Linux that matter

Introduction to Basic Linux
CEH, iLab Africa Strathmore.
By John (Troon) O.

The $HELL

It is a program that interprets the commands.

- If the command is valid then the shell directs the kernel to carry out the request
- If invalid then an error message is displayed.
- Shell starts when an user logs in, and terminates when the user logs out.
- Presence of shell is indicated by a special symbol known as the shell prompt ($ or #)
- Several shells are available to handle the same hardware in different ways.
- Redirection of data : the shell facilitates chaining or "pipelining" of commands, i.e. the output of one program flows down the pipe and becomes an input to the next program

Bourne shell

- Bourne shell or Standard shell (sh) :

  – Introduced in 1978 and is widely used in AT&T Unix.

  – Gives "$" as the prompt to the user and " # " to the superuser (root).

Basic Commands

cd Change directories date Display time & date

echo Display text on your screen

grep Is a pattern-recognition command.

history Gives you the commands entered previously by users. ***$ history –3***

passwd To change users password

pwd Display present working directory

uname Display the machines symbolic name

More basic commands

Whereis - As the name of this command indicates, whereis will give you the exact location of the executable file for the utility in question.

$ whereis who: /usr/bin/who /usr/share/man1.z/who.1$

which - Enables you to find out which version of a command the shell is using. ***$ /bin/cat$$ which cat***

who - Display list of all the users currently logged into the system.

Whoami - Indicates who you are logged in as.

I/O redirects

- **<** Redirects standard input
- **>** Redirects standard output
- **>>** Appends standard output to a file
- **<<** Appends standard input to a file
- **2>** Redirects standard error

Files in Linux

- **Ordinary files**
  - These files can contain text, data, or programs.

- **Directories**
  - Directories contain files & directories.

- **Special file**
  - These files are use for input/output devices such as printers and terminals.

- **Linking Files**
  - A symbolic link is a pointer to another file.

  $ ln clear cls

File Permission

SYMBOLIC	OCTAL NUMBER	DESCRIPTION
---	0	No privileges
-- x	1	Execute only
-w-	2	Write only
-wx	3	Write & execute
r--	4	Read only
r-x	5	Read & execute
rw-	6	Read & write
rwx	7	Read, write & execute

Important Directories

/bin – user binaries

/boot – Boot-up related files

/dev – Interface for system devices

/etc – System configuration files

/home – Base directory for user files

/lib – Critical software libraries

/opt – Third party software

/proc – System and running programs

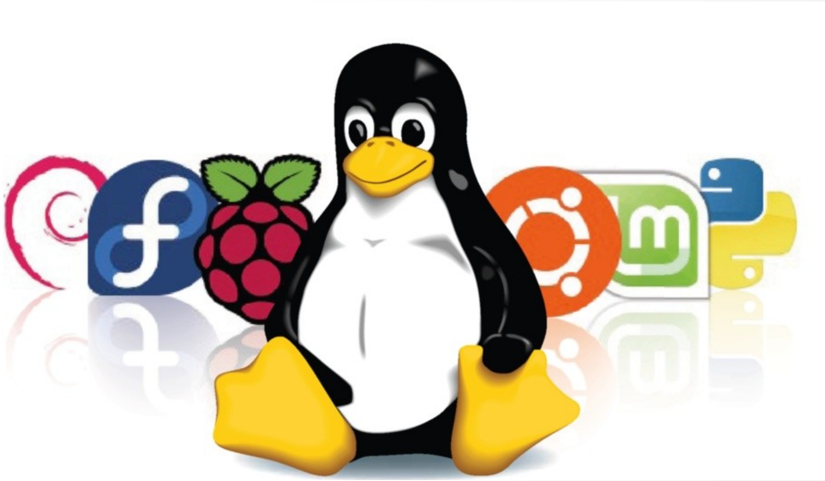
/root – Home directory of root user

/sbin – System administrator binaries

/tmp – Temporary files

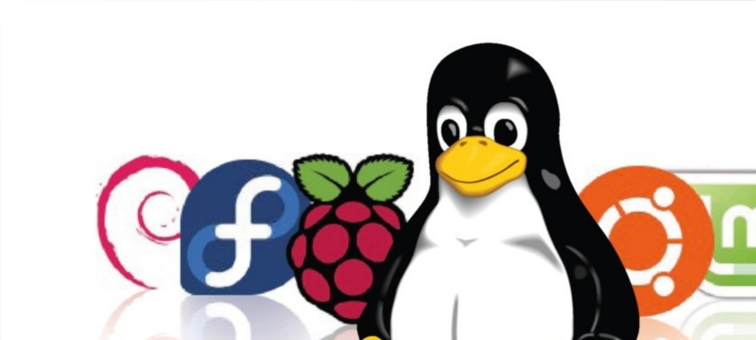
/usr – Less critical files

/var – Variable System files



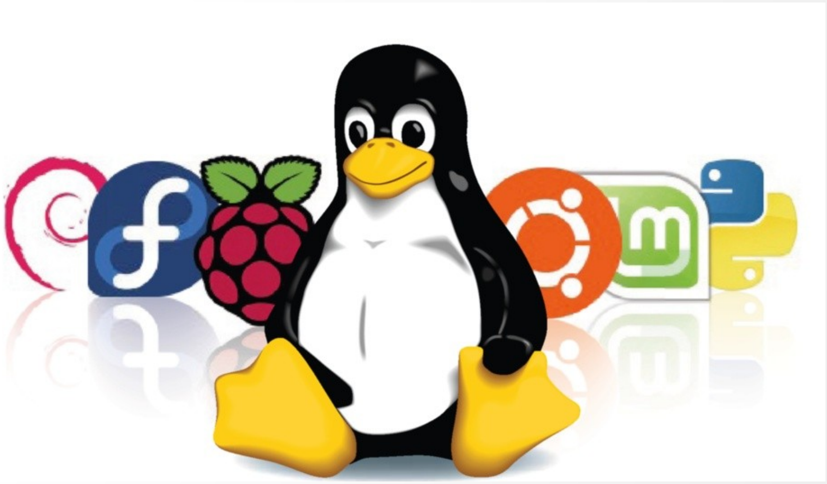
File you should know..

/etc/shadow	Local users' hashes
/etc/passwd	Local users
/etc/group	Local groups
/etc/hosts	known hostnames & IPs
/etc/network/interfaces	Networking Configurations
/**etc/apt/sources.list**	Debian/Ubuntu sources list
/etc/resolv.conf	Nameserver configuration
/home/use/.bash_history	Bash history (/root/ too)
-/.ssh/	SSH keystore
/var/log/	System log file (for most linux)
/etc/fstab	Static file system info



Linux System Info

Nbtstat -A ip-address	Get hostname for ip
id	Current Username and UID
w	Logged on users
who -a	User information
last -a	Last User logged on
ps -ef	Process lisitng (top)
df -h	Disk usage (free)
uname -a	Kernel version/CPU in
mount	Mounted file system
getent passwd	Show list of users
kill pid	Kills process with pid
cat /etc/issue	**S**how OS info
cat /etc/'release'	Show OS version info
cat /proc/version	Shows Kernel info



Network Commands

watch ss -tp	Network connections
netstat -ant	Tcp connections **-anu=udp**
netstat -tulpn	Connections with PIDs
lsof -i	Established connections
smb:// ip /share	Access windows smb share
share user x.x.x.x c$	Mount Windows share
smbclient -u user \\\\ ip \\ share	SMB connect
ifconfig eth# ip / cidr	Set IP and netmask
ifconfig eth0:1 ip / cidr	Set virtual interface
route add default gw gw_ip	Set GW

Cont... Network commands

ifconfig eth# mtu [size]	Change MTU size
macchanger -m MAC int	Change MAC
iwlist int scan	Built-in wifi scanner
dig -x ip	Domain lookup for IP
host ip	Domain lookup for IP
ip xfrm state list	Print existing VPN keys
/var/log/messages I grep DHCP	List DHCP assignments
echo "1" /proc/sys/net/ipv4/ip_forward	Turn on IP Forwarding
echo "nameserver x.x.x.x" /etc/resolv.conf	Add DNS Server

Utility Commands

- **wget http:// url -0 url.txt -o /dev/null** Grab url
- **rdesktop ip** Remote Desktop to ip
- **scp /tmp/file user@x.x.x.x:/tmp/file** put-file
- **scp user@ remoteip :/tmp/file /tmp/file** Get file
- **useradd -m user** Add user
- **passwd user** Change user password
- **rmuser uname** remove user
- **apropos subject** Find related command
- **history** view user command history
- **! num** Executes line num in history

File Commands

touch filename	creates a file
diff file1 file2	compare files
shred -f -u file	**o**verwrite/delete file
mount /dev/sdb# /mnt/usbkey	**m**ount USB
sudo fdisk -l	list connect drives
echo -n “string” | md5sum	md5 hash
md5sum -t file	compute md5 hash
sort -u	sort/show unique lines
split -b 9K file prefix	split file into 9k chunks
file afile	determine file type/info
tar cf file.tar files	creates a .tar file from files
tar xf file.tar	extract .tar file

Cover your tracks

- **echo " " /var/log/auth.log** clear auth.log file
- **echo " " ~/.bash history** clear user bash history
- **rm ~/.bash_history -rf** delete .bash_history file
- **history -c** clear current session history
- **export HISTFILESIZE=0** set history max lines to 0
- **export HISTSIZE=0** set histroy max commands to 0 (should logout to take effect)
- **Kill -9 $$** Kills current session
- **ln /dev/null ~/.bash_history -sf** permanently send all bash history commands to /dev/null

root@host:~#echo “end!”

QUESTION(S)?

QUESTION(S)?

QUESTION(S)?

QUESTION(S)?

QUESTION(S)?

QUESTION(S)?

QUESTION(S)?