致理书院暑期基础学科交叉实践课程项目申请表

<table>
<tr><td>姓 名</td><td>段海新</td><td>性别</td><td>男</td><td>院系</td><td>网研院</td></tr>
<tr><td>主要科研方向和成果</td><td colspan="5">段海新博士，清华大学网络研究院长聘教授，国务院学位委员会第八届学科评议组成员，清华大学-奇安信集团联合研究中心主任。从事网络空间安全教学科研二十多年，带领团队发现了互联网基础协议的重要安全漏洞，促使谷歌、微软、亚马逊、华为、BAT 等公司多次升级安全产品，促使 IETF 等国际标准化组织多次修改协议，提高了互联网协议的安全性。多项研究成果发表在网络安全国际顶级的安全学术会议上，并多次获得国际网络安全顶级会议最佳论文奖，在国内外学术和工业界具有较高的影响力。</td></tr>
<tr><td>课程题目</td><td colspan="5">《网络安全攻防实践》</td></tr>
<tr><td>教学团队介绍
（请附上团队每位老师照片）</td><td colspan="5">责任教师：段海新教授
 
段海新教授 2016 年获中央网信办首届“网络安全优秀人才”奖，世界知名网络攻防战队“蓝莲花”的联合创始人，网络安全研究国际学术论坛（InForSec）的联合发起人，网络空间安全协会理事，中国密码学会协议专委会委员，互联网协会安全专委会委员，多次受邀担任 NDSS 等国际安全领域顶级学术会议的程序委员和 Transaction on Privacy and Security 等著名国际期刊的副主编。
段海新教授在网络安全领域有近 20 年的教学经验，曾先后承担清华大学计算机系、网络研究院和信息学院三门网络安全相关的课程教学工作，获学生好评，2020 年获评清华大学第十七届“良师益友”。带领学生多次参加网络安全相关的竞赛，多次获得 GeekPwn 等网络安全竞赛大奖，组织发起的“蓝莲花”战队曾获世界网络安全攻防竞赛第二名。</td></tr>
</table>

	合讲教师：刘保君博士  刘保君博士目前担任清华大学网络研究院助理教授/特聘研究员、博士生导师，入选清华大学 2020 年“水木学者”计划，获得 ACM 中国计算机安全分会 2022 年度“科技新星奖”，担任国际互联网治理领域权威机构 ICANN 根域名服务器咨询委员会核心专家组成员。近年来累计于网络安全领域四大顶级学术会议发表论文 17 篇，在国内外青年学者之中名列前茅。学术研究成果获得互联网研究任务组与国际互联网协会颁发的 2020 年网络研究应用奖、网络安全领域顶会 NDSS 2019 最佳论文奖、网络可靠系统领域顶会 DSN 2020 最佳论文奖，网络测量领域顶会 IMC 2019 最佳论文奖与社区贡献奖提名。作为项目负责人主持十四五装备预研项目、国家自然科学基金青年项目、泉城实验室重大科研项目及阿里巴巴创新研究计划 AIR 项目。
课程对学生的先修要求	建议选课学生应当同时具备以下两方面条件： （1）具有一定的计算机编程能力，熟悉 C/C++，可随堂学习 Python 语言 （2）熟悉 Linux 或 MacOS 操作系统，了解常见命令行工具的使用方法

课程设计	教学资源或设备： （1）网络研究院提供在线的实验环境作为课程平台； （2）教室内由课程助教搭建专用 Wi-Fi 网络环境； （3）上课时学生必须携带笔记本电脑，安装最新版本 Firefox 浏览器。 目标和特色：以攻防对抗实战的形式，学习网络空间安全技术。 网络空间安全学科的本质是人在网络空间中的攻防对抗。本课程通过课堂实验，让学生在网络攻防对抗实战中，掌握网络安全的基本知识和技能，激发学生对网络安全研究的兴趣。
课程方案	**总体设计：** 网络空间安全学科具有极强的实践特点。为了更好的理解网络安全知识，掌握网络攻击原理，本课程精心设计了多组网络安全实验。通过鼓励学生动手实践，提高学生网络攻击与防御的实战能力。 课程实验涵盖了局域网网络流量嗅探、域名缓存污染攻击、Web 系统漏洞利用以及网络渗透等多类典型攻防场景，有利于培养本科生同学对于网络空间安全的兴趣。 **课程实施步骤：** 每次课程均分包括两个部分：一，教师讲解网络安全知识与原理；二，学术组队利用课程平台，动手完成相应的实验。 **课程大纲：** **第一课：课程概要（1 学时）** （1）介绍课程目的、主要课程内容以及考核要求。 （2）介绍实验平台、基本操作方法和常用工具。 **第二课：搭建一个基本的企业网络（2 学时）** （1）教师介绍基础知识 计算机网络工作原理，包括 TCP/IP 协议和局域网设备的工作原理、常见的网络服务和网络应用协议，网络分析工具的配置和使用方法，基本的网络故障分析知识。 （2）学生实践操作 在实验平台中搭建一个基本的企业网络，包括路由器、交换机、域名服务器、DHCP 服务器、Web 服务器等，并配置公钥证书。在此过程中，理解网络故障分析方法。

	第三课：局域网安全与情报收集（3 学时） （1）教师介绍基础知识 局域网环境常见攻击方法和防范措施的技术原理，包括 ARP 攻防和 DHCP 攻防基础；介绍端口扫描等网络资产探查原理。 （2）学生实践操作 学生基于上节课搭建的企业网络，构造 ARP 欺骗或 DHCP 欺骗，实现中间人攻击；利用端口扫描等工具，发现局域网环境中其它队伍搭建的网络服务以及潜在的安全漏洞； **第四课：网络流量分析与密码破解（3 学时）** （1）教师介绍基础知识 介绍网络流量分析技术原理，Tcpdump 以及 Wireshark 等常见的流量分析工具；介绍几种常见的网络协议、常用密码算法及其破解原理。 （2）学生实践操作 学生使用 Tcpdump 或 Wireshark 捕获网络流量，分析 HTTP、电子邮件等协议交互过程；分析企业网络环境中流量数据，提取流量中敏感密码字段，并使用相应的密码破解工具和口令字典对密码进行破解。 **第五课：防火墙以及入侵检测系统（3 学时）** （1）教师介绍基础知识 介绍常用的防火墙以及入侵检测系统的基本工作原理，介绍常见的逃逸安全检测原理； （2）学生实践操作 学生熟悉防火墙配置规则，配置特定场景的安全防范策略；学生使用开源的入侵检测系统，检测特定的网络攻击事件。 **第六课：域名系统（DNS）典型攻击与防范（3 学时）** （1）教师介绍基础知识 介绍 DNS 系统的工作原理、系统结构、权威服务器、递归解析服务器等原理；介绍常见 DNS 攻击和防范措施；介绍 DNS 相关工具的基本操作。 （2）学生实践操作 学生自主搭建配置 DNS 权威服务体系，配置 DNS 递归解析服务，实现从根、顶级域到二级域名的完整 DNS 解析过程。在实验环境中编程实现 DNS 链路注入攻击、DNS 缓存污染攻击，劫持域名访问流量；为域名权威服务器配置 DNSSEC 签名记录，为 DNS 递归解析服务开启 DNSSEC 验证功能，解决域名缓存污染攻击问题。

	第七课：Web 安全典型攻击与防范（3 学时） （1）教师介绍基础知识 Web 基础知识，包括 HTML，Javascript，SQL 等；Web 安全领域常见的攻击方式，如 SQL 注入、跨站脚本攻击、服务器端请求伪造、文件上传漏洞；Web 安全领域常见的防御方法， （2）学生实践操作 学生基于开源软件搭建 Web 漏洞测试网站；完成搭建网站上的 Web 安全实验，包括 XSS、SQL 注入、跨站请求伪造（CSRF）等。基于开源软件搭建内容分发网络和 WAF（Web 应用防火墙），防御特定类型攻击。 **第八课： 典型 VPN 协议与基于流量的对抗分析（3 学时）** （1）教师介绍基础知识 介绍常见的 VPN 协议基本工作原理，介绍 VPN 协议工作流程中潜在的攻击面，以及典型的流量分析方法。 （2）学生实践操作 学生配置使用 L2TP、SSL VPN 和 WireGuard VPN；通过网络流量分析的形式，甄别 OpenVPN 网络流量，并对其进行阻断。 **第九课：电子邮件安全（3 学时）** （1）教师介绍基础知识 介绍电子邮件安全相关的基本原理，以及基本操作；介绍电子邮件典型的安全风险，包括邮件攻击方法；介绍电子邮件若干邮件安全扩展协议，分析安全防御措施。 （2）学生实践操作 学生基于开源软件，搭建自己的邮件服务器；编写脚本发送并接收电子邮件；伪装受害者的身份，发送钓鱼邮件；配置邮件服务器的安全机制，检测邮件发件人伪造现象，抵御邮件伪造攻击。 **第十课：网络渗透和安全竞赛 – 数据分析篇（3 学时）** （1）教师提供某模拟企业网络环境中的网络流量数据。学生在课堂内综合运用课程中的知识，编写程序分析网络流量，发现企业网络环境中的攻击行为。 **第十一课：网络渗透和安全竞赛 – 夺旗篇 CTF（5 学时）** （1）教师搭建夺旗赛实验环境。学生综合运用课程中的知识，在模拟环境中开展一次网络渗透测试和安全夺旗赛（CTF）竞赛。 **课程参考资料：**

	以教师提供的课程课件为主，课程中指定部分参考文献。 **课程考核设计：** （1）完成课堂布置的所有实验，提交实验报告：分值 50% （2）完成课程的网络渗透和安全竞赛，在课堂上分享经验：分值 30% （3）出勤与课堂展示：20% （4）课程互动：10%（加分项）