征途： HardenedLinux 社区 2016

Shawn C

#whois

* Shawn C[a.k.a "citypw"]
* Day job at TYA infotech
    * Open source security consulting
* GNU/Linux 安全工程师
* 自由软件狂热分子
* EFF/FSF/FSFE/SFC 会员
* Hardenedlinux 社区 (https://hardenedlinux.github.io/) 发起人

#cat /proc/agenda

* Genesis
* HardenedLinux 社区成员组
* HardenedLinux 社区愿景
* HardenedLinux 社区项目
* HardenedLinux 社区未来关注的方向
* 如何关注我们

#Genesis

* when:
  2014

* why:
  * Truth
  * Rational Anarchist
  * “Cyber” security
  * Defense In Depth

#HardenedLinux 社区成员组成

* 自由软件狂热分子
* 反权威主义
* 信息安全研究人员

其他作出贡献志愿者成员

https://hardenedlinux.github.io/about2/

现状

今天的 IT 基础设施 (IDC 、数通产品 ）及物联网、移动网络都重度依赖自由软件，自由软件已经成为重要基础设施的一部分，不管对于政府、企业、个人都是非常重要的。

资助 HOST(美国国土安全部的开放安全技术) 项目的美国国土安全部的在 13636 号行政命名中描述到：“这是美国改善安全和国家重要基础设施的防御能力的政策，去维护一个鼓励高效，创新和经济繁荣同时保证安全，商业机密和人生自由的网络环境。 “

愿景

推进自由软件基础架构安全的工程化。

加固一小步，自由软件一大步。


HardenedLinux's roadmap
Crypto Engineering
Firmware
Compiler
Security operations
Situational Hardening
KERNEL
Free/Libre & Open Source Software's eco-system:
+ GPL-compliance
+ Legislation
+ Education
Adversary
The West Of Middle Earth At The End Of The Third Age
FORODWAITH
Angmar
Mount Gunduband
Ered Mithrin
Iron Hills
ARNOR
HITHAEGLIR
ERED LUIN
Forlindon
Ettenmoors
Weather Hills
Rhudaur
Erebor (The Lonely Mountain)
Erareth on the Long Lake
ARTHEDAIN
Old Forest
The Shire
Bree
Rivendell
Mirkwood
East Bight
RHÛN
Sea of Rhun
Blue Mountains
Harlindon
ERIADOR
Eregion
MINHIRIATH
Dunland
Lorien
Fangorn
Isengard
The Brown Lands
ENEDWAITH
Helms
Ered Lithui (Ash Mountians)
N. Ithilien
Plateau of Gorgoroth
MORDOR
NURN
Anfalas
Lebennin
S. Ithilien

#Kernel

* PaX/Grsecurity 是核心基石
* KSPP(Linux 内核自防护)
* Sandboxing via seccomp

发行版默认支持 PaX/Grsecurity

* 已经支持：

* 未来会支持的发行版本？

https://github.com/hardenedlinux/hardenedlinux_profiles/blob/master/aosc_desktop/pax-bites.conf

#Compiler

LangSec 架构：

* 针对应用程序的 mitigation
* 利用编译器内部特性的加固，e.g: GCC plugins
* 形式化
  * DDC --> reproducible builds

#Firmware

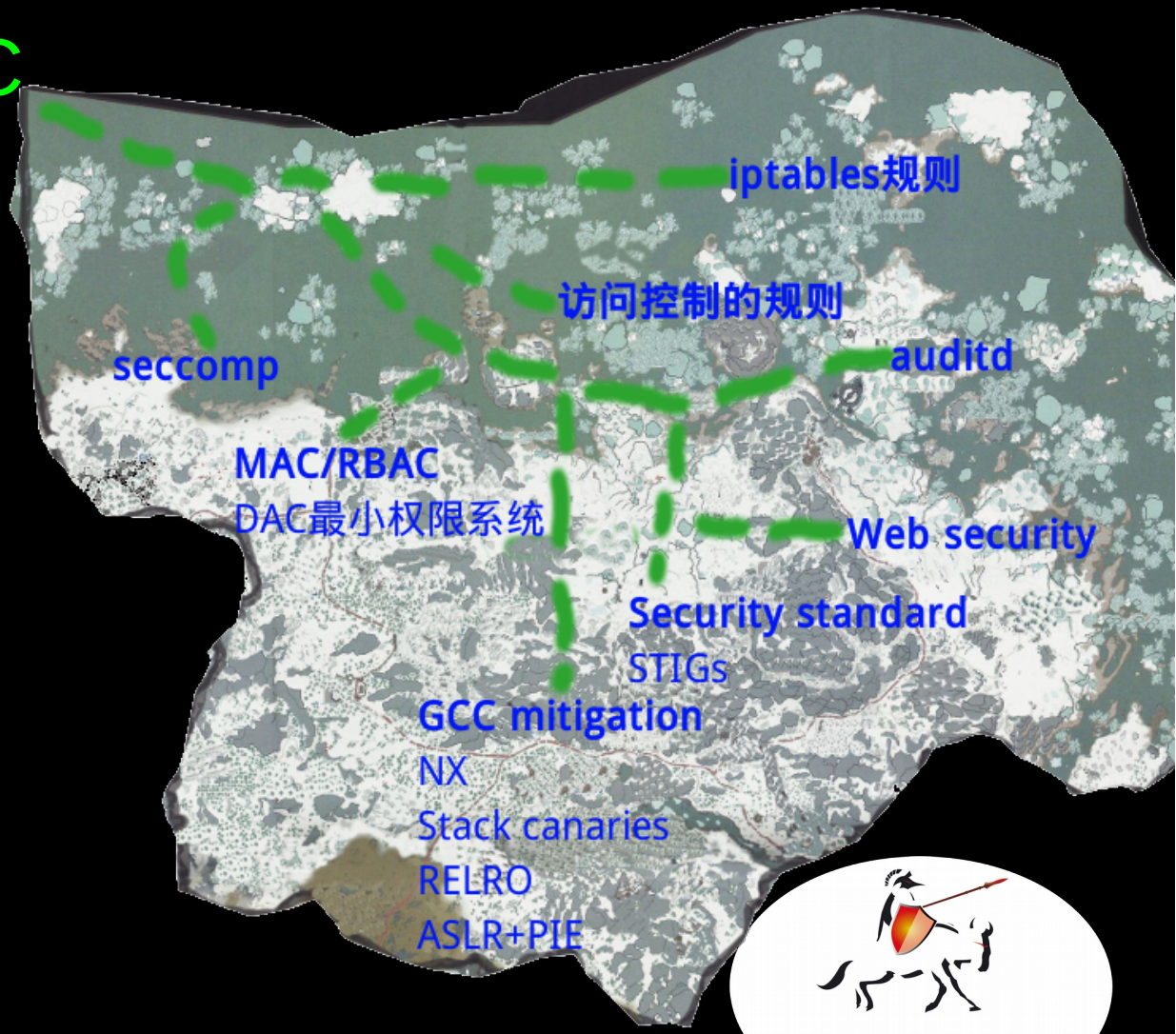
Need your contribution;-)

密码工程

* SSL/TLS 最佳部署实践
* IPsec 最佳实践

#GNU/Linux 安全运维

* DAC/MAC/RBAC
* iptables/nftables
* auditd
* web security
* etc



基于自由软件的场景化加固

* 针对业务的分析
* 制定场景化方案
* DEVOPS
* 数据分析与联动防御

#Situational hardening case study

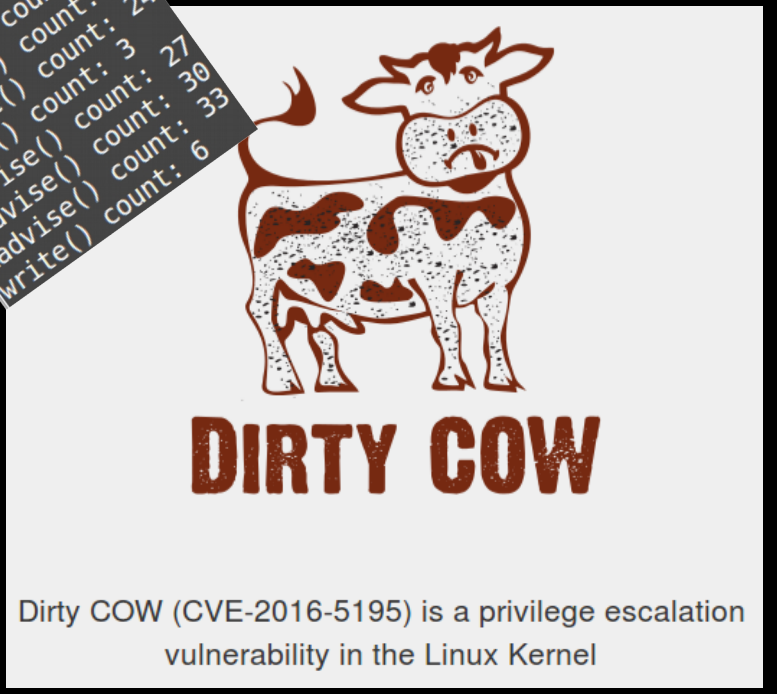
Threat model via public info:

Trigger code path with “FOLL_FORCE” via get_user_pages():

* Writing at /proc/pid/mem
* ptrace()’s POKEDATA
* Extra bonus? vDSO;-)

Other potential risk:

* weaponized exploit via unknown?



* 方案 N
  * Upgrade or backport fix
  * PaX’s tuned vDSO(KSPP does it later)
  * PaX’s restriction on file perm
  * Seccomp-bpf
  * Grsecurity’s RBAC
  * Syscall/*hook hijacking madvise() “s/MADV_DONTNEED/MADV_*/g”? A rootkit? Seriously;-)

生态

* 推动自由软件相关立法
* GPL 合规
* 支持相关机构（ FSF, FSFE, EFF, SFC, ETC)
* 支持更多自由软件基础架构的安全改进，比如 CII（基础架构联盟）

已完成的项目 -1

Hardened PoC: PaX for Android ， PaX 是 PaX/Grsecurity 的集合的一部分，所有的 feature 都是针对 memory corruption 利用的防御，完成了针对 msm-3.4 的加固，包括部分 PaX 特性的移植以及相关加固， Nexus 7 2013 上测试通过。

已完成的项目 -2

STIG-4-Debian ， STIG （安全技术实现指南）是由 DISA 为了 IT 安全态势给 DoD(美国国防部）提供的一套防御指南， GNU/Linux 的发行版只有针对 RHEL 的，由 Red Hat 实现的，我们移植了 STIG for RHEL 并且做了相关改动，比如针对 SELinux 的检测由 AppArmor 替换，最终在 Debian 8 上测试通过，未来会基于 STIG-4-DEBIAN 框架参考 compliance 实现（比如 Lynis Enterprise) 进行安全标准实现的加强。

已完成的项目 -3

Reproducible build for PaX/Grsecurity ， Reproducible packaging 是由 EFF 和 Debian 社区开发的用于对抗大规模监控的一种打包机制，它能重现 binary 在编译时的场景，我们完成了针对 PaX/Grsecurity 的 reproducible builds 。

进行中的项目？

项目名称	描述
Offensive PoC	针对可利用的 bug 编写 PoC
Debian GNU/Linux: best practice profiles	Debian GNU/Linux 的运维护以及安全最佳实践
Community QA	利用 sanitized 环境进行 bug hunting
???	Your contribution?

社区捐赠 -why?

改变自由软件的现状不是由几个人能够去改变的，需要更多的人或社区来一起推进和完成，而我们捐赠的自由软件社区和组织是和我们有着一样的愿景的，同时我们也是他们所做出的项目的受益者和使用者，所以我们选择给予捐赠给他们。

社区贡献 - 翻译文档

* 黑客与英雄们：双国战记
* 黑客与英雄们： CCC 和黑客空间的崛起
* CCC(混沌通讯会议)：一场很德国的黑客大会
* PaX 早期设计文档概述
* MPROTECT 早期设计文档
* 关于 RAP 的 FAQ
* Linux 内核自防护项目的初始文档
* 自由 / 开源软件 (FLOSS) 的最佳实践标准（第一部分）
* 自由 / 开源软件 (FLOSS) 的最佳实践标准（第二部分）

社区贡献 - 文档贡献

* How to build Clang toolchains for Android
* (A/T/KT) - Sanitized GNU/Linux: a new way of bug hunter in FLOSS Community
* NX(No-eXecute) 的实现分析
* PIC/PIE 分析
* Reproducible builds for PaX/Grsecurity
* 面向桌面的 PaX/Grsecurity 内核配置注释与评论
* Build debug environment for the dynamic linker of Glibc
* shared library wrinkle

未来关注的方向

主要会关注 3 个基础架构的系统安全：

* Kernel
* Compiler
* Firmware

同时也关注开放环境中的防御的另一块基石：

* 密码工程

关注我们的社区

* Hardenedlinux 社区

  # 官方网站： http://hardenedlinux.org

  # github: https://github.com/hardenedlinux

  # twitter: https://twitter.com/hardenedlinux

  # 新浪微博： @hardenedlinux

* 使用自由软件的方案加固一切
* 狂热的自由软件玩家以及 Anarchy

  (Anarchy 翻译成“反权威主义”更准确)
* 关注企业安全

谢 谢 大 家 !

https://hardenedlinux.github.io/