下载编译Chromium源码

Author：wnagzihxa1n
Mail：wnagzihxa1n@163.com

编译Chromium的源码绝对是个看人品的活，测试了很多方法，编译了很久，各种报错

接下来我介绍我发现的一种下载编译Chromium的骚姿势

0x00 准备材料

- Ubuntu 14.04 x64
- 8G内存
- 一个好梯子，我使用SSR
- 比较充足的时间

0x01 配置梯子环境

老祖宗说：“工欲善其事，必先利其器。”

鉴于某些我们都知道的原因，直接按照谷歌官方的描述是下载不了源码的

我这里使用SSR来配置梯子，梯子代理到了本地的1080端口，这个过程自己配置，我不过多叙述

梯子配置完后，我们需要给git也设置代理

```
git config --global http.proxy 'socks5://127.0.0.1:1080'
git config --global https.proxy 'socks5://127.0.0.1:1080'
```

如果不想用了，关闭git代理

```
git config --global --unset http.proxy
git config --global --unset https.proxy
```

有了git代理是不够的，还需要给终端设置代理

```
sudo apt-get install polipo
```

打开终端配置，位置在`/etc/polipo/config`

```
logSyslog = true:
logFile = "/var/log/polipo/polipo.log"

socksParentProxy = "127.0.0.1:1080"  #这是socks代理的地址和端口
socksProxyType = socks5

chunkHighMark = 50331648
objectHighMark = 16384

serverMaxSlots = 64
serverSlots = 16
serverSlots1 = 32

# 我们最后要使用这个地址作为代理，它会去走SSR的代理
proxyAddress = "127.0.0.1" #这是本代理的地址端口
proxyPort = 8123
```

重启polipo

```
sudo service polipo restart
```

最后设置环境变量

```
export http_proxy="http://127.0.0.1:8123"
export https_proxy="https://127.0.0.1:8123"
```

此时所有环境变量都配置完成

0x02 下载Chromium源码

在Ubuntu下编译的教程在此，然而即使是开了代理也会有很多奇奇怪怪的错误

- https://chromium.googlesource.com/chromium/src/+/master/docs/linux_build_instructions.md

创建一个工程文件夹

```
mkdir ChromePwn
cd ChromePwn
```

下载`depot_tools`

```
git clone https://chromium.googlesource.com/chromium/tools/depot_tools.git
```

设置环境变量，我这里在`.bashrc`中加入

```
export PATH="$PATH:/path/to/depot_tools"
```

修改完毕，使其生效

```
source ~/.bashrc
```

创建Chromium源码文件夹

```
mkdir Chromium
cd Chromium
```

执行下载

```
fetch --nohooks chromium
```

如果中途断开，继续下载即可

```
gclient sync
```

看起来是很完美的，然而我下载了很久，每次都是莫名其妙断开，于是继续重新开始下载，这么大一个工程竟然不支持断点续传

下载步骤从这里真正开始，上面都是瞎扯的

好在我找到了一个Github项目，上面存放了Chromium众多版本源码，顺手就fork了一份，我准备把40以后的源码都下载一份备用

- https://github.com/wnagzihxa1n/chromium-source-tarball

这里因为要复现一个漏洞，所以我选择了`59.0.3071.104`

下载回来，解压缩，目前项目情况是

```
Chromium/chromium-59.0.3071.104
```

这个目录下面就是全部的源码，没有`src`目录，进入这个目录，我们在这个目录下创建两个文件

```
.gclient
.gclient_entries
```

第一个文件`.gclient`

```
solutions = [
  { "name"        : "src",
    "url"         : "https://chromium.googlesource.com/chromium/src.git",
    "deps_file"   : "DEPS",
    "managed"     : True,
    "custom_deps" : {
    },
    "safesync_url": "",
  },
]
cache_dir = "/chromium/cache"
```

第二个文件`.gclient_entries`

```
entries = {
  'src': 'https://chromium.googlesource.com/chromium/src.git',
  'src/breakpad/src': 'https://chromium.googlesource.com/breakpad/breakpad/src.git@2dadd64db9965d8a621d52712abe95f96c4a1e0a',
  'src/buildtools': 'https://chromium.googlesource.com/chromium/buildtools.git@991f459071f96102b7bcb5fb5db6757b52d4238f',
  'src/chrome/test/data/perf/canvas_bench': 'https://chromium.googlesource.com/chromium/canvas_bench.git@a7b40ea5ae0239517d78845a5
  'src/chrome/test/data/perf/frame_rate/content': 'https://chromium.googlesource.com/chromium/frame_rate/content.git@c10272c88463e
  'src/media/cdm/api': 'https://chromium.googlesource.com/chromium/cdm.git@6a62dcef02523e2d5be4defb68a7d9363c7389d2',
  'src/native_client': 'https://chromium.googlesource.com/native_client/src/native_client.git@163dfeb43e76995b4265ecd4e78670f7dd43
  'src/sdch/open-vcdiff': 'https://chromium.googlesource.com/external/github.com/google/open-vcdiff.git@2b9bd1fe548520e9355e457a13
  'src/testing/gmock': 'https://chromium.googlesource.com/external/googlemock.git@0421b6f358139f02e102c9c332ce19a33faf75be',
  'src/testing/gtest': 'https://chromium.googlesource.com/external/github.com/google/googletest.git@6f8a66431cb592dad629028a50b3dd
  'src/third_party/SPIRV-Tools/src': 'https://chromium.googlesource.com/external/github.com/KhronosGroup/SPIRV-Tools.git@9166854ac
  'src/third_party/angle': 'https://chromium.googlesource.com/angle/angle.git@a4aaa2de57dc51243da35ea147d289a21a9f0c49',
  'src/third_party/bidichecker': 'https://chromium.googlesource.com/external/bidichecker/lib.git@97f2aa645b74c28c57eca56992235c798
  'src/third_party/bison': 'https://chromium.googlesource.com/chromium/deps/bison.git@083c9a45e4affdd5464ee2b224c2df649c6e26c3',
  'src/third_party/boringssl/src': 'https://boringssl.googlesource.com/boringssl.git@e1cc35e581a6d42f618d8c783f36faebc6023bb7',
  'src/third_party/catapult': 'https://chromium.googlesource.com/external/github.com/catapult-project/catapult.git@81f71e551ef2375
  'src/third_party/ced/src': 'https://chromium.googlesource.com/external/github.com/google/compact_enc_det.git@9012c0ab648025dd0f8
  'src/third_party/cld_2/src': 'https://chromium.googlesource.com/external/github.com/CLD2Owners/cld2.git@84b58a5d7690ebf05a91406f
  'src/third_party/cld_3/src': 'https://chromium.googlesource.com/external/github.com/google/cld_3.git@ae02d6b8a2af41e87c956c7c7d3
  'src/third_party/colorama/src': 'https://chromium.googlesource.com/external/colorama.git@799604a1041e9b3bc5d2789ecbd7e8db2e18e6b
  'src/third_party/cygwin': 'https://chromium.googlesource.com/chromium/deps/cygwin.git@c89e446b273697fadf3a10ff1007a97c0b7de6df',
  'src/third_party/dom_distiller_js/dist': 'https://chromium.googlesource.com/external/github.com/chromium/dom-distiller-dist.git@
  'src/third_party/ffmpeg': 'https://chromium.googlesource.com/chromium/third_party/ffmpeg.git@4c35fe00477f20343294cc5827cc5abab6c
  'src/third_party/flac': 'https://chromium.googlesource.com/chromium/deps/flac.git@d0c35f878ec26f969c1631350b1d36fbd88ad8bb',
  'src/third_party/flatbuffers/src': 'https://chromium.googlesource.com/external/github.com/google/flatbuffers.git@e92ae5199d52fd5
  'src/third_party/glslang/src': 'https://chromium.googlesource.com/external/github.com/google/glslang.git@210c6bf4d8119dc5f8ac21d
  'src/third_party/gnu_binutils': 'https://chromium.googlesource.com/native_client/deps/third_party/gnu_binutils.git@f4003433b61b2
  'src/third_party/gperf': 'https://chromium.googlesource.com/chromium/deps/gperf.git@d892d79f64f9449770443fb06da49b5a1e5d33c1',
  'src/third_party/hunspell_dictionaries': 'https://chromium.googlesource.com/chromium/deps/hunspell_dictionaries.git@dc6e7c25bf47
  'src/third_party/icu': 'https://chromium.googlesource.com/chromium/deps/icu.git@85817893162f4fdcc30ccdd288d43540d4a2b358',
  'src/third_party/jsoncpp/source': 'https://chromium.googlesource.com/external/github.com/open-source-parsers/jsoncpp.git@f572e8e
  'src/third_party/leveldatabase/src': 'https://chromium.googlesource.com/external/leveldb.git@a7bff697baa062c8f6b8fb760eacf658712
  'src/third_party/libFuzzer/src': 'https://chromium.googlesource.com/chromium/llvm-project/llvm/lib/Fuzzer.git@2ed967ccadb496a1e9
  'src/third_party/libaddressinput/src': 'https://chromium.googlesource.com/external/libaddressinput.git@4d18a0d4be9add0dc479e7b93
  'src/third_party/libjpeg_turbo': 'https://chromium.googlesource.com/chromium/deps/libjpeg_turbo.git@7260e4d8b8e1e40b17f03fafdf1c
  'src/third_party/libphonenumber/dist': 'https://chromium.googlesource.com/external/libphonenumber.git@a4da30df63a097d67e3c429ead
  'src/third_party/libsrtp': 'https://chromium.googlesource.com/chromium/deps/libsrtp.git@0e0936f3013fe5884eac82f95e370c8d460a179f
  'src/third_party/libvpx/source/libvpx': 'https://chromium.googlesource.com/webm/libvpx.git@3219aac9dfb0a087c9e79c02ebe4704b97769
  'src/third_party/libwebm/source': 'https://chromium.googlesource.com/webm/libwebm.git@9a235e0bc94319c5f7184bd69cbe5468a74a025c',
  'src/third_party/libyuv': 'https://chromium.googlesource.com/libyuv/libyuv.git@97fb18b846c52ef3596763184cf1f2686eed5f3c',
  'src/third_party/lighttpd': 'https://chromium.googlesource.com/chromium/deps/lighttpd.git@9dfa55d15937a688a92cbf2b7a8621b0927d06
  'src/third_party/mesa/src': 'https://chromium.googlesource.com/chromium/deps/mesa.git@ef811c6bd4de74e13e7035ca882cc77f85793fef',
  'src/third_party/mingw-w64/mingw/bin': 'https://chromium.googlesource.com/native_client/deps/third_party/mingw-w64/mingw/bin.git
  'src/third_party/nacl_sdk_binaries': 'https://chromium.googlesource.com/chromium/deps/nacl_sdk_binaries.git@759dfca03bdc774da7ec
  'src/third_party/openh264/src': 'https://chromium.googlesource.com/external/github.com/cisco/openh264@0fd88df93c5dcaf858c57eb789
  'src/third_party/openmax_dl': 'https://chromium.googlesource.com/external/webrtc/deps/third_party/openmax.git@57d33bee7823e76393
  'src/third_party/pdfium': 'https://pdfium.googlesource.com/pdfium.git@75c2af49705f99267ef74e742d536c7327aeb452',
  'src/third_party/pefile': 'https://chromium.googlesource.com/external/pefile.git@72c6ae42396cb913bcab63c15585dc3b5c3f92f1',
  'src/third_party/perl': 'https://chromium.googlesource.com/chromium/deps/perl.git@ac0d98b5cee6c024b0cffeb4f8f45b6fc5ccdb78',
```

```
  'src/third_party/psyco_win32': 'https://chromium.googlesource.com/chromium/deps/psyco_win32.git@f5af9f6910ee5a8075bbaeed0591469f
  'src/third_party/py_trace_event/src': 'https://chromium.googlesource.com/external/py_trace_event.git@dd463ea9e2c430de2b9e53dea57
  'src/third_party/pyftpdlib/src': 'https://chromium.googlesource.com/external/pyftpdlib.git@2be6d65e31c7ee6320d059f581f05ae8d89d7
  'src/third_party/pywebsocket/src': 'https://chromium.googlesource.com/external/github.com/google/pywebsocket.git@2d7b73c3acbd0f4
  'src/third_party/re2/src': 'https://chromium.googlesource.com/external/github.com/google/re2.git@dba3349aba83b5588e85e5ecf2b56c9
  'src/third_party/scons-2.0.1': 'https://chromium.googlesource.com/native_client/src/third_party/scons-2.0.1.git@1c1550e17fc26355
  'src/third_party/sfntly/src': 'https://chromium.googlesource.com/external/github.com/googlei18n/sfntly.git@64f78562d2003eb7cacaa
  'src/third_party/shaderc/src': 'https://chromium.googlesource.com/external/github.com/google/shaderc.git@cd8793c34907073025af262
  'src/third_party/skia': 'https://skia.googlesource.com/skia.git@dd45f8195783efc7b8044b006eae5ea5ac127cc2',
  'src/third_party/smhasher/src': 'https://chromium.googlesource.com/external/smhasher.git@e87738e57558e0ec472b2fc3a643b838e5b6e88
  'src/third_party/snappy/src': 'https://chromium.googlesource.com/external/snappy.git@762bb32f0c9d2f31ba4958c7c0933d22e80c20bf',
  'src/third_party/swiftshader': 'https://swiftshader.googlesource.com/SwiftShader.git@a6e99c02de6162a6a55f5de3d42c2e8c190cf3f2',
  'src/third_party/usrsctp/usrsctplib': 'https://chromium.googlesource.com/external/github.com/sctplab/usrsctp@7f9228152ab3d70e684
  'src/third_party/visualmetrics/src': 'https://chromium.googlesource.com/external/github.com/WPO-Foundation/visualmetrics.git@1ed
  'src/third_party/webdriver/pylib': 'https://chromium.googlesource.com/external/selenium/py.git@5fd78261a75fe08d27ca4835fb6c5ce4b
  'src/third_party/webgl/src': 'https://chromium.googlesource.com/external/khronosgroup/webgl.git@d12037a99155a7d884845759d0f7461c
  'src/third_party/webpagereplay': 'https://chromium.googlesource.com/external/github.com/chromium/web-page-replay.git@3cd3a3f6f06
  'src/third_party/webrtc': 'https://chromium.googlesource.com/external/webrtc/trunk/webrtc.git@f141d331e4a42bfd7755cf8011b9c22207
  'src/third_party/yasm/binaries': 'https://chromium.googlesource.com/chromium/deps/yasm/binaries.git@52f9b3f4b0aa06da24ef8b123058
  'src/third_party/yasm/source/patched-yasm': 'https://chromium.googlesource.com/chromium/deps/yasm/patched-yasm.git@7da28c6c7c6a1
  'src/tools/gyp': 'https://chromium.googlesource.com/external/gyp.git@e7079f0e0e14108ab0dba58728ff219637458563',
  'src/tools/page_cycler/acid3': 'https://chromium.googlesource.com/chromium/deps/acid3.git@6be0a66a1ebd7ebc5abc1b2f405a945f6d8715
  'src/tools/swarming_client': 'https://chromium.googlesource.com/external/swarming.client.git@ebc8dab6f8b8d79ec221c94de39a921145a
  'src/v8': 'https://chromium.googlesource.com/v8/v8.git@93947afa548945132d5069544f881257d36df5f8',
  'src\\buildtools\\clang_format\\script': 'https://chromium.googlesource.com/chromium/llvm-project/cfe/tools/clang-format.git@6a4
  'src\\buildtools\\third_party\\libc++\\trunk': 'https://chromium.googlesource.com/chromium/llvm-project/libcxx.git@b1ece9c037d87
  'src\\buildtools\\third_party\\libc++abi\\trunk': 'https://chromium.googlesource.com/chromium/llvm-project/libcxxabi.git@0edb61e
}
```

执行下面的命令，我这个姿势，就这里需要用到梯子

```
gclient runhooks
```

中间会遇到很多问题，自己慢慢解决就好，虽然很多问题都是搜不到的，相信我，搜不到

这一步其实挺折腾的，我建议在`depot_tools/update_depot_tools.bat`中添加一句，去掉自动更新

```
set DEPOT_TOOLS_UPDATE=0 我们加的一句

:: Shall skip automatic update?
IF "%DEPOT_TOOLS_UPDATE%" == "0" GOTO :EOF
```

如果开始提示缺少`wasm`什么的文件，这个时候就需要骚姿势上场了

我们先查看一下我们的Chromium版本对应的V8b版本

- https://omahaproxy.appspot.com/

查询结果

```
Commit: 98a3a7375652f76d056123496d91a1acc9dc819e
Branch Base Commit: a106f0abbf69dad349d4aaf4bcc4f5d376dd2377
Branch Base Position: 464641
V8 Commit: c7fae8b9e56616d71d4f6d5c6160a75c52900ffa
V8 Version: 5.9.211.35
V8 Position: 74
Skia Commit: ef6f9c65527412ec4057ea0551f2e051beb94d32
```

我们在下面这个地址下载对应的谷歌Chromium源码和V8源码

- https://chromium.googlesource.com/chromium/src/+/59.0.3071.104
- https://chromium.googlesource.com/v8/v8/+/c7fae8b9e56616d71d4f6d5c6160a75c52900ffa

点击下面的`[tgz]`就可以下载整个压缩包

```
commit    98a3a7375652f76d056123496d91a1acc9dc819e    [log] [tgz]
```

然后就可以缺什么就补充什么了

最后就可以完成啦

再下载一些文件

```
./build/install-build-deps.sh –no-chromeos-fonts
```

开始执行编译，先生成编译文件

```
gn gen out/Default
```

执行编译，这一步也有可能缺少文件，按照上面的方法，缺什么，就补什么，需要说明的一点是，V8可以整个直接覆盖过去

```
ninja -C out/Default
```

会很慢，特别是后面链接过程，机子都卡的不能动

好在最后还是编译完了，设置一下沙箱，因为我们没有沙箱

```
export CHROME_DEVEL_SANDBOX=/usr/local/sbin/chrome-devel-sandbox
```

跑起来，在`out/Default`目录下

```
./chrome
```

大功告成