|  |
| --- |
| 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=4426  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=4431  修改eth0 的地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4437  地址生效  service  network restart  ping 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4434  启动服务器  http://10.144.53.6/api/attachment?type=courseDocument&id=4435  修改地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4428  修改生效  http://10.144.53.6/api/attachment?type=courseDocument&id=4423  3、  启动防火墙  http://10.144.53.6/api/attachment?type=courseDocument&id=4429  查看防火墙地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4418  ping 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4412  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=4432  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=4427  查看路由信息  #route -n  http://10.144.53.6/api/attachment?type=courseDocument&id=4421  防火墙增加转发功能  http://10.144.53.6/api/attachment?type=courseDocument&id=4416  然后在内网ping外网地址 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4414  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=4436  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=4419  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=4415这时在外网抓包  #tcpdump –i eth0 icmp  http://10.144.53.6/api/attachment?type=courseDocument&id=4422    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=4430  #Iptables –L FORWARD  http://10.144.53.6/api/attachment?type=courseDocument&id=4417  查看nat 表的规则  #iptables –t nat –L  http://10.144.53.6/api/attachment?type=courseDocument&id=4425  4、  如果外网有ftp服务器,配置规则,允许内网访问  首先配置外网规则,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=4438  其次在防火墙上配置允许内网访问的规则  查看防火墙当前时间  **注意：以下所有的规则均根据防火墙时间来进行**  #date  http://10.144.53.6/api/attachment?type=courseDocument&id=4424  #iptables –I FORWARD 2 –s 192.168.100.0/24 –m time –timestart 16:10 –timestop 18:10 –j ACCEPT  #iptables –I FORWARD 2 –d 192.168.100.0/24 –m time –timestart 16:10 –timestop 18:10 –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=4440  #iptables –L FORWARD  http://10.144.53.6/api/attachment?type=courseDocument&id=4439  在内网ftp 外网地址  #ftp 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4420  我们修改下时间,然后再进行访问  注：如果ftp访问不成功，可以更改防火墙系统时间，例：date   072016182005，然后在server主机上ftp 192.168.99.100。  #iptables –D FORWARD 2  #iptables –D FORWARD 2  #iptables –I FORWARD 2 –s 192.168.100.0/24 –m time –timestart 13:10 –timestop 15:10 –j ACCEPT  #iptables –I FORWARD 2 –d 192.168.100.0/24 –m time –timestart 13:10 –timestop 15:10 –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=4413  http://10.144.53.6/api/attachment?type=courseDocument&id=4433  思考:  为何ftp 返回的是no route to host  是防火墙的那条规则导致的呢?  5、  实验完毕，关闭实验窗口和网络拓扑图。 |
|