

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.leads4pass.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

What is a description of a social engineering attack?

- A. fake offer for free music download to trick the user into providing sensitive data
- B. package deliberately sent to the wrong receiver to advertise a new product
- C. mistakenly received valuable order destined for another person and hidden on purpose
- D. email offering last-minute deals on various vacations around the world with a due date and a counter

Correct Answer: D

QUESTION 2

Which utility blocks a host portscan?

- A. HIDS
- B. sandboxing
- C. host-based firewall
- D. antimalware

Correct Answer: C

QUESTION 3

What is the difference between the rule-based detection when compared to behavioral detection?

- A. Rule-Based detection is searching for patterns linked to specific types of attacks, while behavioral is identifying per signature.
- B. Rule-Based systems have established patterns that do not change with new data, while behavioral changes.
- C. Behavioral systems are predefined patterns from hundreds of users, while Rule-Based only flags potentially abnormal patterns using signatures.
- D. Behavioral systems find sequences that match a particular attack signature, while Rule- Based identifies potential attacks.

Correct Answer: D

QUESTION 4

Refer to the exhibit.

The screenshot displays a malware analysis report for a file named 'VAC-Bypass-Loader.exe'. The report includes the following details:

- File name:** VAC-Bypass-Loader.exe
- Full analysis:** <https://app.any.run/tasks/b6c8538c-0b3d-4e57-8900-863115142a98>
- Verdict:** Malicious activity
- Threats:** nJRAT. A description states: 'nJRAT is a remote access Trojan. It is one of the most widely accessible RATs on the market that features an abundance of educational information. Interested attackers can even find tutorials on YouTube. This allows it to become one of the most popular RATs in the world.'
- Analysis date:** 12/13/2020, 19:21:33
- OS:** Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
- Tags:** trojan, rat, nprat, Metasploit
- Indicators:** [Icons representing various indicators]
- MIME:** application/x-dosexec
- File info:** PE32 executable (GUI) Intel 80386, for MS Windows
- MD5:** 111EE18A3A2310D9EE6765D4630209AT

Where is the executable file?

- A. info
- B. tags
- C. MIME
- D. name

Correct Answer: C

QUESTION 5

An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection.

Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)

- A. signatures
- B. host IP addresses
- C. file size
- D. dropped files
- E. domain names

Correct Answer: BE

[Latest 200-201 Dumps](#)

[200-201 VCE Dumps](#)

[200-201 Study Guide](#)