

➤ **Vendor: Cisco**➤ **Exam Code: 200-201**➤ **Exam Name: 200-201 Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)**➤ **New Updated Questions from [Braindump2go](#) (Updated in [May/2022](#))****[Visit Braindump2go and Download Full Version 200-201 Exam Dumps](#)****QUESTION 260**

A user received a targeted spear-phishing email and identified it as suspicious before opening the content. To which category of the Cyber Kill Chain model does this type of event belong?

- A. weaponization
- B. delivery
- C. exploitation
- D. reconnaissance

Answer: B**QUESTION 261**

According to the NIST SP 800-86, which two types of data are considered volatile? (Choose two.)

- A. swap files
- B. temporary files
- C. login sessions
- D. dump files
- E. free space

Answer: CE**QUESTION 262**

Refer to the exhibit. An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

**[200-201 Exam Dumps](#) [200-201 Exam Questions](#) [200-201 PDF Dumps](#) [200-201 VCE Dumps](#)****<https://www.braindump2go.com/200-201.html>**

- A. The file will appear legitimate by evading signature-based detection.
- B. The file will not execute its behavior in a sandbox environment to avoid detection.
- C. The file will insert itself into an application and execute when the application is run.
- D. The file will monitor user activity and send the information to an outside source.

Answer: B

QUESTION 263

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

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

Answer: D

QUESTION 264

What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

- A. central key management server
- B. web of trust
- C. trusted certificate authorities
- D. registration authority data

Answer: C

QUESTION 265

Which tool gives the ability to see session data in real time?

- A. tcpdstat
- B. trafdump
- C. tcptrace
- D. trafshow

Answer: C

QUESTION 266

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

Answer: D

QUESTION 267

What describes a buffer overflow attack?

- A. injecting new commands into existing buffers

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

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

- B. fetching data from memory buffer registers
- C. overloading a predefined amount of memory
- D. suppressing the buffers in a process

Answer: C

QUESTION 268

Which are two denial-of-service attacks? (Choose two.)

- A. TCP connections
- B. ping of death
- C. man-in-the-middle
- D. code-red
- E. UDP flooding

Answer: BE

QUESTION 269

Refer to the exhibit. Where is the executable file?



File name	VAC-Bypass-Loader.exe
Full analysis	https://app.any.run/tasks/b6c8538c-0b3d-4e57-8900-863115142a98
Verdict	Malware activity
Threats	njRAT 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 cat njrat stealer
Indicators	
MIME	application/x-dosexec
File info	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	111EE18A3A931C05EE6765D463C208A7

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

Answer: C