全国高等职业教育计算机类规划教材
工作过程系统化教程系列

过程导向
项目驱动
能力培养
面向就业

- 6个学习情境，对应企业6个网络安全防护技术领域
- 22个工作任务，设计知识由浅入深、技能由简到繁
- 1台主机环境，即可完成书中全部网络安全实训任务
- 4个主要步骤，任务引导文、设计规划、实施与检查

网络安全与防护

迟恩宇　刘天飞　杨建毅　王　东　主编
李明革　王东育　主审

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

全国高等职业教育计算机类规划教材·工作过程系统化教程系列

网络安全与防护

迟恩宇　刘天飞　杨建毅　王　东　主编
李明革　王东育　主审

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书共设计了6个学习情境，分别对应当前企业网络安全管理与防护的6个方面的技术：网络故障；保护数据在公网上的传输；对网络访问行为进行控制；对入侵进行检测、审计与防护；对主机部署与实施安全防护；保护网络安全可靠运行的综合技术。6个学习情境共设计了28个工作任务，并在每一个学习情境的工作任务后面安排了拓展训练。

本书可作为高职高专的计算机网络和信息安全专业教学用书，也可作为网络工程技术人员、网络管理人员和信息安全管理人员的参考书和自学用书。

图书在版编目（CIP）数据

网络安全与防护 / 迟恩宇等主编.—北京：电子工业出版社，2009.8
全国高等职业教育计算机类规划教材·工作过程系统化教程系列
ISBN 978-7-121-08965-7

Ⅰ. 网… Ⅱ. 迟… Ⅲ. 计算机网络－安全技术－高等学校：技术学校－教材
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2009）第 086182 号

策划编辑：程超群
责任编辑：宋兆武　李施诺
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：19.5　字数：497.6 千字
印　　次：2009 年 8 月第 1 次印刷
印　　数：4 000 册　　定价：31.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

《网络安全与防护》读者意见反馈表

尊敬的读者：

感谢您购买本书。为了能为您提供更优秀的教材，请您抽出宝贵的时间，将您的意见以下表的方式（可从 http://www.huaxin.edu.cn 下载本调查表）及时告知我们，以改进我们的服务。对采用您的意见进行修订的教材，我们将在该书的前言中进行说明并赠送您样书。

姓名：_____ 电话：_____

职业：_____ E-mail：_____

邮编：_____ 通信地址：_____

1．您对本书的总体看法是：

□很满意 □比较满意 □尚可 □不太满意 □不满意

2．您对本书的结构（章节）：□满意 □不满意 改进意见_____

_____

_____

3．您对本书的例题：□满意 □不满意 改进意见_____

_____

_____

4．您对本书的习题：□满意 □不满意 改进意见_____

_____

_____

5．您对本书的实训：□满意 □不满意 改进意见_____

_____

_____

6．您对本书其他的改进意见：

_____

_____

_____

_____

7．您感兴趣或希望增加的教材选题是：

_____

_____

_____

请寄：100036 北京市海淀区万寿路 173 信箱高等职业教育分社 收

电话：010-88254565 E-mail：gaozhi@phei.com.cn

反侵权盗版声明

前　言

互联网资源的日益丰富，为新知识、新技术的学习带来了方便，仅掌握书本上的理论已经无法跟上时代的步伐，也不符合科学发展的思想，更无法满足学习者持续增多知识和技能的需求。因此本书强调的是方法和能力的传授。本书充分借鉴了国内外基于行动导向的职业教育成功经验进行开发设计。

本书共设计了6个学习情境，每一个学习情境对应企业网络中不同的安全防护需求。学习情境1——通过流量分析定位网络故障；学习情境2——保护数据在公网上的传输；学习情境3——对网络访问行为进行控制；学习情境4——对入侵进行检测、审计与防护；学习情境5——对主机部署与实施安全防护；学习情境6——保护网络安全可靠运行的综合技术。这6个方面所涉及的技术是目前企业网络安全管理与防护的主要技术。

除第一个学习情境只设置了一个工作任务外，其他每个学习情境中都设计了若干个工作任务，每一个工作任务为具体的安全防护需求的知识介绍内容并提出解决措施。同一学习情境中的多个工作任务之间采用由简单到复杂的过程进行设计，第一个工作任务侧重于对本学习情境所涉及基础知识的介绍，并进行简单地实现；后续工作任务知识介绍减少，但操作与实施逐渐复杂，同时也是对前面工作任务的强化与提升，并在任务设计上使其更能符合企业网络安全防护的实际需求，对全部内容进行合理的排序，使其更符合人的认知规律。

每个任务按如下过程进行：工作任务需求分析→任务相关知识收集整理→工具和方法的选择→规划与实施→结果检查。每一个工作任务在设计上，首先，通过引导文本对工作任务所需的知识进行介绍；其次，对任务所需使用的工具软件的选择与介绍；接下来是对企业网络安全防护的环境进行转化设计，便于在一台计算机或简单的网络环境下实现，即对任务场景的最小化设计，有利于实施；然后，对任务的具体实施的介绍；最后，对结果测试方法的介绍。

本书在设计上的特点是注重通过任务引领知识的学习，重点介绍一种学习和解决问题的方法。不同于一般网络安全教材过多地强调知识的特点，本书将知识引入到具体工作需求中来，通过对工作任务的理解与实施加强对知识的学习，同时具备自学的方法与能力。另外，本书中所设计的全部工作任务都可以借助虚拟机、模拟路由器等软件在一台配置较高的计算机上完成。使学习者可以在单机环境下随时完成本书所涉及的知识与任务的学习。

本书结合国际主流网络设备厂商思科网络公司的网络产品进行具体实施。书中借用了思科公司的网络设备图标，使每个任务中的图更易于理解，并在此对提供图标库和经验指导的思科公司韩江经理和刘亢经理表示感谢。同时，也对来自互联网上为本书的编写提供参考资料及工具软件的朋友们表示感谢。

为了便于高职网络安全课程教师进行网络安全教材和课程建设与改革的经验交流，我们建立了“高职网络安全课程交流”QQ群，群号为：26236380，本教材编者邮箱为：cey1976@gmail.com，通过这些方式可以实现广泛交流与本教材中所涉及的课件、文档和视频文件等资源的共享。我们正在建设本教材对应的课程网站，教材所涉及资源将逐步上网以方便互相学习与交流使用。

本书具有较强的针对性和适用性，可供职业院校教学和企业网络安全管理人员培训学习使用。也适用于已经具备一定网络设备与服务配置经验的网络工程师自学使用。由于本教材的编写是职业教育教学改革的初步尝试和探索，不足之处在所难免，恳请广大读者提出宝贵意见，以便我们对本书进行修改和完善。

本书由迟恩宇、刘天飞、杨建毅、王东主编，姜惠民、苏东梅、刘宝庆、钟玉珍、施丽男、杨亚洲、叶郁文、陈永昌、金照春参加编写。全书由李明革教授与企业专家王东育主审。

编　者

2009 年 4 月

目　录

学习情境1　通过流量分析定位网络故障

1.0　总体介绍

网络协议是网络中所有设备（网络服务器、计算机、交换机、路由器及防火墙等）之间通信规则的集合与约定，它定义了通信时信息必须采用的格式和这些格式的意义。协议的安全直接影响着整个网络的安全。

目前，使用最为广泛的网络协议是 TCP/IP 协议簇，在 TCP/IP 协议设计之初，重点考虑的是网络的互联特性，并没有过多考虑其安全性。所以网络中经常发生针对 TCP/IP 协议的攻击，如针对 ARP、IP、ICMP、TCP、UDP、FTP、TELNET、SNMP 等一系列协议的安全攻击。计算机病毒也借助网络协议的漏洞进行传播或发起针对网络的攻击。

因此，作为网络安全管理与防护人员，要掌握网络协议的分析技术，发现、定位并防护针对网络协议发起的攻击。

1.0.1　情境描述

在一个企业局域网中经常会发生一些攻击，其中多数是来自内部，导致网络性能下降，表现为访问互联网速度明显变慢，打开网页或下载速度都很慢，甚至无法访问。究其原因，多数是由于 TCP/IP 协议自身设计问题导致的。

本学习情境的设计，以最典型的 ARP 协议攻击为主，通过展开学习，学会对网络协议进行分析的方法，掌握一个对协议分析的工具软件，具备项目应用的拓展能力，能够解决 ARP 以外的 TCP/IP 中的协议的安全分析及协议流量引发的网络安全故障，并能提供有效的防护措施。

1.0.2　总体目标

- ◆ 在不影响网络安全可靠运行的前提下，对网络中各协议数据进行捕获；
- ◆ 能对捕获到的不同类型协议数据进行准确的分析判断，发现异常（这需要有一定的经验积累）；
- ◆ 快速有效地定位网络中的故障，在不投入新的设备情况下解决问题；
- ◆ 熟悉协议封装格式及原理，明确网络协议本身是不安全的；
- ◆ 至少学会使用一种协议分析工具软件，通过拓展训练和后期学习中的经验积累能解决由于协议安全引发的网络安全故障。

1.0.3　内容描述

在本学习情境中只设计了 1 个工作任务。建议多人在可以访问互联网的环境下完成本工作任务，具体过程为：阅读引导文本；安装协议分析软件、进行协议捕获、模拟攻击，并对攻击进行检查，最后进行拓展训练，完成对其他协议的分析任务，例如，可以选择在宿舍、

实训室、办公室或在网络中心的安排下完成同类工作任务。

1.0.4 情境教学条件

整体教学环境要求

- 保证所有实训计算机可以访问互联网。
- 建议实训计算机使用 Windows XP 操作系统。
- 建议实训计算机硬件配置足够，内存至少 512MB。

工具及软件要求

- 协议分析软件 Sniffer Pro。
- ARP 攻击器。

特定的硬件设备要求

- 在实际工作中建议使用笔记本电脑，并配置一条直通双绞线和一条交换机配置线，以便于对网络流量进行分析与定位。
- 一台支持端口镜像功能的交换机及相关配置线缆。

参考资料及视频建议

- Sniffer Pro 中文手册。
- TCP/IP 协议详解（卷 1、卷 2）或同类书籍。
- 关于本部分的视频教程。

1.0.5 学习情境 1 整体网络场景

学习情境 1 整体网络场景如图 1.0 所示。

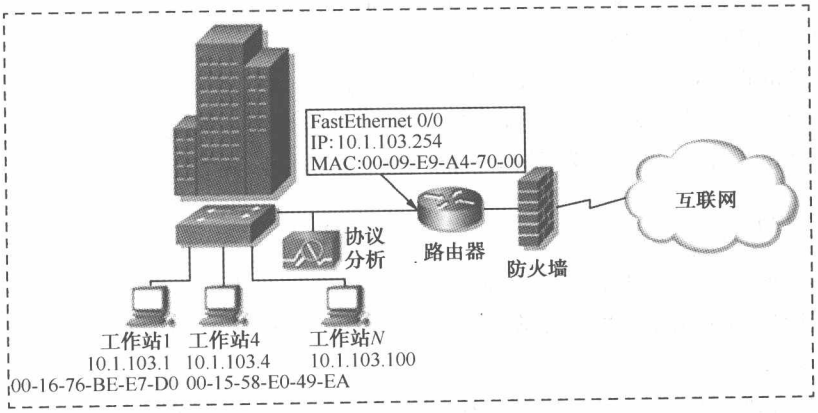

图 1.0 典型企业局域网络的协议分析整体场景

1.1 工作任务 1——基于 Sniffer Pro 进行协议、模拟攻击分析

1.1.1 工作任务总体描述与实施流程表

本工作任务是对 ARP 协议的攻击进行协议分析、模拟攻击、测试与流量分析。通过本工作任务的学习，将学会协议分析技术的要点，通过经验的积累能够定位网络故障所在。具体

工作任务描述与实施流程如表 1.1 所示。

表 1.1　工作任务描述与实施流程表

学习情境 1——通过流量分析定位网络故障
任务名称：基于 Sniffer Pro 进行协议、模拟攻击分析
企业工作情境描述
在一个企业局域网中经常会发生一些攻击，其中多数是来自内部，导致网络性能下降，表现为访问互联网速度明显变慢，打开网页或下载速度都很慢，甚至无法访问
工作任务分析
通过对此类现象的资料搜索、查阅及分析，发现网络性能下降或无法访问外部网络的多数情况是由于计算机蠕虫病毒、木马、ARP 攻击、带宽滥用（P2P 下载软件）等造成的。其原因是利用网络协议的特点发起的攻击
任务目标
1．在不影响网络安全可靠运行的前提下，对网络中不同类型的协议数据进行捕获 2．能对捕获到的不同类型协议数据进行准确的分析判断，发现异常（需要有一定的经验积累） 3．快速有效地定位网络中的故障原因，在不投入新的设备情况下解决问题 4．熟悉协议封装格式及原理，明确网络协议本身是不安全的
学习场景简化
对典型企业局域网进行简化，使其足以满足完成本次实验，简化后如图 1.1 所示，搭建出这样的网络结构。此工作任务可在这样的实训室完成：实训计算机通过交换机连接在一起构成局域网，同时一台路由器将这个局域网连接到外部网络去，这样的实验很容易搭建。本任务主要针对 ARP 的协议数据进行捕获、分析、模拟攻击测试，并最后提出防范 ARP 方案
工具及软件选用
1．协议分析软件 Sniffer pro 2．ARP 攻击器 3．在实际工作中建议使用笔记本电脑并配置一条直通双绞线和一条交换机配置线
任务实施流程
1．知识准备：阅读引导文本或利用网络查找 ARP 协议封装相关资料 2．工具及软件选用：安装 Sniffer Pro 软件、进行捕获过滤设置 3．捕获 ARP 协议数据，并进行分析 4．明确 ARP 协议的缺陷，制定模拟 ARP 攻击方法 5．构造 ARP 攻击协议数据帧，实施 ARP 协议模拟攻击与攻击结果检查 6．利用 ARP 攻击器发起攻击，确定 ARP 攻击流量并加以分析 7．针对此类攻击的防范措施
参考资料手册
1．利用互联网搜索相关知识 2．Sniffer Pro 中文手册 3．TCP/IP 协议详解（卷 1、卷 2）或同类书籍 4．教材中的引导文本 5．相关视频教程