概要设计

# 1 引言

## 编写目的

随着计算机技术、网络技术的飞速发展和普及应用，网络安全已日渐成为人们关注的焦点问题之一。安全扫描是增强系统安全性的重要措施之一，它能有效地预先评估和分析系统中的安全问题。弱口令检测是用来自动检测远程或本地主机的服务漏洞。漏洞扫描是指通过网络远程检测目标和主机系统漏洞的程序，它对网络系统和设备进行安全漏洞检测和分析，从而发现可能被非法入侵者非法利用的漏洞。

因此，一个在线弱口令检测工具就变得至关重要。

## 1.2 背景

账号口令安全是保障各类设备安全的至关重要的基础，但长期以来，弱口令一直作为电信企业常见的高风险安全问题存在。弱口令是指容易被破解的口令，如123456等。长期以来，弱口令一直作为各种安全检查、风险评估报告中最常见的高风险安全问题存在，成为攻击者控制系统的主要途径，很多安全防护体系是基于密码的，口令被破解在某种意义上来讲意味着其安全体系的全面崩溃。

那我们的项目——**搜查令**，便应运而生。

## 1.3 定义

**弱口令**：容易被别人猜测到或者被破解工具破解的口令。

**口令字典**：用来破解账户口令的一个工具。

**暴力破解**：用穷举法来计算，也就是说从键盘上的字母数字一个一个的试，直到找到正确的密码。

# 2 总体设计

## 2.1运行环境

项目支持32位及以上电脑使用，支持IE6及以上浏览器使用。

## 2.2 基本设计概念与处理流程

### 2.2.1基本设计概念

集中弱口令系统的整体服务体系架构分为Web端、采集探针、分析服务器3部分，如图2-1所示，支持各种客户端接入，通过采集探针支持多个网络接入，并在后台破解分析服务器上基于负载均衡机制进行分布式弱口令破解分析。

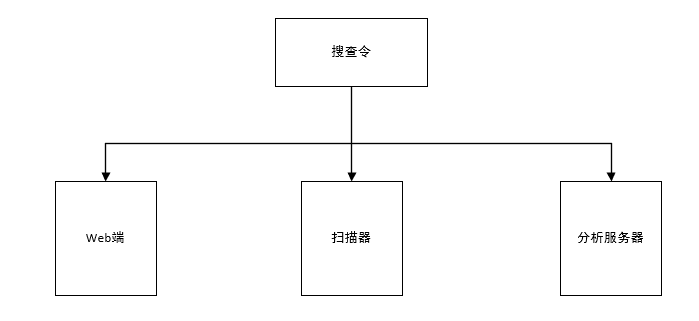


图2-1 整体服务体系架构

系统功能架构如图2-2所示，采集层通过手工获取密码文件，或通过4A系统获取各设备的帐号权限，自动登录设备将密码文件采集到集中分析服务器，分析层则通过字典库进行弱口令比对分析，在展示层展现弱口令数量、分布、排名和趋势，在业务层对字典库、脚本等进行管理。

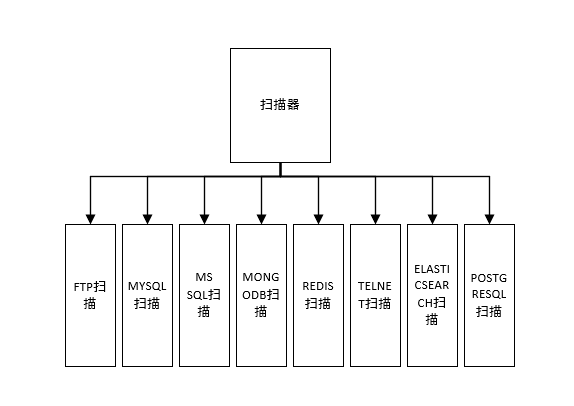


图2-2  系统功能架构

## 2.4 基本需求与程序的关系

集中弱口令检查系统是为实现对通信运营商全网所有网元中的所有帐号口令强度的高效、全面、准确、及时掌控，整合现有安全技术手段，引入和优化现有口令检查工具的方法，从而实现大规模口令的常态化检查，支持完全不影响业务系统正常运行的、以在线或者离线获取各网元口令文件、后台集中破解为主要特征的“无损探伤”模式弱口令核查功能，支持集中核查各类在网主机、数据库、网络设备、应用系统的弱口令核查功能，以实现全面掌控在网设备口令设置情况的目的。主要有4个方面需求。   
　　①建设符合企业和运维特点的弱口令字典：自动或手工搜集全网各类主机、网络设备、应用、数据库等网元常见出厂缺省配置、基于维护习惯选择等导致的弱口令，结合互联网上典型的字典库，形成具备企业特有的弱口令字典。   
　　②密码密文（口令文件）采集：通过4a（即集中账号口令管理系统）提供的连接网元的网络通道，采集各类主机、网络设备、防火墙、数据库、的口令文件，支持在线直连网元采集、人工方式导入的离线采集两种方式。   
　　③弱口令分析：针对不同类型设备的口令文件，采用对应的破解引擎和弱口令字典库，通过匹配的方式逐一尝试破解各个帐号的口令，发现其中的弱口令进行对比。   
　　④弱口令分布统计：对全网弱口令现状进行分析，分公司、部门、系统、设备各个维度，得出各弱口令数量、比例、排名和变化趋势。

## 2.5 尚未解决的问题

1. 目前程序只是一个脚本程序，还未搭建好网络端。
2. 扫描结果还不能以图标的形式直观地呈现出来。
3. 还未实现定时扫描的功能。