

## MK0-201<sup>Q&As</sup>

CPTS - Certified Pen Testing Specialist

### Pass Mile2 MK0-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/mk0-201.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Mile2  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



## QUESTION 1

If the DS Client software has been installed on Windows 95, Windows 98, and NT 4 computers, what setting of the LanMan Authentication level should be applied to counteract LanMAN hash sniffing and offline cracking? Choose the best answer.

- A. Send NTLM v2/Refuse LM and NTLM
- B. Send NTLM only
- C. Send LM and NTLM responses
- D. Send NTLM v2/Refuse LM

Correct Answer: A

---

## QUESTION 2

Which of the following might be used to give false positives when a UDP scan is being performed against a DMZ server running DNS? Choose the best answer.

- A. On the firewall, block ICMP TTL Exceeded
- B. On the firewall, block all incoming UDP
- C. On the firewall, block all TCP SYN packets
- D. On the firewall, block all ICMP Port Unreachable messages

Correct Answer: D

---

## QUESTION 3

Bob is doing a penetration test.

He was able to get system level access on one of the servers exploiting one of the known weaknesses of the web server.

Bob attempted to copy the SAM database but it was locked and his operation was not allowed.

How could Bob succeed in getting a copy of the SAM database if it locked while the system is up and running?

- A. By bringing the system to single user mode
- B. By running samdump to create a backup of the SAM
- C. By running rdisk /s to create an unlocked backup copy of the SAM

D. By changing the permissions on the file using his System privileges

Correct Answer: C

---

#### QUESTION 4

Which of the following statements explain why hardware-based keystroke loggers are so dangerous? Choose three.

- A. They are expensive.
- B. They can be installed or removed in seconds.
- C. They are totally transparent to both the operating system and the user applications
- D. Neither system administrator nor users routinely inspect the back of their PCs for suspicious devices

Correct Answer: BCD

---

#### QUESTION 5

Which of the following ports could be associated with a trojan on a Windows computer? Choose two.

- A. 135
- B. 3268
- C. 12345
- D. 27374

Correct Answer: CD

[MK0-201 Practice Test](#)

[MK0-201 Exam Questions](#)

[MK0-201 Braindumps](#)