Linux Commands

broala

Getting around

Command	Description
`cd logs`	Move to the logs directory, which is located in the **current** directory.
`cd /logs`	Move to the logs directory, which is located in the **top-level** directory.
`cd ..`	Move up one directory.
`cd ~`	Move to your home directory (the "tilde" character is left of the 1 key).
`cd -`	Move to the directory you were previously in.

Tip – Tab Completion

Use tab completion to type filenames faster.
As you're typing a filename (or directory), hit the tab key. If there's only one file that matches what you've typed, the rest of the filename will be filled in. If nothing happens when you hit tab, simply hit tab again to see a list of matches.

Viewing and searching in files

Command	Description
`cat data.txt`	Display data.txt
`cat *.txt`	Display all files that end with .txt
`head data.txt`	Display the **first** 10 lines of data.txt.
`head -n 20 data.txt`	Display the **first** 20 lines of data.txt.
`tail data.txt`	Display the **last** 10 lines of data.txt.
`tail -n 30 data.txt`	Display the **last** 20 lines of data.txt.
`tail -F data.txt`	Display the last 10 lines of data.txt and continue running, displaying any new lines in the file. *Note: Press Ctrl+C to exit.*
`grep malware data.txt`	Display all lines in data.txt that contain 'malware'.
`grep -v malware data.txt`	Display all lines that **do not** contain 'malware'.
`grep 'mal ware' data.txt`	To search for phrases with spaces, use single quotes.
`grep -F 1.2.3.4 data.txt`	To search for phrases with periods, use –F
`grep -c exe data.txt`	Display how many lines in data.txt contain 'exe' (but don't display them).
`grep -F -c 1.2.3.4 *.txt`	Display the number of lines with IP 1.2.3.4 in each file that ends in .txt.
`less large.file`	Display large.file in less (see right).
`less -S large.file`	Display large.file in less (see right), **and allow for side-to-side scrolling**.

Navigating in less

Key or Command	Description
`q`	Quit
`Up/down arrow`	Move up/down one line.
`Left/right arrow`	Move left/right half of a page. *Note: requires less –S*
`Page up/down`	Move up/down one page.
`g`	Go to the **first** line
`G`	Go to the **last** line
`F`	Go to the last line, and display any new lines (similar to tail –F). *Note: Press Ctrl+C to exit.*
`/malware`	Search - go to the next line containing the word 'malware.'
`/!malware`	Search – go to the next line **NOT** containing the word 'malware.'
`?malware`	Search – go to the previous line containing the word 'malware.'
`n`	Repeat a previous search.
`N`	Repeat a previous search, but in the opposite direction.

Putting it all together

Command	Description
`| (AKA "pipe")`	Pass the output of one command to another command. *Note: For the "pipe" character, use the key above enter (same key as backslash).*
`grep malware data.txt | tail -n 30`	Display the last 30 lines in data.txt that contain the word 'malware.'
`grep malware data.txt | grep blaster`	Display lines in data.txt that contain 'malware' **and also contain 'blaster.'**
`cat data.txt | sort`	Display data.txt, sorted alphabetically.
`cat data.txt | sort | uniq`	Display data.txt, sorted alphabetically, with duplicates removed.
`cat data.txt | sort | uniq -c`	Sort, remove duplicates, and display the number of times each line occurred.
`cat data.txt | sort | uniq -c | sort -n`	Sort, remove duplicates, and display the most frequent lines.
➔ `cat data.txt | sort | uniq -c | sort -n | tail -n 20`	Sort, remove duplicates, and display the 20 most frequent lines.
`cat conn.log | bro-cut id.resp_h proto service`	Only display the id.resp_h, proto and service columns of the conn Bro log.
`cat http.log | bro-cut -d ts method host uri`	Only display the timestamp, method, host and uri columns, **and convert the timestamp to human-readable format.**

Tip – Compressed Files

Files that end in .gz are compressed, and might require some different commands:

Command	Modification for .gz
cat or grep	Use zcat or zgrep.
head or tail	Use zcat | head or zcat | tail

Tip – Documentation

Linux commands are all well documented. To view the documentation:

- Run the command with --help (e.g. tail --help) to see the options.
- Use the manual pages for more detail (e.g. man tail). *Note: these open in less.*

Tip – Working With Big Files

Commands take longer to run on larger files. Some things to keep in mind are:

- Use grep –F instead of plain grep.
- For viewing the file, use less instead of cat.
- Try to use grep as early as possible, so if you pipe to other tools, there's less data to crunch.

In order to promote its wide distribution, this work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (http://creativecommons.org/licenses/by-nc-sa/4.0/). We at Broala are committed to helping you understand Bro to the fullest so you can be a monitoring hero.

© Broala LLC.

Basic Linux Commands

SYSTEM

uname -a =>Displaylinux system information
uname -r =>Display kernel release information
uptime =>Show how long the system has been running + load
hostname =>Show system host name
hostname -i =>Display the IP address of the host
last reboot =>Show system reboot history
date =>Show the current date and time
cal =>Show this month calendar
w =>Display who is online
whoami =>Who you are logged in as
finger user =>Display information about user

HARDWARE

dmesg =>Detected hardware and boot messages
cat /proc/cpuinfo =>CPU model
cat /proc/meminfo =>Hardware memory
cat /proc/interrupts =>Lists the number of interrupts per CPU per I/O device
lshw =>Displays information on hardware configuration of the system
lsblk =>Displays block device related information in Linux
free -m =>Used and free memory (-m for MB)
lspci -tv =>Show PCI devices
lsusb -tv =>Show USB devices
dmidecode =>Show hardware info from the BIOS
hdparm -i /dev/sda =>Show info about disk sda
hdparm -tT /dev/sda =>Do a read speed test on disk sda
badblocks -s /dev/sda =>Test for unreadable blocks on disk sda

USERS

id =>Show the active user id with login and group
last =>Show last logins on the system
who =>Show who is logged on the system
groupadd admin =>Add group "admin"
useradd -c "Sam" =>g admin -m sam #Create user "sam"
userdel sam =>Delete user sam
adduser sam =>Add user "sam"
usermod =>Modify user information
chgrp => Changes a users group

FILE COMMANDS

ls –al =>Display all information about files/ directories
pwd =>Show the path of current directory
mkdir directory-name =>Create a directory
rm file-name =>Delete file
rm -r directory-nam =>Delete directory recursively
rm -f file-name =>Forcefully remove file
rm -rf directory-name =>Forcefully remove directory recursively
cp file1 file2 =>Copy file1 to file2
cp -r dir1 dir2 =>Copy dir1 to dir2, create dir2 if it doesn't exist
mv file1 file2 =>Rename source to dest / move source to directory
ln –s /path/to/file-name link-name #Create symbolic link to file-name
touch file =>Create or update file
cat > file =>Place standard input into file
more file =>Output contents of file
head file =>Output first 10 lines of file
tail file =>Output last 10 lines of file
tail -f file =>Output contents of file as it grows starting with the last 10 lines
gpg -c file =>Encrypt file
gpg file.gpg =>Decrypt file
wc =>print the number of bytes, words, and lines in files
xargs =>Execute command lines from standard input

PROCESS RELATED

ps =>Display your currently active processes
ps aux | grep 'telnet' =>Find all process id related to telnet process
pmap =>Memory map of process
top =>Display all running processes
kill pid =>Kill process with mentioned pid id
killall proc =>Kill all processes named proc
pkill process-name =>Send signal to a process with its name
bg =>Resumes suspended jobs without bringing them to foreground
fg =>Brings the most recent job to foreground
fg n =>Brings job n to the foreground

FILE PERMISSION RELATED

chmod octal file-name =>Change the permissions of file to octal Example
chmod 777 /data/test.c =>Set rwx permission for owner,group,world
chmod 755 /data/test.c =>Set rwx permission for owner,rx for group and world
chown owner-user file =>Change owner of the file
chown owner-user:owner-group file-name =>Change owner and group owner of the file
chown owner-user:owner-group directory =>Change owner and group owner of the directory

NETWORK

ip addr show =>Display all network interfaces and ip address
ip address add 192.168.0.1 dev eth0 =>Set ip address
ethtool eth0 =>Linux tool to show ethernet status
mii-tool eth0 =>Linux tool to show ethernet status
ping host =>Send echo request to test connection
whois domain =>Get who is information for domain
dig domain =>Get DNS information for domain
dig -x host =>Reverse lookup host
host google.com =>Lookup DNS ip address for the name
hostname –i =>Lookup local ip address
wget file =>Download file
netstat -tupl =>Listing all active listening ports

COMPRESSION / ARCHIVES

tar cf home.tar home =>Create tar named home.tar containing home/
tar xf file.tar =>Extract the files from file.tar
tar czf file.tar.gz files =>Create a tar with gzip compression
gzip file =>Compress file and renames it to file.gz

INSTALL PACKAGE

rpm -i pkgname.rpm =>Install rpm based package
rpm -e pkgname =>Remove package

INSTALL FROM SOURCE

./configure
make
make install

SEARCH

grep pattern files =>Search for pattern in files
grep -r pattern dir =>Search recursively for pattern in dir
locate file =>Find all instances of file
find /home/tom -name 'index*' =>Find files names that start with "index"
find /home -size +10000k =>Find files larger than 10000k in /home

LOGIN (SSH AND TELNET)

ssh user@host =>Connect to host as user
ssh -p port user@host =>Connect to host using specific port
telnet host =>Connect to the system using telnet port

FILE TRANSFER

sftp 192.16875.2 =>Connect remote host
scp
scp file.txt server2:/tmp =>Secure copy file.txt to remote host /tmp folder
rsync
rsync -a /home/apps /backup/ =>Synchronize source to destination

DISK USAGE

df –h =>Show free space on mounted filesystems
df -i =>Show free inodes on mounted filesystems
fdisk -l =>Show disks partitions sizes and types
du -ah =>Display disk usage in human readable form
du -sh =>Display total disk usage on the current directory
findmnt =>Displays target mount point for all filesystem
mount device-path mount-point =>Mount a device

DIRECTORY TRAVERSE

cd .. =>To go up one level of the directory tree
cd =>Go to $HOME directory
cd /test =>Change to /test directory