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

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

-Thomas W., USMC

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.**

For many analysts, "wireless" was once synonymous with "WiFi," the ever-present networking technology, and many organizations deployed complex security systems to protect these networks. Today, wireless takes on a much broader meaning – not only encompassing the security of WiFi systems, but also the security of Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even proprietary wireless systems. To effectively evaluate the security of wireless systems, your skillset needs to expand to include many different types of wireless technologies.

SEC617 will give you the skills you need to understand the security strengths and weaknesses of wireless systems. You will learn how to evaluate the ever-present cacophony of WiFi networks and identify the WiFi access points (APs) and client devices that threaten your organization. You will learn how to assess, attack, and exploit deficiencies in modern WiFi deployments using WPA2 technology, including sophisticated WPA2 Enterprise networks. You will gain a strong, practical understanding of the many weaknesses in WiFi protocols and how to apply that understanding to modern wireless systems. Along with identifying and attacking WiFi access points, you will learn to identify and exploit the behavioral differences in how client devices scan for, identify, and select APs, with deep insight into the behavior of the Windows 10, macOS, Apple iOS, and Android WiFi stacks.

A significant portion of the course focuses on Bluetooth and Bluetooth Low Energy (BLE) attacks, targeting a variety of devices, including wireless keyboards, smart light bulbs, mobile devices, audio streaming devices, and more. You will learn to assess a target Bluetooth device, identify the present (or absent) security controls, and apply a solid checklist to certify a device's security for use within your organization.

Beyond analyzing WiFi and Bluetooth security threats, analysts must also understand many other wireless technologies that are widely utilized in complex systems. SEC617 provides insight and hands-on training to help analysts identify and assess the use of ZigBee and Z-Wave wireless systems used for automation, control, and smart home systems. The course also investigates the security of cordless telephony systems in the worldwide Digital Enhanced Cordless Telephony (DECT) standard, including audio eavesdropping and recording attacks.

Radio frequency identification (RFID), near field communication (NFC), and contactless smart card systems are more popular than ever in countless applications such as point of sale systems and data center access control systems. You will learn how to assess and evaluate these deployments using hands-on exercises to exploit the same kinds of flaws discovered in mass transit smart card systems, hotel guest room access systems, and more.

In addition to standards-based wireless systems, we also dig deeper into the radio spectrum using software-defined radio (SDR) systems to scour for signals. Using SDR, you will gain new insight into how widely pervasive wireless systems are deployed. **With your skills in identifying, decoding, and evaluating the data these systems transmit, you will be able to spot vulnerabilities even in custom wireless infrastructures.**

SANS
www.sans.org/SEC617

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

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

617.1 HANDS ON: WiFi Data Collection and Analysis

The first section of the course quickly looks at wireless threats and attack surfaces and analyzes where you will likely see non-WiFi systems deployed in modern networks. We start off with a look at fundamental analysis techniques for evaluating WiFi networks, including the identification and analysis of rogue devices, and finish with a dive into remote penetration testing techniques using compromised Windows 10 and macOS devices to pivot.

Topics: Characterize the Wireless Threat; Sniffing WiFi; Rogue Access Point (AP) Analysis

617.2 HANDS ON: WiFi Attack and Exploitation Techniques

After developing skills needed to capture and evaluate WiFi activity, we start our look at exploiting WiFi, targeting AP and client devices. We cover techniques that apply to any WiFi products, from consumer to enterprise-class devices, focusing on understanding protocol-level deficiencies that will continue to be applied throughout the course on non-WiFi wireless systems as well.

Topics: Exploiting WiFi Hotspots; WiFi Client Attacks; Exploiting WEP; Denial of Service (DoS) Attacks; WiFi Fuzzing for Bug Discovery

617.3 HANDS ON: Enterprise WiFi, DECT, and ZigBee Attacks

We finish our look at WiFi attack techniques with a detailed look at assessing and exploiting WPA2 networks. Starting with WPA2 consumer networks, we investigate the flaws associated with pre-shared key networks and WiFi Protected Setup (WPS) deployments, continuing with a look at exploiting WPA2 Enterprise networks using various Extensible Authentication Protocol (EAP) methods. We continue to investigate the security of wireless networks on day 3, switching to non-WiFi analysis with a look at exploiting the worldwide Digital Enhanced Cordless Telephony (DECT) standard to capture and export audio conversations from cordless headsets and phones. We also investigate the security of ZigBee and IEEE 802.15.4 networks, looking at cryptographic flaws, key management failures, and an introduction to hardware attacks.

Topics: Attacking WPA2 Pre-Shared Key Networks; Attacking WPA2 Enterprise Networks; Attacking Digital Enhanced Cordless Telephony Deployments; Attacking ZigBee Deployments

617.4 HANDS ON: Bluetooth and Software Defined Radio Attacks

Bluetooth technology is nearly as pervasive as WiFi, with widespread adoption in smart phones, fitness trackers, wireless keyboard, smart watches, and more. In this module, we dig into the Bluetooth Classic, Enhanced Data Rate, and Low Energy protocols, including tools and techniques to evaluate target devices for vulnerabilities. Immediately following our look at Bluetooth technology, we jump into the practical application of Software Defined Radio (SDR) technology to identify, decode, and assess proprietary wireless systems. We investigate the hardware and software available for SDR systems, and look at the tools and techniques to start exploring this exciting area of wireless security assessment.

Topics: Bluetooth Introduction and Attack Techniques; Bluetooth Low Energy Introduction and Attack Techniques; Practical Application of Software-Defined Radio (SDR)

617.5 HANDS ON: RFID, Smart Cards, and NFC Hacking

On day 5, we evaluate RFID technology in its multiple forms to identify the risks associated with privacy loss and tracking, while also building an understanding of both low-frequency and high-frequency RFID systems and NFC. We examine the security associated with contactless Point of Sale (PoS) terminals, including Apple Pay and Google Wallet, and proximity lock access systems from HID and other vendors. We also examine generalized techniques for attacking smart card systems, including critical data analysis skills needed to bypass the intended security of smart card systems used for mass transit systems, concert venues, bike rentals, and more.

Topics: RFID Overview; RFID Tracking and Privacy Attacks; Low-Frequency RFID Attacks; Exploiting Contactless RFID Smart Cards; Attacking NFC

617.6 HANDS ON: 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: identifying unauthorized/rogue WiFi access points, attacking live and recorded WiFi networks, decoding proprietary wireless signals, exploiting smart card deficiencies, and more. During this wireless security event you will put into practice the skills you have learned in order to evaluate systems and defend against attackers, simulating the realistic environment you will be prepared to protect when you get back to the office.

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

"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