普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

网络安全实验教程

Wangluo Anquan
Shiyan Jiaocheng

崔宝江　李宝林　编著

北京邮电大学出版社
www.buptpress.com

网络安全实验教程

Wangluo Anquan
Shiyan Jiaocheng

普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

网络安全实验教程

崔宝江　李宝林　编著

北京邮电大学出版社
·北京·

内 容 简 介

本书以解决和分析具体网络安全问题为目的，按照由浅入深、由攻击到防守的思路，全面介绍了网络安全领域的实用技术。全书共分 4 章，第 1 章首先介绍网络探测技术，第 2 章和第 3 章介绍了基于网络的攻防技术以及基于主机的攻防技术，第 4 章较为系统的介绍了网络安全防御的多种技术。读者可在前面对攻击技术了解的基础上，通过和网络安全防御技术的一一对应，全面掌握网络攻击的防范手段和技术。

本书适合作为计算机类、网络类和信息安全类相关专业本科生的专业教材。同时，由于包含了极为丰富的网络维护和网络安全实用技术，也适合企、事业单位的网络和系统管理，网络维护人员和其他相关技术人员作为常用的技术工具书。

图书在版编目(CIP)数据

网络安全实验教程/崔宝江，李宝林编著. —北京：北京邮电大学出版社，2008

ISBN 978-7-5635-1574-5

Ⅰ. 网… Ⅱ. ①崔…②李… Ⅲ. 计算机网络—安全技术—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 114191 号

书　　名：网络安全实验教程
作　　者：崔宝江　李宝林
责任编辑：崔　珞
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京源海印刷有限责任公司
开　　本：787 mm×960 mm　1/16
印　　张：15.75
字　　数：341 千字
印　　数：1—3 000 册
版　　次：2008 年 9 月第 1 版　2008 年 9 月第 1 次印刷

ISBN 978-7-5635-1574-5　　定　价：26.00 元

信息安全专业系列教材（第2版）

编 委 会

第 2 版总序

发展 21 世纪中国信息安全要靠教育，而搞好信息安全教育就需要好的教材。2004 年，灵创团队北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材，该套教材被教育部列入了“普通高等教育‘十五’国家级规划教材”。至今，三年多的时间过去了，这套教材在信息安全专业的教学中发挥了重要的作用，起到了较好的教学效果，受到教师和学生的好评。

在这三年中，我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设和校企就业（创业）平台建设等在内的信息安全本科专业的全面建设。2005 年，作为组长单位我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题；召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”。我们完成的国内第一次制定的信息安全专业规范，从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系；由通识教育内容、专业教育内容和综合教育内容三大部分，构建课程参考体系；采用顶层设计的方法构建了带有实践性环节的教学体系。我们在国内第一次较全面地提出信息安全学科专业教学改革与创新的研究以及发展思路和政策建议；这些成果已提交教育部相关教学指导委员会，对于引导高等学校信息安全学科专业教学改革与建设，指导信息安全学科专业评估，促进信息安全学科专业教学规范建设与管理，提高专业教育质量和水平起到了重要的作用。多所举办信息安全专业的高校都参照该课题成果调整了自己的教学计划、课程体系和实验方案。

我们积极搭建信息安全专业校际交流平台，组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”和“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。在四川绵阳建设了占地 40 亩的全国信息安全专业本科生实习实训基地，接受了来自全国近 30 所高校的本科生进入该基地参加丰富多彩的实训。

我们努力建设精品课程，主办了“全国高校信息安全专业精品课程建设经验交流会议”，来自全国各地高校的专家齐聚北京邮电大学，介绍了精品课程建设的经验。我们组织建设了全国第一批信息安全实验室，并且编写出版了实验教材《信息安全实验指导》，我们的《现代密码学》课程已经被评为北京市精品课程，并在 2007 年度被评为“国家精品课程”。

经过灵创团队全体人员的共同努力，北京邮电大学信息安全本科专业被教育部评为

第二类优势特色专业。

三年多的时间过去了，无论信息安全的教育和产业都取得了丰硕的成果，随着信息安全向更高层次的发展，其趋势已经从基础的网络层建设开始向内容层建设过渡。为适应信息安全教育的发展需要，积极探索培养创新型高素质人才，我们按照制定的学科发展战略和专业规范的精神，结合近几年的教学实践，我们对这套信息安全专业本科系列教材进行了全面修订，并及时成立了灵创团队北京邮电大学数字内容研究中心。这次修订不仅对原来的系列教材在第 1 版的基础上进行修改和完善，还补充了信息安全最新的研究成果，使教材的内容更加翔实和新颖。同时，在原有的教材上又增加了一些新的课程教材，在新修订的系列教材中，目前有《信息安全概论》(第 2 版)、《现代密码学及其应用》、《网络安全》(第 2 版)、《信息安全管理》、《计算机病毒原理及防治》(第 2 版)、《数字版权管理》、《计算机系统安全》、《网络安全实验教程》、《信息安全专业科技英语》、《防火墙、入侵检测与 VPN》、《对称密码学及其应用》、《信息安全导论》、《数字图像取证技术》等 13 本教材，今后随着信息安全专业教学的需要，还将不断地有新的教材补充到这个系列中来，使之更加完善和系统。目前，计划列入的相关教材还有：《入侵检测》(第 2 版)、《信息内容安全》、《信息安全工程》、《软件安全》及《信息安全标准与法律法规》等。

我们组织了强大的师资队伍，广泛吸收了有着丰富教学科研经验并多次讲授该系列教材的教师充实到这次修订工作中。作者队伍中不但包括北京邮电大学的教师，还包括哈尔滨工程大学、北京交通大学等重点院校的教师。经过反复研讨，本着理论与实际相结合的原则，对原来的系列教材进行了较大的修改和扩充，我们希望这套新修订的系列教材能够满足国内各类高校信息安全本科专业以及相关方向专业的不同需求。

这次修订我们对内容进行了精心的组织和安排，希望能促进信息安全课程的建设，涌现出更多的信息安全精品课程。虽然我们在这次修订中投入了很大精力，但是由于水平有限，时间仓促，且信息安全专业的发展速度非常快，书中的不足之处和错误在所难免，我们衷心期望使用和关心该系列教材的师生，继续对新的系列教材提出宝贵的意见和建议。

本套系列教材也是国家重点基础研究发展计划(973)(课题编号：2007CB310704 和 2007CB311203)资助的成果，并被教育部增补为“普通高等教育‘十一五’国家级规划教材”的选题。

在本系列教材的修订过程中，得到了北京邮电大学出版社的大力支持，同时也得到了灵创团队的骨干机构(北京邮电大学信息安全中心和北京邮电大学数字内容研究中心)三百余位成员的支持与配合，在此一并表示感谢。

教授、博导、长江学者特聘教授

杨义先

2007 年 7 月

前　言

随着互联网技术的普及和下一代网络技术的逐渐应用，网络对经济的推动作用日益突出。越来越多的企、事业单位和用户成为互联网的受益者，互联网也越来越成为相互沟通和信息传递的主要手段。随着网络在日常生活和经济社会中发挥的作用日趋重要，针对网络的威胁和攻击也愈演愈烈，网络安全问题成为严重影响网络经济健康发展的一个重要因素。在经济利益和追求名誉的驱动下，漏洞利用、网站入侵、盗号木马等技术不断提升，也滋生了以此为营利手段的新的地下产业链，从而不断推进对网络的安全威胁。

为了提高网络的安全性，维护众多企、事业单位和网络用户的权益，上到国家下到企、事业单位都非常重视，投入了众多的人力、物力和财力，研究开发了大量网络安全防御软硬件产品，以期保护脆弱的网络不受威胁和攻击。这些网络安全产品在一定程度上提高了网络安全防范的能力，使攻击者成功攻击的难度越来越大，对提高企、事业单位和计算机用户的网络安全水平起到了促进作用。

虽然网络安全产品给我们提供了安全防范的手段，但由于各单位受到各自在财力和人力方面的限制，或者无法使用较多的网络安全产品，或者人员的技术水平难以达到相应水平，使当前的网络安全问题仍然比较突出。这点在众多个人网络用户方面尤其突出，他们在安全防范方面的意识和技术都更显薄弱。

作者在网络攻防方面从事了多年的教学、科研和社会培训工作，深感这个问题非常突出。由于网络安全涉及的技术层面较多较广，非专业的网络维护和网络管理人员一般难以全面把握网络攻击的原理和网络防范的措施，造成计算机经常中毒，内网中病毒、木马横行，而又感觉没有很有效的手段。针对国内网络安全水平有待提高的这种现状，本书的目的在于全面系统的介绍网络攻防的技术和原理，以期为网络维护管理人员、计算机网络用户、网络及安全相关专业的学生等用户，在学习和掌握网络安全原理和防范技术方面，搭建起一个桥梁。通过这个桥梁，使网络用户能够深入到网络安全的广阔知识领域，全面掌握其原理后做到有效合理的部署和使用网络安全防御技术，提高网络安全的防范水平。

本书共包括 4 章，各章节内容的组织是按照从攻击到防守的思路。正如医生下药前先要了解由哪种病菌造成的感染一样，要做到有效的防范，首先要了解攻击的手段。为

此，第 1 章首先介绍网络探测技术，这也是攻击者在攻击前必要的前期活动，以了解目标网络的情况，为入侵做准备。第 2 章和第 3 章介绍了基于网络的攻防技术以及基于主机的攻防技术，这是攻击者攻击时真正发挥实效以达到其目的的技术。在前 3 章的内容中，每个实验除了介绍攻击技术的原理外，针对每种攻击技术都对应介绍了其防范措施，使读者对每种手段可实现行之有效的防范。第 4 章较为系统的介绍了网络安全防御的多种技术，读者可在前面对攻击技术了解的基础上，通过和网络安全防御技术的一一对应，全面掌握网络攻击的防范手段和技术。

在各个实验的设计上，本书综合考虑了网络安全的各个领域，试图从多方位囊括网络安全的主要知识点。本书从实践教学的角度，通过网络安全实验的形式使读者在动手过程中了解网络攻防的原理和技术，并在实验的操作和实施过程中提高实际动手能力。这种实践动手能力的培养和提高，才是网络用户应对网络各种威胁时所必须和急缺的。同时，本书的另一个目的，是希望读者能逐渐培养并形成自己独立分析解决问题的一整套思路，建立了这套思路后，当遇到新出现的网络威胁时，读者不会手忙脚乱，会按照这套分析解决问题的思路去分析应对这种新威胁。

本书涉及到的内容主要集中在初级和中等水平的层面，以期通过这本深入浅出的教材，使读者能较快地了解掌握网络安全方面的知识。为了不断提高读者在网络安全方面的能力和水平，我们后续将陆续出版内容更加深入的高级实验教材，为高层次读者提供更加深入的技术，应对当前技术水平日趋提高的网络威胁。

本书由北京邮电大学信息安全中心和公安部公共信息网络安全监察局的专家学者共同组织编写。其中，第 1、2、3 章由崔宝江编写，第 4 章由崔宝江和李宝林共同编写，全书由崔宝江策划。参与本书编写的人员还有范文庆、黄玮、赵鑫、王欣、胡楠、刘昕、周彬彬、安靖、陈鑫、钟金鑫、张艾俐、马玉会等网络攻防组的成员。本书在编写过程中得到了杨义先、钮心忻、罗群、徐国爱和周淑萍的鼎力支持，在此对他们的工作表示衷心的感谢。

需要声明的是，本书的目的是希望帮助读者全面了解网络安全方面的基本技术，以期建立起安全方面的防范意识，绝不是为怀有不良动机的人提供支持，也不承担因为技术被滥用而产生的连带责任。

本书编写过程中参考了互联网上公布的相关资料，由于互联网上的资料较多，引用复杂，无法一一注明原出处，故在此声明，原文版权属于原作者。

由于作者水平有限，书中难免有疏漏之处，希望读者多多批评指正，以期再版修订。

作　者

目　　录

第 1 章　网络探测及其防范

实验 1-1　互联网信息搜索和 DNS 服务攻击与防范 …… 1
实验 1-2　网络服务和端口的扫描 …… 7
实验 1-3　综合漏洞扫描和探测 …… 24
实验 1-4　协议分析和网络嗅探 …… 38

第 2 章　基于网络的攻防技术

实验 2-1　诱骗性攻击与防范 …… 53
实验 2-2　DoS/DDoS 攻击与防范 …… 61
实验 2-3　欺骗攻击技术——ARP 欺骗与防范 …… 71
实验 2-4　木马攻击与防范 …… 81
实验 2-5　熊猫烧香病毒的查杀 …… 94

第 3 章　基于主机的攻防技术

实验 3-1　口令的破解截获与防范 …… 107
实验 3-2　系统安全漏洞的攻击与防范 …… 120

第 4 章　网络系统的安全防御技术

实验 4-1　防火墙 …… 136
实验 4-2　入侵检测系统与入侵防御系统 …… 154
实验 4-3　虚拟专用网 …… 170
实验 4-4　PKI 系统 …… 190
实验 4-5　SSH、SSL 的加密 …… 208
实验 4-6　无线网络加密 …… 227

参考文献 …… 241

第1章

网络探测及其防范

对于网络攻防技术而言，发起网络攻击的第一步，就是进行网络探测，以获取目标网络和主机的外围关键信息，为下一步入侵做好准备。在本章中，从4个方面介绍了攻击者常用的网络探测技术和防范措施，以使读者了解其原理，并掌握其防范手段。它们包括互联网信息搜索和DNS服务的攻防、网络服务和端口的扫描、综合漏洞扫描和探测、协议分析和网络嗅探。针对网络探测的有效防范手段有两个：一是尽可能限制对外提供的网络服务，限制对外发布内部信息；二是采用防火墙、加密等防护手段，避免在网络中暴露过多的网络服务和数据信息。

实验1-1　互联网信息搜索和DNS服务攻击与防范

一、实验目的

通过对Whois和Google Hack的使用，使读者理解和掌握利用网络搜索敏感信息；通过学习DNS服务攻击原理的了解，更深刻的理解DNS服务攻击和防护。

二、实验原理

1. Whois

Whois是因特网上提供的一种查找个人电话号码、E-mail信箱、常用的邮箱、相关域名等信息的一种服务。提供这种服务的机构首推InterNIC（Internet Network Information Center），即因特网的网络信息服务中心。InterNIC是负责因特网的域名注册和维护工作的，它把那些到中心来进行域名注册的网络管理人员和技术负责人的信息，如他们的电话号

码、E-mail 信箱、常用的邮箱、IP 地址等组织成一个大数据库，并提供相应的查询服务。这就是 InterNIC 的 Whois 服务。InterNIC 的这个数据库首先是集中的，后来按不同的地区进行了划分，分成了拉美地区、欧洲地区、亚太地区等。查询时，也应按不同地区进行查询。

中国互联网络信息中心(China Internet Network Information Center，CNNIC)是经我国国务院主管部门批准授权，行使我国国家互联网络信息中心职责的管理和服务机构。作为我国的域名体系注册管理机构，CNNIC 也提供了所辖范围内域名信息查询的 Whois 服务。

2. Google Hack

随着搜索引擎的不断发展，利用搜索引擎可以轻松查到各种信息。但是过于强大的搜索机器人有时会把保密信息也提交给数据库保存，从而暴露个人秘密信息。Google Hack 就是一个搜索敏感信息的工具。例如利用一些简单的语法就能搜索到一些重要的密码文件。

Google Hack 的实现很简单；当然，想要得到比较敏感的信息，就需要了解关于搜索引擎的基础知识。下面是 Google 的一些常用的语法：

① Intitle：搜索网页标题中是否有所要找的字符。例如，搜索“intitle：login”，将返回所有网页标题中包含“login”的网页。注意搜索不包括中文引号，且语法中的标点都为英文标点，否则 Google 会把语法一起当作关键字搜索。

② Allintitle：和上面的类似，搜索所有关键字构成标题的网页。

③ Intext：它是把网页正文内容中的某个字符作为搜索条件(也就是忽略了标题、URL 等的文字)。例如，在 Google 里输入“intext：信息”，将返回在网页正文部分包含“信息”的所有网页。

④ Allintext：使用方法和 Allintitle 类似。

⑤ Inurl：搜索 URL 中含有检索单词的 URL 链接。例如，输入“inurl：admin”，将返回多个类似于这样的连接 http：//www. xxx. com/xxx/admin。

⑥ Allinurl：也同 Inurl 类似，可指定多个检索关键词。例如，“allinurl：etc/passwd”会查找 URL 中包含“etc”和“passwd”的页面，单词之间的“/”会被 Google 忽略掉。

⑦ Cache：将显示在 Google cache 中的网页。例如，“cache：www. hackingspirits. com”会列出 Google cache 中 hackingspirits 的主页。注意“cache：”和网页 URL 之间不应有空格。如果查询串中包含其他词，Google 会在 cache 的文档中高亮显示这些词。例如，“cache：www. hackingspirits. com admin”会显示在 cache 中的网页内容，并高亮显示“admin”。

⑧ Define：搜索某个词语的定义，搜索：“define：calculator”，将返回关于 calculator 的定义。

⑨ Filetype：无论是撒网式攻击还是后面要说的对某一特定目标进行信息收集都需要用到这个语法。搜索指定类型的文件，例如，“filetype：txt site：gov confidential”将在所有政府域相关的网站中查找页面中或. txt 文件中包含关键词“confidential”的扩展名为. txt 的文件。也就是结果会包含所有政府网站中有 confidential 关键词的文档的链接。当然

如果找. bak、. mdb 或. inc 也是可以的，获得的信息也许会更丰富。

⑩ Info：用来显示与某链接相关的一系列搜索，提供这个链接的 cache、link、related 信息，以及完全包含该链接的网页。注意，这里搜索的结果取决于 Google 是否对该 URL 进行了索引。如果没有的话，搜索结果将会少很多。

⑪ Link：例如搜索“link：www. baidu. com”，可以返回所有和 www. baidu. com 做连接的 URL。

⑫ Related：用来搜索结构内容方面相似的网页，比如搜索“related：google. com”会得到很多类似于 Google 的网站，如 Yahoo!、AltaVista、MSN. com 等。

⑬ Site：将限制 Google 只在特定的站点或域中检索关键词。例如，“exploits site：hackingspirits. com”（不包括引号）将在所有“hackingspirits. com”域的链接页面中查找关键词 “exploits”。“site：”和“hackingspirits. com”之间不应有空格。

下面介绍相关的一些操作符：

＋　对“＋”号后面的字符进行精确查找；

－　逻辑非，可把某个关键字忽略掉，比如“A－B”表示包含 A 但不包含 B 的网页；

|　逻辑与操作；

.　单一的通配符；

*　通配符，可代表多个字母；

""　精确查询，用短语作关键词时，可加上引号，以免被当作与操作。

对于 Google Hack，简单的防范措施是将自己敏感网页信息让 Google 不检索，可以通过访问 URL：http：//www. google. com/remove. html，在这个 Google 网站上把自己站点或网页的信息删除掉即可。

3. DNS 服务攻击原理

DNS(Domain Name System)即域名系统，是一种分布式的、层次型的、客户机/服务器式的数据库管理系统。它实现了将域名翻译为 IP 地址的功能。因为 IP 地址不容易被记住，人们习惯记忆简单的域名；但计算机互相通信只能识别 IP 地址，因此需要把域名和 IP 一一对应并转换。域名解析需要专门的域名解析服务器来进行，整个过程是通过 DNS 系统自动完成的。

域名解析的工作原理及其步骤是：

第 1 步：用户提出域名解析请求，并将该域名发送给本地的 DNS 域名服务器。

第 2 步：当本地的 DNS 域名服务器收到请求后，就先查询本地的缓存，如果有该域名对应的 IP 地址，则本地的 DNS 域名服务器就直接把查询的结果返回给用户。

第 3 步：如果本地的缓存中没有该记录，则本地 DNS 域名服务器就直接把请求发给根 DNS 域名服务器，然后根 DNS 域名服务器再返回给本地 DNS 域名服务器一个所查询域（根的子域，如 CN）的主域名服务器的 IP 地址。

第 4 步：本地服务器再向上一步骤中所返回的主域名 DNS 服务器发送请求，收到该请求的主域名 DNS 服务器查询其缓存，返回与此请求所对应的记录或相关的下级域名服

务器 IP 地址。本地域名服务器将返回的结果保存到缓存。

第 5 步:重复第 4 步,直到找到正确的记录。

第 6 步:本地域名服务器把返回的结果保存到缓存,以备下一次使用,同时还将结果返回给客户机。

在域名解析过程中,如果提交给某个域名服务器的域名解析请求数据包被截获,然后将一个虚假的 IP 地址作为应答信息返回给请求者。这时,用户就会连接这个假的 IP 地址,从而使用户被欺骗,这就是 DNS 服务攻击的基本原理。

DNS 服务攻击看似简单,但是实现起来有一定难度的。因为在构造虚假应答信息时,服务器也同时会给出应答信息,因此虚假的应答信息和真实的应答消息产生冲突。当真实的服务器给出的应答信息比虚假信息先到时,则 DNS 服务攻击不会成功。此外,在 DNS 查询包中有一个重要的字段叫查询 ID(Query IDentifier),它用来表示查询包的顺序号,一般由发出 DNS 请求的计算机在其请求数据包中设置,DNS 服务器返回的响应数据包中将此值加 1 后返回,用于匹配请求响应。如果查询 ID 不匹配,DNS 服务攻击也不会成功。因此,要想使服务攻击成功,就必须获得正确的查询 ID。一般是通过在局域网安装嗅探器(Sniffer)嗅探得到这个 ID。

防范 DNS 服务攻击可采用以下两种办法:(1)直接用 IP 访问重要的服务器,这样至少可以避开 DNS 欺骗攻击。但这需要记住要访问的 IP 地址。(2)加密所有对外的数据流,对服务器来说就是使用 SSH 等加密协议,对一般用户应该用 PGP 等软件加密所有发到网络上的数据。

三、实验环境

局域网内的两台运行 Windows 的计算机,通过网络连接并且可以上因特网。

四、实验内容和任务

1. 为了加深对 Whois 域名查询服务的了解,自己找一些域名进行查询

可以访问 http://ewhois.cnnic.net.cn/,利用 CNNIC 对其 CN 域名信息查询的 Whois 服务,来查询某些域名或 IP 的信息,例如查询 sina.com.cn。如果是国际域名,就需要访问 http://www.internic.net/whois.html,例如查询微软 www.microsoft.com。对于某些.edu 域名的查询,CNNIC 是不支持的,为了解决这种情况,可访问 http://www.nic.edu.cn/cgi-bin/reg/otherobj 进行查询,例如查询清华大学的域名信息。

2. Google Hack 的具体应用

上面所说得 Google 语法查询可以精确的查找需要的资料。对于黑客来说,他们感兴趣的是如何利用 Google 从站点挖掘信息,以及如何利用这些信息。例如可以利用“index of”来查找开放目录浏览的站点。下面将介绍如何利用“index of”语法来得到开放目录浏览的

Web 服务器列表。

可尝试使用 Google 搜索以下内容：

Index of /admin

Index of /passwd

Index of /password

Index of /mail "Index of /" +passwd "

Index of /" +password. txt "

Index of /" +. htaccess "

Index of /secret" "

Index of /confidential" "

Index of /root" "

Index of /cgi-bin" "

Index of /credit-card" "

Index of /logs" "

Index of /config"

"#-FrontPage-"inurl:service. pwd

从上面的搜索结果可知，一些重要的密码可能因为不同的原因被放置到公开的网络上，如果被别有用心的人获得，那么危害是很大的。

另外可以用 Google 来搜索一些具有缺陷的站点，例如利用“allinurl: winnt/system32/”（不包括引号）会列出所有通过 Web 可以访问限制目录如“system32”的服务器链接。如果幸运的话可以访问到“system32”目录中的 cmd. exe，能够访问“cmd. exe”就可以执行它，从而获得在这个服务器中的控制权。

再如利用[allintitle:“index of /admin”]（不包括括号）会列出所有开放 “admin”目录浏览权限的 Web 站点链接列表。大多数 Web 应用程序通常使用“admin”来存储管理凭证，在这个目录中有时包含可通过简单 Web 查询得到的敏感信息。

此外还可以查找有跨站脚本漏洞（XSS）的站点：allinurl:/scripts/cart32. exe，allinurl:/CuteNews/show_archives. php，allinurl:/phpinfo. php 等。

查找有 SQL 注入漏洞的站点：allinurl:/privmsg. php。

读者可利用上面所提的 Google Hack 的语法和关键词查询某些敏感信息，感受搜索引擎的强大功能，并加强对此的防范意识。

3. DNS 服务攻击

（1）DNS 服务器攻击原理

当已经成功的控制了 200. 20. 20. X 子网中的一台主机（如 200. 20. 20. 2）时，可通过安装 Sniffer 网络嗅探软件的方法对整个子网中传输的包进行嗅探。假设该网段中本地域名服务器的 IP 地址为 200. 20. 20. 1，可设置网络嗅探软件只对进出 200. 20. 20. 1 的数据包进行捕获，

在它的 DNS 数据包中可以获取所需要的查询 ID。当 DNS 服务器 200.20.20.1 发出查询包时，它会在包内设置查询 ID，只有应答包中的 ID 值和 IP 地址都正确的时候才能为服务器所接受。这个 ID 每次自动增加 1，所以可以第一次向要攻击的 DNS 服务器发一个查询包并监听到该 ID 值，随后再发一个用于干扰的查询包，紧接着马上发送构造好的应答包，包内的查询 ID 为预测的可能值。为了提高成功效率可以指定一个范围，比如在前面监听到的那个 ID+1 值后面的一个范围内。

例如 200.20.20.100 上的 DNS 请求者向 DNS 服务器 200.20.20.1 发来请求，要求查 www.abc.com 域名所对应的 IP 地址。此时，DNS 的攻击者就要伪造 DNS 服务器的响应数据包，响应给 DNS 请求者一个假的 IP 地址。

详细的 DNS 欺骗过程如下，首先 200.20.20.100 上的 DNS 请求者向 DNS 服务器 200.20.20.1 发来请求，要求查 www.abc.com 域名所对应的 IP 地址，请求者发送的请求数据包如下：

200.20.20.100→200.20.20.1 [Query]

QY：www.abc.com A

DNS 攻击者 200.20.20.10 在局域网中可以监听到这个包，从而得到它的 ID 为 3403。然后，马上再向 DNS 服务器 200.20.20.1 发出一个新查询请求，这个新的查询请求用于干扰 DNS 服务器，使 DNS 服务器忙于应答这个新查询数据包，从而延缓对旧查询数据包的应答。这个新的查询请求数据包的内容如下：

200.20.20.10→200.20.20.1 [Query]

QY：other.abc.com A

然后攻击者马上再以 DNS 服务器的身份伪造一个带有预测 QID 的应答包，返回给 200.20.20.100 上的请求者。

200.20.20.1→200.20.20.100 [Answer]

QID：3404

QY：www.abc.com PTR

AN：www.abc.com PTR a.b.c.d

其中 a.b.c.d 就是攻击者伪造的 www.abc.com 的 IP 地址。注意发这个包时查询 ID 为前面监听到的 ID 值加 1。这样，DNS 欺骗就完成了。200.20.20.100 就会把 a.b.c.d 当 www.abc.com 的 IP 地址了。假如 a.b.c.d 是一台已经被攻击者控制的计算机，可以把它的主页改成攻击者想要的内容，这时当被欺骗的用户连接 www.abc.com 时，就以为这个网站已经被黑掉了。

(2) DNS 服务攻击的检测和防范

通过上面 DNS 服务攻击过程的学习，可更加深入的了解 DNS 服务攻击的原理。当通过域名访问网站以及通过 IP 访问网站时，访问的网站不相同时，可判断 DNS 服务器被实施了欺骗攻击。这时，需要清除 DNS 欺骗程序，此后通过域名进行的访问将恢复正常。

五、实验报告要求

1. 通过 Whois 域名查询网站，输入相关域名或者 IP，记录并分析 Whois 域名查询的结果，提交实验报告。

2. 通过学习原理，了解了 Google Hack 的使用方法，同时采用 Google Hack 技术查询某些感兴趣的结果，进行截图记录，提交报告。

3. 学习了 DNS 攻击的原理后，编程实现实验内容中的第(3)部分 DNS 欺骗攻击，并找出防范 DNS 攻击的方法，提交实验报告。

实验 1-2　网络服务和端口的扫描

一、实验目的

通过 Ping 等命令了解目标主机的可访问性。通过使用网络扫描软件，了解目标主机端口和服务的开放情况，从而进一步获取系统信息，找出系统安全漏洞。本实验中，将使用 SuperScan 以及 Nmap 来进行网络扫描。通过本次实验，读者可以了解到端口与服务开放的风险，增强在网络安全防护方面的意识。

二、实验原理

在扫描探测的过程中，最常用到的就是一些操作系统提供的简单命令，比如 Ping、Tracert。其次，可使用一些功能比较强大的扫描工具，本实验中使用的是 SuperScan 和 Nmap，下面简单介绍一下它们的原理。

1. Ping 以及 Tracert

普通的 Ping 和 Tracert 都是使用的因特网控制消息协议(Internet Control Message Protocol，ICMP)。

Ping 命令：Ping 命令可以判断目标主机是否开机，并且可判断目标主机和本机之间网络链路是否链通。Ping 命令首先会构建一个固定格式的 ICMP 请求数据包 Echo Request，然后由 ICMP 协议将这个数据包连同目的主机的地址一起交给 IP 层协议。IP 层协议将以本机 IP 地址作为源地址，加上一些其他的控制信息，构建一个 IP 数据包。同时，在本机的物理地址映射表中查找出目的主机 IP 地址所对应的物理地址(也叫 MAC 地址，这是数据链路层协议构建数据链路层的传输单元——帧所必需的)，一并交给数据链路层，数据链路层将构建一个数据帧，主要包含目的主机的 MAC 地址和源主机的