Linux主机加固丨如何优雅的控制系统权限？

xmirror / 2017-09-15 09:06:00 / 浏览数 3181 安全技术 技术讨论 顶(0) 踩(0)

Author：悬镜实验室

综述

在日常业务运维中，经常会受到权限的困扰，给多了就违背了最小权限原则，造成系统出现一些安全隐患，给少了业务又无法正常进行，下面我们来看看如何优雅的控制系统

0x01修改应用版本信息

修改应用版本信息虽然和权限无关，但对应用可以起到一定的保护作用，本节我们以tengine为例，来介绍如何修改应用的版本信息。其他apache等方法类似。

1、修改配置文件隐藏版本信息

配置文件nginx.conf中http段添加server_tokens off，但此方法只能隐藏版本号，服务信息还是可以看到的。

配置如下图所示。

2、要想修改的彻底，可以通过修改源码进行隐藏，解压缩tar包，修改$BASE_DIR/src/core/nginx.h文件。

修改前：

修改后：

编译过程这里不做介绍，编译后运行效果如下图所示，可以看到http头中服务和版本信息都已经修改。

0x02构建受限的shell环境

有时候我们想限制用户登录后的行为，让用户在一个受限的shell环境操作，这里我们介绍如何利用lshell来快速实现，lshell提供了一个针对每个用户可配置的限制性shell，

安装过程不做介绍，yum安装后配置文件路径为/etc/lshell.conf。
主要的配置项有logpath：配置日志路径、allowed：允许执行的命令、forbidden：禁止使用的字符或者命令、path：只允许访问的路径、env_vars：环境变量。

配置好后，修改你想要限制的用户shell，chsh -s /usr/bin/lshell $USER_NAME，或者vipw直接修改。日志目录需要手工创建并赋权。

配置如上图所示，只允许使用的命令为：ls、echo、cd、ll，只允许访问的路径为/home/tomcat/、/usr、/etc、/tmp、/opt。
在受限shell下进行操作，可以看到不允许的操作被禁止。

日志记录

应用场景可以有很多，大家根据自己的实际业务环境灵活应用。

注意：前外不要把bash、sh等命令允许，一旦允许这些命令，该用户就可以逃逸出lshell的受限环境了。

0x03 linux ACL

linux默认的3种基本权限(rwx)以及3种特殊权限
(suid,sgid,sticky)在平常情况下做适当调整即可，但是如果出现多个组多个用户情况下对某些文件或目录做权限配置就会发现不够分配，所以为了解决此类情况linux内核出现

使用acl前要安装acl和libacl，查看系统是否支持acl，Linux默认是支持的。

dumpe2fs -h /dev/sda1|grep acl（根据自己磁盘情况更改）

开启分区的acl权限：

临时开启：mount –o remount,acl 磁盘分区，永久开启的话需要修改/etc/fstab

场景：某文件只允许属主和其他用户A访问（只读），其余用户都不允许访问。

假设A用户名为tomcat，改文件只允许属主root和其他用户tomcat访问（只读） 设置acl前，tomcat用户读取操作被拒绝。

设置acl后，tomcat用户可以读取，user1用户被拒绝。

0x04 严格限制网络出入站规则

在攻击场景中，攻击者通常在获取到一定权限后，会反弹shell进行交互式操作，严格限制出入站规则，可以对此攻击行为进行有效阻断。

通常情况下，我们对入站访问策略会进行严格的限制，但出站策略经常被忽略，这就使得攻击者反弹shell成为可能，这里我们介绍使用iptables进行有效限制。

iptables功能非常强大，大家可以仔细研究一下，有很多好玩的东西。

上一篇：Empire中的Invoke-WS... 下一篇：Shellcode另类使用方式
1. 0 条回复
   - 动动手指，沙发就是你的了！