《网络空间安全技术》复习提纲 2023

考试题型：

一、选择题 15 题单项选择题（1 分/题，共 15 分）

二、判断题 10 题（1 分/题，共 10 分，错误的打 ×， 正确的打 ✓ ）

三、综合应用分析题 (共 6 题，共 75 分)

1. 网络安全概论

- 网络安全的基本目标：保密性、完整性、可用性、不可抵赖性和可控性， 清楚每个安全目标的含义以及为了达到该安全目标所能采取的措施。
- CIA 安全模型，保密性、完整性、可用性，CIA 三元组
- P2DR 模型的组成（哪个是核心，哪些是要素）

2. 局域网攻击与防御技术

- 网络攻击的分类：主动攻击和被动攻击， 主动攻击和被动攻击的定义，主动攻击有哪些类型，被动攻击有哪些类型?
- 窃听攻击的原理：集线器窃听、MAC 表溢出攻击原理、交换机端口镜像攻击原理及其相应的防御技术
- 截获攻击的原理：MAC 地址欺骗攻击的原理、DHCP 欺骗攻击的原理、ARP 欺骗攻击的原理、生成树欺骗攻击的原理及其各自的防御技术
- 欺骗攻击原理：源 IP 地址欺骗攻击原理、 钓鱼网站实施原理和防御机制

1. Web 攻击

（1）Web 攻击的类型与防范措施

（2）SQL 注入的原理、发生的原因、导致的结果、闭合语句、万能密码、注入类型、安全防范【数据与代码分离】、SQL 注入过程中使用的函数【结合实验】

（3）XSS、CSRF 攻击原理、导致的结果

（4）Cookie 和 Session

2. 防火墙

（1） 防火墙类型、部署位置、安全策略与规则配置、功能【结合实验】

（2） 动态包过滤防火墙的工作原理、缺点，防范作用

（3） 应用级防火墙（WAF）的原理

3. 恶意代码

（1） 恶意代码的类型、特点、危害、生命周期

（2） 木马病毒的特点、危害及典型木马名称

（3） 勒索病毒的特点、危害及典型病毒名称

（4） 蠕虫病毒的特点、危害及典型蠕虫名称

【高老师部分】

1. 互联网安全技术

（1） 路由项欺骗攻击、拒绝服务攻击原理
（2） 安全路由原理
（3） 流量管制算法原理
（4） NAT 原理
（5） VRRP 原理

2. 虚拟专用网络技术

（1） VPN 概述基础知识
（2） 第三层隧道和 IPSec 结构与原理（除协议、安全关联等具体步骤）
（3） 第二层隧道和 IPSec 结构与原理（除协议、安全关联等具体步骤）
（4） SSL VPN 结构与原理
（5） 各类 VPN 的区别、优缺点

3. 入侵检测技术

（1） IDS 定义、特点、与防火墙差异
（2） IDS 通用框架
（3） IDS 类型（异常检测和误用检测）

（4） IDS 应用方式

4. 安全技术基础-密码算法

（1） 密码算法的安全性和现代密码学原则

（2） 密码算法的分类和典型代表算法

（3） 典型代表算法实现原理和特点

5. 安全技术基础-认证技术

（1） 消息认证的含义

（2） 消息认证的各种方案实现原理

（3） 消息认证各方案的优缺点和解决方案

6. 无线局域网安全技术

（1） 无线局域网的特点和问题

（2） 无线局域网 WEP 协议的原理和优缺点

（3） 无线局域网 TKIP 和 CCMP 协议的原理和优缺点

7. 网络安全协议

（1） 网络安全协议的分类

（2） 网络安全协议 IPSEC、SSL 的原理和实现方式

8. 网络攻击

（1） 主动攻击、被动攻击概念

（2） 嗅探攻击原理

（3） 截获攻击原理

（4） 拒绝服务攻击原理

（5） 欺骗攻击原理

9. 以太网安全技术（结合攻击、如何防御）

（1） 以太网接入控制技术原理、功能

（2） 防欺骗攻击机制原理、功能

（3） 生成树欺骗攻击与防御机制原理、功能

（4） 虚拟局域网原理、功能