实践报告

学院：工程师学院 专业：电气工程 班级：高阶6班

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 姓名 | 钟启迪 | 学号 | 22260281 | 成绩 |  |
| 实践时间 | 2023.3.29 | 指导老师 | 陈亮 | 实验组 |  |
| **实践名称** | **实验课-01\_端口扫描** | | | | |
| 实践环节1 | 虚拟操作机IP确定 | | | | |
| 实践环节2 | 调用nmap:输入指令nmap | | | | |
| 实践环节3 | 端口扫描：输入指令nmap -v –A 192.168.210.158 | | | | |
| 实验心得 | 学会应用端口扫描工具，完成目标系统端口扫描，发现445、135、139、3389、49153等端口处于开放状态。 | | | | |
| **实践名称** | **实验课-02\_漏洞利用** | | | | |
| 实践环节1 | 虚拟操作机和靶机IP确定 | | | | |
| 实践环节2 | 调用nmap对靶机IP进行端口扫描，确认所需端口是否处于开放状态 | | | | |
| 实践环节3 | 调用msfconsole，对靶机进行攻击。 | | | | |
| 实践环节4 | 调用攻击模块，对靶机进行攻击 | | | | |
| 实践环节5 | 结果显示RHOST参数没有设置，设置其参数，显示攻击结果 | | | | |
| 实验心得 | 掌握metaspolit系统漏洞利用，对评估操作系统的安全性具有重要意义。 | | | | |
| **实践名称** | **实验课-03\_拓扑探测** | | | | |
| 实践环节1 | 虚拟操作机IP确定 | | | | |
| 实践环节2 | Zenmap软件扫描结果 | | | | |
| 实践环节3 | 单击 Topology 按键，完成网络拓扑绘制 | | | | |
| 实验心得 | 为了绘制网络拓扑图，Nmap的发送特制的数据包到目标主机，然后对返回数据包进行分析。Nmap是一款枚举和测试网络的强大工具。 | | | | |
| **实践名称** | **实验课-04\_Wireshark软件安装** | | | | |
| 实践环节1 | 软件安装 | | | | |
| 实践环节2 | 软件测试 | | | | |
| 实验心得 | 安装wireshark工具包为基础工作，主要在过程中需要注意是否安装了winpcap，当你成功的在你的系统中装好了Wireshark，你就可以开始使用它。 | | | | |
| **实践名称** | **实验课-05\_Wireshark数据流跟踪** | | | | |
| 实践环节1 | 打开软件，导入文件 | | | | |
| 实践环节2 | 过滤 | | | | |
| 实践环节3 | 追踪数据流 | | | | |
| 实践环节4 | 保存文字结果 | | | | |
| 实践环节5 | 追踪数据流，获取相关信息 | | | | |
| 实践环节6 | 获取图片数据流 | | | | |
| 实践环节7 | 保存图片数据 | | | | |
| 实验心得 | 通过数据流跟踪可将数据流重组成原始的形式数据形式，便于进行分析查看，也可将数据流内容进行还原，对产生的网络故障、攻击溯源提供有力的技术支持。 | | | | |
| **实践名称** | **实验课-06\_Wireshark内网入侵分析** | | | | |
| 实践环节1 | 内容查找 | | | | |
| 实践环节2 | 追踪信息流TCP流 | | | | |
| 实践环节3 | 发现图片文件 | | | | |
| 实践环节4 | 图片处理 | | | | |
| 实践环节5 | 图片处理结果 | | | | |
| 实验心得 | 本课程主要讲解内网某木马攻击行为，通过发现通过一个端口进行命令传输，通过另外一个端口进行了数据执行。 | | | | |
| **实践名称** | **实验课-07\_ DLL 劫持漏洞** | | | | |
| 实践环节1 | Process Explorer 检查，主要查看应用程序的所以DLL | | | | |
| 实践环节2 | 注册表中的DLL | | | | |
| 实践环节3 | 脚本一键生成劫持指定DLL的CPP源码文件，将编译好的dll文件名改为cryptsp.dll，并完成拷贝。 | | | | |
| 实践环节4 | 攻击场景展现 | | | | |
| 实验心得 | DLL(Dynamic Link Library)文件为动态链接库文件，又称“应用程序拓展”，是软件文件类型。在Windows中，许多应用程序并不是一个完整的可执行文件，它们被分割成一些相对独立的动态链接库，即DLL文件，放置于系统中。当我们执行某一个程序时，相应的DLL文件就会被调用。一个应用程序可使用多个DLL文件，一个DLL文件也可能被不同的应用程序使用，这样的DLL文件被称为共享DLL文件。如果在进程尝试加载一个DLL时没有指定DLL的绝对路径，那么Windows会尝试去按照顺序搜索这些特定目录时下查找这个DLL，只要黑客能够将恶意的DLL放在优先于正常DLL所在的目录，就能够欺骗系统优先加载恶意DLL，来实现“劫持”。 | | | | |
| **实践名称** | **实验课-08\_ 永恒之蓝攻击和防御** | | | | |
| 实践环节1 | 主机和靶机IP确定 | | | | |
| 实践环节2 | 操作机中终端输入命令 msfconsole 运行 MSF 工具 | | | | |
| 实践环节3 | 使用 Metasploit 进行漏洞利用，获取目标系统权限 | | | | |
| 实践环节4 | 病毒上传 | | | | |
| 实践环节5 | 靶机防御 | | | | |
| 实验心得 | 本实验通过利用Metasploit对目标IP进行漏洞扫描确定目标存在漏了之后，进行漏洞利用获取系统权限之后，上传并植入病毒。通过dos命令删除默认共享，服务管理器通过关闭服务的方式，注册表添加子键值的方式来进行系统加固，防御MS17-010攻击。 | | | | |
| 教师意见 | 签名： 年 月 日 | | | | |
|  | | | | |