

# 内蒙古农牧技师学院

## 网络安防系统安装与维护专业(全日制)

# 人才培养方案

专 业 名 称 :	网络安防系统安装与维护
专 业 代 码 :	0311
专 业 负 责 人 :	李洁璞
团 队 主 要 成 员 :	孙伟 张婷婷 张哲 张连连 赵楠
编 制 ( 修 订 ) 时 间 :	2024 年 12 月

# 目 录

一、专业信息 .....	1
(一) 专业名称 .....	1
(二) 专业编码 .....	1
(三) 学业年限 .....	1
(四) 就业方向 .....	1
(五) 职业资格/职业技能等级 .....	1
二、培养目标和要求 .....	1
(一) 培养目标 .....	1
(二) 培养要求 .....	2
三、培养模式 .....	4
(一) 培养体制 .....	4
(二) 运行机制 .....	4
四、课程安排 .....	4
(一) 课程设置 .....	4
(二) 教学安排 .....	5
五、 课程标准 .....	6
(一) 计算机网络系统搭建 .....	6
(二) 网络安全产品安装与调试 .....	8
(三) 基于等保的信息系统安全配置 .....	10
(四) 网络安全日常运维与监控 .....	12
(五) WEB 安全渗透测试 .....	14
六、实施建议 .....	16
(一) 师资队伍 .....	16
(二) 场地设备 .....	17
(三) 教学资源 .....	18
(四) 教学管理制度 .....	18

七、 考核与评价 .....	19
(一) 综合职业能力评价 .....	19
(二) 职业技能评价 .....	19
(三) 毕业生就业质量分析 .....	20

# 网络安防系统安装与维护专业人才培养方案

## 一、专业信息

### （一）专业名称

专业名称：网络安防系统安装与维护

### （二）专业编码

专业代码：0311

### （三）学业年限

全日制，学习年限为 3 年。

### （四）就业方向

网络安防系统安装与维护：面向信息技术行业，包括软件开发、网络架构设计、系统集成等。技术公司、互联网企业以及其他信息技术相关机构都需要网络应用人才来支持其业务。电信行业，电信公司是计算机网络应用人才的主要雇主之一。他们需要专业人员来设计和维护通信网络，确保用户能够稳定、高效地使用各种通信服务。金融行业，银行、保险公司和其他金融机构对网络的依赖性很高。网络应用人才在这个行业中负责保障金融交易的安全、稳定和高效进行。医疗行业，医疗信息技术的发展使得医疗机构需要网络应用人才来建设和维护医疗信息系统，确保医疗数据的安全和流畅的交流。制造业，现代制造业越来越依赖自动化和网络化生产流程。计算机网络应用人才在制造业中可以负责设计和管理工业网络，提高生产效率。政府机构，各级政府机构也需要网络应用人才来维护政府信息系统、提升网络安全水平，以更好地为公众提供服务。

### （五）职业资格/职业技能等级

HCIA(网络工程师助理) 、红帽认证

## 二、培养目标和要求

### （一）培养目标

网络工程师的培养目标主要包括掌握计算机网络的基本原理和技术，能够熟练地使用网络协议、网络设备和网络管理工具。具备计算机系统、网络系统和安全系统的基本知识，能够进行系统集成和系统优化。具备良好的沟通能力和团队协作能力，能够与其他专业人员合作开展网络工程项目。具备良好的学习能力和创新能力，能够不断学习和掌握最新的网络技术和安全技术。具备良好的服务意识

识和职业道德，能够为用户提供高质量的网络服务和技术支持。

## **(二) 培养要求**

### **1.素质**

1.1 具有良好的思想品德，良好的心理承受力；有良好的自信心、积极进取的精神。

1.2 具有努力拼搏的热情，阳光心态，能调节个人情绪的能力。

1.3 具有踏实肯干、吃苦耐劳和爱岗敬业的精神；

1.4 具有不断积极进取、超越自我的精神；

1.5 具有良好的团队协作精神。

### **2.知识**

2.1 计算机网络的基本原理

2.2 网络协议

2.3 网络设备的配置与管理

2.4 网络安全等方面的专业知识和技能。

### **3.能力**

#### **一、技术技能**

1.掌握计算机网络的基本原理和协议，熟悉各种网络设备的配置和管理。

2.了解网络安全的相关知识，掌握各种网络攻击和防御技术。

3.熟练掌握网络监控和诊断工具的使用，具备网络故障排除和恢复的能力。

4.具备服务器的安装、配置和管理能力，熟悉数据库的设计和管理。

5.熟练掌握网络编程语言和技术，能够进行网络应用程序的开发和维护。

#### **二、创新创业能力**

1.具备创新思维和创意能力，能够发现和解决网络系统设计和运维中的问题。

2.了解网络系统的发展趋势和未来发展方向，具备前瞻性思维。

3.能够独立开展网络项目，具备创业意识和创业能力。

#### **三、分析问题解决问题能力**

1.能够分析网络系统设计和运维中的问题，找出问题的根本原因。

2.具备解决网络系统问题的能力，能够提出有效的解决方案并加以实

施。

3. 能够对网络系统的性能进行评估和优化，提高网络系统的可靠性和稳定。

#### 四、信息技术应用能力

- 1.能够熟练使用办公自动化软件和网络管理工具。
- 2.掌握云计算、大数据等新技术的基本原理和应用方法。
3. 了解物联网和人工智能等新兴技术的发展趋势和应用场景。

#### 五、沟通表达能力

- 1.具备良好的口头和书面表达能力，能够清晰地传达自己的思想和观点。
- 2.具备良好的听取和理解能力，能够正确理解他人的意图和需求。
- 3.具备良好的团队协作和沟通能力，能够与其他专业人员合作开展网络工程项目。

#### 六、团队合作能力

- 1.具备良好的团队协作意识和精神，能够积极参与团队工作。
- 2.具备良好的团队协作能力，能够与团队成员合作完成工作任务。
- 3.具备解决团队内部矛盾和冲突的能力，能够维护团队的稳定和和谐。

#### 七、终身学习能力

- 1.具备自主学习和终身学习的意识和能力，能够不断更新自己的知识和技能。
- 2.能够关注最新的网络技术和发展动态，不断提高自己的专业水平。
- 3.能够参加相关的专业培训和认证，不断提升自己的职业技能。

### 三、培养模式

#### （一）培养体制

网络安防系统安装与维护专业的培养体制围绕岗位需求构建，以“岗课赛证融合”为核心，设置公共基础、专业核心等课程模块，采用理实一体化、项目驱动等教学模式，通过校内实训与校外实习分层递进培养实践能力。同时，以过程性考核和技能达标替代单一考试，并通过校企合作、订单培养保障就业。

该体制打破传统教学局限，将理论与实践深度结合，不仅让学生掌握网络组建、设备配置、故障排查等基础技能，还对接云计算、物联网等新兴技术，助力学生考取职业资格证书，实现“毕业即上岗”，为网络运维、系统集成等领域输送高素质技术技能人才。

#### （二）运行机制

围绕组织、资源、质量、反馈四大板块协同发力。通过专业建设委员会统筹管理，联合多部门协同推进，确保培养方向紧跟市场；从师资、硬件、资金多方面提供资源保障，为教学活动筑牢根基。

同时，构建“学校 - 企业 - 学生”三方质量监控体系，及时发现并解决教学问题；建立动态反馈闭环，依据就业数据与企业需求优化培养方案，形成“规划 - 实施 - 监控 - 改进”的完整链条，推动专业培养持续契合行业发展需求。

### 四、课程安排

#### （一）课程设置

课程类别	课程名称
公共基础课程	思想政治
	语文
	历史
	数学
	英语
	数字技术应用
	体育与健康
	美育
	劳动教育
	通用职业素质
	其他
	计算机网络技术
	信息网络布线

专业基础课程	数据库技术应用
	计算机程序设计
	网页设计与制作
	网络安全法律法规
工学一体化课程	计算机网络系统搭建
	网络安全产品安装与调试
	基于等保的信息系统安全配置
	网络安全日常运维与监控
	WEB 安全渗透测试
	网络安全产品部署与配置
	网络安全评估与加固
	网络安全综合运维管理
	网络安全综合渗透测试
	网络安全代码审计
	网络安全漏洞挖掘
	网络安全事件分析与应急响应
	网络安全项目方案设计
选修课程	云计算基础与应用
	大数据基础与应用
	物联网技术基础
	人工智能基础与应用
	技师综合实践与毕业设计指导

## (二) 教学安排

课程类别	课程名称	参考学时	学期					
			第 1 学期	第 2 学期	第 3 学期	第 4 学期	第 5 学期	第 6 学期
公共基础课程	思想政治	144	√	√	√	√		
	语文	198	√	√	√			
	历史	72	√	√				
	数学	90	√	√				
	英语	90			√	√		
	数字技术应用	72	√	√				
	体育与健康	108	√	√	√	√	√	
	美育	18	√					
	劳动教育	48	√	√	√	√		
	通用职业素质	90		√	√	√		
	其他	18	√	√	√			



课程类别	课程名称	参考学时	学期					
			第 1 学期	第 2 学期	第 3 学期	第 4 学期	第 5 学期	第 6 学期
专业基础课程	计算机网络技术	144	√					
	信息网络布线	72		√				
	计算机程序设计	144			√			
	数据库技术应用	72				√		
	网页设计与制作	108					√	
	网络安全法律法规	36					√	
工学一体化课程	计算机网络系统搭建	324	√	√				
	网络安全产品安装与调试	144			√			
	基于等保的信息系统安全配置	252				√		
	网络安全日常运维与监控	144					√	
	WEB 安全渗透测试	144					√	
选修课	云计算基础与应用	72				√		
	大数据基础与应用	72					√	
机动		324	√	√	√	√	√	
岗位实习		600						√
总学时		3 600	√	√	√	√	√	√

## 五、课程标准

### （一）计算机网络系统搭建

工学一体化课程名称	计算机网络系统搭建	基准学时	324
-----------	-----------	------	-----

#### 典型工作任务描述

为中小型企业或校园网络系统的规划、搭建与调试。要求学生依据用户需求，完成网络拓扑结构设计，选取合适的网络设备（如交换机、路由器、防火墙等），进行设备硬件连接与软件配置，实现局域网内计算机互联互通、Internet 接入及基础网络服务（如 DHCP、DNS）部署。同时，需对搭建后的网络系统进行测试，排查网络故障，确保网络稳定运行，满足用户日常数据传输、资源共享等需求，培养学生符合网络安全领域岗位要求的系统搭建实操能力。

#### 工作内容分析

工作内容涵盖需求调研与方案设计，需收集用户网络规模、功能需求等信息，绘制网络拓扑图并制定设备选型方案；设备安装与连接，包括交换机、路由器等硬件设备的物理安装，

---

以及网线制作、设备间线路连接；设备配置与调试，通过命令行或图形界面配置设备 IP 地址、VLAN、路由协议等，实现网络通信；网络服务部署，搭建 DHCP 服务器分配 IP 地址、DNS 服务器解析域名；网络测试与故障排查，使用 ping、tracert 等工具测试网络连通性，定位并解决设备配置错误、线路故障等问题，最终提交网络搭建报告。

---

### 课程目标

---

1. 知识目标：掌握计算机网络基础理论（如 TCP/IP 协议、VLAN 技术）、网络设备工作原理，熟悉网络拓扑设计方法及常用网络服务（DHCP、DNS）的实现原理。
  2. 技能目标：能独立完成网线制作与测试，熟练进行交换机、路由器的基本配置与调试，具备中小型网络拓扑设计、设备选型及系统搭建能力，能运用工具排查常见网络故障
  3. 素养目标：培养严谨的工作态度与团队协作精神，树立网络安全意识，遵守网络搭建规范，提升问题分析与解决能力，适应网络安防岗位工作需求。
- 

### 学习内容

---

1. 理论知识：计算机网络体系结构（OSI/RM、TCP/IP 模型）、常用网络协议（IP、ARP、ICMP、HTTP）、VLAN 划分与 trunk 技术、路由协议（静态路由、RIP、OSPF）、网络安全基础（防火墙基本原理）、网络服务（DHCP、DNS）工作机制。
  2. 实操技能：网线（直通线、交叉线）制作与测试，交换机 VLAN 配置、端口聚合，路由器静态路由与动态路由配置，DHCP 服务器搭建与地址分配，DNS 服务器配置与域名解析，网络连通性测试（ping、tracert）及故障排查（设备配置错误、线路故障）。
- 

### 参考性学习任务

---

任务一：家庭局域网搭建：为模拟家庭环境设计简单网络拓扑，制作网线连接路由器与两台计算机，配置路由器实现 Internet 接入，测试两台计算机间文件共享及上网功能，提交搭建过程记录与测试报告。

任务二：中小型企业网络搭建：针对 10 - 20 台计算机的企业需求，设计含 VLAN 的网络拓扑，选取交换机、路由器，完成 VLAN 划分、路由配置，搭建 DHCP 服务器分配 IP，测试不同 VLAN 间计算机通信及 Internet 访问，排查可能出现的路由配置错误、VLAN 不通等故障。

任务三：网络故障排查实战：给定已搭建但存在故障的网络环境（如无法上网、部分计算机无法通信），使用测试工具定位故障点（如路由器网关配置错误、网线故障），记录排查过程并解决故障，恢复网络正常运行。

---

### 教学实施建议

---

1. 教学模式：采用“项目导向、任务驱动”教学模式，将学习内容融入具体项目任务，以学生为主体，教师引导学生完成任务，实现“做中学、学中做”。
2. 教学方法：结合理论讲授、案例分析、实操演示、小组协作等方法。理论课利用多媒体讲解网络原理与配置命令，实操课在网络实验室进行设备配置演练，小组协作完成复杂网络搭建任务，培养团队能力。
3. 资源利用：借助网络仿真软件（如 Packet Tracer）辅助教学，让学生在虚拟环境中预演配置操作；引入企业真实网络搭建案例，邀请企业工程师开展专题讲座，提升教学针对性与实用性。
4. 进度安排：总课时 64 学时，理论 24 学时、实操 40 学时，其中基础理论学习 8 学时，网线制作与设备连接 6 学时，设备配置与调试 20 学时，网络服务搭建 12 学时，故障排查 10 学时，项目考核 8 学时。

### 教学考核要求

考核方式：采用过程性考核与终结性考核相结合，过程性考核占比 60%，终结性考核占比 40%。

过程性考核：包括课堂出勤（10%）、实操任务完成情况（30%，如网线制作质量、设备配置准确性、任务提交及时性）、小组协作表现（10%）、学习笔记与报告（10%），重点关注学生实操能力与学习态度。

终结性考核：以综合项目实操考核为主，要求学生在规定时间（4 学时）内完成中小型网络搭建（含拓扑设计、设备配置、服务部署、故障排查），根据网络搭建完整性、配置准确性、测试结果及报告撰写质量评分，考核学生综合运用知识与技能解决实际问题的能力。

合格标准：过程性考核与终结性考核均需达到 60 分及以上，总成绩合格方可通过课程考核。

### （二）网络安全产品安装与调试

工学一体化课程名称	网络安全产品安装与调试	基准学时	144
-----------	-------------	------	-----

### 典型工作任务描述

网络安全产品现场安装与调试，涵盖企业、校园等场景下防火墙、入侵检测系统（IDS）、VPN 设备、防病毒网关等主流产品。任务需依据用户网络拓扑与安全需求，完成设备开箱检查、硬件安装固定、网络线缆连接，随后进行初始化配置、系统参数调试、安全策略部署，

---

最终通过功能测试与性能优化，确保产品稳定运行并满足防护要求，同时需出具安装调试报告，响应后续简单故障排查需求，全程遵循行业安全操作规范与质量标准。

---

### 工作内容分析

---

六个核心环节：一是前期准备，收集用户网络架构图、安全需求文档，核查产品型号、配件完整性，准备工具与测试设备；二是硬件安装，按规范固定设备、连接电源与网络线路，做好接地防护；三是系统初始化，通过 Console 口或 Web 界面完成设备启动、密码设置、固件升级；四是参数配置，划分安全区域、配置 IP 地址、路由协议与端口映射；五是策略部署，设置访问控制列表、入侵检测规则、VPN 隧道参数与病毒防护策略；六是测试优化，进行连通性、防护功能与性能压力测试，根据结果调整参数，最后整理文档并交付。

---

### 课程目标

---

1. 知识目标：掌握防火墙、IDS、VPN 等产品工作原理，熟悉主流品牌设备硬件结构与配置界面，理解网络安全区域划分、访问控制、入侵检测等核心技术原理，了解行业相关标准与规范。
  2. 技能目标：能独立完成常见网络安全产品开箱检查与硬件安装，熟练操作 Console 口与 Web 界面进行初始化配置，精准部署安全策略并完成功能测试，具备初步故障排查与性能优化能力，能规范撰写安装调试报告。
  3. 素养目标：培养严谨的工作态度与安全生产意识，提升团队协作与沟通能力，树立自主学习与适应行业技术更新的意识，遵守职业操守与信息安全法规。
- 

### 学习内容

---

围绕核心任务分层展开：一是基础知识，包括网络安全产品分类与应用场景、TCP/IP 协议栈安全要点、常见攻击类型与防护原理；二是硬件操作，涵盖设备选型与配件识别、安装工具使用、线缆制作与连接规范、设备固定与接地操作；三是配置技术，包括 Console 口与远程登录配置、设备初始化参数设置、安全区域划分与接口配置、访问控制列表（ACL）与安全策略配置、VPN 与 IDS 系统部署；四是测试与优化，学习测试方案制定、连通性与防护功能测试方法、性能指标分析与参数调整技巧；五是职业规范，了解行业安全操作流程、文档撰写标准与客户沟通礼仪。

---

### 参考性学习任务

---

基础任务：完成某品牌防火墙开箱检查与硬件安装，包括设备固定、电源及网线连接，通过 Console 口登录设备并完成初始化配置（设置管理员密码、系统时间）。

核心任务：针对小型企业网络场景，在防火墙上划分内网、外网与 DMZ 区域，配置 ACL

---

策略实现内网访问外网限制、外网禁止访问内网，部署基础入侵检测规则。

综合任务：为异地分公司搭建 VPN 隧道，完成总部与分公司防火墙 VPN 参数配置（如 IPSec 协议设置、预共享密钥配置），测试跨地域网络连通性与数据传输安全性。

拓展任务：对已部署的网络安全产品进行功能与性能测试，模拟常见攻击（如 Ping Flood），分析防护效果并优化策略，撰写完整安装调试与测试报告。

### 教学实施建议

教学采用“理实一体化”模式，以真实工作任务为导向，分三个阶段实施：

1. 理论铺垫阶段（20%课时），通过多媒体课件、产品手册与案例视频，讲解产品原理与配置基础，结合课堂提问强化关键知识点；
2. 实操训练阶段（60%课时），在实训室搭建模拟网络环境，学生分组完成任务，教师巡回指导，重点纠正操作规范与配置错误，采用“学生演示 + 教师点评”方式巩固技能；
3. 综合提升阶段（20%课时），引入企业真实项目案例，组织小组竞赛，要求完成方案设计、实施与报告撰写，培养综合应用能力。同时，利用线上平台分享教学资源，布置课后拓展任务，鼓励学生考取相关职业技能证书。

### 教学考核要求

考核采用“过程性考核 + 终结性考核”相结合的方式，总分 100 分。1. 过程性考核（50 分），包括课堂出勤（10 分）、实操任务完成质量（20 分，依据操作规范性、配置准确性评分）、学习态度与团队协作（10 分）、课后作业与报告（10 分）；2. 终结性考核（50 分），采用现场实操形式，学生在规定时间内完成指定网络安全产品安装、配置与测试任务（如防火墙策略部署 + VPN 配置），考核内容涵盖硬件操作（15 分）、系统配置（20 分）、功能测试（10 分）、文档撰写（5 分）。考核合格标准为总分 60 分及以上，同时需满足实操环节无安全操作违规行为，否则判定为考核不合格。

### （三）基于等保的信息系统安全配置

工学一体化课程名称	基于等保的信息系统 安全配置	基准学时	252
-----------	-------------------	------	-----

### 典型工作任务描述

依据《信息安全技术网络安全等级保护基本要求》，针对企业、学校等不同场景的信息系统，开展安全配置实施与验证工作。需按照等保二级及以上标准，完成网络设备（路由器、交换机）、服务器（Windows Server、Linux）、安全设备（防火墙、入侵检测系统）的安全配置，解决账号权限混乱、端口开放不当、数据加密缺失等常见安全问题，确保信息系统

---

满足等保合规要求，保障系统稳定运行与数据安全，为后续系统安全维护奠定基础。

---

### 工作内容分析

---

工作内容涵盖等保合规需求调研，收集信息系统拓扑结构、业务类型、数据敏感级别等信息，确定等保防护等级与具体要求；开展网络设备安全配置，包括划分 VLAN、配置访问控制列表、关闭不必要端口、启用 SSH 加密管理；进行服务器安全配置，设置账号密码策略、安装安全补丁、开启防火墙、配置数据备份方案；部署安全设备，完成防火墙策略配置、入侵检测规则设置；最后进行安全配置验证，通过漏洞扫描、渗透测试等手段，检查配置是否符合等保标准，形成配置报告并优化调整。

---

### 课程目标

---

1. 知识目标：掌握等保基本要求（二级及以上），理解信息系统安全配置核心原理，熟悉网络设备、服务器、安全设备的安全配置参数与标准。
  2. 技能目标：能独立完成等保合规需求调研与分析，熟练操作路由器、交换机、防火墙等设备进行安全配置，具备服务器系统安全优化能力，可通过工具验证配置合规性并解决常见安全配置问题。
  3. 素养目标：培养严谨的安全操作意识与合规思维，树立责任意识与团队协作精神，提升应对信息系统安全配置突发问题的应变能力，符合网络安防行业职业素养要求。
- 

### 学习内容

---

学习内容包括等保基础知识，如《信息安全技术网络安全等级保护基本要求》核心条款、等保分级标准与适用场景；网络设备安全配置，涵盖路由器 ACL 配置、交换机 VLAN 划分与端口安全、设备远程管理加密（SSH）设置；服务器安全配置，包含 Windows Server 账号策略、Linux 系统防火墙配置、服务器安全补丁管理、数据备份与恢复方案；安全设备配置，学习防火墙访问控制策略、入侵检测系统（IDS）规则配置；安全配置验证，掌握漏洞扫描工具（如 Nessus）使用、渗透测试基础方法、配置合规性检查与优化。

---

### 参考性学习任务

---

1. 等保需求调研任务：针对校园图书馆信息系统，收集系统架构、业务数据类型等信息，依据等保标准确定防护等级，撰写需求调研分析报告。
  2. 网络设备配置任务：给定企业网络拓扑，完成路由器 ACL 配置（限制特定网段访问互联网）、交换机 VLAN 划分与端口安全设置，验证配置有效性。
  3. 服务器安全配置任务：在 Windows Server 2019 系统中，设置账号密码复杂度策略、安装最新安全补丁、配置系统防火墙，实现数据定时备份。
-

4. 安全设备部署任务：配置防火墙策略（允许办公网段访问服务器网段，禁止外部网段直接访问），设置 IDS 规则检测常见攻击行为。
5. 配置验证任务：使用 Nessus 扫描已配置系统，生成漏洞报告，针对高危漏洞优化配置，形成最终合规配置文档。

### 教学实施建议

教学采用“理实一体化”模式，理论教学依托多媒体课件，结合等保案例讲解核心知识，借助虚拟仿真平台（如 GNS3、VMware）演示设备配置流程；实践教学以项目为导向，将参考性学习任务分解为课堂实操项目，学生分组完成，教师巡回指导，及时纠正操作错误；引入企业真实案例，邀请网络安防企业工程师开展专题讲座，分享实际工作中的配置经验与问题解决技巧；利用线上学习平台上传教学视频、课件与拓展资料，方便学生课后复习与自主学习，定期组织技能竞赛，提升学生实操积极性。

### 教学考核要求

考核采用过程性考核与终结性考核相结合的方式，过程性考核（占比 60%）包括学习任务完成情况（30%，依据任务报告、实操表现评分）、课堂参与度（15%，含提问回答、小组协作表现）、课后作业（15%，如配置方案设计、知识习题）；终结性考核（占比 40%）为综合实操考核，给定企业信息系统场景与等保等级要求，学生独立完成网络设备、服务器、安全设备的安全配置，并进行合规性验证，提交配置报告与验证结果，考核小组依据配置准确性、合规性、完成效率综合评分；考核合格标准为总分 $\geq 60$ 分，其中终结性考核成绩 $\geq 30$ 分，确保学生达到课程目标要求。

### （四）网络安全日常运维与监控

工学一体化课程名称	网络安全日常运维与监控	基准学时	144
-----------	-------------	------	-----

### 典型工作任务描述

网络安全日常运维与监控，即技工校学生在企业网络安防岗位中，需依据网络安全规范，运用运维工具对企业局域网、服务器集群及终端设备开展日常巡检，实时监控网络流量、设备运行状态及安全威胁，及时发现并处置病毒攻击、漏洞风险、异常访问等问题，定期生成运维报告，保障网络系统持续稳定、安全运行，同时协助完成网络安全策略优化与应急响应配合工作，满足企业对网络安全常态化管理的需求。

### 工作内容分析

主要包括三方面：一是日常运维，需定期检查路由器、交换机、防火墙等网络设备运行

---

参数，排查设备故障与性能瓶颈，更新终端安全软件病毒库，备份网络配置与重要数据；二是实时监控，通过安全监控平台（如 SIEM 系统）监测网络流量异常、端口扫描、恶意代码传播等安全事件，跟踪服务器 CPU、内存、磁盘等资源占用情况；三是问题处置与报告，对发现的安全隐患及时采取隔离、查杀、补丁修复等措施，记录运维过程与处置结果，按周期撰写包含网络安全状态、风险预警的运维报告，为后续安全策略调整提供依据。

---

### 课程目标

---

1. 知识目标：学生能掌握网络安全运维基础理论，熟悉常见网络设备（路由器、防火墙）运维要点，了解 SIEM 等监控系统工作原理，明确病毒攻击、漏洞利用等安全事件处置流程，知晓网络安全相关法规与行业标准。
  2. 技能目标：能独立使用 Ping、Tracert 等工具进行网络连通性检测，熟练操作监控平台查看网络流量与设备状态，具备识别常见安全事件并实施初步处置的能力，可规范撰写运维记录与报告。
  3. 素养目标：培养严谨细致的工作态度，树立网络安全责任意识，提升应急处置与团队协作能力，养成遵循行业规范开展运维工作的职业习惯。
- 

### 学习内容

---

涵盖四大模块：一是网络运维基础，包括网络设备（路由器、交换机）日常检查方法、设备参数配置与备份操作，终端安全软件（杀毒软件）安装与病毒库更新；二是安全监控技术，学习 SIEM 监控系统使用，掌握网络流量分析、设备资源（CPU、内存）监控、安全事件（端口扫描、恶意代码）识别方法；三是问题处置技能，涵盖病毒查杀、漏洞补丁修复、异常终端隔离等操作，以及常见运维故障（网络中断、设备离线）排查流程；四是文档撰写与规范，学习运维日志记录要求、周期性运维报告（网络安全状态、风险分析）撰写方法，了解网络安全相关法规（《网络安全法》）与行业运维标准。

---

### 参考性学习任务

---

1. 基础运维任务：给定企业小型局域网环境（含 2 台路由器、3 台交换机、10 台终端），学生分组完成设备运行参数检查，备份网络配置文件，为终端安装杀毒软件并更新病毒库，提交运维检查记录表。
  2. 监控实操任务：利用模拟 SIEM 平台，模拟网络流量异常（如某 IP 大量发送数据包）、终端感染病毒场景，学生需实时监控并识别安全事件，记录事件类型、发生时间与涉及设备，生成监控日志。
  3. 综合处置任务：设置“服务器漏洞导致恶意访问”故障场景，学生需排查漏洞位置，
-



---

完成补丁修复，隔离受影响终端，撰写包含故障原因、处置过程与预防建议的运维报告。

---

### 教学实施建议

---

教学方法：采用“理实一体化”教学，理论讲解结合仿真软件（如 EVE-NG）模拟操作，通过案例教学（如真实企业网络安全运维案例）强化知识应用，引入项目式教学，以完整运维任务驱动学习。

教学资源：搭建网络安全运维实训平台（含真实路由器、交换机、监控服务器），配备 SIEM 系统模拟软件与运维工具包，编制校本教材（含任务工单、操作手册），收集行业运维案例库与法规文件。

---

### 教学考核要求

---

考核采用“过程性考核 + 终结性考核”结合方式，总分 100 分。过程性考核（占比 60%）包括：运维任务完成质量（30%，如设备检查准确性、监控日志完整性）、课堂实操表现（20%，含操作规范性、团队协作）、学习档案（10%，如运维记录、作业提交）。终结性考核（占比 40%）为综合实操考试，给定复杂运维场景（含设备故障、安全事件），学生需在规定时间内（120 分钟）内完成设备检查、事件识别、问题处置并提交运维报告，考核其综合技能应用能力；考核合格标准为总分 60 分及以上，其中终结性考核成绩不低于 24 分。

---

### （五）WEB 安全渗透测试

工学一体化课程名称	WEB 安全渗透测试	基准学时	144
-----------	------------	------	-----

---

### 典型工作任务描述

---

WEB 安全渗透测试工程师日常工作，即依据网络安全法规与行业规范，对企业 WEB 应用系统开展全面渗透测试。需模拟黑客攻击手段，挖掘系统漏洞，如 SQL 注入、XSS 跨站脚本等，评估系统安全防护能力。测试前需与企业沟通确定测试范围与目标，测试中实时记录漏洞信息，测试后撰写专业测试报告，提出漏洞修复建议，并协助开发团队验证修复效果，保障企业 WEB 应用系统数据安全与稳定运行，预防网络安全事件发生。

---

### 工作内容分析

---

工作内容涵盖前期准备、渗透测试实施、后期总结三大模块。前期准备需收集目标 WEB 系统信息，包括域名、IP 地址、服务器类型等，搭建渗透测试环境，选取合适测试工具如 Burp Suite、Nessus。实施阶段运用多种渗透技术，进行端口扫描、漏洞探测、权限提升等操作，精准定位系统漏洞，记录漏洞细节与攻击路径。后期整理测试数据，撰写规范测试报告，详细说明漏洞危害等级与修复方案，组织企业相关人员进行报告评审，跟进漏洞修复进度，验

---

---

证修复成果，确保漏洞彻底解决，形成完整工作闭环。

---

### 课程目标

---

#### 1. 技能目标

能熟练使用主流渗透测试工具，独立完成 WEB 系统信息收集、漏洞探测与利用；可准确识别常见 WEB 安全漏洞，制定针对性渗透测试方案；具备撰写专业测试报告与协助修复漏洞的能力，能有效应对实际工作中的渗透测试任务。

#### 2. 知识目标

掌握 WEB 应用系统架构与工作原理，熟悉 SQL 注入、XSS 等常见漏洞原理与利用方法；了解网络安全法规与渗透测试行业标准，明晰渗透测试流程与规范；知晓主流安全防护技术，理解漏洞修复的基本原则与方法。

#### 3. 素养目标

培养严谨细致的工作态度，树立网络安全法治意识与责任意识；提升团队协作能力与沟通表达能力，增强自主学习与问题解决能力；养成规范操作与文档记录的职业习惯，适应网络安全行业发展需求。

---

### 学习内容

---

围绕 WEB 安全渗透测试全流程展开。首先学习 WEB 系统基础，包括 HTTP 协议、网站架构、数据库原理等，奠定知识基础；其次掌握信息收集技术，如域名解析、端口扫描、目录爆破等，获取目标系统关键信息；然后深入学习常见漏洞原理与利用，涵盖 SQL 注入、XSS、文件上传漏洞等，结合工具实操掌握漏洞探测与利用方法；还需学习渗透测试报告撰写，掌握报告结构、漏洞描述、修复建议的规范表述；最后了解漏洞修复与验证流程，学习与开发团队协作的技巧，同时穿插网络安全法规与职业道德相关内容学习。

---

### 参考性学习任务

---

1. 信息收集任务：给定目标 WEB 网站域名，使用 Nmap、Whois 等工具，收集网站 IP 地址、服务器类型、开放端口、子域名等信息，形成信息收集报告，要求信息完整度达 90% 以上。
  2. 漏洞探测任务：针对搭建的存在 SQL 注入漏洞的测试网站，使用 SQLMap 工具进行漏洞探测与利用，获取数据库账号密码，记录操作步骤与结果，撰写漏洞分析报告。
  3. 综合渗透测试任务：模拟企业真实 WEB 系统，组建小组完成从信息收集、漏洞探测、权限提升到撰写完整测试报告的全流程任务，需发现至少 3 类不同漏洞，并提出合理修复建议。
-

- 
4. 漏洞修复验证任务：根据前期发现的漏洞，协助“开发团队”制定修复方案，修复后进行渗透测试验证，判断漏洞是否彻底解决，形成验证报告。
- 

### 教学实施建议

---

教学采用“理论 + 实操 + 项目驱动”模式，理论教学以案例讲解为主，结合实际漏洞事件剖析原理，借助多媒体资源增强理解；实操教学在虚拟实验环境开展，提供丰富测试靶场，让学生动手操作工具，教师实时指导纠错。以参考性学习任务为项目载体，将课程内容融入项目实施，分组完成任务，培养团队协作能力。引入企业真实渗透测试案例，邀请行业专家开展讲座，分享实战经验。采用线上线下混合教学，利用学习平台发布学习资源、布置作业与答疑，定期组织技能竞赛，激发学习兴趣，保障教学效果。

---

### 教学考核要求

---

考核采用过程性考核与终结性考核相结合的方式，过程性考核占比 60%，包括课堂表现（10%）、实操任务完成情况（30%）、学习任务报告质量（20%），重点关注学生实操能力与学习态度；终结性考核占比 40%，采用综合项目测试形式，要求学生独立完成指定 WEB 系统的渗透测试，提交测试报告，考核漏洞发现数量、报告规范性与解决方案合理性。考核成绩实行百分制，60 分及以上为合格。同时注重对学生职业素养的考核，将团队协作、规范操作、文档记录等纳入考核评价，确保全面评估学生综合能力。

---

## 六、实施建议

### （一）师资队伍

#### 1. 队伍结构

信息工程系现有教职工 47 人，其中高级讲师 10 人，讲师 6 人，省学术带头人 1 人，市级专业带头人 2 人，其中硕士研究生 7 人，企业引进专家 20 余人，专任教师队伍职称、年龄梯队结构合理，“双师型”教师占 90%。学生数与本专业专任教师数比例约为 10:1。

#### 2. 专任教师

专任教师具有高校教师资格和本专业领域有关证书；有本科及以上学历；扎实的专业理论功底和实践能力；具有较强信息化教学能力，能够开展课程教学改革和科学研究；每 5 年累计不少于 6 个月的企业实践经历。

#### 3. 专业带头人

专业带头人具有高级职称，能够较好地把握国内外行业、专业发展，能密切联系行业企业，了解行业企业对计算机应用技术专业人才的需求实际，教

学设计、专业研究能力强，牵头组织开展教科研工作能力强，在本区域本领域有一定的专业影响力。

#### **4.兼职教师**

兼职教师主要从计算机应用技术专业相关合作企业中聘任，具备良好的思想政治素质、职业道德和工匠精神，具有扎实的专业知识和三年以上丰富的实际工作经验，能承担专业课程教学、实习实训指导等专业教学任务。专业核心课程应由校内专任专业教师和行业企业兼职教师共同完成教学，其中，实践实训部分应以行业企业兼职教师指导为主。

### **(二)场地设备**

本专业教学场地满足培养要求中规定的职业典型工作任务实施的环境及设备设施要求，同时保证教学场地具备良好的安全、照明和通风条件。其中校内教学场地和设备设施应能支持资料查阅、教师授课、小组研讨、任务实施、成果展示等活动的开展；企业实训基地应具备工作任务实践与技术培训等功能。教学设施主要包括能够满足正常的课程教学、实习实训所需的专业教室、校内实训室和校外实训基地等。

#### **1.专业教室基本条件**

专业教室一般配备智慧黑（白）板、多媒体计算机、音响设备，互联网接入或Wi-Fi 环境，并实施网络安全防护措施；安装应急照明装置并保持良好状态，符合紧急疏散要求，标志明显，保持逃生通道畅通无阻。

#### **2.校内实训室基本要求**

##### **网络安全管理中心**

配备中控台及功放系统、多媒体教学系统、投影仪与幕布、白板、交换机、路由器、PC 机、网络测试仪及工具、相关软件。用于计算机网络技术、数据备份与恢复等实训教学。

##### **软件开发中心**

配备计算机、服务器、交换机、网络机柜、多媒体中控台、投影仪、投影幕、交互式电子白板、操作系统软件、办公软件、项目开发软件等设备（设施），用于程序设计、数据结构、操作系统应用、计算机网络技术、数据库技术等实训教学。

#### **3.学生实习基地基本要求**

学生实习基地基本要求为：具有稳定的校外实习基地；可接纳一定规模的学

生实习；能够配备相应数量的指导教师对学生实习进行指导和管理；有保证实习生日常工作、学习、生活的规章制度，有安全、保险保障。由企业提供场地、办公设备、项目和技术指导人员，企业技术人员与教师共同组织和带领学生完成真实项目设计、施工、调试与维护，使学生真正进入企业项目实战，形成校企共建、共管的格局学生通过在企业真实环境中的实践，积累工作经验，具备职业素质综合能力，达到“准职业人”的标准，从而完成从学校到企业的过渡。

### **（三）教学资源**

#### **1. 教材选用基本要求**

按照国家规定选用优质教材，优先选用国家规范教材，禁止不合格的教材进入课堂。学校了建立由专业教师、行业专家和教研人员等参与的教材选用机构，完善教材选用制度，经过规范程序择优选用教材。

#### **2. 图书文献配备要求**

图书文献配备满足人才培养、专业建设、教科研等工作的需要，方便师生查询、借阅。专业类图书文献主要包括：有关药品生产技术的基础知识、生产技术方法、操作实践、技能比赛等。

#### **3. 数字教学资源配置基本要求**

建设、配备与本专业有关的音视频素材、教学课件、数字化教学案例库、在线精品课等专业教学资源库，种类丰富、形式多样、使用便捷、动态更新、满足教学。

### **（四）教学管理制度**

在教学过程中，采用项目教学、案例教学、情境教学、模块化教学等教学方式，运用启发式、探究式、讨论式、参与式等教学方法，推广翻转课堂、混合式教学、理实一体教学等新型教学模式，推动“三教”改革。加强课堂教学管理，规范教学秩序，打造优质课堂，提升教学效果。

充分发挥网络教学优势，利用数字资源，创设工作情景，以工作任务引领提高学习兴趣，采取“线上+线下”结合的方式对学生进行行之有效的知识传授和技能培训。在教学过程中紧密结合职业技能证书的考证、职业岗位能力、课程思政，强化实践实操和职业道德素养内容，切实保证教学质量。

## 七、考核与评价

### （一）综合职业能力评价

综合运用考试、素质评价、技能测试等多种方式进行学习成果考核，学生的学业成绩考核实行过程性考核、期中考核和期末考核相结合的考核方式。

（1）过程性考核是对学生学习过程的测评，由课堂教学的出勤情况、平时作业、专业实验实训等组成，成绩占学业成绩的30%。

（2）期中考核和期末考核为各门课程的期末综合考试，成绩分别占学业成绩的20%和50%，考核方式主要为实操考核。

（3）除了学历教育相关课程的学习评价要求外，对学习培训经历、职业技术技能、社会实践锻炼等，按学校有关规定和程序认定为学历教育相关课程学分，同时，要求本专业学生毕业前按系部要求考取响应的职业技能等级证书，逐步完善和推进“1+X”证书制度。

### （二）职业技能评价

计算机网络应用专业职业技能评价以“贴合行业需求、衔接职业标准”为核心，构建“课证赛”深度融合的考核体系。一方面，将行业权威证书考核内容与课程评价紧密挂钩，例如把“网络系统建设与运维（中级）”“Adobe After Effects 认证”“计算机技术与软件专业技术资格（网络工程师方向）”等证书的知识点、实操要求融入《网络设备配置》《影视后期制作》等对应课程，学生取得证书即可替代相关课程期末考核，实现“以证代考、以考促学”；另一方面，参照全国职业院校技能大赛“网络系统管理”“数字艺术设计”等赛项标准，针对三维建模、网络故障排查、动画制作等核心技能设置专项实操考核，考核时长对标企业工作节奏（如2小时内完成指定网络拓扑搭建、1.5小时内完成模型优化），全面检验学生岗位适配能力。

同时，专业建立健全技能补考与持续提升机制，保障技能达标质量。对未通过核心技能考核的学生，安排10学时/项的专项实训，由企业导师结合考核漏洞（如UV拆分不规范、网络路由配置错误等）开展针对性指导，实训后组织二次补考；为每位学生建立“技能提升档案”，详细记录每次考核的薄弱环节、改进方案及提升成效，既为学生个性化补弱提供明确方向，也为课程内容优化、教学方法调整提供数据支撑，最终确保专业核心技能达标率稳定在92%以上，

切实提升学生职业竞争力。

### **（三）毕业生就业质量分析**

本专业毕业生就业质量呈现出积极向好态势。在就业岗位方面，分布广泛且与行业发展紧密相连。大量毕业生投身网络工程与运维领域，担任网络管理员、系统运维工程师，负责企业网络日常维护与优化，约占就业人数的 35%。随着网络安全重要性日益凸显，安全监控工程师、网络安全分析师等岗位吸引了约 20% 的毕业生，他们为企业筑牢网络安全防线。云计算与大数据产业兴起，云平台助理工程师、大数据运维专员等岗位也吸纳了约 15% 的毕业生，推动相关技术落地应用。整体来看，岗位需求与行业数字化转型趋势高度契合，为毕业生提供了丰富选择。