



LanSecS[®]

信息安全等级保护检查工具箱



产品概述

LanSecS[®] 信息安全等级保护检查工具箱是一款依据信息安全等级保护国家标准及行业标准，专门为等级保护工作监管部门及行业单位开展信息安全等级保护检查、自查的一体化便携式工具装备。并为等级保护监管部门和行业单位，快速高效地执行信息安全等级保护检查、自查工作提供专业化的技术支持。



产品功能

● 检查管理

以等级保护1.0、2.0相关法规政策及指导性要求为设计依据，提供完整的等级保护检查、自查工作流程，以指导整个检查工作的顺利进行。

● 知识库

内置等级保护检查知识库，提供最佳的操作指南和结果判定标准，保证检查、自查工作的顺利开展。

● 技术检测工具集

系统提供专业的技术检测工具，检测结果可自动匹配检查指标，实现了等级保护安全检查、自查工作的自动化，提高了用户检查和自查工作效率。

U盘
检查工具



windows
主机配置
检查工具

- 支持检查系统信息、硬件信息、启动项、异常服务
- 支持检查审计策略、系统安全补丁、安装软件、进程扫描
- 支持检查用户权限、安全选项、组策略、运行保护等



病毒
检查工具

- 支持快速扫描系统关键目录和发现目录中是否存在病毒
- 支持对所有盘符下的文件进行全面深度检查
- 支持快速选择桌面、文档、关键目录、内存、U口等



木马
检查工具

- 支持快速扫描系统关键目录和发现关键目录中是否存在木马
- 支持对所有盘符下的文件进行全面深度检查
- 支持快速选择桌面、文档、系统关键目录、U口等区域



网站恶意代码
检查工具

- 支持ASP、ASPX、JSP、PHP、CSS等文件格式检查
- 支持IIS、Apache、Nginx、Weblogic、Websphere等
- 支持制定检查目录路径、文件类型等

主要功能

网口
检查工具



网络及安全设备
配置检查工具

- 支持对路由器、交换机和防火墙进行配置信息采集并分析
- 支持H3C、思科、华为、天融信、网神、启明星辰、网御星云、Juniper、黑盾等



Linux主机配置
检查工具

- 支持检查系统信息、账户信息、账户口令策略
- 支持检查活动端口、用户权限、安全审计
- 支持检查SNMP服务、SSH协议等



系统漏洞
检查工具

- 支持各类操作系统、软件、网络设备等目标进行漏洞扫描
- 支持多种扫描策略,包括不同强度的扫描策略
- 支持自动统计总体和分析漏洞数量



弱口令
检查工具

- 支持协议类型: SMB、MSSQL、FTP、MYSQL、Oracle、RDP、POP3、SSH、HTTP、Telnet、VNC和SyBase等
- 支持设置通过SSL方式进行检查
- 支持本地、远程主机及多协议同时检查



网站安全
检查工具

- 支持Oracle、MSSQL、DB2、Informix、Sybase、Mysql、PostgreSQL、Access、Ingres等后台数据库类型
- 支持WEB 2.0及各类JavaScript脚本、WAP、FLASH解析
- 支持JSP、CGI、ASP、.NET等类型动态页面
- 支持ERP、HTTP 1.0和1.1标准等复杂Web应用系统扫描



数据库安全
检查工具

- 支持弱口令扫描
- 支持Oracle、MSsql、DB2、Informix、Mysql、Sybase、PostgreSQL等数据库类型
- 支持对数据库的深层次安全检测及准确评估

主要功能



用户价值



应用场景

- ◎ **监管部门**: 依据网络安全等级保护制度和相关标准要求, 通过检查工具箱对网络运营使用单位的网络进行等保合规检查, 督导落实等级保护管理和技术保护措施。
- ◎ **测评机构**: 使用检查工具箱开展等级测评业务, 依据测评准备、方案编制、现场测评、分析及报告编制流程输出测评报告。
- ◎ **重点行业**: 运营、使用单位可以定期使用检查工具箱对系统安全状况、安全保护制度及措施的落实情况进行自查。