

《网络信息安全》教学大纲

学时数：（理论学时）42+（试验学时）18

编写日期：2023 年 5 月

一、课程性质、目的和任务

《网络信息安全》是一门综合性和实践性很强的核心课程，具体地介绍网络信息安全的根底理论、原理及其实现方法。课程内容包括：计算机网络与网络安全概述、操作系统安全、黑客攻击与防范、计算机病毒、防火墙技术、密码学、VPN 技术、入侵检测、构造网络安全体系、数据备份、信息隐蔽与数字水印、计算机犯罪与取证等。

依据培育基层应用型人才的需要，本课程的目的与任务是使学生通过本课程的学习，了解网络信息安全的根本学问和把握具体应付方法，为更深入地学习和今后从事公安信息化治理工作打下良好的根底。

1、学问要求：

学生通过学习该课程后主要应把握以下内容：

- 〔一〕网络安全现状与需求、安全防范的必要性；
- 〔二〕几种常用的加密算法：传统的加密方法，数据加密标准 DES，公开密钥加密算法，RSA 加密方法；
- 〔三〕病毒的作用机制及其防护
- 〔四〕深入理解主要操作系统存在的安全问题，（Windows 98/NT/2023、Unix 等）和安全治理的重要性
- 〔五〕常见黑客技术及防范措施
- 〔六〕防火墙的根本概念、特性及根本准则
- 〔七〕VPN 的概念和核心技术。着重把握实现VPN 的其次层隧道协议、第三层隧道协议。
- 〔八〕入侵检测系统的概念、分类、部署及常用技术，着重把握 Snort 入侵检测系统
- 〔九〕把握数据备份的方法、RAID 技术及基于 SAN 的备份系统
- 〔十〕信息隐蔽的概念、模型及方法及数字水印攻击技术
- 〔十一〕 计算机犯罪的概念、分类、特点及计算机取证技术

2、素养要求

学生通过学习该课程后能够运用独立解决在网络安全方面遇到的一些比较根本的问题。

3、力气要求

学生通过学习该课程后能够维护网路效劳器的安全以及个人电脑的网络安全。

二、教学内容和根本要求：

1、 根本内容：

第 1 章计算机网络与网络安全概述

1.1 计算机网络概述

1.2 网络安全概述

第 2 章操作系统安全

2.1 漏洞和后门

2.2UNIX 系统安全

▲2.3Windows NT/2023 系统安全

第 3 章黑客攻击与防范

3.1 黑客的影响和危害

3.2 黑客的特点及攻击手段

▲3.3 黑客的防范

第 4 章计算机病毒

4.1 概述

4.2 蠕虫病毒

4.3 计算机病毒的防治措施

4.4 病毒程序实例分析

第 5 章 防火墙技术

5.1 防火墙的概念

5.2 防火墙的构成

▲5.3 防火墙设计

5.4 分布式防火墙技术

第 6 章 密码学

6.1 密码学概述

6.2 经典密码学

▲6.3 对称加密技术

▲6.4 公钥密码体制

第 7 章 VPN 技术

7.1 VPN 概述

7.2 VPN 主要技术

▲7.3 其次层隧道协议——L2F，PPTP 和 L2TP

▲7.4 第三层隧道协议——GRE 和 IPSec

第 8 章 入侵检测

8.1 概述

8.2 入侵检测系统分类

8.3 入侵检测系统的部署

▲8.4 入侵检测技术

▲8.5Snort 入侵检测系统

第 9 章构造网络安全体系

9.1 网络安全体系概述

9.2 设计网络安全体系

9.3 网络安全方案的实施

9.4 网络安全治理

9.5 证券行业网络安全方案介绍

第 10 章数据备份

10.1 概述

10.2 数据备份系统

▲10.3 基于 SAN 的数据备份系统

10.4 基于因特网的数据备份技术

10.5 归档和分级存储治理

10.6 数据容灾系统

第 11 章信息隐蔽与数字水印

11.1 信息隐蔽

▲11.2 数字水印技术

▲11.3 水印攻击

▲11.4 数字指纹技术

第 12 章计算机犯罪与取证

▲12.1 计算机犯罪

▲12.2 计算机取证

2、根本要求：

网络安全现状与需求、安全防范的必要性；

几种常用的加密算法：传统的加密方法，数据加密标准 DES，公开密钥加密算法，RSA 加密方法；

病毒的作用机制及其防护

主要操作系统存在的安全问题，〔Windows 98/NT/2023、Unix 等〕和安全治理的重要性

常见黑客技术及防范措施

防火墙的根本概念、特性及根本准则

VPN 的概念和核心技术。着重把握实现VPN 的其次层隧道协议、第三层隧道协议。

入侵检测系统的概念、分类、部署及常用技术，着重把握 Snort 入侵检测系统

把握数据备份的方法、RAID 技术及基于 SAN 的备份系统

信息隐蔽的概念、模型及方法及数字水印攻击技术

计算机犯罪的概念、分类、特点及计算机取证技术

三、教学的重点及难点：

本课程的教学重点在于网络信息安全的根本学问和常用的安全技术，在内容上以介绍方法为主，突出应用的需要，尽量避开原理性介绍和根本数学理论内容，力争反映网络安全技术的最进展，满足构造安全的网络应用系统的需要。

教学重点包括：

- 1) 数加密的根本方法，DES 加密算法，RSA 密码体制
- 2) 计算机病毒的工作原理及其防范
- 3) 操作系统的安全
- 4) 黑客入侵技术与黑客攻击技术，安全防范和安全监测
- 5) 实现 VPN 的其次层隧道协议、第三层隧道协议
- 6) 信息隐蔽的模型、方法
- 7) 数字水印攻击技术

8) 计算机取证技术

依据以往的教学阅历，教学难点主要集中在比较抽象和难以理解的概念、原理，主要有：

- 1) 对称加密算法：DES 加密算法，非对称加密算法：RSA 密码体制
- 2) 密钥验证与密钥安排
- 3) 网络协议的安全
- 4) 防火墙体系构造
- 5) 实现 VPN 的其次层隧道协议、第三层隧道协议
- 6) 信息隐蔽的模型、方法

四、课程各教学环节要求：

〔一〕课堂讲授要求：

主要通过上课讲授，可以适当地结合多媒体课件。

五、学时安排

总学时：60 学时

章节	主要内容	各教学环节学时安排							作业 题量	备注
		讲授	试验	争论	习题	课外	其它	小计		
1	计算机网络与 网络安全概述	2						2		
2	操作系统安全	2						2		重点
3	黑客攻击与防 范	2	2	2				6		重点
4	计算机病毒	2	2	2				6		重点
5	防火墙技术	4	2					6		重点
6	密码学	6						6		难点
7	VPN 技术	4	2					6		难点
8	入侵检测	4	2					6		重点
9	构造网络安全	4	2					6		

	体系									
10	数据备份	4	2					6		
11	信息隐蔽与数字水印	2	2					4		重点
12	计算机犯罪与取证	2	2					4		重点

理论学时：42 学时
试验学时：18 学时

六、其他课程的联系：

本课程是在计算机文化根底上讲授的，要求前续课程对操作系统、网络数据传输的根本概念和根本理论具体讲解，并应把握一门高级程序设计语言如 vb 语言等。

七、教材与参考书

教材：

《网络信息安全》 张辉等 石油大学出版社；

主要参考书目：

1. 《密码编码学与网络安全：原理与实践》 William Stallings 电子工业出版社
2. 《系统安全与入侵检测》 戴英侠，连一峰 国防工业出版社
3. 《计算机病毒诊断与防治》 张小磊 北京希望电子出版社

本章教学重点、难点：

- λ 1、计算机网络的概念、分类作用及其产生与进展
- λ 2、计算机网络的根本体系构造
- λ 3、计算机网络协议
- 4、网络安全的概念、影响因素及安全模型

第一章:计算机网络与网络安全概述

1.1 计算机网络概述

从不同的角度，以不同的观点，可以给计算机网络下不同的定义。目前，比较公认的定义

义是：“凡将地理位置不同，并具有独立功能的多个计算机系统通过通信设备和线路连接起来，以功能完善的网络软件实现网络中的资源共享的系统，称之为计算机网络。”

依据网络的定义知道，网络不仅使计算机超越了地理位置，而且更重要的是增加了计算机本身的功能。网络的功能有以下几点：

1. 资源共享
2. 提高牢靠性
3. 分布式处理

计算机网络中各台主机的类型和规格可能不同，每台主机使用的操作系统也可能不同，因此为使计算机网络能正常运行，就必需有一套网络中各节点共同遵守的规程，这就是网络协议。它是一组关于数据传输、输入输出格式和把握的规约。有了这些规约就可在物理线路的根底上，构成规律上的连接，实现在网络中的计算机、终端及其他设备之间直接进展数据交换。鉴于网络节点的功能有多层，网络协议也承受对应的层次构造。1978 年国际标准化组织ISO 提出了著名的开放系统互联参考模型 OSI 将网络中的通信治理程序与其他程序分开，并依据数据在网络中传输的过程将通信治理程序分为7 个层次的模块，从下往上依次为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。其中每一层都有相对独立的明确的功能；每一层的功能都依靠于它的下一层供给的效劳，每一层又为它的上一层供给必要的效劳；相邻的上下两层间通过界面接口(即软件接口)进展通信。该模型的第一至四层是面对数据传输的，第五至七层是面对应用的，而最下面的物理层直接负责物理线路的传输，最上面的应用层直接面对用户。

1.2 网络安全概述

网络安全泛指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的缘由而遭到破坏、更改、泄漏。系统连续牢靠正常地运行，网络效劳不被中断。

网络安全的内容包括了系统安全和信息安全两个局部。系统安全主要指网络设备的硬件、操作系统和应用软件的安全；信息安全主要指各种信息的存储、传输的安全，具体表达在保密性、完整性及不行抵赖性上。

从内容看，网络安全大致包括 4 个方面。

- 网络实体安全：如计算机机房的物理条件、物理环境及设施的安全标准；计算机硬件、附属设备及网络传输线路的安装及配置等。
- 软件安全：如保护网络系统不被非法侵入，系统软件与应用软件不被非法复制、篡改、不受病毒的侵害等。
- 数据安全：保护数据不被非法存取，确保其完整性、全都性、机密性等。
- 安全治理：运行时突发大事的安全处理等，包括实行计算机安全技术，建立安全治理制度，开展安全审计，进展风险分析等。

从特征上看，网络安全包括 5 个根本要素。

- 机密性：确保内容不暴露给未授权的实体。
- 完整性：只有得到允许的人才能够修改数据，并能判别数据是否已被篡改。
- 可用性：得到授权的实体在需要时可访问数据，即攻击者不能占用全部资源阻碍授权者的工作。
- 可控性：可以把握授权范围内的信息流向以及行为方式。
- 可审查性：对消灭的网络安全问题供给调查的依据和手段。

由于系统自身的脆弱性使网络信息的机密性、完整性、可用性和资源的合法使用受到威逼。

所谓系统的脆弱性是指系统的硬件资源、通信资源、软件及信息资源等，因可预见或不行预见甚至恶意的缘由，可能导致系统受到破坏、更改、泄漏和功能失效，从而使网络处于特别状态，甚至导致崩溃、瘫痪等的根源和起因。计算机网络本身由于系统主体和客体的缘由可能存在不同程度的脆弱性，为各种动机的攻击供给了入侵、骚扰或破坏系统的可利用的途径和方法。

本章教学重点和难点：

- 1、漏洞和后门
- 2、NetWare 系统安全
- 3、Windows NT 系统安全
- 4、UNIX 系统安全

2.1 漏洞和后门

在计算机网络安全领域，“漏洞”是指硬件、软件或策略上的缺陷，这种缺陷导致非法用户未经授权而获得访问系统的权限或提高其访问权限。有了这种访问权限，非法用户就可以为所欲为，从而造成对网络安全的威逼。

安全漏洞存在不同的类型，包括：允许拒绝效劳的漏洞；允许有限权限的本地用户未经授权提高其权限的漏洞；允许外来团体〔在远程主机上〕未经授权访问网络的漏洞。

1. 允许拒绝效劳的漏洞
2. 允许有限权限的本地用户未经授权提高其权限的漏洞
3. 允许外来团体〔在远程主机上〕未经授权访问网络的漏洞

随着网络经济时代的到来，网络将会成为一个无处不在、无所不用的工具。经济、文化、军事和社会活动将会猛烈地依靠于网络。网络的安全和牢靠性成为世界各国共同关注的焦点。而Internet 的无主管性、跨国界性、不设防性、缺少法律约束性的特点，在为各国带来进展机遇的同时，也带来了巨人的风险。目前，Internet 和 Web 站点风险的很多事例可能已使一些用户坐立担忧了，似乎处处都有漏洞，处处都是黑客的行迹。确实，漏洞严峻地影响着Internet 的安全。

1. 漏洞影响Internet 的牢靠性和可用性
2. 漏洞导致Internet 上黑客入侵和计算机犯罪
3. 漏洞致使Internet 患病网络病毒和其他软件的攻击

2.2 UNIX 系统安全

UNIX 系统的安全性得到用户的公认，已在 Internet 上广为使用。不过，UNIX 系统也存在一些安全漏洞。

2.2.1 UNIX 系统的安全等级

UNIX 系统符合国家计算机安全中心的C2 级安全标准，引进了受控访问环境〔用户权限级别〕的增加特性。进一步限制用户执行某些系统指令；审计特性跟踪全部的“安全大事”〔如登录成功或失败〕和系统治理员的工作〔如转变用户访问权限和密码〕。

2.2.2 UNIX 系统的安全性

1. 按控制台安全
2. 口令安全
3. 网络文件系统
4. FTP 安全

2.2.3 UNIX 系统的安全漏洞

UNIX 系统存在以下安全漏洞：

- Sendmail 漏洞
- Passwd 命令漏洞
- Ping 命令问题
- telnet 问题
- 网络监听
- yppasswd 漏洞

这些已知的 UNIX 安全漏洞都有具体的解决或补救方法，有兴趣的读者可查看有关书籍，这里不再赘述。

2.1 Windows NT/2023 的安全

2.3.1 Windows NT/2023 的安全等级

作为一个标准的系统，Windows NT server 自 3.5 版就已到达了国家计算机安全中心的 C2 级安全级的要求。局部程序，如身份确认、审计和把操作者账号与治理员账号分开的功能，甚至到达了更高的安全级（即 B2 级）要求。目前，美国国家计算机安全留神将 Windows NT server4.0 评定为网络安全系统的一个组成局部。

在 Windows NT server 3.5 上实现 C2 级安全标准仅仅是建立在软件根底上的为了得到符合 C2 级安全标准的系统设置，必需：

- 拥有对系统的非网络访问。
- 去除或制止使用软盘驱动器。
- 更加严格地把握对标准文件系统的访问。

用户利用 Windows NT 的资源治理工具箱中的 C2 配置工具，可以获得符合 C2 级安全标准的系统。

在 Windows NT 3.5 上，最重要的 C2 级安全标准特性是：

- 可以自由打算访问把握：允许治理员或用户自己定义对它们所拥有的对象的访问把握。
- 对象重用：当内存被一个程序释放后，不再允许对它进展读访问。当对象被删除后，即使对象所在的磁盘空间已经重进展了安排，也不再允许用户对对象进展访问。
- 身份确实认和验证：在对系统进展访问之前，用户必需首先确认自己的身份。用户可以通过输入用户名称、口令或域的组合来完成对自己身份确实认。
- 审计：必需创立并维护对对象的访问记录，并防止他人对此记录进展修改，必需严格规定只有指定的治理员才能访问审计信息。

2.3.2 Windows NT/2023 的安全性

Windows NT 的设计目的是为了帮助人们完善它们的安全机制，供给具体的访问把握、信息保护、把握“外来”访问等功能。另外，为了增加对基于 Internet 的企业网络的支持，Windows NT 在安全性方面也做出了很多提高。

1. Windows NT 安全性分析
2. Kerberos 和 Windows NT
3. 加密文件系统

第三章：黑客攻击与防范

本章教学重点和难点：

- 1、黑客的特点、影响和危害
- 2、黑客的攻击过程
- 3、黑客常用的攻击手段
- 4、防范黑客的方法

3.1 黑客的影响和危害

黑客是英文“Hacker”的英文译音，我国台湾地区译为“骇客”，它起源于美国麻省理工学院的

计算机试验室中。早期的黑客是指那些精力旺盛，智力超群，具有超群编程力气的计算机程序员。他们的行为主要包括设计黑客软件、盗打长途 以及利用 进展欺诈。目前，按 照公安部 1997 年 4 月 21 日公布的《计算机信息系统安全专用产品分类原则》中术语的定义，黑客是指对计算机信息系统进展非授权访问的人员。也有人认为，黑客就是指那些利用通讯 软件、通过网络非法进入公共和他人的计算机系统，截获或篡改计算机中的信息，危害信息 系统安全的电脑入侵者，其入侵行为称为黑客行为。

黑客的特点

(1) 充当黑客的年轻人居多

黑客年龄一般在 10 余岁到 30 岁之间，其中有很多未成年的小孩，如美国号称“世界头号计算机黑客”的 Kevin Mitnick，13 岁迷上计算机，15 岁闯入“北美空中防务指挥系统”；英国的 Mathew Bevan 14 岁侵入英国的电信公司；我国呼和浩特市一个 10 岁的初中生破译了该市通信公司的系统治理员的账号，等等。

(2) 人员的构成相对集中

70% 以上的黑客大事是由内部人员或外部与内部合谋进展的。一般来说，外部黑客入侵的目的主要是破坏系统，而内部或内外勾结的入侵多数是为了猎取信息；外部黑客对一个站点可能只入侵一次，内部或内外勾结的入侵可能会连续几次。

(3) 黑客活动时间相对固定

黑客活动主要是在晚上到凌晨、周末或节假日。由于职业化的黑客很少，一般黑客多 有自己的工作，实施黑客活动需要利用休息时间，又由于在这些时间里，工作场所的人员少， 便于隐蔽。

(4) 从进展趋势看，黑客正在不断地走向系统化、组织化和年轻化

黑客甚至定期召开会议，如他们每四年在荷兰进展一次 Hack - Tic 会议、每年在纽约进展“2600 公文”、在拉斯维加斯进展 DefCon 会议和在加利福尼亚的 Lake Tahoe 进展“黑客大会”。

黑客攻击危害程度的划分

黑客攻击所使用的方法不同，产生的危害程度也不同，一般分为八个层次：

第一层：邮件炸弹攻击；

其次层：简洁拒绝效劳；

第三层：本地用户获得非授权的读访问；

第四层：本地用户获得他们非授权的文件写权限；

第五层：远程用户获得了非授权的账号；

第六层：远程用户获得了特权文件的读权限；

第七层：远程用户获得了特权文件的写权限；

第八层：远程用户拥有了根权限（黑客已经攻克了系统）。

在这八层中，随着层号增大，危害的程度加重。

3.2 黑客的特点及攻击手段

黑客攻击的手段

目前，黑客攻击网络的手段种类繁多，而且的手段层出不穷，黑客攻击可以分为以下两大类：

一类是主动攻击，这种攻击以各种方式猎取攻击目标的相关信息，找出系统漏洞，侵入系统后，将会有选择地破坏信息的有效性和完整性。例如：邮件炸弹。

另一类是被动攻击，这种攻击是在不影响网络正常工作的状况下，进展截获、窃取、破译以获得重要机密信息，其中包括窃听和通信流量分析。例如：扫描器。

当前黑客攻击承受的主要手段是利用目前网络系统以及各种网络软件的漏洞，比方基于 TCP/IP 协议本身的不完善、操作系统的种种缺陷等；防火墙设置不当；电子欺诈；拒绝效劳（包括 DDoS）；网络病毒；使用黑客工具软件；利用用户自己安全意识薄弱，比方口令设置不当；或直接将口令文件放在系统等等。下面简洁介绍几种黑客常用的方法：

(1) 扫描器

所谓扫描器，实际是一种自动检测目标计算机安全性弱点的程序。黑客通过使用扫描器，可以不留痕迹的觉察远程效劳器的各种 TCP 端口的安排及供给的效劳、使用的软件版本以及其他一些效劳信息。

(2) 口令破解

黑客进展攻击常常是从破解用户口令开头的。

(3) 炸弹攻击与病毒

炸弹攻击是指黑客利用自编的炸弹攻击程序或工具软件，集中在一段时间内，向攻击的目标机器发出大量信息，使机器消灭负载过重、网络堵塞，最终使系统崩溃的一种网络攻击手段。

(4) 电子哄骗 (Spoofing)

电子哄骗一般包括任何使用计算机进展哄骗的行为。

(5) 监听法

网络监听是局域网中的一种黑客技术，由于在进展监听时，不与其他主机交换信息，也不修改密码，因此，网络监听是一种被动的攻击方式，仅用于局域网中。

(6) 拒绝效劳攻击 (Denial of Service)

拒绝效劳攻击是指攻击者占有大量的共享资源，使系统无法为其他用户供给资源或以过多的恳求造成“溢出”，使效劳器或路由器过载，甚至迫使效劳器关闭，终止为用户供给效劳的一种攻击方法。拒绝效劳攻击是一种主动的破坏性攻击。

从造成的危害上划分，拒绝效劳攻击可分为两类，一是破坏或毁坏系统资源，使用户无法使用；其次类是过载系统效劳或消耗系统资源，阻挡其他用户使用这些效劳。

3.3 黑客的防范

防范黑客的攻击，保证计算机网络的正常运行，是一个困难但又必需努力争论和探究的问题。目前，还不能靠某种单一的方法完全阻挡黑客的攻击，但是可以实行一个综合的策略或系统，多层次的设防。包括治理、制度、法律和技术等方面，以阻挡和削减黑客攻击计算机网络大事的发生。

防范黑客，保障网络安全，应当制定一个完善的网络安全策略，其中包括安全标准标准体系、安全技术防范体系和安全治理保障体系这三大方面。

目前主要防范黑客措施有以下几种：

3.3.1 安全治理

网络的安全治理包括：确定安全治理等级和安全治理范围；制订有关网络操作使用规程和人员出入机房治理制度；制定网络系统的维护制度和应急措施等。

3.3.2 黑客的防范技术

防范黑客的技术措施有很多，下面介绍几种根本的防范技术。

(1) 防火墙技术

建立“防火墙”是一种常见的有用技术措施。

“防火墙”是一种形象的说法，其实它是一种计算机硬件和软件的组合体。防火墙使互联网与内部网之间建立起一个安全网关，从而保护内部网免受外部非法用户的侵入。防火墙就是因特网与内部网隔开的屏障。

虽然防火墙是防范外部黑客的最重要的手段之一，但是，假设设置不当，会留下漏洞，成为黑客攻击网络的桥梁。