《信息安全工具开发》

课程标准

|  |  |
| --- | --- |
| 适用专业 | 信息安全与管理 |
| 学 制 | 三年 |
| 课 时 | 72 |
| 执 笔 人 | 刘佳 |
| 参与人员 | 石春宏 |
| 编写日期 | 2022.02 |
| 审 核 人 |  |

# 《信息安全工具开发》课程标准

**一、课程性质**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 课程编号 |  | 开课系部 | 网络与信息安全学院 | 授课学期 | 第4学期 |
| 课程名称 | 信息安全工具开发 | 授课层次 | 三年大专 | 课程性质 | 专业核心课 |
| 课程类别 | 选修课 | 考核方式 | 考试 | 课程学分 | 2.0 |
| 总学时 | 72 | 理论学时 | 36 | 实践学时 | 36 |
| 前导课程 | 《Python程序设计》 | | | | |
| 后续课程 |  | | | | |
| 适用专业 | 信息安全与管理 | | | | |

**二、课程设计思路**

该课程是依据《信息安全与管理专业实施性人才培养方案》设置的。

其总体设计思路是，打破以知识传授为主要特征的传统学科课程模式，转变为以工作任务为中心组织课程内容，并让学生在完成具体项目的过程中学会完成相应工作任务，并构建相关理论知识，发展职业能力。

课程内容突出对学生职业能力的训练，理论知识的选取紧紧围绕工作任务完成的需要来进行，同时又充分考虑了高等职业教育对理论知识学习的需要，并融合了相关职业资格证书对知识、技能和态度的要求。以网络为基础、平台为中枢、数据为要素、安全为保障，既是工业数字化、网络化、智能化转型的基础设施，也是互联网、大数据、人工智能与实体经济深度融合的应用模式，同时也是一种新业态、新产业的理念贯穿于教学中。要通过校企合作，校内实训基地建设等多种途径，采取工学结合等形式，充分开发学习资源，给学生提供丰富的实践机会。教学效果评价采取过程评价与结果评价相结合的方式，通过理论与实践相结合，重点评价学生的职业能力。

**三、课程目标**

本课程在信息安全与管理专业教学资源库专业核心课程体系中处于拓展能力学习领域课程。以《Python程序设计》课程为基础，通过本门课程的学习，能把Python编程应用到实际的渗透当中，提高网络渗透测试工程师、信息安全工程师的工作效率，同时也能打造属于自己的工具。

（一） 素质目标

（1） 培养学生的观察和模仿能力；

（2） 培养学生的团队协作和动手能力；

（3） 锻炼学生自我学习的能力；

（4） 提高学生语言表达能力，提高思维的敏捷性，增强学生举一反三的能力。

（二） 能力目标

（5） 能对目标主机进行本地扫描、TCP安全连接扫描；

（6） 能调用metaspolit进行Windows SMB服务进行渗透、无线网络渗透，嗅探FTP服务传输信息。

（7） 能利用常规的安全漏洞进行渗透测试；

（8） 能利用Python进行网络恶意流量的识别、分析网络流量进行定位。

（三） 知识目标

（1） 掌握Python常用模块、包、正则表达式；

（2） 掌握Python多线程、Socket类；

（3） 掌握Python本地扫描、TCP安全扫描和NMAP扫描器；

（4） 掌握Python调用Metaspolit框架的方法；

（5） 熟悉Python网络流量分析模块pygeoip、pcap。。

**四、课程内容与要求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **学习模块** | **学习单元** | **知识技能点** | **建议学时** |
| 1 | 模块一：认识Python语言的应用领域 | 单元一：Python应用现状 | 网络运维方向  大数据方向  信息安全方向 | 2 |
| 单元二：Python的安全应用简介 | 网页数据爬取  网络服务扫描  渗透测试  网络流程监测 | 2 |
| 2 | 模块二：Python基础进阶 | 单元一：模块 | 模块的作用  动手编写模块  OS模块  用OS模块实现文件遍历实例 | 4 |
| 单元二：包 | 包的作用与模块的区别  实例详解包结构 | 2 |
| 单元三：常用标准库 | 数学类模块  系统日期和时间类模块 | 2 |
| 单元四：正则表达式 | 正则表达式的作用  元字符的特殊作用及示例  RE模块  几个常用函数及返回值分析  内置属性的用法  正则表达式用于单个页面图片文件的爬取实例 | 4 |
| 单元五：多线程 | 多线程threading模块简介  函数运行在多线程的两种实现方法  threading.Thread在线程中运行函数  继承threading.Thread类创建线程  线程类Thread的方法和属性 | 4 |
| 3 | 模块三：网络编程基础 | 单元一：支持底层网络编程的socket模块 | 网络编程预备知识  用socket建立服务器端程序  用socket建立客户端程序  用socket建立基于UDP协议的客户端程序  用socketserver模块建立服务器 | 4 |
| 单元二：面向HTTP协议的Requests库（客户端编程） | 认识Requests库-客户端编程  环境准备  HTTP协议原理分析  用urllib实现简单的客户端访问  用requests实现简单的客户端访问  请求方法  带参数的请求  请求的异常处理方法  自定义request  服务端响应的基本API  图片下载  事件钩子  HTTP协议的认证  Proxy代理  Session和Cookie | 4 |
| 单元三：Flask Web框架（服务器端编程） | Flask Web框架简介  Flask Web框架的安装并运行一个最小Flask应用  URL装饰器与URL参数传递  GET和POST请求的参数传递  cookie和session跟踪用户  使用静态文件资源与页面文件  接收上传文件  使用数据库 | 6 |
| 单元四：Python数据库编程 | Python数据库应用程序接口简介  数据库游标使用  SQLite3数据库简介  Python操作SQLite3数据库 | 4 |
| 4 | 模块四：Python扫描 | 单元一：本地扫描 | tkinter模块界面菜单设计  编制菜单响应事件  OS模块迭代遍历目录  界定垃圾文件并扫描  多线程加速扫描过程  全磁盘扫描垃圾文件并清除  按名称实现文件搜索  搜索超大文件 | 4 |
| 单元二：TCP全连接安全扫描 | 访问BCD套接字接口  socket API函数解析  TCP全连接扫描工作步骤  optparse标准库用于创建选项分析器并指定命令选项  optparse模块快速解析目标主机和扫描端口实例分析  端口扫描函数调用socketAPI解析地址并枚举端口发起连接扫描  连接扫描函数产生到目标主机端口的连接，成功则获得端口开放信息  在连接扫描函数中发送数据进行服务器信息探测  多线程加速扫描过程  用多线程去改造端口扫描函数  对多线程的信号量提供加锁和释放 | 6 |
| 单元三：nmap扫描器 | Python-nmap库简介与安装  多类型扫描（SYN、NULL、FIN、XMAS）  使用nmap库完成扫描 | 2 |
| 5 | 模块五：Python渗透测试 | 单元一：利用Metasploit框架测试WindowsSMB服务 | ms08-067\_netapi漏洞两个可用攻击特征  攻击用密码列表制作  Metasploit框架下载安装  利用Metasploit的执行攻击的步骤  启动配置文件执行攻击  利用python-nmap模块探测所有主机445端口的开放状态  设置TCP反弹连接的Payload  针对用户名和密码组合暴破 | 4 |
| 单元二：无线网络渗透 | 无线渗透环境设置  aircrack-ng工具套件设置网卡为混杂模式  新监控接口设置  scapy库sniff函数截获无线数据包 | 4 |
| 单元三：嗅探FTP服务的明文传输 | FTP服务的明文传输缺陷分析  正则表达式匹配FTP用户凭证  从嗅探数据分析明文凭证 | 2 |
| 6 | 模块六：Python电子取证 | 单元一：恢复回收站中被删除的文件 | 操作系统对于已删除文件的处理  OS模块查找已删除的项目并打印文件  \_winreg模块简介  \_winreg模块确定执行删除文件的用户 | 2 |
| 单元二：读取PDF文档的元数据 | 元数据的作用  pyPDF库简介  getDocumentInfo()函数的使用及返回值的遍历 | 2 |
| 7 | 模块七：Python网络流量分析 | 单元一：识别网络中的恶意流量 | DNS协议请求  Scapy解析DNS流量  Fast流量简介  pcap检测Fast流量（包含DNSRR的数据包）  Scapy分析蠕虫感染的机器 | 4 |
| 单元二：分析网络流量确定地理位置 | 开源GeoliteCity数据库从IP地址映射至物理地址  开源GeoliteCity数据库的下载与本地保存  pygeoip模块实现对GeoliteCity数据库的查询  Dpkt数据包操作工具分析数据包  pcap得到数据包的源目IP地址  实例化pygeoip模块的GeoIP类实现源目IP地址到物理地址的转化 | 4 |
| 总学时 | | | | 72 |

**五、实施建议**

**（一）教学建议**

本课程采用以项目为主的模块结构，将理论与实践的内容进行整合。在教学中采用理论与实践一体化的教学模式，在课程实施中积极探索实训导向性、问题导向性和项目导向性的教学。

采用理论与实践一体化的教学模式，并不是完全抛弃传统的教学，而是发挥传统教学的长处，将其融入理论实践一体化教学模式这中，注重教学的有效性。

教学中要充分发挥学生的主体作用和教师的主导作用，从学生的实际和企业岗位的需求出发，遵照学生的学习特点和认识规律，突出培养学生解决实际问题的能力和应变能力，强化情感态度价值观的教育。

本课程建议在实施过程中多和学生进行交流和互动，进行分组教学，进行大量实验。在课余最好能完成实际项目，有助于学生理解。

**（二）评价建议**

对学生的评价不仅要重视终结性的评价，同时重视过程性的评价，将阶段评价和目标评价相结合。

倡导评价的多主体性，学生要参与学习过程的评价，可进行学生的自我评价、学生对学生的评价和师生之间的互相评价，还可引入企业的评价。

**（三）教材编写和选用建议**

教材编写要体现项目课程的物色与设计思想，教材内容应体现先进性、实用性、典型产品、案例的选取要科学，体现地区产业特点，具有可操作性。教材呈现方式要图文并茂，文字表述要规范、正确、科学。开发相关辅导用书、教师指导用书、网络资源，要注重仿真软件的应用及开发。

**（四）课程资源开发与利用建议**

1.可将本课程的教学内容与地区经济实际工作情况紧密结合，开发体现本地区特点的网络综合布线教学项目。

2.要较充分利用当前丰富的网络资源。

3.教学中学生的问题、困惑、见解、情感和体验等都是动态生成的课程资源，教师应重视这些教学过程中动态生成的课程资源，并主动性和创造性地运用使以项目为主的教学充满生机与活力。

特别是可充分利用学校内网络资源，可在学校建设计算机机房、行政办公用的信息安全与管理出现故障后让学生在老师的指导下进行维护，提高学生解决实际问题的能力。

**六、考核方式与标准**

本课程教学学期结束学生参加阶段考试。最后成绩的评定根据阶段性考核和过程性考核结合综合性考核形成。

本课程最终成绩由以下形式组成：

|  |  |  |  |
| --- | --- | --- | --- |
| **课程基本要求** | | | **以实际成绩计入总分** |
| **期末考试（知识+技能）** | **考试成绩** | | **评分标准** |
| 小于60分 | | 本课程不及格 |
| 大于等于60分 | | 本课程及格 |
| **阶段性考核** | | | **50 %** |
| **阶段性集中考核** | 无纸化考试（知识+技能） | |  |
| **过程性考核** | | | **25 %** |
| **项目技能专项考核** | **项目单元** | **完成等级** | **评分标准** |
| 各项目单元分别评定 | A级：体现创新特色 | A |
| B级：实现拓展功能 | B |
| C级：实现基本功能 | C |
| **综合性考核** | | | **25 %** |
| **对各模块项目进行综合考核** | A级：体现创新特色以及合作能力 | | A |
| B级：实现拓展功能 | | B |
| C级：实现综合功能 | | C |
| **总分 =** 阶段性考核 + 过程性考核 + 综合性考核  **注：**总分最高100分。 | | | |

**七、说明**

1.本课程标准依据五年制高职信息安全与管理培养方案。

2.本课程标准适用于信息安全与管理专业或其它相近专业。