

210-255^{Q&As}

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

Free Download Real Questions & Answers PDF and VCE file from:

https://www.geekcert.com/210-255.html

100% Passing Guarantee 100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers



https://www.geekcert.com/210-255.html 2024 Latest geekcert 210-255 PDF and VCE dumps Download

QUESTION 1

Which string matches the regular expression r(ege)+x?	
A. rx	

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

Correct Answer: B

QUESTION 2

Refer to the exhibit.

\$ cuckoo submit --machine cuckool /path/to/binary

Which event is occurring?

- A. A URL is being evaluated to see if it has a malicious binary.
- B. A binary on device cuckoo1 is being submitted for evaluation.
- C. A binary named "submit" is running on cuckoo1.
- D. A binary is being submitted to run on device cuckoo1.

Correct Answer: D

QUESTION 3

DRAG DROP

Drag and drop the Cyber Kill Chain elements from the left into the correct order on the right.

Select and Place:

https://www.geekcert.com/210-255.html 2024 Latest geekcert 210-255 PDF and VCE dumps Download

command and control	1
weaponization	2
reconnaissance	3
action and objectives	4
exploitation	5
installation	6
delivery	7

Correct Answer:

	reconnaissance
	weaponization
	delivery
	exploitation
	installation
co	ommand and control
а	ction and objectives

QUESTION 4

Which event artifact can be used to identify HTTP GET requests for a specific file?

- A. HTTP status code
- B. TCP ACK
- C. destination IP



https://www.geekcert.com/210-255.html

2024 Latest geekcert 210-255 PDF and VCE dumps Download

D. URI

Correct Answer: D

QUESTION 5

Which component of the NIST SP800-61 r2 incident handling strategy reviews data?

A. preparation

B. detection and analysis

C. containment, eradication, and recovery

D. post-incident analysis

Correct Answer: D

210-255 VCE Dumps

210-255 Practice Test

210-255 Exam Questions