第一章　安全基础技术实验

1.1　实验要求

利用西普信息安全教育平台，从以下课程部分选取 2 个实验项目进行学习、理解、设计和完成实验，书写所完成的内容。

1.2　实验内容

- 密码学及应用
- 防火墙 (*)
- 入侵检测系统
- 日志数据分析
- 数据库安全 (*)

1.3　防火墙

1.3.1　实验目的-熟悉 iptables 的表链操作

熟悉 iptables 的表链操作.

1.3.2　实验原理

通过 iptables 命令对防火墙 iptables 的表链进行相关操作（因环境策略不同，表链会有所不同），如查看、添加、删除、修改等等。

1.3.3　实验环境

操作系统：CentOS 6.5

1.3.4 实验步骤

1.3.4.1 Iptables 链操作

查看 CentOS 6.5 中防火墙 iptables 的表名（因环境策略不同，表会有所不同）。在终端输入命令

```
cat /proc/net/ip_tables_names
```

若无结果，请查看是否开启服务。可执行

```
service iptables restart
```

重启服务后再次执行，可以看到 iptables 包含 4 张表，分别是 mangle、raw、filter 和 nat （默认只有 filter 表，如果之前有对其他表进行过相关操作，才会有其他表）。

在终端输入命令

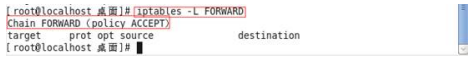
```
iptables -t filter -L
```

查看表 filter 中的链及其链中的规则。`-t filter` 指定表 filter，也可不加，不加时默认表 filter。可知表 filter 有 3 条链：INPUT、FORWARD 和 OUTPUT，这 3 条链的默认规则都为 ACCEPT。

若要查看某条链上的规则，在 `-L` 参数后指明链名。例如在终端输入命令

```
iptables -L FORWARD
```

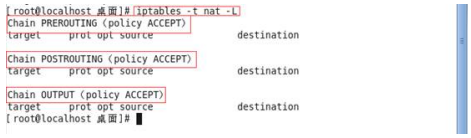
查看表 filter 中链 FORWARD 上的规则。



在终端输入命令

```
iptables -t nat –L
```

查看表 nat 中的链及其链中的规则。可知表 nat 有 3 条链：PREROUTING、POSTROUTING 和 OUTPUT，这 3 条链的默认规则都为 ACCEPT。



在终端输入命令

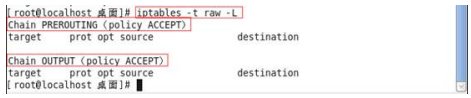
```
iptables -t mangle –L
```

查看表 mangle 中的链及其链中的规则。可知表 nat 有 5 条链：PREROUTING、INPUT、FORWARD、OUTPUT 和 POSTROUTING，这 5 条链的默认规则都为 ACCEPT。

在终端输入命令

```
iptables -t raw –L
```

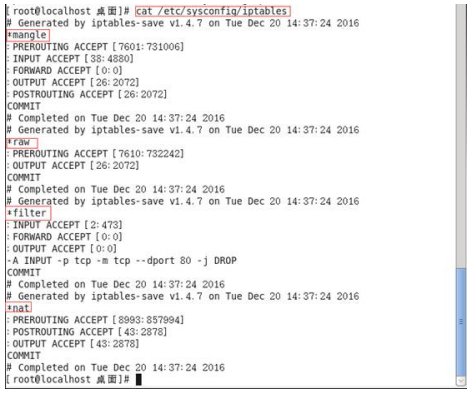
查看表 nat 中的链及其链中的规则。可知表 raw 有 2 条链：PREROUTING 和 OUTPUT，这 2 条链的默认规则都为 ACCEPT。



在终端输入命令

```
cat /etc/sysconfig/iptables
```

(因环境策略不同，表中链及链中规则会有所不同)，查看防火墙配置文件，可以查看到 iptables 所有表中的链及其链中规则（默认只有 filter 表，如果之前有对其他表进行过相关操作，才会有其他表)。



这 4 张表 5 条链中的规则 target 为目标；prot 为协议；opt 为 option，选项；source 为源地址，destination 为目的地址。在终端输入命令

```
cat /proc/net/ip_tables_targets
```

查看 iptables 中的 targets。

在终端输入命令

```
iptables -N simpleware1
```

在表 filter 中添加一条名为 simpleware1 的新链。这里没有使用 `-t` 指定表，默认是 filter 表，还可用 `-t nat/mangle/raw` 在指定的表中添加新的链。再使用

```
iptables -L
```

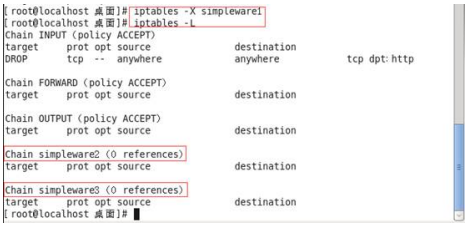
进行查看。

使用上一步的方法继续在表 filter 中添加两条新链 simpleware2 和 simpleware3。

若想删除某条自定义的链，使用 `-X` 参数。在终端输入命令

```
iptables -X simpleware1
```

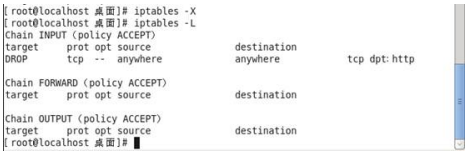
删除表 filter 中自定义的链 simpleware1。



在终端输入命令

```
iptables -X
```

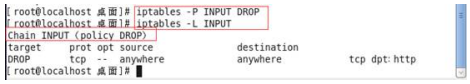
直接删除表 filter 中所有自定义的链。



可以使用 -P 参数修改某条链的默认规则。例如在终端输入命令

```
iptables -P INPUT DROP
```

将表 filter 中的链 INPUT 的默认规则改为 DROP。

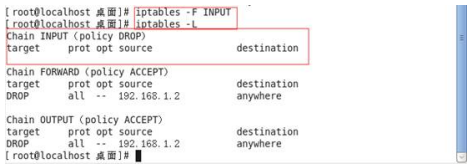


在终端输入如下命令，分别在 filter 表的 3 条链上添加一条防火墙规则。

在终端输入命令

```
iptables -F INPUT
```

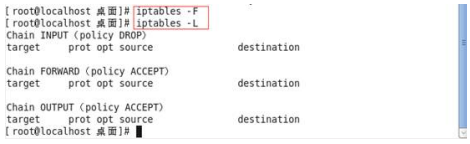
清空 filter 表中 INPUT 链上的所有规则。



在终端输入命令

```
iptables -F
```

不指明链名时，删除表 filter 中所有链上的规则。



1.4 数据库安全