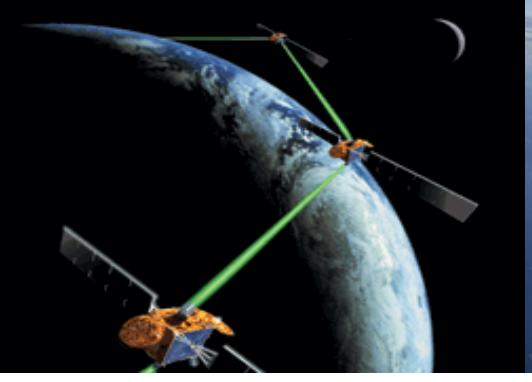
普通高等教育“十一五”国家级规划教材
教育部2011年精品教材

网络安全—技术与实践（第2版）

刘建伟 王育民 编著

清华大学出版社




课件制作人声明

- 本课件总共有17个文件，版权属于刘建伟所有，仅供选用此教材的教师和学生参考。
- 本课件严禁其他人员自行出版销售，或未经作者允许用作其他社会上的培训课程。
- 对于课件中出现的缺点和错误，欢迎读者提出宝贵意见，以便及时修订。

课件制作人：刘建伟

2016年3月28日

第3章 高层协议的安全性

一 电子邮件协议

二 Internet电话协议

三 消息传输协议

四 远程登录协议

五 简单网络管理协议

六 网络时间协议

七 信息服务

第3章 高层协议的安全性

一 电子邮件协议

二 Internet电话协议

三 消息传输协议

四 远程登录协议

五 简单网络管理协议

六 网络时间协议

七 信息服务

简单邮件传输协议—SMTP：端口号25

- SMTP 是一种TCP协议支持的、提供可靠且有效电子邮件传输的应用层协议，主要用于发送电子邮件，采用25号端口。
- SMTP最常用的实现方案是Sendmail。Sendmail有一个致命的缺陷：它常以root用户权限工作，违背了“最小信任”原则。SMTP后台程序不必以root权限运行。
- 黑客可以向邮件服务器发动拒绝服务攻击。要提高SMTP的安全性，就要启用SMTP认证。
- Sendmail配置非常复杂，常用的替代方案是Qmail。

邮局协议—POP3：端口号110

- 它是一个邮件接收协议，POP3允许用户从服务器上把邮件存储到本地主机（即自己的计算机）上，同时删除保存在邮件服务器上的邮件。
- POP3使用的端口号为110号端口。
- 该协议非常简单，甚至可以采用Perl脚本程序非常容易地实现，所以也非常不安全。
- 在访问邮件服务器时，POP3采用的口令以明文方式传送。而且在邮件服务器上，用户的口令以明文形式保存，这是非常不安全的。

多用途网间邮件扩充协议—MIME

- MIME在1992年应用于电子邮件系统，后来也应用于浏览器。服务器将MIME标志放入所传送的数据中，浏览器据此标志启用相应的插件来读取文件。
- MIME可以告诉浏览器哪些是MP3文件，哪些是Shock wave文件。
- 对MIME存在一种分段攻击。有一种MIME类型允许将单个电子邮件分段，客户端可重组这个邮件。如果分段做得巧妙，可以逃避邮件网关的病毒检测。
- MIME的其它安全风险包括：邮递可执行程序，或邮件自身含有危险的PostScript文件。它是传播蠕虫和病毒的主要途径。

消息访问协议IMAP4：端口号143

- 它提供了同POP3一样的邮件下载服务，在邮箱访问上有更加强大的功能。若一封邮件里含有５个附件，而只需要其中2个附件，则可以选择只下载这2个附件。
- 能够支持许多种安全的认证方法。在“挑战—响应”机制中，使用一个共享的秘密，这个秘密信息也必须存储在服务器上。通常将该秘密与域字符串进行杂凑运算，可消除某些口令的泄露的风险。
- 多个认证选项会提高IMAP遭受版本反转攻击（version-rollback attack）的可能性，该攻击迫使服务器使用较弱的认证或密码算法。

第3章 高层协议的安全性

一 电子邮件协议

二 Internet电话协议

三 消息传输协议

四 远程登录协议

五 简单网络管理协议

六 网络时间协议

七 信息服务

ITU的互联网电话协议—H.323

- H.323是标准的音频、视频、数据传输协议，是ITU-T制订的在各种网络上提供多媒体通信的系列协议H.32x的一部分。
- H.323协议被普遍认为是目前在分组网上支持语音、图像和数据业务最成熟的协议。
- 采用H.323协议，各个不同厂商的多媒体产品和应用可以进行互相操作，用户不必考虑兼容性问题。
- 该协议是许多VoIP应用的基础。随着近几年IP网络的发展及VoIP的普及，加速了H.323的推广应用。

IETF的会话启动协议—SIP

- SIP 协议是由IETF 提出并主持研究的一种基于应用层的多媒体会话控制协议，它是实现IMS (IP Multimedia Subsystem) 网络通信的关键技术。
- 因为SIP使用简便，功能强大，分布广泛，它在整个IETF内迅速得到了使用者的认同，特别应用于VoIP应用。
- SIP 协议采用文本形式表示消息的词法和语法，对文本形式的分析比较简单，使得SIP 会话容易遭受安全问题，包括欺骗、会话截获以及窃听等问题。

第3章 高层协议的安全性

简单文件传输协议—TFTP

- TFTP（Trivial File Transfer Protocol）是一个简单的基于UDP的文件传输协议。该协议中没有使用认证。
- 适当配置TFTP后台可以限制到1个或2个目录的文件传输，这两个目录通常为usr/local/boot和X11字库。
- 很多路由器（特别是低端的路由器）都使用TFTP来装载可执行的镜像或配置文件。
- 因为tftp实现非常的简单，很多设备升级内核都是通过tftp协议上传的。TFTP没有安全控制机制，因此它的安全问题应该多加考虑。

文件传输协议—FTP：端口号21

- 从服务器到客户机，或者从客户机到服务器，均可以用FTP打开一条数据通道。
- 该服务如果没有设防，FTP能够在短时间内泄露公司大量的重要文件。
- 该访问依赖于口令，能够被很容易地探测或猜测到；
- ftpd后台程序开始时以root用户权限运行，因为它要处理帐户的登录过程，包括口令处理。此缺陷可能会被黑客利用，从而带来安全问题。
- 在匿名FTP服务中，不法分子利用全球可读写的目录存储和发布盗版软件或其它违法的软件或数据。

网络文件系统协议—NFS：端口号2049

- 网络文件系统NFS（Network File System）最早是由SUN Microsystem公司开发的，它是许多工作站的重要组成部分。NFS是一个流行的基于TCP/IP网络的文件共享协议，提供了文件共享服务。

- NFS服务器的端口号由于它处于“无特权的”范围内，该端口常常被分配给那些普通的进程。因此，必须要对包过滤器防火墙进行配置，以阻止进入到2049端口的访问。

第3章 高层协议的安全性

远程登录协议—Telnet：端口号23

- Telnet提供了简单终端到某台主机的访问。主叫用户输入帐户名称和口令来进行登录。
- Telnet程序可能会泄露秘密信息，攻击者可以通过Sniffer记录用户名和口令组合，或者记录整个会话。
- 如果黑客掌握了使用TCP劫持工具的方法，就能够劫持TCP会话。Telnet会话是黑客通常的攻击目标。
- 目前出现了几种telnet的加密解决方案，它们分别为Stel、SSLtelnet、Stelnet、SSH等协议。

安全壳协议—SSH：端口号22

- 该协议设计的初衷是用来取代rlogin, rdisk, rsh和rpc。
- SSH 支持身份认证和数据加密，对所有传输的数据进行加密处理。
- 同时可以对传输数据进行压缩处理，这样就可以加快数据传输的速度。
- 它既可以代替Telnet作为安全的远程登录方式，又可以为FTP、POP等服务提供一个安全的“隧道”。

第3章 高层协议的安全性

一 电子邮件协议

二 Internet电话协议

三 消息传输协议

四 远程登录协议

五 简单网络管理协议

六 网络时间协议

七 信息服务

简单网络管理协议—SNMP

- 简单网络管理协议是互联网工程工作小组（IETF，Internet Engineering Task Force）定义的internet协议簇的一部分。
- SNMP是由IETF的研究小组为了解决Internet上的路由器管理问题而提出的。
- SNMP被设计成与协议无关，所以它可以在IP，IPX，AppleTalk，OSI以及其他传输协议上使用
- SNMP用来集中控制路由器、网桥及防火墙等设备。
- SNMP已经出到V3版本，其功能较以前已经大大地加强和改进了。

第3章 高层协议的安全性

一 电子邮件协议

二 Internet电话协议

三 消息传输协议

四 远程登录协议

五 简单网络管理协议

六 网络时间协议

七 信息服务

网络时间协议—NTP：端口号123

- 网络时间协议（NTP—Network Time Protocol）主要用于调整系统时钟与外部时间源同步。外部时间源可以是原子钟、天文台、卫星，也可以从Internet上公开的时间服务器获取。如果无法与Internet连接，也可以指定内部的主机作为时间服务器。
- NTP服务器自身可能成为攻击的目标，目的是试图改变攻击目标的正确时间。例如，攻击者可对基于时间的认证设备和协议发起攻击。如果黑客能够将机器的时钟重新设置成先前的某个值，他就能重发某个先前的认证字符串来实施重发攻击。

第3章 高层协议的安全性

一 电子邮件协议

二 Internet电话协议

三 消息传输协议

四 远程登录协议

五 简单网络管理协议

六 网络时间协议

七 信息服务

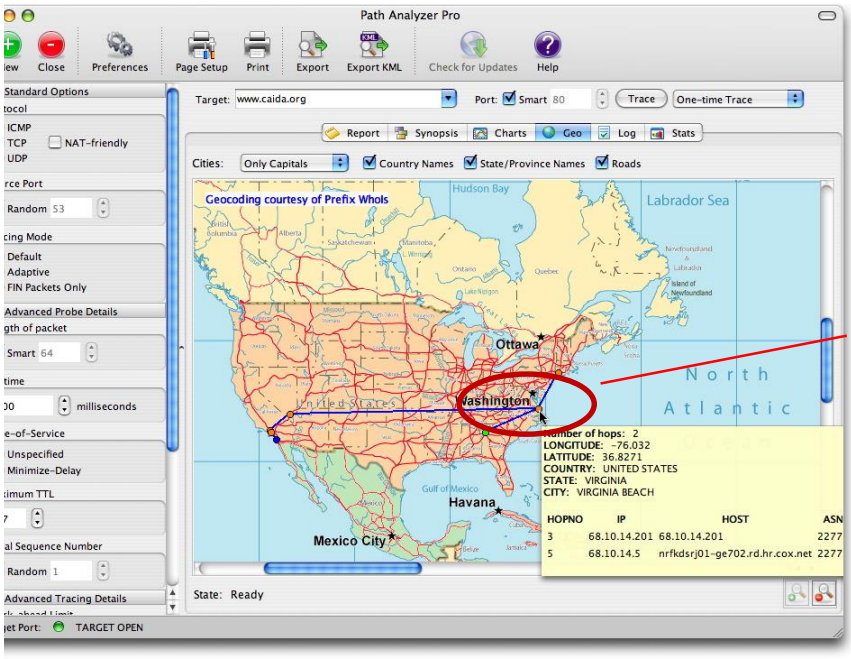
用户查询服务Finger

- Finger功能可以帮助用户查询系统中某一个用户的细节，如其全名、住址、电话号码、登录细节等。
- Finger协议可以被黑客用来调查并发现潜在的攻击目标。它所提供的信息，很可能被黑客用来实施口令猜测攻击。黑客还可以发现用户最近与哪个实体相连，这个实体可能成为潜在的攻击目标；黑客还可以发现用户最后使用的是哪个账号。
- Finger协议不可能在防火墙上运行，因此对于受防火墙保护的网站来说，它不是主要考虑的问题。对于防火墙内部的用户来说，可以使用其他方法获得大量同样的信息。但是，如果把一台机器暴露在防火墙外部的话，那么关闭Finger后台程序，或者对其施加某些限制才是明智之举。

数据库查询服务Whois

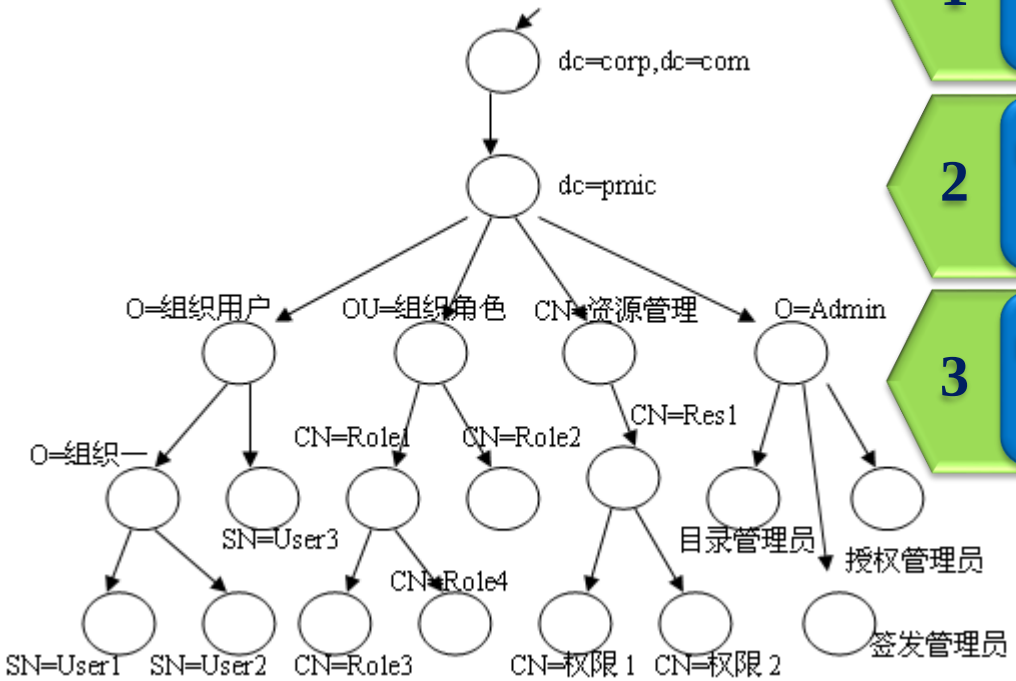
- **Whois**被用来查询域名所有者的身份及数据库中的其他信息。

- 在Whois标签中，在地址框中输入“sipb.mit.edu”，在query框中输入“Whois-Server”，单击Go按钮，得到最新的Whois服务器列表。只有在对象所属区域内的Whois服务器上查询，才有可能查到正确的结果。



轻量级目录访问协议—LDAP

- **LDAP**的全称是轻量级目录访问协议。
- 1993年7月，第一个LDAP规范**RFC1487**由密歇根大学开发成功。它在**功能性、数据表示、编码和传输方面都优于笨重的X.500目录访问协议**。



1. **信息量大小**：适合于存放相对小的信息量。
2. **信息类型**：目录通常是基于属性的信息。
3. **读写比**：目录适合于读操作更多的应用。
4. **搜寻能力**：自身包含的信息。
5. **标准访问**：目录是提供标准访问信息的好选择。

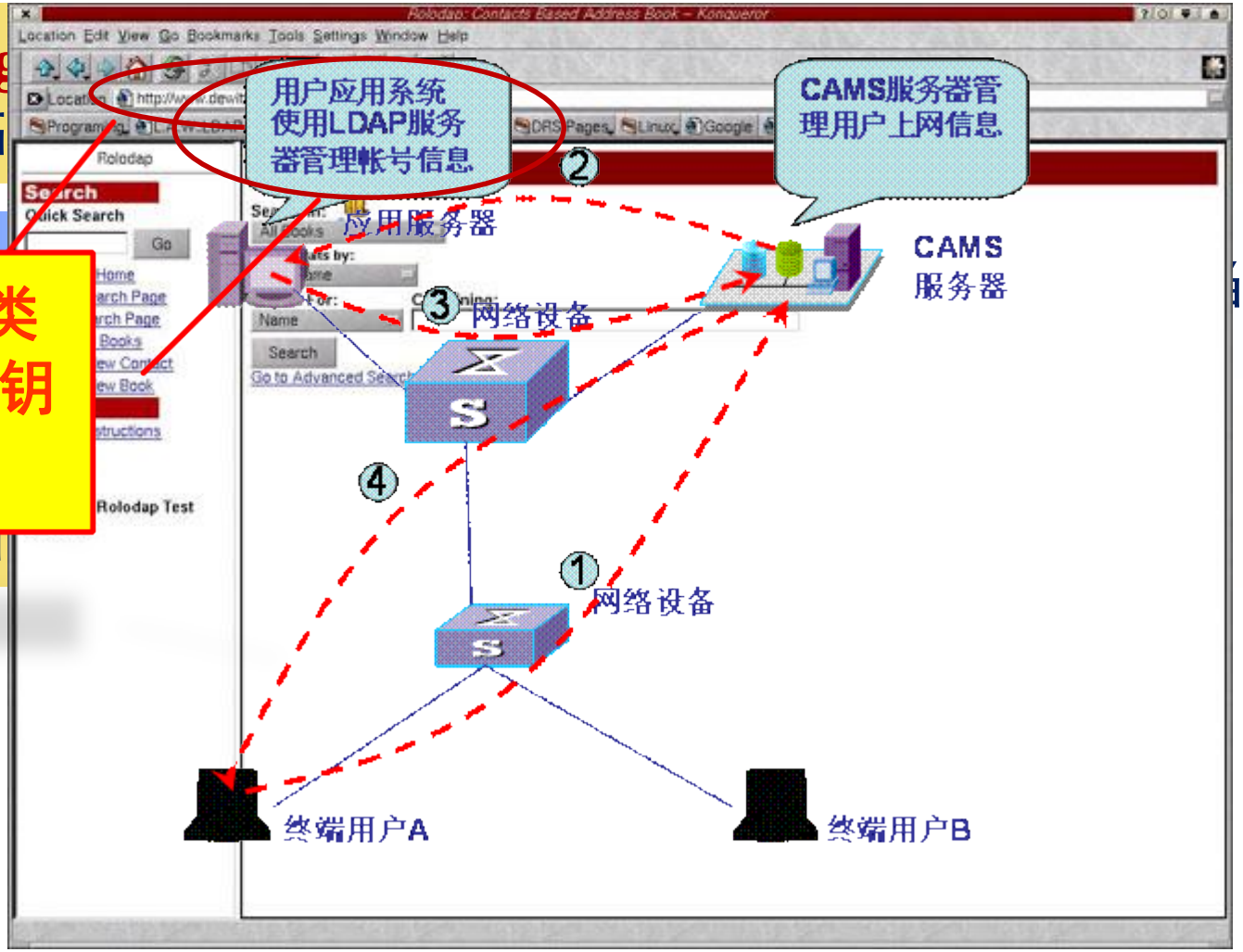
LDAP的安全性分析

- LDAP与Fing
息，因此面临

使用LDAP

使用LDAP提供类似目录数据和公钥证书的服务

选择一种恰当

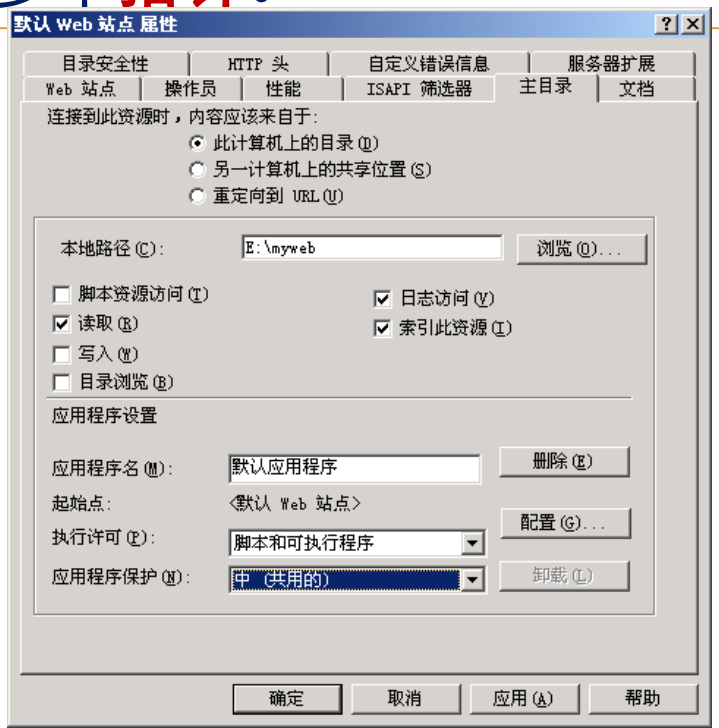


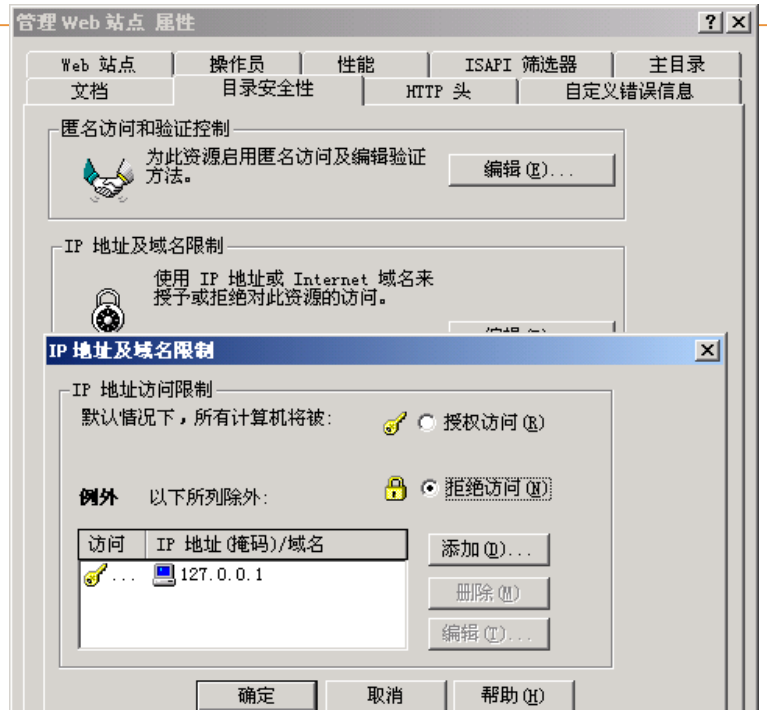
目前，LDAP的应用越来越广泛。

WWW服务

- WWW浏览器根据**URL**开头部分的名称来处理各种因特网服务。最常用的是**HTTP**服务，其次是**FTP**服务。

- 当主机连接某个服务器时，它会向服务器发送一个**查询**信息或信息**指针**，并接收服务器的响应。该响应可能是一个可以显示的**文件**，也可能是指向其他某个服务器的一个或多个**指针**。





WWW服务的安全性

- MIME编码可以被用来返回信息到客户端，返回的文档中包含一些**格式标签**将指定处理该文档的**程序**。这是**非常危险**的事情。
- 服务器**盲目**接收各种URL，也会面临某些**风险**。
- 返回指针中的端口是**电子邮件端口**，登录会话是一个**短脚本**。该脚本指示向某个人发送**垃圾邮件**，导致**严重安全问题**。
- 当服务器与匿名的FTP**共享一个目录树**时，将造成同样的危险。
- 服务器所面临的最大风险来自于**查询**。当运行由信息提供者编写的某一**脚本文件**时，就传承了该脚本的全部**风险**，并且攻击者可以由此定位语言编译器的**位置**。

应该尽可能让WWW服务器运行于受保护的环境中。

网络消息传输协议—NNTP

- 网络消息通常通过网络消息传输协议**NNTP**进行传输，采用的会话与SMTP相类似，接收和发送的消息条目通过**网关**来处理和转发。主要用于这种协议只用来阅读新闻。

缺点

1. 网络消息非常耗费**系统资源**。
2. 所有的这些程序可能会带来**安全漏洞**。
3. 很多的防火墙结构在设计时假设网关可能遭受攻击。
4. 若传递消息的NNTP存在漏洞，内部的消息主机会很危险。

优点

1. 可以了解邻居是谁，从而拒绝不友好的连接请求。

使用隧道策略，但仍有风险。

谢谢！