

# 网络攻击与防范

---

国家计算机网络入侵防范中心

中国科学院大学

张玉清

**zhangyq@nipc.org.cn**

# □ 课前情况介绍

---

- 开设本课的目的与要求
- 主要教学内容
- 主讲教师介绍
- 课程安排
- 攻防实验介绍
- 教学&参考资料
- 选课情况
- 交流渠道



# 开设本课的目的

---

- 全面介绍网络攻击与防御技术的背景、基本原理和实际应用
  - 从理论和实践两个方面对网络攻击和防御技术这两个问题进行系统阐述
  - 对网络攻击技术有较全面的了解，并具备对各种常见网络攻击进行基本防御的能力
  - 解读网络攻防的前沿技术和热点网络安全事件

# 教学要求

---

- 先修课程：计算机网络，计算机编程语言
- 选课对象：计算机、网络空间安全等专业硕士、博士研究生或信息安全爱好者
- 本课程为网络空间安全学科研究生的专业核心课。本课程将系统化讲授网络攻防技术的基本原理、方法和关键技术，并将对网络攻防的前沿技术和热点网络安全事件进行细粒度研讨，同时通过相关实验加强理解。通过本课程的学习，使学生系统掌握网络攻防技术，探讨个人兴趣点和特长所在，为进一步深入研究信息安全和定位研究方向打好基础。

# 教学内容

---

## □ 一、概论（**3学时**），授课教师：张玉清

- 网络攻击与黑客、网络安全基础知识、网络安全的威胁与根源、网络攻击的原理及过程、国内外现状与趋势、近年来重大网络安全事件

## □ 二、网络攻防基础（**27学时**），授课教师：张玉清

- 常见的网络攻击及其防范技术：安全扫描、口令破解、网络监听、欺骗攻击、拒绝服务、缓存区溢出、木马、Web攻击、病毒与蠕虫等典型网络攻击及其防范技术
- 典型的防范技术 防范技术概述、防火墙、入侵检测系统（IDS）、日志审计、蜜罐等
- 攻防基础实验

# 教学内容

---

## □ 三、网络攻击高级技术与前沿技术（**30学时**）

- 逆向工程与恶意代码分析 (**5学时**)，龚晓锐（讲逆向分析基础知识和常规工具使用，案例分析）
- 漏洞原理分析及利用(**6学时**)，张玉清（讲几类常见漏洞的产生机理，漏洞挖掘与利用方法的原理）
- 网络安全竞赛与实践（**4学时**），龚晓锐（用**1学时**讲竞赛知识，**3学时**做解题报告）
- 网络战与**APT**攻击（**3学时**），吴槟
- 社会工程与网络钓鱼（**3学时**），吴槟
- 后门利用、隐信道、僵木蠕与勒索软件（**4学时**），吴槟
- 人工智能与网络安全(**4学时**)，张玉清
- 网络系统安全国际顶级会议**TOP4**介绍（**1学时**），张玉清

# 主讲教师自我介绍

---

## □ 张玉清

- 国科大 计算机学院 教授、博导
- 国家计算机网络入侵防范中心 主任
- 学科：网络与系统安全，计算机网络

## □ 国家计算机网络入侵防范中心

- 主页：<http://www.nipc.org.cn>

# 主要研究领域

---

- 网络攻防
- 网络与系统安全
- 漏洞挖掘与利用
- 物联网安全
- 人工智能与安全
- 智能手机安全



# 主讲教师自我介绍

---

- ❑ 发表论文100余篇，有ACM CCS、USENIX SECURITY、IEEE S&P、NDSS、IEEE Trans. (TPDS)、IEEE Trans. (TCC)、INFOCOM等
- ❑ 制定国家及行业标准7个，中国的CVE国家标准、CERT第一个国家标准
- ❑ 先后承担国家重点研发计划项目、国家自然科学基金重点项目、国家发改委信息安全专项、国家高科技发展计划（863）项目、中国科学院知识创新工程重要方向项目、国家242信息安全计划项目等课题
- ❑ 任高校教师20多年





2022/2/23

# 主讲教师介绍 龚晓锐

---

- ❑ 男，中科院信工所，正高级工程师，硕士生导师
- ❑ 主要围绕网络攻防、软件逆向分析、恶意代码对抗等方向开展研究
- ❑ 主持或参与国家保密局重点项目、中国科学院先导专项、国家重点研发计划、北京市科技计划等项目，国家关键信息基础设施网络攻防实战演习裁判长
- ❑ 创建并指导的**NeSE**战队是国内**CTF**社区中的一线战队，近**2**年在国际大赛中保持全球前**20**的成绩
- ❑ 在教学、授课方面具有较好的经验



# 主讲教师介绍 吴槟

---

- 男，博士，副研究员，中科院信工所信息安全国家重点实验室
- 先后主持了国家自然科学基金项目、发改委信息安全专项工程子系统研制项目、中科院先导专项子课题等**10**余项；担任国家自然科学基金联合基金重点项目联合单位主持人、国家**863**计划项目副组长
- 申请发明专利**7**项，获得专利授权**2**项，发表论文**5**篇
- 在教学、授课方面具有较好的经验

# 课程安排

---

- 学时：**60**
- 学分：**3**
- 内容：课堂讲授 + 攻防实验
- 考核方式：笔试（闭卷，**40**分）+ 实验（**60**分）

# 攻防实验介绍

---

## □ 实验一 网络监听实验

- 文件安全传输系统设计与分析 or 嗅探器实验
- 网络监听章节后

## □ 实验二 缓冲区溢出漏洞攻击

- DNSTracer 缓冲区溢出攻击 or CCProxy代理服务器缓冲区溢出攻击
- 缓冲区溢出攻击章节后

# 教学&参考资料

---

## □ 教材

- 课堂讲义为主，附之以文献阅读

## □ 参考教材

- 张玉清等编著，网络攻击与防御技术实验教程，清华大学出版社，2010.7
- 张玉清等编著，网络攻击与防御技术，清华大学出版社，2011.1



# 交流渠道

---

- 教师：张玉清    **zhangyq@ucas.ac.cn**  
          龚晓锐    **gongxiaorui@iie.ac.cn**  
          吴  槟    **wubin@iie.ac.cn**
- 助教：杨毅宇    **yangyy@nipc.org.cn**  
          贺凡女    **hefn@nipc.org.cn**
  
- 课程网站： **http://www2.ucas.ac.cn**
- 上课教室：周二晚上**9-11**节课，教**1-208**，**1-20**周
- **2月22日（周二）**
- 微信群：交流攻防技术，讨论攻防实验

---

预祝学习成功！  
谢谢！

**Email: zhangyq@ucas.ac.cn**