基于数据中心的安全加固

HardenedLinux

文百川
ID: Samson W
sccxboy@gmail.com

whois

* Samson W
* Day job at 广州腾御安科技
* 高级安全工程师
* 自由软件支持者
* HardenedLinux 社区成员
* EFF/FSF 会员

list

* 数据中心安全现状
* 安全相关的面及威胁
* 安全加固防御实践
* 对未知漏洞的防护
* 正确的安全理念

#现状

* 边界 --->> 不断变化
* 设备的多样化 --->> 复杂化
* 安全技术涉及广 --->> 防护经验不足
* 新技术的引入 --->> 更多攻击面
* 不同部门的安全需求存异 --->> 协同步署难
* 基线安全的认知不足 --->> 低级错误频出
* 国与国间的骇客军备不断升级 --->> 防御难、成本高
* 基础设施的非自主可控 --->> 核心控制的缺失

#安全相关的面

* 物理硬件安全
* 网络基础设施安全
* 虚拟化的安全
* 固件安全
* 操作系统的安全
* 中间件安全
* 应用安全
* 第三方安全设备的安全
* 数据安全
* 安全管理

HardenedLinux

#物理硬件安全

* 机房环境的安全 ----------> ** 温度 / 湿度的监测
  ** 过水的监测与防水
  ** 烟雾探测
  ** 电源失效的 UPS 系统
  ** 摄像头 / 移动监测
  ** 机柜门打开探测
* 设备的物理隔离 (上锁)
* 对不使用的硬件接口进行封口
* 访问硬盘密码
* 磁盘加密
* 磁盘的安全擦除
* BIOS 设置限制不使用的硬件口

HardenedLinux

网络基础设施安全

* 无线接入点的安全 ---------> ** 设备的固件安全 -----> *** 固件的安全漏洞
* 路由器/交换机的安全 ---> ** 配置安全 *** 固件的最新稳定版本检查

\--> *** 配置页面登录的用户名/密码是否为默认的
*** 配置页面登录的用户名/密码是否健壮
*** 无线接入的密码长度是否安全
*** 无线接入的密码是否健壮
*** 配置页面是否仅为在有线连接情况下方可访问
*** 连接超时

* 不同功能子网的隔离

HardenedLinux

虚拟化的安全 - 安全合规 (VMware 为例)

* NSX(網路虛擬化平台) 的安全配置
* Virtual SAN&Virtual Volumes 的安全配置
* vSphere 的安全配置
* ESXi 虚拟化管理程序安全
* vCenter Server 系统及关联服务安全
* 虚拟机安全
* 密码的安全
* 存储安全
* 时钟同步

固件安全

* secureboot trustchain
* 移除固件安全影响的部分（如：去除 ME）

#操作系统的安全

* 内核安全------→-→-→-→->
  ** 内核开启 SYN 特性 (2.6 后)
  ** NETFILTER 的 SYNPROXY 特性
  ** tcp_max_orphan 调整
  ** 内核的 tcp 调优
  ** PAX/Grsecurity
* 最小安装
* 安全通信软件的安装
* 自主开发的安全
* 软件更新------→-→-→-→->
  ** 官方软件源的完整性验证
  ** 必须使用官方源
* 安全漏洞处理
* 安全配置------→->
  ** ssh 的配置
  ** 防火墙的配置------→->
    *** 网络进出的白名单设置
    *** 远程服务的暴力破解配置
    *** DDOS 防护的配置

HardenedLinux

#操作系统的安全

加密------→-→-→-→-→-→-→-→-→-→-→-→-→-→-→-→-> 系统中生成 GPG 密码对时选择的哈希算法是否非 MD5 、 sha-1
系统中生成的密码组件是否非 RC4
称加密的密钥强度必须不少于 128 位
安全审计
SETUID 、 SETGID 应用的排查
杀毒程序 (clamAV)
强制访问控制
软件安装及软件更新必须进行密钥对的验证
日志的收集
NTP 服务器的设置
安全访问控制（ RBAC 、 VPN 接入、证书、双因素认证）
文件权限
最小权限 (capabilities)
终端连接超时
密码的定期更换
弱密码
web 安全
沙箱
dns 安全

HardenedLinux

中间件安全

* 中间件的安全基线的配置
* 中间件安装程序的完整性验证
* 中间件的安全漏洞跟踪及处理
* 中间件的安全加固
* 防火墙白名单的配置

#应用安全

* 系统应用的安全 ----------->
  ** 安全漏洞的检查及及时更新
  ** 应用配置是否存在漏洞的检查
  ** 应用的安全基线配置（数据库， web 服务器）
  ** 应用系统的安全加固
  ** 根据应用的业务流程进行 iptables 、强制访问控制规则的制定
  ** 安装程序包的认证

* 自研应用的安全 ----------->
  ** 代码的安全审计
  ** 代码的静态分析
  ** 编译时加固编译选项
  ** 应用中使用的加密算法是否为易受到攻击的漏洞算法
  ** 应用的配置是否存在漏洞的检查
  ** 应用的 Fuzzing 安全测试

HardenedLinux

第三方安全设备的安全

* 设备规则是否更新
* 本身是否有安全漏洞
* 配置是否安全
* 信息泄漏
* 对于误报的处理

数据安全

* 数据备份与恢复
  ** 完整性
  ** 可用性
  ** 保密性（使用加密组件进行加密）
* 数据的安全销毁

#安全管理

* 开发的安全管理 ------->
  ** 代码仓库中是否存在敏感信息
  ** 代码仓库访问控制
  ** 代码仓库的权限最小化

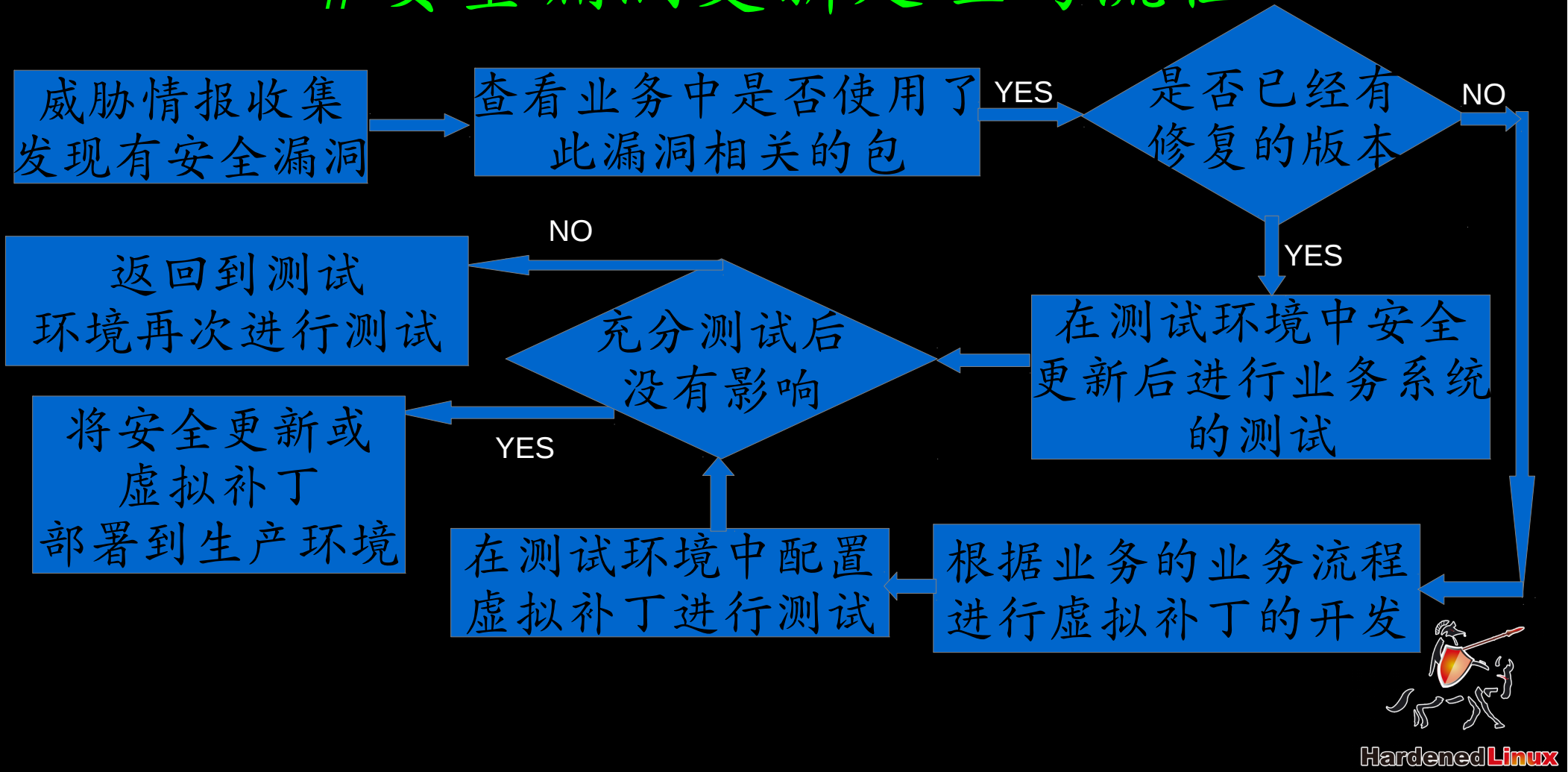
* 运维安全管理 ---------->
  ** 不同职责的帐号的分离
  ** 禁止分享账号的密码和使用权
  ** 双因素认证/动态口令牌
  ** 访问控制

* 安全补丁的更新流程

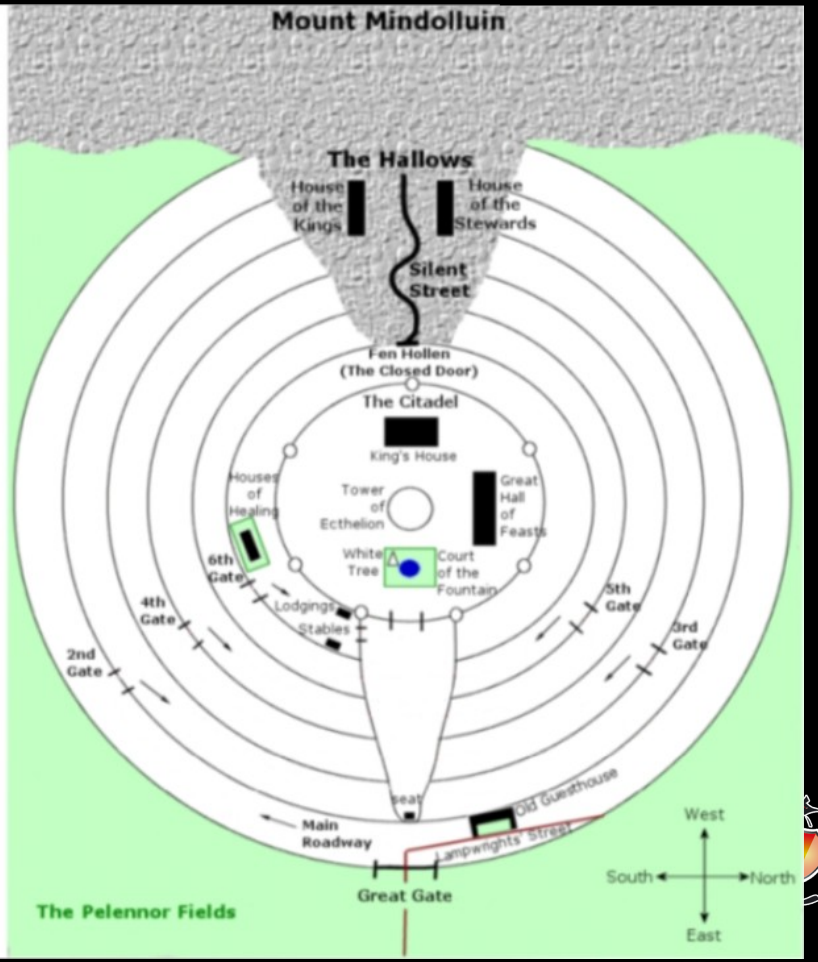
* 员工安全意识的培养 -->
  ** 邮件钓鱼
  ** 社工
  ** 对于不明应用使用沙箱隔离运行
  ** 好奇心

HardenedLinux

#安全漏洞更新处理的流程



#纵深防御是唯一的选择？



安全加固防御实践

* 基于 Debian 最佳实践
* PaX/Grsecurity 最佳实践
* 主机安全基线检测
* Coreboot 分析

基于 Debian 最佳实践（已完成）

* DNS
* HA
* Harbian QA
* Hardened boot
* IDS
* IPSEC
* Security Operation Center
* Storage
* SSH and Cluster
* TLS
* MAC/RBAC

PaX/Grsecurity 最佳实践

* 开始使用 Grsecurity
* PaX 基础
* 面向桌面的 PaX/Grsecurity 配置详细注释与评论
* 在桌面 GNU/Linux 上使用 PaX/Grsecurity 的一点经验
* Linux kernel mitigation checklist
* Linux kernel vulnerablity & exploitation & silent fixes
* PaX/Grsecurity 相关特性分析
* MAC-RBAC: Grsecurity RBAC system with nginx practice

主机安全基线检测

STIG-4-Debian

根据 STIG 的 RHEL 6/7 标准编写的支持 Debian 8/9 的主机安全基线检测项目。

Security Technical Implementation Guides (STIGs): 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，是 DOD IT 安全安装及维护的标准。针对多种操作系统及多种应用都有相应的标准。

STIG 的所有标准：
http://iase.disa.mil//index.aspx

HardenedLinux

对未知漏洞的防护

PaX/Grsecurity:

* 优势：
  ** 强大的社区支持，Debian/Gentoo
  ** 防御未知 (0Day) 漏洞利用的能力
  ** 能防御内核本身的漏洞

* 劣势：
  ** 没有商业 GNU/Linux 发行版原生支持
  ** 测试与业务兼容的成本较高

对未知漏洞的防护 - 代码安全

* 编码安全概述

指由代码质量问题引发的安全问题。

怎么造成的：

- 开发和安全的鸿沟
- 开发人员欠缺安全知识
- 上线压力 VS 代码质量
- 功能 VS 代码质量
- 没有严格的 QA 流程

C/C++ 代码的安全性提高

* 编译器加固选项
* 代码审计

HardenedLinux

#正确的安全理念 -- 基本原则

我们坚信 ：信息安全 .....

* 不是安装一堆防火墙
* 不是一个产品或者服务 (by Bruce Scheiner)
* 不是一个产品 ，而是一个持续不断的过程 (by Bruce Scheiner)
* 不是”安全感“
* 不是为了”安标”而”安标”
* 安全审计不是 " 扫描一堆端口 "
* 不是一劳永逸的

HardenedLinux

#正确的安全理念 -- 基本原则（续）

我们坚信：信息安全 .....

* 是考虑 "你能在不影响业务的情况下不被入侵吗 ？"
* 是最薄弱的防线将成为你的短板
* 是你所在企业的资源（机器和人）的风险管理，需要专业技能，时间管理，实施成本，数据备份/恢复的一系列流程
* 是关乎过程，方法论，成本，策略和人是考虑 "有人能社工进入公司并且访问计算机，磁盘和磁带 "
* 是 24*7*365..... 持续不断……并且永不停止
* 持续对抗的零和游戏

HardenedLinux

#安全工作的持续性

就是没完没了……

致谢

对 GNU/Linux 安全作出巨大贡献的、启发 HardenedLinux 社区打造基础架构防御链条的 PaX/Grsecurity 的缔造者 PaX team 和 spender 。

https://grsecurity.net

#引用

https://grsecurity.net/index.php

https://en.wikibooks.org/wiki/Grsecurity

https://github.com/hardenedlinux/

HardenedLinux

加固一小步，自由软件一大步。

https://hardenedlinux.github.io