网络安全运维

职业技能等级标准

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：中科软科技股份有限公司。

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、彭金华、杨毅、何琳、胡志齐、徐雪鹏、孙雨春、邹君雨、张天乐等。

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 36626-2018 信息安全技术 信息系统安全运维管理

GB 17859-1999 计算机信息系统安全保护等级划分准则

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

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/T 20269-2006 信息安全技术信息系统安全管理要求

3 术语和定义

国家、行业标准界定的以及下列术语和定义适用于本标准。

3.1 网络安全基础运维类岗位

中小型企、事业单位桌面及服务器操作系统安全运维岗位。

3.2 网络安全服务类岗位

企、事业单位、安全厂商等从事安全服务的岗位。

3.3 网络安全生产、研发型岗位

企、事业单位、安全厂商从产品研发、测试、生产，安全项目集成的相关岗位。

4 对应院校专业

中等职业学校：计算机应用、网络技术、网站建设与管理、网络信息安全等专业。

高等职业学校：计算机应用技术、计算机网络技术、计算机系统与维护、信息安全技术、信息安全与管理等专业。

应用型本科学校：计算机科学与技术专、网络工程、信息安全技术、网络空间安全等专业。

5 面向工作岗位（群）

【网络安全运维】(初级)：主要面向 IT 互联网企业、企事业单位、政府部门等用人单位的基础运维类岗位，从事网络安全策略部署、操作系统安全管理与维护、系统安全测试、网络安全测试等工作。

【网络安全运维】(中级)：主要面向 IT 互联网企业、企事业单位、政府部门等用人单位的安全服务类岗位，从事网络安全渗透测试、系统安全加固、WEB 安全防护、网络安全项目集成等工作。

【网络安全运维】(高级)：主要面向 IT 互联网企业、企事业单位、政府部门等用人单位的研发、生产类岗位，从事网络安全渗透测试、风险评估、企业 WEB 安全防护，网络安全方案咨询、风险评估及网络安全产品售前、售后等工作。

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。

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.安全基本理论	1.1 CIA 安全模型配置	1.1.1 能根据 CIA 安全模型配置工作任务书要求，独立完成使用 PGP 描述网络安全 CIA 模型之私密性、完整性方案。 1.1.2 能根据 CIA 安全模型配置工作任务书要求，独立完成配置 Linux 描述网络安全 CIA 模型之可用性案例。
2.Windows 操作系统安全配置	2.1 Windows 系统加固	2.1.1 能根据 Windows 系统加固工作任务书要求，独立完成配置系统管理员账户安全，进行 Windows 系统加固。 2.1.2 能根据 Windows 系统加固工作任务书要求，独立完成配置磁盘访问权限，进行 Windows 系统加固。 2.1.3 能根据 Windows 系统加固工作任务书要求，独立完成配置系统账户数据库安全，进行 Windows 系统加固。 2.1.4 能根据 Windows 系统加固工作任务书要求，独立完成配置操作系统服务安全，进行 Windows 系统加固。 2.1.5 能根据 Windows 系统加固工作任务书要求，独立完成配置端口安全，进行 Windows 系统加固。 2.1.6 能根据 Windows 系统加固工作任务书要求，独立完成配置 Windows 系统漏洞安全，进行 Windows 系统加固。
	2.2 活动目录安全	2.2.1 能根据系统安全工作任务书要求，按照 Windows 操作系统活动目录安全要求，独立完成配置目录数据库访问权限。 2.2.2 能根据系统安全工作任务书要求，按照 Windows 操作系统活动目录安全要求，独立完成配置活动目录数据库。 2.2.3 能根据系统安全工作任务书要求，按照 Windows 操作系统活动目录安全要求，独立完成重定向活动目录数据库。
	2.3 组策略安全配置	2.3.1 能根据系统安全工作任务书，按照 Windows 操作系统组策略安全要求，独立完成配置账户策略。 2.3.2 能根据系统安全工作任务书，按照 Windows 操作系统组策略安全要求，独立完成配置审核策略。

		2.3.3 能根据系统安全工作任务书，按照 Windows 操作系统组策略安全要求,独立完成配置用户权限分配。 2.3.4 能根据系统安全工作任务书，按照 Windows 操作系统组策略安全要求,独立完成配置设备限制安全策略。 2.3.5 能根据系统安全工作任务书，按照 Windows 操作系统组策略安全要求,独立完成配置软件限制策略。
	2.4 用户账户安全管理	2.4.1 能根据系统安全工作任务书，按照 Windows 操作系统用户账户安全要求,独立完成配置用户账户的管理。 2.4.2 能根据系统安全工作任务书，按照 Windows 操作系统用户账户安全要求,独立完成配置用户组的管理。 2.4.3 能根据系统安全工作任务书，按照 Windows 操作系统用户账户安全要求,独立完成配置用户权限的安全。 2.4.4 能根据系统安全工作任务书，按照 Windows 操作系统用户账户安全要求,独立完成配置用户环境安全。 2.4.5 能根据系统安全工作任务书，按照 Windows 操作系统用户账户安全要求,独立完成配置域用户配置文件安全。
	2.5 文件系统安全管理	2.5.1 能根据系统安全工作任务书，按照 Windows 操作系统文件系统安全要求,独立完成配置基于 NTFS 文件系统的安全。 2.5.2 能根据系统安全工作任务书，按照 Windows 操作系统文件系统安全要求,独立完成配置权限管理服务。 2.5.3 能根据系统安全工作任务书，按照 Windows 操作系统文件系统安全要求,独立完成配置域用户配置文件安全。
	2.6 网络安全服务管理	2.6.1 能根据系统安全工作任务书，按照 Windows 操作系统网络安全服务配置要求,独立完成配置 IIS 安全机制。 2.6.2 能根据系统安全工作任务书，按照 Windows 操作系统网络安全服务配置要求,独立完成配置 www 安全。 2.6.3 能根据系统安全工作任务书，按照 Windows 操作系统网络安全服务配置要求,独立完成配置 ftp 服务安全。 2.6.4 能根据系统安全工作任务书，按照 Windows 操作系统网络安全服务配置要求,独

		立完成配置终端服务安全。 2.6.5 能根据系统安全工作任务书，按照 Windows 操作系统网络安全服务配置要求，独立完成配置文件服务安全。
	2.7 windows 防火墙配置	2.7.1 能根据系统安全工作任务书，按照 Windows 操作系统防火墙配置要求，独立完成配置 windows 防火墙。 2.7.2 能根据系统安全工作任务书，按照 Windows 操作系统防火墙配置要求，独立完成配置 windows 防火墙事件审核。 2.7.3 能根据系统安全工作任务书，按照 Windows 操作系统防火墙配置要求，独立完成配置 windows 防火墙的维护。
	2.8 事件和日志管理	2.8.1 能根据系统安全工作任务书，按照 Windows 操作系统事件和日志配置要求，独立完成配置事件查看器。 2.8.2 能根据系统安全工作任务书，按照 Windows 操作系统事件和日志配置要求，独立完成配置安全性日志。 2.8.3 能根据系统安全工作任务书，按照 Windows 操作系统事件和日志配置要求，独立完成配置可靠性和性能。
	2.9 数据备份与恢复	2.9.1 能根据系统安全工作任务书，按照 Windows 操作系统数据备份与恢复操作要求，独立完成配置备份活动目录数据库。 2.9.2 能根据系统安全工作任务书，按照 Windows 操作系统数据备份与恢复操作要求，独立完成配置备份服务状态信息。 2.9.3 能根据系统安全工作任务书，按照 Windows 操作系统数据备份与恢复操作要求，独立完成配置 DHCP 服务器备份。 2.9.4 能根据系统安全工作任务书，按照 Windows 操作系统数据备份与恢复操作要求，独立完成配置磁盘配额备份。 2.9.5 能根据系统安全工作任务书，按照 Windows 操作系统数据备份与恢复操作要求，独立完成配置 DNS 服务器备份。 2.9.6 能根据系统安全工作任务书，按照 Windows 操作系统数据备份与恢复操作要求，独立完成配置网络配置备份。
3.Linux 操作系统安全配置	3.1 用户和组的管理	3.1.1 能根据系统安全工作任务书，按照 Linux 操作系统用户和组的管理配置要求，独立完成配置密码及账户安全。 3.1.2 能根据系统安全工作任务书，按照

		Linux 操作系统用户和组的管理配置要求,独立完成配置 PAM 认证模块。 3.1.3 能根据系统安全工作任务书，按照 Linux 操作系统用户和组的管理配置要求,独立完成配置用户权限。
	3.2 Samba 服务的安全管理	3.2.1 能根据系统安全工作任务书，按照 Linux 操作系统 Samba 服务的安全管理配置要求，独立完成设置用户账号映射。 3.2.2 能根据系统安全工作任务书，按照 Linux 操作系统 Samba 服务的安全管理配置要求，独立完成设置主机访问控制。 3.2.3 能根据系统安全工作任务书，按照 Linux 操作系统 Samba 服务的安全管理配置要求，独立完成配置用 PAM 实现用户和主机访问控制。 3.2.4 能根据系统安全工作任务书，按照 Linux 操作系统 Samba 服务的安全管理配置要求，独立完成配置用户建立独立的配置文件。
	3.3 vsftpd 服务的安全服务配置	3.3.1 能根据系统安全工作任务书，按照 Linux 操作系统 vsftpd 服务的安全配置要求，独立完成虚拟用户配置。 3.3.2 能根据系统安全工作任务书，按照 Linux 操作系统 vsftpd 服务的安全配置要求，独立完成配置主机访问控制。 3.3.3 能根据系统安全工作任务书，按照 Linux 操作系统 vsftpd 服务的安全配置要求，独立完成配置用户访问控制。 3.3.4 能根据系统安全工作任务书，按照 Linux 操作系统 vsftpd 服务的安全配置要求，独立完成配置 FTP 服务器的资源限制。
	3.4 DNS 的安全配置	3.4.1 能根据系统安全工作任务书，按照 Linux 操作系统 DNS 的安全配置要求,独立完成配置 DNS 的查询方式。 3.4.2 能根据系统安全工作任务书，按照 Linux 操作系统 DNS 的安全配置要求,独立完成配置限制区域传输。 3.4.3 能根据系统安全工作任务书，按照 Linux 操作系统 DNS 的安全配置要求,独立完成配置限制查询者。 3.4.4 能根据系统安全工作任务书，按照 Linux 操作系统 DNS 的安全配置要求,独立完成配置分离 DNS。 3.4.5 能根据系统安全工作任务书，按照

		Linux 操作系统 DNS 的安全配置要求,独立完成配置域名转发。 3.4.6 能根据系统安全工作任务书，按照 Linux 操作系统 DNS 的安全配置要求,独立完成配置特定的用户运行 Apache 服务器。 3.4.7 能根据系统安全工作任务书，按照 Linux 操作系统 DNS 的安全配置要求,独立完成配置主机访问控制。 3.4.8 能根据系统安全工作任务书，按照 Linux 操作系统 DNS 的安全配置要求,独立完成配置 HTTP 用户认证。 3.4.9 能根据系统安全工作任务书，按照 Linux 操作系统 DNS 的安全配置要求,独立完成配置虚拟目录和目录权限。 3.4.10 能根据系统安全工作任务书，按照 Linux 操作系统 DNS 的安全配置要求,独立完成配置 Iptables 防火墙策略。
	3.5 Apache 的安全策略配置	3.5.1 能根据系统安全工作任务书，按照 Linux 操作系统 Apache 的安全策略配置要求,独立完成配置特定的用户 Apache 服务器。 3.5.2 能根据系统安全工作任务书，按照 Linux 操作系统 Apache 的安全策略配置要求，独立完成配置主机访问控制。 3.5.3 能根据系统安全工作任务书，按照 Linux 操作系统 Apache 的安全策略配置要求，独立完成配置 HTTP 用户认证。 3.5.4 能根据系统安全工作任务书，按照 Linux 操作系统 Apache 的安全策略配置要求，独立完成配置虚拟目录和目录权限。
	3.6 防火墙安全策略配置	3.6.1 能根据系统安全工作任务书，按照 Linux 操作系统防火墙安全配置策略要求,独立完成配置 Iptables 防火墙策略。
4.网络设备安全管理	4.1 网络设备安全管理	4.1.1 能根据网络设备安全管理工作任务书，按照网络设备安全配置要求，独立完成利用 BackTrack5 渗透测试工具实现 Ethernet 协议渗透测试。 4.1.2 能根据网络设备安全管理工作任务书，按照网络设备安全配置要求，独立完成利用 Scapy 实现 IEEE802.1Q 渗透测试。 4.1.3 能根据网络设备安全管理工作任务书，按照网络设备安全配置要求，独立完成利用 BackTrack5 渗透测试工具进行 ARP 协议渗透测试。

		4.1.4 能根据网络设备安全管理工作任务书，按照网络设备安全配置要求，独立完成利用 Scapy 进行 DNS 协议渗透测试。 4.1.5 能根据网络设备安全管理工作任务书，按照网络设备安全配置要求，独立完成利用 BackTrack5 渗透测试工具进行 DHCP 协议渗透测试。
5.网络协议分析	5.1 网络协议分析	5.1.1 能根据网络协议分析工作任务书，按照网络协议配置要求，独立完成 Ethernet 协议分析及配置。 5.1.2 能根据网络协议分析工作任务书，按照网络协议配置要求，独立完成 ARP 协议分析及配置。 5.1.3 能根据网络协议分析工作任务书，按照网络协议配置要求，独立完成 IP 协议分析及配置。 5.1.4 能根据网络协议分析工作任务书，按照网络协议配置要求，独立完成 ICMP 协议分析及配置。 5.1.5 能根据网络协议分析工作任务书，按照网络协议配置要求，独立完成 TCP 协议分析及配置。 5.1.6 能根据网络协议分析工作任务书，按照网络协议配置要求，独立完成 UDP 协议分析及配置。 5.1.7 能根据网络协议分析工作任务书，按照网络协议配置要求，独立完成 RIP 协议分析及配置。 5.1.8 能根据网络协议分析工作任务书，按照网络协议配置要求，独立完成 VRRP 协议分析及配置。 5.1.9 能根据网络协议分析工作任务书，按照网络协议配置要求，独立完成生成树协议分析及配置。 5.1.10 能根据网络协议分析工作任务书，按照网络协议配置要求，独立完成 VLAN 协议分析及配置。
6.应用层协议分析	6.1 应用层协议分析	6.1.1 能根据应用层协议分析工作任务书，按照应用层协议配置要求，独立完成 Apache HTTP 协议分析及配置。 6.1.2 能根据应用层协议分析工作任务书，按照应用层协议配置要求,独立完成使用 IIS 进行 FTP 协议分析及配置。 6.1.3 能根据应用层协议分析工作任务书，

		按照应用层协议配置要求，独立完成使用 OpenSSH 进行 SSH 协议分析。 6.1.4 能根据应用层协议分析工作任务书，按照应用层协议配置要求，独立完成使用 Xinetd 进行 Telnet 协议分析。 6.1.5 能根据应用层协议分析工作任务书，按照应用层协议配置要求,独立完成使用 IIS 进行 HTTPS 协议分析。 6.1.6 能根据应用层协议分析工作任务书，按照应用层协议配置要求，独立完成通过 Windows2003 网络服务搭建 DNS 协议分析。 6.1.7 能根据应用层协议分析工作任务书，按照应用层协议配置要求，独立完成通过 Windows2003 网络服务搭建 DHCP 协议分析。 6.1.8 能根据应用层协议分析工作任务书，按照应用层协议配置要求，独立完成通过 Windows2003 网络服务搭建 SNMP 协议分析。
7.VPN 安全管理	7.1 VPN 安全管理	7.1.1 能根据 VPN 安全管理工作任务书，按照 VPN 安全配置要求，独立完成通过 Windows2003 网络服务搭建 IPSec 协议分析。 7.1.2 能根据 VPN 安全管理工作任务书，按照 VPN 安全配置要求，独立完成通过 WireShark 进行 IKE 协议分析。
8.渗透测试常用 工具使用	8.1 渗透测试常用 工具使用	8.1.1 能根据渗透测试工具工作任务书要求，独立完成使用 arping、fping、genlist、nbtscan、onesixtyone 等渗透测试工具进行目标机器识别。 8.1.2 能根据渗透测试工具工作任务书要求，独立完成使用 p0f、autoscan、nmap 等渗透测试工具进行操作机器识别。 8.1.3 能根据渗透测试工具工作任务书要求，独立完成使用 xprobe2 进行操作系统识别。 8.1.4 能根据渗透测试工具工作任务书要求，独立完成使用 zenmap 进行端口扫描。 8.1.5 能根据渗透测试工具工作任务书要求，独立完成使用 amap、httprint 进行服务枚举。 8.1.6 能根据渗透测试工具工作任务书要求,能独立完成使用 admsnmp 进行 snmp 分析。 8.1.7 能根据渗透测试工具工作任务书要求,独立完成使用 Metasploit 进行漏洞利用。 8.1.8 能根据渗透测试工具工作任务书要

		求，独立完成使用 dsniff、wireshark 进行网络嗅探。 8.1.9 能根据渗透测试工具工作任务书要求，独立完成使用 tcpdump 进行数据包抓取。 8.1.10 能根据渗透测试常用工具任务书要求,能独立完成使用 arpspoof 进行 arp 欺骗。 8.1.11 能根据渗透测试工具工作任务书要求,独立完成使用 ettercap 进行局域网攻击。 8.1.12 能根据渗透测试工具工作任务书要求，独立完成使用 ptunnel、stunnel、3proxy 进行内网穿透。
9.实训演练	9.1 实训演练	9.1.1 能根据网络安全攻防工作任务书要求，独立完成二层网络 Sniffer 监听安全攻防。 9.1.2 能根据网络安全攻防工作任务书要求，独立完成数据库安全加固。 9.1.3 能根据网络安全攻防工作任务书要求，独立完成 Web 应用程序 SQL Inject 安全攻防。 9.1.4 能根据网络安全攻防工作任务书要求，独立完成 Web 应用程序文件包含安全攻防。 9.1.5 能根据网络安全攻防工作任务书要求，独立完成 ARP 扫描渗透测试。 9.1.6 能根据网络安全攻防工作任务书要求，独立完成操作系统及应用程序扫描渗透测试。 9.1.7 能根据网络安全攻防工作任务书要求，独立完成 ARP 协议渗透测试。 9.1.8 能根据网络安全攻防工作任务书要求，独立完成暴力破解密码字典生成渗透测试。 9.1.9 能根据网络安全攻防工作任务书要求，独立完成 Linux 操作系统安全加固。 9.1.10 能根据网络安全攻防工作任务书要求，独立完成服务端口扫描渗透测试。

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.渗透测试常用工具使用	1.1 渗透测试常用工具使用	1.1.1 能根据渗透测试工具工作任务书要求，独立完成使用Weevely工具上传一句话木马。 1.1.2 能根据渗透测试工具工作任务书要求，独立完成使用Nessus扫描操作系统漏洞。

		1.1.3 能根据渗透测试工具工作任务书要求，独立完成使用metPsploit进行HPsh传递获取靶机权限。 1.1.4 能根据渗透测试工具工作任务书要求，独立完成使用MSF实现Web传递获取靶机权限。 1.1.5 能根据渗透测试工具工作任务书要求，独立完成使用XSSer进行自动化渗透测试。 1.1.6 能根据渗透测试工具工作任务书要求，独立完成使用fimPp进行文件包含渗透测试漏洞审计。 1.1.7 能根据渗透测试工具工作任务书要求，独立完成使用dPrkmysqli进行sql注入。 1.1.8 能根据渗透测试工具工作任务书要求，独立完成使用VegP对Web进行漏洞扫描。 1.1.9 能根据渗透测试工具工作任务书要求，独立完成使用啊D进行网页漏洞扫描。 1.1.10 能根据渗透测试工具工作任务书要求，独立完成使用HydrP进行密码破解。 1.1.11 能根据渗透测试工具工作任务书要求，独立完成使用SSHMitm中间人拦截SSH。 1.1.12 能根据渗透测试工具工作任务书要求，独立完成使用JSKY进行网页漏洞扫描。 1.1.13 能根据渗透测试工具工作任务书要求，独立完成使用NetcPt进行反弹链接实验。 1.1.14 能根据渗透测试工具工作任务书要求，独立完成使用PWVS进行网站漏洞扫描。 1.1.15 能根据渗透测试工具工作任务书要求,独立完成使用EternPl Blues进行Windows漏洞利用。 1.1.16 能根据渗透测试工具工作任务书要求，独立完成使用SPminside+OphcrPck破解本地用户密码。 1.1.17 能根据渗透测试工具工作任务书要求，独立完成使用Beef对客户端浏览器进行劫持。 1.1.18 能根据渗透测试工具工作任务书要求，独立完成使用Prpspoof进行中间人渗透测试。 1.1.19 能根据渗透测试工具工作任务书要求，独立完成使用cobPltstrike接口来传递MSF中的shell。 1.1.20 能根据渗透测试工具工作任务书要

		求，独立完成使用w3Pf进行Web应用安全漏洞测试。 1.1.21 能根据渗透测试工具工作任务书要求，独立完成使用Kimi生成deb包进行代码捆绑实践。 1.1.22 能根据渗透测试工具工作任务书要求，独立完成使用ferret进行Cookie劫持。 1.1.23 能根据渗透测试工具工作任务书要求，独立完成使用PrmitPge的MSF进行自动化集成渗透测试1。 1.1.24 能根据渗透测试工具工作任务书要求，独立完成使用PrmitPge的MSF进行自动化集成渗透测试2。 1.1.25 能根据渗透测试工具工作任务书要求，独立完成使用msfvenom生成木马进行渗透测试。 1.1.26 能根据渗透测试工具工作任务书要求，独立完成使用meterpreter模块进行后渗透测试。
2.操作系统漏洞验证及加固	2.1 操作系统漏洞验证及加固	2.1.1 能根据操作系统加固工作任务书要求，独立完成对系统MS08_067漏洞利用并进行安全加固。 2.1.2 能根据操作系统加固工作任务书要求，独立完成对系统MS10_003漏洞利用并进行安全加固。 2.1.3 能根据操作系统加固工作任务书要求，独立完成对系统MS12_020漏洞利用并进行安全加固。 2.1.4 能根据操作系统加固工作任务书要求，独立完成对系统MS14_064漏洞利用并进行安全加固。 2.1.5 能根据操作系统加固工作任务书要求，独立完成对系统MS17_010漏洞利用并进行安全加固。
3.服务漏洞利用及加固	3.1 服务漏洞利用及加固	3.1.1 能根据系统服务加固工作任务书要求，独立完成利用CVE-2012-2122漏洞绕过Mysql身份认证。 3.1.2 能根据系统服务加固工作任务书要求，独立完成利用CVE-2015-0240漏洞实现Samba远程代码执行。 3.1.3 能根据系统服务加固工作任务书要求，独立完成利用CVE-2016-5195漏洞实现Linux系统本地提权。 3.1.4 能根据系统服务加固工作任务书要

		求，独立完成利用CVE-2017-7269漏洞渗透IIS6.0实现远程控制。 3.1.5 能根据系统服务加固工作任务书要求，独立完成利用CVE-2017-7494漏洞实现Samba远程代码执行。 3.1.6 能根据系统服务加固工作任务书要求，独立完成利用CVE-2017-8464漏洞实现LNK文件远程代码执行。 3.1.7 能根据系统服务加固工作任务书要求，独立完成利用CVE-2017-9791漏洞结合burp提权。 3.1.8 能根据系统服务加固工作任务书要求，独立完成利用CVE-2017-12617漏洞实现Tomcat远程代码执行。 3.1.9 能根据系统服务加固工作任务书要求，独立完成利用CVE-2017-15715绕过上传黑名单限制。 3.1.10 能根据系统服务加固工作任务书要求，独立完成利用CVE-2018-4878漏洞上传实现远程控制。 3.1.11 能根据系统服务加固工作任务书要求，独立完成利用CVE-2018-12613漏洞实现远程文件包含。 3.1.12 能根据系统服务加固工作任务书要求，独立完成利用Java序列化漏洞进行渗透测试。 3.1.13 能根据系统服务加固工作任务书要求，独立完成利用Redis未授权访问漏洞进行提权。 3.1.14 能根据系统服务加固工作任务书要求，独立完成利用Redis弱口令实现远程h连接。 3.1.15 能根据系统服务加固工作任务书要求，独立完成利用structs2实现远程命令执行。
4.论坛漏洞分析及利用	4.1 论坛漏洞分析及利用	4.1.1 能根据论坛漏洞分析及利用工作任务书要求，独立完成针对Wordpre论坛进行信息收集与漏洞扫描。 4.1.2 能根据论坛漏洞分析及利用工作任务书要求，独立完成针对Wordpre论坛插件实现远程代码执行。 4.1.3 能根据论坛漏洞分析及利用工作任务书要求，独立完成针对bWapp进行web渗透测试。

		4.1.4 能根据论坛漏洞分析及利用工作任务书要求，独立完成针对Dicuz!X 论坛进行网页挂马。 4.1.5 能根据论坛漏洞分析及利用工作任务书要求，独立完成针对Dicuz!X论坛前台进行任意文件删除。
5.Web安全应用	5.1 Web安全应用	5.1.1 能根据Web安全应用工作任务书要求，独立完成对Web页面进行Command Injection命令注入。 5.1.2 能根据Web安全应用工作任务书要求，独立完成对Web页面进行Brute force初级暴力破解。 5.1.3 能根据Web安全应用工作任务书要求，独立完成对Web页面进行Brute force进阶暴力破解。 5.1.4 能根据Web安全应用工作任务书要求，独立完成对Web页面进行File Inclusion文件包含漏洞初级利用。 5.1.5 能根据Web安全应用工作任务书要求，独立完成对Web页面进行File Inclusion文件包含漏洞进阶利用。 5.1.6 能根据Web安全应用工作任务书要求，独立完成对Web页面进行File Upload文件上传漏洞初级利用。 5.1.7 能根据Web安全应用工作任务书要求，独立完成对Web页面进行File Upload文件上传漏洞进阶利用。 5.1.8 能根据Web安全应用工作任务书要求，独立完成对Web页面进行CSRF跨站初级请求伪造。 5.1.9 能根据Web安全应用工作任务书要求，独立完成对Web页面进行CSRF跨站进阶请求伪造。 5.1.10 能根据Web安全应用工作任务书要求，独立完成对Web页面进行初级SQL注入。 5.1.11 能根据Web安全应用工作任务书要求，独立完成对Web页面进行进阶SQL注入。 5.1.12 能根据Web安全应用工作任务书要求，独立完成对Web页面进行初级SQL盲注。 5.1.13 能根据Web安全应用工作任务书要求，独立完成对Web页面进行进阶SQL盲注。 5.1.14 能根据Web安全应用工作任务书要求，独立完成对Web页面进行初级XSS跨站脚本利用。

		5.1.15 能根据Web安全应用工作任务书要求，独立完成对Web页面进行进阶XSS跨站脚本利用。 5.1.16 能根据Web安全应用工作任务书要求，独立完成对Web页面进行DOM型XSS注入。 5.1.17 能根据Web安全应用工作任务书要求，独立完成对Web页面进行反射型XSS注入。 5.1.18 能根据Web安全应用工作任务书要求，独立完成对Web页面进行存储型XSS注入。
6.PHP应用安全	6.1 PHP应用安全	6.1.1 能根据PHP应用安全工作任务书要求，独立完成SQL注入漏洞开发及渗透测试。 6.1.2 能根据PHP应用安全工作任务书要求，独立完成针对SQL注入漏洞进行安全开发。 6.1.3 能根据PHP应用安全工作任务书要求，独立完成客户端脚本注入漏洞开发及渗透测试。 6.1.4 能根据PHP应用安全工作任务书要求，独立完成针对客户端脚本注入漏洞的安全开发。 6.1.5 能根据PHP应用安全工作任务书要求，独立完成反射型XSS漏洞开发及渗透测试。 6.1.6 能根据PHP应用安全工作任务书要求，独立完成针对反射型XSS漏洞的安全开发。 6.1.7 能根据PHP应用安全工作任务书要求，独立完成存储型XSS漏洞开发及渗透测试。 6.1.8 能根据PHP应用安全工作任务书要求，独立完成针对存储型XSS漏洞的安全开发。
7.Python安全渗透测试	7.1 Python安全渗透测试	7.1.1 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行IP FRAG网络渗透测试。 7.1.2 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行LAND网络渗透测试。 7.1.3 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行SMURF网络渗透测试。 7.1.4 能根据Python安全渗透测试工作任务书要求,独立完成运用Python语言进行TCP No FLAG网络渗透测试。 7.1.5 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行TCP SYN FLOOD网络渗透测试。 7.1.6 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行UDP

		FLOOD网络渗透测试。 7.1.7 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行TEARDROP渗透测试。 7.1.8 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行路由协议渗透测试。 7.1.9 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行数据库密码暴力破解渗透测试。 7.1.10 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行网络服务判断渗透测。 7.1.11 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行应用程序判断渗透测。 7.1.12 能根据Python安全渗透测试工作任务书要求，独立完成运用Python语言进行SSH密码暴力破解渗透测试。
8.数据库安全	8.1 数据库安全	8.1.1 能根据数据库安全工作任务书要求，结合数据库知识进行accesss数据库改名。 8.1.2 能根据数据库安全工作任务书要求，结合数据库知识进行mysql管理员账号修改。 8.1.3 能根据数据库安全工作任务书要求，结合数据库知识修改默认密码。 8.1.4 能根据数据库安全工作任务书要求，结合数据库知识删除或锁定无效账号。 8.1.5 能根据数据库安全工作任务书要求，结合数据库知识加固TCPIP协议栈。 8.1.6 能根据数据库安全工作任务书要求，结合数据库知识进行角色创建与权限赋。 8.1.7 能根据数据库安全工作任务书要求，结合数据库知识进行mysql用户权限设置及登陆限制。 8.1.8 能根据数据库安全工作任务书要求，结合数据库知识禁止或限制远程连接数据库。 8.1.9 能根据数据库安全工作任务书要求，结合数据库知识限制超级管理员登录。 8.1.10 能根据数据库安全工作任务书要求，结合数据库知识创建profile。 8.1.11 能根据数据库安全工作任务书要求，结合数据库知识删除不必要的存储过程。 8.1.12 能根据数据库安全工作任务书要求，

		结合数据库知识启用数据库归档模式。 8.1.13 能根据数据库安全工作任务书要求，结合数据库知识进行日志记录功能设置。 8.1.14 能根据数据库安全工作任务书要求，结合数据库知识进行手工注入access数据库。 8.1.15 能根据数据库安全工作任务书要求，结合数据库知识修改iis配置并对access数据库进行防护。 8.1.16 能根据数据库安全工作任务书要求，结合数据库知识进行手工注入mssql数据库。 8.1.17 能根据数据库安全工作任务书要求，结合数据库知识进行Sa权限超级管理员的创建。 8.1.18 能根据数据库安全工作任务书要求，结合数据库知识进行手工注入Oracle数据库。 8.1.19 能根据数据库安全工作任务书要求，结合数据库知识进行手工注入mysql数据库。 8.1.20 能根据数据库安全工作任务书要求，结合数据库知识使用sqlmap注入mysql数据库。
9.实训演练	9.1 实训演练	9.1.1 能根据网络安全攻防工作任务书要求，独立完成文件MD5校验。 9.1.2 能根据网络安全攻防工作任务书要求，独立完成数据库安全加固。 9.1.3 能根据网络安全攻防工作任务书要求，独立完成WEB渗透扫描与加固。 9.1.4 能根据网络安全攻防工作任务书要求，独立完成Nmap扫描渗透测试。 9.1.5 能根据网络安全攻防工作任务书要求，独立完成操作系统服务端口扫描渗透测试。 9.1.6 能根据网络安全攻防工作任务书要求，独立完成漏洞扫描与利用。 9.1.7 能根据网络安全攻防工作任务书要求，独立完成mssql数据库渗透测试。 9.1.8 能根据网络安全攻防工作任务书要求，独立完成主机发现与信息收集。 9.1.9 能根据网络安全攻防工作任务书要求，独立完成SNMP信息收集与利用。 9.1.10 能根据网络安全攻防工作任务书要求，独立完成Linux操作系统渗透测试。 9.1.11 能根据网络安全攻防工作任务书要

		求，独立完成Windows操作系统渗透测试。

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	1.1 PHP代码审计	1.1.1 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成PHP代码审计。 1.1.2 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成常见的INI配置。 1.1.3 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成常见危险函数及特殊函数配置。 1.1.4 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成XDebug的配置和使用。
	1.2 PHP应用安全	1.2.1 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成PHP命令注入。 1.2.2 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成安装问题的审计。 1.2.3 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成SQL数字型注入。 1.2.4 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成XSS后台敏感操作。 1.2.5 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成文件包含漏洞的审计。 1.2.6 能根据 PHP代码审计工作任务书要求，能按照PHP代码审计基础方法，能独立完成任意文件读取。 1.2.7 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成越权操作。 1.2.8 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成登录密码爆破。 1.2.9 能根据PHP代码审计工作任务书要求，按照PHP代码审计基础方法，独立完成二次注入。
2.Web应用程序漏	2.1 Web应用程序漏	2.1.1 能根据工作任务书要求，按照Web应用

洞	洞	程序漏洞加固方法，独立完成x-forwarded-for注入。 2.1.2 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成支付漏洞加固。 2.1.3 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成垂直越权。 2.1.4 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成url跳转操作。 2.1.5 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成GET任意文件下载。 2.1.6 能根据工作任务书要求，按照 Web应用程序漏洞加固方法，独立完成POST任意文件下载。 2.1.7 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成无验证上传。 2.1.8 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成校验扩展名上传。 2.1.9 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成验证来源去向的url跳转。 2.1.10 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成文件包含。 2.1.11 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成POST文件包含。 2.1.12 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成HOST注入。 2.1.13 能根据工作任务书要求，按照Web应用程序漏洞加固方法，独立完成延时注入。
3.开源cms实战渗透测试	3.1 开源cms实战渗透测试	3.1.1 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成DiscuzX 7.2论。 3.1.2 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成DiscuzX 3.2 存储型XSS配置。 3.1.3 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成phpmyadmin任意文件包含漏洞。 3.1.4 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成齐博系统SQL注入。 3.1.5 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成海盗云商

		getshell。 3.1.6 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成PHP168任意代码执行GET SHELL。 3.1.7 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成ecshop 注入。 3.1.8 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成ShopXp系统SQL注射漏洞。 3.1.9 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成Dcore(轻型CMS系统)注入漏洞。 3.1.10 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成MetInfo 任意文件包含漏洞可getshell。 3.1.11 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成Metinfo news.php盲注。 3.1.12 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成Metinfo img.php盲注。 3.1.13 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成万众电子期刊在线阅读系统PHP和ASP最新版本通杀SQL注入。 3.1.14 能根据工作任务书要求，按照开源cms实战渗透测试方法,独立完成BEESCMS sql注入，无视防御。 3.1.15 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成ourphp 注入。 3.1.16 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成 phpwind命令执行漏洞。 3.1.17 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成使用metinfo命令对任意用户密码进行修改。 3.1.18 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成aspcms命令注入。 3.1.19 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成DedeCMS flink.php友情链接注入。 3.1.20 能根据工作任务书要求，按照开源

		cms实战渗透测试方法，独立完成DedeCms?recommend.php注入。 3.1.21 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成BEESCMS小于等于V4四处注入以及无需密码直接进后台。 3.1.22 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成海洋x-forwarded-for注入。 3.1.23 能根据工作任务书要求，按照开源cms实战渗透测试方法，独立完成php截断利用。
4.综合渗透测试	4.1 综合渗透测试	4.1.1 能根据综合渗透测试工作任务书要求，独立完成使用Apache Solr远程代码执行漏洞。 4.1.2 能根据综合渗透测试工作任务书要求，独立完成libSSh的漏洞分析。 4.1.3 能根据综合渗透测试工作任务书要求，独立完成libSSh的维持访问。 4.1.4 能根据综合渗透测试工作任务书要求，独立完成Webmin远程代码执行。 4.1.5 能根据综合渗透测试工作任务书要求，独立完成Nexus远程代码执行。 4.1.6 能根据综合渗透测试工作任务书要求，独立完成使用DNS域传送漏洞。 4.1.7 能根据综合渗透测试工作任务书要求，独立完成通过Linux系统命令对后门端口进行查杀。 4.1.8 能根据综合渗透测试工作任务书要求，独立完成利用MS15-034远程代码执行漏洞进行渗透。 4.1.9 能根据综合渗透测试工作任务书要求，独立完成利用Ubuntu本地提权漏洞进行渗透及加固。 4.1.10 能根据综合渗透测试工作任务书要求，独立完成利用docker容器的不安全部署获取宿主机权限。 4.1.11 能根据综合渗透测试工作任务书要求，独立完成利用Java反序列化漏洞在受限环境中从漏洞发现到获取反向Shell。 4.1.12 能根据综合渗透测试工作任务书要求，独立完成利用Java无效的数组索引漏洞进行鱼叉式网络钓鱼渗透测试。 4.1.13 能根据综合渗透测试工作任务书要

		求，独立完成利用Kerberos渗透测试域控服务器并获取权限。 4.1.14 能根据综合渗透测试工作任务书要求，独立完成利用Powershell在设备上生成反向shell进行持续控制具。 4.1.15 能根据综合渗透测试工作任务书要求，独立完成利用RSA对称密钥对HTTPS数据包进行解码。 4.1.16 能根据综合渗透测试工作任务书要求，独立完成在未知场景下利用SSH私钥泄露进行提权获取主机FLAG。 4.1.17 能根据综合渗透测试工作任务书要求，独立完成在未知场景下利用反弹木马进行提权获取主机shell。 4.1.18 能根据综合渗透测试工作任务书要求，独立完成在未知场景下利用crontab任务计划提权获取主机shell。 4.1.19 能根据综合渗透测试工作任务书要求，独立完成在未知场景下利用通过EvilMaid进行渗透提权。 4.1.20 能根据综合渗透测试工作任务书要求，独立完成在未知场景下利用Esteemaudit进行渗透提权。 4.1.21 能根据综合渗透测试工作任务书要求，独立完成在未知场景下利用SMB服务漏洞进行渗透提权。 4.1.22 能根据综合渗透测试工作任务书要求，独立完成在未知场景下利用FTP服务漏洞进行渗透提权。 4.1.23 能根据综合渗透测试工作任务书要求，独立完成利用CVE-2019-0708 BlueKeep远程代码执行漏洞进行渗透提权。 4.1.24 能根据综合渗透测试工作任务书要求，独立完成利用Ollydbg分析CVE-2010-2883 解密pdf文档中的阴谋。
5.信息隐藏	5.1 信息隐藏	5.1.1 能根据信息隐藏工作任务书要求，独立完成使用隐写术来防止敏感数据被盗用。 5.1.2 能根据信息隐藏工作任务书要求，独立完成利用C语言实现LSB图像信息隐藏。 5.1.3 能根据信息隐藏工作任务书要求，独立完成利用Python脚本对CTF中的图像隐写进行处理。 5.1.4 能根据信息隐藏工作任务书要求，独立完成利用Python脚本来处理CTF中的音频

		隐写。 5.1.5 能根据信息隐藏工作任务书要求，独立完成利用十六进制分析工具对CTF中的图像隐写进行处理。
6.Python安全渗透测试	6.1 Python安全渗透测试	6.1.1 能根据Python安全渗透测试工作任务书要求，独立完成利用Python暴力破解FTP服务器账号。 6.1.2 能根据Python安全渗透测试工作任务书要求，独立完成利用Python暴力破解ZIP文件口令。 6.1.3 能根据Python安全渗透测试工作任务书要求，独立完成利用Python进行套接字编程及其应用。 6.1.4 能根据Python安全渗透测试工作任务书要求，独立完成利用Python进行资源探测。 6.1.5 能根据Python安全渗透测试工作任务书要求，独立完成利用Python实现AES加密算法。 6.1.6 能根据Python安全渗透测试工作任务书要求，独立完成利用Python实现DES加密算法。 6.1.7 能根据Python安全渗透测试工作任务书要求，独立完成利用Python实现非对称加密。 6.1.8 能根据Python安全渗透测试工作任务书要求，独立完成利用Python实现漏洞利用渗透测试。 6.1.9 能根据Python安全渗透测试工作任务书要求，独立完成利用Python实现模糊测试。 6.1.10 能根据Python安全渗透测试工作任务书要求，独立完成利用Python实现字典攻击渗透测试。
7.逆向分析	7.1 逆向分析	7.1.1 能根据逆向分析工作任务书要求，独立完成 Array 数据类型逆向分析。 7.1.2 能根据逆向分析工作任务书要求，独立完成 Bool 数据类型逆向分析。 7.1.3 能根据逆向分析工作任务书要求，独立完成Char数据类型逆向分析。 7.1.4 能根据逆向分析工作任务书要求，独立完成Float数据类型逆向分析。 7.1.5 能根据逆向分析工作任务书要求，独立完成Integer数据类型逆向分析。 7.1.6 能根据逆向分析工作任务书要求，独立完成NULL数据类型逆向分析。

		7.1.7 能根据逆向分析工作任务书要求，独立完成Point数据类型逆向分析。 7.1.8 能根据逆向分析工作任务书要求，独立完成String数据类型逆向分析。 7.1.9 能根据逆向分析工作任务书要求，独立完成Struct数据类型逆向分析。 7.1.10 能根据逆向分析工作任务书要求，独立完成函数参数逆向分析。 7.1.11 能根据逆向分析工作任务书要求，独立完成函数返回值逆向分析。 7.1.12 能根据逆向分析工作任务书要求，独立完成函数逆向分析。 7.1.13 能根据逆向分析工作任务书要求，独立完成局部变量逆向分析。 7.1.14 能根据逆向分析工作任务书要求，独立完成类和对象逆向分析。 7.1.15 能根据逆向分析工作任务书要求，独立完成面向对象逆向分析：多态。 7.1.16 能根据逆向分析工作任务书要求，独立完成面向对象逆向分析：封装。 7.1.17 能根据逆向分析工作任务书要求，独立完成面向对象逆向分析：继承。 7.1.18 能根据逆向分析工作任务书要求，独立完成全局变量逆向分析。 7.1.19 能根据逆向分析工作任务书要求，独立完成条件语句逆向分析。 7.1.20 能根据逆向分析工作任务书要求，独立完成循环语句逆向分析。
8.实训演练	8.1 实训演练	8.1.1 能根据网络安全攻防工作任务书要求，独立完成 Wireshark 数据包分析。 8.1.2 能根据网络安全攻防工作任务书要求，独立完成服务漏洞扫描与利用。 8.1.3 能根据网络安全攻防工作任务书要求，独立完成中间人攻击渗透测试。 8.1.4 能根据网络安全攻防工作任务书要求，独立完成 Web 渗透测试。 8.1.5 能根据网络安全攻防工作任务书要求，独立完成 Web 信息收集。 8.1.6 能根据网络安全攻防工作任务书要求，独立完成文件上传渗透测试。 8.1.7 能根据网络安全攻防工作任务书要求,独立完成 FTP 及 Telnet 弱口令渗透测试。 8.1.8 能根据网络安全攻防工作任务书要求，独立完成网络爬虫渗透测试。

		8.1.9 能根据网络安全攻防工作任务书要求，独立完成 Netcat 批量连接渗透测试。 8.1.10 能根据网络安全攻防工作任务书要求，独立完成 Windows 操作系统渗透测试。 8.1.11 能根据网络安全攻防工作任务书要求，独立完成Linux操作系统渗透测试。

参考文献

[1] 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）

[2] 中等职业学校专业教学标准（试行）

[3] 高等职业学校专业教学标准（2018年）

[4] 国家职业技能标准编制技术规范（2018年版）

[5] 信息安全国家标准目录（2016版）

[6] 2019年全国职业院校技能大赛 ZZ-2019024 网络空间安全赛项规程

[7] 2019年全国职业院校技能大赛 GZ-2019028 信息安全管理与评估赛项规程

[8] SJ/T 11623-2016 信息技术服务从业人员能力规范

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

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

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

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