xairy / linux-kernel-exploitation

A bunch of links related to Linux kernel exploitation

linux-kernel linux kernel-exploitation exploit privilege-escalation security

28 commits 1 branch 0 releases 5 contributors

Branch: master New pull request Find file Clone or download

xairy Update README.md Latest commit 4f95fc0 on May 4

README.md Update README.md a month ago

README.md

Linux Kernel Exploitation

Some exploitation methods and techniques are outdated and don't work anymore on newer kernels.

Pull requests are welcome.

Books

2012: "A Guide to Kernel Exploitation: Attacking the Core" by Enrico Perla and Massimiliano Oldani

Exploitation techniques

2018: "Linux-Kernel-Exploit Stack Smashing" [article]

2018, HitB: "Mirror Mirror: Rooting Android 8 with a Kernel Space Mirroring Attack" by Wang Yong [slides]

2018, BlackHat: "KSMA: Breaking Android kernel isolation and Rooting with ARM MMU features" by Wang Yong [slides]

2018, OffensiveCon: "Concolic Testing for Kernel Fuzzing and Vulnerability Discovery" by Vitaly Nikolenko [video]

2018: "Still Hammerable and Exploitable: on the Effectiveness of Software-only Physical Kernel Isolation" [paper]

2017: "KERNELFAULT: Pwning Linux using Hardware Fault Injection" by Niek Timmers and Cristofaro Mune [video]

2017: "Escalating Privileges in Linux using Fault Injection" by Niek Timmers and Cristofaro Mune [slides]

2017: "Escalating Privileges in Linux using Fault Injection" by Niek Timmers and Cristofaro Mune [whitepaper]

2017: "Kernel Driver mmap Handler Exploitation" by Mateusz Fruba [whitepaper]

2017: "Linux kernel addr_limit bug / exploitation" by Vitaly Nikolenko [video]

2017: "The Stack Clash" by Qualys Research Team [article]

2017: "New Reliable Android Kernel Root Exploitation Techniques" [slides]

2017: "Unleashing Use-Before-Initialization Vulnerabilities in the Linux Kernel Using Targeted Stack Spraying" [whitepaper]

2017: "Breaking KASLR with perf" by Lizzie Dixon [article]

2016: "Getting Physical Extreme abuse of Intel based Paging Systems" by Nicolas Economou and Enrique Nissim [slides]

2016: "Linux Kernel ROP - Ropping your way to # (Part 1)" by Vitaly Nikolenko [article]

2016: "Linux Kernel ROP - Ropping your way to # (Part 2)" by Vitaly Nikolenko [article]

2016, Ruxcon: "Exploiting COF Vulnerabilities in the Linux kernel" by Vitaly Nikolenko [slides]

2016: "Using userfaultfd" by Lizzie Dixon [article]

2016, DEF CON 24: "Direct Memory Attack the Kernel" by Ulf Frisk [video]

2016, MOSEC 2016: "Talk is cheap, show me the code" by Keen Lab [slides]

2015: "Kernel Data Attack is a Realistic Security Threat" [whitepaper]

2015: "From Collision To Exploitation: Unleashing Use-After-Free Vulnerabilities in Linux Kernel" [whitepaper]

2015: "Linux Kernel Exploitation" by Patrick Biernat [slides]

2014: "Writing kernel exploits" by Keegan McAllister [slides]

2013: "Kernel stack overflows (basics)" by Essa Alkuwari [article]

2013, Black Hat USA: "Hacking like in the Movies: Visualizing Page Tables for Local Exploitation"

2013: "Exploiting linux kernel heap corruptions" by Mohamed Channam [article]

2012: "Understanding Linux Kernel Vulnerabilities" by Richard Carback [slides]

2012: "A Heap of Trouble: Breaking the Linux Kernel SLOB Allocator" by Dan Rosenberg [whitepaper]

2012: "Attacking hardened Linux systems with kernel JIT spraying" by Keegan McAllister [article]

2012: "The Linux kernel memory allocators from an exploitation perspective" by Patroklos Argyroudis [article]

2011: "Stackjacking Your Way to grsec/PaX Bypass" by Jon Oberheide [article]

2010: "Much ado about NULL: Exploiting a kernel NULL dereference" [article]

2010: "Exploiting Stack Overflows in the Linux Kernel" by Jon Oberheide [article]

2010, SOURCE Boston: "Linux Kernel Exploitation: Earning Its Pwnie a Vuln at a Time" by Jon Oberheide [slides]

2009, CanSecWest: "There's a party at ring0, and you're invited" by Tavis Ormandy and Julien Tinnes [slides]

2007: "Kernel-mode exploits primer" by Sylvester Keil and Clemens Kolbitsch [whitepaper]

2007, Phrack: "Attacking the Core : Kernel Exploiting Notes" [article]

2007: "The story of exploiting kmalloc() overflows" [article]

2005, CancSecWest: "Large memory management vulnerabilities" by Gael Delalleau [slides]

2005: "The story of exploiting kmalloc() overflows" [article]

Writeups

Information leak

2017: "Linux kernel 2.6.0 to 4.12-rc4 infoleak due to a data race in ALSA timer" by Alexander Potapenko [announcement, CVE-2017-1000380]

2017: "The Infoleak that (Mostly) Wasn't" by Brad Spengler [article, CVE-2017-7616]

2016: "Exploiting a Linux Kernel Infoleak to bypass Linux kASLR" [article]

2010: "Linux Kernel pktcdvd Memory Disclosure" by Jon Oberheide [article, CVE-2010-3437]

2009: "Linux Kernel x86-64 Register Leak" by Jon Oberheide [article, CVE-2009-2910]

2009: "Linux Kernel getname() Stack Memory Disclosures" by Jon Oberheide [article, CVE-2009-3001]

LPE

2018: "MMap Vulnerabilities – Linux Kernel" [article, CVE-2018-8781]

2018: "Ubuntu kernel eBPF 0day analysis" [article, CVE-2017-16995]

2017: "Adapting the POC for CVE-2017-1000112 to Other Kernels" [article, CVE-2017-1000112]

2017: "The Art of Exploiting Unconventional Use-after-free Bugs in Android Kernel" by Di Shen [slides, CVE-2017-0403, CVE-2016-6787]

2017: "Exploiting CVE-2017-5123 with full protections. SMEP, SMAP, and the Chrome Sandbox!" by Chris Salls [article, CVE-2017-5123]

2017: "Exploiting CVE-2017-5123" by Federico Bento [article, CVE-2017-5123]

2017: "Escaping Docker container using waitid() – CVE-2017-5123" by Daniel Shapira [article, CVE-2017-5123]

2017: "Exploiting on CVE-2016-6787" [article, CVE-2016-6787]

2017: "Race For Root: The Analysis Of The Linux Kernel Race Condition Exploit" by Alexander Popov [video, CVE-2017-2636]

2017: "Race For Root: The Analysis Of The Linux Kernel Race Condition Exploit" by Alexander Popov [slides, CVE-2017-2636]

2017: "Dirty COW and why lying is bad even if you are the Linux kernel" [article, CVE-2016-5195]

2017: "NDAY-2017-0103: Arbitrary kernel write in sys_oabi_epoll_wait" by Zuk Avraham [article, CVE-2016-3857]

2017: "NDAY-2017-0106: Elevation of Privilege in NVIDIA nvhost-vic driver" by Zuk Avraham [article, CVE-2016-2434]

2017: "PWN2OWN 2017 Linux kernel privilege escalation analysis" [article, CVE-2017-7184]

2017: "Exploiting the Linux kernel via packet sockets" by Andrey Konovalov [article, CVE-2017-7308]

2017: "NDAY-2017-0105: Elevation of Privilege Vulnerability in MSM Thermal Drive" by Zuk Avraham [article, CVE-2016-2411]

2017: "NDAY-2017-0102: Elevation of Privilege Vulnerability in NVIDIA Video Driver" by Zuk Avraham [article, CVE-2016-2435]

2017: "CVE-2017-2636: exploit the race condition in the n_hdlc Linux kernel driver bypassing SMEP" by Alexander Popov [article, CVE-2017-2636]

2017: "CVE-2017-2636: local privilege escalation flaw in n_hdlc" by Alexander Popov [announcement, CVE-2017-2636]

2017: "CVE-2017-6074: DCCP double-free vulnerability (local root)" by Andrey Konovalov [announcement, CVE-2017-6074]

2016: "CVE-2016-8655 Linux af_packet.c race condition (local root)" by Philip Pettersson [announcement, CVE-2016-8655]

2016, Black Hat: "Rooting Every Android From Extension To Exploitation" by Di Shen and James Fang [slides, CVE-2015-0570, CVE-2016-0820, CVE-2016-2475, CVE-2016-8453]

2016: "Talk is Cheap, Show Me the Code" by James Fang, Di Shen and Wen Niu [slides, CVE-2015-1805]

2016: "CVE-2016-3873: Arbitrary Kernel Write in Nexus 9" by Sagi Kedmi [article, CVE-2016-3873]

2016, Project Zero: "Exploiting Recursion in the Linux Kernel" by Jann Horn [article, CVE-2016-1583]

2016: "ANALYSIS AND EXPLOITATION OF A LINUX KERNEL VULNERABILITY (CVE-2016-0728)" By Perception Point Research Team [article, CVE-2016-0728]

2016: "CVE20160728 Exploit Code Explained" by Shilong Zhao [article, CVE-2016-0728]

2016: "CVE-2016-0728 vs Android" by Collin Mulliner [article, CVE-2016-0728]

2016: "Notes about CVE-2016-7117" by Lizzie Dixon [article, CVE-2016-7117]

2016: "CVE-2016-2384: exploiting a double-free in the usb-midi linux kernel driver" by Andrey Konovalov [article, CVE-2016-2384]

2016: "CVE-2016-6187: Exploiting Linux kernel heap off-by-one" by Vitaly Nikolenko [article, CVE-2016-6187]

2016: "CVE-2014-2851 group_info UAF Exploitation" by Vitaly Nikolenko [article, CVE-2014-2851]

2016, HITB Ams: "Perf: From Profiling To Kernel Exploiting" by Wish Wu [slides, CVE-2016-0819]

2016, HITB Ams: "Perf: From Profiling To Kernel Exploiting" by Wish Wu [video, CVE-2016-0819]

2015: "Android linux kernel privilege escalation vulnerability and exploit (CVE-2014-4322)" by Gal Beniamini [article, CVE-2014-4322]

2015: "Exploiting "BadIRET" vulnerability" by Rafal Wojtczuk [article, CVE-2014-9322]

2015: "Follow-up on Exploiting "BadIRET" vulnerability (CVE-2014-9322)" by Adam Zabrocki [article, CVE-2014-9322]

2015, Black Hat: "Ah! Universal Android Rooting Is Back" by Wen Xu [whitepaper, CVE-2015-3636]

2015, Black Hat: "Ah! Universal Android Rooting Is Back" by Wen Xu [slides, CVE-2015-3636]

2015, Black Hat: "Ah! Universal Android Rooting Is Back" by Wen Xu [video, CVE-2015-3636]

2015: "When is something overflowing" by Keen Team [slides]

2015, Project Zero: "Exploiting the DRAM rowhammer bug to gain kernel privileges" by Mark Seaborn and Thomas Dullien [article, rowhammer]

2014: "Exploiting CVE-2014-0196 a walk-through of the Linux pty race condition PoC" by Samuel Gross [article, CVE-2014-0196]

2014: "CVE-2014-4943 - PPPoL2TP DoS Analysis" by Vitaly Nikolenko [article, CVE-2014-4943]

2014: "CVE-2014-4014: Linux Kernel Local Privilege Escalation "exploitation"" by Vitaly Nikolenko [article, CVE-2014-4014]

2014: "CVE-2014-4699: Linux Kernel ptrace/sysret vulnerability analysis" by Vitaly Nikolenko [article, CVE-2014-4699]

2014: "How to exploit the x32 recvmmsg() kernel vulnerability CVE 2014-0038" by Samuel Gross [article, CVE-2014-0038]

2014: "Exploiting the Futex Bug and uncovering Towelroot" [article, CVE-2014-3153]

2014: "CVE-2014-3153 Exploit" by Joel Eriksson [article, CVE-2014-3153]

2013: "Privilege Escalation Kernel Exploit" by Julius Plenz [article, CVE-2013-1763]

2013: "A closer look at a recent privilege escalation bug in Linux (CVE-2013-2094)" by Joe Damato [article, CVE-2013-2094]

2012: "Linux Local Privilege Escalation via SUID /proc/pid/mem Write" by Jason Donenfeld [article, CVE-2012-0056]

2011, DEF CON 19: "Kernel Exploitation Via Uninitialized Stack" by Kees Cook [slides, CVE-2010-2963]

2011, DEF CON 19: "Kernel Exploitation Via Uninitialized Stack" by Kees Cook [video, CVE-2010-2963]

2010: "CVE-2010-2963 v4l compat exploit" by Kees Cook [article, CVE-2010-2963]

2010: "Exploiting large memory management vulnerabilities in Xorg server running on Linux" by Rafal Wojtczuk [article, CVE-2010-2240]

2010: "CVE-2010-4258: Turning Denial-of-service Into Privilege Escalation" by Nelson Elhage [article, CVE-2010-4258]

2010: "CVE-2007-4573: The Anatomy of a Kernel Exploit" by Nelson Elhage [article, CVE-2007-4573]

2010: "Linux Kernel CAN SLUB Overflow" by Jon Oberheide [article, CVE-2010-2959]

2010: "af_can linux kernel overflow" by Ben Hawkes [article, CVE-2010-2959]

2010: "linux compat vulns (part 1)" by Ben Hawkes [article, CVE-2010-3081]

2010: "linux compat vulns (part 2)" by Ben Hawkes [article, CVE-2010-3301]

2010: "Some Notes on CVE-2010-3081 Exploitability" [article, CVE-2010-3081]

2010: "Anatomy of an exploit: CVE-2010-3081" [article, CVE-2010-3081]

2010: "CVE-2010-4258: Turning denial-of-service into privilege escalation" by Nelson Elhage [article, CVE-2010-4258]

2009: "Linux NULL pointer dereference due to incorrect proto_ops initializations (CVE-2009-2692)" [article, CVE-2009-2692]

2009: "Even when one byte matters" [article, CVE-2009-1046]

2009: "CVE-2008-0009/CVE-2008-0010: Linux kernel vmsplice(2) Privilege Escalation" [article, CVE-2008-0009, CVE-2008-0010]

2008: "vmsplice(): the making of a local root exploit" by Jonathan Corbet [article, CVE-2008-0600]

2004: "Linux kernel do_mremap VMA limit local privilege escalation vulnerability" [article, CVE-2004-0077]

RCE

2017: "BlueBorn: The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks" [whitepaper, CVE-2017-1000251]

2016: "CVE Publication: CVE 2016-8633" by Eyal Itkin [article, CVE-2016-8633]

2011, DEF CON 19: "Owned Over Amateur Radio: Remote Kernel Exploitation in 2011" [slides, CVE-2011-1493]

2011, DEF CON 19: "Owned Over Amateur Radio: Remote Kernel Exploitation in 2011" [video, CVE-2011-1493]

2009: "When a "potential D.o.S." means a one-shot remote kernel exploit: the SCTP story" [article, CVE-2009-0065]

Other

2017: "initroot: Bypassing Nexus 6 Secure Boot through Kernel Command-line Injection" [article, CVE-2017-1000363]

2016: "Motorola Android Bootloader Kernel Cmdline Injection Secure Boot Bypass" [article, CVE-2016-10277]

Protection bypass techniques

2016: "Linux Kernel x86-64 bypass SMEP - KASLR - kptr_restric" [article]

2016, KIWICON: "Practical SMEP bypass techniques on Linux" by Vitaly Nikolenko [slides]

2016: "Micro architecture attacks on KASLR" by Anders Fogh" [article]

2016: "Jump Over ASLR: Attacking Branch Predictors to Bypass ASLR" by Dmitry Evtyushkin, Dmitry Ponomarev and Nael Abu-Ghazaleh [slides]

2016, CCS: "Prefetch Side-Channel Attacks: Bypassing SMAP and Kernel ASLR" by Daniel Gruss, Clementine Maurice, Anders Fogh, Moritz Lipp and Stefan Mangard [video]

2016, Black Hat USA: "Using Undocumented CPU Behavior to See Into Kernel Mode and Break KASLR in the Process" [video]

2016, Black Hat USA: "Breaking KASLR with Intel TSX" Yeongjin Jang, Sangho Lee and Taesoo Kim [slides]

2016, Black Hat USA: "Breaking KASLR with Intel TSX" Yeongjin Jang, Sangho Lee and Taesoo Kim [video]

2016: "Breaking KASLR with micro architecture" by Anders Fogh [article]

2015: "Effectively bypassing kptr_restrict on Android" by Gal Beniamini [article]

2014, Black Hat Europe: "ret2dir: Deconstructing Kernel Isolation" by Vasileios P. Kemerlis, Michalis Polychronakis, Angelos D. Keromytis [whitepaper]

2014, Black Hat Europe: "ret2dir: Deconstructing Kernel Isolation" by Vasileios Kemerlis [video]

2013: "A Linux Memory Trick" by Dan Rosenberg [article]

2011: "SMEP: What is It, and How to Beat It on Linux" by Dan Rosenberg [article]

2009: "Bypassing Linux' NULL pointer dereference exploit prevention (mmap_min_addr)" [article]

Defensive

2018, BlackHat: "kR^X: Comprehensive Kernel Protection Against Just-In-Time Code Reuse" [video]

[2018: "KASR: A Reliable and Practical Approach to Attack Surface Reduction of Commodity OS Kernels"] (https://arxiv.org/pdf/1802.07062.pdf) [paper]

2018, Linux Conf AU: "The State of Kernel Self Protection" by Kees Cook [slides]

2017: "Towards Linux Kernel Memory Safety" [whitepaper]

2017: "Proposal of a Method to Prevent Privilege Escalation Attacks for Linux Kernel" [slides]

2017: "Linux Kernel Self Protection Project" by Kees Cook [slides]

2017: "PT-Rand: Practical Mitigation of Data-only Attacks against Page Tables" [whitepaper]

2017: "KASLR is Dead: Long Live KASLR" [whitepaper]

2017: "Honey, I shrunk the attack surface – Adventures in Android security hardening" by Nick Kralevich [video]

2017: "Fine Grained Control-Flow Integrity for The Linux Kernel" by Sandro Rigo, Michalis Polychronakis, Vasileios Kemerlis [slides]

2016: "Thwarting unknown bugs: hardening features in the mainline Linux kernel" by Mark Rutland [slides]

2016: "Emerging Defense in Android Kernel" by James Fang [article]

2016: "Randomizing the Linux kernel heap freelists" by Thomas Garnier [article]

2015: "Protecting Commodity Operating Systems through Strong Kernel Isolation" by Vasileios Kemerlis [whitepaper]

2014: "Kernel Self-Protection through Quantified Attack Surface Reduction" by Anil Kurmus [whitepaper]

2013: "KASLR: An Exercise in Cargo Cult Security" by Brad Spengler [article]

2012: "How do I mitigate against NULL pointer dereference vulnerabilities?" by RedHat [article]

2011: "Linux kernel vulnerabilities: State-of-the-art defenses and open problems" [paper]

2009, Phrack: "Linux Kernel Heap Tampering Detection" by Larry Highsmith [article]

Fuzzing & detectors

2018, BlackHat: "New Compat Vulnerabilities In Linux Device Drivers" [slides]

2018: "Precise and Scalable Detection of Double-Fetch Bugs in OS Kernels" [paper]

2017: "The android vulnerability discovery in SoC" by Yu Pan and Yang Dai [slides]

2017, Black Hat USA: "Evolutionary Kernel Fuzzing" by Richard Johnson [slides]

2017: "DIFUZE: Interface Aware Fuzzing for Kernel Drivers" [whitepaper]

2017: "DIFUZE: Interface Aware Fuzzing for Kernel Drivers" [slides]

2017, CCS: "SemFuzz: Semantics-based Automatic Generation of Proof-of-Concept Exploits" [whitepaper]

2017, USENIX: "kAFL: Hardware-Assisted Feedback Fuzzing for OS Kernels" [whitepaper]

2017, USENIX: "How Double-Fetch Situations turn into DoubleFetch Vulnerabilities: A Study of Double Fetches in the Linux Kernel" [whitepaper]

2017, USENIX: "DR. CHECKER: A Soundy Analysis for Linux Kernel Drivers" [whitepaper]

2016, Linux Plumbers: "Syzkaller, Future Developement" by Dmitry Vyukov [slides]

2016: "Coverage-guided kernel fuzzing with syzkaller" [article]

2016: "Filesystem Fuzzing with American Fuzzy Lop" by Vegard Nossum and Quentin Casasnovas [slides]

2016, ToorCon: "Project Triforce: AFL + QEMU + kernel = CVEs! (or) How to use AFL to fuzz arbitrary VMs" [slides]

2015, LinuxCon North America: "KernelAddressSanitizer (KASan): a fast memory error detector for the Linux kernel" by Andrey Konovalov [slides]

2015, DEF CON 23: "Introduction to USB and Fuzzing" by Matt DuHarte [video]

2015, Black Hat: "Don't Trust Your USB! How to Find Bugs in USB Device Drivers" by Sergej Schumilo, Ralf Spenneberg, and Hendrik Schwartke [video]

2012: "Comprehensive Kernel Instrumentation via Dynamic Binary Translation" [whitepaper]

2010: "Automatic Bug-finding Techniques for Linux Kernel" by Jiri Slaby [whitepaper]

Fuzzers

https://github.com/google/syzkaller

https://github.com/kernelslacker/trinity

http://web.eece.maine.edu/~vweaver/projects/perf_events/fuzzer/

https://github.com/nccgroup/TriforceLinuxSyscallFuzzer

https://github.com/oracle/kernel-fuzzing

https://github.com/rgbkrk/iknowthis

https://github.com/schumilo/vUSBf

https://github.com/ucsb-seclab/difuze

Exploits

https://www.exploit-db.com/search/?action=search&description=linux+kernel

https://github.com/offensive-security/exploit-database/tree/master/platforms/linux/local

https://bugs.chromium.org/p/project-zero/issues/list?can=1&q=linux+kernel&colspec=ID+Type+Status+Priority+Milestone+Owner+Summary&cells=ids

http://vulnfactory.org/exploits/

https://www.kernel-exploits.com/

https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs

https://github.com/ScottyBauer/Android_Kernel_CVE_POCs

https://github.com/f47h3r/hackingteam_exploits

https://github.com/xairy/kernel-exploits

https://github.com/Kabot/Unix-Privilege-Escalation-Exploits-Pack

https://github.com/SecWiki/linux-kernel-exploits

https://grsecurity.net/~spender/exploits/

https://github.com/jiayy/android_vuln_poc-exp

https://github.com/marsyy/littl_tools/tree/master/bluetooth

https://github.com/nongiach/CVE/tree/master/CVE-2017-5123

http://seclists.org/fulldisclosure/2010/Sep/268

https://github.com/hardenedlinux/offensive_poc

https://github.com/jiayy/android_vuln_poc-exp

https://github.com/brl/grlh

Practice

CTF tasks

CSAW CTF 2010: writeup, source

CSAW CTF 2011: writeup, source

CSAW CTF 2013: writeup, source and exploit

CSAW CTF 2014: source and exploit

CSAW CTF 2015: writeup 1, writeup 2, source and exploit

Insomni'hack finals 2015: writeup, source and exploit

rwth2011 CTF (ps3game): writeup

PlaidCTF 2013 (Servr): writeup, source

0ctf2016: writeup, exploit

0ctf2017: source and exploit

0ctf2018: writeup 1, writeup 2

Tools

https://github.com/jonoberheide/ksymhunter

https://github.com/jonoberheide/kstructhunter

https://github.com/ngalongc/AutoLocalPrivilegeEscalation

https://github.com/PenturaLabs/Linux_Exploit_Suggester

https://github.com/jondonas/linux-exploit-suggester-2

https://github.com/mzet-/linux-exploit-suggester

https://github.com/spencerdodd/kernelpop

https://github.com/vnik5287/kaslr_tsx_bypass

http://www.openwall.com/lkrg/

https://github.com/IAIK/meltdown

Misc

https://github.com/Fuzion24/AndroidKernelExploitationPlayground

https://github.com/ReverseLab/kernel-pwn-challenge

https://github.com/NoviceLive/research-rootkit

https://github.com/djrbliss/libplayground

pwnable.kr tasks (syscall, rootkit, softmmu, towelroot, kcrc, exynos)

RPISEC kernel labs

https://github.com/hackedteam

https://github.com/mncoppola/Linux-Kernel-CTF

https://crowell.github.io/blog/2014/11/24/hosting-a-local-kernel-ctf-challenge/

https://github.com/ukanth/afwall/wiki/Kernel-security

https://github.com/a13xp0p0v/linux-kernel-defence-map

https://github.com/kmcallister/alameda

https://github.com/01org/jit-spray-poc-for-ksp

https://forums.grsecurity.net/viewforum.php?f=7