SEC580

Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course
12 CPEs
Laptop Required

Who Should Attend

- This class would be essential to any industry that has to test regularly as part of compliance requirements or regularly tests their security infrastructure as part of healthy security practices.
- Penetration testers
- Vulnerability assessment personnel
- Auditors
- General security engineers
- Security researchers

Author Statement

Metasploit is the most popular free exploitation tool available today. It is in widespread use by penetration testers, vulnerability assessment personnel, and auditors. However, most of its users rely on only about 10 percent of its functionality, not realizing the immensely useful, but often poorly understood, 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 the course, they will learn how to make a free tool achieve the power of many much more costly commercial tools.

- Ed Skoudis, John Strand, and James Lyne

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

-Tom Reeves, Northrup Grumman

"SEC580 is an excellent deep-dive into Metasploit. This course is exactly what I needed to get my skills up!"

-Chris Schultz, Deloitte

SANS

www.sans.org/SEC580

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 such 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.

SANS

SEC580 Training Formats

(subject to change

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

Summit Events
www.sans.org/summit

Private Training
www.sans.org/onsite

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen 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, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing 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.

Course Day Descriptions

580.1 HANDS ON: Metasploit Kung Fu for Enterprise Pen Testing: Day 1

Day 1 of SANS Security 580: Metasploit Kung Fu for PenetrationTesters 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 framework with numerous exercises that make this class one of the most hands-on courses ever developed by SANS.

In SEC580.1, you will go from zero to exploit and beyond faster than you ever thought possible. For example, after this day of class, 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: A Guided Overview of Metasploit's Architecture and Components; A Deep Dive into the Msfconsole Interface, including Logging and Session Manipulation; Careful and Effective Exploitation; The Ultimate Payload: The Metasploit Meterpreter In Depth; Merciless Pivoting: Routing Through Exploited Systems; Metasploit Sniffing on Exploited Systems; Windows Process Token Manipulation for Fun and Profit; 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; Port and Vulnerability Scanning with Metasploit, Including Integration with Nmap, Nessus, and Qualys; Wielding Metasploit Databases for Analysis and Ownage; Integrating Db_autopwn Functionality in Safe and Effective Penetration Testing

580.2 HANDS ON: Metasploit Kung Fu for Enterprise Pen Testing: Day 2

In SANS Security 580.2, 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 by the bad guys. They 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.

We'll also cover how Metasploit can effectively integrate with tools like NeXpose, Nmap, and Nessus to manage large scan results to find exactly which system(s) you wish to exploit. We also cover how Metasploit can become a main component of your wireless penetration testing regimen and how Metasploit can be used to attack databases and web applications.

Topics: Metasploit Integration with Other Tools; Client-Side Exploitation; Automating Client-Side Attacks with Browser_autopwn; Using Metasploit to Model Malware Attacks via Msfpayload; Dodging Detection Like the Bad Guys with Msfencode; Ultra Stealthy Techniques for Bypassing Anti-Virus Tools; Making the Most of Windows Payloads; Effective Tips and Tricks for Launching Unix Payload Attacks; Adobe, Microsoft, and Java… Oh My… Attacking via File Format Exploits; Exploiting the Soft Underbelly of Most Organizations through the Social Engineering Toolkit; Evading Countermeasures to Mimic Sophisticated Attackers; Scripting Up the Meterpreter to Customize Your Own Attacks; Attacking Target Databases to Demonstrate Business Risk Effectively; Metasploit's Myriad of Wireless Features for Attacking Access Points and Clients; Metasploit and the Web: Integration and Astonishing Automation via Metasploit, MySQL, and More!