



# 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.pass4itsure.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**

One key skill a penetration Tester must possess is documentation.

There are different documents that will be produced in the course of doing a penetration test, out of the documents listed below which one would be the most important document that a Penetration Tester must have in order to be performing a test?

- A. Network Diagram
- B. Host and services list
- C. Written Authorization
- D. Security Policies

Correct Answer: C

---

**QUESTION 2**

An attacker is sending packets with no flag set. This is also known as doing a NULL scan. Usually, operating system networking stacks will respond with a RST packet, however, some operating systems do not conform to this behavior and respond inappropriately. Such behavior could allow for the identification of the remote OS being used. Which of the following would be one of the Operating systems that responds differently?

- A. Solaris
- B. Linux
- C. Windows
- D. HP-UX

Correct Answer: C

---

**QUESTION 3**

Mary has learned about the different ways authentication can be implemented on a web site. Which of the following forms of authentication would consist of the most basic form and also the less secure?

- A. Digest Authentication
- B. Basic Authentication
- C. LDAP Authentication
- D. Token Base Authentication

Correct Answer: A

---

**QUESTION 4**

Which of these methods would be considered examples of active reconnaissance? (Choose three.)

- A. Ware dialing
- B. Firewalking
- C. Whois lookup
- D. FTP banner retrieval

Correct Answer: ABD

---

**QUESTION 5**

While performing a penetration test you discover that the system being tested is already compromised by an intruder. Further examination shows the intruder being currently on the system and doing his deeds. As a Certified Penetration Testing Specialist What should you do?

- A. Retaliate immediately and attempt to break into the attacker system before you lose track of where he is doing the attack from.
- B. Suspend your test immediately and advise your client. Once the client gives you authorization you would resume your testing.
- C. Immediately attempt to gather as much information as possible about the intruder, monitor his moves very closely but never attempt to break into this system or retaliate.
- D. Call 911 immediately and then call management to notify them of your prompt action. Once management gives you authorization you can resume your testing.

Correct Answer: B

[Latest MK0-201 Dumps](#)

[MK0-201 VCE Dumps](#)

[MK0-201 Exam Questions](#)