SEC406 Lab Commands

COMMAND	EXPLANATION
ssh labD.L	Begin a Lab “L” from Day “D”
ssh del_labD.L	Reset the specified lab to start over
#?	Repeat the question for the current task
#hint	Get a hint on how to complete the task

Bash Keyboard Shortcuts

KEY COMBO	EXPLANATION
Control L	Clear the screen
Control C	Kill the currently running Program
Control S	Squelch (Pause the output)
Control Q	Un-squelch (Unpause the output)
Control A	Go to the beginning of the line
Control E	Go to the end of the lin
Control R	Recall a command by searching history
Up Arrow	Recall the previous command from history
Down Arrow	Go to next command in the command history

SANS
CYBER DEFENSE

Linux Essentials Cheat Sheet v1.0

This guide was created by Mark Baggett
Twitter: @markbaggett | sans.org/sec406

Windows User Quick Reference

WINDOWS COMMAND	UBUNTU LINUX EQUIVALENT	WHAT IT DOES
dir	ls -la	A directory listing with sizes and dates
ipconfig.exe	ifconfig or ip	Show you network interfaces and addresses
ipconfig/release	dhclient -r	Release your DHCP ip address
ipconfig /renew	dhclient	Request a new IP from DHCP server
cd <new dir>	cd <new dir>	Change directories to new directory
cd<enter>	pwd	Tell you the current working directory
tasklist	ps	List processes running
type	cat	Show the contents of a file
findstr	grep	Search output for a matching string
copy	cp	Copy a file from the file system
echo	echo	Echo output to the screen
del	rm	Delete a file from the file system
rename	mv	Rename a file

File System Commands

COMMAND	EXPLANATION	EXAMPLE
ls	List files in directory; current directory is used if no directory is supplied	$ ls ~/Desktop
cd	Change the current working directory	$ cd /home/me/
pwd	Print the current working directory	$ pwd /home/me/
cp	Copy a file	$ cp orig.txt copy.txt
mv	Move or rename a file	$ mv a.txt Desktop/b.txt
rm	Delete a file	$ rm file.txt
mkdir	Create a directory	$ mkdir examples/
rmdir	Delete a directory (must be empty)	$ rmdir examples/
find	Search the file system for files	$ find / -name "myfile.txt"
chmod	Change file permissions	$ chmod 755 myfile.txt
Touch	Create an empty file	$ touch new_empty_file

User Switching Commands

COMMAND	EXPLANATION	EXAMPLE
su	su – otheruser	Switch to otheruser and use their user environment
su	su otheruser	Switch to otheruser and keep your existing environment
sudo	sudo <cmd>	Run command as another user, when no user is specified it assumes root
whoami	whoami	Tell you the name you are running processes as
id	id	Display the user information including user number and group number
visudo	visudo	Edit the /etc/sudoers file to define who can run what as other users (root only)

Network Commands

COMMAND	EXPLANATION	EXAMPLE
ping	Send ICMP ECHO_REQUEST to a network host to test connectivity	$ ping 10.1.1.1
netstat	Display TCP & UDP connection info (deprecated)	$ netstat -na
ss	Display socket statistics; replaces netstat	$ ss –l4t
ifconfig	Display information about your network interfaces, such as your IP address (deprecated)	$ ifconfig
ip	Display/manipulate routing, network devices, interfaces, and tunnels; replaces ifconfig	$ ip a show [interface] $ ip address show ens33

File Examination Commands

COMMAND	EXPLANATION	EXAMPLE
cat	Print one or more files to STDOUT	$ cat file.txt $ cat file1 file2 file3 > allfiles
grep	Search for text within a file or STDIN	$ grep 10.10.1.1 /var/log/apache/*
file	Identify the file type	$ file image.jpg image.jpg: JPEG Image Data
head	Display the first 10 lines of a file, by default (use "-n X" to display first X lines)	$ head /etc/passwd $ head -n 5 /etc/passwd
tail	Display the last 10 lines of a file, by default (use "-n X" to display last X lines)	$ tail /var/log/syslog $ tail -n 5 .bashrc
tail -F	Display new data as it's appended to the end of a file (useful for watching logs; aka follow a file)	$ tail -F /var/log/messages
less	Display text from STDIN or a file, one screen at a time; text disappears from console	$ less /etc/passwd $ cat file | less
more	Display text from STDIN or a file, one screen at a time; text remains on console	$ more /etc/passwd $ cat file | more

Other Important Commands

COMMAND	EXPLANATION	EXAMPLE
chmod	Change the permissions (mode) of a file or directory	$ chmod +w file.txt
stat	View detailed information about a file	$ stat file.txt
passwd	Change a user's password, or your own if no username is specified	$ passwd [username]
kill	Terminate or send a signal to a running process by process ID (PID)	$ kill 8573
ln	Create a hard or symbolic link to a file	$ ln [file] [link]
sort	Sort the contents of a file or STDIN	$ sort /etc/passwd $ cat numlist.txt | sort –n
uniq	Remove duplicate lines from a sorted file or sorted STDIN	$ uniq mylist.txt $ cat mylist.txt | uniq
which	Identify which program on your drive executes when you run a command	$ which python /usr/bin/python

HFS Common Locations

/	Root of the file system
/etc	"etcetera" folder holds configuration files
/var	"variable" folder holds files that change frequently
/usr	"Universal System Resources" is a Distributed mount folder that holds binaries (installed programs)
/opt	"options" folder is usually where compiled pages not installed by a package manager go
/dev	"devices" is a dynamic folder for accessing system hardware devices
/root	The root users home folder
/home	All other users home folders