在 linux 上用 arptables 配置 arp 防火墙

局域网里有一台电脑不知道是中了 ARP 病毒还是用 P2P 终结者一类的软件每 5 秒钟就会对我的主机进行一次 ARP 攻击。。弄得我上网奇卡无比。在 WINDOWS 下用个金山 ARP 防火墙就搞定了。但是在 linux 下还是有点麻烦。研究了一个晚上终于弄好了。原作者写的已经非常详细了。我加了点注释。为了方便和我一样的小白。。。红色字体为要在终端上运行的命令。蓝色字体为终端上的显示结果。绿色字体为我加的注释。高手飘过。最后特别感谢原作者!!!

原文出自 http://ask.phpfans.net/?do=show&id=164893

1.安装 arptablesarptables 的下载页面是:http://sourceforge.net/projects/ebtables/files/0.0.3.3 版本的下载链接:http://downloads.sourceforge.net/project/ebtables/arptables/arptables-v0.0.3/arptables-v0.0.3-3.tar.gz

下载以后安装:tarzxvfarptables-v0.0.3-3.tar.gzcdarptables-v0.0.3-3/makemakeinstall

生成的命令是/usr/local/sbin/arptables、/usr/local/sbin/arptables-save、/usr/local/sbin/arptables-restore,系统启动脚本/etc/rc.d/init.d/arptables,这个脚本读的配置文件必须放在/etc/sysconfig/arptables 里。(这一段知道就行了不用操作)

打开 arptables 服务:chkconfigarptableson

2.配置 arptableslinux 服务器的网关 MAC 是 00:24:51:E9:C7:10,同网段另一台服务器 192.168.1.10(主机名是 nh-blade-67)的 MAC 地址是 00:17:A4:A8:68:11。

用命令行配置 arp 防火墙:在 eth0 上如果源 IP 是 192.168.1.10,并且源 MAC 不是 00:17:A4:A8:68:11 的话,就禁止这个数据桢。

/usr/local/sbin/arptables-AINPUT-ieth0--src-ip192.168.1.10--src-mac!00:17:A4:A8:68:11-jDROP(这里把 192.168.1.10 和 00:17:A4:A8:68:11 换成你同网段另一台服务器的 ip 和 mac.注意!的前后都有空格)

在 eth0 上如果源 MAC 不是 00:24:51:E9:C7:10(网关的 MAC 地址),就禁止这个数据桢,这一条针对外网过来的访问。

/usr/local/sbin/arptables-AINPUT-ieth0--src-mac!00:24:51:E9:C7:10-jDROP(这里把 00:24:51:E9:C7:10 换成你网关的 mac 地址)

注意:添加 arp 防火墙策略的次序不能错,针对网关 MAC 地址的语句必须放在最后,否则本网段 IP 的访问策略不能生效。

把以上策略写入配置文件:/usr/local/sbin/arptables-save>/etc/sysconfig/arptables

/etc/sysconfig/arptables 文件的内容:(查看方法 vi/etc/sysconfig/arptables)

```
    *filter:INPUTACCEPT:OUTPUTACCEPT:FORWARDACCEPT-AINPUT-
jDROP-ieth0-oany-snh-blade-67!--src-mac00:17:a4:a8:68:11-
AINPUT-jDROP-ieth0-oany!--src-mac00:24:51:e9:c7:10
```

用命令/etc/init.d/arptablesrestart 重启 arptables 的时候提示出错:

```
    StoppingArpfiltering(arptables):[OK]StartingArpfilteri
ng(arptables):arptablesv0.0.3-3:Can'tuse-owithINPUT

    Try`arptables-h'or'arptables--help'formoreinformation.
ERROR(line5):[FAILED]
```

修改/etc/sysconfig/arptables 文件以后的内容:(vi/etc/sysconfig/arptables 把-oany 删除:wq 保存都退出)

```
    *filter:INPUTACCEPT:OUTPUTACCEPT:FORWARDACCEPT-AINPUT-
jDROP-ieth0any-snh-blade-67!--src-mac00:17:a4:a8:68:11/'
```

再重启 arp 防火墙就没有错误。查看 arp 防火墙状态 /etc/init.d/arptablesstatus:

*filter:INPUTACCEPT:OUTPUTACCEPT:FORWARDACCEPT-AINPUT-jDROP-ieth0-oany-snh-blade-67!--src-mac00:17:a4:a8:68:11-AINPUT-jDROP-ieth0-oany!--src-mac00:24:51:e9:c7:10

注:RHEL5U1 自带 arptables 的版本是 0.0.8,命令里不能带--source-ip 参数,这个版本不是 sourceforge.net 上发布的。

)重启后生效开启:chkconfigarptableson 关闭:chkconfigarptablesoff

2)即时生效,重启后失效开启:servicearptablesstart 关闭:servicearptablesstop