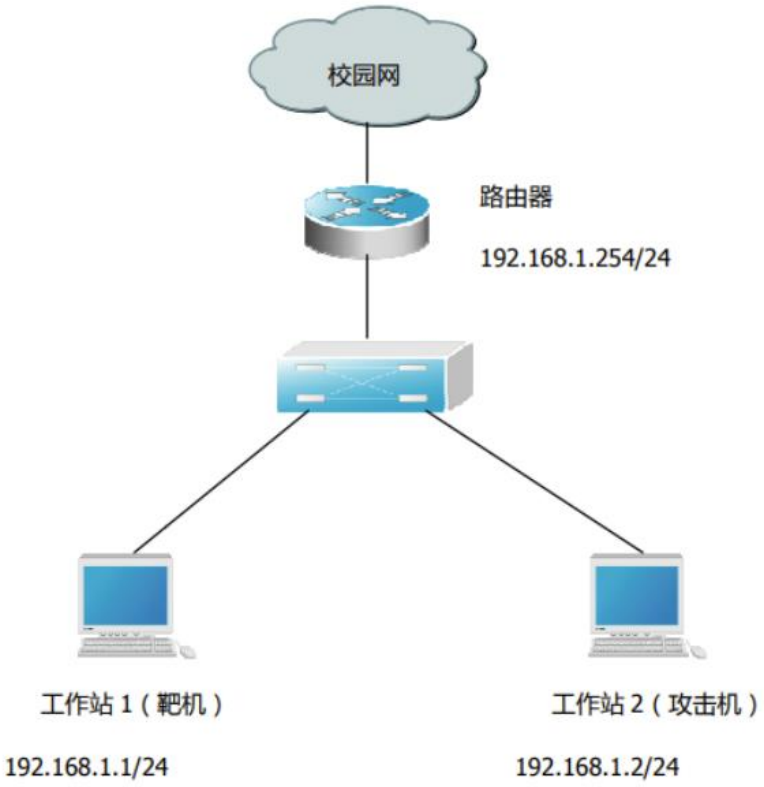
实验二：windows 下 dns 欺骗实验

2152701-陈玟桦

1. 依照实验拓扑，完成连线



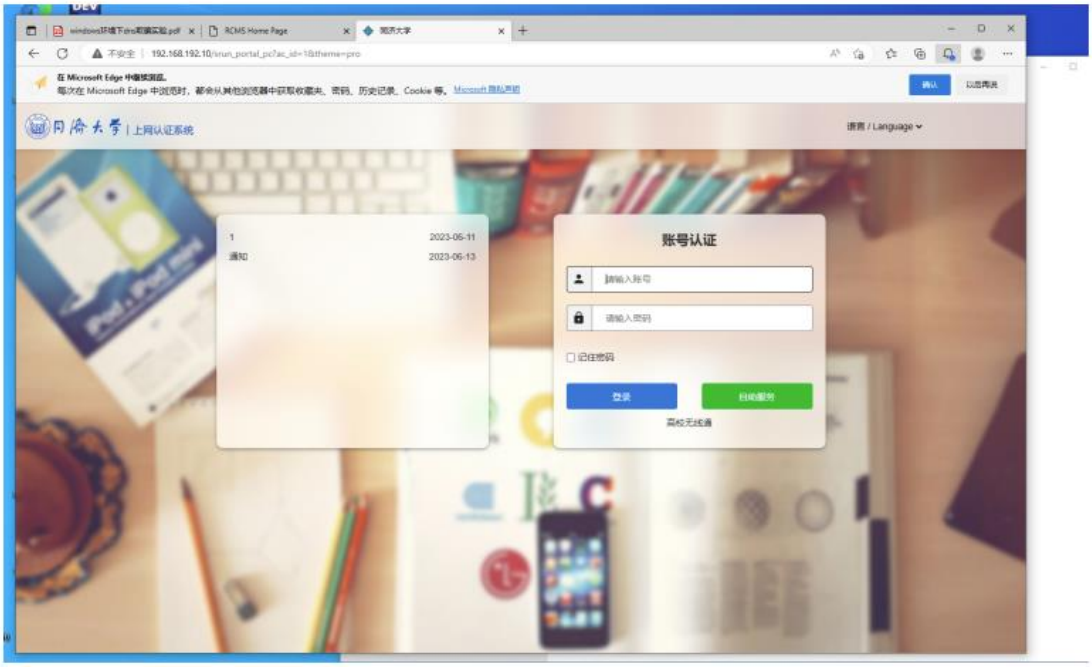
2. 配置路由

Telnet 172.16.0.5

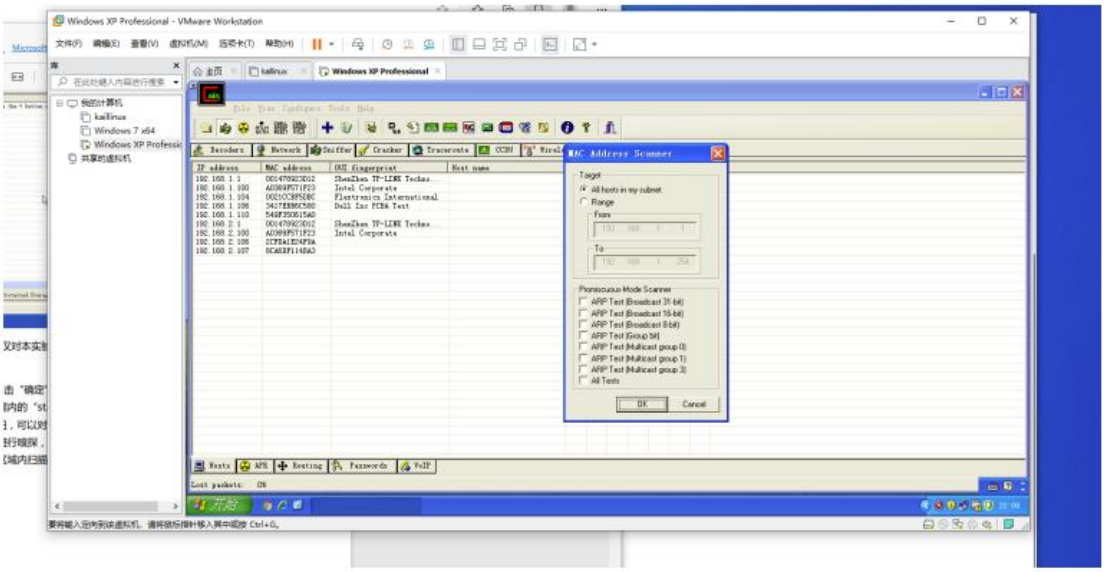
```
Red-Giant(config-if)#exit
Red-Giant(config)#sh ip int b
Interface                  IP-Address(Pri)      OK?      Status
serial 1/2                 no address           YES      DOWN
serial 1/3                 no address           YES      DOWN
FastEthernet 1/0           192.168.1.254/24     YES      UP
FastEthernet 1/1           100.64.253.117/17    YES      UP
Null 0                     no address           YES      UP
Red-Giant(config)#
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to DOWN
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to UP
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to DOWNint fa 1/0
Red-Giant(config-if)#
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to UPip nat inside
Red-Giant(config-if)#exit
Red-Giant(config)#int fa 1/1
Red-Giant(config-if)#ip nat outside
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to DOWN
Red-Giant(config-if)#exit
Red-Giant(config)#
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to UPip nat pool onlyone 100.64.186.43 100.
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to DOWN64.186.43 p
Red-Giant(config)#$186.43 100.64.186.43 prefix-length 17
Red-Giant(config)#access-list
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to DOWN 1 permit 192.168
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to UP.1.0 0.0.0.255
Red-Giant(config)#ip nat inside source list 1
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to DOWNpool onlyone overloa
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to UPd
Red-Giant(config)#
```

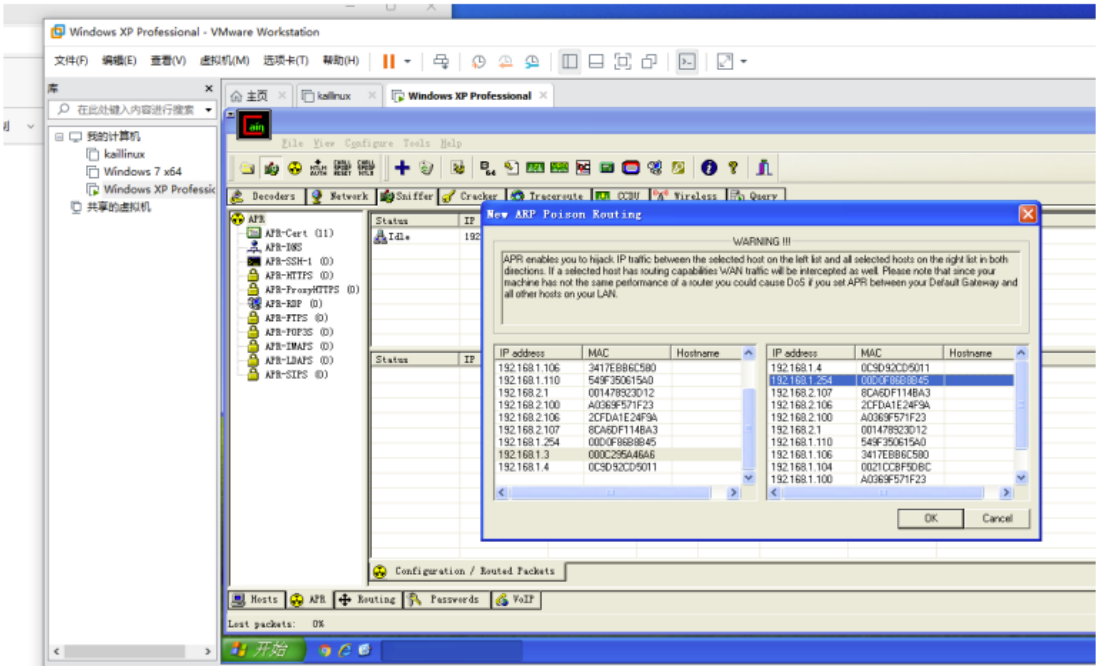
3. 正确设置攻击机和靶机的 ip 地址和网关，并登录上校园

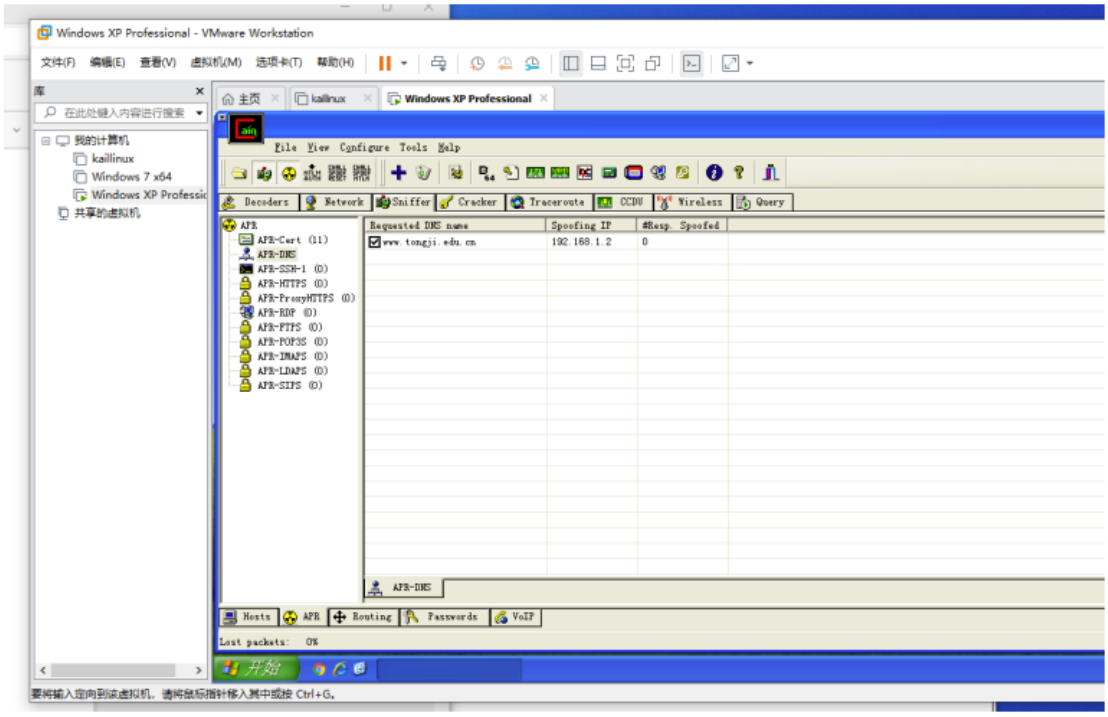
网



4. cain 软件实施攻击




Windows XP Professional - VMware Workstation
New ARP Poison Routing
WARNING !!!
OK
Cancel


Windows XP Professional - VMware Workstation
www.tongji.edu.cn
192.168.1.2

5. 欺骗成功

6. 心得体会

通过本次 APR 模拟攻防和 DNS 欺骗实验，我学习了 sniffer pro 软件抓包， 修改和重发的基本方法，了解了欺骗和防护的基本原理。在本次实验中，攻击机 和靶机位于同一个局域网内，攻击机轻易地使用 sniffer pro 完成了 APR 欺骗或 DNS 欺骗，这告诉我们在连接陌生公共网络服务时应当谨慎，提高防护意识