《网络安全技术（Network security technology)》

教学大纲

制定时间：2020 年 03 月（2024 年 4 月修订）

一、课程基本信息

（一）适用专业：本科计算机科学与技术

（二）课程代码：3DX0564A

（三）学分/课内学时：3 学分/48 学时

（四）课程类别：专业教育

（五）课程性质：必修/理论课

（六）先修课程：《计算机网络》、《C 语言程序设计》、《TCP/IP 协议编程》、《操作系统》、《数据结构》等

（七）后续课程：《网络安全技术综合训练》、《网络测试与故障诊断》、《毕业设计》

二、课程教学目标

《网络安全技术》课程是计算机科学与技术专业的专业必修课程，内容涉及网络安全概述、信息收集技术、口令破解、欺骗攻击、Web 安全技术、木马及病毒、网络安全防御技术等。学生在学习完本课程后，应达到对网络安全的基本概念、防护原理及使用有较深程度的理解和掌握；能配置基本的 Web 服务安全；能够运用独立解决在网络安全方面遇到的一些比较基本的问题；能够维护网路服务器的安全以及个人电脑的网络安全；能够结合网络安全技术，能对现有网络进行安全管理。该课程有利于激发学生的学习动机和提高学习兴趣，最终达到让学生掌握该课程所传授的技能，并能将这些技能应用到未来的工作中。

按照“以能力为本位、以职业实践为主线、模块化课程体系”的总体设计要求，该门课程以满足以下要求为基本理念：一是辅助学生学习，重点帮助学生巩固所学的网络安全相关知识，诱导学生积极思考，帮助学生发现探索知识；二是用于学生的兴趣扩展，使学生掌握一定的网络安全管理技能，重点用于帮助学生发展兴趣爱好、增长见识、形成个性；三是培养学生的爱国意识和遵纪守法意识，养成吃苦耐劳、爱岗敬业、团队协作的职业精神和诚实、守信、善于沟通与合作的良好品质，为发展职业能力奠定良好的基础。

（一）具体目标

目标 1：理解网络安全的现状，理解网络安全法，了解常用网络安全技术，能将其应用于分析复杂网络中的安全问题。

目标 2：能够对中小型企业网络进行基本的安全管理。能识别和判断软件系统中的涉及

的网络安全问题。

目标 3：能够完成常见的网络攻击和防御。能运用基本原理分析实际工程的影响因素，证实解决方案的合理性。

目标 4：了解网络信息安全体系。能够选择和使用适当的技术手段、现代工程工具和信息技术工具，解决计算机网络应用过程中遇到的网络工程及网络安全问题。了解国家网络安全观。

（二）课程目标与毕业要求的对应关系

毕业要求	毕业要求指标点	课程目标	教学单元	评价方式
1.掌握专业必需的数学、自然科学、工程基础和专业知识，能够用于解决计算机软件开发中的复杂工程问题。	指标点 1.3：掌握计算机软件与理论、计算机系统结构、计算机应用技术的基本理论、基本知识和基本技能。	目标 1	网络安全技术概述、过程攻击的一般步骤信息收集技术	纸笔考试 课内实验
2.能够应用数学、自然科学和工程科学的基本原理，识别、表达、并通过文献研究分析系统中的安全问题，以获得有效结论。	指标点 2.5：能运用等级保护基本原理分析实际工程的影响因素，证实解决方案的合理性。	目标 2	口令破解与防御技术、欺骗攻击与防御技术	纸笔考试 课内实验
5.能够针对计算机应用系统的复杂工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息技术工具，实现对复杂工程问题的预测与模拟，理解其局限性。	指标点 5.3：能够选择和使用适当的技术手段、现代工具，解决计算机网络应用过程中遇到的网络工程及网络安全问题。	目标 3	Web 攻击与防御技术、SQL 攻击与防御技术、跨站脚本攻击技术的实现及防御	纸笔考试 课内实验
6.能够基于工程背景知识和技术标准，对计算机应用系统工程进行合理分析，评价系统及其复杂工程问题解决方案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。	指标点 6.3：能识别和分析计算机应用系统的安全潜在影响；能评价系统失效对社会、健康、安全、法律以及文化的潜在影响。	目标 4	木马攻击与防御技术、计算机病毒、典型防御技术	纸笔考试 课内实验

三、教学内容与方法

（一）教学内容及要求

序号	教学单元	教学内容	学习产出要求	推荐学时	推荐教学方式	支撑课程目标	备注
1	网络安全技术概述	网络安全的定义、特征及重要性，网络安全法,网络安全的主要威胁因素，常用的网络安全防范措施,网络安全策略,网络安全体系设计,远程攻击的步骤。	掌握网络安全的定义，理解网络安全的特征及重要性，了解网络安全法；了解网络安全的威胁因素，理解常用的网络安全防范措施，了解网络安全策略及网络安全体系设计，掌握远程攻击的步骤。	4	讲授	目标 1	自主学习
2	信息收集技术	扫描器、扫描过程、扫描类型，端口扫描技术，常用的扫描器，网络嗅探,扫描及嗅探的防御。	了解网络安全扫描技术的原理，掌握端口扫描技术，掌握几类扫描器的应用方法，掌握网络嗅探的原理及常用工具，掌握扫描及嗅探的防御技术。	6	讲授	目标 1	自主学习
3	口令破解与操作系统安全	口令的历史与现状,口令破解方式,口令破解工具,口令破解的防御,操作系统权限安全管理。	了解口令的历史与现状，掌握常用的口令破解方式，掌握常用口令破解工具，了解口令破解的防御，掌握操作系统权限安全管理。	2	讲授	目标 2	自主学习
4	欺骗攻击及防御	欺骗攻击概述，IP 欺骗攻击及防御，ARP 欺骗攻击及防御,电子邮件欺骗攻击及防御，DNS 欺骗攻击及防	掌握 IP 欺骗攻击及防御的相关技术，掌握 ARP 欺骗攻击及防御，电子邮件欺骗攻击及防御，DNS 欺骗攻击及防御，Web 欺骗攻击及防御，拒绝服务攻击及	4	讲授	目标 2	自主学习

序号	教学单元	教学内容	学习产出要求	推荐学时	推荐教学方式	支撑课程目标	备注
		御，Web 欺骗攻击及防御，拒绝服务攻击及防御。	防御。				
5	Web 安全技术	Web 安全概述，Web 服务器指纹识别，Web 页面盗窃及防御，跨站脚本攻击及防御，SQL 注入攻击及防御，Google Hacking，网页验证码，防御 Web 攻击。	了解 Web 安全相关概念，了解 Web 服务器指纹识别，掌握 Web 页面盗窃及防御，掌握跨站脚本攻击及防御，掌握 SQL 注入攻击及防御，理解 Google Hacking，了解网页验证码，掌握常用 Web 攻击防御策略。	8	讲授	目标 3	自主学习
6	黑客与木马攻防技术	黑客的概念及攻击途径，木马概述，木马的实现原理与攻击步骤，木马实例介绍，木马的防御技术，木马的发展趋势。	了解黑客的概念，理解黑客的攻击途径，了解木马的相关概述，理解木马的实现原理与攻击步骤，掌握木马的应用，掌握木马的防御技术，了解木马的发展趋势。	2	讲授	目标 3	自主学习
7	计算机病毒攻防技术	计算机病毒概述，计算机病毒工作原理与分类，典型的计算机病毒，计算机病毒的预防与清除，计算机病毒技术的新动向，手机病毒。	了解计算机病毒的相关概念及发展，掌握计算机病毒的工作原理，掌握计算机病毒的分类，了解典型的计算机病毒，掌握计算机病毒的预防与清除，了解计算机病毒技术的新动向，了解手机病毒。	2	讲授	目标 4	自主学习

序号	教学单元	教学内容	学习产出要求	推荐学时	推荐教学方式	支撑课程目标	备注
8	典型防御技术	加密技术,身份认证，防火墙，入侵检测系统，虚拟专用网技术，日志和审计，蜜罐与取证。	掌握加密技术，理解身份认证，掌握防火墙技术和入侵检测系统应用，理解虚拟专用网技术，了解日志和审计，了解蜜罐技术与取证。	4	讲授	目标 4	自主学习
9	实验一	信息收集技术	X-Scan、Nmap 等扫描工具的应用，实现各类端口扫描。Wireshark 等嗅探工具的应用。	2	讲授 示范 实验	目标 1 目标 2	
10	实验二	口令破解	词典攻击、暴力破解、组合攻击等口令破解方法的实现。Linux、Windows 操作系统口令破解工具的应用。	2	讲授 示范 实验	目标 1 目标 2	
11	实验三	欺骗攻击	IP 欺骗、ARP 欺骗等欺骗攻击技术实现。	2	讲授 实验	目标 1 目标 2	
12	实验四	网络层欺骗攻击	DNS 欺骗、Web 欺骗等欺骗攻击技术实现	2	讲授 示范 实验	目标 1 目标 2	
13	实验五	应用层欺骗攻击	跨站脚本攻击技术的实现及防御。SQL 注入攻击及防御。Google Hacking 的实际应用。	2	讲授 示范 实验	目标 1 目标 3	
14	实验六	木马攻击	常见木马工具的应用，木马的清除及防御。	2	讲授 示范 实验	目标 3 目标 4	
15	实验七	计算机病毒	常见计算机病毒的实现，常用杀毒软件的使用和杀毒原理。病毒的清除及防御。	2	讲授 实验	目标 3 目标 4	
16	实验八	防火墙及入侵检测	操作系统防火墙的配置，入侵检测系统的应用。	2	讲授 实验	目标 1 目标 4	

（二）教学方法

1.课堂讲授

（1）采用启发式教学，以学生为中心，激发学生主动学习的兴趣，培养学生独立思考、分析问题和解决问题的能力，引导学生主动通过实践和自学获得自己想学到的知识。

（2）在教学内容上，系统讲授网络安全技术概述、信息收集技术、口令破解与操作系统安全、欺骗攻击及防御、Web 安全技术、黑客与木马攻防技术、计算机病毒攻防技术、典型防御技术等。

（3）在教学过程中采用多媒体教学与传统板书、教具教学相结合，提高课堂教学信息量，增强教学的直观性。

（4）理论教学与工程实践相结合，引导学生应用数学、自然科学和工程科学的基本原理，采用现代设计方法和手段，掌握网络安全技术，解决实际应用中面临的网络安全问题，培养学生分析问题、解决问题的思维方法和实践技能。

2.实验教学

实验教学是网络安全技术课程中教学过程中重要的环节，目的是培养学生运用实验方法研究解决网络应用领域面临的威胁的能力。课程必做实验 8 个，各实验按照实验指导书要求学生独立完成，并提交实验报告。同时，利用网络攻防与移动互联安全实验室的教学资源，发布额外实验题目，鼓励学生结合自己的兴趣进行自主实验。

四、考核及成绩评定

（一）考核内容及成绩构成

课程目标	考核内容	成绩评定方式	成绩占总评分比例	目标成绩占当次考核比例	学生当次考核平均得分	目标达成情况计算公式
目标 1：理解网络安全的现状，理解网络安全法，了解常用网络安全技术，能将其应用于分析复杂网络中的安全问题。	网络安全的基本概念，网络安全法，网络安全的主要威胁因素，常用的网络安全防范措施，网络安全策略，网络安全体系设计，远程攻击的步骤，信息收集及防御技术	纸笔考试	15%	100%	T1	$\left(\frac{T1}{100\%}\times 15\% + \frac{A1}{50\%}\times 5\%\right)$ / 20
		平时作业	5%	50%	A1	

课程目标	考核内容	成绩评定方式	成绩占总评分比例	目标成绩占当次考核比例	学生当次考核平均得分	目标达成情况计算公式
目标 2：能够对中小型企业网络进行基本的安全管理。能识别和判断软件系统中的涉及的网络安全问题。	口令破解方式、工具及防御，欺骗攻击概述，IP、ARP、电子邮件、DNS、Web、拒绝服务等攻击及防御。	纸笔考试	20%	90%	T2	$\frac{(\frac{T2}{100\%}\times 20\% + \frac{E1}{50\%}\times 10\%)}{20}$
		实验	10%	80%	E1	
目标 3：能够完成常见的网络攻击和防御。能运用基本原理分析实际工程的影响因素，证实解决方案的合理性。	黑客，木马的实现原理、攻击步骤与防御技术，计算机病毒工作原理与分类，计算机病毒的预防与清除，计算机病毒技术的新动向，手机病毒。	纸笔考试	20%	100%	T3	$\frac{(\frac{T3}{100\%}\times 20\% + \frac{E2}{50\%}\times 10\%)}{20}$
		实验	10%	80%	E2	
目标 4：了解网络信息安全体系。能够选择和使用适当的技术手段、现代工程工具和信息技术工具，解决计算机网络应用过程中遇到的网络工程及网络安全问题。	Web 安全概述，Web 服务器指纹识别，Web 页面盗窃及防御，跨站脚本攻击及防御，SQL 注入攻击及防御，网页验证码，防御 Web 攻击。加密技术，身份认证，防火墙，入侵检测系统，虚拟专用网技术，日志和审计，蜜罐与取证。	纸笔考试	15%	100%	T4	$\frac{(\frac{T4}{100\%}\times 15\% + \frac{A2}{50\%}\times 5\%)}{20}$
		平时作业	5%	50%	A2	
总评成绩（100%）=实验（20%）+纸笔考试（70%）+平时作业（10%）			100%	——	——	$\frac{\text{学生总评平均分}}{100}$

（二）平时考核成绩评定

1.实验

实验 8 次，支持目标 2、目标 3，共占总评分 20%，目标 1 占 10%、目标 3 占 10%。对应目标评分标准如下：

对应目标		目标 2：能够对中小型企业网络进行基本的安全管理。能识别和判断软件系统中的涉及的网络安全问题。	目标 3：能够完成常见的网络攻击和防御。能运用基本原理分析实际工程的影响因素，证实解决方案的合理性。
考查点		实验内容	实验报告
总评分占比		50%	50%
评分标准	**100%至90%**	安全管理策略制定科学、严谨；熟练使用各类网络安全工具，能够准确分析网络安全中的相关漏洞及缺陷；能够提出可行的网络安全解决方案，效果良好。	有很强的总结实验和撰写报告的能力，实验报告内容完整、正确，有很好的分析与见解。文本表述清晰，书写工整，格式规范，专业术语用语准确。
	89.9%至80%	安全管理策略制定科学；熟练使用各类网络安全工具，能够准确分析网络安全中的相关漏洞及缺陷；能够提出可行的网络安全解决方案。	有较强的总结实验和撰写报告的能力，实验报告内容完整、正确，有较好的分析与见解。文本表述较为清晰，书写比较工整，格式规范。
	79.9至70%	安全管理策略制定较为完备；熟练使用主流网络安全工具，能够准确分析网络安全中的相关漏洞及缺陷；能够提出可行的网络安全解决方案。	有良好的总结实验和撰写报告的能力，实验报告内容较完整、正确，有自己的分析与见解。文本表述较为清晰，书写较为工整，格式较为规范。
	69.9%至60%	安全管理策略制定合理；能够使用主流的网络安全工具，能够分析网络安全中的相关漏洞及缺陷；能够提出适当的网络安全解决方案。	有一定的总结实验和撰写报告的能力，实验报告内容基本完整、正确，没有分析或见解。文本表述基本清晰，书写基本工整，格式基本规范。
	59.9%至0	安全管理策略制定有待完善；能够使用一些网络安全工具，对网络安全中的相关漏洞及缺陷有所了解；对网络安全解决方案的制定缺乏完整性和可行性。	总结实验和撰写报告的能力差，实验报告内容不完整、错误多。文本表述不清晰，书写潦草、格式不规范。

2.平时作业

平时作业 2 次，支持目标 1、目标 4，共占总评分 10%，目标 1 占 5%、目标 4 占 5%。对应目标评分标准如下：

对应目标		目标 1：理解网络安全的现状，理解网络安全法，了解常用网络安全技术，能将其应用于分析复杂网络中的安全问题。	目标 4：了解网络信息安全体系。能够选择和使用适当的技术手段、现代工程工具和信息技术工具，解决计算机网络应用过程中遇到的网络工程及网络安全问题。
考查点		作业内容	成果显示、讲解
总评分占比		50%	50%
评分标准	**100%至90%**	对网络安全现状了解深入，对技术应用熟练；能够根据提出的问题，构建可行的解决方案，并具有个人独到的见解。	有很强的分析总结和撰写报告的能力，有很好的分析与见解；作业文本表述清晰，书写工整，格式规范，专业术语用语准确；态度端正。
	89.9%至80%	对网络安全现状了解深入，对技术应用相对熟练；能够根据提出的问题，构建基本可行的解决方案，并具有个人的见解。	有很强的分析总结和撰写报告的能力，有很好的分析与见解；作业文本表述清晰，书写工整，格式规范；态度端正。
	79.9至70%	对网络安全现状了解，对技术应用熟练；能够根据提出的问题，构建有一定参考价值的解决方案，并具有个人见解。	有良好的分析总结和撰写报告的能力，有个人的分析与见解；作业文本表述清晰，格式相对规范；态度相对端正。
	69.9%至60%	对网络安全现状基本了解，对技术应用水平一般；能够根据提出的问题，构建有一定参考价值的解决方案，但缺乏个人见解。	有一定的分析总结和撰写报告的能力，作业文本表述清晰，格式基本规范，但缺少个人的分析与见解；态度基本端正。
	59.9%至0	对网络安全现状了解甚少，对技术应用水平非常一般；对提出的问题，很难独立完成解决方案的构建；对相关安全问题缺乏个人见解。	分析总结能力差，作业内容描述不完整、错误多。文本表述不清晰，书写潦草、格式不规范；态度不端正。

五、参考学习资料

（一）推荐教材：吴礼发，洪征，李华波. 网络攻防原理与技术. 北京：机械工业出版社，2023.

（二）参考资料：

贾铁军. 网络安全技术及应用实践教程. 北京：机械工业出版社，2016.

王艳军, 崔升广. 计算机网络安全技术（微课版）. 北京：人民邮电出版社, 2024.

（三）在线资源：《网络安全——应用技术与工程实践》https://www.icourse163.org/learn/BIT-1449611164?tid=1450076442

360 网络安全大学：https://university.360.cn/index.html

制订人：　葛继科　　审核人：刘金源

2024 年 4 月