IMMERSIVELABS

NEW SERIES

INTRODUCTION TO STATIC CODE ANALYSIS FOR REVERSE ENGINEERING

Reverse engineering helps you understand how something works, and it's usable in the context of malware analysis and binary exploitation.

These three introductory series will help you understand how to approach malware from an in-depth perspective, and help you analyse the make-up of programs in order to exploit them.

COMPUTER ARCHITECTURE SERIES

This skill series takes you through the basics of how modern day computers work. You'll gain an understanding of different computer architectures, hardware, software, and the operating systems that everyone interacts with daily.

Labs in the series:

- Introduction to Computer Memory and Architecture
- Introduction to 32-Bit Architectures
- Introduction to 64-Bit Architectures
- An Introduction to Linux Internals
- Introduction to Windows Internals
- The Inside of a PE File
- The Inside of an ELF File
- What Is the Heap?
- What Is the Stack?
- Introduction to ELF Reverse Engineering
- ELF Execution Structure

ASSEMBLY LANGUAGE SERIES

Assembly language is an abstraction of machine code, and is notoriously complex to work with. This series will teach you how to write assembly language for different operating systems, as well as the nuances involved for both 32-bit and 64-bit architectures.

Labs in the series:

- 32-Bit Linux Assembly: Ep.1 – Structure and Registers
- 32-Bit Linux Assembly: Ep.2 – New Sections and File Manipulation
- 32-Bit Windows Assembly: Ep.1 – Windows API and the Stack
- 32-Bit Windows Assembly: Ep.2 – Windows APIs and Structs
- 64-Bit Linux Assembly: Ep.1 – Structure and Registers
- 64-Bit Linux Assembly: Ep.2 – New Sections and File Manipulation
- 64-Bit Windows Assembly: Ep.1 – Windows APIs and Registers
- 64-Bit Windows Assembly: Ep.2 – Structs And The Stack

Why are these series important?

Malware and exploits are big business – they're exactly what companies must defend against. The series will introduce you to these practices and provide fundamental knowledge around them.

Who are they for?

- Incident Responders
- Threat Hunters
- Defence Analysts
- Exploit Analysts

INTRODUCTION TO REVERSE ENGINEERING SERIES

Reverse engineering is one of the hardest but ultimately rewarding skills in cyber security. By completing this series of labs, you will gain hands-on reverse engineering experience, learn how the process works and understand how to begin reverse engineering an artefact.

Labs in the series:

- Ghidra: An Introduction
- 32-Bit Linux Reversing: Ep.1
- 32-Bit Linux Reversing: Ep.2
- 64-Bit Linux Reversing: Ep.1
- 64-Bit Linux Reversing: Ep.2
- 32-Bit Windows Reversing: Ep.1
- 32-Bit Windows Reversing: Ep.2
- 64-Bit Windows Reversing: Ep.1
- 64-Bit Windows Reversing: Ep.2
- PEDA
- Objdump
- Apktool

Immersive Labs is the world's first human cyber readiness platform.

Our technology delivers challenge-based cybersecurity content developed by experts and powered by the latest threat intelligence. Our unique approach enables businesses to battle-test and evidence their workforce's preparedness to face emerging cyber threats.