SEC504 Q&As

Hacker Tools, Techniques, Exploits and Incident Handling

Pass SANS SEC504 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/sec504.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by SANS Official Exam Center

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

QUESTION 1

You work as a Senior Marketing Manager for Umbrella Inc. You find out that some of the software applications on the systems were malfunctioning and also you were not able to access your remote desktop session. You suspected that some malicious attack was performed on the network of the company. You immediately called the incident response team to handle the situation who enquired the Network Administrator to acquire all relevant information regarding the malfunctioning. The Network Administrator informed the incident response team that he was reviewing the security of the network which caused all these problems. Incident response team announced that this was a controlled event not an incident.

Which of the following steps of an incident handling process was performed by the incident response team?

A. Containment

B. Eradication

C. Preparation

D. Identification

Correct Answer: D

QUESTION 2

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.

A. IIS buffer overflow

B. NetBIOS NULL session

C. SNMP enumeration

D. DNS zone transfer

Correct Answer: A

QUESTION 3

In which of the following attacks does an attacker spoof the source address in IP packets that are sent to the victim?

A. Dos

B. DDoS

C. Backscatter

D. SQL injection

Correct Answer: C

QUESTION 4

John, a part-time hacker, has accessed in unauthorized way to the www.yourbank.com banking Website and stolen the bank account information of its users and their credit card numbers by using the SQL injection attack. Now, John wants to sell this information to malicious person Mark and make a deal to get a good amount of money. Since, he does not want to send the hacked information in the clear text format to Mark; he decides to send information in hidden text. For this, he takes a steganography tool and hides the information in ASCII text by appending whitespace to the end of lines and encrypts the hidden information by using the IDEA encryption algorithm.

Which of the following tools is John using for steganography?

A. Image Hide

B. 2Mosaic

C. Snow.exe

D. Netcat

Correct Answer: C

QUESTION 5

Which of the following statements are true regarding SYN flood attack?

A. The attacker sends a succession of SYN requests to a target system.

B. SYN flood is a form of Denial-of-Service (DoS) attack.

C. The attacker sends thousands and thousands of ACK packets to the victim.

D. SYN cookies provide protection against the SYN flood by eliminating the resources allocated on the target host.

Correct Answer: ABD

QUESTION 6

Which of the following incident response team members ensures that the policies of the organization are enforced during the incident response?

A. Information Security representative

B. Legal representative

C. Human Resource

D. Technical representative

Correct Answer: C

QUESTION 7

Which of the following tasks can be performed by using netcat utility? Each correct answer represents a complete solution. Choose all that apply.

A. Checking file integrity

B. Creating a Backdoor

C. Firewall testing

D. Port scanning and service identification

Correct Answer: BCD

QUESTION 8

Which of the following penetration testing phases involves reconnaissance or data gathering?

A. Attack phase

B. Pre-attack phase

C. Post-attack phase

D. Out-attack phase

Correct Answer: B

QUESTION 9

You want to measure the number of heaps used and overflows occurred at a point in time. Which of the following commands will you run to activate the appropriate monitor?

A. UPDATE DBM CONFIGURATION USING DFT_MON_TABLE

B. UPDATE DBM CONFIGURATION DFT_MON_TIMESTAMP

C. UPDATE DBM CONFIGURATION USING DFT_MON_BUFPOOL

D. UPDATE DBM CONFIGURATION USING DFT_MON_SORT

Correct Answer: D

QUESTION 10

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.wearesecure.com. He enters a single quote in the input field of the login page of the We-are-secure Web site and receives the following error message:

Microsoft OLE DB Provider for ODBC Drivers error \\'0x80040E14\\'

This error message shows that the We-are-secure Website is vulnerable to _____.

A. A buffer overflow

B. A Denial-of-Service attack

C. A SQL injection attack

D. An XSS attack

Correct Answer: C

QUESTION 11

Which of the following wireless network security solutions refers to an authentication process in which a user can connect wireless access points to a centralized server to ensure that all hosts are properly authenticated?

A. Remote Authentication Dial-In User Service (RADIUS)

B. IEEE 802.1x

C. Wired Equivalent Privacy (WEP)

D. Wi-Fi Protected Access 2 (WPA2)

Correct Answer: B

QUESTION 12

Peter works as a Network Administrator for the PassGuide Inc. The company has a Windows-based network. All client computers run the Windows XP operating system. The employees of the company complain that suddenly all of the client computers have started working slowly. Peter finds that a malicious hacker is attempting to slow down the computers by flooding the network with a large number of requests.

Which of the following attacks is being implemented by the malicious hacker?

A. SQL injection attack

B. Denial-of-Service (DoS) attack

C. Man-in-the-middle attack

D. Buffer overflow attack

Correct Answer: B

QUESTION 13

Which of the following statements about a Trojan horse are true? Each correct answer represents a complete solution.

Choose two.

A. It is a macro or script that attaches itself to a file or template.

B. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.

C. It is a malicious software program code that resembles another normal program.

D. It infects the boot record on hard disks and floppy disks.

Correct Answer: BC

QUESTION 14

Mark works as a Network Administrator for Perfect Inc. The company has both wired and wireless networks. An attacker attempts to keep legitimate users from accessing services that they require. Mark uses IDS/IPS sensors on the wired network to mitigate the attack.

Which of the following attacks best describes the attacker\\'s intentions?

A. Internal attack

B. Reconnaissance attack

C. Land attack

D. DoS attack

Correct Answer: D

QUESTION 15

You want to create an SSH tunnel for POP and SMTP protocols. Which of the following commands will you run?

A. ssh -L 110:mailhost:110 -L 25

B. ssh -L 110:mailhost:110 -L 25:mailhost:25 -1

C. ssh -L 25:mailhost:110 -L 110

D. ssh -L 110:mailhost:110 -L 25:mailhost:25 -1 user -N mailhost

Correct Answer: D