**第九章 课后作业**

1、下表显示了对于一个IP地址从192.168.1.0到192.168.1.254的虚拟网络的包过滤防火墙规则集的一个样本。请描述一下每条规则的作用。



(1) 允许来自任意网络终端的任意端口访问网络192.168.1.0上的非熟知端口

(2) 拒绝IP地址为192.168.1.1的设备访问网络

(3) 拒绝任意网络终端的任意端口访问IP地址为192.168.1.1的设备

(4) 允许网络192.168.1.0上的任意设备访问网络

(5) 允许任意网络设备访问IP地址为192.168.1.2的设备的SMTP端口

(6) 允许任意网络设备访问IP地址为192.168.1.3的设备的HTTP端口

(7) 拒绝任何网络上的设备访问网络

2、SMTP（简单邮件传递协议）是一个通过TCP协议在主机之间传递邮件的标准协议。在用户代理端和服务程序之间建立一个TCP连接。服务程序监视25 TCP端口来查看是否有连接请求。连接的用户端部分的TCP端口号在1023以上。假设你要做一个包过滤策略集来允许进出的SMTP网络流量，并且生成了如下的规则集：



a. 描述这些规则的作用。

A：允许从外部源入站的电子邮件流量

B：试图允许对入站的SMTP连接进行响应

C：允许向外部源出站的电子邮件

D：试图允许对出站的SMTP连接进行响应

E：默认规则，拒绝任意其他的流量出入站

b. 假设你的主机在这个例子中的IP地址是172.16.1.1。某个人想从IP地址为192.168.3.4的远程主机发邮件给你。如果成功了，则将会在远程主机和你机器上的SMTP服务之间建立一个由SMTP命令和邮件组成的SMTP会话。另外，假设你主机上的一个用户想发送电子邮件到远程主机上的SMTP服务器上。则这一过程会产生如下的四个典型的包：



指出哪些包将会被允许或者阻止，并且指出每种情况使用了哪条规则。

四个包都会被允许。

包1使用了规则A

包2使用了规则B

包3使用了规则C

包4使用了规则D

c. 假设外部的某人试图从IP地址为10.1.2.3的远程主机上通过该主机上的5150端口建立一个到本地主机（172.16.3.4）上运行的Web代理服务器（端口为8080）的连接，来发动一个远程攻击。典型的包显示如下：



这个攻击会成功吗？给出详细说明。

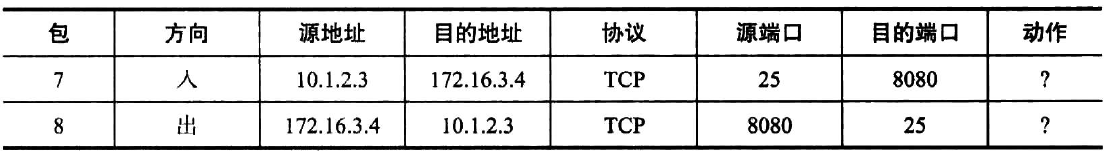
会成功。

包5应用规则D，被允许

包6应用规则B，被允许

攻击产生的包都没有被包过滤策略集过滤掉，因此，该攻击可以成功。

3、一个攻击者试图用他/她自己机器上的25号端口建立一个到你的Web代理服务器的连接。会产生如下的数据包：



解释为什么使用以下的规则集时该次攻击会成功。



包7应用了规则D，被允许

包8应用了规则C，被允许

因此，攻击者成功建立了连接，攻击成功。