

312-50V7^{Q&As}

Ethical Hacking and Countermeasures (CEHv7)

Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

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

<https://www.certbus.com/312-50v7.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

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



QUESTION 1

This attack technique is used when a Web application is vulnerable to an SQL Injection but the results of the Injection are not visible to the attacker.

- A. Unique SQL Injection
- B. Blind SQL Injection
- C. Generic SQL Injection
- D. Double SQL Injection

Correct Answer: B

QUESTION 2

Which type of password cracking technique works like dictionary attack but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

- A. Dictionary attack
- B. Brute forcing attack
- C. Hybrid attack
- D. Syllable attack
- E. Rule-based attack

Correct Answer: C

QUESTION 3

Which type of scan is used on the eye to measure the layer of blood vessels?

- A. Facial recognition scan
- B. Retinal scan
- C. Iris scan
- D. Signature kinetics scan

Correct Answer: B

QUESTION 4

Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

- A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
- B. The root CA stores the user's hash value for safekeeping.
- C. The CA is the trusted root that issues certificates.
- D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

Correct Answer: C

QUESTION 5

Which of the following is a preventive control?

- A. Smart card authentication
- B. Security policy
- C. Audit trail
- D. Continuity of operations plan

Correct Answer: A

QUESTION 6

This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data. See foobar What is this attack?

- A. Cross-site-scripting attack
- B. SQL Injection
- C. URL Traversal attack
- D. Buffer Overflow attack

Correct Answer: A

QUESTION 7

You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running on ports 21, 110 and 123.

Here is the output of your scan results:

```
PORT      STATE      SERVICE    VERSION
21/tcp    open       ftp        vsftpd 2.0.7
110/tcp   open       pop3       Courier pop3d
123/tcp   closed     ntp
```

```
Device type: general purpose
Running: Linux 2.8.X
```

```
OS details: Linux 2.8.18, Linux 2.8.20 - 2.8.24
Uptime: 65.658 days (since Mon Jun 19 00:43:29 2011)
Network Distance: 0 hops
Service Info: OS: Unix
```

Which of the following nmap command did you run?

- A. nmap -A -sV -p21,110,123 10.0.0.5
- B. nmap -F -sV -p21,110,123 10.0.0.5
- C. nmap -O -sV -p21,110,123 10.0.0.5
- D. nmap -T -sV -p21,110,123 10.0.0.5

Correct Answer: C

QUESTION 8

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

- A. The gateway is not routing to a public IP address.
- B. The computer is using an invalid IP address.
- C. The gateway and the computer are not on the same network.
- D. The computer is not using a private IP address.

Correct Answer: A

QUESTION 9

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results? TCP port 21 no

response TCP port 22 no response TCP port 23 Time-to-live exceeded

- A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
- B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
- C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall.
- D. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

Correct Answer: C

QUESTION 10

Perimeter testing means determining exactly what your firewall blocks and what it allows. To conduct a good test, you can spoof source IP addresses and source ports. Which of the following command results in packets that will appear to originate from the system at 10.8.8.8? Such a packet is useful for determining whether the firewall is allowing random packets in or out of your network.

- A. `hping3 -T 10.8.8.8 -S netbios -c 2 -p 80`
- B. `hping3 -Y 10.8.8.8 -S windows -c 2 -p 80`
- C. `hping3 -O 10.8.8.8 -S server -c 2 -p 80`
- D. `hping3 -a 10.8.8.8 -S springfield -c 2 -p 80`

Correct Answer: D

QUESTION 11

Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

- A. Configure Port Security on the switch
- B. Configure Port Recon on the switch
- C. Configure Switch Mapping
- D. Configure Multiple Recognition on the switch

Correct Answer: A

QUESTION 12

This method is used to determine the Operating system and version running on a remote target system. What is it called?

- A. Service Degradation
- B. OS Fingerprinting
- C. Manual Target System
- D. Identification Scanning

Correct Answer: B

QUESTION 13

Which of the following is optimized for confidential communications, such as bidirectional voice and video?

- A. RC4
- B. RC5
- C. MD4
- D. MD5

Correct Answer: A

QUESTION 14

Hampton is the senior security analyst for the city of Columbus in Ohio. His primary responsibility is to ensure that all physical and logical aspects of the city's computer network are secure from all angles. Bill is an IT technician that works with Hampton in the same IT department. Bill's primary responsibility is to keep PC's and servers up to date and to keep track of all the agency laptops that the company owns and lends out to its employees. After Bill setup a wireless network for the agency, Hampton made sure that everything was secure. He instituted encryption, rotating keys, turned off SSID broadcasting, and enabled MAC filtering. According to agency policy, only company laptops are allowed to use the wireless network, so Hampton entered all the MAC addresses for those laptops into the wireless security utility so that only those laptops should be able to access the wireless network.

Hampton does not keep track of all the laptops, but he is pretty certain that the agency only purchases Dell laptops. Hampton is curious about this because he notices Bill working on a Toshiba laptop one day and saw that he was on the Internet. Instead of jumping to conclusions, Hampton decides to talk to Bill's boss and see if they had purchased a Toshiba laptop instead of the usual Dell. Bill's boss said no, so now Hampton is very curious to see how Bill is accessing the Internet. Hampton does site surveys every couple of days, and has yet to see any outside wireless network signals inside the company's building.

How was Bill able to get Internet access without using an agency laptop?

- A. Bill spoofed the MAC address of Dell laptop
- B. Bill connected to a Rogue access point
- C. Toshiba and Dell laptops share the same hardware address
- D. Bill brute forced the Mac address ACLs

Correct Answer: A

QUESTION 15

Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

- A. They are written in Java.
- B. They send alerts to security monitors.
- C. They use the same packet analysis engine.
- D. They use the same packet capture utility.

Correct Answer: D

[312-50V7 VCE Dumps](#)

[312-50V7 Study Guide](#)

[312-50V7 Exam Questions](#)