翼支付终端入侵防护平台功能测试报告

# 版本介绍

## 版本用途

为了落实网络安全集约化目标,通过中国电信 SOC 综合运营管理平台(以下简称:集团一体化平台)实现全网安全基础信息动态管理、全网主流漏扫设备集中调度管理以及全网安全基线的集约化管理，实现如下目标：

1. 上海部署与集团一体化平台互通的省级节点,包括不同网络的采集机、前置机及相接口。省级节点在 IT类资产上运行自动采集 Agent 能够上传网络安全基础信息和安全配置基线信息,实现 IT 类资产的全覆盖;
2. 省级节点与省内各专业网管平台对接定期采集各自域内的非 IT 类资产的网络安全基础信息,实现非 IT 类资产的全覆盖。
3. 省内漏扫设备与集团一体化平台互联互通,能够接收集团一体化平台扫描任务并执行;扫描结果能够上传集团一体化平台;漏扫设备与省内资产网络可达。
4. 构建基于主机的入侵检测系统，实现对所有主机、VM实时检测。
5. 结合以上几点，组建完善的终端入侵防护平台，能够实现资产清点、风险发现、入侵检测，确保所有资产安全合规

## 版本信息

迭代版本：1.1.5

# 测试策略

## 测试投入

测试人员：胡恩平，汪海波，刘孝

测试时间：2019/6/17 — 2019/6/18

### 功能测试内容

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **入侵防护平台测试清单** | | | | | | |
| **模块** | **分类1** | **分类2** | **分类3** | **分类4** | **测试人** | **测试结果** |
| 用户登录 | 密码设置 |  |  |  | 汪海波 | 存在bug |
| 系统管理 | 用户管理 |  |  |  | 刘孝 | OK |
| 系统监控 | 系统日志 |  |  |  | 刘孝 | OK |
| 代理信息 |  |  |  |  | 刘孝 | OK |
| 非IT资产管理 | 配置管理 | 添加 |  |  |  |  |
| 修改 |  |  |  |
| 删除 |  |  |  |
| 搜索 |  |  |  |
| 刷新 |  |  |  |
| 资产管理 | 搜索 |  |  |  |
| IT资产管理 |  |  |  |  |  |  |
| 基线信息 | 基线信息查看 | 检查对象 | Windows server 2008 R2 | 系统信息 | 刘孝 | OK |
| Redhat（cent os 7、cent os6.7） | 系统信息 | 汪海波 | 存在bug |
| oracle | 汪海波 | OK |
| mysql | 汪海波 | OK |
| tomcat | 汪海波 | OK |
| nginx | 汪海波 | OK |
| 漏洞库管理 |  |  |  |  | 刘孝 | OK |
| 漏扫设备管理 | 设备管理 | 添加设备 |  |  |  |  |
| 搜索 |  |  |  |
| 任务管理 | 添加 |  |  |  |
| 启动 |  |  |  |
| 删除 |  |  |  |
| 刷新表 |  |  |  |
| 结果导出 |  |  |  |
| 搜索 |  |  |  |
| 刷新 |  |  |  |
| HIDS日志管理 | 用户会话日志 |  |  |  | 胡恩平 | OK |
| 文件检测日志 |  |  |  | 胡恩平 | OK |
| 软件包变更日志 |  |  |  | 胡恩平 | OK |
| 恶意软件检测日志 |  |  |  | 胡恩平 | OK |
| 监控与分析日志 |  |  |  | 胡恩平 | OK |
| 用户审计日志 |  |  |  | 胡恩平 | OK |
| Agent配置 | 告警邮件配置 |  |  |  | 刘孝 | OK |
| 文件完整性配置 |  |  |  | 胡恩平 | 存在bug |
| 代理告警配置 |  |  |  | 汪海波 | OK |
| 用户黑名单告警 |  |  |  | 胡恩平 | 存在bug |
| Agent守护 |  |  |  | 胡恩平 | OK |
| Hids可视化 | HIDS图表 |  |  |  | 胡恩平 | OK |
| Kibana |  |  |  | 胡恩平 | OK |
| PCI-DSS |  |  |  | 胡恩平 | OK |
| 报表导出 |  |  |  | 胡恩平 | OK |
| HIDS漏扫管理 | 本地漏洞扫描 |  |  |  | 汪海波 | OK |
| HIDS漏扫结果 | 选择查看agent |  |  | 汪海波 | OK |

# 缺陷分析

## BUG记录（共4个）

**一级bug：0个**

**二级bug：2个**

**1.**  [文件完整性配置下，配置路径框和注册表配置框，输入超多检测行数时，保存报错，但是没有相应的限制说明和提示；](http://192.168.50.196/zentao/bug-view-3486.html)

**2.** [用户登录告警名单中，添加告警名单，没有对输入框进行特殊符号限制，空格和代码"</br>"可以被保存和编译](http://192.168.50.196/zentao/bug-view-3474.html)**；**

**三级bug：2个**

1. [linux基线采集 是否启用Syslog日志 获取到数据显示不达标](http://192.168.50.196/zentao/bug-view-3500.html)；

**2.**  [linux基线采集 是否记录行为日志 获取到数据显示不达标](http://192.168.50.196/zentao/bug-view-3499.html)；

## 版本遗留问题

测试后发现：

1.[用户管理 admin用户可以同源ip登录](http://192.168.50.196/zentao/bug-view-3247.html)（延期处理）

2.[用户管理 普通用户在登录后被删除不会强制退出，还可以操作](http://192.168.50.196/zentao/bug-view-3246.html)（延期处理）

# 新增及变动

新增

暂无

变更

暂无

# 测试结论

本轮测试用时2天，共发现bug4个，与上期相比bug数明显减少，且bug优先级和严重程度不高；hids模块的bug不影响功能使用，且预计下个版本将不会存在影响功能使用的bug，1.1.6版本中功能完全可用，达到交付预期标准。

本轮测试结束，以上测试发现和结论，请相关人员查看！