网络安全技术岗位职业技能等级标准

（征求意见稿）

中国电子学会

目录

前　言

本标准按照 GB/T1.1-2009 给出的规则起草。

为配合《中华人民共和国网络安全法》的实施，根据《国家职业教育改革实施方案》、《关于加强网络安全学科建设和人才培养的意见》的要求，以及国务院《关于加快发展现代职业教育的决定》的有关规定。同时，为了进一步完善职业教育标准体系，为职业教育、职业培训和职业技能鉴定提供科学、规范的依据，标准编写组在广泛调查研究的基础上，并征求了有关单位和专家的意见，结合“网络安全等级保护 2.0”标准，经反复讨论、修改和完善，制定了《网络安全技术岗位职业技能等级标准》（以下简称《本标准》）。

本标准起草单位：中国电子学会、北京中安国发信息技术研究院。

本标准主要起草人：张胜生、王海涛、杨帆、李锦、徐振华、张晓琦、罗先录、楚文波、刘静、李想、杜永清、张德丽、张树立、赵薇、唐洪玉、王祥武、周利斌、王聪睿、孙浩文、刘天炜、翟林、刘延春、刘亚欣、殷国强。

1 适用范围

本标准规定了网络安全技术岗位职业技能等级对应的职业技能要求及相关岗位人员的工作领域、工作任务。本标准适用于网络安全技术人员的职业技能培训、考核与评价，相关用人单位的人员聘用、培训、考核可参照使用。

2 规范性引用文件

GB/Z 20985-2007《信息技术安全技术信息安全事件管理指南》

GB/Z 20986-2007《信息安全技术信息安全事件分类分级指南》

GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》

GB/T 24363-2009《信息安全技术信息安全应急响应计划规范》

3 术语和定义

规范性引用文件中的术语和定义适用于本文件。

3.1 信息系统 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/Z 20986-2007]

3.2 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者故障的原因，对信息系统造成危害，或者在信息系统内发生的对社会造成负面影响的事件。

[GB/Z 20986-2007]

3.3 应急响应 emergency response

组织为了应对突发/重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施。[GB/T 24363-2009]

3.4 渗透测试 penetration

渗透测试是从一个攻击者的角度来检查和审核一个信息系统安全性的过程。通过信息收集、扫描、漏洞挖掘与验证等方法对目标系统进行测试，发现系统存在的安全风险。

3.5 木马 trojan

木马是特洛伊木马（Trojan horse）的简称，是一种伪装成正常程序，未经授权，植入目标系统并允许入侵者远程操控受害系统的一种恶意程序。

3.6 漏洞 vulnerability

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统，是计算机、组件、应用程序等无意中留下的不受保护的入口点。

3.7 漏洞扫描 vulnerability scan

漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的漏洞进行检测，发现可利用漏洞的一种安全检测（或渗透攻击）行为。

3.8 端口 port

端口可以认为是设备与外界通讯交流的出口。端口可分为物理端口和虚拟端口，物理端口又称为接口，是可见端口。虚拟端口是计算机内部或交换机路由器内的不可见的端口，例如计算机中的 80 端口、21 端口、23 端口等，本标准中所涉及的端口是指虚拟端口。

3.9 蜜罐/蜜网 honeypot/honeynet

蜜罐/蜜网是通过布置一些作为诱饵的主机、网络系统、模拟的业务应用系统或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，从而了解自身所面对的安全威胁的一种技术。

3.10 系统提权 system privilege elevation

系统提权是攻防技术中的专用术语，指入侵者在入侵过程中提高自己在计算机操作系统中的权限，以夺得目标主机控制权限的行为。一般用于网站入侵和系统入侵过程中。

4 缩略语

IPS：入侵防御系统（Intrusion Prevention System）

WAF：网站应用防火墙（Web Application Firewall）

MAC：媒体存取控制地址，也叫物理地址（Media Access Control Address）

ARP：地址解析协议（Address Resolution Protocol）

DNS：域名系统（Domain Name System）

SQL：结构化查询语言（Structured Query Language）

OSI：开放系统互连（Open System Interconnect）

DHCP：动态主机配置协议（Dynamic Host Configuration Protocol）

5 面向工作岗位（群）

主要面向从事计算机设备管理、网络管理、IT 系统安全运维与管理、渗透测试、安全分析、应急响应等相关的网络安全管理和技术类岗位。具体参见下表：

职业技能等级	岗位类别	工作内容
基础Ⅰ级 （1A级-网络与操作系统安全基础）	a) 桌面技术支持工程师 b) 设备管理员 c) 网络管理员 d) 服务器管理员	可在政府机关、企事业单位从事Windows 操作系统的桌面运维、服务器管理、桌面技术支持、网络管理与运维等相关工作。
基础Ⅱ级 （2A 级-应用系统安全基础）	a) 服务器管理员 b) 应用系统运维工程师	可在政府机关、企事业单位从事Linux 服务器管理、应用系统的部署安装、运营维护等相关工作。
初级 （3A 级-安全运维与监控）	a) 安全运维工程师 b) 安全监控工程师 c) 安全架构工程师 d) 系统管理员 e) 应用管理员	可在政府机关、企事业单位从事各类信息系统的安全运维工作，包括但不限于对设备、主机、网络、应用系统等运维对象实施安全检查、监控、分析与评估，并根据检查结果进行安全加固和维护。
中级 （4A 级-漏洞检测与加固）	a) 风险评估工程师 b) 渗透测试工程师 c) 应用安全工程师 d) 安全合规工程师	可在政府机关、企事业单位从事各类信息系统的运维和安全性测试工作，包括但不限于对设备、主机、网络、应用系统等开展全面的漏洞检测、渗透测试，并根据测试结果进行漏洞修补和安全加固。
高级 （5A 级-入侵分析与应急）	a) 安全分析工程师 b) 安全审计工程师 c) 应急响应工程师 d) 安全技术主管 e) 安全技术总监	可在政府机关、企事业单位从事各类信息安全事件的应急响应、入侵分析、调查取证等技术类工作以及应急响应流程与预案的制定等应急管理类工作。

6 面向院校专业领域

院校	专业类	专业代码	专业名称
中职	09 信息技术类	092000	网络信息安全
		090100	计算机应用
		090500	计算机网络技术

		090700	网络安防系统安装与维护
		091200	电子与信息技术
高职	61 电子信息类	610201	计算机应用技术
		610202	计算机网络技术
		610204	计算机系统与维护
		610211	信息安全与管理
本科	0809 计算机类	080901	计算机科学与技术
		080903	网络工程
		080904K	信息安全
		080911TK	网络空间安全
	0838 公安技术类	083108TK	网络安全与执法

7 职业技能等级标准

7.1 职业技能等级划分

网络安全职业技能等级分为五个等级，基础Ⅰ级（1A 级-网络与操作系统安全基础）、基础Ⅱ级（2A 级-应用系统安全基础）、初级（3A 级-安全运维与监控）、中级（4A 级-漏洞检测与加固）、高级（5A 级-入侵分析与应急）。级别依次递进，高级别涵盖低级别职业技能要求。

7.2 职业技能等级标准要求

7.2.1 综合素质要求

1）基础Ⅰ级（1A 级-网络与操作系统安全基础）

具备相关技术文档的阅读理解能力，能够按照工作规范与手册开展具体工作。

2）基础Ⅱ级（2A 级-应用系统安全基础）

具备相关技术文档的阅读理解能力、现象分析能力，能够按照工作规范、手册或具体要求开展具体工作。

3）初级（3A 级-安全运维与监控）

具备相关技术文档的阅读理解能力、现象分析能力、异常识别能力、实验能力、文

档编写能力。

4）中级（4A 级-漏洞检测与加固）

具备相关技术文档的阅读理解能力、现象分析能力、异常识别能力、逻辑推理能力、实验能力、文档编写能力、组织沟通能力。

5）高级（5A 级-入侵分析与应急）

具备相关技术文档的阅读理解能力、现象分析能力、异常识别能力、逻辑推理能力、关联分析能力、实验能力、文档编写能力、组织沟通能力和项目管理能力。

7.2.2 职业技能要求

各等级的职业技能要求具体参见下表：

表 1：基础Ⅰ级（1A 级-网络与操作系统安全基础）

工作领域	工作任务	职业技能要求
桌面管理	Windows 操作系统安装与配置	1. 能够安装 Windows 系列（包括桌面版、服务器版）操作系统及虚拟机，并进行基本配置和安全加固。 2. 能够进行操作系统镜像文件制作以及利用镜像文件进行操作系统安装或还原。 3. 能够解决常见的 Windows 操作系统故障,对故障系统进行恢复。 4. 能够利用工具对操作系统进行密码重置、病毒查杀等桌面技术支持工作。
网络管理	组网与配置	1. 能够掌握 OSI 模型、TCP/IP 模型中的功能及协议，能够掌握网络互联基础、互联设备、组网方法等基础知识，并利用相关知识进行组网。 2. 能够对常见网络设备进行安全配置和配置优化。 3. 能够对常见网络故障进行定位和排除。

表 2：基础Ⅱ级（2A 级-应用系统安全基础）

工作领域	工作任务	职业技能要求
服务器管理	服务器搭建与配置	1. 能够安装常见 Linux 操作系统及虚拟机，掌握常见命令并进行基本的安全配置。 2. 能够熟练使用服务器远程管理工具，对服务器进行管理和维护。 3. 能够综合应用 DNS 工作原理等知识，进行各种类型的 DNS 服务器的安装和配置。 4. 能够综合应用 DHCP 工作原理等知识，进行 DHCP 服务的安装和配置。 5. 能够进行常见邮件服务器的搭建和配置。

应用系统运维	应用系统部署与配置	1. 能够进行主流 Web 服务器的搭建和配置。 2. 能够进行应用系统的部署和 WEB 服务的配置及发布。

表 3：初级（3A 级-安全运维与监控）

工作领域	工作任务	职业技能要求
安全运维	网络安全运维	1. 熟练掌握主流网络设备及安全设备的操作方法及常用命令，熟悉安全配置基线规范要求，能够根据规范要求对相关网络设备及安全设备进行巡检。 2. 能够综合应用网络安全域划分和访问控制规则设计的原理和方法，进行网络安全架构设计。 3. 熟练掌握主流网络设备和安全设备的日志类型及分析方法，能够熟练使用常见的日志分析工具。 4. 熟悉一种或多种日志分析工具或平台，熟练掌握日志数据源读取方式、同步数据的方法、简单查询语句的使用，能够进行日志分析。 5. 能够综合应用上述知识、手段，对设备安全状况进行判断，并进行设备配置优化。
	操作系统安全运维	1. 能够熟练应用 Linux 基本常用命令，Windows 安全事件查看、注册表查看、策略查看等操作方法开展安全运维工作。 2. 能够综合应用 Windows、Linux 主机系统的安全运维知识，独立完成主机系统的安全巡检和运维任务，包括： 1) 利用主流的扫描工具，对系统端口和安全配置基线进行自动化扫描，能够理解、分析扫描结果。 2) 能够对病毒、木马感染情况进行检测和分析。 3) 掌握系统日志异常规则，能够对系统日志进行分析并判断系统安全状态。
	数据库及中间件安全运维	熟悉主流数据库、中间件和常见漏洞，能够独立完成数据库和中间件的安全巡检和运维工作，包括： 1) 对主流数据库进行安全基线检查和入侵分析。 2) 对常见中间件进行安全配置和日志分析。
安全加固	操作系统加固	1. 能够理解相关漏洞补丁的官方通告，熟练掌握各种操作系统的升级和补丁安装方法，并能验证补丁加载有效性。 2. 了解 Windows、常见 Linux 系统自身漏洞利用、系统提权的原理和方法，能够对 Windows、常见 Linux 系统进行安全加固。
	数据库加固	1. 能够理解相关漏洞补丁的官方通告，熟练掌握主流数据库的升级和补丁安装方法，并能验证补丁加载有效性。 2. 了解主流数据库漏洞利用原理和防范方法，能够对数据库进行安全加固。
	中间件加固	1. 能够理解相关漏洞补丁的官方通告，熟练掌握常见中间件的升级和补丁安装方法，并能验证补丁加载有效性。 2. 了解常见中间件的漏洞利用原理和防范方法，能够对中间件进行安全加固。

应急响应	信息安全事件应急	1. 了解常见的网络层攻击现象和手法,能够根据应急预案进行应急处置。 2. 了解常见的应用层攻击手段和方法,能够识别相关攻击事件并进行应急处置。 3. 熟悉 Windows、常见 Linux 系统的常见漏洞利用方法，能够对系统进行漏洞修补和安全加固。 4. 熟悉常用的应急工具,能够应对简单的网络攻击和一般的网络安全事件。

表 4：中级（4A 级-漏洞检测与加固）

工作领域	工作内容	职业技能要求
漏洞检测与加固	漏洞检测工具使用	熟悉常见的漏洞检测与扫描工具、渗透测试工具及其优缺点，掌握工具使用方法，能够熟练使用相关工具对漏洞进行检测。
	操作系统漏洞检测与加固	1. 熟悉常见的操作系统安全漏洞，能够对操作系统漏洞进行检测。 2. 能够理解相关漏洞补丁的官方通告，对漏洞修补建议进行验证，并对漏洞进行修补。 3. 熟悉 Windows、常见 Linux 系统提权过程，能够进行攻击重现，能够对系统提权漏洞进行防范和安全加固。 4. 能够对 Windows、常见 Linux 系统的隐藏账号进行检测。 5. 能够对常见的木马、后门进行分析检测和防范。
	数据库漏洞检测与加固	1. 熟悉主流数据库的常见安全漏洞，能够对数据库漏洞进行检测。 2. 能够理解相关漏洞补丁的官方通告，对漏洞修补建议进行验证，并对漏洞进行修补。
	应用程序漏洞检测与加固	1. 熟练掌握各种应用程序漏洞的利用方法和攻击原理，能够对相关漏洞进行检测、分析和攻击再现，包括但不限于： 1) SQL 注入漏洞； 2) XSS 跨站脚本攻击； 3) CSRF 跨站请求伪造攻击； 4) 文件上传漏洞； 5) 应用程序后门漏洞。 2. 熟练掌握上述各种攻击的防范措施和加固方法，能够提出对相关漏洞进行修补和加固的建议。
应急响应	信息安全事件应急	1. 熟练掌握常见的黑客入侵行为和攻击手段，能够对攻击事件进行检测、防范和应急处置。 2. 熟悉各种日志分析工具、技术，能够进行事件分析和推理。 3. 能够根据国家应急响应计划规范相关标准的要求，进行应急预案的编写。 4. 熟练使用常用的应急工具，能够应对常见的网络攻击和较大的网络安全事件。

表 5：高级（5A 级-入侵分析与应急）

工作领域	工作任务	职业技能要求
入侵分析	入侵分析	1. 能够利用网站入侵、内网渗透过程的相关技术和手法进行渗透测试或攻击重现。 2. 能够搭建日志服务器或日志分析平台，结合人工，对网络日志、系统日志、应用日志进行关联分析，对安全状况进行评估，对入侵事件进行侦查和判断。 3. 能够灵活运用态势感知、蜜罐、蜜网等技术，对入侵流量进行分析，对攻击行为进行检测、分析。 4. 能够利用反编译、程序逆向解析等技术对恶意程序进行破解，对攻击行为特征进行分析。
	电子数据取证	1. 能够利用常见的计算机取证技术和证据收集手段，配合司法鉴定人员对网络安全事件进行有效调查取证，包括但不限于： 1） 内存信息取证； 2） 磁盘文件取证； 3） 浏览器历史信息取证； 4） 日志取证； 5） 聊天工具取证； 6） 电子邮件取证； 7） 移动终端取证； 2、了解我国电子数据取证的相关立法，掌握电子证据的提取和保全方法。
应急响应	信息安全事件应急	1. 具备网络安全事件监控体系的设计能力，能够对信息安全事件进行检测、综合分析和应急处置。 2. 能够根据国家应急响应计划规范相关标准的要求，进行应急响应流程的策划与制定。 3. 能够策划有效的应急演练方案，通过演练过程对应急预案进行优化。 4. 能够综合应用网络基础知识、应急工具等，识别和判断网络中潜在的威胁和安全风险，能够应对高级的、复杂的网络攻击和重大网络安全事件。

参考文献

[1] GB/T 20984-2007《信息安全技术信息安全风险评估规范》

[2] GB/Z 20985-2007《信息技术安全技术信息安全事件管理指南》

[3] GB/Z 20986-2007《信息安全技术信息安全事件分类分级指南》

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

[5] GB/T 24363-2009《信息安全技术信息安全应急响应计划规范》

[6] GB/T 31509-2015《信息安全技术信息安全风险评估实施指南》

[7] GB/T 33132-2016《信息安全技术信息安全风险处理实施指南》

[8] GB/T 36627-2018《信息安全技术网络安全等级保护测试评估技术指南》

[9] 中等职业学校专业目录

[10] 普通高等学校高等职业教育（专科）专业目录

[11] 普通高等学校本科专业目录

[12] 高等职业学校专业教学标准

[13] 中华人民共和国职业分类大典

[14] 国务院《关于印发国家职业教育改革实施方案的通知》

[15] 中网办发文〔2016〕4号《关于加强网络安全学科建设和人才培养的意见》