文章编号：1005-8451（2015）02-0051-04

信息系统主机安全等级保护测评方法研究

司　群，刘育欣
（中国铁道科学研究院　电子计算技术研究所，北京　100081）

摘　要：随着等级保护在全国各个行业的推广，对《信息安全技术信息系统安全等级保护基本要求》和《信息安全技术信息系统安全等级保护测评要求》中的测评内容对应的测评方法和技术的研究越来越重视，本文针对主机测评技术进行分析研究，通过分析测评项，提出符合标准的测评指标、方法和实施步骤。

关键词：等级保护；主机测评；访谈；人工检查；测试
中图分类号：U29-39　　**文献标志码：**A

Security level protection evaluation methods for host of Information System

SI Qun, LIU Yuxin
(Institute of Computing Technologies, China Academy of Railway Sciences, Beijing　100081, China)

Abstract: With the popularization of level protection in various industries of countrywide, it was paid more and more attention on testing methods and techniques in the "information security technology - basic requirements of security level protection for Information System" and "information security technology - evaluation requirements of security level protection for Information System". This paper researched on the host evaluation technology, put forward the standard evaluation index, methods and implementation steps through analyzing evaluation items.

Key words: level protection; host evaluation; interview; manual inspection; test

1994 年国务院颁发《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）明确了我国对计算机信息系统进行分等级保护的要求。相继 2003 年中办发《国家信息化领导小组关于加强信息安全保障工作的意见》（27 号文）提出了重点保护基础信息网络和关系国家安全、经济命脉和社会稳定等方面的重要信息系统，制定信息安全等级保护的管理办法和技术指南，2004 年公通字《关于信息安全等级保护工作的实施意见》(66 号文)及 2007 年《信息安全等级保护管理办法》（43 号文）等文件发布并推广，逐步明确信息安全等级保护是国家的一项基本制度，等级测评是整个等级保护工作中的重要一环，各行业包括铁路行业都十分重视，铁公安 2012 年发布《关于进一步做好铁路信息安全等级保护工作的通知》（94 号文）。

1　主机安全测评概述

信息系统等级测评技术层面由包括物理安全、主机安全、网络安全、应用安全和数据安全 5 个方面，各个方面相互关联并保持独立性，主机安全测评主要是对服务器、终端 / 工作站等计算机设备的操作系统和数据库系统层面的安全，其中终端 / 工作站是带外设的台式机和笔记本电脑，服务器则指包括应用程序、网络、Web、文件与通信等服务器。

国家标准 GB/T 22239-2008《信息安全技术—信息系统安全等级保护基本要求》（简称：基本要求），以三级信息系统为例将主机安全测评内容分为 7 个控制点，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范和资源控制 [1]，随着信息系统等级降低，主机安全保护能力的要求逐级减少，相应系统等级提升，保护能力的要求逐级增加，基本要求中提出了主机安全测评的基本要求项，《信息系统安全等级保护测评要求》梳理出各个等级主机安全的测评实施过程包括测评内容、测评实施及测评结果判定条件，但是均比较抽象，对于系统测试实际操作起来并不适用，必须根据基本要求和测评要求梳理出被测对象的测评方法和步骤，表 1 列出了三级信息系统主机安全 7 个控制点的测

收稿日期：2014-10-08
作者简介：司　群，工程师；刘育欣，助理研究员。

试方法，通过此表可以更清晰了解现场测试的重点，提早合理安排安全测试人员做好测试计划。

表1 三级信息系统主机安全测评方法

控制点	访谈	检查	测试
身份鉴别	✓	✓	✓
访问控制	✓	✓	×
安全审计	✓	✓	✓
剩余信息保护	×	✓	×
入侵防范	✓	✓	×
恶意代码防范	✓	✓	×

注：✓表示该控制点包括此测评方法，× 表示不包括此测评方法

2 主机安全测评实施

2.1 测评指标确定

根据基本要求，详细梳理出适合铁路行业3级信息系统主机安全测评指标，现仅以身份鉴别测评控制项为例，列出测评指标内容，主要包括：如标识、鉴别、密码复杂度、密码长度、密码更换周期、弱口令、非法登录次数、帐户锁定时间、加密传输、用户名唯一及鉴别方式11个测评指标项，并对其进行了详细的解释，加密传输测评指标指采用SSH加密的远程管理软件，对用户名和口令进行传输；鉴别方式指除用户名口令外还需增加至少以下一种鉴别技术，包括：挑战应答、动态口令、物理设备和生物识别技术。

2.2 前期访谈调研

访谈是对信息系统主机安全使用情况进行了解，依据测试指标要求及实际测试场景，与系统管理员、安全管理员及安全审计员等主机的使用者举行咨询性和针对性的会谈、交流，了解主机的安全策略配置、安全使用情况，对服务器和终端设备的全局情况进行了解[5]。下面从主机安全的7个控制点分别介绍前期需访谈内容。

2.2.1 身份鉴别访谈

（1）询问系统管理员操作系统的身份标识和鉴别机制采取何种措施实现；

（2）询问数据库管理员数据库管理系统的身份标识和鉴别机制采取何种措施实现；

（3）询问系统管理员操作系统用户的口令策略；

（4）询问数据库管理员数据库管理系统用户的口令策略；

（5）询问系统管理员服务器操作系统的远程管理方式和加密措施；

（6）询问系统管理员操作系统除采取用户名/口令身份标识和鉴别方式以外有无其他措施。

2.2.2 访问控制访谈

（1）询问系统管理员操作系统是否实现系统管理、安全审计和安全管理三权分立；

（2）询问数据库管理员数据库管理系统是否实现数据库系统管理、安全审计和安全管理三权分立；

（3）询问系统管理员用户列表中各个用户的作用，是否存在多余的、过期的和共享帐户；

（4）询问数据库系统管理员用户列表中各个用户的作用，是否存在多余的、过期的和共享帐户；

（5）询问系统管理员是否对重要信息资源设置敏感标记；

（6）询问系统管理员敏感标记的策略设置情况。

2.2.3 安全审计访谈

（1）询问系统管理员服务器操作系统是否开启审计功能或安装第三方审计工具；

（2）询问数据库管理员数据库管理系统是否开启日志功能或安装第三方审计工具；

（3）询问安全审计员是否对日志记录进行分析生成审计报表的措施或工具；

（4）询问安全审计员对审计记录的保护措施；

（5）询问安全审计员审计记录的存储、备份措施。

2.2.4 入侵防范访谈

（1）询问系统管理员是否部署入侵防范产品；

（2）询问系统管理员查看日志的周期；

（3）询问系统管理员程序完整性检测措施及破坏后的恢复措施，是否对系统、程序等重要文件进行备份；

（4）询问系统管理员系统升级方式和是否安装了最新补丁。

2.2.5 恶意代码防范访谈

询问系统管理员主机操作系统的恶意代码产品的升级方式，是否采用统一的更新和查杀策略。

2.2.6 资源控制访谈

（1）询问系统管理员查看系统资源监控器的频率或使用第三方监控软件实现服务器系统的监视；

（2）询问系统管理员日常监控系统服务水平的措施。

2.3 主机安全现场评测

主机安全现场测评主要是通过检查和测试两种方式交互进行。

检查是主要的测评手段，通过对测评对象进行观察、查验和分析得出符合性结论。可以进行文档检查（也就是证据类信息的检查）、实地察看（如机房选址、物理环境测评）、配置检查（主要是检查主机操作系统、应用系统、网络交换设备与网络安全设备的配置情况）。如测试人员欲对某应用服务器身份鉴别功能进行检查，则需登录该服务器，输入相关命令对其进行操作，按照操作结果对服务器的身份鉴别策略进行检查确认，核实其密码长度、密码复杂度、登陆失败锁定等配置项是否符合要求。

测试主要是测试人员采用专用的测试工具，搭建特定测试环境，按照预定的方法操作，使被测对象在测试环境中与测试工具进行联动，产生特定的行为。依据测试工具记录的信息，对待测设备的指标进行检查分析，获取证据以证明信息系统安全保护措施及策略是否有效，包括系统漏洞扫描和渗透性测试等。

检查和测试是测试人员在现场采用手工的方式验证信息系统具体的安全配置机制和运行的有效性，因此相比较访谈方法更逼近客观事实，是取得测试证据的重要途径，将检查和测试融合起来更能全面的取证。但是，对于拥有成百上千甚至更多台主机的大型信息系统而言，通常采取抽样检测的方式，选取典型测评对象主机进行检测，无特殊要求不需要逐一检查所有主机。基本要求中，三级主机安全测评检查项包括 7 个单元，32 个测评要求点。主机层面现场检查内容和测试流程采用流程图的方式展现，如图 1 所示。

如在身份鉴别单元中需要确定用户名是否唯一与在访问控制单元中查看是否存在默认帐户、多余帐户和共享帐户等单元项需要同一个测试命令。

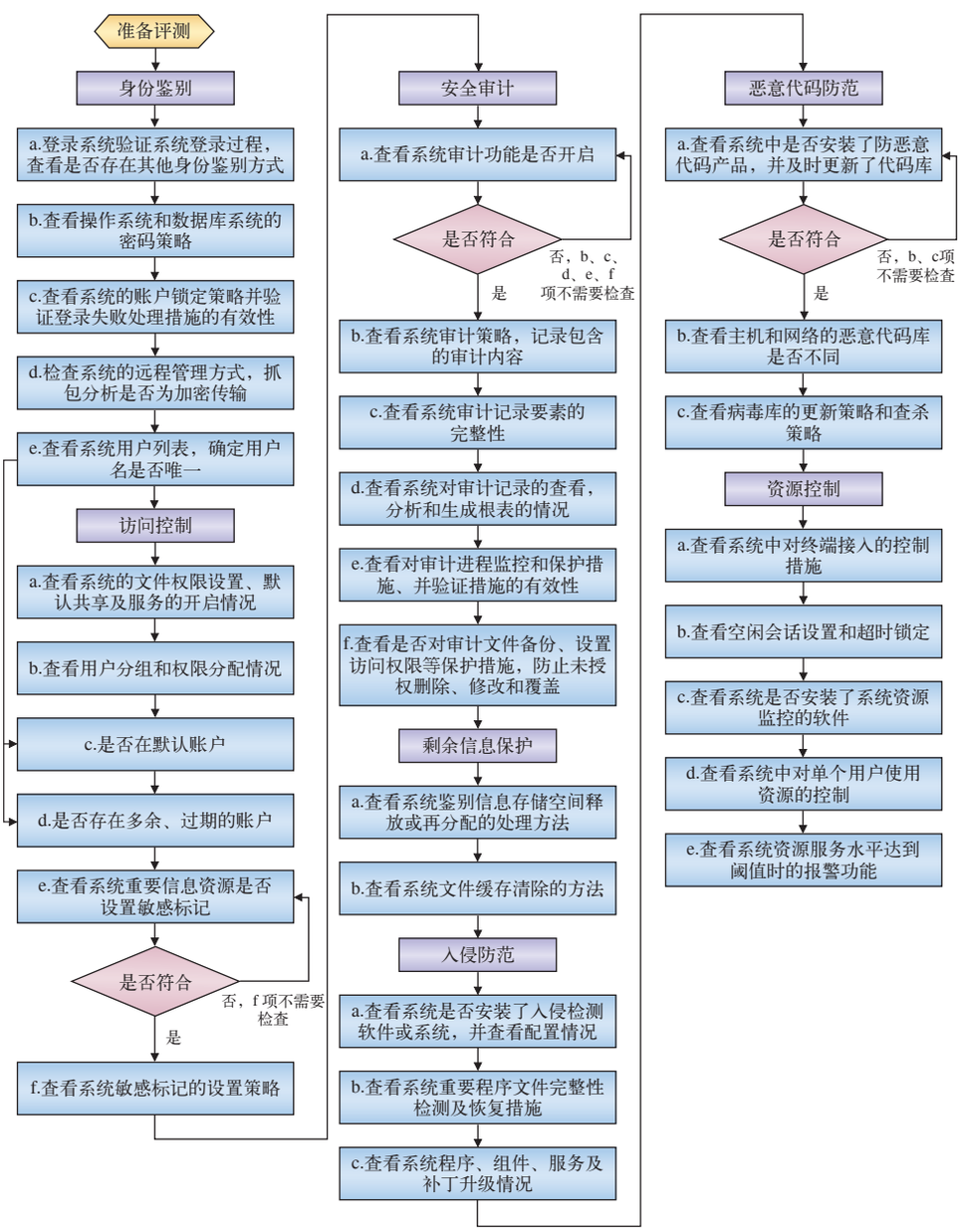

图1　主机安全现场检查作业指导手册

3 结束语

本文提出了三级主机安全测评的原理、方法和测评实施过程，对基本要求进行了分析解读，用简单易懂的形式阐述了标准的精髓，希望提出的测评实施方法及指导手册对主机安全测评有所帮助。在后续的工作中会更详细地总结其他等级主机安全测评流程，并提出更具体化的测评指标体系。

参考文献：

[1] 中华人民共和国质量监督检验检疫局，中国国家标准化管理委员会 .GB/T 22239-2008，信息安全技术—信息系统安全等级保护基本要求 [S]. 北京：中国标准化出版社，2008.

[2] 中华人民共和国质量监督检验检疫局，中国国家标准化管理委员会 .GB/T28448-2012，信息安全技术—信息系统安全等级保护测评要求 [S]. 北京：中国标准化出版社，2012.

[3] 中华人民共和国质量监督检验检疫局，中国国家标准化管理委员会 .GB/T20272-2006, 操作系统安全技术要求 [S]. 北京：中国标准化出版社，2006.

[4] 中华人民共和国质量监督检验检疫局，中国国家标准化管理委员会 .GB/T20273-2006, 数据库管理系统安全技术要求 [S]. 北京：中国标准化出版社，2006.

[5] 李 倩，杨晓明，罗恒峰，等 . 级测评的主机安全检测 [J]. 电子产品可靠性与环境试验，2011，29（6）.

责任编辑 徐侃春

（上接 P40）

险评估、等级评测等工作，确保等级保护安全手段能贯穿重要信息系统的始终；通过完善铁路两级三线安全运维服务体系，建立总公司、铁路局两级信息安全技术督查工作机制，将信息安全技术和管理有机结合起来，实现安全管理、运维、督办相辅相成、相互监督的局面。

6.7 等级保护示范工程仿真实验环境及试点工程建设

针对信息系统、安全产品建立等级测评验证与运行仿真环境，开展等级保护定级模型、测评模型以及测评技术研究，按等级保护相关要求开展信息安全等级保护工程的试点建设，为铁路信息安全等级保护工作提供技术支撑，确保铁路信息系统与安全产品的高可靠性与稳定性。

7 结束语

信息安全等级保护工作是我国规范信息安全管理工作的一种有效制度，铁路行业除按等级保护管理流程做好定级备案、方案设计、等保测评、建设与整改几方面的工作外，还需从源头的标准制定和后期的措施落实两方面抓好一头一尾的工作，使得信息安全工作能在铁路行业全面实施。

参考文献：

[1] 余 勇，林为民 . 电力行业信息系统等级保护的研究及实施 [J]. 信息网络安全，2009（12）.

责任编辑 徐侃春

（上接 P50）

测评有效开展的前提。通过在重要时间节点（如春运、暑运等）开展安全检查专项检查及等级保护自查，一方面提高了系统运维人员的专业测评效率，节约了各类资源；另一方面，将安全建设整改工作常态化稳步推进的同时，必将使铁路总公司及铁路局、管理人员保持安全意识，逐渐深刻理解信息安全防护的实际意义，更是从实际出发推动等级保护测评体系及制度尽快建立和实施的有效手段。

参考文献：

[1] 中华人民共和国质量监督检验检疫局，中国国家标准化管理委员会 . GBT 22239-2008，信息安全技术—信息系统安全等级保护基本要求 [S]. 北京：中国标准化出版社，2008.

[2] 中华人民共和国质量监督检验检疫局，中国国家标准化管理委员会 .GBT 28448-2012，信息安全技术信息—信息系统安全等级保护测评要求 [S]. 北京：中国标准化出版社，2012.

[3] 刘 寅 . 发电集团等级保护自测评实践分析 [J]. 中国电力，2012，10（2）：77-79.

[4] 郭启全 . 国家信息安全等级保护工作的开展与实施 [J]. 警察技术，2007（5）：52-55.

责任编辑 徐侃春