小议Linux安全防护(一)

时间 2016-01-08 16:11:17 WooYun知识库

原文 http://drops.wooyun.org/运维安全/11801
主题 Linux

0x00 前言

在linux服务器随处可见的网络环境中，网络运维人员保障Linux安全就成了必要条件。当然现在有很多的硬件防火墙以及WAF，但是那不是小资企业可以hold住的，本文从软件以及服务配置方面简单总结Linux安全防护。

0x01 使用软件级别安全防护

1、使用SELinux

SELinux是用来对Linux进行安全加固的，它可以让你指定谁可以增加文件，谁只可以删除文件，或者谁还可以移动文件，从文件的层次上来说，它相当于一个ACL；

配置文件：/etc/selinux/config (centos7系统)

状态：getenforce 与 setenforce命令可以修改

- disabled：关闭策略
- permissive：启用SELinux但是即使违反了策略它也会让你继续操作；仅仅一个记录功能
- enforcing：启用SELinux，违反策略时阻止你的操作

查看文件标签： `ls -Z`

```
[root@bogon ~]# ls -Z
-rw-------. root root system_u:object_r:admin_home_t:s0 anaconda-ks.cfg
[root@bogon ~]#
```

在文件所属组的后面就是我们文件的标签，它表示SELinux对这个文件的策略

修改策略：chcon与semanage

```
[root@bogon tmp]# touch test.txt
[root@bogon tmp]# ls -Z
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 test.txt
[root@bogon tmp]# chcon -t etc_t test.txt
[root@bogon tmp]# ls -Z
-rw-r--r--. root root unconfined_u:object_r:etc_t:s0   test.txt
```

恢复文件标签：restorecon

常见场景分析：

当我们需要配置一个Web目录时，如果Web目录不是默认的目录，访问可能出现403

这个时候，我们需要将我们的Web目录的标签修改为 `httpd_sys_content_t`

```
[root@bogon ~]# ls -dZ /var/www/html/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /var/www/html/
[root@bogon ~]# mkdir /web
[root@bogon ~]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@bogon ~]# ls -dZ /web/
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /web/
[root@bogon ~]# restorecon -vvRF /web/
restorecon reset /web context unconfined_u:object_r:default_t:s0->system_u:object_r:httpd_sys_content_t:s0
[root@bogon ~]# ls -dZ /web/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /web/
[root@bogon ~]#
```

2、使用**iptables**

Iptables是一个应用框架，它允许用户为自己系统建立一个强大的防火墙。它是用来设置、维护和检查Linux内核中IP包过滤规则的。

配置文件：/etc/sysconfig/iptables-config (centos7系统)

这里贴出一个在博客园的关于iptables的使用：

http://www.cnblogs.com/JemBai/archive/2009/03/19/1416364.html

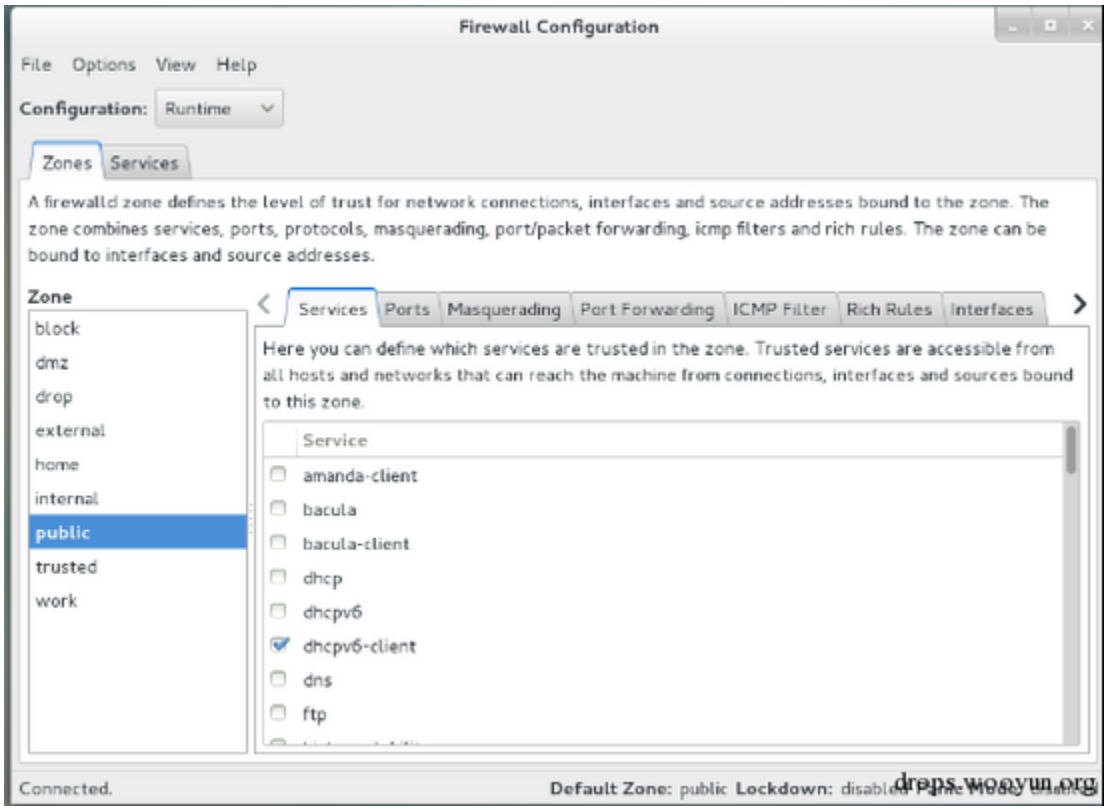
3、使用firewall

在centos7中，防火墙具备很强的软件防护功能，在默认程度上：

```
[root@localhost ~]# firewall-cmd --list-all
public (default, active)
  interfaces: eno16777736
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

默认开启了dhcpv6客户端以及ssh防火墙功能；

防火墙具备很多功能，同时他具备图形界面与命令行界面两种模式，对于基本的防火墙配置，个人推荐使用命令行模式，当我们需要配置一些负责的规则策略时，就可以使用我们的图形界面：



4、使用入侵检测系统

IDS：入侵检测系统，在linux中有针对它的开源的入侵检测系统：Snort；

0x02 安全配置服务

1、SSH访问控制

尽可能的取消telnet登录，采用ssh进行登录；

ssh配置文件：/etc/ssh/sshd_config

- 修改默认端口：Port 10512
- 不允许使用空密码：PermitEmptyPasswords no
- 不允许root用户登录：PermitRootLogin no
- 不允许输入密码登录：PasswordAuthentication no (可以很好的防止爆破，但是如果密钥文件泄漏则会出现安全问题，当然可以通过其他方式来进行防御)
- 重新生成密钥：KeyRegenerationInterval 1h (如果我们使用密钥进行登陆，可以设置多少时间后密钥重新生成)
- 密钥加密方式：RSAAuthentication yes (是否使用RSA进行加密)

2、禁用不必要的服务及用户

在我们的Linux系统中有很多用户不需要的服务和应用，然而这些服务还是会运行，这样会导致攻击者利用这些服务的漏洞来进行攻击，最好的办法就是停止这些服务。

比如我们的Linux服务器只是一台Web服务器，那么就不需要ftp、smtp等服务我们就可以关闭；当然我们也可以让服务不允许通过防火墙，这样通过防火墙来保护我们的服务器也可以。

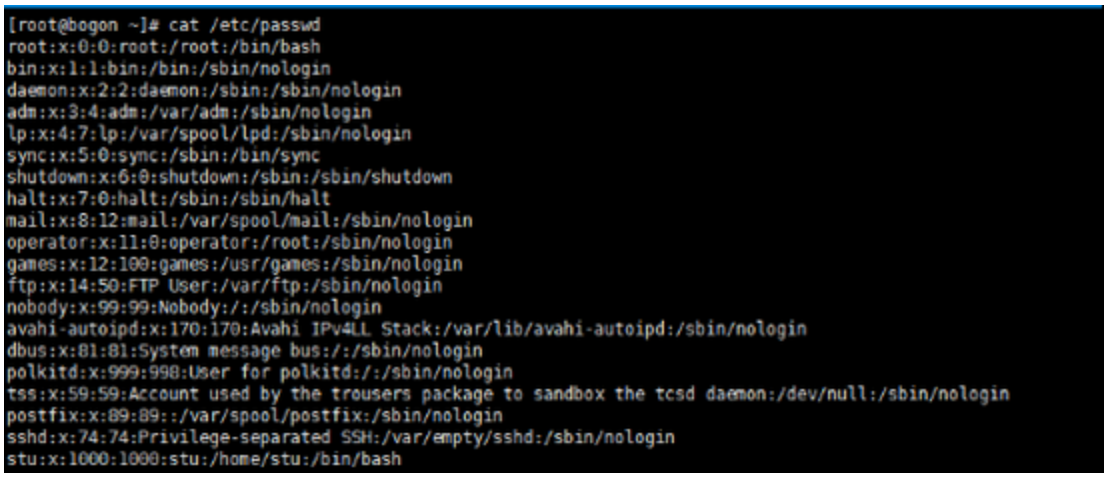
任务	旧指令	新指令
使某服务自动启动	chkconfig --level 3 httpd on	systemctl enable httpd.service
使某服务不自动启动	chkconfig --level 3 httpd off	systemctl disable httpd.service
检查服务状态	service httpd status	systemctl status httpd.service（服务详细信息） systemctl is-active httpd.service（仅显示是否 Active)
显示所有已启动的服务	chkconfig --list	systemctl list-units --type=service
启动某服务	service httpd start	systemctl start httpd.service

任务	旧指令	新指令
停止某服务	service httpd stop	systemctl stop httpd.service
重启某服务	service httpd restart	systemctl restart httpd.service

在linux系统中，系统运行所必须的服务

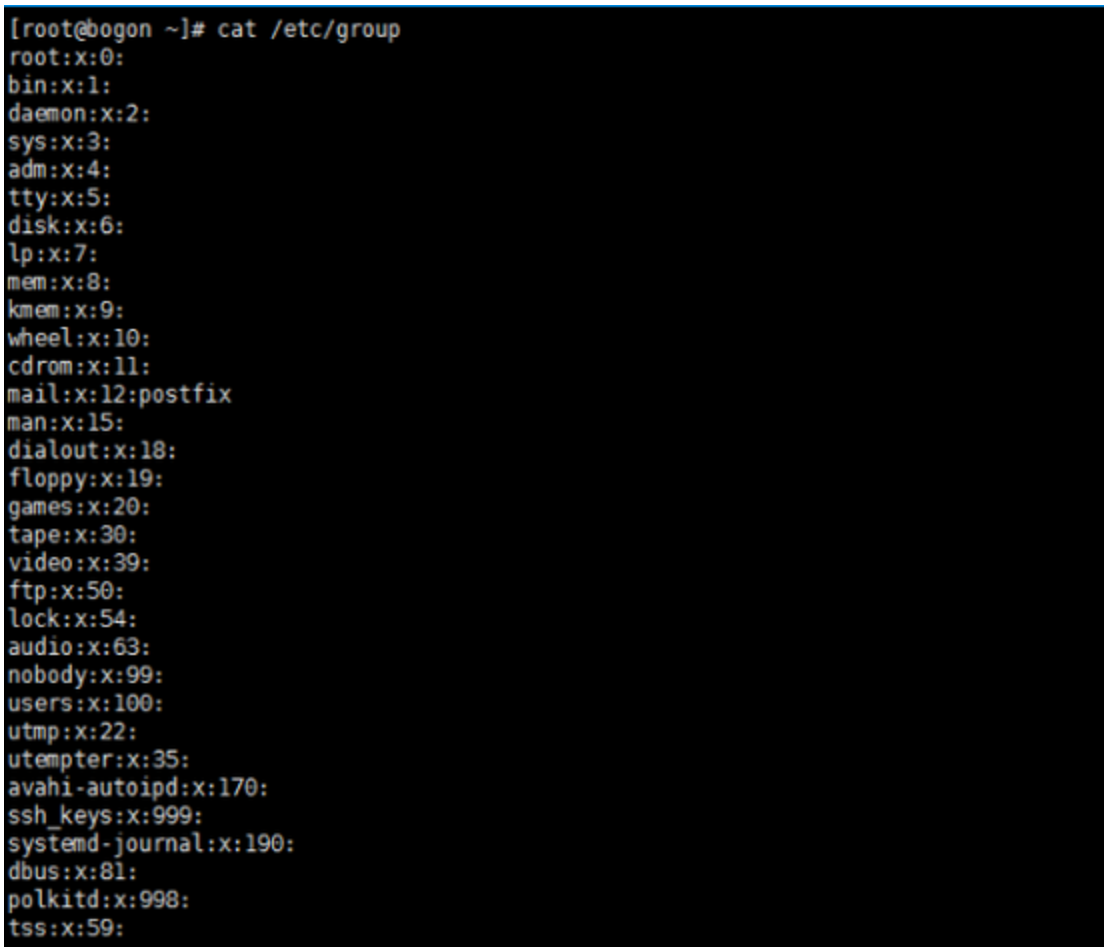
服务名称	说明
acpid	用于电源管理，对于笔记本和台式电脑很重要
apmd	高级电源能源管理服务，可用于监控电脑
kudzu	检测硬件是否变化的服务
crond	为Linux下自动安排的进程提供运行服务
iptables/firewall	Linux内置的防火墙
xinetd	支持多种网络服务的核心守护进程
syslog	记录系统的日志服务
network	网络服务，要用网必须启动这个服务

同时，一台新的Linux操作系统中有很多我们用不到的角色用户，我们同样可以删除这些用户，或者将这些用户设置为不能登录系统；



可被删除的用户：adm、lp、sync、shutdown、halt、operator、games

- userdel adm
- groupdel adm



可被删除的用户组：adm、lp、games、dip等；

当然具体的需要还是要根据用户的选择，同时我们也可以修改用户的bash文件禁止用户登录系统也是防护方式的一种。

```
#!bash
usermod -s /sbin/nologin username
```

3、使用全盘加密

加密的数据更难被窃取，在安装Linux系统的时候我们可以对整个系统进行加密，采用这种方式，即使有人进入了我们的系统，也不能得到我们的数据；

4、Web应用配置

提供Web服务时，需要更新我们组件的补丁，防止利用已知漏洞来进行攻击；

严格限制权限，防止得到Web Shell以后直接得到系统权限；

限制Web用户只能访问Web目录，不能访问其他目录；

严格控制提供上传点的文件类型

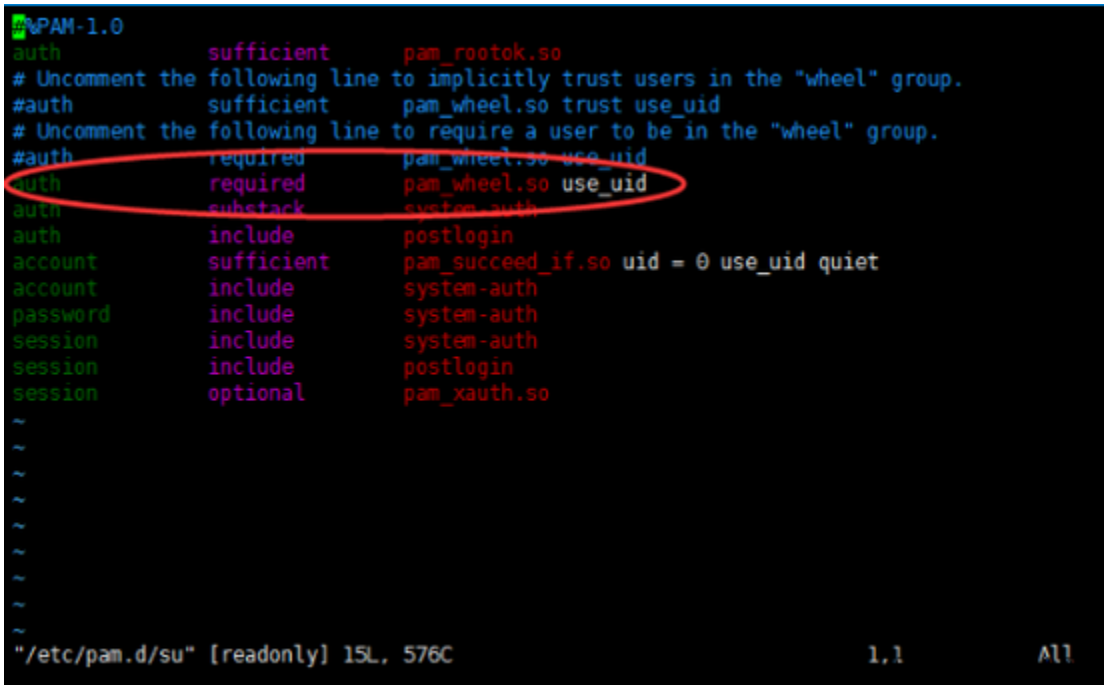
等等

5、系统安全

使用su 与 sudo命令时：

- su：切换用户
- sudo：提升权限，所以sudo是su的特定一种形态

这里是指定可以使用su命令的用户



注意红色圈起来的一行，就是启用 `pam_shell` 认证，这个时候没有加入wheel的用户就不能使用su命令了！

```
[root@bogon ~]# gpasswd -a stu wheel
Adding user stu to group wheel
[root@bogon ~]# su - stu
Last login: Tue Jan  5 05:46:26 EST 2016 on pts/0
[stu@bogon ~]$ su - stu1
Password:
Last login: Tue Jan  5 05:45:44 EST 2016 on pts/0
Last failed login: Tue Jan  5 05:46:33 EST 2016 on pts/0
There was 1 failed login attempt since the last successful login.
[stu1@bogon ~]$ exit
logout
[stu@bogon ~]$ exit
logout
[root@bogon ~]# su - stu1
Last login: Tue Jan  5 05:47:43 EST 2016 on pts/0
[stu1@bogon ~]$ su - stu
Password:
su: Permission denied
[stu1@bogon ~]$
```

对于sudo的一些配置 `vim /etc/sudoers` 在centos7中，如果你不想修改原来的配置文件，你可以将这一行 `includedir /etc/sudoers.d` 的注释去掉，然后在 `/etc/sudoers.d/` 目录下写我们的配置文件

```
# 允许stu用户执行ifconfig命令
stu     localhost=/sbin/ifconfig


# 给多个用户设置命令
User_Alias      USERS=stu1,stu2
Cmnd_Alias      PKFTOOLS=/bin/yum
USERS           localhost=PKFTOOLS

# 启用sudo日志功能
Defaults logfile="/var/log/sudo"

# 不需要使用密码执行命令
stu     localhost=NOPASSWD:/sbin/ifconfig
```

删除提示信息

在linux的4个文件中存在提示系统的一些信息：

- /etc/issue,/etc/issue.net:这两个文件记录了操作系统的名称及版本号，用户通过本地终端就会显示/etc/issue文件中内容，通过ssh或telnet登录就会显示/etc/issue.net的文件内容；
- /etc/redhat-release:这个文件也记录了操作系统名称和版本号；
- /etc/motd:这个文件是系统的公告信息，每次用户登录后就会显示在终端上；

未完待续~~~

分享

收藏 纠错

推荐文章

- 1. 轻松创建R包
- 2. Linux下最快速共享目录的方法
- 3. 分享一篇文章《Dtrace isn't just a tool; it's a philosophy》
- 4. Ubuntu apt-get 自动选择最快镜像
- 5. Linux光速入门之Linux光速入门
- 6. 博客园 Mac客户端 2.0-Beta

我来评几句

请输入评论内容...

登录后评论

已发表评论数()

相关站点

WooYun知识库

+ 订阅

热门文章

- 1. 轻松创建R包
- 2. Linux下最快速共享目录的方法
- 3. 如何利用 Docker 环境加速 Android 应用的构建
- 4. 分享一篇文章《Dtrace isn’t just a tool; it’s a philosophy》
- 5. Ubuntu apt-get 自动选择最快镜像
- 6. Linux光速入门之Linux光速入门

分享本文

收藏到推刊 创建推刊

收 藏 取消

已收藏到推刊！

推刊名(必填) 请填写推刊名

推刊描述

描述不能大于100个字符!

权限设置： 公开 仅自己可见

创建 取消

×

文章纠错

邮箱地址

错误类型 正文不准确

补充信息

提交

网站相关

关于我们
移动应用
建议反馈

关注我们


推酷网


tuicool2012

友情链接

人人都是产品经理 魔部网 PM256 品途网 移动信息化 行晓网 Code4App 智城外包网 LAMP人 安卓航班网 虎嗅 缘创派 IT耳朵 艾瑞网 创媒工场 雷锋网 经理人分享 市场部网 砍柴网 CocoaChina 北风网 云智慧 我赢职场 大数据时代 奇笛网 咕噜网 红联linux Win10之家 鸟哥笔记 爱游戏 投资潮 31会议网 极光推送 Teambition Cocos引擎中文官网 硅谷网 leangoo 更多链接>>