

网络安全运营平台管理

职业技能等级标准

(2021年1.0版)

深信服科技股份有限公司 制定

2021年4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	10

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：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、聊城职业技术学院、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、徐洪祥、赵科、李展、李洋、严波、黄浩、袁泉、石岩、方明理、迟忠旻、吕沐阳、祖少良。

声明：本标准的知识产权归属深信服科技股份有限公司，未经深信服科技股份有限公司同意，不得印刷、销售。

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 computer information system

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/T 25069-2010，定义 2.1.14]

3.2 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, 定义 2.1.53]

3.3 信息安全事件 information security incident

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/T 25069-2010, 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/T 25069-2010, 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/T 25069-2010, 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/T 25069-2010, 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/T 25069-2010, 定义 2.3.94]

3.8 威胁分析 threat analysis

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/T 25069-2010, 定义 2.3.96]

3.9 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, 定义 2.1.48]

3.10 安全审计 security audit

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/T 25069-2010, 定义 2.2.1.8]

3.11 检查评估 inspection assessment

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/T 20984-2007, 定义 3.9]

3.12 安全事件 security incident

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防护措施失效, 或未预知的不安全状况。

[GB/T 20984-2007, 定义 3.14]

3.13 安全措施 security measure

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/T 20984-2007, 定义 3.15]

4 适用院校专业

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、网络信息安全等计算机类相关专业。

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计算机类相关专业。

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

5 面向职业岗位（群）

【网络安全运营平台管理】（初级）：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，从事网络安全设备安装、网络安全设备维护、网络安全运维等岗位工作。

【网络安全运营平台管理】（中级）：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，从事网络安全设备配置、网络安全设备交付、网络安全运营服务等岗位工作。

【网络安全运营平台管理】（高级）：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，从事渗透测试、风险评估、资产管理与识别、安全基线检查、安全加固、漏洞扫描、安全事件分析、网络安全运营管理等岗位工作。

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设备安装、网络安全设备维护、系统服务器配置、网络安全运维等工作。

【网络安全运营平台管理】（中级）：能根据任务要求完成网络安全设备配置、网络安全设备交付、网络安全现场调试、网络安全设备故障处理、网络安全运营服务等工作。

【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、风险评估、资产管理与识别、安全基线检查、安全加固、漏洞扫描、安全事件分析、网络安全运营管理工作。

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	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，分析网络安全发展形势
	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，解读《信息安全风险评估实施指南》 1.2.4 能根据国家相关规定，解读《网络安全事件应急演练指南》
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

工作领域	工作任务	职业技能要求
		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	3.1 密码学研究	3.1.1 能根据工作任务需求,使用古典密码学 3.1.2 能根据工作任务需求,使用对称密码 3.1.3 能根据工作任务需求,使用公钥密码 3.1.4 能根据工作任务需求,使用密码交换 3.1.5 能根据工作任务需求,使用哈希密码
	3.2 网络渗透基础分析与实践	3.2.1 能根据工作任务需求,分析HTTP协议 3.2.2 能根据工作任务需求,使用kali环境搭建方法 3.2.2 能根据工作任务需求,使用kali系统工具 3.2.3 能根据工作任务需求,使用常用浏览器插件
4. 网络安全设备安装与维护	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,使用边界安全设备 4.1.2 能根据工作任务需求,使用终端安全设备 4.1.3 能根据工作任务需求,使用身份与访问安全设备 4.1.4 能根据工作任务需求,使用威胁检测设备 4.1.5 能根据工作任务需求,使用安全审计与运营设备

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	1.1.1 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

工作领域	工作任务	职业技能要求
		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,使用Session攻击 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 网络安全运营平台组建	3.1.1 能根据工作任务需求,组建网络安全运营组织 3.1.2 能根据工作任务需求,使用网络安全运营服务 3.1.3 能根据工作任务需求,配置网络安全设备

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DNS信息收集方法 1.2.2 能根据工作任务需求,使用子域名收集方法 1.2.3 能根据工作任务需求,使用C段扫描方法 1.2.4 能根据工作任务需求,使用Web目录扫描方法 1.2.5 能根据工作任务需求,使用指纹识别方法 1.2.6 能根据工作任务需求,使用GoogleHacking方法

工作领域	工作任务	职业技能要求
		1.2.7 能根据工作任务需求,使用网络空间搜索引擎方法 1.2.8 能根据工作任务需求,使用情报分析方法 1.2.9 能根据工作任务需求,使用社工库方法
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,使用Cookie攻击 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 安全运维管理	3.1.1 能根据工作任务需求,安全管理资产 3.1.2 能根据工作任务需求,使用安全风险评估方法 3.1.3 能根据工作任务需求,对安全事件进行分析和处置
	3.2 安全运营中心组建	3.2.1 能根据工作任务需求,制定安全运营流程 3.2.2 能根据工作任务需求,建设安全运营中心

参考文献

- [1] GB/T 33132-2016 信息安全技术 信息安全风险处理实施指南
- [2] GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南
- [3] GB/T 20984-2007 信息安全技术 信息安全风险评估规范
- [4] GB/T 22080-2016 信息安全技术 信息安全管理体系要求
- [5] GB/T 22081-2016 信息安全技术 信息安全控制实践指南
- [6] GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范
- [7] GB/Z 24364-2009 信息安全技术 信息安全风险管理指南
- [8] GB/Z 20985-2007 信息技术 安全技术 信息安全事件管理指南
- [9] GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南
- [10] GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求
- [11] GB/T 20270-2006 信息安全技术 网络基础安全技术要求
- [12] GB/T 34990-2017 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
- [13] GB/T 30283-2013 信息安全技术 信息安全服务 分类
- [14] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
- [15] GB/T 25069-2010 信息安全技术 术语
- [16] GB/T 36626-2018 信息安全技术 信息系统安全运维管理指南
- [17] 中等职业学校专业目录
- [18] 普通高等学校高等职业教育（专科）专业目录
- [19] 普通高等学校本科专业目录