ASM Educational Center (ASM) *Est. 1992*

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

Authorized CWSP Certified Wireless Security Professional Boot Camp

Course Outline

Module 1 - Introduction to WLAN Security Technology

- Security policy
- Security concerns
- Security auditing practices
- Application layer vulnerabilities and analysis
- Data Link layer vulnerabilities and analysis
- Physical layer vulnerabilities and analysis
- 802.11 security mechanisms
- Wi-Fi Alliance security certifications

Module 2 - Small Office / Home Office WLAN Security Technology and Solutions

- WLAN discovery equipment and utilities
- Legacy WLAN security methods, mechanisms, and exploits
- Appropriate SOHO security

Module 3 - WLAN Mobile Endpoint Security Solutions

- Personal-class mobile endpoint security
- Enterprise-class mobile endpoint security
- User-accessible and restricted endpoint policies
- VPN technology overview

Module 4 - Branch Office / Remote Office WLAN Security Technology and Solutions

- General vulnerabilities
- Preshared Key security with RSN cipher suites
- Passphrase vulnerabilities
- Passphrase entropy and hacking tools
- WPA/WPA2 Personal - how it works

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

- WPA/WPA2 Personal - configuration
- Wi-Fi Protected Setup (WPS)
- Installation and configuration of WIPS, WNMS, and WLAN controllers to extend enterprise security policy to remote and branch offices

Module 5 - Enterprise WLAN Management and Monitoring

- Device identification and tracking
- Rogue device mitigation
- WLAN forensics
- Enterprise WIPS installation and configuration
- Distributed protocol analysis
- WNMS security features
- WLAN controller security feature sets

Module 6 - Enterprise WLAN Security Technology and Solutions

- Robust Security Networks (RSN)
- WPA/WPA2 Enterprise - how it works
- WPA/WPA2 Enterprise - configuration
- IEEE 802.11 Authentication and Key Management (AKM)
- 802.11 cipher suites
- Use of authentication services (RADIUS, LDAP) in WLANs
- User profile management (RBAC) Public Key Infrastructures (PKI) used with WLANs
- Certificate Authorities and x.509 digital certificates
- RADIUS installation and configuration
- 802.1X/EAP authentication mechanisms
- 802.1X/EAP types and differences
- 802.11 handshakes
- Fast BSS Transition (FT) technologies