Cisco.Premium.210-255.by.VCEplus.70q

Number: 210-255 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 3.0

Exam Code: 210-255
Exam Name: Implementing Cisco Cybersecurity Operations
Certification Provider: Cisco
Corresponding Certification: CCNA Cyber Ops
Website: www.vceplus.com
Free Exam: https://vceplus.com/ccna-exam-210-255-secops/

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in 210-255 exam products and you get latest questions. We strive to deliver the best 210-255 exam product for top grades in your first attempt.

QUESTION 1
Which option can be addressed when using retrospective security techniques?

A. if the affected host needs a software update
B. how the malware entered our network
C. why the malware is still in our network
D. if the affected system needs replacement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which CVSSv3 Attack Vector metric value requires the attacker to physically touch or manipulate the vulnerable component?

A. local
B. physical
C. network
D. adjacent

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which option is a misuse variety per VERIS enumerations?

A. snooping
B. hacking
C. theft
D. assault

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
In the context of incident handling phases, which two activities fall under scoping? (Choose two.)

A. determining the number of attackers that are associated with a security incident
B. ascertaining the number and types of vulnerabilities on your network
C. identifying the extent that a security incident is impacting protected resources on the network
D. determining what and how much data may have been affected
E. identifying the attackers that are associated with a security incident

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which regular expression matches "color" and "colour"?

A. col[0-9]+our
B. colo?ur
C. colou?r
D.]a-z]{7}

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which kind of evidence can be considered most reliable to arrive at an analytical assertion?

A. direct
B. corroborative
C. indirect
D. circumstantial
E. textual

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
You see 100 HTTP GET and POST requests for various pages on one of your webservers. The user agent in the requests contain php code that, if executed, creates and writes to a new php file on the webserver. Which category does this event fall under as defined in the Diamond Model of Intrusion?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which string matches the regular expression r(ege)+x?

A. rx
B. regeegex
C. r(ege)x
D. rege+x

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which statement about threat actors is true?

A. They are any company assets that are threatened.
B. They are any assets that are threatened.
C. They are perpetrators of attacks.
D. They are victims of attacks.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which data element must be protected with regards to PCI?

A. past health condition
B. geographic location
C. full name
D. recent payment amount

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
What mechanism does the Linux operating system provide to control access to files?

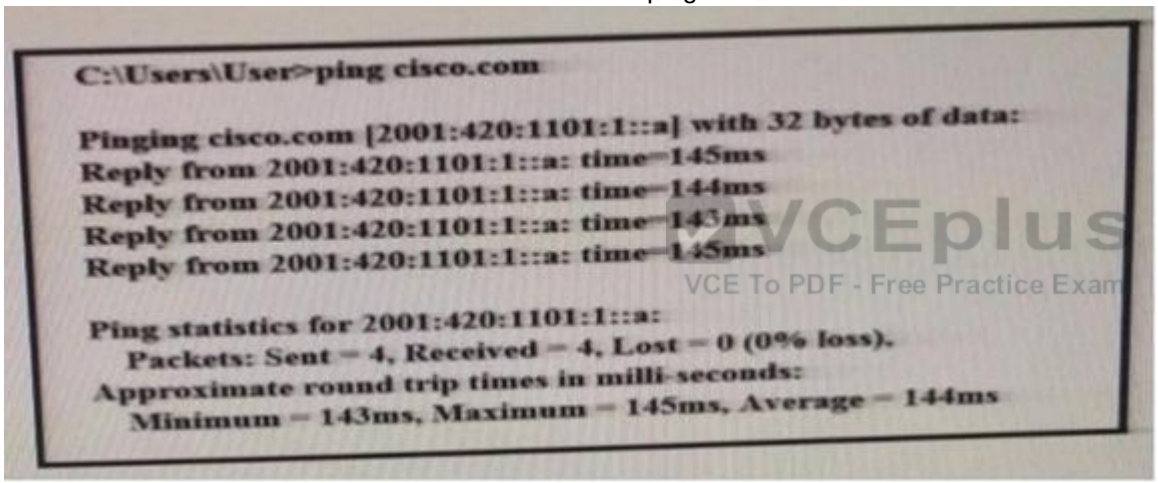
A. privileges required

B. user interaction
C. file permissions
D. access complexity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Refer to the exhibit. What can be determined from this ping result?



A. The public IP address of cisco.com is 2001:420:1101:1::a.
B. The Cisco.com website is down.
C. The Cisco.com website is responding with an internal IP.
D. The public IP address of cisco.com is an IPv4 address.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: