|  |
| --- |
| 1、  单击“网络拓扑”，启动并进入目标主机，进入实验环境，如图  http://10.144.53.6/api/attachment?type=courseDocument&id=4644  2、  启动系统并修改ip 地址  启动client(密码123456)  http://10.144.53.6/api/attachment?type=courseDocument&id=4650  修改eth0 的地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4661  地址生效  service  network restart  ping 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4654  启动服务器  http://10.144.53.6/api/attachment?type=courseDocument&id=4657  修改地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4647  修改生效  http://10.144.53.6/api/attachment?type=courseDocument&id=4640  3、  启动防火墙  http://10.144.53.6/api/attachment?type=courseDocument&id=4648  查看防火墙地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4635  ping 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4628  从防火墙到客户端是通的  ping 192.168.100.102  http://10.144.53.6/api/attachment?type=courseDocument&id=4651  从防火墙ping 内网是通的  需要内网地址能访问外网地址需要  增加缺省路由  #route add default gw 192.168.100.101  http://10.144.53.6/api/attachment?type=courseDocument&id=4645  查看路由信息  #route -n  http://10.144.53.6/api/attachment?type=courseDocument&id=4638  防火墙增加转发功能  http://10.144.53.6/api/attachment?type=courseDocument&id=4633  然后在内网ping外网地址 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4630  说明防火墙规则不让转发ping 的  我们增加一条允许 ping 的规则，此规则必须在红线圈定的规则之前  #iptables –I FORWARD 1 –p icmp   –j ACCEPT  然后在内网ping 外网地址  ping 192.168.100.99  http://10.144.53.6/api/attachment?type=courseDocument&id=4659  发现这次不同是因为路由问题,同时为了隐藏内网地址.  这时候需要在防火墙上增加地址伪装规则  http://10.144.53.6/api/attachment?type=courseDocument&id=4636  这时再在内网ping 外网地址  #ping 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4632这时在外网抓包  #tcpdump –i eth0 icmp  http://10.144.53.6/api/attachment?type=courseDocument&id=4639    在内网ping 外网地址  #ping 192.168.99.100  再回到外网,发现抓包的数据  http://10.144.53.6/api/attachment?type=courseDocument&id=4649  #Iptables –L FORWARD  http://10.144.53.6/api/attachment?type=courseDocument&id=4634  查看nat 表的规则  #iptables –t nat –L  http://10.144.53.6/api/attachment?type=courseDocument&id=4643  4、  配置外网主机规则,允许ftp 服务可以被访问  #iptables –I INPUT 5 –p tcp –dport 21 –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=4662  然后从server   ftp  192.168.99.100  发现不能ftp到client主机。  5、  回到防火墙  #iptables –I FORWARD 1 –p tcp –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=4665  回到内网主机  #ftp 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4664  回到防火墙，准备修改支持的最大并发连接  #cd /proc/sys/net  http://10.144.53.6/api/attachment?type=courseDocument&id=4637  nf\_conntrack\_max  是最大并发连接接口文件  #cat nf\_conntrack\_max  http://10.144.53.6/api/attachment?type=courseDocument&id=4629  通过echo 可以修改此文件  #echo 100000 > nf\_conntrack\_max  http://10.144.53.6/api/attachment?type=courseDocument&id=4652  # cat nf\_conntrack\_max  http://10.144.53.6/api/attachment?type=courseDocument&id=4658  现在防火墙的最大并发连接到达100000  #cd /proc/sys/net/netfilter  #ls  http://10.144.53.6/api/attachment?type=courseDocument&id=4655  这些都是可以在用户层修改的。不过修改这些文件的时候要非常小心，修改不好会严重影响系统的性能  #cd /proc/net  #cat nf\_conntrack  http://10.144.53.6/api/attachment?type=courseDocument&id=4656  可以看到正在访问的ftp 对应的连接  #cd /proc/net  http://10.144.53.6/api/attachment?type=courseDocument&id=4660  查看系统支持的规则表  #cat ip\_tables\_names  http://10.144.53.6/api/attachment?type=courseDocument&id=4660  #modprobe iptable\_mangle  http://10.144.53.6/api/attachment?type=courseDocument&id=4663  #cat ip\_tables\_names  http://10.144.53.6/api/attachment?type=courseDocument&id=4642  新增加的表mangle 出现了  查看支持的规则匹配模块  #cat ip\_tables\_matches  http://10.144.53.6/api/attachment?type=courseDocument&id=4631  通过modprobe 可以加载需要的模块  #modprobe xt\_string[字符串匹配]  http://10.144.53.6/api/attachment?type=courseDocument&id=4653  #cat ip\_tables\_matches  http://10.144.53.6/api/attachment?type=courseDocument&id=4646  string  模块出现  实验完毕，关闭实验窗口和网络拓扑图。 |
|