



ZERO TO LINUX

Hal Pomeranz

WHO IS HAL POMERANZ?

Unix user since 1985 – first system was BSD SunOS on a Sun 3/50

Spent 20 years doing System/Network/Security Admin

Recently it's been Forensics and Incident Response, Expert Witness

Wouldn't be here without some great mentors

hrpomeranz@gmail.com

@hal_pomeranz@infosec.exchange



Attribution-ShareAlike
CC BY-SA



COMMAND LINE SKILLS ARE FOR...

Penetration testing

Post-exploitation

System and Network administration

DevOps and automation

Forensics and incident response

Data transformation

The background features abstract, flowing, ribbon-like shapes in shades of green and orange, creating a sense of movement and depth. The green shapes are primarily on the left and bottom, while the orange shapes are on the right and top. The central area is white, providing a clean space for the text.

GETTING AROUND

WELCOME TO LINUX!

/								
/usr	/bin	/lib	/etc	/dev	/tmp	/var	/home	/root
/usr/bin /usr/lib /usr/local /usr/local/bin /usr/local/lib				/dev/shm		/var/tmp	/home/<USER> ★	
						/var/log		

You are here



THERE'S NO PLACE LIKE HOME

```
[lab@LAB ~]$ pwd
```

```
/home/lab
```

```
[lab@LAB ~]$ ls
```

```
Desktop  Documents  Downloads  Exercises  Music  Pictures  Public  Templates  Videos
```

```
[lab@LAB ~]$ ls -a
```

.	.bash_history	.bashrc	.esd_auth	.pki	Downloads	Pictures	Videos
..	.bash_logout	.cache	.local	Desktop	Exercises	Public	
.ICEauthority	.bash_profile	.config	.mozilla	Documents	Music	Templates	

```
[lab@LAB ~]$
```


TRAVELING AND RETURNING

```
[lab@LAB ~]$ cd /var/tmp
```

```
[lab@LAB tmp]$ pwd
```

```
/var/tmp
```

```
[lab@LAB tmp]$ cd
```

```
[lab@LAB ~]$ pwd
```

```
/home/lab
```

```
[lab@LAB ~]$
```

ABSOLUTE VS RELATIVE

You start in:	/home/lab
You type:	cd /home/lab/Pictures
You finish in:	/home/lab/Pictures
You start in:	/home/lab
You type:	cd Pictures
You finish in:	/home/lab/Pictures

EXTRA TRICKS

.	(current directory)	./myprog <i>(run myprog from current dir)</i> cp /etc/passwd . <i>(make a copy of /etc/passwd in current dir)</i>
..	(directory above)	cd /var/tmp; cp ../log/messages . <i>(copies /var/log/messages to /var/tmp)</i> cat ../../../../../../../../etc/passwd <i>(likely directory traversal attack)</i>
~<user> ~/<file>	(home directory of <user>) (file in your home directory)	cp ~testuser/.bash_history /tmp <i>(copies testuser's command history to /tmp)</i> cp ~/.bash_history /tmp <i>(copies your command history to /tmp)</i> cd ~/Pictures <i>(go to Pictures dir in your home directory)</i>

TAB COMPLETION

Faster

Helps catch errors

```
[lab@LAB tmp]$ cd ~/Do<Tab><Tab>  
Documents/ Downloads/  
[lab@LAB tmp]$ cd ~/Dow<Tab>  
[lab@LAB Downloads]$ pwd  
/home/lab/Downloads  
[lab@LAB Downloads]$
```

→ Becomes *cd ~/Downloads/*

LAB – DIRECTORY JEOPARDY!

There's usually more than one right answer



The background features abstract, flowing waves in shades of green and orange. The green waves are on the left and bottom left, while the orange waves are on the right and bottom right. The waves have a soft, ethereal quality with some transparency, creating a sense of movement and depth.

BASIC COMMANDS

FILE MANIPULATION

cp <i>(copy file/directory)</i>	cp passwd passwd.bak <i>(make a copy here)</i> cp .bash_history /tmp <i>(make a copy over there)</i> cp passwd shadow group /root <i>(copy multiple files to another directory)</i> cp -r /var/log /tmp <i>(copy an entire directory)</i>
mv <i>(rename or move file/directory)</i>	mv ssl.crt old.crt <i>(rename a single file)</i> mv /root/.ssh/authorized_keys /evidence <i>(move a file to a new directory)</i> mv /root/.ssh /evidence/root-dotssh <i>(move directory to a new location&name)</i>
rm <i>(remove file/directory)</i>	rm passwd.bak <i>(remove unneeded file)</i> rm -r /tmp/log <i>(remove directory)</i>

THE MANY FACES OF LS

Display	Sorting
ls -a <i>(show "hidden" files)</i>	ls -t <i>(sort by modified time)</i>
ls -A <i>(show "hidden" files w/o "." & "..")</i>	ls -u <i>(sort by access time)</i>
ls -d <i>(show directory itself, not contents)</i>	ls -S <i>(sort by size)</i>
ls -l <i>(long, detailed listing)</i>	ls -r <i>(reverse any sort)</i>
ls -lh <i>(file details, sizes in "human" units)</i>	
COMBOS!	
ls -ld /tmp <i>(see the details about a directory, not its contents)</i>	
ls -lAh <i>(detailed listing including hidden files, file sizes in K/M/G)</i>	
ls -lAShr ~/Downloads <i>(directory listing, big files at the bottom)</i>	
ls -lArt <i>(detailed listing, newer files last)</i>	

I'LL NEVER REMEMBER ALL THAT!

--help is available	
ls --help	<i>(get a summary of options, works with almost all commands)</i>
RTFM	
man ls	<i>("manual pages" – online documentation)</i>
man -k <keyword>	<i>(search manual for pages referencing <keyword>)</i>



YOUR SHELL REMEMBERS!

Navigate your history of previous commands with up/down arrow

Search backwards through your history with **^R**

Edit commands with backspace, left/right arrow, etc

<Enter> key re-runs the command, **^C** aborts

history command displays your saved history

SEE INSIDE!

cat <i>(dump file(s) to terminal)</i>	cat /etc/passwd <i>(see contents of small file)</i> cat log.2 log.1 log less <i>(concatenate multiple files, see them in less)</i>
less <i>(view file one screen at a time)</i> Useful commands in less : b <i>(go back one screen)</i> G <i>(jump to end of file)</i> g <i>(jump to start of file)</i> /keyword <i>(search forward for keyword)</i> ?keyword <i>(search backwards)</i> = <i>(show your position in the file)</i>	less /var/log/messages less +G /var/log/messages <i>(view file, starting at the bottom)</i>

GETTING WILD

<p>* (match any number of any chars)</p>	<pre>cp -r * /backup (copy all files/dirs to /backup) mv *.jpg ~/Pictures (move JPEGs to ~/Pictures) cp ~/.bash* ~newuser (give your Bash config files to somebody else)</pre>
<p>? (match any single char)</p>	<pre>cat log.? log less (concatenate old/new logs into less) ls /tmp/?????? (list files with six char names)</pre>
<p>[...] (match any of a range of chars)</p>	<pre>cat log.[0-9] log less (concatenate old/new logs into less) cp -r .[A-Za-z0-9]* * /backup (backup hidden files too, be careful of “..”!)</pre>

BEING SUPER

Regular users have only limited access to files/directories

Become the superuser ("root") to do real damage!

su <i>(become root w/ root password)</i>	su <i>(enter root's password to become root)</i> su - <i>(become root as if login as root)</i> su - oracle <i>(become a different account)</i>
sudo <i>(become root w/ your password)</i>	sudo cat /etc/shadow <i>(enter your password, run one command as root)</i> sudo -s <i>(enter your password, get root shell)</i> sudo -u oracle less ~oracle/.profile <i>(sudo also lets you be other users)</i>

KNOWING WHO YOU ARE

```
[lab@LAB ~]$ whoami
lab
[lab@LAB ~]$ sudo -s
[sudo] password for lab:
[root@LAB lab]# whoami
root
[root@LAB lab]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconf...
[root@LAB lab]# exit
[lab@LAB ~]$ id
uid=1000(lab) gid=1000(lab) groups=1000(lab),10(wheel) context=unconfined...
```

The biggest clue is your command prompt!

*Just type **^D** to exit*

LAB – ONLY SEVEN COMMANDS? NO WORRIES!

You can do a lot of damage with only seven commands!



The background features abstract, flowing waves in shades of green and orange. The green waves are on the left side, and the orange waves are on the right side, creating a dynamic, organic feel. The waves have a slight gradient and a soft, ethereal quality.

BUILDING BLOCKS

A PHILOSOPHICAL MOMENT



The Unix design philosophy is:

Simple commands that do one thing

Glued together with *pipes* to accomplish complex tasks

```
awk '{print $1}' access_log* | sort | uniq -c | sort -nr | head
```

SLICING AND DICING

cut <i>(simple splitting for well formed data)</i>	cut -d: -f1,5 /etc/passwd <i>(extract username and full name)</i> ls -lA cut -c1 <i>(get file types)</i>
awk <i>(handles whitespace well)</i>	awk '{print \$1}' access_log* <i>(first column is source IP addresses)</i> df awk '{print \$5, \$6}' <i>(extract pct full and file path)</i> ps -ef awk '/sshd/ {print \$1}' <i>(who is SSH-ing into the system?)</i> awk -F: '{print \$1, \$5}' /etc/passwd <i>(awk can do delimited data too)</i>

SELECTING

grep	<i>(output lines matching patterns)</i>	ps -ef grep sshd	<i>(similar to earlier awk)</i>
		grep -i Hal userlist	<i>(find "Hal" regardless of case)</i>
		grep -v bash /etc/passwd	<i>(spot the accounts that don't do bash)</i>
		grep -f myIoCs *	<i>(match multiple patterns from file)</i>
		grep -f myIoCs -r /evidence	<i>(search though an entire directory)</i>
		grep -f myIoCs -rl /evidence	<i>(only output file names, not matches)</i>

SORTING AND COLLECTING

sort <i>(sort whole lines, or just subfields)</i>	sort mywordlist <i>(basic alpha sort)</i> sort -r mywordlist <i>(reverse sort, Z → A)</i> sort -u words[123] >merged <i>(unique words from three files, saved)</i> sort -n -t: -k3,3 /etc/passwd <i>(sort passwd file numerically by UID)</i> df awk '{print \$5, \$6}' sort -nr <i>(sort file systems by pct full)</i>
uniq <i>(deal with duplicate entries)</i>	sort words[123] uniq >merged <i>(similar to sort -u line above)</i> cut -d: -f3 /etc/passwd sort uniq -d <i>(show any duplicate UIDs)</i> ls Photos[12] uniq -u <i>(photos that are only in one directory)</i> awk '{print \$1}' access_log* sort uniq -c <i>(how many times does each IP appear?)</i>

SAMPLING

head <i>(displays beginning of input)</i>	sort -n -t: -k3,3 /etc/passwd head <i>(just looking for extra UID=0 accounts)</i> head -3 access_log <i>(quickly check log format)</i>
tail <i>(displays end of input)</i>	tail auth.log <i>(most recent security logs)</i> cut -d: -f3 /etc/passwd sort -n tail -1 <i>(biggest UID in passwd file)</i> df tail -n +2 <i>(skip the header line, show rest)</i>
wc <i>(counts number of chars/words/lines)</i>	wc -w my_essay.txt <i>(how many words?)</i> awk '{print \$1}' access_log* sort -u wc -l <i>(how many unique IPs?)</i> wc -L access_log* <i>(longest log entry?)</i>



ONE LAST TAIL TRICK

tail -f displays the end of a file but keeps the file open

New lines will be displayed as they are added

Great for keeping an eye on log files!



NOW TELL ME WHAT THIS DOES

```
awk '{print $1}' access_log* | sort | uniq -c | sort -nr | head
```

LAB – LEARNING TO LINUX

Plumbing is an honorable trade



THANK YOU!

Thanks for participating!
Any final questions?



*Linux Command Line
for Analysts and Operators*

hrpomeraanz@gmail.com
@hal_pomeraanz@infosec.exchange
<https://RighteousIT.com/resources>



Attribution-ShareAlike
CC BY-SA