

A Brief Primer on Linux

T-110.5102

Laboratory Works in Networking and Security

18.9.2012 Otaniemi

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 current 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 from 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 char)
 - 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 dir
 - 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)

Important Directories

- Your personal home directory is tilde: “~”
 - Usually maps to /home/<myusername>
- 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 kind of type file is it?
 - file filename – displays file type
- System executables
 - System apps: 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 Tools (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 command lines

Installing Software in Debian

- aptitude or apt-get
 - Use one of them but don't mix them!
 - Here, the format is the same for both
- Searching
 - aptitude search softwarename
 - apt-get: none, use apt-cache search softwarename
- Installation
 - aptitude/apt-get install softwarename
- Uninstall
 - 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: use the -h flag

Reading and Writing I/O

- Read from an unnamed input stream
 - Example: `grep "abc" <file`
- Redirect normal output of a tool to a file ">"
 - Example 1: `find . >file`
 - Example 2: `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 processnumber`
 - `kill `pidof name``
 - `killall name`
- Start a background process: `app &`
- 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 it
 - service cups start
- Stop + start
 - service cups restart
- Reload configuration
 - service cups reload
- Old style of invocation
 - /etc/init.d/cups start
- In Debian, services are in
 - /etc/rc2.d/
 - S = start in boo
- “runlevel” tells the run level

Ssh Access

- Login `ssh user@hostname.domain`
- Exiting: `exit` (if unresponsive, press `alt-gr + ~ + .`)
- Reset: “reset” command
- 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!

Miscellaneous

- System information
 - `uname -a` (processor architecture)
 - `lsb_release -a` (Linux release)
- Screen
 - Exiting ssh kills running processes
 - Screen avoids this (e.g. for IRC sessions)
- Crontab - execute binaries periodically
- Chroot (or jail) sandbox
 - Execute processes in constrained environment
- Apparmor and SELinux – security enhancements

Networking Commands 1 / 2

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

Networking Commands 2 / 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

Questions?

Was something missing?