The patch for installation r2ghidra to latest radare2 version

(by : unixfreaxjp / 20201216)

1. The background

I have noticed that r2ghidra has been changed and recent installation (from early December) can not perform the installation of r2ghidra decompiler plugin.

What really upset me is, there is no announcement that the incapability to install r2ghidra on radare2 will occur from the r2ghidra or ghidra plugin development side (since obviously they are the one who suddenly made changes based on the recent changes in the Github) , as the impact it is clearly shown that radare2 users are the ones who suffer for the result.

As a radare2 long time user, I introduced radare2 to many people in my community, so I feel being obligated to make a workaround on the issue by providing the patch and writing this document, while pancake and team will fix this problem in the next release.

2. Installation of radare2 latest stable version (4.5.1)

You need to have the latest stable version of radare2, I recommend version **4.5.1** for the generalization of the filenames and paths etc to make this patch installation work well.

After you download and extract the r2 package you should edit these two lines in **sys/install.sh** before making the installation to make sure no update has been made. This way you will have the pure offline release version in your box.

```
# find root
cd "$(dirname "$0")" ; cd ..

# update
if [ "$1" != "--without-pull" ]; then
        if [ -d .git ]; then
# [redacted]            git branch | grep "^¥* master" > /dev/null
                if [ $? = 0 ]; then
                        echo "WARNING: Updating from remote repository"
# [redacted]                    git pull
                fi
        fi
else
        export WITHOUT_PULL=1
        shift
fi

umask 0002

export NOSUDO
if [ -n "${NOSUDO}" ]; then
        SUDO=""
else
```

You can install by executing **sys/install.sh** until all radare2 installation is done to here:

```
cd ~/usr/local/lib/radare2/~ ;¥
        rm -f last ; ln -fs 4.5.1 last
cd ~/usr/local/share/radare2/~ ;¥
        rm -f last ; ln -fs 4.5.1 last
mkdir -p ~/usr/local/share/radare2/4.5.1/~
/bin/sh sys/ldconfig.sh
/bin/sh ./configure-plugins --rm-static //usr/local/lib/radare2/last/
configure-plugins: Loading ./plugins.cfg ..
Removed 0 shared plugins that are already static
```

Then in the radare2 root of installation directory setup the r2pm by command **r2pm init** and then **r2pm update** ; you will see the result something like this.

```
git clone https://github.com/radareorg/radare2-pm
Cloning into 'radare2-pm'...
remote: Enumerating objects: 189, done.
remote: Counting objects: 100% (189/189), done.
remote: Compressing objects: 100% (179/179), done.
remote: Total 189 (delta 27), reused 67 (delta 8), pack-reused 0
Receiving objects: 100% (189/189), 52.46 KiB | 0 bytes/s, done.
Resolving deltas: 100% (27/27), done.
/home/[redacted]/.local/share/radare2/r2pm/git/radare2-pm
r2pm database initialized. Use 'r2pm update' to update later today.
[redacted]~/radare2-TEST/radare2-4.5.1$ r2pm update
HEAD is now at 163fbe1 Add esilsolve package
Updating 163fbe1..a51ae13
Fast-forward
 db/esilsolve    | 1 +
 db/rlang-python | 1 +
 db/rlang-vlang  | 1 +
 3 files changed, 3 insertions(+)
Updating /home/[redacted]/.local/share/radare2/r2pm/db ...
Already up-to-date.
```

Let's perform the normal installation for the r2ghidra first with the below r2pm command

$ r2pm install r2ghidra

(noted, radare2 changed r2ghidra's plugin base name from **r2ghidra-dec** to **r2ghidra**)

And you will see the message showing it fetches recent components from the several github repositories including the r2ghidra and ghidra components needed to make the ELF module plugin needed by radare2 to parse the code to ghidra's sleighs binary:

```
Cloning into 'r2ghidra'...
remote: Enumerating objects: 88, done.
remote: Counting objects: 100% (88/88), done.
remote: Compressing objects: 100% (86/86), done.
remote: Total 88 (delta 1), reused 39 (delta 0), pack-reused 0
Unpacking objects: 100% (88/88), done.
Submodule 'ghidra/ghidra' (https://github.com/thestr4ng3r/ghidra.git) registered for path 'ghidra/ghidra'
Submodule 'third-party/pugixml' (https://github.com/zeux/pugixml.git) registered for path 'third-party/pugixml'
Cloning into '/home/    /.local/share/radare2/r2pm/git/r2ghidra/ghidra/ghidra'...
remote: Enumerating objects: 70865, done.
Receiving objects:  98% (69448/70865), 106.64 MiB | 15.84 MiB/s
```

3. The problem with installation of r2ghidra

And you will see plenty of installation errors like this caused by it seems now r2ghidra is not supporting radare2 software's code, and it is not leaving any compatibility option either to the previous radare2 code. You will see that clearly in the error message if you scroll up.

```
/home/    /.local/share/radare2/r2pm/git/r2ghidra/src/SleighAnalValue.cpp:244:18: error: 'R_ANAL_VAL_REG' was not declared in this scope
       tmp.type = R_ANAL_VAL_REG;
                  ^~~~~~~~~~~~~~

/home/    /.local/share/radare2/r2pm/git/r2ghidra/src/SleighAnalValue.cpp: In member function 'void SleighAnalValue::mem(uint4)':
/home/    /.local/share/radare2/r2pm/git/r2ghidra/src/SleighAnalValue.cpp:267:2: error: 'type' was not declared in this scope
  type = R_ANAL_VAL_MEM;
  ^~~~

/home/    /.local/share/radare2/r2pm/git/r2ghidra/src/SleighAnalValue.cpp:267:9: error: 'R_ANAL_VAL_MEM' was not declared in this scope
  type = R_ANAL_VAL_MEM;
         ^~~~~~~~~~~~~~

CMakeFiles/anal_ghidra.dir/build.make:108: recipe for target 'CMakeFiles/anal_ghidra.dir/src/SleighAnalValue.cpp.o' failed
make[2]: *** [CMakeFiles/anal_ghidra.dir/src/SleighAnalValue.cpp.o] Error 1
make[2]: *** Waiting for unfinished jobs....
Scanning dependencies of target asm_ghidra
[ 97%] Building CXX object CMakeFiles/asm_ghidra.dir/src/SleighAsm.cpp.o
[ 98%] Building CXX object CMakeFiles/asm_ghidra.dir/src/SleighInstruction.cpp.o
CMakeFiles/Makefile2:152: recipe for target 'CMakeFiles/anal_ghidra.dir/all' failed
make[1]: *** [CMakeFiles/anal_ghidra.dir/all] Error 2
make[1]: *** Waiting for unfinished jobs....
[ 98%] Building CXX object CMakeFiles/asm_ghidra.dir/src/asm_ghidra.cpp.o
/home/    /.local/share/radare2/r2pm/git/r2ghidra/src/asm_ghidra.cpp:88:18: warning: 'radare_plugin' initialized and declared 'extern'
 R_API RLibStruct radare_plugin = {
                  ^~~~~~~~~~~~~

[ 99%] Linking CXX shared library asm_ghidra.so
[ 99%] Built target asm_ghidra
WARNING riscv.table.sinc:30: Unreferenced table 'rs1W'
WARNING riscv.table.sinc:37: Unreferenced table 'rdW'
WARNING riscv.table.sinc:160: Unreferenced table 'FRM'
WARNING riscv.table.sinc:176: Unreferenced table 'crs1'
WARNING riscv.table.sinc:230: Unreferenced table 'clqimm'
WARNING riscv.table.sinc:232: Unreferenced table 'cldspimm'
[ 99%] Built target sla
Makefile:149: recipe for target 'all' failed
make: *** [all] Error 2
```

(the image of installation failure in recent r2ghidra via radare2)

4. The workaround to install r2ghidra to radare2

So, don't worry, here is a workaround to make r2ghidra in radare2 works again as workaround until radare2 development fix this permanently

4.1. You will need to download this patch (zip file) contains of :

- r2ghidra full compilation source

- r2pm tweak to perform installation of r2ghidra locally
- r2ghidra database for r2pm

Save the patch zip file anywhere depending on your flavor, to the directory unrelated to radare2 file distribution is good. And then extract it (you can use the /temp or /var/temp if you want).

```
$
$ ls r2ghidra-build*
r2ghidra-build-patch.zip
$
$ unzip r2ghidra-build-patch.zip
Archive:  r2ghidra-build-patch.zip
   creating: patch/
  inflating: patch/r2ghidra-allsrc-20200730.tgz
  inflating: patch/r2ghidra-pdg
  inflating: patch/r2pm-pfg
  inflating: patch/README.txt
$
$ cd patch/
$ ls
README.txt  r2ghidra-allsrc-20200730.tgz  r2ghidra-pdg  r2pm-pfg
$
$
```

Explanation of the files:

1. **r2ghidra-allsrc-xxx.tgz** : the all git sources for work version for r2ghidra
2. **r2ghidra-pdg** : the r2pm database patch needed to install work version for r2ghidra
3. **r2pm-pfg** : the r2pm patch meant to execute the local installation of r2ghidra

4.2. How to install the patch

You need to deploy the patch manually to your radare2 flavors, the steps are:

- Copy the **r2pm-pfg t**o below directory and making sure it has an execution permission:

  $ cp **r2pm-pfg** ~/{any path}/radare2-4.5.1/binr/r2pm/**r2pm-pfg**
  $ chmod 755 ~/{any path}/radare2-4.5.1/binr/r2pm/**r2pm-pfg**

- **Go to the r2pm database directory and backup the r2ghidra file and install r2 ghidra-pdg**

  $ cd ~/.local/share/radare2/r2pm/git/radare2-pm/db/
  $ mv r2ghidra r2ghidra-original

  Check the backup by this command:

  $ ls ~/.local/share/radare2/r2pm/db/r2ghidra-original
  /home/$USER/.local/share/radare2/r2pm/db/r2ghidra-original

Now copy the **r2ghidra-pfg** into **r2ghidra** in the database directory:

$ cp {path/to}/**r2ghidra-pdg** ~/.local/share/radare2/r2pm/db/**r2ghidra**

- Now extract and replace the contains of r2ghidra git local version in tgz into current path in **~/.local/share/radare2/r2pm/git/r2ghidra** . You can set your default permission and ownership file attribute for this data.

```
$ cd  ~/.local/share/radare2/r2pm/git/r2ghidra
$
$ ls -l
total 52
-rw-r--r-- 1 2816 Jul 30 18:59 CMakeLists.txt
-rw-r--r-- 1 7652 Oct 27  2019 COPYING
-rw-r--r-- 1 4077 Jan 11  2020 README.md
drwxr-xr-x 2 4096 Dec 16 16:24 assets
drwxr-xr-x 5 4096 Dec 16 16:24 build
drwxr-xr-x 2 4096 Dec 16 16:24 cmake
drwxr-xr-x 2 4096 Dec 16 16:24 cutter-plugin
drwxr-xr-x 3 4096 Dec 16 16:24 ghidra
drwxr-xr-x 3 4096 Dec 16 16:24 scripts
drwxr-xr-x 2 4096 Dec 16 16:24 src
drwxr-xr-x 4 4096 Dec 16 16:24 test
drwxr-xr-x 3 4096 Dec 16 16:24 third-party
```

- If you have different path, edit the path for **R2PM_GIT** contains of the extraction of r2ghidra git local version directory, by the default I set it in:

  ~/.local/share/radare2/r2pm/db/r2ghidra

```
R2PM_BEGIN

# R2PM_GIT "https://github.com/radareorg/r2ghidra"
# rpm patch to install r2ghidra quick - has 1 to-edit & 1 omitted line
# @unixfreaxjp 20201215, tokyo, japan
# Change below R2PM_GIT into any local path w/older ghidra git data

R2PM_GIT ""/.local/share/radare2/r2pm/git/r2ghidra"

R2PM_DESC "Ghidra Disassembler, Analysis and Decompiler Plugins"

R2PM_DOC=""

R2PM_INSTALL() {
#       git submodule init && git submodule update || exit 1  # <== omit this line
        rm -rf build # clean build
        mkdir -p build && cd build || exit 1
        cmake -DRADARE2_INSTALL_PLUGDIR="${R2PM_PLUGDIR}"    || exit 1
```

4. 3. Installation for the patched r2ghidra

All you have to do now is just type below command:

```
~/{any path}/radare2-4.5.1/binr/r2pm/r2pm-pfg install r2ghidra
```

And it should be installed:

```
INFO    8 unnecessary extensions/truncations were converted to copies
Use -u switch to list each individually
INFO    4 operations wrote to temporaries that were not read
Use -t switch to list each individually
WARNING riscv.table.sinc:30: Unreferenced table 'rs1W'
WARNING riscv.table.sinc:37: Unreferenced table 'rdW'
WARNING riscv.table.sinc:160: Unreferenced table 'FRM'
WARNING riscv.table.sinc:176: Unreferenced table 'crs1'
WARNING riscv.table.sinc:230: Unreferenced table 'clqimm'
WARNING riscv.table.sinc:232: Unreferenced table 'cldspimm'
[100%] Built target sla
[  1%] Built target pugixml
[ 31%] Built target ghidra_decompiler_base
[ 39%] Built target ghidra_decompiler_sleigh
[ 40%] Built target ghidra_libdecomp
[ 45%] Built target core_ghidra
[ 48%] Built target sleighc
[100%] Built target sla
Install the project...
-- Install configuration: ""
-- Installing:        /.local/share/radare2/plugins/core_ghidra.so
-- Set runtime path of          /.local/share/radare2/plugins/core_ghidra.so" to ""
-- Installing:           .local/share/radare2/plugins/r2ghidra_sleigh/6502.sla
-- Installing:           .local/share/radare2/plugins/r2ghidra_sleigh/68020.sla
-- Installing:           .local/share/radare2/plugins/r2ghidra_sleigh/68030.sla
-- Installing:           .local/share/radare2/plugins/r2ghidra_sleigh/68040.sla
-- Installing:           .local/share/radare2/plugins/r2ghidra_sleigh/coldfire.sla
-- Installing:           .local/share/radare2/plugins/r2ghidra_sleigh/6805.sla
-- Installing:           .local/share/radare2/plugins/r2ghidra_sleigh/6809.sla
-- Installing:           .local/share/radare2/plugins/r2ghidra_sleigh/8048.sla
-- Installing:           .local/share/radare2/plugins/r2ghidra_sleigh/80251.sla
```