网络安全评估
职业技能等级标准

标准代码：510004

（2021年2.0版）

北京奇虎测腾科技有限公司　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：北京奇虎测腾科技有限公司、三六零科技集团有限公司、北京奇虎科技有限公司、北京奇付通科技有限公司、弘大教育咨询（天津）有限责任公司、河南新工科产业学院有限公司、南京米好信息安全有限公司、西安电子科技大学、山东科技大学、北京信息职业技术学院、武汉职业技术学院。

本标准主要起草人：姜思红、王志威、何宛馨、冯玉涛、齐飞、张彬哲、张记卫、秦江艳、刘凯、周家豪、杨莹、刘虎城、杨超、梁永全、史宝会、王海、杨旭东、江岚。

1 范围

本标准规定了网络安全评估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评估职业技能培训、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 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

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

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，定义 2.1.53]

3.3 **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，定义 2.2.1.6]

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 **安全分级 security classification**

根据业务信息和系统服务的重要性和受损影响，确定实施某种程度的保护，并对该保护程度给以命名。依据访问数据或信息需求，而确定的特定保护程度，同时赋予相应的保护等级。例：“绝密”、“机密”、“秘密”。

[GB/T 25069-2010，定义 2.2.1.2]

3.6 **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]

3.7 **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，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：计算机应用、计算机网络技术、软件与信息服务、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、网站建设与管理等。

高等职业学校：计算机应用技术、计算机网络技术、软件技术、软件与信息服务、计算机信息管理、大数据技术与应用、云计算技术与应用、信息安全与管理、计算机系统与维护等。

应用型本科学校：计算机应用工程、网络工程、软件工程、大数据技术与应用、信息安全与管理等。

4.2 参照新版职业教育专业目录

中等职业学校：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、网站建设与管理等。

高等职业学校：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。

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。

应用型本科学校：信息安全、信息对抗技术、信息工程、大数据管理与应用、网络安全与执法、网络工程、网络空间安全、计算机科学与技术、软件工程等。

5 面向职业岗位（群）

【网络安全评估】（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，从事安全加固、安全产品研发、风险评估、渗透测试、安全运维等工作岗位。

【网络安全评估】（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、攻防对抗、渗透测试、源代码安全检测、等级保护、安全运维等工作岗位。

【网络安全评估】（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，从事安全管理、安全研究、实战攻防、网络安全防御、等保体系建设、网络安全应急响应等工作岗位。

6 职业技能要求

6.1 职业技能等级划分

网络安全评估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。

【网络安全评估】（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，掌握基本的安全评估基础知识，从事系统主机、网络系统、Web 系统等评估分析工作，并根据企业安全建设要求进行安全区域边界的基础管理。

【网络安全评估】（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，掌握安全评估的总体架构，从事系统主机、网络系统、网络协议、Web 系统，软件代码等评估分析工作。并根据企业安全建设要求进行安全区域边界的进阶管理。

【网络安全评估】（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，从事系统主机、网络协议、网络系统、Web 系统，软件代码、内网系

统等评估分析工作。并根据企业安全建设要求进行安全管理中心的管理，并掌握应急响应的能力。

6.2 职业技能等级要求描述

表 1 网络安全评估职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1.网络安全基础知识准备	1.1 安全概念准备	1.1.1 了解网络安全发展历程
		1.1.2 了解网络安全概念
		1.1.3 了解网络安全事件的分类
	1.2 安全意识准备	1.2.1 了解信息安全常识
		1.2.2 了解办公安全常识
		1.2.3 了解防电信诈骗方法和社会工程学安全
	1.3 安全法律法规知识准备	1.3.1 了解网络安全相关法律法规及规定
		1.3.2 了解网络安全法规行业案例
		1.3.3 熟悉安全从业人员行为规范及法律责任
	1.4 等级保护知识准备	1.4.1 了解网络安全等级保护标准体系
		1.4.2 了解网络安全等级保护测评方法
		1.4.3 了解网络安全等级保护体系建设方案
2.操作系统基础准备	2.1 Windows 系统基础准备	2.1.1 了解计算机系统结构和操作系统功能
		2.1.2 了解操作系统常见的安全问题
		2.1.3 了解 Windows 操作系统基础知识
3.计算机网络基础准备	3.1 Web 基础准备	3.1.1 了解 HTML 基础知识和语法
		3.1.2 熟悉 Web 应用请求过程
		3.1.3 了解 HTTP 协议、请求、响应、方法、状态码和消息
	3.2 计算机网络及协议安全准备	3.2.1 了解 OSI 七层模型
		3.2.2 了解 TCP/IP 协议模型
		3.2.3 了解抓包工具的基本使用方法（比如 Wireshark、Tcpdump）
		3.2.4 了解 TCP/IP 协议簇中常见协议原理
4.网络安全	4.1 网络安全评估	4.1.1 了解网络安全评估概念和必要性

工作领域	工作任务	职业技能要求
评估准备	基础准备	4.1.2 了解渗透测试常规流程和各个环节内容
		4.1.3 掌握网络渗透测试报告编写
	4.2 网络安全评估环境搭建	4.2.1 了解 Kali 操作系统的使用场景
		4.2.2 掌握 Kali 小工具以及命令使用
		4.2.3 掌握常用浏览器以及插件使用
		4.2.4 了解常用编程语言和运行环境
		4.2.5 掌握渗透测试网络环境搭建的方法
	4.3 网络安全评估工具使用	4.3.1 掌握渗透工具 Burp Suite 使用
		4.3.2 掌握渗透工具 sqlmap 使用
		4.3.3 掌握渗透工具 nmap 使用
		4.3.4 掌握渗透工具 AWVS 使用
		4.3.5 掌握渗透工具 Metasploit 使用
		4.3.6 掌握渗透工具 SET 使用
5.主机系统安全评估实践	5.1 Windows 系统安全评估	5.1.1 了解操作系统安全配置作用
		5.1.2 掌握 Windows 操作系安全加固方法
6.网络系统安全评估实践	6.1 信息收集与社工	6.1.1 了解 DNS 记录、子域名收集、C 段扫描、web 目录扫描、指纹识别等信息收集工具和方法
		6.1.2 了解社工库、多维度信息收集方法、钓鱼邮件、宏病毒等
		6.1.3 熟悉 Shodan、ZoomEye 网络空间搜索引擎使用方式，Google Hacking 信息收集方法
	6.2 漏洞扫描	6.2.1 了解漏洞扫描的原理及主流系统漏洞扫描器
		6.2.2 了解 Web 漏洞扫描器
		7.2.3 了解第三方软件漏洞扫描器
7.Web 系统安全评估实践	7.1 Web 安全知识准备	7.1.1 了解 Web 安全事件和 Web 体系结构
		7.1.2 了解 OWASP Top10
		7.1.3 熟悉 Web 安全案例分析
	7.2 Web 漏洞	7.2.1 了解 SQL 语法和数据库方法

工作领域	工作任务	职业技能要求
	-SQL 注入安全评估	7.2.2 掌握 SQL 注入利用方法
		7.2.3 掌握 sqlmap 工具使用
		7.2.4 掌握 HTTP 文件头注入方法
	7.3 会话管理配置	7.3.1 了解 session cookie、Token 会话管理
		7.3.2 了解 session 攻击方法
		7.3.3 了解 Cookie 的安全机制
	7.4 Web 漏洞 -XSS 安全评估	7.4.1 了解跨站脚本的概念
		7.4.2 了解持久型和 DOM 型 XSS 原理
		7.4.3 掌握 XSS 攻击的常见方法
		7.4.4 了解 Cookie 会话攻击原理
		7.4.5 掌握 XSS 攻击常见防御方法
	7.5 Web 漏洞-文件上传安全评估	7.5.1 了解文件上传漏洞原理
		7.5.2 掌握文件上传绕过方法
8. 企业安全建设实践	8.1 企业安全建设准备	8.1.1 了解安全建设的各阶段及目标
		8.1.2 了解组织建立安全团队的流程
		8.1.3 了解不同场景下网络架构设计
	8.2 安全区域边界 -防火墙搭建	8.2.1 了解防火墙功能及工作模式
		8.2.2 了解包过滤、状态检测、代理服务及 NAT 相关技术
		8.2.3 熟悉 Linux 防火墙的工作原理
		8.2.4 掌握 Linux 防火墙的基本配置
	8.3 安全区域边界 -入侵检测与入侵防御搭建	8.3.1 了解 IDS 系统概念、结构、工作模式、分类和工作原理
		8.3.2 了解入侵检测系统工作模式和流程
		8.3.3 掌握入侵检测系统部署方式
		8.3.4 了解 IPS 系统概念、结构、工作模式、分类和工作原理
		8.3.5 掌握 IPS 系统部署方法

表 2 网络安全评估职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1.操作系统基础准备	1.1 Linux 系统基础准备	1.1.1 了解 Linux 基础架构（如文件系统、权限控制和安全机制）
		1.1.2 了解 Linux 系统相关的基础常见命令
		1.1.3 了解 Linux 用户管理、进程、Shell 相关知识
2.编程语言基础准备	2.1 PHP 基础知识准备	2.1.1 了解 PHP 环境配置方法
		2.1.2 了解 PHP 编程基础知识
		2.1.3 掌握 PHP 基本代码编写
3.主机系统安全评估实践	3.1 Linux 系统安全评估	3.1.1 了解 Linux 安全基线一般要求
		3.1.2 掌握 Linux 操作系统安全加固方法
4.网络协议安全评估实践	4.1 网络协议安全评估准备	4.1.1 了解网络安全基本概念和属性
		4.1.2 了解网络协议安全性概念
		4.1.3 掌握 TCP/IP 协议的网络安全体系
		4.1.4 了解网络嗅探的原理
	4.2 网络协议链路层安全评估	4.2.1 掌握 ARP 协议攻击及防御方法
		4.2.2 掌握 DHCP 协议攻击及防御方法
		4.2.3 掌握 MAC 泛洪攻击方法
	4.3 网络协议网络层安全评估	4.3.1 了解 IP 协议基础
		4.3.2 掌握 IP 协议相关的攻击及防御方法
		4.3.3 掌握 ICMP 协议及相关的攻击及防御方法
5.网络系统安全评估实践	5.1 中间件利用评估	5.1.1 掌握 IIS 短文件名漏洞利用方法
		5.1.2 掌握 FastCGI 任意命令执行漏洞方法
		5.1.3 掌握 PHPCGI 远程代码执行漏洞方法
		5.1.4 掌握 Nginx 配置不当导致的安全问题及修复方法
6.Web 系统安全评估实践	6.1 Web 漏洞-XSS 安全评估	6.1.1 了解跨站脚本的概念
		6.1.2 了解持久型和 DOM 型 XSS 原理
		6.1.3 掌握 XSS 攻击的常见方法
		6.1.4 了解 Cookie 会话攻击原理
		6.1.5 掌握 XSS 攻击常见防御方法

工作领域	工作任务	职业技能要求
	6.2 CSRF&SSRF 漏洞安全评估	6.2.1 了解 CSRF 跨站请求伪造原理
		6.2.2 掌握 CSRF 防御方法
		6.2.3 了解 SSRF 漏洞原理
		6.2.4 掌握 SSRF 漏洞绕过技巧
	6.3Web 漏洞-文件上传安全评估	6.3.1 了解文件上传漏洞原理
		6.3.2 掌握文件上传绕过方法
	6.4Web 漏洞-文件包含安全评估	6.4.1 了解文件包含漏洞原理
		6.4.2 掌握常规文件包含漏洞
	6.5 Web 漏洞-命令执行安全评估	6.5.1 了解命令执行漏洞原理
		6.5.2 掌握 DVWA 中命令执行漏洞
		6.5.3 掌握常见框架命令执行漏洞
	6.6 逻辑漏洞安全评估	6.6.1 了解逻辑漏洞概念
		6.6.2 了解访问控制与访问控制模型
		6.6.3 了解应用系统的验证机制(包括暴力破解和密码重置)
		6.6.4 掌握针对令牌的常用攻击手段
		6.6.5 了解权限控制的方法
		6.6.6 了解常见业务逻辑漏洞
7.软件代码安全评估实践	7.1 软件代码安全评估知识准备	7.1.1 了解代码审计思路
		7.1.2 掌握代码审计测试方法及流程
	7.2 代码审计工具准备	7.2.1 了解代码审计工具
		7.2.2 了解 PHP 调试原理
		7.2.3 掌握 PHP 调试方法
	7.3 PHP 代码安全评估实施	7.3.1 熟练对常见 Web 漏洞进行代码审计（注入漏洞、上传漏洞、SSRF 漏洞等）
		7.3.2 熟练运用代码审计流程进行测试工作
		10.3.3 具备较丰富的安全代码编写经验
8. 企业安全建设实践	8.1 安全区域边界-VPN 搭建	8.1.1 了解 VPN 技术的原理和分类及基本原理
		8.1.2 熟悉 IPSec VPN 体系结构、工作模式和报文结构

工作领域	工作任务	职业技能要求
	8.2 安全区域边界-WAF 搭建	8.1.3 了解 WAF 概念、分类和工作过程
		8.2.1 掌握 WAF 的加固方法
		8.2.2 了解 ModSecurity 结构和工作原理及规则
		8.2.3 掌握 ModSecurity 部署配置

表 3 网络安全评估职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1.编程语言基础准备	1.1 Python 基础知识准备	1.1.1 掌握 Python 语言中基本变量、赋值、函数等基本概念
		1.1.2 掌握 Python 语言数据类型如列表、元组、字典、集合等
		1.1.3 掌握 Python 语言控制语句
		1.1.4 掌握 Python 语言类与对象的使用
		1.1.5 掌握 Python 语言网络编程
2.网络协议安全评估实践	2.1 网络协议安全评估准备	2.1.1 掌握网络安全基本概念和属性
		2.1.2 掌握网络协议安全性概念
		2.1.3 掌握 TCP/IP 协议的网络安全体系
		2.1.4 掌握网络嗅探的原理
	2.2 网络协议传输层安全评估	2.2.1 掌握 TCP、UDP 协议基础知识
		2.2.2 掌握 TCP 相关攻击及防御方法
		2.2.3 掌握 UDP 相关攻击及防御方法
	2.3 网络协议应用层安全评估	2.3.1 掌握 DNS 协议安全问题
		2.3.2 掌握 HTTP 协议的安全问题
		2.3.3 掌握邮件协议的安全问题
3.网络系统安全评估实践	3.1 数据库利用评估	3.1.1 掌握 Mysql 数据库提权过程
		3.1.2 掌握 Mssql 数据库利用方法
		3.1.3 掌握 Rsync 数据库利用方法
		3.1.4 掌握 Elasticsearch 工作原理，及几个漏洞利用方法

工作领域	工作任务	职业技能要求
4.内网渗透评估实践	4.1 内网渗透评估准备	4.1.1 掌握内网定义及内网渗透测试流程
		4.1.2 掌握 Windows 域概念
		4.1.3 运用搭建内网渗透测试实验环境
	4.2 内网渗透信息收集评估	4.2.1 掌握信息收集种类
		4.2.2 掌握 DNS 记录查询方法和域名信息查询方法
		4.2.3 掌握子域名收集方法
		4.2.4 掌握 C 段扫描方法
		4.2.5 掌握 Web 目录扫描方法
		4.2.6 运用系统、中间件、Web 程序、防火墙等指纹识别方法
		4.2.7 掌握 Google Hacking 语法和组合搜索方式
		4.2.8 掌握 Shodan 用法
		4.2.9 掌握社工库概念
		4.2.10 掌握社工库使用方法
	4.3 Windows 下信息收集评估	4.3.1 掌握 Windows 下收集涉及内容
		4.3.2 熟练使用凭证收集工具
		4.3.3 掌握 Windows 访问令牌的作用与利用方法
	4.4 Linux 下信息收集评估	4.4.1 掌握 Linux 下信息收集方法
		4.4.2 掌握 Linux 凭证收集方法
	4.5 端口转发配置	4.5.1 掌握端口转发原理
		4.5.2 掌握端口转发工具使用方法
		4.5.3 掌握反弹 shell 方法
	4.6 内网文件传输配置	4.6.1 掌握内网文件传输技术
		4.6.2 掌握内网中文件传输工具的使用
	4.7 密码记录和欺骗攻击配置	4.7.1 掌握密码记录工具使用
		4.7.2 掌握 ARP 欺骗和 DNS 欺骗的方法
	4.8 域内横向移动配置	4.8.1 掌握 SMB 协议以及常见漏洞的利用方法
		4.8.2 掌握 RPC 协议以及常见漏洞的利用方法

工作领域	工作任务	职业技能要求
		4.8.3 运用 MSF 工具进行内网攻击
	4.9 内网渗透安全进阶评估	7.9.1 掌握内网渗透技巧
		7.9.2 掌握权限维持的方法
5.Web 系统安全评估实践	5.1 SQL 注入安全进阶评估	5.1.1 掌握 SQL 注入的 WAF 检测方法
		5.1.2 掌握 SQL 注入的绕过方法
		5.1.3 掌握宽字节注入原理和利用方法
	5.2 反序列化漏洞安全评估	5.2.1 掌握序列化和反序列化的作用及引起漏洞的原因和影响范围
		5.2.2 掌握 PHP 反序列化漏洞利用方法
		5.2.3 掌握 JAVA 反序列化漏洞
	5.3 Web 容器解析漏洞安全评估	5.3.1 掌握 IIS 相应漏洞原理
		5.3.2 掌握 Apache 文件解析漏洞
		5.3.3 掌握 Nginx 文件解析漏洞
		5.3.4 掌握 Tomcat 任意文件上传漏洞
6.软件代码安全评估实践	6.1 代码审计进阶安全评估	6.1.1 掌握 ThinkPHP 漏洞挖掘
		6.1.2 掌握 Vmins 文件上传漏洞挖掘
		6.1.3 掌握 Seacms 代码执行分析
		6.1.4 掌握 Joomla 反序列化漏洞原理
7. 企业安全建设实践	7.1 安全管理中心-堡垒机搭建	7.1.1 掌握堡垒机架构和安装方式
		7.1.2 运用堡垒机的使用及审计原理
	7.2 安全管理中心-态势感知搭建	7.2.1 掌握 ELK 安装及基础配置
		7.2.2 运用 ELK 的基础架构及相互协作关系
		7.2.3 掌握 ELK 使用（包括 logstash 的配置、beats 配置和 kibana 使用）
	7.3 安全管理中心-网络监视搭建	7.3.1 掌握 Zabbix 系统功能
		7.3.2 掌握监控系统 Zabbix 安装
		7.3.3 掌握 Zabbix 自定义 SNMP 监控项使用
		7.3.4 掌握 snmpwalk 与 snmpget 工具
		7.3.5 掌握使用 agent 监控 centos
		7.3.6 掌握 Zabbix 自定义脚本监控

工作领域	工作任务	职业技能要求
		7.3.7 运用 Zabbix 对 WEB 服务器进行监控。
	7.4 安全应急响应	7.4.1 掌握电子数据取证原则和流程
		7.4.2 掌握硬盘寻址和文件系统
		7.4.3 运用数据恢复技术
		7.4.4 掌握 Windows 下 rootkit 原理和检测方式
		7.4.5 掌握内存取证的原理
		7.4.6 运用内存取证工具的使用方法
		7.4.7 运用追踪溯源的工具和方法

参考文献

[1] 高等职业学校专业教学标准

[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] 国家职业技能标准编制技术规程.2018 年版

[5] 中华人民共和国网络安全法

[6] 信息安全技术网络安全等级保护基本要求

[7] 信息安全技术网络安全等级保护测评要求

[8] 信息安全技术网络安全等级保护安全设计技术要求

[9] 关键信息基础设施安全保护条例

[10] 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）

[11] 《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）

[12] 《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）