# ECSAV10 $^{Q\&As}$

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

## Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

**QUESTION 1**

John is working as a cloud security analyst in an organization. The management instructed him to implement a technology in the cloud infrastructure which allows the organization to share the underlying cloud resources such as server, storage devices, and network.

Which of the following technologies John must employ?

A. VoIP technology

B. Virtualization technology

C. RFID technology

D. Site technology

Correct Answer: B

**QUESTION 2**

Sam is auditing a web application for SQL injection vulnerabilities. During the testing, Sam discovered that the web application is vulnerable to SQL injection. He starts fuzzing the search field in the web application with UNION based SQL queries, however, he realized that the underlying WAF is blocking the requests.

To avoid this, Sam is trying the following query:

```
UNION/**/SELECT/**/\\'/**/OR/**/1/**/=/**/1
```

Which of the following evasion techniques is Sam using?

A. Sam is using char encoding to bypass WAF

B. Sam is using obfuscated code to bypass WAF

C. Sam is using inline comments to bypass WAF

D. Sam is manipulating white spaces to bypass WAF

Correct Answer: C

**QUESTION 3**

Allen and Greg, after investing in their startup company called Zamtac Ltd., developed a new web application for their company. Before hosting the application, they want to test the robustness and immunity of the developed web application against attacks like buffer overflow, DOS, XSS, and SQL injection. What is the type of the web application security test Allen and Greg should perform?

A. Web fuzzing

B. Web crawling

C. Web spidering

D. Web mirroring

Correct Answer: A

**QUESTION 4**

Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing

B. Double Blind Testing

C. Announced Testing

D. Blind Testing

Correct Answer: B

**QUESTION 5**

How many possible sequence number combinations are there in TCP/IP protocol?

A. 320 billion

B. 32 million

C. 4 billion

D. 1 billion

Correct Answer: C

**QUESTION 6**

Output modules allow Snort to be much more flexible in the formatting and presentation of output to its users. Snort has 9 output plug-ins that push out data in different formats. Which one of the following output plug-ins allows alert data to be written in a format easily importable to a database?

A. unified

B. csv

C. alert_unixsock

D. alert_fast

Correct Answer: B

**QUESTION 7**

George is the network administrator of a large Internet company on the west coast. Per corporate policy,

none of the employees in the company are allowed to use FTP or SFTP programs without obtaining

approval from the IT department.

Few managers are using SFTP program on their computers.

Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal

to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in

Ethereal?

A. net port 22

B. udp port 22 and host 172.16.28.1/24

C. src port 22 and dst port 22

D. src port 23 and dst port 23

Correct Answer: C

**QUESTION 8**

A hacker initiates so many invalid requests to a cloud network host that the host uses all its resources responding to invalid requests and ignores the legitimate requests. Identify the type of attack

A. Denial of Service (DoS) attacks

B. Side Channel attacks

C. Man-in-the-middle cryptographic attacks

D. Authentication attacks

Correct Answer: A

**QUESTION 9**

Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

A. Vulnerability Report

B. Executive Report

C. Client-side test Report

D. Host Report

Correct Answer: B

**QUESTION 10**

Adam is a senior penetration tester at XYZsecurity Inc. He is auditing a wireless network for vulnerabilities.

Before starting the audit, he wants to ensure that the wireless card in his machine supports injection. He decided to use the latest version of aircrack-ng tool.

Which of the following commands will help Adam check his wireless card for injection?

A. aireplay-ng -9 wlan0

B. airodump-ng wlan0

C. airdecap-ng -3 wlan0

D. aireplay-ng -5 –b wlan0

Correct Answer: B

**QUESTION 11**

A web application developer is writing code for validating the user input. His aim is to verify the user input against a list of predefined negative inputs to ensure that the received input is not one among the negative conditions.

Identify the input filtering mechanism being implemented by the developer?

A. Black listing

B. White listing

C. Authentication

D. Authorization

Correct Answer: A

**QUESTION 12**

Fred, who owns a company called Skyfeit Ltd., wants to test the enterprise network for presence of any vulnerabilities and loopholes. He employed a third-party penetration testing team and asked them to perform the penetration testing over his organizational infrastructure. Fred briefed the team about his network infrastructure and provided them with a set of IP addresses on which they can perform tests. He gave them strict instruction not to perform DDoS attacks or access the domain servers in the company. He also instructed them that they can carry out the penetration tests even when the regular employees are on duty since they lack the clue about the happenings. However, he asked the team to take care that no interruption in business continuity should be caused. He also informed the penetration testing team that they get only 1 month to carry out the test and submit the report. What kind of penetration test did Fred ask the third-party penetration testing team to perform?

A. Announced testing

B. Blind testing

C. Grey-Box testing

D. Unannounced testing

Correct Answer: D

**QUESTION 13**

What is the target host IP in the following command?

C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP

A. Firewalk does not scan target hosts

B. 172.16.28.95

C. This command is using FIN packets, which cannot scan target hosts

D. 10.10.150.1

Correct Answer: A

**QUESTION 14**

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She

implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security

measures were taken, none of the hosts on her network can reach the Internet.

Why is that?

A. IPSEC does not work with packet filtering firewalls

B. NAT does not work with IPSEC

C. NAT does not work with statefull firewalls

D. Statefull firewalls do not work with packet filtering firewalls

Correct Answer: B

**QUESTION 15**

A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table: http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype=\\'U\\')=3) WAITFOR DELAY \\'00:00:10\\'-http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY \\'00:00:10\\'-http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY \\'00:00:10\\'-http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY \\'00:00:10\\'-What is the table name?

A. CTS

B. QRT

C. EMP

D. ABC

Correct Answer: C

ECSAV10 Study Guide    ECSAV10 Exam Questions    ECSAV10 Braindumps