SWRhapsody

Install syzkaller

于10月 26, 2018由**SWRhapsody**发布

Introduction

Some notes about how to install syzkaller.

Code

Follow the instruction of official document [1] .

During building GCC you may encounter an error

```
./md-unwind-support.h: In function 'x86_64_fallback_frame_state':
./md-unwind-support.h:65:47: error: dereferencing pointer to incomplete type 'struct ucontext'
       sc = (struct sigcontext *) (void *) &uc_->uc_mcontext;
                                           ^~
```

this link [2] can solve this error.

After you using the second reference, this error may raise

```
/gcc/libsanitizer/sanitizer_common/sanitizer_stoptheworld_linux_libcdep.cc: In function ‘int __
/gcc/libsanitizer/sanitizer_common/sanitizer_stoptheworld_linux_libcdep.cc:276:22: error: aggre
   struct sigaltstack handler_stack;
```

And this [3] shall fix it.

During the installation of perf, the program will complain some libraries are missing, use

```
sudo chroot stretch /bin/bash -c "apt-get update; apt-get install -y ${missing_library}"
```

to install missing libraries.

Reference

[1] https://github.com/google/syzkaller/blob/master/docs/linux/setup_ubuntu-host_qemu-vm_x86-64-

SWRhapsody

[3] https://github.com/google/sanitizers/issues/822

分类: EXERCISE

0 条评论

发表评论

名称 *

电子邮件 *

网站

在想些什么?

发表评论

近期评论

文章归档

2018年2月

2018年1月

分类目录

Article Collection

Cheat Sheet

cryptography

Exercise

Exploit

HackTheBox

Penetration Test

Uncategorized

相关文章

EXERCISE

CodeQL部分源码简读

Introduction CodeQL 也用了不少时间了，从最初的不会 阅读更多…

CodeQL 部分使用记录

前言 CodeQL 是一个代码分析引擎，主要原理是通过对代码进行构建并 阅读更多…

EXERCISE

Java 反编译工具

在复现 CVE-2019-15012 遇到了一个非常坑的地方，使用 J 阅读更多…