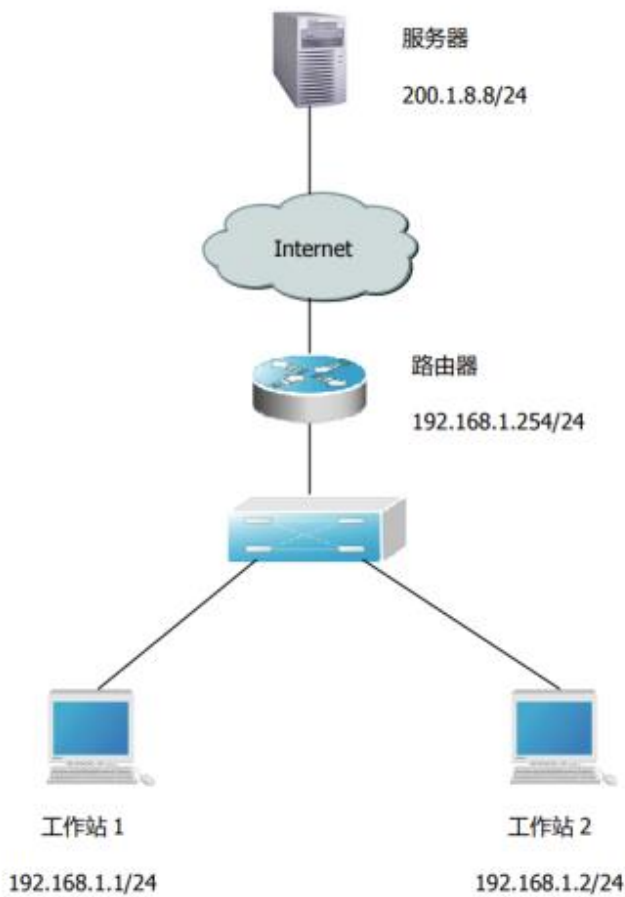


系统安全评估与应用安全实验一：ARP 模拟攻击测试与防护

2152701 陈玟桦

1. 依照实验拓扑，完成连线

实验拓扑



2. 登录路由器，正确配置设备

Telnet 172.16.0.5

```
Red-Giant(config)#show 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         200.1.8.1/24        YES      DOWN
Null 0                  no address           YES      UP
Red-Giant(config)#_
```

3. 正确设置 ip 地址

C:\ 管理员: 命令提示符

```
Microsoft Windows [版本 10.0.19045.2604]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Net317>ping 192.168.1.254

正在 Ping 192.168.1.254 具有 32 字节的数据:
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=63

192.168.1.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Net317>ping 192.168.1.2

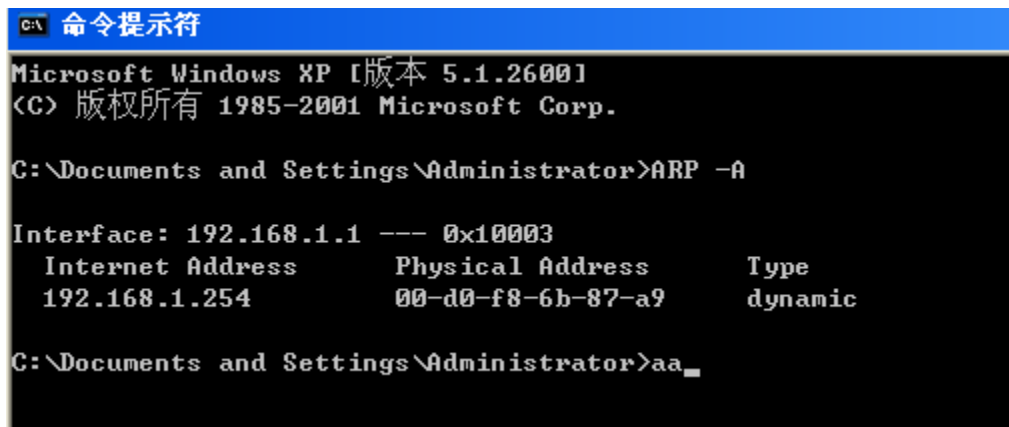
正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128

192.168.1.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

4. 启动 sniffer pro 软件捕获解码分析并攻击



5. 查看结果



```
C:\ 命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.1 --- 0x10003
   Internet Address      Physical Address      Type
   192.168.1.254         00-d0-f8-6b-87-a9     dynamic

C:\Documents and Settings\Administrator>aa_
```

6. 心得与体会

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