CertNexus Certified Internet of Things Security Practitioner Course Description:

Exam ITS-110

Course Content

Lesson 1: Managing IoT Risks

Topic A: Map the IoT Attack Surface

- Case Study: Connected Services Company
- The IoT Ecosystem
- The IoT Attack Surface
- Shadow IT
- IoT Risk Management
- Security Versus Risk
- Guidelines for Identifying Threats to IoT
- Identifying Strategies to Deal with IoT Threats

Topic B: Build in Security by Design

- Security by Design
- Guidelines for Implementing Security by Design
- Building Security into IoT Systems

Lesson 2: Securing Web and Cloud Interfaces

Topic A: Identify Threats to IoT Web and Cloud Interfaces

- Web Protocols
- H2M Interfaces
- M2M Interfaces
- The Request/Response Model
- Send Data with a Request
- Asynchronous HTTP
- Data Serialization
- Common Attack Patterns
- Guidelines for Protecting Against Threats to IoT Web-Based User Interfaces
- Identifying Threats to IoT Web and Cloud Interfaces

Topic B: Prevent Injection Flaws

- Injection Flaws
- SQL Injection
- Consequences of a SQL Injection Attack
- Second Order SQL Injection
- LDAP Injection
- Shell Attack
- Reverse Shell
- URL-Based Attacks

- Malformed URL Attack
- Unsecure Direct Object References
- Setting Up an Account
- Exploiting Injection Flaws
- Guidelines for Preventing Injection Flaws
- Preventing Injection Flaws

Topic C: Prevent Session Management Flaws

- Session Tokens
- Token Management
- Session Management
- Session Replay
- Man-in-the-Middle
- Simulating an MITM Attack
- Guidelines for Preventing Session Management Flaws
- Preventing Session Management Flaws

Topic D: Prevent Cross-Site Scripting Flaws

- Cross-Site Scripting (XSS)
- Persistent XSS
- Exploiting XSS to Run Untrusted Code
- Guidelines for Preventing XSS Flaws
- Preventing XSS Flaws

Topic E: Prevent Cross-Site Request Forgery Flaws

- Cross-Site Request Forgery (CSRF)
- Exploiting CSRF to Access Another User's Privileges
- Guidelines for Preventing CSRF Flaws
- Preventing CSRF Flaws

Topic F: Prevent Unvalidated Redirects and Forwards

- Unvalidated Redirects and Forwards
- Exploiting an Unvalidated Redirect
- Guidelines for Preventing Unvalidated Redirects and Forwards
- Preventing Unvalidated Redirects and Forwards

Lesson 3: Securing Data

Topic A: Use Cryptography Appropriately

- Cryptography
- Encryption Functions
- Symmetric Key Encryption
- Asymmetric Key Encryption
- Hashing
- Hashing Functions
- Salt
- Cipher Suites
- Handshaking
- Block Versus Stream Ciphers
- Strength and Processing Requirements
- Common Algorithms
- Hardware-Based Encryption Modules on IoT Devices
- Guidelines for Selecting Appropriate Encryption
- Selecting Appropriate Cryptography

Topic B: Protect Data in Motion
- Data in Motion
- Data in Motion Vulnerabilities
- Interprocess Communication
- Content Provider Leakage
- Capturing Data Leakage from a Content Provider
- Transport Encryption
- PKI
- Vulnerabilities Related to PKI
- Outdated Cipher Suites
- Secure SSH Implementation
- IPSec
- IPSec Modes
- IPSec Security Association
- IPSec Process
- SDN
- Benefits of SDN for IoT
- S/MIME
- Blockchain
- Guidelines for Securing Data in Motion
- Protecting Data in Motion

Topic C: Protect Data at Rest
- Data at Rest Vulnerabilities
- Data at Rest Protections
- Guidelines for Protecting Data at Rest
- Protecting Data at Rest

Topic D: Protect Data in Use
- Data in Use Vulnerabilities
- Buffer overflow
- Rootkits
- Malicious Hardware and Firmware
- Performing a Memory-Based Attack
- Data in Use Protections
- Guidelines for Securing Data in Use
- Protecting Data in Use

Lesson 4: Controlling Access to IoT Resources

Topic A: Identify the Need to Protect IoT Resources
- The Need to Protect IoT Resources
- AAA
- Identifying the Need to Protect IoT Resources

Topic B: Implement Secure Authentication
- Authentication Throughout the IoT Ecosystem
- Threats Related to Inadequate Authentication
- Password Attacks
- Credential Protection Flaws
- Accessing Unsecured Credentials
- Password Recovery Flaws
- Account Enumeration

- Exploiting Poor Password Recovery
- Machine Authentication
- Challenges of Authentication on Constrained Devices
- Credential Protection Strategies
- Reauthentication
- Multifactor Authentication
- Problems Mitigated by MFA
- Example Authentication Factors
- Account Lockout Policies
- Guidelines for Implementing Secure Authentication
- Implementing Secure Authentication in IoT

Topic C: Implement Secure Authorization
- Threats Related to Inadequate Authorization
- Vulnerabilities That Undermine Authorization
- Exploiting Authorization Flaws
- Role-Based Access Control
- Access Control Throughout the IoT Ecosystem
- Guidelines for Implementing Secure Authorization
- Implementing Secure Authorization in IoT

Topic D: Implement Security Monitoring on IoT Systems
- Security Logging and Monitoring
- Log Tuning
- Use of AI and Machine Learning in IoT Monitoring
- Guidelines for Implementing Secure Logging and Monitoring
- Implementing Security Monitoring

Lesson 5: Securing IoT Networks

Topic A: Ensure the Security of IP Networks
- TCP/IP in IoT
- Common Threats to IP Networks
- Spoofing
- DoS/DDoS
- DNS Poisoning
- Reconnaissance
- Packet Manipulation/Injection
- Scanning the Local Network
- IP Versions
- DNSSEC
- IEEE 802.15.4
- Guidelines for Securing IP Networks
- Securing IP Networks

Topic B: Ensure the Security of Wireless Networks
- Common Threats to Wireless Networks
- Identifying Wireless Network Vulnerabilities
- Guidelines for Securing Wireless Networks
- Securing Wireless Networks

Topic C: Ensure the Security of Mobile Networks
- Mobile Networking
- Generations of Cellular Protocols

- Cellular Protocols
- Cellular Communications in IoT
- Custom APNs
- Threats to Cellular Communication
- Mobile Client Security
- Threats to Low-Power Mobile Devices
- Guidelines for Ensuring Mobile Network Security
- Securing Mobile Networks

Topic D: Ensure the Security of IoT Edge Networks

- Threats to Edge Networks
- Edge Network Security Strategies
- Security in IoT Edge Network Protocols
- Guidelines for Ensuring IoT Edge Network Security
- Securing IoT Edge Networks

Lesson 6: Ensuring Privacy

Topic A: Improve Data Collection to Reduce Privacy Concerns

- Data Lifecycle
- Data Collection Concerns
- Identifying Data Collection Privacy Concerns
- Compliance Requirements
- PHI
- PII
- Metadata
- Guidelines for Managing Data Collection
- Improving Data Collection

Topic B: Protect Sensitive Data

- Data Protection Concerns
- Gaining Unauthorized Access to Private Data
- Appropriate Access
- Identifiability
- Guidelines for Protecting Sensitive Data
- Protecting Sensitive Data

Topic C: Dispose of Sensitive Data

- Data Retention and Disposal Concerns
- Data Retention Policies
- Data Disposal Policies
- Guidelines for Retaining and Disposing of Sensitive Data
- Disposing of Sensitive Data

Lesson 7: Managing Software and Firmware Risks

Topic A: Manage General Software Risks

- Software and Firmware Within the IoT Ecosystem
- Exploiting Common Application Flaws
- Lack of Secure End-to-End Solutions
- Common Software Flaws
- Desktop and Mobile Apps
- Special Concerns for Mobile Apps
- Smartphones and Consumer IoT Devices

- Input Validation
- Validation Approaches
- Fuzzing
- Secure Application Development
- IoT Product Research and Evaluation
- Guidelines for Managing IoT Software Risks
- Improving Software Security

Topic B: Manage Risks Related to Software Installation and Configuration
- IoT Misconfiguration Flaws
- Guidelines for Securing Installed Applications
- Managing Software Installation and Configuration Risks

Topic C: Manage Risks Related to Software Patches and Updates
- Vulnerabilities in Software Updating and Patching
- Secure Updates
- IoT Device Asset Management
- Guidelines for Implementing Secure Patches and Updates
- Managing Risks Related to Patches and Updates

Topic D: Manage Risks Related to IoT Device Operating Systems and Firmware
- Constrained Devices with Limited Security Features
- IoT Device Operating System Vulnerabilities
- Bootloader/Boot Vulnerabilities
- RoT
- Guidelines for Securing IoT Device Operating Systems and Firmware
- Managing Risks Related to Operating Systems and Firmware.

Lesson 8: Promoting Physical Security

Topic A: Protect Local Memory and Storage
- Physical Access
- Mobile Device Vulnerabilities
- Guidelines for Protecting Local Memory and Storage
- Protecting Local Memory and Storage

Topic B: Prevent Physical Port Access
- Physical Port Access
- Guidelines for Protecting Devices from Physical Shell Access
- Protecting Devices from Shell Access and Reverse Engineering