VCE & PDF
GeekCert.com

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.geekcert.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

A system administrator is ensuring that specific registry information is accurate.

Which type of configuration information does the HKEY_LOCAL_MACHINE hive contain?

A. file extension associations

B. hardware, software, and security settings for the system

C. currently logged in users, including folders and control panel settings

D. all users on the system, including visual settings

Correct Answer: B

https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows- registry-advanced-users

QUESTION 2

Refer to the exhibit.

```
Capturing on 'eth0'
    1 0.000000000 ca:4f:4d:4b:38:5a ? Broadcast    ARP 42 Who has 192.168.88.149?
Tell 192.168.88.12
    2 0.000055428 82:69:61:3e:fa:99 ? ca:4f:4d:4b:38:5a ARP 42 192.168.88.149 is at
82:69:61:3e:fa:99
    3 0.000080556 192.168.88.12 ? 192.168.88.149 TCP 74 49098 ? 80 [SYN] Seq=0
Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=65609529 TSecr=0 WS=128
```

What must be interpreted from this packet capture?

A. IP address 192.168.88 12 is communicating with 192 168 88 149 with a source port 74 to destination port 49098 using TCP protocol

B. IP address 192.168.88.12 is communicating with 192 168 88 149 with a source port 49098 to destination port 80 using TCP protocol.

C. IP address 192.168.88.149 is communicating with 192.168 88.12 with a source port 80 to destination port 49098 using TCP protocol.

D. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 49098 to destination port 80 using TCP protocol.

Correct Answer: B

QUESTION 3

What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?

A. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator

B. MAC is the strictest of all levels of control and DAC is object-based access

C. DAC is controlled by the operating system and MAC is controlled by an administrator

D. DAC is the strictest of all levels of control and MAC is object-based access

Correct Answer: B

QUESTION 4

Refer to the exhibit.

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE_11-PolicyGroupName-Identity-
OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy
<IW_comp,6.9,-,"-",-,-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-",
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> -
```

Which technology produced the log?

A. antivirus

B. IPS/IDS

C. firewall

D. proxy

Correct Answer: B

QUESTION 5

Which type of data must an engineer capture to analyze payload and header information?

A. full packet

B. frame check sequence

C. alert data

D. session logs

Correct Answer: A

Latest 200-201 Dumps   200-201 Practice Test   200-201 Study Guide