

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

\$0.00 0 items

[Cart](#)[Discounts](#)[About](#)[Home](#) > [Quiz](#) > [CEHv10 – Module 8 – Quiz](#)

# CEHv10 – Module 8 – Quiz

## CEHv10 – Module 8 – Quiz

### Results

4 of 5 questions answered correctly

Your time: 00:03:04

**Course**  
**Progress**

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

[Click Here to Continue](#)

**RESTART QUIZ**

**VIEW QUESTIONS**

1. Question

From the following identify the technique through which an attacker distributes malware on the web by sending a malware attached email and tricking the victim to click the attachment.

- ☐ a. Social Engineered Click-jacking
- ☐ b. Spearphishing Sites
- ☒ **c. Spam Emails**
- ☐ d. Drive-by Downloads

**Correct**

2. Question

Identify the type of virus that adds its code to the host code without relocating the host code to insert its own code at the beginning?

- ☐ a. Intrusive Viruses
- ☐ b. Transient Viruses
- ☒ **c. Add-on Viruses**

## Course Navigation

n

- [➔ Meet Your Instructor](#)
- [➔ Module 01: Introduction to Ethical Hacking](#)
- [➔ Module 02: Footprinting and Reconnaissance](#)
- [➔ Module 03: Scanning Networks](#)
- [➔ Module 04: Enumeration](#)
- [➔ Module 05: Vulnerability Analysis](#)
- [➔ Module 06: System Hacking](#)
- [➔ Module 07: Malware Threats](#)
- [⬇ Module 08: Sniffing](#)
  - ✓ Overview of Sniffing Concepts
  - ✓ Understanding MAC Attacks
  - ✓ Understanding DHCP Attacks
  - ✓ Understanding ARP Poisoning

☐ d. Shell Viruses

**Correct**

3. Question

Sam receives an email with an attachment, he downloads the file and finds that it is infected with virus which overwrites a part of the host file with a constant content without increasing the length of the file and preserving its functionality. Which type of virus that the file was infected by?

- ☒ a. **Cavity Viruses**
- ☐ b. Shell Viruses
- ☐ c. File Extension Viruses
- ☐ d. Cluster Viruses

**Incorrect**

4. Question

Using which port the attacker can compromise the entire network, and receive a copy of every packet that passes through a switch

☒ a. **SPAN Port**

- ✓ Understanding MAC Spoofing Attacks
- ✓ Understanding DNS Poisoning
- ✓ Sniffing Tools
- ✓ Sniffing Countermeasures
- ✓ Understanding Various Techniques to Detect Sniffing
- ✓ Overview of Sniffing Penetration Testing
- ✓ Module 08 Lab 01
- ✓ Module 08 Lab 02
- ✓ Module 08 Lab 03
- ✓ Module 08 Lab 04
- ✓ Module 08 Lab 05
- ✓ Module 08 Lab 06
- ✓ Module 8 - Full

➔ [Module 09: Social Engineering](#)

➔ [Module 10: Denial-of-Service](#)

➔ [Module 11: Session Hijacking](#)

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

- ☐ b. TAP Port
- ☐ c. UDP port
- ☐ d. TCP port

**Correct**

5. Question

Switch Port Stealing sniffing technique uses the following attack to sniff the packets

- ☒ a. **MAC flooding**
- ☐ b. ARP Spoofing
- ☐ c. DHCP attacks
- ☐ d. DNS poisoning

**Correct**

➔ [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