

电子科技大学 计算机科学与工程
程（网络空间安全） 学院

标准实验报告

（实验）课程名称 信息对抗综合设计实验

电子科技大学

实验报告

学生姓名： 黄鑫 学号： 2021050901013 指导教师：汪小芬

实验地点： 主楼 A2-413-1 实验时间： 2023.10.24

一、实验室名称：主楼 A2-413-1

二、实验项目名称：ARP 欺骗实验

三、实验学时：4

四、实验原理：

(1) ARP 的作用：ARP 的主要作用是将目标设备的网络地址（通常是 IP 地址）映射到其物理地址（通常是 MAC 地址）。这允许设备在局域网内正确地路由和传输数据包，因为它们需要知道目标设备的 MAC 地址以便进行直接通信。

(2) ARP 数据包类型：

- ARP 请求包：ARP 请求包用于查询目标 IP 地址对应的 MAC 地址。当一个设备需要与另一个设备通信，它会广播一个 ARP 请求包以获取目标设备的 MAC 地址。
- ARP 应答包：ARP 应答包用于回应 ARP 请求，提供目标 IP 地址对应的 MAC 地址。这是目标设备的响应，它包含了所需的 MAC 地址信息。

(3) ARP 缓存表：每台主机和路由器都会维护一个 ARP 缓存表，其中存储了已知设备的 IP 地址与 MAC 地址的映射关系。这个表可以包含静态和动态记录。静态记录是手动配置的，而动态记录是根据设备之间的通信动态生成的。

(4) 查看 ARP 缓存表：在 Windows 系统中，可以使用命令 "arp -a" 来查看 ARP 缓存表，这个表可以显示已知设备的 IP 地址和 MAC 地址的对应关系。

五、实验目的：

了解 SHA 密码加密原理、学习 SHA 散列暴力破解的过程

(5) ARP 的工作原理: ARP 工作的基本原理是通过广播 ARP 请求包来获取目标设备的 MAC 地址,然后将这些信息存储在 ARP 缓存表中,以便以后的通信。如果目标设备不在同一网络段,数据包需要通过网关进行中转,因此主机会首先检查 ARP 缓存表中是否有网关的 MAC 地址,如果没有,它会发送 ARP 请求来获取网关的 MAC 地址。

(6) ARP 欺骗攻击: ARP 欺骗是一种非法攻击,利用 ARP 协议的漏洞来实施。攻击者可以欺骗网络中的设备,导致网络问题或窃取敏感信息。这种攻击可能会导致以下危害:

- 使同一网络段的其他用户无法正常上网。
- 攻击者可以嗅探和窃取通信数据。
- ARP 欺骗可以用于篡改信息或注入恶意内容。

(7) 检测 ARP 欺骗攻击: 一些迹象可能表明存在 ARP 欺骗攻击,如网络频繁掉线、网速变慢、ARP 缓存表中 MAC 地址不匹配等。使用 Sniffer 软件等工具可以检测大量的 ARP reply 包,从而发现潜在的攻击。

(8) 防御 ARP 欺骗攻击: 为了防御 ARP 欺骗攻击,可以采取以下措施:

- 使用 MAC 地址绑定,将每台计算机的 IP 地址与硬件地址一一对应,不可更改。
- 使用静态 ARP 缓存,手动更新缓存中的记录。
- 使用 ARP 服务器来响应其他机器的 ARP 广播,确保 ARP 服务器不受攻击。
- 使用 ARP 欺骗防护软件,如 ARP 防火墙,来检测并隔离攻击主机。

五、实验目的:

- 1、通过 ARP 欺骗技术获取网站用户名、密码等信息。
- 2、了解 ARP 欺骗的基本原理。
- 3、熟悉 ARP 欺骗的工具使用,以及实验完成过程。

六、实验内容:

ARP 欺骗实验的内容包括模拟攻击者在局域网中发送伪造的 ARP 响应以欺骗其他主机,导致网络通信中断、数据嗅探和信息篡改等安全问题,并探讨相应的防御措施


七、实验器材(设备、元器件):

三台 Windows Server 2012R2

主机 A: 192.168.1.2 主机 B: 192.168.1.3 主机 C: 192.168.1.4

八、实验步骤:

- (1) 在主机 C 上打开 cmd，输入命令 arp -d，先清空 ARP 缓存，再使用命令 “arp -a” 进行查看，此时没有主机 A 和主机 B 的 ARP 缓存。



```
管理员: 命令提示符
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>arp -d

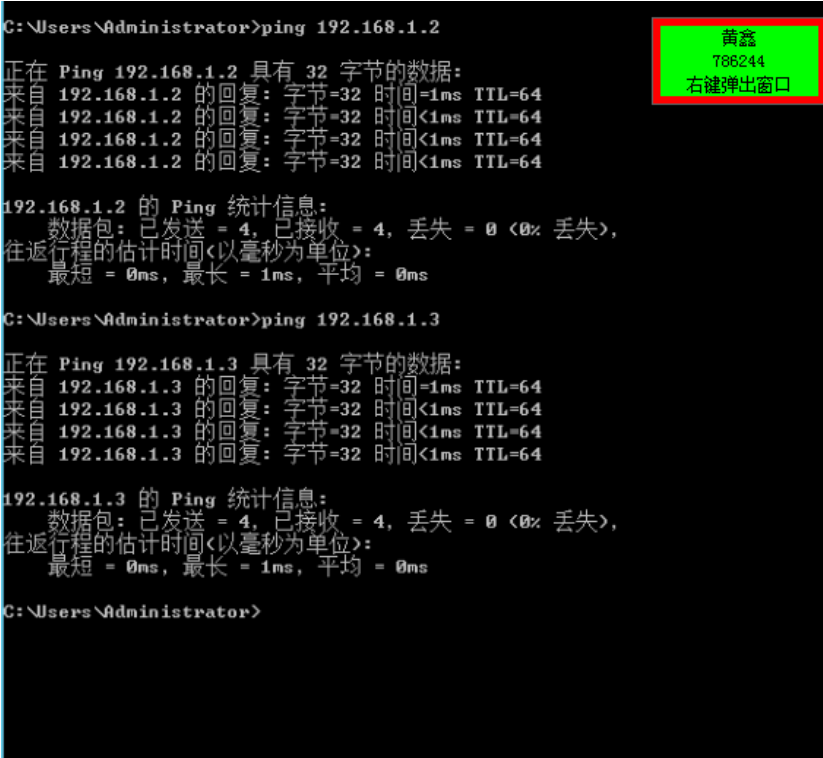
C:\Users\Administrator>arp -a

接口: 192.168.1.4 --- 0xe
Internet 地址      物理地址      类型
224.0.0.22         01-00-5e-00-00-16  静态

C:\Users\Administrator>
```

黄鑫
786244
右键弹出窗口

- (2) 输入命令 ping 192.168.1.2 和 ping 192.168.1.3，使之产生 ARP 缓存。



```
C:\Users\Administrator>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=64
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=64

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 = 1ms, 平均 = 0ms

C:\Users\Administrator>ping 192.168.1.3

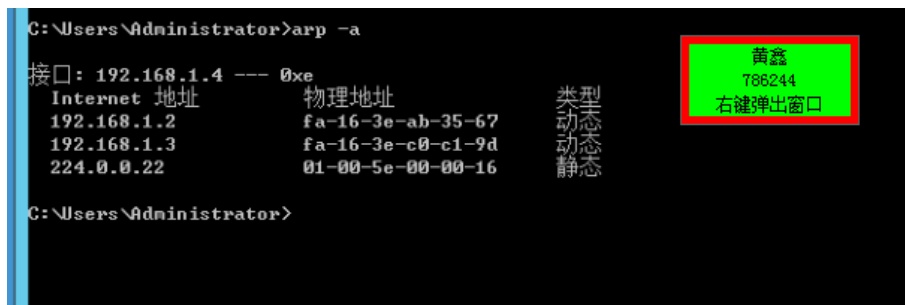
正在 Ping 192.168.1.3 具有 32 字节的数据:
来自 192.168.1.3 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=64

192.168.1.3 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 = 1ms, 平均 = 0ms

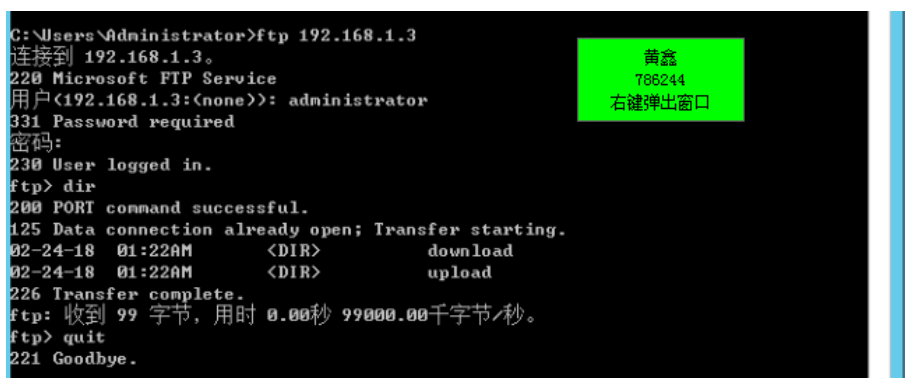
C:\Users\Administrator>
```

黄鑫
786244
右键弹出窗口

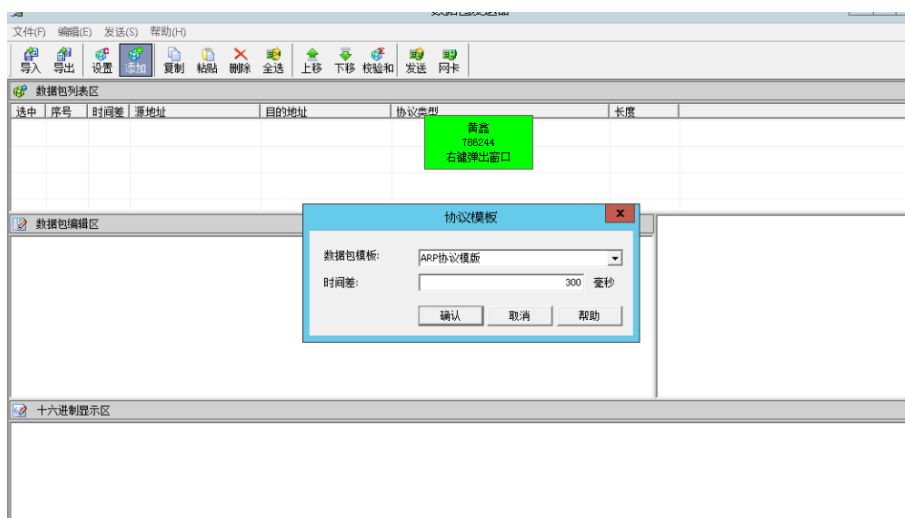
- (3) 此时再输入命令 arp -a，可以看到主机 A 和主机 B 的 ARP 缓存。



(4) 在主机 C 输入命令 ftp 192.168.1.3, 输入用户名 administrator 和密码 Simplexue123, 回车进行登录。输入命令 dir 查看目录, 再输入命令 quit 退出 FTP。即未进行 ARP 地址欺骗前, 可在主机 C 上访问 FTP



(5) 双击主机 A 桌面上的“数据包发送工具”快捷方式, 打开数据包发送器, 单击“添加”按钮, 数据包模板选择“ARP 协议模板”, 时间差使用默认的 300 毫秒。



(6) 在数据包编辑区, 按如下编辑 ARP 协议包。

Ethernet 封装:

目的物理地址: FF-FF-FF-FF-FF-FF, 将 ARP 请求设置为广播报文, 目的地址为广播地址;

源物理地址: 00-0C-29-70-31-70 (选择前先更新地址本, 下同), 为发送端

192.168.1.2 物理地址；

类型：0806，上层协议是 ARP 协议；

ARP 封装：

硬件类型：0001，表示硬件类型为以太网；

协议类型：0800，表示上层协议是 IP 协议；

硬件长度：6，表示硬件地址长度为 6 字节；

协议长度：4，表示协议地址长度为 4 字节；

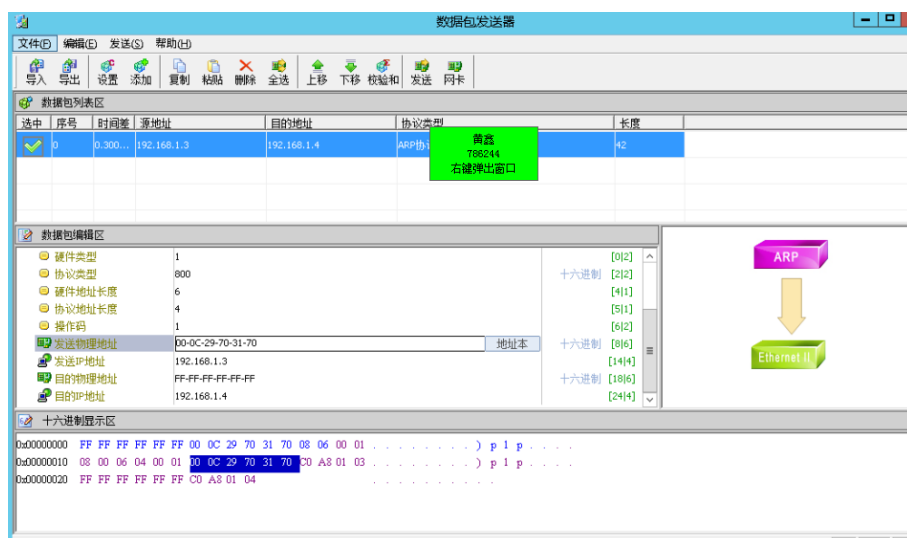
操作码：1，表示此 ARP 报文为 ARP 请求报文。

发送物理地址：00-0C-29-70-31-70，为发送 ARP 请求报文的主机的物理地址；

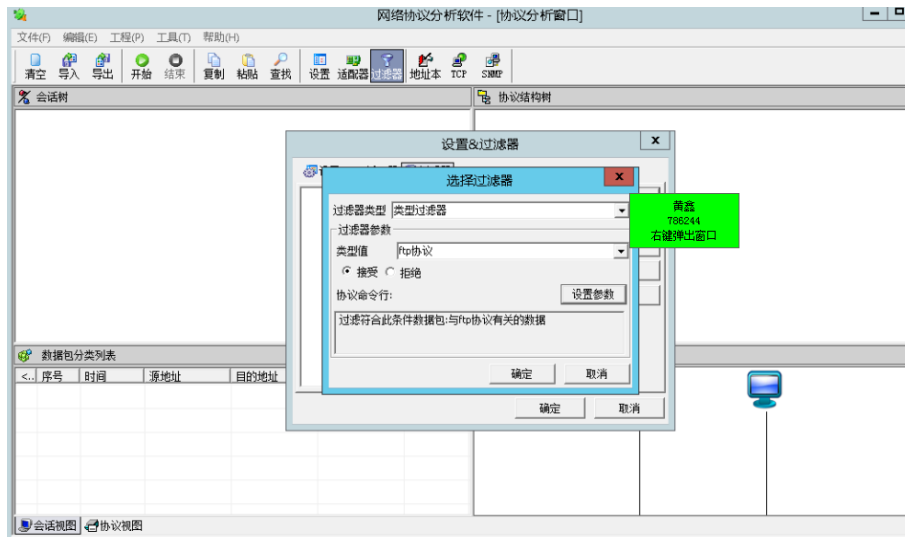
发送 IP 地址：192.168.1.3，为发送 ARP 请求报文主机的 IP 地址；

目标物理地址：FF-FF-FF-FF-FF-FF，ARP 请求为广播报文，目的地址为广播地址；

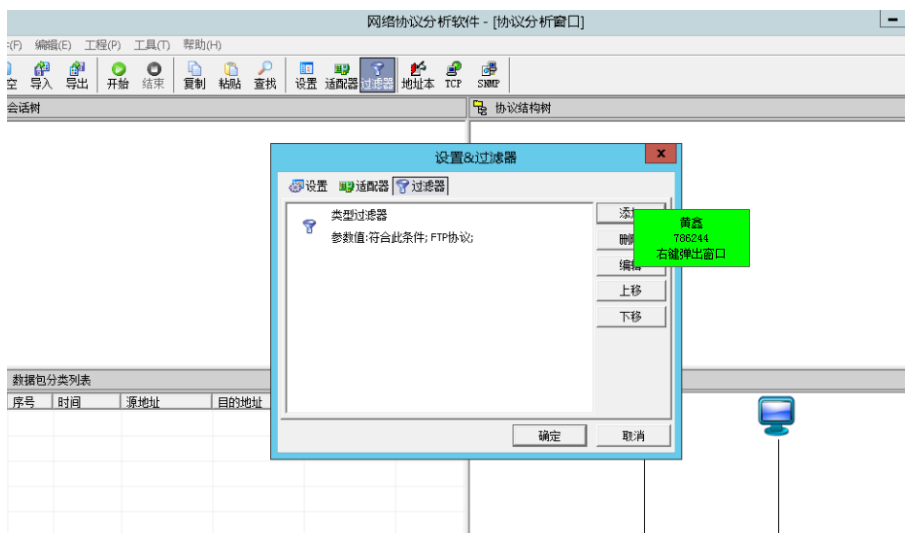
目标 IP 地址：192.168.1.4，目标主机 IP 地址。



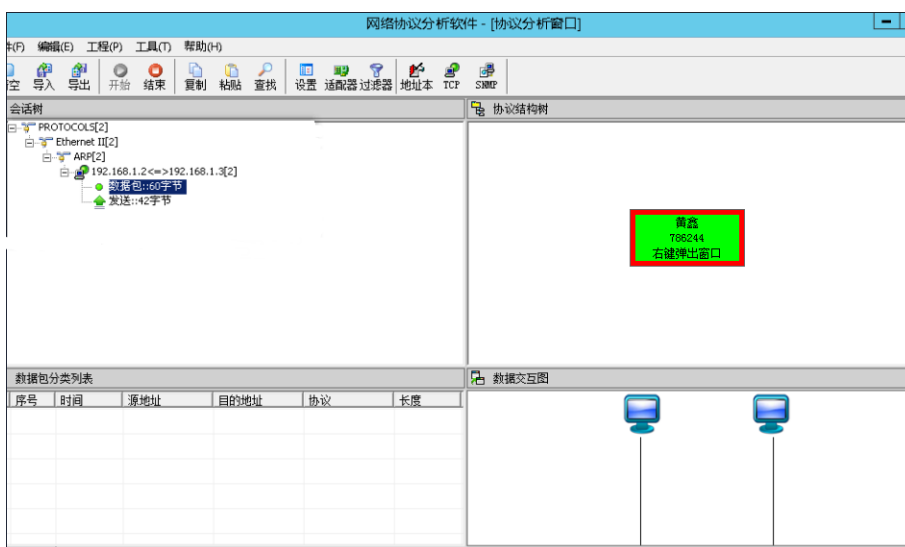
(7) 回到主机 C，双击桌面上的“网络协议分析工具”快捷方式，打开网络协议分析软件，单击“过滤器”按钮，单击“添加”按钮，过滤器类型选择“类型过滤器”，在过滤器参数中，类型值选择“ftp 协议”，选择“接受”，单击“设置参数”，提示“过滤符合此条件数据包:与 ftp 协议有关的数据”，说明设置成功，单击“确定”按钮，过滤器设置完毕，单击“确定”按钮。



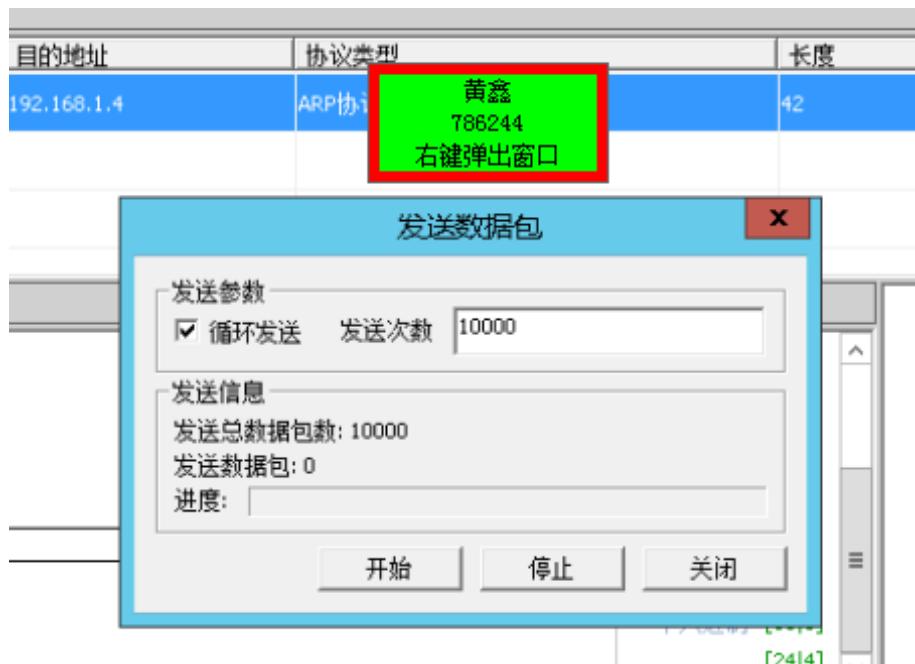
(8) 过滤器设置完毕，单击“确定”按钮。



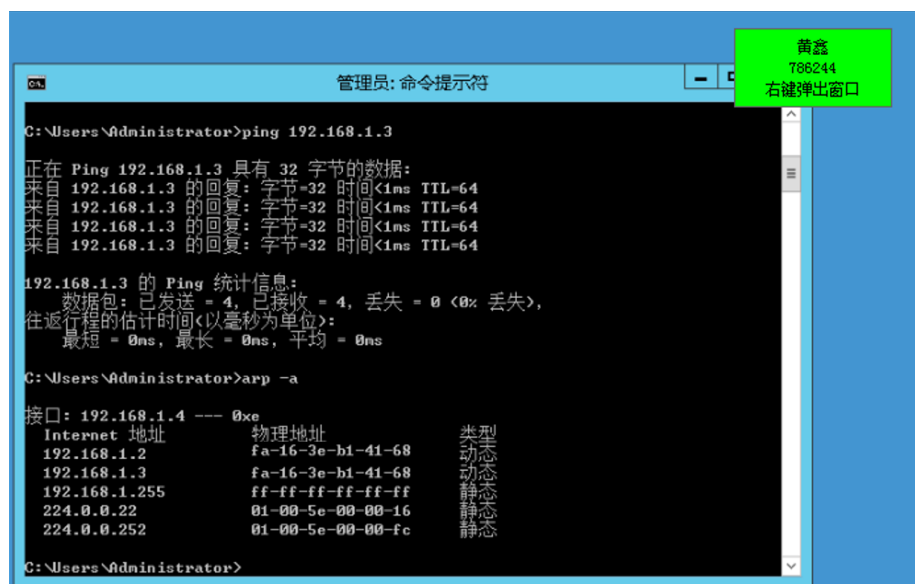
(9) 单击“开始”按钮。



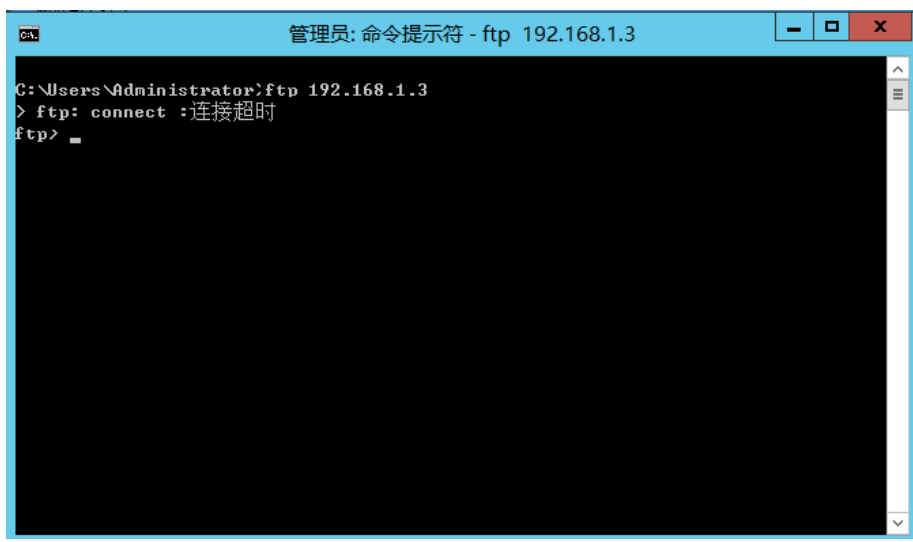
(10) 切换到主机 A，单击“发送”按钮，勾选“循环发送”，为了使 ARP 地址的时间长一点，便于后面的实验，将发送次数设置得大一点，这里设置为 10000，单击“开始”。



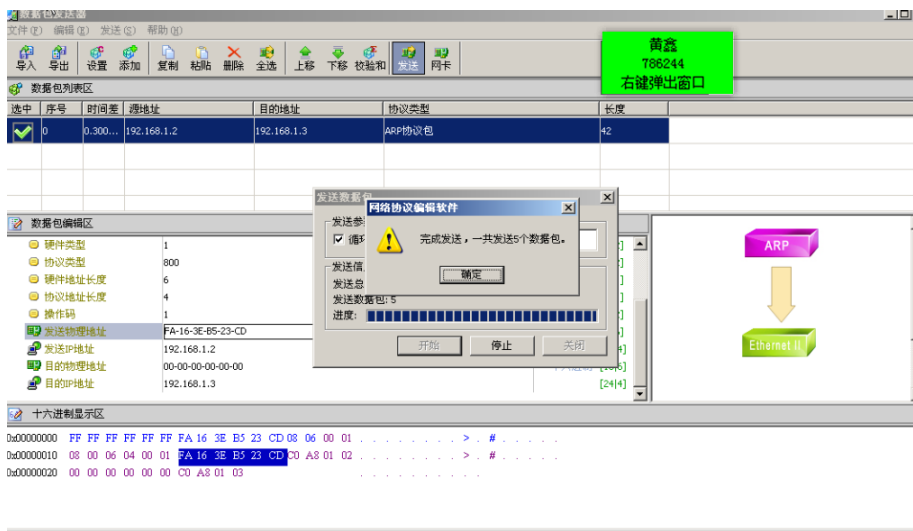
(11) 切换到主机 C，在 cmd 中输入命令 arp -a，显示主机 C 的 ARP 缓存，发现主机 A 和主机 B 的物理地址一样，说明 ARP 地址欺骗成功。



(12) 输入命令 ftp 192.168.1.3，登录主机 B 的 FTP 服务，但数据包根据 ARP 缓存表，把数据包发送主机 A 处，故 FTP 连接失败，显示连接超时，即进行 ARP 地址欺骗后，无法成功登录 FTP。



(13) 切换到主机 A，单击“关闭”，提示发送数据包的总数，单击“确定”



九、实验数据及结果分析：

可以看到网络协议分析软件捕获的 FTP 数据包，在协议视图下，单击 192.168.1.3<=>192.168.1.4, 可以看到源 IP 地址为 192.168.1.4、目标 IP 地址为 192.168.1.3，而目标物理地址不是主机 B 的物理地址，而是主机 A 的物理地址。这是由于链路层数据帧传输只识别 MAC 地址，无法识别 IP 层数据，验证成功实现欺骗。

十、实验结论：

本实验成功模拟了 ARP 地址欺骗攻击，通过伪造 ARP 响应包，欺骗了主机 C，使其将数据包发送到错误的目标主机 A 而不是主机 B。这导致了 FTP 连接失败，因为数据包被发送到了错误的地方。实验结果表明 ARP 欺骗攻击可以导致网络通信中断，数据包的错误路由，以及安全问题的发生。

十一、总结及心得体会：

通过本次实验，我深刻理解了 ARP 地址欺骗攻击的原理和危害。ARP 地址欺骗攻击是一种潜在的网络安全威胁，可以用于导致网络中的混乱和信息泄露。了解这种攻击的原理对于网络管理员和安全专业人员来说非常重要，以便采取适当的措施来防御这种威胁。

在实验中，我学会了如何使用数据包编辑工具来创建伪造的 ARP 响应包，并如何使用网络协议分析工具来捕获和分析数据包。这些技能对于理解和检测网络攻击非常有用。我还学到了一些防御 ARP 欺骗攻击的方法，如使用 MAC 地址绑定和静态 ARP 缓存。

总的来说，本次实验帮助我更深入地理解了网络安全领域的一些概念和技术，我认为这对我今后的学习和职业发展将非常有帮助。

十二、对本实验过程及方法、手段的改进建议：

1.更详细的实验目的和预期结果：在实验前，应该明确列出实验的详细目的和预期结果，以便学生更好地理解实验的目标和意义。

2.实验步骤的细化和清晰度：一些实验步骤可能需要更详细的解释和说明，特别是在使用特定工具和软件时。清晰的步骤说明可以帮助学生更轻松地完成实验。

3.安全注意事项：在实验中涉及到网络攻击和欺骗，应该强调学生只能在受控的环境中进行这些操作，并遵循合法和伦理的原则。

4.更多的实验材料和资源：提供更多的实验材料和资源，以帮助学生更深入地理解实验原理和方法。这可以包括参考文献、视频教程或在线资源。

5.实验改进和安全性考虑：考虑到 ARP 欺骗攻击的潜在危害，实验可以包括更多的安全性措施和提醒，以确保学生在实验中不会对网络造成实际危害。

报告评分：

指导教师签字：

电子科技大学 计算机 学院

标准实验报告

(实验) 课程名称 信息对抗综合实验

电子科技大学教务处制表

电子科技大学

实 验 报 告

学生姓名：黄鑫 学 号：2021050901013 指导教师：汪小芬

实验地点：主楼 A2-413-1

实验时间：10.24

一、实验室名称：主楼 A2-413-1

二、实验项目名称：ARP 地址解析协议

三、实验学时：4

四、实验原理：

(1) ARP 的作用：ARP 的主要作用是将目标设备的网络地址（通常是 IP 地址）映射到其物理地址（通常是 MAC 地址）。这允许设备在局域网内正确地路由和传输数据包，因为它们需要知道目标设备的 MAC 地址以便进行直接通信。

(2) ARP 数据包类型：

- ARP 请求包：ARP 请求包用于查询目标 IP 地址对应的 MAC 地址。当一个设备需要与另一个设备通信，它会广播一个 ARP 请求包以获取目标设备的 MAC 地址。
- ARP 应答包：ARP 应答包用于回应 ARP 请求，提供目标 IP 地址对应的 MAC 地址。这是目标设备的响应，它包含了所需的 MAC 地址信息。

(3) ARP 缓存表：每台主机和路由器都会维护一个 ARP 缓存表，其中存储了已知设备的 IP 地址与 MAC 地址的映射关系。这个表可以包含静态和动态记录。静态记录是手动配置的，而动态记录是根据设备之间的通信动态生成的。

(4) 查看 ARP 缓存表：在 Windows 系统中，可以使用命令 "arp -a" 来查看 ARP 缓存表，这个表可以显示已知设备的 IP 地址和 MAC 地址的对应关系。

五、实验目的：
了解 SHA 密码加密原理、学习 SHA 散列暴力破解的过程

(5) ARP 的工作原理：ARP 工作的基本原理是通过广播 ARP 请求包来获取目标设备的 MAC 地址，然后将这些信息存储在 ARP 缓存表中，以便以后的通信。如果目标设备不在同一网络段，数据包需要通过网关进行中转，因此主机会首先检查 ARP 缓存表

中是否有网关的 MAC 地址，如果没有，它会发送 ARP 请求来获取网关的 MAC 地址。

(6) ARP 欺骗攻击：ARP 欺骗是一种非法攻击，利用 ARP 协议的漏洞来实施。攻击者可以欺骗网络中的设备，导致网络问题或窃取敏感信息。这种攻击可能会导致以下危害：

- 使同一网络段的其他用户无法正常上网。
- 攻击者可以嗅探和窃取通信数据。
- ARP 欺骗可以用于篡改信息或注入恶意内容。

(7) 检测 ARP 欺骗攻击：一些迹象可能表明存在 ARP 欺骗攻击，如网络频繁掉线、网速变慢、ARP 缓存表中 MAC 地址不匹配等。使用 Sniffer 软件等工具可以检测大量的 ARP reply 包，从而发现潜在的攻击。

(8) 防御 ARP 欺骗攻击：为了防御 ARP 欺骗攻击，可以采取以下措施：

- 使用 MAC 地址绑定，将每台计算机的 IP 地址与硬件地址一一对应，不可更改。
- 使用静态 ARP 缓存，手动更新缓存中的记录。
- 使用 ARP 服务器来响应其他机器的 ARP 广播，确保 ARP 服务器不受攻击。
- 使用 ARP 欺骗防护软件，如 ARP 防火墙，来检测并隔离攻击主机。

(9) ARP 请求或应答的分组格式：

| 32bits | | |
|-------------------|------|-------------------|
| 硬件类型 | | 协议类型 |
| 硬件长度 | 协议长度 | 操作 |
| 发送方 MAC (八位组 0-3) | | |
| 发送方 MAC (八位组 4-5) | | 发送方 IP |
| 发送方 IP | | 接收方 MAC (八位组 0-1) |
| 接收方 MAC (八位组 2-5) | | |
| 接受方 IP | | |

五、实验目的：

掌握 ARP 协议的作用和格式

六、实验内容：

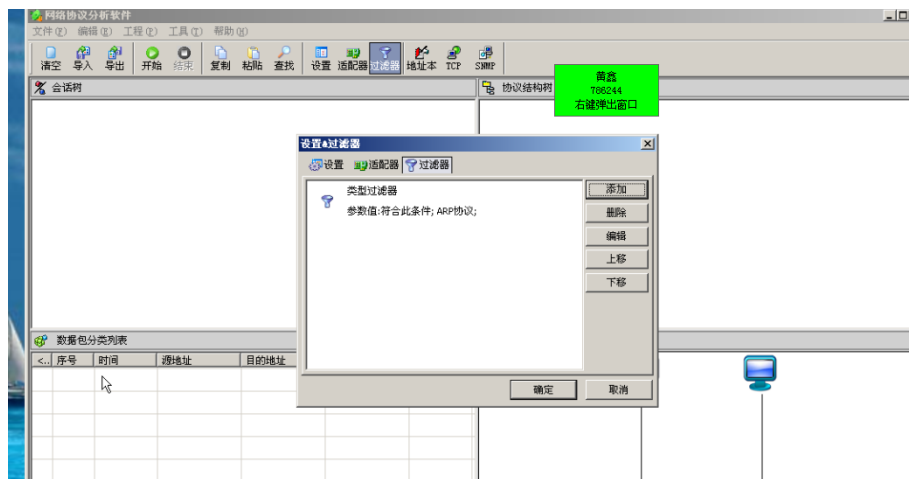
通过虚拟机实验实现 ARP 地址解析实验，掌握 ARP 协议的作用和格式。使用数据包发送器发送 ARP 数据包，并通过主机上的网络协议分析软件，捕获主机发送的 ARP 应答报文，并分析报文结构

七、实验器材（设备、元器件）：

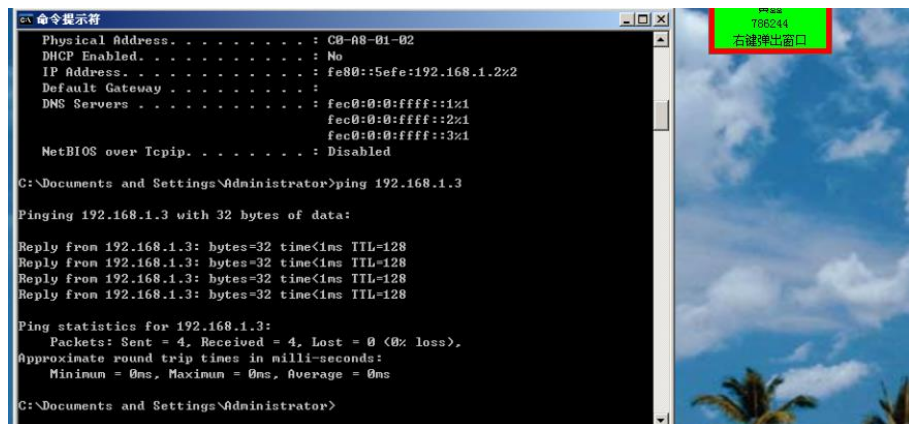
两台虚拟主机 A、B

八、实验步骤：

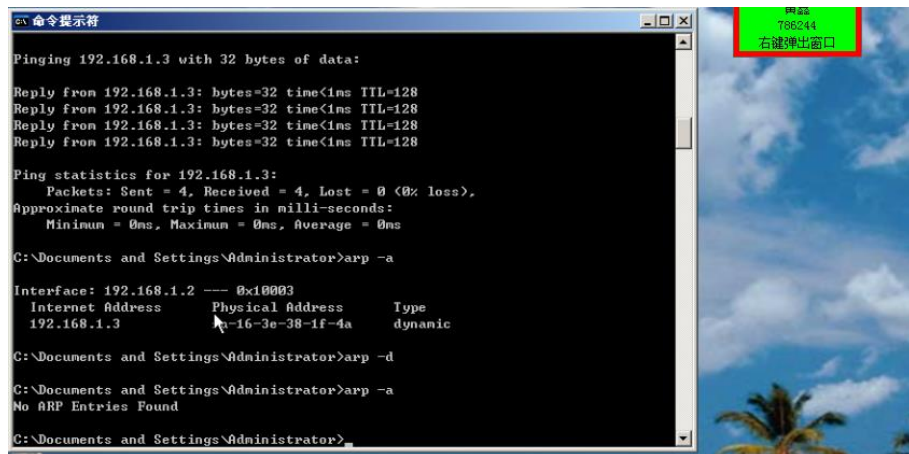
（1）打开主机 B192.168.1.3 上的“网络协议分析”软件，单击工具栏”过滤器“->”添加“->”类型过滤器“->”arp 协议“->”接受”->”设置参数”->”确定“，然后单击”开始“按钮，捕捉 arp 数据包。



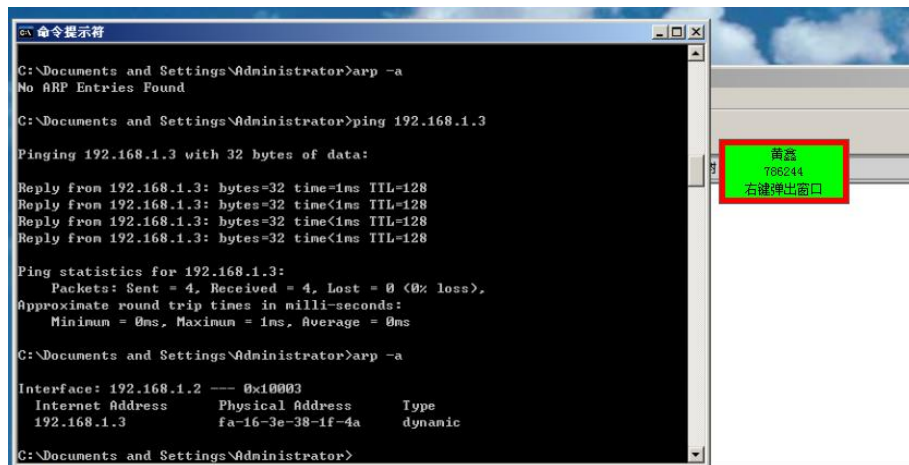
（2）在主机 A192.168.1.2 命令行窗口输入 ping 192.168.1.3。输入 arp -a 查看 ARP 缓存表。



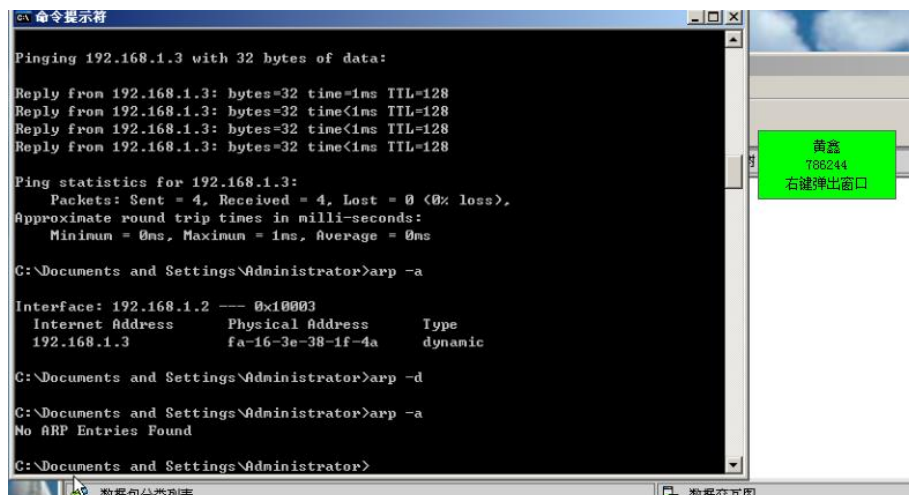
（3）在主机 A 输入命令 arp -d 删除 ARP 缓存表。



(4) 在主机 A 192.168.1.2 命令行窗口输入 ping 192.168.1.3。输入 arp -a 查看 ARP 缓存表。

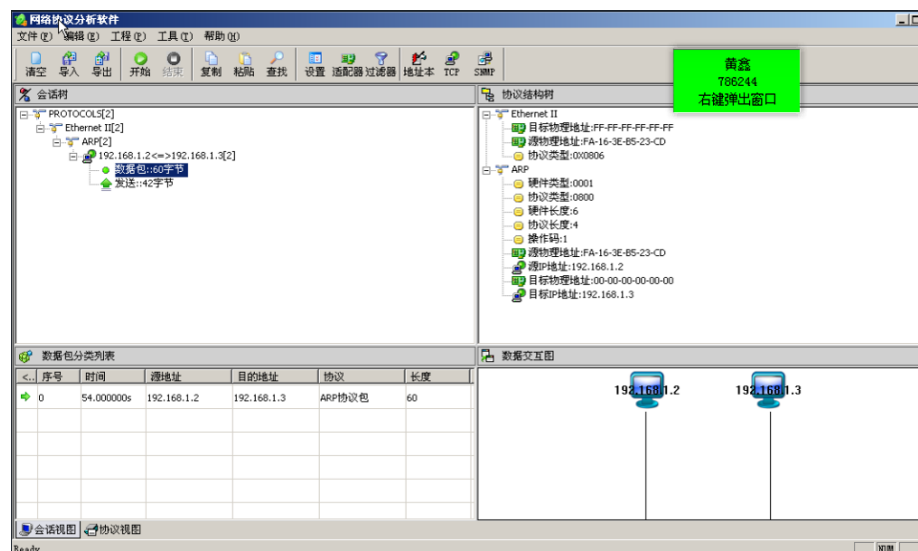


(5) 在主机 A 输入命令 arp -d 删除 ARP 缓存表

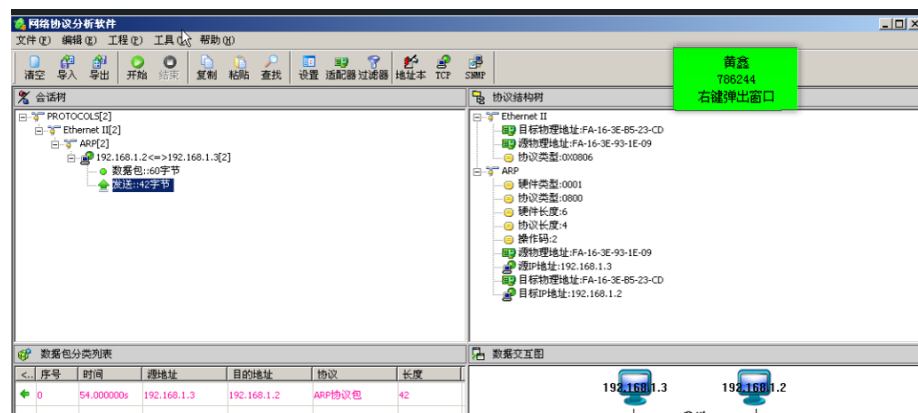


(6) 查看主机 B 192.168.1.3 上的网络协议分析软件，捕获到 ARP 请求报文，点击“结束”按钮。在 ARP 请求报文的数据帧头中，源物理地址为发送请求的主机地址为：A 主机实际 MAC 地址，目的物理地址是广播地址：

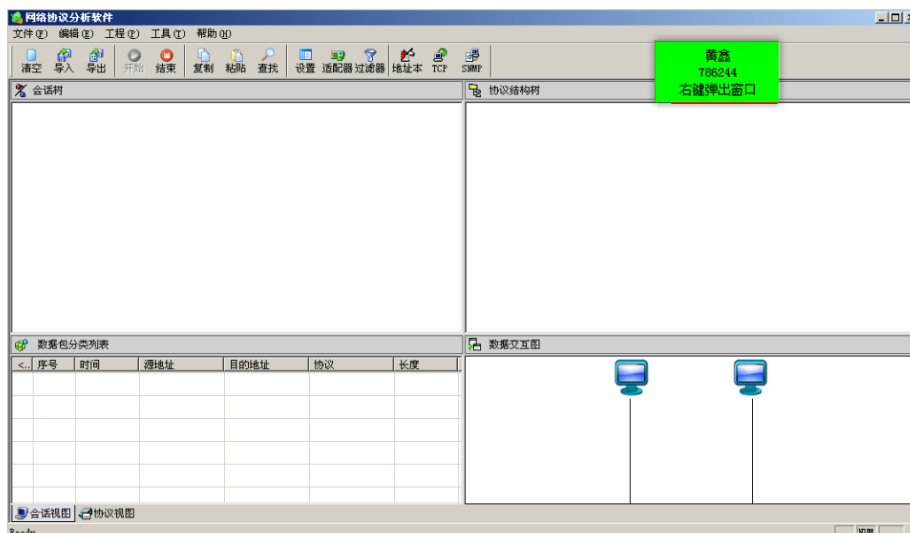
FF-FF-FF-FF-FF-FF，协议类型为 0800，表示上层协议为 IP 协议



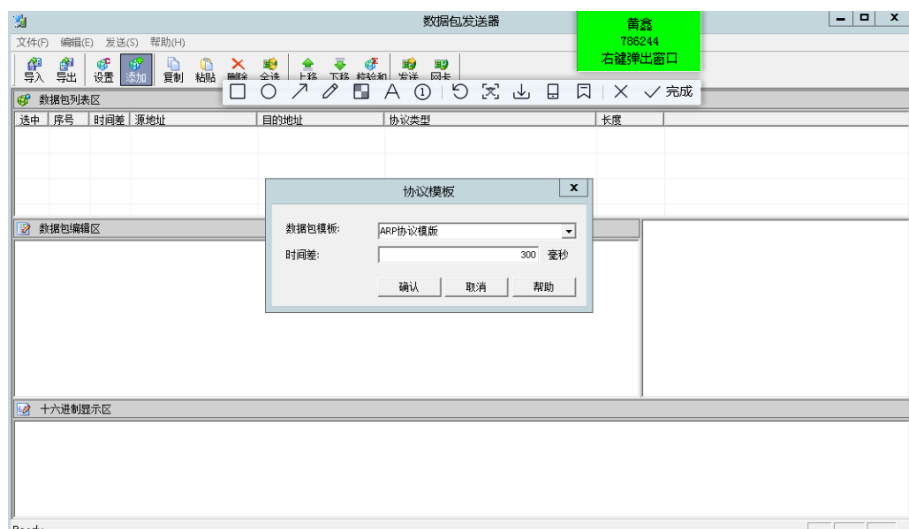
(7) 查看主机 B 192.168.1.3 上的网络协议分析软件，捕获到主机 B 发送的 ARP 应答报文。捕获的 ARP 应答报文，在 ARP 应答报文中的数据帧头中，源物理地址为主机 B 的物理地址：B 主机实际 MAC 地址，目的物理地址为发送 ARP 请求报文的主机 A 的物理地址：A 主机实际 MAC 地址，协议类型为 0806，表示上层协议为 ARP 协议



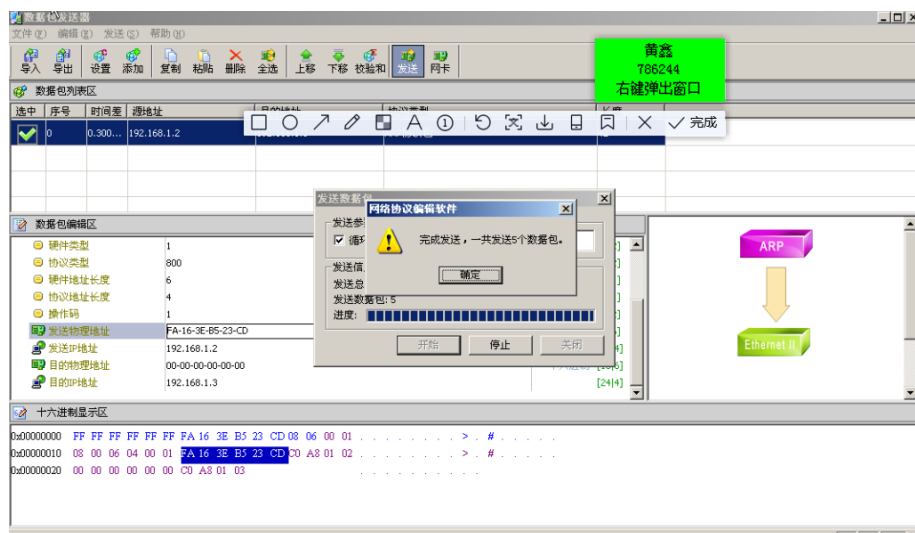
(8) 点击左上角“清空”按钮，清空现有报文。点击“开始”



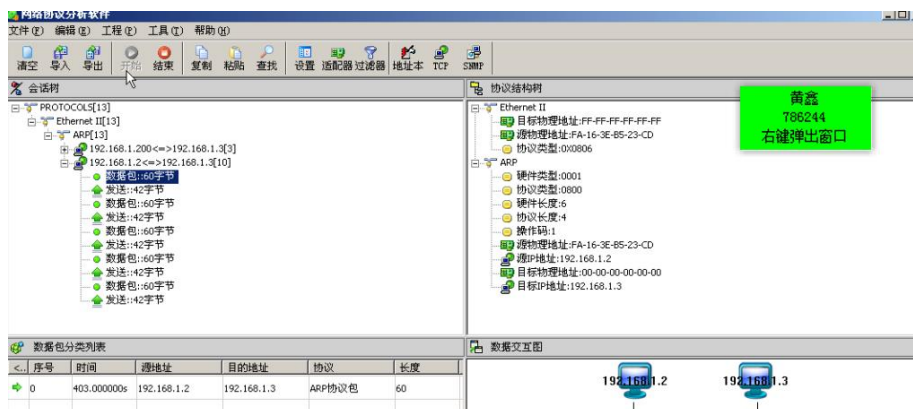
(9) 在主机 A192.168.1.2 上打开”数据包发送器”，单击工具栏“添加”按钮，选择“ARP 协议模板”，单击“确认”按钮，建立一个 ARP 数据包



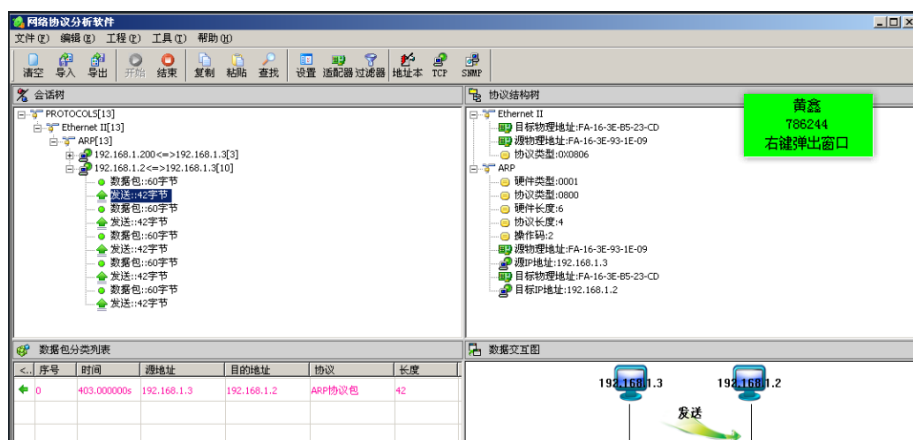
(10) 在数据包编辑区，设置 ARP 数据包的各项数值。设置源物理地址为主机 A192.168.1.2 的 MAC 地址，目的物理地址为“FF-FF-FF-FF-FF-FF”，即广播地址，在主机 B192.168.1.3 上,单击”开始”->”运行”->输入“cmd”->arp -d,清空 ARP 高速缓存，在主机 192.168.1.2 的数据包发送器上单击工具栏中“发送”按钮，选中“循环发送”->”5”->“开始”，发送 5 个 ARP 请求报文（先打开主机 B 上的网络协议分析软件，并单击菜单栏“开始”按钮，开始抓包）



(11) 主机 B 192.168.1.3 收到主机 A 的第一个数据包为 arp 请求数据包，目的 MAC 地址为广播地址，操作码值为 1（表示 arp 请求数据包）



(15) 在数据包分类列表中，单击第二个数据包。目的 MAC 地址为主机 A 的 MAC 地址，操作码值为 2（表示为 ARP 应答数据包），主机 B 发送一个 ARP 单播帧给主机 A，告诉主机 A 主机 B 的 MAC 地址



九、实验数据和结果分析：

在本次实验中，我们使用了数据包发送工具和网络协议分析工具，成功捕获了主机发出的 ARP 请求数据包和 ARP 应答数据包，并进行了详细分析。这些数据包的结构与 ARP 请求和应答的标准格式相符。

十、实验结论：

ARP 请求数据包包含了源 MAC 地址、源 IP 地址、目标 MAC 地址和目标 IP 地址等信息。这些请求数据包用于在局域网内查询目标主机的 MAC 地址。

ARP 应答数据包也包括了源 MAC 地址、源 IP 地址、目标 MAC 地址和目标 IP 地址等内容。这些应答数据包用于目标主机向请求主机发送 MAC 地址，从而完成地址解析过程。

ARP 协议采用广播方式进行通信，发送 ARP 请求的主机会将请求数据包广播到局域网内的所有主机，而目标主机则通过应答数据包来响应请求。

十一、总结和体会：

本次实验让我们深入理解了 ARP 协议的功能和数据包格式，并成功分析了 ARP 请求和应答数据包。这有助于我们更好地理解和应用地址解析过程，从而提高局域网中网络通信的效率和可靠性。

十二、对本实验过程和方法的改进建议：

除了验证数据包的格式之外，我们还可以对实验结果进行量化分析。例如，可以记录数据包的发送和接收时间，计算丢包率等指标，以评估 ARP 协议的性能和有效性。这将进一步完善实验方法，提供更全面的数据分析。

报告评分：

指导教师签字：

电子科技大学 计算机科学与工程
程（网络空间安全） 学院

标准实验报告

（实验）课程名称 信息对抗综合设计实验

电子科技大学

实验报告

学生姓名： 黄鑫 学号： 2021050901013 指导教师：汪小芬

实验地点： 主楼 A2-413-1

实验时间： 2023.10.24

一、实验室名称：主楼 A2-413-1

二、实验项目名称：网络欺骗实现中间人攻击实验-

三、实验学时： 4

四、实验原理：

(1) ARP 地址解析协议 (ARP)：ARP 是一个 TCP/IP 协议，用于将 IP 地址映射到物理 MAC 地址，以便在局域网中进行通信。主机通过发送 ARP 请求广播来获取目标 IP 地址对应的 MAC 地址，然后将其缓存以提高通信效率。

(2) ARP 协议缺陷：ARP 缓存是动态更新的，受到更新周期的限制，可能存在安全风险。ARP 请求是广播形式发送的，缺乏真实性验证，可能导致 ARP 欺骗攻击，使攻击者伪装成其他主机。

(3) DNS (域名系统)：DNS 用于将域名解析为 IP 地址，使互联网上的客户端能够访问网站和服务器。DNS 查询请求和应答数据包通过 ID 进行关联，以确保匹配。

(4) DNS 欺骗攻击原理：DNS 欺骗攻击依赖于攻击者的能力，通过 ARP 欺骗成为中间人，拦截目标主机与 DNS 服务器之间的通信。攻击者捕获 DNS 请求包，获取其中的 ID 序列号和 Port 信息。攻击者发送虚假的 DNS 请求包，伪造合法的 ID 和 Port，使客户端认为它是合法的 DNS 应答。客户端接收到虚假的 DNS 响应后，可能被重定向到攻击者指定的非法站点，从而威胁客户端的信息安全。

(5) 使用 Cain 进行 ARP 欺骗和中间人攻击：Cain 是一个 Windows 平台上的网络安全工具，可用于执行各种攻击，包括 ARP 欺骗和中间人攻击。ARP 欺骗是通过发送伪造的 ARP 请求来欺骗目标主机，将攻击者插入到通信路径中，以便拦截通信。一旦

成为中间人，攻击者可以执行 DNS 欺骗攻击，伪装成 DNS 服务器，篡改 DNS 响应，引导客户端访问恶意站点或者截取数据。

五、实验目的：

利用 arp 协议缺陷实现中间人攻击获取网络中传输的明文密码。利用中间人攻击实现 DNS 欺骗攻击

六、实验内容：

利用 ARP 欺骗原理进行中间人攻击实验

七、实验器材（设备、元器件）：

3 台 Win2003:

攻击机为 192.168.1.2

靶机 ip 分别为 192.168.1.3, 192.168.1.4,

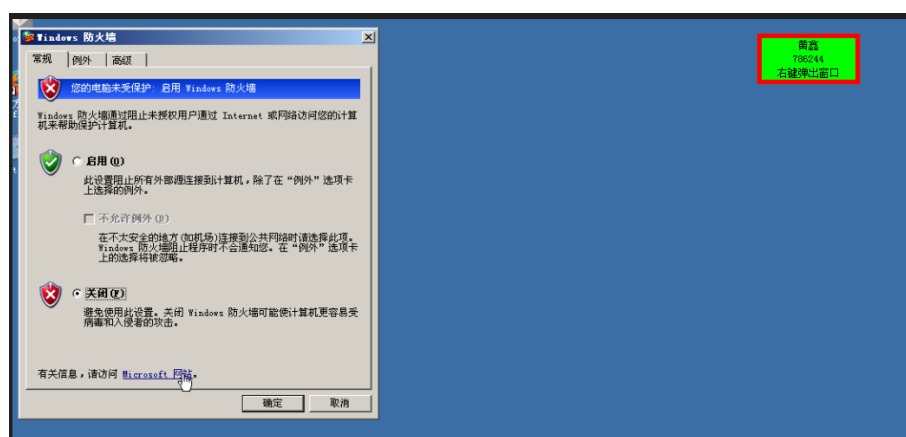
192.168.1.4 搭建了 ftp 服务器，账户为：administrator，密码为 Simplexue123。

192.168.1.4 配置了 dns 服务。

软件：cain

八、实验步骤：

(1) 由于环境原因需切换到 192.168.1.3 上，关闭系统防火墙。步骤：“开始”→“控制面板”→“Windows 防火墙”→“关闭”→“确定”。



(2) 更改 192.168.1.4 的中 FTP 设置: 点击“开始”→“管理工具”→“Internet 信息服务 (IIS) 管理器”→选择本地计算机中的“FTP 站点”→右键“FTP 站点”→选择“属性”→“安全账户”→取消勾选“允许匿名连接”→

Internet 信息...

文件(F) 编辑(E) 格式(O) 工具(T) 窗口(W) 帮助(H)

FTP 站点 安全帐户 消息 主目录 目录安全性

Internet 信息...

VIRUS2 (本地)

FTP 站点

应用程...

网站

Web 服...

允许匿名连接(A)

对匿名访问使用下列 Windows 用户帐户:

用户名(U): IUSR_VIRUS2 浏览(B)...

密码(P): *

☐ 只允许匿名连接(L)

确定 取消 应用(A) 帮助

地址 端口

未分配 * 21

病毒
786244
右键弹出窗口

File View Configure Tools Help

Decoders Network Sniffer Cracker Traceroute CCDR Wireless Query

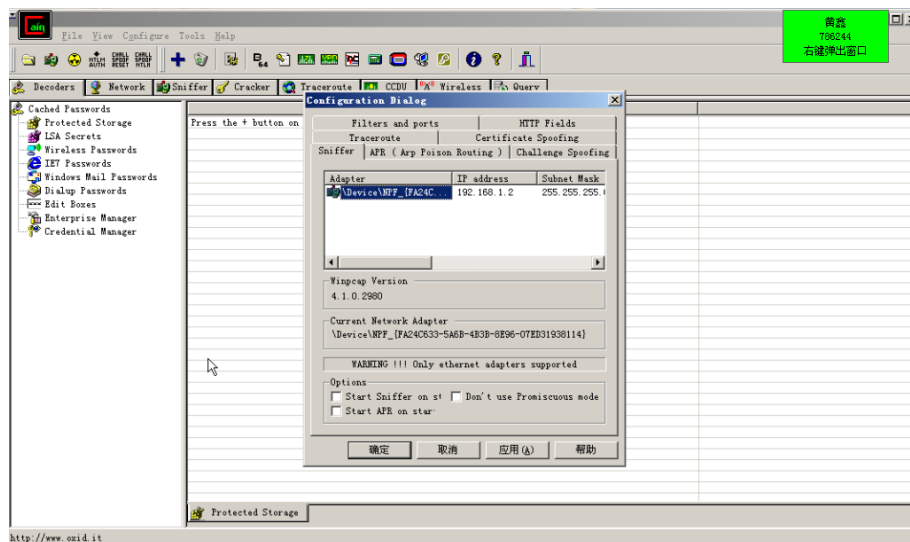
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
NET Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager

Press the + button on the toolbar to dump the Protected Storage

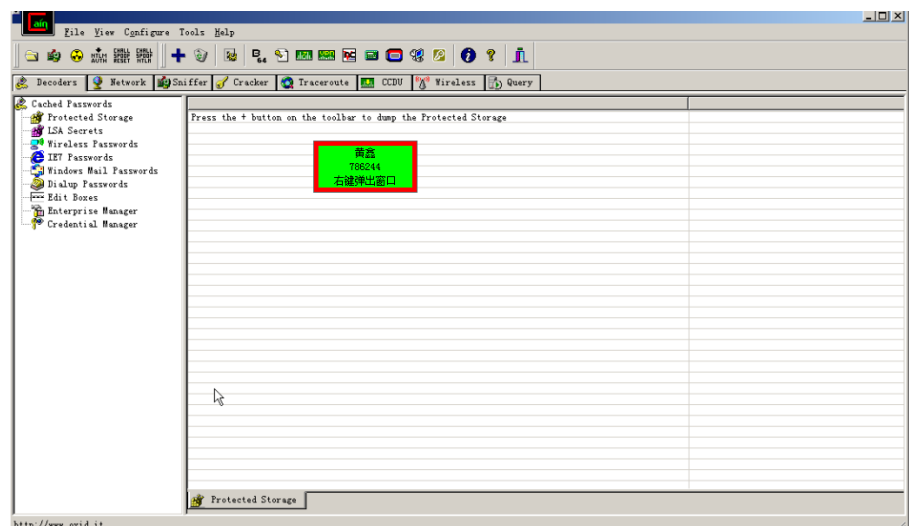
前送
706244
右鍵彈出窗口

Protected Storage

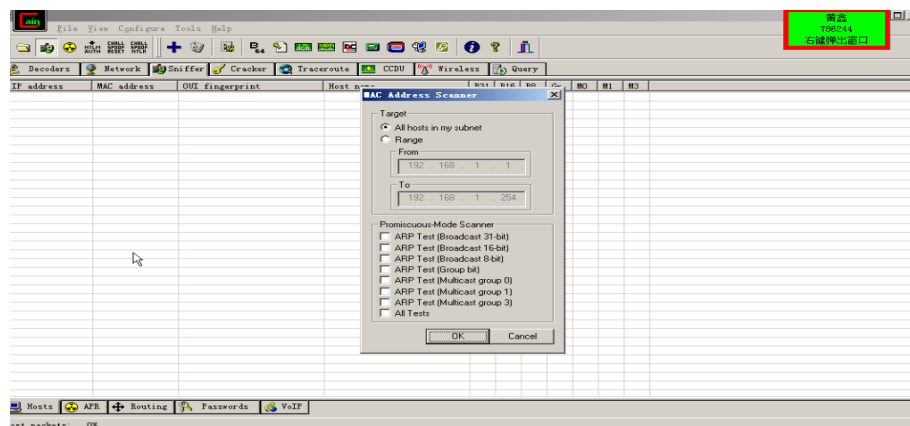
<http://www.oxid.it>



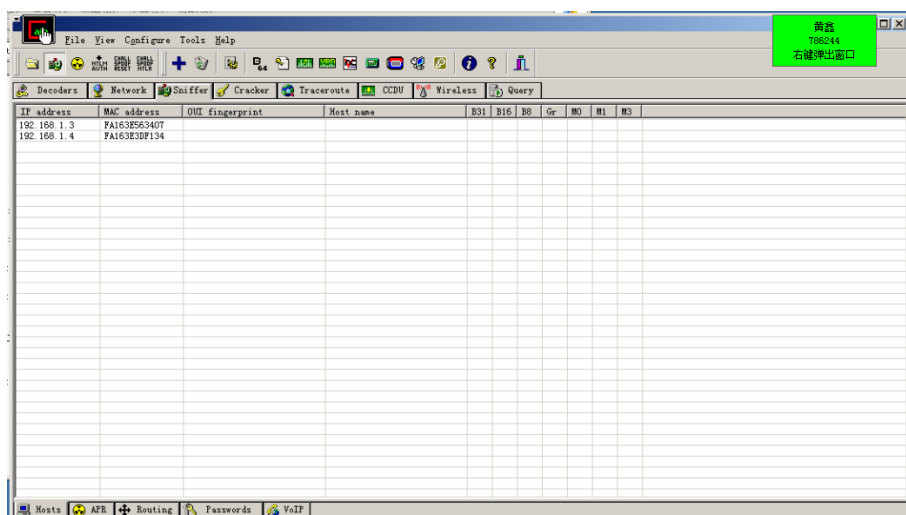
(5) 选择好网卡之后，单击 Start/Stop Sniffer 光标开启 Sniffer 功能，进入 Sniffer 选项卡，选择下方的 Hosts 选项，右击空白处，选择 Scan MAC Addresses，进入扫描。



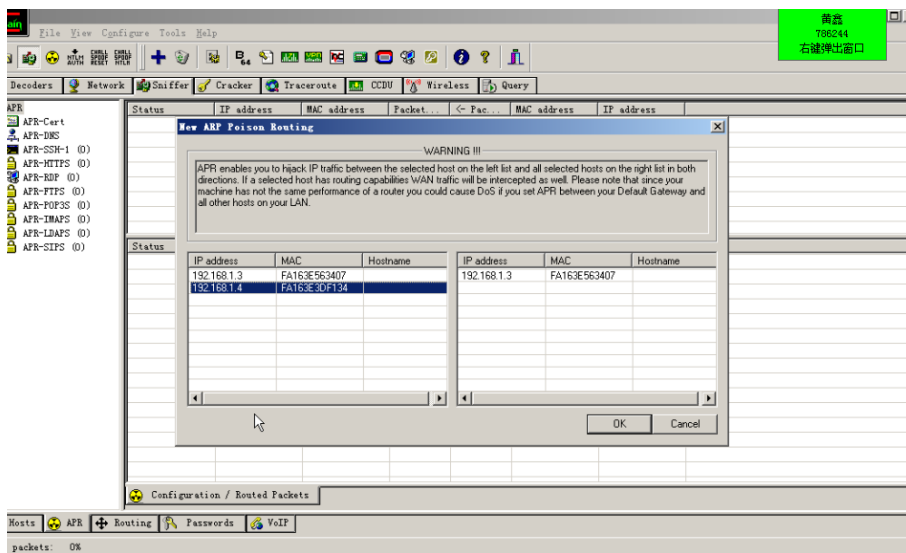
(6) 选择了 Scan MAC Addresses 后，选择扫描的网段，选择 All hosts in my subnet。单击 ok，进行扫描。



(7) 将本网段除了本机外的其他机器全部扫描出来了。可以看到 192.168.1.4 和 192.168.1.3 两个 ip 地址。如果扫出其他 ip 地址，将其删除。只留下 (192.168.1.3) 和 (192.168.1.4) 两个 ip 及其 mac 地址 (MAC 地址的值以实际显示为准)。

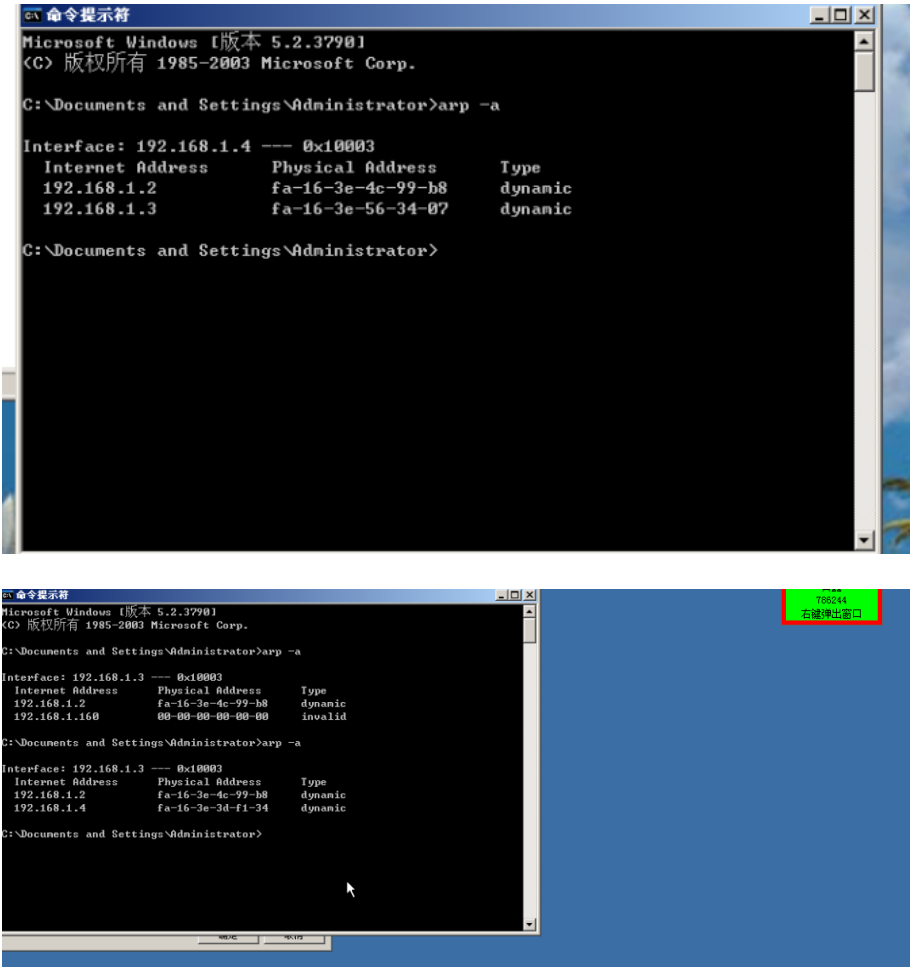


(8) 单击左下角“APR”标签，然后单击软件空白处，激活菜工具栏中的“+”按钮，然后单击“+”按钮。扫描出 mac 地址后，选择下方的 arp 选项，进入 arp 选项页面。单击 (+) 添加目标地址 192.168.1.4，选中 192.168.1.4 条目。单击 ok。

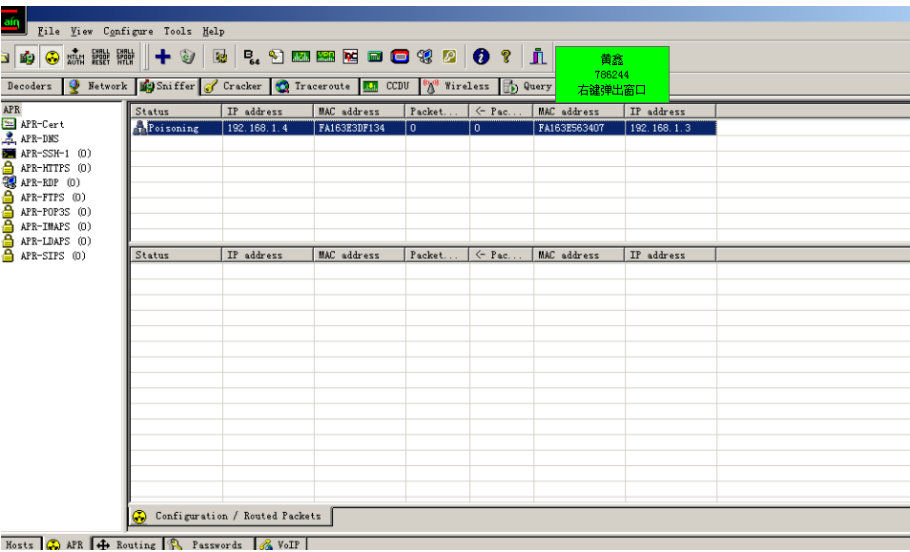


(9) 在 cmd 命令行模式下，使用 arp -a 命令查看本地缓冲中的项目。分别在 (192.168.1.3) 和 (192.168.1.4) 两台机器上查看。如果没有条目出现或条目显示不全，可以切换到对应的系统使用 ping 命令去 ping 对方的 ip 地址。

再使用 arp -a 就可以了，由于 mac 地址是唯一的，实验中的 mac 地址与文档中的截图中 mac 地址不一致，是正常的。



(10) 在主机 192.168.1.2 中，选中图示目标后，单击 (start/stop ARP) 按钮开启 arp。



(11) 开启 arp 后，再分别进入 192.168.1.3 和 192.168.1.4 的 cmd 中，使用 arp-a 命令查看。发现查看到的 192.168.1.3 和 192.168.1.4 的 MAC 地址发生了改变，其 MAC 地址变得与 192.168.1.2 的 MAC 地址一样，说明 arp 欺骗已经成功。

```
C:\WINDOWS\system32\cmd.exe
192.168.1.109      00-00-00-00-00-00      invalid

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

Interface: 192.168.1.3 --- 0x10003
Internet Address      Physical Address      Type
192.168.1.2           fa-16-3e-1c-a7-04     dynamic
192.168.1.4           fa-16-3e-6c-e3-f2     dynamic
192.168.1.123         00-00-00-00-00-00     invalid

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

Interface: 192.168.1.3 --- 0x10003
Internet Address      Physical Address      Type
192.168.1.2           fa-16-3e-1c-a7-04     dynamic
192.168.1.4           fa-16-3e-1c-a7-04     dynamic
192.168.1.145         00-00-00-00-00-00     invalid

C:\Documents and Settings\Administrator>_

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>arp -a

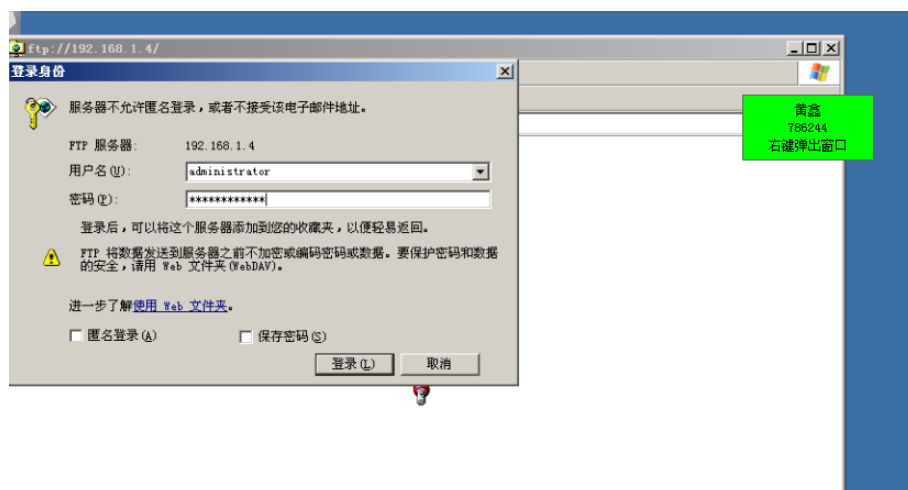
Interface: 192.168.1.4 --- 0x10003
Internet Address      Physical Address      Type
192.168.1.2           fa-16-3e-1c-a7-04     dynamic
192.168.1.3           fa-16-3e-fc-4b-e5     dynamic

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

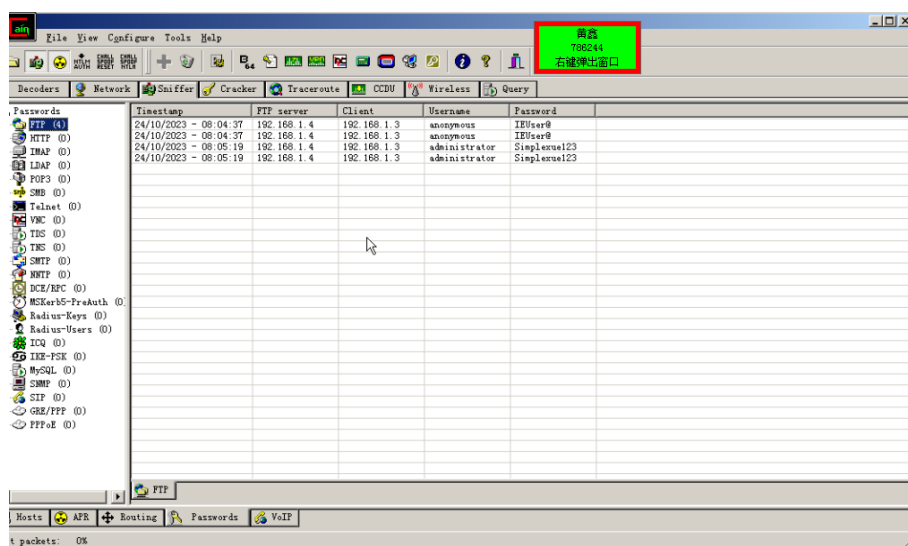
Interface: 192.168.1.4 --- 0x10003
Internet Address      Physical Address      Type
192.168.1.2           fa-16-3e-1c-a7-04     dynamic
192.168.1.3           fa-16-3e-1c-a7-04     dynamic

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

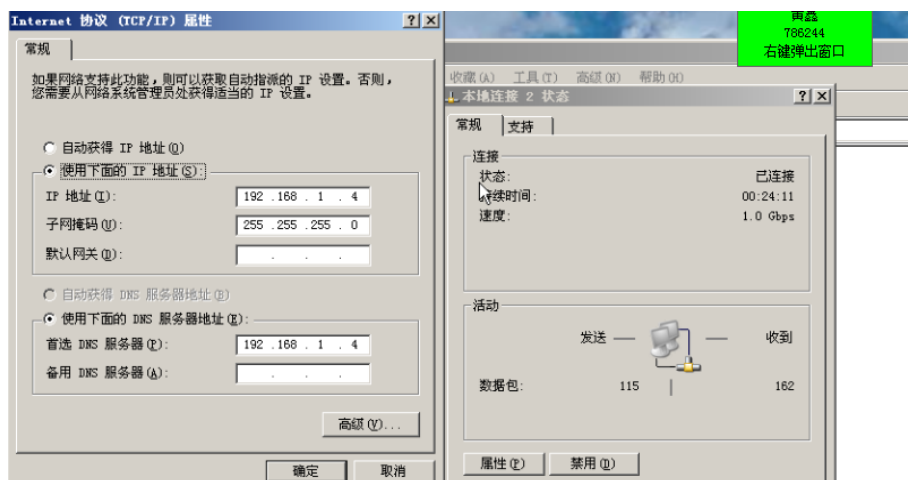
(12) 切换到 (192.168.1.3) 系统中，使用资源管理器连接在 192.168.1.4 上搭建的 ftp 服务器（打开任意一个文件夹，在地址栏输入 ftp://192.168.1.4）。输入正确的账户名密码 (administrator/Simplexue123)，单击登录。



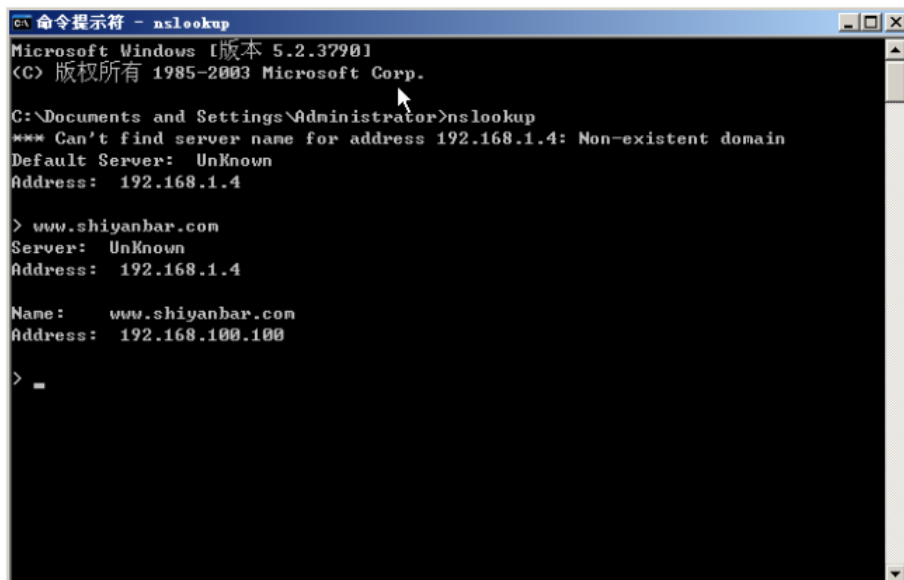
(13) 输入正确的用户名密码之后，即可进入 ftp 服务器中。再次切换到 (192.168.1.2) 系统中。选择 cain 下方的 Passwords 选项页面。选择左侧的 FTP 选项。即可看到刚刚在进入 ftp 时输入的 ftp 账户名和密码。如图 14 所示。



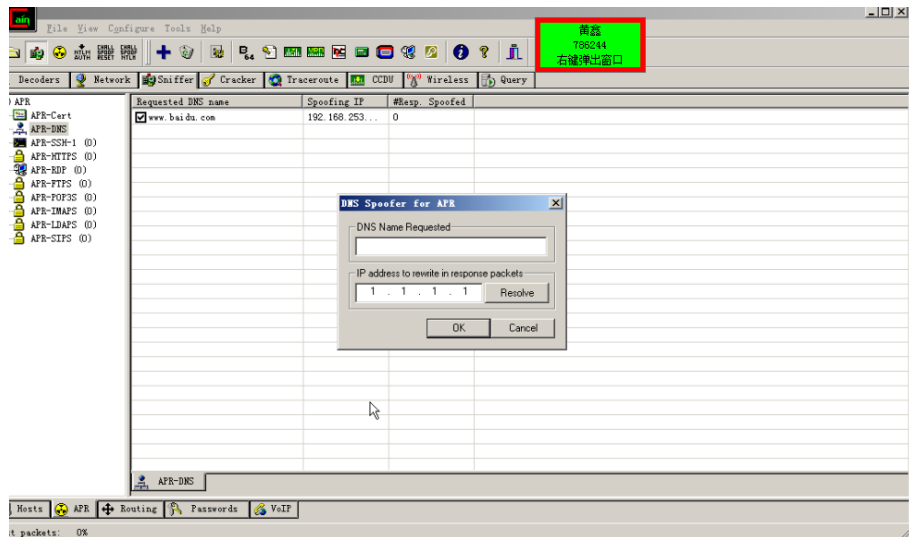
(14) 于环境限制，需要自行指定 dns。在 192.168.1.3 和 192.168.1.4 上都需要进行指定。将 dns 地址指向 192.168.1.4，右键“网上邻居”（或右键屏幕右下角小电脑图标，选择“打开网络连接”）—>选择“属性”—>双击“本地连接 2”—>“属性”—>“Internet 协议 (TCP/IP)” —>修改 DNS 服务器地址（若弹出窗口警告选择“否”即可）—>“确定”。



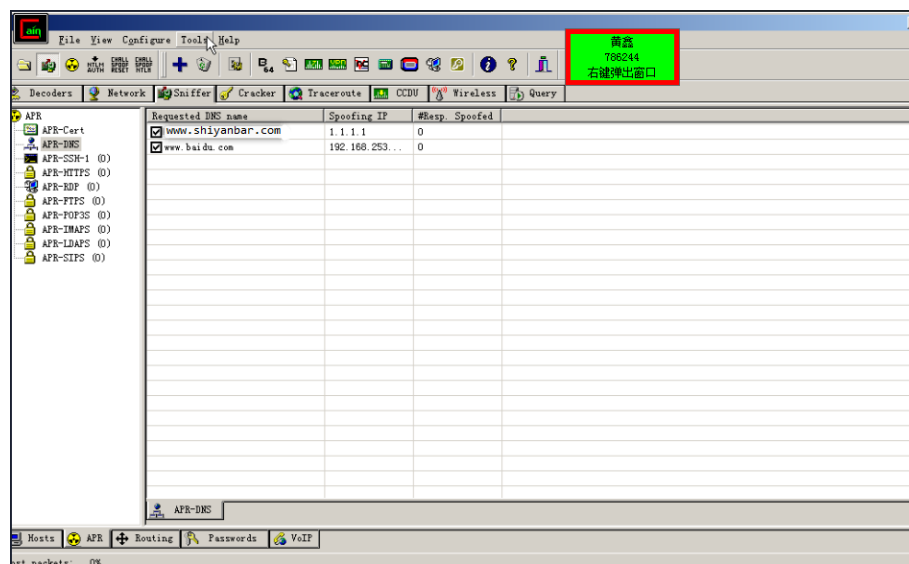
(15) 首先切换到 192.168.1.2 中进入 cain，单击 (start/stop ARP) 按钮关闭 arp。在切换到 192.168.1.3 中，进入 cmd 命令行使用 nslookup 查询。



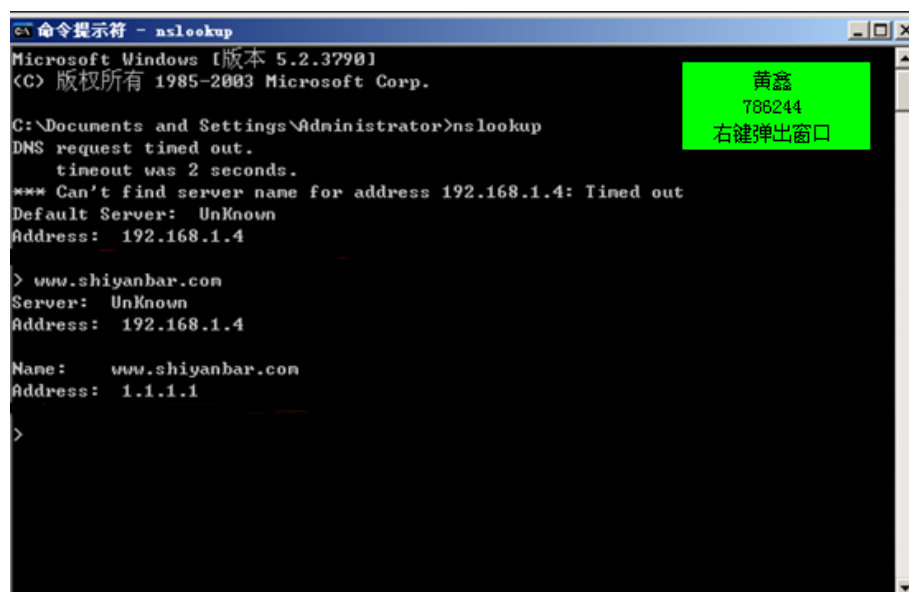
(16) 切换到 192.168.1.2 中，进入 cain 软件中，选择下方的 ARP 页面，选择左侧的 APR-DNS 选项。在单击上方的 (+) 添加一个目标，将网址解析的 ip 改为 1.1.1.1，单击 ok。单击 (start/stop ARP) 按钮开启 arp。



(17) 单击 ok 后页面可以看到刚刚设置的解析。



(18) 切换到 192.168.1.3 的 cmd 命令行模式中。



九、实验数据及结果分析：

www.shiyanbar.com 的 dns 解析已经被改变成为设定的 1.1.1.1，成功地做到了 dns 欺骗。

十、实验结论：

本实验成功演示了如何利用 ARP 欺骗攻击来实施中间人攻击，以获取网络传输的明文密码。通过修改目标主机的 ARP 缓存，攻击者能够中继通信并窃取敏感信息。此外，还演示了如何使用中间人攻击来进行 DNS 欺骗，改变 DNS 解析，将合法的域名解析到恶意 IP 地址上，威胁了网络安全。

十一、总结及心得体会：

通过这个实验，我学到了如何利用 ARP 和 DNS 协议的缺陷来进行网络攻击，特别是中间人攻击和 DNS 欺骗。我了解了 ARP 协议的工作原理，以及如何使用工具（如 Cain）来进行 ARP 欺骗，将攻击者插入到通信路径中。我还学习了如何修改目标主机的 ARP 缓存，以截获敏感信息。

在 DNS 欺骗攻击方面，我了解了如何伪造 DNS 响应，将合法的域名解析到恶意 IP 地址上，从而引导客户端访问恶意站点或截取数据。这个实验强调了网络安全的重要性，以及如何保护网络免受此类攻击的威胁。

十二、对本实验过程及方法、手段的改进建议：

在进行网络安全实验时，应格外小心，确保在合法的网络环境下进行，避免对未经授权的网络进行攻击。安全意识和法规遵守至关重要。

在实验中使用工具时，应遵循合法和伦理准则，不要滥用工具进行恶意攻击。网络攻击可能违反法律。

实验中的文档中提到的 IP 地址、MAC 地址、用户名和密码等敏感信息应进行模糊处理或者替换，以保护隐私和安全。

在进行网络攻击实验时，应严格遵循合法授权和道德规范，以避免潜在的法律和伦理问题。

报告评分：

指导教师签字：