SEC573: Python for Penetration Testers

Your target has been well hardened. So far, your every attempt to compromise their network has failed. But you did find evidence of a vulnerability, a break in their defensive posture. Sadly, all of your tools have failed to successfully exploit it. Your employers demand results. What do you do when off-the-shelf tools fall short? You write your own tool.

The best penetration testers can customize existing open-source tools or develop their own tools. The ability to read, write, and customize software is what distinguishes the good penetration tester from the great penetration tester. This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools to put you on the path of becoming a great penetration tester. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it.

Unfortunately, many penetration testers do not have these skills today. The time and effort required to develop programming skills may seem overwhelming. But it is not beyond your reach. This course is designed to meet you at your current skill level, appealing to a wide variety of backgrounds ranging from people without a drop of coding experience all the way up to skilled Python developers looking to increase their expertise and map their capabilities to penetration testing. Because you can't become a world-class tool builder by merely listening to lectures, the course is chock full of hours of hands-on labs every day that will teach you the skills required to develop serious Python programs and how to apply those skills in penetration testing engagements. Join us and learn Python in-depth and fully weaponized!

The course begins with an introduction to SANS pyWars, a four-day Capture the Flag competition that runs parallel to the course material. It will challenge your existing programming skills and help you develop new skills at your own individualized pace. This allows experienced programmers to quickly progress to more advanced concepts while novice programmers spend time building a strong foundation. This individualized approach allows everyone to hone their current skills to make them the most lethal weapon they can be.

After introducing pyWars the course covers the essential skills required to get the most out of the Python language. The essential skills workshop labs will teach those who are new to software development the concepts and techniques required to develop their own tools. The workshop will also teach shortcuts that will make experienced developers even more deadly. Then we turn to applying those skills in today's real-world penetration testing scenarios. You will develop a port scanning, antivirus evading, client infecting backdoor for placement on target systems. You will develop a SQL injection tool to extract data from websites that fail with off-the-shelf tools. You will develop a multi-threaded password guessing tool and a packet assembling network reconnaissance tool. The course concludes with a one-day Capture the Flag event that will test your ability to apply your new tools and coding skills in a penetration testing challenge.

"I benefitted from not only the excellent course material of SEC573, but also the additional information and the very satisfactory percentage of hands-on time."

-Roswitha MacLean, Self

Who Should Attend

- Security professionals who want to learn how to develop Python applications
- Penetration testers who want to move from being a consumer of security tools to the creator of security tools
- Technologists who need custom tools to test their infrastructure and desire to create those tools themselves

You Will Be Able To

- Write a backdoor that uses exception handling, sockets, process execution, and encryption to provide you with your initial foothold in a target environment. The backdoor will include features such as a port scanner to find an open outbound port, the ability to evade antivirus software and network monitoring and the ability to embed payload from tools such as Metasploit.
- Write a SQL injection tool that uses standard Python libraries to interact with target websites. You will be able to use different SQL attack techniques for extracting data from a vulnerable target system.
- Develop a tool to launch password guessing attacks. While developing this tool you will also make your code run faster by using multi-threading. You will handle a modern authentication system by finding cookies and bypassing CAPTCHAs. You will know how to enhance your program with local application proxies and how to create and use target customized password files.
- Write a network reconnaissance tool that uses SCAPY, cStringsIO and PIL to reassemble TCP packet streams, extract data payloads such as images, display images, and extract Metadata such as GPS coordinates and link those images with GPS coordinates to Google maps.

You Will Receive

- A virtual machine with sample code and working examples
- A copy of "Violent Python"

573.1 HANDS ON: Essentials Workshop – PART 1

The course begins with a brief introduction to Python and the pyWars Capture-the-flag game. We set the stage for students to learn at their own pace in the 100% hands-on pyWars lab environment. As more advanced students take on Python-based Capture-the-Flag challenges, students who are new to programming will start from the very beginning with Python essentials.

Topics: Variables; Math Operators; Strings; Functions; Modules; Compound Statements; Introspection

573.2 HANDS ON: Essentials Workshop – PART 2

You will never learn to program by staring at Powerpoint slides. The second day continues the hands-on lab-centric approach established on day one. This section continues covering the essentials of the language, including data structures and programming concepts. With the essentials of the language under your belt, the pyWars challenges and the in-class labs start to cover more complex subjects.

Topics: Lists; Loops; Tuples; Dictionaries; The Python Debugger; System Arguments & OptParser; File Operations

573.3 HANDS ON: Pen Testing Applications – PART 1

Day 3 shifts gears. With a core set of skills established, we can begin developing penetration testing tools that you can use in your next engagement. You will develop a backdoor command shell that evades antivirus software and provides you with that critical initial foothold in the target environment. You will then develop a customizable SQL injection tool that you can use to extract all the data from a vulnerable database when off-the-shelf tools fail. Finally, we will discuss how to speed up your code with multi-threading.

Topics: Network Sockets; Exception Handling; Process Execution; Metasploit Integration; Antivirus; IDS Evasion; Introduction to SQL; Blind SQL Injection Techniques; Developing Web Clients; Multi-Threaded Applications; Mutexes and Semaphores; Message Queues; Thread Communications

573.4 HANDS ON: Pen Testing Applications – PART 2

In this section you will develop more tools that will make you a more lethal penetration tester. First, you will develop a custom web-based password guesser. This will teach you how to get the most out of Python's web-based libraries and interact with websites using cookies, proxies, and other features to p0wn the most difficult web-based authentication systems. Then, you'll write a network reconnaissance tool that will demonstrate the power of Python's third-party libraries.

Topics: HTTP Form Password Guessing; Advanced Web Client Techniques; HTTP Proxies/HTTP Cookies; Session Hijacking; TCP Packet Reassembly With Scapy; Extracting Images from TCP Streams; Analyzing Image Metadata

573.5 HANDS ON: Capture the Flag

In this final section you will be placed on a team with other students. Working as a team, you will apply skills you have mastered in a series of penetration testing challenges. Participants will exercise the skills and code they have developed over the previous four days as they exploit vulnerable systems, break encryption cyphers, and remotely execute code on target systems. Test your skills! Prove your might!

"Scripting is a necessity for any serious pen tester. SEC573 provides useful hands-on knowledge."

-Jeffrey Moy, Atlas Air

SEC573 COIN

SEC573 Training Formats

(subject to change)

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

OnSite
sans.org/onsite

Simulcast
sans.org/simulcast

SelStudy
sans.org/selfstudy

"SEC573 was excellent – it will be useful right away."

-Jerry Shenk Windstream