【技能点：进程中抓下管理员明文密码】结题思路

原创

loveleaves66 于 2020-12-20 11:03:42 发布 446 收藏 1

文章标签： 网络安全 安全

本文链接：https://blog.csdn.net/qq_33771823/article/details/111414730

封神台 - 掌控安全在线演练靶场系列教程-第七章：GET THE PASS！ 【技能点：进程中抓下管理员明文密码】结题思路

原文链接

本章重点–进程中抓下管理员明文密码！

1. 在上一章中，我已经通过用已经组装好的wscript.shell（iis6.exe）创建了一个administrators组成员，继续用此用户继续远程访问。
2. 下载mimikatz并用菜刀上传mimikatz至服务器。注意路径中绝对不能有中文（可以有空格）！否则加载DLL的时候会报错：找不到文件。

在远程终端（3389、mstsc.exe）、虚拟桌面中抓取密码的方法：

通常你在远程终端中运行该程序会提示：存储空间不足，无法处理此命令。

这是因为在终端模式下，不能插入远线程，跨会话不能注入，你需要使用如下方法执行该程序：
首先提取几个文件，只抓取密码的话，只需要这几个文件：（并打包）
1.mimikatz_trunk\tools\PsExec.exe
2.mimikatz_trunk\Win32\mimikatz.exe
3.mimikatz_trunk\Win32\sekurlsa.dll
｛
mimikatz作者主页：L’aide mémoire d’un kiwi
mimikatz官方下载地址：Blog de Gentil Kiwi
mimikatz基础命令：
1.cls 清屏
2.exit 退出
3.version 查看mimikatz的版本
4.system::user 查看当前登录的系统用户
5.process::list 列出进程
6.service::list 列出系统的服务
7.privilege::list 列出权限列表
8.privilege::debug 提升权限
9.sekurlsa::wdigest 获取本地用户信息及密码
10.sekurlsa::logonPasswords 获取登陆用户信息及密码
｝
3. 通过远程桌面连接使用上一章创建的administrators组用户登录目标服务器，并找到自己刚才上传的mimikatz。
4.获取密码有很多方法，下面介绍一种：
1.运行主程序：mimikatz.exe；
2.输入：privilege::debug；（提升权限，成功显示：Privilege ‘20’ OK）
3.输入：sekurlsa::logonPasswords，然后找到对应用户和密码。（ * NTLM后即为密码）
4.复制NTLM后内容到CMD5解密即得管理员administrator密码！(CMD5官网：https://cmd5.com/） 或用其他方法直接得到明文密码（及password后）。
最后一步就是获得FLAG!
打开桌面文件SEVEN-小芳.txt，此时显示拒绝访问，为什么呢？权限不够吗？只是权限受限，此时需要选择SEVEN-小芳.txt，右键选择属性，点击安全选项框，选中administrator，点击高级，在弹出的对话框中，把属性为拒绝的全部改为允许。双击属性为拒绝的栏目，在弹出的对话框中把完全控制改为允许并确定保存即可。
打开SEVEN-小芳.txt显示“解压密码就是administrator的登陆密码”，它告诉我们文件想找到小芳吗.zip的解压密码为administrator的登陆密码。打开想找到小芳吗.zip显示权限不够！权限又不够！其实是文件的用户使用权限受限，其实解决方法同上，跟打开SEVEN-小芳.txt一样。设置完成打开输入解压密码，里面就是FLAG！
“小芳在我的手上！
如果想要她活命的话，
你必须为我们工作！
哈哈哈你没有理由拒绝我的，对吧？
快来找我吧，完成靶场第八关，获得未知的资格吧！
第七关FLAG*********”
注意flag包含FLAG，只输入flag后内容是不对的，必须包含FLAG！【哭笑】。

附件：（文件请到原文链接下载）
1.mimikatz_runk
2.菜刀

附：up主专享注册码推广注册链接：https://bbs.zkaq.cn/Index/s/OMRdTNHg
知乎