KTest

更に上のクオリティ　更に上のサービス

問題集

http://www.ktest.jp

1年で無料進級することに提供する

Exam : **200-201**

Title : Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Version : DEMO

1.While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header.
Which technology makes this behavior possible?
A. encapsulation
B. TOR
C. tunneling
D. NAT
Answer: D

2.When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification.
Which information is available on the server certificate?
A. server name, trusted subordinate CA, and private key
B. trusted subordinate CA, public key, and cipher suites
C. trusted CA name, cipher suites, and private key
D. server name, trusted CA, and public key
Answer: D

3.A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor.
Which type of evidence is this?
A. best evidence
B. prima facie evidence
C. indirect evidence
D. physical evidence
Answer: C

4.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
Answer: AB
Explanation:
Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

5.Which utility blocks a host portscan?
A. HIDS
B. sandboxing
C. host-based firewall
D. antimalware
Answer: C