## 项目2　应用系统信息安全保护

|  |  |  |
| --- | --- | --- |
| **项目2 应用系统信息安全保护** | | |
| **教学设计** | | |
| **一、教学目标**  素质目标：培养学生严慎细实的职业素养，提升集体意识和团队合作意识。  知识目标：掌握保护应用系统信息安全的方法；了解信息系统安全的检测与安全加固。  能力目标：能根据需求完成企业安全保护方案的设计；会利用工具探测系统信息并关闭非必要端口；能使用账户策略、关闭非必要服务、映射端口等技术手段安全加固系统。  **二、教学重难点**  教学重点：设计保护方案；探测系统信息；安全加固系统。  教学难点：结合具体的项目需求制定实施方案，利用技术探测系统信息并加固安全防护。  **三、课时安排**  6课时  **四、教学策略**  教法：项目教学法、任务驱动法、讲授法、演示法  学法：自主探究学习法、讨论法、小组合作学习法  教学资源：多媒体教学设备、理实一体化实训室、信息化教学平台、配套教学课件 | | |
| **教学过程** | | |
| **教学环节** | **教学设计** | **设计意图** |
| 课前学习 | 1.学习教师布置的课前学习任务。  2.查阅资料，掌握保护应用系统信息安全的方法；了解信息系统安全的检测与安全加固。 | 培养学生自主学习、创新学习能力。 |
| 项目背景 | 一家小型公司组建了网络，并启用了私有云存储等应用系统，为了保障信息安全，邀请小小所在公司对网络进行安全保护，小小所在的项目组承接了该项目。 | 设置贴近实际的项目，激发学生学习兴趣，引入学习任务。 |
| 项目分析 | 一家小型公司组建了网络，并启用了私有云存储等应用系统，为了保障信息安全，邀请小小所在公司对网络进行安全保护，小小所在的项目组承接了该项目。 | 分析项目并形成项目结构，培养学生分析归纳梳理信息的能力，培养结构化处理事情的习惯。 |
| **任务1　设计保护方案** | | |
| **教学过程** | | |
| **教学环节** | **教学设计** | **设计意图** |
| 任务描述 | 在项目中，调研了解客户的真实需求，依此制订出满足客户需求的规划方案是项目工作的重中之重，本阶段需要反复确认与沟通。 | 直观描述内容，明确教学内容，帮助学生抓住重点。 |
| 任务分析 | 信息安全保护，首先要确认安全需求;然后有针对性地制订实施方案;最后为了保障实施方案的顺利完成，还需要完善信息安全管理制度。任务路线如图10-2-2所示。 | 理清思路，养成学生有条理、合逻辑地开展工作的习惯，培养学生严谨细实的职业素养。 |
| 任务实施 | 成员按照拟定的任务线路实施任务。  **1.安全需求确认**  **（1）实地勘察**  教师情景引入：小小项目组到小型公司实地勘察，了解了网络设备、计算机、服务器等设备的部署情况，绘制了网络拓扑图。  教师结合图“10-2-3 网络拓扑图”进行教学。  **（2）需求确认**  教师明确公司的功能需求：  ①外网用户、内网用户均能访问私有云存储服务器。  ②保障私有云存储服务器的安全。  小提示：标准的网络安全需求调研，要求制作需求调研表，并进行实地访谈，从现行系统、现行需求、未来需求及约束条件等多方面进行了解，最后对结果进行专业分析后确定客户的真实需求，并获得预算情况。本项目中做了简化，有兴趣的同学可以查阅相关资料了解。  **2.制定实施方案**  教师讲解：通常建议企事业单位进行等级保护，按照自主定级、自主保护的原则，通过定级、备案、安全建设和整改、信息安全等级测评、信息安全检查5个阶段构建立体的防护系统，这需要借助专业的公司来实现。  教师补充：网络信息安全项目的实施方案，会根据公司的情况进行个性化定制，通常分为网络安全防护、服务器安全防护、网络与数据安全措施保障、规范管理等几方面。在本项目中，根据需求重点采用技术手段进行应用系统的防护，方案的主要防护技术手段如下：  ①通过本地扫描、远程扫描的方式探测私有云存储服务器，确定薄弱点，然后关闭非必要的端口。  ②采用设置账户策略、关闭非必要服务等技术手段加固私有云存储服务器。  ③将私有云存储服务器端口映射到公网，让外网用户也能访问。  结合图“10-2-4 方案效果拓扑图”和表“10-2-1 拟定的设备配置情况”进行教学。  **3.完善信息安全管理制度**  教师明确：因为该小型公司预算有限，不能购买防火墙、安全网关、入侵检测系统等安全硬件设备，为了在有限的技术条件下实现更大的安全防护，保障业务的正常运行，将原有的网络安全管理制度进行完善，完善后的网络安全管理制度分3层。  第一层为总则，第二层为具体的专项管理制度，第三层为操作手册和行为规范。 | 根据拟定的任务路线展开任务实施，教学路线清晰，教学内容明确，帮助学生很好地掌握知识，同时锻炼有条理地处理问题的能力。  小提示补充了教学内容，拓展学生认知，引导学生延伸课堂知识。  引导学生认识信息安全的重要性，增强学生信息安全保护意识。  强调制度化保护信息安全，增强学生的信息安全意识，保护信息安全的同时，也要遵守信息安全管理制度，自觉维护网络安全。 |
| 任务延伸 | 调查学校网络安全管理制度的相关类别和内容，划分小组做网络调研，了解相关法律法规，制定班级网络安全管理制度。 | 启发学生思考，培养学生知识运用于迁移的能力。 |
| **任务2　探测系统信息** | | |
| **教学过程** | | |
| **教学环节** | **教学设计** | **设计意图** |
| 任务描述 | 信息安全保护方案设置好之后，需要进一步确定应用服务器、内网计算机等设备的安全状况。 | 直观描述内容，明确教学内容，帮助学生抓住重点。 |
| 任务分析 | 要确定和排查信息安全风险，通常需要进行渗透测试，本任务中简化流程，仅进行渗透测试中的信息收集，然后关闭非必要的端口。任务路线如图10-2-5所示。 | 理清思路，养成学生有条理、合逻辑地开展工作的习惯，培养学生严谨细实的职业素养。 |
| 任务准备 | **1.渗透测试**  教师讲解：渗透测试是通过模拟恶意黑客攻击的方法，来评估计算机网络系统安全的一种评估方法。在渗透测试前应该认真阅读《中华人民共和国网络安全法》等相关法律法规，通常渗透测试的步骤有获得授权、明确目标、信息收集、漏洞探测、漏洞验证、信息分析、获取所需、信息整理、形成报告。  **2.信息收集**  教师讲解：信息收集是渗透测试的初期环节，目的是充分了解被渗透对象的信息，它分为被动信息收集、主动信息收集和主动扫描。信息收集常用工具有nmap、Zenmap、X-scan、Nessus流光等工具，其中Zenmap是nmap 的图形界面版本。 | 任务准备环节帮助学生梳理后续教学需要的基础知识，推动教学的有序开展。 |
| 任务实施 | 成员按照拟定的任务线路实施任务。  **1. 部署服务器环境**  教师讲解：按照任务1中的表10-2-1拟定的设备情况安装内网用户计算机，并参考专题8项目2网络云应用系统搭建、部署私有云存储服务器。  **2.收集系统信息**  **（1）下载安装Zenmap**  教师结合图“10-2-6 下载Zenmap”教学详细的操作步骤。  **（2）扫描服务器**  教师结合图“10-2-7 扫描结果”和图“10-2-8 查看服务器开放的端口”教学详细的操作步骤。  **3.关闭非必要的端口**  **（1）分析开放端口**  结合表“10-2-2 开放端口分析”教学详细的操作步骤。  **（2）关闭端口**  结合图“10-2-9 打开‘高级安全Windows Detender防火墙’对话框”、图“10-2-10 新建入站规则”和图“10-2-11 创建入站规则”教学关闭端口的操作步骤。  **（3）扫描服务器**  教师讲解：在内网用户计算机上，先测试私有云存储服务器的功能，确认能正常使用后，再次使用Zenmap扫描私有云存储服务器，结果如图10-2-12所示，关闭端口成功。 | 教师详细讲解操作步骤，直观演示操作过程，帮助学生学会实际操作，提升学生理论联系实际的能力。  教师讲解与图示教学相结合，直观展示操作界面，让学生真正学会操作。 |
| 任务延伸 | 1.想办法使用高级安全Windows Defender防火墙中的入站规则及出站规则，禁止QQ访问网络。  ⒉学习信息收集工具的相关知识，对网络内的其他计算机进行信息收集，理解端口与服务的对应关系，同时分析可能产生的网络信息安全风险，并在班上做交流。 | 启发学生思考，培养学生知识运用于迁移的能力。 |
| **任务3　安全加固系统** | | |
| **教学过程** | | |
| **教学环节** | **教学设计** | **设计意图** |
| 任务描述 | 私有云存储系统关闭了非必要的端口，减少了网络信息安全风险，还需要进一步加固系统,并让外网用户能使用。 | 直观描述内容，明确教学内容，帮助学生抓住重点。 |
| 任务分析 | 加固应用系统的方法很多，从技术面上主要应该设置账户策略，关闭非必要的协议及服务，最后根据需求将私有云存储服务器映射到外网。任务路线如图10-2-13所示。 | 理清思路，养成学生有条理、合逻辑地开展工作的习惯，培养学生严谨细实的职业素养。 |
| 任务准备 | **1.安全加固**  教师讲解：安全加固是指根据专业安全评估结果，制订相应的系统加固方案，通过打补丁、修改安全配置、增加安全机制等方法进行安全性加强。安全加固的对象有操作系统、网络设备、安全设备策略、网络架构、数据库、应用软件等。  **2.端口映射**  教师讲解：端口映射可以将内网的地址翻译成外网地址，当内网的服务器需要对外网提供服务或接收数据时，都需要端口映射。外网通过访问这个翻译出来的外网地址再访问内网的服务器，能保障内网服务器的安全。 | 任务准备环节帮助学生梳理后续教学需要的基础知识，推动教学的有序开展。 |
| 任务实施 | 成员按照拟定的任务线路实施任务。  **1.设置账户策略**  **（1）定期清理账户**  教师结合图“10-2-14 禁用账户”教学定期清理账户的具体操作步骤。  **（2）账户密码策略**  教师结合图“10-2-15 设置密码策略”讲解具体操作步骤。  **（3）账户登录策略**  教师结合图“10-2-16 设置账户锁定策略”进行教学。  **2.关闭非必要的协议及服务**  **（1）关闭协议**  教师讲解：禁用TCP/IP上的 NetBIOS协议，可以关闭监听的UDP 137、UDP 138以及 TCP 139端口。双击“Internet 协议版本4（TCP/IPv4)”，然后选择“高级”选项卡，最后在“WINS”卡式菜单中进行如图10-2-17所示的设置。  **（2）关闭服务**  教师讲解：在任务栏搜索框中输入关键字“服务”，在服务列表中右击“TCP/IP NetBIOS Helper”服务，在弹出的快捷中选择“停止”选项，如图10-2-18所示。  教师补充：其他还可以禁用的服务建议，结合表“10-2-3 可禁用的服务建议”进行教学。  **3.映射端口**  教师讲解：在主流的路由器、防火墙上均具有端口映射的功能，各个品牌的操作界面不同，但功能类似。登录无线路由器，在“高级”选项卡中找到“端口映射”，这里将私有云存储服务器的访问端口 8000，映射为外网的8001端口。  结合图“10-2-19 设置路由器端口映射”进行教学。 | 教师讲解操作步骤，并以图片的形式展示操作内容，加深学生对教学内容的理解。  锻炼学生的实际操作能力，提高学生的职业岗位水平。  详细的步骤教学让学生真正学会操作。 |
| 拓展延伸 | 学习安全加固相关技术，尝试从账户策略、文件权限、安全选项等多方面对自己的计算机进行安全加固，最后整理一套个人计算机安全加固策略，到班上进行分享。 |  |
| 项目分享 | 方案1：各工作团队展示交流项目，谈谈自己的心得体会，并选派代表分享交流。  方案2：由学生代表与指导教师组成项目评审组，各工作团队制作汇报材料并进行答辩。 | 团队协作交流、分享自己的体会，增强学生的团队精神。 |
| 项目评价 | 请根据项目完成情况填涂表10-2-4完成项目评价。 | 自我评价，找出学习薄弱的地方，继续巩固。 |
| 项目总结 | 本项目依据行动导向理念，将行业中的应用系统信息安全保护的典型工作过程转化为项目学习内容，共分为设计保护方案、探测系统信息、安全加固系统3个任务。让学生了解网络信息系统安全保护的流程，认识行业中的渗透测试、安全加固等相关技术及方法，为以后的专业学习打下基础，同时培养网络信息安全意识。 | 通过项目总结，提炼课程的要点，帮助学生明确教学内容，同时还能帮助学生巩固所学知识，查补缺漏，培养学生严谨治学、踏实认真的品质。 |
| 教学反思 | | |
|  | | |