网络安全渗透测试

职业技能等级标准

（2021年1.0版）

北京天融信网络安全技术有限公司　制定

2021 年 3 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：北京天融信网络安全技术有限公司、北京天融信教育科技有限公司、北京天融信科技有限公司、中基石油通信建设有限公司、四川大学、华中科技大学、西安邮电大学、金陵科技学院、岭南师范学院、宁波大学科学技术学院、湖北民族大学、晋中职业技术学院、东营科技职业学院、四川水利职业技术学院、西藏职业技术学院。

本标准主要起草人：于海波、李雪莹、毛丽艳、李跃忠、程晓峰、王春伟、方勇、周安民、王志航、苗春羽、郝钢、温晓飞、张正、张晓、阎浩、柳亚男、沈济南、张君华、符强、闵笛、高海燕、汪晓华、周健。

1 范围

本标准规定了网络安全渗透测试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渗透测试职业技能培训、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 25069-2010 信息安全技术 术语

GB/T 25068.1-2012 信息技术 安全技术 IT网络安全

GB/T 30283-2013 信息安全技术 信息安全服务 分类

GB/T 20270-2006 信息安全技术 网络基础安全技术要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

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

3 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本标准。

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、抗抵赖性、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。也称渗透性测试或逆向测试。

[GB/T 25069-2010，定义 2.3.87]

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、网络安防系统安装与维护、软件与信息服务等。

高等职业学校：计算机网络技术、信息安全与管理、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、信息管理与信息系统等。

5 面向职业岗位（群）

【网络安全渗透测试】（初级）：主要面向 IT 互联网企业、传统企事业单位、

政府等的信息安全部门或安全服务部门的相关技术岗位，如网络安全巡检、Web渗透测试、Web安全加固、安全运维等。

【网络安全渗透测试】(中级): 主要面向IT互联网企业、传统企事业单位、政府等的信息安全部门或安全服务部门的相关技术岗位,如风险评估、渗透测试、系统运维与安全管理、等级保护、应急响应等。

【网络安全渗透测试】(高级): 主要面向IT互联网企业、传统企事业单位、政府等的信息安全部门或安全服务部门的相关技术岗位，如攻防对抗研究、漏洞挖掘、高级威胁分析、等保体系建设、网络安全管理等。

6 职业技能要求

6.1 职业技能等级划分

网络安全渗透测试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。

【网络安全渗透测试】(初级): 主要面向IT互联网企业、传统企事业单位、政府等的信息安全部门或安全服务部门，从事网络安全巡检、简单Web应用渗透测试及安全加固等工作。

【网络安全渗透测试】(中级): 主要面向IT互联网企业、传统企事业单位、政府等的信息安全部门或安全服务部门,从事信息系统安全渗透测试及应急响应等工作，根据信息系统安全需求，灵活使用各类安全工具对常见网络设备、操作系统和应用系统进行渗透测试，编制渗透测试报告，为网络安全事件应急响应工作提供理论和技术支撑。

【网络安全渗透测试】(高级): 主要面向IT互联网企业、传统企事业单位、政府等的信息安全部门或安全服务部门，从事信息系统整体安全解决方案设计、

信息系统安全风险评估、入侵行为监测与分析、应急预案编制与实施等工作。

6.2 职业技能等级要求描述

表 1 网络安全渗透测试职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1. 渗透测试	1.1 应用系统渗透测试	1.1.1 理解渗透测试相关基本概念，理解渗透测试的必要性和可行性。 1.1.2 理解我国网络安全相关法律法规。深刻理解《中华人民共和国网络安全法》。 1.1.3 深刻理解渗透测试服务中取得客户授权的重要性，充分理解渗透测试服务对测试人员职业道德素质与保密要求。 1.1.4 理解渗透测试基本流程，包括外部信息收集、漏洞扫描、威胁建模、漏洞利用、权限提升、内网渗透、输出渗透测试报告等。 1.1.5 能够独立撰写渗透测试报告。 1.1.6 能够完成包括 DNS 记录、子域名、C 段扫描、Web 目录扫描、指纹识别等常见信息收集操作。 1.1.7 掌握 Nmap、AWVS、Nessus、Burp Suite、Sqlmap、Metasploit 等常见工具的原理及高级使用方法。 1.1.8 熟练掌握常见 Web 编程语言，包括 PHP/JS/Python 等，能够进行网站搭建、Web 应用场景部署及安全配置。 1.1.9 深入理解 OWASP Top 10 漏洞形成原因及修复方式，如 SQL 注入漏洞，XSS 漏洞，CSRF 漏洞，XXE 漏洞，文件上传漏洞等。 1.1.10 了解常见开发框架及开源应用历史漏洞利用方法。
	1.2 操作系统渗透测试	1.2.1 深入理解 Windows 操作系统安全机制。 1.2.2 掌握 Windows 系统域环境搭建、域控制器配置等。 1.2.3 掌握常见 Windows 操作系统漏洞利用方法。包括 MS08-067、MS17-010 等。 1.2.4 掌握 Metasploit、Cobalt Strike 等常见漏洞利用平台的安装、配置和使用方法。 1.2.5 熟悉内网常见安全协议,如 LDAP、Kerberos,Radius、802.1x 等。
2. 安全巡检	2.1 网络设备安全巡检	2.1.1 能够按照网络设备检查列表，对网络设备操作系统版本更新、口令管理、服务安全、策略安全进行逐项检查，输出检查结果。 2.1.2 熟练掌握常见网络安全设备的基本功能设置和安全配置方法。
	2.2 网络服务器安全巡检	2.2.1 能够按照服务器检查列表，对 Windows 操作系统进行补丁安装情况、账户策略、安全设置、注册表安全、需关闭的服务项等进行逐项检查，并输出检查结果。

工作领域	工作任务	职业技能要求
		2.2.2 能够按照服务器检查列表，对 Linux 操作系统进行登录控制、用户策略、服务安全及其他安全设置进行逐项检查，并输出检查结果。
	2.3 数据库系统安全巡检	2.3.1 能够按照数据库检查列表，对数据库版本升级情况、安全设置、安全使用外部存储过程、账户和密码安全设置、安全配置审计功能及保护关键文件进行逐项检查。 2.3.2 熟练掌握常见数据库管理系统基本操作及安全配置方法。
3.安全加固	3.1 网络设备安全加固	3.1.1 理解常见网络通信设备工作原理，能够对常见网络设备进行安全加固和安全配置。 3.1.2 掌握主流交换机账号管理、认证和授权配置技术、日志配置技术、通信协议配置技术。 3.1.3 掌握主流路由器账号管理、认证和授权配置技术、日志配置技术、通信协议配置技术。
	3.2 操作系统安全加固	3.2.1 能够对 Windows 系统和 Linux 系统进行安全加固和安全配置。 3.2.2 掌握 Windows 操作系统账号管理、认证授权、日志配置、共享权限配置、补丁管理、防病毒管理、服务管理、启动项管理、策略配置等技术。 3.2.3 掌握 Linux 操作系统账号管理、认证授权、日志审计、共享权限配置、补丁管理、系统状态、启动项管理、防火墙技术。

表 2 网络安全渗透测试职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1.渗透测试	1.1 应用系统渗透测试	1.1.1 能够完成常见 OWASP TOP 10 Web 安全漏洞诊断及安全加固工作，包括 SQL 注入漏洞，XSS 漏洞，CSRF 漏洞，XXE 漏洞，文件上传漏洞等。 1.1.2 能够复现常见开发框架及开源应用系统历史漏洞。 1.1.3 掌握常见的中间件及组件漏洞利用方法。 1.1.4 掌握常见数据库管理系统漏洞利用方法。
	1.2 操作系统渗透测试	1.2.1 能够完成常见 Windows 操作系统安全漏洞诊断及安全加固工作,包括 MS03-026、MS08-067、MS17-010 等。 1.2.2 理解 Linux 系统安全机制，包括文件系统、权限控制等。 1.2.3 掌握 Shell 编程，掌握 awk/grep/sed 的使用。 1.2.4 掌握常见 Linux 操作系统漏洞利用方法。 1.2.5 熟练掌握用户管理相关知识，掌握 UGO/ACL 权限配置方法。
	1.3 网络设备渗透测试	1.3.1 掌握常见网络层扫描及渗透测试工具使用方法。 1.3.2 理解 OSI 七层模型、TCP/IP 协议模型。

工作领域	工作任务	职业技能要求
		1.3.3 理解 TCP/IP 协议簇中常见协议原理，对 DNS/HTTP/TLS/FTP/DHCP/ARP 等协议细节有深入的理解。 1.3.4 掌握 Wireshark 等常见抓包工具的使用方法。 1.3.5 理解交换协议、静态/动态路由协议原理。 1.3.6 具备操作配置主流网络设备的能力。
2.安全巡检	2.1 网络及网络服务器安全巡检	2.1.1 能够按照网络设备检查列表，完成相应的安全巡检工作。 2.1.2 能够按照应用服务器检查列表，完成相应的安全巡检工作。 2.1.3 能够按照数据库服务器检查列表,完成相应的安全巡检工作。
	2.2 防火墙安全巡检	2.2.1 能够按照防火墙检查列表，对防火墙系统进行自身安全性、运行维护项、防火墙策略、运行状况进行逐项检查，并输出检查结果。 2.2.2 熟练掌握防火墙的基本操作及安全策略配置方法。
	2.3 IDS/IDP 安全巡检	2.3.1 能够按照 IDS/IPS 检查列表，对 IDS/IPS 的网络部署、探测引擎的安全性、日志管理及运行维护项进行逐项检查，并输出检查结果。 2.3.2 熟练掌握 IDS/IPS 系统的部署及基本配置方法。
3.安全加固	3.1 网络及操作系统安全加固	3.1.1 能够完成常见网络设备的安全加固工作。 3.1.2 能够完成 Windows 和 Linux 系统的安全加固工作。
	3.2 数据库系统安全加固	3.2.1 掌握常见数据库管理系统工作原理。 3.2.2 能够按照 MySQL 数据库系统安全加固规范开展包括 MySQL 账号管理、认证授权、日志系统配置及通信协议安全配置等安全加固工作。 3.2.3 能够按照 MS SQL Server 数据库系统安全加固规范开展包括 MS SQL Server 账号管理、认证授权、日志系统配置及通信协议安全配置等安全加固工作。 3.2.4 能够按照 Oracle 数据库系统安全加固规范开展包括 Oracle 账号管理、认证授权、日志系统配置及通信协议安全配置等安全加固工作。
	3.3 中间件应用框架安全加固	3.3.1 熟悉常见中间件应用平台，能够按照实际需求部署相应应用场景。 3.3.2 能够按照 IIS 中间件系统安全加固规范开展包括 IIS 账号管理、认证授权、日志系统配置及通信协议安全配置等安全加固工作。 3.3.3 能够按照 Apache 中间件系统安全加固规范开展包括 Apache 账号管理、认证授权、日志系统配置及通信协议安全配置等安全加固工作。 3.3.4 能够按照 Tomcat 中间件系统安全加固规范开展包括 Tomcat 账号管理、认证授权、日志系统配置及通信协议安

工作领域	工作任务	职业技能要求
		全配置等安全加固工作。
4.应急响应	4.1 网站安全事件应急响应	4.1.1 了解我国网络安全事件应急响应相关政策及标准。 4.1.2 能够快速定位网站故障原因，具备应急处置能力。 4.1.3 掌握网站黑链检测排查技术及 WebShell 查杀技术。 4.1.4 能够分析 Web 日志及相关告警信息。具备 Web 安全事件总结分析及漏洞复现能力。 4.1.5 熟练部署 WAF 网站应用防火墙及网页防篡改系统。
	4.2 操作系统安全事件应急响应	4.2.1 熟练掌握 Windows/Linux 系统常见入侵排查命令及工具，如 Process Explorer、Autoruns、chkrootkit 等。 4.2.2 能够完成 Windows/Linux 系统可疑账号（包括弱口令账号、隐藏账号、克隆账号）排查；异常端口、异常进程、可疑连接排查；启动项、计划任务及服务排查。 4.2.3 熟练掌握 Windows/Linux 系统病毒查杀、系统日志分析技术。

表 3 网络安全渗透测试职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1.渗透测试	1.1 应用系统渗透测试	1.1.1 能够完成对常见 Web 应用、中间件、数据库进行安全漏洞诊断、分析及安全加固工作。 1.1.2 理解常见 WAF 及 IDS 等安全设备规则绕过方法。 1.1.3 能够读懂常见漏洞 EXP，熟练使用 Python 等开发语言编写关键 Payload。 1.1.4 掌握 Office 等其他常见应用软件漏洞利用方法。
	1.2 操作系统渗透测试	1.2.1 熟练掌握 Windows/Linux 操作系统漏洞利用方法。 1.2.2 熟练掌握常见内网渗透技术，包括端口转发，DNS 隧道、ICMP 隧道、域渗透等。
	1.3 网络设备渗透测试	1.3.1 熟练掌握常见网络网络安全扫描工具的使用方法。 1.3.2 具备对常见网络设备及防火墙策略绕过的能力。 1.3.3 理解 WEP、WPA-PSK 等常见 Wifi 加密方式安全漏洞技术原理。 1.3.4 能够完成无线网络安全渗透测试、诊断分析及安全加固工作。
2.安全巡检	2.1 网络及网络服务器安全巡检	2.1.1 能够按照网络设备检查列表，完成相应的安全巡检工作。 2.1.2 能够按照应用服务器检查列表，完成相应的安全巡检工作。 2.1.3 能够按照数据库系统检查列表，完成相应的安全巡检工作。
	2.2 网络安全设备巡检	2.2.1 能够按照网络安全设备检查列表，完成对防火墙设备的安全巡检工作。 2.2.2 能够按照网络安全设备检查列表，完成对 IDS/IPS

工作领域	工作任务	职业技能要求
		设备的安全巡检工作。
	2.3 防病毒系统安全巡检	2.3.1 能够按照防病毒系统检查列表，对防病毒系统进行符合性要求、部署合理性、病毒库升级、病毒查杀、日志记录、告警机制、应急恢复等进行逐项检查。 2.3.2 熟练掌握防病毒过滤系统安装、部署与配置方法。
	2.4 网络审计系统安全巡检	2.4.1 能够按照审计系统检查列表，对审计系统进行审计数据产生、审计记录的查阅、审计数据存储、审计系统自身防护等进行逐项检查，并输出检查结果。 2.4.2 熟练掌握常见审计系统的安装、部署与配置方法。
3.安全加固	3.1 网络及操作系统安全加固	3.1.1 能够完成常见网络设备的安全加固工作。 3.1.2 能够完成对 Windows/ Linux 系统的安全加固工作。
	3.2 数据库及中间件安全加固	3.2.1 能够完成常见数据库系统的安全加固工作。 3.2.2 能够完成常见中间件应用平台的安全加固工作。
	3.3 应用程序代码安全加固	3.3.1 具备代码阅读能力。 3.3.2 掌握代码审计测试方法及流程，能够输出代码审计报告。 3.3.3 掌握包括 RIPS、Fortify SCA、VCG 等常见代码审计工具的使用。 3.3.4 具备常见 Web 应用漏洞代码审计及加固能力。
4.应急响应	4.1 应急预案编制与应急演练	4.1.1 了解 GB/Z 20986-2007 《信息安全技术 信息安全事件分类分级指南》。 4.1.2 了解 GB/T 24364-2009 《信息安全技术 信息安全应急响应计划规范》。 4.1.3 能够根据业务特点以及不同安全事件场景编制相应的专项应急预案。 4.1.4 能够在应急预案的基础上组织协同各业务系统开展沙盘演练及实战演练。
	4.2 应用系统安全事件应急响应	4.2.1 具备网站安全类事件应急检测、遏制、故障原因分析、系统恢复、总结跟踪能力。 4.2.2 具备操作系统安全类事件的应急检测、遏制、故障原因分析、系统恢复、总结跟踪能力。 4.2.3 具备数据库相关安全事件的应急检测、遏制、故障原因分析、系统恢复、总结跟踪能力。
	4.3 恶意程序事件应急响应	4.3.1 熟悉恶意代码的基本分类及应急处置措施。 4.3.2 熟练掌握常见调试分析工具，如 PEiD、OllyICE、IDA Pro 等，能够使用静态分析和动态调试技术进行恶意代码行为预测与分析。 4.3.3 熟悉汇编语言，熟悉 PE 结构，熟悉反调试技术。 4.3.4 能够对恶意代码的运作过程进行详细描述。

工作领域	工作任务	职业技能要求
	4.4 网络攻击事件应急响应	4.4.1 熟练掌握网络抓包分析技术，能够熟练识别常见网络攻击，如 ARP 欺骗攻击、DNS 劫持、DDoS 攻击等。 4.4.2 能够准确分析网络流量、各类日志及告警信息。 4.4.3 能够合理选择应急处置措施。 4.4.4 具备网络攻击事件的取证和追踪溯源能力。

参考文献

[1] 中等职业学校专业目录（2010年修订）

[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] SJ/T 11623-2016 信息技术服务从业人员能力规范

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

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

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

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

[14] GB/T 20281-2015 信息安全技术 防火墙安全技术要求和测试评价方法

[15] GB/T 28454-2012 信息技术 安全技术 入侵检测系统的选择、部署和操作