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.passapply.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

You have collected a series of messages that are all encrypted.

You do not have access to the matching plaintext nor do you have any idea of the key and algorithm that

were used to encrypt those messages.You will attempt a crypto attack in order to find the key. How would you call such an attack?

A. chosen Plaintext Attack

B. Known ciphertext attack

C. Chosen Key Attack

D. Cliphertext only attack

Correct Answer: D

QUESTION 2

While doing a penetration test you were able to extract a copy of the password database from a Windows

server using a vulnerable SQL server that had a blank password.

You now have a copy of the password file in LAN Manager Format,you notice two accounts that could be

very interesting to get into.

The first account is the administrator account and there is a terminal user account as well.

It is very likely that the same password might be reused on all hosts for one of these two accounts or both.

Which of the following tools would you to crack the password the fastest?

A. L0pthcrack

B. John the ripper

C. Rainbowcrack

D. CainandAbel buit in cracker

Correct Answer: C

QUESTION 3

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 4

Yannick who is a very smart security tester has mentioned to one of his friends that he has found a way of appending data to an existing file using the built in Windows tools and no third party utility.

This text appended does not affect the functionality,size,or display within traditional file browsing utilities such as dir or Internet Explorer.What is Yannick making reference to in this case?

A. Steganography

B. Hybrid Encryption

C. Alternate Data Streams

D. Append.exe

Correct Answer: C

QUESTION 5

Which of the following best describes a Script Kiddie?

A. A programmer who is less than 18 years old but already creating exploits that take advantage of vulnerabilities in software

B. A programmer who reverses engineer application in order to find weaknesses

C. A person who uses already written software or tools in order to compromise systems

D. A person who mastered scripting language since a very early age

Correct Answer: C