Szkolenie: The Linux Foundation
LFD440 Linux Kernel Debugging and Security

Cel szkolenia:

This instructor-led course focuses on the important tools used for debugging and monitoring the kernel, and how security features are implemented and controlled.

This course is for experienced developers who need to understand the methods and internal infrastructure of the Linux kernel.

This four day course includes extensive hands-on exercises and demonstrations designed to give you the necessary tools to develop and debug Linux kernel code.

You will walk away from this course with a solid understanding of Linux kernel. debugging techniques and tools.

Plan szkolenia:

- Introduction
  - Objectives
  - Who You Are
  - The Linux Foundation
  - Linux Foundation Training
  - Certification Programs and Digital Badging
  - Linux Distributions
  - Platforms
  - Preparing Your System
  - Using and Downloading a Virtual Machine
  - Things change in Linux
  - Documentation and Links
- Preliminaries
  - Procedures
  - Kernel Versions
  - Kernel Sources and Use of git
- How to Work in OSS Projects **

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Overview on How to Contribute Properly
- Stay Close to Mainline for Security and Quality
- Study and Understand the Project DNA
- Figure Out What Itch You Want to Scratch
- Identify Maintainers and Their Work Flows and Methods
- Get Early Input and Work in the Open
- Contribute Incremental Bits, Not Large Code Dumps
- Leave Your Ego at the Door: Don’t Be Thin-Skinned
- Be Patient, Develop Long Term Relationships, Be Helpful

- Kernel Features
  - Components of the Kernel
  - User-Space vs. Kernel-Space
  - What are System Calls?
  - Available System Calls
  - Scheduling Algorithms and Task Structures
  - Process Context
  - Labs
- Monitoring and Debugging
  - Debuginfo Packages
  - Tracing and Profiling
  - sysctl
  - SysRq Key
  - oops Messages
  - Kernel Debuggers
  - debugfs
  - Labs
- The proc Filesystem **
  - What is the proc Filesystem?
  - Creating and Removing Entries
  - Reading and Writing Entries
  - The seq file Interface **
  - Labs
- kprobes
  - kprobes
  - kretprobes
  - SystemTap **

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Labs
- Ftrace
  - What is ftrace?
  - ftrace, trace-cmd and kernelshark
  - Available Tracers
  - Using ftrace
  - Files in the Tracing Directory
  - Tracing Options
  - Printing with trace printk()
  - Trace Markers
  - Dumping the Buffer
  - trace-cmd
  - Labs
- Perf
  - What is perf?
  - perf stat
  - perf list
  - perf record
  - perf report
  - perf annotate
  - perf top
  - Labs
- eBPF
  - BPF
  - eBPF
  - Installation
  - bcc Tools
  - bpftrace
  - Labs
- Crash
  - Crash
  - Main Commands
  - Labs
- kexec
  - kexec
  - Kernel Configuration

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

    - kexec-tools
    - Using kexec
    - Labs
- Kernel Core Dumps
    - Producing and Analyzing Kernel Core Dumps
    - Labs
- Virtualization**
    - What is Virtualization?
    - Rings of Virtualization
    - Hypervisors
- QEMU
    - What is QEMU?
    - Emulated Architectures
    - Image Formats
    - Third Party Hypervisor Integration
    - Labs
- Linux Kernel Debugging Tools
    - Linux Kernel (built-in) tools and helpers
    - kdb
    - qemu+gdb
    - kgdb: hardware+serial+gdb
    - Labs
- Embedded Linux**
    - Embedded and Real Time Operating Systems
    - Why Use Linux?
    - Making a Small Linux Environment
    - Real Time Linuxes
- Notifiers**
    - What are Notifiers?
    - Data Structures
    - Callbacks and Notifications
    - Creating Notifier Chains
    - Labs
- CPU Frequency Scaling**
    - What is Frequency and Voltage Scaling?
    - Notifiers

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Drivers
- Governors
- Labs

- Netlink Sockets**
  - What are netlink Sockets?
  - Opening a netlink Socket
  - netlink Messages
  - Labs
- Introduction to Linux Kernel Security
  - Linux Kernel Security Basics
  - Discretionary Access Control (DAC)
  - POSIX ACLs
  - POSIX Capabilities
  - Namespaces
  - Linux Security Modules (LSM)
  - Netfilter
  - Cryptographic Methods
  - The Kernel Self Protection Project
- Linux Security Modules (LSM)
  - What are Linux Security Modules?
  - LSM Basics
  - LSM Choices
  - How LSM Works
  - An LSM Example: Tomoyo
- SELinux
  - SELinux
  - SELinux Overview
  - SELinux Modes
  - SELinux Policies
  - Context Utilities
  - SELinux and Standard Command Line Tools
  - SELinux Context Inheritance and Preservation**
  - restorecon**
  - semanage fcontext**
  - Using SELinux Booleans**
  - getsebool and setsebool**

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Troubleshooting Tools
- Labs

- AppArmor
  - What is AppArmor?
  - Checking Status
  - Modes and Profiles
  - Profiles
  - Utilities
- Netfilter
  - What is netfilter?
  - Netfilter Hooks
  - Netfilter Implementation
  - Hooking into Netfilter
  - Iptables
  - Labs
- The Virtual File System
  - What is the Virtual File System?
  - Available Filesystems
  - Special Filesystems
  - The tmpfs Filesystem
  - The ext2/ext3 Filesystem
  - The ext4 Filesystem
  - The btrfs Filesystem
  - Common File Model
  - VFS System Calls
  - Files and Processes
  - Mounting Filesystems
- Filesystems in User-Space (FUSE)**
  - What is FUSE?
  - Writing a Filesystem
  - Labs
- Journaling Filesystems**
  - What are Journaling Filesystems?
  - Available Journaling Filesystems
  - Contrasting Features
  - Labs

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Closing and Evaluation Survey
  - Evaluation Survey
- Kernel Architecture I
  - UNIX and Linux **
  - Monolithic and Micro Kernels
  - Object-Oriented Methods
  - Main Kernel Components
  - User-Space and Kernel-Space
- Kernel Programming Preview
  - Error Numbers and Getting Kernel Output
  - Task Structure
  - Memory Allocation
  - Transferring Data between User and Kernel Spaces
  - Object-Oriented Inheritance - Sort Of
  - Linked Lists
  - Jiffies
  - Labs
- Modules
  - What are Modules?
  - A Trivial Example
  - Compiling Modules
  - Modules vs Built-in
  - Module Utilities
  - Automatic Module Loading
  - Module Usage Count
  - Module Licensing
  - Exporting Symbols
  - Resolving Symbols **
  - Labs
- Kernel Architecture II
  - Processes, Threads, and Tasks
  - Kernel Preemption
  - Real Time Preemption Patch
  - Labs
- Kernel Configuration and Compilation
  - Installation and Layout of the Kernel Source

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Kernel Browsers
- Kernel Configuration Files
- Kernel Building and Makefiles
- initrd and initramfs
- Labs

- Kernel Style and General Considerations
  - Coding Style
  - Using Generic Kernel Routines and Methods
  - Making a Kernel Patch
  - sparse
  - Using likely() and unlikely()
  - Writing Portable Code, CPU, 32/64-bit, Endianness
  - Writing for SMP
  - Writing for High Memory Systems
  - Power Management
  - Keeping Security in Mind
  - Labs
- Race Conditions and Synchronization Methods
  - Concurrency and Synchronization Methods
  - Atomic Operations
  - Bit Operations
  - Spinlocks
  - Seqlocks
  - Disabling Preemption
  - Mutexes
  - Semaphores
  - Completion Functions
  - Read-Copy-Update (RCU)
  - Reference Counts
  - Labs
- Memory Addressing
  - Virtual Memory Management
  - Systems With and Without MMU and the TLB
  - Memory Addresses
  - High and Low Memory
  - Memory Zones

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Special Device Nodes
- NUMA
- Paging
- Page Tables
- page structure
- Labs

- Memory Allocation
  - Requesting and Releasing Pages
  - Buddy System
  - Slabs and Cache Allocations
  - Memory Pools
  - kmalloc()
  - vmalloc()
  - Early Allocations and bootmem()
  - Memory Defragmentation
  - Labs

Wymagania:

Przed rozpoczęciem tego kursu powinieneś:

- Być biegły w języku programowania C.
- Znać podstawowe narzędzia systemu (UNIX), takie jak ls, grep i tar.
- Swobodnie używać edytorów tekstów (np. Emacs, vi itp.).
- Doświadczenie z jakąkolwiek dużą dystrybucją Linuxa jest pomocne, ale nie jest wymagane.
- Ukończyć kurs **LFD420**: **Linux Kernel Internals and Development** lub mieć równoważne doświadczenie/ wiedzę.

Poziom trudności

Certyfikaty:

The participants will obtain certificates signed by The Linux Foundation

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Prowadzący:

The Linux Foundation Certified Trainer

Informacje dodatkowe:

Live Online (Virtual) or Live (Classroom)
4 days of Instructor-led class time
Hands-on Labs & Assignments
Resources & Course Manual
Certificate of Completion
Digital Badge

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001