附件：

**南山区医疗集团总部**

**安全评估系统项目需求**

# 项目背景

随着互联网的快速发展，各企事业单位加快了企业信息化建设的脚步，大量的网络设备、安全设备、各类应用系统及其服务器在各企事业单位得到了广泛应用，支撑业务运行的信息系统已经变得越来越重要，甚至已经已广泛地融合于社会和国民经济的各个领域。国内网络攻击行为呈现出多元化、常态化的特点。用户业务呈现多样化，资产基础信息很难梳理，各类设备的不合规配置、弱口令、XSS、溢出攻击等漏洞容易被黑客利用，对网络造成严重后果无从知晓。

当前网络信息安全形势极其严峻，甚至危机了国家安全。随着《中华人民共和国网络安全法》的颁布实施，以等保为基础对各政企单位提出了网络层面的保障要求：各企业应采取监测、记录网络运行状态、网络安全事件的技术措施，不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施。尤其关注关键基础设施的安全问题，以及来自互联网的重大突发事件。

面对当前极其严峻的网络安全形势，以及来自各地网信、公安、工信等国家监管单位和各行业监管单位重重检查和处罚的压力。因此，在保证网络业务资产的安全、可靠、持续的运行的同时，具备发现信息系统存在的安全风险状态和处置的能力建设势在必行。

# 项目周期

项目建设周期为60天。

# 项目需求

## 合规需求分析

* **《中华人民共和国网络安全法》（2017年6月1日施行）**

第21条 国家实行网络安全等级保护制度。

第38条 关键信息基础设施运营者应当自行或者委托第三方供应商对其网络的安全性和可能存在的风险每年至少进行一次检测评估；

* **《网络安全等级保护制度》**

漏洞和风险管理（G1/G2/G3/G4）章节

明确提出“应采取必要的措施识别安全漏洞和隐患，对发现的安全龙洞和隐患及时进行修补火评估可能影响后进行修补”

## 业务需求分析

基于网络现状的分析，业务需求如下所示：

* 风险发现：能够发现网络中存在的资产信息，能够发现资产存在的安全漏洞、不合规配置检查、弱口令等风险
* 事件处置：能够针对已知和未知的资产风险提供闭环处置手段
* 安全运维：需具备自动化数据分析，减少运维工作量
* 满足合规：满足国家、监管、行业对政企用户漏洞风险的建设要求
* 事件追溯：漏洞安全事件发生后，需快速追踪风险责任人
* 简单易用：需求适配已有的第三平台接入方便操作

# 技术分析

以攻击为视角，通过摸清家底、漏洞检测、修复指导为技术路线。通过梳理资产，形成清晰的资产池，然后对资产进行全面风险检查，进而找出易被攻击的资产或企业安全建设中的攻击突破口，进行安全加固和修复后，再进行复测，确保攻击突破口完全修复。



理清资产：明确要保护的对象及相关信息，便于资产风险检查的全覆盖和风险资产的追踪查询。

查找攻击突破口：从基线和资产两方面，进行全面盘查，快速定位易被攻击的资产或企业安全建设中的攻击突破口，进而模拟攻击者对防护措施进行检验。

快速精准检测易利用的高危害漏洞：尤其是命令执行等权限相关漏洞和弱口令系列容易泄露数据信息的漏洞。

及时响应漏洞信息情报：漏洞情报信息的及时预警和响应，可以很好地帮助防守方抢占先机检测并解决问题，提前做好防范工作。

# 建设内容

本次安全评估系统安全建设主要目的利用安全评估设备专业的漏洞扫描技术，及时发现服务器、网络设备、数据库、中间件等资产中可能存在的漏洞风险，并进行针对性的修复，保证网络业务资产的安全、可靠、持续的运行。

# 方案设计

## 部署拓扑



## 系统功能实现

### 资产信息发现

具备主机服务、综合Web探测和被动探测引擎，提供主机系统、Web应用和域名的多维度资产信息发现功能，能够又快又全的获取目标资产的全部信息，避免因资产信息掌握不全而导致的脆弱点遗漏。

### 主机服务探测

具备自主研发的主机服务探测引擎，提供快速便捷的主机服务资产探测功能，用户仅需输入目标IP范围即可快速实现主机服务资产信息的准确采集。用户可自定义端口探测组，便于常用服务的快速探测，依托系统内置的指纹库，实现准确快速的主机服务资产识别。主机服务探测功能还提供域名反解析功能，辅助用户对主机服务资产和Web资产进行关联分析。

### 综合Web探测

具备综合Web探测引擎，以应对复杂多样的Web应用架构。能够根据目标URL对页面进行识别分析，根据页面类型选取普通爬虫或浏览器爬虫，力求全面采集目标站点的页面信息，特别是针对Web2.0的单页面应用，浏览器爬虫会模拟真实浏览器的本地渲染和解析过程，确保Web站点信息采集的全面和准确性。用户可自定义请求方式和URL关键字，避免爬虫爬取过程对数据的误操作。

综合Web探测引擎支持多种登录方式，包括Http基础认证、Cookie/Session认证、token认证和证书认证等，实现Web应用的登录扫描。

### 验证式漏洞发现

具备验证式漏洞检测技术，通过内置漏洞扫描插件，模拟真实攻击行为，发送攻击载荷，根据分析发送和返回数据内容，智能判断是否存在漏洞。相较于传统漏洞特征匹配的猜测式检测技术，验证式漏洞检测技术具有准确性高，误报率低的优势。

|  |  |
| --- | --- |
| 插件类型 | 支持检测的漏洞种类 |
| 主机服务漏洞检测插件 | 操作系统、系统服务、数据库服务等开源和商用软件的不安全配置、未授权访问、后门、信息泄露等 |
| 网络设备漏洞检测插件 | 常见交换机、防火墙、VPN、邮件网关等设备的命令注入、未授权访问、不安全配置等 |
| 通用Web应用漏洞检测插件 | SQL注入、CSRF、CRFL注入、命令注入、XXE、SSRF、XSS、文件上传、服务器错误信息、敏感信息泄露、表单弱口令、不安全的HTTP配置、路径穿越、任意跳转等 |
| 常见Web组件检测插件 | Apache、IIS、JBoss、WordPress等常用组件的不安全配置、注入、未授权访问、权限绕过等 |

扫描插件可覆盖Web和主机常见漏洞类型，根据目标资产的响应信息自动调整参数，扫描结果中能详细阐述漏洞位置、危害和利用方式，在不影响业务正常运行前提下，精准报告漏洞信息。

### 友好的扫描报告

需杜绝以往猜测式扫描器报告中，问题描述看不懂、结果无法验证，甚至使用通用安全开发、运维管理建议作为每个报告的安全建议。

需提供友好度很高的报告展示系统，支持以任务、漏洞、资产维度独立生成各类报告，针对目标系统的安全评级、资产信息统计、漏洞分类与统计进行直观展示。

扫描报告中漏洞描述内容包括以下维度：

|  |  |
| --- | --- |
| 漏洞描述 | 说明 |
| 编号 | 漏洞在公开漏洞库中的编号 |
| 描述 | 1. 漏洞类型及其原理性描述
2. 漏洞存在的URL路径
3. 漏洞存在的参数未知
 |
| 危害 | 攻击者可利用该漏洞实现哪些操作 |
| 验证方式 | 提供PoC代码和验证方式指导，用户可手动验证 |
| 利用方式 | 指导构造攻击载荷的代码，用户可实际利用漏洞 |
| 修复方式 | 穷举出可以修正该漏洞的方法，包括但不限于：调整设计、修改代码、部署防护设备等 |

### 全开放的功能接口

提供全功能的调用接口，用户可通过SoC、SIEM等平台实现对安全评估工具的调用，实时将扫描结果对接至资产、漏洞数据平台，也可通过工单系统实现安全处置调度。

# 效益分析

通过部署安全评估系统，定期对网络资产进行自动化高效率的扫描，将网络资产的各类型安全漏洞进行统一展示，及时了解当前内部及外部资产的安全状态和告警事件，为用户的网络资产安全提供有力支撑,具体如下：

1. 定期的资产漏洞检测，及时发现当前网络资产存在的问题；
2. 准确识别被扫描对象的资产信息，如操作系统、服务端口开放情况、域名资产情况等资产的发现与资产管理；
3. 全面的走出安全分析报告，直观展示被扫描对象的整体风险等级、资产发现情况；
4. 漏洞提供详细的验证利用方式及修补建议，辅助安全管理员了解漏洞情况，快速修复漏洞；
5. 对于国家或行业监管单位所提出的安全规范合规性要求得以满足，避免日后产生不必要的麻烦。
6. 重大漏洞24小时响应：扫描引擎和漏洞插件由通过安全厂商安全研究团队提供更新维护。遇到突发重大安全漏洞事件时，由安全厂商24小时内响应并提供检测插件，确保第一时间掌握漏洞影响范围，及时制定和执行修复计划。

# 安全评估系统清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 数量 | 单位 | 备注 |
| 1 | 安全评估系统 | 1 | 套 | 支持主机漏洞扫描、web漏洞扫描、基线合规检查。支持并发扫描任务数≥30，IP、域名扫描数量无限制单任务最大扫描目标数：一个IPB段web单任务最大目标数不低于80个支持集群部署  |