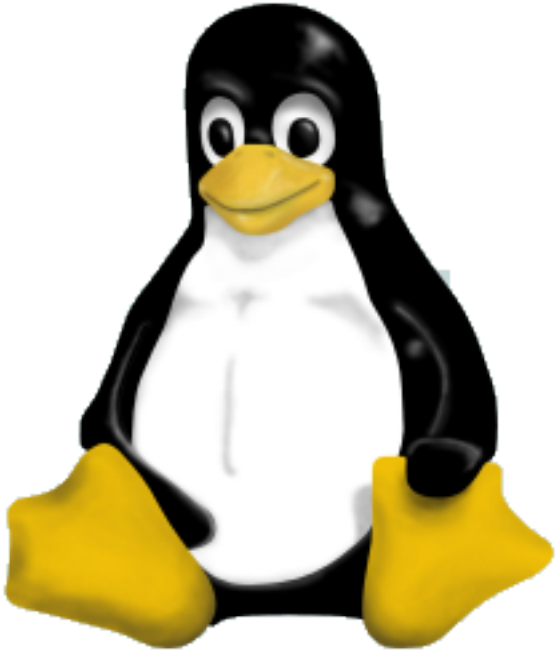
Linux Kernel Hacking Free Course, 3rd edition

D. P. Bovet, M. Cesati
University of Rome “Tor Vergata”

An introduction to Linux



January 18, 2006

What is Linux

- Linux is a POSIX-compliant kernel, although it is not a full Unix-like operating system because it does not include all the Unix applications, such as filesystem utilities, windowing systems and graphical desktops, system administrator commands, text editors, compilers, and so on

- The GNU project started in 1984, and in particular the gcc compiler/linker has played a crucial role in the development of Linux

- from the Open Software Foundation website: *Variants of the GNU operating system, which use the kernel Linux, are now widely used; though these systems are often referred to as Linux, they are more accurately called GNU/Linux system*

Privilege levels

- Modern computers can run in at least two different modes or *privilege levels*
- This hardware feature has been introduced many years ago to protect the operating system (OS) from faulty programs and to forbid users to access some critical I/O devices such as disks
- In the IA-32 computers, the 16-bit Code Segment register contains 2 bits that can encode up to 4 different privilege levels: level 0 (most privileged), level 1, level 2, level 3 (less privileged)

What is a kernel

- The *kernel* of an OS consists of the set of programs that run in a privileged level (for IA-32 computers, a level smaller than 3)
- Some kernels such as the kernel of Windows NT use privilege level 0 for the basic functions and privilege levels 1 and 2 for the I/O drivers
- Linux uses only 2 privilege levels called *User Mode* and *Kernel Mode*

Entering and leaving Kernel Mode

- A User Mode program enters in kernel mode by issuing a special `int` instruction: in Linux, interrupt `0x80` is reserved to implement system calls
- Many I/O devices issue interrupts to signal the end of an I/O operation: each of these interrupts puts the CPU into Kernel Mode
- The CPU issues special interrupts called *exceptions* to signal the occurrence of abnormal conditions: overflow, page fault, etc.
- A program in Kernel Mode can put the CPU back in User Mode by executing the `iret` (Interrupt Return) instruction

The kernel program

- The kernel is a huge program, which must be compiled and linked before being loaded in RAM
- Contrary to ordinary programs (sequential programs), the kernel has the following main characteristics:
  - It does not have a single entry point; a different entry point must be provided for every type of interrupt recognized by the kernel
  - The kernel image produced by the gcc linker cannot be loaded as any other executable file, simply because the loader is not available when booting the system: a more rudimentary technique based on bootstrapping must be used

The kernel program