Security components in Linux (code: LX-Security)

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

Overview

An intensive workshop dedicated to security mechanisms available in Linux, including the basics of circumventing those mechanisms with examples of attacker's code hiding techniques. This workshop is recommended for both administrators and system security testers. Topics presented during this workshop might also be useful for Linux administrators in big institutions. The acquired knowledge will be helpful when it comes to avoiding "catching" the so-called "nasty surprises" on servers. These are not only individually aimed attacks, but also the common *bugs* spreading through outdated or not secured "overlooked" machines which can happen extremely easily especially in big environments.

Duration

4 days

Agenda

1. Strengthening mechanisms
   - SELinux
   - GRSec
   - AppArmor
   - chroot/sandbox/LXC
   - ASLR
   - PaX
2. Advanced compilation techniques
   - position independent code
   - optimalisations, strengthening
3. Security bypassing techniques
   - escaping chroot
   - bypassing ASLR
4. Code hiding methods
   - based on the kernel module
   - not based on the kernel module
5. Honeypots
   - structure
   - detection

Target audience and prerequisites

Medium-advanced knowledge of Linux systems.

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

1540 EUR

The price includes:

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

Ask for details

Phone +44 203 608 6289
info@alx.training