附件:

网络安全等级保护测评服务技术需求

一、网络安全等级保护测评服务

（一）测评对象

等级保护范围参考《信息安全技术 网络安全等级保护定级指南》，结合保山市中医医院实际网络及信息系统现状进行判定，本次测评系统对象如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 系统定级 |
| 1 | HIS系统 | 三级 |

（二）测评依据

《中华人民共和国网络安全法》

《信息安全等级保护管理办法》

《信息安全技术 网络安全等级保护定级指南》

《信息安全技术 网络安全等级保护基本要求》

《信息安全技术 网络安全等级保护测评要求》

《信息安全技术 网络安全等级保护测评过程指南》

（三）三级系统测评指标

依据《信息安全技术 网络安全等级保护基本要求》，本次保山市中医医院等级测评的指标如下：

| 安全要求 | 安全分类 | 安全子类 | 测评项数 | 备注 |
| --- | --- | --- | --- | --- |
| 安全通用要求 | 安全物理环境 | 物理位置的选择 | 2 |  |
| 物理访问控制 | 1 |  |
| 防盗窃和防破坏 | 2 |  |
| 防雷击 | 1 |  |
| 防火 | 2 |  |
| 防水和防潮 | 2 |  |
| 防静电 | 1 |  |
| 温湿度控制 | 1 |  |
| 电力供应 | 2 |  |
| 电磁防护 | 1 |  |
| 安全通信网络 | 网络架构 | 2 |  |
| 通信传输 | 1 |  |
| 可信验证 | 1 |  |
| 安全区域边界 | 边界防护 | 1 |  |
| 访问控制 | 4 |  |
| 入侵防范 | 1 |  |
| 恶意代码防范 | 1 |  |
| 安全审计 | 3 |  |
| 可信验证 | 1 |  |
| 安全计算环境 | 身份鉴别 | 3 | 实际测评项数根据测评对象数量确定，每个测评对象有23个测评项。 |
| 访问控制 | 4 |
| 安全审计 | 3 |
| 入侵防范 | 5 |
| 恶意代码防范 | 1 |
| 可信验证 | 1 |
| 数据完整性 | 1 |
| 数据备份恢复 | 2 |
| 剩余信息保护 | 1 |
| 个人信息保护 | 2 |
| 安全管理中心 | 系统管理 | 2 |  |
| 审计管理 | 2 |  |
| 安全管理制度 | 安全策略 | 1 |  |
| 管理制度 | 2 |  |
| 制定和发布 | 2 |  |
| 评审和修订 | 1 |  |
| 安全管理机构 | 岗位设置 | 2 |  |
| 人员配备 | 1 |  |
| 授权和审批 | 2 |  |
| 沟通和合作 | 3 |  |
| 审核和检查 | 1 |  |
| 安全管理人员 | 人员录用 | 2 |  |
| 人员离岗 | 1 |  |
| 安全意识教育和培训 | 1 |  |
| 外部人员访问管理 | 3 |  |
| 安全建设管理 | 定级和备案 | 4 |  |
| 安全方案设计 | 3 |  |
| 产品采购和使用 | 2 |  |
| 自行软件开发 | 2 |  |
| 外包软件开发 | 2 |  |
| 工程实施 | 2 |  |
| 测试验收 | 2 |  |
| 系统交付 | 3 |  |
| 等级测评 | 3 |  |
| 服务供应商选择 | 2 |  |
| 安全运维管理 | 环境管理 | 3 |  |
| 资产管理 | 1 |  |
| 介质管理 | 2 |  |
| 设备维护管理 | 2 |  |
| 漏洞和风险管理 | 1 |  |
| 网络和系统安全管理 | 5 |  |
| 恶意代码防范管理 | 3 |  |
| 配置管理 | 1 |  |
| 密码管理 | 2 |  |
| 变更管理 | 1 |  |
| 备份与恢复管理 | 3 |  |
| 安全事件处置 | 3 |  |
| 应急预案管理 | 2 |  |
| 外包运维管理 | 2 |  |

（四）测评方式

本次保山市中医医院等级测评实施严格遵循《信息安全技术 网络安全等级保护测评要求》，将综合采用访谈、检查和测试三类测评方式。

1．访谈

访谈是指测评人员通过与被测系统有关人员（个人/群体）进行交流、询问等活动，获取证据以证明信息系统安全保护措施是否有效的一类方法。本次等级测评采取访谈方式涉及对象为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理等方面内容。其中安全物理环境、安全管理重点采取访谈方式。在访谈的广度上，访谈覆盖不同类型的系统管理人员，包括系统负责人、机房管理员、系统管理员、网络管理员、开发人员、应用业务人员、文档管理员等；在访谈的深度上，访谈包含通用和高级的问题以及一些有难度和探索性的问题。

2．检查

检查是指测评人员通过对评估对象进行观察、查验、分析等活动，获取证据以证明信息系统安全保护措施是否有效的一类方法。本次测评采取检查方式主要涉及对象为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面的内容。检查又可细分为配置检查、文档审查及实地查看三种方式。

A.配置检查

利用上机验证的方式检查服务器操作系统、数据库、网络设备、安全设备、应用系统的配置是否正确，测评其实施的正确性、有效性及完整性。

B.文档审查

检查制度、策略、操作规程、制度执行情况记录等文档（包括安全方针文件、安全管理制度、安全管理的执行过程文档、系统设计方案、网络设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文档、机房建设相关资料、机房出入记录等过程记录文档）的完整性，以及这些文件之间的内部一致性。

C.实地查看

通过实地的观察网络安全技术设施部署情况、关键网络节点连接情况、机房物理环境、办公环境等方面的安全情况，评估相关安全措施是否达到了相应等级的安全要求。

3．测试

测试是指评估人员使用预定的方法/工具使评估对象产生特定的行为，通过查看、分析这些行为的结果，获取证据以证明信息系统安全保护措施是否有效的一类方法。测试又可细分为漏洞扫描及案例验证测试。

A.漏洞扫描

通过漏洞扫描工具对操作系统、数据库及WEB应用系统等进行脆弱性探测，定位目标系统存在的安全漏洞。

B.案例验证测试

通过人工的方式对安全策略、应用系统安全功能、安全漏洞等进行验证性测试。

（五）检查工具

通过漏洞扫描服务工具，结合人工分析实现的方式对网络设备、安全设备、服务器、业务系统、数据库、终端进行资产测绘分析及漏洞扫描。

漏洞扫描服务工具需具备以下功能（单台设备，需分别提供截图证明）：

1．任务扫描：支持自定义添加规则，支持资产扫描、资产及漏洞扫描两种任务类型；支持Treck协议栈指纹检测、域名解析扫描；任务支持暂停、删除；支持查看本任务的资产数据、漏洞数据；支持针对本任务设置扫描参数，如扫描速率、协议并发数等。

2．可指定资产范围进行漏洞专扫：可选定自定义资产范围及自定义漏洞POC进行漏洞专扫扫描; 针对已扫描出来的资产，罗列出每个POC可能影响和可扫描的单位资产。支持对存在APT组织使用过的漏洞进行识别并标记。

3．风险识别：系统通过规则识别对资产存在可疑风险（木马后门、集成工具、远程运维）的风险详情进行识别统计，并展示在报告中。

4．协议识别数：支持300种以上的主流协议识别，包括但不限于如下协议：ancp(6068)、bitcoin(8333)、ceph(1311|1302|1314)、dgraph\_grpc(5080|7080|9080)、hikvision(8000)、git(9418)。

5．端口识别数：识别资产目标开放的端口不少于700种，包括:23（crestron-ctp，telnetOld，ztelnet）、113（isakmp，isakmp-udp，identd）、2628（dictionary）、6001（x11，ncacn\_http，jt808，http，acti-control）等特殊端口的识别。

6．识别规则数目和POC数量：总规则集数量超过350000条，系统POC数量超过4200条。

（六）测评结果输出

《网络安全等级保护测评报告》

（七）项目服务人员要求

测评机构派遣参与项目组的成员至少3人，派遣的服务人员须已取得网络安全层面的资格认证证书，其中，担任本项目的项目经理人员需同时具备信息系统项目管理师（高级）证书和CIIP-I、CISP、CISSP、网络安全等级测评师（高级）证书；派遣项目组成员须有cisp、网络安全等级保护测评师证书，项目人员需要提供不少于6个月的社保缴纳证明（需体现参保时间、身份证号码、参保机构等）。