 DOI: https://doi.org/10.12349/iser.v7i1.9037

Research and Practice of Cybersecurity Attack and Defense Technologies

Zhe Li

Fujian Mindun Network Security Co., Ltd., Fuzhou, Fujian, 350001, China

Abstract

As a critical node in the cybersecurity assurance system, the classified protection assessment serves as a vital tool for identifying system security risks and evaluating the effectiveness of defensive measures. This paper, based on practical scenarios of classified protection assessments, focuses on typical categories and core methods of current cyber attacks. It provides an in-depth analysis of the underlying logic of attack behaviors and their threat pathways to information systems of varying classification levels. By incorporating real-world examples from assessment practices, the study explores targeted strategies for building and implementing a defense technical system that aligns with classified protection requirements. Special emphasis is placed on methods for validating the effectiveness of defensive measures and optimizing their direction. The findings offer practical references tailored to business realities, facilitating the efficient execution of classified protection assessments and the steady enhancement of information system security defenses, thereby helping information systems meet the corresponding security protection requirements.

Keywords

Level Protection Assessment; Cybersecurity Attacks; Defense Technologies; Security Protection; Practical Implementation

网络安全攻击与防御技术研究与实践

李哲

福建闽盾网络安全有限公司，中国 · 福建 福州 350001

摘　要

等级保护测评作为网络安全保障体系的关键节点，是辨别系统安全隐患、检验防御措施有效性的重要手段。本文依托等级保护测评实操场景，聚焦当前网络安全攻击的典型类别与核心方式，深刻解析攻击行为的底层逻辑与对不同等级信息系统的威胁路径，结合测评工作中的实际事例，有针对性地探究适配等级保护要求的防御技术体系搭建与落地策略，着重讲述防御措施的有效性验证办法与优化走向，为等级保护测评工作的高效开展、信息系统安全防护能力的稳步提升，提供贴合业务实际的实践参照，助力信息系统符合对应等级的安全保护要求。

关键词

等级保护测评；网络安全攻击；防御技术；安全防护；实操落地

1 引言

随着数字化转型的深入，信息系统已然成为各行业运作的核心载体，其安全稳定性直接关系到业务连续性与数据安全。等级保护测评作为我国网络安全保障的基础性制度，借助分级分类保护的准则，给不同重要程度的信息系统划定安全防护底线 [1]。当下，网络攻击手段不断更新升级，攻击路径更具隐蔽特性与针对性，给等级保护测评工作带来了新的难题。鉴于此，从等级保护测评角度出发，深入研究网络安全攻击的核心特点与防御技术的实操重点，明确攻击与防御的动态博弈联系，对提升测评工作精准度、增强信息系统安全防护能力具有重要现实意义。

【作者简介】李哲（1991–），男，中国福建闽侯人，本科，工程师，从事计算机科学与技术、网络安全研究。

2 等级保护测评下网络安全攻击的典型类型与核心特征

2.1 恶意代码攻击

恶意代码攻击是各等级信息系统均高频面对的攻击类型，亦是等级保护测评中重点核查的风险点。此类攻击通过植入病毒、木马、勒索软件等恶意程序，达成对系统的控制、数据窃取或破坏。和传统泛化攻击有别，当前恶意代码更具针对性，部分攻击团伙会针对特定行业的信息系统定制恶意代码，躲避常规杀毒软件的检测 [2]。在测评过程中察觉，低等级信息系统多面临常规病毒、蠕虫攻击，主要通过 U 盘、邮件附件等途径传播，攻击目的以破坏系统正常运行为主；高等级信息系统则容易遭遇定制化木马与勒索软件攻击，攻击者通过社工渗透获取系统入口，植入恶意代码之后控制核心业务模块，以加密数据索要赎金为主要目的，对系统的破

坏性质极强。除此之外，恶意代码的持久化驻留能力明显提升，部分恶意程序会修改系统注册表、创建隐藏进程，即便系统重启也难以彻底清除，给测评过程中的隐患排查带来了挑战 [3]。

2.2 网络渗透攻击

网络渗透攻击为攻击者冲破系统边际防护、非授权访问内部资源的核心方式，也是等级保护测评里对边界安全、访问管控有效性验证的关键切入点。此类攻击遵循“侦察—扫描—利用—提权—维持”的完整轨迹，实操特性极强。在侦察时期，攻击者借助端口扫描、信息搜集工具，获取目标系统的 IP 地址区段、开放端口、操作系统版本等基础信息，为后续攻击进行准备；在扫描时期则将焦点置于系统漏洞与弱口令，针对测评中常见的未修复高危漏洞、默认密码未调整、密码复杂度不足等状况实施精确突破；利用时期通过漏洞利用工具获取系统低权限访问权，再经由提权操作获取管理员权限，最终达成对系统核心资源的掌控。在高等级信息系统测评中，还察觉攻击者会采用“旁路渗透”策略，绕开核心防护装置，通过办公终端、无线网络等薄弱节点切入内部网络，此类攻击轨迹隐蔽性强，易于绕过常规边际防护举措，给测评带来了更大难题 [4]。

2.3 数据泄露攻击

数据作为信息系统的核心资产，是攻击者的主要目标之一，数据泄露攻击也成为等级保护测评中数据安全核查的核心内容。此类攻击的核心意图是窃取系统中的敏感数据，包含用户信息、业务数据、核心机密等，攻击手段呈现出“技术 + 社工”融合的特征。技术层面，攻击者通过 SQL 注入、XSS 跨站脚本等途径，利用系统数据交互接口的漏洞，非法读取、下载敏感数据；社工层面，通过钓鱼邮件、伪基站短信等方式，引诱系统管理员或普通用户泄露账号密码、验证码等关键信息，进而登录系统获取数据。

3 适配等级保护测评要求的防御技术体系搭建与实操要点

3.1 边界防护技术：筑牢系统安全首道防线

边界防护是等级保护测评中边界安全核查的重点，其核心目的是阻断非法访问，过滤恶意流量，保障网络边界的可操控性。针对不同等级信息系统，边界防护技术的配置需体现差异化。低等级信息系统可运用防火墙、入侵检测系统（IDS）搭建基础边界防护，防火墙需严格配置访问控制策略，仅开放业务必需的端口与协议，禁用不必要的服务，防止出现“宽进宽出”的情形；IDS 则用于实时监测边界流量，及时对异常访问行为发出告警。高等级信息系统需在基础防护之上，增设入侵防御系统（IPS）、下一代防火墙（NGFW），实现“检测—防御—阻断”一体化管控 [5]。

3.2 终端防护技术：增强末端安全防护能力

终端作为信息系统的末端节点，是恶意代码攻击、渗透攻击的主要入口，终端防护成效径直作用于体系整体安全，亦是等级保护测评中终端安全核查的关键内容。终端防护技术需聚焦“准入把控—实时防护—应急回应”全流程。准入把控方面，借助终端准入体系，对接入网络的终端开展身份验证与安全状态核查，仅准许契合安全要求（像安装杀毒软件、系统补丁完备）的终端接入，根绝不安全终端接入产生的风险；实时防护方面，布置终端安全管理体系，整合杀毒、恶意代码拦截、主机入侵检测（HIDS）等功能，定时更新病毒库与恶意代码特征库，对终端的文件操作、进程运行、网络连接等行为实施实时监测，及时处理异常行为。

3.3 数据防护技术：守住核心资产安全底线

数据防护是等级保护测评中数据安全与备份恢复核查的核心，需围绕数据“存储—传输—运用—销毁”全生命周期搭建防护架构，保障数据的机密性、完整性与可用性。存储层面，针对敏感数据运用加密存储技术，低等级信息体系可采用文件加密、数据库加密等途径，高等级信息体系需采用透明加密技术，在不干扰业务运用的前提下，达成数据自动加密存储，同时配备访问权限管控，细化不同角色的数据访问范畴；传输层面，对数据传输过程采用 SSL/TLS 等加密协议，规避数据在传输过程中被监听、篡改，特别是跨网络传输的敏感数据，必须经由加密通道传输；在备份恢复层面，依照等级保护测评要求，制定完善的数据备份策略，定时开展全量备份与增量备份，备份数据需存储于安全的离线介质或异地备份中心，同时定时开展备份恢复演练，验证备份数据的完整性与可用性，确保体系遭遇攻击后能迅速恢复数据与业务。

3.4 访问控制技术：构建精细化权限管理架构

访问控制是防范未授权访问、数据泄露的关键是技术，亦是等级保护测评中访问控制核查的核心要求，核心准则是“最小权限”与“权责对等”。低等级信息体系可采用基于角色的访问控制（RBAC）模型，依据用户的岗位职责分配体系权限，确保用户仅具备完成工作所需的最小权限，杜绝超权限访问；同时严格施行密码策略，要求密码具备足够复杂度，定期更换，禁止使用默认密码、弱密码。高等级信息体系需于 RBAC 模型架构之上，构建多因素认证（MFA）、权限审计等制度体系，多因素认证可联合密码设置、动态验证码生成、生物特征识别等形式手段，提升身份认证环节的安全系数，规避单一认证模式遭到破解；权限审计则需周期性对用户权限实施核查工作，清除冗余权限配置、休眠账号数据，对权限变动情形、超权限访问行为开展实时记录与预警操作。测评实践过程当中，需着重验证权限分配的合理程度、身份认证的有效状态，核查权限审计日志的完整情况，保障访问活动具备可追溯性、可管控性。

4 等级保护测评范畴内防御技术有效性验证及优化策略

4.1 防御技术有效性验证手段运用

等级保护测评实操场景下，防御技术有效性验证需采

取“静态核查结合动态测试”的复合方式。静态核查主要围绕防御设备的参数配置、策略规则、日志记录等实施合规性检查，确认防护举措是否契合相应等级的测评规范，是否存在配置层面的漏洞隐患与冗余策略内容。动态测试则通过模拟攻击的技术途径，验证防御技术的实际防护效能，诸如模拟恶意代码传输过程、漏洞利用场景、弱口令破解行为等攻击活动，检测防火墙设备、IPS 系统、终端防护软件等是否及时阻断攻击进程、发出预警信息；针对数据防护技术体系，可模拟未授权访问情形、数据窃取行为，验证加密技术应用、访问控制机制的有效程度。同时，结合系统日常运行阶段的安全事件记录，追溯防御技术的响应效果表现，评估预警信息的准确水平、处置工作的及时程度，判断防御技术能否适配实际攻击场景需求。

4.2 防御策略优化方向指引

基于测评流程中发现的问题事项，防御策略优化需聚焦三个核心方向。其一为贴合业务需求维度优化防护粒度标准，部分信息系统在部署防御技术期间，过度追求防护强度而影响业务正常运行，需结合业务应用场景调整防护策略内容，在安全保障与便捷操作之间寻求平衡状态，例如针对核心业务模块强化防护力度，对非核心功能模块采用适度防护措施。其二为针对攻击手段演变优化防御技术体系，伴随攻击手段的持续升级，传统防御技术可能逐步丧失效能，需定期跟踪最新攻击趋势动态，更新防御设备特征库数据、漏洞库信息，升级防护软件版本程序，在必要情况下引入新型防御技术手段，弥补防护体系短板弱项。其三为强化人员安全意识与操作规范建设，多数安全事件的发生成因与人员操作失当存在关联，需定期组织安全培训活动，提升管理员群体与普通用户的安全意识水平，规范操作流程环节，避免因人为失误因素导致防御体系遭受突破，同时建立健全安全事件应急处置预案体系，定期开展实战演练活动，提升应对攻击行为的快速响应能力。

5 结论

网络安全攻击与防御的动态博弈构成等级保护测评事项的核心背景情况，攻击办法的迭代升级给防御技术的针对性及实操性设定更高规格要求。以等级保护测评角度作为出发点，构造适配于不同等级信息系统的防御技术体系架构，需要紧紧扣住测评标准内容，从边界实施防护、终端开展防护、数据进行防护、访问加以控制等核心维度落地防护相关措施，同时借助“静态核查 + 动态测试”的形式验证防御实际效果，持续不断优化防御策略规划。于实操流程当中，需要兼顾合规性与实用性，防止出现形式化防护现象，切实筑牢信息系统安全防护防线。伴随数字化技术的不停发展，网络攻击将会呈现出更为复杂的态势状况，需要持续深入深化攻击与防御技术方面的研究，结合等级保护测评工作的实践经验内容，推动防御技术体系的迭代升级进程，为信息系统安全稳定运行态势提供有力保障支持。

参考文献

[1] 成翔,匡苗苗.基于相似性度量的APT攻击意图识别方法[J].扬州大学学报(自然科学版),1-10.

[2] 许亚美,王子威,王婵飞.双阶段结合流形优化的调制识别网络对抗攻击[J].西安电子科技大学学报,1-14.

[3] 蔡秋富.基于流量异常特征的网络攻击行为检测方法研究[J].电脑编程技巧与维护,2025,(12):164-166.

[4] 朱志猛.基于门控循环单元的信息安全态势感知系统设计[J].计算技术与自动化,2025,44(04):154-159.

[5] 王梦,张玲,张位,冯毓,刘赟,高吉宏.大语言模型驱动的认知型蜜罐技术综述[J].人工智能,1-9.

[6] 汤永金,王嘉,韩海,肖磊.人工智能技术在网络攻击检测与防御中的应用研究[J].通信与信息技术,2025,(S1):89-92.

[7] 张煜炫,莫宇铖.基于强化学习的虚假数据注入攻击下电力系统安全性研究[J].电气开关,2025,63(06):84-87+91.