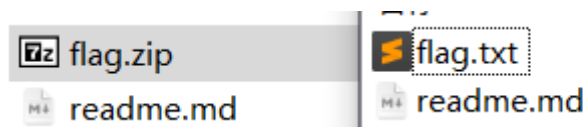


flag.zip中存在和readme.md相同的文件，根据提示进行了解。此处为zip明文攻击。



注意明文攻击需要完全相同的加密算法，如这里文件内使用store，则构造readme.zip时也得使用store算法。

名称	大小	压缩后大小	修改时间	创建时间	访问时间	属性	加密	注释	CRC	算法
flag.txt	37	49	2021-09-2...	2021-09-2...	2021-09-2...	A	+		28E79BA1	ZipCrypto Store
readme.md	170	182	2021-09-2...	2021-09-2...	2021-09-2...	A	+		ED047374	ZipCrypto Store

压缩包(A): C:\Users\86199\Downloads\level-1\level-2\zip\level-3\tuiqian\flag\

readme.zip

压缩格式(F): zip

更新方式(U): 添加并替换文件

压缩等级(L): 标准压缩

压缩方法(M): 仅存储

字典大小(D): 快速压缩

单词大小(W): 标准压缩

固实数据大小: 最大压缩

CPU 线程数: 32

路径模式: 相对路径

选项:

☐ 创建自释放程序(x)

☐ 压缩共享文件

☐ 操作完成后删除源文件

加密:

输入密码:

☒ 显示密码(S)

加密算法: ZipCrypto

确定 取消 帮助

使用archpr明文攻击。

口令已成功恢复!



Advanced Archive Password Recovery 统计信息:

总计口令	n/a
总计时间	1m 41s 393ms
平均速度(口令/秒)	n/a
这个文件的口令	ooh0ooh!
十六进制口令	6f 6f 68 30 6f 6f 68 21

保存... 确定

ARCHPR 4.54 - 0%

文件(F) 恢复(R) 帮助(H)

打开 开始! 停止 基准测试 升级 帮助 关于 退出

加密的 ZIP/RAR/ACE/ARJ 文件

攻击类型

明文

范围 长度 字典 明文 自动保存 选项 高级

明文选项

明文文件路径:

C:\Users\86199\Downloads\level-1\level-2\zip\level-3\tuiqian\flag\flag.zip

开始于: 0

密钥 4a4bf6e2 密钥 91006f97 密钥 f4b14545

☐ 允许使用二进制文件作为明文 ZIP 档案文件

状态窗口

2021/10/1 12:27:54 - 明文攻击已开始
2021/10/1 12:29:35 - 加密密钥已成功恢复!
2021/10/1 12:29:35 - 口令已成功恢复!
2021/10/1 12:29:35 - 'ooh0ooh!' 是这个文件的一个有效口令

当前口令: n/a 平均速度: n/a
已用时间: 1m 41s 剩余时间: 1h 19m 13s

明文攻击正在进行, 尝试找回口令(最长 9 个符号)

0%

ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

经过1m41s, 明文攻击成功。

flag: Aurora{Happy_Nati0na1_Day!with_m1sc!}