

#1LinuxThingADay

Everyday Linux Use Cases

whoiam



- Work for @hurricanelabs doing vulnerability management and other neat stuff.
- Yes, I purposely titled this slide as “whoiam” instead of “whoami” just to bother you.

I Love Linux.



Why Linux?



UNIX AS A SECOND LANGUAGE

By [Sandra Henry-Stocker](#), Unix Dweeb, Network World | JANUARY 12, 2019 07:07 AM PT

OPINION

First step to becoming a cybersecurity pro: Linux

“Linux is open source, tool developers (and you) have a level of access that is unsurpassed. Linux is transparent... you can learn to manipulate it in ways that are not possible with most OSes... most cybersecurity tools are written to run on Linux.” - Sandra Henry-Stocker

A few things before launch...

- Slides: roxyd.github.io/talks demos: asciinema.org/~roxy
- Distro: Ubuntu 19.04
- Postings encouraged :)
 - [Twitter](#)
@bsidesSATX (#BsidesSATX),
@hurricanelabs, @theroxyd
 - [Instagram](#)
@hurricanelabs & @theroxydee

Agenda

- User Management
- Working with Files
- System Administration
- Other Shenanigans

Managing your users...

ominous tones playing in background



User Management: adduser



- Purpose of adduser: to create new users.
- Use: adduser [OPTIONS]
 - Note: create a new user with a different Home Directory than the default.
 - Use Case: Juliette will only be working on creating content, so the Content Directory is her Home Directory.
 - `sudo adduser --home /content juliette`

User Management: deluser



- Purpose of deluser: delete a user and remove all their files.
- Use: deluser [OPTIONS]
 - Note: delete a user and remove all files they own.
- Use Case: Juliette only wrote 2 articles and then quit. You need to delete her account and all her files
 - sudo deluser juliette --remove-all-files

User Management: passwd



- Purpose of passwd: change and manage passwords for users.
- Use: passwd [OPTIONS] [USERNAME]
 - Note: check the status of a user's account.
 - Use Case: Is Bob's account locked again?
 - passwd -S bob
 - Output: username; status; date of last password change; minimum age (days); maximum age (days); warning period (days); inactivity period (days)

Quick!
Grab the files!

Working with Files: cat



- Purpose of cat: concatenate, read, and create files.
- Use: cat [OPTIONS] [FILENAME]
Sometimes you need to add a direction and destination.
 - Note: concatenate files
 - Use Case: you stored a bunch of text messages in separate files and wants to combine them into one file.
 - cat Jan.txt Feb.txt Mar.txt Apr.txt > 2019.txt
you can also pipe commands such as more, less, grep, uniq, sort, and more!

Working with Files: touch



- Purpose of touch: create an empty file; update a file's timestamp.
- Use: touch [OPTIONS] [FILENAME]
 - Note: put files at top of “sort by last modified” list.
- Use Case: Jill is reviewing all of your work for the month, but you want her to see the best stuff first. Use -c so you don't accidentally create a new file!
 - touch -c prettygood.txt amazing.txt
amazing.txt will be the most recently “touched” file and prettygood.txt will be next.

Working with Files: wc



- Purpose of wc: find out how many lines, words, and/or characters are in a file.
- Use: wc [OPTIONS] [FILENAME]
 - Note: update a file with a timestamp and word count.
 - Use Case: You're writing everyday for a month and want to keep a log of the word count at the end of every day.
 - { date && wc -w longstory.txt; } >>wordcount.txt
to count: bytes -c; characters -m; lines -l; length of the longest line -L

Working with Files: ls



- Purpose of ls: list files and their properties.
- Use: ls [OPTIONS] [FILENAME]
 - Note: list the largest images files.
- Use Case: You want to delete the largest image files that are JPG & PNG.
 - ls *.png *.jpg -lSh | head
 - S to sort by file size; use -h to make it human readable

Working with Files: uniq



- Purpose of uniq: find duplicate lines.
- Use: uniq [OPTIONS] [INPUT FILENAME] [OUTPUT FILENAME]
 - Note: see only the duplicate entries in a file.
- Use Case: You have answers from a survey of favorite shows and you want to see only ones that were mentioned more than once.
 - `sort shows.txt | uniq -d`



Whelp,
looks like it's
SysAdmin time.

System Administration: alias



- Purpose of alias: define an action for a named string.
- Use: alias [NAME = [VALUE]]
 - Note: set up an alias for a frequent task.
- Use Case: you're tired of typing an entire two commands when you want to update stuff
 - alias updateme='sudo apt-get update && sudo apt-get upgrade'

System Administration: mkdir



- Purpose of mkdir: create directories.
- Use: `mkdir [OPTIONS] [DIRECTORY NAME]`
 - Note: make a new directory with subdirectories
- Use Case: you want to make directories (months) and subdirectories (weeks) and need a verbose output
 - `mkdir -pv January/{1-7,8-14,15-21,22-29}`

System Administration: shutdown



- Purpose of shutdown: shutdown or reboot the system.
- Use: shutdown [OPTIONS] [TIME][“MESSAGE”]
 - Note: shutdown but give users 10 minutes notice
- Use Case: you need to shutdown the server for the rest of the day
 - sudo shutdown 10 “shutting down in 10 minutes for the rest of the day!”

System Administration: motd



- Purpose of motd: display a message upon login.
- Use: you favorite text editor to edit /etc/motd
 - Note: update the motd
- Use Case: users need to be aware of next scheduled maintenance time.
 - sudo echo “The next maintenance is at 4AM UTC on 6/14/19”>/etc/motd

Anddd a few other helpful things
you might want to know...

Other Things: History

- Purpose of history: view history of what you've done on the command line.
- Use: history [OPTIONS]
 - Note: search history for a command.
- Use Case: you want to see how many times out of 100 you're used clear.
 - `history 100 | grep -c 'clear$'`

Other Things: whatis

- Purpose of `whatis`: print a short description of the specified command(s).
- Use: `whatis [OPTIONS][COMMANDS]`
 - Note: create a file contain output of `whatis` for a few commands.
- Use Case: you are training a new coworker.
 - `whatis file pwd ps >> commands.txt`

Other Things: tree

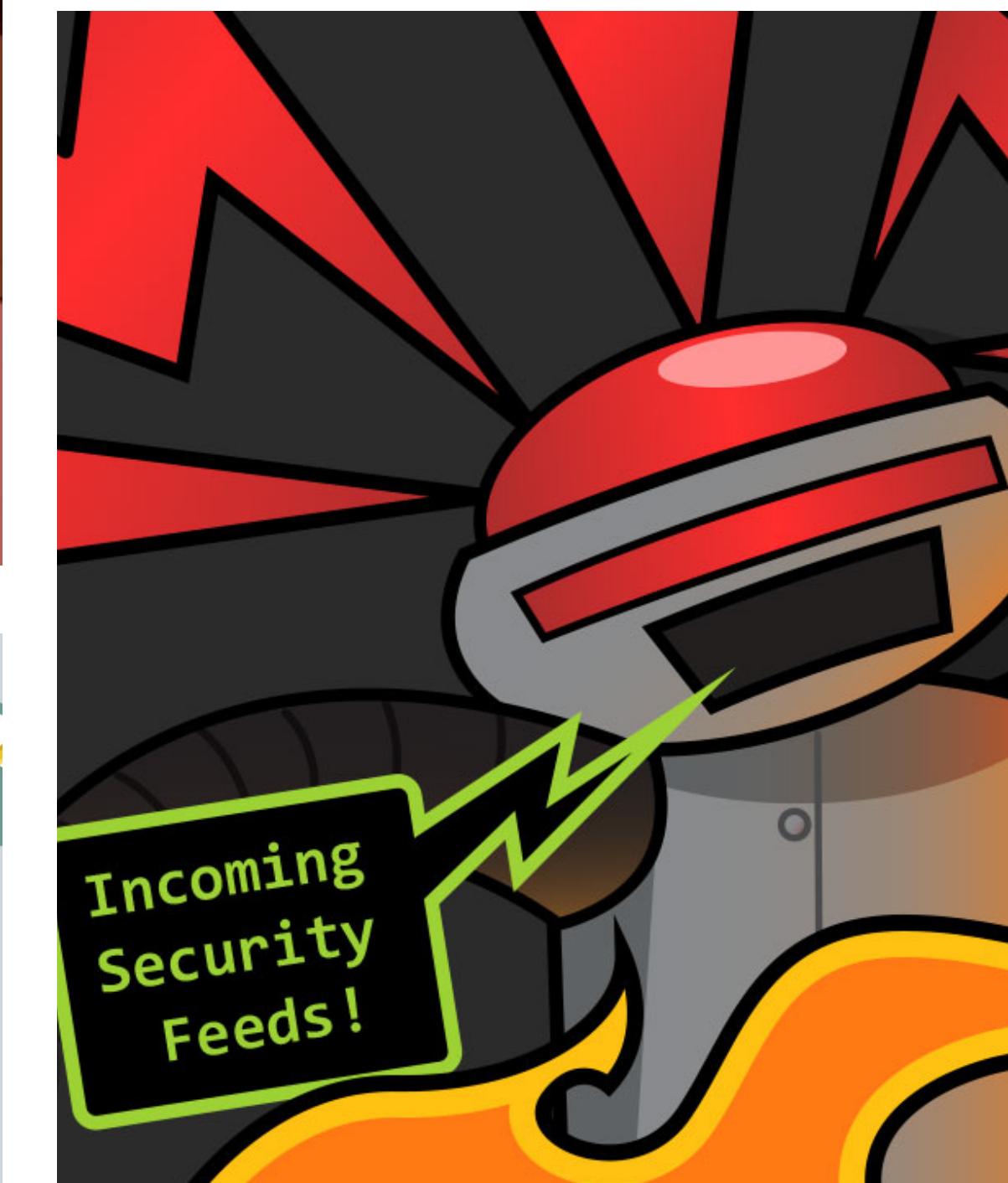
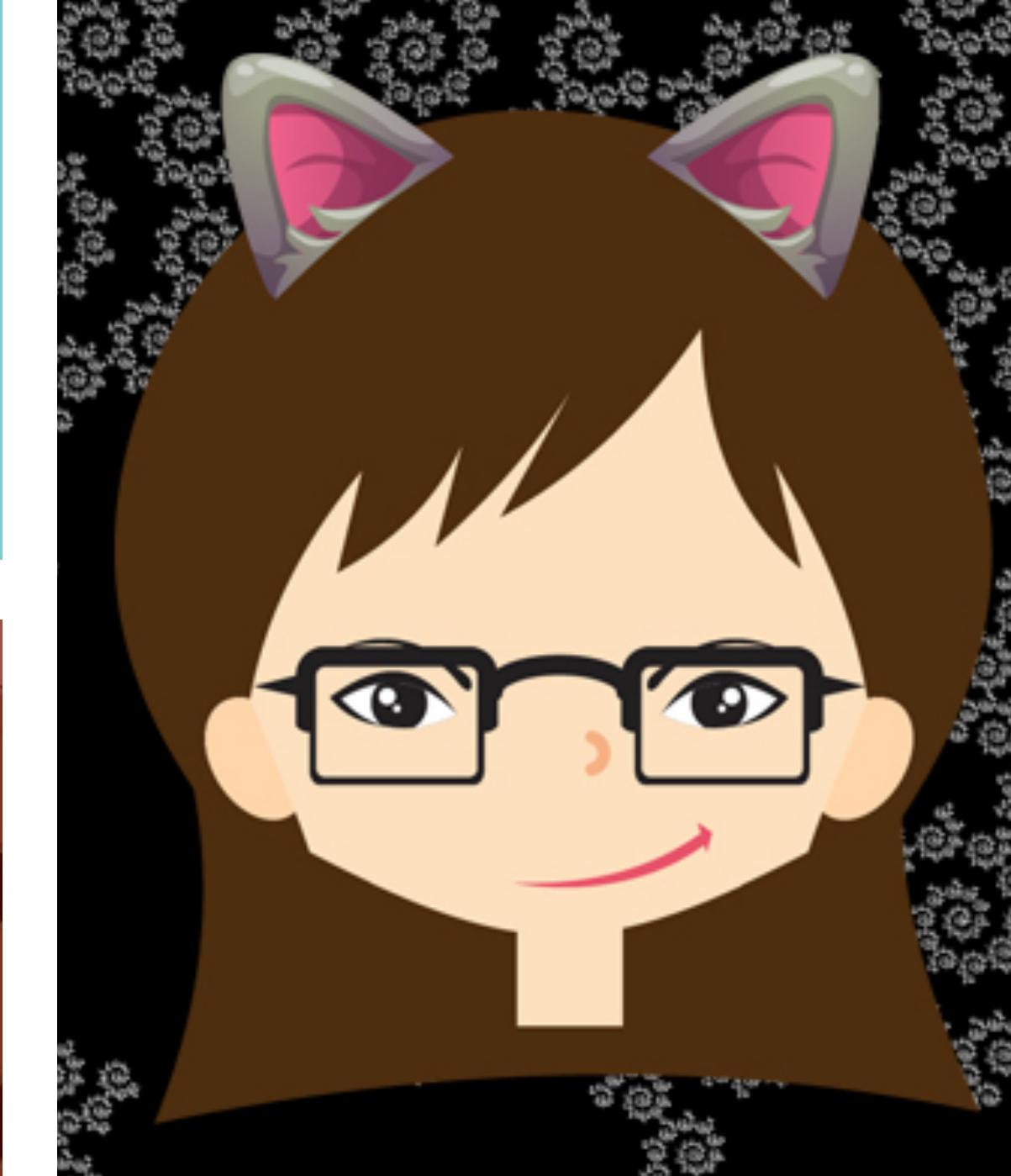
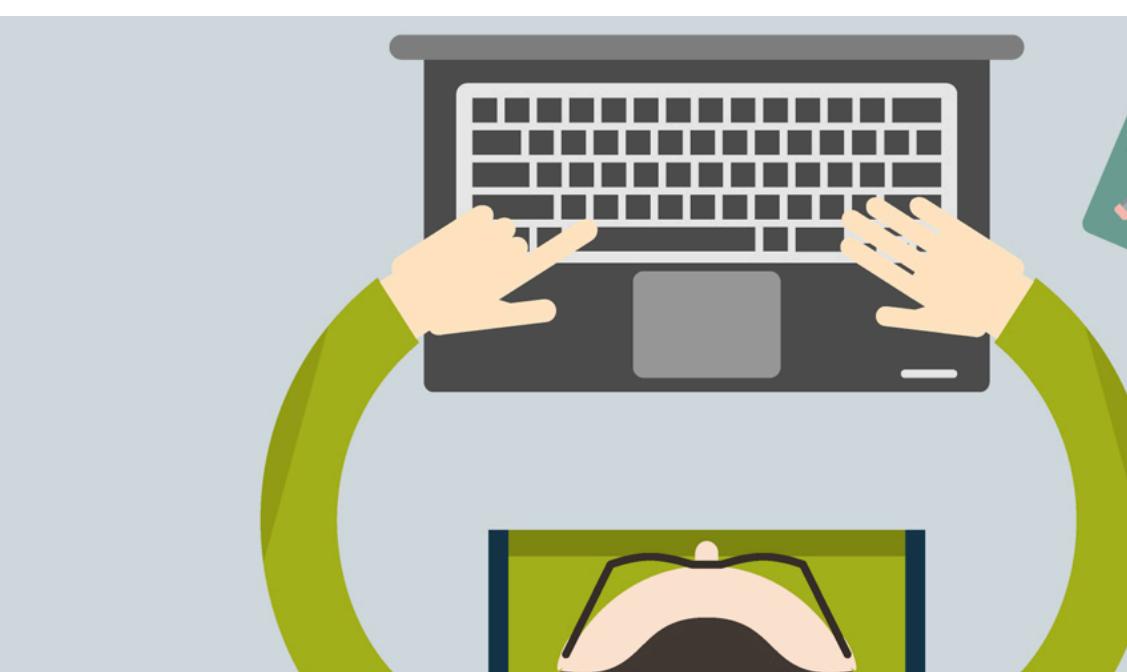
- Purpose of tree: show all files and directories in a tree format.
- Use: `tree [OPTIONS]`
 - Note: view all directories in a tree.
- Use Case: you forgot what's on this server.
 - `tree -d | less`

Other Things: cal or gcal

- Purpose of cal/gcal: see the calendar.
- Use: cal/gcal [OPTIONS] [[[day]month]year]
 - Note: view a calendar with week numbers & starting on Mondays.
- Use Case: you're making bullet journal weekly spreads.
 - cal 6 2019 -M -w
 - gcal -K --starting-day=Monday 6 2019

Resources

- linuxacademy.com
- manpages (from the terminal or linux.die.net)
- info.org
- [cyberciti.biz \(Nixcraft\)](http://cyberciti.biz)
- penguintutor.com/linux



Any questions?

My www things:

roxyd.github.io

Email me! roxy@hurricanelabs.com