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.certbus.com/cs0-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

When investigating a compromised system, a security analyst finds the following script in the /tmp directory:

```
PASS=password123
for user in 'cat allusers.txt'
do
   ./trylogin.py dc1.comptia.org $user $PASS
done
```

Which of the following attacks is this script attempting, and how can it be mitigated?

A. This is a password-hijacking attack, and it can be mitigated by using strong encryption protocols.

B. This is a password-spraying attack, and it can be mitigated by using multifactor authentication.

C. This is a password-dictionary attack, and it can be mitigated by forcing password changes every 30 days.

D. This is a credential-stuffing attack, and it can be mitigated by using multistep authentication.

Correct Answer: B

https://owasp.org/www-community/attacks/Password_Spraying_Attack

A credential stuffing attack would be using the full credentials and most likely being used across many common platforms. A credential stuffing attack depends on the reuse of passwords. With so many people reusing their passwords for multiple accounts, just one set of credentials is enough to expose most or all of their accounts.

QUESTION 2

A company that is hiring a penetration tester wants to exclude social engineering from the list of authorized activities. Which of the following documents should include these details?

A. Acceptable use policy

B. Service level agreement

C. Rules of engagement

D. Memorandum of understanding

E. Master service agreement

Correct Answer: C

QUESTION 3

In SIEM software, a security analysis selected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers.

Based on this behavior, which of the following actions should be taken FIRST to prevent a more serious compromise?

A. Fully segregate the affected servers physically in a network segment, apart from the production network.

B. Collect the network traffic during the day to understand if the same activity is also occurring during business hours

C. Check the hash signatures, comparing them with malware databases to verify if the files are infected.

D. Collect all the files that have changed and compare them with the previous baseline

Correct Answer: A

QUESTION 4

A cybersecurity analyst is currently using Nessus to scan several FTP servers. Upon receiving the results of the scan, the analyst needs to further test to verify that the vulnerability found exists. The analyst uses the following snippet of code:

```
Username: admin ' ; - -
Password : ' OR 1=1 - -
```

Which of the following vulnerabilities is the analyst checking for?

A. Buffer overflow

B. SQL injection

C. Default passwords

D. Format string attack

Correct Answer: B

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.

QUESTION 6

A security analyst is investigating malicious traffic from an internal system that attempted to download proxy avoidance software as identified from the firewall logs but the destination IP is blocked and not captured. Which of the following should the analyst do?

A. Shut down the computer

B. Capture live data using Wireshark

C. Take a snapshot

D. Determine if DNS logging is enabled.

E. Review the network logs.

Correct Answer: D

The DNS debug log provides extremely detailed data about all DNS information that is sent and received by the DNS server, similar to the data that can be gathered using packet capture tools such as network monitor.

QUESTION 7

An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by public users accessing the server. The results should be written to a text file and should include the date, time, and IP address associated with any spreadsheet downloads. The web server\\'s log file is named webserver.log, and the report file name should be accessreport.txt. Following is a sample of the web server\\'s log file:

2017-10-12 21:01:12 GET /index.html - 84.102.33.7 - return=200 1622

Which of the following commands should be run if an analyst only wants to include entries in which a spreadsheet was successfully downloaded?

A. more webserver.log | grep *.xls > accessreport.txt

B. more webserver.log > grep "*xls" | egrep -E `success\\' > accessreport.txt

C. more webserver.log | grep -E "return=200 | xls" > accessreport.txt

D. more webserver.log | grep -A *.xls

Correct Answer: C

QUESTION 8

An analyst has received a notification about potential malicious activity against a web server. The analyst logs in to a central log collection server and runs the following command: "cat access.log.1 | grep "union". The output shown below appears:

??[31/Jan/2020:10:02:31 ?400] "Get /cgi-bin/backend1.sh?id=%20union%20select%20192.168.60.50 HTTP/1.1"

Which of the following attacks has occurred on the server?

A. Cross-site request forgery

B. SQL injection

C. Cross-site scripting

D. Directory traversal

Correct Answer: C

QUESTION 9

Understanding attack vectors and integrating intelligence sources are important components of:

A. a vulnerability management plan.

B. proactive threat hunting.

C. risk management compliance.

D. an incident response plan.

Correct Answer: B

QUESTION 10

A company\\'s Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company\\'s business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?

A. Utilize the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises.

B. Do not utilize the CASB solution for this purpose, but add DLP on premises for data in motion.

C. Utilize the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud.

D. Do not utilize the CASB solution for this purpose, but add DLP on premises for data at rest.

Correct Answer: C

"CASB solutions generally offer their own DLP policy engine, allowing you to configure DLP policies in a CASB and apply them to cloud services."

https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on- premises-dlp- solution/

QUESTION 11

An analyst wants to identify hosts that are connecting to the external FTP servers and what, if any, passwords are being used. Which of the following commands should the analyst use?

A. tcpdump –X dst port 21

B. ftp ftp.server –p 21

C. nmap –o ftp.server –p 21

D. telnet ftp.server 21

Correct Answer: A

QUESTION 12

A security administrator has uncovered a covert channel used to exfiltrate confidential data from an internal database server through a compromised corporate web server. Ongoing exfiltration is accomplished by embedding a small amount of data extracted from the database into the metadata of images served by the web server. File timestamps suggest that the server was initially compromised six months ago using a common server misconfiguration. Which of the following BEST describes the type of threat being used?

A. APT

B. Zero-day attack

C. Man-in-the-middle attack

D. XSS

Correct Answer: A

QUESTION 13

An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets. Which of the following should be considered FIRST prior to disposing of the electronic data?

A. Sanitization policy

B. Data sovereignty

C. Encryption policy

D. Retention standards

Correct Answer: D

QUESTION 14

While reviewing a cyber-risk assessment, an analyst notes there are concerns related to FPGA usage. Which of the following statements would BEST convince the analyst\\'s supervisor to use additional controls?

A. FPGAs are expensive and can only be programmed once. Code deployment safeguards are needed.

B. FPGAs have an inflexible architecture. Additional training for developers is needed.

C. FPGAs are vulnerable to malware installation and require additional protections for their codebase.

D. FPGAs are expensive to produce. Anti-counterfeiting safeguards are needed.

Correct Answer: C

QUESTION 15

For machine learning to be applied effectively toward security analysis automation, it requires _____.

A. relevant training data.

B. a threat feed API.

C. a multicore, multiprocessor system.

D. anomalous traffic signatures.

Correct Answer: A