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

Updated on 09/16/2026

Sign Up

Ghidra Training

3 days (21 hours)

Overview

Ghidra is a reverse engineering platform designed to analyze binaries, understand their logic, and accelerate the investigation of malicious code. Through disassembly, decompilation, graphs, and scripts, it helps analysts produce reliable diagnoses of complex executables.

Our Ghidra training course will enable you to master essential static analysis methods for examining suspicious executables in a controlled environment. You'll learn how to import binaries, configure automated analyses, and navigate efficiently between code, memory, and reference views.

You will study the principles of reading assembly code, interpreting the pseudocode generated by the decompiler, and progressively enriching functions with appropriate names, comments, structures, and signatures.

The training also covers techniques for identifying behaviors relevant to malware analysis, such as persistence mechanisms, system calls, significant strings, network communications, and encryption functions.

By the end of the course, you will be able to conduct a structured analysis with Ghidra, document your findings, compare binary versions, and automate certain repetitive tasks using Python scripts.

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

Objectives

- Get started with the Ghidra environment to analyze compiled binaries
- Interpret disassembly, pseudocode, and control flow graphs
- Reconstruct a program’s logic using functions, types, structures, and references
- Identify characteristic behaviors during a static analysis of malware
- Document the results and automate repetitive analyses using scripts

Target Audience

- Cybersecurity Analyst
- SOC Analyst
- Malware analyst
- Incident response engineer
- Offensive Security Consultant

Prerequisites

- Knowledge of cybersecurity fundamentals
- Experience with the command line in Windows or Linux
- Basic programming skills in C or Python
- Basic understanding of processor architecture and x86 or x64 assembly language

Technical Prerequisites

- Computer running Windows 10 or 11, Linux, or macOS (64-bit compatible)
- Installation of a recent version of Ghidra with JDK 25 (64-bit)
- Computer with at least 8 GB of RAM and 2 GB of available disk space
- Isolated virtual machine for working with the provided samples
- Stable internet connection to set up the environment and install dependencies

Our Ghidra Training Course Schedule

[Day 1 - Morning]

Fundamentals of Reverse Engineering with Ghidra

- The role of Ghidra in reverse engineering and static malware analysis
- Overview of executable formats, processor architectures, and information available in a binary
- Installation, workspace configuration, and organization of Ghidra projects
- Importing an executable, selecting the processor language, and automatic analysis settings
- Exploring the CodeBrowser, Listing, Symbol Tree, Program Trees, and Memory Map views

[Day 1 - Afternoon]

Reading and interpreting disassembled code

- Principles of reading x86 and x64 assembly code, registers, the stack, and calling conventions
- Differences between code, data, strings, imports, exports, and resources
- Navigating via cross-references, searching for strings, and identifying important functions
- Using bookmarks, labels, comments, and groupings to map out the analysis
- Hands-on workshop: Import a training executable, locate its entry point, imports, and significant strings.

[Day 2 - Morning]

Decompiling and reconstructing application logic

- How the decompiler works and its limitations; the relationship between pseudocode and assembly language
- Identifying parameters, local variables, return values, and function calls
- Renaming symbols and functions to create a comprehensible naming convention
- Applying types, structures, enumerations, and signatures to improve the pseudocode
- Analysis of control flow graphs, branches, loops, and execution paths

[Day 2 - Afternoon]

Analyzing suspicious behavior

- Static triage method to prioritize relevant areas of a sample
- Identifying persistence mechanisms, process execution, and file manipulation
- Identifying indicators related to network communications, configuration, and encryption
- Analysis of simple obfuscation techniques, encoded strings, and unreachable code
- Hands-on workshop: Reconstruct the behavior of a training binary and produce an initial analysis report.

[Day 3 - Morning]

Deepening and validating investigations

- Manually correcting the disassembly and redefining code or data sections
- Creating and reusing data types to clarify complex functions
- Using call trees, cross-references, and similar functions
- Comparing programs and tracking changes between two versions of a binary
- Best practices for traceability, assumptions, confidence levels, and technical reporting

[Day 3 - Afternoon]

Automating Analyses with Scripts

- Introduction to the script manager and automation capabilities in Ghidra
- API fundamentals, program flow, functions, symbols, and references
- Creating Python scripts to extract information and enhance an analysis
- Introduction to headless mode for processing multiple binaries in a reproducible manner
- Hands-on workshop: Create a Python script to inventory functions and strings, then prepare a summary report on a sample.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific industry 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 in 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 running 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 the skills.

Certification

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

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg