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.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

QUESTION 1

Which type of analysis assigns values to scenarios to see what the outcome might be in each scenario?

A. deterministic

B. exploratory

C. probabilistic

D. descriptive

Correct Answer: A

QUESTION 2

DRAG DROP

sIP	dIP	sPort	dPort	pro	packets	bytes	flags	sTime	duration		eTime
10.232.38.20	208.100.26.233	80	39613	6	60	3120	A	2016/10/09T00:09:43.112	1774.708	2016/10/09T00:39:17.820	

Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the NetFlow v5r record from a security event on the right.

Select and Place:

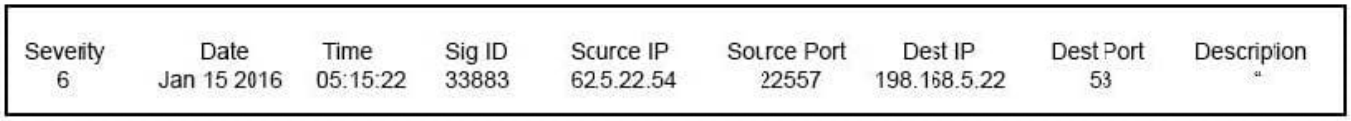
source address	10.232.38.20
destination address	3120
source port	80
number of packets transmitted	208.100.26.233
bytes transmitted	60
protocol	39613
destination port	TCP

Correct Answer:

	source address
	bytes transmitted
	source port
	destination address
	number of packets transmitted
	destination port
	protocol

QUESTION 3

Refer to the exhibit. Which type of log is this an example of?



Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2016	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	"

A. IDS log

B. proxy log

C. NetFlow log

D. syslog

Correct Answer: C

A typical output of a NetFlow command line tool (nfdump in this case) when printing the stored flows may look as follows:

Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Packets Bytes Flows 2010-09-01 00:00:00.459 0.000 UDP 127.0.0.1:24920 -> 192.168.0.1:22126 1 46 1 2010-09-01 00:00:00.363 0.000 UDP 192.168.0.1:22126 -> 127.0.0.1:24920 1 80 1

Reference: http://nfdump.sourceforge.net/

QUESTION 4

Which two HTTP header fields relate to intrusion analysis? (Choose two).

A. user-agent

B. host

C. connection

D. language

E. handshake type

Correct Answer: AB

QUESTION 5

What define the roadmap for implementing the incident response capability?

A. incident response plan

B. incident response procedure

C. incident handling guide

D. incident response policy

Correct Answer: A