链滴

DenyHosts —— 让你的服务器少受点攻击

作者：Complexity-Naughty
原文链接：https://ld246.com/article/1533634842743
来源网站：链滴

[TOC]

DenyHosts简介

DenyHosts是Python语言写的一个程序软件，运行于Linux上预防SSH暴力破解的，它会分析sshd的志文件（/var/log/secure），当发现重复的攻击时就会记录IP到/etc/hosts.deny文件，从而达到自屏IP的功能。

本文整理自HeJD博客的相关博文 和 lclc博客的相关博文。在此感谢两位博主。侵删。

使用

安装

我的Linux版本：**CentOS 7**，编写这篇博客时，DenyHosts的版本为：**denyhosts-2.9-4.el7.noarch**
如何查看DenyHosts的版本？使用命令$ rpm -qa | grep denyhosts即可查看。

使用以下命令即可**安装DenyHosts**：

```
yum install -y denyhosts
```

配置和使用

- 打开配置文件

```
vim /etc/denyhosts.conf
```

- 然后配置DenyHosts（有默认配置，可以按需修改）

```
SECURE_LOG = /var/log/secure  #ssh日志文件

HOSTS_DENY = /etc/hosts.deny  #将阻止IP写入到hosts.deny

PURGE_DENY = 4w  #过多久后清除已经禁止的IP，其中w代表周，d代表天，h代表小时，s代表，m代表分钟

BLOCK_SERVICE  = sshd  #阻止服务名

DENY_THRESHOLD_INVALID = 5  #无效用户名限制登陆次数。 // --> 主要

DENY_THRESHOLD_VALID = 10  #有效用户名限制登陆次数。 // --> 主要

DENY_THRESHOLD_ROOT = 5  #root限制登陆次数。  // --> 主要

DENY_THRESHOLD_RESTRICTED = 1  #受限用户限制登录次数。  // --> 主要

WORK_DIR = /var/lib/denyhosts  #将deny的host或ip纪录到Work_dir中（限制过的ip和host存案底，列入受限名单）

HOSTNAME_LOOKUP=YES  #是否做域名反解
```

```
LOCK_FILE = /var/lock/subsys/denyhosts  #将DenyHOts启动的pid纪录到LOCK_FILE中，已确服务正确启动，防止同时启动多个服务。

ADMIN_EMAIL = denyhosts@163.com  #设置管理员邮件地址
SMTP_HOST = localhost
SMTP_PORT = 25
SMTP_FROM = DenyHosts
SMTP_SUBJECT = DenyHosts Report

AGE_RESET_ROOT = 1d  #root用户登录失败计数归零的时间（1d：1天）

AGE_RESET_RESTRICTED=25d  #受限用户的失败登录计数归零的时间

AGE_RESET_VALID=1d   #有效用户登录失败计数归零的时间

AGE_RESET_INVALID=10d  #无效用户登录失败计数归零的时间

DAEMON_LOG = /var/log/denyhosts  #自己的日志文件
```

- 查看和配置IP黑名单、白名单

```
vim /etc/hosts.deny    //黑名单（拦截记录）
vim /etc/hosts.allow    //白名单
```

- 黑白名单配置规则

```
sshd:*.*.*.*     //如sshd:192.168.21.34
```

- 相关命令
  - 启动命令

```
service denyhosts start   //启动服务
service denyhosts stop    //停止服务
service denyhosts status   //查看服务状态
```

  - 加入自启动

```
chkconfig denyhosts on
```

其他

想要解禁一个已经被禁止掉的IP，并加入到允许主机列表，只在 /etc/hosts.deny 删除是没用的。需进入 /var/lib/denyhosts 目录，进入以下操作：

- 1、停止DenyHosts服务： `$ sudo service denyhosts stop`
- 2、在 /etc/hosts.deny 中删除你想取消禁止的主机IP
- 3、编辑 DenyHosts 工作目录（配置文件中WORK_DIR）的所有文件，一个个删除文件中你想取的主机IP所在的行

/var/lib/denyhosts/hosts

/var/lib/denyhosts/hosts-restricted

/var/lib/denyhosts/hosts-root

/var/lib/denyhosts/hosts-valid

/var/lib/denyhosts/users-hosts

- 不知道有哪些文件包含了这个IP地址，可以使用以下命令：

$ sudo grep *.*.*.*(IP地址) /var/lib/denyhosts/*

搜索结果可能有

/var/lib/denyhosts/hosts

/var/lib/denyhosts/hosts-restricted

/var/lib/denyhosts/hosts-root

/var/lib/denyhosts/hosts-valid

/var/lib/denyhosts/users-hosts

- 4、添加你想允许的主机IP地址到

/var/lib/denyhosts/allowed-hosts

- 在文件中的位置大概在这段代码下方：

```
# We mustn’ t block localhost
127.0.0.1
*.*.*.*  //你想添加允许的IP地址
```

- 5、启动DenyHosts服务： service denyhosts start
- 6、如果不想自己解禁，可以等到一个重置周期后，自动解禁

总结

再好的防止攻击的手段，也总会有更加厉害的hacker攻破。所以说，绝对的安全是不可能存在的，我可以做的就是定期更换安全性高的密码，注意个人隐私的保护，及时发现并修复漏洞，这就已经是很责的自我保护了。

over