Aalto University
School of Science

Linux crash lecture

by Andrey Lukyanenko

T-110.5102 Laboratory Works in Networking and Security

20.1.2015 Otaniemi
based on material of Miika Komu, 2013

Traversing Directories

- **cd – Change Directory**
  - Change to a directory
  - Give the directory as an argument
  - With no arguments, changes to your home directory

- **pwd – Print Working Directory**
  - Displays your curret working directory

Use the tab key for auto-completion!

Files and Directories on Linux

- **By default, all file names are case sensitive!**
  - Foo.txt is different than foo.txt (unless working with FAT32)
- **Dot “.”**
  - Means current directory
  - Example: find .
- **Double dot “..”**
  - The previous directory
  - Example: cd ..
- **Asterisk “*”**
  - Matches zero or more characters (use “?” for a single character)
  - Example (list all files ending in “txt”): ls *.txt

More on Files and Directories

cp – copy files

- cp source dest

mv – move files

- mv source dest

rm – remove file/dir

- rm file
- rm –rf directory
- **Use with care!**

ls – list files

mkdir – make directory

- mkdir mydir

head – front of a file

tail – tail of a file

- tail /var/log/syslog
- default is 10 lines
- follow: -f

Access Privileges

Check file permissions

- ls –ld filename
- ls –la

Change file permissions

- chmod ugo+rwx
- User, Group, Others
- Add +, remove –
- Read, Write, eXecute
- S = Set user id or Set group id (extra rights)

What are my groups?

- groups

Change ownership

- chown – change user
- chgrp – change group

Switch to root shell

- su
- sudo –s
- See also /etc/sudoers.d/

Important directories

- **Your personal home directory is tilde: “~”**
  - Usually maps to /home/myaccountname
- **Superuser home directory is /root**
- **Temporary storage in /tmp**
  - Wiped out on reboot!
- **Configuration files usually located in /etc**
  - Sometimes in /var (as with BIND DNS server)
- **Log files in /var/log**
  - Important in diagnosing problems with services

Usage of Files

- **What type of file is it?**
  - file filename – displays file type
- **System executables**
  - System applications: just type the command, e.g. “ls”
  - Non-system applications: “./my_binary”
- **Text files**
  - cat file – displays the contents
  - less file – displays scrollable contents (q=quit)
  - Text editors: nano, emacs, vi(m)

Searching for Files

- **Locate**
  - Searches file names using a precreated index
  - Fast, but may not be up-to-date
  - Example: locate foo.txt
- **Find**
  - Searches file names without a precreated index
  - Slow but always up-to-date
  - Example: find /etc –name ‘*cfg’
- **Grep**
  - Search file contents (always up-to-date)
  - Example: grep –r ssh /etc

Searching for Executables

- **Where is tool xyz located?**
  - which xyz – displays the path of xyz
- **What was the tool related to “keyword”?**
  - man –k keyword
  - Note: manual pages describe command line use
  - Start with the examples in the manual pages
- **What was the command I used yesterday?**
  - history – displays all typed commands

Installing software in Debian based Linux distributions

- **aptitude or apt-get**
  - Use one of them but don't mix them!
  - Here, the syntax is the same for both
- **Searching**
  - aptitude search softwarename
  - apt-cache search softwarename
- **Installation**
  - aptitude/apt-get install softwarename
- **Uninstalling**
  - aptitude/apt-get remove softwarename

Volumes and Disks

- **mount – attaches a volume to a directory**
- **umount – detaches a volume**
- **df – how full is the disk?**
  - Human readable: df –h

Reading and Writing I/O

- **Read from an unnamed input stream <**
  - grep “abc” <file
- **Redirect normal output of a tool to a file >**
  - find . >file
  - cat > foo.txt
  - Ctrl+d ends stdin!
- **Redirect error output of a tool to a file 2>**
  - find /etc 2>file
- **Just redirect everything to a file**
  - find /etc >file 2>&1
- **Appending is >>**
  - echo “foo” >>file
  - Note: > overwrites the file
- **Piping |**
  - find /etc | less
- **Stop/resume output**
  - Ctrl+s / Ctrl+q

Process Management

- **Process running?**
  - ps axu | grep ssh
  - Or just “top”
- **Kill process**
  - kill process id
  - kill ‘pidof processname’
  - killall processname
- **Start in background &**
  - processname &
- **Bring a background application to the foreground**
  - fg
- **Put the application to the background**
  - bg
- **Suspend: Ctrl+z**
- **Terminate Ctrl+c**

Service Management

- **Is “cups” service running?**
  - service cups status
- **Stop “cups” service**
  - service cups stop
- **Start “cups” service**
  - service cups start
- **Stop + start “cups” service**
  - service cups restart
- **Reload configuration**
  - service cups reload
- **Old style invocation**
  - /etc/init.d/cups start
- **In Debian, services are in**
  - /etc/rc2.d/
  - S – start in boot
- **“runlevel” tells the run level**

SSH Access

- **Login ssh user@hostname.domain**
- **Exiting: exit (if unresponsive, press alt-gr+~+.)**
- **Clear terminal: reset**
- **Upload: scp local_file user@remotemachine:dir/**
- **Download scp user@remotemachine:remote_file .**
  - Recursive copy: -r
- **Annoyed by password prompts?**
  - man ssh-keygen, man authorized_keys
  - Make sure ~/.ssh permissions are correct!
  - Spend 5 minutes now to set up, save countless minutes later!
- **SSH tunneling / proxying (ssh –L)**

Miscellaneous

- **System Information**
  - uname –a (processor architecture)
  - lsb_release –a (linux release)
- **Crontab – execute binaries periodically**
- **Chroot (or jail) sandbox**
  - Execute processes in constrained environment
- **Apparmor and SElinux – security enhancements**
- **Screen**
  - Exiting ssh kills running processes
  - Screen avoids this (e.g. for IRC sessions)
    - screen programname *opens up the program inside a screen*
    - Ctrl+a+d *to detach*
    - screen –r *to reattach*
    - screen –list *lists all opened screen sockets*
- **TMUX**
  - Alternative for screen

Networking Commands 1 of 2

- **Recommended**
  - ip addr, ip neigh
  - ip route
  - ip xfrm
  - ip iw
- **Old skool**
  - ifconfig, arp
  - route
  - setkey (ipsec)
  - iwconfig
- **DNS look-up**
  - host
  - dig
  - nslookup (depr.)
  - hosts file
- **Firewall**
  - iptables
  - ip6tables
  - No DNS: -n flag
- **ping, ping6, traceroute**

Networking commands 2 of 2

- **Netmasks**
  - netmask nw/mask
- **Traffic capture**
  - tcpdump
  - wireshark
- **Fine tune n/w stack**
  - /proc/sys/net
  - /proc/net
- **What service is up?**
  - netstat (local)
  - nmap (remote)
- **Web testing**
  - lynx
  - wget (note –r)
  - curl
- **Performance**
  - iperf, netperf
  - t-stat, httperf, jperf

Aalto University
School of Science

Questions?

Was something missing?