Patch Diffing in the Dark

Binary Diffing for Vulnerability Researchers and Reverse Engineers

2024 Course Syllabus and Overview

Updated: May 28, 2024

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

https://www.clearseclabs.com/

contact@clearseclabs.com

Overview

The goal of this course is to teach participants how to use patch diffing techniques to analyze real-world vulnerabilities in Windows and Android. Students will use open-source tools like the Ghidra SRE framework to reverse engineer the latest CVEs and discover that you already have the information and tools needed to get started. This course will help students develop the confidence and competence to reverse engineer and discover complex vulnerabilities.

Abstract

Every day, a new CVE (Common Vulnerabilities and Exposure) is published or a new blog post comes out detailing the latest and greatest vulnerability. Often, we know about a vulnerability but feel like we don't have the skills or time to understand its root cause. What if you could change that? What if you could learn a skill that would lead you step by step towards understanding modern vulnerabilities? If you feel like you are always "in the dark" about the latest CVE and want to take a step towards the light (understanding), this course is for you.

Binary patch diffing is an essential skill for reverse engineering, vulnerability research, and malware analysis. The process helps a researcher identify the security-relevant code changes of a patched binary and helps highlight the underlying security issues. The process is not magic, and with a little guidance, anyone can learn the basics and improve with practice.

This fast-paced training will teach you how to reverse engineer the latest CVEs. We will start with a simple CVE description, progress towards identifying a vulnerability, and eventually gain a complete understanding of the underlying vulnerability and identify its root cause. You will analyze (7+) real-world CVEs, dive into the patch diffing process, and learn a step-by-step approach to modern patch diffing using open-source tools. The short topical lessons and hands-on exercises will have you patch diffing recent CVEs and their corresponding binaries across both Android and Windows platforms. You will learn about best practices, how to avoid patch diffing pitfalls, and get useful scripts to enhance your analysis workflow.

The best part about the training is that there is no secret ingredient. Using free tools (Ghidra SRE framework, BinDiff, and more) and leveraging readily available CVE information, you will learn how to discover and analyze complex vulnerabilities. The course, via hands-on exercises and lectures that cover real-world CVEs challenges, provides students with practical reverse engineering exercises to help them learn and practice the concepts and techniques. Participants will discover that you can leverage CVEs as a guide for reverse engineering and vulnerability research.

This course teaches the skill of patch diffing to enable students to progress from knowing about a vulnerability to actually understanding its root cause.

Intended Audience

- Cybersecurity professionals seeking to advance their skills in reverse engineering complex vulnerabilities to learn how to mitigate risk and evaluate recent CVEs.
- Vulnerability Researchers hoping to learn a practical technique for vulnerability discovery. This course will challenge the researcher to go one step past learning (what others understand) and arrive in a place of actual research (discovering something new).
- Reverse engineers that want to learn how operating system securities are compromised by vulnerable application, services, and low-level interactions of modern operating systems.

Student Requirements

This course is rated intermediate, but suitable for beginners with heart.

Suggested Prerequisites

- Basic Knowledge of Vulnerabilities or CVEs: Understand how the Common Vulnerabilities and Exposures (CVE) system identifies unique vulnerabilities and understand the concept of vulnerability classes.
- Understanding of Security Principles: A foundational grasp of cybersecurity concepts and practices.
- Assembly Language Basics: An introductory understanding of assembly language or familiarity with programming in C.

No prior experience with Ghidra is required.

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

- **CVE Analysis**: Learn how to analyze Common Vulnerabilities and Exposures (CVEs) to understand the impact and exploitability of vulnerabilities.
- **Patch Diffing**: Learn the fundamentals of patch diffing, including what it is and how it can be used in vulnerability research.
- **Binary Analysis**: Gain skills in analyzing binary files in order to understand their structure and behavior.
- **Identifying Vulnerabilities**: Develop the ability to identify potential vulnerabilities in software through comparative analysis.
- **Reverse Engineering Techniques**: Acquire new techniques for reverse engineering binaries to discover how they work by leveraging static and dynamic analysis.
- **Exploit Development**: Understand the principles of developing exploits based on the vulnerabilities found through patch diffing.
- **SRE Tool Utilization**: Become proficient in using various open-source tools and software that aid in the process of patch diffing and vulnerability discovery.

Practical Exercises:

Patch Diffing and Root Cause Analysis of over 7 realworld CVEs

- 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.

Combined Static and Dynamic Analysis

- Learn to use static analysis to patch diff and find vulnerable areas of code
- Leverage dynamic analysis using debuggers and 3rd party tools to dig deep into a CVE for root cause verification.
- Write Frida scripts to investigate vulnerable functions on mobile devices

Course Outline

Part 1

Learn the value of using readily available security information (CVEs, Github POCs, and blog posts) to dive deep into reverse engineering the latest CVEs.

- Introduction
    - Binary Diffing Use Cases
    - Seeking Binary Truth
    - Overview of the CVE vulnerabilities and their impact
    - Introduce the tools and data sets (Ghidra, WinDbg, Frida, CVEs)
- Patch Analysis
    - Finding the CVE binaries
    - Patch Diffing Workflow
    - Reverse Engineering
    - Interpreting Diff Results
    - Patching Holes in Ghidra Version Tracking
    - Root Cause Exercises
    - BinDiff Alternative
- Vulnerability Analysis
    - Discovering the vulnerable code path
    - Identifying the vulnerability
    - Ghidra scripting Version Tracking analysis
    - Research/Download Grab Bag CVEs

Part 2

Learn how to go from a simple CVE description to finding the underlying root cause of the vulnerability. This day will provide the background on how to research CVEs, find the binaries of interest, and reverse engineer the vulnerabilities using both static and dynamic analysis.

- Windows: Zero to Hero - CVE-2023-28302
    - Identify vulnerable application
    - Research methods to reach vulnerable code paths
    - Static and Dynamic Analysis

    - Root Cause the vulnerability
    - Develop exploit trigger POC
- Android: Zero to Average - WhatsApp CVE-2022-36934
    - Android APK Reverse Engineering
    - Identify vulnerable application
    - Extracting native files from WhatsApp APKs
    - Patch Diff Several WhatsApp CVEs
    - Frida instrumentation for Dynamic Analysis

Part 3

Learn how to use a brand new Ghidra feature called Binary Similarity (BSim). BSim allows a researcher to build and explore a large set of binaries for comparison. Experience live patch diffing, where together as a class we walk through several recent CVE examples in real time to discover what we can learn.

- The Power of BSim
    - Experience Ghidra's latest feature Binary Similarity toolset
    - Learn how to build training data sets for binary exploration
    - Leverage BSim to broaden your patch diffing across binary data sets
- Grab Bag CVEs
    - This exercise will provide an instructor led walk through of as many live patch diffs of preselected CVEs and/or student suggested CVEs
    - This experience sometimes reaches beyond Windows or Android operating systems. Experience will be unique for each class.

Part 4

Last, we will conclude with a final project. The final project is designed to cement the concepts learned throughout the course and prepares a researcher for patch diffing outside of class. It will consist of several patch diffing challenges allowing you to flex the skills developed during the course.

- Final Project
    - Practical application of skills learned in the course
    - Challenge will be validated with live course CTF server

Course Pricing

4-day*

Type	Venue	Minimum	Cost (USD)	Notes
Public	Onsite	10	Varies	Conference Negotiated
Public	Virtual	5	4000	
Private	Onsite	5	4500	Limited destinations. Contact for more info.
Private	Virtual	5	4000	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 by email or the booking form on the web.

Private Course Requests:

- Interested in a private course session? Please reach out to us at 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.