9．重复上述过程，进行 http 连接捕捉。

在本实验中，我们可以很清晰地看到 IIS 服务器（FTP 和 HTTP）和 Windows 2000 之间的联系使攻击者有可能入侵整个系统。

实验 4-2：从邮件传输捕获用户名和密码

在本实验中，我们将学习如何从邮件传输过程中嗅探密码。具体操作如下：

1．为确定 SMTP 和 POP3 服务器的位置，使用已安装在 Windows 2000 操作系统里的 ping ProPack 对整个网络实施端口扫描，也可以使用其他的扫描工具。

2．记下扫描到的 SMTP 和 POP3 服务器的 IP 地址。

3．打开 Ethereal，对整个网络的数据包传输进行捕捉。

4．打开 E-mail 客户端，向你的搭档发送一个邮件，你的老师可能会提供另外的信息。

5．停止捕捉。

6．查看数据包以获得信息。你应该可以读到各种各样的信息，找出 E-mail 客户端和服务器之间用来进行身份认证的用户名和密码。

7．在 Ethereal 里，有一个简单的方法可找出密码，那就是把鼠标单击到一个 POP3 数据包，然后打开 **Tools|Follow TCP Stream**。你可以对任何 TCP 会话(HTTP、Telnet 等)进行该操作。Ethereal 将会重组这个会话并以用户名和密码结束。

实验 4-3：登录到 Windows 2000 服务器

在本实验中,我们将使用嗅探到的用户名和密码尝试登录到 Windows 2000 服务器上。

使用在前面实验 4-2 中的方法捕捉到网络中某一台主机的捕捉的用户名和密码，通过 Windows 资源管理器将网络驱动器映射到你搭档的计算机上。现在你已经渗透了一个网络服务器并得到对它的访问权限。它是中间人攻击的现实模仿。

单元概述

项目实践

在本单元中，我们学习了如何破解加密的口令以及使用嗅探工具获得未加密的口令。现在，从 www.ethereal.com 下载 Linux 下的 Ethereal 并用它对在网络上传输的未加密的口令进行审核。

小结

对网络和主机的渗透可以发生在许多不同的层面上。你已经了解到包括获得服务器的访问权在内的一些策略。在本课中，你学习了各种攻击手法和一些渗透攻击网络主机的程序和方法。你还学习了攻击者如何在一次攻击中综合运用不同的策略。例如，攻击者将拒绝服务攻击和 IP 欺骗技术结合起来攻击路由器。

完成本单元的学习后，你应该掌握：

- ✓ 了解网络渗透技术
- ✓ 理解攻击特征与审核技术之间的关系
- ✓ 了解易受攻击的服务和目标
- ✓ 掌握对路由器、数据库、Web 服务器、FTP 服务器、E-mail 服务器、名称服务的审核
- ✓ 掌握对系统漏洞的审核
- ✓ 掌握对缓冲区溢出的审核
- ✓ 掌握对拒绝服务攻击的审核

单元练习

1.什么是非法服务？

2.什么是攻击特征？

3.哪些是最容易受攻击的网络目标？

4.为什么 Web 服务器和 FTP 服务器特别容易受到攻击？

5.什么是 Web 页面篡改？

6.系统管理员和安全管理者如何才能避开拒绝服务攻击？

