LINUX COMMAND LINE

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

COMMAND LINE SKILLS ARE FOR…

Penetration testing

Post-exploitation

System and Network administration

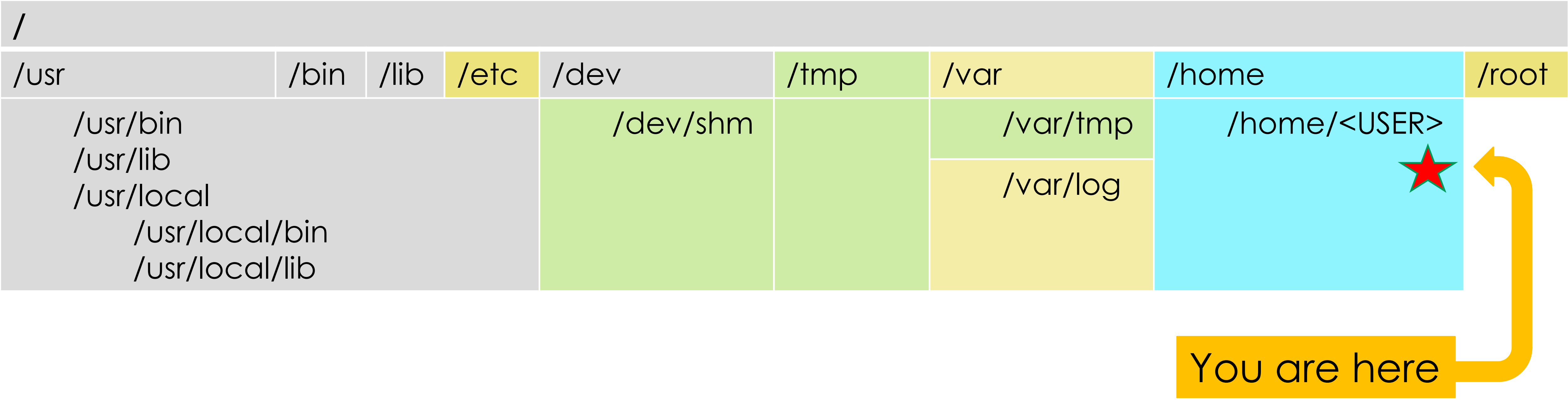
DevOps and automation

Forensics and incident response

Data transformation

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

/var/log

/home/<USER>

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

TAB COMPLETION

Faster

Helps catch errors

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

LAB – DIRECTORY JEOPARDY!

There's usually more than one right answer

BASIC COMMANDS

FILE MANIPULATION

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

THE MANY FACES OF LS

Display		**Sorting**	
`ls -a`	*(show “hidden” files)*	`ls -t`	*(sort by modified time)*
`ls -A`	*(show “hidden” files w/o “.” & “..”)*	`ls -u`	*(sort by access time)*
`ls -d`	*(show directory itself, not contents)*		
		`ls -S`	*(sort by size)*
`ls -l`	*(long, detailed listing)*		
`ls -lh`	*(file details, sizes in “human” units)*	`ls -r`	*(reverse any sort)*

COMBOS!	
`ls -ld /tmp`	*(see the details about a directory, not its contents)*
`ls -lAh`	*(detailed listing including hidden files, file sizes in K/M/G)*
`ls -lAShr ~/Downloads`	*(directory listing, big files at the bottom)*
`ls -lArt`	*(detailed listing, newer files last)*

I’LL NEVER REMEMBER ALL THAT!

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

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` *(dump file(s) to terminal)*	**`cat /etc/passwd`** *(see contents of small file)* **`cat log.2 log.1 log | less`** *(concatenate multiple files, see them in **less**)*

`less` *(view file one screen at a time)*
Useful commands in **`less`**:
`b` *(go back one screen)*
`G` *(jump to end of file)*
`g` *(jump to start of file)*
`/`*`keyword`* *(search forward for keyword)*
`?`*`keyword`* *(search backwards)*
`=` *(show your position in the file)*
	`less /var/log/messages`
	`less +G /var/log/messages`
	(view file, starting at the bottom)

GETTING WILD

`*` *(match any number of any chars)*	**`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)*
`?` *(match any single char)*	**`cat log.? log | less`** *(concatenate old/new logs into* ***`less`****)* **`ls /tmp/??????`** *(list files with six char names)*

`[…]` *(match any of a range of chars)*	**`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 “`..`”!)

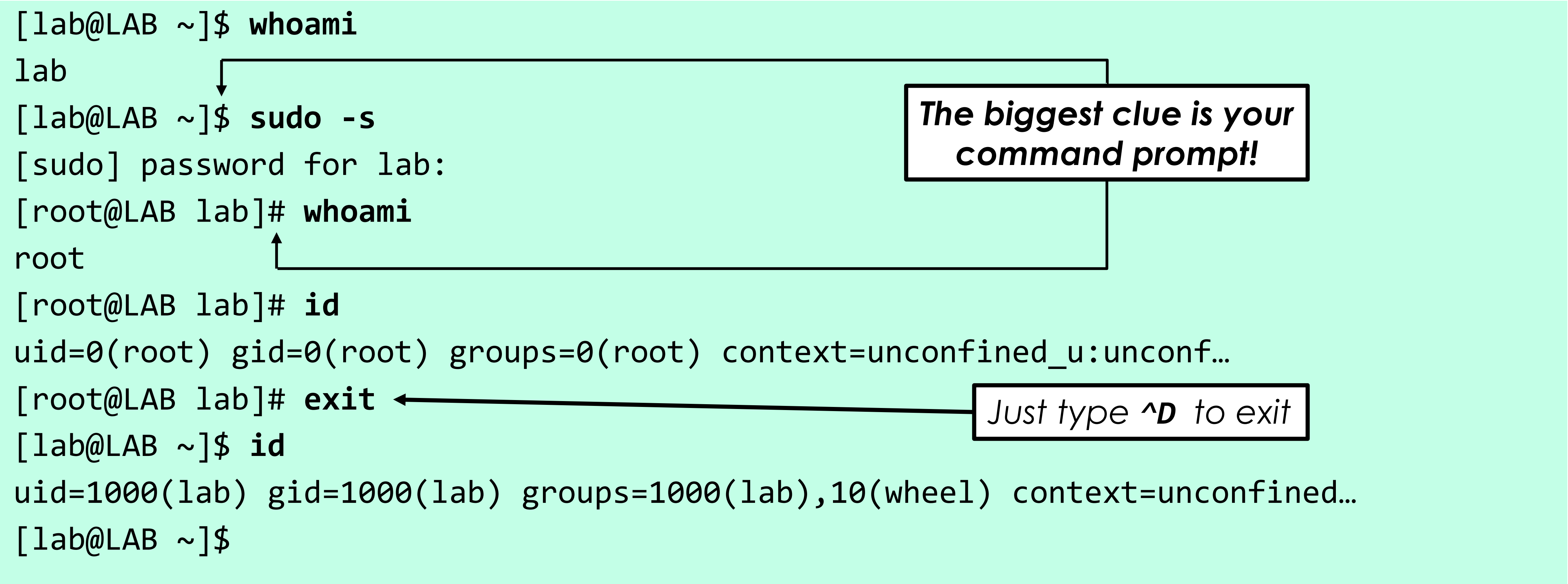
BEING SUPER

Regular users have only limited access to files/directories

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

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

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…
[lab@LAB ~]$
```

The biggest clue is your command prompt!

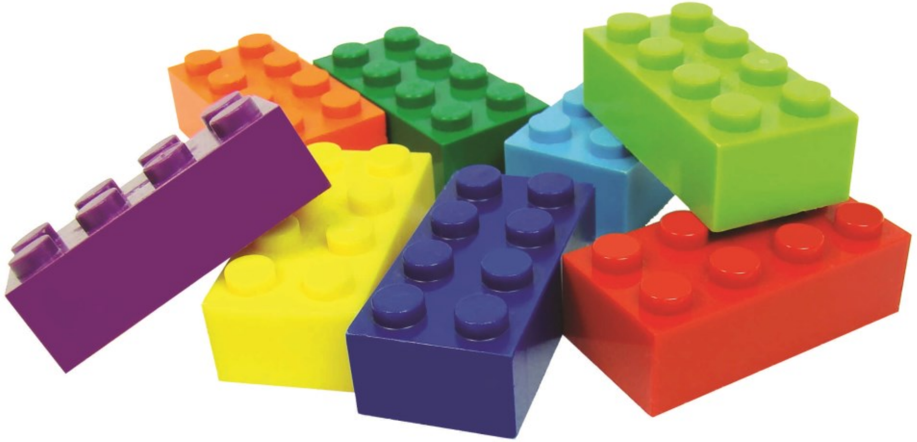
Just type ***^D*** *to exit*

LAB – ONLY SEVEN COMMANDS? NO WORRIES!

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

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

SELECTING

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

SORTING AND COLLECTING

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

SAMPLING

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

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

hrpomeranz@gmail.com

@hal_pomeranz@infosec.exchange

https://RighteousIT.com/resources