网络安全运营平台管理

职业技能等级标准

标准代码：510035

（2021年2.0版）

深信服科技股份有限公司　制定

2021年12月　**发布**

目　次

前言.....1

1.范围.....2

2.规范性引用文件.....2

3.术语和定义.....2

4.适用院校专业.....4

5.面向职业岗位（群）.....5

6.职业技能要求.....5

参考文献.....11

前　　言

本标准按照GB/T1.1-2020《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：深信服科技股份有限公司、暨南大学、北京邮电大学、青岛大学、吉利学院、深圳职业技术学院、深圳信息职业技术学院、天津职业大学、深圳技师职业学院、北京信息职业技术学院、武汉职业技术学院、重庆电子工程职业学院、内蒙古电子信息职业技术学院、许昌职业技术学院、盐城工业职业技术学院、山东商业职业技术学院、河南司法警官职业学院、河南信息工程学校。

本标准主要起草人：魏林锋、雷敏、咸鹤群、吕峻闽、王隆杰、柳伟、张景强、廖银萍、史宝会、杨旭东、武春岭、郝俊寿、孟敏杰、王国军、单锦宝、王惠斌、余飞跃、李文杰、李洋、严波、黄浩、袁泉、石岩、傅先全、迟忠旸、吕沐阳、代亭亭。

1 范围

本标准规定了网络安全运营平台管理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运营平台管理职业技能等级培训、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/Z 20985-2007 信息技术安全技术信息安全事件管理指南

GB/T 22080-2016 信息安全技术信息安全管理体系要求

GB/T 20282-2006 信息安全技术信息系统安全工程管理要求

GBZ 20986-2007 信息安全技术信息安全事件分类分级指南

GB/T 24363-2009 信息安全技术信息安全应急响应计划规范

GB/T 33132-2016 信息安全技术信息安全风险处理实施指南

GB/T 36626-2018 信息安全技术信息系统安全运维管理指南

GB/T 25069-2010 信息安全技术术语

3 术语和定义

3.1 计算机信息系统 computerinformationsystem

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

[GB/T25069-2010，定义2.1.14]

3.2 信息安全 informationsecurity

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/T25069-2010，定义2.1.53]

3.3 **信息安全事件 informationsecurityincident**

由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

[GB/T25069-2010，定义2.1.54]

3.4 **攻击者 attacker**

故意利用技术上或非技术上的安全弱点，以窃取或泄露信息系统或网络的资源，或危及信息系统或网络资源可用性的任何人。

[GB/T25069-2010，定义2.1.7]

3.5 **脆弱性 vulnerability**

资产中能被威胁所利用的弱点。

[GB/T25069-2010，定义2.3.30]

3.6 **风险 risk**

一个给定的威胁，利用一项资产或多项资产的脆弱性，对组织造成损害的潜能。可通过事件的概率及其后果进行度量。

[GB/T25069-2010，定义2.3.35]

3.7 **威胁 threat**

对资产或组织可能导致负面结果的一个事件的潜在源。

[GB/T25069-2010，定义2.3.94]

3.8 **威胁分析 threatanalysis**

对信息处理系统的威胁源所做的查考及其可能引起负面结果的推断。

[GB/T25069-2010，定义2.3.96]

3.9 **安全服务 securityservice**

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/T25069-2010，定义2.1.48]

3.10 安全审计 securityaudit

对信息系统的各种事件及行为实行监测、信息采集、分析，并针对特定事件及行为采取相应的动作。

[GB/T25069-2010，定义2.2.1.8]

3.11 检查评估 inspectionassessment

由被评估组织的上级主管机关或业务主管机关发起的，依据国家有关法规与标准，对信息系统及其管理进行的具有强制性的检查活动。

[GB/T20984-2007，定义3.9]

3.12 安全事件 securityincident

指系统、服务或网络的一种可识别状态的发生，它可能是对信息安全策略的违反或护措施的失效，或未预知的不安全状况。

[GB/T20984-2007，定义3.14]

3.13 安全措施 securitymeasure

保护资产、抵御威胁、减少脆弱性、降低安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制。

[GB/T20984-2007，定义3.15]

4 适用院校专业

4.1 参照原版专业目录

中等职业学校：网络安防系统安装与维护、计算机应用、计算机网络技术、通信技术、网络信息安全等相关专业。

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、信息网络安全监察等相关专业。

应用型本科学校：信息安全、通信工程、计算机应用工程、网络空间安全、网络工程、计算机科学与技术、网络安全与执法等相关专业。

4.2 参照新版职业教育专业目录

中等职业学校：物联网技术应用、计算机应用、计算机网络技术、软件与信息服务、大数据技术应用、移动应用技术与服务、网络信息安全、网络安防系统安装与维护等相关专业。

高等职业学校：物联网应用技术、移动互联应用技术、计算机应用技术、计算机网络技术、软件技术、大数据技术、云计算技术应用、信息安全技术应用、密码技术应用等相关专业。

应用型本科学校：信息安全、通信工程、计算机应用工程、网络空间安全、网络工程、计算机科学与技术、网络安全与执法、密码科学与技术等相关专业。

高等职业教育本科学校：计算机应用工程、网络工程技术、软件工程技术、大数据工程技术、云计算技术、信息安全与管理等相关专业。

5 面向职业岗位（群）

主要面向网络空间安全领域、IT互联网企业、企事业单位、政府等信息安全部门或安全服务部门，从事服务器安装与运维、网络渗透、网络安全运营、安全服务、应急响应等岗位工作。

6 职业技能要求

6.1 职业技能等级划分

网络安全运营平台管理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。

【网络安全运营平台管理】（初级）：能根据任务要求完成网络安全形势解读、网络安全法律解读、服务器操作系统使用、网络协议分析、渗透测试工

具的使用和 HTTP 协议的分析;

【网络安全运营平台管理】（中级）：能根据任务要求完成 PHP 代码的读写和 Web 漏洞代码分析、部分 Web 漏洞挖掘、网络安全运营服务、安全运营平台组建和密码学的应用;

【网络安全运营平台管理】（高级）：能根据任务要求完成渗透测试、常见 Web 漏洞挖掘、基线安全配置、安全事件管理处置、安全运营中心建设。

6.2 职业技能等级要求描述

表 1 网络安全运营平台管理职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1.网络安全法律法规解读	1.1 网络安全认知	1.1.1 能根据工作任务需求，分析网络安全体系框架。 1.1.2 能根据工作任务需求，分析网络安全发展形势。 1.1.3 能根据工作任务需求，分析简单网络安全事件。
	1.2 网络安全法律法规解读与相关案例分析	1.2.1 能根据国家相关规定，解读《中华人民共和国网络安全法》。 1.2.2 能根据国家相关规定，解读《网络安全等级保护》。 1.2.3 能根据国家相关规定，分析相关网络安全案例。
2.网络安全运维	2.1 操作系统使用	2.1.1 能根据工作任务需求，分析操作系统原理。 2.1.2 能根据工作任务需求，使用 Linux 操作系统。 2.1.3 能根据工作任务需求，使用 Windows 操作系统。
	2.2 网络协议基础分析	2.2.1 能根据工作任务需求，使用 Wireshark 工具分析网络协议。 2.2.2 能根据工作任务需求，使用 Tcpdump 工具分析网络协议。 2.2.3 能根据工作任务需求，分析数据链路层、网络层协议。 2.2.4 能根据工作任务需求，分析传输层协议。 2.2.5 能根据工作任务需求，分析应用层协议。

3.网络安全渗透应用	3.1 网络渗透基础	3.1.1 能根据工作任务需求，分析 HTTP 协议。 3.1.2 能根据工作任务需求，使用 kali 环境搭建方法。 3.1.3 能根据工作任务需求，使用 kali 系统工具。 3.1.4 能根据工作任务需求，使用常用浏览器插件。
4.网络安全设备运维	4.1 网络安全设备安装与使用	4.1.1 能根据工作任务需求，安装并使用边界安全设备。 4.1.2 能根据工作任务需求，安装并使用终端安全设备。 4.1.3 能根据工作任务需求，安装并使用数据传输安全设备。 4.1.4 能根据工作任务需求，安装并使用移动接入安全设备。 4.1.5 能根据工作任务需求，安装并使用上网安全可视设备。

表 2 网络安全运营平台管理职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1.PHP开发技能	1.1 PHP漏洞环境编写与数据库操作	1.1.1能根据工作任务需求，使用PHP循环与函数。 1.1.2能根据工作任务需求，使用PHP数组和字符串的技能。 1.1.3能根据工作任务需求，使用PHP表单及文件操作。 1.1.4能根据工作任务需求，使用PHP正则表达式。
	1.2 PHP开发应用	1.2.1能根据工作任务需求，使用PHP会话控制及数据库操作。 1.2.2能根据工作任务需求，编写PHP文件上传功能。 1.2.3能根据工作任务需求，编写网站爬虫。
2.Web安全漏洞测试	2.1 SQL注入漏洞挖掘	2.1.1能根据工作任务需求，操作数据库。 2.1.2能根据工作任务需求，分析SQL注入漏洞原理、危害、利用等。 2.1.3能根据工作任务需求，挖掘字符型与数字型的SQL注入漏洞。

	2.2 XSS漏洞挖掘	2.2.1能根据工作任务需求，分析会话管理机制。 2.2.2能根据工作任务需求，掌握Session攻击的方法。 2.2.3能根据工作任务需求，分析Cookie安全机制。 2.2.4能根据工作任务需求，挖掘XSS跨站脚本漏洞。
	2.3命令执行漏洞挖掘	2.3.1能根据工作任务需求，分析命令执行漏洞原理。 2.3.2能根据工作任务需求，分析命令执行常见函数与场景。 2.3.3能根据工作任务需求，从源码角度分析命令执行漏洞。 2.3.4能根据工作任务需求，挖掘命令执行相关漏洞。
3.网络安全运营服务与组建	3.1网络安全运营认知	3.1.1能根据工作任务需求，分析网络安全运营的概念和模型。 3.1.2能根据工作任务需求，分析网络安全运营的目标和模式。
	3.2网络安全运营服务	3.2.1能根据工作任务需求，分析网络安全运营服务的概念。 3.2.2能根据工作任务需求，分析网络安全运营服务的职责划分。 3.2.3能根据工作任务需求，分析网络安全运营服务的内容与模式。 3.2.4能根据工作任务需求，管理网络安全运营服务的项目。
	3.3网络安全运营平台组建建设	3.3.1能根据工作任务需求，部署网络安全运营平台。 3.3.2能根据工作任务需求，使用网络安全运营技术。 3.3.3能根据工作任务需求，理解网络安全运营平台应用场景。
	3.4密码学应用	3.4.1能根据工作任务需求，使用古典密码学。 3.4.2能根据工作任务需求，使用对称密码。 3.4.3能根据工作任务需求，使用公钥密码。 3.4.4能根据工作任务需求，使用密码交换。 3.4.5能根据工作任务需求，使用哈希密码。

表 3 网络安全运营平台管理职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1.渗透测试	1.1渗透测试流程梳理	1.1.1能根据工作任务需求，解读网络渗透测试执行标准。 1.1.2能根据工作任务需求，完成渗透测试相关工作。 1.1.3能根据工作任务需求，编写网络渗透测试报告。
	1.2信息收集	1.2.1能根据工作任务需求，使用各种工具、Google Hacking语法、网络空间搜索引擎、社工库等各种方法收集DNS、子域名、C段、Web目录、指纹等各种信息。 1.2.2能根据工作任务需求，进行情报分析。 1.2.3能根据工作任务需求，进行网站克隆和钓鱼。
2.漏洞挖掘	2.1 SQL注入漏洞挖掘	2.1.1能根据工作任务需求，利用各种手法挖掘SQL注入漏洞。 2.1.2能根据工作任务需求，使用SQLmap工具挖掘SQL注入漏洞。 2.1.3能根据工作任务需求，对SQL注入漏洞进行防御。
	2.2 XSS漏洞挖掘	2.2.1能根据工作任务需求，掌握Cookie攻击的方法。 2.2.2能根据工作任务需求，使用XSS相关工具挖掘XSS漏洞。 2.2.3能根据工作任务需求，分析XSS防御和挖掘思路。
	2.3文件上传漏洞挖掘	2.3.1能根据工作任务需求，分析文件上传漏洞原理、危害等。 2.3.2能根据工作任务需求，利用文件上传各种绕过方法绕过上传限制。 2.3.3能根据工作任务需求，利用Web容器解析漏洞绕过上传限制。 2.3.4能根据工作任务需求，利用Tomcat容器漏洞进行任意文件上传。
	2.4文件包含漏洞挖掘	2.4.1能根据工作任务需求，分析文件包含漏洞原理。 2.4.2能根据工作任务需求，挖掘文件包含漏洞。 2.4.3能根据工作任务需求，对文件包含漏洞进行防御。

	2.5逻辑漏洞挖掘	2.5.1能根据工作任务需求，分析逻辑漏洞原理。 2.5.2能根据工作任务需求，挖掘逻辑漏洞。 2.5.3能根据工作任务需求，对逻辑漏洞进行防御。
3.网络安全运营中心组建	3.1基线管理与安全配置	3.1.1能根据工作任务需求，进行Windows基线安全配置。 3.1.2能根据工作任务需求，进行Linux基线安全配置。 3.1.3能根据工作任务需求，进行mariadb基线安全配置。 3.1.4能根据工作任务需求，进行mongodb基线安全配置。
	3.2安全事件管理处置	3.2.1能根据工作任务需求，理解应急响应概念、事件分级分类和处置思路。 3.2.2能根据工作任务需求，进行windows应急响应。 3.2.3能根据工作任务需求，进行Linux应急响应。 3.2.4能根据工作任务需求，进行web网站应急响应。
	3.3安全运营流程建设	3.3.1能根据工作任务需求，理解安全运营工作策略、日常制度。 3.3.2能根据工作任务需求，制定安全运营常用流程。 3.3.3能根据工作任务需求，进行重大活动保障及制度建设。
	3.4安全运营中心建设与应用	3.4.1能根据工作任务需求，理解终端安全和服务器安全检测与防御技术。 3.4.2能根据工作任务需求，理解安全评估与动态检测技术。 3.4.3能根据工作任务需求，进行xhack安全测试。 3.4.4能根据工作任务需求，使用高可用性配置方法。 3.4.5能根据工作任务需求，掌握态势感知上架部署和常用功能使用。

参考文献

[1]《信息安全技术信息安全风险处理实施指南》GBT33132-2016

[2]《信息安全技术信息安全风险评估实施指南》GB/T31509-2015

[3]《信息安全技术信息安全风险评估规范》GB/T20984-2007

[4]《信息安全技术信息安全管理体系要求》GB/T22080-2016

[5]《信息安全技术信息安全控制实践指南》GB/T22081-2016

[6]《信息安全技术信息安全应急响应计划规范》GB/T24363-2009

[7]《信息安全技术信息安全风险管理指南》GB/Z24364-2009

[8]《信息技术安全技术信息安全事件管理指南》GB/Z20985-2007

[9]《信息安全技术信息安全事件分类分级指南》GB/Z20986-2007

[10]《信息安全技术信息系统安全工程管理要求》GB/T20282-2006

[11]《信息安全技术网络基础安全技术要求》GB/T20270-2006

[12]《信息安全技术信息系统安全管理平台技术要求和测试评价方法》GB/T34990-2017

[13]《信息安全技术信息安全服务分类》GB/T30283-2013

[14]《信息安全技术网络安全等级保护基本要求》GB/T22239-2019

[15]《信息安全技术术语》GB/T25069-2010

[16]《信息安全技术信息系统安全运维管理指南》GB/T36626-2018

[17] 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）

[18]《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）

[19]《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）