EDUSUM

#1 Online Certification Guide

CERTNEXUS ITS-110

CERTNEXUS CIOTSP CERTIFICATION QUESTIONS & ANSWERS

Exam Summary – Syllabus –Questions

ITS-110

CertNexus Certified IoT Security Practitioner (CIoTSP)

100 Questions Exam – 60% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your ITS-110 Certification Well:

The ITS-110 is best suitable for candidates who want to gain knowledge in the CertNexus Internet of Things. Before you start your ITS-110 preparation you may struggle to get all the crucial CIoTSP materials like ITS-110 syllabus, sample questions, study guide.

But don't worry the ITS-110 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 ITS-110 syllabus?
- How many questions are there in the ITS-110 exam?
- Which Practice test would help me to pass the ITS-110 exam at the first attempt?

Passing the ITS-110 exam makes you CertNexus Certified IoT Security Practitioner (CIoTSP). Having the CIoTSP certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CertNexus ITS-110 CIoTSP Certification Details:

Exam Name	CertNexus Certified IoT Security Practitioner (CIoTSP)
Exam Code	ITS-110
Exam Price	$367.50 (USD)
Duration	120 mins
Number of Questions	100
Passing Score	60%
Books / Training	**ITS training**
Schedule Exam	**Pearson VUE**
Sample Questions	**CertNexus CIoTSP Sample Questions**
Practice Exam	**CertNexus ITS-110 Certification Practice Exam**

ITS-110 Syllabus:

Topic	Details	Weights
Securing IoT Portals	- Identify common threats used to compromise unsecure web, cloud, or mobile interfaces. • Account enumeration • Weak default credentials • Injection flaws • Unsecure direct object references • Sensitive data exposure • CSRF • Unvalidated redirects and forwards • Session Management • Malformed URLs • Session replay • Reverse shell • Misconfiguration • Weak account lockout settings • No account lockout • Unsecured credentials • Lack of integration credentials on Edge devices	29%

Topic	Details	Weights
	- Implement countermeasures used to secure web, cloud, or mobile interfaces. • Change default passwords • Secure password recovery mechanisms • Secure the web interface from XSS, SQLi, or CSRF • Protect credentials • Robust password policies • Account lockout policies • Protect against account enumeration • 2FA if possible • Granular role-based access	
Implementing Authentication, Authorization, and Accounting	- Identify common threats used to exploit weak authentication/authorization schemes. • Lack of password complexity • Poorly protected credentials • Lack of 2FA • Unsecure password recovery • Privilege escalation	14%

Topic	Details	Weights
	• Lack of RBAC • Unsecure databases and datastores • Lack of account lockout policy • Lack of access auditing • Lack of security monitoring • Lack of security logging - Implement countermeasures used to provide secure authentication, authorization, and accounting. • Granular access control • Password management • Ensure re-authentication is required for sensitive features • Event logging and IT/OT admin notification • Security monitoring	
Securing Network Services	- Identify common threats used to exploit unsecure network services. • Vulnerable services • Buffer overflow • Open ports via UPnP	14%

Topic	Details	Weights
	• Exploitable UDP services • DoS/DDoS • DoS via network device fuzzing • Endpoint (address) spoofing • Packet manipulation/injection • Networking, protocols, radio communications - Implement countermeasures used to provide secure network services. • Port control • Secure memory spaces • DoS mitigation/DDoS • Secure network nodes • Secure field devices • Secure network pathways	
Securing Data	- Identify common threats used to exploit unsecure data. • Vulnerable data in motion • Vulnerable data at rest • Vulnerable data in use	14%

Topic	Details	Weights
	- Implement countermeasures used to secure data. • Encrypt data in motion, at rest, and in use	
Addressing Privacy Concerns	- Identify common threats used to compromise privacy. • Collection of unnecessary personal or sensitive information (PII, PHI, metadata) • Unsecured data in transit or at rest • Unauthorized access to personal information • Lack of proper data anonymization • Lack of data retention policies - Implement countermeasures used to ensure data privacy. • Only collect critical data • Protect sensitive data • Comply with regulations/laws • Authorize data users • Data retention policies • Data disposal policies	12%

Topic	Details	Weights
	• End-user notification policies (GDPR) • Enable courtesy notifications to end users • Enable notifications as required by law	
Securing Software/Firmware	- Identify common threats used to exploit unsecure software/firmware. • Poorly designed/tested software/firmware • Unsecure updates/patches • Firmware contains sensitive information • Lack of OTA updates • Constrained devices with non-existent security features • Lack of end-to-end solution • Software/firmware not digitally signed • Unsecure bootloader/boot • Unsecure key storage - Implement countermeasures used to provide secure software/firmware.	10%

Topic	Details	Weights
	• Digitally signed updates • Remote update capability for, e.g., bootloader, firmware, OS, drivers, application, certificates • Secure updates/digitally signed updates • Root-of-trust/secure enclave • Secure bootloader/boot, measured boot	
Enhancing Physical Security	- Identify common threats used to exploit poor physical security. • Access to software/configuration via physical ports • Access to or removal of storage media • Unprotected shell access for accessible ports • Unrestricted physical access to vulnerable devices • Easily disassembled devices - Implement countermeasures used to ensure physical security. • Protect data storage medium • Encrypt data at rest	7%

Topic	Details	Weights
	• Protect physical ports • Tamper-resistant devices • Limit physical access when possible • Hardened security for shell access • Limit administrative capabilities and access	

CertNexus ITS-110 Sample Questions:

Question: 1

Why are buffer overflow vulnerabilities dangerous in network services?

a) They increase packet latency
b) They only impact user interface design
c) They can lead to remote code execution
d) They prevent firmware updates

Answer: c

Question: 2

Which encryption strategies are effective for securing data at rest?

(Choose two)

a) Store data in HTML format
b) Use AES-256 encryption for stored files
c) Use secure key storage
d) Send all data to public cloud unencrypted

Answer: b, c

Question: 3

What two factors make IoT web portals susceptible to CSRF attacks? (Choose two)

a) Reuse of HTTPS certificates
b) Lack of token validation in POST requests
c) Inclusion of CSRF tokens in HTML
d) Reliance solely on cookies for session authentication

Answer: b, d

Question: 4

Why is anonymizing personal data a recommended practice in IoT systems?

a) It reduces the risk of identifying specific individuals
b) It prevents automatic updates
c) It makes the UI faster
d) It increases firmware size

Answer: a

Question: 5

Which actions strengthen password recovery mechanisms? (Choose two)

a) Sending password via email link without verification
b) Requiring multi-step identity verification
c) Limiting recovery attempts
d) Not logging recovery events

Answer: b, c

Question: 6

Why is role-based access control (RBAC) effective for large-scale IoT deployments?

a) It enforces minimal privilege principles by grouping users
b) It ensures each user gets equal access
c) It disables unused accounts
d) It enables firmware isolation

Answer: a

Question: 7

What is the impact of failing to secure memory spaces in network-exposed field devices?

a) Overheating
b) Buffer overflow attacks
c) Stronger encryption
d) Disconnected session states

Answer: b

Question: 8

Why should physical access to administrative interfaces be limited?

a) To reduce bandwidth consumption
b) To lower heat generation
c) To avoid excessive logging
d) To prevent unauthorized configuration changes

Answer: d

Question: 9

Which of the following would help protect the shell (e.g., UART) access on an IoT device?

a) Disabling cloud sync
b) Setting maximum CPU frequency
c) Password-protecting or disabling shell ports
d) Adding thermal paste to the processor

Answer: c

Question: 10

What actions secure network services against buffer overflow attacks? (Choose two)

a) Implement memory bounds checking
b) Use encrypted ZIP files
c) Enforce strict input validation
d) Allow remote telnet access

Answer: a, c

Study Guide to Crack CertNexus CIoTSP ITS-110 Exam:

- Getting details of the ITS-110 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 ITS-110 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 CertNexus provided training for ITS-110 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 ITS-110 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 ITS-110 practice tests is must. Continuous practice will make you an expert in all syllabus areas.