PROGRAMMA CWNP Certified Wireless Security Professional (CWSP-206)

32 ore

Parts I: Security Policy

- Define WLAN security Requirements
- Develop WLAN security policies
- Ensure proper training is administered for all stakeholders related to security policies and ongoing security awareness

Parts II: Vulnerabilities, Threats, and Attacks

- Identify potential vulnerabilities and threats to determine the impact on the WLAN and supporting systems and verify, mitigate, and remediate them
- Describe and perform risk analysis and risk mitigation procedures

Parts III: WLAN Security Design and Architecture

- Select the appropriate security solution for a given implementation and ensure it is installed and configured according to policy requirements
- Implement or recommend appropriate wired security configurations to support the WLAN
- Implement authentication and security services
- Implement secure transitioning (roaming) solutions
- Secure public access and/or open networks
- Implement preventative measures required for common vulnerabilities associated with wireless infrastructure devices and avoid weak security solutions

Parts IV: Security Lifecycle Management

- Understand and implement management within the security lifecycle of identify, assess, protect, and monitor
- Use effective change management procedures including documentation, approval, and notifications
- Use information from monitoring solutions for load observation and forecasting of future requirements to comply with security policy
- Implement appropriate maintenance procedures including license management, sofware/code upgrades, and configuration management
- Implement effective auditing procedures to perform audits, analyze results, and generate reports