系统安全实验四

Julius Karl

2024 年 6 月 26 日

1 实验内容

Windows 操作系统本地用户的账户与密码信息被存储在本地计算机的安全账户管理器（SAM）中。该文件位于系统盘 Windows 目录下的 system32\config 文件夹中，如图 1-1 所示。

在 SAM 文件中，账户和密码信息不是以纯文本形式存储的，而是经过散列计算的，而且该散列是经过严格加密的，具有不可逆向计算的特性。

当用户输入账户和密码登录时，计算机即将该信息提交到本地计算机的 SAM 数据库中进行对比，如果对比结果相同，则登录验证成功；否则，登录验证失败。本地用户登录后，其账户与密码信息以明文形式保存于 winlogon.exe 的进程中。

因此，网络安全管理员或黑客对 Windows 操作系统用户信息进行恢复或破解的方法主要有以下 3 类：

方法 1：利用 LC、SAMInside 以及 Ophcrack 等工具破解 SAM 数据库中的账户与密码信息。

方法 2：利用 mimikatz 等工具从 winlogon.exe 进程中破解用户的账户与密码信息。

方法 3：利用 Windows PE 工具修改操作系统文件，使 SAM 数据库中包含已知的账户与密码信息。

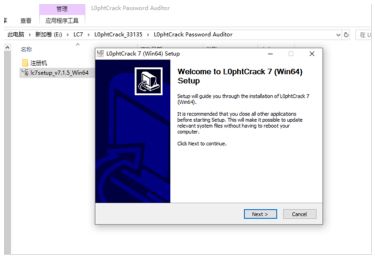
这 3 类方法中，方法 1 中的 LC 工具支持远程破解，能够快速破解简单的密码，对于复杂程度较高的密码，破解时间很长，Ophcrack 工具采用查表的方式破解密码，对于复杂程度较高的密码，破解时间大大缩短；方法 2 中的 mimikatz 工具由于读取的是进程中的明文信息，成功率极高，但需要用户的账户和密码信息存在于内存中；方法 3 适用于无法进入操作系统的情况，但需要进入 BIOS 修改计算机的启动方式。

2 实验目的

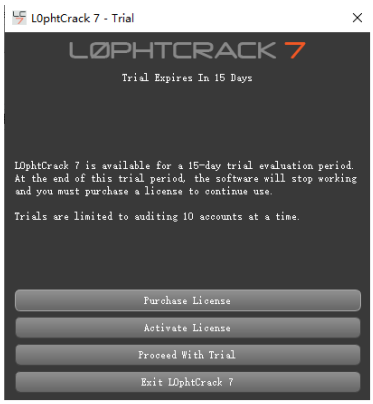
1. 使用 LC 工具破解 SAM 数据库中的用户信息
2. 使用 Qphcrack 工具破解 SAM 数据库中的用户信息
3. 保护 SAM 数据库中用户信息免被破解

3 过程

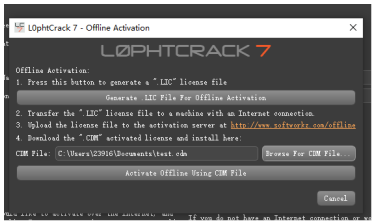
3.1 方法一：LC



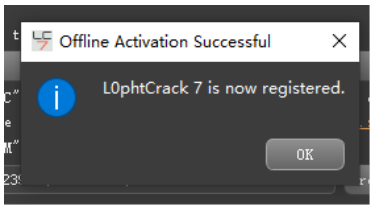
(a) 安装 LC 程序



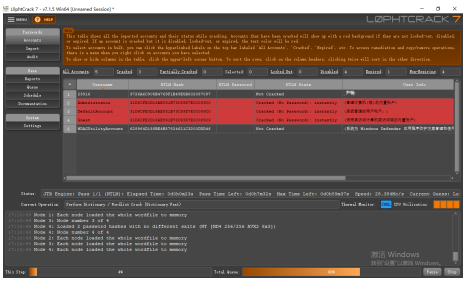
(b) 启动激活程序



(c)



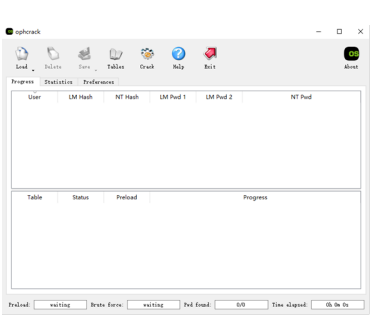
(d)



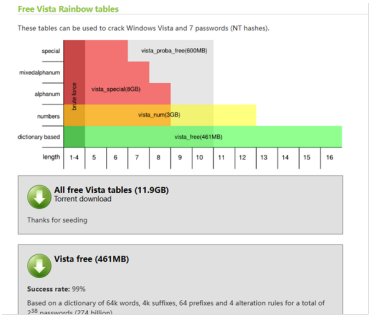
破解完成

3.2 方法二：彩虹表

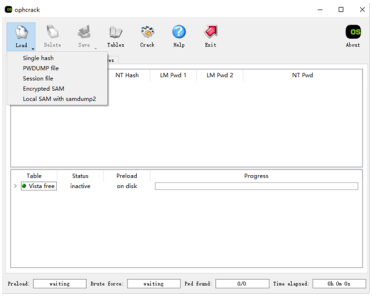
使用 Qphcrack 工具破解 SAM 数据库中的用户信息



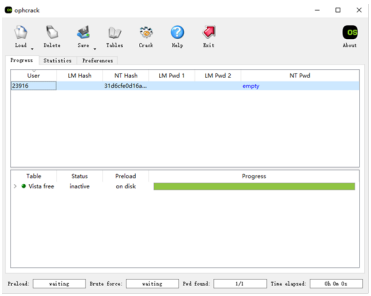
(a)



(b)



(c)



(d)

3.3 方法三：使用 SysKey 加密 SAM 数据库中用户信息

现已停用

4 实验总结：

破解方法的有效性取决于多种因素，如目标系统的安全性、密码的复杂度、使用的工具和技术等。LC 工具和 Ophcrack 都是知名的密码恢复工具，它们使用不同的技术来破解密码。

LC 工具：这种工具通常使用暴力破解或字典攻击来恢复密码。如果密码较短或不够复杂，这种方法可能相对有效。然而，对于长且复杂的密码，这种方法可能需要很长时间。

Ophcrack：这个工具使用彩虹表来破解密码，这是一种预先计算好的哈希值表。如果彩虹表中包含了密码的哈希值，那么 Ophcrack 可以快速恢复密码。这种方法对于标准的密码库非常有效，但如果密码非常独特或复杂，彩虹表可能不包含相应的哈希值。总的来说，如果密码较为简单或常见，Ophcrack 可能更有效，因为它可以快速匹配彩虹表中的哈希值。但对于非常复杂的密码，任何工具都可能需要相当长的时间来破解。