构建McSema

1. 搭建McSema的环境

https://github.com/lifting-bits/mcsema

https://cn-sec.com/archives/974652.html

McSema 是一个开源工具集，用于将 x86/x86-64 二进制代码转换为 LLVM IR（中间表示）。它由 Trail of Bits 公司开发，旨在支持二进制分析、漏洞利用和二进制重定向等领域的研究和开发。

为了不污染本机环境，搭建一个ubuntu的docker，在容器中按照官网中的**Native Build**步骤来做（**不按照官网的docker步骤**）

1. 构建docker环境：

```
docker pull ubuntu:20:04
docker run -it --privileged \
-v /work/stu/wtxiao/WorkSpace/mcsema/dockerimages:/work/stu/wtxiao/WorkSpace/mcsema/dockerimages \
--name x86_64-ubuntu_20.04 ubuntu:20.04 /bin/bash
#项目映射路径为/work/stu/wtxiao/WorkSpace/mcsema/dockerimages，你可以更改为你自己的
```

2. 进入docker后，首先安装相关依赖（大概1G左右）：

```
apt-get update
apt-get upgrade
apt-get install \
     git \
     curl \
     cmake \
     python3 python3-pip python3-virtualenv \
     wget \
     xz-utils pixz \
     clang \
     rpm \
     build-essential \
     gcc-multilib g++-multilib \
     libtinfo-dev \
     lsb-release \
     zip \
     zlib1g-dev \
     ccache
```

3. 直接进到映射目录：

```
cd /work/stu/wtxiao/WorkSpace/mcsema/dockerimages
```

4. 搭建他的虚拟环境（讲道理你前面下了依赖可以不用他的虚拟环境，但是这里我还是这么做了）：

```
mkdir mcsema-ve
virtualenv mcsema-ve
cd mcsema-ve
source bin/activate
```

5. 下载并构建：

```
git clone https://github.com/lifting-bits/remill.git
pushd .
cd remill

# For LLVM versions (<=11)(这里我构建11的版本，12以上版本虽然应该也可以，
# 但是官网说支持的版本只有9-11)
git checkout -b all_llvm 9006baf7db
```

```
popd
```

6. 接着跑：

```
git clone --depth 1 --single-branch --branch master https://github.com/lifting-bits/mcsema.git

# Get a compatible anvill version
git clone --branch master https://github.com/lifting-bits/anvill.git
( cd anvill && git checkout -b release_bc3183b bc3183b )

export CC="$(which clang)"
export CXX="$(which clang++)"
#这里不知道为什么我不管是在虚拟环境中加变量还是在docker中加入变量，最后build时cmake指定
的编译器还是gcc一类，接下来需要修改些东西
```

7. 这一步注意看注释

```
# Download cxx-common, build Remill. 首先是下载这个remill，有个
#vcpkg_ubuntu-20.04_llvm-11_amd64.tar.xz 的包在服务器上下的非常慢，你可以采用两种
#方案来解决，
#方案一:第一种修改your/path/to/mcsema-ve/remill/scripts/build.sh
#找到if ! curl -LO "${URL}"; then 这一行
#修改为if ! curl -LO -C - "${URL}"; then，之后只要它curl超时，你再重新跑下面
#这句话，它就会从下载中断处接着下载，而不是重新下载。
#方案而:直接在你的电脑上下载它，利用xftp等工具传到
#your/path/to/mcsema-ve 下面即可
./remill/scripts/build.sh --llvm-version 11 --download-dir ./
```

8. 这一步同样注意看注释

```
pushd remill-build
#这一步可能会报某些函数未定义的错误，原因是cmake用了默认的gcc编译器而非clang
#作者写了些只有clang支持的函数或者类型出错，故此时直接修改
#your/path/to/mcsema-ve/remill/CMakeLists.txt ,
#并在其中加入两句话，如果clang没有还得装一下
#set(CMAKE_CXX_COMPILER "clang++")
#set(CMAKE_C_COMPILER "clang")
#这一步操作对于后面构建avill和mcsema也是必要的，记得做
sudo cmake --build . --target install
popd
```

9. 接着按官网操作，最后输入mcsema-disass --version如果有输出代表构建成功。

```
# Build and install Anvill
mkdir anvill-build
pushd anvill-build
# Set VCPKG_ROOT to whatever directory the remill script downloaded
cmake -DVCPKG_ROOT=$(pwd)/../vcpkg_ubuntu-20.04_llvm-11_amd64 ../anvill
sudo cmake --build . --target install
popd

# Build and install McSema
mkdir mcsema-build
pushd mcsema-build
# Set VCPKG_ROOT to whatever directory the remill script downloaded
cmake -DVCPKG_ROOT=$(pwd)/../vcpkg_ubuntu-20.04_llvm-11_amd64 ../mcsema
sudo cmake --build . --target install
```

10. 接下来需要安装IDA Pro，首先需要安装一些依赖项

```
apt install libxcb-icccm4 libxcb-image0 libxcb-keysyms1 libxcb-randr0 libxcb-render-util0 libxcb-xkb1 libxcb-shape0 libxkbcommon-x11-0
apt install libxcb-xinerama0 libxcb-cursor0

cat <<EOF | sudo tee /etc/apt/sources.list
deb http://archive.ubuntu.com/ubuntu/ focal main universe multiverse restricted
deb http://security.ubuntu.com/ubuntu/ focal-security main universe multiverse restricted
```

```
deb http://archive.ubuntu.com/ubuntu/ focal-updates main universe multiverse restricted
deb http://archive.ubuntu.com/ubuntu/ focal-backports main universe multiverse restricted
deb-src http://archive.ubuntu.com/ubuntu/ focal main universe multiverse restricted
deb-src http://security.ubuntu.com/ubuntu/ focal-security main universe multiverse restricted
deb-src http://archive.ubuntu.com/ubuntu/ focal-updates main universe multiverse restricted
deb-src http://archive.ubuntu.com/ubuntu/ focal-backports main universe multiverse restricted
EOF

dpkg --add-architecture i386
apt-get update
apt-get install libncurses5:i386 zlib1g:i386
ln -s /lib/i386-linux-gnu/libncurses.so.5 /lib/i386-linux-gnu/libcurses.so
apt-get install python-protobuf
apt-get install mlocate
updatedb
pip install opencv-python
apt update && apt install -y libsm6 libxext6
apt-get install -y libxrender-dev
```

11. 其次安装IDA PRO，直接运行安装包就可以了，一路yes，最后只要不报错就行。

2. 使用McSema的困境

由于IDA PRO 7.0以上需要license，一直没有取得，故搁置。