

《03345 信息与网络安全管理》

实践考核大纲

一、课程性质与目标

(一) 课程性质和特点

本课程是网络空间安全及相关专业的核心专业课程。旨在培养学生建立系统的网络空间安全观，理解信息安全的基本原理，并掌握主流的安全防护技术。课程通过理论与实践相结合的方式，使学生从攻防两个视角理解网络威胁，具备病毒防范、数据加密、防火墙配置及入侵检测等实际操作能力，为从事实践性网络安全工作打下坚实基础。

(二) 课程目标

本课程设置的目的在于培养学生具备安全防御能力，能够识别常见的网络攻击手段（如病毒、木马、ARP 欺骗等）并实施防御措施。同时，他们还应该掌握安全配置能力，可以熟练对 Windows/Linux 操作系统、防火墙、数据库及无线网络进行安全加固。此外，学生还应该熟练运用密码技术，掌握数据加密、数字签名及身份认证的工具与方法。他们应该具备综合分析能力，可以独立分析安全日志，使用 Snort 等工具进行入侵检测。

(三) 课程的重点

本课程的重点内容包括：考察学生的攻防原理理解，主要包括病毒机理、黑客入侵过程、密码学算法（DES/RSA）等；培养学生的安全工具使用，让他们掌握杀毒软件配置、抓包分析（Wireshark）、PGP 加密工具等内容；关注网络设备配置，学生需掌握防火墙 ACL 策略配置、NAT 配置等；最后，重视综合实战应用，要求学生能够进行简单的渗透测试实验及安全加固方案设计。

二、考核内容和考核目标

第一章 网络空间信息安全概论

一、学习目的与要求

(1) 了解网络空间安全面临的主要威胁与挑战。

(2) 掌握网络安全的基本属性及相关法律法规。

通过本章学习，学生应能识别社会工程学攻击、Web 安全漏洞等基本风险，

建立整体安全意识。

二、课程内容

- (1) Internet 及常用服务 (Email、Web、FTP) 的安全问题。
- (2) 社会工程学攻击手段。
- (3) 网络空间信息安全的主要内容与七大趋势。

三、考核知识点及要求

1. 了解不同的版面结构和网格系统的原理；
2. 理解各种版面结构和网格系统的特点。

识记：网络空间信息安全的定义、CIA 三要素（机密性、完整性、可用性）。

领会：Web 站点及文件传输面临的主要安全风险。

应用：分析简单的社会工程学攻击案例并提出防范建议。

第二章 病毒防范技术

一、学习目的与要求

通过本章学习，学生应能够掌握计算机病毒的特征、分类及工作原理，并且具备独立检测与清除常见病毒（如 U 盘病毒）的能力。

二、课程内容

- (1) 病毒、蠕虫、木马的区别与联系。
- (2) autorun.inf 文件分析与 U 盘病毒防护。
- (3) 杀毒软件的工作原理。

三、考核知识点及要求

识记：恶意代码的分类，典型病毒（如 CIH、熊猫烧香）的特征。

领会：杀毒软件的特征码扫描与行为监测原理。

应用：手动清除简单的 U 盘病毒，配置杀毒软件策略。

第三章 远程控制与黑客入侵

一、学习目的与要求

通过本章学习，学生应能够了解理解黑客入侵的一般过程及远程控制技术，并且掌握 ARP 欺骗的原理及防御方法。

二、课程内容

- (1) 远程控制软件原理及 Windows 远程桌面配置。
- (2) 黑客入侵的步骤（扫描、利用、提权、留后门、清理痕迹）。
- (3) ARP 欺骗原理与防范。

三、考核知识点及要求

识记：常见远程控制工具的功能，黑客攻击链的各个阶段。

领会：端口扫描的目的，ARP 协议的漏洞机制。

应用：使用命令（如 arp -a）检测 ARP 欺骗，配置主机防火墙防止非法远程连接。

。

第四章 网络空间信息密码技术

一、学习目的与要求

通过本章学习，学生应能够了解理解密码学的基本概念及发展历史，并且掌握对称加密与非对称加密的核心算法与应用场景。

二、课程内容

(1) 对称密码体系：流密码、分组密码、DES 与 AES 标准。

(2) 非对称密码体系：RSA 算法原理。

(3) 混合加密机制

三、考核知识点及要求

识记：对称与非对称加密的区别，常见算法名称（DES, AES, RSA）。

领会：分组密码的工作模式（ECB/CBC），公钥与私钥的配对逻辑。

应用：使用工具对文件进行对称加密与解密操作。

第五章 数字签名与验证技术

一、学习目的与要求

通过本章学习，学生应能够掌握数字签名的作用及实现过程，并且理解和熟悉 Hash 函数在完整性校验中的应用。

二、课程内容

(1) 数字签名算法（ElGamal, Schnorr）。

(2) 安全散列函数（MD5, SHA-1）。

(3) PKI（公钥基础设施）技术及 CA 认证中心。

三、考核知识点及要求

识记：数字签名的核心功能（防抵赖、身份认证），PKI 的组成。

领会：报文摘要（Digest）的生成与验证过程。

应用：计算文件的 MD5 值以校验完整性，模拟申请与查看数字证书。

第六章 网络安全协议

一、学习目的与要求

通过本章学习，学生应能够理解并且掌握常见网络层、传输层及应用层安

全协议的工作机制，熟悉 SSL/TLS 在 Web 安全中的重要性。。

二、课程内容

- (1) IPSec 协议族 (AH、ESP、IKE)。
- (2) SSL/TLS 握手协议与记录协议。
- (3) 应用层安全协议 (HTTPS, SSH, PGP)。

三、考核知识点及要求

识记：IPSec 的两种工作模式 (传输/隧道)，SSL 握手过程。

领会：如何通过 VPN 技术保障数据传输安全。

应用：配置浏览器查看 HTTPS 证书详情，分析 SSL 连接建立过程。

第七章 无线网络安全机制

一、学习目的与要求

通过本章学习，学生应能够了解无线网络 (Wi-Fi, Bluetooth, RFID) 的安全隐患，掌握无线网络的安全加密配置与防范措施。

二、课程内容

- (1) 无线网络分类及 Wi-Fi 安全协议 (WEP, WPA/WPA2)。
- (2) 无线网络入侵方法与工具。
- (3) 移动通信 (LTE) 架构安全。

三、考核知识点及要求

识记：SSID 隐藏、MAC 地址过滤的概念，WPA2 与 WEP 的安全性对比。

领会：无线中间人攻击与钓鱼热点的原理。

应用：安全配置无线路由器 (设置高强度加密、禁用 WPS)。

第八章 访问控制与防火墙技术

一、学习目的与要求

通过本章学习，学生应能够深入理解防火墙的功能、分类及工作原理，熟练掌握 NAT 技术及防火墙策略配置。

二、课程内容

- (1) 访问控制策略与实现。
- (2) 防火墙类型 (包过滤、状态检测、代理)。
- (3) NAT 技术 (源 NAT、服务器映射)。
- (4) 双机热备与虚拟防火墙。

三、考核知识点及要求

识记：DMZ 区的作用，防火墙的安全区域概念。

领会：NAT 转换表的工作逻辑，包过滤规则的匹配顺序。

应用：编写防火墙 ACL 规则（如禁止特定 IP 访问 Web 服务），配置端口映射。

第九章 入侵防御系统

一、学习目的与要求

通过本章学习，学生应能够区分防火墙、IDS 与 IPS 的功能差异，掌握入侵防御系统的工作过程与部署方式。

二、课程内容

(1) 入侵检测与防御机制。

(2) 网络 IPS 与主机 IPS 的结构。

(3) Snort 系统的基本概念。三、考核知识点及要求

识记：误报与漏报的概念，IPS 的在线部署模式。

领会：基于特征（签名）检测与基于异常检测的区别。

应用：分析简单的入侵检测日志，识别攻击类型。

第十章 网络数据库安全与备份技术

一、学习目的与要求

通过本章学习，学生应能够了解数据库面临的安全威胁及防护模型，掌握主流数据库（Oracle/SQL Server）的安全配置与备份恢复。

二、课程内容

(1) 自主访问控制与强制访问控制。

(2) SQL 注入漏洞原理（结合第 1 章）。

(3) 数据库身份验证、审计与备份技术。三、考核知识点及要求

识记：数据库最小权限原则，全量备份与增量备份的区别。

领会：SQL 注入攻击对数据库安全的危害。

应用：制定数据库备份策略，进行基本的数据库用户权限设置。

第十一章 网络空间信息安全实验及实训

一、学习目的与要求

本章为综合实践章节，要求将前 10 章的理论知识转化为实际操作技能，重点考核学生对安全工具的熟练度及故障排查能力。

二、课程内容

(1) 网络 ARP 病毒分析与防治实验。

(2) 网络端口扫描实验（使用 Nmap 等工具）。

- (3) 网络信息加解密与数字签名实验。
- (4) Windows SSL 配置与防火墙配置实验。
- (5) Snort 安装与配置实验。

三、考核知识点及要求

综合应用：

- 1 能够搭建实验环境，演示 ARP 欺骗并实施防御。
- 2 能够使用端口扫描工具探测目标主机开放的服务。
- 3 能够配置主机或网络防火墙规则以阻断特定流量。
- 4 能够对敏感文件进行加密传输。

三、参考教材与考核实施要求

(一) 本课程使用的参考书

《网络空间信息安全（第2版）》，苏永红、蒋天发 著，电子工业出版社，2022 年第 2 版。

(二) 本课程的考试要求

- 1 考察基础理论掌握：要求学生识记网络安全的基本概念、协议原理及法律法规。
- 2 考察技术应用能力：重点考察对防火墙、杀毒软件、加密工具的配置与使用，以及对网络流量的分析能力。
- 3 考察综合分析能力：能够针对给定的网络场景（如企业内网被攻击），分析原因并提出完整的安全解决方案。
- 4 考察实战操作逻辑：在非上机考试环境下，通过书写命令、配置步骤或分析截图来考核实际操作流程。。

(三) 关于本课程考试命题的若干规定

1. 本门课程采用闭卷考试，时间为 150 分钟。根据本课程考试所提供的环境条件，携带必要的创作工具（如画具、纸张）等。

2. 本大纲各章所规定的基本要求，知识点及知识点下的知识细目，都属于考核的内容。考试命题既要覆盖到章，又要避免面面俱到。要注意突出课程的重点、章节重点，加大重点内容的覆盖度。

3. 命题不应有超出大纲中考核知识点范围的题，考核目标不得高于大纲中所规定的相应的最高能力层次要求。命题应着重考核自学者对基本概念、基本知识和基本理论是否了解或掌握，对基本创作实践方法是否会用或熟练。不应出与基本要求不符的偏题或怪题。

4. 本课程在试卷中对不同能力层次要求的分数比例大致为：识记占 10%，领

会占 10%，简单应用占 20%，综合应用占 60%。

6. 本门课程考试可选用的命题题型范围为单项选择题、多项选择题、判断题、简答题、综合应用题等题型。