目录

环境

```
ubuntu@ubuntu-VirtualBox:~$ uname -a
Linux ubuntu-VirtualBox 6.8.0-45-generic #45-Ubuntu SMP PREEMPT_DYNAMIC Fri Aug
30 12:02:04 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
ubuntu@ubuntu-VirtualBox:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.1 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.1 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-poli
cy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
```

LLVM 编译 linux-5.4 内核并获取 CFG

 # 安装 llvm clang graphviz(编译过程中会遇到缺其他工具，按照提示进行安装即可)
apt install llvm clang graphviz build-essential

 # 下载 Linux-5.4 tarball
wget https://cdn.kernel.org/pub/linux/kernel/v5.x/linux-5.4.284.tar.xz
tar -xvf linux-5.4.284.tar.xz

 # 安装 wllvm
python -m venv ~/venv00
source ~/venv00/bin/bash
pip install wllvm

```
(venv00) ubuntu@ubuntu-VirtualBox:~$ pip show wllvm
Name: wllvm
Version: 1.3.1
Summary: Whole Program LLVM
Home-page: https://github.com/SRI-CSL/whole-program-llvm
Author: Ian A. Mason, Tristan Ravitch, Dan Liew, Bruno Dutertre, Benjamin Schube
rt, Berkeley Churchill, Marko Dimjasevic, Will Dietz, Fabian Mager, Ben Liblit,
Andrew Santosa, Tomas Kalibera, Loic  Gelle, Joshua Cranmer, Alexander Bakst, Mi
guel Arroyo.
Author-email: iam@csl.sri.com
License: MIT
Location: /home/ubuntu/venv00/lib/python3.12/site-packages
Requires:
Required-by:
(venv00) ubuntu@ubuntu-VirtualBox:~$ python --version
Python 3.12.3
```

 # 编译 linux-5.4

cd linux-5.4.284

export LLVM_COMPILER=clang

make CC=clang defconfig

make CC=wllvm LLVM=1

```
(venv00) ubuntu@ubuntu-VirtualBox:~/code/linux-5.4.284$ ls
arch            fs       LICENSES                net          usr
block           include  MAINTAINERS             README       virt
certs           init     Makefile                samples      vmlinux
COPYING         ipc      mm                      scripts      vmlinux.bc
CREDITS         Kbuild   modules.builtin         security     vmlinux.o
crypto          Kconfig  modules.builtin.modinfo sound
Documentation   kernel   modules.order           System.map
drivers         lib      Module.symvers          tools
```

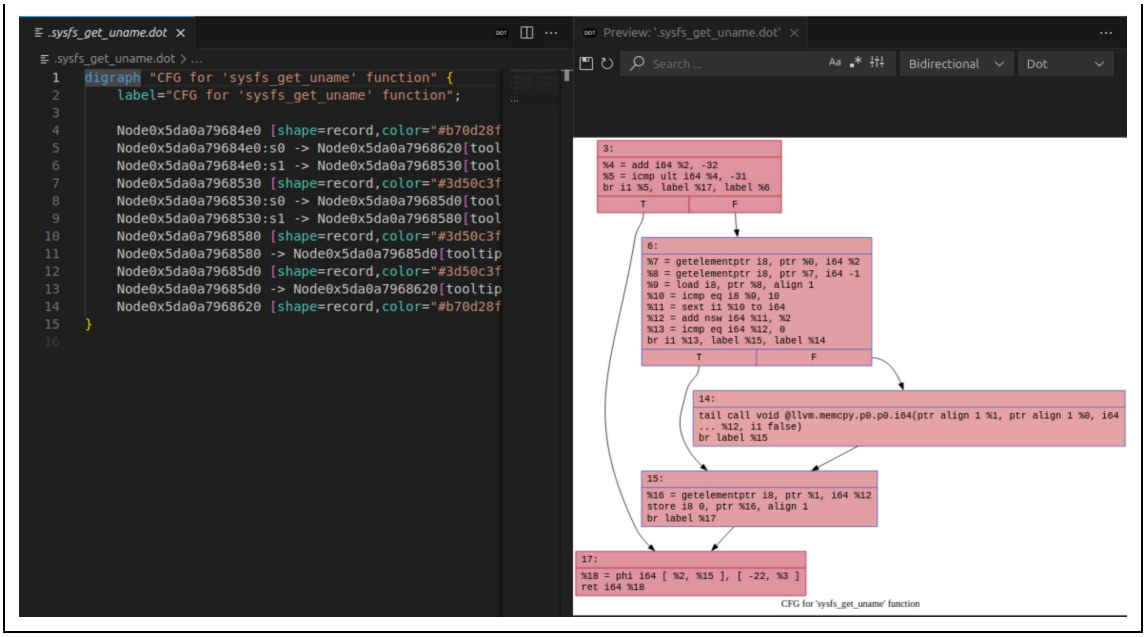
 # 从 bitcode 提取 dot(dot 文件很多)

extract-bc vmlinux.bc

```
.sysfs_format_mac.dot
.sysfs_fs_context_free.dot
.sysfs_get_tree.dot
.sysfs_get_uname.dot
.sysfs_init_fs_context.dot
.sysfs_init.dot
.sysfs_kf_bin_mmap.dot
```

 # dot 文件转换为 CFG 图

借助 vscode 中的 Graphviz Interactive Preview 插件



以 sysfs_get_uname 函数为例

- sysfs_get_uname 函数位于 kernel/time/clocksource.c 文件中

```
ssize_t sysfs_get_uname(const char *buf, char *dst, size_t cnt)
{
    size_t ret = cnt;

    /* strings from sysfs write are not 0 terminated! */
    if (!cnt || cnt >= CS_NAME_LEN)
        return -EINVAL;

    /* strip of \n: */
    if (buf[cnt-1] == '\n')
        cnt--;
    if (cnt > 0)
        memcpy(dst, buf, cnt);
    dst[cnt] = 0;
    return ret;
}
```

- 将 vmlinux.bc 转换为可阅读的 vmlinux.ll，全局搜索 sysfs_get_uname 找到对应的代码

llvm-dis vmlinux.bc

```
; Function Attrs: mustprogress nofree norecurse noredzone nosync nounwind null_pointer_is_valid sspstrong willreturn memory(argmem: readwrite)
define dso_local noundef i64 @sysfs_get_uname(ptr nocapture noundef readonly %0, ptr nocapture noundef writeonly %1, i64 noundef %2) local_unnamed_addr #37 {
  %4 = add i64 %2, -32
  %5 = icmp ult i64 %4, -31
  br i1 %5, label %17, label %6

6:                                                ; preds = %3
  %7 = getelementptr i8, ptr %0, i64 %2
  %8 = getelementptr i8, ptr %7, i64 -1
  %9 = load i8, ptr %8, align 1
  %10 = icmp eq i8 %9, 10
  %11 = sext i1 %10 to i64
  %12 = add nsw i64 %11, %2
  %13 = icmp eq i64 %12, 0
  br i1 %13, label %15, label %14

14:                                               ; preds = %6
  tail call void @llvm.memcpy.p0.p0.i64(ptr align 1 %1, ptr align 1 %0, i64 %12, i1 false)
  br label %15

15:                                               ; preds = %14, %6
  %16 = getelementptr i8, ptr %1, i64 %12
  store i8 0, ptr %16, align 1
  br label %17

17:                                               ; preds = %3, %15
  %18 = phi i64 [ %2, %15 ], [ -22, %3 ]
  ret i64 %18
}
```

- 通过 dot 命令获取 CFG 的 png 图片

dot -Tpng -o sysfs_get_uname.png .sysfs_get_uname.dot

```
(venv00) ubuntu@ubuntu-VirtualBox:~/code/linux-5.4.284$ dot -Tpng -o sysfs_get_uname.png .sysfs_get_uname.dot
(venv00) ubuntu@ubuntu-VirtualBox:~/code/linux-5.4.284$ ls
arch            init          modules.builtin          sysfs_get_uname.png
block           ipc           modules.builtin.modinfo  System.map
certs           Kbuild        modules.order            tools
COPYING         Kconfig       Module.symvers           usr
CREDITS         kernel        net                      virt
crypto          lib           README                   vmlinux
Documentation   LICENSES      samples                  vmlinux.bc
drivers         MAINTAINERS   scripts                  vmlinux.ll
fs              Makefile      security                 vmlinux.o
```

- 查看 CFG 图片