ECSAV10$^{Q\&As}$

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

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

https://www.pass2lead.com/ecsav10.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

Which of the following tasks is done after submitting the final pen testing report?

A. Kick-off meeting

B. System patching and hardening

C. Exploiting vulnerabilities

D. Mission briefing

Correct Answer: B

QUESTION 2

Sandra, a wireless network auditor, discovered her client is using WEP. To prove the point that the WEP encryption is very weak, she wants to decrypt some WEP packets. She successfully captured the WEP data packets, but could not reach the content as the data is encrypted.

Which of the following will help Sandra decrypt the data packets without knowing the key?

A. Fragmentation Attack

B. Chopchop Attack

C. ARP Poisoning Attack

D. Packet injection Attack

Correct Answer: B

QUESTION 3

Jason is working on a pen testing assignment. He is sending customized ICMP packets to a host in the target network. However, the ping requests to the target failed with "ICMP Time Exceeded Type = 11" error messages.

What can Jason do to overcome this error?

A. Set a Fragment Offset

B. Increase the Window size in the packets

C. Increase the TTL value in the packets

D. Increase the ICMP header length

Correct Answer: C

QUESTION 4

A disgruntled employee Robert targeted to acquire business secrets of the organization he is working in and wants to sell the same to a competing organization for some financial gain. He started gathering information about the organization and somehow came to know that the organization is conducting a meeting to discuss future business plans. To collect the information about the organization\\'s business plans, he had built a listening device housed in his bag and arrived the meeting location wearing a suit and tie. One of the employees of the organization thought he was a senior executive from other branch who came to attend the meeting and readily took him to the meeting room. Robert waited until that employee left the meeting room and planted listening devices at multiple places in the room. Then, he went outside the building and started listening and recorded all the conversations in the meeting. Identify the type of attack being performed by Robert on the target organization?

A. Vishing

B. Phishing

C. Shoulder surfing

D. Eavesdropping

Correct Answer: D

QUESTION 5

A user unknowingly installed a fake malicious banking app in his Android mobile. This app includes a configuration file that consists of phone numbers of the bank. When the user makes a call to the bank, he is automatically redirected to the number being used by the attacker. The attacker impersonates as a banking official. Also, the app allows the attacker to call the user, then the app displays fake caller ID on the user\\'s mobile resembling call from a legitimate bank. Identify the attack being performed on the Android mobile user?

A. Tailgating

B. SMiShing

C. Vishing

D. Eavesdropping

Correct Answer: C

QUESTION 6

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 7

James is a security consultant at Big Frog Software Pvt Ltd. He is an expert in Footprinting and Social engineering tasks. His team lead tasked him to find details about the target through passive reconnaissance. James used websites to check the link popularity of the client\\'s domain name. What information does the link popularity provide?

A. Information about the network resources

B. Information about visitors, their geolocations, etc.

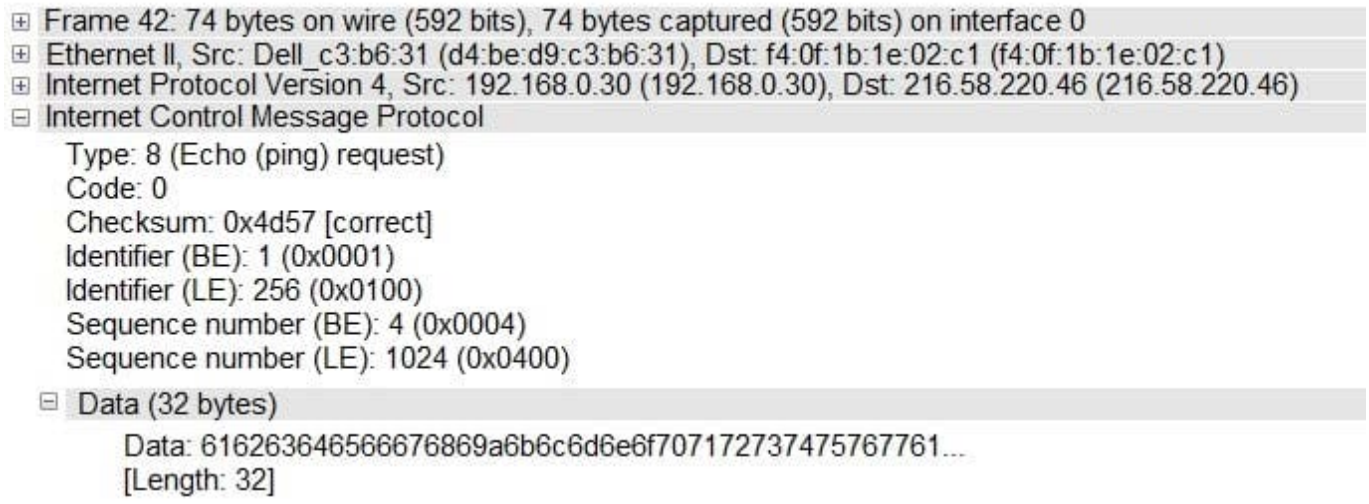
C. Information about the server and its infrastructure

D. Information about the partner of the organization

Correct Answer: D

QUESTION 8

Analyze the ICMP packet below and mark the correct statement.



A. It is a ping packet that requires fragmentation, but the Don\\'t Fragment flag is set

B. It is a ping request, but the destination port is unreachable

C. It is a ping response, when the destination host is unknown

D. It is a ping request, but the destination network is unreachable

Correct Answer: D

QUESTION 9

Christen is a renowned SQL penetration testing specialist in the US. A multinational ecommerce company hired him to check for vulnerabilities in the SQL database. Christen wanted to perform SQL penetration testing on the database by entering a massive amount of data to crash the web application of the company and discover coding errors that may lead to a SQL injection attack. Which of the following testing techniques is Christen using?

A. Fuzz Testing

B. Stored Procedure Injection

C. Union Exploitation

D. Automated Exploitation

Correct Answer: A

QUESTION 10

Michael, a Licensed Penetration Tester, wants to create an exact replica of an original website, so he can

browse and spend more time analyzing it.

Which of the following tools will Michael use to perform this task?

A. VisualRoute

B. NetInspector

C. BlackWidow

D. Zaproxy

Correct Answer: C

QUESTION 11

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida; They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company\\'s main office in Iowa; She states that she needs the receptionist\\'s network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Reciprocation

B. Friendship/Liking

C. Social Validation

D. Scarcity

Correct Answer: A

QUESTION 12

Recently, Jacob was assigned a project to test the perimeter security of one of a client. As part of the

project, Jacob wants to test whether or not a particular port on the firewall is open or closed. He used the

hping utility with the following syntax:

#hping –S –c 1 –p -t

What response will indicate the particular port is allowed in the firewall?

A. Host Unreachable

B. TTL Exceeded

C. No Response

D. ICMP Port Unreachable

Correct Answer: C

QUESTION 13

HDC Networks Ltd. is a leading security services company. Matthew works as a penetrating tester with this firm. He was asked to gather information about the target company. Matthew begins with social engineering by following the steps:

I. Secretly observes the target to gain critical information

II. Looks at employee\\'s password or PIN code with the help of binoculars or a low-power telescope

Based on the above description, identify the information gathering technique.

A. Phishing

B. Shoulder surfing

C. Tailgating

D. Dumpster diving

Correct Answer: B

QUESTION 14

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 15

ABC Technologies, a large financial company, hired a penetration tester to do physical penetration testing.

On the first day of his assignment, the penetration tester goes to the company posing as a repairman and

starts checking trash bins to collect the sensitive information.

What is the penetration tester trying to do?

A. Trying to attempt social Engineering using phishing

B. Trying to attempt social engineering by shoulder surfing

C. Trying to attempt social engineering by eavesdropping

D. Trying to attempt social engineering by dumpster diving

Correct Answer: D