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.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

Clement is someone who greatly enjoys fishing.

Clement recently visited a web site that is very proactive in its attempt to save marine life.

While on the site he downloaded a disobedience kit where his free CPU cycle can help contribute to the noble cause of saving the rainbow trout from extinction. Which of the following terms best describes Clements activity?

A. Compulsive Fishing

B. Hacktivism

C. Green Peace

D. Crackering

Correct Answer: B

QUESTION 2

Which of the following is the most effective way to reduce the threat of social engineering?Choose the best answer.

A. Require employees to sign a computer usage policy

B. Prevent employees from going to happy hour

C. Require employees to communicate only face-to-face

D. Extensive user education on the nature of social engineering

Correct Answer: D

QUESTION 3

Which of the following statements would best describe the act of signing a message with a Digital Signature?

A. The sender creates a hash value of the message he wishes to send He uses his private key to encrypt the hash value. The message and the encrypted hash value are sent to the receiver.

B. The sender creates a hash value of the message he wishes to send. He uses his public key to encrypt the hash value. The message and the encrypted has value are sent to the receiver.

C. The sender creates a hash value of the message he wihes to send. The message and the hash value are sent to the receiver.

D. The sender uses his public key to create a digital signature. The digital signature is sent along with the text message. The receiver will use the sender private key to validate the signature.

Correct Answer: A

QUESTION 4

Which of the following password and encyption cracking methods is guaranteed to successfully crack any password or encryption algorithm?

A. Dictionary

B. Hybrid

C. Brute Force

D. RainbowCrack

Correct Answer: B

QUESTION 5

Which of the following methods would allow an attacker to get access to the local SAM file if the attacker had physical access? Choose three.

A. Reboot with a Linu-based floppy or CD that can read NTFS filesystems

B. Reboot with NTFSDOS floppy and copy the SAM file

C. Physically remove the hard drive and install it as a second drive in another Windows computer

D. Rebooting into Windows using Safe Mode.

Correct Answer: ABC

QUESTION 6

You are concerned about other people sniffing your data while it is travelling over your local network and the internet.

Which of the following would be the most effective countermeauser to protect your data against sniffing while it is in transit?Choose the best answer.

A. Encryption

B. AntiSniff

C. PromiScan

D. Usage of a switch

Correct Answer: A

QUESTION 7

Detailed logging is the enemy of all cracers.

After getting unauthorized access to a computer,a cracker will attempt to disable logging on the remote

hosts that he compromises.

In order to do so there are a few tools that could be used.

Which of the following command lines would disable auditing on a Windows platform?

A. auditpol/disable

B. auditlog/disable

C. auditpol/off

D. auditlog/off

Correct Answer: A

QUESTION 8

Why are Trojans such as Beast a lot harder to detect? Choose the best answer.

A. They use a well known name to hide themselves

B. They inject themselves into another process

C. They have a polymorphic payload

D. They are self garbling and cannot be detected

Correct Answer: B

QUESTION 9

Why is it more difficult to sanitize information about a company that has publicly-traded stock?Choose the best answer.

A. The company wants to promote itself as much as possible

B. The company must regularly submit financial information to the Securities and Exchange Commission which is then made public

C. It is impossible to remove information from search engines databases

D. The company must hire a security consultant with the expertise to santize the information.

Correct Answer: B

QUESTION 10

Which tools are capable of capturing Kerberos domain authentication credentials and then running either dictionary or brute force offline password cracking?Choose two.

A. LC5

B. Cain and Abel

C. Ettercap

D. Kerbsniff and kerbcrack

Correct Answer: BD

QUESTION 11

Why is it important to the security of a network to create a complex password for the SA account on a MSSQL server installation?

A. The SA account is a pseudo-account and does not have any privileges.

B. The SA account can add/delete or change Domain User accounts.

C. The SA account can have privileges of the local adminstrators group on the host OS.

D. The SA account is the most powerful account on the domain controller.

Correct Answer: C

QUESTION 12

Which of the following countermeasures could be taken to implement security through obscurity and thus limit reconnaissance if an attacker issues this command against a web server? Choose the best answer.

nc www.domain.com 80

GET HEAD HTTP/1.1

[return]

[return]

A. Change the default error messages

B. Change the webservers banner

C. Enable SYN flood protection on a capable firewall

D. Change the default homepage

Correct Answer: B

QUESTION 13

From the items listed below,which would be expected from a cracker or hacker but NOT from an Ethical Hacker or Certified Penetration tester?

A. Code of ethics

B. Signed Authorization

C. Disregard for potential losses

D. Presentation of a detailed report

Correct Answer: C

QUESTION 14

Clement is someone who greatly enjoys fishing.

Clement recently visited a web site that is very proactive in its attempt to save marine life.

While on the site he downloaded a disobedience kit where his free CPU cycle can help contribute to the

noble cause of saving the rainbow trout from extinction.

Which of the following terms best describes Clementss activity?

A. Compulsive Fishing

B. Hacktivism

C. Green Peace

D. Crackering

Correct Answer: B

QUESTION 15

Which of the following actions can often be used as countermeasures to port scans?Choose all that apply.

A. Block unassigned port traffic

B. Monitor transport-layer connections (control of TCP,SYN,RST,ACK)

C. Block ICMP type 3 and 8

D. Use active network monitoring

Correct Answer: ABCD

MK0-201 Practice Test MK0-201 Exam Questions MK0-201 Braindumps