* **南昌大学《网络安全概论实验》**

**实验报告**

**---（1）扫描工具的使用**

学生姓名： 学 号： 专业班级：

实验类型：■ 验证 □ 综合 □ 设计 □ 创新 实验日期： 实验成绩：

**一、实验目的**

为了发现系统缺陷和漏洞，入侵者和网络管理员都常常使用扫描的方式来侦测系统和网络， 不过两者目的不一致。入侵者是通过扫描技术来收集信息和检测漏洞，为入侵做好前期准备 工作；网络管理员则是发现系统漏洞后及时修补，以提高安全性能。

**二、实验内容**

1、使用X-Scan综合扫描器扫描某服务器，看看该服务器存在哪些漏洞，并写出扫描结果。

2、使用Nmap对网络进行探查和安全审核。

**三、实验要求**

1. 根据实验任务书的具体任务要求完成实验；
2. 独立完成实验并形成实验报告；
3. 实验报告侧重实验步骤、实验数据及分析、实验体会及改进三部分内容；
4. 尽可能用自己的语言文字而不是实验任务书及实验平台重的操作指南文字来组织实验报告。

**四、主要实验步骤**

**五、实验数据及分析结果**

**六、实验体会或对改进实验的建议**

**七、参考资料**

**南昌大学《网络安全概论实验》**

**实验报告**

**---（2）木马测试及清除**

学生姓名： 学 号： 专业班级：

实验类型：■ 验证 □ 综合 □ 设计 □ 创新 实验日期： 实验成绩：

**一、实验目的**

学习木马远程控制软件的使用，通过实验可以了解木马和计算机病毒的区别，熟悉使用木马 进行网络攻击的原理和方法，了解木马程序的自启动和隐藏方法。

**二、实验内容**

使用木马做相关测试。

1. **实验要求**
   1. 根据实验任务书的具体任务要求完成实验；
   2. 独立完成实验并形成实验报告；
   3. 实验报告侧重实验步骤、实验数据及分析、实验体会及改进三部分内容；

4、尽可能用自己的语言文字而不是实验任务书及实验平台重的操作指南文字来组织实验报 告。

**四、主要实验步骤**

**五、实验数据及分析结果**

**六、请阐述发现木马的常见方法**

**七、参考资料**

* **南昌大学《网络安全概论实验》**

**实验报告**

**---（3）古典加密及数字签名**

学生姓名： 学 号： 专业班级：

实验类型：■ 验证 □ 综合 □ 设计 □ 创新 实验日期： 实验成绩：

**一、实验目的**

学习古典加密技术和数字签名技术的原理和方法，使用DSAToolv13.exe工具对一段信息进行 加密和解密，了解DSA算法的原理。

**二、实验内容**

1、使用DSAToolv13.exe工具对一段信息进行加密和解密，了解DSA算法的原理。

2、编程实现仿射密码。

**三、实验要求**

1. 根据实验任务书的具体任务要求完成实验；
2. 独立完成实验并形成实验报告；
3. 实验报告侧重实验步骤、实验数据及分析、第六部分问题回答三部分内容；

4、尽可能用自己的语言文字而不是实验任务书及实验平台重的操作指南文字来组织实验报 告。

**四、主要实验步骤**

**五、实验数据及分析结果**

**六、请阐述仿射密码的局限性**

**七、参考资料**

* **南昌大学《网络安全概论实验》**

**实验报告**

**---（4）对称加密算法DES**

学生姓名： 学 号： 专业班级：

实验类型：■ 验证 □ 综合 □ 设计 □ 创新 实验日期： 实验成绩：

**一、实验目的**

通过编程实现DES算法，对实际的数据进行加密和解密来深刻理解DES的工作原理。

**二、实验内容**

使用DES工具对一段信息进行加密和解密，了解DES算法的原理。

**三、实验要求**

1. 根据实验任务书的具体任务要求完成实验；
2. 独立完成实验并形成实验报告；
3. 实验报告侧重实验步骤、实验数据及分析、第六部分问题回答三部分内容；

4、尽可能用自己的语言文字而不是实验任务书及实验平台重的操作指南文字来组织实验报 告。

**四、主要实验步骤**

**五、实验数据及分析结果**

**六、请简单分析下双重DES的密码强度及其安全性**

**七、参考资料**

* **南昌大学《网络安全概论实验》**

**实验报告**

**---（5）非对称加密算法RSA**

学生姓名： 学 号： 专业班级：

实验类型：■ 验证 □ 综合 □ 设计 □ 创新 实验日期： 实验成绩：

**一、实验目的**

通过编程实现RSA算法，对实际的数据进行加密和解密来深刻理解RSA的工作原理。

**二、实验内容**

通过使用RSATOOL工具软件，对信息实现非对称加解密，验证RSA标准，理解RSA算法的原 理和方法。

**三、实验要求**

1. 根据实验任务书的具体任务要求完成实验；
2. 独立完成实验并形成实验报告；
3. 实验报告侧重实验步骤、实验数据及分析、第六部分问题回答三部分内容；

4、尽可能用自己的语言文字而不是实验任务书及实验平台重的操作指南文字来组织实验报 告。

**四、主要实验步骤**

**五、实验数据及分析结果**

**六、请阐述非对称加密和对称加密各自的优缺点及应用场景**

**七、参考资料**

* **南昌大学《网络安全概论实验》**

**实验报告**

**---（6）Hash算法及数字签名**

学生姓名： 学 号： 专业班级：

实验类型：■ 验证 □ 综合 □ 设计 □ 创新 实验日期： 实验成绩：

**一、实验目的**

HASH函数是将任意长的串变成较短的定长串的函数，结果为HASH值。MD5是主要 的哈希函数算法之一，是计算消息摘要的标准之一。MD5单向散列函数对任意输入 值处理后产生128位的输出值。

通过实验实例了解RSA算法数字签名

**二、实验内容**

1、根据给出的MD5算法，编写C代码源程序实现，使用MD5对一段信息产生信息 摘要。通过实验更深入、透彻地理解MD5算法的基本原理。

2、完成一次数字签名

**三、实验要求**

1. 根据实验任务书的具体任务要求完成实验；
2. 独立完成实验并形成实验报告；
3. 实验报告侧重实验步骤、实验数据及分析、第六部分问题回答三部分内容；

4、尽可能用自己的语言文字而不是实验任务书及实验平台重的操作指南文字来组织实验报 告。

**四、主要实验步骤**

**五、实验数据及分析结果**

**六、简述HASH运算在区块链（比特币）中的作用**

**七、参考资料**

* **南昌大学《网络安全概论实验》**

**实验报告**

**---（7）Linux文件管理**

学生姓名： 学 号： 专业班级：

实验类型：■ 验证 □ 综合 □ 设计 □ 创新 实验日期： 实验成绩：

**一、实验目的**

1、了解并使用命令：chmod

2、了解并使用命令：unmask

3、了解并使用命令：chown

**二、实验内容**

1、了解使用chmod按照要求更改用户对于特定文件的权限

2、使用unmask命令更改默认权限

3、使用chown命令更改文件的属主、属组

**三、实验要求**

1. 根据实验任务书的具体任务要求完成实验；
2. 独立完成实验并形成实验报告；
3. 实验报告侧重实验步骤、实验数据及分析、实验体会及改进三部分内容；

4、尽可能用自己的语言文字而不是实验任务书及实验平台重的操作指南文字来组织实验报 告。

**四、主要实验步骤**

**五、实验数据及分析结果**

**六、实验体会或对改进实验的建议**

**七、参考资料**

* **南昌大学《网络安全概论实验》**

**实验报告**

**---（8）防火墙及入侵检测**

学生姓名： 学 号： 专业班级：

实验类型：■ 验证 □ 综合 □ 设计 □ 创新 实验日期： 实验成绩：

**一、实验目的**

通过iptables命令设置简单的防火墙。

理解入侵检测的作用和原理，掌握snort入侵检测的数据包记录的方法

**二、实验内容**

学习使用iptables命令。

学习使用snort工具

**三、实验要求**

1. 根据实验任务书的具体任务要求完成实验；
2. 独立完成实验并形成实验报告；
3. 实验报告侧重实验步骤、实验数据及分析、实验体会及改进三部分内容；

4、尽可能用自己的语言文字而不是实验任务书及实验平台重的操作指南文字来组织实验报 告。

**四、主要实验步骤**

**五、实验数据及分析结果**

**六、实验体会或对改进实验的建议**

**七、参考资料**