Linux - exploiting applications and operating system. Low level attacks. (code: LX-Exploit)

Ask for details
Phone +44 203 608 6289
info@alx.training

Overview

This course covers low level attacks against x86 (32 and 64 bit) architecture. Agenda includes bypassing of strengthening mechanisms. Participants of this course are required to have participated in **Linux – application and kernel debugging** course or have comparable knowledge. Techniques presented during the classes serve only the educational purpose. Please note that in certain circumstances using them might be against the law.

Duration

5 days

Agenda

1. Introduction
   - Aim of attack
   - Available means (remote, local)
2. Low level attacks (x86 and x86_64)
   - Format string
   - buffer overflow - stack, heap
3. Bypassing of exploitation prevention mechanisms
   - Bypassing DEP
   - Bypassing ASLR
4. Security analysis and evaluation of applications meant to operate in the system

Target audience and prerequisites

Good knowledge of C programming and x86 architecture. Basic knowledge of Assembler. Basic knowledge of Python programming. Basic knowledge of Linux.

Certificates

Course participants receive completion certificates signed by ALX.

Locations

- Online (English) – your home, office or wherever you want
- Warsaw (English) – Jasna 14/16A
- any other location (London, UK, EU) on request

Price

1990 EUR

The price includes:

- course materials,
- snacks, coffee, tea and soft drinks,
- course completion certificate,
- one-time consultation with the instructor after course completion.