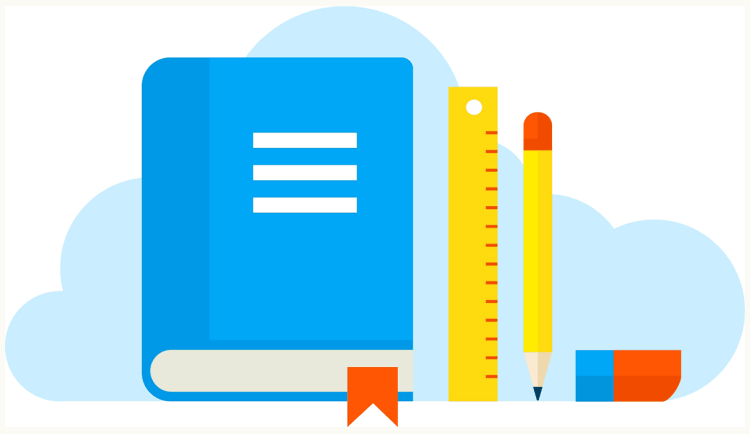

Syzkaller Notes

Date: 06/04/2023

---

https://www.youtube.com/results?search_query=coverage-guided+USB+fuzzing+with+syzkaller	Syzkaller all

Below list of issues I found with SyzKaller -

1] Issue - Failed to ssh into qemu

Why - Didn't created ssh key

Fix

- generate an SSH key pair, using ssh-keygen command

2] Issue - Failed to compile syzkaller

After firing make command, it used to exit in a minute.

Fix - Was using some older laptop/machine, switch to latest hardware.

3] Issue - Missing reproducer

BUG: unable to handle kernel NULL pointer dereference in __io_remove_buffers

e.g. https://syzkaller.appspot.com/bug?extid=70de24bf68bee5f644e3

Some of issues that syzkaller generated dont have reproducer

If we try to fix such issues, syzkaller failed to verify.

---

https://www.kernel.org/doc/Documentation/admin-guide/bug-hunting.rst

---

Learn to use syzkaller

Learn to use syzkaller

Using syzkaller, part 1: Fuzzing the Linux kernel

https://www.collabora.com/news-and-blog/blog/2020/03/26/syzkaller-fuzzing-the-kernel/

Using syzkaller, part 2: Detecting programming bugs in the Linux kernel

https://www.collabora.com/news-and-blog/blog/2020/04/17/using-syzkaller-to-detect-programming-bugs-in-linux/

Using syzkaller, part 3: Fuzzing your changes

https://www.collabora.com/news-and-blog/blog/2020/05/12/using-syzkaller-fuzzing-your-changes/

Using syzkaller, part 4: Driver fuzzing

https://www.collabora.com/news-and-blog/blog/2020/06/26/using-syzkaller-part-4-driver-fuzzing/

Date: 06/04/2023

Tools and Techniques to Debug an Embedded Linux System

Tools and Techniques to Debug an Embedded Linux System - watch this mentoring webinar to learn about tools and techniques to debug. This will be help you as you get started with debugging problems during this program and beyond. Write a summary of what you learned and upload. Send email to mentors to indicate you completed the task.

https://www.youtube.com/watch?v=Paf-1I7ZUTo

Date: 06/04/2023

Getting started with Linux Kernel Debugging

Getting started with Linux Kernel Debugging

Sharing resources to get you started with understanding Linux kernel crashes: These give you a primer on what each word in the panic means and how to interpret them. This self study and write summary of what you learned from these resources.

- https://sanjeev1sharma.wordpress.com/tag/debug-kernel-panics/
- https://www.opensourceforu.com/2011/01/understanding-a-kernel-oops/

Date: 06/04/2023

Dynamic Program Analysis for Fun and Profit

Dynamic Program Analysis for Fun and Profit

Dynamic Program Analysis for Fun and Profit Watch this mentoring webinar to learn about Dynamic analysis and how it is employed in the Linux kernel. Please write summary of what you learned and upload. Send email to Shuah Khan <skhan@linuxfoundation.org>

https://events.linuxfoundation.org/mentorship-session-dynamic-program-analysis/

Date: 06/04/2023

Getting started with Linux Kernel Debugging

Getting started with Linux Kernel Debugging

Sharing resources to get you started with understanding Linux kernel crashes: These give you a primer on what each word in the panic means and how to interpret them. This self study and write summary of what you learned from these resources.

- https://sanjeev1sharma.wordpress.com/tag/debug-kernel-panics/
- https://www.opensourceforu.com/2011/01/understanding-a-kernel-oops/

Date: 06/04/2023

Fuzzing Linux Kernel

Fuzzing Linux Kernel

Fuzzing Linux Kernel Watch this mentoring webinar to learn about fuzz testing and how it is used to find bugs in the Linux kernel using syzbot and other fuzzing tools. Please write summary of what you learned and upload. Send email to Shuah Khan <skhan@linuxfoundation.org>

- https://events.linuxfoundation.org/mentorship-session-fuzzing-linux-kernel/

Date: 06/04/2023

http://185.161.209.143/ - Linux Kernel patch ideas, collected by Coccinelle

Date: 06/04/2023