

## 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。

表 9-5 样本包过滤防火墙规则集

	源地址	源端口	目的地址	目的端口	行动
1	任意	任意	192.168.1.0	>1023	允许
2	192.168.1.1	任意	任意	任意	拒绝
3	任意	任意	192.168.1.1	任意	拒绝
4	192.168.1.0	任意	任意	任意	允许
5	任意	任意	192.168.1.2	SMTP	允许
6	任意	任意	192.168.1.3	HTTP	允许
7	任意	任意	任意	任意	拒绝

- (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：

规则	方向	源地址	目的地址	协议	目的端口	动作
A	入	外部	内部	TCP	25	允许
B	出	内部	外部	TCP	>1023	允许
C	出	内部	外部	TCP	25	允许
D	入	外部	内部	TCP	>1023	允许
E	出和入	任意	任意	任意	任意	拒绝

- 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：

包	方向	源地址	目的地址	协议	目的端口	动作
1	入	192.168.3.4	172.16.1.1	TCP	25	?
2	出	172.16.1.1	192.168.3.4	TCP	1234	?
3	出	172.16.1.1	192.168.3.4	TCP	25	?
4	入	192.168.3.4	172.16.1.1	TCP	1357	?

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：

包	方向	源地址	目的地址	协议	目的端口	动作
5	入	10.1.2.3	172.16.3.4	TCP	8080	?
6	出	172.16.3.4	10.1.2.3	TCP	5150	?

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：

包	方向	源地址	目的地址	协议	源端口	目的端口	动作
7	入	10.1.2.3	172.16.3.4	TCP	25	8080	?
8	出	172.16.3.4	10.1.2.3	TCP	8080	25	?

解释为什么使用以下的规则集时该次攻击会成功。

规则	方向	源地址	目的地址	协议	源端口	目的端口	动作
A	入	外部	内部	TCP	>1023	25	允许
B	出	内部	外部	TCP	25	>1023	允许
C	出	内部	外部	TCP	>1023	25	允许
D	入	外部	内部	TCP	25	>1023	允许
E	出和入	任意	任意	任意	任意	任意	拒绝

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。