200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An analyst received a ticket regarding a degraded processing capability for one of the HR department\\'s servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

A. Recovery

B. Detection

C. Eradication

D. Analysis

Correct Answer: D

QUESTION 2

What is a Heartbleed vulnerability?

A. denial of service

B. information disclosure

C. buffer overflow

D. command injection

Correct Answer: B

QUESTION 3

A forensic investigator is analyzing a recent breach case. An external USB drive was discovered to be connected and transmitting the data outside of the organization, and the owner of the USB drive could not be identified. Video surveillance shows six people during a two-month period had close contact with the affected asset. How must this type of evidence be categorized?

A. best evidence

B. indirect evidence

C. direct evidence

D. corroborative evidence

Correct Answer: B

QUESTION 4

Which two elements are used for profiling a network? (Choose two.)

A. session duration

B. total throughput

C. running processes

D. listening ports

E. OS fingerprint

Correct Answer: AB

A network profile should include some important elements, such as the following:

Total throughput the amount of data passing from a given source to a given destination in a given period of time Session duration the time between the establishment of a data flow and its termination Ports used a list of TCP or UDP processes that are available to accept data Critical asset address space the IP addresses or the logical location of essential systems or data Profiling data are data that system has gathered, these data helps for incident response and to detect incident Network profiling = throughput, sessions duration, port used, Critical Asset Address Space Host profiling = Listening ports, logged in accounts, running processes, running tasks,applications

QUESTION 5

The SOC team has confirmed a potential indicator of compromise on an endpoint. The team has narrowed the executable file\\'s type to a new trojan family. According to the NIST Computer Security Incident Handling Guide, what is the next step in handling this event?

A. Isolate the infected endpoint from the network.

B. Perform forensics analysis on the infected endpoint.

C. Collect public information on the malware behavior.

D. Prioritize incident handling based on the impact.

Correct Answer: C

ference: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf