Lustin' over Linux

Gabe 'n Justin

Sign In

https://da.gd/ELgN

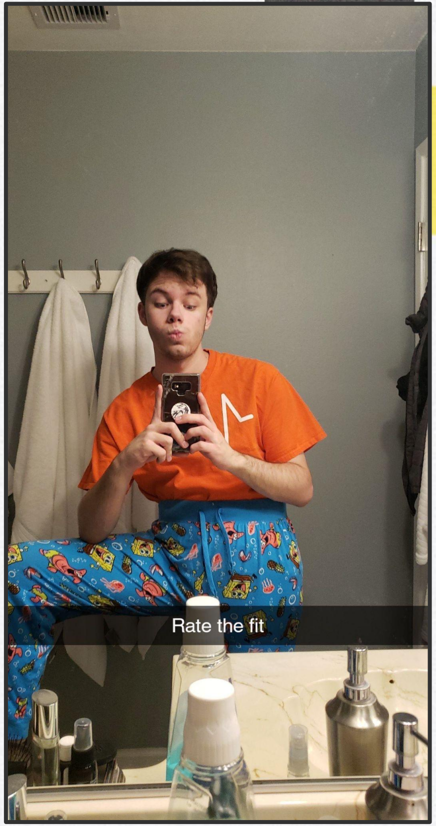
IMPORTANT TRYOUTS CHANGE
Sign in: https://da.gd/ELgN

New Time:

<u>11:00AM – 6:00PM</u>

whoami

Justin Covairt
CPTC Captain
CCDC Threat ~~Hunter~~
CPTC/CCDC 2021-2022



Next on Bronco CCDC...

When	What
July 2nd	Informational Meeting
July 9th	Practicing Safe Cyber
July 16th	Intro to Networking
July 23rd	Windows and Active Directory
July 30th	Linux
August 6th	Business and Injects
August 13th	Mock Presentations
August 20th	CPTC Tryouts - No meeting!
August 27th	**CCDC Tryouts!**

← You are here

Agenda

1

Linux Basics

Key knowledge points

2

Administration

How to administer Linux

3

Services

Burger King

4

Firewalling

There is no war in Ba Sing Se

01

Linux Basics

Linux baseqs (very cool) (and epic)

Nuanced Vocabulary

Terminal

Embedded System

Terminal Emulator

Application / Program

Command Prompt

Different than Windows

Command Line

Overall CLI

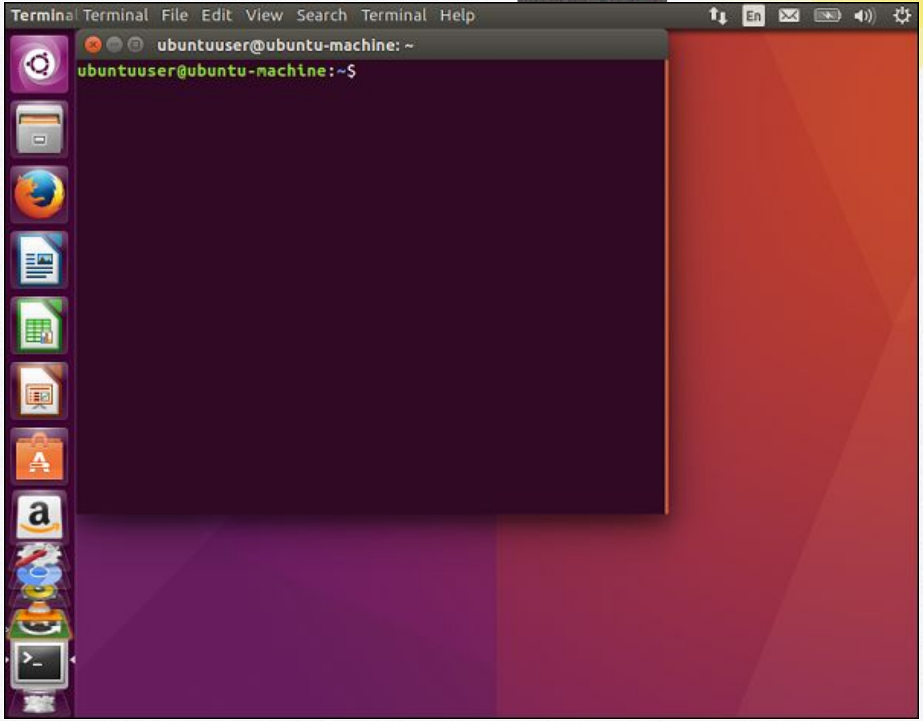
Kernel

Inner workings near hardware

Shell

Wraps/protects kernel

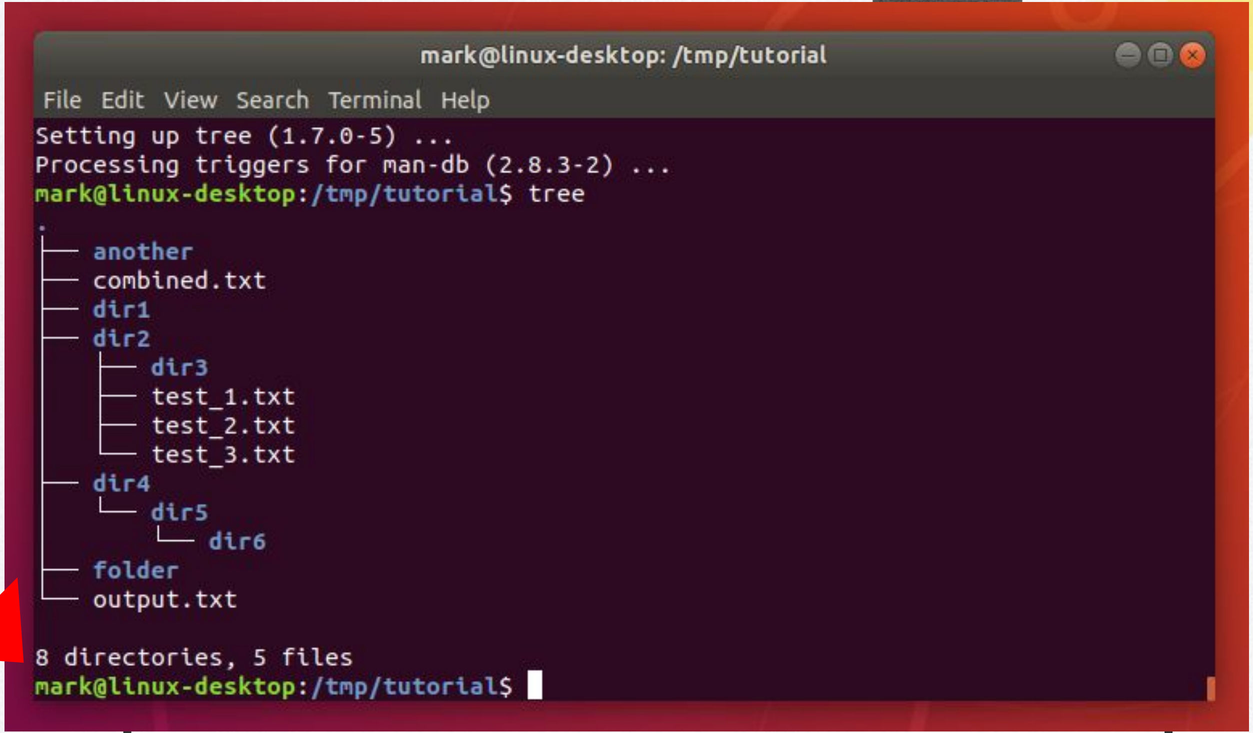
Terminal


Terminal Terminal File Edit View Search Terminal Help
En
ubuntuuser@ubuntu-machine: ~

```
ubuntuuser@ubuntu-machine:~$
```

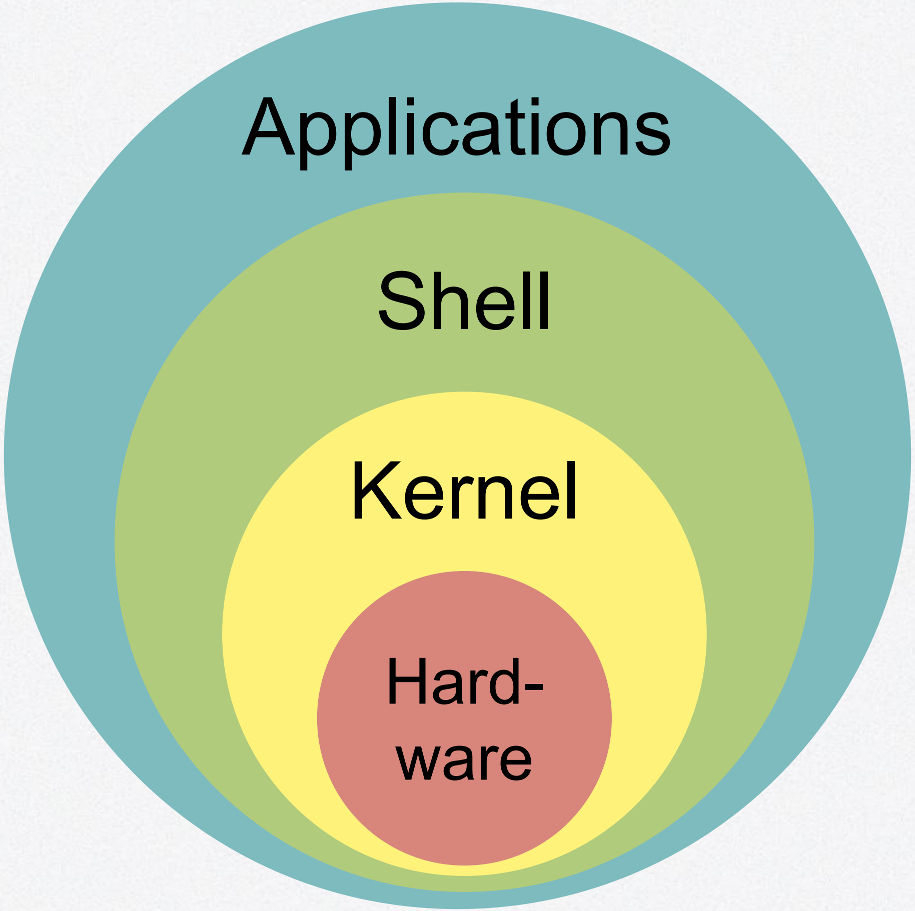
Terminal Emulator

Command Prompt


mark@linux-desktop: /tmp/tutorial
File Edit View Search Terminal Help

```
Setting up tree (1.7.0-5) ...
Processing triggers for man-db (2.8.3-2) ...
mark@linux-desktop:/tmp/tutorial$ tree
.
├── another
├── combined.txt
├── dir1
├── dir2
│   ├── dir3
│   ├── test_1.txt
│   ├── test_2.txt
│   └── test_3.txt
├── dir4
│   └── dir5
│       └── dir6
├── folder
└── output.txt

8 directories, 5 files
mark@linux-desktop:/tmp/tutorial$
```

Command Line



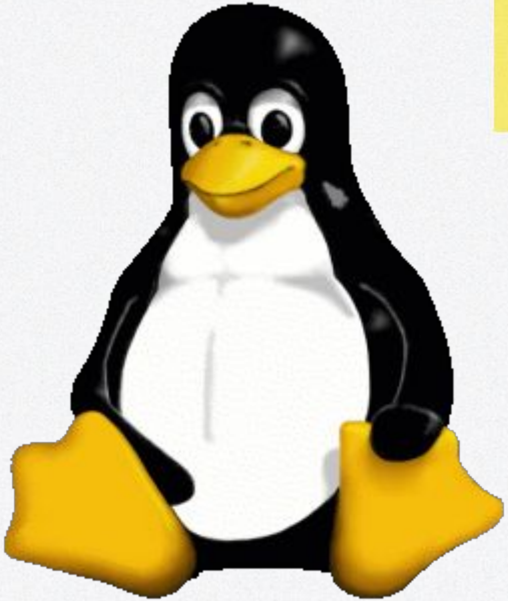
Applications

Shell

Kernel

Hard-
ware

What is Linux?



- **Not** an operating system
- Free & open-source **kernel**
- Built on **Unix** (unix-like)
  - OpenBSD
- Many flavors of **Linux-based** OS
  - Ubuntu, Debian, Red Hat, Fedora, CentOS, Mint, Arch, Slackware, Kali, and many more

Where is Linux?

- Linux accounts for **2.14% of all desktop** operating systems worldwide.
- **All 500 of the world’s** supercomputers run on Linux.
- Linux powers **85% of all smartphones.**
- **96.3% of the top 1 million** web servers are running Linux

According to 99firms.com
& zdnet.com

Why is Linux?

Blazing Fast

Half the load times

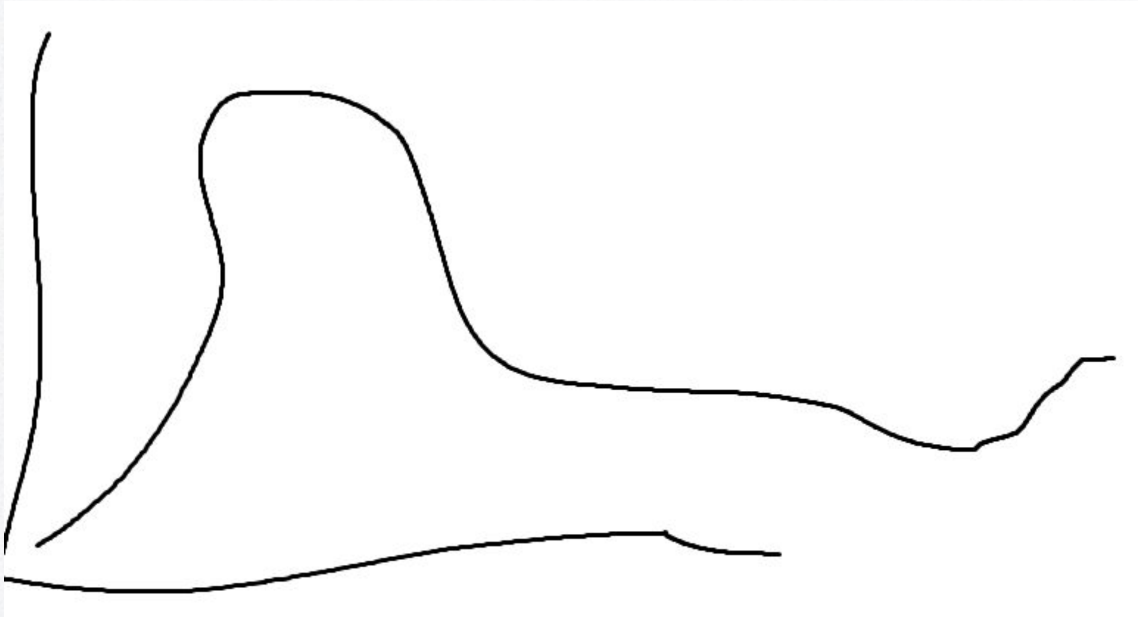
Super Light

Orders of magnitude

Amazingly Extensible

Customizable & free

The Linux Hump



More Linux Concepts…

01.

The File Structure

02.

File Permissions

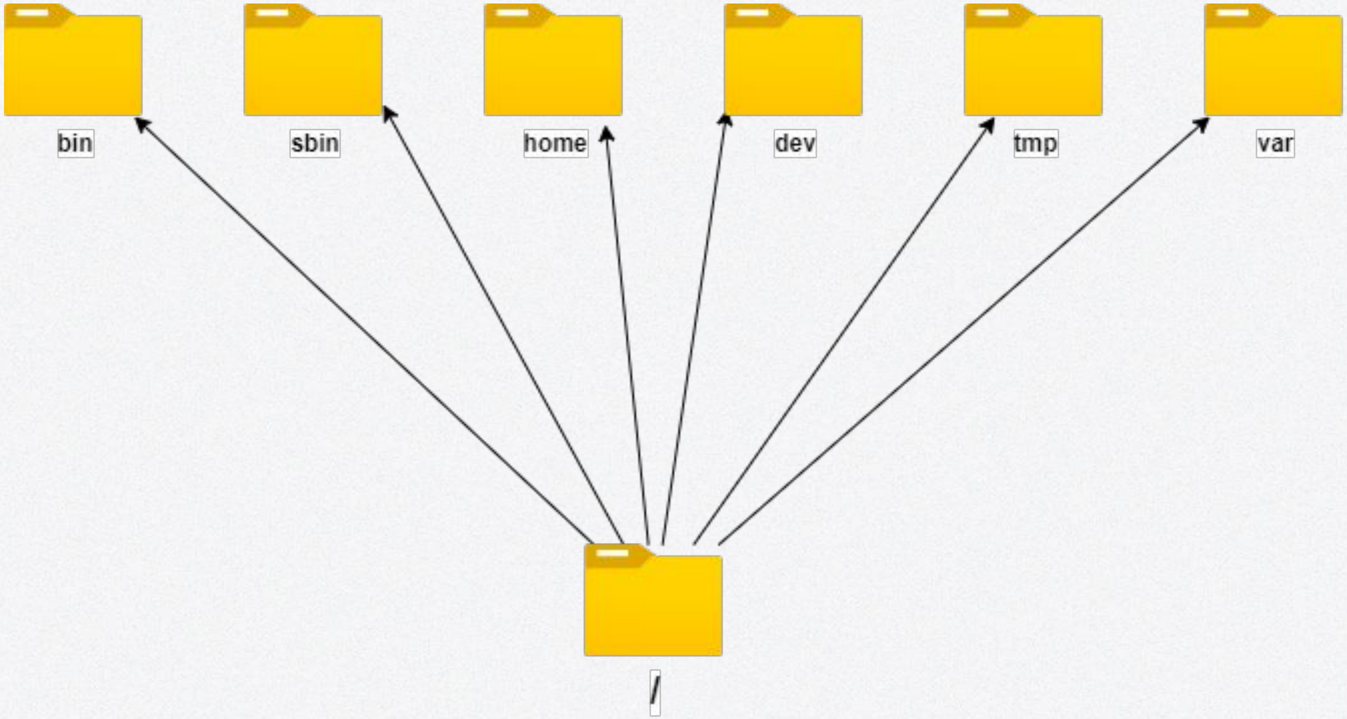
03.

Command Syntax

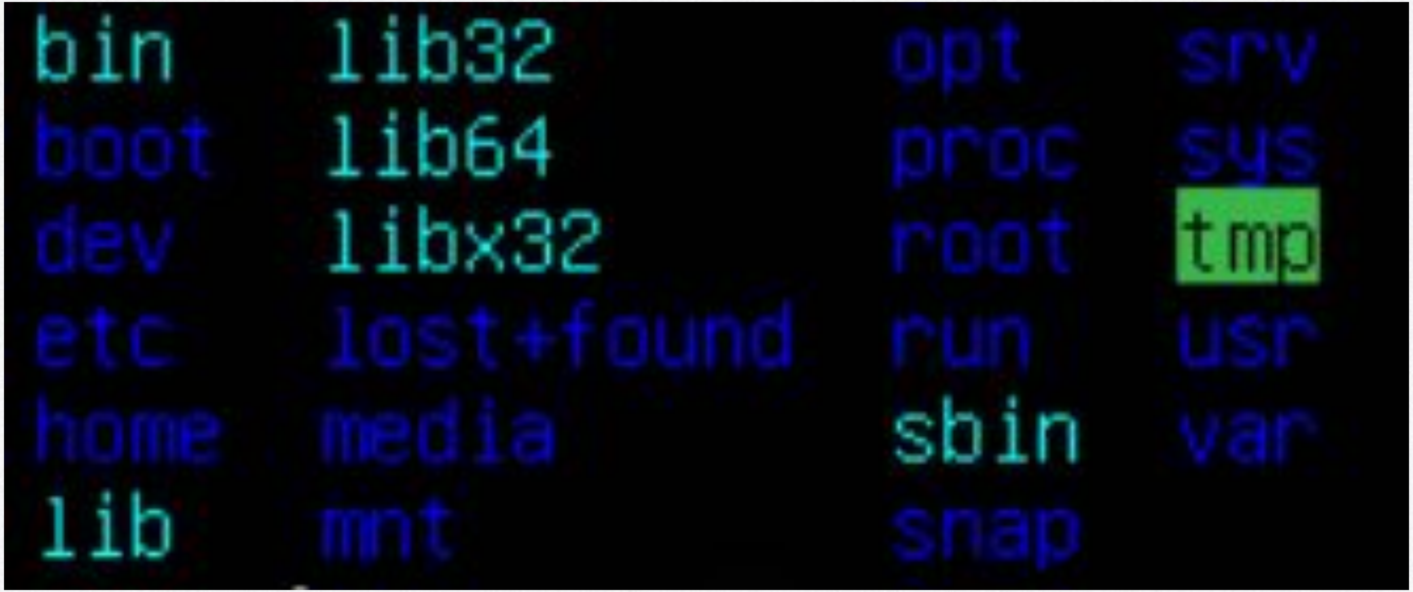
04.

Terminal Multiplexing

File Tree – As a Tree

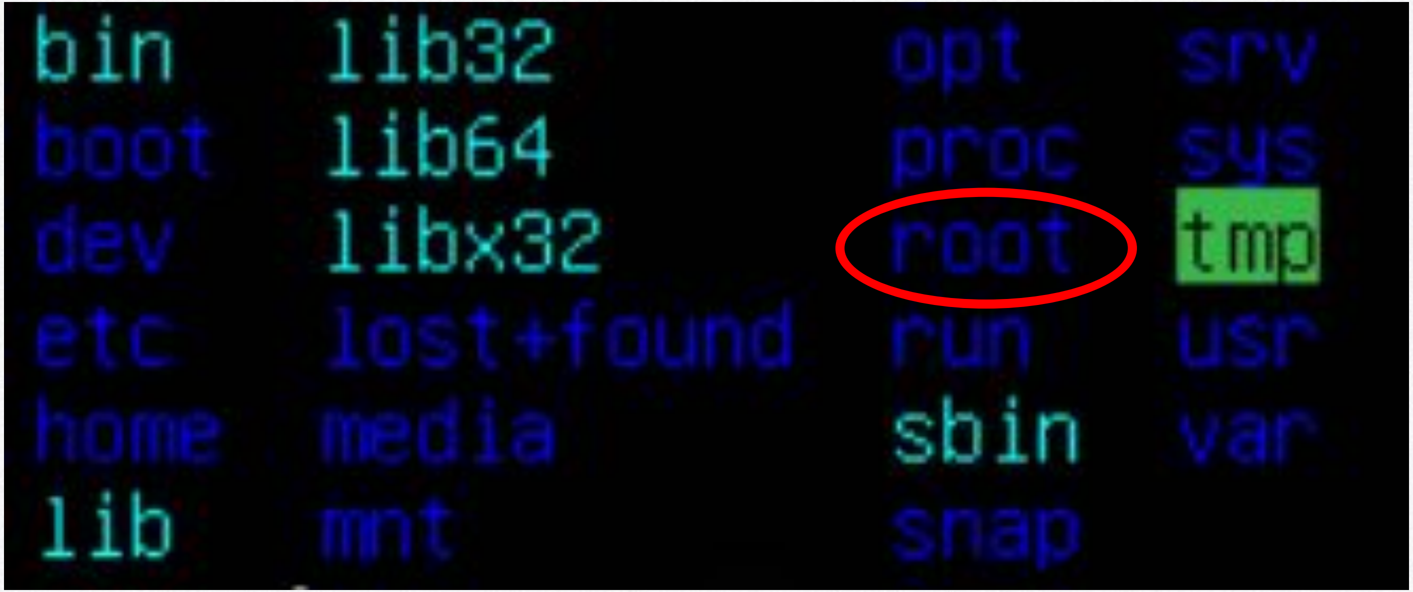


File Tree – Contents of /



```
bin   lib32       opt   srv
boot  lib64       proc  sys
dev   libx32      root  tmp
etc   lost+found  run   usr
home  media       sbin  var
lib   mnt         snap
```

File Tree – Contents of /



```
bin   lib32       opt   srv
boot  lib64       proc  sys
dev   libx32      root  tmp
etc   lost+found  run   usr
home  media       sbin  var
lib   mnt         snap
```

root vs /root vs /

ℹ **root user = admin**

ℹ **root (/) directory = start of file system**

ℹ **root's home = /root**

ℹ **sudo = super user do**

Paths

Absolute Path

Starts with /

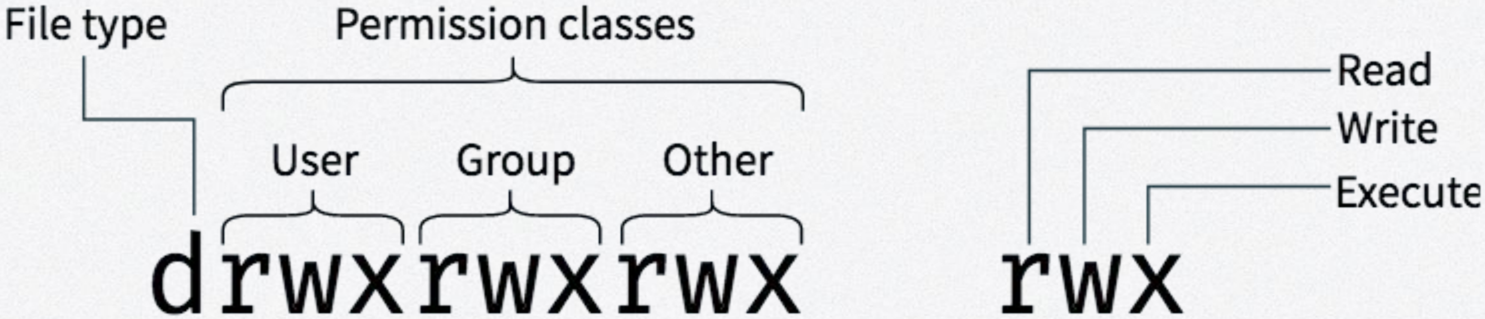
Relative Path

Starts with pwd

Examples

/home/user/Desktop	..
/var/www/html	./script.sh
/etc/ssh/sshd_config	pam.d/common-auth
/etc/crontab	var/www/html

Linux File Permissions



File type

Permission classes

User

Group

Other

drwxrwxrwx

rwx

Read

Write

Execute

SUPER EXCITING MATH TIME!!!

Decimal

- You already know/use this
- AKA Base 10
- Values 0-9
- Syntax: 10_{10}, 123_{10}, 42_{10}, …
- $2_{10} + 2_{10} = 4_{10}$
- **$34_{10} = 3*10^1 + 4*10^0$**

SUPER EXCITING MATH TIME!!!

Binary

- AKA Base 2
- Values 0-1
- Good for true-false
- Unit: **Bits**
- EX: $7_{10} = 111_2$
- EX: $8_{10} = 1000_2$
- **$1101_2 = 1*2^3 + 1*2^2 + 0*2^1 + 1*2^0$**

Octal

- AKA Base 8
- Values 0-7
- Unit: **Octal digit**
- EX: $7_{10} = 7_8$
- EX: $8_{10} = 10_8$
- **$640_8 = 6*8^2 + 8*8^1 + 0*8^0$**

SUPER EXCITING MATH TIME!!!

Binary

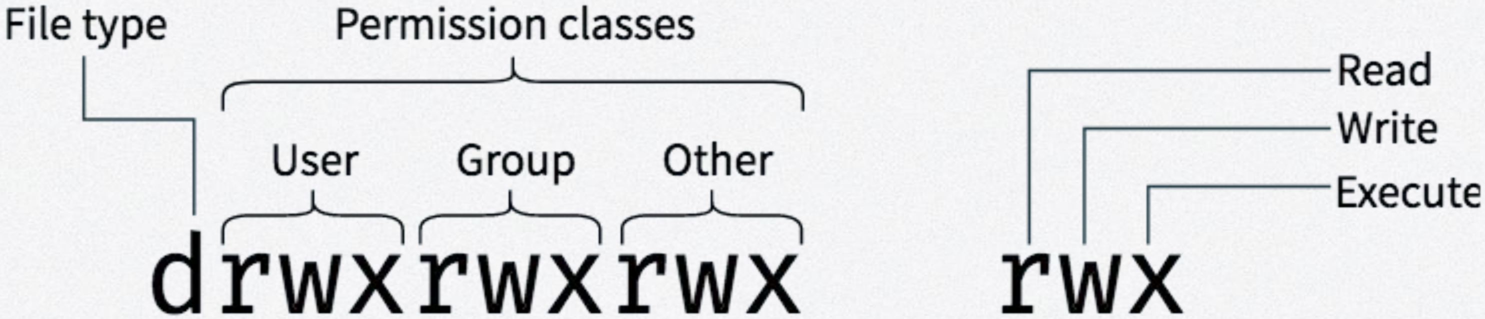
Example: 111 101 101

Octal

Example: 755

- Let's make an observation:
- $2_{10} = 2^1$
- $8_{10} = 2^3$
- This must mean...
- An octal digit is just 3 binary bits!

Linux File Permissions (w/math)



$$111_2 = 4_8 + 2_8 + 1_8 = 7_8$$

Each group of permissions, can be an octal digit!

Pop Quiz!

Convert to octal

rwxr-xr-x

Convert to octal

r-x-w---x

Convert to rwx

644

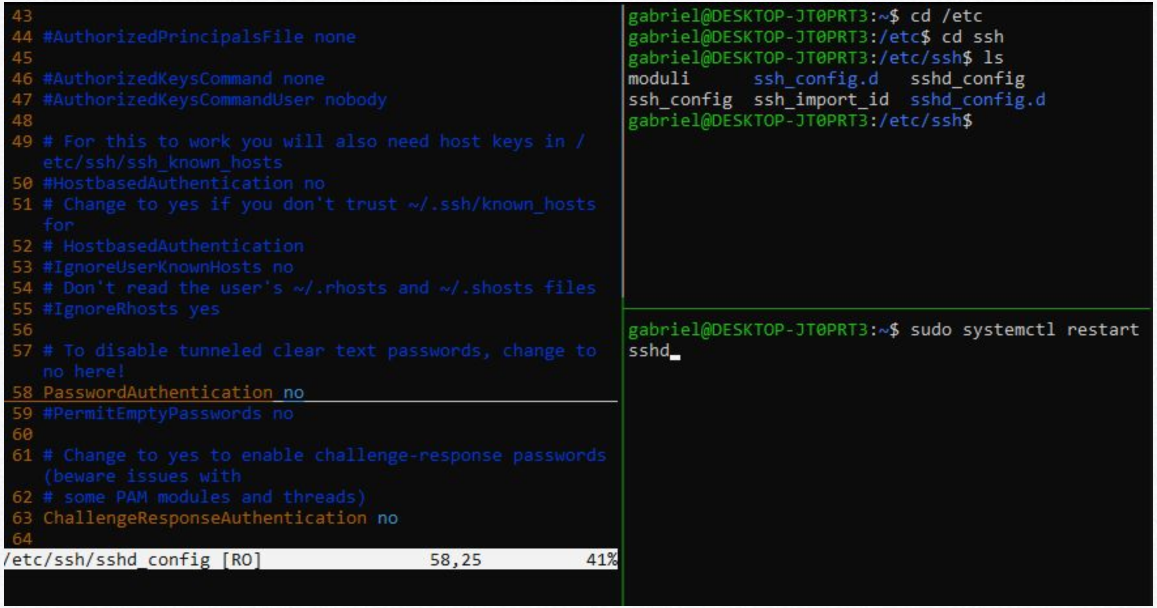
Convert to rwx

777

Shell and Syntax

- command -options arguments
- EXAMPLE: ls
- EXAMPLE: cd /home/user1
- EXAMPLE: ls -la user1/Downloads
- EXAMPLE: ls -R

Terminal Multiplexing (Tmux)



```

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

/etc/ssh/sshd_config [RO]                    58,25          41%
```

```
gabriel@DESKTOP-JT0PRT3:~$ cd /etc
gabriel@DESKTOP-JT0PRT3:/etc$ cd ssh
gabriel@DESKTOP-JT0PRT3:/etc/ssh$ ls
moduli      ssh_config.d   sshd_config
ssh_config  ssh_import_id  sshd_config.d
gabriel@DESKTOP-JT0PRT3:/etc/ssh$
```

```
gabriel@DESKTOP-JT0PRT3:~$ sudo systemctl restart sshd
```

- Use terminal space more efficiently
- Multitask
- High customizability

02

Linux Administration

Linux Demon Time😈

Table of Contents (for this)

01

Terminal Text Editing

02

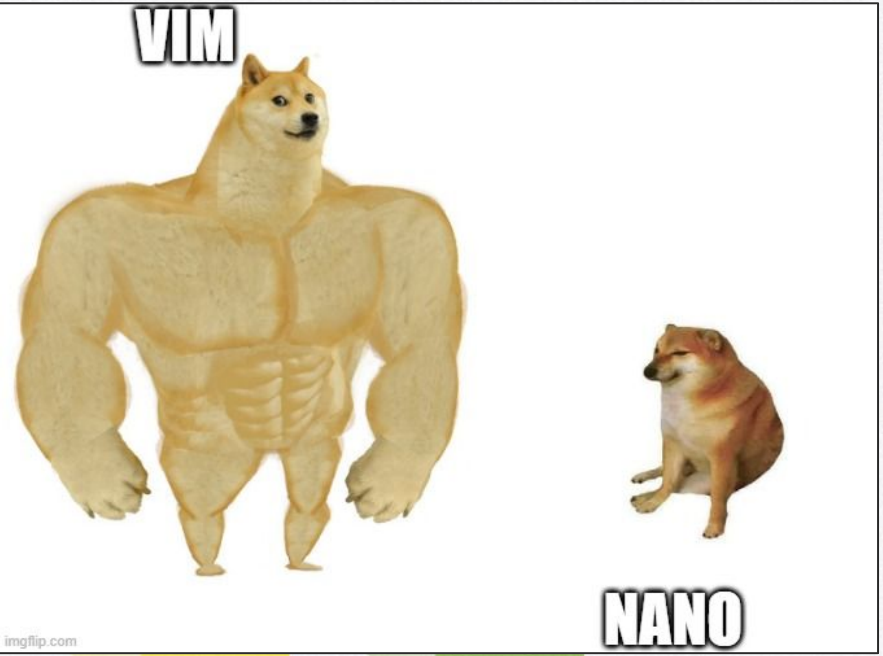
User Management

03

Package Management

04

PAM

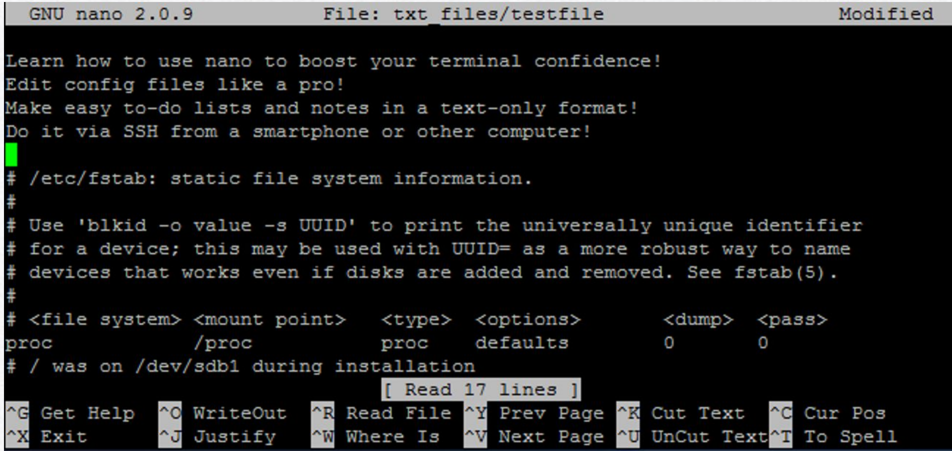


02-01

Terminal Text Editing

NANO (Ol' Reliable)

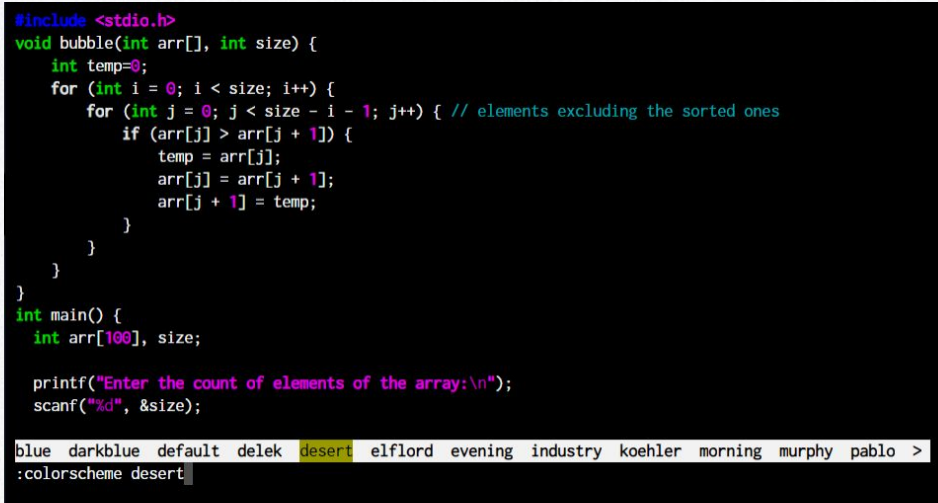
- **nano** <filename>
- installed by default - unless tampered with ;)
- very basic
- CTRL+X to exit "Y" to save as same name



```
  GNU nano 2.0.9              File: txt_files/testfile                     Modified

Learn how to use nano to boost your terminal confidence!
Edit config files like a pro!
Make easy to-do lists and notes in a text-only format!
Do it via SSH from a smartphone or other computer!

# /etc/fstab: static file system information.
#
# Use 'blkid -o value -s UUID' to print the universally unique identifier
# for a device; this may be used with UUID= as a more robust way to name
# devices that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
proc            /proc           proc    defaults        0       0
# / was on /dev/sdb1 during installation
                                [ Read 17 lines ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text^T To Spell
```

VIM (The better one imo)

- **vim** <filename>
- sometimes not installed by default
- extremely customizable
- :wq to close and save file
- 5 modes
- can run commands in the editor
- vimtutor to get started



```
#include <stdio.h>
void bubble(int arr[], int size) {
    int temp=0;
    for (int i = 0; i < size; i++) {
        for (int j = 0; j < size - i - 1; j++) { // elements excluding the sorted ones
            if (arr[j] > arr[j + 1]) {
                temp = arr[j];
                arr[j] = arr[j + 1];
                arr[j + 1] = temp;
            }
        }
    }
}
int main() {
  int arr[100], size;

  printf("Enter the count of elements of the array:\n");
  scanf("%d", &size);

blue  darkblue  default  delek  desert  elflord  evening  industry  koehler  morning  murphy  pablo  >
:colorscheme desert
```

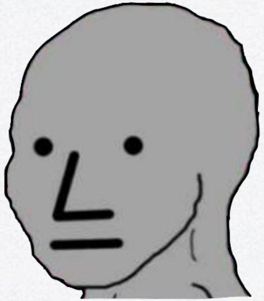
02-02

User/File Management

Permissions

root = 0

services < 1000



users > 999

I am ~~g~~root

✓ sudo

✨sudo <command>✨

sudo -i

sudo su

✗ su

su root

su -

Adding Users

✓ adduser

wrapper for useradd

less clunky

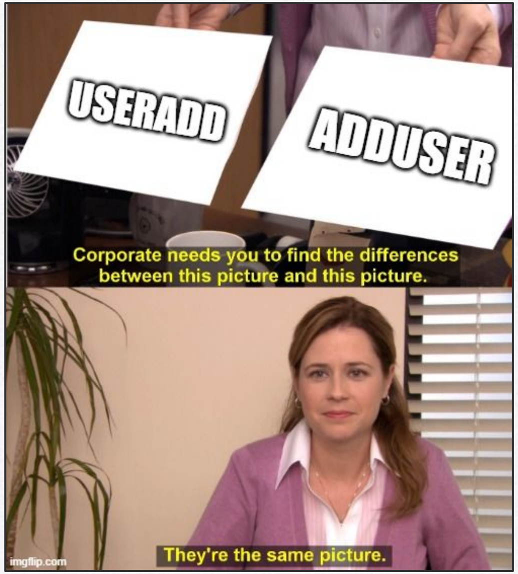
prompts for password

☒ useradd

much less efficient

doesn't create home directories

manually set password


USERADD
ADDUSER
Corporate needs you to find the differences between this picture and this picture.
They're the same picture.
imgflip.com

Managing Users

Group Management

not group policy

groups users together

✨**usermod**✨

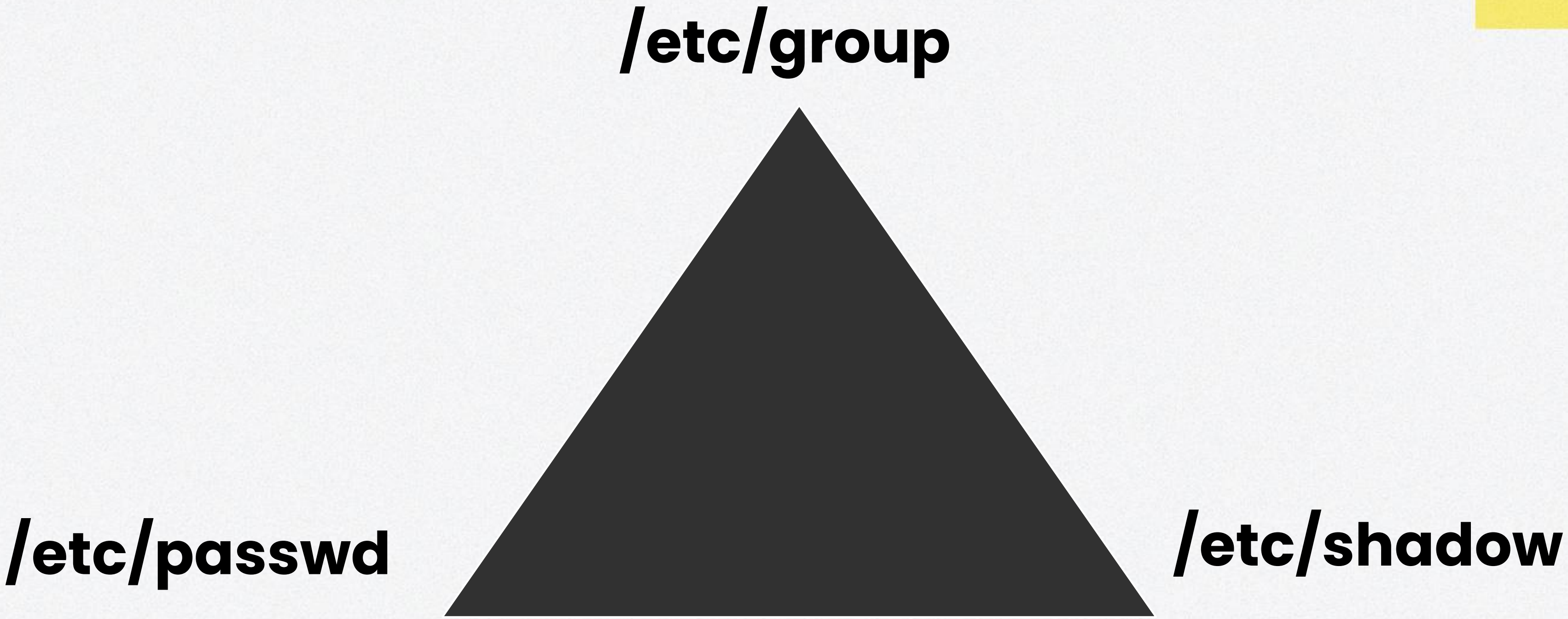
✨**id**✨

Password Management

passwd

chpasswd

The Holy Trinity of User Management



/etc/group

/etc/passwd

/etc/shadow

The Holy ~~Trinity~~ Quadarinity of User Management

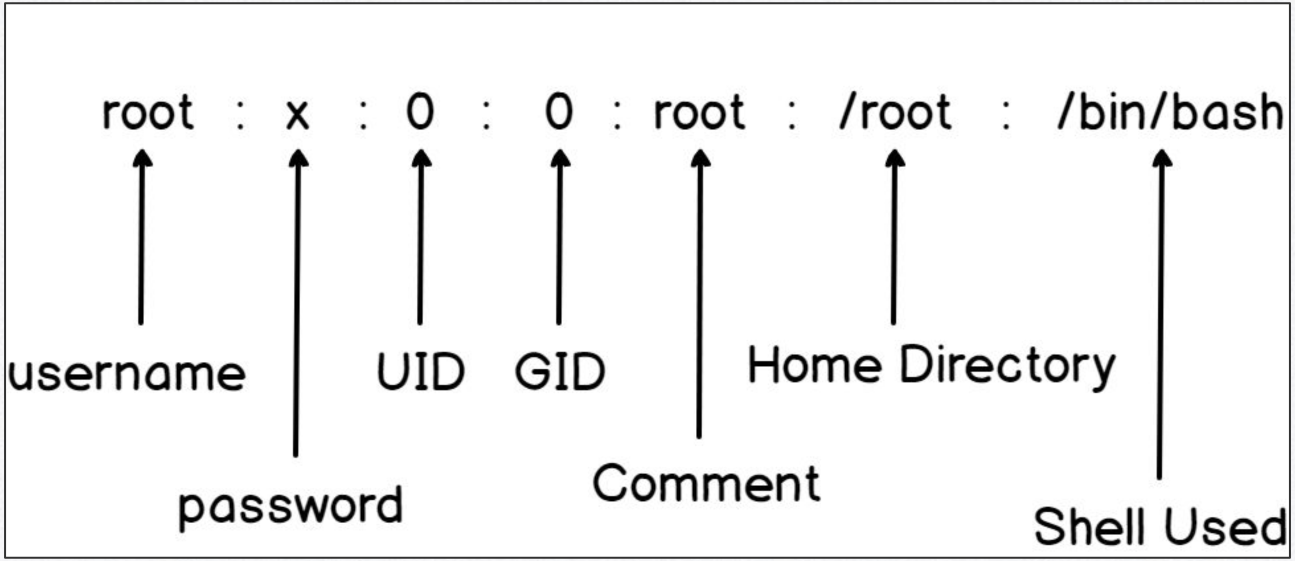
/etc/group

/etc/sudoers

/etc/passwd

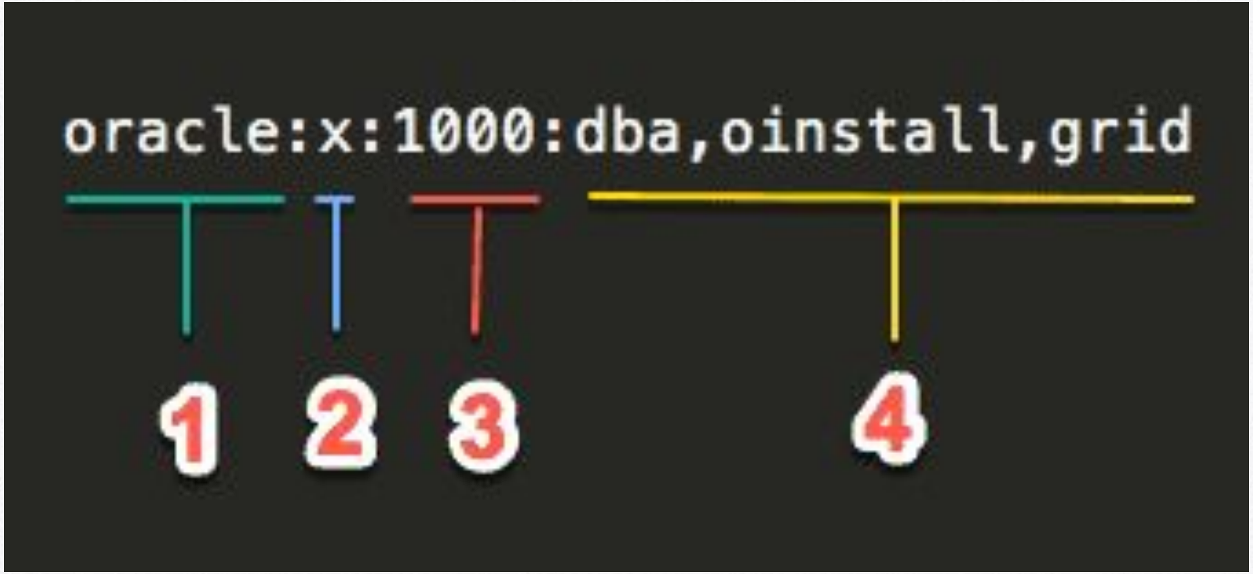
/etc/shadow

/etc/passwd



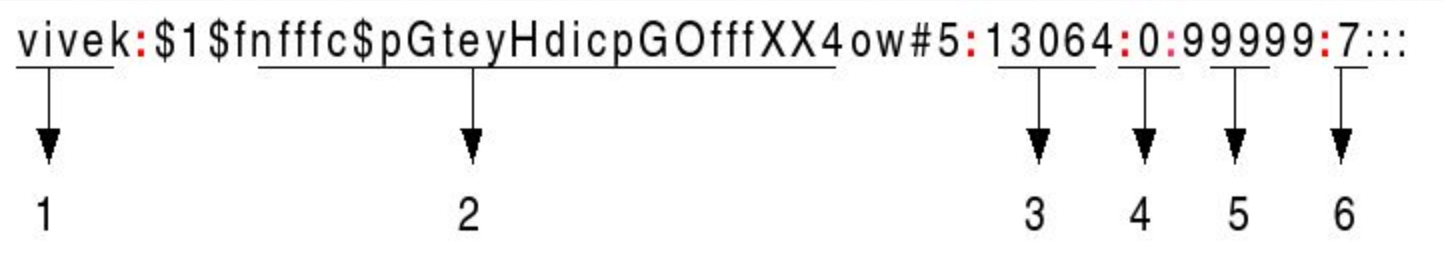
```
root : x : 0 : 0 : root : /root : /bin/bash
```

/etc/group



```
oracle:x:1000:dba,oinstall,grid
```

/etc/shadow



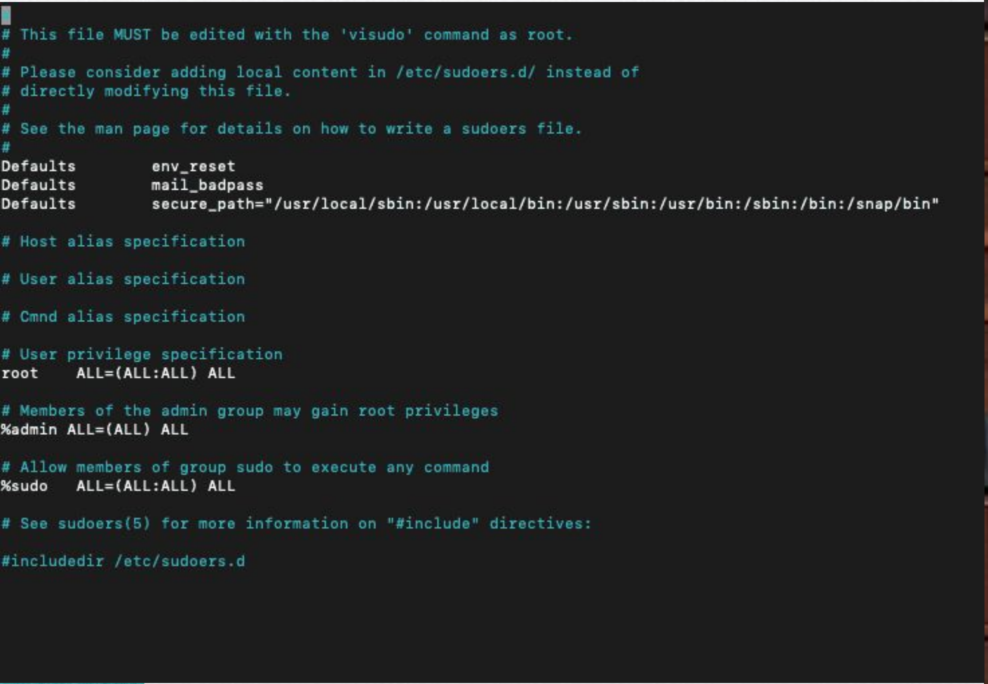
```
vivek:$1$fnfffc$pGteyHdicpGOfffXX4ow#5:13064:0:99999:7:::
```

1: username

2: password hash
different algorithms

3: last changed time (epoch)
4: minimum days between password changes
5: maximum days password is valid

/etc/sudoers



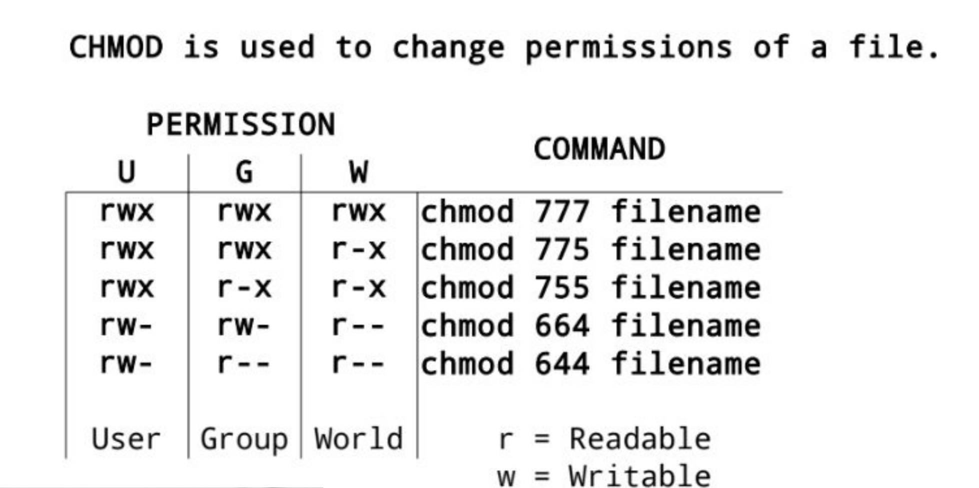
```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

JUSTIN
I think I forgot something.
GABE
If you forgot, then it wasn't important.
JUSTIN
Yeah, you're right.
THIS SLIDE
imgflip.com

Changing File Permissions

chmod to change permissions

chown to change file owner
ex user1:group1 <file>



CHMOD is used to change permissions of a file.

PERMISSION			COMMAND
U	G	W	
rwx	rwx	rwx	chmod 777 filename
rwx	rwx	r-x	chmod 775 filename
rwx	r-x	r-x	chmod 755 filename
rw-	rw-	r--	chmod 664 filename
rw-	r--	r--	chmod 644 filename
User	Group	World	

r = Readable
w = Writable
x = Executable
- = None

Immutability

Make file immutable

```
chattr +i <file>
```

Check for immutable bit

```
lsattr <file>
```

Remove immutable bit

```
chattr –i <file>
```

this is an i

02–03

Package Management

Different Distros

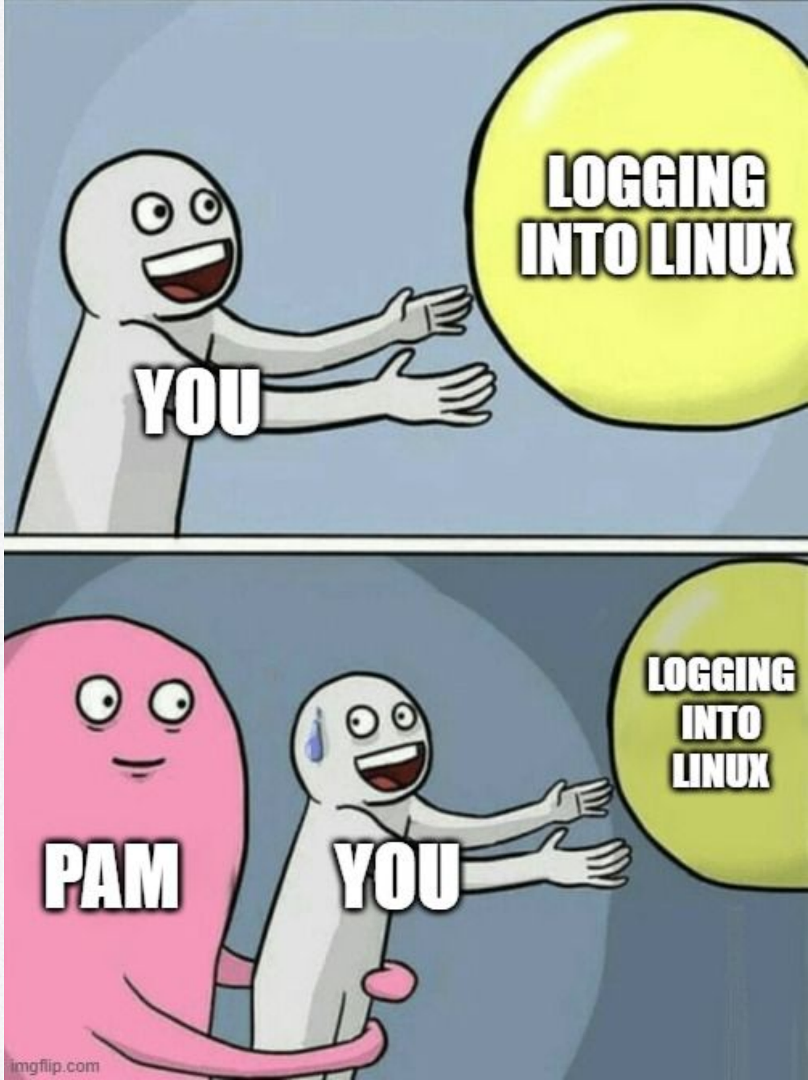
Debian-based	RHEL-based	Other
apt update	yum update	suffering
apt upgrade	yum upgrade	apk
apt install	yum install	pacman
apt purge/remove	yum remove/erase	solaris

02-04

PAM

What is PAM?

- pluggable authentication module
- manages authentication
- system-auth and password-auth



How fix PAM?

HERES WHERE ID
PUT MY SECURE PAM CONFIG
IF I HAD ONE
imgflip.com

Linux Tips & Tricks

- grep – Parse text using regular expressions
- cd - (“tack”) – Go to directory previously in
- cd ~ (tilde) – Go to user’s home directory
- Tab completion – Hit tab to autocomplete command
- Ctrl+L - clear terminal
- Ctrl+Shift+C and Ctrl+Shift+V – copy and paste into terminal (!CAUTION!)
- Ctrl+C – Kill running command
- Ctrl+R – Search command history
- Ctrl+U/Y – Cut everything before the cursor/Paste it back
- Home key/Ctrl+A, End Key/Ctrl+E – Go to beginning of line or end of line
- less – Different way to display contents of a file or command
- && and || – Run commands in sequence
- !! – Run previous command again
- yes – repeat input to answer prompts
- Alt+. – reuse recent arguments

03

Services

ba ga kingu

Common Linux Services

Web Server

Apache, Nginx,
Tomcat

Database

MySQL, Postgresql,
MongoDB

Mail Server

Postfix, Dovecot,
Exim, Squirrelmail

FTP Server

vsftpd, proftpd,
pureftpd, sftp vs ftps

DNS Server

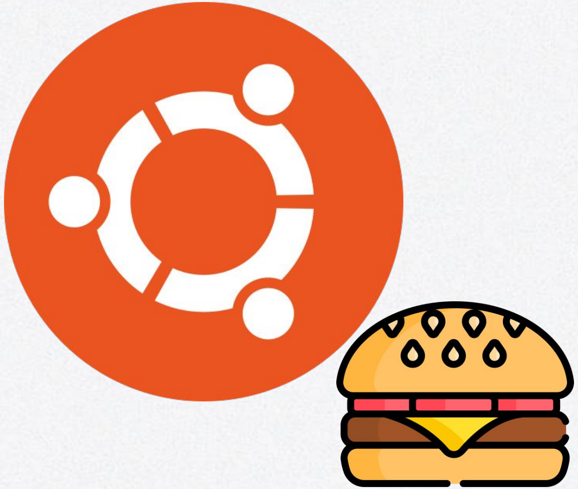
Bind9, named

VPN Server

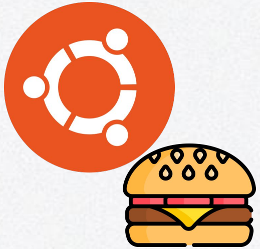
openvpn

baga kingu

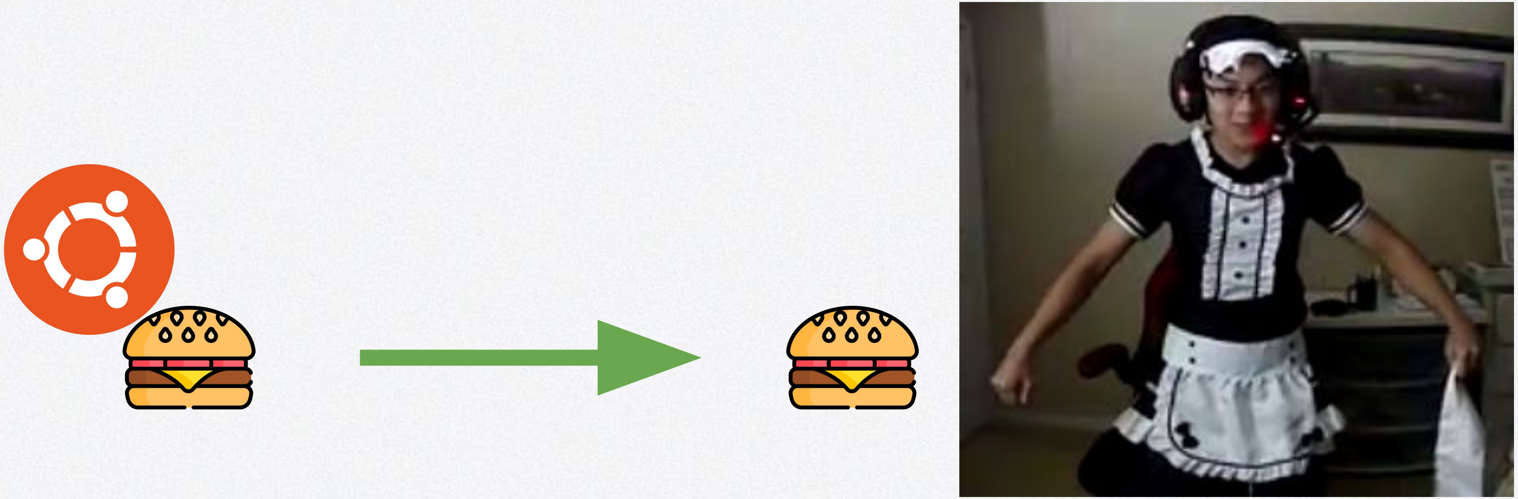
baga kingu



baga kingu

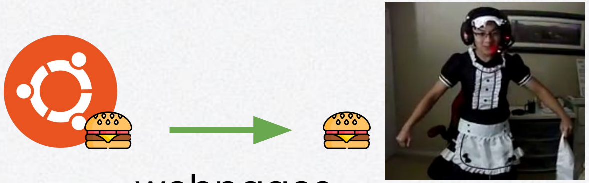


baga kingu



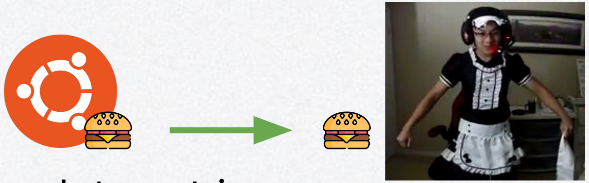
baga kingu

Web Server



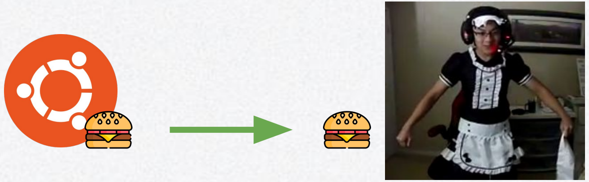
webpages

Database



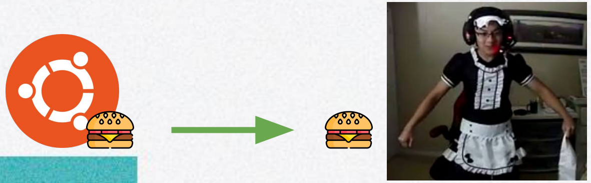
data entries

Mail Server



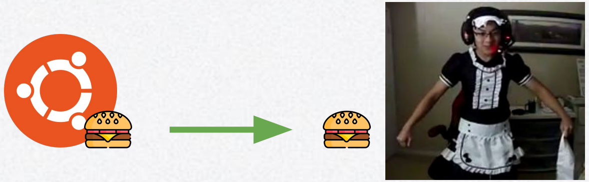
mail

FTP Server



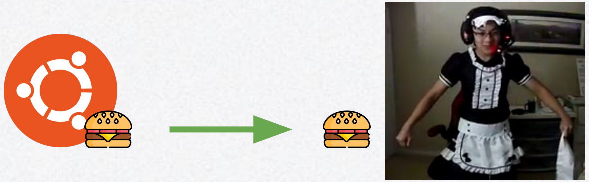
files

DNS Server



domain
records

VPN Server



traffic

How services work

In the kitchen	In Linux
Raw ingredients	Package
Make the burger	Service root/configs
Serve the burger	Systemd/Sysvinit

Identify your services

nmap

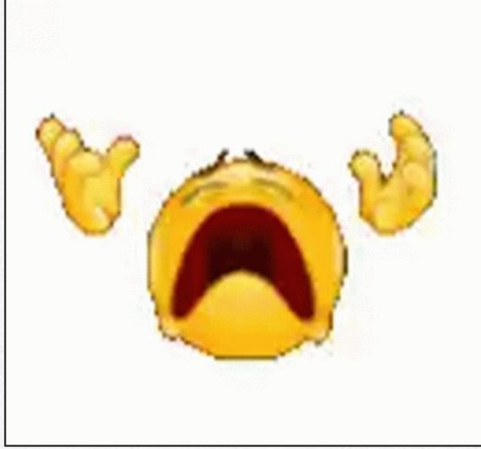
Scan your openings

netstat

View your connections

ps

Process your processes



04

Firewalling

when the fire is walling (idk i didnt pay attention during networking)

Not this kind of fyrwall...

Firewalls

- More ports = larger attack surface

- Firewalls should operate with the **Implicit Deny** principle

Block by default, allow by exception

IP Tables

3 Chains:

- INPUT
- OUTPUT
- FORWARD

Default Policy:

```
iptables --policy INPUT DROP
iptables --policy OUTPUT DROP
iptables --policy FORWARD DROP
```

Flush Rules:

```
iptables -F
```

List Rules:

```
iptables -L
```

Uncomplicated Firewall

Start/Stop

```
ufw enable/disable
```

Firewall Status:

```
ufw status
```

Default Policy:

```
ufw default deny
```

All Firewall Settings:

```
ufw status verbose
```

Flush rules:

```
ufw reset
```

04

~~Blooket~~ & LAB

LEMP Stack

me is also lab

How is Linux?

Tasks:

- Creds: ccdc:ccdc
- On bustin, run the command: `sudo dhclient`
- On bustin, create a new user and call it whatever you want
  - Add this user to the sudo group and change its password
  - Install the parts of a LEMP stack
    - L: Linux
    - E: Nginx
    - M: MySQL
    - P: PHP
  - Change the port of the web server to 8080
  - Create proper firewall rules so only resources that are critical to the LEMP stack are accessible