一 、请同学们在下列（15）题目中任选一题，写成期末研究报告。

1．面向安全的网络体系结构设计

在设计TCP/IP网络协议和OSI标准通信模型的初期，网络设计者关心的问题是如何将数据从一台计算机有效和可靠的传输到另外一台计算机上去。数据的安全性在当时并没有提到议事日程。因此，TCP/IP通信协议和OSI标准通信模型没有内置的安全机制。当人们逐渐意识到这个设计缺陷之后，便想方设法在现有的框架内加入各种安全机制。但是，由于这些通信协议和通信模型不是为网络安全设计的，其体系结构也许并不适用于新的安全功能。为了从根本上纠正这一缺陷，网络设计者们开始研究如下课题：如果从头开始设计网络通信协议，使其包含现有的安全机制及在未来能有效地加入新的安全功能，网络体系结构应该怎样设计才是最好的。

2．MD5散列算法安全性分析

UNIX和Linux操作系统使用一个名为crypt(3)的常规加密算法将用户登录密码转化成一个散列值后存储在登录密码文件中。为增强安全性，crypt(3)算法后来采用MD5散列函数计算密码散列值。上网或者到图书馆查询资料，写一篇研究报告描述这个算法，并分析其安全性。

3．SSH中身份认证和加密算法使用分析

访问网页www.openssh.com并阅读SSH文件，写一篇研究报告描述SSH如何使用身份认证和加密算法的。

4．SOCKS网管协议分析

阅读RFC3098文档(http://www.ietf.org/rfc/rfc3089.txt)，写一篇研究报告描述SOCKS网管协议。

5．网页臭虫制作原理及检测方法分析

网页臭虫web bug（也成为网络信标, web beacon）是一种网页窃听器，它是安装在网页或者电子邮件汇总的一个不可见的小图像，通常只有1x1像素大小。网页臭虫的目的是收集网页访问者的资料。查询网页臭虫的相关资料，写一篇研究报告描述网页臭虫的作用、制作原理和检测方法。

6．Tor原理分析

人们一直在不断探索和研究各种匿名上网的方法，Tor就是其中一种。收集有关Tor的资料，写一篇研究报告介绍Tor的具体用途、组织结构、原理及所采用的算法。

7．Freenet原理分析

人们一直在不断探索和研究各种匿名上网的方法，Freenet就是其中一种。收集有关Freenet的资料，写一篇研究报告介绍Freenet的具体用途、组织结构、原理及所采用的算法。

8．蜜罐和沙盒原理分析

沙盒技术是一种隔离措施，它是真实的主机或操作系统。任何未经严格安全检验的程序通常放在这个系统内运行，在保证其他主机安全的同时也为研究人员提供了方便。写一篇研究报告比较蜜罐和沙盒技术，探讨它们的共同和不同之处。

9. 入侵检测日志分析

在自己的网络环境中安装IDS系统，运行一周时间，根据IDS系统日志分析有无入侵行为，写一篇研究报告描述你的分析结果。

10. 国产IDS产品功能和性能分析

查找具有代表性的国产的入侵检测系统IDS，寻找相关资料，写一篇研究报告描述一下它们的功能及性能。

11. 登陆密码大规模泄露案例分析

查找近几年国内各种网站平台泄露大量用户账号和密码信息的案例，分析导致信息泄露的原因以及如何进行预防的有效措施。

12. 基于智能手机的信息窃听方法、原理及防御措施分析

通过查找相关文献，分析和总结采用智能手机进行信息窃听的方法、原理以及对应的防御措施。

13.区块链网络安全漏洞分析

通过查找相关文献，了解区块链网络构建的方法、原理，详细分析区块链网络中可能存在的安全漏洞。

14.HTTPS协议中间人劫持原理及防御措施分析

查找相关文献，总结针对HTTPS协议的各种攻击方法，重点分析中间人劫持攻击方法及原理，以及对应的防御措施。

15.WiFi密码破解原理及防御措施分析

查找相关文献，了解WEP和WPA-PSK的加密原理，详细分析针对WEP和WPA-PSK的密码破解方法、原理及对应的防御措施。

二、研究报告写作要求

研究报告要层次清晰、论点清楚、论据准确；

研究报告写作要理论联系实际，同学们应结合课堂讲授内容，广泛收集与研究报告有关资料，含有一定案例，参考一定文献资料。

三、研究报告写作格式要求：

研究报告字数要控制在2000－2500字；研究报告一律以《计算机学报》为模板（word模板链接：http://cjc.ict.ac.cn/wltg/new/submit/index.asp），写明专业、姓名、学号等信息。

四、研究报告提交注意事项：

1、研究报告保存为word文件，以“课程名+学号+姓名”命名。

2、研究报告一律采用线上提交方式，在规定时间内上传到雨课堂，逾期平台关闭，将不接受补交。

3、不接受纸质研究报告。

4、如有抄袭雷同现象，将按学院规定严肃处理。