Updated on 02/04/2026

Register

Villager Framework Training

3 days (21 hours)

Overview

Villager is the first AI-native pentesting framework, designed to replace traditional post-exploitation tools such as Cobalt Strike. This approach relies on autonomous agents and the MCP protocol to automate the entire attack chain.

Our Villager training will enable you to master this new generation of security audit tools. You will learn how to orchestrate agents capable of generating dynamic exploits, adapting to defenses in real time, and automating complex tasks via ephemeral containers.

By the end of the training, you will be able to deploy a Villager infrastructure, manage a fleet of AI agents for security audits, and industrialize your Red Team workflows for professional projects.

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

Objectives

- Understand the architecture of autonomous AI agents applied to pentesting.
- Install and configure the Villager framework and its agent infrastructure.
- Master natural language control and the MCP protocol.
- Automate the reconnaissance, exploitation, and lateral movement phases.
- Assess the capabilities and limitations of AI in the face of defense solutions.

Target audience

- Penetration testers and cybersecurity consultants

- Red Team engineers
- SOC managers and security analysts

Prerequisites

- Solid knowledge of pentesting (networks, systems)
- Familiarity with the Linux command line
- Basic knowledge of LLMs and APIs

Software prerequisites

- Minimum 16 GB of RAM
- Linux (preferably Ubuntu) or Windows with WSL2
- Docker and Docker-compose installed
- API access (OpenAI, Anthropic, or DeepSeek) for exercises

Villager Training: Pentesting & AI Agents

[Day 1 - Morning]

Introduction to Villager and Offensive Agents

- Overview of AI pentesting: from traditional scripting to autonomous agents
- Presentation of Villager: philosophy, architecture, and comparison with Cobalt Strike
- Understanding the role of LLMs in offensive decision-making
- Introduction to the Model Context Protocol (MCP)
- Hands-on workshop: Installing Villager and configuring LLM API access.

[Day 1 - Afternoon] Orchestration

and First Scenario

- Control interface: controlling an agent using natural language
- Management of ephemeral containers for tool execution (Nmap, Metasploit)
- Breakdown of objectives (Task Planning) by AI
- Log tracking and agent action monitoring
- Hands-on workshop: Launching an automated reconnaissance mission on a target perimeter.

[Day 2 - Morning]

Dynamic Exploitation and Adaptation

- Generation of exploits "on-the-fly" by AI
- Bypassing first lines of defense (firewalls, filtering)
- Analysis of error returns by the agent and autonomous correction of the attack code
- Use of Villager plugins and extensions
- Hands-on workshop: Scenario for exploiting a known vulnerability with agent adaptation.

[Day 2 - Afternoon]

Post-Exploitation and Lateral Movement

- Discreet persistence via AI agents
- Lateral movement: pivoting and automated domain enumeration
- Selective and intelligent data exfiltration
- Cleaning up traces and AI-generated activity reports
- Hands-on workshop: Compromising an Active Directory network with Villager.

[Day 3 - Morning]

Security, Ethics, and Advanced Evasion

- Evasion techniques against AI-powered EDR/XDR
- Dynamic payload obfuscation
- Current limitations: hallucinations, API costs, and latency
- Legal and ethical framework for the use of offensive AI
- Hands-on workshop: Testing Villager detection against a modern defense solution.

[Day 3 - Afternoon] Industrialization

and Practical Cases

- Integrating Villager into a DevSecOps Pipeline
- Customizing system prompts for specific missions
- Real-world case studies (Cyberspike/Straiker reports)
- Red Team workflow and supervision
- Hands-on workshop: Final project - Simulation of a complete attack under supervised autonomy.

Target companies

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Placement at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon final registration, learners receive a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives 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 be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and discussion sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.