



Free Questions for [SEC504](#) by [braindumpscollection](#)

Shared by [Swanson](#) on [15-04-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

Which of the following practices come in the category of denial of service attack?

Each correct answer represents a complete solution. Choose three.

Options:

- A- Performing Back door attack on a system
- B- Disrupting services to a specific computer
- C- Sending thousands of malformed packets to a network for bandwidth consumption
- D- Sending lots of ICMP packets to an IP address

Answer:

B, C, D

Question 2

Question Type: MultipleChoice

Which of the following statements about buffer overflow are true?

Each correct answer represents a complete solution. Choose two.

Options:

- A-** It is a situation that occurs when a storage device runs out of space.
- B-** It is a situation that occurs when an application receives more data than it is configured to accept.
- C-** It can improve application performance.
- D-** It can terminate an application.

Answer:

B, D

Question 3

Question Type: MultipleChoice

Adam works as a Security Analyst for Umbrella Inc. CEO of the company ordered him to implement two-factor authentication for the employees to access their networks. He has told him that he would like to use some type of hardware device in tandem with a security or

identifying pin number. Adam decides to implement smart cards but they are not cost effective.

Which of the following types of hardware devices will Adam use to implement two-factor authentication?

Options:

- A- Biometric device
- B- Security token
- C- Proximity cards
- D- One Time Password

Answer:

B

Question 4

Question Type: MultipleChoice

Which of the following tools are used as a network traffic monitoring tool in the Linux operating system?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A- Netbus

B- IPTraf

C- MRTG

D- Ntop

Answer:

B, C, D

Question 5

Question Type: MultipleChoice

Which of the following penetration testing phases involves gathering data from whois, DNS, and network scanning, which helps in mapping a target network and provides valuable information regarding the operating system and applications running on the systems?

Options:

- A- Post-attack phase
- B- On-attack phase
- C- Attack phase
- D- Pre-attack phase

Answer:

D

Question 6

Question Type: MultipleChoice

Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing department has been affected by a malicious hacking attack. Supervisors are also claiming that some sensitive data are also stolen.

Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to image the entire system. He captures volatile data, such as running process, ram, and network connections.

Which of the following steps of the incident handling process is being performed by Adam?

Options:

A- Recovery

B- Eradication

C- Identification

D- Containment

Answer:

D

Question 7

Question Type: FillInTheBlank

with the appropriate term.

_____ is a technique used to make sure that incoming packets are actually from the networks that they claim to be from.

Answer:

Question 8

Question Type: MultipleChoice

You are concerned about rootkits on your network communicating with attackers outside your network. Without using an IDS how can you detect this sort of activity?

Options:

- A- By examining your domain controller server logs.
- B- You cannot, you need an IDS.
- C- By examining your firewall logs.
- D- By setting up a DMZ.

Answer:

C

Question 9

Question Type: MultipleChoice

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint.

Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?

Options:

- A- nmap -sS
- B- nmap -sU -p
- C- nmap -O -p
- D- nmap -sT

Answer:

C

Question 10

Question Type: MultipleChoice

You want to add a netbus Trojan in the chess.exe game program so that you can gain remote access to a friend's computer. Which of the following tools will you use to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A- Tripwire

B- Yet Another Binder

C- Pretator Wrapper

D- Beast

Answer:

B, C

Question 11

Question Type: MultipleChoice

Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts. Which of the following attacks is being used by Eve?

Options:

- A- Replay
- B- Firewalking
- C- Session fixation
- D- Cross site scripting

Answer:

A

To Get Premium Files for SEC504 Visit

<https://www.p2pexams.com/products/sec504>

For More Free Questions Visit

<https://www.p2pexams.com/sans/pdf/sec504>

