



Vendor: Cisco

Exam Code: 210-255

Exam Name: Implementing Cisco Cybersecurity Operations

Version: DEMO

QUESTION 1

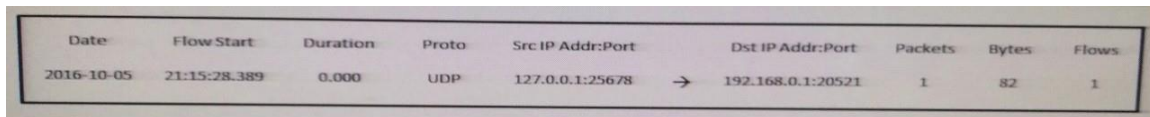
Which option can be addressed when using retrospective security techniques?

- 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

Answer: A

QUESTION 2

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



Date	Flow Start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2016-10-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→ 192.168.0.1:20521	1	82	1

- A. IDS log
- B. proxy log
- C. NetFlow log
- D. syslog

Answer: A

QUESTION 3

Which option is a misuse variety per VERIS enumerations?

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

Answer: B

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

Answer: DE

QUESTION 5

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

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

Answer: C

QUESTION 6

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

Answer: B

QUESTION 7

Which option is generated when a file is run through an algorithm and generates a string specific to the contents of that file?

- A. URL
- B. hash
- C. IP address
- D. destination port

Answer: C

QUESTION 8

Which data type is protected under the PCI compliance framework?

- A. credit card type
- B. primary account number
- C. health conditions
- D. provision of individual care

Answer: C

QUESTION 9

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

Answer: A

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives®

10% Discount Coupon Code: ASTR14