SEC556: **IoT Penetration Testing™**

3 Day Course	18 CPEs	Laptop Required

You Will Be Able To

- Assess IoT network controls comprehensively
- Investigate hardware interaction points
- Uncover firmware vulnerabilities
- Analyze wireless technology weaknesses
- Manipulate Bluetooth Low Energy devices
- Reverse-engineer unknown radio protocols
- Use AI as a force multiplier for penetration testing activities

Business Takeaways

- Faster detection of real threats
- Maximized ROI on existing tools
- Develops in-house threat detection expertise
- Defensive coverage against modern tactics
- Operational confidence and retention
- Alignment with security goals and audit requirements

"I really liked the firmware dumping hardware-based stuff, followed by the Bluetooth BLE and SDR exercises. I had not done this before and it was taught well enough that I could go out into the field and do them again."

—Caleb Jaren; **Microsoft**

IoT Security Spans Every Technology Layer

A growing trend in recent years has seen small-form-factor computing devices increasingly accessing networks to provide connectivity to what typically used to be disconnected devices. While we can debate if your home appliances truly need Internet access, there is no debate that the Internet of Things (IoT) is here to stay. It allows for deeper connectivity of many devices that are indeed useful, with great benefits to homes and enterprises alike.

Unfortunately, with the proliferation of connected technology, many of these devices do not consider, or only minimally consider, security in the design process. While we have seen this behavior in other types of testing as well, IoT is different because it utilizes and mixes many different technology stacks such as custom Operating System builds, web and API interfaces, various networking protocols (e.g., Zigbee, LoRA, Bluetooth/BLE, WiFi), and proprietary wireless.

This wide range of diverse, poorly secured technology makes for a desirable pivot point into networks, opportunities for modification of user data, network traffic manipulation, and more. That's why dedicated IoT security training is essential for professionals responsible for defending or assessing modern connected systems.

SANS SEC556 training is a hands-on IoT hacking course that will familiarize you with common interfaces in IoT devices and recommend a process along with the Internet of Things Attack (IoTA), testing framework to evaluate these devices within many layers of the Open Systems Interconnection (OSI) model. From firmware and network protocol analysis to hardware implementation issues and all the way to application flaws, we will give you the tools and hands-on techniques to evaluate the ever-expanding range of IoT devices.

The course approach facilitates examining the IoT ecosystem across many different verticals, from automotive technology to healthcare, manufacturing, and industrial control systems. In all cases, the methodology is the same, but the risk model is different. This IoT security training framework ensures students are equipped to assess devices across sectors, with the adaptability to handle emerging technologies and threats.

Once we have been empowered to understand each challenge, we can understand the need for more secure development and implementation practices with IoT devices.

"The labs work well for bringing concepts home and making them real. The work done to scale/virtualize them and make them repeatable is amazing."

—Lee Neely; **Lawrence Livermore National Laboratory**

"This course is perfect to learn essential contents of IoT pen testing."

—Junya F., **Hitachi**

Section Descriptions

SECTION 1: Introduction to IoT Network Traffic and Web Services

This section introduces IoT security challenges, focusing on testing methodologies applicable across diverse implementations. Students explore threat modeling, network reconnaissance, web application vulnerabilities, and API interaction techniques. The section emphasizes practical strategies for identifying and exploiting IoT network and web-based vulnerabilities.

TOPICS: Course Methodology Introduction; IoT Testing Framework; Network Discovery Techniques; Web Service Reconnaissance; Vulnerability Exploitation Strategies

SECTION 3: Exploiting Wireless IoT: WiFi, BLE, Zigbee, LoRA, and SDR

This section explores wireless technologies prevalent in IoT ecosystems, providing comprehensive techniques for traffic capture, network access, and device compromise. Students will gain expertise in analyzing standard and proprietary wireless communication protocols.

TOPICS: WiFi Security Assessment; Bluetooth Low Energy Vulnerabilities; Zigbee Protocol Analysis; LoRA Communication Techniques; Software-Defined Radio Exploration

SECTION 2: Exploiting IoT Hardware Interfaces and Analyzing Firmware

Students will learn advanced hardware testing techniques, including device deconstruction, communication interface analysis, and firmware recovery. The section covers destructive and non-destructive testing methodologies, focusing on identifying hardware vulnerabilities and extracting critical system information.

TOPICS: Hardware Testing Fundamentals; Device Disassembly Techniques; Communication Port Identification; Firmware Analysis Methodologies; Filesystem Exploitation

Authors Statement

"It has been amazing to watch the progression and widespread adoption of what we now know as the Internet of Things in both our homes and enterprises whether you realize it or not! However, while IoT-enabled technologies have arguably made our lives better by improving conveniences and our ability to obtain more accurate data about our environment, we unknowingly increase our attack surface through their use."

"In other words, the benefits often come at a cost, in many cases because of lackluster development practices by many IoT manufacturers that fail to consider the entirety of the attack surface of their device ecosystem. This failure is largely seen as financial; baking security in from the start is an expense that reduces the already low profit margins on IoT devices. Delays from adopting enhanced security measures can prevent a timely push to market, further compounding profit-per-device issues.

"With the increased adoption of IoT, attackers have also focused their efforts on IoT platforms. Techniques and tool capabilities have become exponentially more sophisticated, and they are often used for "good" to unlock additional features and capabilities. However, less-ethical attackers have gained the same sophistication with their toolsets, giving them the upper hand in exploiting the technology we rely on for critical tasks. The IoT adoption rate, in combination with the sophistication of attackers, paints a grave picture for the future of IoT and the networks IoT devices are connected to unless we begin now to improve the security of all facets of the IoT ecosystem.

"We are very excited to deliver interactive, hands-on labs and a suite of hardware and software tools to equip IoT analysts and developers with practical skills, methodologies, and thought processes that they can bring back to their organizations and apply on day one. The skills you will build in this class will be valuable for today's IoT technology and serve as a foundation for tomorrow's advancements, regardless of your vertical, application, or data."

–Larry Pesce and James Leyte-Vidal

Who Should Attend

This course enables attack-focused and defense-focused security practitioners, as well as those designing and implementing embedded, IoT, and IIoT solutions across many verticals (automotive, healthcare, consumer electronics, industrial instrumentation, smart home, etc.). This course is best suited for:

- Penetration testers
- Embedded system developers
- Security analysts
- Security architects
- Product security engineers
- IoT product developers
- Anyone releasing an IoT device to market

NICE Framework Work Roles:

- System Testing and Evaluation Specialist (OPM 671)
- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Adversary Emulation Specialist/ Red Teamer (OPM 541)
- Cyber Ops Planner (OPM 332)