永州职业技术学院

学生专业技能考核标准

专业代码：510207

专业名称：信息安全技术应用

二级学院：信息学院

永州职业技术学院

2024 年 8 月

目 录

永州职业技术学院学生专业技能考核标准

一、专业名称

1．专业名称：

信息安全技术应用（专业代码：510207）

2．适用对象

高职信息安全技术应用专业全日制毕业年级学生

二、考核目标

依据本专业人才培养方案，通过设置网络平台搭建与安全设备配置防护、服务器配置与安全管理、系统安全攻防及运维安全管控三大考核模块，以真实项目案例形式测试学生网络构建、网络配置、网络管理的能力，具备网络售前技术支持、网络系统运维、网络系统集成岗位的技术技能，以及良好的职业道德、创新意识等职业素养。

1．检验学生的职业技能和素质：检验学生网络设备安装调试、网络系统服务器的安装与调试、网络环境搭建与维护、网络信息安全管理等专业技能，测试学生的网络构建、网络管理、项目管理能力以及从事网络信息安全技术工作的团队协作、成本控制、质量效益、安全规范等职业素养，进而检验我院信息安全技术应用专业的教学质量和办学水平。

2．促进教育教学改革：通过技能考核促进我院信息安全技术应用专业深化课程教学改革，强化实践教学环节，增强学生实践动手能力、创新创业能力，促进学生个性化发展，培养适应信息时代发展需要的信息安全技术高素质技术技能人才。

3．推动信息安全技术应用专业高质量发展：改善实训教学条件、促进专业的实践教学体系建设，深化工学结合人才模式改革与创新，推动产教融合，提高专业人才培养质量，为社会提供高技术技能人才。

三、考核内容

根据高职高专信息安全技术应用专业的人才培养目标和实际工作内容，本专业技能考核分专业基本技能模块和岗位核心技能模块。测试范围包括企业网搭建

与维护、网络安全设备配置与防护、Windows Server 服务器构建与管理、Linux 服务器构建与管理、网络协议安全，Web 安全攻防、网络渗透测试与漏洞利用、网络安全事件响应。其主要内容如下：

模块一、专业基础模块

项目 1：企业网搭建与维护

本模块主要定位于企业网络的规划、设计、配置与维护，以企业网设备互联项目为背景，完成企业网网络设备的简单部署、基本配置、运行监控和简单故障排除，并具备协助设计企业网络及使用交换路由设备的实施设计能力。以企事业单位办公网网络系统管理项目为背景，根据企业部门职能的不同和网络服务器的管理要求，对现有网络及系统进行实施、管理、故障排除等工作。

基本要求：

（1）具备 IP 地址、掩码和子网划分的知识，能根据需求进行 IP 地址划分；

（2）能根据需求进行网络设备的安装、部署和连接，包括网络设备的连接端口选择、网络传输介质的选用、网线的选用与测试；

（3）能够搭建基础 IP 网络，进行设备基础配置，包括主机名设置、用户权限和密码设置、IOS 备份和升级、配置文件导入导出、端口 TCP/IP 参数设置、运行状态监控、本地和远程管理等。

（4）能根据用户业务需求、数量和管理要求进行 VLAN 的划分，能在交换机上完成基于端口划分的 VLAN 配置和 VLAN 地址设置，能正确设置交换机端口的 ACCESS 模式和 TRUNK 模式。能正确完成 VLAN 之间通信配置。

（5）能在交换机之间连接链路使用链路聚合，能正确创建链路聚合通道，能正确设置协商协议类型、负载平衡方式等参数。

（6）能在交换机上启用 STP、MSTP 协议，正确设置根桥优先级、端口优先级等生成树协议常见配置参数。

（7）能根据企业局域网络项目设计要求完成企业局域网出口路由器、核心三层交换机静态路由、RIP、OSPF 路由协议的配置，能利用静态路由、RIP 路由协议、OSPF 路由协议实现企业局域网三层网络互联互通。

（8）具备网络维护和基本故障排除的基本能力，具备规划、配置、运维和管理企业网络的能力。

（9）具备分工协作、严肃认真、规范高效的工作态度和良好的职业道德与职业价值观，具有创新思维、工匠精神、集体意识、团队合作精神等网络设备配置与运行维护工作必备的职业素养。

项目 2：网络安全设备配置与防护

本模块主要以以企业网络建设项目为背景，主要运用防火墙及 VPN 等技术，以完成安全网络的规划管理、网络中加密技术的应用等为主要工作内容，基本涵盖了网络安全运维人员从事网络安全规划、配置与管理所需的核心技能。

基本要求：

（1）能根据用户需求合理设计安全的局域网络并进行管理；

（2）能根据安全需求选择合理的加密技术、网络安全防护技术，根据需求进行防火墙网络架构部署，选择合适的品牌、性能、参数、功能的防火墙；

（3）能运用两层、三层体系结构和双核心技术构建安全可靠高速数据交换骨干网；

（4）能根据企业局域网络项目设计要求完成企业局域网企业局域网中防火墙 NAT 技术、策略路由技术实现三层网络安全互联互通；

（5）能根据企业局域网络项目设计要求完成防火墙配置与管理、入侵检测配置与管理，能实现企业局域网内网用户安全访问互联网和外网用户安全访问企业内网服务器等网络安全服务功能。

模块二、专业核心模块

项目 1：Windows Server 服务器构建与管理

本模块主要定位于企业网络的规划、设计、配置与维护，以企业网设备互联项目为背景，完成企业网网络设备的简单部署、基本配置、运行监控和简单故障排除，并具备协助设计企业网络及使用交换路由设备的实施设计能力。以企事业单位办公网网络系统管理项目为背景，根据企业部门职能的不同和网络服务器的管理要求，对现有网络及系统进行实施、管理、故障排除等工作。主要运用 Windows Server 网络服务器平台构建与管理关键技术，完成 Windows Server 网络操作系统各种网络服务的构建与管理。本模块基本涵盖了：网络售前技术支持岗位，从事网络设备配置与运行维护工作所需的基本技能；网络系统集成岗位，从事服务器管理与运行维护工作所需的基本技能。

基本要求：

（1）能正确安装网络操作系统平台，合理使用管理控制台进行系统设置 ，能对 Windows Server 系统设置本地安全策略和组策略，会使用安全模板设置合理的用户访问控制权限、系统安全策略和 IP 安全策略，确保数据进出系统的安全性。

（2）能正确创建本地用户账户、本地组，合理分配本地用户和组的权限，正确设置文件和文件夹的权限，创建、使用和管理共享文件夹，配置漫游策略满足远程用户管理。

（3）能正确安装活动目录，能正确创建域、子域、额外域、域林服务器，能正确配置域策略、组织单元、域用户等，从而实现服务器及用户的系统管理与授权。

（4）能正确安装和配置 DNS、DHCP、WEB、FTP 等服务。

（5）能在 WEB 服务器和 FTP 服务器与客户端之间搭建 SSL 安全访问通道。

（6）能正确处理操作系统的日志，对常见的用户登录、文件及文件夹访问等操作系统使用与管理操作进行系统安全审计。监控操作系统的进程与服务运行状态，根据安全管理需要打开、关闭、查看系统和应用程序的进程与服务

（7）能严格遵守网络服务器系统的设计、安装、测试和管理的工作规范，硬件服务器设备操作符合电子设备安全操作规范。

（8）具备网络管理员必备的分工配置、严肃认真、规范高效的工作态度和良好的职业道德与职业价值观，具有创新思维、工匠精神、集体意识、团队合作精神等服务器管理与运行维护工作必备的职业素养。

项目 2：Linux 服务器构建与管理

本模块以企业网络服务系统管理项目为背景，根据企业部门职能的不同和网络服务器的管理要求，主要运用 Linux 服务器构建与管理关键技术，完成 Linux 网络操作系统的安装、管理的构建与管理。本模块基本涵盖了网络管理工程师岗位从事 Linux 服务器部署、管理与维护工作所需核心技能。

基本要求：

（1）能按照设计要求完成 Linux 操作系统的安装和部署，完成服务器网卡参数、磁盘分区等相关设置和配置，能用系统信息类命令查看系统时间、内存使

用、硬盘分区及使用、目录硬盘占用等信息，确保系统正常可用。

（2）能理解和使用基本工具，通过命令提示符来正确输入命令及语法，创建和编辑文本文件；创建、删除、复制和移动文件和目录；创建硬链接和软连接；查看、设置和修改标准文件权限；查找、读取和使用系统帮助文档等。

（3）能管理运行中的 LINUX 操作系统，如启动、重启和关闭系统；根据需求中断引导过程，识别进程的占用 CPU/Memory，使用 renice 调整进程优先级，并且 kill 进程；定位和识别系统 log 及 journals；访问虚拟机控制台；启动和停止虚拟机；开启，关闭和检查网络服务的状态；通过加密方式在系统之间传输文件等；

（4）能进行安全管理，包括使用 system-config-firewall 或者 iptables 管理防火墙；配置 SSH 使用 key 认证；设置 SELinux 使用 Enforcing 或者 Permissive 模式；查看和识别 SELinux 文件和进程上下文等。

（5）能严格遵守网络服务器系统的设计、安装、测试和管理的工作规范，硬件服务器设备操作符合电子设备安全操作规范。

（6）具备把握用户需求准确、项目工程质量评判专业、项目子任务划分合理、现场故障分析判断准确、突发情况处理及时、团队协作规范等服务器系统工程师必备的职业素养。

项目 3：网络协议安全

本模块聚焦于网络协议的安全性，涵盖 ARP、VLAN、STP、ICMP、TCP 和 RIP 等关键协议的基本原理与安全隐患。通过使用 Kali Linux 和 CentOS Linux 系统进行模拟，学生将深入理解这些协议的工作机制及其可能面临的攻击风险，帮助学生掌握网络协议分析与攻击防护的技能。

（1）ARP 协议安全：理解 ARP 协议的工作原理，模拟 ARP 欺骗攻击，利用 Wireshark 进行抓包分析，并探讨相应的防护措施。

（2）VLAN 协议安全：掌握 VLAN 的基本概念及各字段的意义，构建 VLAN 数据包，通过 Wireshark 分析其对网络安全的影响。

（3）STP 协议安全：理解生成树协议（STP）的基本功能，模拟 STP 攻击场景，使用 Wireshark 抓包分析，并探讨如何通过 STP 配置增强网络安全。

（4）ICMP 协议安全：分析 ICMP 协议的作用，构建 ICMP 数据包，通过

Wireshark 抓包分析，理解防范 ICMP 相关网络攻击的方法。

（5）TCP 协议安全：理解 TCP 协议的工作原理，掌握 TCP 三次握手过程，构建 TCP 数据包，通过 Wireshark 抓包分析，探讨增强 TCP 连接安全性的措施。

（6）RIP 协议安全：理解 RIP 路由协议的工作原理，模拟 RIP 数据包，使用 Wireshark 抓包分析其对网络路由的潜在威胁及防护策略。

项目 4：Web 安全攻防

本模块聚焦于 Web 系统漏洞利用和加固，运用渗透测试工具和关键技术，完成对 Web 系统漏洞的检测与渗透，旨在强化学生对 Web 系统安全知识的理解，以及实战技能的提升。模块涵盖了 Web 渗透中常见的漏洞以及渗透测试的工作所需的核心技能。

基本要求：

（1）掌握 Web 基础知识，漏洞常见类型；

（2）掌握 SQL 注入方式和防范，成功获取数据库的信息表和字段；

（3）掌握反射型和存储型 XSS 的工作原理和漏洞渗透，并获取 cookie 信息；

（4）掌握 CSRF 的攻击与防护；

（5）掌握命令注入的方式和防范，获取；

（6）熟练常见的文件上传防护绕过方式；

（7）掌握文件包含漏洞的利用与防御。

（8）掌握 DVWA 平台的搭建，

（9）掌握渗透工具如 Burp suite、sqlmap 的使用

（10）项目实施过程符合网络安全、系统安全、WEB 应用安全工程设计、实施、测试的工作规范。安全软件使用合理，硬件服务器设备操作符合电子设备安全操作规范。文档整洁、表达清晰、排版紧凑、符合要求。举止文明、作业操作紧凑有序、有团队意识。

模块三、专业拓展模块

项目 1：网络渗透测试与漏洞利用

本模块聚焦于渗透测试的各个流程和步骤，通过运用渗透测试工具和关键技术，完成系统漏洞的检测与利用，旨在提升学生的实战技能和安全意识。模块涵盖渗透测试工程师在进行漏洞评估与风险管理工作所需的核心技能。

基本要求：

（1）能使用 Netdiscover 等网络扫描工具识别网络中的活动设备，获取目标 IP 地址和 MAC 地址信息，掌握基础网络拓扑结构；

（2）能使用 Nmap 等端口扫描工具进行端口扫描，识别开放端口及其状态，结合服务探测技术，确定目标主机上运行的服务及版本信息，为后续攻击奠定基础；

（3）能使用 Metasploit 框架进行全面的漏洞扫描，覆盖操作系统漏洞、SSH 协议漏洞、MySQL 数据库漏洞以及 Web 系统的潜在风险，帮助学生了解常见的安全缺陷；

（4）掌握漏洞利用技术，包括 SSH 弱口令攻击、MS17-010 永恒之蓝漏洞利用、MySQL 数据库攻击及 Linux 系统攻击等，培养实际攻击能力；

（5）掌握 Linux 系统提权技术，通过多种方法获取更高权限并获取 Flag，以验证提权的成功性，理解系统安全的重要性；

（6）项目实施过程中，要求学生遵循信息安全与伦理规范，合理利用安全工具，确保测试环境的完整性与安全性。同时，文档需整洁、表达清晰、排版紧凑，符合项目要求，强调团队合作与有效沟通。

项目 2：网络安全事件响应

本模块模拟真实的网络安全事件场景，旨在考察学生面对网络安全攻击时的快速响应与处置能力。本模块基本涵盖了案例分析、实战演练及工具应用，从事件监测、分析、响应到恢复的全流程技能。

基本要求：

（1）能够使用 wireshark 或者系统日志实时监测网络流量和日志，识别异常行为或潜在威胁；

（2）快速分析相关 web 或者系统攻击等威胁信息，包括攻击手法、攻击者特征、受影响系统模块等；

（3）根据事件类型和影响范围，快速制定应急响应计划，包括隔离受感染系统、阻断攻击路径、数据备份与恢复策略等，确保响应行动有序进行；

（4）收集关键证据，包括日志文件、网络数据包等，通过深入分析，确定攻击源、攻击路径及影响范围；

（6）根据事件分析结果，及时修复受影响的系统漏洞，并对相关系统配置进行加固，提升整体安全防护能力；

（7）详细记录的网络安全事件的关键信息，通过复盘分析，不断提升团队的安全响应能力和应急管理水平；

（8）团队协作与沟通：强调团队协作精神，确保团队成员间信息畅通、配合默契。在事件响应过程中，能够高效沟通、协同作战，共同应对复杂的安全挑战。

四、评价标准

1.评价方式：本专业技能考核采取过程考核与结果考核相结合，技能考核与职业素养考核相结合。根据考生操作的规范性、熟练程度和用时量等因素评价过程成绩；根据设计作品、运行测试结果和提交文档质量等因素评价结果成绩。

2.分值分配：本专业技能考核满分为 100 分，其中专业技能占 90 分，项目文档和职业素养占 10 分。

3.技能评价要点：根据模块中考核项目的不同，重点考核学生对该项目所必须掌握的技能和要求。虽然不同考试题目的技能侧重点有所不同，但完成任务的工作量和难易程度基本相同。各模块和项目的技能评价要点内容如表 1 所示。

表1　信息安全应用技术专业技能考核评价要点

序号	模块	项目	评价要点
1	网络平台搭建与安全设备配置防护	企业网搭建与维护	（1）具备 IP 地址、掩码和子网划分的知识，能根据需求进行 IP 地址划分； （2）能根据需求进行网络设备的安装、部署和连接，包括网络设备的连接端口选择、网络传输介质的选用、网线的选用与测试； （3）能够搭建基础 IP 网络，进行设备基础配置，包括主机名设置、用户权限和密码设置、IOS 备份和升级、配置文件导入导出、端口 TCP/IP 参数设置、运行状态监控、本地和远程管理等。 （4）能根据用户业务需求、数量和管理要求进行 VLAN 的划分，能在交换机上完成基于端口划分的 VLAN 配置和 VLAN 地址设置，能正确设置交换机端口的 ACCESS 模式和 TRUNK 模式。能正确完成 VLAN 之间通信配置。 （5）能在交换机之间连接链路使用链路聚合，能正确创建链路聚合通道，能正确设置协商协议类型、负载平衡方式等参数。 （6）能在交换机上启用 STP、MSTP 协议，正确设置根桥优先级、端口优先级等生成树协议常见配置参数。 （7）能根据企业局域网络项目设计要求完成企业局域网出口路由器、核心三层交换机静态路由、RIP、OSPF 路由协议的配置，能利用静态路由、RIP 路由协议、OSPF 路由协议实现企业局域

			网三层网络互联互通。 （8）具备网络维护和基本故障排除的基本能力，具备规划、配置、运维和管理企业网络的能力。 （9）具备分工协作、严肃认真、规范高效的工作态度和良好的职业道德与职业价值观，具有创新思维、工匠精神、集体意识、团队合作精神等网络设备配置与运行维护工作必备的职业素养。
		网络安全设备配置与防护	（1）能根据用户需求合理设计安全的局域网络并进行管理； （2）能根据安全需求选择合理的加密技术、网络安全防护技术，根据需求进行防火墙网络架构部署，选择合适的品牌、性能、参数、功能的防火墙； （3）能运用两层、三层体系结构和双核心技术构建安全可靠高速数据交换骨干网； （4）能根据企业局域网络项目设计要求完成企业局域网企业局域网中防火墙 NAT 技术、策略路由技术实现三层网络安全互联互通； （5）能根据企业局域网络项目设计要求完成防火墙配置与管理、入侵检测配置与管理，能实现企业局域网内网用户安全访问互联网和外网用户安全访问企业内网服务器等网络安全服务功能。
2	服务器配置与安全管理	Windows Server 系统构建与管理	（1）能正确安装网络操作系统平台，合理使用管理控制台进行系统设置 ，能对 Windows Server 系统设置本地安全策略和组策略，会使用安全模板设置合理的用户访问控制权限、系统安全策略和 IP 安全策略，确保数据进出系统的安全性。 （2）能正确创建本地用户账户、本地组，合理分配本地用户和组的权限，正确设置文件和文件夹的权限，创建、使用和管理共享文件夹，配置漫游策略满足远程用户管理。 （3）能正确安装活动目录，能正确创建域、子域、额外域、域林服务器，能正确配置域策略、组织单元、域用户等，从而实现服务器及用户的系统管理与授权。 （4）能正确安装和配置 DNS、DHCP、WEB、FTP 等服务。 （5）能在 WEB 服务器和 FTP 服务器与客户端之间搭建 SSL 安全访问通道。 （6）能正确处理操作系统的日志，对常见的用户登录、文件及文件夹访问等操作系统使用与管理操作进行系统安全审计。监控操作系统的进程与服务运行状态，根据安全管理需要打开、关闭、查看系统和应用程序的进程与服务 （7）能严格遵守网络服务器系统的设计、安装、测试和管理的工作规范，硬件服务器设备操作符合电子设备安全操作规范。 （8）具备网络管理员必备的分工配置、严肃认真、规范高效的工作态度和良好的职业道德与职业价值观，具有创新思维、工匠精神、集体意识、团队合作精神等服务器管理与运行维护工作必备的职业素养。
		Linux 服务器构建与管理	（1）能按照设计要求完成 Linux 操作系统的安装和部署，完成服务器网卡参数、磁盘分区等相关设置和配置，能用系统信息类命令查看系统时间、内存使用、硬盘分区及使用、目录硬盘占用等信息，确保系统正常可用。 （2）能理解和使用基本工具，通过命令提示符来正确输入命令及语法，创建和编辑文本文件；创建、删除、复制和移动文件和目录；创建硬链接和软连接；查看、设置和修改标准文件权限；查找、读取和使用系统帮助文档等。

			（3）能管理运行中的 LINUX 操作系统，如启动、重启和关闭系统；根据需求中断引导过程，识别进程的占用 CPU/Memory，使用 renice 调整进程优先级，并且 kill 进程；定位和识别系统 log 及 journals；访问虚拟机控制台；启动和停止虚拟机；开启，关闭和检查网络服务的状态；通过加密方式在系统之间传输文件等； （4）能进行安全管理，包括使用 system-config-firewall 或者 iptables 管理防火墙;配置 SSH 使用 key 认证;设置 SELinux 使用 Enforcing 或者 Permissive 模式；查看和识别 SELinux 文件和进程上下文等。 （5）能严格遵守网络服务器系统的设计、安装、测试和管理的工作规范，硬件服务器设备操作符合电子设备安全操作规范。 （6）具备把握用户需求准确、项目工程质量评判专业、项目子任务划分合理、现场故障分析判断准确、突发情况处理及时、团队协作规范等服务器系统工程师必备的职业素养。
3	系统安全攻防及运维安全管控	网络协议安全	（1）能正确配置虚拟机系统和虚拟机网络连接，并完成网络连通性测试； （2）能使用 Kali Linux，在在 Python 解释器中使用命令“from scapy.all import *”导入 Scapy 库，与 CentOS Linux 系统进行模拟测试，使用 Wireshark 抓取数据包并分析，帮助理解网络协议的交互机制及其在实际应用中的安全问题。 （3）能掌握 ARP 协议的工作原理，模拟 ARP 欺骗攻击，利用 Wireshark 进行抓包分析，并探讨相应的防护措施。 （4）能掌握 VLAN 的基本概念及各字段的意义，构建 VLAN 数据包，通过 Wireshark 分析其对网络安全的影响。 （5）能掌握生成树协议（STP）的基本功能，模拟 STP 攻击场景，使用 Wireshark 抓包分析，并探讨如何通过 STP 配置增强网络安全。 （6）能理解 TCP 协议的工作原理，掌握 TCP 三次握手过程，构建 TCP 数据包，通过 Wireshark 抓包分析，探讨增强 TCP 连接安全性的措施。 （7）能理解 RIP 路由协议的工作原理，掌握其各字段的意义，模拟 RIP 数据包，使用 Wireshark 抓包分析其对网络路由的潜在威胁及防护策略。
		Web 安全防护	（1）能正确安装网络操作系统平台，实现测试环境搭建； （2）能综合运用 NMAP 等网络探测和安全扫描工具对目标网络服务器进行扫描，获取并分析目标系统的端口、服务等信息； （3）能使用 wireshark 等网络嗅探工具对网络传输数据进行网络监听和数据分析； （4）能根据企业需求对主机进行安全测评； （5）能根据企业需求对企业产品运维维护，进行安全配置巡检、服务器安全巡检。
		网络渗透测试与漏洞利用	（1）能正确配置虚拟机系统和虚拟机网络连接，并完成网络连通性测试； （2）能使用 Netdiscover、Nmap 等工具完成网络和目标系统探测； （3）能创建字典文件以供暴力破解使用； （4）能启动并配置 Kali Linux 中的 Metasploit 框架，并用它对 CentOS Linux 系统进行渗透攻击； （5）能使用渗透测试工具 msfconsole 对 Windows 7 系统进行漏洞检测和漏洞利用；

			（6）能使用 msfconsole 工具对 Windows 7 系统的 MySQL 数据库进行渗透攻击测试，对 MySQL 服务进行安全性评估，以验证其安全性和抵御能力； （7）能识别 Drupal CMS 系统，并利用 Metasploit 工具获取反向 Shell；，查找设置了 SUID 位的文件，找到设置了 SUID 位的“find”命令，并使用“find”命令获取 root Shell，获得 Flag。 （8）能通过扫描和枚举获取靶机的基本信息，使用扫描工具发现系统中存在的安全漏洞，发现的漏洞获取非特权用户的访问权限，通过利用 Linux 服务器系统中的漏洞或错误配置，提升到 root 权限，最终找到存储在系统中的最终 Flag。
		网络安全事件响应	（1）能够使用 wireshark 或者系统日志实时监测网络流量和日志，识别异常行为或潜在威胁； （2）快速分析相关 web 或者系统攻击等威胁信息，包括攻击手法、攻击者特征、受影响系统模块等； （3）根据事件类型和影响范围，快速制定应急响应计划，包括隔离受感染系统、阻断攻击路径、数据备份与恢复策略等，确保响应行动有序进行； （4）收集关键证据，包括日志文件、网络数据包等，通过深入分析，确定攻击源、攻击路径及影响范围； （6）根据事件分析结果，及时修复受影响的系统漏洞，并对相关系统配置进行加固，提升整体安全防护能力； （7）详细记录的网络安全事件的关键信息，通过复盘分析，不断提升团队的安全响应能力和应急管理水平； （8）团队协作与沟通：强调团队协作精神，确保团队成员间信息畅通、配合默契。在事件响应过程中，能够高效沟通、协同作战，共同应对复杂的安全挑战。

五、考核方式

本专业技能考核为现场操作考核，成绩评定采用过程考核与结果考核相结合。具体方式如下：

1.学生参考模块确定：参考学生按规定比例随机抽取考试模块，其中，25%学生参考专业基础模块、50%学生参考专业核心模块、25%学生参考专业拓展模块。考试方案可以根据实际情况对参考学生比例进行适当调整。各模块考生人数按四舍五入计算，剩余的尾数考生随机在两个模块中抽取应试模块。

2. 试题抽取方式：学生在相应模块题库中随机抽取 1 道试题考核。

六、附录

1.相关法律法规（摘录）

（1）《中华人民共和国计算机信息系统安全保护条例》第四章第二十三条规定：故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者

未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以 5000 元以下的罚款、对单位处以 15000 元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。

（2）《中华人民共和国计算机信息系统安全保护条例》第二章第十三条规定：计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

（3）《中华人民共和国计算机信息系统安全保护条例》第二章第十四条规定：对计算机信息系统中发生的案件，有关使用单位应当在 24 小时内向当地县级以上人民政府公安机关报告。

2.相关规范与标准（摘录）

本专业标准主要依据的计算机行业国家技术标准如表 2 所示。

表2 引用技术标准和规范

序号	标准号	中文标准名称
1	GB 21671-2008	基于以太网技术的局域网系统验收测评规范
2	GB/T 20008-2005	操作系统安全评估准则
3	GB/T 19716 - 2005	信息技术信息安全管理实用规则
4	GB/T 22239-2008	信息系统安全等级保护基本要求
5	GB50311-2007	综合布线系统工程设计规范
6	GB50312-2007	综合布线系统工程验收规范
7	GB50174-2008	电子信息系统机房设计规范
8	GB/T20271-2006	信息安全技术-信息系统通用安全技术要求
9	GB/T 25068.1-2012	信息技术 安全技术 IT 网络安全