

# **Linux course**

## System Administration and Networking

23.05.2006 - 26.05.2006

## System Administration and Network Course overview

### ***Installing and running Linux:***

- Distributions(04), Live CD/DVDs,
- Installing with CDs, DVDs and via Internet

### ***What happens when the PC starts:***

- Linux Loader - LILO/GRUB (20)
- Initialization: LILO, Kernel, Modules, Init, Runlevels, Login, Prompt (51)
- reboot, halt, shutdown, grubonce(16)

### ***Getting information on Linux commands:***

- man and info system
- /usr/share/doc

### ***Installing programs under Linux:***

- RPM(50), DEB(82), Yast(SuSE only)

### ***Users and File access rights in the system:***

- Users: root, system users and normal users,
  - whoami, w, who, finger, users
- Login, bash shell(09), su, su -
- Standard Access directories after installation
  - /home, /tmp, /var/tmp
- Users administration:(53)
- Access rights, acls and attributes(12)

### ***The file system in Linux(11):***

- The kernel and its single file system tree
- What is where in Linux: /bin, /sbin, /boot, /root, /proc, /lib, etc
- Hard and symbolic links: ln, cp, mc

### ***Finding files in Linux:***

- Finding normal files: find(42), mc, stat, locate, slocate
- Finding commands: whereis, which, type

### ***Running commands and automatizing system maintenance?***

- Terminals and consoles in Linux(05)
- Often used and useful commands(10)
  - Relative and absolute paths
  - user commands (/bin, /usr/bin)
  - system administration commands (/sbin, /usr/sbin)
  - Pipes and redirections (33)
- Execute commands at a later time/date (56)
  - echo "command" | at time
- Regularly execute commands with **cron** (57)
  - crontab -e, /etc/crontab, /etc/cron.daily
  - /var/spool/cron/tab
- Regular expressions (94)
  - . \* ^ \< \> \b \B \$ [...] \ (..) {...} + ? |

**Running root commands as normal user:**

- Sudo (83)
  - visudo, /etc/sudoers, sudo su -

**Processes under Linux:(41)**

- Process administration tools:
  - Text based: ps, top, nice, renice, kill, skill, xkill, killall
  - Graphic: ksysguard

**The Linux kernel and what it does:(52)**

- Central lowest level unit + modules
- Loading/unloading modules
  - Hardware modules
    - (in Kernel and in /lib/modules/<kernel>/)
  - Manual Start-Stop of Kernel modules
    - insmod, modprobe, rmmod, lsmod, modinfo, lsof
    - /lib/modules/\$(uname -r)/modules.dep
- Compiling a kernel: /usr/src/linux

**Monitoring what is going on in the system:**

- Log Files (55)
  - syslogd and /etc/syslog.conf
  - Installation as Log-Server
  - Installation as log client

**System rescue: (81)**

- With or without external system

**Preparing a new hard disk for the system:(40)**

- Partitioning(13): fdisk, cfdisk, parted, fdformat
- Filesystem(11): mkfs, mkreiserfs, fsck, reiserfsck
- Mounting(39): mount, umount
- Status: df -h, du -sh, kdiskfree, kwikdisk
- Solving problems: lsof, mount, cat /dev/xxxx

**Installing new hardware in the system:(78)**

- Hotplug(USB, Firewire,pci)
  - lsusb
  - modprobe usb-storage
  - /etc/hotplug/usb.agent
  - /etc/hotplug/pci.agent
  - /etc/hotplug/ieee1394.agent
- PCMCIA (PCI Bridge)
  - cardinfo (x-programx)
  - cardmgr, cardctrl, dump\_cis
- Network card (Auto detection)

**Graphic interface:**

- X-Server, Windowmanagers, Launchers

- Configuring the X-Server(18)
  - Ver. 3.0, Ver 4.0, FrameBuffer
  - (SuSE)Config with sax and sax2
- Display Manager (runlevel 5)
- Window Manager (kwin,twm)
- Desktops (47)(KDE, Gnome, Enlightenment, Windowmaker)

### **Controlling the amount of space used on hard disks by users:**

- Quotas (59)
  - in /etc/fstab: usrquota, grpquota
  - quotacheck -vaugm (quota.group, aquota.user)
  - edquota -u *username*
  - repquota -a (show all quotas)
  - quotaon and quotaoff
  - soft, hard and grace period

### **Printing in Linux:**

- CUPS - Common Unix Printing System (48)
  - CUPS server Configuration
  - /etc/printcap
  - kprinter, kups, yast2

### **Compiling the kernel:**

- Install the kernel-source package
- Compiling the kernel (52)
 

```
cd /usr/src/linux
make xconfig
make dep
make clean
make bzImage
make modules
make modules_install
```

## Networking with Linux

### **Configuring the network card manually:**

- Network Configuration (21)
  - Network Card drivers
  - ifconfig, netstat

### **Configure the network card automatically:**

- DHCP und BOOTCP (75)
  - Server Configuration
    - /etc/dhcpd.conf
  - Client Configuration
    - dhcpd, pump, dhclient

### **Connecting Linux to a local network or Internet?**

- TCP/IP Basics (60)
  - TCP, UDP, IP, ICMP, ARP, Ethernet, Frame

- TCP/IP Services (61)
  - Daemons(runlevels) , inetd , /etc/inetd.conf
- RPC Services (Remote Procedure Call) (80)
  - portmap, rpcinfo -p localhost, NFS
- Network Diagnostics (86)
  - Packet Sniffing' tools (see security below)
  - Text based: tcpdump, ngrep, tethereal
  - X-Based: ethereal
- Routing und Gateway (65)
  - General Routing Principle
  - Routing under Linux
    - route, routed, zebra, gated, RIP, BGP
  - Standard Gateway

### **Remote administration of Linux:**

- **SSH** Secure Shell (72)
  - Priv./Pub. keys principle
  - Generating keys pairs
  - Tunneling
- Graphic programs for remote administration
  - X-Server (18b)
  - VNC (97)
  - Webmin (96)
  - Windows SSH - WinSCP, Filezilla
  - Java - Mindterm

### **Transferring files between same or different operating systems: (90)**

#### **FTP (Server-Client)**

- FTP clients
  - mc, ftp
  - gftp, kbear, ncftp
  - IglooFTP, xftp
- FTP Servers
  - As 'Daemon' or via inetd
  - FTP servers
  - proftpd, pure-ftpd
  - wu.ftpd, in.ftpd, vsftpd

#### **Samba Clients**

- mount -t smbfs
- smbclient

#### **SSH Clients**

- Linux SSH Clients
  - scp
  - rsync

- rdist
- Windows SSH Clients
  - Mindterm (Java)
  - SSH Win (SSH Secure Shell) \*\*\*
  - pscp (with Putty)
  - WinSCP

### **Domain name resolving in Linux:**

- resolver library functions, /etc/host.conf, /etc/nsswitch.conf,
- /etc/hosts, /etc/resolv.conf
- **DNS** (Domain Name Service) (66)
  - Bind9 Configuration
    - /etc/hosts, /etc/hosts.conf, /etc/resolv.conf
    - /etc/named.conf
    - /var/named/
  - Slave DNS Konfiguration
    - /var/named/slave

### **Security in Linux:**

- System Files access rights rules
  - chkstat -set /etc/permissions
  - /etc/permissions & /etc/permissions.local
  - /etc/permissions.easy
  - /etc/permissions.secure
  - /etc/permissions.paranoid
- Firewall: iptables and tools to configure it
  - webmin (Very good)
  - fwbuilder
  - jay's firewall generator
- Packet sniffers
  - Text based: tcpdump, iptraf, ngrep, tethereal
  - X-Based: ethereal
- Firewall and intrusion testing programs
  - Port scanners: nmap, nessus
- File Intrusion Detection systems (IDS)
  - AIDE, Tripwire
- Network Intrusion Detection systems(NIDS)
  - SNORT
- Intrusion prevention system:
  - fail2ban, port knocking
- Virus scanners:
  - ClamAV
- System logs monitoring

- Scanlog, logsurf

***Email in Linux:***

**Postfix** as Mail server (74)

- Mail Server/Client Components
- Mail Routing and Filtering
- Extra Mail Service Programs
  - pop3, pop3s,imap
  - fetchmail