Advanced Wireless Security

Module 1: Introduction to Wireless Security

- Overview of Wireless Security: Types of Attacks, Vulnerabilities, and Countermeasures
- Wi-Fi Security Protocols: WEP, WPA, and WPA2
- Wireless Intrusion Detection and Prevention Systems: Techniques and Tools

Module 2: Wireless Network Auditing

- Scanning and Mapping Wireless Networks
- Analyzing Vulnerabilities and Threats
- Wireless Network Auditing Techniques and Tools

Module 3: Advanced Encryption Techniques for Wi-Fi Networks

- 802.11i, WPA3, and EAP
- Wi-Fi Security Policies and Access Controls
- Wi-Fi Security Auditing and Penetration Testing: Techniques and Tools

Module 4: Wireless Network Security Architecture

- Layered Security, Defense in Depth, and Network Segmentation
- Wireless Intrusion Prevention Systems: Techniques and Tools
- Network Access Control for Wireless Networks: 802.1X, MAC Filtering, and Captive Portals

Module 5: Wireless Network Threats

- Rogue APs, Evil Twin Attacks, and Man-in-the-Middle Attacks
- Wireless Network Forensics: Capturing and Analyzing Wireless Traffic, and Identifying Attacks and Intrusions
- Wireless Network Defense Techniques: Network Monitoring, Incident Response, and Disaster Recovery

Module 6: Emerging Wireless Security Technologies and Standards

- Wi-Fi 6, WPA3, and 5G Security
- Wireless Security for IoT Devices and Systems: Challenges and Solutions
- Wireless Security for Mobile Devices: Threats and Defenses

Module 7: Wireless Security Best Practices

- Wireless Security Policy Design and Implementation
- Wireless Security Training and Awareness
- Ongoing Monitoring, Testing, and Review of Wireless Security Measures