QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

Cisco

210-255

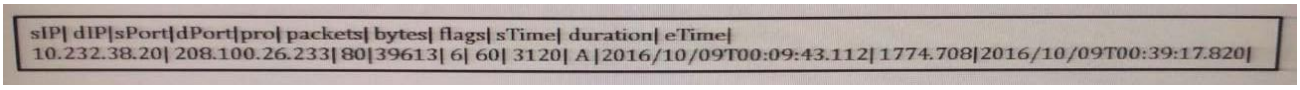
Implementing Cisco Cybersecurity Operations

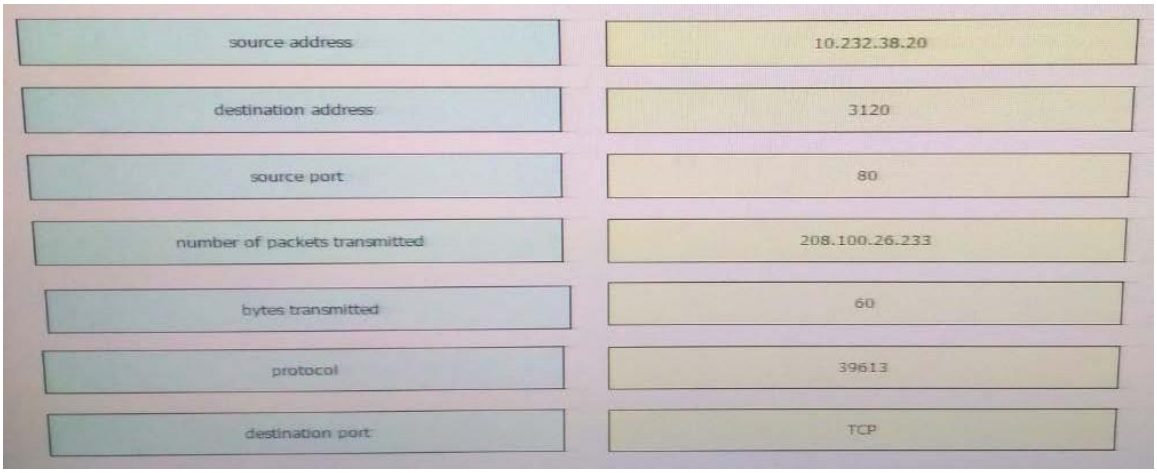
QUESTION: 58
Which data element must be protected with regards to PCI?

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

Answer: D

QUESTION: 59
DRAG DROP
Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the NetFlow vs record from a security event on the right.





Answer:

QUESTION: 60
You receive an alert for malicious code that exploits Internet Explorer and runs arbitrary code on the site visitor machine. The malicous code is on an external site that is being visited by hosts on your network. Which user agent in the HTTP headers in the requests from your internal hosts warrants further investigation?

A. Mozilla/5.0 (compatible, MSIE 10.0, Windows NT 6.2, Trident 6.0)
B. Mozilla/5.0 (XII; Linux i686; rv: 1.9.2.20) Gecko/20110805
C. Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 400) Gecko/20100101
D. Opera/9.80 (XII; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16

Answer: A

QUESTION: 61
You have run a suspicious tile in a sandbox analysis tool to see what the tile does. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed or required to investigate the callouts? (Choose two.)

A. file size
B. domain names
C. dropped files
D. signatures
E. host IP addresses

Answer: A, E

QUESTION: 62

A CMS plugin creates two files that are accessible from the Internet myplugin.html and exploitable.php. A newly discovered exploit takes advantage of an injection vulnerability in exploitable.php. To exploit the vulnerability, one must send an HTTP POST with specific variables to exploitable.php. You see traffic to your webserver that consists of only HTTP GET requests to myplugin.html. Which category best describes this activity?

A. weaponization
B. exploitation
C. installation
D. reconnaissance

Answer: B

QUESTION: 63
During which phase of the forensic process are tools and techniques used to extract the relevant information from the collective data?

A. examination
B. reporting
C. collection
D. investigation

Answer: B

QUESTION: 64
Which feature is used to find possible vulnerable services running on a server?

A. CPU utilization
B. security policy
C. temporary internet files
D. listening ports

Answer: D

QUESTION: 65
Which element can be used by a threat actor to discover a possible opening into a target network and can also be used by an analyst to determine the protocol of the malicious traffic?

A. TILs
B. ports
C. SMTP replies
D. IP addresses

Answer: A