

---

# 信息安全攻防技术

## 一、 课程背景

近年来，我国互联网蓬勃发展，网络规模不断扩大，网络应用水平不断提高，成为推动经济发展和社会进步的巨大力量。与此同时，网络和业务发展过程中也出现了许多新情况、新问题、新挑战，尤其是当前网络安全问题频发、网络安全立法系统性不强、及时性不够和立法规格不高，物联网、云计算、大数据等新技术新应用、数据和用户信息泄露等的网络安全问题日益突出。未来，我国将不断加强网络安全依法管理、科学管理，更加重视新技术新应用安全问题，促进移动互联网应用生态环境优化，加速构建网络安全保障体系，推动网络安全相关技术和产业快速发展。

本课程通过教师讲解、案例分析、小组讨论、互动等授课方式，给学员系统的讲解信息安全知识，带来全面的认识和思考，让信息安全技术的学习变得妙趣横生。整个课程主要先让大家认识什么是信息和信息安全，网络攻击的方法，并了解网络安全技术的起源和发展现状、目前的最新研究成果等，再由网络攻击过渡到现实生活中企业如何在系统开发阶段就加入安全要素，使学员深刻理解软件安全的现实运用。然后讲解攻防技术新进展。

课程将通过大量的案例分析，介绍国内外对于网络安全这门技术的应用和深入情况，使学员在理解了网络安全这一概念后思维能够从理论性的阐述中逐渐联系实际应用，以此全面了解网络安全，使之贴合，做到理论和实际能紧密联系，有效运用。

## 二、 课程特点

授课形式：理论讲解+案例分析+小组讨论+互动答疑

突出理论特点，注重知识理解、案例分析与小组讨论，其中理论讲解 60%，案例分析 30%，讨论 10%。

## 三、 课程收益

1. 详细了解信息安全、网络安全的概念和体系。
2. 详细了解网络攻击方法。
3. 详细了解网络攻击防御技术。
4. 详细了解软件安全和恶意软件安全。
5. 掌握网络安全的最新研究成果及未来应用的领域，以及可能出现的新技术和产品。
6. 具备从网络空间安全视角看待行业未来的发展的能力，理解网络空间安全在行业运用中的关键。

## 四、 课程模式

1. 中文教学、面授
2. 理论讲解
3. 案例分析

- 
4. 互动式答疑

## 五、 受众对象

1. IT 行业人员
2. 管理支持组织中复杂工作、重要工作的人员
3. 希望提升自身职业能力的人员、其他对网络安全感兴趣的人员

## 六、 时间安排

系统学习 2 天 (12 小时)

## 七、 授课教师

芦效峰，北京邮电大学网络空间安全学院副教授，软件安全中心副主任  
EXIN 认证云计算专家，微软认证专家，CCNA 讲师

## 八、 课程内容

---

# 信息安全攻防技术

## 第一章 信息安全基础

本节要点：介绍信息安全知识架构，时长 3 小时

### 1. 信息安全

- ◆ 信息与信息系统
- ◆ 信息安全
- ◆ 网络安全
- ◆ 安全威胁

### 2. OSI 安全体系

- ◆ 安全服务
- ◆ 安全技术
- ◆ 安全模型

### 3. 密码技术

- ◆ 对称加密
- ◆ 非对称加密
- ◆ 密码的管理和分配
- ◆ 数字证书
- ◆ 数字签名
- ◆ DES 和 RSA 混合加密

## 第二章 网络攻击技术

本节要点：网络攻击的方法，时长 4 小时

### 1. 网络攻击基础

- ◆ 攻击分类
- ◆ 攻击流程
- ◆ 攻击目的

### 2. 数据链路层攻击技术

- ◆ MAC 地址欺骗
- ◆ 网络监听

### 3. 网络层攻击技术

- ◆ 网络层扫描
- ◆ IP 欺骗攻击
- ◆ ICMP 攻击
- ◆ 路由欺骗
- ◆ ARP 欺骗

### 4. 传输层攻击技术

- ◆ 端口扫描
- ◆ TCP 序号预测
- ◆ SYN 泛洪

- 
- ◆ TCP 欺骗
  - 5. **应用层攻击**
    - ◆ SQL 注入
    - ◆ DNS 欺骗
    - ◆ 口令攻击
  - 6. **拒绝服务攻击**
    - ◆ DDOS

## 第三章 网络安全防御技术

本节要点：网络攻击防御的方法，时长 3 小时

1. **防火墙**
  - ◆ 防火墙概述
  - ◆ 防火墙技术
  - ◆ 防火墙的体系结构
2. **入侵检测技术**
  - ◆ 入侵检测系统概述
  - ◆ 入侵检测系统的分类及技术
  - ◆ 入侵检测系统的实施
3. **VPN**
  - ◆ 概念
  - ◆ 功能
  - ◆ 隧道技术
  - ◆ VPN 类型
  - ◆ 网络层 VPN：IPsec
  - ◆ 应用层 VPN：SSL

## 第四章 软件安全在企业中的应用

本节要点：软件安全在 IT 行业信息系统的应用，时长 3 小时

1. **软件安全技术如何在企业应用**
  - ◆ 软件开发模型
  - ◆ 威胁模型
  - ◆ 软件安全设计原则
  - ◆ 微软安全开发模型
2. **恶意软件**
  - ◆ 病毒
  - ◆ 木马
  - ◆ 蠕虫
  - ◆ 僵尸

## 第五章 攻防技术新进展

本节要点：物联网安全及对互联网安全的影响，时长 1 小时

---

## 1. 物联网安全

- ◆ 智能家庭漏洞
- ◆ 智慧医疗攻击缺陷
- ◆ 智慧设备的攻击点等
- ◆ 智能家居、工业控制系统、车联网等新兴技术产业面临严峻网络安全威胁

## 课程总结