湖南信息职业技术学院

信息安全技术应用专业技能考核标准

一、专业名称及适用对象

1.专业名称

信息安全技术应用（专业代码：610211）。

2.适用对象

高职全日制在籍毕业年级学生

二、考核内容

本专业技能考核，依据本专业人才培养方案，通过设置网络安全运维工程师、渗透测试工程师、反病毒工程师、数据恢复工程师等岗位的网络设备配置与调试、服务器系统管理与安全加固、网络安全设备配置、系统安全攻防及运维安全管控四个技能考核模块，测试学生的网络构建、服务器系统的安全管理、网络安全设备配置、渗透测试、项目管理能力以及从事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。引导学校加强专业教学基本条件建设，深化课程教学改革，强化实践教学环节，增强学生创新创业能力，促进学生个性化发展，提高专业教学质量和专业办学水平，培养适应信息时代发展需要的信息安全技术应用技术高素质技术技能人才。

网络设备配置与调试模块以企事业单位网络设备互联项

目为背景，主要运用局域网的组网技术，完成小型企业局域网网络设备简单部署、基本配置、运行监控和简单故障排除为主要工作内容。基本涵盖了网络安全运维工程师岗位从事网络设备配置与运行维护工作所需的基本技能。

服务器系统管理与安全加固模块以企事业单位系统安全构建与管理项目为背景，主要运用加密技术、主机安全技术、网络协议安全技术、系统安全加固技术、服务器系统安全技术和Linux系统管理与维护技术，完成网络安全信息分析和系统安全检测、服务器安全管理等工作任务。本模块基本涵盖了网络安全运维工程师岗位从事运行维护、评估工作所需基本技能。

网络安全设备配置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工程师从事网络安全规划、配置与管理所需的核心技能。

系统安全攻防及运维安全管控以企事业单位网络系统安全构建与管理项目为背景，主要运用网络渗透测试与漏洞利用、Web渗透测试与防御知识、Web安全评估知识、操作系统渗透测试与漏洞利用，完成Web应用安全加固、数据库安全维护、操作系统安全加固、网络安全加固等工作任务。本模块基本涵盖了渗透测试工程师岗位从事系统渗透测试、推动企业安全漏洞整改工作所需岗位技能。

四个考核模块中网络设备配置与调试、服务器系统管理

与安全加固为专业基本技能模块，网络安全设备配置、系统安全攻防及运维安全管控为岗位核心技能模块。

（一）专业基础技能

模块一　网络设备配置与调试

项目1．交换设备配置与维护

基本要求：

（1）技能要求

能根据网络拓扑结构完成交换机的安装、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、网线制作与测试；

能对交换机设备进行本地和远程管理，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、运行状态监控等；

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，能实现VLAN之间的通信；

能利用链路聚合技术、生成树技术为企业局域网提升链路带宽和可靠性；

能根据网络拓扑结构完成路由器的安装、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、网线制作与测试。

（2）素养要求

能严格遵守交换设备安装、管理、测试的工作规范，对

交换机、终端设备的连接和配置操作符合电子设备安全操作规范；

能严格遵守网络工程项目设计、实施、测试的工作规范；

具有安全意识、信息素养、工匠精神、创新思维。

具有集体意识、团队合作精神等

项目2. 路由设备配置与维护

基本要求：

（1）技能要求

能根据网络拓扑结构完成路由器的安装、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、网线制作与测试；

能对路由器设备进行本地和远程管理，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、运行状态监控等；

能在路由器上配置静态路由器、能利用静态路由实现三层网络互通，能在路由器上配置RIP、OSPF路由协议的配置动态路由协议实现三层网络互联互通；

能在路由器上配置地址转换，能利用路由器的地址转换功能隐藏内网、提升安全、实现内网用户访问互联网，能将内网服务器发布到外网供外网用户访问。

（2）素养要求

能严格遵守网络工程项目设计、实施、测试的工作规范，对路由器设备的操作符合电子设备安全操作规范；

具有安全意识、信息素养、工匠精神、创新思维。

具有集体意识、团队合作精神等。

模块二 服务器系统管理与安全加固

项目1．Linux系统管理与维护

基本要求：

（1）技能要求

能安装和部署Linux操作系统，完成相关设置和配置；

能设置服务器网卡参数，保证服务器与网络连接畅通；

能用命令方式创建、修改、删除、停用、启用、切换本地用户账户，能用命令方式创建、修改、删除本地组；

能用文件和目录类命令创建、修改、删除、查找、查看、复制、移动，压缩、解压文件和文件夹，查看、修改文件及文件夹权限，设置文件的拥有者；

能用命令完成Linux 下文件系统的创建、挂载与卸载；

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；

能用RPM和YUM方式安装、管理、卸载软件；能用命令对磁盘进行正确分区、挂载光盘。

（2）素养要求

能严格遵守Linux系统安装、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。

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；

具有安全意识、信息素养、工匠精神、创新思维。

具有集体意识、团队合作精神等。

项目2．主机安全技术

基本要求：

（1）技能要求

能正确安装网络操作系统平台，实现测试环境搭建；

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；

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；

能根据企业需求对主机进行安全测评；

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。

（2）素养要求

能严格遵守网络安全、系统安全及服务器安全管理工作规范；

具备较高安全管理意识，服务器系统管理维护符合信息系统安全管理操作规范；

具有安全意识、信息素养、工匠精神、创新思维。

具有集体意识、团队合作精神等。

项目3．加密技术应用

基本要求：

（1）技能要求

能根据要求使用PGP软件实现文件的加密解密，安全传输；

能通过PGP加密软件创建自解密文档，在任何一台电脑上都可以随时解密数据；

通过PGP加密软件划分出一部分的磁盘空间来存储敏感数据；

能利用EPS加密文件系统、BitLocker加密驱动器等加密技术对网络数据和系统文件进行一些常规的加密工作，并实现对磁盘内的文件或者文件夹的资源使用权限的控制，使网络数据能够安全的传输。

（2）素养要求

能严格遵守加密软件的管理工作规范；

具备较高安全管理意识，系统加密的操作符合信息系统安全管理操作规范；

具有安全意识、信息素养、工匠精神、创新思维。

具有集体意识、团队合作精神等。

项目4．网络协议安全

基本要求：

（1）技能要求

通过对网络协议安全项目的学习与实践，培养学生使用网络协议分析技术解决校园网络潜在的安全漏洞风险，提高校园网络系统抵抗网络攻击的安全能力；

培养学生网络安全风险识别和防范能力，培养学生运用安全知识、工具、技术手段进行基础网络系统安全加固的能力；

能正确的搭建测试机的网络安全协议编程环境，包括安装测试操作系统，安装编程工具，安装网络协议数据库；

能正确设置测试机和靶机的端口TCP/IP参数设置，并进行连通性测试；

能够使用网络协议数据编辑工具构建以太网、虚拟局域网（VLAN）、ARP、生成树协议、互联网协议、TCP协议、UDP协议、ICMP协议、生成树协议、路由信息协议、DNS协议、HTTP协议的数据包，并且配置其协议的关键数据参数。

能够使用网络协议分析工具对以太网、虚拟局域网（VLAN）、ARP、生成树协议、互联网协议、TCP协议、UDP协议、ICMP协议、生成树协议、路由信息协议、DNS协议、HTTP协议的通信数据进行抓包和拦截分析。

能够掌握cam表溢出攻击与端口安全；操纵生成树协议与BPDU防护技术；DHCP耗竭、DHCP欺骗与DHCP安全防护。

能够掌握ARP欺骗与动态ARP监控；VLAN跳转攻击与缓解；IP SEC VPN配置与管理；ASA IPSEC VPN配置的网络协议安全技术方法。

（2）素养要求

能严格遵守网络协议、网络安全、系统安全及服务器安

全管理工作规范；

具备较高安全管理意识，网络安全管理操作规范；

具有安全意识、信息素养。

有爱岗敬业、谦虚好学和勤于思考的精神、团队精神和协调工作能力、管理能力和全局观念、创新、创业、开拓发展的精神。

（二）专业核心技能

模块三 网络安全设备配置

项目1．防火墙配置与维护

基本要求：

（1）技能要求

能根据用户需求合理设计安全的局域网络并进行管理；

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；

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；

能根据企业局域网络项目设计要求完成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；

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）素养要求

能严格遵守网络工程安全设计、实施、测试的工作规范，设备操作符合电子设备安全操作规范；

具备网络安全运维人员必备的良好的职业道德、正确的职业价值观和持续学习新的网络组网技术等良好职业习惯；

具有安全意识、信息素养、工匠精神、创新思维。

具有集体意识、团队合作精神等。

项目2．VPN配置与维护

基本要求：

（1）技能要求

能根据用户需求合理设计安全的局域网络并进行管理；

能根据安全需求选择合理的加密技术、网络安全防护技术；

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；

能根据企业局域网络项目设计要求完成企业局域网中策略路由技术、VPN技术实现三层网络安全互联互通；

能根据企业局域网络项目设计要求完成VPN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）素养要求

能严格遵守网络工程安全设计、实施、测试的工作规范，设备操作符合电子设备安全操作规范；

具备网络安全运维人员必备的良好的职业道德、正确的职业价值观和持续学习新的网络组网技术等良好职业习惯；

具有安全意识、信息素养、工匠精神、创新思维。

具有集体意识、团队合作精神等。

模块四 系统安全攻防及运维安全管控

项目1．网络渗透测试与漏洞利用

基本要求：

（1）技能要求

熟悉常用渗透测试工具、字典的使用；

熟练掌握Metasploit 和Web渗透攻击两种渗透测试技术；

能够进行渗透测试实例深度剖析等;

熟悉LINUX的安全防护；

熟悉常用扫描工具、能够对扫描原理进行剖析；

能够在Linux操作系统下使用X-scan进行扫描；

能根据系统应用项目设计合规的渗透测试实例，推进漏洞整改，从而构建较高安全性能的系统应用、提高操作系统的安全性。

（2）素养要求

能严格遵守系统安全工程设计、实施、测试的工作规范；

具备较高安全管理意识，LINUX操作系统维护符合信息

系统安全管理操作规范；

具有安全意识、信息素养、工匠精神、创新思维。

项目2．操作系统渗透测试与漏洞利用

基本要求：

（1）技能要求

熟悉常用渗透测试工具；

熟练掌握Kali Linux的使用及Metasploit渗透测试技术；

熟悉WINDOWS系统的安全防护；

熟悉LINUX的安全防护；

能够测试Linux操作系统中ssh的安全性。

（2）素养要求

能严格遵守系统安全工程设计、实施、测试的工作规范；

具备较高安全管理意识，WINDOWS操作系统、LINUX操作系统管理维护符合信息系统安全管理操作规范；

具有安全意识、信息素养、工匠精神、创新思维。

项目3．Web应用和数据库渗透测试与漏洞利用

基本要求：

（1）技能要求

熟悉常用渗透测试工具；

熟练掌握Kali Linux的使用及Metasploit渗透测试技术；

熟悉WINDOWS系统的安全防护；

能够搭建DVWA漏洞环境；

熟悉木马的工作原理；

熟悉PHP语言；

能够搭建DVWA漏洞环境、SQL注入平台和XSS测试平台；

能够灵活应用Burp Suite进行渗透测试；

熟悉XSS漏洞原理及防范；

熟悉服务器的安全防护；

熟悉命令漏洞原理及防范。

（2）素养要求

能严格遵守系统安全工程设计、实施、测试的工作规范；

具备较高安全管理意识，WINDOWS操作系统管理维护符合信息系统安全管理操作规范；

具有安全意识、信息素养、工匠精神、创新思维。

三、评价标准

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。

本专业技能考核满分为100分，其中专业技能占80分，项目文档和职业素养各占10分。

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　信息安全技术应用专业技能考核评价要点

序号	类型	模块	评价要点
1	专业基本技能	网络设备配置与调试	专业技能： 1．网络设备连接正确，端口选择正确，连接线缆选用正确； 2．交换机部署合理、运行状态监控操作正确； 3．交换机端口参数、主机名、用户名、密码等基本参数设置正确； 4．交换机本地和远程管理操作正确； 5．VLAN划分配置正确，实现了合理的端口隔离； 6．生成树配置正确，实现了链路的冗余； 7．路由器部署合理、运行状态监控操作正确； 8．路由器端口参数、主机名、用户名、密码等基本参数设置正确； 9．路由器本地和远程管理操作正确； 10．静态路由、动态路由设计合理、配置正确，能实现数据正确转发，实现三层网络互通； 11．地址转换配置正确，可以实现内网访问；
			专业素养： 1.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，场地整洁； 2.文档整洁、表达清晰、排版紧凑、符合要求； 3.按照要求创建、存放有关文档； 4.举止文明、作业操作紧凑有序、有团队意识； 5.把握用户需求正确，对项目质量完成判断专业，故障分析正确。
		服务器系统管理	专业技能： 1.正确按照需求在安装系统时进行分区、主机名、根密码等设置，并成功安装系统； 2.正确通过命令、文件等方式设置网卡参数，保证网络正常运行； 3.正确使用使用命令创建、修改、删除、停用、启用、切换本地用户账户，4.正确使用命令创建、修改、删除

		与安全加固	本地组，能进行用户管理； 5.正确使用文件和目录类命令创建、修改、删除、查找、查看、复制、移动，压缩、解压文件和文件夹，查看、修改文件及文件夹权限，设置文件的拥有者，进行文件管理； 6.正确使用命令完成 Linux 下文件系统的创建、挂载与卸载； 7.正确使用命令查看系统时间、内存使用、硬盘分区及使用、目录硬盘占用等信息； 8.正确使用 RPM 和 YUM 的方式安装、管理、卸载软件，正确使用命令对磁盘进行分区，挂载光盘； 9.严格遵守 Linux 系统安装、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； 10.能正确安装网络操作系统平台，实现测试环境搭建； 11.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； 12.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； 13.能根据企业需求对主机进行安全测评,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； 14.能利用 PGP 加密软件、EPS 加密文件系统、用 BitLocker 加密驱动器等加密技术对网络数据和系统文件进行一些常规的加密工作，并实现对磁盘内的文件或者文件夹的资源使用权限的控制，使网络数据能够安全的传输； 15.能安装 scapy 并能成功进入 scapy 数据包； 16.建立复合数据包对象成功,正确配置复合数据包各个对象的参数，成功进行 BPDU 数据包、VLAN 协议数据包、以太网数据包、IP 数据包、ICMP 协议数据包、TCP 协议数据包、RIP 数据包、DNS 协议数据包、HTTP 协议数据包的编辑和发送，并能对协议数据包进行抓包分析；
			专业素养： 1.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； 2.文档整洁、表达清晰、排版紧凑、符合要求； 3.举止文明、作业操作紧凑有序、有团队意识；

			4.把握用户需求正确，对项目质量完成判断专业，故障分析正确。 5.严格遵守系统安全、测试、安全管理工作规范；
2	岗位核心技能	网络安全设备配置	专业技能： 1.防火墙主机名、IP 地址配置正确，划分区域、安全级别配置正确，地址池配置正确，主 DNS、域名配置正确、DHCP 配置正确； 2.防火墙 NAT 配置正确，设计合理，能实现内网与公网的正确访问； 3.VPN 软件安装正确，根据需求配置 VPN 正确，能实现为远程客户机分配 IP 能实现使用路由和远程访问对连接请求验证身份； 4.创建 VPN 用户正确，修改 VPN 用户属性正确，VPN 连接正确； 5.防火墙、VPN 技术配置合理，能实现网络的安全配置与管理； 6.在路由器配置 GRE 隧道、路由协议配置正确，实现正常通信，查看隧道信息正确；
			专业素养： 1.项目实施过程符合网络安全工程设计、实施、测试的工作规范； 2.路由器、交换机、防火墙设备操作符合电子设备安全操作规范； 3.文档整洁、表达清晰、排版紧凑、符合要求； 4.举止文明、作业操作紧凑有序、有团队意识。
		系统安全攻防及运维安全管控	专业技能： 1.创建字典文件正确； 2.启动 Metaspoit 工具，正确加载 ssh_login 模块，并设置参数正确，实现 ssh 登录用户名和密码破解； 3.正确使用 X-Scan 工具进行漏洞扫描,正确获得操作系统登录用户名和密码； 4.启动 Metaspoit 工具，正确加载 ms17_010_psexec 模块，设置参数，正确渗透攻击至目标主机； 5.配置测试环境 Web 网站，正确编写、上传一句话木马，渗透 Web 服务器正确； 6.配置测试环境 Web 网站，设置代理，使用 Burp Suite 工具抓包，实现密码破解； 7.配置测试环境 Web 网站，设置 XSS 验证，成功获取站

			点 cookie 值； 8.配置测试环境 Web 网站，设置命令执行漏洞验证，成功判断操作系统；
			专业素养： 1.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； 2.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； 3.文档整洁、表达清晰、排版紧凑、符合要求； 4.举止文明、作业操作紧凑有序、有团队意识； 5.保证质量完成项目，具有应急处理能力，能把握项目关键点。

四、抽考方式

1.模块抽取

本专业技能考核标准的四个模块均为必考模块。按每个模块25%比例参考学生随机抽取考试模块，原则上所有模块都有学生参考，其中，参加核心技能考核的学生不少于参考学生的50%。各模块考生人数按四舍五入计算，剩余的尾数考生随机在四个模块中抽取应试模块。

2.项目抽取

每个考核模块均设若干考核项目。考生根据抽取的考核模块，随机从对应模块中随机抽取考核项目。

3.试题抽取

学生在相应项目题库中随机抽取1套试题进行测试。

五、附录

1.相关法律法规

2.相关规范与标准