|  |  |  |  |
| --- | --- | --- | --- |
| 1. .启动 iptables 并查看当前防火墙的配置：   |  | | --- | | http://10.144.53.6/api/attachment?type=courseDocument&id=1773 |   2. 清空防火墙表中的所有配置策略：  http://10.144.53.6/api/attachment?type=courseDocument&id=1775  3. 将 iptables 中的 filter 表的各条链默认值设为 DROP，具体操作如下所示：  http://10.144.53.6/api/attachment?type=courseDocument&id=1779  从上图中可以看出，初始默认的策略为 ACCEPT，更改后的为 DROP，此时本台机子无法收数据和发送数据包。  4. 允许其它机器可以 ping 通本机：  首先，允许其它机器从 eth0 进入的 ping 数据包，此时需要给本机配置合适的 IP 地址，    并写如合适的规则，如下图所示：   |  | | --- | | http://10.144.53.6/api/attachment?type=courseDocument&id=1777 |   进行测试：  http://10.144.53.6/api/attachment?type=courseDocument&id=1778  在这种情况下是由于该规则只允许接收数据，并不允许通过 eth0  发送数据，所以就收 不到回应数据包，从下图可以直观的看到发送数据被禁止。  http://10.144.53.6/api/attachment?type=courseDocument&id=1786  为了可以使主机之间可以互通，需要添加以下语句，并查看 iptables：  http://10.144.53.6/api/attachment?type=courseDocument&id=1781    http://10.144.53.6/api/attachment?type=courseDocument&id=1784  再次进行测试，结果如下图所示：  http://10.144.53.6/api/attachment?type=courseDocument&id=1774  思考：想想我们最加入的语句倒底起到了什么作用。上例中我们的目标地址和源地址都  是 anywhere，如觉得有必 要，可进行更严格的限制（上例中虽然我们已经对网络接口限制到了 eth0 上，但 eth0 可能会进行 IP 的修改，这样我们上 面的 ping 仍旧有效）；  5. 可以用 ssh 登录本机  在允许之前我们先测试一下看看能不能用 putty 进行 ssh 登录，或者直接 telnet ssh 端口 看看能没有反应，以确认是否可以访问目标主机的 ssh 服务，不能登录：  http://10.144.53.6/api/attachment?type=courseDocument&id=1770  接着尝试使用 telnet 进行连接，出现端口不打开，访问失败。  http://10.144.53.6/api/attachment?type=courseDocument&id=1783  以上测试说明我们的默认策略 DROP 是生效的，接下来修改 iptables 的策略如下图所示    （注意：该策略的 ip 地址为本机 IP 地址）：  http://10.144.53.6/api/attachment?type=courseDocument&id=1771  然后进行连接测试：  http://10.144.53.6/api/attachment?type=courseDocument&id=1769  http://10.144.53.6/api/attachment?type=courseDocument&id=1780  思考：为什么我们这次只设置了一条规则就可以访问了？  6.上面设置中，我们允许了所有机器可 ping 和 ssh 登录我们的主机，是不是觉得有些不安全呢？如果我们知道需要 SSH 登录我们主机的 IP 范围，则我们可以将允许范围缩小到我们需要的 IP 范围。当然你也可以明确禁止某个或某个网段登录禁止 172.16.5.190 这个 IP ssh 登录我们的主机:  http://10.144.53.6/api/attachment?type=courseDocument&id=1785  但是测试结果表明 172.16.5.190 还是可以登录主机，注意上图上我们策略的顺序，策略顺序是很重要的。重新来设置看看结果如何为方便查看设置，我们列出每条规则的编号（注意使用— line-number 参数）：  http://10.144.53.6/api/attachment?type=courseDocument&id=1772  删掉我们刚才建立的那条规则：    http://10.144.53.6/api/attachment?type=courseDocument&id=1776  再来，我们接下来在正确的位置添加一条规则，但这里我们是在原来的规则中插入一条新的  规则到指定的位置：   |  | | --- | | http://10.144.53.6/api/attachment?type=courseDocument&id=1782 |   再来测试，发现 172.16.5.190 已经不能正常登录本机了。  【实验思考】  1)      需注意的是我们上例中目标 IP  没有指定，请大家考虑一下如果 172.16.5.190  要通 过本防火墙的路由功能的访问另一主机的 ssh,那么此规则是否会对此有影响呢？  2)      Linux 防火墙如何进行 TCP、UDP 以及 NAT 的配置与防护。 |
|