网络安全运维

职业技能等级标准

（2020年2.0版）

中科软科技股份有限公司　制定

2020 年 3 月　发布

目　次

前　　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准起草单位：中科软科技股份有限公司、北京中科磐云科技有限公司、北京师范大学、北京理工大学、北京信息职业技术学院、常州信息职业技术学院、深圳信息职业技术学院、湖北生物科技职业学院、贵州电子职业技术学院、北京市求实职业学校、北京市信息管理学校等。

本标准主要起草人：宫亚峰、孙波、李宝林、罗森林、史宝会、杨诚、龙翔、蔡铁、曹炯清、彭金华、杨毅、何琳、胡志齐、徐雪鹏、孙雨春、邹君雨、张天乐等。

1 范围

本标准规定了网络安全运维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维职业技能培训、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 36626-2018 信息安全技术 信息系统安全运维管理指南

GB/T 20271-2006 信息安全技术信息系统通用安全技术要求

GB/T 20270-2006 信息安全技术网络基础安全技术要求

GB/T 20272-2006 信息安全技术操作系统安全技术要求

GB/T 20273-2006 信息安全技术数据库管理系统安全技术要求

GB/T 20269-2006 信息安全技术信息系统安全管理要求

GA/T 671-2006 信息安全技术终端计算机系统安全等级技术要求

GB 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 25069-2010 信息安全技术 术语

3 术语和定义

GB/T 25069-2010界定的以及下列术语适用于本标准。

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、抗依赖性、可靠性等性质。

[GB/T 25069-2010，定义 2.1.52]

3.2 **信息系统安全 IT security**

与定义、获得和维护保密性、完整性、可用性、可核查性、真实性和可靠性有关的各个方面。

[GB/T 25069-2010，定义 2.1.57]

3.3 **风险评估 risk assessment**

风险标识、分析和评价的整个过程。

[GB/T 25069-2010，定义 2.3.44]

3.4 **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 2.1.47]

3.5 **渗透测试 penetration testing**

以未经授权的动作绕过某一系统的安全机制的方式，检查数据处理系统的安全功能，以发现信息系统安全问题的手段。

[GB/T 25069-2010，定义 2.3.87]

3.6 **网络安全策略 network security policy**

由陈述、规则和惯例等组成的集合，说明其使用网络资源的组织途径，并指明如何保护网络基础设施和服务。

[GB/T 25069-2010，定义 2.3.92]

4 适用院校专业

中等职业学校：网络信息安全、计算机应用、计算机网络技术、网站建设与管理、软件与信息服务等专业。

高等职业学校：信息安全与管理、计算机应用技术、计算机网络技术、计算机信息管理、计算机系统与维护等专业。

应用型本科学校：信息安全、网络空间安全、计算机科学与技术、网络工程等专业。

5 面向职业岗位（群）

【网络安全运维】（初级）：主要面向 IT 互联网企业、企事业单位、政府部门等的信息安全部门或安服部门，从事网络安全策略部署、操作系统安全管理与维护、系统安全测试、网络安全测试等工作岗位。

【网络安全运维】（中级）：主要面向 IT 互联网企业、企事业单位、政府部门等的信息安全部门或安服部门，从事网络安全渗透测试、系统安全加固、Web 安全防护、网络安全项目集成等工作岗位。

【网络安全运维】（高级）：主要面向 IT 互联网企业、企事业单位、政府部门等的信息安全部门或安服部门，从事网络安全渗透测试、风险评估、企业 Web 安全防护，网络安全方案咨询、风险评估及网络安全产品售前、售后等工作岗位。

6 职业技能要求

6.1 职业技能等级划分

网络安全运维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。

【网络安全运维】（初级）：根据网络和系统安全需求，完成常见操作系统的安全管理与维护、网络安全策略的部署、常见操作系统和网络安全的渗透测试等作业。

【网络安全运维】（中级）：根据网络和系统安全需求，使用各类安全工具对常见操作系统进行漏洞诊断及安全加固，完成系统安全渗透测试和 Web 安全防护等作业。

【网络安全运维】（高级）：根据网络和系统安全需求，完成对网络安全和系统安全进行风险评估、Web 安全的诊断及加固，网络安全方案的设计和咨询、入侵行为检测及安全攻防等作业。

6.2 职业技能等级要求描述

表 1 网络安全运维职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1.Windows 操作系统安全配置	1.1Windows 操作系统安全配置	1.1.1 能根据 Windows 操作系统安全配置工作任务书要求，完成用户和组的安全管理。 1.1.2 能根据 Windows 操作系统安全配置工作任务书要求，完成文件系统安全配置。 1.1.3 能根据 Windows 操作系统安全配置工作任务书要求，完成服务安全配置。 1.1.4 能根据 Windows 操作系统安全配置工作任务书要求，完成域与活动目录安全管理。 1.1.5 能根据 Windows 操作系统安全配置工作任务书要求，完成防火墙安全配置。
2.Linux 操作系统安全配置	2.1Linux 操作系统安全配置	2.1.1 能根据 Linux 操作系统安全配置工作任务书要求，完成用户和组的安全管理。 2.1.2 能根据 Linux 操作系统安全配置工作任务书要求，完成 SSH 服务的安全配置。 2.1.3 能根据 Linux 操作系统安全配置工作任务书要求，完成 Apache 服务的安全配置。 2.1.4 能根据 Linux 操作系统安全配置工作任务书要求，完成 vsftpd 服务的安全配置。 2.1.5 能根据 Linux 操作系统安全配置工作任务书要求，完成 Samba 服务的安全配置。 2.1.6 能根据 Linux 操作系统安全配置工作任务书要求，完成防火墙安全配置。

工作领域	工作任务	职业技能要求
3.渗透测试常用工具	3.1 数据包分析	3.1.1 能根据数据包分析工作任务书要求，使用 Wireshark 完成网络嗅探。 3.1.2 能根据数据包分析工作任务书要求，使用 Dsniff 完成网络嗅探。 3.1.3 能根据数据包分析工作任务书要求，使用 TCPDump 完成数据包抓取。
	3.2 目标主机识别	3.2.1 能根据目标主机识别工作任务书要求，使用 Arping 工具完成目标主机识别。 3.2.2 能根据目标主机识别工作任务书要求，使用 Fping 工具完成目标主机识别。 3.2.3 能根据目标主机识别工作任务书要求，使用 GenList 工具完成目标主机识别。 3.2.4 能根据目标主机识别工作任务书要求，使用 NBTScan 工具完成目标主机识别。 3.2.5 能根据目标主机识别工作任务书要求，使用 P0f 工具完成目标主机识别。 3.2.6 能根据目标主机识别工作任务书要求，使用 Xprobe2 工具完成目标主机识别。 3.2.7 能根据目标主机识别工作任务书要求，使用 Autoscan 工具完成目标主机识别。 3.2.8 能根据目标主机识别工作任务书要求，使用 Nmap 工具完成目标主机识别。 3.2.9 能根据目标主机识别工作任务书要求，使用 Zenmap 工具完成目标主机识别。
	3.3 漏洞检测	3.3.1 能根据漏洞检测工作任务书要求，使用 Metasploit 完成漏洞验证。 3.3.2 能根据漏洞检测工作任务书要求，使用 Meterpreter 模块完成渗透测试。
4.操作系统漏洞验证及加固	4.1 操作系统漏洞验证及加固	4.1.1 能根据操作系统漏洞验证及加固工作任务书要求，完成 MS08_067 漏洞验证与安全加固。 4.1.2 能根据操作系统漏洞验证及加固工作任务书要求，完成 MS10_003 漏洞验证与安全加固。 4.1.3 能根据操作系统漏洞验证及加固工作任务书要求，完成 MS12_020 漏洞验证与安全加固。 4.1.4 能根据操作系统漏洞验证及加固工作任务书要求，完成 MS15_034 漏洞验证与安全加

工作领域	工作任务	职业技能要求
		固。 4.1.5 能根据操作系统漏洞验证及加固工作任务书要求，完成 MS14_064 漏洞验证与安全加固。 4.1.6 能根据操作系统漏洞验证及加固工作任务书要求，完成 MS17_010 漏洞验证与安全加固。

表 2 网络安全运维职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1.渗透测试常用工具	1.1 密码破解测试	1.1.1 能根据密码破解测试工作任务书要求，使用 Hydra 完成密码破解测试。 1.1.2 能根据密码破解测试工作任务书要求，使用 Metasploit 完成密码破解测试。
	1.2 Web 渗透测试	1.2.1 能根据 Web 渗透测试工作任务书要求，使用 Vega 完成漏洞扫描。 1.2.2 能根据 Web 渗透测试工作任务书要求，使用 Ferret 完成 Cookie 劫持测试。 1.2.3 能根据 Web 渗透测试工作任务书要求，使用 W3af 完成 Web 渗透测试。
	1.3 木马生成测试	1.3.1 能根据木马生成测试工作任务书要求，使用 Weevely 工具完成木马上传测试。 1.3.2 能根据木马生成测试工作任务书要求，使用 Beef 完成对客户端浏览器劫持测试。 1.3.3 能根据木马生成测试工作任务书要求，使用 Netcat 完成反弹连接测试。 1.3.4 能根据木马生成测试工作任务书要求，使用 Msfvenom 生成木马完成渗透测试。
	1.4 内网渗透测试	1.4.1 能根据内网渗透测试工作任务书要求，使用 ARPspoof 完成中间人渗透测试。 1.4.2 能根据内网渗透测试工作任务书要求，使用 Ptunnel 完成内网穿透测试。 1.4.3 能根据内网渗透测试工作任务书要求，使用 Stunnel 完成内网穿透测试。 1.4.4 能根据内网渗透测试工作任务书要求，使用 3proxy 完成内网穿透测试。
2.安全漏洞验证及加固	2.1Windows 漏洞验证及加固	2.1.1 能根据 Windows 漏洞验证及加固工作任务书要求，验证使用 CVE-2017-7269 漏洞渗透

工作领域	工作任务	职业技能要求
		IIS6.0 实现远程控制试。 2.1.2 能根据 Windows 漏洞验证及加固工作任务书要求，验证使用 CVE-2017-8464 漏洞实现 LNK 文件远程代码执行。 2.1.3 能根据 Windows 漏洞验证及加固工作任务书要求，验证使用 CVE-2018-4878 漏洞上传实现远程控制。
	2.2 Linux 漏洞验证及加固	2.2.1 能根据 Linux 漏洞验证及加固工作任务书要求,验证使用 CVE-2016-5195 漏洞实现 Linux 系统本地提权。 2.2.2 能根据 Linux 漏洞验证及加固工作任务书要求，验证使用 CVE-2017-7494 漏洞实现 Samba 远程代码执行。 2.2.3 能根据 Linux 漏洞验证及加固工作任务书要求，验证使用 Redis 未授权访问漏洞进行提权。 2.2.4 能根据 Linux 漏洞验证及加固工作任务书要求，验证使用 Redis 弱口令实现远程 SSH 连接。
	2.3 中间件漏洞验证及加固	2.3.1 能根据中间件漏洞验证及加固工作任务书要求，验证使用 CVE-2017-9791 漏洞结合 BurpSuite 提权。 2.3.2 能根据中间件漏洞验证及加固工作任务书要求，验证使用 CVE-2017-12617 漏洞实现 Tomcat 远程代码执行。 2.3.3 能根据中间件漏洞验证及加固工作任务书要求，验证使用 CVE-2017-15715 绕过上传黑名单限制。 2.3.4 能根据中间件漏洞验证及加固工作任务书要求，验证使用 CVE-2018-12613 漏洞实现远程文件包含。 2.3.5 能根据中间件漏洞验证及加固工作任务书要求，验证使用 Java 序列化漏洞进行渗透测试。 2.3.6 能根据中间件漏洞验证及加固工作任务书要求，验证使用 Structs2 实现远程命令执行。
3.Python 安全渗透测试	3.1Python 安全渗透测试	3.1.1 能根据 Python 安全渗透测试工作任务书要求，完成 SMURF 网络渗透测试。 3.1.2 能根据 Python 安全渗透测试工作任务书

工作领域	工作任务	职业技能要求
		要求，完成 UDP FLOOD 网络渗透测试。 3.1.3 能根据 Python 安全渗透测试工作任务书要求，完成网络服务判断渗透测试。 3.1.4 能根据 Python 安全渗透测试工作任务书要求，完成数据库密码暴力破解渗透测试。 3.1.5 能根据 Python 安全渗透测试工作任务书要求，完成 SSH 密码暴力破解渗透测试。 3.1.6 能根据 Python 安全渗透测试工作任务书要求，完成 FTP 密码暴力破解渗透测试。 3.1.7 能根据 Python 安全渗透测试工作任务书要求，完成暴力破解 ZIP 文件口令渗透测试。 3.1.8 能根据 Python 安全渗透测试工作任务书要求，完成套接字编程及其应用渗透测试。 3.1.9 能根据 Python 安全渗透测试工作任务书要求，完成模糊测试渗透测试。 3.1.10 能根据 Python 安全渗透测试工作任务书要求，完成漏洞验证渗透测试。
4.数据库安全配置	4.1 数据库安全配置	4.1.1 能根据数据库安全配置工作任务书要求，完成 Access 数据库改名。 4.1.2 能根据数据库安全配置工作任务书要求，完成 MySQL 管理员账号修改。 4.1.3 能根据数据库安全配置工作任务书要求，完成加固 TCP/IP 协议栈。 4.1.4 能根据数据库安全配置工作任务书要求，完成 MySQL 用户权限设置及登录限制。 4.1.5 能根据数据库安全配置工作任务书要求，完成禁止或限制远程连接数据库。 4.1.6 能根据数据库安全配置工作任务书要求，完成限制超级管理员登录。 4.1.7 能根据数据库安全配置工作任务书要求，完成删除不必要的存储过程。 4.1.8 能根据数据库安全配置工作任务书要求，完成日志记录功能设置。 4.1.9 能根据数据库安全配置工作任务书要求，完成手工注入 Access 数据库。 4.1.10 能根据数据库安全配置工作任务书要求，完成修改 IIS 配置对 Access 数据库进行防护。 4.1.11 能根据数据库安全配置工作任务书要

工作领域	工作任务	职业技能要求
		求，完成手工注入 SQL Server 数据库。 4.1.12 能根据数据库安全配置工作任务书要求，完成使用 Sa 权限创建超级管理员。 4.1.13 能根据数据库安全配置工作任务书要求，完成手工注入 MySQL 数据库。 4.1.14 能根据数据库安全配置工作任务书要求，完成使用 Sqlmap 注入 MySQL 数据库。

表 3 网络安全运维职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1.PHP 代码审计	1.1PHP 代码审计	1.1.1 能根据 PHP 代码审计工作任务书要求，完成常见 PHP 危险函数及特殊函数配置。 1.1.2 能根据 PHP 代码审计工作任务书要求，完成常见的 INI 配置。 1.1.3 能根据 PHP 代码审计工作任务书要求，完成 PHP 框架与结构审计。 1.1.4 能根据 PHP 代码审计工作任务书要求，完成代码审计。 1.1.5 能根据 PHP 代码审计工作任务书要求，完成 XDebug 的配置和使用。 1.1.6 能根据 PHP 代码审计实例工作任务书要求，验证命令注入。 1.1.7 能根据 PHP 代码审计工作任务书要求，验证安装问题的审计。 1.1.8 能根据 PHP 代码审计工作任务书要求，验证 SQL 数字型注入。 1.1.9 能根据 PHP 代码审计工作任务书要求，验证 XSS 后台敏感操作。 1.1.10 能根据 PHP 代码审计工作任务书要求，验证文件包含漏洞的审计。 1.1.11 能根据 PHP 代码审计工作任务书要求，验证任意文件读取。 1.1.12 能根据 PHP 代码审计实例工作任务书要求，验证越权操作。 1.1.13 能根据 PHP 代码审计工作任务书要求，验证登录密码爆破。 1.1.14 能根据 PHP 代码审计工作任务书要求，验证二次注入。

工作领域	工作任务	职业技能要求
2.Web 应用程序漏洞验证	2.1Web 应用程序漏洞验证	2.1.1 能根据 Web 应用程序漏洞验证工作任务书要求，验证 X-Forwarded-For 注入。 2.1.2 能根据 Web 应用程序漏洞验证工作任务书要求，验证支付漏洞。 2.1.3 能根据 Web 应用程序漏洞验证工作任务书要求，验证垂直越权。 2.1.4 能根据 Web 应用程序漏洞验证工作任务书要求，验证 URL 跳转操作。 2.1.5 能根据 Web 应用程序漏洞验证工作任务书要求，验证 GET 任意文件下载。 2.1.6 能根据 Web 应用程序漏洞验证工作任务书要求，验证 POST 任意文件下载。 2.1.7 能根据 Web 应用程序漏洞验证工作任务书要求，验证 JS 上传绕过。 2.1.8 能根据 Web 应用程序漏洞验证工作任务书要求，验证文件上传 Content-Type 绕过。 2.1.9 能根据 Web 应用程序漏洞验证工作任务书要求，验证 Host 注入。 2.1.10 能根据 Web 应用程序漏洞验证工作任务书要求，验证 Boolean 盲注。 2.1.11 能根据 Web 应用程序漏洞验证工作任务书要求，验证 GET 文件包含。 2.1.12 能根据 Web 应用程序漏洞验证工作任务书要求，验证任意文件包含绕过截断。 2.1.13 能根据 Web 应用程序漏洞验证工作任务书要求，验证延时注入。
3.开源 CMS 实战渗透测试	3.1 开源 CMS 实战渗透测试	3.1.1 能根据开源 CMS 实战渗透测试工作任务书要求，验证海洋 search.php 注入。 3.1.2 能根据开源 CMS 实战渗透测试工作任务书要求，验证 BEESCMS 注入。 3.1.3 能根据开源 CMS 实战渗透测试工作任务书要求，验证 DedeCMS flink.php 友情链接注入。 3.1.4 能根据开源 CMS 实战渗透测试工作任务书要求，验证 Dcore(轻型 CMS 系统)SQL 注入。 3.1.5 能根据开源 CMS 实战渗透测试工作任务书要求，验证 Shopxp 系统 SQL 注入。 3.1.6 能根据开源 CMS 实战渗透测试工作任务书要求，验证 MetInfo 任意用户密码修改。

工作领域	工作任务	职业技能要求
		3.1.7 能根据开源 CMS 实战渗透测试工作任务书要求，验证 PHP 截断上传。
4.综合渗透测试	4.1 综合渗透测试	4.1.1 能根据综合渗透测试工作任务书要求，验证使用 Eternalblue-Doublepulsar 获取主机权限。 4.1.2 能根据综合渗透测试工作任务书要求，验证使用 SSH 私钥泄露提权获取主机权限。 4.1.3 能根据综合渗透测试工作任务书要求，验证使用 crontab 任务计划提权获取主机权限。 4.1.4 能根据综合渗透测试工作任务书要求，验证使用反弹木马进行提权获取主机 Shell。 4.1.5 能根据综合渗透测试工作任务书要求，验证使用 Java 效的数组索引漏洞进行鱼叉式渗透测试。 4.1.6 能根据综合渗透测试工作任务书要求，验证使用 Kerberos 渗透测试域控服务器并获取权限。 4.1.7 能根据综合渗透测试工作任务书要求，验证使用 Esteemaudit RDP 漏洞进行渗透提权。 4.1.8 能根据综合渗透测试工作任务书要求，验证使用 RSA 对称密钥对 HTTPS 数据包进行解码。 4.1.9 能根据综合渗透测试工作任务书要求，验证使用 SMB 服务漏洞结合 NTLM 中继进行渗透测试。 4.1.10 能根据综合渗透测试工作任务书要求，验证使用 Evil Maid 物理访问安全漏洞进行渗透测试。 4.1.11 能根据综合渗透测试工作任务书要求，验证使用 Exchange SSRF 漏洞结合 NTLM 中继进行渗透测试。
5.信息隐藏	5.1 信息隐藏	5.1.1 能根据信息隐藏工作任务书要求，完成使用隐写术防止敏感数据被盗用。 5.1.2 能根据信息隐藏工作任务书要求，完成使用 C 语言实现 LSB 图像信息隐藏。 5.1.3 能根据信息隐藏工作任务书要求，完成使用 Python 脚本对 CTF 中的图像隐写进行处理。 5.1.4 能根据信息隐藏工作任务书要求，完成使

工作领域	工作任务	职业技能要求
		用 Python 脚本来处理 CTF 中的音频隐写。 5.1.5 能根据信息隐藏工作任务书要求，完成使用十六进制分析工具对 CTF 中的图像隐写进行处理。

参考文献

[1] 中等职业学校专业目录（征求意见稿）

[2] 普通高等学校高等职业教育（专科）专业目录及专业简介（截至2019年）

[3] 普通高等学校本科专业目录

[4] 中等职业学校专业教学标准（试行）

[5] 高等职业学校专业教学标准（2018年）

[6] 本科专业类教学质量国家标准

[7] 国家职业技能标准编制技术规范（2018年版）

[8] 信息安全国家标准目录（2016版）

[9] 2019年全国职业院校技能大赛 ZZ-2019024 网络空间安全赛项规程

[10] 2019年全国职业院校技能大赛 GZ-2019028 信息安全管理与评估赛项规程

[11] SJ/T 11623-2016 信息技术服务从业人员能力规范

[12] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[13] GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南

[14] GB/T 20270-2016 信息安全技术 网络基础安全技术要求

[15] GB/T 21050-2019 信息安全技术 网络交换机安全技术要求

[16] GB/T 20272-2019 信息安全技术 操作系统安全技术要求

[17] GB/T 37939-2019 信息安全技术 网络存储安全技术要求

[18] GB/T 20271-2006 信息安全技术 信息系统安全通用技术要求

[19] GB/T 21052-2007 信息安全技术 信息系统物理安全技术要求