



200-201^{Q&As}

Understanding Cisco Cybersecurity Operations Fundamentals
(CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/200-201.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 two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

- A. detection and analysis
- B. post-incident activity
- C. vulnerability management
- D. risk assessment
- E. vulnerability scoring

Correct Answer: AB

Reference: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

QUESTION 2

Which attack method is being used when an attacker tries to compromise a network with an authentication system that uses only 4-digit numeric passwords and no username?

- A. replay
- B. SQL injection
- C. dictionary
- D. cross-site scripting

Correct Answer: C

QUESTION 3

DRAG DROP

Drag and drop the data source from the left onto the data type on the right.

Select and Place:



Wireshark	session data
NetFlow	alert data
server log	full packet capture
IPS	transaction data

Correct Answer:

	NetFlow
	IPS
	Wireshark
	server log

QUESTION 4

An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

- A. sequence numbers
- B. IP identifier
- C. 5-tuple
- D. timestamps

Correct Answer: C

QUESTION 5



```
05:18:26.673345 IP 10.0.2.15.34920 > fra16s56-in-f3.1e100.net.http: Flags [F.], seq 748, ack 1404, win 63791, length 0
05:18:26.673717 IP fra16s56-in-f3.1e100.net.http > 10.0.2.15.34920: Flags [.], ack 749, win 65535, length 0
05:18:26.674227 IP 10.0.2.15.53046 > fra16s48-in-f3.1e100.net.https: Flags [P.], seq 1265:1289, ack 37720, win 62780, length 24
05:18:26.674254 IP 10.0.2.15.53046 > fra16s48-in-f3.1e100.net.https: Flags [F.], seq 1289, ack 37720, win 62780, length 0
05:18:26.674517 IP fra16s48-in-f3.1e100.net.https > 10.0.2.15.53046: Flags [.], ack 1289, win 65535, length 0
05:18:26.674528 IP fra16s48-in-f3.1e100.net.https > 10.0.2.15.53046: Flags [.], ack 1290, win 65535, length 0
05:18:26.674683 IP 10.0.2.15.43402 > cloudproxy10041.sucuri.net.http: Flags [F.], seq 370, ack 2357, win 62780, length 0
```

What can be identified from the exhibit?

- A. NetFlow data
- B. spoofed TCP reset packets
- C. DNS hijacking
- D. tcpdump data

Correct Answer: D

[Latest 200-201 Dumps](#)

[200-201 VCE Dumps](#)

[200-201 Study Guide](#)