QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

Cisco

210-255

Implementing Cisco Cybersecurity Operations

QUESTION: 111
Which function does an internal CSIRT provide?

A. incident handling services across various CSIRTs
B. incident handling services for a country's government
C. incident handling services for a parent organization
D incident handling services as a service for other organization

Answer: C

QUESTION: 112
Which expression creates a filter on a host IP address or name?

A. [src|dst] host <host host >
B. [tcp|udp] [src|dst] port<port>
C. ether [src|dst] host<ehost>
D. gateway host <host>

Answer: A

https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html

QUESTION: 113
The united State CERT provides cybersecurity protection to Federal, civilian, and executive branch agencies through intrusion detection and prevention capabilities. Which type of incident response team is this an example of?

A. Federal PSIRT
B. National PSIRT
C. National CSIRT
D. Federal CSIRT

Answer: B

QUESTION: 114
Which two potions are the primary 5-tuple components? (Choose two)

A. destination IP address
B. header length
C. sequence number
D. checksum
E. source IP address

Answer: A, E,

QUESTION: 115
According to NIST-SP800-61R2, which option should be contained in the issue tracking system?

A. incidents related to the current incident
B. incident unrelated to the current incident
C. actions taken by nonincident handlers
D. latest public virus signatures

Answer: A

QUESTION: 116
Employees are allowed access to internal websites. An employee connects to an internal website and IDS reports it as malicious behavior. What is this example of?

A. true positive
B. false negative
C. false positive
D. true negative

Answer: C

QUESTION: 117
Which purpose of data mapping is true?

A. Visualize data.

B. Find extra vulnerabilities.
C. Discover the identities of attackers
D. Check that data is correct.

Answer: A

QUESTION: 118
Which value in profiling servers in a system is true?

A. it can identify when network performance has decreased
B. it can identify servers that have been exploited
C. it can identify when network ports have been connected
D. it can protect the address space of critical hosts.

Answer: C

QUESTION: 119
Which type of analysis shows what the outcome is as well how likely each outcome is?

A. exploratory
B. descriptive
C. probabilistic
D. deterministic

Answer: C

QUESTION: 120
How is confidentiality defined in the CVSS v3.0 framework?

A. confidentiality of the information resource managed by person due to an unsuccessfully exploited vulnerability
B. confidentiality of the information resource managed by a person due to a successfully vulnerability
C. confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability
D. confidentiality of the information resource managed by a software component due

to an unsuccessfully exploited vulnerability

Answer: C