SEC580: **Metasploit Kung Fu for Enterprise Pen Testing**

2 Day Course	12 CPEs	Laptop Required

Who Should Attend

- IT security engineers
- Penetration testers
- Security consultants
- Vulnerability assessment personnel
- Vulnerability management personnel
- Network security analysts
- Auditors
- General security engineers
- Security researchers

"SEC580 is the best course available on the planet for in-depth knowledge of Metasploit."

— Tom Reeves, **Northrup Grumman**

Course Preview
available at: **sans.org/demo**

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of these tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers confirm vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

SEC580 will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, and according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, anti-virus evasion, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created to exploit and analyze security flaws.

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

Author Statement

"Metasploit is the most popular free exploitation tool available today. It is in widespread use by penetration testers, vulnerability assessment personnel, auditors, and real-world threat actors. However, most of its users rely on and understand only about 10 percent of its functionality, not realizing the immensely useful other features that Metasploit offers. This course will enable students to master the 10 percent they currently rely on (applying it in a more comprehensive and safe manner), while unlocking the other 90 percent of features they can then apply to make their tests more effective. By attending this course, students will learn how to make a free tool achieve the power of many much more costly commercial tools."

— Jeff McJunkin

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

Section Descriptions

SECTION 1: Metasploit Kung Fu for Enterprise Pen Testing

Section 1 is designed to help attendees master the most heavily used exploitation framework on the planet and see how they can wield it effectively in professional penetration testing. We analyze some of the most powerful and yet often overlooked capabilities of the Metasploit Framework, using numerous exercises that make this one of the most hands-on courses ever developed by SANS. In this first course section you will go from zero to exploit and beyond faster than you ever thought possible. For example, after this class day you will understand the Ruby foundations of Metasploit and how interacting with these underpinnings will greatly optimize and enhance your testing activities. Further, you will understand how far you can extend your exploitation activities through the effective use of some of the late-breaking features of the amazing Meterpreter. Finally, have you ever wondered how you can compromise an entire domain from simple Windows system access? After this day you will know exactly how to achieve this kind of result. After all, shell is only the beginning.

TOPICS: Guided Overview of Metasploit's Architecture and Components; Deep Dive into the Msfconsole Interface, including Logging and Session Manipulation; Careful and Effective Exploitation; The Ultimate Payload: The Metasploit Meterpreter In-Depth; Metasploit's Integration into a Professional Testing Methodology; Automation with Meterpreter Scripts to Achieve More in Less Time with Consistency; It's Not All Exploits - Using Metasploit as a Recon Tool; Using Auxiliary Modules to Enhance your Testing; Ultra-Stealthy Techniques for Bypassing Anti-Virus Tools; Client-Side Attacks - Using One-Liners instead of Executables; Port and Vulnerability Scanning with Metasploit, Including Integration with Nmap, Nessus, and Qualys; Capturing SMB Credentials and Metasploit's awesome PowerShell integration

SECTION 2: Metasploit Kung Fu for Enterprise Pen Testing

In this second course section, we build upon the deep foundations of day 1 to see how Metasploit can be used within a penetration tester's ecosystem of tools and techniques to attack systems in new and creative ways. We'll analyze the activities of the most effective bad guys to see how they target enterprises via complex and often non-traditional attack vectors so that we can model their behaviors in our penetration testing processes. Client-side attacks launched via email, phishing, and document payload attacks are currently some of the most heavily used attack vectors. The bad guys use these techniques because they almost always work. The course shows penetration testers how to wield such attacks with the goal of determining the business implications of vulnerabilities, all with the goal of improving the target organization's security stance.

TOPICS: Merciless Pivoting: Routing Through Exploited Systems; Exposing Metasploit's Routing Using SOCKS Proxies; Privilege Escalation Attacks; Metasploit Integration with Other Tools; Making the Most of Windows Payloads; Advanced Pillaging - Gathering Useful Data from Compromised Machines; Evading Countermeasures to Mimic Sophisticated Attackers; Scripting Up the Meterpreter to Customize Your Own Attacks; Persisting Inside an Environment; Carefully Examining Your Attack's Forensic Artifacts; Integration with CrackMapExec, a Stand-alone Testing Tool

What You Will Receive

- Custom distribution of the Linux SANS Slingshot Linux virtual machine containing Metasploit and other tools, additional PowerShell modules, and a custom exploit module
- Custom Windows 10 Professional virtual machine containing vulnerable software, post-exploitation targets, and additional software and information for pillaging
- Step-by-step lab instructions that you can use anywhere, anytime
- MP3 audio files of the complete course lecture

"SEC580 has well-thought-out course material that takes you step-by-step through the meat and potatoes of Metasploit."

— Scott Tirapelle, **Franchise Tax Board**

"I come back to SEC580 every two years to see the current penetration testing models, as well as Meterpreter changes."

— Jim O'Keeffe, **Willis Towers Watson**