Everyday Ghidra: Practical Windows Reverse Engineering

2024 Course Syllabus and Overview

Updated: May 23, 2024

Clearseclabs LLC
1942 Broadway St. STE 314C
Boulder, CO 80302, US

https://www.clearseclabs.com/

contact@clearseclabs.com

Overview

This course provides a comprehensive guide to using Ghidra, covering fundamental operations to advanced techniques, with hands-on exercises on real-world Windows applications. It's designed for those with foundational Windows and security knowledge, aiming to equip them with practical "everyday" reverse engineering skills using Ghidra.

Abstract

In this course, you will learn how to use Ghidra effectively to reverse engineer Windows binaries. You will start with the basics of Ghidra, such as creating projects, importing and analyzing binaries, and using Ghidra's native tools. You will then learn how to customize Ghidra to suit your needs, such as building custom data types and configuring optimal analysis. From there, you will complete progressively challenging labs that will teach you to apply static and dynamic analysis techniques to dive deep into Windows application behavior using Ghidra's Windows-specific features and scripts.

The course will also provide you with a series of "everyday" reversing examples, covering several aspects of Windows reverse engineering. Your journey will involve reversing Windows malware, debugging a Windows RPC server, and even learning how to root cause a recent Windows CVE. You will also learn how to use other Windows specific RE tools, such as WinDbg, RPCView, and System Informer to complement Ghidra's functionality.

By the end of this course, you will have gained practical skills and experience in reverse engineering Windows binaries using Ghidra. You will be able to apply these skills to your own projects, research, or career in cybersecurity.

Intended Audience

- Cybersecurity professionals seeking to advance their skills in reverse engineering and malware analysis on the Windows platform.
- Software developers interested in deepening their understanding of Windows internals
- Vulnerability Researchers hoping to gain practical experience with Ghidra for uncovering and understanding vulnerabilities in Windows binaries

Student Requirements

This course is rated intermediate, but suitable for beginners with heart. It is assumed that students have a basic knowledge of Windows, security, and assembly language. No prior experience with Ghidra is required.

Suggested Prerequisites

- **Basic Knowledge of Windows**: Familiarity with the Windows operating system and its core functionalities.
- **Understanding of Security Principle**s: A foundational grasp of cybersecurity concepts and practices.
- **Assembly Language Basics**: An introductory understanding of assembly language or familiarity with programming in C.

What Students Will Be Provided With

- Course slides / Training materials
- Recording of classes (if virtual)
- Virtual machines with all the labs
- Resources for further learning
- Access to course CTF server during and beyond the course
- Access to instructor(s) via Discord during the course and beyond

Laptop Requirements

- 64-bit i7+ Laptop with 16GB+ RAM
- 60 GB disk space
- Ability to run Intel based VM similar to https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/
- Virtual Box or VMware.

Key Learning Objectives

- **Ghidra Proficiency**: Gain comprehensive skills in using Ghidra for static and dynamic analysis of Windows binaries.
- **Tool Mastery**: Master Ghidra's primary tools—Code Browser, Debugger, and Version Tracking—to tackle diverse reverse engineering tasks.
- **Enhanced Analysis Techniques**: Learn to create custom data types and leverage Ghidra's PDB support to deepen analysis capabilities.
- **Malware Behavior Identification**: Develop the ability to reverse engineer and analyze Windows malware, identifying key behaviors like persistence and network communication.
- **Vulnerability Assessment**: Use Ghidra's patch diffing feature to compare binary versions and pinpoint changes addressing modern vulnerabilities.
- **Dynamic Debugging**: Acquire the skills to dynamically debug Windows applications, enhancing problem-solving techniques in live environments
- **Ghidra Scripting:** Learn how to extend Ghidra's core library to automate several aspects of reverse engineering.

Practical Exercises:

Reverse Engineering Windows Malware

Learn to reverse engineer a Windows malware sample and identify its malicious behavior, such as persistence, network communication, and obfuscation.

Dynamically Debugging a Windows RPC Server

- Gain insight into Windows RPC and learn how to dynamically inspect a Windows RPC server with Ghidra's Debugger.
- Examine PetitPotam NTLM authentication relay security issues and more.

Patch Diffing and Root Cause Analysis of a Windows CVE

- Learn how to use Ghidra's Patch Diffing to compare two versions of a Windows binary and identify the changes made to fix a vulnerability. You will learn how to root cause the vulnerability and understand its exploitation.

Course Outline

Part 1

Introduction to Reverse Engineering With Ghidra

- Getting Started with Ghidra
- Import, Analyze, Repeat
- Windows Security Concepts
- Managed vs Native Binaries
- Ghidorah: Taming the 3-headed dragon
    - Code Browser
    - Debugger
    - Version Tracking
- Ghidra Scripting

Part 2

Reverse Engineering Windows Binaries - Static

- A Practical RE Workflow
- Setting Reverse Engineering Goals
- Binary Acquisition
- Analysis Improvements
- Building Custom Ghidra Data Types
- Reversing Windows Malware

Part 3

Reverse Engineering Windows Binaries - Dynamic

- Ghidra Debugger Overview
- Debugging an Application
- Pretending All Binaries Come with Source
- Debugging a Windows RPC Service
- Debugging a RPC call
- Reversing Petitpotam (NTLM Authentication Bypass) Case Study
- RPCview, NtObjectManager,System Informer, Sysinternals

Part 4

Patch Diffing and Root Cause Analysis of Windows CVE

- Patch Diffing in Ghidra
- Finding a CVE
- Patch Diffing Windows Binaries
- Hunting for the vulnerability
- Finding the root cause
- Building a trigger POC

Course Pricing

4-day*

Type	Venue	Minimum	Cost (USD)	Notes
Public	Onsite	10	Varies	Conference Negotiated
Public	Virtual	5	4200	
Private	Onsite	5	Contact	Limited destinations. Contact for more info.
Private	Virtual	5	4200	Contact for details. Restrictions apply.

* Other course durations are possible. Please email to discuss pricing and content for a 2,3, or 5 day variant of the course.

Group Discounts:

- For groups of 10 or more participants, we provide special group rates. For more information, contact us at contact@clearseclabs.com.

Private Course Requests:

- Interested in a private course session? EmIL contact@clearseclabs.com with your inquiry.
- A minimum of 5 students is required to organize a private course.

In-Person Training Considerations:

- **Venue and Catering**: Additional charges apply if the provision of a venue and catering services is necessary.
- **Travel and Accommodation**: For in-person training conducted outside of Colorado, reasonable instructor travel and accommodation expenses will be incurred.

Extended Training Option:

- An additional day of training can be included to provide a more comprehensive learning experience as needed.

Conference-Associated Training:

- Please note that pricing may vary when training sessions are hosted in conjunction with external conferences or partners.

For any further questions or to begin the enrollment process, please contact us directly at contact@clearseclabs.com.