Computer Science and Application 计算机科学与应用, 2012, 2, 101-107
http://dx.doi.org/10.12677/csa.2012.22019 Published Online June 2012 (http://www.hanspub.org/journal/csa)

Construction and Exploration of the System Security Course Design*

Wei Li, Xiaoling Xia, Xiaohu Huang

School of Computer Science and Technology, Donghua University, Shanghai
Email: {weili, sherlysha, htiger}@dhu.edu.cn

Received: May 3rd, 2012; revised: May 21st, 2012; accepted: May 27th, 2012

Abstract: The system security course design is one of the most important components of information security courses. It is also an application-oriented practical course. This paper investigates the teaching content, discusses the teaching designing, and thus investigates the teaching constructions.

Keywords: Information Security; System Security; Teaching Research

系统安全课程设计的建设与探索*

李　玮，夏小玲，黄晓虎

东华大学计算机科学与技术学院，上海
Email: {weili, sherlysha, htiger}@dhu.edu.cn

收稿日期：2012 年 5 月 3 日；修回日期：2012 年 5 月 21 日；录用日期：2012 年 5 月 27 日

摘　要：系统安全课程设计是信息安全专业教学体系实践教学中的重要组成部分。通过结合实际教学经验，围绕课程存在的问题，以课程教学目标为中心，研讨教学内容设计，探索适合于本课程的教学建设。

关键词：信息安全；系统安全；教学

1. 引言

随着计算机及网络技术的不断发展，信息安全问题日益突出，同时，国家对于掌握信息安全理论以及具有较强实践动手能力的信息安全管理、维护和开发人员的需求量也在急剧增长[1,2]。这不仅要求从业人员不仅要具备扎实的理论水平，而且要具有一定的实际动手与解决问题的能力[3-5]。因此，信息安全人才培养是国家信息安全保障体系建设的基础和先决条件。然而，我国信息安全学科的发展与世界发达国家相比，理论研究水平与技术开发能力方面还存在较大差距[6-9]。

国外发达国家十分重视信息安全，多年来把确保信息系统安全作为国家安全战略最重要的组成部分之一[10]。美国一直将信息安全技术列为国防重点，并已形成庞大的信息安全产业，作为实现信息掌控的有效手段。美国历届政府都高度重视信息安全，制定和颁布了一系列的规划和计划，并加以实施。2009 年 5 月 29 日，奥巴马新政府公布了名为《网络空间政策评估——保障可信和强健的信息和通信基础设施》的报告，把信息安全纳入到新的社会职业中。为了适应新形势发展的需要，美国国家安全局委任斯坦福大学、麻省理工学院等多所国外知名高校成立信息安全学术人才中心用于信息安全人才培养，并把信息安全教育和人才培养列为重点。在信息安全人才培养课程体系中，除了密码学、网络安全等基础专业课之外，

*资助信息：教育部高等学校信息安全类专业教学指导委员会信息安全类专业建设和人才培养项目(编号：JZW201013)，中国密码学会教育工作委员会 2012 年密码类教育教学改革项目(编号：CACR2012E06)，上海市高等教育学会课题，东华大学计算机科学与技术学院教改项目。

还设置了提高学生实践动手能力的实践课程，例如，系统安全课程设计等，用于培养培养学生具有良好的科学素养，系统地掌握系统安全技术的基础理论与方法，使学生对计算机系统各层次可能存在的安全问题和普遍采用的安全机制有较全面的了解，并具备一定的实际操作和计算机系统安全管理的实践能力。

2. 课程介绍

在信息社会中，系统是信息的载体，是直接面对用户的服务系统。用户通过系统得到信息的服务，感知到信息的安全与否。系统安全的特点是从系统级的整体上考虑安全威胁与防护。它研究系统的安全威胁、系统安全的理论与模型、系统安全技术和应用。因此，系统安全课程设计是一门融合密码学、计算机硬件与环境安全、操作系统安全、网络安全、数据库安全、应用系统安全、应急相应与灾难恢复、计算机系统安全风险评估以及计算机系统安全管理等诸多知识点的长期知识积累和最新发展成果，同时涉及社会问题和法律问题综合性课程。上海交通大学、武汉大学等信息安全专业的教学情况表明，系统安全课程设计涵盖内容广泛，技术和方法更新速度迅速，对于学习的预备知识要求较高，前导专业课程多、实践性强，但实验缺乏系统性，存在破坏性。

在实践中，我们发现，系统安全课程设计的教学容易出现如下误区：

- **“多演示，少设计”**，教学方式已经落后时代的最新发展，导致学生丧失了学习的主动性，积极性难以被激发。
- **“多攻击，少防御”**，学生的技术方向分化情况较严重，从而偏离了课程的原本教学目的，难以帮助学生树立正确的系统安全意识。
- **“多传授，少交流”**，师生之间缺乏进行自由的交流平台，学生遇到的问题不能及时有效地得到解决。

因此，我们对系统安全课程设计的教学内容和实践平台进行规划和优化建设，希望通过本课程的建设，做到教学内容精于教材内容，理论与实践相结合，融会贯通掌握所学的理论知识，从而进一步提高教学质量，激发学生对知识的兴趣与求知欲，有效培养学生创新能力、分析和解决问题的能力，使学生毕业以后能在系统安全技术领域中有一个质的飞跃，适应国家和社会的发展需要。

3. 教学内容设计

3.1. 联系现实问题，合理安排教学

我们认为，系统安全课程设计的教学过程必须注重攻击和防御两个方面，既讲解常见的基本原理，又要融入最新的流行技术，这样学生在兴趣提高的同时，才能与教师多多交流，教学相长，从而能够准确理解知识要点，把握整体，建立正确的信息安全意识，推陈出新。根据课程教学大纲的要求，结合培养目标，根据学生的实际情况，我们在教学过程中采取“去粗取精”的原则精心设计教学内容，其教学内容的安排不仅不拘泥于知识体系的完整，而且更要具有针对性和实用性。根据知识点组成，课程讲授分为以下部分：密码学基础、计算机硬件与环境安全、操作系统安全、网络安全、数据库安全、应用系统安全、应急相应与灾难恢复、计算机系统安全风险评估以及计算机系统安全管理。同时，紧跟时代，关注各种系统安全事件及相应的安全技术。在实验教学中，我们将避免单纯地理论说教。在介绍系统漏洞时，我们联系 2011 年 3 月份 RSA 遭到黑客攻击，获取认证的 SecureID 相关信息被窃取，以及 2011 年 4 月份“索尼被黑”事件导致黑客从索尼在线 PlayStation 网络中窃取了 7700 万客户的信息这样重大的安全事件。在介绍系统漏洞的修补时，我们在专业实验室里，对没有打安全补丁的计算机进行攻击，使学生真正体会攻击的危险性和系统安全的重要性，从抽象的概念上升到形象上的认识，并结合系统安全事件的真实案例和安全的法律法规，例如“震网”病毒、以新浪微博为载体的 XSS 蠕虫的原理及传播，从而提高信息安全专业学生专业安全意识和素质。

3.2. 拓宽沟通渠道，提高教学质量

系统安全课程设计具有综合性和实践性都很强的特点，在课堂上我们充分发挥以学生为主体的引导作用。在实践内容中注意培养学生在基础教育学习阶段的创新意识，通过培养学生过程探究性、知识创新性学习，使他们具备在实际应用过程中灵活重组所学知识的能力。我们在实践教学中利用校园网，校内 FTP 服务器和 Web 服务器开展讨论式、交互式教学，方便

学生下载资料、上交作业和课后的复习资料整理和答疑，同时还利用 Email 等进行师生信息交流与答疑。丰富多样的实践教学方式很好地满足了培养要求，在培养学生发现问题、分析问题和解决问题的能力方面成绩显著，提高了学生解决本专业领域问题的能力和合作共事、继续学习、自我创新的能力。同时，采用多样的课堂形式和案例，激发学生的学习兴趣和自主学习的积极性，提高学生综合应用知识的能力。通过建立课程的站点，把教学大纲、课件、实验、习题及学习资料等教学相关的材料分门别类上载至网站上，帮助学生课余自学并方便师生间的交流。这种多元化的教学形式，将有效提高了学习效率并增强学习效果。此外，对于一些实时攻击等内容，在备课时制作成教学录像，使理论知识立体化、形象化，提高学生的兴趣，鼓励学生自己把学习的过程记录下来。在此基础上，我们将重点教授网络防御的相关原理和技术，帮助学生树立正确的系统安全危机意识，提高学生的网络防御技术和技巧。

例如，在 ARP 欺骗的讲述中，通过解析 ARP 欺骗演示图(图 1)、ARP 欺骗屏幕录像(截屏如图 2)以及 ARP 欺骗实验教程(图 3)，学生对照表 1 的实验过程演示，参考 ARP 攻击源代码(图 4)，自己逐步独立完成，达到完全理解和掌握 ARP 欺骗的过程。

3.3. 结合综合实践，提升教学水平

由于系统安全实践性很强，我们在讲授这门课程不能像其它概论课程那样去“灌输”，必须抓好实验、实践教学环节，注重学生实际动手操作能力的培养和

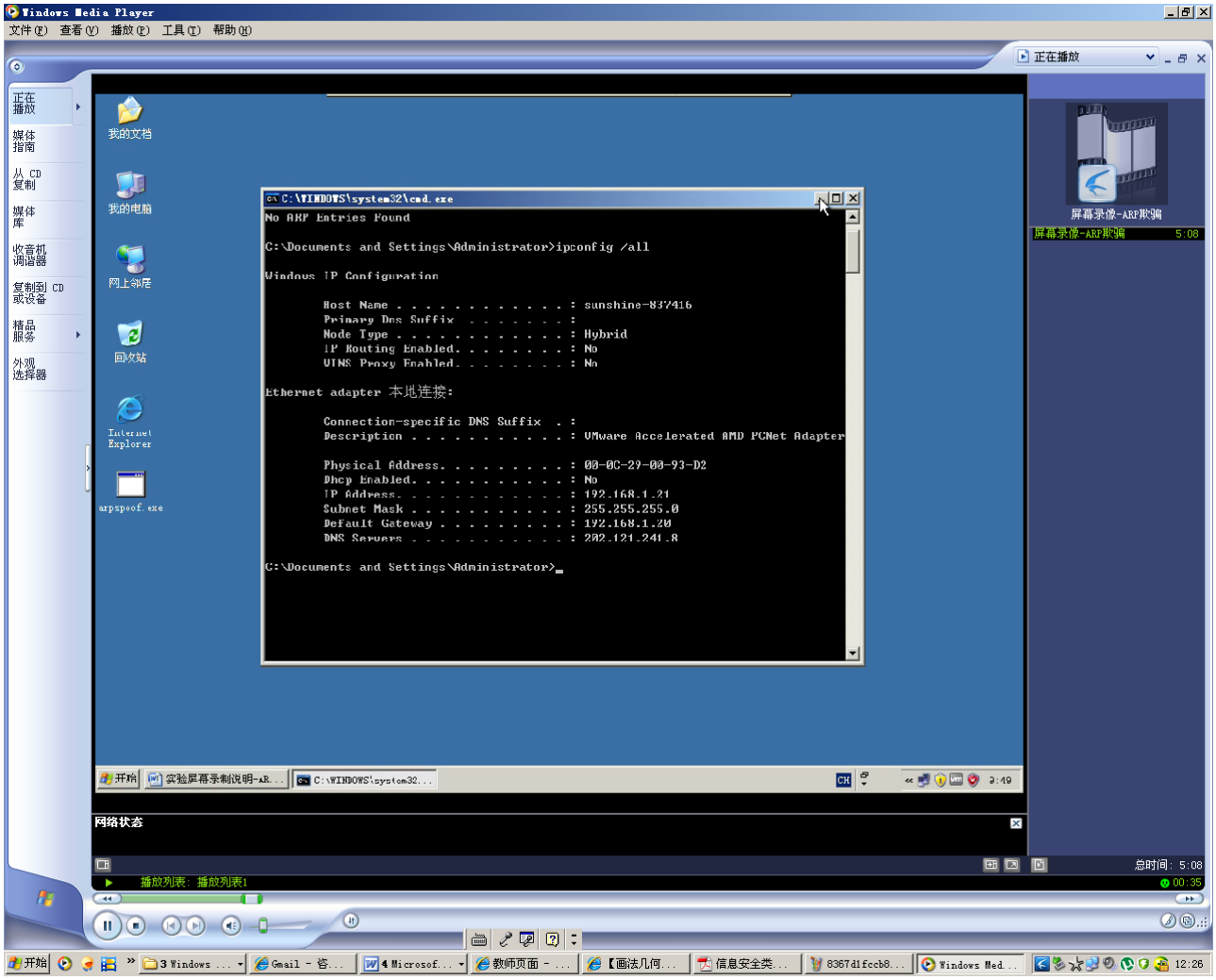


Figure 1. The demo figure of ARP spoofing
图 1. ARP 欺骗演示图

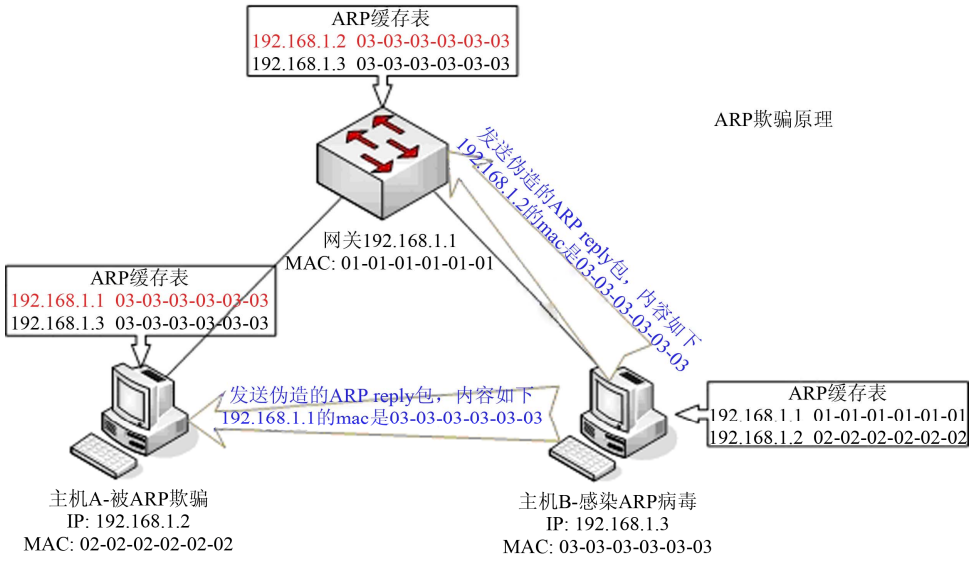


Figure 2. The screenshots of ARP spoofing screencasts
图 2. ARP 欺骗屏幕录像截屏

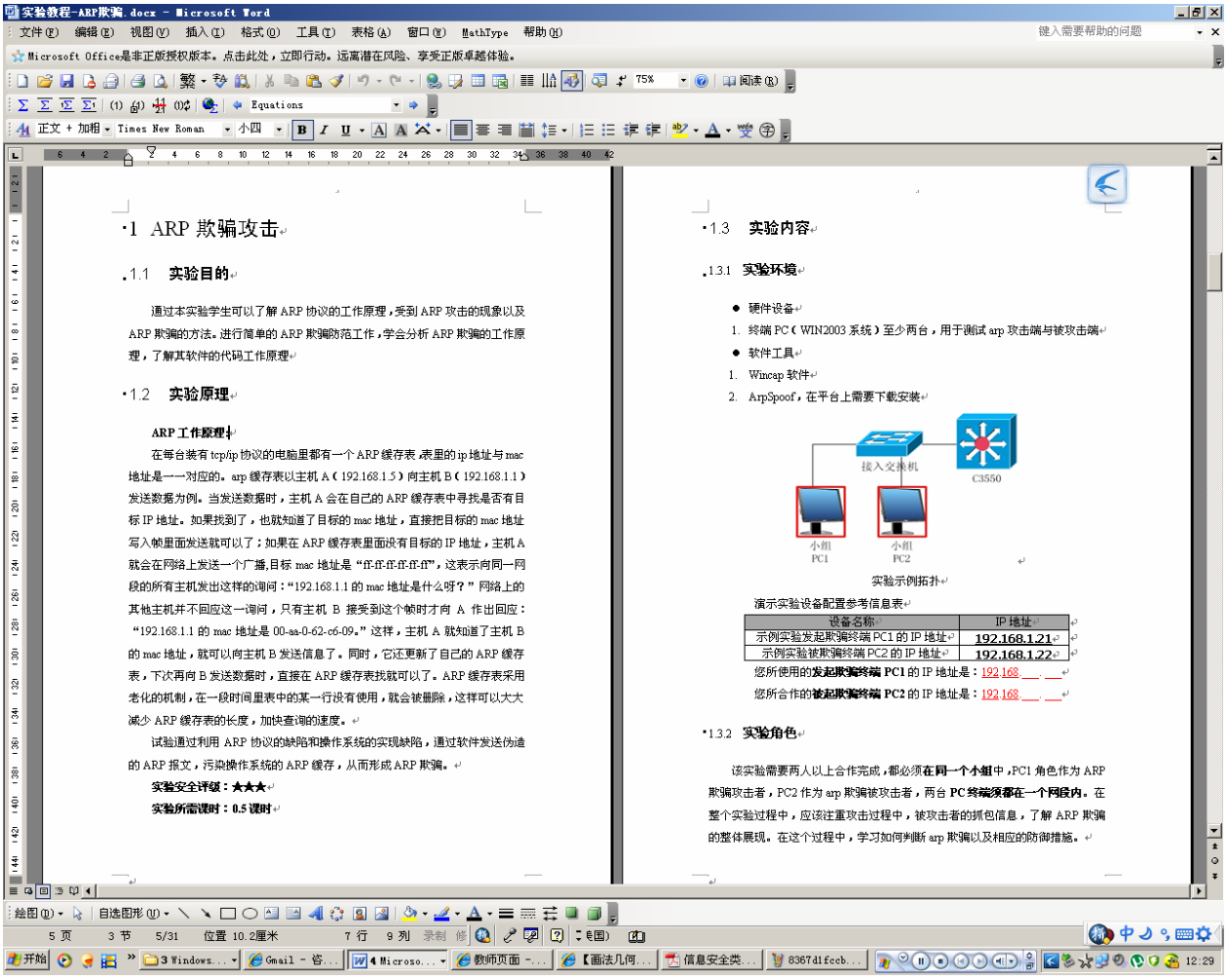


Figure 3. The experimental tutorial ARP spoofing
图 3. ARP 欺骗实验教程

Table 1. The experimental steps of ARP spoofing
表 1. ARP 欺骗实验过程演示表

(网络安全－ARP 欺骗－知识点)	
实验展示步骤：	
第一步：查看 ip 和默认网关；	□步骤完成
第二步：输入 arpspoof.exe/n 命令生成 job.txt 文档(可修改)；	□步骤完成
第三步：查看活动的网卡；	□步骤完成
第四步：进行 ARP 欺骗；	□步骤完成
第五步：打开网页，观察效果。	□步骤完成

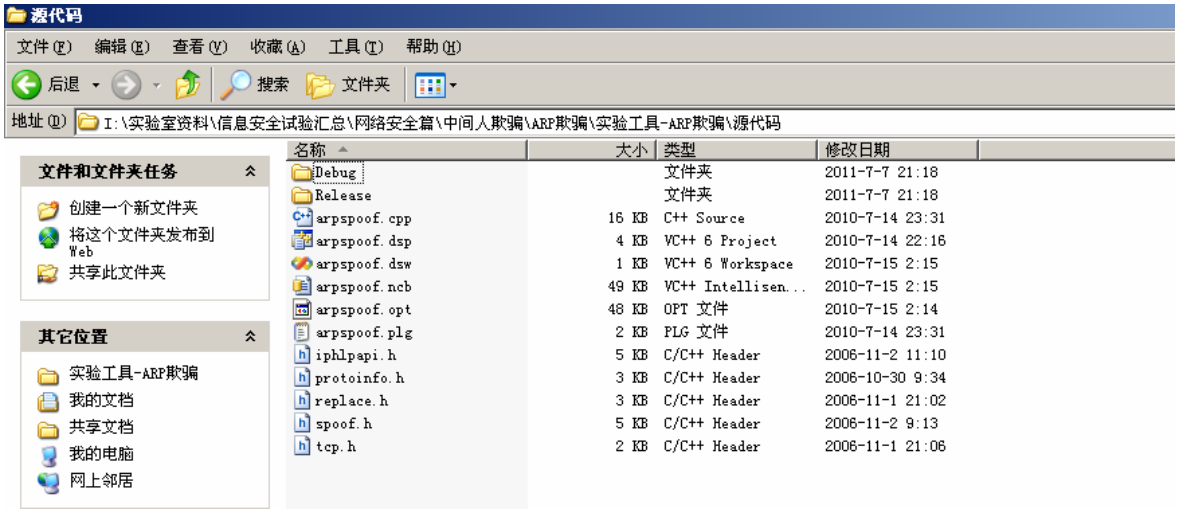


Figure 4. The source code of ARP spoofing
图 4. ARP 欺骗源代码

训练，按照认识论的观点组织和开展教学。我们针对每一理论内容设计单独的实验，也综合相关章节的内容，设计一个综合实验。由于综合实验包含了较多的实验内容和较大的工作量，我们采用分组开设实验的形式，使学生有组织、按计划完成实验。组织和计划的内容包括：确定完成的计划进度表；明确组员要完成的工作；定期组织组员讨论实验中遇到的问题，并共同确定解决方案等等。这样做可以避免学生在实验过程中的封闭性和被动性，使学生可以相互交流讨论开拓视野，提高动手动脑的兴趣，同时能锻炼组织能力、协作能力和交流能力。我们鼓励对有兴趣的学生参加丰富多彩的课外活动，掌握和深化课堂内容。这些活动主要有：鼓励学生参加全国大学生信息安全竞赛、全国普通高校信息技术创新与实践活动；与上海三零卫士信息安全有限公司共同建立了实习基地；组织学生对典型系统安全事件进行讨论分析。

例如，在“编写 SQL 注入漏洞扫描器”的大作业中(图 5)，要求学生组成团队，分工查找相关资料，进行单个和批量网站扫描、基于可维护字典的扫描以及多线程扫描，最后完成作业报告。

通过这样的大作业锻炼，学生认为受益匪浅，不仅整合了原有的零散知识点，而且锻炼了团队合作意识，提高了综合能力。图 6 和图 7 分别为一个团队中学生的分工和心得体会。

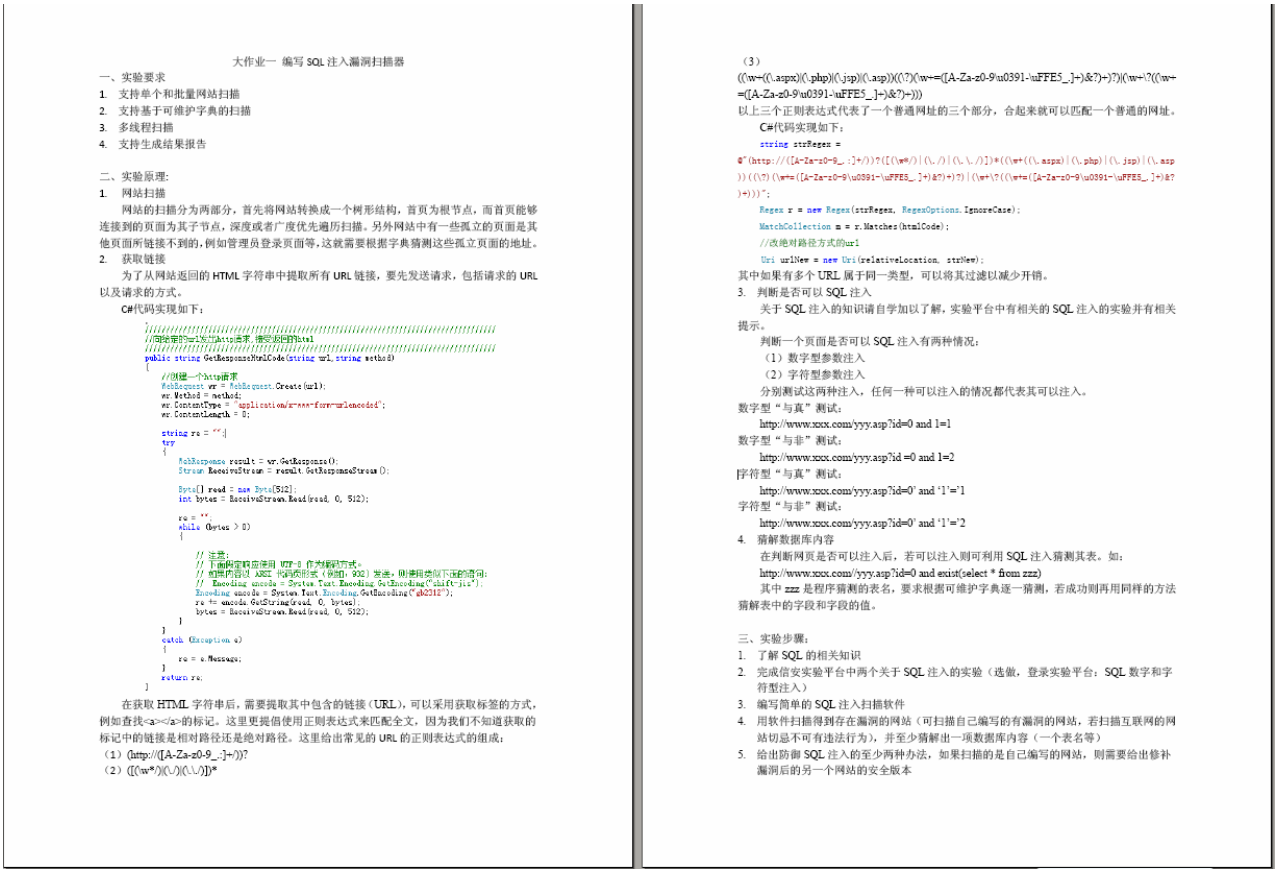
3.4. 加强创新实践，扩展学生视野

研究创新型实验要求学生综合应用多门基础课程和专业课程的知识，针对某些有创新的想法，完成设计和实现的工作，可以来源于教师的科研项目、学生的科研选题、社会实践活动和企事业单位的应用需

求等，因此内容是不断更新变化的。如轻量级密码的研究与分析、基于影音的信息隐藏的研究与应用、敏感信息过滤系统的设计、物联网安全的研讨、网格计算安全问题的研究等，这样不但提高了学生的求知欲、扩大了知识面，而且锻炼了学生的组织能力、协同合作能力和讲解能力，有效提升教学效果。此外，我们非常重视培养学生的职业岗位技能和素质，安排学生通过国家级职业资格认证培训，以适应学生未来毕业后的就业需求，使学生达到学则能用、学则会用的目的。

4. 结束语

目前，鉴于信息安全技术的发展非常迅速，我们在今后的课程教学改革中将不断提高实验教学手段、丰富教学内容，改进教学方法。在借鉴系统安全课程设计建设的基础上，我们将进一步完善信息安全专业其它课程的建设，注重培养学生的应用及创新能力，锻炼团队合作意识，提高教学质量。



大作业一 编写 SQL 注入漏洞扫描器

一、实验要求

1. 支持单个和批量网站扫描
2. 支持基于可维护字典的扫描
3. 多线程扫描
4. 支持生成结果报告

二、实验原理：

1. 网站扫描

网站的扫描分为两部分，首先将网站转换成一个树形结构，首页为根节点，而首页能够连接到的页面为其子节点，深度或者广度优先遍历扫描。另外网站中有一些孤立的页面是其他页面所链接不到的，例如管理员登录页面等，这就需要根据字典猜测这些孤立页面的地址。

2. 获取链接

为了从网站返回的 HTML 字符串中提取所有 URL 链接，要先发送请求，包括请求的 URL 以及请求的方式。

C#代码实现如下：

```
//////////////////////////////////////////////////////////////////////////////////
//向指定的url发出Http请求，得到返回的html
//////////////////////////////////////////////////////////////////////////////////
public string GetResponseHtmlCode(string url, string method)
{
    //创建一个http请求
    WebRequest wr = WebRequest.Create(url);
    wr.Method = method;
    wr.ContentType = "application/x-www-form-urlencoded";
    wr.ContentLength = 0;

    string re = "";
    try
    {
        WebResponse result = wr.GetResponse();
        Stream ReceiveStream = result.GetResponseStream();

        Byte[] read = new Byte[512];
        int bytes = ReceiveStream.Read(read, 0, 512);

        re = "";
        while (bytes > 0)
        {

            // 注意：
            // 下面两套取应使用 UTF-8 作为解码方式
            // 如果内容以 ASCII 内码页形式（例如：936）发送，则要相应下面的语句：
            //  Encoding encode = System.Text.Encoding.GetEncoding("shift-jis");
            Encoding encode = System.Text.Encoding.GetEncoding("gb2312");
            re += encode.GetString(read, 0, bytes);
            bytes = ReceiveStream.Read(read, 0, 512);
        }
    }
    catch (Exception e)
    {
        re = e.Message;
    }
    return re;
}
```

在获取 HTML 字符串后，需要提取其中包含的链接（URL），可以采用获取标签的方式，例如查找<a>的标记。这里更提倡使用正则表达式来匹配全文，因为我们不知道获取的标记中的链接是相对路径还是绝对路径。这里给出常见的 URL 的正则表达式的组成：

（1）(http://)([A-Za-z0-9_.:]+/))?

（2）([(\w*/)((\.\/)((\.\.)])*

（3）

((\w+((\.aspx)|(\.php)|(\.jsp)|(\.asp))((\?)(\w+=([A-Za-z0-9\u0391-\uFFE5_.]+)&?)+)?)|(\w+\?((\w+=([A-Za-z0-9\u0391-\uFFE5_.]+)&?)+)))

以上三个正则表达式代表了一个普通网址的三个部分，合起来就可以匹配一个普通的网址。

C#代码实现如下：

```
string strRegex =
@"(http://([A-Za-z0-9_.:]+/))?([(\w*/)|(\.\/)|(\.\.\/)])*((\w+((\.aspx)|(\.php)|(\.jsp)|(\.asp
))((\?)(\w+=([A-Za-z0-9\u0391-\uFFE5_.]+)&?)+)?)|(\w+\?((\w+=([A-Za-z0-9\u0391-\uFFE5_.]+)&?
)+)))";
Regex r = new Regex(strRegex, RegexOptions.IgnoreCase);
MatchCollection m = r.Matches(htmlCode);
//改绝对路径方式的url
Uri urlNew = new Uri(relativeLocation, strNew);
```

其中如果有多个 URL 属于同一类型，可以将其过滤以减少开销。

3. 判断是否可以 SQL 注入

关于 SQL 注入的知识请自学加以了解，实验平台中有相关的 SQL 注入的实验并有相关提示。

判断一个页面是否可以 SQL 注入有两种情况：

（1）数字型参数注入

（2）字符型参数注入

分别测试这两种注入，任何一种可以注入的情况都代表其可以注入。

数字型“与真”测试：

http://www.xxx.com/yyy.asp?id=0 and 1=1

数字型“与非”测试：

http://www.xxx.com/yyy.asp?id =0 and 1=2

字符型“与真”测试：

http://www.xxx.com/yyy.asp?id=0' and '1'='1

字符型“与非”测试：

http://www.xxx.com/yyy.asp?id=0' and '1'='2

4. 猜解数据库内容

在判断网页是否可以注入后，若可以注入则可利用 SQL 注入猜测其表。如：

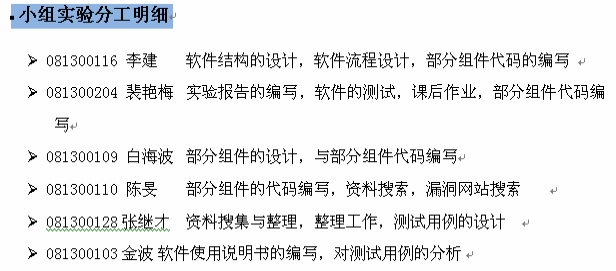
http://www.xxx.com/yyy.asp?id=0 and exist(select * from zzz)

其中 zzz 是程序猜测的表名，要求根据可维护字典逐一猜测，若成功则再用同样的方法猜解表中的字段和字段的值。

三、实验步骤：

1. 了解 SQL 的相关知识
2. 完成信安实验平台中两个关于 SQL 注入的实验（选做，登录实验平台：SQL 数字和字符型注入）
3. 编写简单的 SQL 注入扫描软件
4. 用软件扫描得到存在漏洞的网站（可扫描自己编写的有漏洞的网站，若扫描互联网的网站切忌不可有违法行为），并至少猜解出一项数据库内容（一个表名等）
5. 给出防御 SQL 注入的至少两种办法，如果扫描的是自己编写的网站，则需要给出修补漏洞后的另一个网站的安全版本

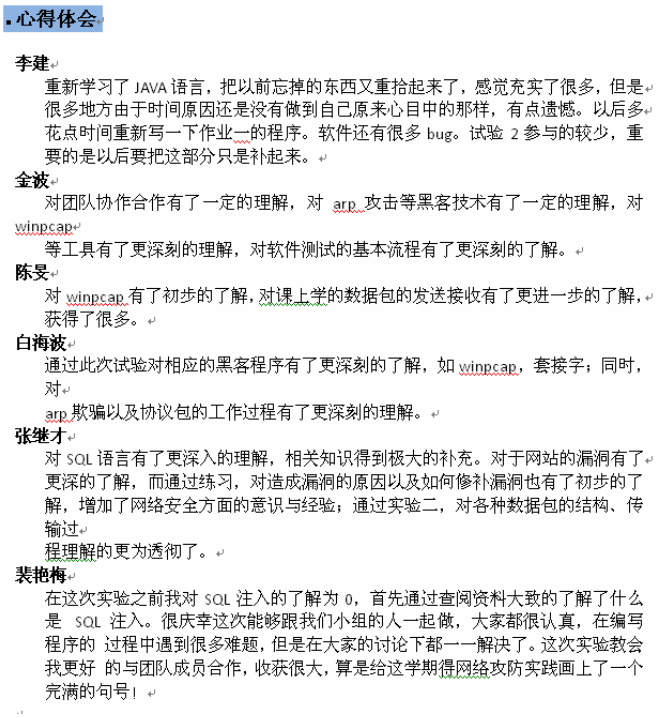
Figure 5. The principles and procedure of the scanner using SQL injection vulnerability
图 5. 大作业“编写 SQL 注入漏洞扫描器”的要求、原理及步骤



小组实验分工明细

- 081300116 李建　软件结构的设计，软件流程设计，部分组件代码的编写
- 081300204 裴艳梅　实验报告的编写，软件的测试，课后作业，部分组件代码编写
- 081300109 白海波　部分组件的设计，与部分组件代码编写
- 081300110 陈旻　部分组件的代码编写，资料搜索，漏洞网站搜索
- 081300128 张继才　资料搜集与整理，整理工作，测试用例的设计
- 081300103 金波 软件使用说明书的编写，对测试用例的分析

Figure 6. Students' groups
图 6. 学生分工


.心得体会

李建

重新学习了 JAVA 语言，把以前忘掉的东西又重拾起来了，感觉充实了很多，但是很多地方由于时间原因还是没有做到自己原来心目中的那样，有点遗憾。以后多花点时间重新写一下作业一的程序。软件还有很多 bug。试验 2 参与的较少，重要的是以后要把这部分只是补起来。

金波

对团队协作合作有了一定的理解，对 arp 攻击等黑客技术有了一定的理解，对 winpcap 等工具有了更深刻的理解，对软件测试的基本流程有了更深刻的了解。

陈旻

对 winpcap 有了初步的了解，对课上学的数据包的发送接收有了更进一步的了解，获得了很多。

白海波

通过此次试验对相应的黑客程序有了更深刻的了解，如 winpcap，套接字；同时，对 arp 欺骗以及协议包的工作过程有了更深刻的理解。

张继才

对 SQL 语言有了更深入的理解，相关知识得到极大的补充。对于网站的漏洞有了更深的了解，而通过练习，对造成漏洞的原因以及如何修补漏洞也有了初步的了解，增加了网络安全方面的意识与经验；通过实验二，对各种数据包的结构、传输过程理解的更为透彻了。

裴艳梅

在这次实验之前我对 SQL 注入的了解为 0，首先通过查阅资料大致的了解了什么是 SQL 注入。很庆幸这次能够跟我们小组的人一起做，大家都很认真，在编写程序的 过程中遇到很多难题，但是在大家的讨论下都一一解决了。这次实验教会我更好 的与团队成员合作，收获很大，算是给这学期得网络攻防实践画上了一个完满的句号！

Figure 7. Students' feelings and experiences
图 7. 学生的心得体会

5. 致谢

感谢本文审稿专家和编辑所提出的宝贵意见和建议。

参考文献 (References)

[1] 肖竞华, 陈建勋. 计算机操作系统教学改革探索与实践[J]. 高等理科教育, 2007, 4(3): 68-70.
[2] 刘承勇. 高校培养创新型人才探析[J]. 大众科技, 2008, 5(3): 101-103.
[3] 俞研, 兰少华. 计算机网络安全课程教学的探索与研究[J]. 计算机教育, 2008, 18(3): 127-128.
[4] 段立娟, 周艺华. 网络安全课程教学研究与探讨[J]. 计算机教育, 2008, 10(2): 74-75.
[5] 李建国. 高校计算机网络安全课程教学研究[J]. 淮北煤炭师范学院学报, 2009, 30(1): 94-96.
[6] 牛雅莉, 王宇飞. 高校是高素质创新型人才的培养基地[J]. 科技进步与对策, 2000, 5(10): 68-69.
[7] 王澍. 时代发展与创新教育——创新教育研究综述[J]. 现代教育科学, 2009, 7(6): 99-101.
[8] 许义文. 高校素质教育重在创新教育[J]. 西南交通大学学报(社会科学版), 2008, 6(12): 63-64.
[9] 杨玉荣. 关于创新型研究人才培养模式、教学内容与课程体系改革的思考[J]. 科技创新导报, 2009, 30(1): 23-25.
[10] 王越. 信息、信息安全与中国特色的信息安全技术体系[J]. 科技导报, 2009, 6(4): 34-35.

