网络安全服务

职业技能等级标准

标准代码：510028

（2021年 2.0版）

北京神州绿盟科技有限公司　制定

2021 年 12 月　发布

目　次

前　　言

本标准按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本标准起草单位：北京神州绿盟科技有限公司、北京航空航天大学、华中科技大学、甘肃政法大学、成都信息工程大学、红河学院、浙江警察学院、常州机电职业技术学院、常州信息职业技术学院、北京亿赛通科技发展有限责任公司、北京易霖博信息技术有限公司、北京西普阳光教育科技股份有限公司、北京金戈大通通信技术有限公司、广东精点数据科技股份有限公司、福建天闻教育发展有限公司、北京和信创天科技股份有限公司、北京星阑科技有限公司。

本标准主要起草人：叶建伟、胡斌、刘钟、杨方宇、毛剑、韩兰胜、安德智、张仕斌、骆洪军、斯进、顾卫杰、吴敏君、李永松、邢云汉、石伟辰、陈迪蝶、张云胜、李贺、徐鹏、林雪纲、李羿、许飞月、何钦淋、乔彩玉、刘瑞明、林陈铮、何光杰。

1 范围

本标准规定了网络安全服务职业技能等级对应的工作领域、工作任务及职业技能要求。

本标准适用于网络安全服务职业技能培训、考核与评价，相关用人单位的人员聘用、培训与考核可参照使用。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 20270-2006 信息安全技术 网络基础安全技术要求

GB/T 30283-2013 信息安全技术 信息安全服务 分类

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

GB/T 20985-2007 信息安全技术 信息安全事件管理指南

GB/T 20986-2007 信息安全技术 信息安全事件分类分级指南

3 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本标准。

3.1 信息安全 information security

保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质。

[GB/T 25069-2010，术语和定义 2.1.52]

3.2 通信安全 communication security

保护网络中所传输信息的完整性、保密性、可用性等。

[GB/T 25069-2010，术语和定义 2.1.38]

3.3 信息安全事件 information security incident

由单个或一系列意外或有害的信息安全事态所组成的，极有可能危害业务运行和威胁信息安全。

[GB/T 25069-2010，术语和定义 2.1.53]

3.4 安全级别 security level

有关敏感信息访问的级别划分，以此级别加之安全范畴能更精细地控制对数据的访问。

[GB/T 25069-2010，术语和定义 2.2.1.6]

3.5 安全服务 security service

根据安全策略，为用户提供的某种安全功能及相关的保障。

[GB/T 25069-2010，术语和定义 2.1.47]

3.6 脆弱性 vulnerability

资产中能被威胁所利用的弱点。

[GB/T 25069-2010，术语和定义 2.3.30]

3.7 入侵检测 intrusion detection

检测入侵的正式过程。该过程一般特征为采集如下知识：反常的使用模式，被利用的脆弱性及其类型、利用的方式，以及何时发生及如何发生。

[GB/T 25069-2010，术语和定义 2.2.1.100]

4 适用院校专业

4.1 参照原版专业目录

中等职业学校：计算机网络技术、计算机应用、网络安防系统安装与维护、网站

建设与管理等。

高等职业学校：信息安全与管理、计算机网络技术、计算机应用技术等。

职业教育本科及应用型本科学校：网络空间安全、信息安全、网络工程、计算机科学与技术、网络安全与执法等。

4.2　参照新版职业教育专业目录

中等职业学校：计算机网络技术、计算机应用、网络安防系统安装与维护、网站建设与管理、网络信息安全等。

高等职业学校：信息安全技术应用、计算机网络技术、计算机应用技术等。

高等职业教育本科学校：计算机应用工程、网络工程技术、信息安全与管理。

应用型本科学校：网络空间安全、信息安全、网络工程、计算机科学与技术、网络安全与执法等。

5　面向职业岗位（群）

【网络安全服务】(初级)：主要面向企事业单位、政府等信息安全部门或安服部门，从事网络安全实施、网络安全设备运维等工作岗位。

【网络安全服务】(中级)：主要面向企事业单位、政府等信息安全部门或安服部门，从事安全管理、等级保护、安全测试等工作岗位。

【网络安全服务】(高级)：主要面向企事业单位、政府等信息安全部门或安服部门，从事安全架构设计、安全应急响应、威胁分析、攻防对抗等工作岗位。

6　职业技能要求

6.1　职业技能等级划分

网络安全服务职业技能等级分为三个等级：初级、中级、高级，三个级别依次递进，高级别涵盖低级别职业技能要求。

【安全服务工程师】(初级):能够熟练掌握常见网络设备、操作系统、中间件、数据库的操作方法；能熟练使用主流安全设备；能完成初级告警日志分析；能完成常见漏洞的扫描,完成初级信息安全服务工作。

【安全服务工程师】(中级):能够熟练使用各类安全工具对组织信息资产安全脆弱性问题进行全面评估；能对安全问题进行落地加固整改；能熟练使用主流安全检测、防御产品和安全运营平台，完成中级信息安全服务工作。

【安全服务工程师】(高级):能够开展信息安全风险评估；能够评估现有攻击入侵路径，输出组织级安全防御方案，完成安全事件应急响应处置；能够指导初级、中级安全服务人员共同完成各项信息安全服务工作。

6.2　职业技能等级要求描述

表 1　网络安全服务职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1.基础安全协议分析	1.1 网络协议初识	1.1.1 能使用工具捕获网络数据包，并完成数据包分析。 1.1.2 能使用工具截取数据包，根据 HTTP 协议工作原理和 HTTP 报文结构，完成请求包和响应包的分析。 1.1.3 能根据 Burpsuite 代理的配置方法，进行 Burpsuite 工具的安装，利用 Burpsuite 工具实现 HTTP 通讯的截断、篡改和重放分析。 1.1.4 能通过通讯报文分析，判断目标 HTTP 通讯是否存在被监听、伪装、篡改的风险。
	1.2 网络协议安全分析	1.2.1 能抓包分析协议握手和通讯过程，基于数据包分析判断是否存在已知安全漏洞。 1.2.2 掌握 DNS 协议工作原理，通过分析双向数据包报文，判断是否存在域名劫持、拒绝服务等攻击。 1.2.3 能抓包分析双向数据包报文，判断是否存在 ARP 欺骗攻击。

2.信息系统安全操作	2.1 网络设备安全操作	2.1.1 能利用工具捕获数据帧，根据以太网数据帧和 MAC 地址格式，完成数据帧的分析。 2.1.2 能理解交换机工作原理，诊断常见网络故障。 2.1.3 理解路由器工作原理，诊断常见网络故障。
	2.2 操作系统安全操作	2.2.1 能根据 Linux 用户和用户组管理机制，新增、修改、删除用户和用户组账号口令。 2.2.2 能根据 Windows、Linux 文件权限管理机制，完成文件日常管理。 2.2.3 能根据 Windows、Linux 系统服务管理机制，查看服务状态、起停特定服务。 2.2.4 能根据 Windows 进程与端口管理方法，通过特定端口查找进程，通过命令行终止特定进程。 2.2.5 能根据 Windows 本地组策略机制，修改账号、口令管理配置。 2.2.6 能根据 Windows、Linux 系统日志留存机制，找到特定日志保存位置，能对日志文件进行分析。
	2.3 中间件安全操作	2.3.1 能根据常见 Web 应用架构，完成中间件应用 Nginx 的安装部署。 2.3.2 能根据 Nginx 配置文件结构，分析和修改配置文件，调整监听端口、日志记录、工作模式等。 2.3.3 能根据 Nginx 正向、反向代理和负载均衡原理，能完成功能配置。 2.3.4 能根据中间件日志留存机制，管理、分析 Nginx 应用日志。
	2.4 数据库安全操作	2.4.1 能根据不同的工作任务设定，选择适合的用户角色，完成数据库用户分类。 2.4.2 根据 SQL 查询语法，在数据库实例下，完成基本操作和简单的数据查询。 2.4.3 理解表空间概念，能通过 SQL 语言进行查询。 2.4.4 能根据数据库用户管理机制，通过 SQL 语言进行配置

		修改、用户增加和删除。 2.4.5 理解数据库密码策略安全，能通过查看、修改 Profile 配置文件调整密码管理策略。
3.网络安全事件分析	3.1 常见安全漏洞验证	3.1.1 能掌握常见的 Web 漏洞成因及危害，并给出通用修复方案，包括 SQL 注入、XSS、文件上传、系统提权、暴力破解、XXE、路径遍历、越权漏洞等。 3.1.2 掌握专项漏洞验证工具使用方法，能利用工具集完成手工验证。 3.1.3 能利用工具完成常见 Web 漏洞的手工验证。 3.1.4 能根据实际情况调整 SQLMAP 配置项检测、验证 SQL 注入漏洞。 3.1.5 能利用工具完成弱口令扫描和验证工作。
	3.2 常见安全设备维护	3.2.1 能根据防火墙工作原理，完成防火墙访问控制策略的调整。 3.2.2 掌握防火墙关键性能指标，能通过界面获取关键指标参数，能判断常见的设备故障和性能不足。 3.2.3 掌握 WAF/IDS/IPS 工作原理，准确查询安全告警日志，并且从告警日志中抽取关键攻击特征。 3.2.4 掌握 WAF/IDS/IPS 工作关键性能指标，能通过界面获取关键指标参数，能判断常见的设备故障和性能不足。
	3.3 设备告警日志分析	3.3.1 能通过 WAF 告警日志进行快速判断，确定分析思路，包括但不限于 SQL 注入、XSS、文件遍历、文件上传、文件包含、命令执行、Webshell 等。 3.3.2 能根据常见 DDoS 攻击特征，判断攻击类型，包括 SYN Flood、ACK Flood、ICMP Flood、等。 3.3.3 基于已有攻击线索，根据常见攻击入侵路径，展开分析操作。 3.3.4 通过人工分析、验证，根据常见攻击特征，判断攻击是否成功。

4.脆弱性评估与处置	4.1 安全漏洞扫描	4.1.1 根据安全漏洞扫描原理，能针对不同对象选择合适的漏洞扫描技术手段。 4.1.2 根据安全漏洞扫描产品使用方法，能根据实际情况调整扫描任务参数配置。 4.1.3 基于常见误漏报场景，能结合实际情况进行验证，并调整、输出最终扫描报告。 4.1.4 根据弱口令扫描原理，能配置弱口令扫描任务，并对扫描结果进行验证。
	4.2 安全配置基线检查	4.2.1 根据现场情况，结合不同的安全配置检查方式，选择合适的安全配置检查实施方法。 4.2.2 根据实际情况，结合安全配置检查产品的使用，调整安全配置检查产品的扫描任务参数配置。 4.2.3 对于安全配置检查产品的扫描结果，进行验证和调整，完成最终检查报告的输出。

表 2 网络安全服务职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1.对网络设备与操作系统安全脆弱性加固	1.1 路由交换常见漏洞加固	1.1.1 能制定路由交换通用漏洞解决方案。 1.1.2 能制定路由交换漏洞加固方案。 1.1.3 能对路由交换设备进行安全加固操作。
	1.2 路由交换安全配置优化	1.2.1 根据路由交换安全机制，能基于具体安全问题定位到需要调整、加固的安全模块。 1.2.2 能基于安全配置检查报告，给出可落地的路由交换配置加固方案。 1.2.3 能完成账号/口令管理、认证授权、日志审计、IP 协议族安全等配置加固。
	1.3 操作系统常见漏洞加固	1.3.1 结合 Windows 常见安全漏洞成因，给出通用漏洞解决方案，能完成以 MS17-010 为例的加固操作。 1.3.2 结合 Windows 常见安全漏洞加固过程中的常见问题，制定加固方案，降低加固风险。 1.3.3 结合 Linux 常见安全漏洞成因，能制定漏洞解决方案，

		以 SSH 系列漏洞为例掌握加固操作。 1.3.4 结合 Linux 常见安全漏洞加固过程中的常见问题，制定加固方案，降低加固风险。
	1.4 操作系统安全配置优化	1.4.1 基于 Windows/RedHat 系统安全机制，能快速定位到相应模块，对模块进行调整和加固。 1.4.2 能对 Windows 核心账号口令和日志进行安全配置，能完成修改关键配置参数的修改。 1.4.3 能对 Windows/RedHat 协议过滤及防火墙配置有所了解，能通过手工修改关键配置参数。 1.4.4 能找到 RedHat 认证授权配置文件位置与格式，通过调整 PAM 模块强化认证授权安全管控。 1.4.5 能对 RedHat 文件系统安全进行配置，识别关键文件，能对访问控制策略和权限进行调整。 1.4.6 能对 RedHat 服务进行配置，针对 SSH、FTP 等关键应用，完成对安全配置的有效调整。
2.对中间件与数据库安全脆弱性加固	2.1 中间件常见漏洞加固	2.1.1 能给出中间件通用漏洞解决方案。 2.1.2 结合中间件常见安全漏洞加固过程中的常见问题，制定加固方案，降低加固风险。 2.1.3 能根据加固方案，对不同的中间件完成漏洞加固操作。
	2.2 中间件安全配置优化	2.2.1 掌握 Apache 安全机制，能基于具体安全问题定位到需要调整、加固的安全模块。 2.2.2 能对 Apache 认证和授权进行安全配置，通过手工完成关键配置参数的修改。 2.2.3 能对 Apache 访问日志进行配置，通过手工完成关键配置参数的修改，包含日志调整和保存等。 2.2.4 能了解 Apache 关键安全配置，通过手工完成关键配置参数的修改。

	2.3 数据库常见漏洞加固	2.3.1 能给出数据库常见安全漏洞解决方案。 2.3.2 结合数据库常见安全漏洞加固过程中的常见问题，制定加固方案，降低加固风险。 2.3.3 能根据加固方案，对不同的数据库漏洞完成加固操作。
	2.4 数据库安全配置优化	2.4.1 掌握 Oracle 安全机制，能基于具体安全问题定位到需要调整、加固的安全模块。 2.4.2 能对 Oracle 核心账号口令、账号权限进行安全配置，能通过手工完成关键配置参数的修改。 2.4.3 能对 Oracle 安全日志和审计进行配置，能通过手工完成关键配置参数的修改。 2.4.4 根据 Oracle 安全组件原理，能通过手工完成关键配置参数的修改。 2.4.5 根据 Oracle 补丁更新机制，能通过查询具体漏洞编号，从官网检索到适合的补丁、补丁包。
3.高级网络安全事件分析	3.1 告警日志关联分析	3.1.1 能基于多产品、大日志文件抽取出关键信息。 3.1.2 根据告警日志核心要素及其分析方法，能基于关键信息提炼安全结论，提供安全事件判断依据。 3.1.3 基于常见事件场景，能从多维度进行关联分析结果的报告和呈现。
	3.2 安全设备策略优化	3.2.1 基于特征的检测规则误报原因及分析方法，能完成不同误报场景的分析，并判断是否为误报。 3.2.2 根据正则表达式语法，能针对数据包进行自定义正则匹配表达式。 3.2.3 能自定义正则表达式来调整相应防护策略。
	3.3 安全运营平台分析研判	3.3.1 能够基于安全运营平台，进行常见故障排查。 3.3.2 结合安全运营平台使用技巧，能运用安全运营平台对安全事件进行综合的分析研判。 3.3.3 结合当前常用 SAAS 安全能力，能将 SAAS 安全能力关联到具体工作任务当中。 3.3.4 掌握常用 SAAS 安全能力使用、操作方法，能结合互

		联网 SAAS 安全能力完成安全运营工作。

表 3 网络安全服务职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1. 安全风险评估与防御方案制定	1.1 信息安全风险评估	1.1.1 根据国内外常用风险评估标准，能根据实际需求选择适用的标准规范进行实施。 1.1.2 基于风险评估各关键要素及其关系，能根据实际情况编制风险评估方案。 1.1.3 基于安全风险计算模型，能根据实际需求选择合适的评价模型。 1.1.4 基于安全风险评估流程，组织项目成员进行合理分工，根据风险评估方案，完成风险评估实施。
	1.2 资产脆弱性评估	1.2.1 能根据实际情况调整、编制资产脆弱性评估方案，能针对特定组织梳理出安全相关资产清单。 1.2.2 能通过调研、访谈的方式，确认资产优先级。 1.2.3 结合资产优先级及脆弱性检查结果，评价各项脆弱性检查工作是否全面、细粒度是否足够。 1.2.4 能对已有脆弱性检查报告进行分析，提炼潜在的关键入侵突破口。 1.2.5 结合常见攻击手法和入侵路径，基于关键入侵突破口梳理出潜在攻击路径，定位关键问题资产。
	1.3 网络架构安全评估	1.3.1 结合行业网络安全标准规范，能根据行业特性对目标组织网络拓扑进行分析。 1.3.2 能基于目标网络特性，提出贴合实际情况的安全域划分建议。 1.3.3 能对安全域进行合理划分，并设计清晰的安全边界。
	1.4 评估攻击路径风险	1.4.1 能梳理内外部网络关键资产暴露面，明确是否存在不必要/不合规的通道。

		1.4.2 基于访问控制梳理方法，能评估网络边界访问控制措施强度与细粒度是否满足要求。 1.4.3 能针对潜在攻击路径检验现有安全监控防御措施是否充足。 1.4.4 结合常见安全问题的加固措施，能针对潜在攻击路径给出针对性的安全加固建议。 1.4.5 综合资产脆弱性评估、网络架构安全评估以及攻击路径风险评估的结果，能整理输出符合特定组织现状的安全防御方案。
2. 安全事件应急响应	2.1 应急响应准备	2.1.1 根据应急响应模型，能基于企业安全能力现状，设计总体应急预案，明确应急组织与职责。 2.1.2 基于常见安全事件分类分级，能基于企业风险现状，编制系列专题安全应急预案。 2.1.3 能根据专题应急预案，结合企业现状，设计安全应急演练流程，形成演练方案。 2.1.4 能基于演练方案开展应急演练工作，识别潜在的流程和设计缺陷，能提出整改优化建议。
	2.2 识别安全事件	2.2.1 能关联分析、使用告警日志，识别安全事件。 2.2.2 基于安全事件分析三要素法，能从时间、地点、事件三个维度切入，梳理攻击入侵路径。 2.2.3 能基于工具进行验证，评估可疑入侵尝试是否成功，并得到受事件影响资产范围。
	2.3 事件分析与侦查	2.3.1 基于安全事件分类分级标准，能根据不同场景选择合适的应急预案和应急流程作。 2.3.2 能完成网络连接、进程、历史命令、后门账号、计划任务、登录日志、自启动项、恶意文件等维度的入侵排查分析工作。 2.3.3 基于 Web 应用排查指南，能围绕 Web 应用完成 Webshell 排查，能基于日志分析定位入侵行为。
	2.4 事件取	2.4.1 能基于特定安全事件应急响应场景，选择合适的快速

	证与隔离	保护方法，保护关键证据不被删除、覆盖。 2.4.2 基于取证与隔离操作标准，能快速定位到需要取证的文件/日志/流量，并使用工具取证留存。 2.4.3 对于可疑资产对象，能基于已掌握的信息，快速落实隔离措施，将安全风险控制到最低。 2.4.4 掌握常见安全问题临时加固方法，能运用加固工具，对目标失陷资产进行临时补救加固。

参考文献

[1] 《高等职业学校专业教学标准（2019版）》

[2] 《本科专业类教学质量国家标准》

[3] 《中等职业学校专业教学标准（试行）》

[4] 教育部关于印发《职业教育专业目录（2021年）》的通知（教职成〔2021〕2号）

[5] 教育部关于公布《2020年度普通高等学校本科专业备案和审批结果的通知》（教高函〔2021〕1号）

[6]教育部关于公布《2019年度普通高等学校本科专业备案和审批结果的通知》（教高函〔2020〕2号）

[7] 《国家职业技能标准编制技术规程（2018年版）》

[8] 《中华人民共和国网络安全法》

[9] 《信息安全技术网络安全等级保护基本要求（GB-T 22239-2019 ）》

[10] 《信息安全技术网络安全等级保护测评要求（GB/T 28448-2019）》

[11] 《信息安全技术网络安全等级保护安全设计技术要求（GB/T 25070-2019）》

[12] 《中华人民共和国职业分类大典（2015版）》