Linux course

System Administration and Networking

03.01.2007 - 16.01.2007

System Administration and Network
Course overview

Installing and running Linux:

- Distributions(04), Live CD/DVDs, `www.distrowatch.com`
- 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)
  `init` is the first process to be started on bootup
- `reboot`, `halt`, `shutdown`, `grubonce`(16)

Getting information on Linux commands:

- `man` and `info` system
- `/usr/share/doc`
- `/usr/share/doc/howto` and Howtos in Internet. (LDP)

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)
  `useradd, userdel, usermod, groupadd, groupdel,`
  `passwd``, /etc/passwd, /etc/shadow`
  `useradd -D` : shows standards values used to create a new user

- Access rights, suid, sgid, stickyBit, attributes and acls(12)
  `chmod --reference=file1 file2`
  uses the `file1`'s rights as template to set `file2`'s rights
  'execute' access right for Directories used to let anybody through
  `chmod 544` **:** owner has `r-x`
  `/tmp` has Sticky Bit set (prevents deleting from other users)

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`
  `/etc` : System configurations
- Hard and symbolic links: `ln`, `cp`, `mc`

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

- Partitions names: `/dev/hdxx`, **`/dev/sdxx`**,
- **Primary(4)**, Extended & logical Partitions(starts with Nr.5)
- How to partition depending on use of system
  `/usr` needs normal more space than `/`
- Partitioning(13): **`fdisk`**`, sfdisk, `**`cfdisk`**`, parted, fdformat`

- Filesystem(11): `mkfs.ext2(mke2fs) mkreiserfs, fsck, reiserfsck`
- Mounting(39): `mount, umount, mount -L` *`Label Mountpoint`*
  - Device busy error message: pwd is in partition, file of partition is opened
  - `/etc/fstab` **:** entries must be there to allow users to mount devices
- Status: `df -h, du -sh, kdiskfree, kwikdisk`
- Solving problems: `lsof , mount, cat /dev/xxxx`

`df` : Shows mounted partitions and their capacity, space used and space left

`cfdisk, fdisk` allows to create new partitions

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)
  - `pwd, cd, ls, whoami, w`
  - `command &` and `command1;command2`
  - Relative and absolute paths
  - user commands (`/bin,/usr/bin`)
  - showing the content of files: `cat`, `more`, `less`, (`less -X`)
  - system administration commands (`/sbin,/usr/sbin`)
  - Pipes and redirections (33)

    `>  >>  <<  <  tee xargs | 1>&2  &> 2> 2>/dev/null`
- Environment variables
  - `read` : Gets keyboard from user into a variable
- 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:
  - `init` is the first process to be started on bootup (`/etc/inittab`)
  - Daemon, scripts, bin , `tty` in `ps`
  - Text based: `ps`, `top`, `nice`, `renice`, `kill`, `skill`, `xkill`, `killall`
  - Graphic: `ksysguard, kpm`

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`
    `/var/log/messages` is the standard system log file
  - Installation as Log-Server
  - Installation as log client

System rescue: (81)

- Using Live CD/DVD
- Using boot kernel option `init=/bin/bash`
- Protecting against these 2 methods
  - Lock computer
  - BIOS Password and booting only form C:
  - Password in `/etc/lilo.conf` or in `/boot/grub/menu.lst`

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)
  xdm, gdm and kdm are 3 mostly used display managers
- 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/cups/cupsd.conf`
    - `/etc/printcap`
    - `lpstat -t, lpq -P printer, lprm`
  - `kprinter, kups, yast2`
  - `http://localhost:631`

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)
  - `rcnetwork restart, /etc/init.d/network restart`
  - `/etc/sysconfig/network/ifcfg-eth-id-xx:xx...`
  - Network Card drivers:
    `/lib/modules/$(uname -r)/kernel/drivers/net/`
  - `ifconfig, netstat -ltupn`

Configure the network card automatically:

- DHCP und BOOTCP (75)
  - Server Configuration
    - `/etc/dhcpd.conf`
  - Client Configuration
    - `dhcpcd, 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)
  - `xinetd`, `/etc/xinetd.d/`*`service`*
  - `inetd`, `/etc/inetd.conf`
  - eg. `http` : Port 80, `https`: Port 443

- TCP Wrappers
  - `tcpd, /etc/hosts.allow, /etc/hosts.deny`

- Protocols of Internet access:
    - ethernet, pppoe, ppp, ATM

- RPC Services (Remote Procedure Call) (80)
    - `portmap`, `rpcinfo -p localhost`, NFS

- Network Diagnostics (86)
    - Packet Sniffing tools (see security below)
    - Network connections: `netstat -tupn`
    - Listening services:
        - `netstat -ltupn`
        - `lsof -Pni4`
    - Text based: `tcpdump, ngrep, tethereal, iptraf`
    - X-Based: `ethereal`

- Routing und Gateway (65)
    - General Routing Principle
    - Default Gateway `/etc/sysconfig/network/routes`
    - Routing under Linux
        - `route`, `routed`, `zebra`, `gated`, RIP, BGP
    - NAT (MASQ)
        - Multiple PC go in Internet with one IP
        - Needs only one IP to route further
        - Higher security by hiding the PC's IPs in LAN

    - PROXY
        - Represents the user in LAN in Internet
        - Speed-up Internet response to LAN clients
        - Better security: Can filter unwanted web sites
        - Same advantages as NAT(MASQ)

Remote administration of Linux:

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

Transfering files between same or different operating systems: (90)

FTP (Server-Client)

- FTP clients
    - Text based: `mc, ftp`
    - Graphic(X) based: `gftp, kbear, ncftp IglooFTP, xftp`
- FTP Servers

- As 'Daemon' or via `inetd/xinetd`
- FTP servers types
    - `in.ftpd, wu.ftpd, proftpd`
    - `pure-ftpd, vsftpd`

<u>NFS</u> (Server-Client)

- NFS server (`/etc/exports`)
- `mount -t nfs` *`server:/path /mount/point`*

<u>Samba Clients</u>

- `mount -t smbfs, smbmount, smbunmount`
- `smbclient`

<u>`Samba:`</u> Can be configured as a Primary Domain Controller for Windows

<u>**SSH** Clients</u>

- Linux SSH Clients
    - `scp`
    - `rsync`
    - `rdist`
    - `unison`
    - `mindterm` (Java)
    - `mc` (shell link)
- 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`, <u>`/etc/resolv.conf`</u>
- **DNS** (Domain Name Service) (66)
    - Bind9 Configuration
        - `/etc/hosts.conf,/etc/hosts, /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, saint

- File Intrusion Detection systems (IDS)
  - AIDE, Tripwire

- Network Intrusion Detection systems(NIDS)
  - SNORT

- Intrusion prevention system:
  - fail2ban(for ssh, ftp, http),
  - 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
  - amavis, ClamAV, spamassassin, AntiVir
  - postgrey,
- Extra Mail Service Programs
  - mmail and mbox mailbox formats
  - pop3, pop3s, imap(dovecot)
  - fetchmail