

# 210-255<sup>Q&As</sup>

Cisco Cybersecurity Operations

## Pass Cisco 210-255 Exam with 100% Guarantee

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

https://www.pass4itsure.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



## VCE & PDF Pass4itSure.com

https://www.pass4itsure.com/210-255.html 2024 Latest pass4itsure 210-255 PDF and VCE dumps Download

QUESTION 1			
Which of the following is not a metadata feature of the Diamond Model?			
A. Direction			
B. Result			
C. Devices			
D. Resources			
Correct Answer: C			
QUESTION 2			
attacker using robots.txt is under which category?			
A. Reconnaissance			
B. Weaponization			
C. Delivery			
D. Exploitation			
E. Installation			
F. Command and control (C2)			
G. Actions on objectives			
Correct Answer: A			
QUESTION 3			
Which two options can be used by a threat actor to determine the role of a server? (Choose two.)			
A. PCAP			
B. tracert			
C. running processes			
D. hard drive configuration			
E. applications			
Correct Answer: CE			

## VCE & PDF Pass4itSure.com

https://www.pass4itsure.com/210-255.html 2024 Latest pass4itsure 210-255 PDF and VCE dumps Download

QUESTION 4
To which category do attributes belong within the VERIS schema?
A. victim demographics
B. incident tracking
C. Discovery and response
D. incident description
Correct Answer: D
QUESTION 5
Which type of analysis shows what the outcome is as well how likely each outcome is?
A. exploratory
B. descriptive
C. probabilistic
D. deterministic
Correct Answer: D
QUESTION 6
You have a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor. Which type of evidence is this?
A. indirect evidence
B. prima facie evidence
C. best evidence
D. physical evidence
Correct Answer: A
QUESTION 7
Which string matches the regular expression r(egg) Lv2

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

A. rx

B. regeegex



https://www.pass4itsure.com/210-255.html 2024 Latest pass4itsure 210-255 PDF and VCE dumps Download

C. r(ege)x
D. rege+x
Correct Answer: B
QUESTION 8
Which option is a misuse variety per VERIS enumerations?
A. snooping
B. hacking
C. theft
D. assault
Correct Answer: B
QUESTION 9
Which HTTP header field is usually used in forensics to identify the type of browser used?
A. User agent
B. Referrer
C. Host
D. Accept-language
Correct Answer: A
QUESTION 10
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
Correct Answer: C

## https://www.pass4itsure.com/210-255.html

#### **QUESTION 11**

#### DRAG DROP

Drag and drop the type of evidence from the left onto the correct description(s) of that evidence on the right.

Select and Place:

direct evidence	hash of a file that has been verified as malware
corroborative evidence	log that shows the download of a verified malicious file, a vulnerability scan of the system verifying the vulnerability, and no logs from mitigating tools
indirect evidence	communication on a new port that was previously unobserved
Correct Answer:	
	direct evidence
	indirect evidence
	corroborative evidence

### **QUESTION 12**

Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked?

A. true positive

### https://www.pass4itsure.com/210-255.html 2024 Latest pass4itsure 210-255 PDF and VCE dumps Download

B. true negative

C. false positive

D. false negative

Correct Answer: C

#### **QUESTION 13**

**DRAG DROP** 

%ASA-6-106015: Deny TCP (no connection) from 10.21.11.3/4288 to 192.168.72.8/80 flags FIN PSH ACK on interface inside

Refer to the exhibit. Drag and drop elements from the log onto the correct 5-tuple category on the right.

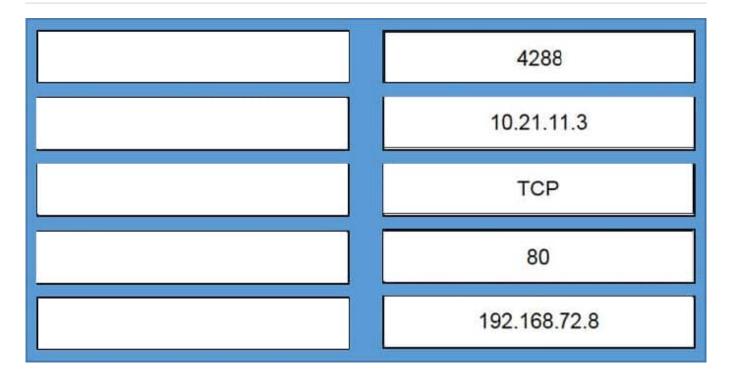
Select and Place:

10.21.11.3	source port
4288	source IP address
80	protocol
192.168.72.8	destination port
ТСР	destination IP address

Correct Answer:

### https://www.pass4itsure.com/210-255.html

2024 Latest pass4itsure 210-255 PDF and VCE dumps Download



#### **QUESTION 14**



Refer to the exhibit. Which description of the IP addresses under the Trajectory section is true?



#### https://www.pass4itsure.com/210-255.html

2024 Latest pass4itsure 210-255 PDF and VCE dumps Download

- A. victim systems running Microsoft Word
- B. spoofed IP addresses
- C. victim systems running Adobe Acrobat
- D. attackers

Correct Answer: A

#### **QUESTION 15**

Which statement about the collected evidence data when performing digital forensics is true?

- A. It must be preserved and its integrity verified.
- B. It must be copied to external storage media and immediately distributed to the CISO.
- C. It must be deleted as soon as possible due to PCI compliance.
- D. It must be stored in a forensics lab only by the data custodian.

Correct Answer: A

210-255 PDF Dumps

210-255 Study Guide

210-255 Braindumps