网络安全运维

职业技能等级标准

标准代码：510005

（2021年2.0版）

中科软科技股份有限公司　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：中科软科技股份有限公司、中科磐云（北京）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、重庆电子工程职业学院、黄冈职业技术学院、北京市求实职业学校、北京市信息管理学校。

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、鲁先志、胡兵、周源、彭金华、杨毅、何琳、胡志齐、徐雪鹏、孙雨春、赵飞、邹君雨、张天乐、王梓。

声明：本标准的知识产权归属于中科软科技股份有限公司，未经中科软科技股份有限公司同意，不得印刷、销售。

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 25069-2010 信息安全技术 术语

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

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]

3.7

密码破译 code breaking

在未知预先约定的情况下，采用适当的方法和技术，由密文获得明文的过程。

[GB/T 25069-2010，定义 2.2.2.97]

3.8

验证 verification

将某一活动或处理过程的输出与其相对应的安全需求或规范相比较，并证实该输出满足需求或规范的过程。

[GB/T 25069-2010，定义 2.3.103]

4 适用院校专业

4.1 参照原版专业目录

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、网络安防系统安装与维护、物联网技术应用、移动应用技术与服务、通信技术、电子商务、跨境电子商务、移动商务。

高等职业学校：信息安全与管理、计算机网络技术、计算机应用技术、计算机信息管理、计算机系统与维护、软件技术、软件与信息服务、电子商务技术、大数据技术与应用、云计算技术与应用、人工智能技术服务、工业网络技术、物联网应用技术、物联网工程技术、通信技术、移动通信技术、司法信息技术、司法信息安全、信息网络安全监察、电子商务、跨境电子商务、移动商务。

高等职业教育本科学校：信息安全与管理、计算机应用工程、网络工程、软件工程、通信工程、物联网工程、大数据技术与应用、轨道交通信号与控制、区块链技术与应用、电子商务、跨境电子商务。

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、软件工程、通信工程、信息工程、物联网工程、数据科学与大数据技术、区块链工程、密码科学与技术、人工智能、网络安全与执法、电子商务、跨境电子商务。

4.2 参照新版职业教育专业目录

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、大数据技术应用、网络安防系统安装与维护、物联网技术应用、移动应用技术与服务、现代通信技术应用、电子商务、跨境电子商务、移动商务。

高等职业学校：信息安全技术应用、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、人工智能技术应用、区块链技术应用、密码技术应用、工业互联网技术、物联网应用技术、现代通信技术、现代移动通信技术、智能互联网络技术、司法信息技术、司法信息安全、网络安全与执法、电子商务、跨境电子商务、移动商务。

高等职业教育本科学校：信息安全与管理、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、人工智能工程技术、工业互联网技术、城市轨道交通信号与控制技术、现代通信工程、物联网工程技术、区块链技术、网络安全与执法、电子商务、跨境电子商务。

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、软件工程、通信工程、信息工程、物联网工程、数据科学与大数据技术、区块链工程、密码科学与技术、人工智能、网络安全与执法、电子商务、跨境电子商务。

5 面向职业岗位（群）

【网络安全运维】（初级）：主要面向互联网及相关服务、软件和信息技术服务行业，网络安全管理与维护、网络安全产品部署维护和营销服务领域的网络

安全管理员、信息安全管理员、信息安全测试员等岗位，从事网络安全策略部署、网络设备安全管理与维护、系统安全管理与维护、网络信息系统渗透测试等工作。

【网络安全运维】（中级）：主要面向互联网及相关服务、软件和信息技术服务行业，网络安全管理与维护、网络安全产品部署维护和营销服务领域的网络安全管理员、信息安全管理员、信息安全测试员等岗位，从事网络安全渗透测试、系统安全渗透测试及加固、安全产品部署与调试、安全产品售前售后等工作。

【网络安全运维】（高级）：主要面向互联网及相关服务、软件和信息技术服务行业，网络安全管理与维护、网络安全产品部署维护和营销服务领域的网络安全管理员、信息安全管理员、信息安全测试员等岗位，从事网络和系统安全防护、WEB 安全防护、风险评估、安全审计、网络安全项目集成等工作。

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运维需求，熟悉网络安全法律法规，完成网络的组建与防护、常见操作系统的安全管理与维护、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运维需求，完成安全产品的部署调试、系统安全渗透测试、常用数据库的安全配置与管理、常见操作系统漏洞诊断及安全加固等作业。

【网络安全运维】（高级）：根据网络和系统安全运维需求，完成网络和系统安全的风险评估、Web 安全的诊断及加固、入侵行为的检测及安全防御、网络安全项目集成等作业。

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.网络安全法律法规与职业素养	1.1 安全法规学习	1.1.1 熟悉《中华人民共和国网络安全法》。 1.1.2 熟悉《中华人民共和国数据安全法》。 1.1.3 熟悉《信息安全技术网络信息安全等级保护基本要求》。 1.1.4 熟悉我国其他网络安全相关法律法规。
	1.2 职业素养认知	1.2.1 树立国家安全意识，自觉维护国家、社会、人民的安全利益。 1.2.2 具有遵纪守法，诚实守信的职业道德。 1.2.3 具有忠于职守，勇于创新的职业素养。 1.2.4 具有认真负责，团结协作的职业能力。
2.网络设备安装调试	2.1 设备安装与配置	2.1.1 能够掌握基础网络体系架构及网络系统的结构设计。 2.1.2 能够掌握网络设备（路由、交换、无线）的作用、原理、分类、部署方式。 2.1.3 能够进行网络设备（路由、交换、无线）的初始化安装。 2.1.4 能够进行网络设备（路由、交换、无线）的组网和配置。
	2.2 设备调试与测试	2.2.1 能够配置网络设备实现基础网络的互联互通。 2.2.2 能够进行网络设备运行状态的监测与记录。 2.2.3 能够依据网络设备状态信息进行系统升级、线路调整、配置调整等常见的维护操作。 2.2.4 能够根据测试报告模板及设备运行情况填写测试报告。
	2.3 设备安全配置与加固	2.3.1 能够根据用户需求，对网络设备进行安全加固。 2.3.2 能够根据用户需求，配置访问策略。 2.3.3 能够根据实施方案，保障设备的物理安全。 2.3.4 能够分析、处理网络设备日志信息。
3.操作系统安全配置	3.1Windows 操作系统安全配置	3.1.1 能够根据用户需求，对 Windows 系统的用户和组进行安全管理。 3.1.2 能够根据用户需求，对 Windows 系统的文件系统、服务、防火墙进行安全配置。 3.1.3 能够根据用户需求，对 Windows 系统的域与活动目录进行安全管理。

		3.1.4 能够根据用户需求，制定 Windows 系统本地安全策略。 3.1.5 能够根据用户需求，搭建 VPN 服务。 3.1.6 能够根据用户需求,完成用户信息迁移、系统数据备份与恢复。
	3.2Linux 操作系统安全配置	3.2.1 能够根据用户需求，对 Linux 系统的用户和组进行安全管理。 3.2.2 能够根据用户需求，对 Linux 系统的 SSH、Apache、DHCP、NFS、Samba、VsFTPd 服务进行安全配置。 3.2.3 能够根据用户需求，对 Linux 系统的防火墙进行安全配置。 3.2.4 能使用 Autid 工具对用户空间进行安全审计。 3.2.5 能使用 Rsyslog 工具对客户端的 history 记录进行安全审计。
	3.3 操作系统漏洞验证及加固	3.3.1 能根据操作系统安全需求，使用漏洞验证工具对 MS08_067 漏洞进行验证与安全加固。 3.3.2 能根据操作系统安全需求，使用漏洞验证工具对 MS10_003 漏洞进行验证与安全加固。 3.3.3 能根据操作系统安全需求，使用漏洞验证工具对 MS12_020 漏洞进行验证与安全加固。 3.3.4 能根据操作系统安全需求，使用漏洞验证工具对 MS15_034 漏洞进行验证与安全加固。 3.3.5 能根据操作系统安全需求，使用漏洞验证工具对 MS14_064 漏洞进行验证与安全加固。 3.3.6 能根据操作系统安全需求，使用漏洞验证工具对 MS17_010 漏洞进行验证与安全加固。
	3.4 木马病毒判断与处理	3.4.1 熟悉并了解远程控制木马工具。 3.4.2 能根据木马病毒判断与处理的需求，对 Office 病毒进行判断与处理。 3.4.3 能根据木马病毒判断与处理的需求，对 Windows 病毒进行判断与处理。 3.4.4 能根据木马病毒判断与处理的需求，对特洛伊木马病毒进行判断与处理。 3.4.5 能根据木马病毒判断与处理的需求，对邮件病毒进行检测与分析。

4.系统安全渗透测试	4.1 数据包分析	4.1.1 掌握常见抓包工具的作用、原理、分类及使用方式。 4.1.2 能根据数据包分析需求,使用 Wireshark 抓包工具对网络进行嗅探。 4.1.3 能根据数据包分析需求，使用 Dsiniff 抓包工具对网络进行嗅探。 4.1.4 能根据数据包分析需求，使用 TCPDump 抓包工具对数据包进行抓取。
	4.2 目标主机识别	4.2.1 能根据目标主机识别需求，使用 Arping 工具对目标主机进行识别。 4.2.2 能根据目标主机识别需求，使用 Fping 工具对目标主机进行识别。 4.2.3 能根据目标主机识别需求,使用 GenList 工具对目标主机进行识别。 4.2.4 能根据目标主机识别需求,使用 NBTScan 工具对目标主机进行识别。
	4.3 信息收集	4.3.1 能根据信息收集需求，使用 Xporbe2 工具对主机信息进行收集。 4.3.2 能根据信息收集需求，使用 Autoscan 工具对主机信息进行收集。 4.3.3 能根据信息收集需求,使用 Nmap 工具对主机信息进行收集。 4.3.4 能根据信息收集需求,使用 Zenmap 工具对主机信息进行收集。

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.网络安全设备部署调试	1.1 设备安装与配置	1.1.1 能够掌握网络安全的体系架构及网络信息系统的结构设计。 1.1.2 能够掌握安全防护设备（防火墙、WAF 等）的作用、原理、分类、部署方式。 1.1.3 能够掌握安全检测设备（入侵检测、入侵防御等）的工作原理及部署方式。 1.1.4 能够掌握安全接入设备（VPN 等）的工作原理及部署方式。 1.1.5 能够进行安全设备（安全防护、安全检测、安全接入）的初始化安装。 1.1.6 能够根据安全设备安装需要，进行操作系统、中间件、数据库系统的安装与配置。
	1.2 设备调试与测试	1.2.1 能够配置安全设备（安全防护、安全检测、安全接入）的安全策略，实现安全策略

		的有效部署。 1.2.2 能够整体联调网络设备和安全设备，实现网络的整体安全运行。 1.2.3 能够对安全设备的运行状态进行监测与记录。 1.2.4 能够依据安全设备状态信息进行系统升级、线路调整、配置调整等常见的维护操作。 1.2.5 能够根据测试报告模板及安全设备运行情况填写测试报告。
	1.3 故障分析与处理	1.3.1 能够根据客户反馈的问题，完成沟通与记录，初步判断设备故障原因。 1.3.2 能够排查发现安全设备的常见故障。 1.3.3 能够向用户有效反馈故障原因及解决办法。 1.3.4 能够处理安全设备的常见故障并编写处理文档。
2.操作系统安全加固	2.1Windows 操作系统漏洞验证及加固	2.1.1 能根据系统安全需求，通过 CVE-2017-7269 漏洞渗透，实现对 IIS6.0 远程代码执行的验证。 2.1.2 能根据系统安全需求，通过 CVE-2017-8464 漏洞渗透，实现对 LNK 文件远程代码执行的验证。 2.1.3 能根据系统安全需求，通过 CVE-2018-4878 漏洞上传，实现对远程控制的验证。 2.1.4 能根据系统安全需求，通过 CVE-2019-0708 漏洞上传，实现对远程控制的验证。
	2.2Linux 操作系统漏洞验证及加固	2.2.1 能根据系统安全需求，通过 CVE-2016-5195 漏洞渗透，实现对 Linux 系统本地提权的验证。 2.2.2 能根据系统安全需求，通过 CVE-2017-7494 漏洞渗透，实现对 Samba 远程代码执行的验证。 2.2.3 能根据系统安全需求，通过 Redis 未授权访问漏洞渗透，实现对主机提权的验证。 2.2.4 能根据系统安全需求，通过 Redis 弱口令，实现对远程 SSH 连接的验证。
	2.3 中间件漏洞验证及加固	2.3.1 能根据中间件安全需求，通过 CVE-2017-9791 漏洞结合 BurpSuite，实现对主机提权的验证。 2.3.2 能根据中间件安全需求，通过 CVE-2017-12617 漏洞渗透，实现对 Tomcat

		远程代码执行的验证。 2.3.3 能根据中间件安全需求，通过 CVE-2017-15715 漏洞渗透，实现对绕过上传黑名单限制的验证。 2.3.4 能根据中间件安全需求，通过 CVE-2018-12613 漏洞渗透，实现对远程文件包含的验证。 2.3.5 能根据中间件安全需求,通过 Java 序列化漏洞，实现对渗透测试的验证。 2.3.6 能根据中间件安全需求，通过 Structs2 框架，实现对远程命令执行的验证。
3.系统安全渗透测试	3.1 密码破解测试	3.1.1 能根据密码安全需求，使用 Hydra 工具实现对密码破解测试的验证。 3.1.2 能根据密码安全需求，使用 Metasploit 工具实现对密码破解测试的验证。 3.1.3 能根据密码安全需求,使用 Crunch 工具实现对密码破解测试的验证。 3.1.4 能根据密码安全需求，使用 Saminside 及 Ophcrack 工具实现对密码破解测试的验证。 3.1.5 能根据密码安全需求,使用 Sparta 工具实现对密码破解测试的验证。
	3.2Web 渗透测试	3.2.1 能根据 Web 安全需求，使用 XSSer 工具实现对自动化渗透测试的验证。 3.2.2 能根据 Web 安全需求，使用 Darkmysqli 工具实现对 SQL 注入测试的验证。 3.2.3 能根据 Web 安全需求，使用 Fimap 工具实现对文件包含渗透测试的验证。 3.2.4 能根据 Web 安全需求,使用 Ferret 工具实现对 Cookie 劫持测试的验证。 3.2.5 能根据 Web 安全需求,使用 W3af 工具实现对 Web 应用安全漏洞渗透测试的验证。
	3.3 木马生成测试	3.3.1 能根据木马防护需求，使用 Weevely 工具实现对木马上传测试的验证。 3.3.2 能根据木马防护需求,使用 Beef 工具实现对客户端浏览器劫持测试的验证。 3.3.3 能根据木马防护需求,使用 Netcat 工具实现对反弹连接测试的验证。 3.3.4 能根据木马防护需求，使用 Msfvenom 工具生成木马实现对渗透测试的验证。
	3.4 内网渗透测试	3.4.1 能根据内网安全需求，使用 ARPspoof 工具实现对中间人渗透测试的验证。 3.4.2 能根据内网安全需求，使用 Ptunnel 工

		具实现对内网穿透测试的验证。 3.4.3 能根据内网安全需求，使用 Stunnel 工具实现对内网穿透测试的验证。 3.4.4 能根据内网安全需求,使用 3proxy 工具实现对内网穿透测试的验证。
4.Python 安全应用	4.1 网络渗透测试	4.1.1 能根据网络安全需求,使用 Python 实现对 SMURF 网络渗透测试的验证。 4.1.2 能根据网络安全需求,使用 Python 实现对 UDP FLOOD 网络渗透测试的验证。 4.1.3 能根据网络安全需求,使用 Python 实现对 LAND 网络渗透测试的验证。 4.1.4 能根据网络安全需求,使用 Python 实现对网络服务判断渗透测试的验证。
	4.2 应用渗透测试	4.2.1 能根据应用安全需求,使用 Python 实现对数据库密码暴力破解渗透测试的验证。 4.2.2 能根据应用安全需求,使用 Python 实现对 SSH 密码暴力破解渗透测试的验证。 4.2.3 能根据应用安全需求,使用 Python 实现对 FTP 密码暴力破解渗透测试的验证。 4.2.4 能根据应用安全需求,使用 Python 实现对暴力破解 ZIP 文件口令渗透测试的验证。 4.2.5 能根据应用安全需求,使用 Python 实现对套接字编程及其应用渗透测试的验证。 4.2.6 能根据应用安全需求,使用 Python 实现对模糊测试、漏洞渗透测试的验证。
	4.3 安全渗透测试	4.3.1 能根据安全渗透测试需求，使用 Python 实现对 AES 加密算法的验证。 4.3.2 能根据安全渗透测试需求，使用 Python 实现对 DES 加密算法的验证。 4.3.3 能根据安全渗透测试需求，使用 Python 实现对非对称加密的验证。 4.3.4 能根据安全渗透测试需求，使用 Python 实现对模糊测试的验证。
5.数据库安全配置与管理	5.1 数据库安全配置	5.1.1 能根据数据库安全需求，通过修改 Access 数据库名实现数据库安全配置。 5.1.2 能根据数据库安全需求,通过修改 MySQL 管理员账号实现数据库安全配置。 5.1.3 能根据数据库安全需求，通过加固 TCP/IP 协议栈实现数据库安全配置。 5.1.4 能根据数据库安全需求，通过对 MySQL 用户权限设置及登录的限制实现数据库安全配置。
	5.2 数据库安全管	5.2.1 能根据数据库安全需求，通过禁止或限

	理	制远程连接数据库实现数据库安全管理。 5.2.2 能根据数据库安全需求，通过限制超级管理员登录实现数据库安全管理。 5.2.3 能根据数据库安全需求，通过删除不必要的存储过程实现数据库安全管理。 5.2.4 能根据数据库安全需求，通过设置日志记录功能实现数据库安全管理。
	5.3 数据库安全运维	5.3.1 能根据数据库安全需求，通过手工注入 Access 数据库实现数据库安全运维。 5.3.2 能根据数据库安全需求，通过修改 IIS 配置实现 Access 数据库的安全防护与运维。 5.3.3 能根据数据库安全需求，通过手工注入 SQL Server 数据库实现数据库安全运维。 5.3.4 能根据数据库安全需求，通过使用 Sa 权限创建超级管理员实现数据库安全运维。 5.3.5 能根据数据库安全需求，通过手工注入 MySQL 数据库实现数据库安全运维。 5.3.6 能根据数据库安全需求，通过使用 Sqlmap 注入 MySQL 数据库实现数据库安全运维。

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 安全应用	1.1.1 能根据 PHP 安全应用需求，使用 PHP 实现 SQL 注入漏洞的安全开发及渗透测试。 1.1.2 能根据 PHP 安全应用需求，使用 PHP 实现客户端脚本注入漏洞的安全开发及渗透测试。 1.1.3 能根据 PHP 安全应用需求，使用 PHP 实现反射型 XSS 漏洞的安全开发及渗透测试。 1.1.4 能根据 PHP 安全应用需求，使用 PHP 实现存储型 XSS 漏洞的安全开发及渗透测试。
	1.2PHP 代码审计	1.2.1 掌握 PHP 代码审计的方法和步骤，能对 PHP 框架与结构进行审计。 1.2.1 掌握 PHP 代码审计的方法和步骤，能对 PHP 代码进行审计。 1.2.3 掌握常见的 PHP 危险函数、特殊函数及常见的 INI 配置。 1.2.4 能根据 PHP 代码审计需求，使用 PHP 完成 XDebug 的配置和使用。 1.2.5 能根据 PHP 代码审计需求，使用 PHP 完

		成命令注入的验证。 1.2.6 能根据 PHP 代码审计需求，使用 PHP 完成安装问题的审计。
	1.3PHP 代码诊断	1.3.1 能根据 PHP 代码诊断需求，使用 PHP 实现 SQL 数字型注入的验证。 1.3.2 能根据 PHP 代码诊断需求，使用 PHP 实现 XSS 后台敏感操作的验证。 1.3.3 能根据 PHP 代码诊断需求，使用 PHP 实现对文件包含漏洞审计的验证。 1.3.4 能根据 PHP 代码诊断需求，使用 PHP 实现对任意文件读取的验证。 1.3.5 能根据 PHP 代码诊断需求，使用 PHP 实现对越权操作、二次注入的验证。 1.3.6 能根据 PHP 代码诊断需求，使用 PHP 实现登录密码爆破的验证。
2.Web 应用安全与防护	2.1Web 应用程序漏洞扫描	2.1.1 能根据 Web 安全需求,使用 Vega 漏扫工具进行 Web 漏洞扫描。 2.1.2 能根据 Web 安全需求，使用啊 D 漏扫工具进行 Web 漏洞扫描。 2.1.3 能根据 Web 安全需求,使用 JSKY 漏扫工具进行 Web 漏洞扫描。 2.1.4 能根据 Web 安全需求,使用 AWVS 漏扫工具进行 Web 漏洞扫描。
	2.2Web 应用程序漏洞验证	2.2.1 能根据 Web 安全需求，对 X-Forwarded-For 注入漏洞、支付漏洞进行分析，并完成漏洞验证。 2.2.2 能根据 Web 安全需求，对垂直越权访问漏洞、URL 跳转漏洞进行分析，并完成漏洞验证。 2.2.3 能根据 Web 安全需求，对 GET 任意文件下载、POST 任意文件下载漏洞进行分析，并完成漏洞验证。 2.2.4 能根据 Web 安全需求,对 JS 上传验证漏洞、文件上传 Content-Type 验证漏洞进行分析，并完成漏洞验证。 2.2.5 能根据 Web 安全需求,对 Host 注入漏洞、Boolean 盲注漏洞、GET 文件包含漏洞进行分析，并完成漏洞验证。 2.2.6 能根据 Web 安全需求，对任意文件包含漏洞进行分析，并完成漏洞验证。
	2.3 开源 CMS 实战渗透测试	2.3.1 能根据 Web 安全需求，对海洋 search.php 注入漏洞、BEESCMS 注入漏洞进行分析，并完成漏洞验证。

		2.3.2 能根据 Web 安全需求，对 DedeCMS flink.php 友情链接注入漏洞进行分析,并完成漏洞验证。 2.3.3 能根据 Web 安全需求,对 Dcore(轻型 CMS 系统)SQL 注入漏洞、ShopXp 系统 SQL 注入漏洞进行分析，并完成漏洞验证。 2.3.4 能根据 Web 安全需求，对 MetInfo 任意用户密码修改漏洞进行分析，并完成漏洞验证。 2.3.5 能根据 Web 安全需求，对 PHP 截断上传漏洞进行分析，并完成漏洞验证。
3.协议分析	3.1 数据链路层与网络层协议分析	3.1.1 能根据数据链路层协议安全需求，完成 Ethernet 协议、VRRP 协议的分析。 3.1.2 能根据数据链路层协议安全需求，完成生成树协议、VLAN 协议的分析。 3.1.3 能根据网络协议安全需求，完成 IP 协议、ICMP 协议的分析。 3.1.4 能根据网络协议安全需求，完成 ARP 协议、RIP 协议的分析。
	3.2 传输层协议分析	3.2.1 能根据网络协议安全需求，完成 TCP 协议的分析。 3.2.2 能根据网络协议安全需求，完成 UDP 协议的分析。 3.2.3 能根据网络协议安全需求，完成 TLS 协议的分析。 3.2.4 能根据网络协议安全需求，完成 SCTP 协议的分析。
	3.3 应用层协议分析	3.3.1 能根据应用层协议安全需求，使用 Apache 配置 HTTP 协议，并对协议进行分析。 3.3.2 能根据应用层协议安全需求，使用 IIS 对 FTP、HTTPS 协议进行分析. 3.3.3 能根据应用层协议安全需求，使用 OpenSSH 对 SSH 协议进行分析。 3.3.4 能根据应用层协议安全需求，使用 Xinetd 对 Telnet 协议进行分析。 3.3.5 能根据应用层协议安全需求，通过搭建 Windows 网络服务对 DNS 协议、DHCP 协议、SNMP 协议进行分析。
4.综合渗透测试	4.1Windows 系统安全综合渗透测试	4.1.1 能根据系统安全防护需求，验证使用 Eternalblue-Doublepulsar 可以获取主机权限，并对系统进行安全加固。 4.1.2 能根据系统安全防护需求，验证使用 Java 无效的数组索引漏洞可以进行鱼叉式渗

		透，并对系统进行安全加固。 4.1.3 能根据系统安全防护需求，验证使用 Kerberos 服务漏洞可以对域控服务器进行渗透，并对系统进行安全加固。 4.1.4 能根据系统安全防护需求，验证使用 Esteemaudit RDP 漏洞可以进行主机渗透提权，并对系统进行安全加固。 4.1.5 能根据系统安全防护需求,验证使用 SMB 服务漏洞结合 NTLM 中继、Exchange SSRF 漏洞结合 NTLM 中继可以进行主机渗透，并对系统进行安全加固。 4.1.6 能根据系统安全防护需求，验证使用 Evil Maid 物理访问安全漏洞可以进行主机渗透，并对系统进行安全加固。
	4.2Linux 系统安全综合渗透测试	4.2.1 能根据系统安全防护需求，验证使用反弹木马进行提权可以获取主机 Shell,并对系统进行安全加固。 4.2.2 能根据系统安全防护需求,验证使用 RSA 对称密钥可以对 HTTPS 数据包进行解码，并对系统进行安全加固。 4.2.3 能根据系统安全防护需求,验证使用 SSH 私钥泄露提权可以获取主机权限，并对系统进行安全加固。 4.2.4 能根据系统安全防护需求，验证使用 crontab 任务计划提权可以获取主机权限,并对系统进行安全加固。
	4.3Web 安全综合渗透测试	4.3.1 能根据 Web 安全防护需求，验证使用 Cookie 注入、过滤绕过注入、函数绕过注入、报错注入、WAF 绕过注入等方式可以进行 Web 渗透，并对 Web 进行安全加固。 4.3.2 能根据 Web 安全防护需求，验证使用文件上传黑名单绕过、白名单绕过、内容检查绕过、竞争条件绕过等方式可以进行 Web 渗透，并对 Web 进行安全加固。 4.3.3 能根据 Web 安全防护需求，验证使用 phpMyAdmin 任意文件包含漏洞可以进行 Web 渗透，并对 Web 进行安全加固。 4.3.4 能根据 Web 安全防护需求，验证使用 Kerberos 渗透测试域控服务器可以获取 Web 权限，并对 Web 进行安全加固。 4.3.5 能根据 Web 安全防护需求,验证使用 RSA 对称密钥可以对 HTTPS 数据包进行解码，并对 Web 进行安全加固。

		4.3.6 能根据 Web 安全防护需求，验证使用 Evil Maid 物理访问安全漏洞可以进行 Web 渗透，并对 Web 进行安全加固。

参考文献

[1] 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）

[2] 《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）

[3] 《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）

[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] 普通高等学校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] 网络与信息安全管理员国家职业技能标准（2020年版）

[10] 信息安全测试员国家职业技能标准（2021年版）

[11] 2021年全国职业院校技能大赛 ZZ-2021029 网络安全赛项规程

[12] 2021年全国职业院校技能大赛 GZ-2021038 信息安全管理与评估赛项规程

[13] SJ/T 11623-2016 信息技术服务从业人员能力规范

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

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

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

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

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

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

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

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