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。

1. 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

1. 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）

1. 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 /