Vendor: Cisco

Exam Code: 210-250

Exam Name: Understanding Cisco Cybersecurity Fundamentals (SECFND)

Version: Demo

QUESTION 1
Which type of attack occurs when an attacker utilizes a botnet to reflect requests off an NTP server to overwhelm their target?

A. man in the middle
B. denial of service
C. distributed denial of service
D. replay

Correct Answer: D

QUESTION 2
For which reason can HTTPS traffic make security monitoring difficult?

A. encryption
B. large packet headers
C. Signature detection takes longer.
D. SSL interception

Correct Answer: D

QUESTION 3
Which two features must a next generation firewall include? (Choose two.)

A. data mining
B. host-based antivirus
C. application visibility and control
D. Security Information and Event Management
E. intrusion detection system

Correct Answer: DE

QUESTION 4
A firewall requires deep packet inspection to evaluate which layer?

A. application
B. Internet
C. link
D. transport

Correct Answer: A

QUESTION 5
An intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources. Which evasion technique does this attempt indicate?

A. traffic fragmentation
B. resource exhaustion
C. timing attack

D. tunneling

Correct Answer: A

QUESTION 6
Which definition of the virtual address space for a Windows process is true?

A. actual physical location of an object in memory
B. set of virtual memory addresses that it can use
C. set of pages that are currently resident in physical memory
D. system-level memory protection feature that is built into the operating system

Correct Answer: A

QUESTION 7
A user reports difficulties accessing certain external web pages, When examining traffic to and from the external domain in full packet captures, you notice many SYNs that have the same sequence number, source, and destination IP address, but have different payloads. Which problem is a possible explanation of this situation?

A. insufficient network resources
B. failure of full packet capture solution
C. misconfiguration of web filter
D. TCP injection

Correct Answer: A

QUESTION 8
Which definition of an antivirus program is true?

A. program used to detect and remove unwanted malicious software from the system
B. program that provides real time analysis of security alerts generated by network hardware and application
C. program that scans a running application for vulnerabilities
D. rules that allow network traffic to go in and out

Correct Answer: A

QUESTION 9
Which security monitoring data type requires the most storage space?

A. full packet capture
B. transaction data
C. statistical data
D. session data

Correct Answer: A

QUESTION 10
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

Correct Answer: C

QUESTION 11
Which hashing algorithm is the least secure?

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

Correct Answer: D

QUESTION 12
Which two tasks can be performed by analyzing the logs of a traditional stateful firewall? (Choose two.)

A. Confirm the timing of network connections differentiated by the TCP 5-tuple
B. Audit the applications used within a social networking web site.
C. Determine the user IDs involved in an instant messaging exchange.
D. Map internal private IP addresses to dynamically translated external public IP addresses
E. Identify the malware variant carried by ^n SMTP connection

Correct Answer: BE

QUESTION 13
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

Correct Answer: D