MK0-201 Q&As

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

QUESTION 1

It is common knowledge that a Penetration Test relies on a testers ability to collect information from

different sources.

Only about 35% to 40% of the information collected will be from technical sources.

Which of the following would NOT be one of the common ways for a security tester to collect information?

A. Physical Access

B. Authorized Access

C. Social Access

D. Digital Access

Correct Answer: B

QUESTION 2

Under the Windows platform,there is something refered to as Null Session.

Which of the following statements would best describe what a null session consists of?

A. It is a session where zero bytes of traffic have been transferred

B. It is a session where erroneous commands are being used showing the a lack of knowledge of the user connected.

C. It is a remote session that is established anonymously to a window machine

D. It is a anonymous FTP session under the Windows platform

Correct Answer: C

QUESTION 3

Which tool speeds up offline password cracking by precomputing tables of password hashes?Choose the best answer.

A. John the Ripper

B. Xcrack

C. Rainbow Crack

D. Cisilia

Correct Answer: C

QUESTION 4

Bob is using a new sniffer called Ethereal.

However,it seems that Bob can only see packets that are sent from and to his own network interface card

(NIC).He cannot see any traffic from the other station.

What could be the cause of Bobs problem?(Select two)

A. The NIC is not in promiscuous mode

B. The network is using UDP traffic

C. Bob is connected to a switched network

D. The sniffer does not support Bobs TCP/IP network stack

Correct Answer: AB

QUESTION 5

If the DS Client software has been installed on Windows 95,Windows 98,and NT 4 comptuers,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 NTML

B. Send NTLM only

C. Send LM and NTLM responses

D. Send NTLM v2/Refuse LM

Correct Answer: A