# SEC560:<br>Network Penetration Testing and Ethical Hacking

**Course Length: Six Days • 36 CPE Credits**
**Laptop Required**

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Lots of people claim to have penetration testing, ethical hacking, and security assessment skills, but precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure. This class covers the ingredients for successful network penetration testing to help attendees improve their enterprise's security stance.

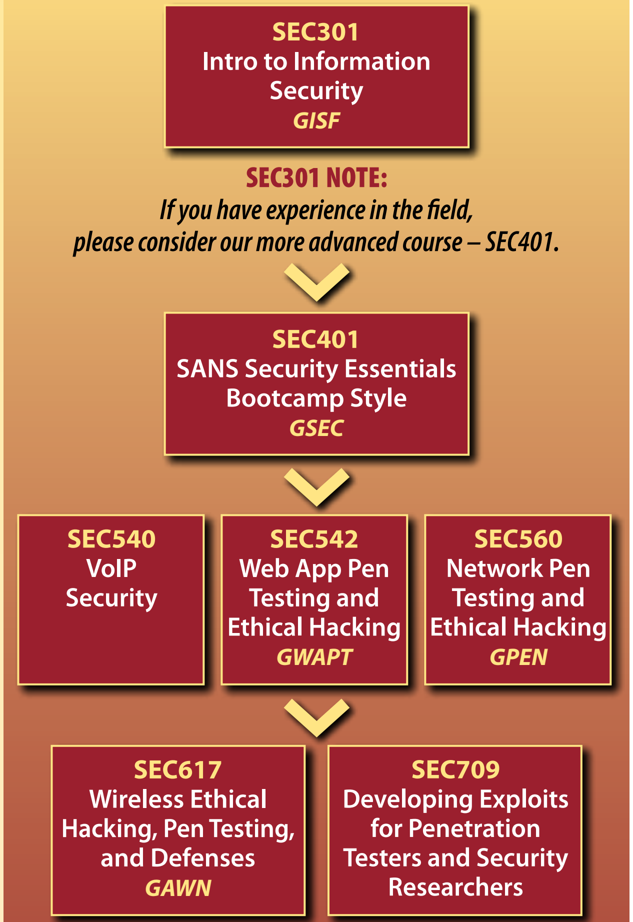
## *Find Security Flaws Before the Bad Guys Do.*

We address detailed pre-test planning, including setting up an effective penetration testing infrastructure and establishing ground rules with the target organization to avoid surprises and misunderstanding. Then we discuss a time-tested methodology for penetration and ethical hacking across the network, evaluating the security of network services and the operating systems behind them.

Attendees will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, and social networking sites. We'll then turn our attention to scanning, experimenting with numerous tools in hands-on exercises. Our exploitation phase will include the use of exploitation frameworks, stand-alone exploits, and other valuable tactics, all with hands-on exercises in our lab environment. The class also discusses how to prepare a final report tailored to maximize the value of the test from both a management and technical perspective.The final portion of the class includes a comprehensive hands-on exercise in which students will conduct a penetration test against a hypothetical target organization following all of the steps.

The course also describes the limitations of penetration testing techniques and other practices that can be used to augment penetration testing to find vulnerabilities in architecture, policies, and processes. We address how penetration testing should be integrated as a piece of a comprehensive enterprise information security program.

### *Penetration Testing Curriculum*



SEC301
Intro to Information Security
*GISF*

**SEC301 NOTE:**
*If you have experience in the field,
please consider our more advanced course – SEC401.*

SEC401
SANS Security Essentials Bootcamp Style
*GSEC*

SEC540
VoIP Security

SEC542
Web App Pen Testing and Ethical Hacking
*GWAPT*

SEC560
Network Pen Testing and Ethical Hacking
*GPEN*

SEC617
Wireless Ethical Hacking, Pen Testing, and Defenses
*GAWN*

SEC709
Developing Exploits for Penetration Testers and Security Researchers

### *Additional Penetration Testing Courses*

**DEV538:** Web App Pen Testing Immersion
**SEC553:** Metasploit for Pen Testers
**SEC559:** Wireless Security Exposed
**SEC561:** Network Pen Testing: Reports, Exploits, and Command Shells
**SEC565:** Data Leakage Prevention – In Depth

SANS www.sans.org

***For more information, visit http://www.sans.org***
When registering, use this promo code ***SEC560***

## Differentiators

This SANS course differs from other penetration testing and ethical hacking courses in several important ways:

- We get deep into the tools arsenal with numerous hands-on exercises that show subtle, less-well-known, and undocumented features that are incredibly useful for professional penetration testers and ethical hackers.
- The course discusses how the tools interrelate with each other in an overall testing process. Rather than just throwing up a bunch of tools and playing with them, we analyze how to leverage information from one tool to get the most bang out of the next tool.
- We focus on the workflow of professional penetration testers and ethical hackers, proceeding step-by-step discussing the most effective means for conducting projects.
- The sessions address common pitfalls that arise in penetration tests and ethical hacking projects, providing real-world strategies and tactics for avoiding these problems to maximize the quality of test results.
- We cover several timesaving tactics based on years of in-the-trenches experience from real penetration testers and ethical hackers, actions that might take hours or days unless you know the little secrets we'll cover that will let you surmount a problem in minutes.
- The course stresses the mind-set of successful penetration testers and ethical hackers, which involves balancing the often contravening forces of creative "outside-the-box" thinking, methodical trouble-shooting, carefully weighing risks, following a time-tested process, painstakingly documenting results, and creating a high quality final report that achieves management and technical buy-in.
- We also analyze how penetration testing and ethical hacking should fit into a comprehensive enterprise information security program.

## Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing target networks and systems to find security vulnerabilities

## SANS Cyber Guardian Program

SANS' Cyber Guardian program is designed for the elite teams of technical security professionals who are part of the armed forces, Department of Defense, or other government agencies whose role includes securing systems, reconnaissance, counterterrorism and counter hacks. These teams will be the cyber security special forces where each individual's role makes the team successful.

The Cyber Guardian program provides intensive, hands-on training for both Red and Blue teams. Participants must complete three core courses and the corresponding certifications within two years of starting the program. After completing all three core courses and exams, candidates will choose their specialization and complete two more courses and certifications. Upon the successful completion of all courses and certifications, candidates will finish the program by taking and passing the GSE (GIAC Security Expert) exam and joining the elite group of GSE certified professionals.

An intensive, real-world exercise on defending and attacking systems has been created to demonstrate how each cyber guardians' skills and expertise will be utilized in an actual attack.

You wouldn't go to battle with a team you have never trained with, so this exercise will show each participant how their role contributes to the success of their team.

For more information, please visit **http://www.sans.org/cyber-guardian**

## GIAC Certified Penetration Tester (GPEN)

The GPEN certification is for security personnel whose job duties involve assessing target networks and systems to find security vulnerabilities. Certification objectives include penetration-testing methodologies, the legal issues surrounding penetration testing and how to properly conduct a penetration test as well as best practice technical and non-technical techniques specific to conduct a penetration test.

### Four Reasons to 'Get GIAC Certified'

GIAC Certification:

1. **Promotes** learning that improves your hands-on technical skills and improves knowledge retention
2. **Provides** proof that you possess hands-on technical skills
3. **Positions** you to be promoted and earn respect among your peers
4. **Proves** to hiring managers that a candidate is qualified for the job

***Learn more about GIAC at www.giac.org.***