

Lustin' over Linux

Dylan

Sign-In: <https://da.gd/lustylinux>



Whoami

Dylan Tran

3rd Year CIS

Intern @ X-Force Red

CCDC

Linux Team 2021-2023

Linux Lead 2023-2024

CPTC

Team Member 2021-2023

Captain 2023-2024



Dylan Tran

@d_tranman

Next on Bronco CCDC...

When	What
July 8	Informational Meeting
July 15	Business Week
July 22	Intro to Networking
July 29	Lustin' over Linux
August 5	Wilding with Windows
August 12	Review Week
August 19-20	CPTC Tryouts - No meeting!
August 26-27	CCDC Tryouts!



You
are
here

01

Linux Basics

02

Linux Administration

03

Services

04

Firewall

01

Linux Basics

What is Linux

- **Not** an operating system
- Free & open-source **kernel**
- Built on **Unix** (unix-like)



Why Linux?



**Blazing
Fast**



**Super
Light**



**Amazingly
Extensible**

Quick Vocab

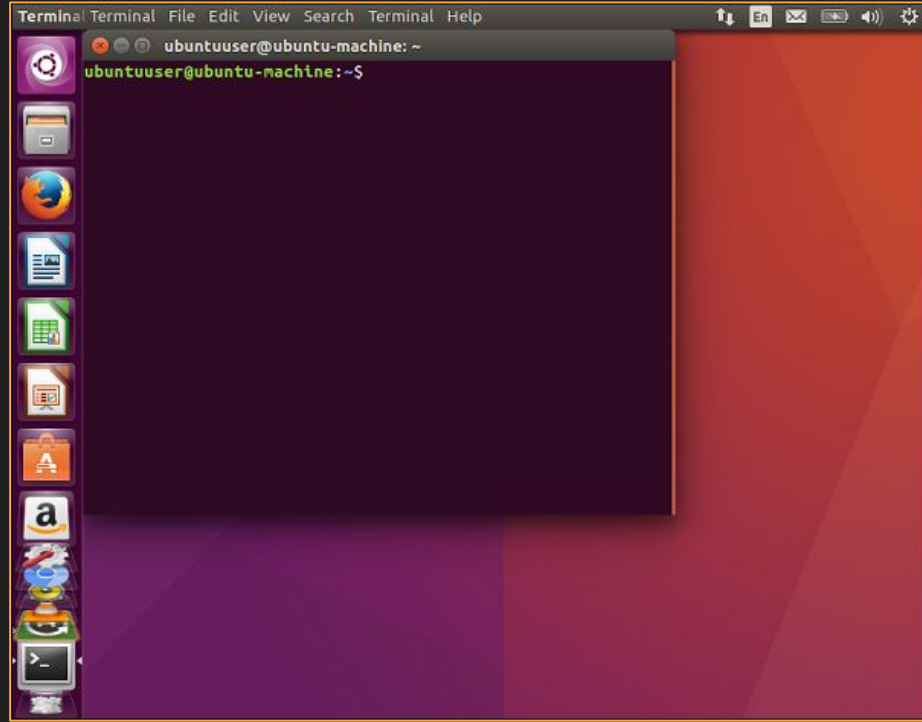
Terminal

Terminal Emulator

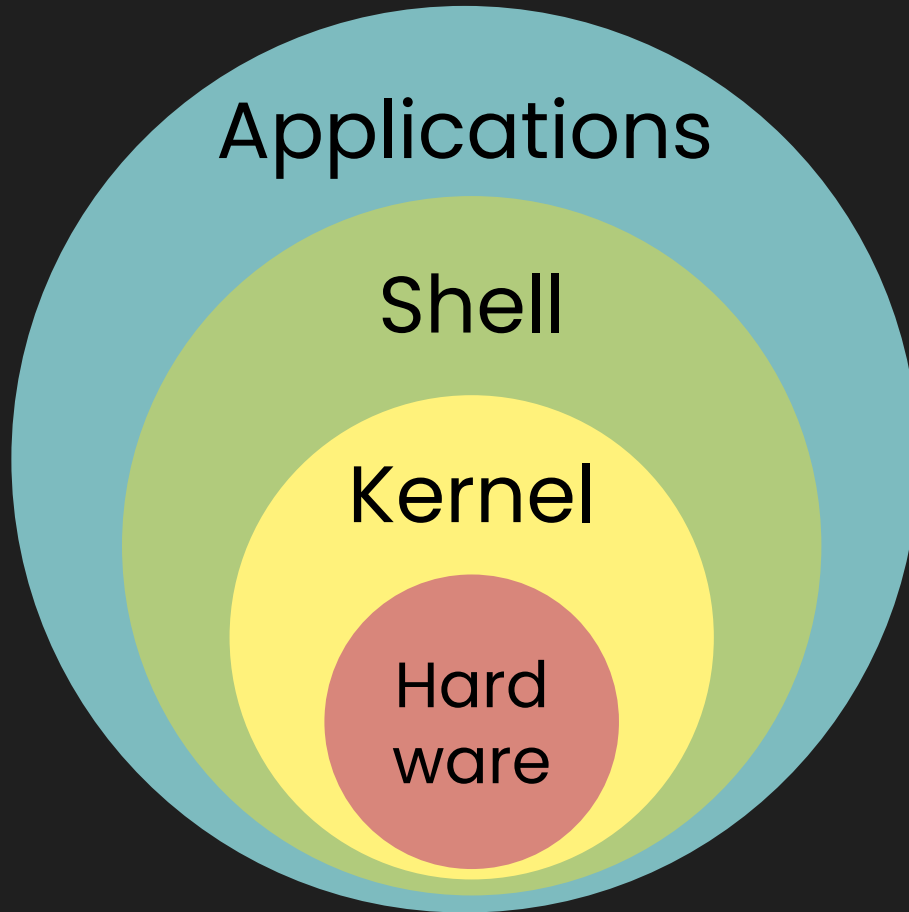
Shell

Kernel

Terminal



Terminal Emulator



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 /



root user (uid 0) = admin



root (/) directory = start of file system



root's home = /root

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/

\$PATH



\$PATH

The directory search order for commands you call

```
echo $PATH
```

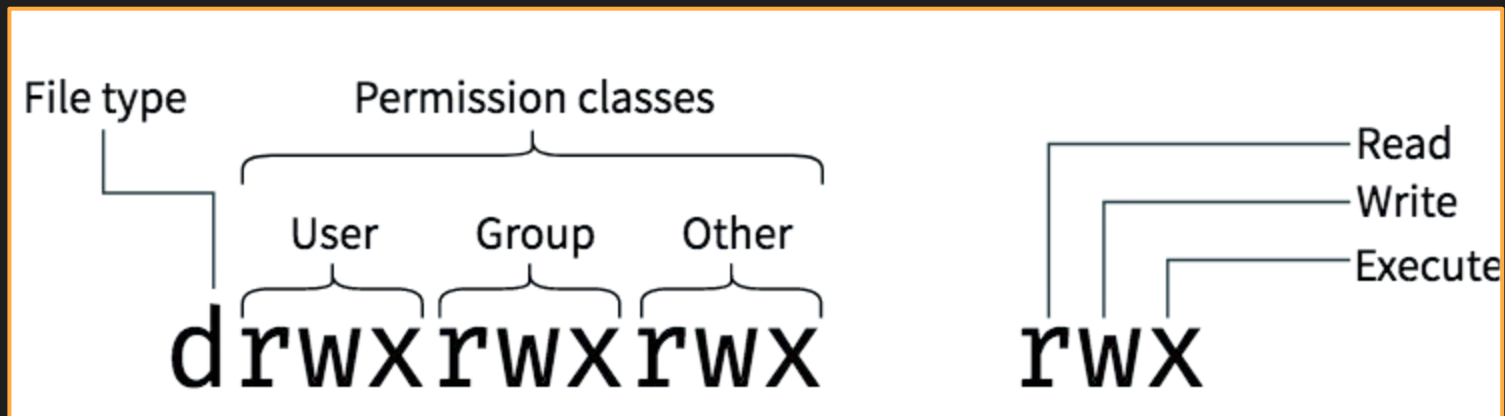


```
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

Aliases

```
root@ilikeguyslol:~# alias bruh='echo bruh'
root@ilikeguyslol:~# alias
alias bruh='echo bruh'
alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l='ls -CF'
alias la='ls -A'
alias ll='ls -aF'
alias ls='ls --color=auto'
root@ilikeguyslol:~# bruh
bruh
```

Linux File Permissions



Convert to octal

`rwXr-Xr-X`

Convert to rwx

`644`

Convert to octal

`r-X-W---X`

Convert to rwx

`777`

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

```
-bash-5.0$ chmod 777 file1
-bash-5.0$ chmod a+rwX file2
-bash-5.0$ ls -l
total 0
-rwxrwxrwx 1 nigerald nigerald 0 Jul 19 01:45 file1
-rwxrwxrwx 1 nigerald nigerald 0 Jul 19 01:45 file2
-bash-5.0$ chmod 744 file1
-bash-5.0$ chmod go+r file2
-bash-5.0$ ls -l
total 0
-rwxr--r-- 1 nigerald nigerald 0 Jul 19 01:45 file1
-rwxrwxrwx 1 nigerald nigerald 0 Jul 19 01:45 file2
```

Immutability

Make file immutable

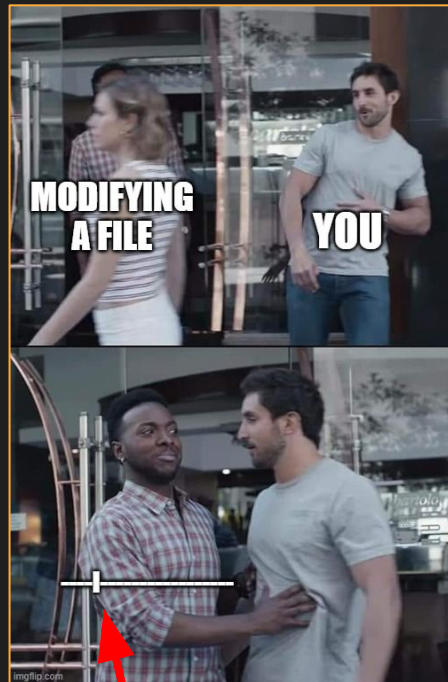
`chattr +i <file>`

Check for immutable bit

`lsattr <file>`

Remove immutable bit

`chattr -i <file>`



this is an i

Shell and Syntax

command -options arguments

- EXAMPLE: ls
- EXAMPLE: cd /home/user1
- EXAMPLE: ls -la user1/Downloads
- EXAMPLE: ls -R

Terminal Multiplexing (Tmux)

```
43
44 #AuthorizedPrincipalsFile none
45
46 #AuthorizedKeysCommand none
47 #AuthorizedKeysCommandUser nobody
48
49 # For this to work you will also need host keys in /
   etc/ssh/ssh_known_hosts
50 #HostbasedAuthentication no
51 # Change to yes if you don't trust ~/.ssh/known_hosts
   for
52 # HostbasedAuthentication
53 #IgnoreUserKnownHosts no
54 # Don't read the user's ~/.rhosts and ~/.shosts files
55 #IgnoreRhosts yes
56
57 # To disable tunneled clear text passwords, change to
   no here!
58 PasswordAuthentication no
59 #PermitEmptyPasswords no
60
61 # Change to yes to enable challenge-response passwords
   (beware issues with
62 # some PAM modules and threads)
63 ChallengeResponseAuthentication no
64
/etc/ssh/sshd_config [R0] 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_
```

Tmux Cheatsheet

Prefix: ctrl + b

Windows

- New Window: prefix + c
- Switch between Windows: prefix + [number] OR (p)revious OR (n)ext
- Delete Window: prefix + &

Panes

- Split Horizontally: prefix + "
- Split Vertically: prefix + %
- Switch between panes: prefix + [arrow key]

Other

- New Session: tmux
- Detach: prefix + d
- Reattach: tmux + a
- Fullscreen: prefix + z

02

Linux Administration

**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



**me typing (my wpm
is very high)**



Text Editors

NANO (Of Reliable)



nano <filename>



installed by default mostly



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 (le funni editor)



vim <filename>



can run commands in the editor



sometimes not installed by default



vimtutor to get started



extremely customizable



:wq to close and save file



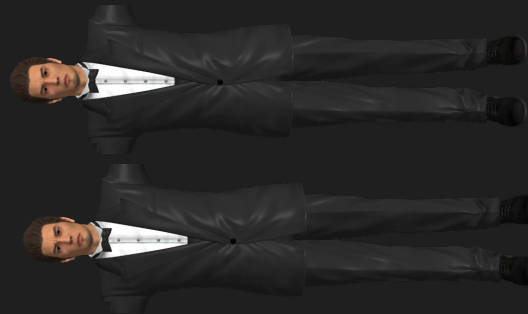
5 modes

```
#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



User & Permission Management

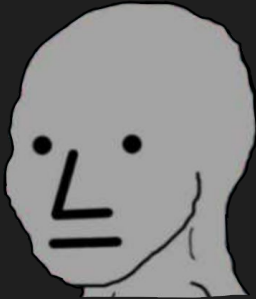


Permissions

root = 0



services < 1000



users > 999



I am groot

✓ 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

```
manav@ubuntulinux: ~  
manav@ubuntulinux:~$ sudo adduser username  
[sudo] password for manav:  
Adding user `username' ...  
Adding new group `username' (1001) ...  
Adding new user `username' (1001) with group `username' ...  
Creating home directory `/home/username' ...  
Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for username  
Enter the new value, or press ENTER for the default  
    Full Name []: username goes here  
    Room Number []:  
    Work Phone []:  
    Home Phone []:  
    Other []:  
Is the information correct? [Y/n] Y  
manav@ubuntulinux:~$
```



```
root@ilikeguyslol:~# useradd bruh
root@ilikeguyslol:~# tail -n 1 /etc/passwd
bruh:x:1002:1002::/home/bruh:/bin/sh
root@ilikeguyslol:~# ls -la /home/bruh
ls: cannot access '/home/bruh': No such file or directory
root@ilikeguyslol:~# tail /etc/shadow -n 1
bruh!:19558:0:99999:7:::
root@ilikeguyslol:~#
```

Managing Users



Group Management

not group policy

groups users together

✨**usermod**✨

✨**id**✨

Password Management



passwd

chpasswd



The Holy Trinity of User Management





The Holy ~~Trinity~~ Quadrinity Square of User Management

/etc/passwd

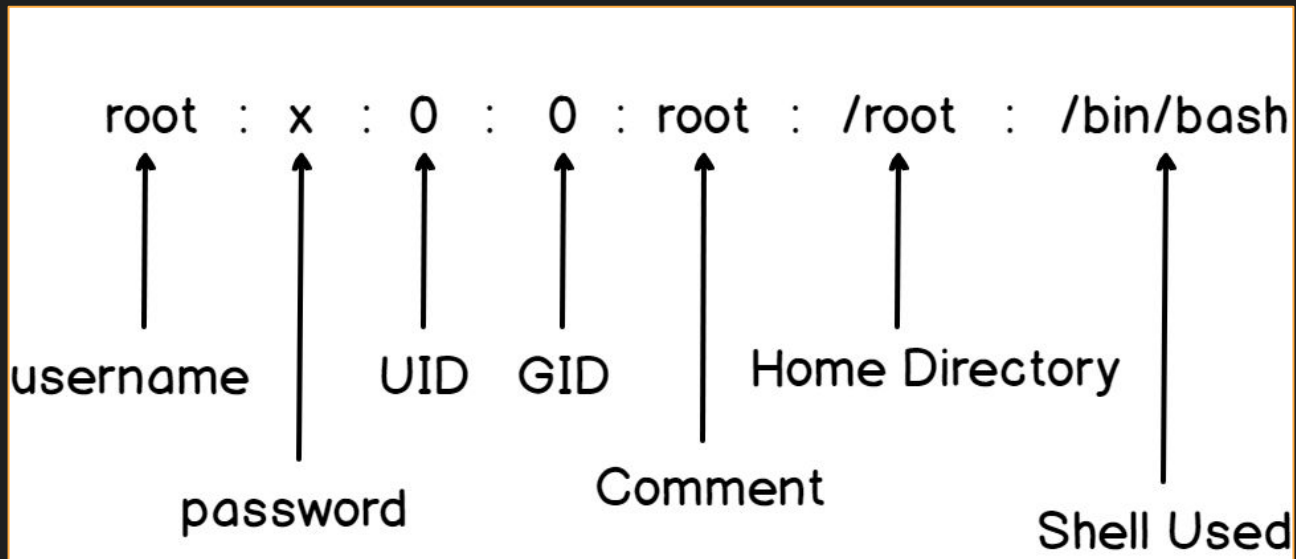
/etc/group



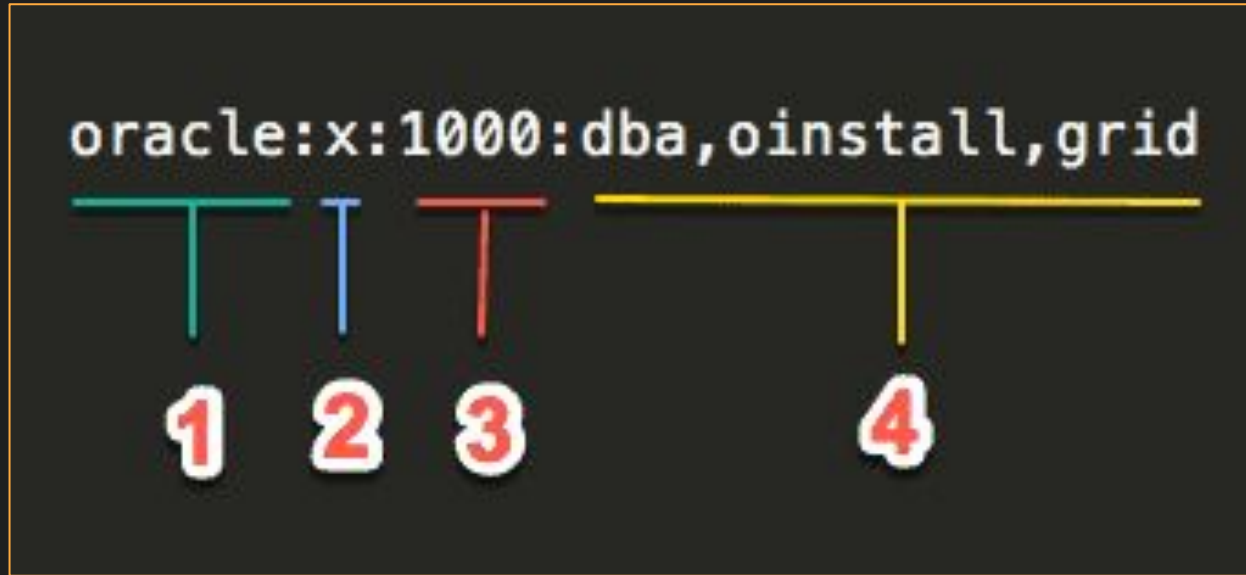
/etc/shadow

/etc/sudoers

/etc/passwd



/etc/group



/etc/shadow

vivek:\$1\$fnfffc\$GteyHdicpGOfffXX4ow#5:13064:0:99999:7:::

The diagram shows a /etc/shadow entry: vivek:\$1\$fnfffc\$GteyHdicpGOfffXX4ow#5:13064:0:99999:7:::. Below the entry, six arrows point to specific fields, which are numbered 1 through 6. Arrow 1 points to 'vivek', arrow 2 points to '\$1\$fnfffc\$GteyHdicpGOfffXX4ow#5', arrow 3 points to '13064', arrow 4 points to '0', arrow 5 points to '99999', and arrow 6 points to '7'.

Field Number	Field Value
1	vivek
2	\$1\$fnfffc\$GteyHdicpGOfffXX4ow#5
3	13064
4	0
5	99999
6	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
```



Packages, PAM, and other stuff

Different Distros

Debian-based

apt update

apt upgrade

apt install

apt purge/remove



RHEL-based

yum update

yum upgrade

yum install

yum remove/erase



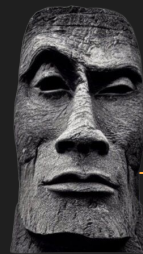
Other

suffering

apk


pacman


solaris



What is PAM?

 pluggable authentication module

 manages authentication

 system-auth and password-auth

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

Common Linux Services

Web Server

Apache, Nginx,
Tomcat

Database

MySQL, Postgresql,
MongoDB

Mail Server

Postfix, Dovecot,
Exim, Squirrelmail

FTP Server

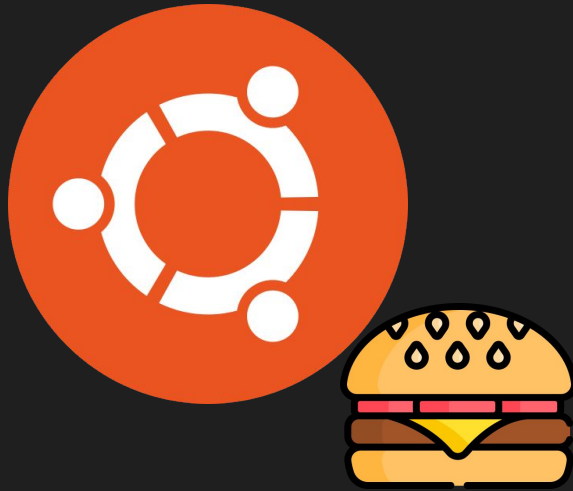
vsftpd, proftpd,
pureftpd, sftp vs ftps

DNS Server

Bind9, named

VPN Server

openvpn

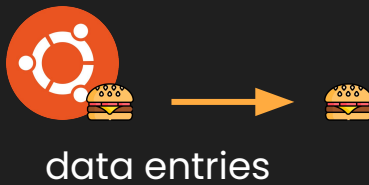




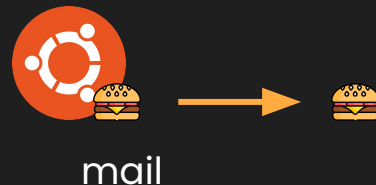
Web Server



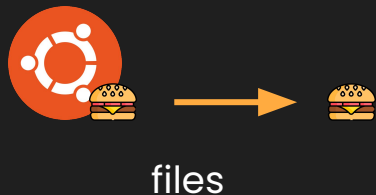
Database



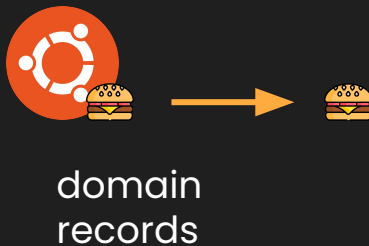
Mail Server



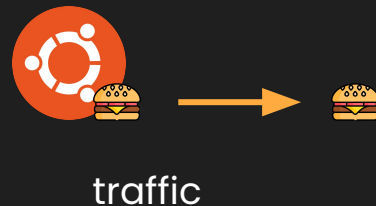
FTP Server



DNS Server



VPN Server



How services work

In the kitchen



Raw ingredients



Make the burger



Serve the burger

In Linux



Package



Service root/configs



Systemd/Sysvinit

Identify your services

nmap

Scan your openings

netstat

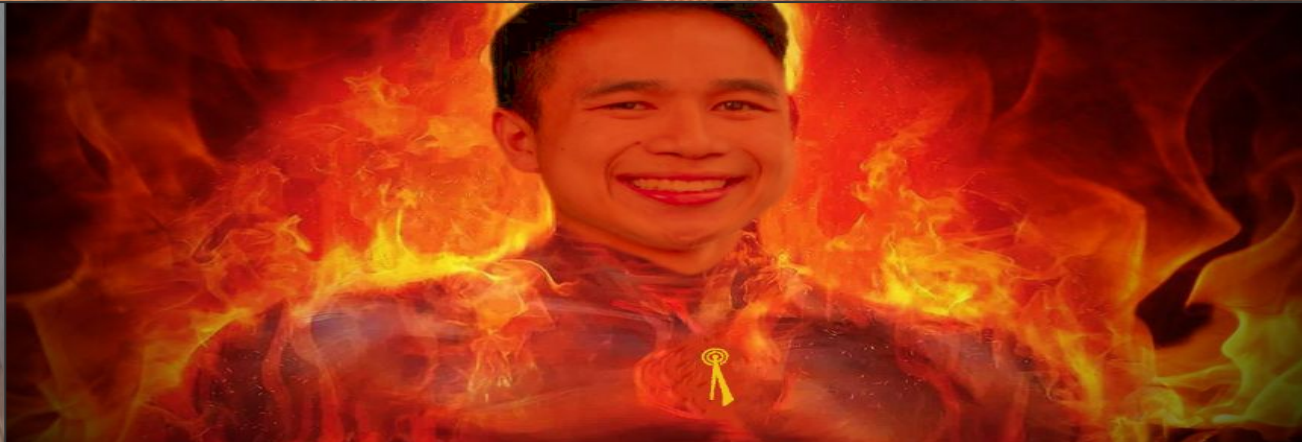
View your connections

ps


Process your processes

04

Firewalling



Firewalls

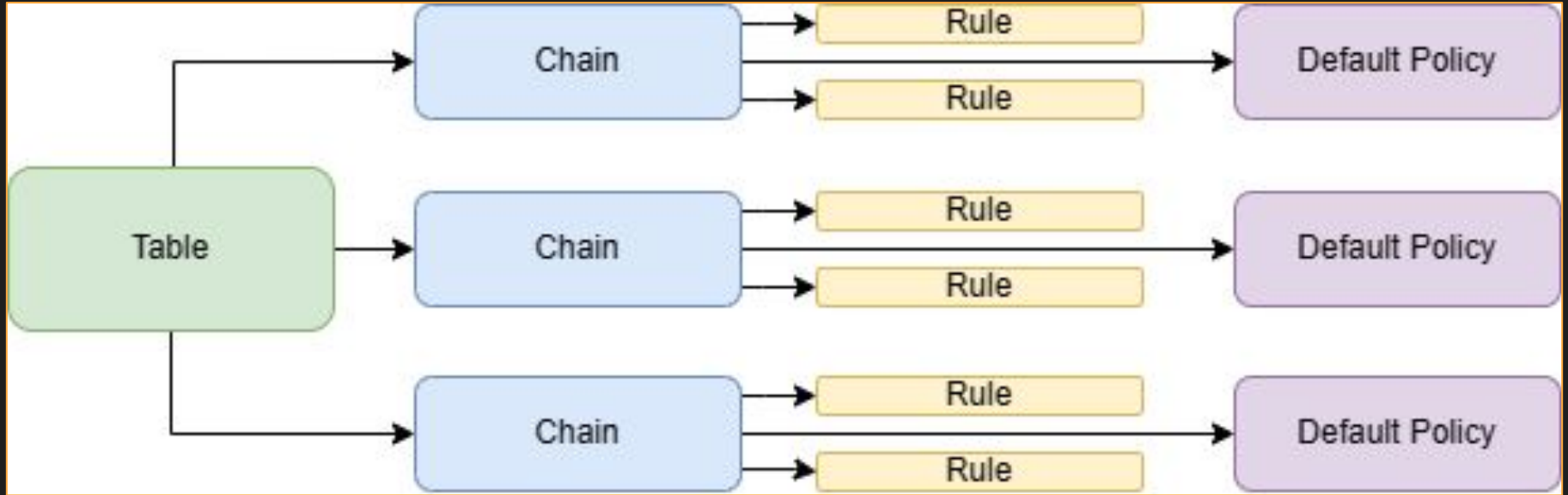
 More ports = larger attack surface

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

Block by default, allow by exception



IP Tables – Overview



IP Tables – Filter Table

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
```

IP Tables – Filtering Revshell Example

Allow incoming on 80

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Drop incoming packets if they do not match a rule

```
iptables -P INPUT DROP
```

Allow outgoing responsive connections

```
iptables -A OUTPUT -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

Drop outgoing packets if they do not match a rule

```
iptables -P OUTPUT DROP
```

05

Secret Lab Slide

TROUBLESHOOTING TIME!

Use the Ubuntu 20 machine named "FixMe" for this lab. The password for both user and root is "bruh". Fix all of the following and **document your steps with text, command snippets, screenshots, and/or all 3. Show proof that the fix works.**

1. FixMe's iptables command seems to be a bit funny
2. FixMe cannot hit the internet
3. Any user can switch into another user, even with the incorrect password being used
4. FixMe's SSH is not running
5. FixMe's SSH port doesn't seem to be right
6. FixMe's web server's index page is returning a 404
7. FixMe's "/test.php" is not rendering php
8. FixMe's FTP server doesn't seem to be serving the right files for the anonymous user
9. FixMe has a backdoor user
10. FixMe has a bunch of sudoers
11. FixMe has a backdoor in /opt
12. FixMe keeps generating files in the root directory