## Linux系统口令破解

计51 柴华君 2015011377

计51 石英昊 2015011384

1. 实验目标

使用适当的工具，破解给定的加密后的linux口令。

1. 实验原理

给定加密口令如下：

test:$6$dRf2Gldj$W4DfAK9vGyz9XCCJrsPOtR7tgf3q6lDH92kE2WKHNXZHfmu7dKFgo5M72jrL2hXJjxcdg596WsWPYYgGr mPZp1:17107:0:99999:7:::

linux加密后的口令一般保存在/etc/shadow下，只有root用户可以查看。保密加密后的密码每一行代表一个用户，每一行通过冒号分为9个部分

1.用户名

2.加密后的密码

3.上次修改密码的时间(从1970.1.1开始的总天数)

4.两次修改密码间隔的最少天数，如果为0，则没有限制

5.两次修改密码间隔最多的天数,表示该用户的密码会在多少天后过期，如果为99999则没有限制

6.提前多少天警告用户密码将过期

7.在密码过期之后多少天禁用此用户

8.用户过期日期(从1970.1.1开始的总天数)，如果为0，则该用户永久可用

9.保留

分析给定的加密字符串可知，用户名为test，加密后的密码为$6$dRf2Gldj$W4DfAK9vGyz9XCCJrsPOtR7tgf3q6lDH92kE2WKHNXZHfmu7dKFgo5M72jrL2hXJjxcdg596WsWPYYgGr mPZp1

加密的密码格式如上，一般为

$id$salt$encrypted

id表示加密算法，1代表MD5，5代表SHA-256，6代表SHA-512 salt表示密码学中的Salt,系统随机生成 encrypted表示密码的hash

结合实验给定的已知条件，我们可以知道该密码是由SHA-512加密算法加密的5位ascii码值，使用了盐值dRf2Gldj来对密码进行随机化加密。

1. 实验过程

实验过程中，我们尝试了使用John the Ripper和hashcat工具，最初使用字典破解，最终没有破解成功。

#此处应有图

所以，我们转向暴力破解的方法。考虑到可见的ascii码值共有95位，他们的随机排列组合共有95＾5种，数量过于庞大，无法在短时间内破解成功。所以，我们从几种简单的情况入手，先考虑小写字母随机组合、数字随机组合和小写字母和数字混合在一起排列组合。最后在自己生成的简单字典了找到了答案。

1. 实验结果

最后linux密码破解的结果为tls13，下图为破解截图