

Administration of Operating Systems

DO2003

<http://www.hh.se/do2003>

Review



Examinations

- **Practical exam**
 - 1 hour
 - Includes preparation (log in, copy the virtual machine) and showing your work to the teacher for grading
 - No Internet access, no cellphones, no books or any notes
 - You can access to the Linux manual and help system
- **Theoretical exam**
 - 4 hours
 - **Make sure you register!**
 - No cellphones, no books or any notes.
- On both exams you can use a dictionary, but it has to be a paper one, and there must be absolutely no notes in it
- **Bring your student card and ID (ID kort, passport)**

Linux and Ubuntu Linux Overview (Ch. 1-4)

- Operating system
 - Types
 - Main components
 - Kernel responsibilities
- Installation
 - Requirements, Partitioning
 - Virtual machines
- Finding documentation
 - Man, apropos, info
- Login and logout
- CLI

Utilities (Ch. 5)

- Manipulating, displaying, comparing, and print files
 - cp , mv, rm, ls, pwd, cat, diff, file, grep, sort, head, tail
- Archiving and (de)compression utilities
 - tar, bzip2, bunzip2, bzip2, gzip, zip, rar
- Location utilities
 - Whereis, which
- User and system information utilities
 - finder, hostname, who
- User communication utilities
 - mesg, write
- Other utilities
 - date, echo, man, apropos, vi, nano, touch

File system (Ch. 6)

- Filesystem
 - Set of data structures used to organize data
 - NTFS, FAT, ext2, ext3, ext4, ISO 9660, UDF
- Files and directories
 - Filenames and pathnames (absolute path vs. relative path)
- Communication between processes: | (pipe)
- Working directory (pwd), home directory(~)
- Name matching (*, ?, [...])
- Important directories and files
- Access permissions: symbols(r, w, x, -), octals (4, 2, 1, 0)
- Link, symbolic link, hard link
- Utilities
 - cd, pwd, mkdir, rmdir, cp, mv, ln, touch, chmod, stat

Shell (Ch. 7)

- Command line
 - Syntax: command name (\$0), arguments (\$1-\$n)
 - Processing and executing
 - PATH
- Stdin (0), stdout (1), stderr (2)
 - > is shorthand for 1>
 - < is short for 0<
 - 2> redirects standard error
- Background (&) and foreground execution
- Generating and expanding filenames (*, ?, [...])
- Builtins
- Utilities
 - tee, bg, fg, kill, jobs, sleep

Bash (Ch. 9)

- Command line interpreter
- Programming language: execute commands from a shell script files
- Running a scripts
 - Techniques and requirements
- Job control (Background (&) and foreground execution)
- Variables
 - User created variables and Shell keyword variables
- Processes (PID)
- Functions
- Aliases
- Command-line expansion
 - Double quotation marks vs. Single quotation marks
 - Special characters and commands that are symbols (Page 327)

Network (Ch. 10)

- Purpose : Communication, resource sharing, ...
- Types of networks: LAN, WLAN, WAN, MAN, PAN
- Network devices: computers, routers, hub, switches, ...
- Protocols: TCP, IP, UDP
- Communication models: broadcast, peer-to-peer, switched
- Addressing
 - Physical vs. logical addresses
 - Static vs. Dynamic IP addresses
- Utilities
 - OpenSSH utilities, telnet, ftp, ping, traceroute, host, dig

System Administration: Core Concepts (Ch. 11)

- Working with root privileges (#)
 - Some commands can only be executed by root
 - File and directory access permissions do not affect root
- su vs. sudo
- Upstart init daemon
 - start and stop system services
- Setting Up a Server
 - Standard Rules in Configuration
 - Security: /etc/host.allow, /etc/hosts.deny, chroot
- Utilities
 - visudo, fsck, kill -TERM PID vs. kill -kill PID
- A syntax error in the sudoers file can prevent you from using sudo to gain root privileges

Files, Directories, and Filesystems (Ch. 12)

- Important standard directories
 - / - Root directory
 - /dev - Contains files that represent peripheral devices
 - /etc - Holds Files used in administrative, configuration and file system management
 - /usr - Contains the majority of user utilities and applications
 - /usr/bin - Contains standard Linux utility programs
 - /root - Root home directory
 - /etc/group - Holds group information and associates users with a group-ID
 - /etc/passwd - Holds user information
 - /etc/hosts - Stores name and ip address
 - /var/log - System log files
 - /media is intended as a mount point for external devices
- File types: (-, d, l, b, c, s, p)
- Mounting (mount) and unmounting (umount) a filesystem
 - /etc/fstab

Downloading and Installing Software (Ch. 13)

- To improve security, administrators must to keep the system and the software on a system up-to-date
- Software packages
- The Debian package (dpkg) management system facilitates the process of adding and removing software packages in deb format
 - Dpkg doesn't download software packages
- APT
 - Downloads and installs software packages from the Internet or DVD
 - Resolves packages dependencies
 - Synaptic, aptitude and apt-get
- Apt-cache and dpkg utilities are used to query and verify dpkg packages
- You can download the source code and build executable files manually as well

Administration Tasks (Ch. 16)

- Managing User Accounts and Group
 - adduser, deluser, moduser
 - addgroup, delgroup, modgroup
- Backing up files using tar and cpio
- Scheduling tasks using cron and at
- System reports using vmstat and top
- Troubleshooting
 - Log files

Configuring and Monitoring a LAN (Ch. 17)

- Hardware
 - NIC, wireless NIC, hub, switch, WAP, hub, router, ...
- `/etc/network/interfaces`
- Servers
 - NFS (Network File System)
 - Allows users to share directory hierarchies
 - OpenSSH
 - Enables secure logins between remote systems
 - DNS (Domain Name Service)
 - Maps IP addresses and fully qualified domain names (FQDN) to one another
 - DHCP (Dynamic Host Configuration Protocol)
 - Assigns Internet address, subnet mask, default gateway and other information to hosts
 - Samba
 - Allow Windows PCs to share files and printers with UNIX and Linux computers

OpenSSH (Ch. 18)

- Set of tools that encrypts all traffic, including passwords, to provide secure communication
 - sshd, ssh, scp, sftp, ssh-keygen
- 1. When an OpenSSH client opens a connection, it verifies that it is connected to the correct server
- 2. Then OpenSSH encrypts communication between the systems
- 3. Finally OpenSSH makes sure that the user is authorized to log in on or copy files to and from the server
- You can secure many protocols: POP, X, IMAP, VNC, and WWW—by tunneling them through ssh.
- OpenSSH also enables secure X11 forwarding
 - Run securely a graphical program on a remote system and have the display appear on the local system

FTP (Ch. 19)

- Is a protocol for downloading files from and uploading files to another system over a network
- Is a non secure protocol
 - Commonly used to download public information only
- Sftp and lftp are secure implementations that use OpenSSH facilities to encrypt the connection
 - OpenSSH tools do not understand the FTP protocol but they map ftp commands to OpenSSH commands
- Users can login as **anonymous** or **ftp**
- FTP provides two modes of transferring files: binary and ASCII

Email (Ch. 20)

- Email Life Cycle
- MSA vs MTA
 - MTA is capable of doing MSA work, and correct minor errors in a message's format, and immediately report an error to the author
- Email protocols
 - SMTP (send), POP3 (receive) and IMAP (receive and store)
- exim4
 - Needed when you own a domain where you want to receive email
 - Stores incoming messages at /var/mail

NIS and LDAP (Ch. 21)

- NIS (Network Information Service) - ypserv
 - Allows a group of machines within an NIS domain to share a common set of configuration files which is kept in one place
 - Simplifies maintenance and administration of multiple computers
 - /etc/passwd, /etc/group, /etc/hosts
 - yppasswd and /etc/ypserv.conf
 - Servers, clients and slaves
- LDAP (Lightweight Directory Access Protocol)
 - A LDAP server holds a search- and read-optimized database (directory)
 - LDAP clients, such as email clients, query and update this directory
 - Authentication servers can use an LDAP directory to authenticate users
 - Kerberos
 - Secure authentication of users on the network

NFS (Ch. 22)

- Allows a server to share selected local directory hierarchies with client systems on a heterogeneous network
 - One central computer can have the files physically on its hard disk and make them available via NFS to the rest of the network
 - Reduces storage needs
- Directories or even entire filesystems can appear as if they are local
- Defines a client/server relationship in which a server provides directory hierarchies that clients can mount
- `/etc/exports` file lists the directory hierarchies that the system exports
- From a client, a `mount` command mounts an exported NFS directory hierarchy
- `/etc/fstab` defines which filesystems are mounted automatically on boot
- Utilities: `df -h`, `mount` and `umount`

Samba (Ch.23)

- Enables Linux and Windows to share directory hierarchies and printers
- Users must authenticate themselves to access a share
- `/etc/samba/smbusers` and `/etc/samba/smbpasswd`.
- `/etc/samba/smb.conf`
- Swat - web-based administration utility
- How to access a share on a Linux Samba server from Windows?
- How to access a share on a Windows server from Linux?
- Utilities
 - `smbtree` (displays shares)
 - `smbclient` (similar to ftp)
 - `mount -t cifs` (mounts shares)

DNS/BIND (Ch. 24)

- DNS (Domain Name Service)
 - Internet service that maps IP addresses and FQDN to one another
- BIND (Berkeley Internet Name Domain)
 - Is the most common implementation of the DNS protocol
- Resolver
 - Queries the local DNS cache, if available, and then queries DNS servers on the LAN or Internet
- Queries: iterative and recursive
- Servers: Master servers, Slave servers and DNS cache servers
- DNS Spoofing
 - When a DNS server receives a non-authentic data, caches it for performance optimization, and supplies the non-authentic data to the clients of the server

Firewall (Ch. 25)

- Design to prevent unauthorized access to a system or network
- Enable to filter incoming and outgoing traffic that flows through your system
- Types: HW and SW firewalls
 - Tradeoffs
- Iptables, (g)ufw, firestarter, netfilter, shorewall
- NAT (Network Address Translation) allows several systems to share a single Internet connection
 - Ensures that all traffic passes through the firewall
- Rules can be set so the firewall can inspect packet's characteristics, such as protocol type, the source or destination host address, and the source or destination port

Apache (Ch. 26)

- Apache is the most commonly used web server on Linux systems
- Web servers serve web pages to clients, which typically use web browsers to request and view web pages
- HTTP
- URI
 - `http://slawek:***@hh.se:80/index.html?lang=Eng#Staff`
- Configuration directives and contexts
 - Document root, scriptalias
 - Virtual hosts
- Hyper Text Transfer Protocol over Secure Sockets Layer (HTTPS)
 - Allows a client to verify the identity of a server
 - Enables secure two-way communication between a client and server

Programming BASH (Ch. 27)

- Control structures
 - Alter the order of execution of commands within a shell script

```
if test-command  
then  
  commands  
fi
```

```
if test-command  
then  
  commands  
else  
  commands  
fi
```

```
for loop-index in argument-list  
do  
  commands  
done
```

```
while test-command  
do  
  commands  
done
```

- Break and continue
- Shell builtins: read, exec, trap, kill
- Arithmetical and logical expressions

