项目介绍

# 项目背景

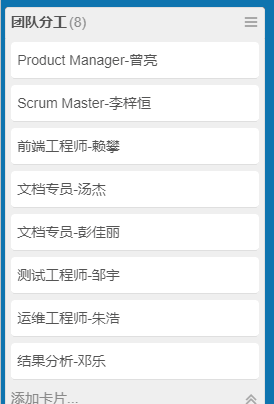
随着计算机技术、网络技术的飞速发展和普及应用，网络安全已日渐成为人们关注的焦点问题之一。安全扫描是增强系统安全性的重要措施之一，它能有效地预先评估和分析系统中的安全问题。弱口令检测是用来自动检测远程或本地主机的服务漏洞。漏洞扫描是指通过网络远程检测目标和主机系统漏洞的程序，它对网络系统和设备进行安全漏洞检测和分析，从而发现可能被非法入侵者非法利用的漏洞。

因此，一个在线弱口令检测工具就变得至关重要。

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。

# 团队介绍



# 3 项目

搜查令这个项目是一个在线服务弱口令检测工具，主要是针对某些服务中可能存在的弱口令账户密码等。由于网络管理者的安全意识不强，在设定某项服务的账户密码时过于简单，使得不法人员能够获得系统控制权。

在线服务弱口令检测工具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，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。

在线服务弱口令检测工具主要有几个步骤：

1. 获取到需要扫描的ip。
2. 扫描ip的C段，也就是C端渗透，是当目标服务器的安全性相对配置较严时，很难通过目标服务器本身实现渗透的目的，那么此时可以尝试通过目标服务器IP地址所在的C段地址进行扫描渗透，渗透目标服务器所在局域网环境的其他主机，在获取权限以后，截取网络传输过程中相关的敏感数据信息，如FTP登录信息、远程终端账号连接信息等，进而实现对目标服务器的渗透。
3. 判断是否存活，如果存活，再探测存活ip常见应用服务器。
4. 按照应用服务侦测，主要有以下几种方式：
5. **FTP弱口令检测：**扫描常见用户名，然后列出用户名及密码。
6. **MYSQL弱口令检测：**扫描root用户，然后列出root用户及其密码。
7. **MSSQL弱口令检测：**扫描sa用户，然后列出sa用户及密码。
8. **MONGODB弱口令检测：**尝试未授权登录。
9. **TELNET弱口令检测：** 扫描admin等常见用户名，然后列出用户米国及密码。
10. **REDIS弱口令检测：**尝试未授权登录。
11. **ELASTICSEARCH弱口令检测：**尝试未授权登录。
12. **POSTGRESQL弱口令检测：**扫描postgres用户，然后列出对应的用户名和密码。