

Malware in C: Keylogger & Registry Persistence

Learn to build C-based malware that hides itself, executes shell commands, persists via the Windows registry, and logs keystrokes.

COURSE OVERVIEW

This course covers writing malware in C, beginning with hiding a program and defining its connection points. It then builds a shell function to execute commands and switch directories from within the program. It proceeds to creating persistence by nesting the program in the Windows registry, then adds a keylogger to the malware, and applies the techniques against Windows 10.

WHO THIS COURSE IS FOR

Security Researchers

Penetration Testers

Malware Analysts

C Developers

Ethical Hackers

8 Modules

01

Training Overview

02

Introduction and Welcome to Hacking With C!

03

Hiding Our Program and Defining Connection Points

04

Building Shell Function and Executing Commands

05

Switching Directories Inside of a Program

06

Creating Persistence and Nesting Our Program in Windows Registry

07

Adding Keylogger to Our Malware

08

Hacking Windows 10

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com