《网络攻防技术及应用》课程教学大纲

执笔人：李勇 编写日期：2022年11月

**一、课程基本信息**

1．课程编号：M401122B

2．课程平台：专业教育平台

3．课程模块：专业拓展选修课程模块

4．课程性质：选修

5．学时/学分：32/2

6．先修课程：互联网原理与技术

7．适用专业：通信工程

8．教学单位名称：网络安全教学团队

**二、课程教学目标及学生应达到的能力**

《网络攻防技术及应用》是电子信息类通信工程专业本科生的专业拓展选修课程。本课程的主要任务是通过课堂教学、报告、讨论等环节培养学生的网络安全意识以及网络安全理论知识的应用能力，使学生掌握网络安全基本概念、基本原理与技术，熟悉基本的网络攻击和防御手段和工具，了解网络攻防技术前沿进展，具有初步的网络攻防技术应用开发能力。

培养学生正确的网络安全观和安全思维，培养网络安全应用与开发能力，为学习后续课程奠定必要的基础。本课程注重以网络安全理论与技术的发展为载体，从个人视角、组织视角、国家视角展现网络空间安全全景，将专业知识与思政育人元素相融合，引导学生树立正确的人生观、价值观、世界观和安全观。

课程目标及能力要求具体如下：

**课程目标1.** 掌握网络攻防技术基础和基本原理，包括信息采集、漏洞挖掘、隐藏、恶意代码等攻击与防范原理、方法，能运用原理和方法进行网络和系统安全攻防的设计、分析与实现，熟悉基本的网络攻击和防御手段和工具；

**课程目标2.** 培养学生的安全思维和正确的网络安全观与网络伦理，建立维护安全、可信网络空间的责任意识。

**课程目标3.** 通过研究性教学环节，锻炼学生的自主学习能力，培养学生主动扩展专业视野，独立思考和追踪技术发展趋势的意识。

**三、课程教学目标和毕业要求的对应关系**

|  |  |  |
| --- | --- | --- |
| **毕业要求** | **毕业要求指标点** | **课程目标对毕业要求的支撑关系** |
| 5. 研究 | 5.1 针对工程问题，收集信息、查阅文献、分析现有技术的特点与局限性。 | 课程目标1 |
| 9. 职业规范 | 9.1具备人文社会科学素养，理解应担负的社会责任，愿意为社会服务。 | 课程目标2 |
| 13. 终身学习 | 13.1 具备主动学习的能力，能够运用信息和文献工具，自主学习知识。 | 课程目标3 |

**四、课程思政育人目标**

**目标1.** 介绍课程相关内容的发展历史，特别是国内重要科技成果与影响力，让学生增强传统文化和民族的自豪感，坚定理想信念、厚植爱国主义情怀，以及使命感和责任感。

**目标2.** 通过介绍课程中科学家的成就和贡献，弘扬科学家的奉献精神，培养学生坚韧不拔的奋斗精神和开拓精神，严谨求实、不迷信不盲从的科学精神。

**目标3.** 引入思政案例及研究型教学，启发辩证思维，培养学生职业素养和责任意识，工匠精神，树立全面的国家安全观，使之内化为学生的精神追求、外化为学生的自觉行动。

**五、课程教学内容和要求**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **知识单元**  **（章节）** | **知识点** | **教学**  **要求** | **推荐学时** | **教学**  **方式** | **支撑课程目标** |
| 1 | 绪论 | 网络安全威胁与攻击案例 | 了解 | 2 | 讲授 | 1, 2 |
| 网络安全历史回顾 | 了解 |
| 网络攻击分类 | 掌握 |
| 网络攻击模型 | 掌握 |
| 网络攻防技术发展趋势 | 了解 |
| 2 | 攻防技术基础 | 网络安全体系结构 | 理解 | 4 | 讲授 | 1, 2 |
| 网络安全模型 | 理解 |
| 密码学基本概念 | 掌握 |
| 加密技术 | 理解 |
| 认证技术 | 理解 |
| 安全协议基础 | 了解 |
| 3 | 网络攻击技术 | 目标系统信息收集、黑客历史及发展 | 掌握 | 12 | 讲授 | 1, 2 |
| 信息踩点、端口扫描 | 了解 |
| 恶意代码 | 掌握 |
| 口令攻击 | 理解 |
| 注入攻击、缓冲区溢出攻击、跨站脚本攻击、漏洞挖掘与利用 | 掌握 |
| 欺骗攻击 | 了解 |
| 拒绝服务攻击 | 了解 |
| 4 | 网络防御技术 | 网络防御策略与体系、信息保障 | 理解 | 12 | 讲授 | 1, 2 |
| 防火墙 | 掌握 |
| 入侵检测 | 理解 |
| 公钥基础设施 | 掌握 |
| 网络认证技术 | 理解 |
| 网络安全协议 | 掌握 |
| 网络诱骗技术 | 理解 |
| 数据库安全 | 理解 |
| 应急响应与取证 | 理解 |
| 5 | 网络攻防新进展 | 高级持续性威胁 | 了解 | 2 | 讲授 | 1, 3 |
| 动态目标防御/拟态防御 | 了解 |
| 网络内容安全 | 了解 |
| 云计算安全 | 了解 |
| 大数据安全 | 了解 |

**六、课程教学方法**

本课是通信工程专业的专业选修课，需要运用计算机基础、计算机网络、信息安全理论基础等专业知识，适宜采用灵活多样的教学方式，将理论教学、自主学习、实验演示、课下自主实验等有机结合。通过课堂理论教学讲解基础原理和分析方法，指导课后学生自学部分拓展知识，并结合课程讲授指导学生开展自主实验。

教学方法设计及教学环节的安排建议和要求。其中，课堂讲授包括教学方法和手段设计；作业方面主要写明布置习题或实验达到的目的与要求，题量、题型要求等，提倡按照教学的层次设计作业，加大专题研究和研究性、综合性作业的比例，可限定比例要求。

**（一）课堂讲授**

1．在教学方法上，结合多媒体教学与传统板书，采用以面向问题的引导式教学为手段，以案例教学为载体，激发学生的学习热情，培养学生发现问题、分析问题和解决问题的能力。上课时，适当提出一些问题，引导学生分析讨论，以调动学生的主动性，活跃课堂气氛提高课堂质量。

2. 在教学内容上，注重对基本概念和基本方法的讲解，以建立概念、形成网络攻防整体思路为基础，指出每章的重点和难点部分。

3．在教学过程中，辅以网络渗透测试软件或系统（如Kali Linux）为工具，将部分攻击技术以动态过程进行形象化展示，帮助学生理解重要概念和原理，熟悉相关网络攻防工具的使用。

**（二）作业及指导分析**

本课程特点是理论与实际相结合，涉及面广，需要一定的课后作业支撑。作业题型包括计算、分析和设计等。通过作业巩固知识点的掌握，并适当布置自学作业，达到培养学生主动学习拓展知识的能力，锻炼其分析问题解决问题的能力。根据情况适当增设课堂习题指导及作业评述。

1. **课外学习**
2. 课后推荐网络攻防技术相关MOOC课程或与章节内容相关的视频资源，引导学生课外自主学习。自主学习内容不仅包括易理解的知识点，如协议基本概念；也包括需要查阅文献获得的知识，如网络攻防技术发展新热点与趋势；还可以包括延展性的知识点，如课堂上讲解漏洞挖掘的过程与方法，课后让学生自己进行一些典型的协议漏洞、Web应用漏洞的挖掘与分析。

2. 根据课程进展，推荐课外参考书目或网络资源，布置若干自主学习任务，适当对知识点进行扩展学习，完成指定的课外作业或撰写报告。

3. 课内讨论和课外答疑相结合，充分利用智慧教学平台进行线上答疑。

**（四）课后实验**

可根据课程进展布置课后实验。根据实验环境条件设置Windows/Linux帐户安全、攻防平台与工具、端口扫描、口令攻击与防御、防火墙实验、木马攻击与防御、漏洞利用与防御实验、网络攻防综合实验等实验内容。课堂布置的实验内容，学生需完成实验报告。

**（五）专题研究与讨论**

结合教学内容进展设置适当的专题，可以包括仿真分析、技术原理分析、新技术追踪等，布置学生以个人或分组方式完成技术原理或仿真分析、撰写分析报告、课堂报告分析结果并开展讨论。要求学生运用文献查找和搜索工具，自主学习与网络攻防技术相关的进展和攻防实验平台与软件，描述和分析实际工程问题，了解专业知识在相关领域的前沿应用。

通过专题研讨活动，培养学生主动学习意识和举一反三、探索质疑的思维方式，锻炼学生自主学习能力，培养学生利用计算机软件解决复杂工程问题中网络安全设计、部署、实现的能力，激发学生探究新知识的兴趣，培养良好的科学研究态度，并通过工程实践反哺理论知识学习，帮助学生在理论与实际之间建立“映射”。

研讨过程组织的参考形式及要求如下：

1. 任课教师给出若干参考题目，题目内容可以包括网络攻防某前沿技术领域文献、对网络攻防某方面方法或技术的归纳总结、实际网络安全应用案例的描述和设计与分析等，要求学生自主完成文献查阅、数据收集、分析归纳等，提交研讨报告，并完成答辩展示。

2. 研讨报告内容主要包括问题描述、主要工具与方法、解决方案描述，理论分析和实验结果。

3. 学生个人或分组完成实验分析或理论研讨，提交书面分析报告，并进行课堂口头报告和讨论，对关键问题进行评讲。在课堂讨论中，引导同学交流研究心得，提出问题，开展讨论，对分析研究的结果进行评价比较，从而使学生能够相互借鉴，从不同角度获得对同一问题的充分理解，或交流探讨网络安全理论或应用最新进展，相互促进，共同提高。

**（六）课程思政**

课程思政坚持正确的政治方向，紧紧围绕立德树人根本任务，针对《网络攻防技术及应用》课程学科交叉性强、理论结合实践的特点，细化分解课程思政育人主题，深挖知识点中隐含的思政元素，将课程思政案例（见下表）有机融入相关知识点和教学环节中，通过案例讲解、学生提问、课后调研、课堂展示等方式，在进行知识传授、能力培养的同时，以“润物无声”的形式浸润学生心灵，使之内化为学生的精神追求、外化为学生的自觉行动。

表1《网络攻防技术及应用》思政案例

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 章节名称 | 知识点 | 所挖掘的思政元素 |
| 1 | 第1章 绪论 | 网络安全威胁与攻击案例 | 【**时事政治 责任担当**】**-安全事件介绍**  **1、美国封禁华为、断供华为芯片事件**  激发学生对“卡脖子技术”研发的危机感、增强我国网信领域关键技术自主可控能力的责任感和爱国情怀。  **2、震网攻击、勒索软件、俄乌冲突与网络战等**  理解网络空间安全与国家主权、国家利益的关系，培养“没有网络安全就没有国家安全”的网络安全观，弘扬爱国主义精神，树立为实现中华民族伟大复兴而努力学习的使命感与责任感。 |
| 2 | 第2章 攻防技术基础 | 密码学的发展历程；代换密码 | 【**爱国主义 家国情怀**】-**红色密码**  **1、周恩来与“豪密”**  中国共产党和中国工农红军第一本无线电通讯密码。  **2、永不消逝的电波**  介绍人物原型：李白，100位为新中国成立做出突出贡献的英雄模范的故事。 |
| 3 | 第2章 攻防技术基础 | 杂凑函数 | 【**科学精神**】-**王小云对系列密码杂凑算法的碰撞攻击**  该成果直接导致了美国NIST开始面向全球征集新一代安全杂凑算法标准。宣传中国科学家刻苦钻研的精神和为国奉献的情怀，深刻理解“网络安全要尽快在核心技术上取得突破”这个观点，提高学生对核心技术必须自主可控的认识，认识密码算法安全是国家安全的重要组成部分。 |
| 4 | 第5章 网络攻防新进展 | 网络内容安全 | 【**安全思维 爱国情怀】**-**美国瓦解前苏联、美国搞垮乌克兰的案例**  使学生认清霸权国家用经济打压、军备竞赛、心理战和舆论战、传播所谓的“民主与自由”、发动“橙色革命”等手段的本质。通过网络煽动极端情绪和传播虚假的政治观点，会危害一个国家的安全和社会的稳定。 |

**七、课程考核**

本课程考核包括作业与研讨、阶段随堂测验、课后实验、综合作业四个部分，四部分的成绩占课程总成绩的权重分别是20%、20%、20%、40%。

|  |  |  |  |
| --- | --- | --- | --- |
| 考核环节 | 建议分值 | 考核/评价细则 | 对应的课程目标 |
| 作业与研讨 | 20 | （1）主要考核学生对章节知识点的复习、理解和掌握程度；  （2）作业按10分制单独评分，多次作业取各次成绩的平均值作为此环节的最终成绩。 | 1,2,3 |
| 阶段随堂测验 | 20 | （1）可设置结合某场景的综合应用题，分析相应的攻击与防御措施和机制，并给出安全建议。 | 1 |
| 课后实验 | 20 | （1）结合章节讲授内容，考核学生对网络攻防相关机制、算法的理解和掌握程度。  （2）实验内容可包括经典加密算法设计与实现、信息搜集与扫描等。  （3）实验报告按报告模板各内容模块和要求进行整理。 | 1,2,3 |
| 综合作业 | 40 | （1）考查学生自主学习、独立思考和拓展专业知识的能力。并且通过口头和文字表达能力以及讨论交流过程评价学生的掌握程度。  （2）由教师根据专题报告、研究成果展示等综合评定，辅以完成课堂综合作业。 | 1,2,3 |

课程总成绩根据四部分成绩计算后综合评定：

**课程成绩=作业成绩×0.2+阶段随堂测验成绩×0.2+课后实验成绩×0.2+综合作业成绩×0.4**

课程总成绩由百分制对应转换成五级十一段制（A、A-、B+、B、B-、C+、C、C-、D+、D、F）。绩点与成绩的换算关系如下：

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 百分制成绩 | 100-90 | 89-  85 | 84-  81 | 80-  78 | 77-  75 | 74-  72 | 71-  68 | 67-  65 | 64-  63 | 62-  60 | 60以下 |
| 五级制成绩 | A | A- | B+ | B | B- | C+ | C | C- | D+ | D | F |
| 绩点 | 4.0 | 3.7 | 3.3 | 3 | 2.7 | 2.3 | 2.0 | 1.7 | 1.3 | 1.0 | 0 |

**八、本课程与其它课程的联系与分工**

本课程的先修课程为“互联网原理与技术”。相关选修课：信息安全理论基础(B)、信息安全管理与风险评估、信息系统安全，课程间内容应避免重复。

**九、建议教材及教学参考书**

［1］ C.Kaufman等著, 许剑卓等译, 网络安全—公众世界中的秘密通信, 第二版. 北京. 电子工业出版社, 2004

［2］安德森 著, [齐宁](http://www.dangdang.com/author/%C6%EB%C4%FE_1" \t "http://product.dangdang.com/_blank), [韩智文](http://www.dangdang.com/author/%BA%AB%D6%C7%CE%C4_1" \t "http://product.dangdang.com/_blank), [刘国萍](http://www.dangdang.com/author/%C1%F5%B9%FA%C6%BC_1" \t "http://product.dangdang.com/_blank) 译, 信息安全工程, 第2版. 北京. [清华大学出版社](http://www.dangdang.com/publish/%C7%E5%BB%AA%B4%F3%D1%A7%B3%F6%B0%E6%C9%E7_1" \t "http://product.dangdang.com/_blank). 2012

［3］James Graham, Ryan Olson, Rick Howard, Cyber Security Essentials. CRC Press. 2011.

［4］诸葛建伟, 网络攻防技术与实践. 北京. 电子工业出版社. 2011

［5］[卿斯汉](http://www.dangdang.com/author/%C7%E4%CB%B9%BA%BA_1" \t "http://product.dangdang.com/_blank), 蒋建春 编著, 网络攻防技术原理与实战. 北京. [科学出版社](http://www.dangdang.com/publish/%BF%C6%D1%A7%B3%F6%B0%E6%C9%E7_1" \t "http://product.dangdang.com/_blank). 2011

［6］牛少彰, 江为强, 网络的攻击与防范——理论与实践. 北京. 北京邮电大学出版社. 2006

［7］吴礼发, 洪征, 李华波, 网络攻防原理与技术（第2版）. 北京. 机械工业出版社. 2017

［8］张玉清, 陈深龙, 杨彬, 网络攻击与防御技术实验教程. 北京. 清华大学出版社. 2010

［9］吴礼发, 洪征, 计算机网络安全原理. 北京. 电子工业出版社. 2020

**十、大纲审核人**

**十一、学院审核程序说明**

由网络安全教学团队制定，负责本科教学工作的系主任审核，经学院教学指导委员会审核批准。

1. **学院审定日期**

**附：达成度评价方法：**

课程目标达成度评价包括课程分目标达成度评价和课程总目标达成度评价，具体计算方法如下：





课程目标评价内容及符号意义说明如附表1，字母*A*、*B*、*C、D*则分别表示作业与研讨、阶段随堂测验、课后实验、综合作业的实际平均得分。

附表1 课程评价考核基本信息表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **课程目标评价内容** | **作业与研讨** | **阶段随堂测验** | **课后实验** | **综合作业** | **课程总评成绩** |
| 目标  分值 | 20 | 20 | 20 | 40 | 100 |
| 学生平均得分 | *A* | *B* | *C* | *D* | *A*+*B*+*C+D* |

课程目标达成度评价值计算具体说明如附表2。

附表2课程达成度评价计算方法

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课程目标** | **考核环节** | **目标分值** | **学生平均得分** | **达成度计算示例** |
| 课程目标1 | 作业与研讨 | 20 | *A*1 |  |
| 阶段随堂测验 | 20 | *B*1 |
| 课后实验 | 20 | *C*1 |
| 综合作业 | 40 | *D*1 |
| 课程目标2 | 作业与研讨 | 20 | *A*2 |  |
| 课后实验 | 20 | *C*2 |
| 综合作业 | 40 | *D*2 |
| 课程目标3 | 作业与研讨 | 20 | *A*2 |  |
| 课后实验 | 20 | *C*2 |
| 综合作业 | 40 | *D*2 |
| 课程总体目标 | 总评成绩 | 100 | *A*+*B*+*C+D* |  |