# SEC617

**GAWN** Certification
Assessing and Auditing Wireless Networks
www.giac.org/gawn

## Wireless Ethical Hacking, Penetration Testing, and Defenses

**Six-Day Program**
**36 CPEs**
**Laptop Required**

### 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

### You Will Be Able To

- Identify and locate malicious rogue access points using free and low-cost tools
- Conduct a penetration test against low-power wireless including ZigBee to identify control system and related wireless vulnerabilities
- Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks using Ubertooth, CarWhisperer, and btaptap to collect sensitive information from headsets, wireless keyboards and Bluetooth LAN devices
- Utilize wireless capture tools to extract audio conversations and network traffic from DECT wireless phones to identify information disclosure threats exposing the organization
- Implement an enterprise WPA2 penetration test to exploit vulnerable wireless client systems for credential harvesting
- Utilize wireless fuzzing tools including Metasploit file2air, and Scapy to identify new vulnerabilities in wireless devices

Despite the security concerns many of us share regarding wireless technology, it is here to stay. In fact, not only is wireless here to stay, it is growing in deployment and utilization with wireless LAN technology and WiFi as well as other applications, including cordless telephones, smart homes, embedded devices, and more. Technologies like ZigBee and Z-Wave offer new methods of connectivity to devices, while other wireless technology, including WiFi, Bluetooth, Bluetooth Low Energy, and DECT, continue their massive growth rate, each introducing its own set of security challenges and attacker opportunities.

"SEC617 gave me the knowledge and skill sets in areas that I lacked, allowing me to become a better InfoSec professional."
-Kirk Wah Yick, US Bank

To be a wireless security expert, you need to have a comprehensive understanding of the technology, threats, exploits, and defensive techniques along with hands-on experience in evaluating and attacking wireless technology. Not limiting your skill-set to WiFi, you'll need to evaluate the threat from other standards-based and proprietary wireless technologies as well. This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, you'll navigate your way through the techniques attackers use to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems. You'll also develop attack techniques leveraging Windows 7 and Mac OS X. We'll examine the commonly overlooked threats associated with Bluetooth, ZigBee, DECT, and proprietary wireless systems. As part of the course, you'll receive the SWAT Toolkit, which will be used in hands-on labs to back up the course content and reinforce wireless ethical hacking techniques.

Using assessment and analysis techniques, this course will show you how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

"SEC617 gave me a greater appreciation for the risks associated with wireless technologies. The course was well worth my time."
-Thomas W., USMC

www.sans.org/SEC617

www.sans.edu

www.sans.org/cyber-guardian

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

*Course Day Descriptions*

## 617.1 HANDS ON: Wireless Data Collection and WiFi MAC Analysis

Students will identify the risks associated with modern wireless deployments as well as the characteristics of physical layer radio frequency systems, including 802.11a/b/g systems. Students will leverage open-source tools for analyzing wireless traffic and mapping wireless deployments.

**Topics: Understanding the Wireless Threat; Wireless LAN Organizations and Standards; Using the SANS Wireless Auditing Toolkit; Sniffing Wireless Networks: Tools, Techniques and Implementation; IEEE 802.11 MAC: In-Depth**

## 617.2 HANDS ON: Wireless Tools and Information Analysis

Students will develop an in-depth treatise on the IEEE 802.11 MAC layer and operating characteristics. Using passive and active assessment techniques, students will evaluate deployment and implementation weaknesses, auditing against common implementation requirements including PCI and the DoD Directive 8100.2. Security threats introduced with rogue networks will be examined from a defensive and penetration-testing perspective. Threats present in wireless hotspot networks will also be examined, identifying techniques attackers can use to manipulate guest or commercial hotspot environments.

**Topics: Wireless LAN Assessment Techniques; Rogue AP Analysis; Wireless Hotspot Networks; Attacking WEP**

SANS

### *SEC617 Training Formats*

*(subject to change)*

**Live Training**
www.sans.org/security-training/by-location/all

**Summit Events**
www.sans.org/summit

**Mentor Training**
www.sans.org/mentor

**Private Training**
www.sans.org/onsite

## 617.3 HANDS ON: Client, Crypto, and Enterprise Attacks

Students will continue their assessment of wireless security mechanisms, such as the identification and compromise of static and dynamic WEP networks and the exploitation of weak authentication techniques, including the Cisco LEAP protocol. Next-generation wireless threats will be assessed, including attacks against client systems such as network impersonation attacks and traffic manipulation.

**Topics: Cisco LEAP Attacks; Wireless Client Attacks; Attacking WPA2-PSK Networks; Assessing Enterprise WPA2**

## 617.4 HANDS ON: Advanced WiFi Attack Techniques

**Topics: Deficiencies in TKIP Networks; Leveraging WiFi DoS Attacks; Wireless Fuzzing for Bug Discovery; Bridging the Airgap: Remote WiFi Pentesting; Framework and Post-Exploitation Modules**

## 617.5 HANDS ON: Bluetooth, DECT, and ZigBee Attacks

Advanced wireless testing and vulnerability discovery systems will be covered, including 802.11 fuzzing techniques. A look at other wireless technology, including proprietary systems, cellular technology, and an in-depth coverage of Bluetooth risks, will demonstrate the risks associated with other forms of wireless systems and their impact on organizations.

**Topics: DECT Attacks; Exploiting ZigBee; Enterprise Bluetooth Threats; Advanced Bluetooth Threats**

## 617.6 HANDS ON: Wireless Security Strategies and Implementation

The final day of the course evaluates strategies and techniques for protecting wireless systems. Students will examine the benefits and weaknesses of WLAN IDS systems. Students will also examine critical secure network design choices, including the selection of an EAP type, selection of an encryption strategy, and the management of client configuration settings.

**Topics: WLAN IDS Analyst Techniques; Evaluating Proprietary Wireless Technology; Deploying a Secure Wireless Infrastructure; Configuring and Securing Wireless Clients**

> "If you're thinking about wireless, take this course. If you're not, take this course."
>
> -Greg Notch, NHL

> "SEC617 is a necessity if you're working in wireless security."
>
> -Steven Ostrander, Arma Global