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

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

QUESTION 1

What sniffer program is capable of reconstructing associated TCP packets into a sessions showing application layer data from the client to the server and vice-versa?Choose the best 2 answers.

A. Packetyzer

B. Etherape

C. Ethereal

D. ARPwatch

Correct Answer: AC

QUESTION 2

The Advanced Encryption Standard (AES) was released to protect sensitive data used by

A. S.Government organizations. Up to what classification level was AES built for?

B. Up to Top Secret

C. Up to Secret

D. Up to Confidential

E. Unclassified Information Only

Correct Answer: D

QUESTION 3

Looking at the graphic presented below,what destination port is highlighted in the Hex dump presented? Extract the information from the Hex dump packet captured below.

A. 53

B. 69

C. 50

D. 80

Correct Answer: D

QUESTION 4

What technologies could a company deploy to protect all data passing from an employees home computer to the

corporate intranet?Choose two.

A. L2TP/IPsec

B. PPTP/MPPE

C. WEP

D. IKE

Correct Answer: AB

QUESTION 5

Keystroke loggers can be found in which of the following forms?Choose all that apply.

A. Trojans

B. Spyware

C. Text files

D. A dynamic link library file which replaces the standard GINA.dII

Correct Answer: ABD

QUESTION 6

Which of the following capabilities do rootkits have?Choose all that apply.

A. Hide any file

B. Hide any process

C. Hide any listening port

D. Cause a blue screen of death on Windows computers

Correct Answer: ABCD

QUESTION 7

One of your clients has been the victim of a brute force attack against their SSH server.

They ask you what could be done to protect their Linux servers.You propose the use of IP Tables (the built in kernel firewall) to limit connection attempts to protect their servers.You agree with your client to limit connections to the SSH port to a maximum of only three trials per minutes consideirng there is only one administrator who has a valid need to connect remotely onto this port.

If the threshold of three connectors is exceeded,the attacker will have to wait for another 60 seconds before it will resume allowing connections again.

Which of the following IP Tables entry would meet your clients needs?

A. iptables-A INPUT -p tcp -dport 23 -m state -state NEW -m recent -update -second 60 -hitcount4 -rttl name SSH -j DROP

B. iptables-A INPUT -p tcp -dport 22 -m state -state NEW -m recent -update -second 60 -hit count3 -rttl name SSH -j DROP

C. iptables-A INPUT -p tcp -dport 22 -m state -state NEW -m recent -update -second 60 -hitcount4 -rttl name SSH -j DROP

D. iptables-A OUTPUT -p tcp -dport 23 -m state -state NEW -m recent -update -second 60 -hitcount4 -rttl name SdSH -j DROP

Correct Answer: C

QUESTION 8

What are some of the weaknesses that make LAN Manager Hashes much easier to crak by an attacker? (Select all that apply.)

A. The 14 character paasword is split in two

B. The password is converted to Uppercase

C. The hash value is encrypted using MD5

D. The hash value is encrypted with AES

Correct Answer: AB

QUESTION 9

When conducting a TCP scan for SQL servers on a given network address range,what port is being interrogated?

A. 1453

B. 1334

C. 1433

D. 1434

Correct Answer: C

QUESTION 10

Which of the following ports are used by the Simple Network Management Protocol? (Choose two)

A. 161 UDP

B. 161 TCP

C. 161 TCP

D. 162 UDP

Correct Answer: AD

QUESTION 11

MS SQL server makes use of Stored Procedures.There is an extended stored procedure called sp_makewebtask that can be used with data being returned from executed queries.What would you use this stored procedure for?

A. It is used to start a new web server instance

B. It is used to create and HTML page

C. It is used to perform an entry within a database

D. It is used to schedule a job task

Correct Answer: B

QUESTION 12

Pen testing is another area of security where acronyms and expressions abound. What does the term rooting refers to?

A. Getting access to the root directory

B. Getting administrator access on a Linux system

C. Getting administrator access on a Windows system

D. Planting a worm that will develop and grow within the system

Correct Answer: B

QUESTION 13

Examining all web pages from a site might be a tedious task.

In order to facilitate such as task you can make use of a web crawler.

Which of the choices presented below would best describe what a web crawler is used for?

A. To test the performance of a web server

B. To perform a load test bringing the remote server to a crawl

C. To created a mirror copy of a website for later inspection

D. To attempt escalating your privilege on a compromised web server

Correct Answer: C

QUESTION 14

Session Hijacking is possible due to which weakness within the TCPIP stack implementation?

A. Initial Sequence Number prediction

B. Flags are not validated properly,it is possible to set all flags to 1 or 0.

C. Validation of the size of a packet after reassembly is not implemented properly.

D. Initial Sequence Number are too low

Correct Answer: A

QUESTION 15

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