Thank You for your download
Cisco 200-201 Exam Question & Answers (Demo)
Understanding Cisco Cybersecurity Operations Fundamentals Exam

Version: 11.0

Question: 1

Which event is user interaction?

A. gaining root access
B. executing remote code
C. reading and writing file permission
D. opening a malicious file

Explanation:

Question: 2

Which security principle requires more than one person is required to perform a critical task?

A. least privilege
B. need to know
C. separation of duties
D. due diligence

Explanation:

Question: 3

How is attacking a vulnerability categorized?

A. action on objectives
B. delivery
C. exploitation
D. installation

Explanation:

What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously

Answer: C

Explanation:

Host-based antivirus protection is also known as agent-based. Agent-based antivirus runs on every protected machine. Agentless antivirus protection performs scans on hosts from a centralized system. Agentless systems have become popular for virtualized environments in which multiple OS instances are running on a host simultaneously. Agent-based antivirus running in each virtualized system can be a serious drain on system resources. Agentless antivirus for virtual hosts involves the use of a special security virtual appliance that performs optimized scanning tasks on the virtual hosts. An example of this is VMware's vShield.

Question: 5

Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

A. decision making
B. rapid response
C. data mining
D. due diligence

Answer: B

Explanation: