Security – Linux Command Line Primer

About This Document:

***Add Type conventions-Command syntax-common ports-ethics-license-remoteconnectivity(ssh,telnet)-Packagemanager-Networking**

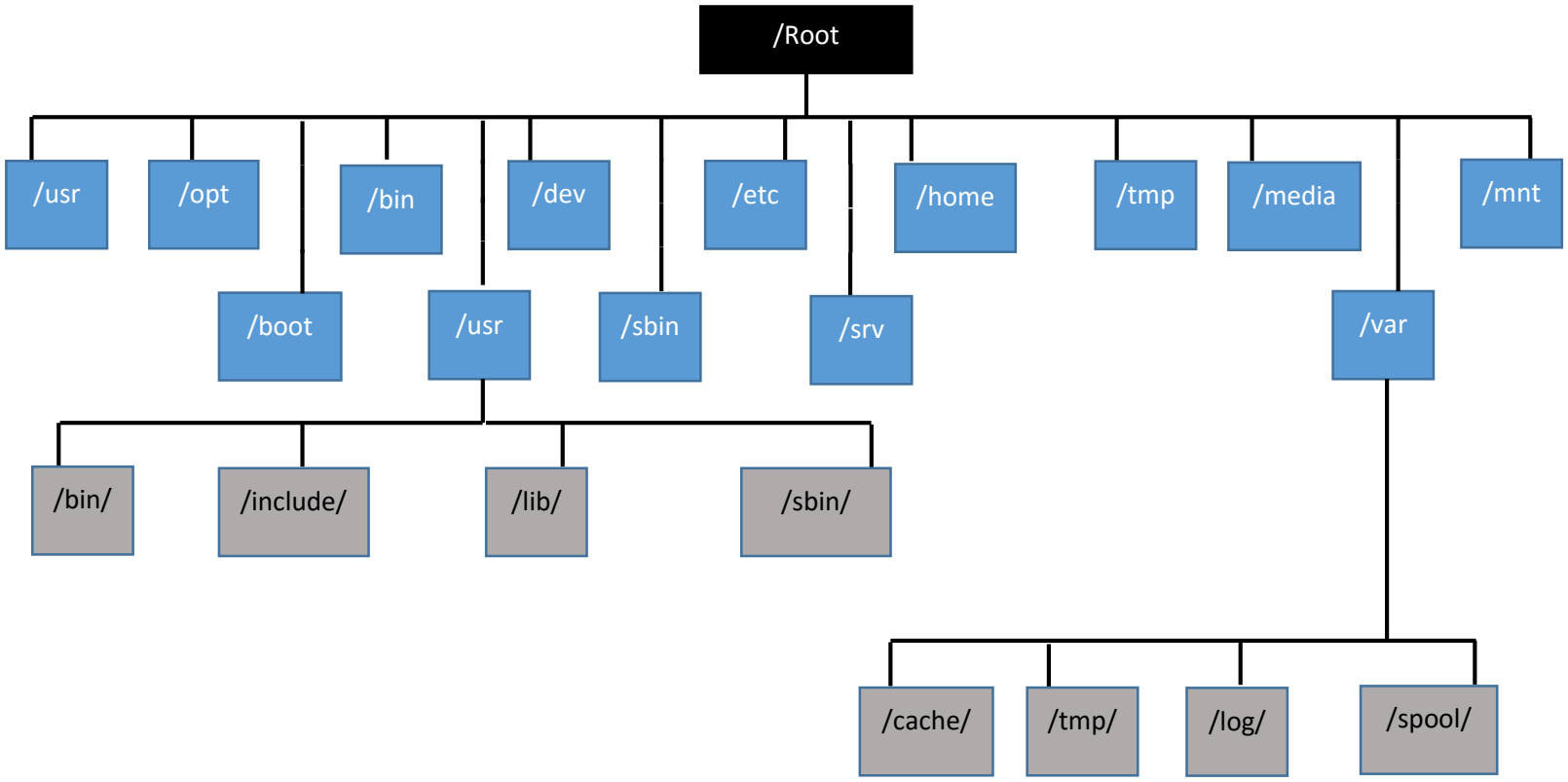
The newest version of Kali Linux (Kali 2.0) is based upon the Debian distribution, whereas the predecessor Back|Track was based on Ubuntu. As a result, the majority of the content is specific to debian distros. For a more complete and distro agnostic overview, check out The Linux Command Line by William E. Shotts (http://linuxcommand.org/tlcl.php/) available for free as a pdf. It's a great starting point for just about anyone. The book is available in print and eBook format from No Starch Press, an awesome publishers of books on technical subjects[1]. If you really want to dive deep into the linux world, EDX offers a free linux course curated and run by the Linux foundation. (Insert url). I personally took this course and found it to be a great indepth introduction.

Changing the default Kali Linux password:

Kali is a little strange as root access is permitted by default. Most commonly used distros (Ubuntu, Mint, ect) do not allow this as it can be a huge security vulnerability. When you first fire up your kali image your default password should be "toor". It's probably a very good idea to change the default password to a unique one the first time you start your Kali Linux VM[2].

1. Enter a terminal window.
2. Your prompt should look something like [*root@kali:~#*]. Go ahead and enter the command [*passwd root*].
3. You will then be asked to enter your new password twice. After successfully entering your new password the prompt will alert you that the password change was successful.
4. Log out via the GUI, then log back in using you new password

Filesystem Hierarchy



/root Filesystem

/bin	Binaries for user commands
/boot	Static files of the boot loader
/dev	Device files
/etc	Host-specific system configuration
/home	User home directories
/lib	Essential shared libraries and kernel modules
/media	Mount point for removable media
/mnt	Mount point for temporarily mounted filesystems
/opt	Add-on application software packages
/root	Home directory for the root user
/sbin	System binaries
/srv	Data for services provided by the system
/tmp	Temporary files

/var Hierarchy

/var/account	Process accounting logs
/var/cache	Application cache data
/var/cache/fonts	Locally-generated fonts
/var/cache/man	Locally-formatted manual pages
/var/crash	System crash dumps
/var/lib	Variable state information
/var/lock	Lock files
/var/log	Log files and directories
/var/mail	User mailbox files
/var/opt	Variable data for /opt
/var/run	Run-time variable data
/var/spool	Application spool data
/var/tmp	Temporary files preserved between system reboots
/var/yp	Network Information Service (NIS) database files

/usr Hierarchy

/usr/X11R6	X Window System
/usr/bin	Most user commands
/usr/include	Directory for standard include files
/usr/lib	Libraries for programming and packages
/usr/local	Local hierarchy
/usr/sbin	Non-essential standard system binaries
/usr/share	Architecture-independent data
/usr/share/dict	Word lists
/usr/share/misc	Misc. Architecture-independent data
/usr/share/sgml	SQML data
/usr/share/xml	XML data
/usr/src	Source code

***From** http://www.pathname.com/fhs/pub/fhs-2.3.pdf

Syntax of Terminal commands

[*Command*] [*options*] [*arguments*]

EX: *ping –c 10.0.54.11*

Where Ping is our command, -c is our selected option, and the IP address 10.0.54.11 is the argument we pass to be evaluated by the command

Navigating the filesystem

Essential to working in Kali Linux, Especially necessary if your target is also a Linux box

The command line has a ton of built in help options. Most of which are easily accessed by entering the command with *–h* or - - *help* as an option

Man (manual) pages are a great resources, try to consult the man page of a command before looking elsewhere:

To use Man pages:

Enter *man ,* followed by the command in question.

Navigating the command line

pwd – Print working directory, returns the current directory you are working in.

ls – List dependent files and directories (similar to "dir" in Windows command prompt)

Common ls options:

-a	show all
-r	Reverse order
-t	sorted by last modified
-S	Sorted by (File) size
-l	Long list, Includes ownership, permissions, last modified, etc * confirm if true

cd – change directory, move through the file system. Enter cd ../ to return to previous directory. Enter cd ~ to return to the user home directory. (EX: cd ~Jeff will return you to the home directory of the username jeff)

mkdir – make directory, create a new directory. Very similar to the Windows Command prompt md

rmdir – remove directory, Remove (delete) current directory

rm – remove (delete) file
EX: *rm file.txt*
Will delete file.txt

cat – Concatenate files/output:
EX: *cat file1.txt file2.txt* will copy the concatenate the contents of file1.txt to file2.txt

mv – move file: mv [filename] [Destination]
EX: *mv file1.txt Documents* will move relocate file1.txt to the documents directory.
cp – copy
EX: *cp file.txt file2.txt*
The contents of file.txt is copied to file2.txt

passwd – See above example, changing default root password

useradd – add an additional (new) user.
EX: *useradd jeff* will create a new user with the name jeff. Follow the passwd example to create and set a unique password for your new user

whoami – Self-explanatory, returns username you are currently operating under.

su – switch user
EX: By default you should be logged as root. To confirm you are logged in as root, enter the *whoami* command. If you followed the above *useradd* example you should also have a user account titled jeff. To switch to this account, enter *su jeff.* If you also set a password for the user account you will be asked to enter before being allowed access. Again, enter the *whoami* command to confirm that you are now signed in as jeff.

cal – Returns a basic calendar with the current day highlighted.
top – returns real time running processes (Think task manager)

ps – snapshot of running processes.

The two above command will provide you with a pid, or process id. Use this to complete the following two kill commands
kill – terminate a running process,
EX: to kill the process with the pid 001634 enter
kill 1634
pkill – terminates process with the name passed as argument *
EX: To kill the process with the name daemon7.exe enter, *pkill daemon7.exe*

killall – Kills all processes with a name that begins with the name passed as argument*

File Permissions and ownership

---

chmod – change mode of file

EX: chmod 741 file.txt

chown – change owner of file

In the command line, file permissions are tracked via a series of numbers divided into three groups

-xxx , Where the first digit represents owner permission, second digit represents group permissions, and third represents permissions for everyone

Three main categories of permission

Read (r) can also be represented numerically as 4

Write (w) can also be represented numerically as 2

Execute (x) can also be represented numerically as 1

Numerical representations of the permissions can be used to quickly change file permissions. To illustrate how this works, create a directory name workspace {mkdir workspace} then move into the workspace directory. {cd workspace}. Make a file named example1.txt {touch example1.txt} and a file named example2.txt {touch example2.txt}. Enter the long form ls command {ls –l} take note of the file permissions (Both should look some like " –rw-r—r—" , translated in order, means owner has read and write permissions, group has read permission, and everyone has read permission. "). Enter {chmod 741 example1.txt} and {chmod 111 example2.txt}. Again, view the contents of the directory {ls –l} and note the changes in file permissions.

Networking in Kali Linux

Network settings are located in /etc/network/interfaces

Ifconfig – View current network settings. This is very similar to the *ipconfig* command in windows.

eht0 – the First Ethernet connection

lo – loopback interface

wlan0 – first wireless network interface

Useful *ifconfig* options

-a - All network interfaces (including inactive connections)

-v – Verbose mode, displays additional information

promisc – Enables promiscuous mode. Interface will receive all packets on the network.

To Disable, enter –promisc

Iwconfig -

Remote Connectivity in linux:

Telnet and SSH

Useful Keyboard shortcuts:

Need a new terminal window? CTRL + SHIFT + a + n

Want to halt a running Command? CTRL + c

Need to pause/sleep a program? CTRL + z

Need to search your previous command history? CTRL + r

Appendix:

Footnotes:

1. *Don't change default passwords on Poland's vms.*

2. *They will also donate 30% of your purchase total to the EFF if you use the code ISUPPORTEFF at checkout.*