高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

网络安全技术原理与实践

主　编　黄晓芳
副主编　孙海峰　左旭辉

西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类“十三五”规划教材

应用型网络与信息安全工程技术人才培养系列教材

网络安全技术原理与实践

主　编　黄晓芳

副主编　孙海峰　左旭辉

参　编　李　波　覃仁超　彭安杰　刘志勤

西安电子科技大学出版社

内 容 简 介

本书共分为三篇(十二章)，系统地介绍了网络安全技术的基础知识体系，涵盖了从网络安全基础到网络攻击以及网络安全防御等方面的内容，并在大部分章节都配备有相关的实践案例和实验思考，引导读者增强对所学知识的融会贯通，有效提高其工程实践能力，帮助其掌握网络安全技术的实践技能。

本书重点突出，理论和实践相结合，通过精选的案例可使读者达到工程实践训练的目的。

本书是一本信息类专业工程实践教材，是依据信息安全类专业、物联网工程类专业的“工程实践教学大纲”的基本要求编写而成的，也可供相关领域专业人员学习参考。

图书在版编目(CIP)数据

网络安全技术原理与实践/黄晓芳主编. —西安：西安电子科技大学出版社，2018.1

ISBN 978-7-5606-4762-3

Ⅰ. ① 网… Ⅱ. ① 黄… Ⅲ. ① 计算机网络—网络安全 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字(2017)第 295156 号

策划编辑 李惠萍

责任编辑 杜 萍 雷鸿俊

出版发行 西安电子科技大学出版社(西安市太白南路 2 号)

电 话 (029)88242885 88201467 邮 编 710071

网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com

经 销 新华书店

印刷单位 陕西天意印务有限责任公司

版 次 2018 年 1 月第 1 版 2018 年 1 月第 1 次印刷

开 本 787 毫米×1092 毫米 1/16 印张 13.5

字 数 313 千字

印 数 1～3000 册

定 价 30.00 元

ISBN 978-7-5606-4762-3/TP

XDUP 5064001-1

*** 如有印装问题可调换 ***

中国电子教育学会高教分会推荐
高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

编审专家委员会名单

前　言

“网络安全技术原理与实践”是一门创新型的实践性课程，一般的实施周期为4～6学期。开设该课程的目的是让学生通过对网络安全技术从原理到实践的学习，熟悉和了解网络安全技术的基本原理、技术方法和相关工具以及相应的安全防范措施。通过对该课程的学习，可激发学生学习网络安全知识的兴趣，引导学生系统地思考网络安全方面的相关知识，培养和锻炼学生的攻防实践能力，使其熟练掌握相关攻防实践技能，从而能够解决网络安全方面的实际工程问题。

本书提供了各种网络与系统攻击技术的基本原理、实现方法和相关工具以及相应的安全防范技术措施，可以帮助学习者运用所学的知识安全地运营网络与信息系统，加强网络与信息系统的安全性能。

本书主要针对信息安全、网络工程等专业开发，共涵盖了三个方向的内容，即网络安全基础、网络攻击和网络安全防御，相关网络工程类专业也可选择性地使用本书内容。各阶段工程实践项目是参照构思、设计、实现、运作(Conceive、Design、Implement、Operate，CDIO)的工程教育理念，并依据信息安全专业、网络工程专业的“工程实践教学大纲”的基本要求，在对大量工程项目分析调研的基础上筛选确定的。项目包含了本专业主要核心课程的能力要求，实施项目的过程贯穿于整个专业培养的全过程。项目要求学生把所学的知识有机地与工程实践项目联系起来，学会以探究的方式获取知识和培养运用知识的能力，在CDIO的整体过程中使自己得到真实的工程实践能力的训练。

本书作者长期坚守科研和教学一线，拥有丰富的网络安全实践经验，在教材编写过程中坚持“在做中学”的教育理念，针对国内信息安全专业的发展需要，在相关章节引入了大量实践案例，以提高学生的实践水平，并增强其在网络安全技术方面的实践动手能力。

全书共分为三篇：网络安全基础篇一般是在学生学习完计算机网络等前修课程后，用以学习、了解网络安全基础知识；网络攻击篇介绍了网络安全攻击相关原理、技术及工具，主要供学生在网络安全攻击实践时使用；网络安全防御篇是让学生在理解并掌握一定攻击技术后，熟悉并掌握网络和信息系统安全防御与加固的技术与方法。

本书具有如下特点：

• 系统性强。本书从安全技术原理基础知识开始，介绍其技术方法、工具使用，通过实例展示与防御技术的剖析，让学生建立起网络安全技术从原理到实践的系统的知识框架。

• 提升实践能力。本书通过实际案例讲解、实用工具介绍，引导学生在掌握网络安全技术知识的基础上，通过实际动手实战，熟悉和理解网络安全技术方法，并能在实际环境中应用。

• 通俗易懂。本书在写作过程中，充分考虑到各层次读者的水平，以浅显的语言描述了相对深奥的计算机专业知识，语言通俗易懂，适合各层次学生和专业人士选用。

由于编者水平有限，书中难免存在不妥和疏漏之处，我们真诚期待各位专家及读者批评指正。

编　者

2017 年 9 月

目　录

第一篇　网络安全基础

第二篇 网络攻击

第三篇　网络安全防御

第一篇

网络安全基础

第一章　网络安全概论

网络安全一般是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断[1]。通常，网络安全主要包含以下五个基本目标：

(1) 保密性：确保网络中受保护的信息仅供那些已获授权的用户或实体访问，信息不被泄漏或呈现给非授权用户或实体，或者即便数据被截获，其所表达的信息也不被非授权者所理解。

(2) 完整性：确保网络中受保护的网络信息未经授权不能进行更改的特性，即受保护的网络信息在传输或者存储过程中不被蓄意删除、恶意修改、伪造以及丢失。

(3) 可用性：指网络系统可被授权实体访问并按照需求使用的特性，即系统能够被授权使用者正常使用，确保合法用户不会无缘无故地被拒绝访问信息或网络资源，是网络系统面向用户的安全性能。

(4) 可控性：确保信息传播者对信息的传播及内容具有控制能力。

(5) 可审查性：确保信息传播出现安全问题时可以提供相应的证明和解决手段。

为了保障这些基本安全目标，网络管理员需要有明确的安全策略，并且通过实施一系列的安全措施来确保安全策略所描述的目标能够实现。

1.1　网络安全的定义

网络安全主要是指网络上的信息安全，包括物理安全、逻辑安全、操作系统安全和网络数据传输安全。

1．物理安全

物理是指用来保护计算机硬件和存储介质的装置和工作程序。物理安全包括防盗、防火、防静电、防雷击和防电磁泄漏等内容。计算机如果被盗，尤其是硬盘被窃，信息丢失所造成的损失可能远远超过计算机硬件本身的价值，因此，防盗是物理安全的重要一环。由于电气设备和线路过载、短路、接触不良等原因可引起电打火而导致火灾，操作人员乱扔烟头、操作不慎也可导致火灾，此外，人为故意纵火或者外部火灾蔓延也可导致机房火灾。一旦发生火灾，后果极其严重，所以平时尤其要注意防火。静电是由物体间相互摩擦、接触产生的，计算机显示器也会产生很强的静电。静电产生后，如果未能释放而留在物体内部，可能使大规模电路损坏，这种损坏通常在不知不觉中造成。保持适当的湿度有助于防静电。防雷击主要是根据电气、微电子设备的不同功能及不同受保护程序和所属保护层确定防护要点，作分类保护，也可根据雷电和操作瞬间过电压危害的可能通道，从电源线到数据通信线路进行多级层保护。屏蔽是防电磁泄漏的有效措施，其主要有电屏蔽、磁屏

蔽和电磁蔽三种类型。

2．逻辑安全

计算机的逻辑安全需要用口令字、文件许可、加密、检查日志等方法来实现。防止黑客入侵主要依赖于计算机的逻辑安全，可以通过以下措施来加强计算机的逻辑安全：

(1) 限制登录的次数，对试探操作加上时间限制；

(2) 把重要的文档、程序和文件加密；

(3) 限制存取非本用户自己的文件，除非得到明确的授权；

(4) 跟踪可疑的、未授权的存取企图等。

3．操作系统安全

操作系统是计算机中最基本、最重要的软件，同一计算机可以安装几种不同的操作系统。如果计算机需要提供给许多人使用，操作系统必须能区分用户，防止他们相互干扰。一些安全性高、功能较强的操作系统可以为计算机的每个用户分配账户，不同账户有不同的权限，操作系统不允许一个用户修改由另一个账户产生的数据。

4．网络数据传输安全

网络数据传输安全主要是保护数据在网络信息系统中传输、交换和存储的保密性、完整性、真实性、可靠性、可用性和不可抵赖性等。加密技术是数据传输安全的核心，它通过加密算法将数据从明文加密为密文并进行通信，密文即使被黑客截取也很难被破译，然后通过对应解密技术解密密文，还原明文。目前，国际上通用的加密方法主要有对称加密和非对称加密。不同的加密方法有不同的特点，在数据传输安全性要求比较高的网络系统中加密方法得到了普遍采用，如电子商务、邮件传输等方面。

1.2　网络常见的安全威胁

随着网络的普及，网络应用已经无处不在，但是网络安全事件也层出不穷。影响计算机网络安全的因素很多，大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。在影响计算机网络安全的因素中，有些因素可能是有意的，也可能是无意的。可能是人为的，也可能是非人为的。可能是外来黑客对网络系统资源的非法使用。归结起来，针对网络安全的威胁主要有下述几种[2]。

(1) 人为的无意失误。如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享等都会给网络安全带来威胁。

(2) 人为的恶意攻击。这是计算机网络所面临的最大威胁，敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一种是被动攻击，它是在不影响网络正常工作的情况下，进行信息截获、密码窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。

(3) 网络软件的漏洞和“后门”。网络软件不可能是百分之百无缺陷和无漏洞的，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标，黑客攻入网络内部很大部分是因为安全措施

不完善所招致的苦果。另外，还有一些软件的“后门”是软件公司的设计编程人员为了自便而设置的，一般不为外人所知，但是一旦“后门”洞开，其造成的后果将不堪设想。

针对具体的网络攻击事件，目前比较常见的攻击主要包括恶意代码攻击、网络协议攻击、拒绝服务攻击、Web 攻击等。

1．恶意代码攻击

恶意代码是计算机按照攻击者意图执行以达到恶意目的的指令集。恶意代码根据其执行方式、传播方式和对攻击目标的影响分为木马程序、僵尸网络、计算机病毒、蠕虫等[3]。

1) 木马(Trojan)程序

RFC 1244 节点安全手册中给出的木马程序定义为：特洛伊木马程序是这样一种程序，它提供了一些有用的或仅仅是有意思的功能，但是通常要做一些用户不希望的事，诸如在你不了解的情况下拷贝文件或窃取你的密码[4]。

木马程序一般由服务器和控制器两部分组成。如果某台计算机“中了”木马，就意味着该计算机被安装了木马服务器程序，那么拥有控制器程序的人就可以通过网络控制该台计算机，所有存储在该计算机上的各种文件、程序以及使用的账号、密码等就被人完全控制。典型的木马工作原理是：当服务器端在目标计算机上被执行后，木马打开一个默认的端口进行监听，当客户端向服务器端提出连接请求时，服务器上的相应程序就会自动运行来应答客户端的请求。当服务器端程序与客户端建立连接后，由客户端发出指令，服务器在计算机中执行这些指令，并将数据传送到客户端，以达到控制主机的目的。

2) 僵尸网络(Botnet)

僵尸网络是指可被攻击者远程控制的被攻陷主机所组成的网络。僵尸网络与其他攻击方式最大的区别特性在于攻击者和僵尸程序之间存在一对多的控制关系。虽然僵尸网络使用了其他形态恶意代码所利用的方法进行传播，如远程攻击软件漏洞、社会工程学方法等，但其定义特性在于对控制与命令通道的使用。

Botnet 的工作机制主要是：首先，攻击者通过各种传播方式使得目标主机感染僵尸程序；其次，僵尸程序以特定格式随机产生的用户名和昵称尝试加入指定的通道命令与控制服务器；接着，攻击者普遍使用动态域名服务将僵尸程序连接的域名映射到其所控制的多台服务器上，从而避免由于单一服务器被摧毁后导致整个僵尸网络瘫痪的情况；然后，僵尸程序加入到攻击者私有的协议命令与控制信道中，加入信道的大量僵尸程序监听控制指令；最后，攻击者登录并加入到协议命令与控制信道中，通过认证后，向僵尸网络发出信息窃取、僵尸主机控制和攻击指令，僵尸程序接受指令，并调用对应模块执行指令，从而完成攻击者的攻击目标。其中，攻击的传播过程主要有以下五种传播形式：

(1) 攻击漏洞：通过主动攻击系统漏洞获得访问权，并在 Shellcode 执行僵尸程序，注入代码，这些漏洞多数都是缓存区溢出漏洞。

(2) 邮件携带：据有关统计资料显示，7%的垃圾邮件含蠕虫。

(3) 即时消息通讯：很多 Bot 程序可以通过即时消息进行传播。2005 年，性感鸡(Worm.MSNLoveme.b)的爆发就是通过 MSN 消息传播的。

(4) 恶意网站脚本：攻击者对有漏洞的服务器挂马或者是直接建立一个恶意服务器，当用户访问了带有恶意代码的网页后，其主机则很容易感染上恶意代码。

(5) 伪装软件：很多 Bot 程序被夹杂在 P2P 共享文件、局域网内共享文件、免费软件

或共享软件中，一旦下载并且打开了这些文件，则会立即感染 Bot 程序。

攻击程序在攻陷主机时，通常是随即将 Bot 程序植入被攻陷的主机，或者让被攻陷的主机自己去指定的地方下载。感染后的主机就会加入 Botnet，不同类型的 Bot 主机加入 Botnet 的方式也不同，下面以基于 IRC(Internet Relay Chat)协议的 Bot 为例，介绍僵尸主机加入 Botnet 的过程。首先，了解一下 IRC 协议的具体含义，IRC 协议是互联网早期就广泛使用的实时网络聊天协议，它使得世界各地的互联网使用者能够加入到聊天频道中进行基于文本的实时讨论。由于 IRC 协议提供了一种简单、低延迟、匿名的实时通信方式，通常也被黑客普遍使用于相互间的远程交流，因此在僵尸网络发展初期，IRC 协议自然成为了构建一对多命令与控制信道的主流协议。具体过程如下：

(1) 如果 Bot 中有域名，则先解析域名，通常采用动态域名。

(2) Bot 主机与 IRC 服务器建立 TCP 连接。为增强安全性，有的 IRC 服务器设置了连接密码，连接密码在 TCP 三次握手后通过 pass 命令发送。

(3) Bot 主机与 IRC 服务器发送 nick 和 user 命令。nick 通常有一个固定的前缀，如 CHN!2345、[Nt]-15120、ph2-1234，前缀通常为国家简称或操作系统版本等。

(4) 加入预定义的频道。频道名一般硬编码在 Bot 体内，为增强安全性，有的控制者为频道设定了密码。CNCERT/CC 的监测数据表明，规模较大(控制 1 万台以上计算机)的 Botnet 通常设置了频道密码，但设置服务器连接密码的 Botnet 还在少数。

控制流程中，控制程序必须保持对僵尸主机的控制，才能利用它们完成预订的任务目标。下面依然以 IRC Bot 为例，简单描述一下控制主机是如何控制 Bot 主机的。具体过程如下：

(1) 攻击者或者 Botnet 的主人建立控制主机。大多数控制主机建立在公共的 IRC 服务上，这样做是为了将控制频道做得隐蔽一些，也有少数控制主机是攻击者自己单独建立的。

(2) Bot 主机主动连接 IRC 服务器，加入到某个特定频道。

(3) 控制者(黑客)使用的主机也连接到 IRC 服务器的这个频道上。

(4) 控制者(黑客)使用 login、!logon、!auth 诸如此类的命令认证自己，服务器将该信息转发给频道内所有的 Bot 主机，Bot 主机将该密码与硬编码在文件体内的密码进行比较，若相同则将该用户的 nick 名称记录下来，以后可以执行该用户发送的命令。控制者具有 channel op 权限，只有他能发出命令。

僵尸网络的发展从良性到恶意 Bot 的实现，从被动传播到利用蠕虫技术主动传播，从使用简单的 IRC 协议构成控制信道到构建复杂多变的 P2P 结构控制模式，再到基于 HTTP 及 DNS 的控制模式，Botnet 逐渐发展成规模庞大、功能多样、不易检测的恶意网络，给当前的网络安全带来了不容忽视的威胁。

3) 计算机病毒(Computer Virus)

计算机病毒是能够自我复制的一组计算机指令或者程序代码，通过编制或者在计算机程序中插入这些代码来破坏计算机的功能或者毁坏数据，影响计算机的使用。计算机病毒主要由感染、载荷和触发等机制组成，而感染过程通常需要人工干预才能完成。病毒的感染动作受到触发机制的控制，病毒触发机制还控制着病毒的破坏动作。病毒程序一般由感染标记、感染模块、破坏模块、触发模块、主控模块等构成。

计算机病毒具有以下几个特点：

(1) 寄生性。计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

(2) 传染性。计算机病毒不但本身具有破坏性，更有害的是具有传染性，一旦病毒被复制或产生变种，其扩散速度之快令人难以预防。传染性是病毒的基本特征。

(3) 潜伏性。有些病毒像定时炸弹一样，让它什么时间发作是预先设计好的。如黑色星期五病毒，不到预定时间一点都觉察不出来，等到条件具备的时候一下子就爆炸开来，对系统进行破坏。

(4) 隐蔽性。计算机病毒具有很强的隐蔽性，有的可以通过病毒软件检查出来，有的根本就查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。

(5) 破坏性。计算机中毒后，可能会导致正常的程序无法运行，把计算机内的文件删除或使文件受到不同程度的损坏。

(6) 可触发性。病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。

4) 蠕虫(Worm)

蠕虫是一种通过网络传播的恶性病毒，它具有病毒的一些共性，如传播性、隐蔽性、破坏性等，但它与普通病毒之间有着很大的区别，它是一类自主运行的恶意代码。普通病毒需要传播受感染的驻留文件来进行复制，而蠕虫不使用驻留文件即可在系统之间进行自我复制，普通病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机。其工作流程可以分为扫描探测、攻击渗透、处理现场、自我复制四部分。扫描探测主要完成对目标网络和主机的信息汇集，包括目标网络拓扑结构和网络中节点主机的操作系统类型，并完成对具体目标主机服务漏洞的检测；攻击渗透利用已发现的服务漏洞实施攻击；处理现场部分的工作包括隐藏、信息搜集等；自我复制完成对目标节点的感染，同时生成多个副本。

蠕虫能控制计算机传输文件或信息，一旦系统感染蠕虫，蠕虫即可自行传播，将自己从一台计算机复制到另一台计算机，而且它还可大量复制。因而在产生的破坏性上，蠕虫病毒也不是普通病毒所能比拟的，网络的发展使得蠕虫可以在很短的时间内蔓延整个网络，造成网络瘫痪。

2. 网络协议攻击

TCP/IP 网络协议栈起源于 20 世纪 60 年代末美国军方资助的一个分组交换网络研究项目，在设计之初的目标是使用一个公用互联网络协议，因此只考虑到数据在网络中的交互问题，并没有考虑到网络中的计算机及用户并非全部都是可信任的。随着互联网的逐步发展与开放，TCP/IP 网络协议栈中存在的安全缺陷开始凸显出来。

TCP/IP 由网间层的 IP 和传输层的 TCP 组成，它定义了网络设备接入 Internet 的方式及网络设备间传输数据的标准。TCP/IP 分为四层结构，每层为完成自己的任务都需要它的下层协议进行配合。举例来讲，TCP 负责传输数据并发现其中可能存在的问题，一旦发现问题就向下层的 IP 发出指令，要求重传数据，直至所有数据准确无误地传输到接收方。

TCP/IP 的四层结构分别是网络接口层、网间层、传输层和应用层，每一层负责不同的功能，各自具有相应的网络协议，每一层上的协议也都存在一定的安全问题或设计缺陷。

1) 网络接口层

网络接口层主要负责定义网络介质的物理特性，包括机械特性、电子特性、功能特性和规程特性等。该层通常包含操作系统的设备驱动程序和对应的网络接口卡，并负责接收和发送 IP 数据包。网络接口层从网络上接收物理信号，从中抽出 IP 数据包并提交给网络层。该层常用的协议主要是以太网协议和 PPP(Point to Point Protocol)。针对该层常见的攻击主要有 MAC 地址欺骗攻击和网络嗅探与协议分析，传输的数据存在被嗅探与监听的安全隐患。

2) 网间层

该层负责网络设备之间的通信，即点到点通信，并提供基本的数据包封装等功能，主要包括处理传输层的发送请求，即当收到数据时，首先将数据帧封装在 IP 数据包中并填充首部，然后选择发往目的主机的路径，将数据包转交给相应的网络接口；处理接收到的数据包，校验数据包的合法性，并选择下一跳的路径，如果数据包的目的主机是本机，则拆掉首部后将其余部分交给传输层协议，如果本机只是中间节点，则对该数据包进行转发。网间层还负责流量控制，避免传输过程中的拥塞等，通常采用因特网控制报文协议(Internet Control Message Protocol，ICMP)。

该层的基础协议是 IP，典型协议还包括地址解析协议(Address Resolution Protocol，ARP)、ICMP 等。网间层受到的协议攻击主要是由于 IP 缺乏身份认证机制，很容易遭到 IP 地址欺骗攻击(详见 4.2.1 节)。ARP 通过广播询问方式来确认目标的 MAC 地址，确保网络正常通信。但是在 ARP 解析过程中，采用广播询问方式来确认目标的 MAC 地址，并且没有做任何真实性验证，因此攻击者只要持续不断地发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP/MAC 条目，造成网络中断或中间人攻击。将 IP 地址转换为 MAC 地址是 ARP 的工作，在网络中发送虚假的 ARP 响应包就是 ARP 欺骗(详见 4.2.2 节)。ICMP 主要用于在主机与路由器之间传递控制信息，包括错误、交换受限控制和状态信息等。针对 ICMP 的攻击主要是基于重定向的路由欺骗技术，攻击者伪造网关向特定主机发送 ICMP 重定向报文从而达到数据监听、数据篡改的目的(详见 4.2.3 节)。

3) 传输层

传输层主要负责提供应用程序间的数据传送服务，也称为端到端的通信，该层将数据包加入传输层首部并提交给下一层。主要功能包括格式化信息流和提供可靠传输。传输层协议规定接收方必须对收到的数据包应答，如果未收到应答必须重传。

传输层主要有传输控制协议(TCP)和用户数据包协议(UDP)。由于 TCP 建立会话之后的连接过程中，仅仅依靠 IP 地址、端口和序列号进行验证通信，容易受到伪造和欺骗，如 TCP RST 复位攻击(详见 4.3.1 节)。而且，由于 TCP 的三次握手过程存在设计缺陷，攻击者可以进行 SYN 泛洪攻击。针对 UDP，比较常见的只有 UDP 泛洪攻击(详见 4.3.2 节)，其目的是耗尽目标网络带宽。

4) 应用层

应用层协议比较多，主要负责应用程序间的沟通，如简单电子邮件传输协议(Simple Mail Transfer Protocol，SMTP)、文件传输协议(File Transfer Protocol，FTP)、域名服务(Domain Name Service，DNS)等。因为应用层协议种类较多，所以存在被嗅探监听、欺骗与中间人攻击的风险，如 DNS 欺骗攻击、FTP 数据嗅探等。