閌蠱：VIRUSMORE

新型全平台 Linux 模拟器(发行版)

2021.5.29

0X00、项目背景

1、为什么要发起“閌蠱“开源项目

为什么要发起“閌(chu)蠱”开源项目？这个项目最终会有什么结果，甚至是后果？必须要这样做吗？没有另外的途径可以实现项目最终的目的吗？

其实，这些问题一直困扰着我。我也在不断地反思，甚至质问自己，毕竟盲目地行为往往不会有善良地结果。

作为一名网络安全从业者或者研究人员，我一开始接触到的是 Windows 操作系统，并且天真的认为世界本就只有 Windows 系统。因为选择了计算机专业，自己对操作系统的认识逐渐深入，对操作系统及其相关技术的认知更加全面，我对这些技术非常着迷，尤其是操作系统底层实现技术。非常幸运的是，我在研究生期间从事了一系列很有趣，很 cool 的底层驱动开发项目，有机会更加深入地了解操作系统运行机制，在内核与杀软对抗。那个时候，Windows 内核木马及反木马软件圈子非常活跃，国内研究 Windows 驱动的牛人开始崭露头角，包括 pfj，mj，楚狂人，wowocock 等等。当然，自己对操作系统的认知也不再局限于 Windows。

因为工作的需要，自己开始慢慢接触 Linux，特别是近两年来，自己的研究方向全面转向 IoT 安全，接触了各种平台上的不同操作系统。从 PC 上的 Kali，ParrotSec，Backbox，到移动终端上的 Android，iOS 和 Windows CE，以及可运行于 Android 之上的 Linux 模拟器 Kali Nethunter 和 andrax,当然还有运行于 iOS 上的 iSH Linux 模拟器。使用过这些软件之后，发现他们或多或少存在这样那样的问题，尤其是当你只能依靠一台智能手机进行渗透测试的时候，你会发现 PC 上的操作体验完全被颠覆，你会有一种纵有万般能耐于一身，奈何被困方寸间的无可奈何。这就是我希望开发一个适合于全新网络环境下 hacking 的 Linux 发行版的初衷。

期间，我也曾尝试着通过与高校在校学生组成兴趣团体，以纯粹的兴趣为导向来维系整个项目前行的源动力。但是，一系列的事情使我认清了现实，并主动放弃了这个想法，现在的学生更看中付出与回报之间的比例，没有了我们当年那种挑灯鏖战，通宵不断的动力和闯劲。“閎蠱”项目本质上来说是一个“劳动力密集型”的项目，缺乏了最关键的因素——人，我因此陷入了迷茫，这个事情也就一拖再拖。

真正触动我的非要做成这件事的“导火索”应该是 thecrackertechnology 公司于今年初发布了 andrax PC 版本。Andrax 从 2016 年起步至今，已经蹿升至全球黑客工具排行版前三甲。那我还有什么可退缩的呢？毕竟，andrax 团队也很小。

我想前面这些唠唠叨叨的话应该能够说明白我为什么坚持于此，执着于此。当然，一个坚定、执着的决定已经做出了，接下来便是未知，挑战，迷茫，彷徨，前行，跌倒，自省和升华。期待有志同道合者，结伴前行！

2、什么是 Linux 模拟器

基于 chroot 技术，在不同类型软硬件计算环境下，提供 Linux 系统及相关应用支持的软件模拟环境。chroot 是在 UNIX 系统的一个操作命令，针对正在运行的软件进程和它的子进程，改变其外显的根目录。一个运行在该环境下，经由 chroot 设置根目录的程序，它不能够对这个指定根目录之外的文件进行访问动作，不能读取，也不能更改它的内容［1,2］。chroot 是一种极为成熟并且在*nix 平台上有着广泛应用的技术，可以用于“閟蠱”项目中实现多种平台下对 Linux 模拟器及其应用软件的支撑。

3、“閟蠱”依托的软件环境

——*nix：chroot 技术本身就源自 UNIX 系统，拥有操作系统内核层次的支持，因此“閟蠱”可以在*nix 系统上稳定运行。由于*nix 系统发行版本众多，直接在各个不同发行版本上搭建统一的系统软件及应用程序环境，工作量极其庞大且完全没有这个必要，基于 chroot 技术可以提供完美的底层操作系统及应用程序支撑。

——MacOS：由于 Mac OS X 使用基于 BSD Unix 的内核 ，因此不论在代码复用上还是系统设计思想上，MacOS 与 Unix 存在天然的“血缘关系”，比如 chroot 机制就被完美的复用到了 MacOS 上。而且，近年来，苹果公司在开源软件上面接受度越来越大，其与 Linux 之间的兼容性也越来越好。因此，不论是基于 Parallels 或 VMWare Fusion 虚拟化软件，还是基于 chroot 技术，“閟蠱”可以很好的适配 MacOS 系统，包括最新的 Arm 架构的 MacOS。

——Windows：对于 Windows 操作系统而言，NT 内核在设计之初就可以支持 POSIX，OS/2 和 Win32 子系。而且，Windows 10 系统引入了 WSL（Windows Subsystem Linux）可以更好的支持 Linux 模拟器，即在 Windows 操作系统上运行 elf 格式的可执行文件。此外，Debian， Ubuntu，Redhat 以及 CentOS 等主流的 Linux 发行版本都已经得到了微软公司支持，可以在微软应用商店直接下载（购买）可运行于 Windows 操作系统上的 Linux 系统应用。也就是说，对于“閟蠱”而言，在 Windows 操作系统上不存在任何前所未有的技术问题。

——Android：谷歌公司推出安卓系统本质上是一个在 Linux 内核基础上定制化开发、优化的 Java 虚拟机，与*nix 系统一脉相承。此外，“閟蠱”对标的 Kali Nethunter 以及 andrax 都是基于 Debian 发行版本开发的 Android 终端模拟器。综上所述，对于“閟蠱”项目而言，在 Android 系统上不存在任何无法逾越的技术鸿沟。

——iOS：iOS 与 MacOS 之间是天然的“同宗同族”，但是在系统权限管理上面，iOS 系统更为严苛。因此，要在 iOS 系统上运行“閌蠱”系统存在一定技术难度，但是国外 iSH 团队已经在无 root 权限的情况下，实现了在本地 iOS 设备上运行 Linux shell 环境。对于“閌蠱”项目而言，可以在 iSH 开源代码基础上进行二次开发，重点打造系统的开放性，易用性以及完整的黑客工具支撑，从而实现“閌蠱”系统的全平台覆盖。

4、“閌蠱”支持的硬件环境

——PC，包括台式电脑，笔记本电脑，Surface 等超级本（i386，arm64 和 amd64）。

——平板电脑，包括安卓平板电脑和 iPad（arm32 和 arm64）。

——智能移动终端，主要是智能手机等设备（arm32，arm64）。

——IoT 设备，主要包括具有较好人机交互条件的智能查询终端等设备（arm32，arm64）。

5、主流 Linux 模拟器简要对比分析

名称	LOGO	优势	劣势
Termux		1.Android 上最老牌的 Linux 模拟器； 2.与 Android 系统深入融合，可以直接访问 Android 系统资源（会受到权限的约束）；	1.操作界面不友好，易用性差； 2.仅提供最基础的 Linux shell 环境支持； 3.网络更新源有限，缺乏对安全工具的支持； 4.不支持非 Android 设备；
Kali Nethunter		1.植根于 Kali Linux，性能优越，稳定性好； 2.有良好的社区生态； 3.软件更新及时，能够满足专业测试人员的大部分需求； 4.已经形成研发，应用及培训一体化的安全产业链条；	1.操作界面并不友善，用户体验差； 2.网络安全攻击集成度远不及 Kali Linux； 3.不支持非 Android 设备；

Andrax		1.当前，网络安全专业工具集成度最高的一款 Linux 模拟器； 2.技术路线更加激进，尽可能优化 UI，提高专业用户体验感； 3.zsh 的引入和优化，极大提高专业用户的工作效率；	1.Andrax 起步较晚，社区生态尚不成熟； 2.受限于社区及开发人员数量，软件更新频率较低； 3.软件 UI 整体效果不错，但是虚拟终端切换方式单一，不利于不同终端之间的频繁切换； 4. 不支持非 Android 设备； 5.andrax 安卓版本和 Arm 版本不运行用户自主更新系统，更新操作必须通过下载并安装官方全量更新包实现；
AnLinux		1.AnLinux 项目开源，并且支持免 root 运行； 2.对主流的 Linux 发行版支持较好；	1.因为种种原因，AnLinux 安装部分 Linux 发行版本时会产生种种异常错误； 2. 不支持非 Android 设备；
閔蠱 virusmore		1.支持*nix，MacOS，Windows 等传统 PC 操作系统； 2.支持 Android，HarmonyOS 以及 iOS 等智能终端操作系统； 3.在软件集成度与系统更新之间充分平衡，支持增量更新，减少不必要的使用成本； 4.从专业渗透测试人员角度思考 UI 设计，通过引入 zsh，水平滑动方式切换	1.国内第一个以中国网络安全人员为主体的全球性网安社区； 2.虽然整体技术路线清晰，但是工作量大，涉及的技术领域宽泛，对于开发者的技术要求略高； 3.作为中国第一个偏向底层系统的、全平台覆盖的开源项目，管理难度较大，尤其缺乏国外开发人员和黑客的技术支持；

		虚拟终端，一键式电池优化管理以及文本智能缩放和选择； 5.基于 Github 的开源方案； 6.以社交软件为主体的社区生态维护； 7.Wiki 知识库构建； 8.线下社区互动； 9.基于“閌蠱”系统的在线攻防演练靶场； 10.基于“閌蠱”系统的付费安全培训及认证；	4.由于项目定位，参与人员的地域特性，“閌蠱“项目的生态建设及维护将会遭遇极大挑战； 5. “閌蠱“项目定位是一个纯粹的开源项目，因此前期项目开发仅能依靠社区力量，没有任何外部资金支持（至少目前如此）； 6.待“閌蠱“项目有了实质性进展，并且社区生态初步形成后，我们可能会通过用户捐赠，广告，项目基金，厂商赞助以及其他可期待的资金筹措方法推动社区发展，加快项目开发速度。总之，利用一切资源和力量推动“閌蠱“项目早日形成全平台覆盖。

6、关于“閌蠱“这个名字

“閌蠱”这个名字一方面是受了犇众团队的启发，另一方面我想突出项目最终所体现的“中国元素”——中国黑客团体的力量。

“閌”(chu)，该字并非繁体，仅在“阿閌佛”一词中有使用。阿閌佛，又称不动如来，梵语为 Aksokhya，意为“不嗔恚”，即不作恶，与项目初衷一致，通过社区的力量开发一款致力于多终端、多系统下可用的安全检测和渗透测试工具集合，而非诱人作恶，危害网络安全。

“蠱”，该字为“蛊”字繁体，泛指虫、疾，取其形意，与“閌”字相呼应。

以“閌蠱”二字作为项目的名称，一是希望集结一帮志同道合者，在同一个地方（“門”）做一些很酷的事情；二是，透过“蠱”字表明所做之事皆为治“蠱”，希望为全新网络形态下的从业者提供更加趁手的安全检测和渗透测试工具集。

0X01、目标与技术路线

1、核心目标

“閎蠱”项目终极目标是要开发一款新型全平台 Linux 模拟器。不仅能够提供多样性环境下的便捷 Linux 系统及丰富的应用软件支撑，并且可以根据不同的应用场景快速“组装”，满足传统企业内部网络管理，IoT 环境下的网络运维以及特殊领域业务需求。

2、技术路线

以*nix 系统（估计最终会选择 Linux）主流版本为基础，以网络安全应用为主要应用场景，集成业界认可且有良好社区生态的安全软件，能够适配传统 PC，智能移动终端以及 IoT 设备的新型全平台 Linux 模拟器(Linux 发行版)。

0X02、预期目标

1、终极目标

随着“閎蠱”技术团队的不断成长，“閎蠱”系统自身的不断迭代，系统本身能够满足日益复杂的网络环境以及网络攻防对抗环境，能够适配各种新型应用场景的严苛技术要求；技术团队能够更快、更好、更专业地支撑项目的不断发展，最终形成以中国网络安全人员为主体，覆盖全球黑客圈的安全社区。

2、初期目标（1-2 年）

以兴趣为导向，组建具有极强技术“冲劲儿”的“核心”团队 vm_kernel，成员总数不超过 5 人。该阶段主要任务包括，当前 Linux 模拟器的技术比对，主流 Linux 与*nix 的技术比对（着重考虑社区生态及活跃度，后期系统及代码运维难度），开源软件许可的选择（采用 GPL 还是其它来源软件规范），技术（github 创建及管理）及资源储备（logo 设计，网站搭建，社交账号，团队共识）。

3、近期目标（2-3 年）

智能移动终端设备普及率日益提高，并且设备的配置和性能逐渐逼近高端 PC 设备，考虑到这一趋势以及 IoT 环境下的网络安全新特征，我们首先针对 Android 开发“閌蠱”系统的 demo。在 vm_kernel 团队基础之上，组建项目开发“基石”团队 vm_bedrock，完成“閌蠱”项目 Demo 的开发任务。

4、中期目标（3-4 年）

1)完成“閌蠱”的 Android 版本迭代，发行 1.0 版本。该部分开发任务将以 vm_bedrock 为基础，组建 vm_android 项目组，完成该部分开发任务。

2)完成“閌蠱”鸿蒙版本 demo 完成。创建 vm_harmony 开发小组，完成鸿蒙版本的开发计划，技术验证以及 demo。尚不清楚 HarmonyOS 是否从硬件层面完全禁止 root，因此该 demo 并不能保证运行所有软件（包括需要 root 权限运行的软件）。

3)完成“閌蠱”PC 版本 demo 开发。创建 vm_pc 项目小组，完成“閌蠱”项目在传统 PC，包括台式机，笔记本电脑以及平板电脑上的技术验证，UI 设计，开发计划以及 demo 开发。

5、中长期目标（4-6 年）

1)“閌蠱”Android 版本持续迭代，发布 2.0，3.0 等后续版本。

2)“閌蠱”PC 版本迭代并发布 1.0 稳定版。

3)“閌蠱”iOS 版本及 MacOS 版本 demo 完成。创建 vm_apple 小组，完成“閌蠱”项目在 Apple 软硬件环境下运行的技术验证，制定开发计划，并完成第一阶段 demo。

6、远景目标（6-8 年）

1)完成“閌蠱”iOS 及 MacOS 1.0 稳定版发布(大概率基于 Arm 架构)；

2)初步形成“閌蠱”系统的全平台覆盖；

3)具备快速编译并发布增量更新的能力；

4)形成成熟的 Bug 检查及处置机制；

5)以“閌蠱”项目 vm_kernel 技术团队为核心，通过团队的迭代，最终整合 vm_bedrock，vm_android，vm_pc，vm_harmony 以及 vm_apple 小组的核心成员形成一个共同管理和维护“閌蠱”全平台 Linux 模拟器的技术团队 vm_universe。该小组将共同决定 “閌蠱”项目未来的发展路线，技术走向，并不断为“閌蠱”项目输送新的创意。

0X03、参考

1. chroot. https://baike.baidu.com/item/chroot/3267609
2. 香菇. 如何在安卓手机上 `chroot` 一个全功能的 `linux` 发行版. https://blog.siitake.cn/chroot-linux.html