



Vendor: Cisco

Exam Code: 200-201

Exam Name: Understanding Cisco Cybersecurity
Operations Fundamentals (CBROPS)

Version: DEMO

QUESTION 1

Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)

- A. UDP port to which the traffic is destined
- B. TCP port from which the traffic was sourced
- C. source IP address of the packet
- D. destination IP address of the packet
- E. UDP port from which the traffic is sourced

Answer: CD

QUESTION 2

In a SOC environment, what is a vulnerability management metric?

- A. code signing enforcement
- B. full assets scan
- C. internet exposed devices
- D. single factor authentication

Answer: C

QUESTION 3

Which category relates to improper use or disclosure of PII data?

- A. legal
- B. compliance
- C. regulated
- D. contractual

Answer: C

QUESTION 4

Which regex matches only on all lowercase letters?

- A. [a-z]+
- B. [^a-z]+
- C. a-z+
- D. a*z+

Answer: A

QUESTION 5

Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

- A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
- B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods
- C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression

methods

D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

Answer: C

QUESTION 6

An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise.

Which kind of evidence is this IP address?

- A. best evidence
- B. corroborative evidence
- C. indirect evidence
- D. forensic evidence

Answer: B

QUESTION 7

Which security technology allows only a set of pre-approved applications to run on a system?

- A. application-level blacklisting
- B. host-based IPS
- C. application-level whitelisting
- D. antivirus

Answer: C

QUESTION 8

Refer to the exhibit. Which type of log is displayed?

Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2020	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	*

- A. IDS
- B. proxy
- C. NetFlow
- D. sys

Answer: D

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