Grsecurity/pax 以及 RBAC 使用简介

1. 维护时（RBAC+admin role）和运行时（RBAC）
   正常运行环境，启用强制访问控制规则，使用最小权限，root 是不被信任的受限用户，没有修改系统管理系统的特权，如果需要更改系统安装软件需要获取 admin 角色权限，维护时，尽量开启 grsecurity 保护，gradm2 –a admin 认证后，root 拥有管理权限，维护完毕立刻 gradm2 –u 放弃管理员角色，切换到正常运行状态，如果没法完成才考虑禁用 RBAC。
   切记，维护时尽可能保持 RBAC 开启，不要随意禁用 RBAC，将系统风险窗口降至最低。
2. 软件包与安装
   Paxctl，paxtest，pax-utils，linux-grsec-base，linux-headers-grsec-amd64，linux-image-grsec-amd64，gradm2_3.1
   系统 debian，deepin linux，gentoo，archlinux，~~ubuntu~~，~~centos7~~
   debian 8 安装
   apt 需要 backports 源
   # vi /etc/apt/sources.list
   deb http://ftp2.cn.debian.org/debian jessie-backports main

   apt-get install linux-base/jessie-backports
   ~~apt-get install linux-image-grsec-amd64 linux-headers-grsec-amd64 paxtest~~
   apt-get install linux-image-4.9.0-2-grsec-amd64 paxtest
   wget
   https://ftp2.cn.debian.org/debian/pool/main/g/gradm2/gradm2_3.1~201701031918-2_amd64.deb
   dpkg –i gradm2_3.1~201701031918-2_amd64.deb

   deepin linux 15.3 安装
   apt-get install linux-image-grsec-amd64 linux-headers-grsec-amd64 paxtest
   gentoo 参见 gentoo wiki
   archlinux 参见 arch wiki
3. PAX 特性
   可信路径执行（Trusted path execution）
   grsec-tpe 组成员信任路径执行（白名单/黑名单）
   chroot 加固
   Socket restrictions （socket 限制）
   受限组
   grsec-sock-all 禁止组成员使用 socket，包括发起连接和监听
   grsec-sock-clt 禁止组成员作为客户端发起连接
   grsec-sock-srv 禁止组成员作为服务端监听
   审计 Auditing
   隐藏/proc 信息
   grsec-proc /proc 访问进程文件系统的组
   PAX 标志管理

可执行文件标志位设定，大写启用，小写禁用

PAGEEXEC P

EMUTRAMP E

MPROTECT M

RANDMMAP R

RANDEXEC X

SEGMEXEC S

三种方式保存 pax 标志 EI_PAX，PT_PAX 和 XATTR_PAX

Paxctl 修改 elf 文件或者 setfattr/getfattr 修改/查看扩展属性

setfattr -n user.pax.flags -v "m" /usr/bin/python2.7

Pspax 查看进程的标志

建议使用 setfattr 设置扩展属性，这样不会修改 elf 文件，不会改变文件校验和，避免干扰 HIDS 和完整性校验之类软件，（将来会淘汰 EI_PAX，PT_PAX）

4. 基于角色的访问控制 RBAC

Gradm2 –P #设置 RBAC 密码

Gradm2 -P admin #设置 admin 角色密码

Gradm2 –P shutdown #设置 shutdown 角色密码

使用学习模式建立规则

先生成学习日志

Gradm2 -F -L /etc/grsec2/learning.log

学习模式使用至少 24 小时，各种任务执行至少重复 4 遍

使用方法 重启所有的服务 或者 将启动命令放入/etc/rc.local，重启机器

Ssh 登陆，切换用户 root，获取 admin 角色，然后退出角色，退出 roo，退出登陆用户

admin 角色，手动运行所有的 cron 任务

学习模式完成，退出 RBAC，生成策略，要人工审核修改，然后启用 RBAC 检查错误日志，然后修改规则，重复以上过程，直至完全没有错误

学习模式处于安全风险状态，应当在最短的时间内完成学习，如果学习模式被入侵，这时制作的规则是无效的

学习完毕后禁用 RBAC

Gradm2 -D 禁用 RBAC

根据学习日志生成 RBAC 访问规则

Gradm2 -F -L /etc/grsec2/learning.log -O /etc/grsec2/policy

警告：学习模式，不要使用 root 执行任何无关命令，更不允许使用 root 进行系统维护任务，目的是确保应用生成的规则后 root 是完全没有特权的受限用户

RBAC 规则需要保密，确保不被其他用户访问，避免规则缺陷泄密。

规则制作完毕后检查是否错误

Gradm2 －CV

无误后启用 RBAC

Gradm2 －E

检查确认 RBAC 运行状态

Gradm2 －S

策略/规则详解

内置变量 define grsec_dennied

角色模式 u 系统中的用户，g 系统中的组，s 特权角色，不属于任何组和用户，也不需要实施安全策略 l 小写 L，启用学习 A 管理员角色，普通角色不具备的特权，通常用于忽略额外的 ptrace 和库限制， G 这个角色可以使用 gradm 授权至内核，自动为此角色添加策略 N 这个色不需要认证 gradm －n 角色名 访问这个角色 P 这个角色使用 PAM 认证 T 这个角色启用 TPE（信任路径执行）R 永久的 仅用于关机

角色属性 role_transitions，role_allow_ip，role_umask

主体模式 a 允许进程访问/dev/grsec

b 这个主体的进程启用进程记账

d 保护 */proc/<pid>/fd*, */proc/<pid>/mem*, */proc/<pid>/cmdline*, and */proc/<pid>/environ*

h 进程隐藏 仅可被 v 模式进程查看

i 启用继承学习

k 这个进程可以杀死保护进程

l 为这个进程开启学习模式

o 覆盖 ACL 继承

p 保护进程 仅仅可以被 k 和相同主体的进程杀死

r 放松 ptrace 限制

s Enable AT_SECURE when entering this subject. This enables the same environment sanitization that occurs in glibc upon execution of a suid binary.

t 允许追踪任何进程

v 可以查看隐藏进程

x 允许执行匿名共享内存

A 保护共享内存

C 自动杀死属于攻击者 ip 的进程

K 进程属于这个主体时 报警并杀死进程

O 允许加载可写库

T 拒绝执行可被其他主体写入的二进制或者脚本

主体属性 user/group transitions ip_override sock_allow_family

客体模式　权限模式
none 留空 隐含 find 访问 可以被 list 属主、大小等信息 但不允许读和修改
a 打开为追加
c 允许文件和目录创建
d 允许文件和目录删除
f 管道
h 这个客体是隐藏的
i 仅用于二进制 执行时继承 acl
l 允许硬链接
m 创建 setuid/setgid 文件和目录
p 禁止 ptrace
r 打开为读
t 可被追踪 但不可以修改运行任务，只读 ptrace
w 写或者追加
x 执行或者 PROT_EXEC 映射 mmap
审计标志
A 追加
C 创建
D 删除
F 发现
I 继承
M setuid/setgid 创建修改
R 读
W 写
X 执行
其他标志
s 不记录日志

内置角色 admin 建议将此内置角色改为其他名字
Shutdown 关机角色用于系统关机和重启
Default 默认权限阻止所有访问
常用角色 man
Root cron 定时任务相关
Root 后台服务相关共有 systemd，init.d,postfix，syslog，sudo，sshd，其他以 root 启动的服务 mysql，php-fpm,nginx 等
禁止 root 作为管理员用户日常工作使用，安装卸载软件配置排查故障
www-data web 服务器角色
hmuser 普通用户可以 sudo 至 root
sshd 远程登录
postfix 邮件
zabbix 监控
Policy 样例
/etc/grsec2/users/<user><subjects>

- you need to run the script grsecurity/setfattr or programs using JIT, especially java, python and javascript using - implying also firefox (iceweasel), thunderbird etc will be blocked by PAX
- binary drivers, including video drivers like proprietary NVidia or Radeon in general will probably not work on higher levels, but they are security risk
- almost all video drivers even the open-ones would be blocked by good security, which is meant mostly for headless (or text) servers. In future a patched Xorg program would allow them to run probably (it's about blocking kmem and ioport access - which blocks important route of attacking kernel by modifying raw memory)
- possibly wine would be blocked by the no-0-address thing? (possibly tunable in runtime?)
- When mounting a remote file system using sshfs: *fuse: device not found, try 'modprobe fuse' first*. You need to manually load fuse module as a root: *# modprobe fuse*
- Same as above for other auto-loaded modules, you might need to load them by hand. (Other solutions perhaps exist too)

Things that work:

- open source video drivers (at least on some levels)
- other open source and built-in drivers - HOW EVER you might need to modprobe load the modules manually for some things
- KVM visualization is known to work (as the host)
- KVM visualization as the guest also works (using this kernels on a system in KVM VM)
- all other normal operation for Desktop and Server
- members of Mempo team along with friends used grsecurity on their primary Desktops for year+ without trouble

深度桌面相关设置

用户加入 grsec-tpe 组

/etc/sysctl.d/grsec.conf

#xorg 需要

kernel.grsecurity.disable_priv_io = 0

~~kernel.grsecurity.linking_restrictions = 0~~

#wine 需要 ptrace

kernel.grsecurity.harden_ptrace = 0

kernel.grsecurity.ptrace_readexec = 0

无 pax 标志默认允许

~~kernel.pax.softmode=1~~

关闭 tpe

kernel.grsecurity.tpe = 0

kernel.grsecurity.tpe_restrict_all=0

常用策略 cron postfix bash dash systemd init.d systemd-journald systemd-logind apt-get

Logger mysqld_safe sudo php5/sessionclean nacctd nginx rsyslogd sshd zabbix

参考：
https://www.grsecurity.net/
https://forums.grsecurity.net
https://en.wikipedia.org/wiki/Grsecurity
https://en.wikibooks.org/wiki/Grsecurity/The_RBAC_System#Policy_Structure
https://en.wikibooks.org/wiki/Grsecurity/Application-specific_Settings
https://wiki.archlinux.org/index.php/Grsecurity#Socket_restrictions
https://wiki.gentoo.org/wiki/Hardened/Grsecurity2_Quickstart
https://wiki.debian.org/grsecurity
https://micahflee.com/2016/01/debian-grsecurity/
https://github.com/mempo/mempo-kernel
http://www.astra-linux.com 俄罗斯军队的 GNU/Linux 发行版

附：
常用程序运行所需 PAX 标志位设置脚本
常用 RBAC 策略/规则

可疑行为
1.systemd-timesyncd 随机监听 udp 端口
2.mysqld_safe 写权限打开 /