

[Contact Us](#)[My Account](#)[Home](#)[Training ▼](#)[Resources ▼](#)[Store](#)

\$0.00 0 items

[Cart](#)[Discounts](#)[About](#)[Home](#) > [CEHv10 – Module 10 – Quiz](#)

CEHv10 – Module 10 – Quiz

CEHv10 – Module 10 – Quiz

Results

4 of 5 questions answered correctly

Your time: 00:00:37

Course
Progress

You have reached 4 of 5 point(s), (80%)

[Click Here to Continue](#)

RESTART QUIZ

VIEW QUESTIONS

1. Question

In a computer based social engineering, a person receives emails that issues warnings to the user on the new viruses, worms or Trojan that may harm the user's system. These kind of computer based social engineering is known as:

- ☒ a. Spam Email
- ☐ b. Chain Letters
- ☐ c. **Hoax Letters**
- ☐ d. Instant Chat Messenger

Incorrect

2. Question

Silicon Pvt Ltd is a reputed company, which is having around 1000's employees working in their company. One day, one of the employees approached the authorized person of the organization claiming that he/she forgot their ID badge and requested the person to allow through a secure door. Whereas the authorized person believed that the person forgot the ID badge and helped the person to go through the entrance by

Course Navigation

- [!\[\]\(adb0331d22f78481623cc605df40612a_img.jpg\) Meet Your Instructor](#)
- [!\[\]\(7e3a264c08e10137510d1aa76522412b_img.jpg\) Module 01:
Introduction to
Ethical Hacking](#)
- [!\[\]\(13ab9bea7a2b6465d20b6fafd4770e28_img.jpg\) Module 02:
Footprinting and
Reconnaissance](#)
- [!\[\]\(fdbd4f3e18d391808e42202d652ce159_img.jpg\) Module 03: Scanning
Networks](#)
- [!\[\]\(8806d7205b0345b477642dd16156e48f_img.jpg\) Module 04:
Enumeration](#)
- [!\[\]\(9010c03fbf93a4fd0cb332a3c425a55f_img.jpg\) Module 05:
Vulnerability
Analysis](#)
- [!\[\]\(2debc9752bae7c1387d97c5dd3ba30db_img.jpg\) Module 06: System
Hacking](#)
- [!\[\]\(cec1b9cb67c9aa26258f55b0efa23108_img.jpg\) Module 07: Malware
Threats](#)
- [!\[\]\(177de50ec6e35d3bba3bf433b757a115_img.jpg\) Module 08: Sniffing](#)
- [!\[\]\(0615f41b0ec148e1c2a47027f1343157_img.jpg\) Module 09: Social
Engineering](#)
- [!\[\]\(c859257b98fd5739fa728c70d3c9e308_img.jpg\) Module 10: Denial-
of-Service](#)

swiping with his/her ID badge. Later on that authorized person realized that the person is a nonemployee of the organization and he/she is an intruder who intentionally entered into the company. From the above scenario, which of the following comes under the Human-based Social Engineering?

- ☐ a. Tailgating
- ☒ **b. Piggybacking**
- ☐ c. Reverse Social Engineering
- ☐ d. None of the above

Correct

3. Question

In the Permanent Denial-of-service, the attacker will use the 'Bricking a system' method, in order to _____

- ☒ **a. Send fraudulent hardware updates to the victims**
- ☐ b. Launch a massive denial of service attacks and compromise websites
- ☐ c. Exploit weaknesses in programming source code
- ☐ d. Send malicious email attached to the victim

Correct

- ✓ Understanding DoS/DDoS Concepts
- ✓ Understanding Different DoS/DDoS Attack Techniques
- ✓ Understanding the Botnet Network
- ✓ Overview of DDoS Case Study
- ✓ Understanding Various DoS/DDoS Attack Tools
- ✓ Understanding Different Techniques to Detect DoS/DDoS Attacks
- ✓ DoS/DDoS Protection Tools
- ✓ Overview of DoS Attack Penetration Testing
- ✓ Module 10 Lab 01
- ✓ Module 10 Lab 02

4. Question

Jack, a skillful hacker targeted a major banking services firm located in Japan, using the LOIC (Low Orbit Ion Cannon) tool, Jack made the number of HTTP requests rise to a high level, which made the victim's server with the number of requests and resulted in failure of server responding to the request and crashed. Which type of attack Jack performed in the above scenario?

- ☐ a. Social engineering attack
- ☐ b. MITM attack
- ☐ c. Packet Injection attack
- ☒ d. DoS and DDoS

Correct

5. Question

Which of the following statement is true for Service Request Floods

- A. An attacker or group of zombies attempts to exhaust server resources by setting up and tearing down TCP connections
- B. It attacks the servers with a high rate of connections from a valid source
- C. It initiates a request for a single connection

✓ **Module 10 Lab**
03

✓ **Module 10 -**
Full

➔ [Module 11: Session Hijacking](#)

➔ [Module 12: Evading IDS, Firewalls, and Honeypots](#)

➔ [Module 13: Hacking Web Servers](#)

➔ [Module 14: Hacking Web Applications](#)

➔ [Module 15: SQL Injection](#)

➔ [Module 16: Hacking Wireless Networks](#)

➔ [Module 17: Hacking Mobile Platforms](#)

➔ [Module 18: IoT Hacking](#)

➔ [Module 19: Cloud Computing](#)

➔ [Module 20: Cryptography](#)

Return to [Certified Ethical Hacker \(CEH\)v10](#)





- ☐ a. Only A is true
- ☐ b. Both B and C are true
- ☒ c. **Both A and B are true**
- ☐ d. Only C is true

Correct


1-888-330-HACK

Mon - Fri / 8:00AM -
5:00PM





Featured Courses

-  CEH
-  C|CISO
-  CHFI
-  ECSA

Featured White Paper

-  How the
Chameleon
Botnet Stole
\$6M Per Month
in Click Fraud
Scam- A Case
Study

Browse

-  Our Courses
-  Learning
Options
-  iClass Specials
-  Cart

© EC-Council iClass 2018