MK0-201 Q&As

CPTS - Certified Pen Testing Specialist

QUESTION 1

On Wireless networks, what is the Service Set Identify used for?

A. It is the network password

B. It is used on the primary key for WEP

C. It is used to distinguish one network from another

D. It is used to authenticate clients.

Correct Answer: C

QUESTION 2

Which of the following scanning methods would be the most stealthy and best at hiding the source of a scan?

A. TCP Connect()

B. Syn-Ack

C. Fin-Ack

D. Idlescan

Correct Answer: D

QUESTION 3

One of the challenges when doing large scale security tests is the time required.

If you have to scan a class B network it might take you a very long time. Scanrand is a tool that has been optimized to scan a large number of hosts in very little time.It was reported that it was used to scan about 8300 web servers in less than 4 seconds.

How does scanrand achieve such an impressive benchmark?

A. It does not maintain any state

B. It makes use of multiple Network Interface Cards (NIC)

C. It has a probabilistic algorithm that can predict if a port is open or not

D. It does not attempt to use UDP due to the overhead involved

Correct Answer: A

QUESTION 4

Mae i a keen system administration; she constantly monitors the mailing list for best practices that are being used out in the field.On the servers that she maintains,Mae has renamed the administrator account to another name to avoid abuse from crackers.However,she found out that it was possible using the sid2user tool to find the new name she used for the administrator account.Mae does not understand; she has NOT shared this name with anyone.How can this be?What is the most likely reason?

A. Her system have been compromised

B. Renaming the administrator account does not change the SID

C. She has not applied all of the patches

D. Someone social engineered her

Correct Answer: B

QUESTION 5

Noah,a penetration tester,has been asked by TestKing.com to perform a security test against the company

network from an internal location.

The owner of TestKing.com has provided Noah with a network diagram,documentations,and assistance.

Which of the following would best describe the type of test that Noah is about to perform?

A. Black Box

B. Zero Knowledge

C. White Box

D. Gray Box

Correct Answer: C

QUESTION 6

While exploiting remote targets using exploits,there are a few stages that have to take place. Which of the following stages is the payload which is executed after exploitation?

A. Shellcode

B. Injection Vector

C. Request Builder

D. Handler routine

Correct Answer: A

QUESTION 7

Password attack fall within two main categories:Social Attacks and Digital Attacks. Which of the following would not be considered a Social Attack on passwords?

A. Social Engineering

B. Shoulder Surfing

C. Dumpster Diving

D. Dictionary Attack

Correct Answer: D

QUESTION 8

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 9

Which of the following is the best security risk that has been experienced within applications over the past few years?

A. Buffer Overflow

B. Heap Overflow

C. String Overflow

D. Format Bug Overflow

Correct Answer: A

QUESTION 10

Which of the following commands would capture all packets going to and from IP address 192.168.1.2 using tcpdump?

A. tcpdump host 192.168.1.2

B. tcpdump dest 192.168.1.2

C. tcpdump any 192.168.1.2/32

D. tcpdump all 192.168.1.2/24

Correct Answer: A

QUESTION 11

Jhezza has just arrived at her office and she is checking her stock portfolio as she does every day.

She connects to her broker web site and decides to buy some stocks that are highly recommended. She makes use of her special Portfolio Credit Card because she wishes to collect travel points.

A few weeks later, Jhezza realized that someone has compromissed her credit Card number and has been doing fraudulent trasactions online,the first of which is on the same day she used it to buy stocks from her office.

How did the Card number get compromised?

A. By a Man in the middle attack

B. By someone who read her emails

C. By someone who was able to perform a FTP server spoofing

D. By a Meet in the middle attack,which comprosmises encryption

Correct Answer: A

QUESTION 12

While doing your testing you discover an MS SQL server within the target range.You attempt to connect to the SA account using the default password which is usually blank.You quickly find out it is not working and the password was changed.Which of the following tools could be used to attempt finding what the new password could be?

A. sqlexec

B. sql2.exe

C. sqlbf

D. Buildsql

Correct Answer: C

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

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 15

Which of the following password implementation is found only in Windows 2000 and newer Windows versions?

A. LM

B. NTLM

C. NTLMv2

D. Kerberos

Correct Answer: D