Linux Debugging

Introduction:

Five day course

Chapter 1: Review of the Linux Kernel

- Role of the Kernel
- Ring Architectures
- Kernel Mode
- User Mode
- System Call Interface

Chapter 2: General Debug Principles

- Symbols
- Link maps
- Optimized builds
- User mode debugging
- Kernel mode challenges
- Strategies to isolate bugs

Chapter 3: Compiling the Linux Kernel

- Reasons to compile a Linux kernel
- Source Source
- Source Tree
- Preparing for compilation
- Compilation options
- Compiling kernel & modules
- Installing modules
- cscope
- git
- Lab: Compiling the kernel

Chapter 4: Modules

- Kernel modules
- Utilities
- Modules & Devices
- Compiling a module
- Inserting a module
- Removing a module
- Module parameters
- Lab: Building a module

Chapter 5: Types of Kernel Crashes

- Hangs vs. Crashes
- Types of Hangs
- Why the kernel crashes
- Oops Messages
- Types of Crashes

- User mode crashes

Chapter 6: Crash Dump File

- What is a post-mortem analysis
- Strategies for recording memory state
- KExec
- KDump
- Analysis after the crash

Chapter 7: KDB

- When live debugging is best
- How KDB works
- Examining memory
- Working with breakpoints
- Single stepping
- Is KDB the best choice?

Chapter 8: The Stack

a. The role of the stack

- How the Intel stack works
- Calling conventions
- Frame pointer
- Kernel vs. User mode stacks
- Stack tears
- Stack analysis

Chapter 9: Synchronization Issues

b. Need for synchronization

- Critical sections race conditions
- Mutexes
- Semaphores
- Atomic Bit operations
- Atomic Integers
- Spinlocks
- Lab: Synchronization

Chapter 10: Memory Management Issues

- Virtual Memory challenge
- x86 Page Tables
- x86-64 Page Tables
- Memory Zones
- Allocations within the kernel
- Page Frames
- Slab Allocator
- Lab: Memory Management

Chapter 11: Process Contexts

- What is a Linux process
- Creating processes
- Process resources
- Process memory
- pmap
- Kernel threads

- Process 0
- Killing a process
- Process context switch
- The scheduler
- Kernel preemption

Chapter 12: Debugging Tools

- kProbes
- SystemTap
- fTrace

Chapter 13: Debugging Device Drivers

- Review of Linux drivers
- User requests
- Driver events
- Device registration
- Why drivers fail
- Strategies for isolating driver faults

Chapter 14: Debugging the Boot Process

- BIOS stage
- Bootloader
- Initial RAM disk
- grub
- Kernel
- init
- Run levels