

《信息安全及实践》课程实验报告

学院： 信息学院 专业： 计算机科学与技术 年级： 2019

姓名： 李泽昊 学号： 20191060065

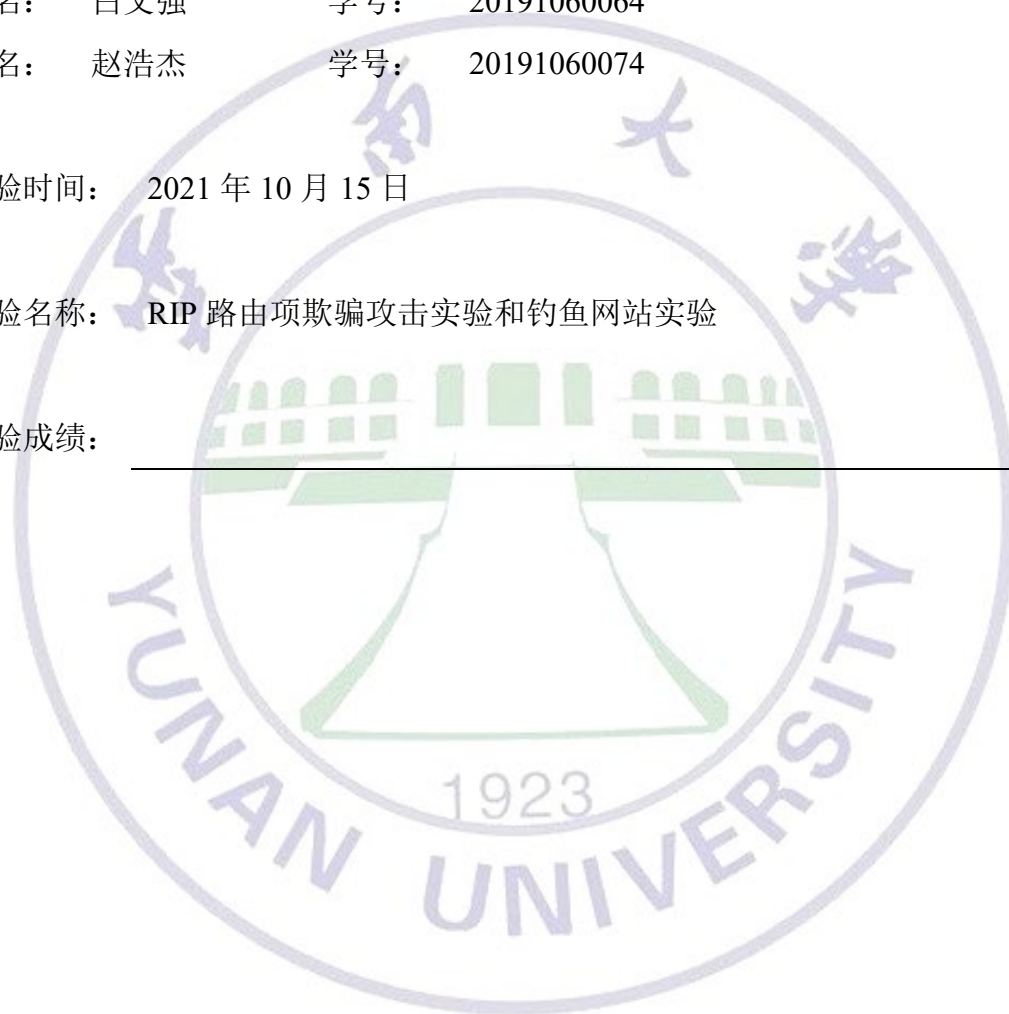
姓名： 白文强 学号： 20191060064

姓名： 赵浩杰 学号： 20191060074

实验时间： 2021 年 10 月 15 日

实验名称： RIP 路由项欺骗攻击实验和钓鱼网站实验

实验成绩：



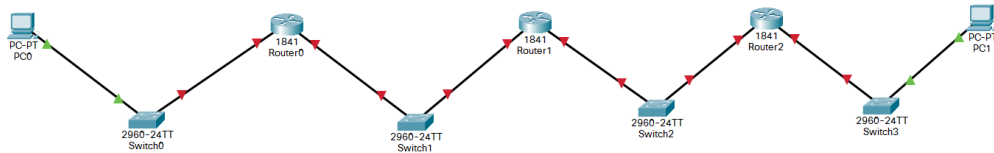
RIP 路由项欺骗攻击实验

一、实验目的

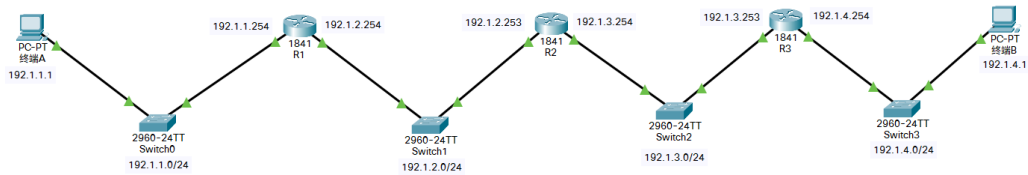
- (1)验证路由器 RIP 配置过程。
- (2)验证 RIP 生成动态路由项的过程。
- (3)验证 RIP 的安全缺陷。
- (4)验证利用 RIP 实施路由项欺骗攻击的过程。

二、实验步骤

(1)完成去掉入侵路由器后的设备放置

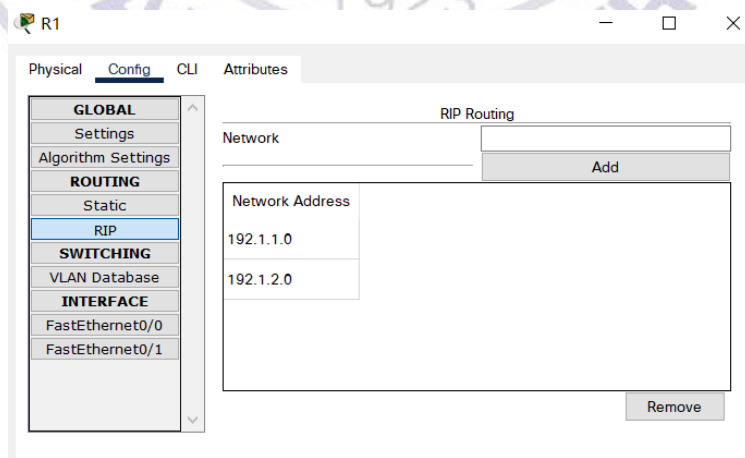


(2) 配置各个设备的 IP 地址和子网掩码

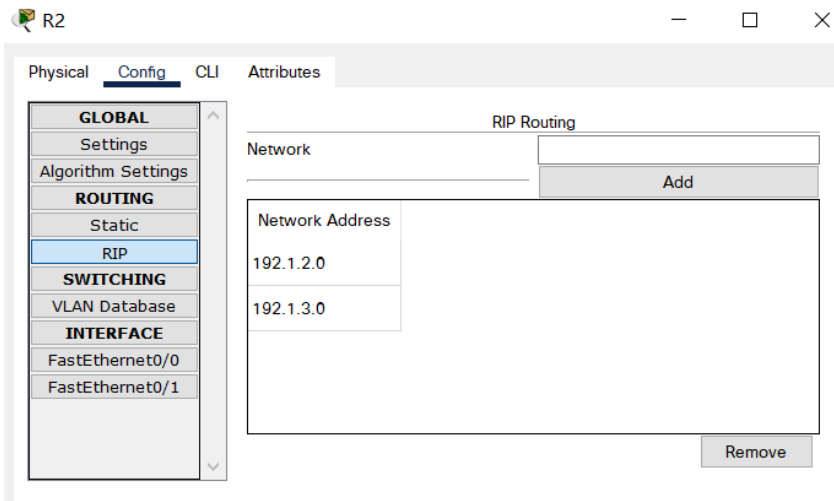


(3)完成路由器 RIP 协议配置

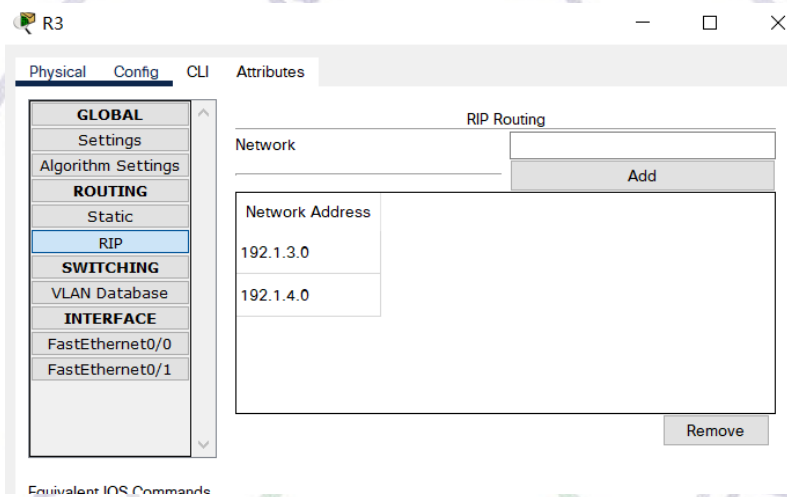
R1:



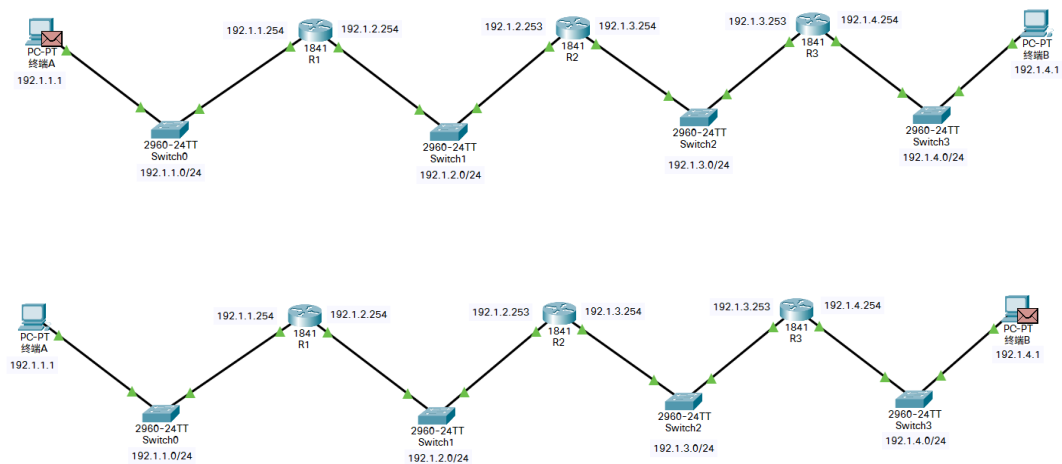
R2:

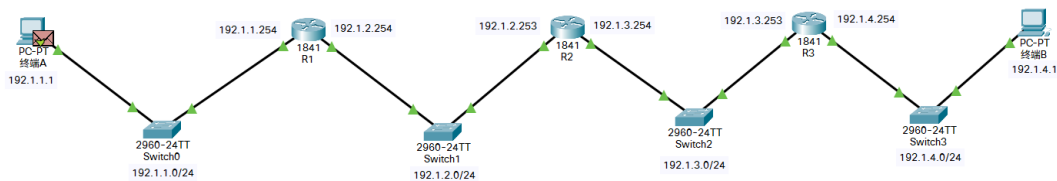


R3:

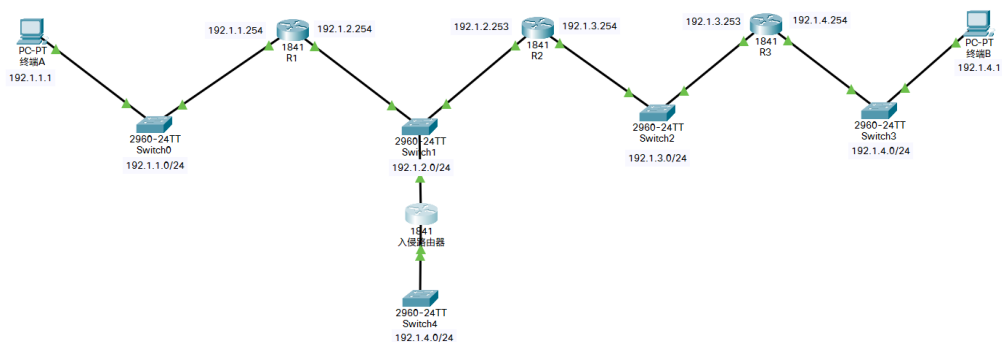


(4)通过启动 PC0 与 PC1 之间的报文传输过程验证 PC0 与 PC1 之间存在 IP 传输路径。

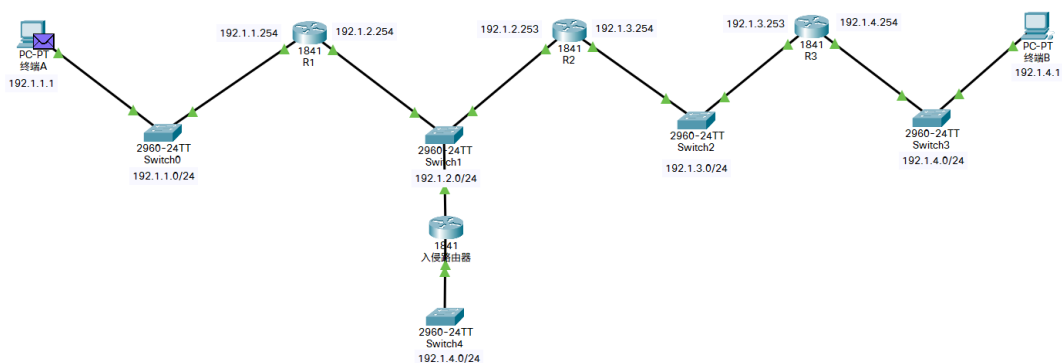


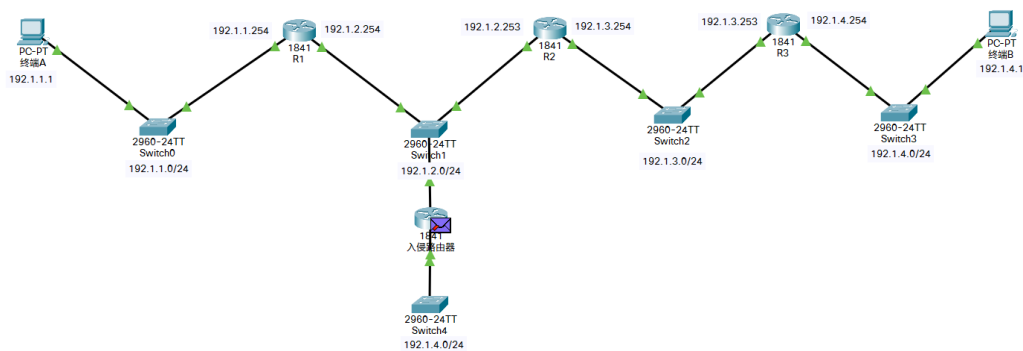


(5) 用路由器 Router 作为入侵路由器进行入侵



(6) 切换到模拟操作模式，启动 PC0 至 PC1 的 IP 分组传输过程，发现 IP 分组无法到达 PC1





三、实验结果及分析

一开始在没有加入入侵路由器之前，配置好各个设备的 IP 地址后，PC0 与 PC1 也就是终端 A 与终端 B 之间是可以进行正常通信的，因为三个路由器都配置好了 RIP 协议，保证网络通信的正常。

在加入入侵路由器之后，配置路由器 IP 协议，一端为 192.1.2.0 的子网，另一端为 192.1.4.0 的子网，也就是模拟 PC1 的子网，通过误导 R0 的 RIP 协议信息，从而使得 PC0 发往 PC1 的 IP 分组转发往入侵路由器。

四、实验总结及体会

如果想要对处在不同子网下的设备进行攻击，我们可以采用 RIP 协议欺骗的方法，通过设置入侵路由器，一端连接正常子网，另一端连接欺騙子网，欺騙子网需要设置为目的 IP 地址所在的子网，通过 RIP 协议自动配置所发的路由消息，误导其他路由器，从而将发往目的 IP 地址的截获下来，转发给入侵路由器。

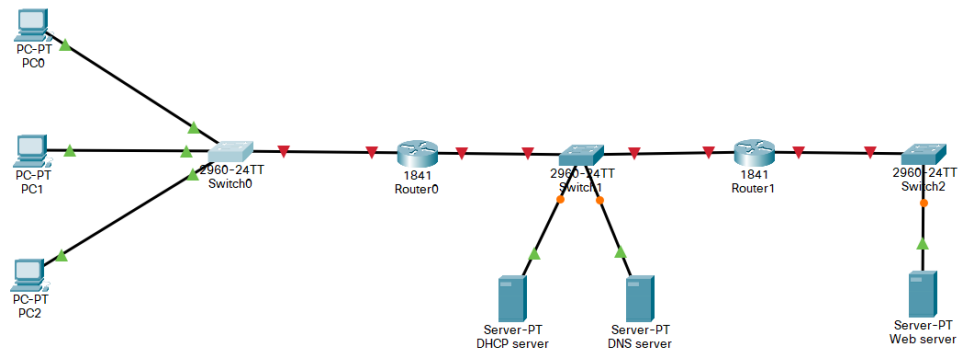
钓鱼网站实验

一、实验目的

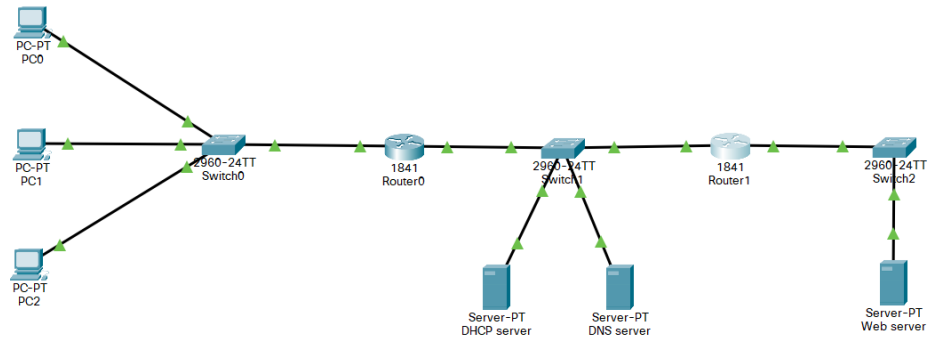
- (1) 验证伪造的 DHCP 服务器为终端提供网络信息配置服务的过程。
- (2) 验证错误的本地域名服务器地址造成的后果。
- (3) 验证利用网络实施钓鱼网站的过程。

二、实验步骤

- (1) 实现正常的 Web 服务器访问过程，完成设备的放置和连接。



- (2) 完成路由器接口 IP、子网掩码配置，完成 RIP 配置过程



- (3) 完成路由器接口中继地址配置过程。

```
Router(config)#int f0/0
Router(config-if)#ip helper-address 192.1.2.2
Router(config-if)#exit
Router(config)#
```

(4)完成服务器 IP 地址、子网掩码、默认网关

DHCP:

DHCP server

Physical Config Services **Desktop** Programming Attributes

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.1.2.2

Subnet Mask 255.255.255.0

Default Gateway 192.1.2.254

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::230:A3FF:FE30:C307

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

DNS:

DNS server

Physical Config Services **Desktop** Programming Attributes

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.1.2.7

Subnet Mask 255.255.255.0

Default Gateway 192.1.2.254

DNS Server 0.0.0.0

IPv6 Configuration

WEB:

Web server

Physical Config Services **Desktop** Programming Attributes

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.1.3.7

Subnet Mask 255.255.255.0

Default Gateway 192.1.3.254

DNS Server 0.0.0.0

IPv6 Configuration

(5)完成 DHCP 服务器配置

DHCP server

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.1.1.254

DNS Server: 192.1.2.7

Start IP Address: 192 1 1 10

Subnet Mask: 255 255 255 0

Maximum Number of Users: 50

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.1.1.254	192.1.2.7	192.1.1.10	255.255.255.0	50	0.0.0.0	0.0.0.0

☐ Top

(6)完成 DNS 服务器配置

DNS server

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management

DNS

DNS Service: ☒ On ☐ Off

Resource Records

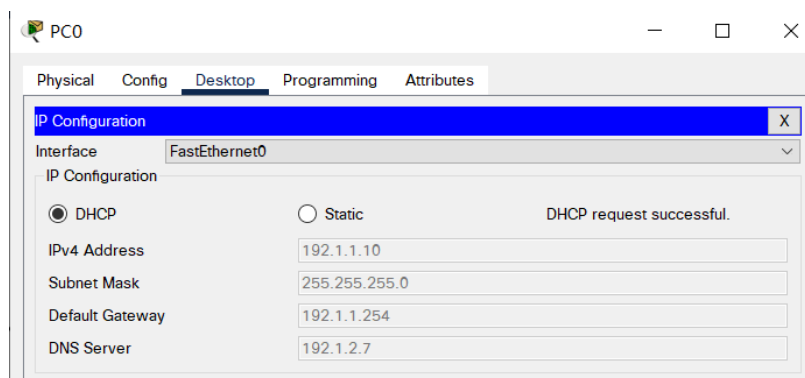
Name: Type: A Record

Address:

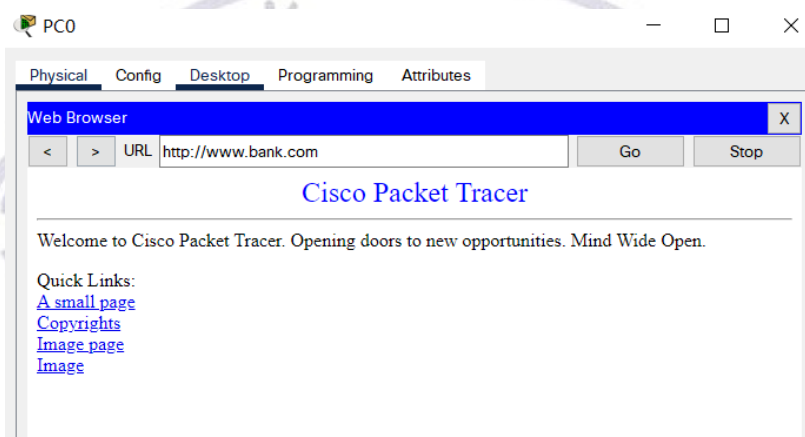
Add Save Remove

No.	Name	Type	Detail
0	www.bank.com	A Record	192.1.3.7

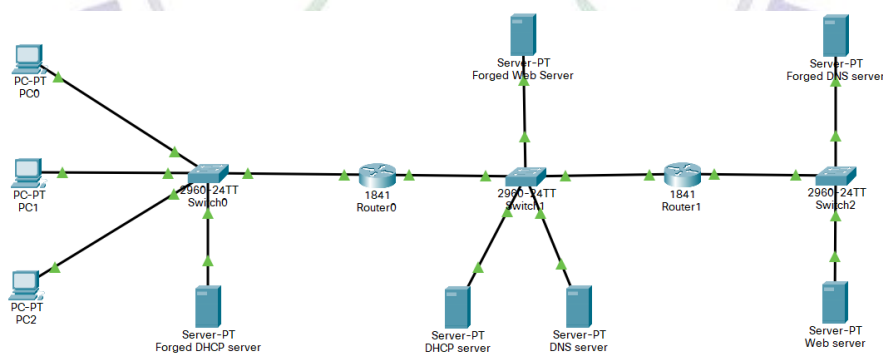
(7)完成 PC0 自动获取网络信息



(8)完成 PC0 浏览服务器过程



(9)接入三台伪造的服务器，完成三台伪造服务器的 IP 地址、子网掩码、默认网关配置



伪造 DHCP:

Forged DHCP server

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.1.1.254

DNS Server: 192.1.3.1

Start IP Address: 192.1.1.10

Subnet Mask: 255.255.255.0

Maximum Number of Users: 50

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.1.1.254	192.1.3.1	192.1.1.10	255.255.255.0	50	0.0.0.0	0.0.0.0

伪造的 DNS:

Forged DNS server

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management

DNS

DNS Service: ☒ On ☐ Off

Resource Records

Name: Type: A Record

Address:

Add Save Remove

No.	Name	Type	Detail
0	www.bank.com	A Record	192.1.2.5

PC0 再次获得 IP 地址:

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

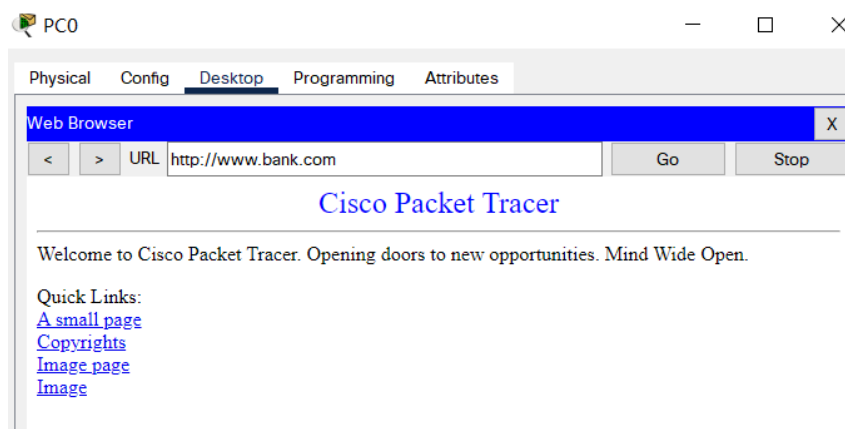
IPv4 Address: 192.1.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.1.1.254

DNS Server: 192.1.3.1

(10)用 PC0 再次访问浏览器



三、实验结果及分析

实验过程中，首先通过搭建好网络，实现 PC 机对 web 服务器的成功访问，终端通过从 DHCP 服务器获得正确的域名解析服务器，继而能够访问正确的网页，但是通过加入伪造的 DHCP 等服务器后，因为伪造的离终端距离更加接近，因此首先接入伪造的 DHCP 服务器，继而找到伪造的域名解析服务器，访问到钓鱼网站。

在实验过程中，路由器 1 采用到了中继的命令，是因为真正的 DHCP 服务器本省并不在终端的作用域里，需要通过中继命令，将 DHCP 服务器虚拟到真正的作用域里，达到分配网路及连接终端的功能。

四、实验总结及体会

这种攻击方法利用的是伪造的 DHCP 服务器比真正的 DHCP 服务器距离终端要更短，因此伪造的 DHCP 服务器会首先捕捉到 PC 终端。采用这种方法成功的关键有两个要点，一个是要保证真正的 DHCP 服务器不在本作用域，在一般情况下，DHCP 距离中端都比较远。第二个要点是要保证做的钓鱼网站和原来的真是网站非常相像，不然很容易导致用户发现端倪，导致最终失败。

对于应用层来讲，钓鱼网站是一个非常好用的攻击手段，对于某些账号密码进行登录的页面，用户应该谨慎判断，谨慎思考，放置被钓鱼网站钓鱼得逞。