Learning Unix

Strap on your crash helmet, as PP takes us on a whirlwind tour of the world's most user friendly (natch) operating system

This file will tell you most of what you need to do to get on, and navigate around a unix system.

First off, you should have a few essential pieces of software:

•
Better Telnet - A telnet application.

•
Blacknight - A terminal dialer (this lets you dial into other systems)

•
As many text files as you can

[Take a look at the links page towards the back for some useful starting points - Ed]

If you can get a hold of the following files, I strongly recommend you read them:

UNIX

Hacking Unix
Basic Unix

Hacking

•
All of the regular newbie guides
•
The 2600 Hack Faq.
•
Hackers Handbook
•

The LOD's 'A novice's guide to hacking' text
•
Every issue of HackAddict
•
Phrack magazine (there are currently 53 issues, so sift through them to find the relevant information)

Contents

Chapter 1 - Connecting to the other system

In this chapter we will use Telnet and Black Night

Connecting is simple - go to the file menu and choose 'Open connection...' First up, try your isp's domain name (ie Maclink.net is the maclink address). If it connects you (a window will open), it will give you a login prompt like this (at least it will if it's Unix):

login:

Type the login that you use to connect to your ISP

password:

And type your ISP password. If it lets you on, it will then give you a whole bunch of crap welcoming you, then it might tell you that you have mail, and finally it will give you the prompt $:

you have mail
$

the $ is your commands prompt. If that all happened as it should have, you are now free to play on a unix system. On your isp's system, you are free to do what you like...this is where you learn...

Chapter 2 - Unix Commands

Have fun with these...
I took most of them out of other files cuz i'm too lazy to type my own

Command

Description

awk
Search for a pattern within a file. Includes

a built-in programming language.

bdiff
Compares two large files.

bfs
Scans a large file.

cal
Displays a calendar.

cat
Concatenates and prints files.

cc
C compiler.

cd
Change directory.

chgrp
Changes a file's group ownership.

chmod
Changes a file's access permissions.

chown
Changes the individual ownership of a file.

cmp
Compares two files; diplays the location (line

and byte) of the 1st difference between these.

comm
Compares two files so as to determine which

lines are common to both.

cp

Copies a file to another location.

cu
Calls another UNIX system.

date
Returns the date and time.

df
Displays free space in the file system.

diff
Displays the differences between two files

or directories.

diff3
Displays the differences between three files

or directories.

du
Reports on file system usage.

echo
Displays its argument.

ed
Text editor.

ex
Text editor.

expr
Evaluates its argument which is generally

a mathematical formula.

f77
FORTRAN compiler.

find
Locates the files w/ specified characteristics.

format
Initializes a floppy disk.

grep
Searches for a pattern within a file. (see awk)

help
Salvation.

kill
Ends a process.

ln
Used to link files.

lpr
Copies the file to the line printer.

ls
Displays info. about one or more files.

mail
Used to receive or deliver e-mail.

mkdir
Creates a new directory.

more
Displays a long file so that the user

can scroll through it.

mv
Used to move or rename files.

nroff
Used to format text.

ps
Display a process's status.

pwd
Display the name of the working directory.

rm
Removes one or more files.

rmdir

Deletes one or more directories.

sleep
Causes a process to become inactive for a

specified length of time.

sort
Sort and merge one or more files.

spell
Finds spelling errors in a file.

split
Divides a file.

stty
Display or set terminal parameters.

tail
Displays the end of a file.

troff
Outputs formatted output to a typesetter.

tset
Sets the terminal type.

umask
Allows the user to specify a new creation

mask.

uniq
Compares 2 files. Finds and displays lines

in one file that are unique.

uucp
UNIX-to-UNIX execute.

vi
Full screen editor.

wc
Displays details in the file size.

who
Information on who else is online.

write
Used to send a message to another user.

awk program filenames
awk -f programfilenames filenames
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
The [awk] utility can be used to find any lines in a file which match a certain pattern; once found, these lines can be processed. In the first configuration, the program that [awk] is to execute is specified in the command line. In the second, the program is stored as the file given in programfilename. The -f option instructs [awk] to read this file.

[bdiff] is used to compare files too large for [diff]. See [diff] for the format.

bfs filename
~~~~~~~~~~~~
[bfs] is used to scan a large file to determine where to split it into smaller files.

cal 01-12 (month) 0-9999 (year)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
[cal] utility can be used to display a calendar of any year from 0 to 9999 AD, and any or all of the twelve months.

cat filename
~~~~~~~~~~~~
[cat] can be used to examine a short file. See [more] for lengthier files.

number[cc]
~~~~~~~~~~
The [cc] command changes the entire current line, or a group of lines starting with the current line. [number] represents the number of old lines to be deleted.
~~~~~~~~~~

cd directory name
~~~~~~~~~~~~~~~~
The [cd] command causes the current working directory to be changed. The [directory name] can be either a full or partial path name.

chgrp groupname filename
~~~~~~~~~~~~~~~~~~~~~~~~
This command changes the group ownership of a file.

chmod ugoa +- rwx
~~~~~~~~~~~~~~~~~~~~~~
The [chmod] utility changes a file's access permissions. [u] specifies the user or owner's login name, [g] specifies a group and [o] indicates all others. [a] indicates the user, group, and all others; it's the default. [+] adds permission; [-] deletes it. [r] indicates read, [w] write, and [x] execute.

chown individualname filename
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
[chown] changes the individual ownership of a file (see chgrp).

cmp filename1 filename2
~~~~~~~~~~~~~~~~~~~~~~
[cmp] is one of the four principle UNIX file comparison utilities. It compares 2 files, and returns the positions where they differ.

comm -options filename1 filename2
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
The [comm] utility, in comparing two files, produces three columns of output. The first contains lines unique to the first file, the second, lines unique to the second, and the third column, lines common to both files. By placing the numbers [1], [2], and/or [3] in the [options] position, any one (or more) of these columns can be suppressed.

cp sendingfile receivingfile
~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~

The [cp] command copies a file. [sendingfile] is the file to be copied, [receivingfile] is the file to which it is copied.

diff [options] filename1 filename2
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Again, a file comparison utility. However, with [diff], the differences are displayed as instructions that can be used to edit the files so that they are identical.

diff3 filename1 filename2 filename3
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Similar to [diff], [diff3] is unique in that it can compare three files. Gee.

ed filename
~~~~~~~~~~~
One of the UNIX's three editing utilities, [ed] is a basic line editor. I'm sure there are other files that will explain how to use [ed]. Thus, I'll confine myself to a rough outline:
e filename ..... edit a different file
f filename ..... changes the currently specified file.
h ..... provides explanation of errors.
I
text ..... inserts text before the current line.
line,linel ..... lists the specified lines.
line,linen ..... displays specified lines, preceded by
their line numbers.
q ..... exit from [ed]
w ..... writes buffer to current filename.
+ or - ..... +number of lines closer to end
-number of lines closer to beginning.

expr formula
~~~~~~~~~~~~
Utility which evaluates an expression.

find directory searchcriteria parameter actioncriteria parameter

The [find] utility can be very useful indeed, especially when confronted by a UNIX with countless files. Basically, this command finds files which meet certain criteria, and then

performs an operation (such as printing the files). Search criteria consists of the following:

Criteria	Parameter	Description
-name	filename	Files whose names match [filename] will meet this criteria.
-type	filetype [b] block special [c] character spec. file [d] directory file [f] plain file	Files whose type matches that specified will meet criteria.
-links	+/- x	Files with # of links indicated by + or - x meet this criteria.
-user	login name or user ID #	Files belonging to user with given login name or ID # meet criteria.
-group	group name or group ID #	Files belonging to group with given group name or ID # meet this criteria.
-size	+ or - x	Files greater than +x bytes or less than -x bytes meet this criteria.
-atime	+ or - x	Files not accessed within +x days, accessed within -x days, or accessed x days ago meet criteria.
-mtime	+ or - x	Files NOT modified within +x days, modified within -x days, or modified x days ago will meet this criteria.
-newer	filename	Files modified more recently than [filename] meet this criteria.
Action Criteria	"	"
-print	-	When search criteria are met, path name of the file is displayed.
-exec	command \;	Executes given command when search criteria are met. indicates filename, [\;] ends the command.
-ok	command \;	Exactly like -exec, except user is prompted [y] or [n] before command.

grep -options searchstring filenames

Another search command, this for a particular string of chars.

ln original new

~~~~~~~~~~~~~~~
[ln] establishes a file link. For this utility, [original] represents the filename to be linked, [new] the filename of the new link to the original.

[ls] provides directory information. [ls -l/] displays a more complete version of the info. list.

mail username username
~~~~~~~~~~~~~~~~~~~~~
This utility allows e-mail to be sent to other system users.

mail
~~~~
Simply typing [mail] checks the user's own mailbox.
When sending mail, several items must be set:
~s text ..... sets the subject field
~c user names ..... sends other users carbon copies of mail
m user names ..... activates the compose mode, with the specified users as the message's recipients.
~h ..... displays and allows editing of all headers.
^D ..... ends message editing; sends mail.
~r filename ..... places file in body of message (keen command)

Reading One's Own Mail:
h number or range ..... causes specified headers to be displayed
p message # ..... displays entire message
d number or range ..... deletes specified messages
u number or range ..... undelete specified mail during SAME mail session (messages removed after q)
q ..... leave the post office

mkdir directoryname
~~~~~~~~~~~~~~~~~~
[mkdir] allows creation of a subdirectory, for your dining enjoyment.

more filename
~~~~~~~~~~~~
For longer files, [more] is a convenient utility. It will display the first screen of file data and then stop, allowing the user to control scrolling henceforth.
~~~~~~~~~~~~

mv oldfilename newfilename
~~~~~~~~~~~~~~~~~~~~~~~~~
The [mv] utility can be used simply to rename a file, or...

mv filea fileb... directory
~~~~~~~~~~~~~~~~~~~~~~~~~~
[mv] can also be used to move files to a new directory, provided the directory exists, and you have write access to it.

ps -options
~~~~~~~~~~
The [ps] command, by itself, displays the status of each active process controlled by your terminal. This status report includes the Process Identification Number (PID), the terminal (TTY), the time the process has been executing (TIME), and the command line used to execute the process (CMD).
[ps]'s three options include -a (displays info. on active processes controlled by any terminal), -x (info. on ALL active processes), and -l (an extensive status report on all active processes).

pwd
~~~
[pwd] command displays the present working directory.

rm filename
~~~~~~~~~~
[rm] removes a file. More than one file can be specified.

rmdir directoryname
~~~~~~~~~~~~~~~~~~
This utility removes a directory, an EMPTY directory (save the hidden files).

sleep seconds
~~~~~~~~~~~~
The [sleep] utility causes a process to become inactive for a certain period of time. Max. seconds is 65,536 (about 18 hrs).
~~~~~~~~~~~~

sort -options filenames
~~~~~~~~~~~~~~~~~~~~~~
[sort] merges and sorts files. Without options, [sort] orders files by the ASCII codes of the characters at the beginning of each line. Options include -b (leading blanks ignored), -d (only letters, digs, and blanks considered; "dictionary sort"), -f (case ignored), -n (numerical sort [for numerical data]), and -r (a reverse sort).

split -size original resulting
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
[split] divides a large file into smaller ones. [size] refers to the number of lines the resulting files contain, [original] is the name of the orig. file, and [resulting] represents the prefix name assigned to the newly created files.

umask ugo
~~~~~~~~~
[umask] changes the file CREATION mask (see [chmod] for already existing files). Here, [u] represents the owner's access permission, [g] the group's a.p., and [o] the a.p. for all others.

[uucp] (UNIX to UNIX copy) can be used to send files to a remote UNIX, or retrieve files from the remote system. Other UNIX comm commands include [cu] (which establishes contact with another system), and [uux] (UNIX to UNIX execute; allows commands to be executed on a remote system).

wc -options filenames
~~~~~~~~~~~~~~~~~~~~
The [wc] utility displays file-size information. This includes the number of lines, words, and characters. By chosing the -l, -w, or -c options, the information can be limited to only line, word, or character number.

who
~~~
A very useful command (which some systems respond to even before a user is actually logged on), [who] displays a list of users currently online. This list includes the user's name, terminal
~~~

device # (tty), and the log-in time. [who am i] displays info.
only on the user who executed the command.

Chapter 3 - Default Unix Logins

login:	Password:
root	root,system,etc..
sys	sys,system
daemon	daemon
uucp	uucp
tty	tty
test	test
unix	unix
bin	bin
adm	adm
who	who
learn	learn
uuhost	uuhost
nuucp	nuucp

guest

unpassworded

Chapter 4 - Getting the Passwords

One of the first things done on the system is print up or capture (in a buffer) the file containing all user names and accounts. This can be done by issuing the following command:

cat /etc/passwd

If you are successful you will a list of all accounts on the system. It should look like this:

root:hvnsdcf:0:0:root dir:/:
joe:majdnfd:1:1:Joe Cool:/bin:/bin/joe
hal::1:2:Hal Smith:/bin:/bin/hal

The "root" line tells the following info :

login name=root
hvnsdcf = encrypted password

0 = user group number
0 = user number
root dir = name of user
/ = root directory

In the Joe login, the last part "/bin/joe " tells us which directory is his home directory (joe) is.

In the "hal" example the login name is followed by 2 colons, that means that there is no password needed to get in using his name.

Chapter 5 - Sending Anonymous E-mail

Get into the normal unix shell and type telnet. That should bring up the following prompt:

telnet>

type "open localhost 25". It should bring up a whole bunch of garbage, then type

"mail". You will get more garbage. Ignore it and type "send to:xxxxx@xxxxx.xxx (whoever you want to send to)"

type "rcpt to:xxxx@xxx.xxx (whoever you want the mail to appear from)". Now type the message by typing "data", and then the message you want to send. End it with a "." on a new line.

It will fool the average user, but will cause suspition with sysops, etc.

Please send comments about this text and any additions you can think of to pp_123@Hotmail.com