

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

\$0.00 0 items

[Cart](#)[Discounts](#)[About](#)[Home](#) > [CEHv10 – Module 12 – Quiz](#)

CEHv10 – Module 12 – Quiz

CEHv10 – Module 12 – Quiz

Results

5 of 5 questions answered correctly

Your time: 00:00:33

Course
Progress

You have reached 5 of 5 point(s), (100%)

[Click Here to Continue](#)

RESTART QUIZ

VIEW QUESTIONS

1. Question

The attacker uses the following attack, in order to listen to the conversation between the user and the server and captures the authentication token of the user. With this authentication token, the attacker replays the request to the server with the captured authentication token and gains unauthorized access to the server

- ☒ **a. Session Replay attack**
- ☐ b. Session Fixation attacks
- ☐ c. Session hijacking using proxy servers
- ☐ d. Client side attacks

Correct

2. Question

At which phase of the Session Fixation attack does the attacker obtains a legitimate session ID by establishing a connection with the target web server.

- ☐ a. Entrance phase

Course Navigation

n

- [!\[\]\(5a0d662075632df1b39c9e3427a70093_img.jpg\) Meet Your Instructor](#)
- [!\[\]\(b9aaeddcca3b0cfd727d0e19f8b22e6b_img.jpg\) Module 01:
Introduction to Ethical Hacking](#)
- [!\[\]\(7985cfc9ac20c5a67d1a49b8edd9370c_img.jpg\) Module 02:
Footprinting and Reconnaissance](#)
- [!\[\]\(c3dc9c5d8504b4ff44583fa2a53f68d3_img.jpg\) Module 03: Scanning Networks](#)
- [!\[\]\(dcc90d5dff4daebc8e015e38f89e1f01_img.jpg\) Module 04:
Enumeration](#)
- [!\[\]\(5a7dbb8a52a41ee78efaae6ec4edbab9_img.jpg\) Module 05:
Vulnerability Analysis](#)
- [!\[\]\(008078a23930834f6c898f09f2c1dae4_img.jpg\) Module 06: System Hacking](#)
- [!\[\]\(7fed1b66d79c9e6145749e5541077e76_img.jpg\) Module 07: Malware Threats](#)
- [!\[\]\(d5b40c91112d7c71a95e25a135682f5b_img.jpg\) Module 08: Sniffing](#)
- [!\[\]\(056075d7878218cdcaa8e4443e6edb04_img.jpg\) Module 09: Social Engineering](#)
- [!\[\]\(97b0396a64369e5bbefad739619e19fa_img.jpg\) Module 10: Denial-of-Service](#)
- [!\[\]\(c698fcdef9d18833b54a7e51fd391d42_img.jpg\) Module 11: Session Hijacking](#)

☒ **b. Session set-up phase**

☐ c. Fixation phase

☐ d. Final phase

Correct

3. Question

Identify which of the following detection is used to detect the intrusion based on the fixed behavioral characteristics of the user and components in a computer system.

☒ **a. Anomaly Detection**

☐ b. Protocol Anomaly Detection

☐ c. Intrusion Detection System

☐ d. Signature Recognition

Correct

4. Question

Identify the type of IDS alert that occurs when an IDS fails to react to an actual attack event.

☐ a. True Positive

↓ **Module 12: Evading
IDS, Firewalls, and
Honeypots**

- ✓ Understanding
IDS, Firewall, and
Honeypot
Concepts
- ✓ IDS, Firewall and
Honeypot
Solutions
- ✓ Understanding
Different
Techniques to
Bypass IDS
- ✓ Understanding
Different
Techniques to
Bypass Firewalls
- ✓ IDS/Firewall
Evading Tools
- ✓ Understanding
Different
Techniques to
Detect
Honeypots
- ✓ IDS/Firewall
Evasion
Countermeasures
- ✓ Overview of IDS
and Firewall
Penetration
Testing
- ✓ Module 12 Lab 01
- ✓ Module 12 Lab 02
- ✓ Module 12 Lab 03

- ☐ b. True Negative
- ☒ **c. False Negative**
- ☐ d. False Positive

Correct

5. Question

Identify the ports that are allowed by the firewall in an organization.

- ☐ a. Port 443 and Port 69
- ☐ b. Port 80 and Port 69
- ☐ c. Port 80 and Port 110
- ☒ **d. Port 80 and Port 443**

Correct

✓ **Module 12 - Full**

➔ [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 Hackin](#)





➔ [Module 19: Cloud Computing](#)

➔ [Module 20: Cryptography](#)


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

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