网络安全评估
职业技能等级标准

（2020年2.0版）

北京奇虎测腾科技有限公司　制定

2020 年 03 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：三六零科技集团有限公司、北京奇虎科技有限公司、北京奇虎测腾科技有限公司、北京奇付通科技有限公司、山东双元教育管理有限公司、天津锐驰科技有限公司、安徽大富鸿学教育科技有限公司、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：吕沐阳、杜廷龙、王大鹏、胡开雨、史锟航、邹艳芸、时荣鹏、孙伟峰、严波、黄浩、袁泉、王梅、张德平、周小龙、吴俊成、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

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、网络安全系统安装与维护、软件与信息服务、移动应用技术与服务等。

高等职业学校：信息安全与管理、计算机网络技术、大数据技术与应用、计算机应用技术、计算机信息管理、软件与信息服务等。

应用型本科学校：信息安全、网络空间安全、网络工程、计算机科学与技术、软件工程、信息管理与信息系统、数据科学与大数据技术等。

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、风险评估、渗透测试、安全服务运维、应急响应等工作岗位。

【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、渗透测试、等级保护、自动化安全运维、安全架构设计等工作岗位。

【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、攻防对抗、安全研究、漏洞挖掘、高级威胁分析、等保体系建设等工作岗位。

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，具备初步应用安全知识积累的能力，能够熟练使用部分安全工具，能了解部分攻击、原理和验证自己的安全想法。

【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，具有了解安全架构体系的工作流，在安全理解和能力上有一定升华，对防御技术有较好的理解，能将部分安全理念、知识创新性融入到所负责的工作内容。

【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，能够对负责安全领域作出深度的理解和一定的独立的解决安全能力，具备主导部分项目或安全攻防场景的能力。

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.网络安全法与职业素养	1.1 网络安全法学习	1.1.1 深刻理解《中华人民共和国网络安全法》; 1.1.2 深刻理解《网络安全等级保护》； 1.1.3 深刻理解我国安全相关的法律法规。
	1.2 职业素养认知	1.2.1 树立起科学的世界观、人生观和价值观; 1.2.2 具有良好道德修养，诚实守信； 1.2.3 具有乐观积极的心态、良好的心理素质和健康体魄，能应对危机和挑战。
	1.3 网络风险认知	1.3.1 能够分析典型网络安全事件的起因; 1.3.2 能够辨别与评定网络安全风险。
	1.4 网络威胁应对	1.4.1 具备应对网络威胁的能力
2.网络安全基础技能	2.1 编程语言、操作系统、计算机网络及协议安全	2.1.1 能够使用(C/C++/PHP/Python 等)，进行简单的小工具编写; 2.1.2 理解 C 语言由源文件编译为可执行文件的过程; 2.1.3 掌握 C 语言中基本变量、赋值、数组、指针、函数等基本概念; 2.1.4 掌握 C 语言控制流语句，如循环、条件判断等; 2.1.5 了解 Linux 基础架构，如文件系统、权限控制，安全机制;

		2.1.6 了解 Linux 系统相关的基础常见命令； 2.1.7 了解用户管理相关知识； 2.1.8 了解进程、软件相关知识； 2.1.9 了解 Shell 编程； 2.1.10 了解 Windows 系统基础知识； 2.1.11 掌握 Python 语言中基本变量、赋值、函数等基本概念； 2.1.12 掌握 Python 语言数据类型如列表、元组、字典、集合等； 2.1.13 掌握 Python 语言控制语句； 2.1.14 掌握 Python 语言类与对象的使用； 2.1.15 掌握 Python 语言网络编程； 2.1.16 了解 PHP 环境配置方法、PHP 工作流程； 2.1.17 掌握 PHP 编程基础知识，能使用 PHP 语言进行基本代码编写； 2.1.18 了解 OSI 七层模型、TCP/IP 协议模型； 2.1.19 了解抓包工具的基本使用方法（wireshark/tcpdump）； 2.1.20 了解 TCP/IP 协议簇中常见协议原理,对 DNS/HTTP/TLS 等应用层协议细节有深入的理解； 2.1.21 掌握交换协议、静态/动态路由协议和 STP,LLDP 等网络协议； 2.1.22 具备操作配置 Cisco/Huawei/H3C 等主流网络设备的能力。
3.Web 安全评估测试	3.1Web 安全/渗透	3.1.1 熟知信息安全基本概念及知识体系结构； 3.1.2 了解 owasp top10 攻击原理利用和修复方式； 3.1.3 能够挖掘常见 web 安全漏洞（如 SQL 注入，XSS，CSRF，SSRF，逻辑漏洞、文件漏洞等）； 3.1.4 了解常见开发框架及开源应用历史漏洞； 3.1.5 了解渗透测试的概念、目的、分类和原则、

		流程； 3.1.6 了解渗透测试执行过程中的主要阶段及其内容； 3.1.7 了解渗透测试过程所涉及技术和渗透测试报告撰写的方法； 3.1.8 了解 APT 攻击的概念、特点、经典案例和危害； 3.1.9 了解常见的渗透工具（BurpSuite、SQLmap、nmap、AWVS）； 3.1.10 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； 3.1.11 熟悉 shodan、zoomeye 网络空间搜索引擎使用方式，Google Hacking 信息收集方法。
4.安全评估	4.1 代码审计	4.1.1 能够表述代码审计的原理； 4.1.2 代码审计工具的使用（RIPS、VCG、Fortify）； 4.1.3 能够对常见 Web 漏洞进行代码审计（OWASP TOP10 漏洞） 4.1.4 了解代码审计测试方法及流程。
5.安全事件分析	5.1 恶意软件分析	5.1.1 熟悉病毒的基本分类； 5.1.2 熟悉病毒的常见技术； 5.1.3 熟练常见的安全工具（OllyICE,IDA Pro,PEiD,Wireshark,ProcMon,SandBoxie）； 5.1.4 熟练地搭建和使用虚拟环境； 5.1.5 熟练地使用静态分析进行行为预测； 5.1.6 熟练地使用动态调试进行行为分析； 5.1.7 可以独立分析出病毒的行为片段； 5.1.8 可以独立分析病毒行为(释放的文件,更改的位置,抓取发送的数据)。
6.企业安全综合策略	6.1 等级保护	6.1.1 理解信息安全等级保护含义,掌握等级保护测评流程；

		6.1.2 具备进行等级保护安全建设的能力； 6.1.3 掌握二、三、四级等保安全基线要求； 6.1.4 适当了解行业安全标准及安全规定，关注行业动态； 6.1.5 具备对攻击事件的攻击取证和追踪溯源能力； 6.1.6 掌握常见安全设备的工作原理，能够操作配置常见主流产品； 6.1.7 具备对流量及安全设备的日志、告警分析的能力； 6.1.8 熟知操作系统知识架构； 6.1.9 能够对 Linux/Windows 操作系统进行日常运维和操作； 6.1.10 具备 Linux/Windows 操作系统应用能力（系统编程、服务搭建）； 6.1.11 表述操作系统安全配置（标识鉴别、访问控制、安全审计） 6.1.12 表述常见操作系统漏洞原理及利用方法； 6.1.13 掌握常见的密码学算法、特点、适用场景 6.1.14 了解构建网络安全防护体系，了解常见安防设备的部署； 6.1.15 了解 SSL 和 SSL 证书体系安全中的常见安全问题。

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. 网络安全基础技能	1.1 编程语言、操作系统、计算机网络及协议安全	1.1.1 熟练掌握一门编程语言(C/C++/PHP/Python 等)，能够根据工作内容进行小工具编写辅助自身； 1.1.2 掌握 Linux 基础架构，如文件系统、权限控制，安全机制等；

		1.1.3 掌握 Shell 编程； 1.1.4 掌握 AWK/SED 的使用； 1.1.5 熟练掌握用户管理相关知识，掌握 UGO/ACL 权限； 1.1.6 熟练掌握进程、软件相关知识； 1.1.7 掌握 Python 爬虫的原理； 1.1.8 掌握 Python urllib、socket 模块的使用； 1.1.9 掌握 PHP 表单、文件、会话处理、数据库操作、正则、文件上传等； 1.1.10 能使用 PHP 语言或借助 CMS 搭建项目； 1.1.11 掌握路由、交换技术； 1.1.12 熟练掌握 wireshark、tcpdump 的使用，并能使用这些工具进行协议分析 1.1.13 理解 TCP/IP 协议存在的脆弱点细节； 1.1.14 了解安全开发生命周期（SDL）的流程及内容； 1.1.15 熟悉内网常见安全协议，如证书、LDAP，kerberos，Radius、802.1x 等。
2.Web 安全评估测试	2.1Web 安全/渗透	2.1.1 熟知信息安全基本概念及知识体系结构； 2.1.2 了解 Web 常见漏洞攻击原理利用和修复方式； 2.1.3 黑盒独立挖掘常见 web 安全漏洞（如 SQL 注入，XSS，CSRF，SSRF，权限绕过等）； 2.1.4 能够复现 owasp top10 漏洞并掌握原理； 2.1.5 能够复现常见开发框架及开源应用历史漏洞； 2.1.6 理解常见 WAF 及 IDS 等安全设备规则绕过方法； 2.1.7 熟练掌握 BurpSuite、SQLMAP、NMAP、AWVS、Metasploit 的使用； 2.1.8 了解浏览器插件配置与应用； 2.1.9 熟练掌握常用的信息收集方法，能充分利

		用收集后的信息进行渗透测试； 2.1.10 了解社工库、多维度信息收集方法、钓鱼邮件、宏病毒等； 2.1.11 了解 CobaltStrike 安装配置和使用方法； 2.1.12 掌握常见的中间件及组件漏洞综合利用； 2.1.13 了解内网渗透技术； 2.1.14 理解 APT 攻击的入侵途径和方法； 2.1.15 掌握 APT 攻击的针对性防护策略。
3.安全评估	3.1 代码审计	3.1.1 掌握代码审计工具的使用（RIPS、VCG、Fortify）； 3.1.2 能够对常见 Web 漏洞进行代码审计(OWASP TOP10 漏洞） 3.1.3 具备代码阅读能力； 3.1.4 掌握代码审计测试方法及流程。
4.安全事件分析	4.1 恶意软件分析	4.1.1 熟悉汇编语言； 4.1.2 熟悉 PE 结构； 4.1.3 可以从高级语言层面去理解对恶意代码的静态分析； 4.1.4 可以从高级语言层面去理解对恶意代码的动态调试； 4.1.5 熟悉 IAT 结构； 4.1.6 熟悉资源结构； 4.1.7 理解恶意代码漏洞利用与攻击载荷思想 4.1.8 熟悉常见 API 与恶意 API； 4.1.9 能够将样本分析特征进行入库,形成检测特征； 4.1.10 能够针对恶意代码的技术实现细节做详细描述； 4.1.11 能够针对恶意代码的运作流程做详细描述。

5. 企业安全综合策略	5.1 等级保护	5.1.1 理解信息安全等级保护含义，熟练掌握等级保护测评流程； 5.1.2 具备独立进行等级保护安全建设的能力； 5.1.3 掌握二、三、四级等保安全基线要求； 5.1.4 了解部分行业安全标准及安全规定，关注行业动态； 5.1.5 具备对攻击事件的攻击取证和追踪溯源能力； 5.1.6 掌握常见安全设备的工作原理，能够熟练操作配置常见主流产品； 5.1.7 具备对流量及安全设备的日志、告警分析的能力，能够对真实发生的安全攻击事件进行定位； 5.1.8 能够复现常见操作系统漏洞，掌握利用方法； 5.1.9 能够对常见操作系统漏洞进行评估，确认危害性并能进行修复/规避； 5.1.10 能够表述内网域环境的基本协议和运行原理，能够手动搭建域环境； 5.1.11 掌握常见的密码学算法、特点、适用场景； 5.1.12 掌握对网络设备进行安全加固的能力，掌握网络设备安全基线； 5.1.13 具备识别常见的网络攻击数据包（如DDoS、局域网攻击、常见攻击特征包、扫描包）能力。

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. 网络安全基础技能	1.1 编程语言、操作系统、计算机网络及协议安全	1.1.1 熟练掌握一门编程语言(C/C++/PHP/Python 等)，能够根据工作内容进行小工具编写辅助自身； 1.1.2 掌握计划任务的应用；

		1.1.3 掌握数据存储管理与性能测试方法； 1.1.4 掌握 Windows 域环境搭建、域控制器配置等； 1.1.5 掌握 Windows 系统安全防护策略； 1.1.6 熟练使用 python 等开发语言进行安全相关应用开发，开发复杂功能和安全工具； 1.1.7 能使用 PHP 搭建复杂项目，熟练掌握 PHP 网址搭建、安全配置等； 1.1.8 掌握常见协议脆弱点的利用方法和应对措施； 1.1.9 熟练掌握常见的协议/流量/网络安全事件分析方法； 1.1.10 掌握安全开发生命周期（SDL）的流程及内容，并能实际运用到程序开发中。
2.Web 安全评估测试	2.1Web 安全/渗透	2.1.1 熟知信息安全基本概念及知识体系结构； 2.1.2 了解 Web 常见漏洞攻击原理利用和修复方式； 2.1.3 能够用黑盒独立挖掘常见 web 安全漏洞（如 SQL 注入，XSS，CSRF，SSRF，权限绕过等）； 2.1.4 能够复现 owasp top10 漏洞并掌握原理； 2.1.5 能够复现常见开发框架及开源应用历史漏洞； 2.1.6 具备对常见 WAF 及 IDS 等安全设备规则绕过的能力； 2.1.7 理解并掌握 BurpSuite、SQLMAP、NMAP、AWVS、Metasploit 等工具的原理及高级使用方法，能灵活使用工具进行渗透测试； 2.1.8 掌握无线渗透原理及常用工具； 2.1.9 掌握常用的社工技巧，掌握 CHM、LNK、HTA 文件生成及利用方法； 2.1.10 掌握 office 常见漏洞及宏钓鱼利用方法；

		2.1.11 熟练掌握内网渗透技术； 2.1.12 能够读懂常见漏洞 EXP，并写出关键 payload。
3.安全评估	3.1 代码审计	3.1.1 掌握代码审计工具的使用（RIPS、VCG、Fortify）； 3.1.2 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）； 3.1.3 具备阅读复杂代码的能力； 3.1.4 熟练运用代码审计流程进行测试工作； 3.1.5 具备较丰富的安全代码编写经验。
4.安全事件分析	4.1 恶意软件分析	4.1.1 熟悉常见加密算法； 4.1.2 能还原常见加密算法； 4.1.3 熟悉自定义算法识别； 4.1.4 能还原自定义加密算法； 4.1.5 熟悉常见反调试技术； 4.1.6 能跳过各种反调试检测； 4.1.7 熟悉常见压缩算法与解压缩算法； 4.1.8 熟练运用内存 DUMP； 4.1.9 熟练使用 010Editor 十六进制编辑； 4.1.10 编写 IDC 脚本解密字节； 4.1.11 可以手工脱壳,压缩壳和加密壳,未知壳。
5.企业安全综合策略	5.1 等级保护	5.1.1 理解信息安全等级保护含义，熟练掌握等级保护测评流程； 5.1.2 具备独立进行等级保护安全建设的能力； 5.1.3 掌握二、三、四级等保安全基线要求； 5.1.4 了解多数行业安全标准及安全规定，关注行业动态； 5.1.5 具备对攻击事件的攻击取证和追踪溯源能力； 5.1.6 掌握常见安全设备的工作原理，能够熟练操作配置常见主流产品；

		5.1.7 能够准确分析网络流量、日志、告警，并能够准确的进行安全评估，提出解决思路； 5.1.8 能够独立处理常见的安全攻击事件； 5.1.9 能够对内网域环境下的主要服务（包括 Exchange、LDAP、Radius、802.1x 等）进行安全加固、安全配置和安全运维； 5.1.10 能够表述 Linux 网络协议栈的高性能处理机制； 5.1.11 能够调试内核协议栈网络相关参数，对 Linux kernel 内核架构有深入理解； 5.1.12 掌握常见的密码学算法、特点、适用场景； 5.1.13 熟练掌握识别常见的网络攻击数据包（如 DDoS、局域网攻击、常见攻击特征包、扫描包）能力； 5.1.14 理解并能够表述新网络技术（如 SDN、Vxlan、虚拟化等） 5.1.15 能够快速定位因安全因素导致的网络故障，掌握排错的能力。

参考文献

[1] 高等职业学校专业教学标准.2019

[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] 普通高等学校本科专业目录.2012

[5] 普通高等学校高等职业教育（专科）专业目录及专业简介

[6] 国家职业技能标准编制技术规程.2018 年版

[7] 中华人民共和国网络安全法

[8] 信息安全技术网络安全等级保护基本要求

[9] 信息安全技术网络安全等级保护测评要求

[10] 信息安全技术网络安全等级保护安全设计技术要求