**计算机系统安全实验文档**

1. 实验名称：

Windows下基于彩虹表的口令破解技术

1. 实验目的：

通过实验，加深Windows的口令破解技术，特别是基于彩虹表的口令破解技术，并且熟悉rainbowcrack的使用，学习彩虹表的生成过程和破解过程。

1. 实验环境：

Windows 10 系统， Win64

1. 实验内容：
2. 生成或抓取hash值（MD5）：
3. 根据需要生成彩虹表：
4. 对彩虹表进行排序，方便破解时查询：
5. 使用彩虹表，破解hash值：
6. 实验方案：
7. 获取hash值的方案有以下五种：

|  |  |  |
| --- | --- | --- |
| 方法编号 | 方法描述 | 示例 |
| 1 | 编译hash源码，如crypt源码 |  |
| 2 | 使用crypt库，调用crypt函数 |  |
| 3 | Hash值生成工具 | Cain、或其他 |
| 4 | 网络嗅探 | 使用wireshark或cain抓取smb包 |
| 5 | 本地抓取 | Mimikatz工具获取windows登录信息 |

1. 生成彩虹表的方案：

使用rainbowcrack工具生成指定算法的彩虹表。

1. 彩虹表排序方案：

使用命令，例如

*rtsort \*.rt*

1. 使用彩虹表的方案：

使用命令，例如

*rcrack .\\*.rt -l .\hashlist.txt*

命令中的hashlist.txt文件中包含了hash值的信息，有多个hash值时，每个hash值占用一行。

也可使用基于GUI的rcrack-gui.exe破解hash值。