SEC561

Immersive Hands-on Hacking Techniques

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Security professionals who want to expand their hands-on technical skills in new analysis areas such as packet analysis, digital forensics, vulnerability assessment, system hardening, and penetration testing
- Systems and network administrators who want to gain hands-on experience in information security skills to become better administrators
- Incident response analysts who want to better understand system attack and defense techniques
- Forensic analysts who need to improve their analysis through experience with real-world attacks
- Penetration testers seeking to gain practical experience for use in their own assessments
- Red team members who want to build their hands-on skills

You Will Be Able To

- Use network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation
- Use password analysis tools to identify weak authentication controls leading to unauthorized server access
- Evaluate web applications for common developer flaws leading to significant data loss conditions
- Manipulate common network protocols to maliciously reconfigure internal network traffic patterns
- Identify weaknesses in modern anti-virus signature and heuristic analysis systems
- Inspect the configuration deficiencies and information disclosure threats present on Windows and Linux servers
- Bypass authentication systems for common web application implementations
- Exploit deficiencies in common cryptographic systems
- Bypass monitoring systems by leveraging IPv6 scanning and exploitation tools
- Harvest sensitive mobile device data from iOS and Android targets

To be a top penetration testing professional, you need fantastic hands-on skills for finding, exploiting and resolving vulnerabilities. Top instructors at SANS engineered **SEC561: Immersive Hands-On Hacking Techniques** from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises, maximizing keyboard time during in-class labs and making this SANS' most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical skills needed to handle today's pen test and vulnerability assessment projects in enterprise environments. Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios using skills that they will be able to apply the day they get back to their jobs.

"80% hands-on is intense and the best way to build on previous pen-testing-focused SANS courses."
-Timothy McKenzie, DELL/Secureworks

People often talk about these concepts, but this course teaches you how to actually do them hands-on and in-depth. SEC561 shows penetration testers, vulnerability assessment personnel, auditors, and operations personnel how to leverage in-depth techniques to get powerful results in every one of their projects. The course is overflowing with practical lessons and innovative tips, all with direct hands-on application. Throughout the course, students interact with brand new and custom-developed scenarios built just for this course on the innovative NetWars challenge infrastructure, which guides them through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.

Topics addressed in the course include:

- **Applying network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation.**
- **Manipulating common network protocols to reconfigure internal network traffic patterns, as well as defenses against such attacks.**
- **Analyzing Windows and Linux systems for weaknesses using the latest enterprise management capabilities of the operating systems, including the super-powerful Windows Remote Management (WinRM) tools.**
- **Applying cutting-edge password analysis tools to identify weak authentication controls leading to unauthorized server access.**
- **Scouring through web applications and mobile systems to identify and exploit devastating developer flaws.**
- **Evading anti-virus tools and bypassing Windows User Account Control to understand and defend against these advanced techniques.**
- **Honing phishing skills to evaluate the effectiveness of employee awareness initiatives and your organization's exposure to one of the most damaging attack vectors widely used today.**

SANS

www.sans.org/SEC561

561.1 HANDS ON: Security Platform Analysis

The first day of the course prepares students for real-world security challenges by giving them hands-on practice with essential Linux and Windows server and host management tools. First, students will leverage built-in and custom Linux tools to evaluate the security of host systems and servers, inspecting and extracting content from rich data sources such as image headers, browser cache content, and system logging resources. Next, students will turn their focus to performing similar analysis against remote Windows servers using built-in Windows system management tools to identify misconfigured services, scrutinize historical registry entries for USB devices, evaluate the impact of malware attacks, and analyze packet capture data. By completing these tasks, students build their skills in managing systems, applicable to post-compromise system host analysis, or defensive tasks such as defending targeted systems from persistent attack threats. By adding new tools and techniques to their arsenal, students are better prepared to complete the analysis of complex systems with greater accuracy in less time.

Topics: Linux Host and Server Analysis; Windows Host and Server Analysis

SANS

SEC561 Training Formats

(subject to change)

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

Private Training
www.sans.org/onsite

561.2 HANDS ON: Enterprise Security Assessment

In this section of the class, students investigate the critical tasks for a high-quality penetration test. We'll look at the safest, most efficient ways to map a network and discover target systems and services. Once the systems are discovered, we look for vulnerabilities and reduce false positives with manual vulnerability verification. We'll also look at exploitation techniques, including the use of the Metasploit Framework to exploit these vulnerabilities, accurately describing risk and further reducing false positives. Of course, exploits are not the only way to access systems, so we also leverage password-related attacks, including guessing and cracking techniques to extend our reach for a more effective and valuable penetration test.

Topics: Network Mapping and Discovery; Enterprise Vulnerability Assessment; Network Penetration Testing; Password and Authentication Exploitation

561.3 HANDS ON: Web Application Assessment

This section of the course will look at the variety of flaws present in web applications and how each of them is exploited. Students will solve challenges presented to them by exploiting web applications hands-on with the tools used by professional web application penetration testers every day. The websites students attack mirror real-world vulnerabilities including Cross-Site Scripting (XSS), SQL Injection, Command Injection, Directory Traversal, Session Manipulation and more. Students will need to exploit the present flaws and answer questions based on the level of compromise they are able to achieve.

Topics: Recon and Mapping; Server-side Web Application Attacks; Client-side Web Application Attacks; Web Application Vulnerability Exploitation

561.4 HANDS ON: Mobile Device and Application Analysis

With the accelerated growth of mobile device use in enterprise networks, organizations find an increasing need to identify expertise in the security assessment and penetration testing of mobile devices and the supporting infrastructure. In this component of the course, we examine the practical vulnerabilities introduced by mobile devices and applications, and how they relate to the security of the enterprise. Students will look at the common vulnerabilities and attack opportunities against Android and Apple iOS devices, examining data remnants from lost or stolen mobile devices, the exposure introduced by common weak application developer practices, and the threat introduced by popular cloud-based mobile applications found in many networks today.

Topics: Mobile Device Assessment; Mobile Device Data Harvesting; Mobile Application Analysis

561.5 HANDS ON: Advanced Penetration Testing

This portion of the class is designed to teach the advanced skills required in an effective penetration test to extend our reach and move through the target network. This extended reach will provide a broader and more in-depth look at the security of the enterprise. We'll utilize techniques to pivot through compromised systems using various tunneling/pivoting techniques, bypass anti-virus and built-in commands to extend our influence over the target environment, and find issues that lesser testers may have missed. We'll also look at some of the common mistakes surrounding poorly or incorrectly implemented cryptography and ways to take advantage of those weaknesses to access systems and data that are improperly secured.

Topics: Anti-Virus Evasion Techniques; Advanced Network Pivoting Techniques; Exploiting Network Infrastructure Components

561.6 HANDS ON: Capture the Flag Challenge

This lively session represents the culmination of the course, where attendees will apply the skills they have mastered throughout all the other sessions in a hands-on workshop. Students will participate in a larger version of the exercises presented in the class to independently reinforce skills learned throughout the course. They will then apply their newly developed skills to scan for flaws, use exploits, unravel technical challenges, and dodge firewalls, all while guided by the challenges presented by the NetWars Scoring Server. By practicing the skills in a combination workshop in which multiple focus areas are combined, participants will have the opportunity to explore, exploit, pillage, and continue to reinforce skills against a realistic target environment.