**山东大学威海分校机电与信息工程学院**

**网络后门与隐身 实验报告**

编号：

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 姓名 | 董喆 | | | 院系 | | 机电与信息工程学院 | | | 学号 | 201600800456 | |
| 任课教师 | | 程杰 | | | | | 指导教师 | | 程杰 | | |
| 实验地点 | | 知行南楼408 | | | | | 实验时间 | | 2019.4.4-2019.4.5 | | |
| 实验名称 | | 网络后门与隐身 | | | | | | | | | |
| 同 组 人 | | 无 | | | | | | | | | |
| 预习报告(对实验主要内容的认识) | | | | | | | | | 得分 |  | |
| **实验内容：**   1. 以虚拟机为攻击对象，使用工具wnc.exe在虚拟机设置网络后门，打开707，808端口，将wnc.exe加载到自启动程序列表中。 2. 使用psu.exe察看虚拟机注册表账户信息，按照课本案例6-4克隆管理员账户到guest账户，并测试结果。 3. 使用clearel.exe清除系统日志，并查看结果。   **实验准备：**  **①什么是Telnet：**  Telnet协议是[TCP/IP协议](https://baike.baidu.com/item/TCP/IP%E5%8D%8F%E8%AE%AE" \t "https://baike.baidu.com/item/_blank)族中的一员，是Internet远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA/455151" \t "https://baike.baidu.com/item/_blank)工作的能力。在[终端](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF/1903878" \t "https://baike.baidu.com/item/_blank)使用者的电脑上使用telnet程序，用它连接到[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8/100571" \t "https://baike.baidu.com/item/_blank)。[终端](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF/1903878" \t "https://baike.baidu.com/item/_blank)使用者可以在telnet程序中输入命令，这些命令会在[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8/100571" \t "https://baike.baidu.com/item/_blank)上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8/100571" \t "https://baike.baidu.com/item/_blank)。要开始一个telnet会话，必须输入用户名和密码来登录[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8/100571" \t "https://baike.baidu.com/item/_blank)。Telnet是常用的[远程控制](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E6%8E%A7%E5%88%B6/934368" \t "https://baike.baidu.com/item/_blank)Web[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "https://baike.baidu.com/item/_blank)的方法。  对于黑客来说Telnet是一个很好的网络后门，一旦入侵者与远程主机建立了Telnet连接，入侵者便可以使用目标主机上的软、硬件资源，而入侵者的本地机只相当于一个只有键盘和显示器的终端而已。  所以现在计算机一般默认将telnet端口关闭，如果打开则认为遭到了入侵。wnc.exe可以打开其他端口来开启telnet服务，有一定迷惑性。  **②wnc.exe的作用**  wnc.exe工具可以建立在对方主机上开启Web服务和Telnet服务。其中Web服务的端口是808，Telnet服务的端口是707。wnc.exe功能十分强大，但是该程序不能自动加载，需要将该文件加载到自启动列表中，让对方主机默无声息的留下后文。808和707端口隐蔽性还是不够的，还需要进一步上传后门软件进行网络隐藏。  **③psu.exe的作用：**  要想创建一个克隆管理员账号，要从注册表中入手。系统用户信息存储在%SystemRoot%\system32\config\sam文件中，这个文件默认被加密，用户无法打开。psu工具可以帮助用户打开sam数据库，从而进一步做到克隆。  **④为什么要清理日志：**  日志文件记录着用户再系统中的种种操作，同样黑客的种种操作也被记录下来，所以需要清理系统日志来做到隐身。clearel.exe是一款功能强大的用来清除系统日志的工具。 | | | | | | | | | | | |
| 实验内容（问题，思路，程序，结果） | | | | | | | | | 得分 |  | |
| 1. **使用wnc.exe**   打开Windows 2000虚拟机，进入C盘下，新建wnc目录，并将wnc.exe、reg.txt和reg.exe放在该目录下：    然后win+r,运行cmd，进入该目录下，执行wnc.exe：    然后运行netstat -an 查看当前打开的端口：      **测试Web服务的808端口：**  首先输入ipconfig,查看系统ip：    可以看到ip地址为169.254.6.207  打开IE浏览器，输入169.254.6.207:808    进入C盘：    可以看到支持上传文件功能。  **测试Telnet：**  进入命令行输入:telnet 169.254.6.207 707:    执行结果是进入了C:\wnc目录：      可以直接使用命令行对远程主机进行各种操作。  由于wnc不能自启动，所以需要将其加载到自启动列表中，做法是：  将reg.exe和wnc.exe拷贝到system32目录下，然后执行命令：  reg.exe add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v service /d wnc.exe  查看自启动项：     1. **使用psu.exe**   打开注册表[HKEY\_LOCAL\_MACHINE\SAM]，发现是无法打开的，因为操作系统对此进行了隐藏：    我们需要使用psu.exe来获得该值的查看和编辑权，将psu.exe拷贝到C盘目录下，然后查看任务管理器查看winlogon.exe的PID:    PID=224,然后cmd进入C盘目录下，执行：  **psu -p regedit -i 224**    然后重新打开注册表：    默认情况下F4为管理员，F5为Guest，其中右侧F记载着用户的各种信息  我们把F5的F信息完全复制给F5：  变为：    接下来我们要实现让Guest用户在金庸的状态登录，这样可以一定程度上骗过管理员。  进入User，然后点击注册表菜单-到处注册表文件：    然后删除Guest和00001F5两个目录，删除后    然后查看用户信息：      然后再将刚才导出的注册表导入：    这样导入竟然会出错，提示有程序正在使用，我的方法是将注册表文件拖入注册表对话框中，导入成功。    然后使用命令行修改属性：    修改密码为123，并将Guest禁用，查看用户：    已禁用  切换用户登录：    测试权限，添加一个新的用户：    并且可以将其设置为管理员权限：    所以Guest也拥有超级用户权限。   1. **使用clearel.exe**   将clearel.exe复制到System32：    然后进入cmd命令行，运行：    然后查看事件查看器：        可以看到实验目录已经清空  **至此，实验结束。** | | | | | | | | | | | |
| 实验结论 | | | | | | | | | 得分 |  | |
| 本实验结论目前正在WIn2000下进行测试：  ①telnet端口打开后，远程的主机可以通过telnet命令对此台主机进行控制。前提是知道用户名密码。通过这种方式可以做一个后门。使用wnc工具可以开启808和707端口，这两个端口分别是web和telnet的端口并且不那么显眼。  ②为了防止管理员更改管理员密码对后门造成影响，可以用克隆管理员权限的方法对Administrator进行复制。使用psu工具可以打开保存系统账号信息的数据库，通过复制数据库权限的方法使Guest拥有Administrator的权限，然后再采用导出-导入-禁用的方法造成Guest被禁用的假象来迷惑管理员。  ③做到网络隐身的一个重要的途径是清除系统日志的方法。黑客在主机上的所有操作会被系统日志记录，为了隐藏自己需要把相关日志清除。使用clearel.exe可以做到使用命令的方式快速清除系统日志，功能强大。 | | | | | | | | | | | |
| 教师评价 | | | 总分 | |  | | | 实际得分 | | |  |
|  | | | | | | | | | | | |