



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.passapply.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

How can TOR impact data visibility inside an organization?

- A. no impact
- B. increases security
- C. increases data integrity
- D. decreases visibility

Correct Answer: D

QUESTION 2

Which type of data is used to detect anomalies in the network?

- A. statistical data
- B. metadata
- C. transaction data
- D. alert data

Correct Answer: A

QUESTION 3

Refer to the exhibit.



Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2013-06-09 18:00:04	2013-06-09 18:02:48	164 seconds	0.6

File Details	
File name	VirusShare_fc1937c1aa536b3744ebdfb1716fd54d
File size	144340 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	EFE79A73
MD5	fc1937c1aa536b3744ebdfb1716fd54d
SHA1	7b9e695efb10ef1e23c7f7c20da1211b27d58c08
SHA256	b48dea670abb434ef50b76dcde4a906cb541c49abd2112782548103b13f5809d
SHA512	4ca2228f5c00ba045e19fceb58b09ed34e24669fa13fbb454cdc527f94832dc414ff5ec784f3a185bd1026d8e72b2823c3d32381148ff12bde7348254d7ecba5
Sedeeep	None
PEID	None matched
Yara	* shellcode (Matched shellcode byte patterns)
VirusTotal	40/47 (collapse)

Antivirus	Result
MicroWorld-eScan	Dropped: Trojan.Generic.7654828

What does this Cuckoo sandbox report indicate?

- A. The file is ransomware.
- B. The file is spyware.
- C. The file will open unsecure ports when executed.
- D. The file will open a command interpreter when executed.

Correct Answer: B

QUESTION 4

An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

- A. Recovery
- B. Detection
- C. Eradication
- D. Analysis



Correct Answer: D

QUESTION 5

Which two protocols are used for DDoS amplification attacks? (Choose two.)

- A. HTTP
- B. DNS
- C. TCP
- D. ICMPv6
- E. NTP

Correct Answer: BE

[Latest 200-201 Dumps](#)

[200-201 VCE Dumps](#)

[200-201 Exam Questions](#)