

**长沙理工大学**

计算机与通信工程学院

**网络安全实验报告**

**实验名称**:**\_\_ 密码破解 \_\_\_\_**

**年级**： **大三 班级**： **网络2102班**

**学号**： **202108060918 姓名**： **王俊\_\_\_\_**

**完成日期**： **2024 年 4 月**  **28 日**

**授课老师： 夏卓群\_\_\_\_\_\_\_\_\_\_\_\_\_**

一、实验名称

密码破解

二、实验目的

对office文档进行密码破解，实现一次密码盗取入侵活动

三、实验内容

对一台操作系统为WINDOWS 11的计算机安装Advanced Office Password Recovery (AOPR)软件，对想获取密码的Office文档进行密码破解，从而盗取文档内容。

四、实验原理：

目前常用的网络攻击手段主要有社会工程学攻击、物理攻击、暴力攻击。

字典攻击是最常见的一种暴力攻击，如果黑客试图通过使用传统的攻击方法去获得密码的话，将不得不尝试每种可能的字符，包括大小写、数字和通配符等。

字典攻击通过仅仅使用某种具体的密码来缩小尝试的范围。一个字典文件本身就是一个标准的文本文件，其中的每一行就代表一个可能的密码。

Office文档是可以加密的，密码一般是3到4位，破解这种密码只需要很短的时间。

五、实验环境：

WINDOWS 11操作系统 ，

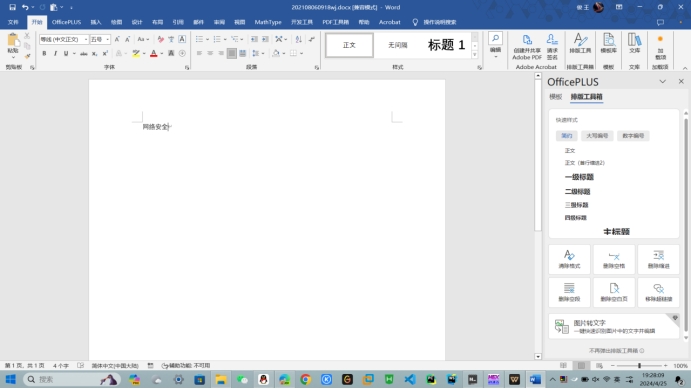
Advanced Office Password Recovery(AOPR)软件

六、实验步骤：

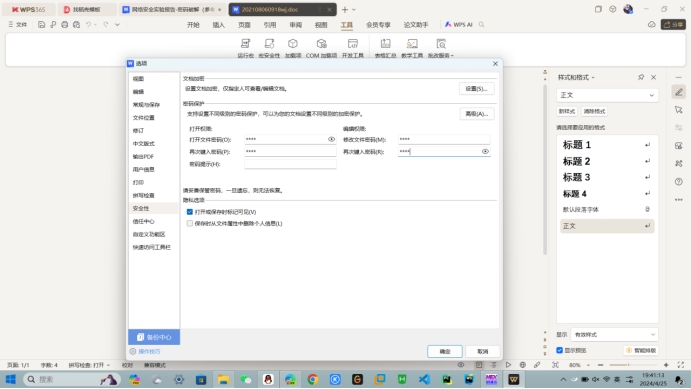
1．新建一个加密的Word文档

具体步骤：

（1）新建一个WORD文档



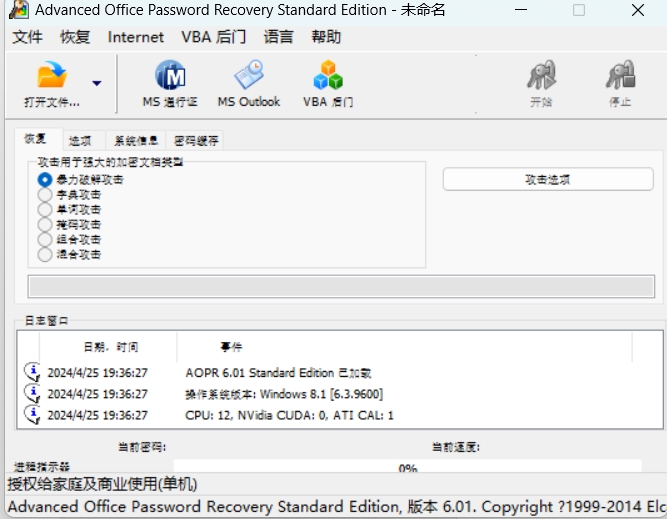
（2）在该文档的“工具”菜单“选项”对话框的“安全性”选项卡中设置密码，在“打开文件时的密码”和“修改文件时的密码”两个文本框中都输入设置的密码，都设置为0000。

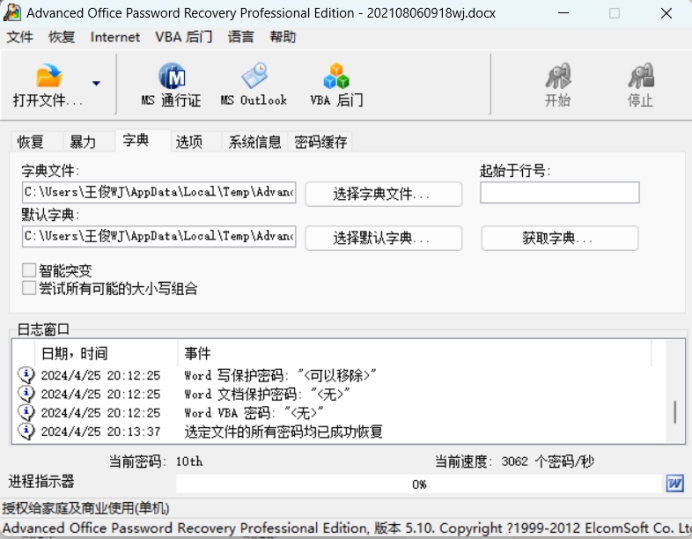


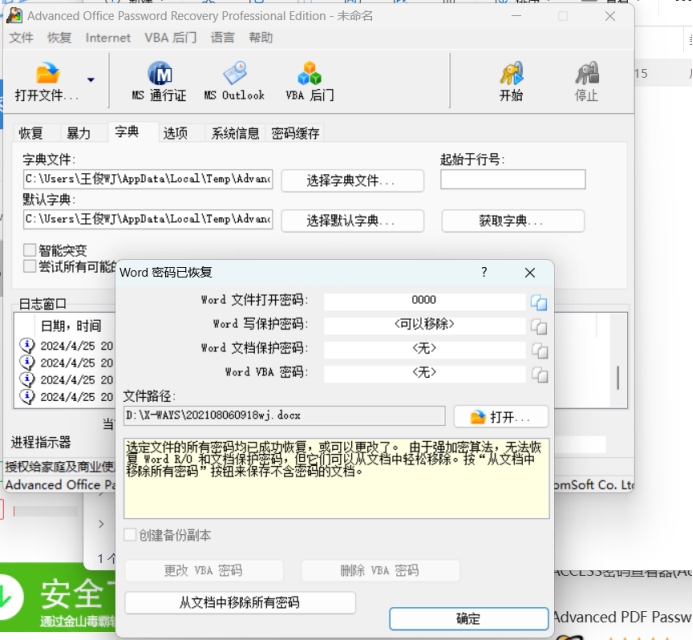
2．使用Office密码破解工具：Advanced Office Password Recovery

具体步骤：

（1）打开暴力破解软件Advanced Office XP Password Recovery(AOXPPR)

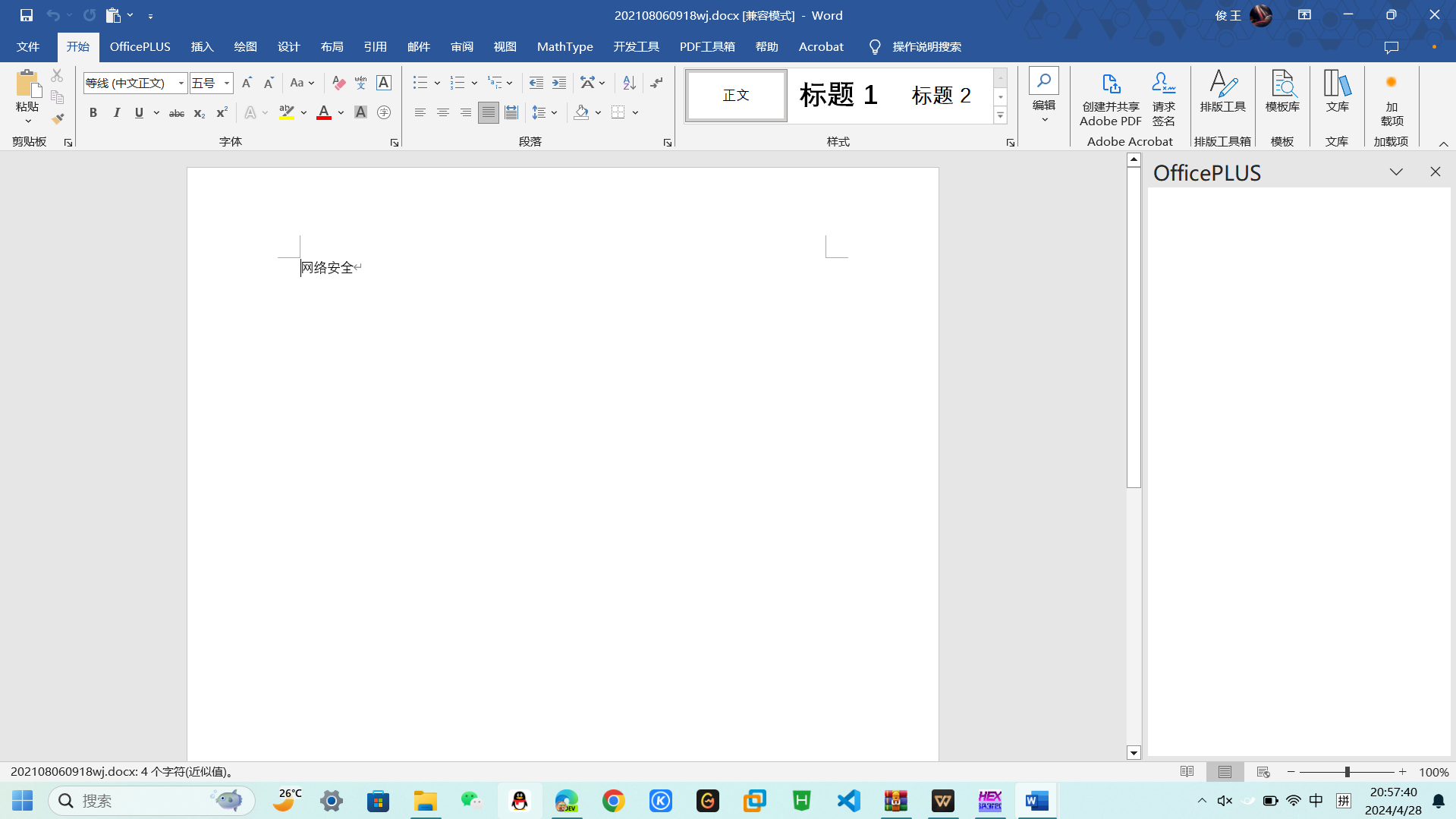
（2）选择字典破解

（3）单击工具栏按钮“打开文件”，打开刚才建立的Word文档“网络安全.doc”，开始进行字典破解 ，得到的结果如图所示：



七、实验总结

通过Advanced Office XP Password Recovery(AOXPPR)软件，成功对加密word文档进行密码破解，得知Word文件打开密码是0000，从而获取文档内容。

 在使用Advanced Office XP Password Recovery (AOXPPR)软件对加密的Word文档进行密码破解的实验过程中，我有以下几点心得和体会：

1. **软件易用性**：AOXPPR软件设计较为人性化，即便是初次使用者也能较快上手。它的界面直观，操作流程清晰，如百度经验所述，从选择暴力破解模式、设定密码条件到打开目标文件，每一步都有明确的指引。
2. **密码策略的重要性**：通过实验我发现，简单的密码（如短密码、纯数字或常见词汇）很容易被破解，而采用复杂密码策略（如混合大小写字母、数字和特殊符号，且长度足够长）的文档，破解所需的时间显著增加，甚至可能无法在合理时间内破解。这凸显了设置强密码对于文档安全的重要性。
3. **破解速度与资源消耗**：我注意到，破解过程的快慢极大地依赖于密码的复杂度和你所选的破解策略。使用暴力破解或字典攻击时，如果密码复杂，破解可能非常耗时，同时也会占用大量的计算资源。这提示我们在日常工作中应合理评估文件的敏感程度，决定是否需要加密以及加密的强度。
4. **备份与管理意识**：该实验增强我对数据备份和密码管理的认识。与其依赖密码破解，不如建立良好的数据备份习惯和密码管理体系，如使用密码管理器，定期更换密码，以防万一。
5. **安全意识提升**：通过实验，我深刻理解到文档加密不是绝对安全的，尤其是在面对专业破解工具时。因此，结合其他安全措施，如访问控制、文件权限管理等，对于维护信息安全至关重要。