|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名：崔文帅 | | 学号：2025060163 | 专业年级： 2020 | 班级： 网三 |
| 分组： | | 实验室：402 | 指导教师：郭念 | 实验日期：2023-04-28 |
| **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** | 实验九 口令攻击 | | |
| **实验目的** | 1）了解密钥穷举、字典、查表攻击的过程  2）理解密钥穷举、字典、查表攻击的原理  3）掌握密钥穷举、字典、查表攻击的基本步骤  1) 理解Getpass本地内存中读取windows口令的原理  2) 学习Getpass本地内存中读取windows口令的过程 | | |
| **实验内容** | **1) 密钥穷举、字典、查表攻击**  a     穷尽密钥搜索攻击    设k是密钥长度，在唯密文攻击下，攻击者依次试用密钥空间中所有2k个密钥解密一个或多个截获的密文，直到得到一个或多个有意义的明文块。当已知（选择）明文攻击下，攻击者试用密钥空间中的所有2k个密钥对一个已知明文加密，将加密结果同该明文相对应的已知密文比较，直至两者相等，然后再用其他几个已知明密文对来验证该密钥的正确性。穷尽密钥搜索的复杂度平均为2k-1次加密。  b     字典攻击    攻击者搜集明密文对，并对它们编排成一个“字典”。攻击者看见密文时，检查这个密文是否在字典里，如果在，他就获得了该密文相对应的明文。如果n是分组长度，那么字典攻击需要2n个明密文对才能使攻击者在不知道密钥的情况下加解密任何消息。  c     查表攻击    设k是密钥长度，查表法采用选择明文攻击，其基本观点是：对一个给定的明文x，用所有2k个密钥k记其全体为k），预计算密文image.png。构造一张有序对表image.png，以image.png给出k的标号。因此，对于给定的密文，攻击者只需从存储空间中找出相对应的密钥K即可。  1) 我们之前学习的是通过获得SAM,破解SAM来获得管理口令，今天我们介绍的是getpass这款软件，在2012年被开发出来，可以直接从 lsass.exe 里获取windows处于active状态账号明文密码。比破解SAM更快，更准。 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | **密钥攻击** | | |
| **实验环境** | Windows 7  工具：C:\tools\密码学课程\02 密码学分析\lab1  Getpass常用于黑客在已经获得目标系统webshell，且拥有system权限时的操作，此次实验在本机完成。   工具: C:\实验工具集\02\_主机安全\02\_Windows口令安全与破解 | | |
| **实验的实施阶段** | **实验步骤及实验结果** | **一、DES加密**  **编辑框**  1) 输入密钥：输入用于加密的十六进制密钥（16位）  2) 输入明文：输入明文串  3) 对应密文：DES加密后的密文，十六进制（16位）  **按钮**  1) 加密：DES加密  2) 导出明文：导出明文文件cleartext.txt到程序所在文件路径  3) 导出密文：导出密文文件cipher.txt到程序所在文件路径  **操作流程**  输入密钥->输入明文->点击加密->得到密文->导出明文->导出密文  1.1 运行【CryptographyLab.exe】打开界面。**实验截图如下:**    1.2 DES加密。输入16位密钥：1234567af1234567，输入明文：nihao，点击加密，可得到密文：df73fb877256e45d。**实验截图如下:**    1.3 点击导出明文和导出密文，在程序所在目录生成ciphertext.txt和cleartext.txt，分别用于存放明文和密文。**实验截图如下:**    **二、穷举攻击**  **编辑框**  1) 导入明文：从之前DES加密导出的明文文件中导入明文  2) 导入密文：从之前DES加密导出的密文文件中导入密文  3) 密钥范围：从低到高，十六进制，16位  4) 对应密钥：穷举攻击破解出的密钥，十六进制，16位  **按钮**  1) 导入明文  2) 导入密文  3) 开始破解  4) 显示密钥  **操作流程**  导入明文->导入密文->输入密钥范围->开始破解->得到密钥  流程如下所示：  2.1 重新打开CryptographyLab.exe，选择穷举攻击，点击导入明文，导入密文，分别从ciphertext.txt和cleartext.txt文件中 导入明文和密文，输入密钥范围1234567af1234565和1234567af1234569。**实验截图如下:**    2.2 点击开始破解，相关输入数据存入程序目录下input.txt文件，弹出运行界面展示破解过程。**实验截图如下:**    2.3 运行完后，将找到的密钥存入output.txt，回到穷举攻击界面，点击显示密钥按钮，将密钥显示出来。**实验截图如下:**    **三、字典攻击**  **编辑框**  1) 输入对数：输入密文明文对数，最大为100000  2) 输入密钥：输入固定的密钥，十六进制，16位  3) 密文明文对：每页显示5对  4) 输入密文：从密文明文对中选择密文  5) 对应明文：查找到的明文，十六进制，16位  **按钮**  1) 修改：修改密文明文对数  2) 生成明文密文对文件：生成的contextCiper.txt存放到程序所在文件路径  3) 上一页  4) 下一页  5) 字典攻击  **操作流程**  输入对数->输入密钥->生成明文密文对文件->输入密文->点击字典攻击->得到对应明文  3.1 重新打开CryptographyLab.exe，选择字典攻击，输入对数50，点击修改。**实验截图如下:**    3.2 输入密钥1234567af1234567，点击生成明文密文对文件，生成50对明密文对。**实验截图如下:**    3.3 从生成的密文明文对中选一个密文，比如输入密文2bbb0420cb1375e1，点击字典攻击，则找到对应明文606b340e0ed4e47b。**实验截图如下:**    **四、查找攻击**  **编辑框**  1) 输入对数：输入密文明文对数，最大为100000  2) 输入明文：输入明文串  3) 密钥密文对：生成随机的密钥密文对  4) 输入密文：从密钥密文对中选择密文  5) 对应密钥：查找到的密钥，十六进制，16位  **按钮**  1) 修改：修改密钥密文对数  2) 生成对照表：生成密钥密文对照表，存放到程序所在文件路径keyList.txt  3) 上一页  4) 下一页  5) 查找攻击：开始进行查找攻击  **操作流程**  输入对数->输入明文->生成密钥密文对->输入密文->点击查找攻击->得到对应密钥  4.1 重新打开CryptographyLab.exe,选择查找攻击，输入对数30，点击修改。**实验截图如下:**    4.2 输入明文12345678，点击生成对照表。**实验截图如下:**    4.3 输入密文b5c9824c5ceb6298，点击查找攻击，成功找到密钥0000000000005b25。**实验截图如下:**    **【实验步骤】**  **一、密码破解**  1.1 打开C:\实验工具集\02\_主机安全\02\_Windows口令安全与破解\第6节Getpass本地内存中读取windows口令文件夹，找到getpass.exe。**实验截图如下:**    1.2 双击打开该软件，可直接获得windows登录口令。**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. 思考穷举攻击、查找攻击和字典攻击的区别。  2. 思考影响穷举攻击、查找攻击和字典攻击的因素。  3. 除了getpass可以直接获得登录口令，还有哪些工具可以直接获取登录口令？ | | |