default SSH port (22). Uninstalling the DNS service, performing a vulnerability scan, changing the server's IP to a private IP address, or blocking port 80 with the host-based firewall would not harden the server or could affect its functionality as a web server. Reference: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

QUESTION NO: 12

An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).

A. Resetting the phone to factory settings

B. Rebooting the phone and installing the latest security updates

C. Documenting the respective chain of custody

D. Uninstalling any potentially unwanted programs

E. Performing a memory dump of the mobile device for analysis

F. Unlocking the device by blowing the eFuse

ANSWER: C E

Explanation:

Documenting the respective chain of custody and performing a memory dump of the mobile device for analysis would help during the forensic analysis of the mobile device. The chain of custody is a record of who handled the evidence, when, where, how, and why. The chain of custody helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss1. A memory dump is a process of capturing and storing the contents of the device's memory (RAM) for analysis. A memory dump can help to recover volatile data that may be lost when the device is powered off or rebooted, such as running processes, network connections, encryption keys, or malware traces2.

QUESTION NO: 13

A security analyst is reviewing WAF logs and notes requests against the corporate website are increasing and starting to impact the performance of the web server. The security analyst queries the logs for requests that triggered an alert on the WAF but were not blocked. Which of the following possible TTP combinations might warrant further investigation? (Select TWO).

A. Requests identified by a threat intelligence service with a bad reputation

B. Requests sent from the same IP address using different user agents

C. Requests blocked by the web server per the input sanitization

D. Failed log-in attempts against the web application

E. Requests sent by NICs with outdated firmware

F. Existence of HTTP/501 status codes generated to the same IP address

ANSWER: A B

Explanation:

Requests identified by a threat intelligence service with a bad reputation are likely to be malicious or suspicious, as they originate from sources that are known to be involved in cyberattacks or other malicious activities. These requests may indicate that an attacker is trying to exploit a vulnerability or perform reconnaissance on the web server.

Requests sent from the same IP address using different user agents are also likely to be malicious or suspicious, as they indicate that an attacker is trying to evade detection or bypass security controls by changing their browser or device identification. These requests may indicate that an attacker is using automated tools or scripts to scan or attack the web server.

QUESTION NO: 14

An organization has the following policy statements:

• All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.

•AM network activity will be logged and monitored.

• Confidential data will be tagged and tracked

• Confidential data must never be transmitted in an unencrypted form.

• Confidential data must never be stored on an unencrypted mobile device.

Which of the following is the organization enforcing?

A. Acceptable use policy

B. Data privacy policy

C. Encryption policy

D. Data management, policy

ANSWER: B

Explanation:

Data privacy policy is the organization's policy that defines how it collects, uses, stores, and shares personal data of its customers, employees, or other stakeholders. Data privacy policy also covers how the organization complies with relevant data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). The policy statements listed in the question are examples of data privacy policy provisions that aim to protect the confidentiality, integrity, and availability of personal data.

QUESTION NO: 15

A digital forensics investigator works from duplicate images to preserve the integrity of the original evidence. Which of the following types of media are most volatile and should be preserved? (Select two).

A. Memory cache

B. Registry file

C. SSD storage

D. Temporary filesystems

E. Packet decoding

F. Swap volume

ANSWER: A F

Explanation:

Memory cache and swap volume are types of media that are most volatile and should be preserved during a digital forensics investigation. Volatile media are those that store data temporarily and lose their contents when the power is turned off or interrupted. Memory cache is a small and fast memory that stores frequently used data or instructions for faster access by

the processor. Swap volume is a part of the hard disk that is used as an extension of the memory when the memory is full or low .

Reference: https://www.techopedia.com/definition/10339/memory-dump