SEC573: Automating Information Security with Python

GPYC Python Coder giac.org/gpyc

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Modify existing open-source tools to customize them to meet the needs of your organization.
- Manipulate log file formats to make them compatible with various log collectors.
- Write new tools to analyze log files and network packets to identify attackers in your environment.
- Develop tools that extract otherwise inaccessible forensic artifacts from computer systems of all types.
- Automate the collection of intelligence information to augment your security from online resources.
- Automate the extraction of signs of compromise and other forensics data from the Windows Registry and other databases.
- 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, techniques for evading antivirus software and network monitoring, and the ability to embed a payload from tools such as Metasploit.

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

All security professionals, including penetration testers, forensic analysts, network defenders, security administrators, and incident responders, have one experience in common: CHANGE. Tools, technologies, and threats change constantly, but Python is a simple, user-friendly language that can help you keep pace with change, allowing you to write custom tools and automate tasks to effectively manage and respond to your unique threats.

Whether you are new to coding or have been coding for years, SEC573: Automating Information Security with Python will have you creating programs that make your job easier and your work more efficient. This self-paced course starts from the very beginning, assuming you have no prior experience with or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the course.

Technology, threats, and tools are constantly evolving. If we don't evolve with them, we'll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require. Maybe your chosen Operating System has a new feature that creates interesting forensic artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensic artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold...or you can write a tool yourself.

Or perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn't be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization. The answer is simple if you have the skills: Write tools to automate various aspects of your defenses.

Or, as a penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when "off-the-shelf" tools and exploits fall short? If you're good, you write your own tool or modify existing capabilities to make them perform as you need them to.

SEC573 is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you to better automate the daily routine of today's information security professional and to achieve more value in less time. 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. Learn Python in-depth with us to become fully weaponized.

"SEC573 is excellent. I went from having almost no Python coding ability to being able to write functional and useful programs."

— Caleb Jaren, **Microsoft**

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: Essentials Workshop with pyWars

The course begins with a brief introduction to Python and the pyWars Capture-the-Flag challenge. We set the stage for students to learn at their own pace in the pyWars lab environment, which is 100 percent hands-on. 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: Syntax; Variables; Math Operators; Strings; Functions; Modules; Control Statements; Introspection

SECTION 2: Essentials Workshop with MORE pyWars

You will never learn to program by staring at PowerPoint slides. This section continues the hands-on, lab-centric approach established at the beginning of the course. It covers data structures and more detailed programming concepts. Next, we focus on invaluable tips and tricks to make you a better Python programmer and to show you how to debug your code.

TOPICS: Lists; Loops; Tuples; Dictionaries; The Python Debugger; Coding Tips; Tricks and Shortcuts; System Arguments; ArgParser Module

SECTION 3: Defensive Python

In this section, we take on the role of a network defender with more logs to examine than there is time in the day. Attackers have penetrated the network and you will have to analyze the logs and packet captures to find them. We will discuss how to analyze network logs and packets to discover where the attackers are coming from and what they are doing. We will build scripts to empower continuous monitoring and disrupt the attackers before they exfiltrate your data. Forensicators and offensive security professionals won't be left out because reading and writing files and parsing data are also essential skills they will apply to their craft.

TOPICS: File Operations; Python Sets; Regular Expressions; Log Parsing; Data Analysis Tools and Techniques; Long Tail/Short Tail Analysis; Geolocation Acquisition; Blacklists and Whitelists; Packet Analysis; Packet Reassembly; Payload Extraction

SECTION 4: Forensics Python

In our forensics-themed section, we will assume the role of a forensic analyst who has to carve evidence from artifacts when no tool exists to do so. Even if you don't do forensics, you will find that the skills covered in this section are foundational to every security role. We will discuss the process required to carve binary images, find appropriate data of interest in them, and extract those data. Once you have the artifact isolated, there is more analysis to be done. You will learn how to extract metadata from image files. Then, we will discuss techniques for finding artifacts in other locations, such as SQL databases, and interacting with web pages.

TOPICS: Acquiring Images from Disk; Memory and the Network; File Carving; The STRUCT Module; Raw Network Sockets and Protocols; Image Forensics and PIL; SQL Queries; HTTP Communications with Python Built in Libraries; Web Communications with the Requests Module

SECTION 5: Offensive Python

During our offensive-themed section, we play the role of penetration testers whose normal tricks have failed. Their attempts to establish a foothold have been stopped by modern defenses. To bypass these defenses, you will build an agent to give you access to a remote system. Similar agents can be used for Incident response or systems administration, but our focus will be on offensive operations.

TOPICS: Network Socket Operations; Exception Handling; Process Execution; Blocking and Non-blocking Sockets; Using the Select Module for Asynchronous Operations; The Select Module; Python Objects; Argument Packing and Unpacking

SECTION 6: Capture-the-Flag Challenge

In this final section you will be placed on a team with other students to apply the skills you have mastered in a series of programming challenges. Participants will exercise the new skills and the code they have developed throughout the course in a series of challenges. You will solve programming challenges, exploit vulnerable systems, analyze packets, parse logs, and automate code execution on remote systems. Test your skills! Prove your might!

"Excellent class for learning how to construct automated and advanced discovery analytics for information systems."

— Mary Gutierrez, **Booz Allen Hamilton**

Who Should Attend

- Security professionals who benefit from automating routine tasks so they can focus on what's most important
- Forensic analysts who can no longer wait on someone else to develop a commercial tool to analyze artifacts
- Network defenders who sift through mountains of logs and packets to find evil-doers in their networks
- Penetration testers who are ready to advance from script kiddie to professional offensive computer operations operator
- Security professionals who want to evolve from security tool consumer to security solution provider

You Will Receive

- A USB containing a virtual machine filled with sample code and working examples
- A copy of The Python Pocket Reference published by O'Reilly Press
- MP3 audio files of the complete course lecture