MK0-201$^{Q\&As}$

CPTS - Certified Pen Testing Specialist

Pass Mile2 MK0-201 Exam with 100% Guarantee

QUESTION 1

Cracking encryption is often impossible due to time constraints whereby it would take hundreds of years in some cases.

Great advancement has taken place lately regarding the cracking of password based on the time memory trade-off.

Such an attack allows an attacker to crack the password within a very short period of time.

Under the memory trade-off technique,which of the followig would be used to speed the cracking of password?

A. Large dictionaries

B. Large collection of common passwords

C. Pre Computed hashes tables

D. Pre sorted dictionaries will most likely matches tried first

Correct Answer: C

QUESTION 2

Which of the following might be used to give false positives when a UDP scan is being performed against a DMZ server running DNS? Choose the best answer.

A. On the firewall,block ICMP TTL Exceeded

B. On the firewall,block all incoming UDP

C. On the firewall,block all TCP SYN packets

D. On the firewall,block all ICMP Port Unreachable messages

Correct Answer: D

QUESTION 3

A malicious hacker has been trying to penetrate TestKing.com from an external network location.He has tried every trick in his bag but still did not succeed.

From the choice presented below,what type of logical attempt is he most likely to attempt next?

A. Elevation of privileges

B. Pilfering of data

C. Denial of service

D. Installation of a back door

Correct Answer: C

QUESTION 4

You have successfully exploited a remote computer.You now have limited privilege on the remote computer.

You tests have revealed that it is possible to download files from the internet but the size of the limited to less than 60K.

You would like to escalate your privilege by scanning the internal network and also setup a permanent backdoor that would allow you to return to the compromised host at will.

Which of the following tools could be used for such purpose?

A. Hijack This

B. Netcat

C. ButtSniff

D. BackOrifice

Correct Answer: B

QUESTION 5

Johny has been trying to defeat a crypto system for some time. He has in his possession a whole

collection of ciphertext documents that were captured from the network.

However,he does not know what algorithm or plain text was used to create this ciphertext.

Through statistical analysis he is attempting to decipher the encrypted text.

What would you call such an attack?

A. Known Plaintext attack

B. Ciphertext Only Attack

C. Chosen Ciphertext Attack

D. Chosen Plaintext Attack

Correct Answer: B

QUESTION 6

Which are methods that attackers use to find buffer overflows?Choose all that apply.

A. Trial and error

B. Decompile the executable binary of the application

C. Decompile the executable binary of a software patch

D. Analyze source code,if available

Correct Answer: ABCD

QUESTION 7

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 8

Types of potential vulnerabilities that are commonly scanned for include:(Choose All that Apply)

A. Password vulnerabilities

B. Weak operating system and application default settings

C. Common configuration and coding mistakes

D. Protocol vulnerabilities (such as the TCP/IP stack vulnerabilities)

E. Physical observation of the target building

Correct Answer: ABCD

QUESTION 9

Which scripting language do most open source vulnerability scanners use?

A. ASNL (Automated Security Nessus Language)

B. NASL (Nessus Attack Scripting Language)

C. SANL (Security Attack Nessus Language)

D. NASA (Nessus Automated Security Attack)

Correct Answer: B

QUESTION 10

When a digital certificate has been revoked before its expiry date,how will the Certification Authority (CA) that issued the certificate inform other CAs that the specific certificate is no longer valid.

A. By posting it on the CA web site

B. By sending an email message to the other CAs

C. By posting it on the certificate revocation list

D. By posting it on the certificate expiry list

Correct Answer: C

QUESTION 11

Which programs might an attacker use to facililate sniffing in a switched network?Choose all that apply.

A. Ettercap

B. Cain and Abel

C. MACof

D. Etherflood

Correct Answer: ABCD

QUESTION 12

To block tunneling remote access trojans like 007Shell,what should you do on your firewall?Choose the best answer.

A. Block all IGMP

B. Block UDP port 1900

C. Block all ICMP

D. Block TCP port 27374

Correct Answer: C

QUESTION 13

Henry and Paul are debating the purchase of a $1500-00 automated vulnerability software package.What is the main disadavantage regarding the automated compared to manual assessments:

A. The network manager gets personal commission when purchasing the software package.

B. False Positive negative results

C. Greater degree of accuracy

D. Reducing Workforce costs

Correct Answer: B

QUESTION 14

A normal TCP connection is always established by using what is called a TCP Three Way Handshake. Which of the packet sequences below would represent a normal TCP connection establishment?

A. SYN,SYN/ACK,ACK

B. SYN,PSH,ACK

C. ACK,SYY,SYN/ACK

D. FIN,ACK,SYN

Correct Answer: A

QUESTION 15

Spyware is either hardware or software installed on a computer which gather information about the user for later retrieval by whoever controls the Spyware.

It is installed without the users knowledge.

What are the two categories of Spyware that exist?(Choose two from the list below)

A. Surveillance

B. Screen capture

C. key loggers

D. Advertising

Correct Answer: AD