Document Generated: 11/24/2026

Learning Style: On Demand

Technology:

Difficulty: Intermediate

Course Duration: 2 Weeks

IoT Security Practitioner



About This Course:

This course teaches learners to protect IoT devices, networks, and data from end to end. Starting with the IoT threat landscape and security-by-design principles, it moves through web and cloud security, cryptography, access control, privacy, software and firmware risks, and physical device protection. Learners practice in 24 browser-based hands-on labs and test their readiness with 135 practice questions.

Course Objectives:

- Identify, assess, and prioritize risks across the IoT attack surface, and plan an incident response
- Build security into IoT systems from the design stage
- Detect and fix common web and cloud interface vulnerabilities, such as SQL injection, cross-site scripting, and session flaws
- Select the right cryptographic methods, including encryption, hashing, and digital signatures, and manage keys securely
- Secure data in transit, in storage, and during processing
- Control access to IoT resources with strong authentication, authorization, and security monitoring
- Defend IoT networks with firewalls, intrusion detection and prevention, and safeguards against Wi-Fi and mobile network weaknesses
- Address security challenges at the edge of IoT networks
- Meet privacy requirements by applying privacy-by-design principles and handling sensitive data responsibly through its full lifecycle
- Reduce software and firmware risks through secure installation, configuration, and patch management
- Harden devices against physical tampering by protecting local storage and physical ports

Audience:

- Cybersecurity analysts and IoT security consultants
- Solution architects and platform engineers who design connected systems
- Network administrators and cloud engineers responsible for IoT infrastructure
- Software, web, and embedded developers building IoT applications
- Product managers overseeing IoT products

Prerequisites:

- No formal prerequisites are required, and the course is suitable for beginners

Course Outline:

Module 1: The IoT Threat Landscape and Risk Management

Why IoT systems are attractive targets for attackers

Mapping the IoT attack surface across devices, networks, applications, and cloud

Applying security-by-design principles from the start of a project

Identifying and prioritizing security risks

Module 2: Securing Web and Cloud Interfaces

Common threats to IoT web applications, APIs, and cloud dashboards

Preventing injection flaws, including SQL injection

Preventing session management, cross-site scripting (XSS), and cross-site request forgery (CSRF) flaws

Preventing unvalidated redirects and forwards

Cloud security principles for IoT platforms

Lab: Exploiting a website using SQL injection

Lab: Scanning for web vulnerabilities with OWASP ZAP

Module 3: Cryptography and Data Protection

Choosing the right cryptographic approach: encryption, hashing, and digital signatures

Creating, distributing, and managing cryptographic keys

Protecting data in motion with secure communication protocols

Protecting data at rest and data in use

Lab: Applying symmetric key encryption

Lab: Using the MD5 hash algorithm

Module 4: Controlling Access to IoT Resources

Understanding why IoT resources need access protection

Implementing secure authentication for users and devices

Implementing secure authorization and access control models

Monitoring IoT systems for suspicious activity

Lab: Exploiting LDAP-based authentication

Module 5: Securing IoT Networks

IP network protocols and their security weaknesses

Configuring firewalls and intrusion detection and prevention systems (IDS/IPS)

Wi-Fi and mobile network vulnerabilities and countermeasures

Security challenges at the network edge

Lab: Creating a new inbound firewall rule

Module 6: Ensuring Privacy

Designing data collection to minimize privacy concerns

Privacy-by-design principles and data privacy regulations

Protecting sensitive and personal data

Securely disposing of sensitive data

Module 7: Managing Software and Firmware Risks

General software security risks in IoT systems

Secure software installation and configuration

Managing patches and updates across device fleets

Securing IoT device operating systems and firmware

Module 8: Physical Security and Device Hardening

Hardening IoT devices against tampering

Protecting local memory and storage

Preventing unauthorized access through physical ports

Responding to security incidents involving IoT devices