

[May-2022]Download Braindump2go 200-201 Exam Dumps 200-201 278Q Free[Q260-Q269]

May/2022 Latest Braindump2go 200-201 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 200-201 Real Exam Questions!
QUESTION 260A 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 261According 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 262Refer to the exhibit. An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?



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 263What 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 264What 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 265Which tool gives the ability to see session data in real time?
A. tcpdstat
B. trafddump
C. tcptrace
D. trafshow
Answer: C
QUESTION 266What 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 267What describes a buffer overflow attack?
A. injecting new commands into existing buffers
B. fetching data from memory buffer registers
C. overloading a predefined amount of memory
D. suppressing the buffers in a process
Answer: C
QUESTION 268Which 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 269Refer to the exhibit. Where is the executable file?



A. info
B. tags
C. MIMED
D. name
Answer: C
Resources From: 1. 2022 Latest Braindump2go 200-201 Exam Dumps (PDF & VCE) Free Share: <https://www.braindump2go.com/200-201.html>
2. 2022 Latest Braindump2go 200-201 PDF and 200-201 VCE Dumps Free Share: <https://drive.google.com/drive/folders/1fTPALtM-eluhFW8sUjNGF7Y-ofOP3s-M?usp=sharing>
3. 2021 Free Braindump2go 200-201 Exam Questions Download: [https://www.braindump2go.com/free-online-pdf/200-201-PDF-Dumps\(260-269\).pdf](https://www.braindump2go.com/free-online-pdf/200-201-PDF-Dumps(260-269).pdf)
Free Resources from Braindump2go, We Devoted to Helping You 100% Pass All Exams!