

SEC617: Wireless Penetration Testing and Ethical Hacking™



GAWN
Assessing & Auditing
Wireless Networks
giac.org/gawn

6
Day Program

36
CPEs

Laptop
Required

You Will Be Able To

- Detect and neutralize rogue wireless access points
- Fuzz systems to identify unknown flaws
- Use AI to support wireless analysis, evaluation, and research
- Exploit Bluetooth network authentication gaps
- Execute advanced WPA2 Enterprise penetration tests
- Develop custom wireless attack tools efficiently

Business Takeaways

- Reduce wireless attack surface by identifying overlooked vulnerabilities across technologies
- Strengthen security posture in critical environments like offices, factories, and data centers
- Validate and certify devices to support secure procurement and deployment decisions
- Enhance detection and response for rogue devices and wireless-based intrusions
- Bridge IT, OT, and physical security through unified wireless threat assessments
- Support compliance and governance with evidence-based wireless security practices
- Equip teams with hands-on tools for real-world wireless penetration testing and defense

“SEC617 is great for someone looking for a top-to-bottom rundown in wireless attacks.”

— Garret Picchioni, **Salesforce**

“I have a better understanding of the technologies and protocols in use and can now perform more accurate risk assessments.”

— Shawn Pray, **Accenture**

Build hands-on skills to assess and exploit vulnerabilities across Wi-Fi, Bluetooth, RFID, NFC, and software-defined radio systems to improve wireless defenses.

Modern organizations often underestimate wireless security, leaving critical infrastructure vulnerable to sophisticated attacks. SEC617 addresses this critical gap by providing security professionals with comprehensive skills to identify, evaluate, and defend against wireless technology threats. From Wi-Fi networks to Bluetooth devices, RFID systems, and software-defined radio, this Wi-Fi hacking course delivers hands-on training that expands your wireless security expertise across multiple technologies and protocols.

This course is designed for professionals seeking a comprehensive technical ability to understand, analyze, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entrance points for attackers.

The authors of SEC617, as penetration testers themselves, know that many organizations overlook wireless security as an attack surface, and therefore fail to establish required defenses and monitoring, even though wireless technologies are now commonplace in executive suites, financial departments, government offices, manufacturing production lines, retail networks, medical devices, and air traffic control systems. Given the known risks of insecure wireless technologies and the attacks used against them, SEC617 was designed to help people build the vital skills needed to identify, evaluate, assess, and defend against these threats. These skills are ‘must-have’ for any high-performing security organization.

Author Statement

“It has been amazing to watch the progression of wireless technology and the near-ubiquitous adoption of it over the past several years. Wi-Fi has grown in maturity and offers strong authentication and encryption options to protect networks. Yet many organizations continue to fail to implement these protections appropriately. We have also watched attacker sophistication grow with their toolsets, giving them the upper hand in exploiting technology we rely on for critical tasks. This pattern has us concerned. With the implementation of wireless technology on the rise, the attack surface continues to grow as well.

It is not surprising that other wireless protocols have also emerged to satisfy the needs of specialty interference-resilient connectivity (Bluetooth Classic and Bluetooth Low Energy), physical security and contactless payments (NFC and RFID), and many others using unknown standards-based and proprietary wireless technologies. It is no longer enough to just be a Wi-Fi expert; you also need to be able to evaluate the entire wireless threat landscape across a whole host of technologies.

We are very excited to deliver updated hands-on labs and a suite of hardware tools to equip modern wireless security analysts with practical skills that they can bring back to their organization and apply on day one. The skills you will build in this class will be valuable for today’s wireless technology, for tomorrow’s technology advancements, and for other complex systems you have to evaluate in the future.”

—Larry Pesce and James Leyte-Vidal

Section Descriptions

SECTION 1: Wi-Fi Data Collection and Analysis

Explore wireless threat landscapes and fundamental analysis techniques. Learn to identify rogue devices, understand protocol weaknesses, and develop remote penetration testing skills using compromised Windows and macOS systems.

TOPICS:

- Wireless Threat Characterization
- Wi-Fi Protocol Layer Analysis
- Packet Capture Techniques
- Rogue Access Point Detection
- Radio Frequency Exposure Mapping

SECTION 2: Wi-Fi Attack and Exploitation Techniques

Develop advanced skills to exploit Wi-Fi vulnerabilities across consumer and enterprise networks. Focus on protocol-level deficiencies and practical attack methodologies.

TOPICS:

- Hotspot network exploitation
- Client-side Wi-Fi attacks
- WEP technology vulnerabilities
- Denial-of-Service strategies
- Wi-Fi protocol fuzzing techniques

SECTION 3: Enterprise Wi-Fi Attacks

Dive deep into WPA2 and WPA3 network assessments, exploring authentication and security modes. Investigate nearest neighbor attacks and operation within constrained environments.

TOPICS:

- WPA2 Network Penetration
- Enterprise Authentication Bypass
- WPA3 Security Analysis
- Nearest Neighbor Attacks

SECTION 4: Bluetooth and Software-Defined Radio Attacks

Examine Bluetooth technologies across classic, enhanced data rate, and low energy protocols. Learn Software Defined Radio techniques for identifying and assessing proprietary wireless systems.

TOPICS:

- Bluetooth Pairing Vulnerabilities
- BLE Device Service Exploitation
- Software-Defined Radio Techniques
- RF Spectrum Analysis
- Wireless Signal Decoding

SECTION 5: Privacy, RFID, Smart Cards, and NFC Hacking

Evaluate RFID technologies, privacy risks, and security vulnerabilities in contactless systems. Develop skills to analyze and exploit smart card and NFC technologies.

TOPICS:

- Tracking and Privacy Attacks
- RFID System Components
- Low-Frequency RFID Exploitation
- Smart Card Reconnaissance
- NFC Protocol Analysis

SECTION 6: Capture-the-Flag Event

On the last day of class we will pull together all the concepts and technology we have covered during the week in a comprehensive Capture-the-Flag event. In this hands-on exercise, you will have the option to participate in multiple roles; attacking recorded Wi-Fi networks, decoding proprietary wireless signals, exploiting smart card deficiencies, and more.

Who Should Attend

- Ethical hackers and penetration testers
- Network security staff
- Network and system administrators
- Incident response teams
- Information security policy decision-makers
- Technical auditors
- Information security consultants
- Wireless system engineers
- Embedded wireless system developers



GAWN
Assessing & Auditing
Wireless Networks
giac.org/gawn

GIAC Assessing and Auditing Wireless Networks

The GIAC Assessing and Auditing Wireless Networks (GAWN) certification validates a technologist's readiness to assess the security of wireless networks. GAWN certification holders have proven fluency in the techniques used to analyze wireless networks and their different security mechanisms, as well as expertise in the tools and techniques used to evaluate and exploit weaknesses. GAWN candidates understand how their tools operate and know the weaknesses in protocols they evaluate.

- Attacking weak encryption, 802.11 fuzzing attacks, and bluetooth attacks
- Bridging the air gap, DECT, DoS on wireless networks, high-frequency RFID attacks, and RFID applications
- Hotspots, low-frequency RFID attacks, NFC, practical SDR attacks, and rogue networks
- Sniffing wireless, wireless basics, wireless client attacks, and WPA

“SEC617 will not only give you a basic understanding of wireless threats and vulnerabilities, but it can be as advanced as you want to make it with the questions that you ask”

—Daniel Mayernik, Integrity Applications Incorporated