100% Money Back Guarantee

Vendor: Mile2

Exam Code:MK0-201

Exam Name:CPTS - Certified Pen Testing Specialist

Version: Demo

QUESTION 1

Which of the following techniques would be effective to get around some of the blocking rules on certain firewalls?

The same technique could be used to avoid detection by intrusion Detection Systems (IDS) in some cases.

A. Injection

B. Spoofing

C. Fragmentation

D. Diffusion

Correct Answer: C

QUESTION 2

Keen administrators (the enemy of penetration testers)will take great steps in order to collect logs on different servers.By having a detailed log of activities they may be able to detect abnormal activities.

A skilled intruder will attempt to modify the logging policy in order to prevent the administrator from having access to his detailed log.What command line tool could an attacker use to disable auditing on a Windows server?

A. Syslog

B. Eventlog

C. Auditpol

D. Auditlog

Correct Answer: C

QUESTION 3

Bob has just produced a very detailed penetration testing report for his client.Bob wishes to ensure that the report will not be changed in storage or in transit.What would be the best tool that Bob can use to assure the integrity of the information and detect any changeds that could have happend to the report while being transmitted or stored?

A. A Symmetric Encryption Algorithm

B. An Asymmetric Encryption Algorithm

C. An Hashing Algorithm

D. The ModDetect Algorithm

Correct Answer: C

QUESTION 4

John is attempting to reduce the likelihood that his Linux server could be compromised through exploitation of ports and services that are not necessary or through the use of packets that might be out of state,modified,or malicious.His first step will be to configure the built in firewall that exists on the recent Linux version. What is the name of the user space program used to configure this firewall?

A. IPChains

B. IPwall

C. IPTables

D. IPFW

Correct Answer: C

QUESTION 5

If the DS Client software has been installed on Windows 95,Windows 98, and NT 4 computers,what setting of the LanMan Authentication level should be applied to counteract LanMAn hash sniffing and offline cracking?Choose the best answer.

A. Send NTLM v2/Refuse LM and NTLM

B. Send NTLM only

C. Send LM and NTLM responses

D. Send NTLM v2/Refuse LM

Correct Answer: A

QUESTION 6

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 7

Which of the following is a MS Access database SQL injection script?

A. OR a=a

B. AND 1=1

C. OR 1=1

D. SELECT *FROM*

Correct Answer: A

QUESTION 8

Given the following diagram,what ports shouldbe blocked on the perimeter and internal firewall to best protect the Microsoft SQL databae server from unauthorized inbound connections?

A. 1433, 1434

B. 443, 434

C. 1443,1444

D. 80,139

Correct Answer: A

QUESTION 9

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 10

Which of the following resource records would you inspect to find out how long a cache poisoning attack might be effective against a remote DNS server?

A. MX

B. NS

C. SOA

D. PTR

Correct Answer: C

QUESTION 11

You have been asked to assist an investigation team in collecting data and evidence related to an internal hacking case.

The investigator in charge of the case would like to capture all keystrokes from the suspect but is afraid the employee under investigation who possesses great technical skills might have installed integrity tools on his system that would detect any new software installed.

What solution would be best to use to reach the investigator requirement?

A. Disable the integrity tools in place

B. Install a software key logger that does not show in the process list

C. Install a hardware based key logger

D. Sniff all traffic and keystrokes from the network

Correct Answer: C

QUESTION 12

Bob has just produced a very detailed penetration testing report for his client.Bob wishes to ensure that the report will not be chnaged in storage or in transit.What would be the best tool that Bob can use to aasure the integrity of the information and detect any changes that could have happened to the report while being transmitted or stored?

A. A Symmetric Encryption Algorithm

B. An Asymmetric Encryption Algorithm

C. An Hashing Algorithm

D. The ModDetect Algorithm

Correct Answer: C