Recap Terminal Commands: Windows and Linux

Reading

25 minutes

Status	Incomplete

Introduction

This section provides you with tables outlining the most important terminal commands for Linux and Windows. It will take some time to learn these commands so having these tables easily available will help you when you are getting started. As you use these commands more frequently during practice, you will find that it becomes easier to remember.

> Bookmark this page, or add these tables to your notes for easy future reference.

Important Linux Commands

In the next few tables, you will learn about the most important **terminal Linux commands** and use them as a cheat sheet to remember them.

SYSTEM INFORMATION

man	Display the manual of the command with examples
uname -a	Display Linux system information
uname -r	Display kernel release information
uptime	Show how long the system has been running
hostname	Show system host name
last reboot	Show system reboot history
date	Show the current date and time

cal	Show this month's calendar
w	Display who is online on the OS
whoami	Who you are logged in as

HARDWARE INFORMATION

dmesg	Display messages from kernel
cat /proc/cpuinfo	Display CPU information
cat /proc/meminfo	Display memory information
free -h	Display free and used memory
lspci -tv	Display connected devices (PCI)
lsusb -tv	Display USB devices
dmidecode	Display DMI/SMBIOS (hardware info)
hdparm -i /dev/sda	Show info about disk sda
hdparm -tT /dev/sda	Speed test read/write on disk sda
badblocks -s /dev/sda	Test for unreadable blocks on disk sda

USER INFORMATION AND MANAGEMENT

sudo	Command to change the privilege of execution of software
id	Display the user and group ids of current user
last	Display the last users who have logged in
who	Show who is logged into the system
w	Show who is logged in and what they are doing
groupadd test	Create a group named "test"
useradd -c "Student Cyber" -m student	Create an account named student, with a comment of "Student Cyber" and create the user's home directory
userdel student	Delete the student account
usermod -aG cyber_lab student	Add the student account to the cyber_lab group

FILE AND DIRECTORY COMMANDS

ls -al	List all files in a detailed format
pwd	Display the current working directory
mkdir directory	Create a directory
rm file	Remove (delete) file
rm -r directory	Remove the directory and its contents recursively
rm -f file	Force removal of file without prompting for confirmation
rm -rf directory	Forcefully removes directory recursively
cp file1 file2	Copy file1 to file2
cp -r source destination	Copy source recursively to destination. If a destination exists, copy the source directory into the destination. Otherwise, create a destination with the contents of the source directory.
mv file1 file2	Rename or move file1 to file2. If file2 is an existing directory, move file1 into directory file2
ln -s /path/to/file linkname	Create a symbolic link to the link name (shortcut)
touch file	Create an empty file or update the access and modification times of the file
cat file	View the contents of file
less file	Browse through a text file
head file	Display the first 10 lines of file
tail file	Display the last 10 lines of file
tail -f file	Display the last 10 lines of the file and "follow" the file as it grows

PROCESS MANAGEMENT

ps	Display your currently running processes
ps -ef	Display all the currently running processes on the system
ps -ef |	grep process
top	Display and manage the top processes
htop	Interactive process viewer (top alternative)
kill <pid>	Kill process with the process ID of pid

killall <process_name>	Kill all processes named process_name
<program> &	Start program in the background
bg	Display stopped, or background jobs
fg	Brings the most recent background job to foreground
fg n	Brings job n to the foreground

FILE PERMISSIONS - Linux chmod Example

PERMISSION	EXAMPLE
U G W	
rwx rwx rwx	chmod 777 filename
rwx rwx r-x	chmod 775 filename
rwx r-x r-x	chmod 755 filename
rw- rw- r--	chmod 664 filename
rw- r-- r--	chmod 644 filename
LEGEND	
U = User	
G = Group	
W = World	
r = Read	
w = write	
x = execute	
- = no access	

NETWORKING

ip a	Display all network interfaces and IP addresses
ip addr show dev eth0	Display eth0 address and details
ethtool eth0	Query or control network driver and hardware settings
ping host	Send ICMP echo request to host

whois domain	Display whois information for domain
dig domain	Display DNS information for domain
dig -x IP_ADDRESS	Reverse lookup of IP_ADDRESS
host domain	Display DNS IP address for domain
hostname -i	Display the network address of the host name
hostname -I	Display all local IP addresses of the host
wget http://domain.com/file	Download http://domain.com/file
netstat -nutlp	Display listening tcp and udp ports and corresponding programs
traceroute domain.com	Display the route to access the domain.com

ARCHIVES (TAR FILES)

tar cf archive.tar directory	Create tar named archive.tar containing directory
tar xf archive.tar	Extract the contents from archive.tar
tar czf archive.tar.gz directory	Create a gzip compressed tar file name archive.tar.gz
tar xzf archive.tar.gz	Extract a gzip compressed tar file
tar cjf archive.tar.bz2 directory	Create a tar file with bzip2 compression
tar xjf archive.tar.bz2	Extract a bzip2 compressed tar file

SEARCH

grep pattern file	Search for pattern in file
grep -r pattern directory	Search recursively for pattern in directory
locate name	Find files and directories by name
find /home/student -name 'prefix*'	Find files in /home/student that start with "prefix"
find /home -size +100M	Find files larger than 100MB in /home

SSH LOGINS

ssh host	Connect to host as your local username

ssh user@host	Connect to host as user
ssh -p port user@host	Connect to host using port

FILE TRANSFERS

scp file.txt server:/tmp	Secure copy file.txt to the /tmp folder on server
scp server:/var/www/ * .html /tmp	Copy * .html files from server to the local /tmp folder
scp -r server:/var/www /tmp	Copy all files and directories recursively from server to the current system's /tmp folder
rsync -a /home /backups/	Synchronize /home to /backups/home
rsync -avz /home server:/backups/	Synchronize files/directories between the local and remote system with compression enabled

DIRECTORY NAVIGATION

cd ..	Change up one level of the directory tree
cd ../../	Change up two levels of the directory tree
cd	Go to the $HOME directory
cd -	Change to the last used directory
cd /etc	Change to the /etc directory

PERFORMANCE MONITORING AND STATISTICS

top	Display and manage the top processes
htop	Interactive process viewer (top alternative)
mpstat 1	Display processor related statistics
vmstat 1	Display virtual memory statistics
iostat 1	Display I/O statistics
tail -100 /var/log/messages	Display the last 100 Syslog messages
(/var/log/syslog for Debian-based systems)	
tcpdump -i eth0	Capture and display all packets on interface eth0

tcpdump -i eth0 'port 80'	Monitor all traffic on port 80 (HTTP)
lsof	List all open files on the system
lsof -u user	List files opened by user
free -h	Display free and used memory (-h for human readable, -m for MB, -g for GB)
watch df -h	Execute the command "df -h", showing periodic updates

DISK USAGE

df -h	Show free and used space on mounted filesystems
df -i	Show free and used inodes on mounted filesystems
fdisk -l	Display disk partition sizes and types
du -ah	Display disk usage for all files and directories in human-readable format
du -sh	Display total disk usage of the current directory

Important cmd Windows Commands

In the following tables, you will learn about the most important **cmd Windows commands** and use them as a cheat sheet to remember the commands.

SYSTEM INFORMATION

date	Show/set date
time	Display/edit the system time
ver	Display OS version
systeminfo	Display computer-specific properties and configurations
cls	Clear screen

USER INFORMATION AND MANAGEMENT

gpresult	Display group policies
gpupdate	Update group policies
prompt	Change command prompt

FILE AND DIRECTORY COMMANDS

dir	List directory content
attrib	Display file attributes
comp	Compare file contents
compact	Display/change file compression
copy / xcopy	Copy files
diskcomp	Compare content of two floppy disks
diskcopy	Copy floppy disk to another one
erase / del	Delete one or more files
expand	Extract files
fc	Compare files and display the differences
mkdir	Create a new directory
move	Move/rename files
rename	Rename files
replace	Replace files
rmdir / rd	Delete directory
tree	Display folder structure graphically
type	Display content of text files

PROCESS MANAGEMENT

taskkill	Terminate a process or an application
tasklist	Display applications and related tasks

NETWORKING

hostname	Display host name
w32tm	Setting time synchronization/time server/time zone
ftp	Transfer files to an FTP server

ftype	Display file type and mapping
getmac	Display MAC address
ipconfig	Display IP network settings
netsh	Configure/control/display network components
netstat	Display TCP/IP connections and status
nslookup	Query the DNS
pathping	Test the connection to a specific IP address
ping	Pings the network
route	Display network routing table, add static routes
telnet	Establish Telnet connection
tftp	Transfer files to a TFTP server
tracert	Trace routes similar to PathPing

SEARCH

find	Find files

DIRECTORY NAVIGATION

cd	Change directory

PERFORMANCE MONITORING AND STATISTICS

verify	Monitoring whether volumes are written correctly
perfmon	Start performance monitor

DISK USAGE

chkdsk	Check volumes
chkntfs	Display/change volume check at startup
defrag	Defragment media

diskpart	Volume management
driverquery	Display installed devices and their properties
format	Format volumes
label	Change volume name
mode	Configure interfaces/devices
mountvol	Assign/delete drive mount points
vol	Show volume description and serial numbers of the HDDs

Previous
Group Share and Feedback

Next
Understand the environment and Wireshark

W01D5

Fri Jun 28

Lectures (1)

Work (11)

7 hrs

- Traffic Monitoring
- Network Monitoring with Wireshark
- Intro to Network Baselines
- Visualizing What's Happening Lab - Windows Logging
- Group Share and Feedback
- Recap Terminal Commands: Windows and Linux
- Understand the environment and Wireshark
- Check the Commands
- Tech Interviews