

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

\$0.00 0 items

[Cart](#)[Discounts](#)[About](#)[Home](#) > [Quiz](#) > [CEHv10 – Module 6 – Quiz](#)

CEHv10 – Module 6 – Quiz

CEHv10 – Module 6 – Quiz

Results

4 of 5 questions answered correctly

Your time: 00:05:00

Course Progress

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

[Click Here to Continue](#)

RESTART QUIZ

VIEW QUESTIONS

1. Question

Identify the type of vulnerability assessment used to determine the vulnerabilities in a workstation or server by performing configuration level check through the command line.

- ☐ a. Active Assessment
- ☐ b. Network Assessments
- ☒ **c. Host-Based Assessment**
- ☐ d. Application Assessments

Correct

2. Question

Vulnerability management life cycle is an important process that helps in finding and remediating security weaknesses before they are exploited. Identify the phase that involves the remediation?

- ☐ a. Pre-Assessment Phase
- ☐ b. Vulnerability Assessment Phase
- ☐ c. Risk Assessment Phase

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](#)

✓ [Understanding
System
Hacking
Concepts](#)

✓ [Understanding
Different
Password
Cracking
Techniques to
Gain Access to
the System](#)

☒ **d. Post Assessment Phase**

Correct

3. Question

Which type of rootkit is used to hide the information about the attacker by replacing original system calls with fake ones?

- ☐ a. Application Level Rootkit
- ☒ **b. Library Level Rootkits**
- ☐ c. Boot Loader Level Rootkit
- ☐ d. Hardware/Firmware Rootkit

Correct

4. Question

Which of the following executing application allows an attacker to modify the registry and to change local admin passwords?

- ☒ **a. RemoteExec**
- ☐ b. PDQ Deploy
- ☐ c. DameWare Remote Support

- ✓ Understanding Privilege Escalation Techniques
- ✓ Understanding Techniques to Create and Maintain Remote Access to the System
- ✓ Understanding Techniques to Hide Malicious Programs
- ✓ Understanding Techniques to Hide the Evidence of Compromise
- ✓ Overview of System Hacking Penetration Testing
- ✓ Module 06 Lab 01
- ✓ Module 06 Lab 02
- ✓ Module 06 Lab 03
- ✓ Module 06 Lab 04
- ✓ Module 06 Lab 05

☐ d. Keyloggers

Correct

5. Question

Identify the rootkit, which helps in hiding the directories, remote connections and logins.

- ☐ a. Azazel
- ☐ b. ZeroAccess
- ☐ c. Necurs
- ☒ d. Avatar

Incorrect

✓ [Module 06 Lab 06](#)

✓ [Module 06 Lab 07](#)

✓ [Module 06 Lab 08](#)

✓ [Module 06 Lab 09](#)

✓ [Module 06 Lab 10](#)

✓ [Module 06 Lab 11](#)

✓ [Module 06 Lab 12](#)

✓ [Module 06 Lab 13](#)

✓ [Module 06 Lab 14](#)

✓ [Module 06 Lab 15](#)

✓ [Module 06 Lab 16](#)

✓ [Module 6 - Full](#)

➔ [Module 07: Malware Threats](#)

➔ [Module 08: Sniffing](#)

➔ [Module 09: Social Engineering](#)

➔ [Module 10: Denial-of-Service](#)

➔ [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](#)


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