普通高等教育“十三五”规划教材

网络安全：技术与实践

Network Security: Technology and Practice

主　编　李　强
副主编　孙　鉴

北京邮电大学出版社
www.buptpress.com

普通高等教育“十三五”规划教材

网络安全：技术与实践

主　编　李　强
副主编　孙　鉴

北京邮电大学出版社
·北京·

内 容 简 介

本书根据作者近年来的第一手教学经验编写而成，从学生感兴趣的实验入手，进行汇总、整理和设计改进，在参考国内外行业发展动态的同时，汇聚我国网络安全重要法律法规及案例。本书的体系结构主要包括网络安全实验操作部分和网络安全法律案例解读部分，具有一定的创新性和实用性。实验部分包括背景介绍、实验目的、实验内容、实验原理、实验环境以及实验步骤等，并提供了实验思考和实验拓展；法律法规部分包括重要条款解读、行业规范分析、重点案例讲解等内容。授课教师可根据具体教学需求和教学进度安排，在兼顾不同类型的教学对象的基础上，进一步提升网络安全技术实践教学的整体教学效果，同时也为学生今后从事相关专业储备丰富的法律法规知识。本书包含基础技术部分和拓展实践部分共 9 个实验，涉及理论教学中的各个基本关键点。所有实验可操作性强，与实践结合紧密，全部实验示例都经过精心设计和反复调试。

图书在版编目(CIP)数据

网络安全：技术与实践/李强主编. -- 北京：北京邮电大学出版社，2018.12

ISBN 978-7-5635-5621-2

Ⅰ.①网… Ⅱ.①李… Ⅲ.①计算机网络—网络安全 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 255784 号

书　　名	网络安全：技术与实践
主　　编	李　强
责任编辑	马　飞
出版发行	北京邮电大学出版社
社　　址	北京市海淀区西土城路 10 号(100876)
电话传真	010-82333010　62282185(发行部)　010-82333009　62283578(传真)
网　　址	www.buptpress3.com
电子信箱	ctrd@buptpress.com
经　　销	各地新华书店
印　　刷	北京九州迅驰传媒文化有限公司
开　　本	787 mm×960 mm　1/16
印　　张	12
字　　数	223 千字
版　　次	2018 年 12 月第 1 版　2018 年 12 月第 1 次印刷

ISBN 978-7-5635-5621-2　　定价：48.00 元

前　言

近年来，网络空间已发展为继海、陆、空、天之后的第五空间，成为影响个人安全、社会安全、国家安全乃至国际安全的重要因素之一。世界各国对于网络空间及其安全问题日益重视，投入了巨大的人力、物力进行发展。其中，网络安全技术的教育与培训作为国家优先发展战略之一，得到了社会各个方面越来越多的重视和支持，未来将进一步与物联网、云计算、区块链、人工智能等重要技术领域紧密结合，为我们的日常生活、社会发展和国家进步打下牢靠的基础。

“网络安全技术”是一门涉及知识面广泛，在多学科知识基础上汇聚融合而成的课程。不但要求学生掌握扎实的理论基础，还要求学生将严密的逻辑性和操作的灵活性相结合，“创造性”地解决各类网络安全问题。因此，该课程实验教学过程充满了挑战性，由于难以权衡不同学生的实际学习情况，往往教学效果差强人意，两极化现象严重。与此同时，虽然我国近年来颁布了多部网络安全方面的法律法规，但是在教学过程中，作者发现学生的法律意识淡薄，操作时常不顾及后果，很多行为令人十分担忧。

本书根据作者近年来的第一手教学经验编写而成，在参考国内外行业发展动态的同时，汇聚我国重要法律法规及案例，从学生感兴趣的实验入手，进行汇总、整理和设计改进。本书的体系结构主要包括实验操作部分和法律案例解读部分，具有一定的创新性和实用性。实验部分包括背景介绍、实验目的、实验内容、实验原理、实验环境以及实验步骤等，并提供了实验思考和实验拓展；法律法规部分包括重要条款解读、行业规范分析、重点案例讲解等内容。授课教师可根据具体教学需求和教学进度安排，在兼顾不同类型的教学对象的基础上，进一步提升网络安全技术实践教学的整体教学效果，同时也为学生今后从事相关专业储备丰富的法律法规知识。《网络安全：技术与实践》共包含 9 个实验，涉及重要网络协议分析、服务器操作、系统安全、渗透测试等理论教学中的相关知识要点。所有实验可操作性强，与实践结合紧密，全部实验示例都经过精心设计和反复调试，可以放心使用。

本书可作为综合性大学网络工程专业中网络安全课程的实验教材①,也可供其他高等院校相关专业或工程技术人员参考使用。

感谢出版社和相关院校,为本书的顺利出版提供了许多帮助,并提出一些很好的修改意见和建议。同时,感谢在本书编著过程中给予大力支持和帮助的专家和工程人员,他们的意见对于完善和提高全书质量起到了关键的作用。此外,本书的编写得到了国家民委教改项目(项目编号:17043)的支持,在此一并致谢。

由于网络安全技术涉及的内容比较繁杂,且相关技术发展迅速、知识更新快,另外,本书编著时间较为仓促,编者经验不足、学识有限,书中难免有不当乃至错误之处,殷切希望使用本书的老师、学生及工程人员批评指正,同时也希望其他读者朋友能就本书内容和叙述方式提出宝贵的意见,从而进一步完善本书的相关内容。作者邮箱地址:E-mail:dr_qiangli@163.com。

编 者

2018 年 08 月 01 日

① 建议在同时开设"网络安全技术"及"密码学"的情况下使用本教材,本书不涉及网络安全与密码学交叉部分实验。

目　录

基础技术与实践部分

拓展技术与实践部分

网络安全与法律法规部分

Part I

基础技术与实践

实验 1
Windows Server 安全管理

作为 20 世纪 80 年代初使用较为广泛的操作系统，微软公司所研发的 Microsoft-DOS 操作系统促进了计算机的普及[1]。1985 年，微软公司突破性地发布了该公司历史上第一个基于图形用户界面(graphics user interface，GUI)的窗口式多任务操作系统——Windows 1.0，打破了以往命令行接收用户指令的方式，单击鼠标就可以完成相关任务。随着计算机硬件和软件的不断升级，微软公司的 Windows 系统也在不断升级，从架构的 16 位、32 位再到 64 位，系统版本从最初的 Windows 1.0 到大家熟知的 Windows 95、Windows 98、Windows XP、Windows 7、Windows 10 等，Windows 操作系统已经占据了个人计算机操作系统 90%以上的市场份额。目前，微软公司的操作系统可分为两大类：一类是面向普通用户的 PC 桌面操作系统，如 Windows XP、Windows Vista、Windows 7 和 Windows 10；另一类是定位在高性能工作站、台式机、服务器，以及政府机关、大型企业网络、异形机互联设备等多种应用环境的企业级服务器操作系统，如 Windows NT Server、Windows Server 2003、Windows Sever 2008、Windows Server 2012 和 Windows Server 2016 等。

Windows Server 是微软公司在 2003 年 4 月 24 日推出的 Windows 的服务器操作系统，其核心是 Microsoft Windows Server System(WSS)，每个 Windows Server 都与其家用(工作站)版对应(2003 R2 除外)[2]。其版本历史如图 1-1 所示。

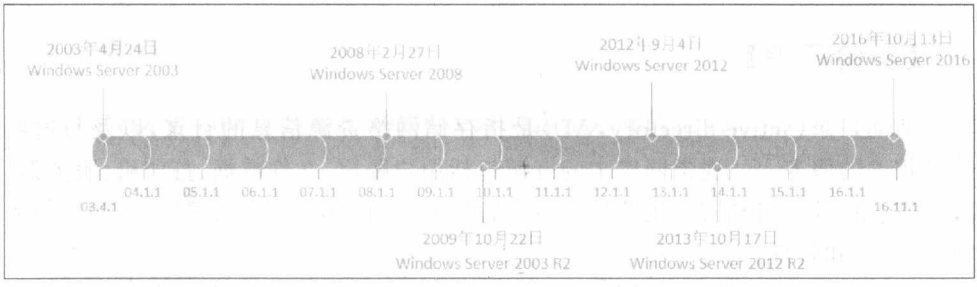

图 1-1　Windows Server 版本历史

从最初的 Windows NT 3.0 到 Windows Server 2012 服务器操作系统,每一款操作系统在界面外观和功能上基本相同,大大降低了用户的学习成本,增强了产品的被依赖性,特别是对企业用户而言。近年来,互联网快速发展,人们对操作系统的功能提出了更高的要求,例如,如何适应虚拟化、云计算和大数据等新的信息化应用。Windows Server 2016 是微软公司于 2016 年 10 月 13 日正式发布的最新服务器操作系统,借助新技术以全新的界面、强大的功能,为用户提供了性能稳定、安全可靠的系统环境,从而更好地满足企业级用户的所有业务负载和应用程序需求。Windows Server 2016 操作系统可向企业和托管提供商提供伸缩、动态、支持多租户以及针对云计算进行优化的基础结构。

1.1 活动目录服务与域模式账户管理

【实验目的】

1. 了解 Windows Server 2016 操作系统的安全功能、缺陷和安全协议。

2. 熟悉 Windows Server 2016 操作系统的活动目录服务与域模式下的账户管理。

3. 熟练使用组策略管理。

【实验内容】

1. 安装活动目录服务。
2. 域模式账户管理。
3. 组的创建及管理。
4. 组策略配置。

【实验原理】

活动目录(active directory,AD)是指存储网络资源信息的目录,以及与这些信息相关的服务[3]。通常网络中的资源包括用户账户、文件数据、打印机、服务器、数据库、组、计算机和安全策略等,这些信息都可以保存于活动目录中,方便用户的检索、使用和管理。

Windows Server 2016 的活动目录功能扩展了 Windows 以往服务器版本操作系统的目录服务,运行范围可以从几百个对象的单一服务器到成千上万个对象的

数百台服务器。而 Windows 域(Domain)就是基于 Windows NT 技术构建组成的计算机网络独立安全范围,是 Windows 的逻辑管理单位。一个域就是由一系列的用户账户、访问权限和其他各种资源的集合构成,也就是包括各种对象属性信息的目录数据库。活动目录由一个或多个域构成,一个域可以跨越不止一个物理地点。每一个域都有自己的安全策略,以及本域与其他域之间的信任关系。当多个域通过信任关系连接起来并且拥有共同的模式、配置和全局目录时,它们就构成了一个域树,多个域树连接起来就形成一个域林,如图 1-2 所示。

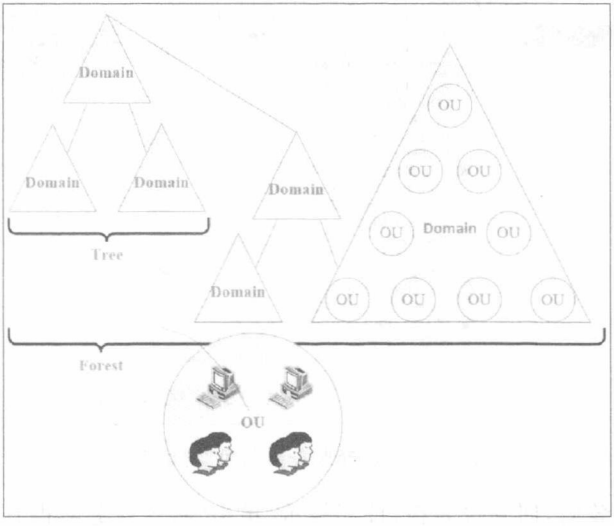

图 1-2　活动目录的结构

组策略是活动目录的重要组成部分,也是活动目录里的重点内容。了解和使用组策略将最大限度地使管理员的管理工作变得简单化、条理化。组策略为操作系统以及操作系统上运行的应用程序的集中配置管理提供了基础结构。基于活动目录的组策略不仅应用于用户和客户机,还应用于成员服务器、域控制器以及管理范围内的任何 Windows 2000 以上操作系统的计算机。

【实验环境】

一台搭载 Windows Server 2016(64-bits)操作系统的主机。

【实验步骤】

1. 创建域控制器

(1)打开“服务器管理器”,单击“添加角色和功能”按钮,进入“添加角色和功能

向导”对话框,选择“服务器选择”窗口,勾选“Active Directory 域服务”,如图 1-3 所示,然后弹出“添加 Active Directory 域服务所需的功能”,单击“添加功能”按钮添加服务,之后根据提示,依次安装。

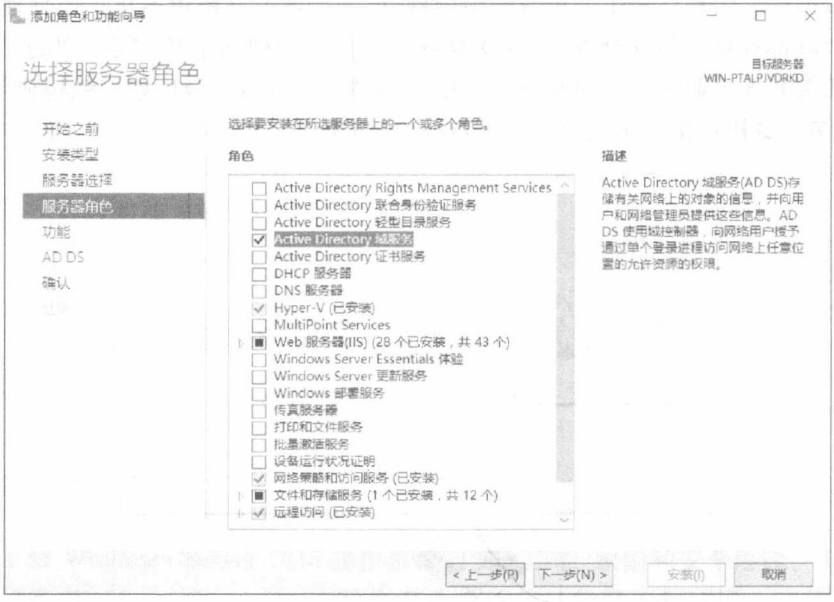

图 1-3 “选择服务器角色”对话框

(2)完成安装后,回到仪表板,按照提示,单击“将此服务器提升为域控制器”超链接,如图 1-4 所示。

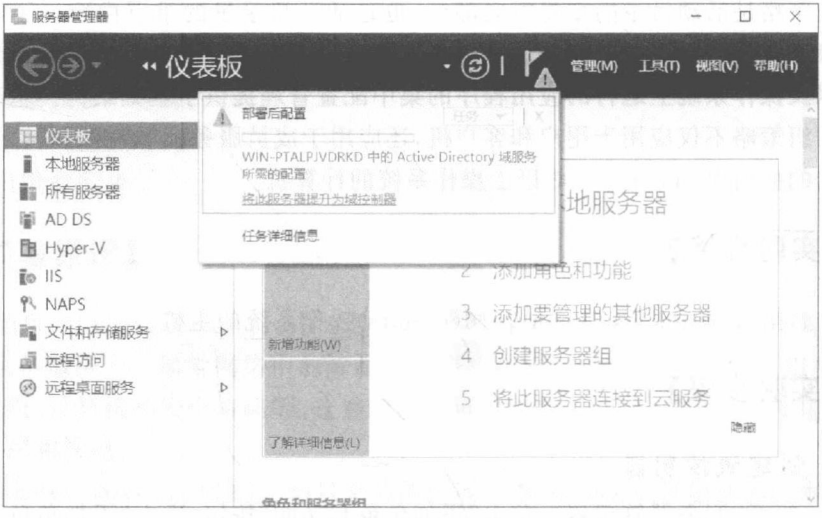

图 1-4 将服务器提升为域控制器

(3)进入“Active Directory 域服务配置向导”,选择“添加新林”,设置根域名为“Administrator. com”,如图 1-5 所示,然后单击“下一步”按钮。

图 1-5　添加新林

(4)进入“域控制选项”窗口,选择“林功能级别”和“域功能级别”(默认为 Windows Server 2016)。设置目录服务还原模式的系统管理员密码(目录服务还原模式,即目录服务修复模式,可以在系统启动时按 F8 键进入选择),用户密码必须至少 7 位,其组成是 A～Z、a～z、0～9、非字母数字字符等 4 组中的 3 组,并且不可包含用户账户中两个以上相连的字符,如图 1-6 所示,单击“下一步”按钮。

(5)指定 DNS 委派选项服务器将自动检查 DNS 服务器是否启用。如果已经启用,则需要指定 DNS 委派选项;如果没有启动,则直接单击“下一步”按钮,因为后面将自动绑定 DNS 服务器,所以不需要提前安装 DNS 服务器,如图 1-7 所示,直接单击“下一步”按钮。

(6)设置 NetBIOS 域名,服务器将自动根据之前输入的域名生成一个 NetBIOS 域名,如无特殊要求默认即可,如图 1-8 所示,单击“下一步”按钮。

(7)指定 AD DS 数据库、日志文件和 SYSVOL 的位置,如无特殊要求默认即可,如图 1-9 所示,然后单击“下一步”按钮。

(8)查看安装参数选项,单击“下一步”按钮,完成先决条件检查后,单击“安装”按钮,域控制器安装完成。

图 1-6 “域控制器选项”窗口

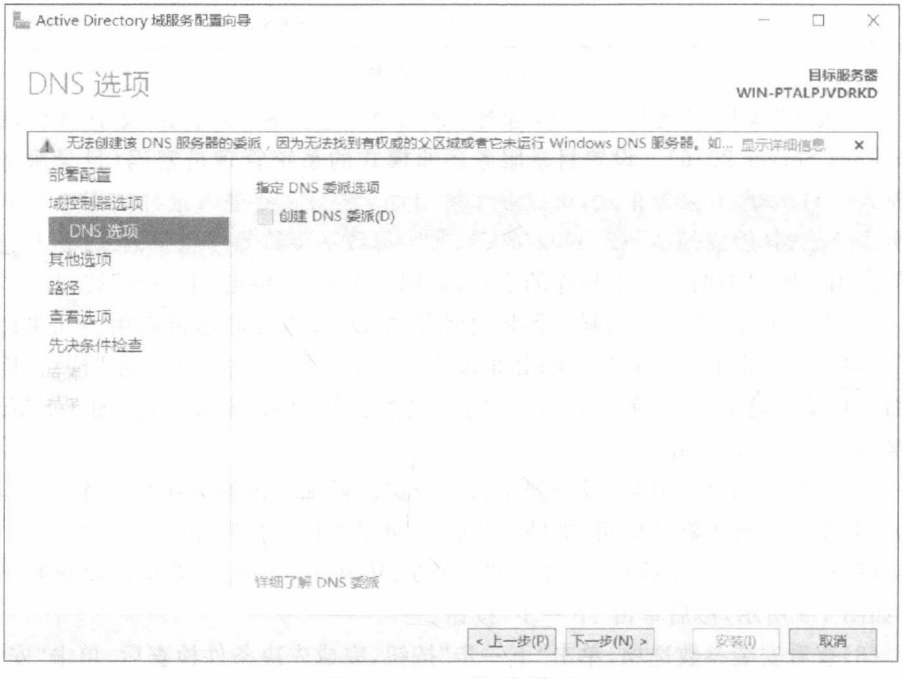

图 1-7 “DNS 选项”窗口

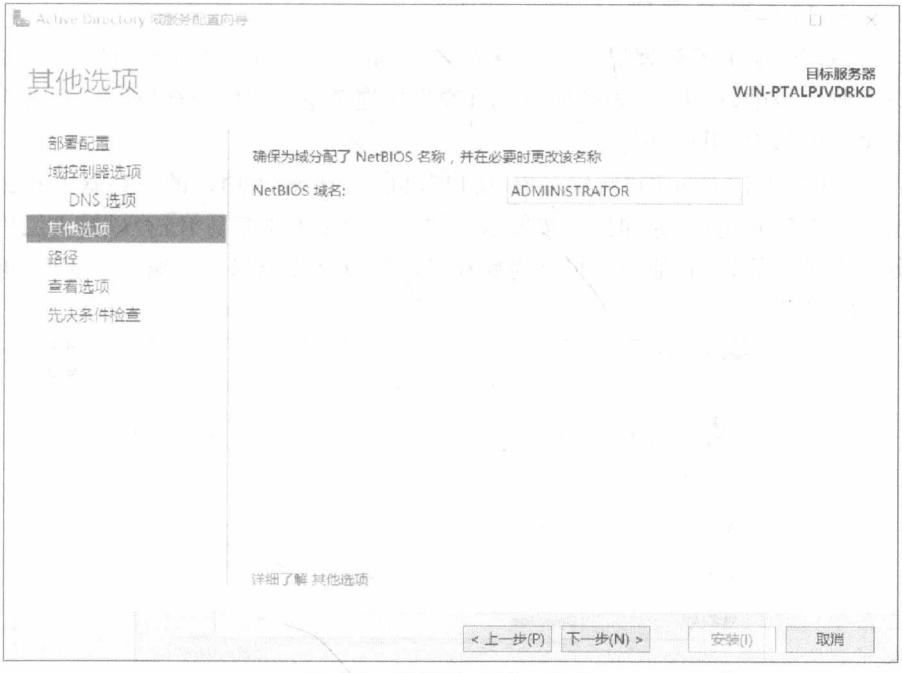

图 1-8　设置 NetBIOS 域名

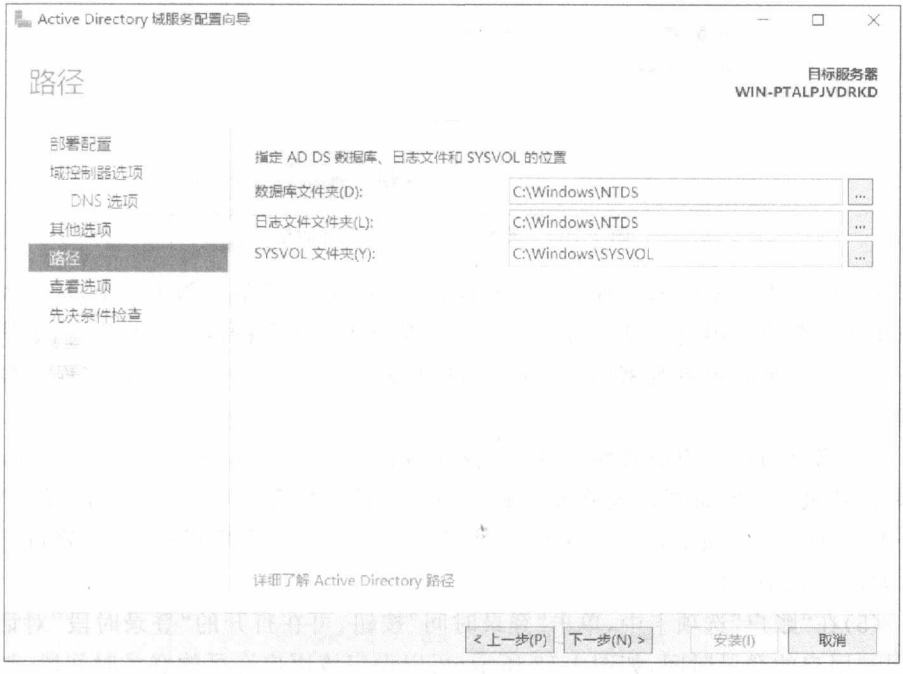

图 1-9　路径选择