Cisco Exam Questions 210-250
SECFND Understanding Cisco Cybersecurity Fundamentals
NEW QUESTION 1
Based on which statement does the discretionary access control security model grant or restrict access?

A. discretion of the system administrator  
B. security policy defined by the owner of an object  
C. security policy defined by the system administrator  
D. role of a user within an organization

Answer: B

NEW QUESTION 2
Which definition of a Linux daemon is true?

A. Process that is causing harm to the system by either using up system resources or causing a critical crash.  
B. Long – running process that is the child at the init process  
C. process that has no parent process  
D. process that is starved at the CPU.

Answer: B

NEW QUESTION 3
Which hashing algorithm is the least secure?

A. MD5  
B. RC4  
C. SHA-3  
D. SHA-2

Answer: A

NEW QUESTION 4
Endpoint logs indicate that a machine has obtained an unusual gateway address and unusual DNS servers via DHCP. Which option is this situation most likely an example of?

A. Command injection  
B. Phishing  
C. Man in the middle attack  
D. Evasion methods

Answer: C

NEW QUESTION 5
You must create a vulnerability management framework. Which main purpose of this framework is true?

A. Conduct vulnerability scans on the network.  
B. Manage a list of reported vulnerabilities.  
C. Identify, remove and mitigate system vulnerabilities.  
D. Detect and remove vulnerabilities in source code.

Answer: C

NEW QUESTION 6
Which of the following are some useful reports you can collect from Cisco ISE related to endpoints? (Select all that apply.)

A. Web Server Log reports  
B. Top Application reports  
C. RADIUS Authentication reports  
D. Administrator Login reports

Answer: ABD

NEW QUESTION 7
Which option is an advantage to using network-based anti-virus versus host-based anti-virus?

A. Network-based has the ability to protect unmanaged devices and unsupported operating systems.  
B. There are no advantages compared to host-based antivirus.  
C. Host-based antivirus does not have the ability to collect newly created signatures.  
D. Network-based can protect against infection from malicious files at rest.

Answer: A

NEW QUESTION 8
A zombie process occurs when which of the following happens?
A. A process holds its associated memory and resources but is released from the entry table.
B. A process continues to run on its own.
C. A process holds on to associate memory but releases resources.
D. A process releases the associated memory and resources but remains in the entry table.

Answer: D

NEW QUESTION 9
According to RFC 1035 which transport protocol is recommended for use with DNS queries?

A. Transmission Control Protocol
B. Reliable Data Protocol
C. Hypertext Transfer Protocol
D. User Datagram Protocol

Answer: D

NEW QUESTION 10
Which term represents the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. integrity validation
B. due diligence
C. need to know
D. least privilege

Answer: D

NEW QUESTION 11
Which process continues to be recorded in the process table after it has ended and the status is returned to the parent?

A. daemon
B. zombie
C. orphan
D. child

Answer: B

NEW QUESTION 12
Which protocol is primarily supported by the third layer of the Open Systems Interconnection reference model?

A. HTTP/TLS
B. IPv4/IPv6
C. TCP/UDP
D. ATM/ MPLS

Answer: B

NEW QUESTION 13
Which information security property is supported by encryption?

A. sustainability
B. integrity
C. confidentiality
D. availability

Answer: C

NEW QUESTION 14
Which definition of Windows Registry is true?

A. set of pages that are currently resident m physical memory
B. basic unit to which the operating system allocates processor time
C. set of virtual memory addresses
D. database that stores low-level settings for the operating system

Answer: D

NEW QUESTION 15
Which type of technology is used for detecting unusual patterns and anomalous behavior on a network?

A. Host Intrusion detection
B. Host malware prevention
C. NetFlow analysis
D. Web content filtering
NEW QUESTION 16
The FMC can share HTML, PDF and CSV data types that relate to a specific event type which event type:

A. Connection
B. Host
C. Netflow
D. Intrusion

Answer: D

NEW QUESTION 17
Which type of exploit normally requires the culprit to have prior access to the target system?

A. Local exploit
B. Denial of service
C. System vulnerability
D. Remote exploit

Answer: A

NEW QUESTION 18
In which case should an employee return his laptop to the organization?

A. When moving to a different role
B. Upon termination of the employment
C. As described in the asset return policy
D. When the laptop is end of lease

Answer: C

NEW QUESTION 19
Which security principle is violated by running all processes as root/admin?

A. RBAC
B. Principle of least privilege
C. Segregation of duty

Answer: B

NEW QUESTION 20
In which context is it inappropriate to use a hash algorithm?

A. Telnet logins
B. Verifying file integrity
C. SSH logins
D. Digital signature verification

Answer: A

NEW QUESTION 21
......
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions
2nd - Questions and Answers in PDF Format

210-250 Practice Exam Features:

* 210-250 Questions and Answers Updated Frequently
* 210-250 Practice Questions Verified by Expert Senior Certified Staff
* 210-250 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 210-250 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 210-250 Practice Test Here