|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名：崔文帅 | | 学号：2025060163 | 专业年级： 20网工 | 班级：网三 |
| 分组： | | 实验室：软件学院402 | 指导教师：郭念 | 实验日期：2023-04-21 |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **网络协议分析与攻防技术** | | |
| **实验名称** | 实验八 计算机木马 | | |
| **实验目的** | 1. 了解上兴远控软件的用法 2. 了解广外女生的使用与清除 3. 探索防治木马的方法 | | |
| **实验内容** | 1. 上兴软件   1）上兴远控是一款功能强大的远程控制软件。  2）大多数特洛伊木马包含客户端和服务器端两个部分，也就是说，木马其实是一个C/S结构程序。 攻击者通常利用一种称为绑定程序（exe-binder）的工具将木马服务器绑定到某个合法的软件上， 诱使用户运行合法软件。只要用户运行该软件，特洛伊木马的服务器就在用户毫无察觉的情况下完成了安装过程。  3）攻击者要利用客户端远程监视、控制服务器，必须先建立木马连接； 而建立木马连接，必须先知道网络中哪一台计算机中了木马。 攻击者可以利用端口扫描工具（木马自带的或网络刺客的专用工具）进行端口扫描，搜索木马服务器， 一旦发现中的木马的计算机，即可添加到客户端控制程序的服务端主机列表中。也可由中了木马的主机主动通知攻击者而获取到所需信息。  4）获取到木马服务器的信息后，即可建立木马服务器和客户端程序之间的联系通道， 攻击者就可以利用客户端程序向服务器端程序发送命令，达到操控用户计算机的目的。 特洛伊木马的服务器通常是可以定制的，攻击者可以定制的项目一般包括： 服务器运行的端口号、程序启动时机、如何发出调用、如何隐身、是否加密。 另外，攻击者还可以设置登录服务器的密码、确定通信方式等。   1. 广外女生 2. 熊猫烧香 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | 1. 防治木马的方法 | | |
| **实验环境** | 目标机：192.168.1.3  工具：C:\实验工具集\04\_恶意代码\02\_木马技术与分析  http://10.11.52.15/upload/init/initimage/1489403946507/image002.jpg | | |
| **实验的实施阶段** | **实验步骤及实验结果** | **一、配置服务器端**  1.1 在操作机的c盘【实验工具集】-->【04\_恶意代码】-->【02\_木马技术与分析】-->【第3节 上兴远控】-->【上兴远控2014】中，打开主程序【rejoice.exe】，在主界面上方会显示操作机IP地址，在左下角会显示打开的端口信息。**实验截图如下：**    1.2 点击菜单栏中的【生成】，生成服务端配置程序，添加操作机IP地址，并再次确认上线端口。**实验截图如下：**    1.3 点击【测试连接】，提示测试成功，解析出的IP即为操作机IP。**实验截图如下：**    1.4 确认服务端配置程序的【安装名称】、【安装路径】，以及运行方式，还有服【服务启动】等相关信息。**实验截图如下：**    1.5 确认配置信息后，点击【生成服务端】，即可生成服务端配置程序，选择路径，点击【保存】，在这我们为了更好的传输文件，选择保存在C盘底下。**实验截图如下：**    **二、模拟中木马情景**  2.1 点击【开始】-->【运行】-->【输入mstsc】，进入到了远程桌面连接服务，输入目标机IP地址，打开选项。**实验截图如下：**    2.2 选择【本地资源】,勾选【磁盘驱动器】。**实验截图如下：**    2.3 选择【常规】,输入服务器管理密码【Simplexue123 】,并且进行连接。**实验截图如下：**    2.4 连接成功后，因为我们已经把我们操作机的硬盘资源映射到了目标机，所以我们可以将生成好的服务端程序拷贝到目标机的桌面上。**实验截图如下：**    2.5 我们双击拷贝到目标机的程序，这时在上兴远控的主界面会出现一条记录。**实验截图如下：**    **三、上兴远控的简单使用**  3.1 右键单击上线的主机，即可查看可以进行的相关管理操作。**实验截图如下：**    3.2 点击【系统管理】，即可进入到系统管理界面。**实验截图如下：**    3.3 右键单击【命令管理】，即可进入到目标机的命令行界面，输入命令【ipconifg】，即可查看IP地址。**实验截图如下：**    3.4 输入命令【net start】，即可查看系统所开启的服务。**实验截图如下：**    3.5 输入命令【netstat -no】，即可查看目标机进行的网络连接，以及所开启的端口号，PID为618。**实验截图如下：**    **一、广外女生的使用**  1.1 打开Windows 7桌面tools\广外女生的使用与手工清除文件夹下的gwg.exe，单击服务端设置。**实验截图如下：**    1.2 这里使用自定义，单击生成服务端，则会在当前目录下生成服务端木马程序GDUFS.exe。**实验截图如下：**    1.3 双击桌面上的共享快捷方式，打开共享文件夹，将在gwgirl文件夹下生成的木马程序GDUFS.exe拷贝到共享文件夹下。**实验截图如下：**    1.4 切换到目标机，在Windows server 2003上双击桌面上的共享快捷方式，打开共享文件夹，将GDUFS.exe复制到桌面上。**实验截图如下：**    1.5 双击运行木马程序，弹出提示。**实验截图如下：**    1.6 单击添加主机选项卡，设置起始和终止IP，验证密码为空，单击开始搜索，搜索到目标主机。**实验截图如下：**    1.7 在文件共享选项卡下，可以对目标机上的目录和文件进行相关操作，如上传、下载文件，打开选定文件，新建、删除文件夹，设置文件或文件夹属性等等。**实验截图如下：**    1.8 向目标主机发送一条信息，发送前可以进行预览。**实验截图如下：**    1.9 在远程注册表选项卡下，可以对目标机的注册表进行相关操作，如新建主键、删除主键、新建字符键值、新建DWORD键值、删除键值等等。**实验截图如下：**    1.10 在进程管理（Win9x）选项卡下，可以查看和终止目标机的进程。**实验截图如下：**    1.11 在屏幕控制选项卡下，可以对目标机的屏幕选择画质的高低及进行预览，预览的同时会在当前目录下截取对方的屏幕并保存为msconfig.jpg。单击开始控制可切换到目标机屏幕并进行控制，但是不是很灵敏且屏幕一直在闪烁，按Alt+F4即可退出。**实验截图如下：**    1.12 在密码记录选项卡下可以对目标机进行密码记录，不过好像没用。**实验截图如下：**    **二、广外女生的清除**  2.1 在目标机上打开运行，输入regedit打开注册表编辑器，找到如下注册项: HKEY\_LOCAL\_MACHINE\software\classes\exefile\shell\open\command\。先不要修改，因为如果这时修改注册表的话，DIAGCFG.EXE进程仍然会立即把它改回来。**实验截图如下：**    2.2 打开“任务管理器”，找到DIAGCFG.EXE进程，选中它按“结束进程”来关掉这个进程。注意：一定也不要先关进程再打开注册表，否则执行regedit.exe时又会启动DIAGCFG.EXE。前功尽弃！**实验截图如下：**    2.3 把HKEY\_LOCAL\_MACHINE\software\classes\exefile\shell\open\command\的键值由原来的 C:\winnt\system32\DIAGCFG.EXE "%1" %\*改为"%1" %\* 。**实验截图如下：**    2.4 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices，删除其中名称为“Diagnostic Configuration”的键值。**实验截图如下：**  2.5 这时就可以删除C:\Windows\System32文件夹下的木马程序DIAGCFG.EXE了，切记不可先删除这个文件，否则，就无法在系统中运行任何可执行文件了。**实验截图如下：** | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | 1.如何防止木马？  1.安装计算机杀毒软件，定期扫描系统查杀病毒  2.及时更新病毒库、更新系统补丁  3.下载软件到官方网站  4.不随意打开不明网页链接  5.使用网络通信工具时，不随意接收陌生人的文件  6.对计算机系统的各个账号要设置口令，及时删除或禁用过期账号  7.定期备份，当遭到病毒严重破坏后能迅速修复。 | | |