|  |  |  |
| --- | --- | --- |
| **项目3 网络攻击安全防御** | | |
| **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：了解网络环境测试与防御；掌握网络攻击安全防御的方法。  能力目标：能部署简单的渗透测试环境；能利用工具软件捕获、查看网络数据包，并且有针对性地防御ARP攻击；会配置上网认证、网页过滤、攻击防护等防火墙功能，防御网络攻击。  **二、教学重难点**  教学重点：部署渗透测试环境；查看与防御ARP攻击；配置防火墙防御攻击。  教学难点：具备网络攻击安全防御意识，并能在实际应用中运用工具软件测试与防御网络攻击。  **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，了解网络环境测试与防御；掌握网络攻击安全防御的方法。 | 培养学生自主学习、创新学习能力。 |
| 项目背景 | 自强设计公司是一家中小型企业，前段时间内部受到ARP攻击，为了避免以后再受攻击，找到小小顶岗实习所在网络安全公司寻求帮助。 | 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 | 网络受到攻击，应该查看攻击发生的原因，在经过授权后，可采用渗透测试的方法模拟攻击，然后有针对性地进行防御，另外为了避免类似的攻击发生，最好配置防火墙进行防御。项目结构如图10-3-1所示。 | 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　部署渗透测试环境** | | |
| **教学过程** | | |
| **教学环节** | **教学设计** | **设计意图** |
| 任务描述 | 小小公司获得自强设计公司的授权，在公司内部搭建简单的渗透测试环境。 | 直观描述内容，明确教学内容，帮助学生抓住重点。 |
| 任务分析 | 为了让项目顺利进行，通过调研后设计实施方案，并规划出网络拓扑，然后部署必要的渗透测试工具。任务路线如图10-3-2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。 |
| 任务准备 | **1.数字取证操作系统**  教师引导学生认识数字取证操作系统：数字取证操作系统是集成了数字取证工具的一种操作系统。  教师介绍常见的数字取证操作系统：结合图“10-3-3 常见数字取证操作系统”进行教学。  **2.数据包分析软件**  教师引导学生认识数据包分析软件：数据包分析软件是指对网络上的流量数据进行截获、分析的软件。  教师介绍常见的数据包分析软件：结合图“10-3-4 常用的数据包分析软件”进行教学。 |  |
| 任务实施 | 成员按照拟定的任务线路实施任务。  **1.规划网络拓扑**  教师讲解：分析自强设计公司网络情况之后，可部署一台渗透测试机。在Windows 10操作系统上安装 VMware Workstation虚拟化软件，然后再部署Kali。使用内网的一台安装了Windows 10操作系统的计算机作为被测试机，规划的网络拓扑如图“10-3-5 规划网络拓扑”所示。  **2.部署渗透测试工具**  **（1）安装虚拟机**  教师讲解：从官网下载VMware Workstation 虚拟化软件，然后安装并运行。  **（2）安装Kali**  教师结合步骤1至步骤6、图“10-3-6 下载安装映像包”、图“10-3-7 载入安装映像”图“10-3-8 选择操作系统版本”、图“10-3-9 选择图形界面安装方式”、图“10-3-10 将改动写入磁盘”、图“10-3-11 设置IP地址”教学安装Kali的安装步骤。  **3.安装数据包分析软件**  教师讲解：在被测试机上按照规划网络拓扑图配置IP地址，并安装数据包分析软件Wiresharko访问Wireshark官方网站，下载Windows 64位版本的安装包。  教师补充：运行安装程序，按照提示依次安装。 | 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。  详细的步骤教学辅以操作图展示，让学生将知识真正落实到实际操作上，让学生真正学会操作。 |
| 任务延伸 | 访问Kali官网，下载虚拟机专用的安装包，导入到VMware Morkstation并且运行，同时进行网络调研，进一步了解数字取证操作系统。 | 启发学生思考，培养学生知识运用与迁移的能力。 |
| **任务2　查看与防御ARP攻击** | | |
| **教学过程** | | |
| **教学环节** | **教学设计** | **设计意图** |
| 任务描述 | 通过任务1完成了渗透测试环境的部署，接下来需要还原自强设计公司以前内部网络被ARP攻击的场景，查看与防御 ARP工具。 | 直观描述内容，明确教学内容，帮助学生抓住重点。 |
| 任务分析 | ARP攻击主要存在于局域网网络中，被攻击时会造成上网时断时续、拷贝文件无法完成、局域网内的ARP包激增、出现不正常的MAC地址等情况。本任务通过数据包分析软件Wireshark，捕获、查看、分析数据包，然后使用技术手段防御ARP攻击，任务路线如图10-3-13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。 |
| 任务实施 | 成员按照拟定的任务线路实施任务。  **1. 查看网络数据包**  **（1）运行Wireshard**  教师结合步骤1至步骤3教学详细的操作步骤。  **（2）发起ARP模拟攻击**  教师结合步骤1至步骤3教学详细的操作步骤。  **（3）查看数据包**  教师讲解：被测试机的Wireshark中停止分组捕获，在“应用显示过滤器”中使用关键字“arp"进行筛选，选出所有ARP数据包。  **（4）停止模拟攻击**  教师讲解：在渗透测试机Kali中按“Ctrl+C”组合键，停止模拟攻击，回到被测试机，再次测试网络连通性，网络可以正常通信。  **2.防御ARP攻击**  **（1）查看ARP地址表**  教师结合步骤1至步骤4、图“10-3-21 查看ARP详细情况”、图“10-3-22 解除所有ARP绑定”和图“10-3-23 绑定网关IP地址和MAC地址”进行教学。 | 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 | 360安全卫士、腾讯电脑管家等工具有防止ARP攻击的功能，使用Kali模拟攻击被测试机，然后在被测试机上分别开启和关闭360安全卫士的ARP攻击功能，并使用wireshark捕获全过程，最后对捕获的数据进行分析，了解攻击前后数据包的变化。 | 启发学生思考，培养学生知识运用与迁移的能力。 |
| **任务3　配置防火墙防御攻击** | | |
| **教学过程** | | |
| **教学环节** | **教学设计** | **设计意图** |
| 任务描述 | 通过前面的模拟渗透攻击，自强设计公司发现自己的网络确实很脆弱，为了预防来自外网的攻击，需要小小提供解决方案。 | 直观描述内容，明确教学内容，帮助学生抓住重点。 |
| 任务分析 | 防御来自外网的攻击，比较好的方式是使用硬件防火墙。本任务采用硬件防火墙，完善自强设计公司的网络防御体系，然后在防火墙上配置了上网认证、网页过滤和开启攻击防护等功能。任务路线如图10-3-24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.部署硬件防火墙**  教师讲解：经自强设计公司同意后，采购了硬件防火墙，部署到公司网络中，用于代替原有的无线路由器，被替换下来的无线路由器只提供无线上网功能，作为有线网络的补充，部署硬件防火墙之后的网络拓扑如图10-3-25所示。  **2.配置硬件防火墙**  **（1）上网认证**  教师结合步骤1、步骤2、图“10-3-26 创建用户”和图“10-3-27 开启认证”教学上网认证的具体操作步骤。  **（2）网页过滤**  教师结合步骤1、步骤、图“10-3-28 打开网页过滤功能”和图“10-3-29 创建过滤规则”教学网页过滤的具体操作步骤。  **（3）开启攻击防护**  教师讲解具体操作步骤：在左边菜单中选择“安全”中的“攻击防护”选项，然后将安全域设置为“trust”,勾选“全部启用”。  图“10-3-30 开启攻击防护”展示操作界面。 | 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 | 请查阅相关资料了解防火墙的流量控制、访问控制、VPN等功能，分小组聊聊身边的网络用了哪些安全功能。 | 启发学生思考，培养学生知识运用与迁移的能力。 |
| 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10-3-1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，将行业中的网络攻击安全防御的典型工作过程转化为项目学习内容，共分为部署渗透测试环境、查看与防御ARP攻击、配置防火墙防御攻击3个任务。让学生了解简单渗透测试的流程及常用渗透测试软件，学会数据包分析软件的简单使用方法，掌握防御ARP攻击的方法，体验硬件防火墙的部署和简单配置，为以后专业学习打下基础，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。 |
| 项目拓展 | 项目名称：**富强公司信息安全保护**  **1.项目背景**  富强公司是一家从事建筑设计的公司，公司内的台式计算机使用有线网络上网，移动设备使用无线路由器上网，并在内网部署了云存储服务器和Web服务器等应用系统。公司的现有网络拓扑如下图所示。    **2.预期目标**  富强公司希望能将公司业务信息、应用系统安全保护起来，并做一定的网络攻击安全防御。具体要求如下:  1）从制度、硬件设备、技术培训等方面设计公司的网络信息安全保护方案。  2）从个人、业务静态数据及业务动态数据等方面进行业务信息安全保护。  3）对私有云存储服务器、Web服务器等应用系统进行信息收集并加固。  4）做简单的渗透测试，让公司的网络能应对常规的网络攻击。  **3.项目资讯**  （1）设计网络信息安全保护方案应该体现内容包括哪些？  （2）探测、收集、捕获网络信息的工具有什么？  （3）通常渗透测试分哪几个步骤，有哪些需要注意的?  **4.项目计划**  绘制项目计划思维导图。  **5.项目实施**  根据实训条件、人员分工等情况参考项目计划实施。  任务1：信息安全防护方案设计  1)制定相关制度。查找资料，结合实际情况制定，以文档形式提交。  2）规划网络拓扑图。根据实际情况选择设备，标注出设备名称、端口号等信息。  3）列出设备清单、功能及P配置。根据上一步的网络拓扑图完成，如表格不够，可自行加页。    任务2：业务信息安全防护  1)保护个人信息，将配置过程截图。  2)加密及备份重要文件，将配置过程截图。  3）设置账户策略保障动态数据安全，将配置结果截图。  任务3：应用系统信息安全保护  1）部署应用系统环境，将配置结果截图。  2）探测系统信息，将探测获得的信息信息截图。  3)使用账户策略、关闭协议及端口、映射端口等方法加固系统，将配置过程截图。  任务4：网络攻击安全防御  1)部署渗透测试环境，将部署结果截图。  2）捕获、查看、分析数据包，将关键数据截图。  3）配置硬件防火墙，将配置过程截图。  **6.项目总结**  （1）过程记录  记录项目实施过程中的各种情况，为工作总结提供依据，如表格不够，可自行加页。    （2）工作总结  从整体工作情况、工作内容、反思与改进等几个方面进行总结。  **7.项目评价** | 通过项目拓展板块，让学生根据项目自己操作设计，有助于学生巩固所学知识，帮助学生真正学会运用所学知识处理实际问题，实现课堂知识与岗位职业需求的对接，增强学生的职业竞争力。 |
| 教学反思 | | |
|  | | |