EDUSUM
#1 Online Certification Guide

EC-COUNCIL 212-82

EC-Council CCT Certification Questions & Answers

Exam Summary – Syllabus –Questions

212-82
EC-Council Certified Cybersecurity Technician (CCT)
60 Questions Exam – 70% Cut Score – Duration of 180 minutes

Table of Contents:

Know Your 212-82 Certification Well:

The 212-82 is best suitable for candidates who want to gain knowledge in the EC-Council CyberTechnician. Before you start your 212-82 preparation you may struggle to get all the crucial CCT materials like 212-82 syllabus, sample questions, study guide.

But don't worry the 212-82 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-
- What is in the 212-82 syllabus?
- How many questions are there in the 212-82 exam?
- Which Practice test would help me to pass the 212-82 exam at the first attempt?

Passing the 212-82 exam makes you EC-Council Certified Cybersecurity Technician (CCT). Having the CCT certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

EC-Council 212-82 CCT Certification Details:

Exam Name	EC-Council Certified Cybersecurity Technician (CCT)
Exam Code	212-82
Exam Price	$499 (USD)
Duration	180 mins
Number of Questions	60
Passing Score	70%
Books / Training	**Courseware**
Schedule Exam	**Pearson VUE** OR **ECC Exam Center**
Sample Questions	**EC-Council CCT Sample Questions**
Practice Exam	**EC-Council 212-82 Certification Practice Exam**

212-82 Syllabus:

Topic
Information Security Threats and Vulnerabilities
Information Security Attacks
Network Security Fundamentals
Identification, Authentication, and Authorization
Network Security Controls - Administrative Controls
Network Security Controls - Physical Controls
Network Security Controls - Technical Controls
Network Security Assessment Techniques and Tools
Application Security
Virtualization and Cloud Computing
Wireless Network Security
Mobile Device Security
IoT and OT Security
Cryptography
Data Security
Network Troubleshooting
Network Traffic Monitoring
Network Logs Monitoring and Analysis
Incident Response
Computer Forensics
Business Continuity and Disaster Recoverys
Risk Management

EC-Council 212-82 Sample Questions:

Question: 1

What is the key difference between a disaster recovery plan and a business continuity plan?

a) Disaster recovery plans focus on data backup, while business continuity plans focus on personnel safety.
b) Disaster recovery plans are concerned with technology recovery, while business continuity plans cover all aspects of business operations.
c) Disaster recovery plans are only applicable to natural disasters, while business continuity plans cover man-made incidents.
d) Disaster recovery plans are shorter and simpler than business continuity plans.

Answer: b

Question: 2

Shawn, a forensic officer, was appointed to investigate a crime scene that had occurred at a coffee shop. As a part of investigation, Shawn collected the mobile device from the victim, which may contain potential evidence to identify the culprits.

Which of the following points must Shawn follow while preserving the digital evidence?

(Choose three.)

a) Never record the screen display of the device
b) Turn the device ON if it is OFF
c) Do not leave the device as it is if it is ON
d) Make sure that the device is charged

Answer: b, c, d

Question: 3

Which of the following are examples of physical security controls?

(Select all that apply)

a) Security guards
b) Firewalls
c) Biometric access control
d) Encryption algorithms

Answer: a, c

Question: 4

Andre, a security professional, was tasked with segregating the employees' names, phone numbers, and credit card numbers before sharing the database with clients. For this purpose, he implemented a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#).

Which of the following techniques was employed by Andre in the above scenario?

a) Tokenization
b) Masking
c) Hashing
d) Bucketing

Answer: b

Question: 5

Tristan, a professional penetration tester, was recruited by an organization to test its network infrastructure. The organization wanted to understand its current security posture and its strength in defending against external threats.

For this purpose, the organization did not provide any information about their IT infrastructure to Tristan. Thus, Tristan initiated zero-knowledge attacks, with no information or assistance from the organization.

Which of the following types of penetration testing has Tristan initiated in the above scenario?

    a) Black-box testing
    b) White-box testing
    c) Gray-box testing
    d) Translucent-box testing

Answer: a

Question: 6

In an incident response plan, what are the phases of the incident response lifecycle?

(Select all that apply)

    a) Detection and analysis
    b) Recovery
    c) Prevention
    d) Containment

Answer: a, b, d

Question: 7

What can be used to ensure data confidentiality?

(Select all that apply)

    a) Access control lists (ACLs)
    b) Encryption
    c) Regular system backups
    d) Social engineering

Answer: a, b

Question: 8

Which security measure can help prevent SQL injection attacks?

(Select all that apply)

 a) Input validation
 b) Cross-site scripting (XSS)
 c) Using weak passwords
 d) Code obfuscation

Answer: a, d

Question: 9

An organization hired a network operations center (NOC) team to protect its IT infrastructure from external attacks. The organization utilized a type of threat intelligence to protect its resources from evolving threats.

The threat intelligence helped the NOC team understand how attackers are expected to perform an attack on the organization, identify the information leakage, and determine the attack goals as well as attack vectors.

Identify the type of threat intelligence consumed by the organization in the above scenario.

 a) Operational threat intelligence
 b) Strategic threat intelligence
 c) Technical threat intelligence
 d) Tactical threat intelligence

Answer: c

Question: 10

During which phase of the incident response process are containment and eradication activities performed?

 a) Preparation
 b) Recovery
 c) Containment
 d) Detection and analysis

Answer: c

Study Guide to Crack EC-Council CCT 212-82 Exam:

- Getting details of the 212-82 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 212-82 exam.

- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.

- Joining the EC-Council provided training for 212-82 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.

- Read from the 212-82 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.

- Practicing on 212-82 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for 212-82 Certification

Make EduSum.com your best friend during your EC-Council Certified Cybersecurity Technician exam preparation. We provide authentic practice tests for the 212-82 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual 212-82 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the 212-82 exam.

Start Online practice of 212-82 Exam by visiting URL
https://www.edusum.com/ec-council/212-82-ec-council-certified-cybersecurity-technician