山东大学 软件 学院

网络安全 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：202200201095 | 姓名：杨伟康 | | 班级：22网安 |
| 实验题目： FAKE-WIFI实验 | | | |
| 实验学时：4 | | 实验日期： 2025.3.18 | |
| 实验目的：  本实验通过建立一个wifi热点，用一个假冒的名字引诱用户接入，可以观察到用户的通信和行为，可以引导用户到一个假冒的网站，骗取口令。  该实验环境可以演示无线上网中的安全的问题。 | | | |
| 硬件环境： | | | |
| **情况说明**：  本次实验我使用了两种方式进行fake wifi的模拟：  一是按照老师的步骤，购买了一个简单的无线网卡在虚拟机上实验，完成了简单的配置和一系列测试，但是由于不知为何，出现物理机WIFI功能消失，掉原生网卡等损害我物理机的情况，所以另寻一条路完成了全部实验；  二是使用window11原生的热点功能，在修改Microsoft Wi-Fi Direct Virtual Adapter 这个适配器之后进行的网站欺骗和IP劫持，能够完美复现实验要求，而且更安全。 | | | |
| 实验过程报告：1.1建立wifi热点 网上购买一个usb无线网卡，花费4.79￥，但是由于忘记取快递，快递柜又多花了5毛😢  写报告时又降价了，令人感叹。。。  **型号**：802.11n  使用管理员端打开cmd后，按照实验提示给的命令试一下能否打开无线网络，失败  查询得知，网卡不支持承载网络，  因此，使用linux虚拟机再次进行实验，通过查询一步步使usb无线网卡能够开热点  暂时失败，可能会在以后重新买一个能够直接适配的吧  重新买了一个这次花了15￥,应该能适配windows了，而且第一个就给了个usb口，第二个还给说明书，贵的就是不一样  自动安装了驱动，成功在虚拟机上出现wifi选择    中间那就是无线网卡    允许其他用户连接internet    通过命令开启承载网络    但是这里我的虚拟机突然不能联网了…  开启网络共享，之后我的手机就能够看到这个虚假的网络了，fake1就是   1.2加入dns欺骗 先打开任务管理器找到server，发现打开    找到刚才的承接网络，进行设置      使用所给的dns服务器  使用windows server（其ip是172.28.1.42），添加“dns服务器”角色  这个重新下一个虚拟机。。。  终于下完了/(ㄒoㄒ)/~~  管理-添加角色和功能  安装dns服务器步骤如下：打开服务器管理器  点击“开始”按钮，选择“服务器管理器”。如果您使用的是Windows Server的桌面体验版本，您可以直接在桌面上找到“服务器管理器”图标。  启动添加角色和功能向导  在“服务器管理器”窗口中，点击“管理”菜单，选择“添加角色和功能”。  这将启动“添加角色和功能向导”，点击“下一步”继续。  选择安装类型  选择“基于角色或基于功能的安装”，然后点击“下一步”。  选择目标服务器  确认目标服务器为IP地址为172.28.1.42的Windows Server，然后点击“下一步”。  选择服务器角色  在“服务器角色”选项卡中，勾选“DNS服务器”。  系统会提示您选择附加功能，根据需求选择相应的功能（通常保持默认即可）。  点击“下一步”继续。  确认安装选择  在“确认”选项卡中，检查所有设置是否正确，然后勾选“如果需要，则自动重启目标服务器”。  7. 点击“安装”开始部署过程。  等待安装完成  安装过程可能需要一些时间，请耐心等待。安装完成后，系统会提示您安装成功。    上面那个ip远程连接不到，只能用自己的192.168.85.129  配置一个冒充的域：  进入dns管理器继续配置      在上行网卡的dns位置设置，最开始已经设置了  如此之后，一个手机或PC连到到这个热点，dns服务是被劫持的，效果如：    再深入的就不做了，在做的过程中，虽然使用虚拟机，插得usb也是接入虚拟机，但是经常出现我的物理机笔记本，掉网（怎么也连不上网），重启后发现电脑没有wifi选项等问题，可能是和笔记本本身的网卡冲突，损害到自己的笔记本就得不偿失了。。。  后续使用window11的热点功能，使用类似手机的功能直接进行设置IP欺骗、网站欺骗等方面的内容： 1. 设置Win11移动热点 打开"设置" → "网络和Internet" → "移动热点"  选择"从以下位置共享我的Internet连接"为您的物理网卡（以太网或WiFi）  设置网络名称（SSID），模仿山大的校园网”sdu.net”  设置网络密码    开启移动热点 2. 配置IP欺骗环境 打开"控制面板" → "网络和共享中心" → "更改适配器设置"  找到您创建的移动热点适配器（通常名为"Microsoft Wi-Fi Direct Virtual Adapter"）    右键点击 → "属性" → 双击"Internet协议版本4(TCP/IPv4)"    手动设置IP地址为192.168.137.1，子网掩码255.255.255.0  点击"确定"保存设置    3.自己写一个虚假的网页（这里我模仿校园网的认证页面）    写一个py启动web服务器，测试能不能成功得到用户的账户密码    启动之后，模拟输入账户密码    成功捕获，准备和刚才搞得虚假wifi联合 4.劫持某些网站的dns 4.1. 以管理员身份打开文本编辑器  按 Win + R 输入：  notepad  然后按 Ctrl + Shift + Enter（以管理员身份运行记事本）  4.2. 通过记事本打开 hosts 文件  在记事本中点击 文件 → 打开  导航至：  C:\Windows\System32\drivers\etc  将右下角文件类型改为 "所有文件"  选择 hosts 文件并打开  4.3. 添加域名劫持规则  在文件 末尾 添加（示例劫持百度）：  192.168.137.1 www.baidu.com  192.168.137.1 baidu.com  这里我是用的山大官网，本科生院，而且劫持登录之后跳转正确网站  192.168.137.1 www.bkjx.sdu.edu.cn  192.168.137.1 bkjx.sdu.edu.cn  格式说明：  [你的服务器IP] [目标域名]  确保IP和域名之间用 空格或制表符 分隔  4.4. 保存文件  按 Ctrl + S 保存  如果提示无权限，请确认第一步是否以管理员身份运行记事本    4.5. 刷新DNS缓存  按 Win + R 输入：  cmd  在命令提示符中执行：  ipconfig /flushdns  成功劫持  此时再登录百度，那么进入的就是我提前设定的IP了   5. 远程测试（通过热点） 让另一台设备连接您的热点（如手机）。  访问 [www.bkjx.sdu.edu.cn](http://www.bkjx.sdu.edu.cn)。  此时，由于我提前开启了我的网页且把网页IP开启在我劫持的IP    显示我的假登录页面而非真实学校网站。————>输入账户密码  这里我展示输入的和后端对比  点击登录，会跳转到正常的官网，而我们后端获得账户密码  后端账户密码：    跳转后的网页：  成功欺骗用户！ | | | |
| 结论分析与体会一、实验结论分析  1. 技术可行性验证 通过搭建虚假WiFi热点和DNS欺骗，成功模拟了公共场所常见的"钓鱼WiFi"攻击场景。实验证明： • 普通用户极易被同名热点诱导连接（如伪装成"CMCC-Free"的热点）   • 未加密的HTTP流量可被直接截取，HTTPS网站通过DNS劫持也能实现钓鱼攻击   1. 实验方案优化 对比两种实现方式发现： | 方案 | 优点 | 缺点 | |-------|------|------| | 外置网卡+虚拟机 | 隔离性好 | 驱动冲突导致物理机断网 | | Win11原生热点 | 操作简便 | 需手动修改hosts文件 | 最终选择方案二因其更稳定，适合教学演示。 2. 安全风险警示 观察到三个典型漏洞： • 手机自动连接曾连过的热点（如"Starbucks-WiFi"）   • 用户常忽略浏览器证书警告  • 相同SSID下，信号强的热点优先被连接 二、实验收获与体会  1. 技术能力提升 • 掌握了热点配置（netsh命令）和DNS欺骗原理   • 学会用Python搭建简易钓鱼网站（模仿校园网登录页）  • 理解ARP欺骗与DNS劫持的关联性   1. 安全意识转变 亲身经历让我养成新习惯： • 在咖啡厅连WiFi必确认商家提供的准确SSID   • 重要操作只用4G网络或VPN  • 首次登录网站会检查地址栏HTTPS标识   1. 学习方法改进 • 遇到驱动冲突时，学会通过设备管理器回滚驱动   • 通过Wireshark抓包分析网络流量特征  • 采用"最小化测试"原则（先用本地设备自测）   1. 延伸思考 • 发现Windows Defender会拦截部分hosts修改   • 思考如何防御：建议同学们开启DNS-over-HTTPS  • 意识到这种攻击对物联网设备（如智能摄像头）威胁更大  三、致谢与展望 特别感谢老师提供的实验思路，虽然最终未采用该方案，但故障排查过程让我深刻理解了硬件驱动的工作原理。未来希望研究：   1. 如何用树莓派搭建便携式检测设备 2. 开发浏览器插件自动识别可疑热点 3. 探索WiFi6环境下的新型攻击防御方法   （注：本实验仅用于教学研究，所有操作均在封闭环境完成，未对真实网络造成影响） | | | |