+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 08/19/2026

Sign Up

Secator Training

1 day (7 hours)

Overview

Secator is a French open-source framework and CLI developed by Freelabz to automate reconnaissance and penetration testing tools. Thanks to its YAML workflows, unified options, and structured results, Secator accelerates the execution of reproducible security assessments.

Our Secator training course will enable you to master the operational use of this tool to orchestrate reconnaissance, mapping, and vulnerability identification phases within explicitly authorized scopes.

You will learn how to install and configure Secator, execute individual tasks, workflows, and scans, and then leverage built-in tools such as subfinder, httpx, naabu, nuclei, and katana.

By the end of the training, you will be able to define targets, configure scan options, control the rate of requests, and interpret standardized output to prioritize your investigations.

This training also covers creating YAML workflows, chaining tasks, filtering results, and best practices for traceability to produce more reliable analyses tailored to a professional context.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Install and configure Secator in a dedicated test environment

- Run tasks, workflows, and scans on authorized targets
- Configure detection, speed, and filtering options
- Interpret structured results and prioritize items for investigation
- Create a simple YAML workflow to automate a detection pipeline

Target Audience

- Penetration tester
- Cybersecurity consultant
- Security analyst
- Offensive security engineer
- Bug bounty hunter

Prerequisites

- Knowledge of the phases of a penetration test and the authorization framework
- Proficiency with common Linux commands
- Basic understanding of network, web, and DNS reconnaissance
- Basic knowledge of JSON and YAML formats

Technical Prerequisites

- Computer equipped with a recent version of Kali Linux or a compatible Linux distribution, either natively installed or in a virtual machine
- 64-bit processor, at least 8 GB of RAM, and 20 GB of available disk space
- Python 3 and Git installed, with the necessary permissions to install dependencies
- Terminal, text editor, or YAML-compatible IDE
- Stable internet connection with no filtering that blocks downloads and access to authorized lab targets

Our Secator Training Program

[Day 1 - Morning]

Getting Started and Automating Recognition

- Secator’s role in a penetration testing process, legal framework, authorized scope, and operational security rules
- CLI architecture, task concepts, workflows, scans, and unified result formats
- Installation, environment verification, and introduction to essential Secator commands
- Executing reconnaissance tasks with subfinder, dnsx, httpx, and naabu
- Configuring targets, global options, throughput limits, and options specific to integrated tools

- Hands-on workshop: Perform a reconnaissance chain within an authorized lab environment; identify subdomains, exposed services, and accessible endpoints

[Day 1 - Afternoon]

YAML workflows and analysis of results

- Reading and analyzing structured output, result types, exports, and criteria for qualifying discoveries
- Using existing workflows for crawling, content search, and identifying vulnerabilities with Katana, FFUF, and Nuclei
- Structure of a YAML file, defining tasks, inputs, options, tags, and filtering results
- Chaining processes, reusing results as targets, and an introduction to parallel executions
- Best practices for load control, manual validation, logging, and reporting results
- Hands-on workshop: running the workflow, filtering results, and producing a summary of prioritized findings

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in a new advanced IT technology or to acquire specific business knowledge or modern methods.

Assessment at the Start of Training

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth operation of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired

of the skills.

Certification

A certificate will be issued to each participant who has completed the entire training program.