EC-COUNCIL ICS/SCADA

EC-Council Industrial Control Systems Supervisory Control and Data Acquisition Certification Questions & Answers

Exam Summary – Syllabus –Questions

ICS/SCADA
EC-Council Industrial Control Systems and Supervisory Control and Data Acquisition
75 Questions Exam – 70% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your ICS/SCADA Certification Well:

The ICS/SCADA is best suitable for candidates who want to gain knowledge in the EC-Council Network Security. Before you start your ICS/SCADA preparation you may struggle to get all the crucial EC-Council Industrial Control Systems Supervisory Control and Data Acquisition materials like ICS/SCADA syllabus, sample questions, study guide.

But don't worry the ICS/SCADA 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 ICS/SCADA syllabus?
- How many questions are there in the ICS/SCADA exam?
- Which Practice test would help me to pass the ICS/SCADA exam at the first attempt?

Passing the ICS/SCADA exam makes you EC-Council Industrial Control Systems and Supervisory Control and Data Acquisition. Having the EC-Council Industrial Control Systems Supervisory Control and Data Acquisition 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 ICS/SCADA EC-Council Industrial Control Systems Supervisory Control and Data Acquisition Certification Details:

Exam Name	EC-Council Industrial Control Systems and Supervisory Control and Data Acquisition (ICS/SCADA)
Exam Code	ICS/SCADA
Exam Price	$699 (USD)
Duration	120 mins
Number of Questions	75
Passing Score	70%
Books / Training	**Courseware**
Schedule Exam	**ECC Exam Center**
Sample Questions	**EC-Council ICS/SCADA Sample Questions**
Practice Exam	**EC-Council ICS/SCADA Certification Practice Exam**

ICS/SCADA Syllabus:

Topic	Details
Introduction to ICS/SCADA Network Defense	- LAB: Security Model • IT Security Model • ICS/SCADA Security Model - LAB: Allowing a Service • Security Posture • Risk Management in ICS/SCADA • Risk Assessment • Defining Types of Risk • Security Policy
TCP/IP 101	- Introduction and Overview - Introducing TCP/IP Networks - Internet RFCs and STDs - TCP/IP Protocol Architecture - Protocol Layering Concepts - TCP/IP Layering - Components of TCP/IP Networks - ICS/SCADA Protocols
Introduction to Hacking	- Review of the Hacking Process - Hacking Methodology - Intelligence Gathering - Footprinting - Scanning - Enumeration - Identify Vulnerabilities - Exploitation - Covering Tracks - LAB: Hacking ICS/SCADA Networks Protocols • How ICS/SCADA Are Targeted • Study of ICS/SCADA Attacks • ICS/SCADA as a High-Value Target • Attack Methodologies In ICS
Vulnerability	- Challenges of Vulnerability Assessment

Topic	Details
Management	- System Vulnerabilities - Desktop Vulnerabilities - ICS/SCADA Vulnerabilities - Interpreting Advisory Notices - CVE - ICS/SCADA Vulnerability Sites - Life Cycle of a Vulnerability and Exploit - Challenges of Zero-Day Vulnerability - Exploitation of a Vulnerability - Vulnerability Scanners - ICS/SCADA Vulnerability Uniqueness - Challenges of Vulnerability Management Within ICS/SCADA - LAB: Vulnerability Assessment • Prioritizing Vulnerabilities • CVSS • OVAL
Standards and Regulations for Cybersecurity	- ISO 27001 - ICS/SCADA - NERC CIP - CFATS - ISA99 - IEC 62443 - NIST SP 800-82
Securing the ICS network	- Physical Security - Establishing Policy - ISO Roadmap - Securing the Protocols Unique to the ICS - Performing a Vulnerability Assessment - Selecting and Applying Controls to Mitigate Risk - Monitoring - Mitigating the Risk of Legacy Machines
Bridging the Air Gap	- Do You Really Want to Do This? - Advantages and Disadvantages - Guard - Data Diode - Next Generation Firewalls
Introduction to Intrusion Detection Systems (IDS) and	- What IDS Can and Cannot Do - Types IDS - Network

Topic	Details
Intrusion Prevention Systems (IPS)	- Host - Network Node - Advantages of IDS - Limitations of IDS - Stealthing the IDS - Detecting Intrusions

EC-Council ICS/SCADA Sample Questions:

Question: 1

Which of the following ports are used for communications in Modbus TCP?

a) 205
b) 502
c) 405
d) 505

Answer: b

Question: 2

Which of the following is the stance on risk that by default allows traffic with a default permit approach?

a) Permissive
b) Promiscuous
c) Prudent
d) Paranoid

Answer: a

Question: 3

Which of the following is the stance that by default has a default deny approach?

a) Paranoid
b) Promiscuous
c) Prudent
d) Permissive

Answer: a

Question: 4

Which publication from NIST provides guidance on Industrial Control Systems?

    a) NIST SP 800-77
    b) NIST SP 800-90
    c) NIST SP 800-44
    d) NIST SP 800-82

Answer: d

Question: 5

Which of the following options for the nbtstat command will show the cache?

    a) s
    b) c
    c) r
    d) a

Answer: b

Question: 6

Which of the following names represents inbound filtering?

    a) Egress
    b) Funnel
    c) Sanity
    d) Ingress

Answer: d

Question: 7

Which component of the IT Security Model is usually the least priority in ICS/SCADA Security?

    a) Availability
    b) Integrity
    c) Authentication
    d) Confidentiality

Answer: d

Question: 8

Which component of the IT Security Model is attacked with interruption?

    a) Integrity
    b) Authentication
    c) Availability
    d) Confidentiality

Answer: c

Question: 9

Which component of the IT Security Model is attacked with masquerade?

    a) Availability
    b) Confidentiality
    c) Integrity
    d) Authentication

Answer: d

Question: 10

Which of the CVSS metrics refer to the exploit quotient of the vulnerability?

    a) Environmental
    b) Temporal
    c) Base
    d) All of the above

Answer: b

Study Guide to Crack EC-Council EC-Council Industrial Control Systems Supervisory Control and Data Acquisition ICS/SCADA Exam:

- Getting details of the ICS/SCADA 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 ICS/SCADA 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 ICS/SCADA 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 ICS/SCADA 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 ICS/SCADA practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for ICS/SCADA Certification

Make EduSum.com your best friend during your EC-Council Industrial Control Systems Supervisory Control and Data Acquisition exam preparation. We provide authentic practice tests for the ICS/SCADA exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual ICS/SCADA 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 ICS/SCADA exam.

Start Online practice of ICS/SCADA Exam by visiting URL
https://www.edusum.com/ec-council/icsscada-ec-council-industrial-control-systems-supervisory-control-and-data-acquisition