Radare2 tutorial learn:

V – for visual view

p – for ascii view, and then assembly view, and other views

arrows to go **up** and **down**, and **left** and **right**

Enter – for entering a function, if the seek is on the function, it is same as **s function**

Use **:** and then **aaa** for analyze

Use **afl** for function list, **afll** for more detailed

Use **s** to change seek, for example: **s main**

u for going back after entering a function

axt for view cross-refercing, after putting the seek in the function

the currenct function is presented at the top of radare2 view (in disassembly mode)

axf for from-reference, and not to-reference. (a – analyze, x – xross-reference, f-from (instead of t-to))

q for quiting from view-screen

i? – I stands for the info, and ? for helping. That is the way how to get help and staff. (for example, s?)

ii – for info imports

iE – for info exports

iS – for info sections

is – for info symbols

iz – info string in sections, **izz** for whole binary file

rabin2 can be used outside of radare2, it does the same as r2, but outside.

rabin2 -I .\tutorial.exe, get info about file.

Arch, canary, language, nx, base address, etc

rabin2 -H .\tutorial.exe, get header info (same as cff)

rabin2 -M .\tutorial.exe, for getting main address

rabin2 -zz .\tutorial.exe, for getting all strings. (same as iz in r2)

****

rafind2 for searching in binary file

rafind2 -s Hello .\tutorial.exe to search for strings in a binary file

****

r2 -nn .\tutorial.exe, starting without any r2 configuration. **nn** stands for non ini, without r2.ini

****

Patching binaries:

r2 -w .\tutorial.exe for opening with write privialges, there a several ways of **w**, only types **w?**

A for change a line, after put the seek on it

****

Debugging.

r2 -d .\tutorial.exe for enter debug mode

e stack.size = 128 for change stack size

db main for breakpoint, debug breakpoint

db for view break points

dc debug continue, same as **f8**, not enter functions

ds debug step, same as **f7**, enters functions.

There is seek, and ip! They aren't the same. To return to ip, only type **.**

Step out of func is **dsf**, step out of frame

We can do both with visual mode and :> mode

dcu main for debug continue until main, means to restart the program until reaching main

****

VV for visual graph mode

You can functions with typing the two letters that are found near the functions call, for example, **ge** and **oa**.

Visual mode graph is same as before, in aspects of **p** and staff.

You can use **X**, like In IDA, instead of **axt**. (if your seek is on what you are looking for)

****

In order to add a comment, only hit **:** and then add your comments.

In order to remove a comment, hit **:** and then **–**

****

afl~main, the ~ stands for grep, so we loop for main

pdf~call, pdf stands for print disassembly functions, and then get all calls.

/ad/ cmp, al for searching all “cmp al…” instructions

****

Control pannel.