063702 网络与信息安全实验 16学时/0.5学分

英文译名：Network & Information Security Experimentation

适用领域：计算机应用技术

开课单位：计算机科学与技术学院

教学目的：“网络与信息安全实验”课程的设置是与“高级计算机网络”课程、“计算机通信”课程和“信息安全技术”课程紧密相关的。在后三门课程充分讲述计算机网络和信息安全的理论性知识的基础之上，与实践相结合，让学生充分了解真实的计算机网络是什么样的，网络和通信课中讲述的知识在实际中是如何运用的，保证信息安全的手段和措施是如何实施的等等内容。最终让学生的网络和安全知识结构更加完整，对所学的知识有真正全面、深刻的认知，同时培养了学生的动手能力。

预备知识或先修课程要求：高级计算机网络、计算机通信、信息安全技术

教学方式及学时分配：课堂授课8学时、实验8学时

|  |  |  |
| --- | --- | --- |
| 第1部分 计算机网络实验 | | |
| 学时 | 教学内容 | 教学方式 |
| 2 | 计算机网络基础知识概述，包括：计算机网络定义与分类； 计算机网络的性能指标；计算机网络体系结构；面向连接与无连接服务的对比；因特网；常用网络命令 | 授课 |
| 1 | 网络连接介质，包括：同轴电缆；双绞线；光纤；无线网络 | 授课 |
| 1 | 网络设备，包括：网卡；交换机；路由器 | 授课 |
| 1 | VLAN的划分，包括： Boson NetSim 操作详解；IP地址；VLAN的设计 | 授课 |
| 1 | 路由器的配置，包括：cisco IOS操作系统即命令解析；路由配置方法 | 授课 |
| 1 | 网络服务器相关硬件技术，包括：多处理器技术和并行技术；高性能存储技术；服务器内存技术；控制与管理技术；可用性技术 | 授课 |
| 1 | 网络服务器的配置，包括：WEB服务器的配置；FTP服务器的配置；邮件服务器的配置；DNS服务器的配置；DHCP服务器的配置 | 授课 |
| 第2部分 信息安全实验 | | |
| 1 | 网络探测与漏洞扫描，包括：使用Sniffer监听；网络检测和扫描工具的使用；漏洞扫描工具的使用 | 实验 |
| 1 | 网络攻击与防范，包括：帐号口令破解；木马攻击与防范；DDOS攻击与防范；缓冲区溢出攻击与防范；欺骗攻击与防范；计算机病毒的防范 | 实验 |
| 2 | 网络安全防护技术，包括：软、硬件防火墙及配置；入侵检测系统及配置；虚拟专网及配置；配置SSL连接 | 实验 |
| 2 | 网络诱捕技术，包括蜜罐、蜜网的基本概念和原理，攻击的捕获和分析方法；虚拟蜜罐、迷网的配置方法 | 实验 |
| 2 | 社会工程学，包括社会工程学的概念、分类和适用范围，社会工程学的案例研究等 | 实验 |

教学主要内容以及对学生的要求：

学习内容：本课程讲授的主要内容包括计算机网络传输媒介与主要设备——交换机与路由器的相关技术概念和特性，网络服务器的软、硬件技术及特性，防火墙、入侵监测系统和虚拟专网三种传统的网络防御技术的基本特点，网络监控以及网络攻击与防范的各种手段等几个方面。要求学生能够熟练掌握网络传输介质、结点设备和服务器的相关知识，熟练掌握网络攻击、防御、社会工程学、攻击诱捕和攻击分析的主要方式方法。

实验内容：包括计算机网络和信息安全两大部分实验。计算机网络实验部分要求学生掌握路由器、交换机以及网络服务器的配置方法，可以根据具体情况改变相关配置参数以符合实际的要求。信息安全实验部分要求学生能够使用相关工具分析网络状态，根据安全策略的不同改变安全机制的配置参数，针对不同的情况设置诱捕网络，并能够分析攻击的种类并进行危害评估。

内容摘要：网络与信息安全实验课程内容分成两个部分：第一部分是计算机网络实验，第二部分是信息安全实验。在第一部分中首先简单介绍了计算机网络的基本知识，让学生有一个总体的认识。其次按照网络的物理构成和特点，进一步细分成网络传输介质、网络设备和网络服务器三个部分。在网络传输介质部分中主要讲解线缆的分类、特性、实际的标准、连接等问题。在网络设备部分中主要讲解设备的分类、作用、特性、标准、实际型号等，重点内容在于设备的配置。在网络服务器部分中主要介绍现在最新的服务器技术以及常用的各种服务器参数的配置。第二部分信息安全实验依据网络安全行为的发生者进行内容的划分与安排。在网络防御部分主要讲解防火墙系统、入侵检测系统和虚拟专网的技术特点和配置问题。同时还讲解了网络安全监控技术，在前三种防御手段的基础上实现网络安全特性的增强。在网络攻击部分主要讲解了现今最主要的几种攻击手段：破解账号、木马攻击、分布式拒绝服务攻击、缓冲区溢出攻击、计算机病毒等。以攻击过程的讲解为主，让学生充分了解几种攻击手段的特点，以便更好地防御这些攻击。在网络诱捕方面，主要介绍蜜罐和蜜网技术，可以进行攻击的捕获和分析。

考核方式：大作业占70%，平时成绩占30%；

课程主要教材：自编讲义

主要参考书目：

[1] 计算机网络（第4版）.（美）Andrew S. Tanenbaum著,潘爱民译.清华大学出版社,2004

[2] 计算机网络（第5版）.谢希仁.电子工业出版社,2008

[3] 计算机网络实验教程.刘兵.中国水利水电出版社,2005

[4] 计算机通信.杨永田.哈尔滨工程大学出版社,2001

[5] 计算机网络实验教程:从原理到实践.陈明.机械工业出版社,2007

[6] 计算机网络布线手册（第2版）.（美）John Vacca著,王宣政等译.人民邮电出版社,2004

[7] 网络安全与保密. 胡建伟等，西安电子科技大学出版社，2003

[8] 网络信息安全技术.周明全等，西安电子科技大学出版社，2003

[9] Honeypot追踪黑客.邓云佳，清华大学出版社，2004