网络安全概述

知识点	要求
课程覆盖的内容和参考资料	课程的知识范畴，与其他课程之间的关系
计算机安全面临的挑战	了解信息在处理、保存、传输等过程中面临的安全威胁。
计算机安全的目标	熟练掌握计算机安全的几个目标：保密性、完整性、授权、认证和不可否认性。
计算机入侵的特点	掌握计算机入侵的基本术语（脆弱点、威胁、控制），最易渗透原则，分析特定场景的脆弱点、威胁、控制。
各类资源的脆弱点及其基本防御方法	分析计算机硬件、软件、数据、传输介质的脆弱点，以及一般性的防御策略
黑客	了解黑客的发展史，黑客的目的，著名黑客，黑客的技术要求
网络攻击事件举例	典型的网络攻击事件
新的攻击手段与趋势	近年流行的恶意代码传播方式，利用僵尸网络、社交网络、智能终端传播垃圾邮件、恶意链接，进而进行恶意代码传播的方式。
安全的相关标准	信息安全和系统安全的国际标准。
信息安全研究的内容	信息安全覆盖的知识体系和研究内容。

密码学、密钥分配和用户认证

知识点	要求
密码学的基本概念	密码算法的表示、分类
典型的加密方法	介绍替换、一次一密、置换的基本方法。
对称密钥标准 DES、3DES，AES；	典型的对称密钥算法及其安全性。
公开密钥标准 RSA Diffie- Hellman；	典型的非对称密钥算法及其安全性
哈希与认证码	哈希函数的特点和应用，消息认证码 HMAC 的原理和作用
密钥分配和用户认证的作用	掌握会话密钥的作用
基于对称加密的密钥分配;Kerberos 认证	掌握 Kerberos 认证适用的场景，认证服务器、票据服务器和提供服务的服务器之间的关系，Kerberos 认证的安全性。
基于非对称加密的密钥分配	掌握利用公钥进行密钥分配的一般原理
X.509 证书	掌握公钥证书包含的内容，如何验证相应的证书的。
公钥基础设施 PKI	掌握 PKI 中 CA 的作用，CA 之间的信任关系。

用户认证的一般技术

知识点	教学要求
认证方法的一般方法（口令认证、令牌认证、生物特征认证）	介绍认证采用的一般方法，口令认证面临的威胁（暴力攻击、彩虹表攻击）、Unix 口令的存储方式
远程认证（同步令牌、挑战应答非同步认证方式）及其安全性	熟练掌握远程认证中需要解决的问题（暴力破解、重放攻击），构造动态一次性口令的方法，挑战应答非同步认证的一般原理及其安全性分析
与远程认证相关的技术	TCP 序列号　DNS　HTTP　SSL　SSH

网络协议与缺陷

知识点	教学要求
Internet 网络协议基本的安全问题	掌握网络协议的多个层次存在的缺陷，缺乏加密和认证，可能的攻击数据包窃听、TCP 连接欺骗、无线攻击
路由的漏洞	网络层面临的安全威胁--广播虚假的路由信息(BGP\ARP) 网络层会话劫持
DNS 系统的安全问题	介绍 DNS 询问应答中没有认证的安全问题，导致 DNS 缓存中毒问题，DNS 重新绑定攻击。
嗅探	介绍被动嗅探和主动嗅探的技术和方法，相应的防御手段
ARP 欺骗	介绍 ARP 欺骗的场景、技术和危害，防御的方法
IP 地址欺骗	介绍 IP 地址欺骗的一般方法和危害，相应的防御方法
TCP 会话劫持	介绍 TCP 会话劫持的一般方法和危害

安全协议标准

（IP 安全）

知识点	教学要求
IPsec 的传输模式与隧道模式	掌握 IPsec 的两种工作模式，协议格式，协议的作用及安全性分析
安全关联 SA 与安全策略数据库 SPD；	掌握 SAD 和 SPD 的作用
密钥交换协议 IKE	介绍 SA 的密钥交换过程及其安全性

（传输层安全）

知识点	要求
传输层安全：SSL；TLS；HTTPS；	介绍 SSL 的功能，认证方法，协议格式以及在 HTTPS 中的应用
传输层安全：SSH	介绍 SSH 的作用和工作原理

（电子邮件安全）

知识点	要求
PGP	掌握 PGP 方法如何保障邮件的秘密性、完整性和不可否认性的
S/MIME	MIME 类型中添加安全类型的作用和工作原理
DKIM	DKIM 是如何验证邮件服务器的，从而防止垃圾邮件

（垃圾邮件及其防范）

知识点	要求
邮件发送的基本原理（SMTP Relay 、HTTP proxies、spamware）、	垃圾邮件发送的一般方法，以及逃避黑名单检测的一般方法。
反垃圾邮件的方法（CAN-SPAM act、SPF、DKIM、Graylists）	垃圾邮件的防御方法

典型网络攻击与防御方法

（攻击手段）

知识点	教学要求
攻击准备阶段	介绍信息查找、战争拨号等发现目标的方法和原理
端口扫描	介绍端口扫描的方法、类别和工作原理。
漏洞扫描	介绍漏洞扫描的基本原理和方法，漏洞扫描的工具和应用
网络测绘	介绍网络测绘的一般技术，利用 ICMP 和 SNMP 进行网络测绘，相应的工具和使用
攻击链 反攻击链	攻击链 反攻击链

（不同协议层次的 DoS 攻击）

知识点	教学要求
802.11b DoS bugs	介绍 WIFI 接入过程中由于缺乏认证可能存在的拒绝服务攻击。
放大式拒绝服务攻击（Smurf amplification attack，DNS Amplification attack）	介绍放大式拒绝服务攻击的基本方式，利用 ICMP 包和 DNS 询问进行拒绝服务攻击的一般原理及其相应防御策略。
SYN Floods	介绍 TCP 连接过程的拒绝服务攻击及其防御策略。
DNS DoS Attacks	介绍 DNS 拒绝服务的原理和攻击举例、一般的防御策略
高层的 DoS 攻击 （利用 SSL、HTTP 的攻击）;	利用高层协议的缺陷进行拒绝服务攻击的原理和方法
DoS 防御的方法（Client puzzles、CAPTCHAs、Source identification）	针对 DoS 在应用层的防御方法，DoS 攻击源追踪的方法。

网络边界安全防御

（防火墙）

知识点	教学要求
包过滤防火墙	介绍一般包过滤防火墙按五元组过滤的工作原理
有状态的动态包过滤	状态防火墙的作用，如何实现动态包过滤
应用层防火墙	应用层防火墙的基本工作原理
包碎片攻击	针对单纯包过滤防火墙的包碎片攻击，基本原理和举例
防火墙的部署（屏蔽主机结构、屏蔽子网结构、双宿主主机结构）	介绍典型的防火墙部署结构，掌握屏蔽子网存在的意义。

（入侵检测）

知识点	教学要求
IDS 的基本结构	介绍入侵检测系统的基本结构
滥用检测	滥用检测的概念、一般方法和局限性
异常检测	异常检测的概念、一般方法和局限性
基于主机的入侵检测	基于主机的入侵检测事件、方法
基于网络的入侵检测	基于网络的入侵检测事件、方法
snort 的结构	Snort 系统的一般结构和应用

Web 应用安全

知识点	要求
命令注入方法与举例；	介绍命令注入的方法、出现场景举例以及防御手段
SQL 注入方法、举例与防御；	介绍 SQL 注入的方法、出现场景举例以及防御手段
CSRF 交叉站点请求伪造方法、举例与防御；	介绍 CSRF 的方法、出现场景举例以及防御手段
XSS 交叉脚本攻击方法、举例（reflected XSS attack、Stored XSS DOM-based XSS ）；；	介绍 XSS 攻击的三种类型反射型、存储型和基于 DOM 的攻击，漏洞存在的根本原因。举例
Web 安全防护策略	介绍服务器端和客户端的防御策略，包括输入数据验证和过滤、输出数据验证和过滤、Dynamic Data Tainting、Static Analysis、
Web 漏洞检测工具	介绍 Web 漏洞扫描的基本原理和工具
Web 应用防火墙	介绍 Web 应用防火墙的作用和工作原理
浏览器终端安全	安全机制 同源策略 （DOM）
Web 会话管理	Cookie 同源策略， Cookie 设置和发送范围，安全问题（Cookie 重写，完整性问题） 会话管理 （token）安全问题（会话劫持，会话 token 防止窃取）

综合：

掌握应用场景安全威胁分析

掌握网络安全策略安全性分析方法（针对不同攻击的防御程度，缺陷和不足）

掌握安全策略设计的一般方法 （认证（防假冒）、加密（防窃听）、防重放等）