Radare2!

By: MIDN J. R. Libby

The Basics

Doc Link: https://www.kali.org/tools/radare2/

Git Link: https://github.com/radareorg/radare2

What this tool does:

Radare2 is an open-source framework for reverse engineering and analyzing files. It provides a tools for disassembly, debugging, and editing executable files. It supports various languages and formats. Its command line interface and scripting capabilities make it powerful for both beginners and advanced users in reverse engineering and software analysis.

How To Install

Clone from github:

```
┌──(kali㉿kali)-[~/radare2]
└─$ git clone https://github.com/radareorg/radare2
```

```
┌──(kali㉿kali)-[~/radare2/radare2]
└─$ ls
autogen.sh    configure      configure.hook      CONTRIBUTING.md  DEVELOPERS.md  env.sh      libr      man           mk          preconfigure.bat  SECURITY.md  test
binr          configure.acr  configure-plugins    COPYING          dist           global.mk   make.bat  meson.build   pkgcfg      README.md         shlr         USAGE.md
COMMUNITY.md  configure.bat  config-user.mk.acr  COPYING.LESSER   doc            INSTALL.md  Makefile  meson_options.txt  preconfigure  scripts  sys  vsfix.bat
```

Usage:

```
┌──(kali㉿kali)-[~/pentesting/pico/c0rrupt]
└─$ ls
mystery  mystery.png  search

┌──(kali㉿kali)-[~/pentesting/pico/c0rrupt]
└─$ r2 mystery
```

Use command: man r2
To find man page.

```
RADARE2(1)                                                    BSD General Commands Manual

NAME
     radare2 – Advanced command-line hexadecimal editor, disassembler and debugger

SYNOPSIS
     radare2 [-a arch] [-b bits] [-B baddr] [-c cmd] [-e k=v] [-i file] [-I prefile] [-k kernel] [-m addr] [-p project] [-P patch
```

To View Files

Use r2 -w *filename* to enter a writable mode in Radare2

Use V to navigate, analyze, and view files.

```
┌──(kali㉿kali)-[~/pentesting/pico/c0rrupt]
└─$ r2 -w mystery
[0x00000000]> V
```

```
[0x00000000 [Xadvc]0 0% 880 mystery]> xc
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF  comment
0x00000000  8965 4e34 0d0a b0aa 0000 000d 4322 4452  .eN4........C"DR
0x00000010  0000 066a 0000 0447 0802 0000 007c 8bab  ...j...G.....|..
0x00000020  7800 0000 0173 5247 4200 aece 1ce9 0000  x....sRGB.......
0x00000030  0004 6741 4d41 0000 b18f 0bfc 6105 0000  ..gAMA......a...
0x00000040  0009 7048 5973 aa00 1625 0000 1625 0149  ..pHYs...%...%.I
0x00000050  5224 f0aa aaff a5ab 4445 5478 5eec bd3f  R$........DETx^..?
0x00000060  8e64 cd71 bd2d 8b20 2080 9041 8302 08d0  .d.q.-.  ..A....
0x00000070  f9ed 40a0 f36e 407b 9023 8f1e d720 8b3e  ..@..n@{.#... .>
0x00000080  b7c1 0d70 0374 b503 ae41 6bf8 bea8 fbdc  ...p.t...Ak.....
0x00000090  3e7d 2a22 336f de5b 55dd 3d3d f920 9188  >}*"3o.[U.==. ..
0x000000a0  3871 2232 eb4f 57cf 14e6 25ff e5ff 5b2c  8q"2.OW...%...[,
0x000000b0  168b c562 b158 2c16 8bc5 62b1 582c 161d  ...b.X,...b.X,..
0x000000c0  d6d7 678b c562 b158 2c16 8bc5 62b1 582c  ..g..b.X,...b.X,
0x000000d0  168b 4597 f5f5 d962 b158 2c16 8bc5 62b1  ..E....b.X,...b.
0x000000e0  582c 168b c562 d165 7d7d b658 2c16 8bc5  X,...b.e}}.X,...
0x000000f0  62b1 582c 168b c562 b158 7459 5f9f 2d16  b.X,...b.XtY_.-.
0x00000100  8bc5 62b1 582c 168b c562 b158 2c16 5dd6  ..b.X,...b.X,.].
```

To Edit Files

Use c and navigate to the hex you want to edit: can be seen by the highlighted characters

```
[0x00000000 *0x00000012 [Xadvc]0 ($$+0x12)]> xc
- offset - | 0 1  2 3  4 5  6 7  8 9  A B  C D  E F| 0123456789ABCDEF  comment
0x00000000 |8965 4e34 0d0a b0aa 0000 000d 4322 4452| .eN4.... ... .C"DR
0x00000010 |0000 066a 0000 0447 0802 0000 007c 8bab| ..j..G.. ... |..
0x00000020 |7800 0000 0173 5247 4200 aece 1ce9 0000| x....sRGB.....
0x00000030 |0004 67a5 4d41 0000 b18f 0bfc 6105 0000| ..g.MA.. ....a...
0x00000040 |0009 7048 5973 aa00 1625 0000 1625 0149| ..pHYs..%..%.I
```

Then, use i to insert the desired hex value!

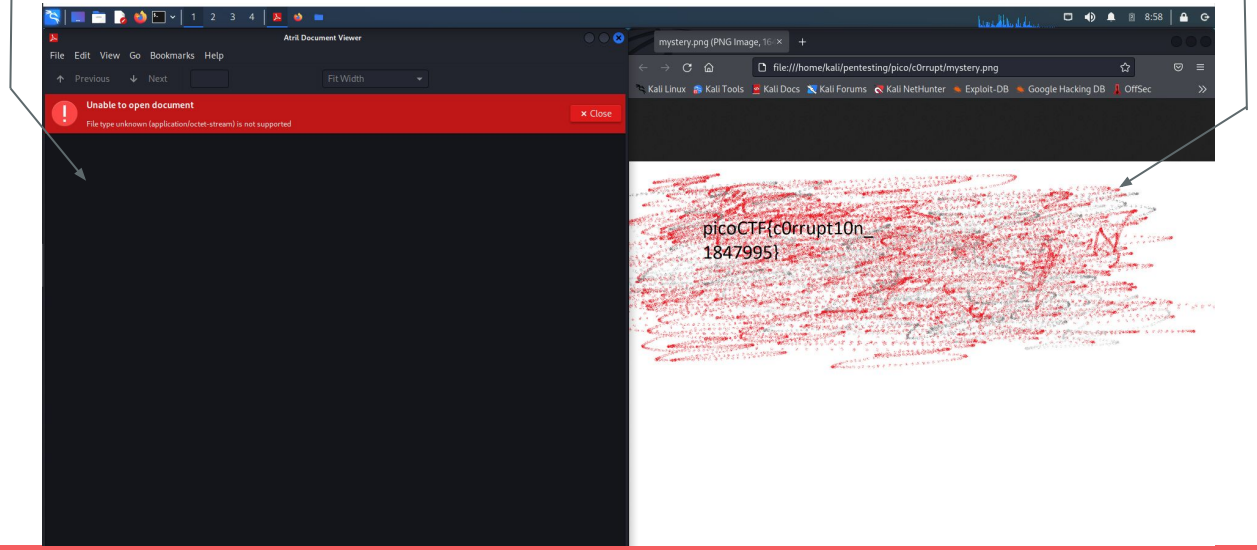
```
[0x00000000 + 18> * INSERT MODE *
- offset - | 0 1  2 3  4 5  6 7  8 9  A B  C D  E F| 0123456789ABCDEF  co
0x00000000 |8965 4e34 0d0a b0aa 0000 000d 4322 4452| .eN4.... ... .C"DR
0x00000010 |0000 ff6a 0000 0447 0802 0000 007c 8bab| ...j..G.. ... |..
0x00000020 |7800 0000 0173 5247 4200 aece 1ce9 0000| x....sRGB.....
0x00000030 |0004 67a5 4d41 0000 b18f 0bfc 6105 0000| ..g.MA.. ....a...
0x00000040 |0009 7048 5973 aa00 1625 0000 1625 0149| ..pHYs..%..%.I
0x00000050 |5224 f0aa aaff a5ab 4445 5478 5eec bd3f| R$....DETx^..?
```

OK, but how is this useful for me?

Well, we can use it for reverse engineering, digital forensics, and to fix corrupted or encrypted files as seen below.

Corrupt File

File after tweaking the hex



So Many Uses!

There are a plethora of uses for Radare2.

Find one that suits your needs!