《安全通论》教学大纲

课程编号：071562B

课程类型：□通识教育必修课 □通识教育选修课

□学科基础课 □专业核心课

☑专业提升课 □专业拓展课

总学时：32 讲课学时：32 实验（上机）学时： 0

学　分：2

适用对象：数据科学与大数据技术专业（信息技术）

先修课程：程序设计基础与应用、计算机网络技术与应用

一、教学目标

随着计算机在社会各个领域的广泛应用，以计算机为核心的信息系统安全问题逐渐引起人们的注意。计算机网络是目前信息存储、获取、传递、交换、应用的一个主要媒介，是信息安全的主要阵地。本通过本课程的学习，不仅要使学生对信息安全技术有一个整体的认识，理解实现信息安全的重要性，掌握信息安全的防御技术和方法，为进一步学习网络安全专项技术打下必要的基础。另一方面，也要使学生具备从事信息系统安全设计和信息系统安全管理工作的专业技能，使学生毕业后能够迅速参与信息系统安全研究、设计与管理的实际工作。本课程的主要内容包括：信息安全体系结构、局域网的攻击防御及控制技术、黑客常用的工具及这些工具的使用方法、操作系统常规安全防范方法、木马和病毒的原理、数据的备份与恢复。

课程思政教学目标：使学生了解当前国内外信息安全局势，进而进行爱国主义教育，激发学生的责任感和使命感，坚定学生积极投身于祖国科技行业的信心和信念。

二、教学内容及其与毕业要求的对应关系

（一）教学内容

本课程主要教学内容包括：信息安全体系结构、局域网的攻击防御及控制技术、黑客常用的工具及这些工具的使用方法、操作系统常规安全防范方法、木马和病毒的攻击及方法、数据的备份与恢复。

（二）教学方法和手段

教学以学生为主老师为辅，以培养学生分析问题解决问题能力为目标，在教学过程中，灵活应用多种教学方法，除传统教学方法外，特别强调以下教学方法的运用：项目驱动教学法，案例教学法，精讲多练法。

（三）实践教学环节要求

根据教学进度和要求布置相应的小作业，完成课余实践。建议安装和配置软件进行自学，完成案例的内容。

（四）学习要求

为有效学习本课程，要求学生首先具备计算机网络等方面的基本知识。自学时应该熟读大纲，提纲挈领地掌握信息安全技术的内容，随后，按照大纲熟读教材，还要参考大量的参考文献，通过课后思考和练习题进行多角度和层次的反复学习。课下多练习，本课程将介绍多种网络攻防工具。建议学生利用课余时间结合教材，使用这些工具进行简单的攻防实验。

（五）与毕业要求的关系

信息安全技术是保障信息系统安全性的重要手段，在学生的毕业设计中，学生可以使用本课程所学习的技术保障其设计的信息系统的安全性。

（六）教学中应注意的问题

由于程序设计基础与应用、计算机网络技术与应用等是该课程的先修基础，如果学生先修基础课没有学好，本课程的课余实验环节将无法正常进行。因此，教学中需要根据学生掌握先修课程基础情况，由易到难循序渐进的学习。

三、各教学环节学时分配

**教学课时分配**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 章节内容 | 讲课 | 实验 | 其他 | 合计 |
| 第一章 | 网络安全基础 | 4 |  |  | 4 |
| 第二章 | 局域网的攻击防御及控制技术 | 4 |  |  | 4 |
| 第三章 | 黑客常用的工具介绍 | 4 |  |  | 4 |
| 第四章 | 操作系统常规的安全防范方法 | 6 |  |  | 6 |
| 第五章 | 木马的攻击与防范 | 6 |  |  | 6 |
| 第六章 | 病毒攻击及其防范 | 4 |  |  | 4 |
| 第七章 | 数据的备份与恢复 | 4 |  |  | 4 |
| **合计** | | **32** |  |  | **32** |

四、教学内容

**第一章 网络安全基础**

教学内容：OSI模型和TCP/IP协议栈；常用的网络协议分析；常用的端口介绍；常用的网络命令；常用的进程服务介绍。

课程思政切入点：习总书记指出：“没有网络安全就没有国家安全，没有信息化就没有现代化。”这一论述将网络安全上升到国家安全的层面，足以看出网络安全的重要性。当前，我国网络安全人才缺口巨大，人才能力素质有待进一步提高，这与维护国家网络安全、建立网络强国的要求不相适应。作为学生，要树立为国担当的信念，积极、认真学习本课程所教授的知识点，将来做到学以致用。

重点和难点：OSI模型、TCP/IP协议、常用端口、网络命令、进程服务。

考核要求：了解OSI模型和TCP/IP协议栈的基础知识；了解常用的网络协议；掌握常用端口以及这些端口的作用；理解并掌握使用常用的网络命令来解决实际问题；了解常用的进程服务。

**第二章 局域网的攻击防御及控制技术**

教学内容：以太网的工作原理介绍；局域网内的IP攻击；隐藏本机真实的MAC地址；QQ攻击与防御；局域网内的流量控制。

重点和难点：IP攻击、隐藏MAC地址、局域网内流量控制。

考核要求：了解以太网的工作原理；局域网内的IP攻击；学会隐藏本机的MAC地址；局域网内的流量控制P2P。

**第三章 黑客常用的工具介绍**

教学内容：黑客概述；X-Scan-v3.3漏洞扫描工具；扫描端口的工具介绍；流光扫描工具；局域网综合扫描工具LanHelper介绍；Shed扫描共享目录；网络监听工具。

课程思政切入点：通过讲解境外黑客组织对我国境内系统发起的攻击案例，引导学生建立正确的价值观导向，激发学生的爱国热情。

重点和难点：黑客工具的使用。

考核要求：了解黑客由来以及黑客攻击的一般方法；掌握几种黑客常用的工具的使用方法。

**第四章**  **操作系统常规的安全防范方法**

教学内容：关闭端口、禁止服务、注册表使用、IE浏览器设置。

重点和难点：关闭端口、禁止服务、注册表使用、IE浏览器设置

考核要求：掌握增强操作系统的安全性的方法。

**第五章 木马的攻击与防治**

教学内容：木马概述；木马驻留位置；木马的功能；木马的特征；反弹式木马的原理；木马伪装；木马的免杀加壳；木马的防治；木马的综合防治。

课程思政切入点：通过讲解“棱镜门”、国家防火墙等案例，使学生认识到科技武装力量，激发学生积极投身于祖国科技行业的信心和信念。

重点和难点：木马的伪装、防治。

考核要求：了解木马的特征、功能及常驻留位置；会分析木马的伪装方法；掌握木马的防治。

**第六章 病毒攻击及其防范**

教学内容：VBS病毒的特点；VBS脚本病毒原理分析；VBS脚本病毒生产机；自定义设置VBS病毒；VBS蠕虫生成器；怎样防范蠕虫病毒；病毒的安全防治；日常病毒防治的原则。

课程思政切入点：CIH病毒、熊猫烧香病毒、“震网”病毒以及众多其他病毒对我国的经济和工业发展产生了严重的负面影响，通过详细介绍这些案例，让学生意识到信息安全的重要性，激发学生的责任感、使命感，培养学生的爱国热情。

重点和难点：病毒的生成器、病毒的防治。

考核要求：了解VBS病毒的特点、原理、生产机以及VBS蠕虫生成器；掌握防治病毒技术。

**第七章 数据的备份与恢复**

教学内容：数据恢复软件使用；Ghost备份与恢复；利用XP自带的还原功能备份与还原；注册表的备份与恢复；驱动程序的备份与恢复。

重点和难点：数据的备份与恢复。

考核要求：认识到数据备份的重要性；掌握备份和恢复的方法。

五、考核方式、成绩评定

本课程的考核分为平时考核及期末考核两种形式。其中，平时成绩占40%，期末考试成绩占60%。

平时考核采用作业、课堂案例讨论等方式。期末考核采用闭卷考试形式，要注重知识应用能力和解决问题能力的考核上，而知识点的记忆和理解要服务于学生能力的提高和巩固。

六、主要参考书及其他内容

（一）推荐教材

1．杨义先.安全通论—刷新网络空间安全观. 北京：电子工业出版社，2018。

2．林国恩，李建彬编著.信息系统安全.北京：电子工业出版社，2010。

（二）主要学习参考书

1．曾庆凯，许峰，张有东编著.信息安全体系结构.北京：电子工业出版社，2010。

2.Ross Anderson编著.信息安全工程.北京：清华大学出版社，2011。

执笔人：孙茂华 教研室主任：范烺 系教学主任审核签名：