

➤ **Vendor: Cisco**

➤ **Exam Code: 200-201**

➤ **Exam Name: 200-201 Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [Sep/2020](#))**

[Visit Braindump2go and Download Full Version 200-201 Exam Dumps](#)

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+

[200-201 Exam Dumps](#) **[200-201 Exam Questions](#)** **[200-201 PDF Dumps](#)** **[200-201 VCE Dumps](#)**

<https://www.braindump2go.com/200-201.html>

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

QUESTION 9

Refer to the exhibit. Which two elements in the table are parts of the 5-tuple? (Choose two.)

Overview | Analysis | Policies Devices Objects | Health | System | Help

Content Explorer | Connections > Security Intelligence Events | Intrusions | Files | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Security Intelligence Events [switch workflow]

Security Intelligence with Application Details > Table View of Security Intelligence Events

Search Constraints (Edit Search Serve Search)

2018-03-02 07:26:16 - 2018-03-07 11:41:20

Expanding Disabled Columns

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port	ICMP Type
2018-03-07 13:42:01		Sinkhole DNS Block	# 10.0.0.75	10.110.10.11	US	VERILABORNE (DOCLLOUD-SOC) (DAP)	10.110.10.11	US	DNS Intelligence-CnC	External	Internal	54925 /udp	
2018-03-07 13:42:01		Sinkhole DNS Block	# 10.0.0.100	10.110.10.11	US	ALP (TRO CHENS) (DOCLLOUD-SOC) (DAP)	10.110.10.11	US	DNS Intelligence-CnC	External	Internal	54925 /udp	
2018-03-07 13:42:01		Sinkhole DNS Block	# 10.152.10.158	192.168.1.153	US	VERNETTA (DONNEL) (DOCLLOUD-SOC) (DAP)	192.168.1.153	US	DNS Intelligence-CnC	External	Internal	54926 /udp	

Page 1 of 1 | Displaying items 1-3 of 3 rows

View All | Delete All

- A. First Packet
- B. Initiator User
- C. Ingress Security Zone
- D. Source Port
- E. Initiator IP

Answer: DE

QUESTION 10

Which security principle is violated by running all processes as root or administrator?

- A. principle of least privilege
- B. role-based access control
- C. separation of duties
- D. trusted computing base

Answer: A

QUESTION 11

What is the function of a command and control server?

- A. It enumerates open ports on a network device
- B. It drops secondary payload into malware
- C. It is used to regain control of the network after a compromise
- D. It sends instruction to a compromised system

Answer: D

QUESTION 12

What is the difference between deep packet inspection and stateful inspection?

- A. Deep packet inspection is more secure than stateful inspection on Layer 4
- B. Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7
- C. Stateful inspection is more secure than deep packet inspection on Layer 7
- D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4

Answer: D

QUESTION 13

Which evasion technique is a function of ransomware?

[200-201 Exam Dumps](#) [200-201 Exam Questions](#) [200-201 PDF Dumps](#) [200-201 VCE Dumps](#)

<https://www.braindump2go.com/200-201.html>

- A. extended sleep calls
- B. encryption
- C. resource exhaustion
- D. encoding

Answer: B

QUESTION 14

What does cyber attribution identity in an investigation?

- A. cause of an attack
- B. exploit of an attack
- C. vulnerabilities exploited
- D. threat actors of an attack

Answer: D

QUESTION 15

Drag and Drop Question

Drag and drop the security concept on the left onto the example of that concept on the right.

Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

Answer:

Threat
Vulnerability
Risk Assessment
Exploit