**南开大学本科课程教学大纲**

**一、课程信息**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **课程名称** | | 恶意代码分析与防治技术 | | | | | | | | | |
| **英文名称** | | Practical Malware Analysis | | | | | | | | | |
| **课程代码** | | COMP0070 | | | | | | | | | |
| **课程类别** | | □通识必修课 □通识选修课  ■专业必修课 □专业选修课 | | | | | | | | | |
| **学分** | | 2.5 | | **主讲学时** | 34 | **实践学时** | 30 | | **总学时** | | 64 |
| **授课语言** | | □中文 □全英文 ■双语 □外语语言类 （单选） | | | | | | | | | |
| **成绩类型** | | ■百分制 □等级制（通过/不通过）（单选） | | | | | | | | | |
| **开课单位** | | 网络空间安全学院、计算机学院 | | | | | | | | | |
| **先修课程** | | 汇编语言与逆向技术 | | | | | | | | | |
| **课程负责人** | | 王志 | | | | | | | | | |
| **课程教材与参考资料** | | | | | | | | | | | |
| **教**  **材** | **作者** | | **名称** | | | **出版社** | | **ISBN** | | **出版时间** | |
| Michael Sikorski and Andrew Honig | | Practical Malware Analysis | | | No Starch Press | | 1593272901 | | Michael Sikorski and Andrew Honig | |
| **参**  **考**  **资**  **料** | **作者** | | **名称** | | | **出版社** | | **ISBN** | | **出版时间** | |
| Kip Irvine | | 汇编语言：基于x86处理器 | | | 机械工业出版社 | | 9787111530367 | | Kip Irvine | |
| Charles Petzold | | Windows程序设计 | | | 人民邮电出版社 | | 9787115329769 | | Charles Petzold | |

**二、中文课程简介**

|  |
| --- |
| （简要介绍课程的目标、主要授课内容、授课对象以及在学生培养中的作用，150—500字。）  恶意代码分析与防治技术课程是信息安全专业的一门基础课程，该课程培养学生对计算机恶意代码进行逆向分析的能力，以及应急响应恶意代码攻击事件的能力。课程内容包括：恶意代码基本概念和分类、二进制代码反汇编、恶意代码的静态和动态分析技术、Windows恶意代码分析、Windows内核调试、恶意代码行为分析等。课程授课对象是三年级本科生。通过本课程的学习，学生可以进行恶意代码逆向分析，剖析恶意代码的内部逻辑，具备与他人合作的意识和能力，能够与其他成员合作完成恶意代码解决方案的设计，为学生进一步从事信息安全相关的工作、科研打下坚实基础。 |

**三、英文课程简介**

|  |
| --- |
| （中文课程简介的英文翻译版。）  "Practical Malware Analysis" is a basic course for information security students. The goal of the course is to cultivate students' ability of malware reverse engineering, and the emergency response ability to malware incident. The content of the course includes: malware basic concepts and classification, binary code disassembly, static and dynamic malware analysis skills, windows malware analysis, windows kernel debugging, malware behavior analysis etc. The course is for the third-year undergraduate students. In this course, students can independently analyze malware behaviors and understand malware internal logic, and have the ability to cooperate with others to design the solution for malware incident. This course lays a solid foundation for students to further engage in information security work or research. |

**四、课程目标**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| （需根据课程性质，描述课程教学在培养学生在知识、能力、素质等方面的贡献，以及课程思政相关目标。）  目标1：理解恶意代码的基本概念、分析目标和技术，掌握恶意代码静态基础和动态基础分析等多种可选择技术，并能够通过文献研究寻求可替代的解决方案；  目标2：会使用虚拟机建立恶意代码动态分析环境，掌握对用户态或内核态恶意代码进行动态分析的方法，正确采集和分析恶意代码的动态行为，提取恶意代码检测特征；  目标3：理解恶意代码存活机制、提权方法、隐蔽启动、数据加密方法，能够选择与使用恰当的分析工具提取恶意代码的特征，设计和开发Yara检测引擎检测规则或者开发机器学习检测模型，实现有效的恶意代码识别与防治。  目标4：、具备与他人合作的意识和能力，能够在团队中独立完成指定任务或者与其他成员合作完成任务，在团队合作中能够履行个体、团队成员或负责人的职责。  **课程目标与毕业要求对应关系**  **（通识课可不填写下列内容）**   |  |  | | --- | --- | | **课程目标** | **毕业要求指标点** | | **课程目标1** | **2.3能够综合分析解决复杂信息安全工程问题的多种可选择方案，并通过文献研究寻求可替代的解决方案。** | | **课程目标2** | **4.3能够根据实验方案构建实验系统，安全地开展实验、正确地采集和分析实验数据，规范地表述实验结果。** | | **课程目标3** | **5.2能够选择与使用恰当的技术、资源、现代工程工具、现代信息技术工具和相关辅助软件对复杂信息安全工程问题进行分析、计算、设计与开发。** | | **课程目标4** | **9.2能够在信息安全工程实践活动中承担个体和团队成员的角色，在团队中独立或合作开展工作。** |   注：课程目标可填写对应相应序号，如“目标2”。课程目标不一定与毕业要求一一对应。 |
|  |

**五、课程内容与教学安排**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **教学内容** | **学时** | **教学方式** | **对应课程目标** |
| 1 | 第1章 恶意代码分析概述  第1.1节 恶意代码分析目标  第1.2节 恶意代码分析技术  第1.3节 恶意代码类型  第1.4节 恶意代码分析通用规则 | 2 | 讲授 | 目标1 |
| 2 | 第2章 静态基础分析技术  第2.1节 反病毒引擎  第2.2节 哈希值  第2.3节 字符串查找  第2.4节 加壳与混淆  第2.5节 文件格式 | 2 | 讲授 | 目标1 |
| 3 | 第3章 虚拟机分析恶意代码  第3.1节 虚拟机的结构  第3.2节 创建虚拟机  第3.3节 虚拟机的使用  第3.4节 虚拟机的风险  第3.5节 虚拟机的快照与恢复 | 2 | 讲授 | 目标2 |
| 4 | 第4章 动态基础分析技术  第4.1节 沙箱  第4.2节 进程监视  第4.3节 进程浏览  第4.4节 注册表快照  第4.5节 网络模拟与抓包 | 4 | 讲授 | 目标1 |
| 5 | 第5章 Windows恶意代码  第5.1节 Windows API  第5.2节 Windows 注册表  第5.3节 网络行为  第5.4节 跟踪恶意代码运行  第5.5节 内核与用户模式 | 2 | 讲授 | 目标1 |
| 6 | 第6章 动态调试  第6.1节 源码级与汇编级调试  第6.2节 内核模式与用户模式调试  第6.3节 调试器的使用  第6.4节 异常处理  第6.5节 修改可执行程序 | 2 | 讲授 | 目标2 |
| 7 | 第7章 使用WinDbg调试内核  第7.1节 驱动与内核代码  第7.2节 WinDbg  第7.3节 Windows符号表  第7.4节 Rootkit | 4 | 讲授 | 目标2 |
| 8 | 第8章 恶意代码行为  第8.1节 下载器和启动器  第8.2节 后门  第8.3节 登陆凭证窃取  第8.4节 存活机制  第8.5节 提权方法  第8.6节 用户态Rootkit | 4 | 讲授 | 目标3 |
| 9 | 第9章 隐蔽启动技术  第9.1节 启动器  第9.2节 进程注入  第9.3节 进程替换  第9.4节 钩子注入  第9.5节 Detour  第9.6节 APC注入 | 2 | 讲授 | 目标3 |
| 10 | 第10章 数据加密  第10.1节 数据加密的目的  第10.2节 简单加密算法  第10.3节 常见加密算法  第10.4节 自定义加密  第10.5节 解密 | 4 | 讲授 | 目标3 |
| 11 | 第11章 Yara引擎  第11.1节 Yara引擎简介  第11.2节 Yara引擎安装  第11.3节 Yara特征编写  第11.4节 Yara引擎实战 | 2 | 讲授 | 目标3 |
| 12 | 第12章 人工智能检测技术  第12.1节 静态特征提取  第12.2节 动态特征提取  第12.3节 机器学习检测模型  第12.4节 恶意代码概念漂移 | 4 | 讲授 | 目标3 |
| 13 | 实验一：静态基础分析实验  内容：了解静态基础分析方法；使用多种静态基础分析工具对恶意代码进行分析，提取恶意代码特征。  性质：验证性  类别：必做  分组：三人一组 | 4 | 上机/实验 | 目标3、4 |
| 14 | 实验二：动态基础分析实验  内容：了解动态基础分析方法；使用多种动态基础分析工具对恶意代码进行分析，提取恶意代码特征。  性质：验证性  类别：必做  分组：三人一组 | 4 | 上机/实验 | 目标3、4 |
| 15 | 实验三：Windows恶意代码分析实验  内容：了解Windows API、注册表、网络API、Native API、互斥量、异常处理的知识；通过反汇编技术，分析Windows恶意代码，从Windows程序的多个位置提取特征。  性质：验证性  类别：三人一组  分组：无 | 4 | 上机/实验 | 目标3、4 |
| 16 | 实验四：Windows内核调试实验  内容：了解Windows内核基础知识；了解WinDbg的使用和Windows表；使用WinDbg分析内核恶意代码，提取恶意代码特征点。  性质：验证性  类别：必做  分组：三人一组 | 4 | 上机/实验 | 目标3、4 |
| 17 | 实验五：恶意代码行为识别实验  内容：了解恶意代码的远程控制、登陆窃取、存活机制、劫持、权限提升等技术；通过静态和动态分析，定位恶意代码行为，提取检测特征。  性质：综合性  类别：必做  分组：三人一组 | 4 | 上机/实验 | 目标3、4 |
| 18 | 实验六：恶意代码隐蔽启动行为检测实验  内容：了解恶意代码隐蔽启动的实现方式；通过静态和动态分析，识别恶意代码的隐蔽启动行为，提取检测特征。  性质：综合性  类别：必做  分组：三人一组 | 4 | 上机/实验 | 目标3、4 |
| 19 | 实验七：数据加密实验  内容：了解恶意代码使用的数据加密方法；了解解密策略；通过静态和动态分析，识别恶意代码的加密方法，构建解密函数，实现对恶意代码秘密数据的解密。  性质：综合性  类别：必做  分组：三人一组 | 4 | 上机/实验 | 目标3、4 |
| 20 | 实验八：Yara引擎实验  内容：了解Yara引擎安装和规则编写；对恶意代码进行分析，编写Yara检测规则。  性质：验证性  类别：必做  分组：三人一组 | 2 | 上机/实验 | 目标3、4 |
| 21 | 最新科研论文的阅读与分享 | 0 | 研讨 | 目标1、4 |
| 22 | 恶意代码最新分析工具的分享 | 0 | 研讨 | 目标1、4 |
| 23 | 勒索病毒的防治技术 | 0 | 研讨 | 目标1、4 |

注：1.对应的课程目标可填写大纲中第四部分课程目标的相应序号。

2.教学方式填写：讲授、研讨、上机、实验、习题课等内容。

3.实验课程要在教学内容中详细列出每个实验的名称、内容、实验性质（验证性、综合性、设计性）、实验类别（选做、必做）和实验的分组情况等。实践教学课程要写出相应的时间、地点、方式、教学内容等。

**5.1讲授课实施**

课前会在学堂在线上发布课程视频、参考资料，学生可以提前预习课程内容。

课堂授课采用雨课堂工具实施，基于雨课堂进行点名签到、每个知识点实时考核、随机点名回答问题，及时统计全班同学答题准确率，根据答题情况调整讲课节奏。

课后布置知识点在线测试和热点问题讨论，了解学生对课上知识点的掌握情况，并对知识点进行扩展，发散学生的思维，关注恶意代码分析与防治技术的最新研究文献，并能够寻求可替代的解决方案。

在知识点讲解时融合网络安全技术服务国家网络安全事业的理念，积极引导同学们树立服务国家网络强国的意识，让同学们能够理解恶意代码的各种风险和危害，以及这些行为应承担的责任。

**5.2 上机/实验课实施**

上机/实验课以学生动手能力，以验证、综合、设计实验，巩固恶意代码分析与防治各章节的知识点，掌握恶意代码分析的基本方法和技术，掌握分析工具的使用。

为了让同学积极参与到上机实验课中，保证上机实验课效果，每组学生由3名同学组成，组长负责总体协调。同学们在团队中独立完成指定任务或者与其他成员合作完成任务，在团队合作中能够履行个体、团队成员或负责人的职责。

**5.3 研讨内容实施**

目标：使学生加深对恶意代码基本概念和行为的正确理解，初步具备运用所学知识进行中等复杂程度的恶意代码问题的分析能力，引导学生积极思考、主动学习，锻炼和提高学生的文献阅读、交流、沟通和表达能力以及团队合作能力。

方式：（1）利用线上学习平台，组织学生就“最新科研论文的阅读与分享”、“恶意代码最新分析工具的分享”、“勒索病毒的防治技术”等主题进行讨论，指导同学进行最新文献的阅读，了解最新的恶意代码防治方案；（2）在论文阅读的基础上，以小组的形式交流和总结恶意代码防治的新工具和方法，由组长负责组织和任务分工，小组成员一起完成指定任务，在线上学习平台的讨论版中分享小组研讨结果。

**六、课程考核**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 请简述本课程考核方案：  （我校推行课程的过程化考核，鼓励采用平时多次考核的方式。过程化考核包括课后书面作业、实践、上机、课堂讨论、课堂作业表现及考试等等。）  课程的考核采用平时成绩和期末考试相结合的考核形式。  平时成绩占总评成绩50%，包括：  1. 课堂表现：通过雨课堂工具的实时答题、点名签到进行考核，占总评成绩10%，支撑课程目标1、2（各占50%）。  2. 课后测试：通过学堂在线的课后测试题进行考核，考察对课上知识点的掌握程度，占总评成绩15%，支撑课程目标1、2（各占50%）  3. 实验报告：通过对实验课堂展示汇报、实验报告评分等方式完成考核，占总评成绩20%，支撑课程目标3、4（各占50%）。  4. 研讨内容：通过线上研讨内容完成度进行考核，占总评成绩5%，支撑课程目标4。  期末考试采用闭卷考试的考核形式（100分），占总评成绩50%，包括：  1. 恶意代码基础分析技术题（20），支撑课程目标1  2. Windows恶意代码题（30），支撑课程目标1  3. 动态调试题（30），支撑课程目标2  4. 恶意代码行为分析与检测题（20），支撑课程目标3  **考核环节占比与课程目标对应关系表**   |  |  |  |  | | --- | --- | --- | --- | | **序号** | **评估环节与内容** | **成绩占比** | **对应课程目标** | | 1 | **平时-课堂表现** | 10% | 1，2（各占50%） | | 2 | **平时-课后测试** | 15% | 1，2（各占50%） | | 3 | **平时-研讨内容** | 5% | 4 | | 4 | **平时-实验报告** | 20% | 3、4（各占50%） | | 5 | **期末-**恶意代码基础分析技术题 | 10% | 1 | | 7 | **期末-** Windows恶意代码题 | 15% | 1 | | 8 | **期末-**动态调试题 | 15% | 2 | | 9 | **期末-**恶意代码行为分析与检测题 | 10% | 3 |   注：对应的课程目标可填写大纲中第四部分课程目标的相应序号。 |

**七、审批意见**

|  |
| --- |
| **开课单位学术委员会或本科教学指导委员会意见：**  **负责人签字： 日期：** |
| **开课单位分管负责人意见：**  **负责人签字： （单位公章）**  **日期：** |
| **教务处意见：**  **负责人签字： （公章）**  **日期：** |