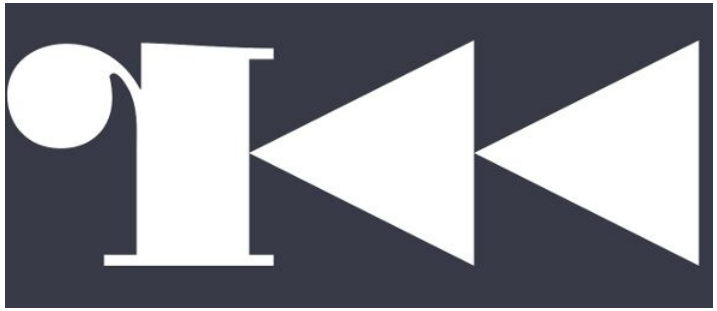


And other valuable commands you will use often.

THIS IS THE PART WHEN WE PUT THE FLAG ON THE BOARD

This is here so we don’t forget

This is not a tutorial on how to get into terminal.

If you are still not sure, thats okay! Go to *sigpwny.com/tutorial* and get set up :)

find

Find files! Most often by filename

```
find [directory] -name ‘spaghetti’

find [directory] -name ‘*.ext’
```

grep

Find text within files!

grep -r “text you want to find” .

grep -A -B -C -r “text you want to find”

cat | grep

strings

see what strings exist in a file

really good initial command for RE/PWN

Why does this command exist???

Some files are not human readable, this prints out all the human readable things

There may or may not be a useful challenge for this one.

file

Determine the file type of a file (what it really is)

Valuable to know what you are looking at before you start attacking/RE'ing something

gdb

Look at executables and slowly step through them.

We can run an entire meeting on gdb, and we will.

gdb --args “is a way to have command line arguments”

b = breakpoint

n = next

s = step

si = step instruction (use this one for binaries)

x = look at the stack

print = print variables

Get onto the pwny server!

https://github.com/sigpwny/sigpwny.github.io/wiki/How-to-get-on-the-SIGPwny-server

What is r2?

- R2 is a “”””great””” free disassembler
  - It is also known as “Radare2”
  - Easy to pick up the basics for
  - Clunky and weird to use, but can be used within your personal terminal
- You can install on your linux environment or ssh into sigpwny server
- A good starter disassembler

git

Git is difficult, we could do meetings on meetings on meetings. For this meeting, know the following.

git clone [url] [folder]

Clones a repository from a url

git add -A

stages all unadded files to the **repository**

git commit -m “Commit message”

Commits those stages to your personal **branch**

git push

Pushes your branch to the main branch

git pull

Pulls the latest changes from the main branch

Basics

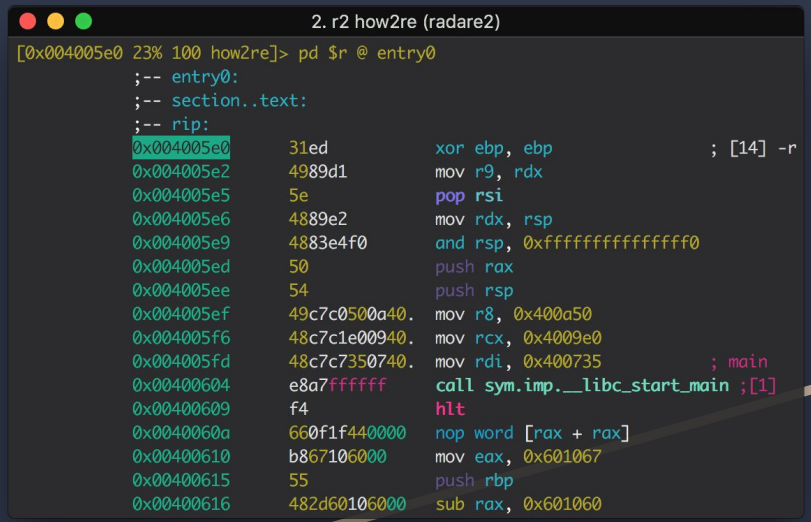
Open terminal

r2 fileName

Press v and then enter to activate visual mode

That looks pretty complicated… but we can make it look a lot easier to understand.

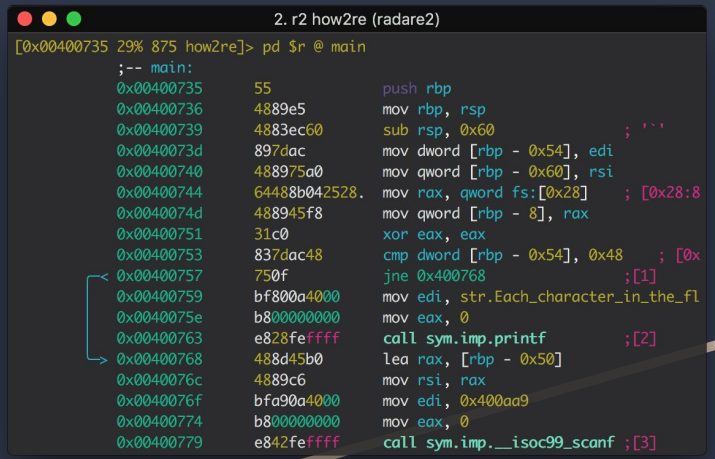
Print mode



Press p to toggle print mode (easier to see instructions)

You can navigate with the arrow keys, but that is slow.

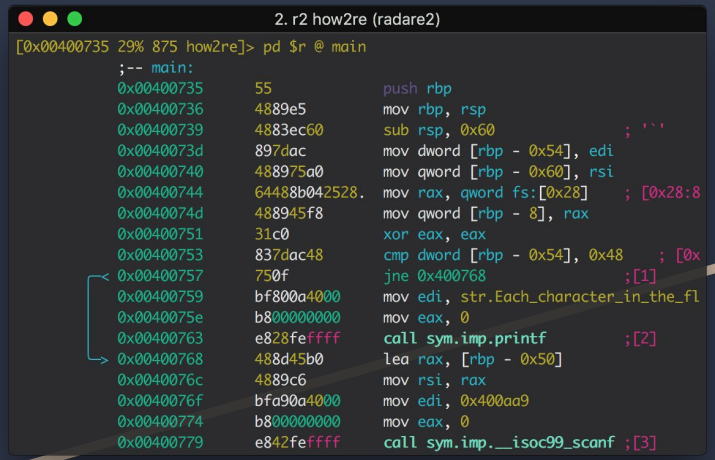
Moving faster



Press **n** and **N** to navigate between sections

You usually want to look for the **main** function, as that is where things are going on.

Making it even easier to read.

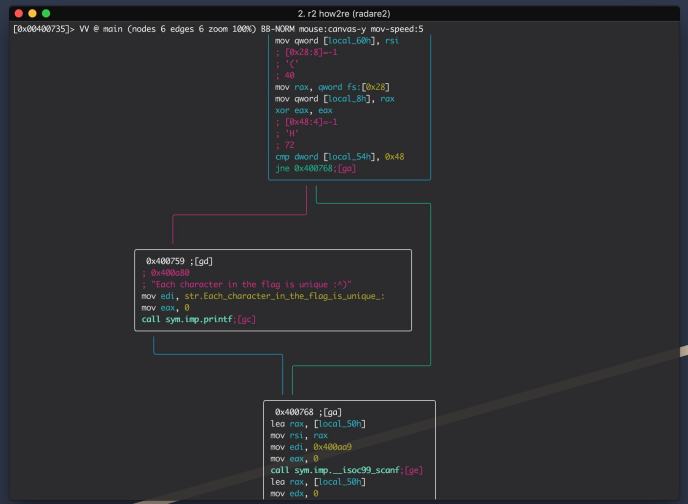


Press d, and then f.

d means define, and **f** is function.

This **defines** main as a **function,** and allows us to look at it in a much easier to understand way (visual representation)

Graphical Representation



Press V to enter visual mode, this allows you to see what is actually going on in the script in a nice visual way.

You can see where jumps go, true or false

Helpful Radare2 Book (From actual website)

https://radare.gitbooks.io/radare2book/content/first_steps/intro.html

tmux

A really jank way to keep processes running after you close the terminal window

(So basically the thing everyone uses)

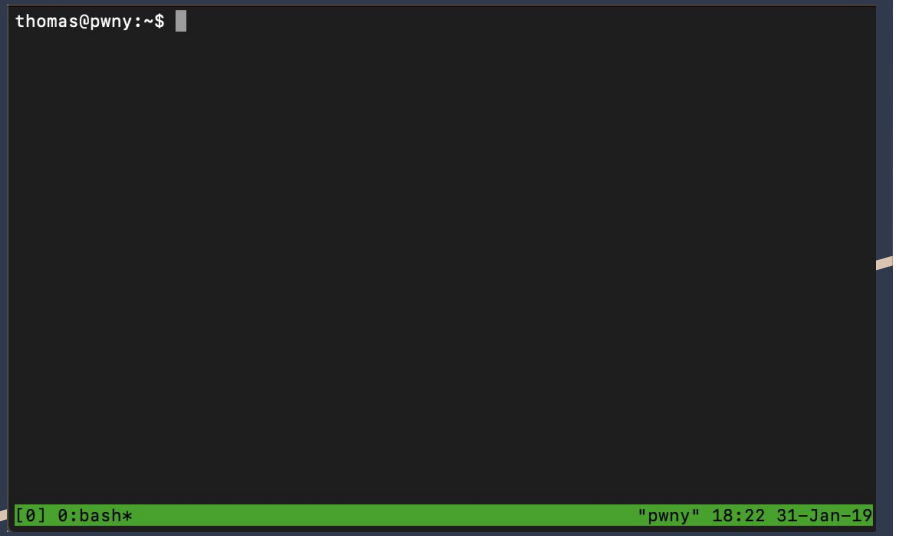
So if you want to… keep a ctf up, run a file sharing system, or run a Minecraft Server without needing a terminal window open.

How to install tmux

It would be a good learning experience if you figure out how to install bash extensions on your operating system. So go try to do that.

It may also already be installed, the command is...
tmux

tmux basics



To create a new window type **tmux**

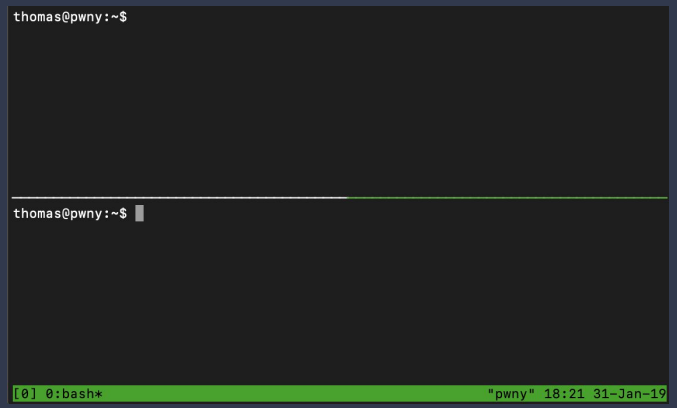
This will open up a new tmux window for you to use.

Mess around with it see what you can do, it is a fully functioning bash window.

NEVER nest multiple tmux windows

Just a bad idea ;P

tmux commands



The command prefix is cntrl + b + ____, some things you can do with this are

- d : detatch your terminal from the tmux window
  - This will keep anything you had running, still running.
  - You can get back to that session with **tmux at -t (number_of_session)**
- “ : horizontal split of terminal
- %: vertical split of terminal
- Force close split
  - Ctrl-d, **exit**

Detaching windows

- Cntrl+b + d to detatch a window
  - Will run REALLY long
- Reattach
  - tmux attach -t NUMBER
  - tmux ls
  - tmux new -s NAME
  - tmux rename-session -t NUMBER NAME

Easy tutorial

https://www.hamvocke.com/blog/a-quick-and-easy-guide-to-tmux/

Vim

- Vim is an in terminal text editor
- It is NOT an IDE
- **vim** to open new vim window

EXIT VIM with :wq (colon + wq)

i = Insert Mode

dd = delete line

p = paste deleted line

:tabnew FILE_NAME = open new tab, gt to navigate tabs

:LINE_NUMBER = jump to line number

Use .vimrc!!!