渗透测试在网络安全等级保护测评中的应用探讨

黄祖任
云南金质信息技术服务有限公司，云南 昆明 650000
DOI: 10.61369/TACS.2025060013

摘　　要： 在数字化转型进程中，各行业领域纷纷开发和接入智慧网络管理平台，对网络安全的重视程度不断提高。而渗透测试是一种信息系统安全评估的有效手段，加强渗透测试在网络安全等级保护中的应用，提高信息系统安全评价的准确性，及时发现和应对高隐蔽未知威胁，成为各行业稳定发展的重要问题。本文围绕等保2.0的技术要求，探讨渗透测试的主要方法、应用流程与等保测评场景化应用，为企业信息安全系统防护提供参考。

关 键 词： 渗透测试；网络安全；等级保护；应用

Discussion on the Application of Penetration Testing in Network Security Level Protection Evaluation

Huang Zuren
Yunnan Hi-Q Information Technology Service Co., Ltd, Kunming, Yunnan 650000

Abstract: In the process of digital transformation, various industries have developed and accessed intelligent network management platforms, and the emphasis on network security has been continuously increasing. Penetration testing is an effective means for information system security assessment. Strengthening the application of penetration testing in network security level protection, improving the accuracy of information system security evaluation, and timely detecting and responding to highly concealed unknown threats have become important issues for the stable development of various industries. Focusing on the technical requirements of Level Protection 2.0, this paper discusses the main methods, application processes of penetration testing and its scenario-based application in level protection evaluation, providing reference for enterprise information security system protection.

Keywords: penetration testing; network security; level protection; application

引言

在数字化与智能化时代下，网络攻击手段日趋多样化和复杂化，传统的安全防护手段已经难以应对高危潜在威胁。网络安全等级保护制度是我国网络安全领域的核心制度，旨在对不同重要程度的信息系统实施分等级保护和监管。随着《网络安全等级保护基本要求》（GB/T22239-2019，简称“等保2.0”）的全面实施，企业网络安全防护从“合规导向”向“实战导向”转型。网络安全等级保护测评（下简称“等保测评”）是验证企业安全能力的核心环节，需通过“模拟攻击”视角发现隐性风险，而渗透测试正是连接“防护建设”与“实战验证”的关键技术。渗透测试作为一种主动、模拟真实攻击的安全检测手段，在网络安全等级保护测评中发挥着愈发关键的作用，能够有效发现系统安全漏洞，评估系统的实际安全防护能力，为等级保护工作提供有力支撑。

一、渗透测试的主要方法

等保测评覆盖“网络安全、应用安全、数据安全、设备和计算环境安全”四大领域，从“测试视角”“测试范围”“技术类型”三类测评场景角度看，渗透测试方法主要如下：

（一）按测试视角分类

渗透测试通过模拟“外部攻击者”“内部运维人员”“混合角色”的视角，验证等保测评中“边界防护”“内部管控”等不同维度的安全能力[1]。

1. 黑盒测试：模拟外部无权限攻击者，仅通过公开接口（如网站URL、APP客户端、网络端口）发起攻击；

2. 白盒测试：模拟内部授权运维/开发人员，深入挖掘系统底层漏洞；灰盒测试是模拟半授权混合角色，结合黑盒的外部攻击与白盒的内部分析，平衡测试效率与深度。

（二）按测试范围分类

渗透测试需针对等保测评的“网络、应用、数据、设备和计算环境”四大领域，制定细分测试方案，确保每个安全域的控制点均得到验证[2]。

1. 网络层渗透测试：通过路由器、交换机、防火墙、VPN、负载均衡器、网络端口等网络设备与链路，验证网络边界与内网

防护；

2.应用层渗透测试：通过Web应用（网站、后台管理系统）、移动应用（APP）、桌面应用、API接口等业务系统，验证业务系统安全；数据层渗透测试是通过数据库（MySQL、Oracle等）、数据备份文件、数据传输链路、敏感数据存储介质（如服务器硬盘、U盘），验证敏感数据全生命周期防护；

3.设备和计算环境渗透测试：通过服务器（WindowsServer、Linux）、终端电脑（员工办公PC）、安全设备（IDS/IPS、杀毒软件），验证终端与服务器安全。

（三）按技术类型分类：自动化工具与人工测试结合

等保测评涉及大量资产（如数百台服务器、数十个应用系统），需通过“自动化工具批量扫描+人工深度验证”的组合方式，兼顾测试效率与准确性[3]。

1.自动化工具测试：利用漏洞扫描、信息收集与漏洞利用工具，对服务器进行批量漏洞扫描；

2.人工测试：通过业务逻辑测试、代码审计、社会工程学测试等方式，模拟真实业务场景进行测试，深挖隐性与逻辑漏洞。

二、等级保护测评中渗透测试的应用流程

等保测评需遵循“准备→测评→分析→整改→验收”的流程，渗透测试作为测评环节的核心技术手段，需同步嵌入并形成标准化流程，确保测试合规、可控、有效。

（一）前期准备阶段：明确目标与风险控制

1.确定测试范围与目标

结合等保测评范围（由企业与测评机构共同确认的资产清单），明确渗透测试对象，避免超出范围影响无关业务[4]。例如：若等保测评范围为“电商交易系统（含Web网站、MySQL数据库、应用服务器）”，则渗透测试仅针对该系统，不涉及企业内部办公系统。同时，需明确测试目标（如验证是否符合等保三级要求、发现高风险漏洞），确保测试方向与等保测评目标一致。

2.签订授权与风险协议

渗透测试需获得企业书面授权（避免法律风险），协议中需明确：测试时间（如非业务高峰时段22:00－次日6:00）、测试手段（禁止使用破坏性技术）、应急方案（如测试导致系统故障时的恢复流程）。同时，需同步告知企业备份核心数据（如数据库备份），符合等保“业务连续性保障”的要求。

3.信息收集与环境准备

测试人员通过“被动收集”（如查询域名信息、公开漏洞库）与“主动收集”（如扫描端口、测试接口）获取目标资产信息，同时搭建测试环境（如模拟生产环境的测试服务器），避免直接在生产环境测试导致业务中断[5]。例如：测试Web应用时，先在企业提供的测试环境中验证漏洞，再在生产环境中进行“非破坏性验证”（如仅发送测试请求，不执行漏洞利用）。

（二）漏洞探测阶段：全面扫描与验证

1.自动化扫描初筛

使用漏洞扫描工具（如Nessus、AWVS）对目标资产进行批量扫描，生成初步漏洞清单。例如：扫描应用服务器时，发现“WindowsServer2012未安装MS17-010漏洞补丁”“Web服务器开启目录浏览功能”等问题，初步判断可能违反等保“设备和计算环境安全”中“系统补丁管理”“安全配置”的要求。

2.人工验证与深度探测

对自动化扫描发现的漏洞进行人工验证（避免误报），同时补充人工测试发现隐性漏洞[6]。例如：自动化工具提示“Web应用存在XSS漏洞”，测试人员通过人工构造恶意脚本，验证是否能成功执行并获取用户Cookie（确认漏洞真实存在）；同时，通过人工测试发现“管理员密码可通过密码重置功能绕过（无需验证手机号）”，此类逻辑漏洞未被自动化工具识别，需人工深度探测。

（三）漏洞利用阶段：模拟攻击与权限验证

1.低风险漏洞利用：验证防护有效性

针对中低风险漏洞（如弱口令、目录遍历），尝试利用以验证防护措施是否生效[7]。例如：使用“admin/123456”弱口令尝试登录数据库，若成功登录，说明未启用“强密码策略”“登录失败锁定”等防护，违反等保“设备和计算环境安全”中“身份鉴别”的要求；若登录失败且触发IDS告警，说明防护措施有效。

2.高风险漏洞利用：控制风险与边界

针对高风险漏洞（如远程代码执行、SQL注入），需在企业授权下进行“有限度利用”，避免影响业务。例如：发现Web应用存在SQL注入漏洞时，仅执行“selectversion()”获取数据库版本，验证漏洞存在即可，不执行“droptable”等破坏性操作；若需验证权限控制，仅获取“普通用户权限”，不尝试提升至管理员权限，符合等保“可控性”要求。

（四）后渗透测试阶段：验证内网与数据防护

1.横向移动测试

若获取某台服务器权限，尝试通过“内网扫描”“漏洞利用”横向渗透至其他资产，验证内网防护能力[8]。例如：从Web服务器横向渗透至数据库服务器，若未被防火墙、IDS拦截，说明内网访问控制存在缺陷，违反等保“网络安全”中“内网防护”的要求。

2.数据访问测试

尝试访问核心敏感数据（如用户信息、业务数据），验证数据防护措施有效性。例如：获取数据库权限后，尝试读取加密的用户密码字段，若能直接解密（说明加密算法不安全），则违反等保“数据安全”中“敏感数据加密”的要求；若无法解密且有访问日志记录，说明数据防护有效。

（五）报告输出阶段：对接等保整改需求

渗透测试报告需结合等保要求，形成“漏洞详情→风险等级→等保控制点映射→整改建议”的结构化内容，为企业整改提供明确指导[9]。例如：

1.漏洞详情：“Web应用存在SQL注入漏洞（CVE-2023-XXXX），可通过构造恶意SQL语句获取数据库敏感数据”；

2.风险等级：高风险（可能导致用户信息泄露，违反等保三级“数据安全”要求）；

3. 等保控制点映射：不符合 GB/T22239-2019中“7.2.4应用安全”的“输入验证”与“7.3.1数据安全”的“数据保密性”要求；

4. 整改建议：“使用预编译 SQL 语句修复注入漏洞，同时启用数据库审计功能，记录敏感数据访问行为”。

三、渗透测试在等保测评中的具体应用分析

等保2.0将系统分为五个等级，不同等级的防护要求差异显著，渗透测试需结合等级要求调整深度与范围，同时针对不同安全域（网络、应用、数据）提供定制化测试方案[10]。

（一）按等保等级差异化应用

1. 等保二级系统：基础漏洞验证

二级系统（如小型企业官网、办公系统）防护要求较低，渗透测试以“外部边界漏洞扫描”为主。以某二级办公系统测试为例，发现“管理员账号使用弱口令”“Web 网站未启用 HTTPS”，需整改以符合等保二级“身份鉴别”“数据传输安全”的要求。

2. 等保三级系统：深度渗透与逻辑验证

三级系统（如电商交易系统、政务服务系统）防护要求较高，渗透测试需覆盖“外部 + 内网”“自动化 + 人工”。以某三级电商系统测试为例，通过人工测试发现“普通用户可越权查看其他用户订单”（业务逻辑漏洞）、“数据库密码以明文存储在配置文件中”（数据安全漏洞），需针对性整改以满足等保三级要求。

3. 等保四级系统：持续性测试与攻防演练

四级系统（如金融核心交易系统、能源调度系统）需“动态防护”，渗透测试需升级为“持续性测试 + 攻防演练”。以某银行核心交易系统（四级）的渗透测试中，红队通过“钓鱼邮件获取员工电脑权限→利用内网漏洞渗透至核心数据库→模拟篡改交易数据”，蓝队通过 IDS 告警、应急响应流程拦截攻击，最终通过演练发现“内网漏洞响应延迟”“应急方案不完善”等问题，推动企业优化安全防护，符合等保四级“动态防御”的要求。

（二）按安全域场景化应用

1. 网络安全域：验证边界与内网防护

在测试某企业网络边界时，发现防火墙未拦截“针对8080端口的暴力破解请求”，且 WAF 未识别出“SQL 注入攻击语句”，说明边界防护存在缺陷，需调整防火墙规则与 WAF 策略，符合等保“网络安全”要求。

2. 应用安全域：验证业务系统与接口安全

在测试某政务 APP 时，发现其 API 接口未对“用户 ID”参数做校验（可修改参数查看其他用户信息），且本地缓存中存储了用户身份证号明文，违反等保“应用安全”与“数据安全”要求，需修复接口逻辑并加密本地缓存数据。

3. 数据安全域：验证敏感数据全生命周期防护

在测试某医疗系统时，发现“患者病历数据备份文件可通过 Web 目录直接下载”“数据传输使用 HTTP 协议（未加密）”，直接违反等保“数据安全”中“数据存储安全”与“数据传输安全”的要求，需立即修复备份文件权限并升级为 HTTPS 传输。

四、结束语

综上所述，渗透测试作为等保测评的实战检验工具，不仅能帮助企业发现显性漏洞，更能挖掘隐性风险，为等保合规提供技术支撑。企业需结合自身等保等级、行业场景，选择适配的渗透测试方法与过程，将测试结果转化为整改行动，最终实现合规性与安全性的双重提升。随着等保2.0的深入推进，渗透测试将从一次性测试升级为持续性安全运营的核心环节，助力企业构建实战化、动态化的网络安全防护体系。

参考文献

[1] 周天熠 . 网络渗透攻击测试技术研究 [J]. 信息与电脑 (理论版), 2024, 36 (01): 186-188+192.

[2] 李雨 , 李江丰 . 关于网络安全渗透测试流程及方法的研究 [J]. 通信管理与技术 , 2024, (01): 42-44.

[3] 方星宇 . 基于民航等级保护的 Web 自动化渗透测试方法的研究与实现 [J]. 信息与电脑 (理论版), 2023, 35 (15): 209-211.

[4] 田嘉豪 , 胡吉祥 . 等级保护 2.0 中渗透测试技术的研究 [J]. 网络安全技术与应用 , 2024, (01): 11-12.

[5] 王远翔 . 等保2.0标准下网络渗透测试研究 [J]. 科技创新与应用 , 2024, 14 (01): 26-29.

[6] 曲峰 , 张倩 , 李媛媛 . 网络安全在等保测评中的设计与应用分析 [J]. 电子元器件与信息技术 , 2024, 8 (08): 153-155.

[7] 王鑫 . 网络安全测评中 Web 应用安全渗透测试方法分析 [J]. 无线互联科技 , 2023, 20 (04): 165-168.

[8] 李群 , 王超 , 任天宇 . 基于渗透测试的多层次网络安全入侵检测方法 [J]. 沈阳工业大学学报 , 2022, 44 (04): 372-377.

[9] 严浩 , 石西华 . 渗透测试在网络安全等保测评中的运用 [J]. 电子技术与软件工程 , 2021, (24): 240-241.

[10] 李劲雄 . 网络安全等级保护测评中渗透测试的应用 [J]. 网络安全技术与应用 , 2021, (03): 9-11.

