《网络安全》课程教学大纲

一、 课程基本信息

1. 课程代码：0320141240
2. 课程名称：网络安全
3. 课程英文名称：Cyber Security
4. 课程性质：必修课
5. 授课对象：2016 级网络工程专业（本科）
6. 开课单位：计算机科学与工程系
7. 先修课程：《计算机网络》，《网络互联技术（一）》，《网络互联技术（二）》
8. 学时安排：

学分	总学时	理论授课	实践教学
4	**64**	**52**	**12**

二、 教学目标

1. 教学目标的总体概括

随着计算机网络广泛应用，各种攻击日益频繁，网安事件日益增加，网安的重要性也日渐突出。国家富强民主需要更多网信人才，课程根据行业需求，重点培养学生对网络设备的安全部署从而掌握有效防御外部攻击的能力。通过走访相关公司、互联网信息查询调研当前计算机网络所面临的典型威胁以及综合防御策略，形成课程培养的知识目标和技能目标。

本课程主要讲授：网络安全基础知识、网络边界设备安全、二层攻击和防御、ACL 工作原理和防火墙配置、密码学基本概念和常见算法、VPN 的原理和解决方案、网络安全设计原则和安全网络运行方法。

通过本课程的学习，培养同学以下专业技能：

（1） 掌握网络病毒、网络攻击的基本类型，并能判断相应类型。

（2） 掌握针对外部网络攻击的防护方式，包括防火墙的设置、加密算法的应用等。

（3） 掌握针对内部网络攻击的防护方式，包括交换机、路由器等的基本安全设置等。

（4） 能够具备网络工程师的角色和责任，熟悉基本行业规范阅读、理解专业领域文献，拥有网络安全道德，培养专业学习的使命感、荣誉感。。

2. 教学目标列表

目标内容	能力指标	能力具体描述	掌握程度
理论知识	1.1 相关科学知识	理解网络运行过程及基础网络配置	理解/掌握
	1.2 专业基础知识	理解并掌握网络安全基础知识，掌握病毒攻击类型和防护方法	理解/掌握

专业技能	2.1 系统思维	全局把握网络安全防护的设计和部署	理解/掌握/运用
	2.4 创新能力	能根据网络漏洞和薄弱处制定相应的防护措施和加密算法	理解/掌握/运用
	3.1 推理和解决问题的能力	能有效定位攻击点，并及时作出反应	理解/掌握/运用
	3.2 实验和发现知识	能够根据验证型实验巩固理论知识	理解/掌握/运用
	4.2 使用外语能力	能熟练使用全英文的课件、作业及实验，能查看英文新技术能力	理解/掌握
个人素质	6.3 对职业的责任感	具备网络工程师的职业道德和责任感， 网络安全对于国家安全的重要性，强调专业知识在国防中的重要作用，培养专业学习更有使命感、荣誉感。	理解/掌握/运用

3．教学目标与课程内容映射图

见教学大纲管理平台中《网络安全课程培养目标与课程内容对应 Mapping 图》。

三、 各单元教学内容及基本要求

第一单元 安全威胁相关知识（4 学时）

1．教学内容

1.1 网络安全与国家安全

1.2 安全网络的原则，网络安全组织，网络安全领域，网络安全策略

1.3 病毒，蠕虫，特洛伊木马，消除他们的方法

1.4 侦查攻击，接入攻击，拒绝访问攻击，消除网络攻击

2．教学要求

2.1 掌握一个安全网络的基本原则

2.2 掌握病毒、蠕虫和特洛伊木马的特点和消除方法

2.3 掌握常见的攻击方式和消除攻击的方法

2.4 理解网络安全的重要性，了解大国间网络安全相关形势，理解国际信息新形势。树立网络安全既是国家安全的初步信念

3．教学重点与难点

3.1 拒绝服务攻击

3.2 消除网络攻击

第二单元 防止外部网络对内部网络攻击（32 学时）

1．教学内容

1.1 保护对设备的访问，配置 SSH

1.2 分配管理角色，控制和管理设备，使用 smtp 和 NTP

1.3 认证、授权和记账，本地 AAA 认证，基于服务器的 AAA，基于服务器的 AAA 认证，基于服务器的 AAA 授权和认证

1.4 访问控制列表，防火墙技术，基于上下文的访问控制 CBAC 防火墙，区域策略防火墙

1.5 IDS 和 IPS 的的特性

1.6 理解外部网络对于内部网络攻击防御在国家安全的重要性

2．教学要求

2.1 重点掌握保护边界路由器的配置和设置

2.2 了解 AAA 的特点和作用，掌握本地 AAA 认证和基于服务器的 AAA 的配置

2.5 通过基本和各种扩展 ACL 的讲解，熟悉和掌握 CBAC 防火墙和基于策略的防火墙的特点和配置

2.6 强调专业知识在国防中的重要作用，使专业学习更有使命感、荣誉感。并不断更新网安的新成果，阿里云发布云盾 Web 应用防火墙，启明星辰发布物联网安全接入防护系统 IoT-VBox，永信至诚推出 e 春秋网络安全实验室靶场平台，并利用该系统承办了多次大型网络安全竞赛等。

3．教学重点与难点

3.1 扩展 ACL

3.2 基于 ACL 的排错

3.3 CBAC 防火墙的策略和设置

3.4 基于区域防火墙的策略和设置

4．项目和实验

4.1 CCNAS_Chp2_ PTActA_Syslog-SSH-NTP

4.2 CCNAS_Chp3_PTActA _AAA

4.3 CCNAS_Chp4_PTActA_ACL

4.4 CCNAS_Chp4_PTActC_Zone_Based_Policy_Firewall

第三单元 局域网防护（8 学时）

1.教学内容

1.1 设置终端安全，第二层安全，MAC 地址欺骗攻击，MAC 地址表溢出攻击，STP 操纵攻击，LAN 风暴攻击，VLAN 攻击

1.2 配置端口安全，配置 BPDU 保护和跟保护，配置风暴控制，配置 VLAN 中继

1.3 无线安全考虑，VOIP 安全解决方案，SAN 安全解决方案。

2.教学要求

2.1 重点掌握二层安全的各种类型，理解各种攻击的原理。

2.2 掌握针对各种二层安全的配置，重点讲解端口安全和生成树的配置

2.3 了解无线、VOIP 和 SAN 安全的考虑和解决方案

2.4 树立学生正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。

3.教学重点与难点

3.1 VLAN 攻击

3.2 配置 VLAN 中继安全

3.3MAC 地址攻击和端口安全配置

3.4 STP 操作攻击和配置 BPDU 保护和根保护

4．项目和实验

4.1 CCNAS_Chp5_PTActA_IPS

4.2 CCNAS_Chp6_PTActA_L2-Security

4.3 CCNAS_Chp6_PTActB_L2-VLAN-Security

第四单元 加密和 VPN（12 学时）

1．教学内容

1.1 密码术和密码学，基本完整性和真实性，机密性，公钥密码术

1.2 VPN 的概述和拓扑，GRE VPN ,IPsec VPN 安全协议

1.3 因特网密钥交换，实现远程访问 VPN

2．教学要求

2.1 掌握完整性、真实性和机密性实现的原理和方法

2.2 掌握 VPN 的概念和 IPSEC 的组件

2.3 重点掌握站点到站点 IPSEC VPN 的配置，了解远程 VPN 设置的现实

2.4 让学生理解摆脱对国外技术和产品的过度依赖，建设行业网络安全环境，增强我国行业信息系统的“安全可控”能力，培养学生坚决维护国家出台的《关于清理规范互

联网网络接入服务市场的通知》，不私自使用不合法的 VPN，严格制止违法“翻墙”行为

3．教学重点与难点

3.1 完整性、真实性和机密性的实现

3.2 IPSEC 的协议和组件

3.3 站点到站点 IPSEC VPN 的配置

4．项目和实验

4.1 CCNAS_Chp8_PTActA_Site-to-Site-IPsec-VPN

第五单元 综合实验（8 学时）

3 级项目：Skills Integration Challenge

教学要求：具备一定的网络工程师职业行为，树立正确的职业态度。

四、 实践教学项目表

对应单元	项目名称	项目级别	项目类型	项目内容	成果物
2	边界路由器-SSH-系统日志	5 级	验证型	CCNAS_Chp2_ PTActA_Syslog-SSH-NTP	实验报告
4	基于区域的防火墙	5 级	验证型	Chp4_PTActC_Zone_Based_Policy_Firewall-	实验报告
6	二层安全	5 级	验证型	CCNAS_Chp6_PTActA_L2-Security	实验报告

五、 教学方法

1.任务驱动：通过查询互联网现有的典型威胁，驱动学生学习目前网络所面临的攻击分类和防御方法。

2.实践学习：通过理论课的讲解，让学生用实验和实践的方式，加深对理论学习的印象。

3.演示教学：利用 PPT、动画、抓包等方式，讲解有关网络安全的防护措施部署及防护效果。

六、 教学资源

1．参考教材

《CCNA 安全》，思科网络技术学院.北京：人民邮电出版社，2019 年 1 月

《网络安全》，沈鑫剡等.北京：清华大学出版社，2017 年 8 月

《网络安全技术及应用》，贾铁军等.北京：机械工业出版社，2017 年 5 月

2．参考资料

《在网络安全和信息化工作座谈会上的讲话》，习近平.北京：人民出版社，2016 年 4 月

《网络战争》，东鸟.北京：九州出版社，2009 年 5 月

《国家网络空间安全战略》，国家互联网信息办公室，2016 年 12 月

《中华人民共和国网络安全法》，中华人民共和国主席令（第五十三号）公布，2017 年 6 月施行

《“十三五”国家信息化规划》，国务院，2016 年 12 月

http://www.cnhonkerarmy.com/forum-4-1.html，红盟社区

https://www.icourse163.org/course/UESTC-235006，《计算机系统与网络安全技术》，中国大学 MOOC 在线课程

七、 课程考核

1．课程考核内容及总体安排

类别	考核项目	考核次数及主要标准	考核时间安排	所占权重
形成性考核	考勤	迟到早退旷课相应扣分	第 1-16 周	5%
	翻转课堂	分小组进行翻转课堂 5 分钟（讲解主题分为网络安全实事+网络安全新技术或者网安成果+网络安全道德三方面），共 3 次	第 1-16 周	10%
	项目实验	共 3 次，项目实验完整性、正确性	第 1-16 周	10%
	作业	共 4 次，独立完成性和正确性	第 1-16 周	10%
	综合项目	综合项目操作正确，答辩逻辑清晰，思路清晰	第 16 周	15%
终结性考核	期末考试	本课程所有教学内容	第 17 周	50%

2．终结性考核安排

（1）试卷考核安排

课程性质	☑必修课　　☐选修课	**考试时长**	120 分钟
组织形式	☑学院统一组织　　☐系部组织	**试卷满分**	百分制
考核方式	☑闭卷　☐开卷　☐机考　☐口试　☐ _____		

重点考核知识	基本概念 保护网络设备 认证授权记账 实现防火墙技术 执行入侵防御 保护局域网 密码系统	**教学大纲覆盖率**	大于 90%
试题类型	☑选择题 ☑名词解释 ☑简答题 ☑综合题 ☐ 判断题		

八、 大纲管理

大纲（模版）版本号：V3.2

大纲制定人签字： 制定日期：2019 年 月 日

团队审核人签字： 审核日期：2019 年 月 日

系部负责人签字： 审核日期：2019 年 月 日