

课程大纲

课程编号: 0839X6M04002H **课时:** 60 **学分:** 3.00 **课程属性:** 专业核心课 **主讲教师:** 张玉清等

课程名称: 网络攻防基础21-22春季

课程英文名称: oundation of Network Attack and Defense

教学目的、要求

本课程是网络空间安全学科研究生的专业核心课,讲授软件安全的基本原理、软件防御机制与攻击手段的博弈演进、软件脆弱性(漏洞)原理分析,以及确保软件安全性的最佳实践方法。课程以软件安全国际知名学者Gary McGraw的三部著作作为教材,让同学通过课程学习与动手实践,深入理解软件的安全内构(building security in)本质与方法,提升在开发过程中确保软件安全性的专业技能;同时,理解软件的漏洞利用与防范在网络空间攻防对抗中的关键地位,掌握围绕软件攻防的“白帽”与“黑帽”思维方法和基本技术,为进一步研习网络攻防奠定基础。

预修课程

计算机网络,高级语言程序设计

教材

主要内容

第一章 网络安全概述 3学时 张玉清

第1节 网络安全概述

第二章 扫描与防御技术 3学时 张玉清

第1节 扫描与防御技术

第三章 网络监听及防御技术 3学时 张玉清

第1节 网络监听及防御技术

第四章 网络监听实验 3学时 张玉清

第1节 网络监听实验

第五章 口令破解与防御技术 3学时 张玉清

第1节 口令破解与防御技术

第六章 欺骗攻击及防御技术 3学时 张玉清

第1节 欺骗攻击及防御技术

第七章 拒绝服务攻击与防御技术 3学时 张玉清

第1节 拒绝服务攻击与防御技术

第八章 缓冲区溢出攻击及防御技术 3学时 张玉清

第1节 缓冲区溢出攻击及防御技术

第九章 缓冲区溢出实验 3学时 张玉清

第1节 缓冲区溢出实验

第十章 Web攻击及防御技术 3学时 张玉清

第1节 Web攻击及防御技术

第十一章 逆向工程 3学时 龚晓锐

第1节 逆向工程

第十二章 恶意代码分析、网络安全竞赛 3学时 龚晓锐

第1节 恶意代码分析、网络安全竞赛

第十三章 实验报告、恶意代码分析案例 3学时 龚晓锐

第1节 实验报告、恶意代码分析案例

第十四章 网络战与APT攻击 3学时 吴槟

第1节 网络战与APT攻击

第十五章 新型后门、木马与勒索软件 3学时 吴槟

第1节 新型后门、木马与勒索软件

第十六章 隐蔽回传技术、基于脚本的恶意代码 3学时 吴槟
第1节 隐蔽回传技术、基于脚本的恶意代码
第十七章 网安行业分析 基于Fuzzing技术的漏洞挖掘及利用
第1节 网安行业分析 1学时 吴槟
第2节 基于Fuzzing技术的漏洞挖掘及利用 2学时 张玉清
第十八章 安全漏洞概述 3学时 张玉清
第1节 安全漏洞概述
第十九章 人工智能与网络安全 3学时 张玉清
第1节 人工智能与网络安全
第二十章 考试 3学时 张玉清
第1节 考试

参考用书

课程教师信息

张玉清,教授、博士生导师,国家计算机网络入侵防范中心主任。主要从事网络与信息系统安全方面的研究与开发工作,在国内外重要学术刊物和学术会议上发表学术论文100余篇,先后承担国家重点研发计划项目、国家发改委信息安全专项、国家863项目、中国科学院知识创新工程重要方向项目和国家自然科学基金等课题。主要研究方向:网络攻击与防护、安全漏洞、智能手机安全等。曾主讲《网络攻击与防范》、《软件与系统安全分析》等研究生课程。

龚晓锐,男,正高级工程师,硕士生导师。主要围绕网络攻防、软件逆向分析、恶意代码对抗等方向开展研究,先后主持或参与国家保密局重点项目、中国科学院先导专项、国家重点研发计划、北京市科技计划等项目,国家关键信息基础设施网络攻防实战演习裁判长。申请发明专利十余项,已获授权12项。创建并指导的NeSE战队是国内CTF社区中的一线战队,近2年在国际大赛中保持全球前20的成绩。在教学、授课方面具有较好的经验。

吴槟,男,博士,副研究员,任职于中科院信工所信息安全国家重点实验室,中国科学院大学网安学院岗位教师,中国计算机学会高级会员、ACM 会员。先后主持了国家自然科学基金项目、发改委信息安全专项工程子系统研制项目、中科院先导专项子课题等10余项;担任国家自然科学基金联合基金重点项目联合单位主持人、国家863计划项目副组长。申请发明专利7项,获得专利授权2项,发表论文5篇,在教学、授课方面具有较好的经验。