1 绪 论

1.1 研究的背景及意义

1.1.1 选题的背景

大数据时代的日益逼近充斥着这个原本安宁和谐的地球村，电子商务的快速兴起严重限制了实体经济的发展。根据 CNNIC 发布的关于我国互联网网络发展统计数据报告显示，到 2019 年 6 月为止，我国拥有上网能力的用户数已经拥有了 8.54 亿人次，相比于去年年底增加了近 2598 万，能够掌握手机上网的人数已经拥有 8.47 亿，相比于去年年底增加了近 2984 万，而从数据中管理员可以看出，拥有上网能力的居民绝大多数都是使用手机上网，占总人数的 99.1%，相比于去年年底增加了近 0.5%，这些网民相对于总人口数占比高达 61.2%，相比于去年年底增加了近 1.6%。与之相应的是，据国家互联网应急中心 2019 年 8 月发布的数据，2019 年上半年，CNCERT 捕获恶意程序的能力和去年相比几乎没有太大的区别，大约能够抓取相关样本有 3200 万之多，每天能自我复制的传播次数平均下来也有大概 998 万次。在 21 世纪大数据时代的环境背景下，互联网和管理员的生活几乎密不可分，管理员的生活被互联网这个新兴的产物所包围。因此无论从可观的统计数据还是个人的直观感受上，互联网已经成为这个时代不可或缺的一员，而在这种时代背景下，保护用户数据的隐私安全就变得格外重要。

网络扫描作为信息安全研究中了解智能终端设备运行状况的一个重要途径，在互联网这个高速发展的新时代，必然是值得管理员花时间去研究和学习的。通过这一途径，管理员可以很方便的获取到网络上一些智能终端设备的特征，如正在运行的操作系统、系统中可能存在的一些安全隐患、未被修复的一些安全漏洞，这些信息可以帮助安全从业人员快速的定位和修复安全隐患及漏洞，减少被不法分子利用的风险和损失，建立起企业与用户之间的信任感，有效的提升系统安全等级，让风险降至最低。

通过对目标主机及网络的扫描，管理员期望获得足够多的可用的信息，使用何种工具、通过何种手段对目标进行实时情报采集变得尤为重要。现有的一些典型的网络扫描器参数过多不易熟记，虽然自身功能很强大，但是对于满足某种特定目的的用户来讲，体积庞大过于臃肿，基于上述原因，本文提出了一种便捷性的开源的网络扫描器。

1.1.2 国内外研究现状

互联网的高速发展深深的影响着人民群众的起居作息，随之而来的安全隐患牵动千万群众的正常生活。为了消除各种可能存在的安全风险，各类安全工具孕育而生，网络扫描即成为一种被用来对网络的安全风险进行评估，确保网络风险降至最低的安全手段。

早期的网络扫描器是专门针对 Unix 操作系统而编写的，现在几乎所有平台都纷纷涌现出了一些网络扫描器。网络扫描器对维护网络的正常秩序和风险评估发挥了巨大的作用。

在国外，目前最受欢迎的扫描器当属 Acunetix 公司的 Acunetix Web Vulnerability Scanner，它为了降低用户的使用难度，开发了面向用户友好型的可视化 GUI 界面，能够帮助安全研究人员去自动扫描应用程序可能存在的安全隐患，帮助用户去自动生成符合用户心理的扫描结果报告，它还可以验证用户信息的可靠性，给可能存在的安全风险提出有针对性建议的解决方案，消除可能存在的安全风险。而 AppScan 和 Acunetix 相比，也是一个重量级的工具，它的主要功能主要是针对开发阶段的测试，主要是在开发的过程中就提供了安全监测，把风险在苗头上就尽可能的根除，等到应用程序推出给用户时，能够给用户最大程度的体验和享受，给用户的正常生活提供了安全型的保障。

在国内，X-Scan 是比较著名的安全漏洞扫描工具，它由安全焦点公司开发，是一款多线程、支持插件的漏洞扫描器。它也是款很牛逼的扫描工具，能够极大的改善国内黑客猖狂的现状，支持多种漏洞的扫描，而像小榕的流光扫描器也是早些年比较经典的网络渗透必备工具。

总的来说，国内的网络扫描器功能相对较为简单，多数偏向于针对某一特定目的而开发的轻量级工具，少有一些重量级的产品。

1.1.3 研究的意义

就目前主流的网络扫描器，大多数采用的是命令行界面，用户使用的门槛相对较高，可视化的图形界面旨在提供给用户一个友好的使用环境，这种用户-界面的体系结构深受广大喜爱。它不需要用户去熟记过多的参数，只需要填入相应的关键信息，通过鼠标点击选择即可完成，大大降低了操作使用的难度。

1.2 系统目标

本设计的最终目标是打造一个具有多种扫描功能的网络扫描器。该扫描器具有以下功能：

(1) 可视化的图形界面，旨在为用户提供友好的使用环境。

(2) 实现一些基本的扫描任务，如读取到目的主机的软硬件信息，开放的端口等等。

(3) 帮助用户去自动生成符合用户心理的扫描结果报告，并将扫描结果以文件的形式展现出了。

其对应的整体层次设计图如图 1-1 所示。

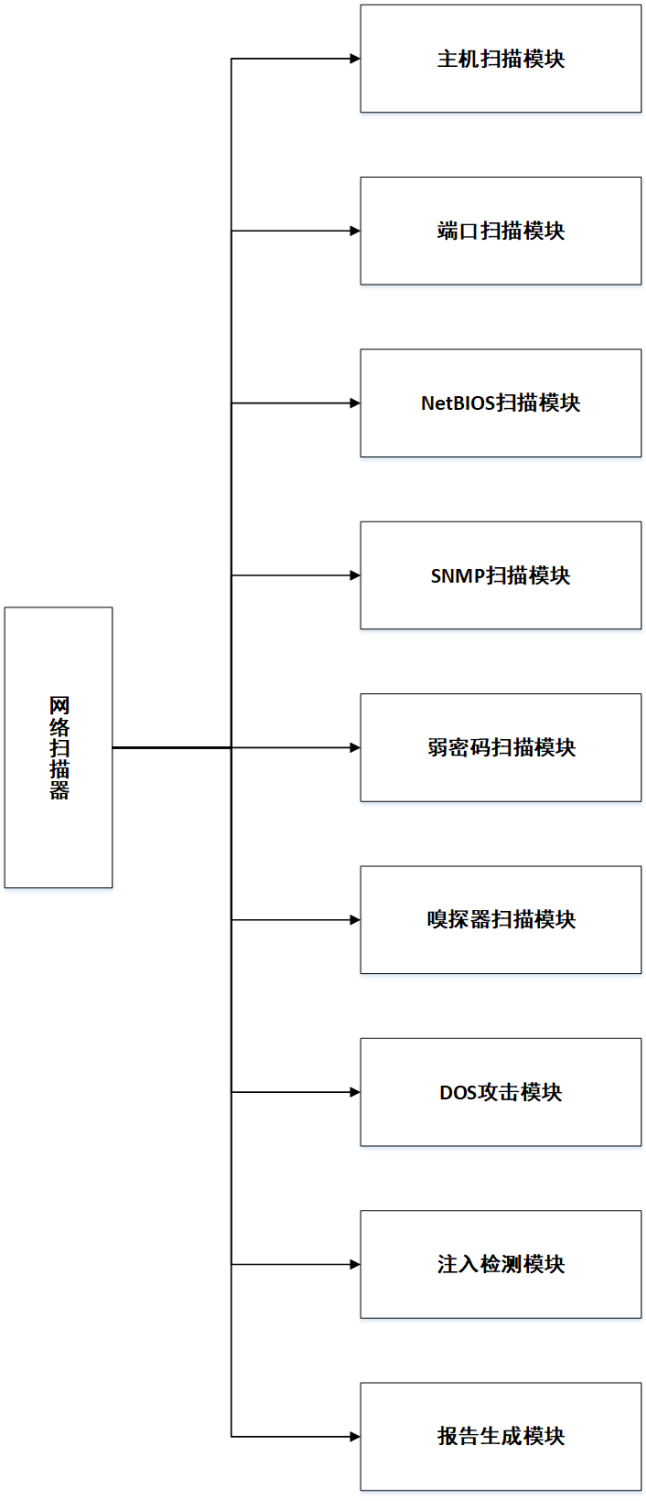


图 1-1 扫描器整体层次设计图

2 网络扫描技术概述

2.1 安全漏洞研究

2.1.1 漏洞描述

漏洞指的是计算机系统在软硬件以及协议的具体相关实现或者系统安全策略上存在的某些缺陷，它一旦被一些攻击者所利用，就可以在未经授权的条件下进行任意的访问，形成强大的安全隐患。世界上没有任何一台智能终端是绝对安全的，也不存在没有漏洞的软件，它们多多少少都可能会存在一些潜在的安全隐患。管理员将针对上述问题去提供一些相关的概念供大家去参考。

一、漏洞的定义

漏洞据文献记载，大概存在三种主流的定义，首先管理员会介绍一下传统的模糊概念的定义方式，其次是目前主流的状态空间的漏洞定义方式，最后管理员将介绍一下访问控制的漏洞定义方式：

(1) 模糊概念

上个世纪九十年代丹尼斯·朗利总和迈克尔·沙恩出版的“数据与计算机安全标准化概念和术语”将漏洞定义为：管理员在对风险进行管理的过程中，可能存在许许多多的安全隐患风险，例如系统存在的某些安全隐患导致未授权用户可能以此为契机读取到了用户的数据信息，未授权用户可能会根据用户的行为特征去实施一些可能存在的有害的攻击行为，造成重大的人生财产损失，而这种风险指标将会是管理员所研究的系统致命的弱点。

(2) 状态空间

马特·毕晓普和大卫·贝利在“漏洞分类法的批判性分析”中指出，对于一个系统中的应用程序而言，它的状态是可以通过系统授权与否的方式去改变的，若存在一个有安全风险的应用程序，它处于系统授权的一种状态，如果存在一种方式使得这个有安全风险的应用程序从授权态跳转到非授权态，它就有可能会威胁到系统的安全，而这种安全隐患的现象就是管理员常说的漏洞。

(3) 访问控制

丹妮在“密码学与数据安全”中提出了一种新的定义方式，他指出了漏洞的产生是由于系统所设置的安全策略不恰当所导致的，而这种安全策略的具体实现是通过对主体对象进行访问控制去管理的，若是系统的某些操作不在安全策略的范畴内，就有可能会出现不合理的访问方式，从而造成安全隐患的出现。

二、漏洞可能产生的原因

漏洞产生的原因有很多，其本质原因还是因为程序员在编写代码的时候对业务理解不够深刻而写出一系列的 bug，导致同组的其他程序员短时间无法定位到相关的业务代码而产生一系列的逻辑漏洞，而从机制上来反观这些安全隐患，大

概可以分为如下 7 类：

(1) 输入验证漏洞

这种漏洞产生的根源在于程序员在编写相关业务逻辑代码的时候未对用户的输入做过多相关的限制，导致一些未授权用户可以通过输入不合法的数据就能访问到一些私密信息，从而导致漏洞的产生，而此类漏洞往往是比较危险的，常出现在各大网站上，对于此类漏洞的修复建议是提供一套规范化的标准去给程序员进行培训，这样就能大大降低此类问题发生的风险。

(2) 访问验证漏洞

这种漏洞产生的根源还是在于程序员在编写相关业务逻辑代码的时候未对用户的输入做过多相关的限制，导致一些未授权用户可以通过输入不合法的数据就能绕过相关的控制权限，从而直达访问到一些私密信息，从而导致漏洞的产生，对于此类漏洞的修复建议是提供一套规范化的标准去给程序员进行培训，这样就能大大降低此类问题发生的风险。

(3) 竞争条件错误

这种漏洞产生的原因在于程序员在编写处理文件相关模块的时候，未考虑到操作系统的一些相关特性，导致系统内线程对 CPU 资源消耗殆尽，使得程序无法正常执行。破坏了进程间的优先级关系，从而导致漏洞的产生，对未授权用户而言，他们可以利用这一特性去对内存进行攻击，以消耗现有资源为代价，从而进行非授权的访问控制，来实现获取到用户的私密信息这一目的。

(4) 意外情况处置漏洞

这种漏洞产生的根源在于程序员在编写相关业务逻辑代码的时候未对异常处理做过多的限制，导致本应该停止运行的程序却无法退出，从而造成进程的死锁，导致操作系统相关程序的崩溃，而这种漏洞的出现可以让非授权的攻击者有机可乘，可以发起 DOS 攻击导致操作系统运行崩溃。

(5) 配置错误

这种漏洞的产生源于程序员在编写相关文件配置信息的时候出现纰漏，未限制非授权用户的访问权限，没有对相关私密数据进行加密操作泄露了相关隐私数据文件的地址，给非授权用户提供了访问的可能性，从而造成用户数据的丢失。

(6) 环境错误

这种漏洞的产生源于程序员在对环境变量配置信息设置的时候出现纰漏，从而导致非授权用户可以执行任意的攻击代码，从而造成用户数据的丢失或者系统的损害。

(7) 设计错误

这种漏洞产生的根源在于软件设计师在对系统设计的过程中未考虑到相关异常处理或者设计逻辑上的过失导致的一些重大漏洞，而程序员在实现这些具体

细节的时候也有可能因为办事不利索导致实现未考虑全面而导致设计上的相关问题。

三、漏洞的特征和属性

只要是人写出来的代码，那必然是存在漏洞的，人往往会用主观思维去判断一些客观事物实现的合理性，从而导致对问题考虑不全面，产生了一系列相关的纰漏，而对于这种纰漏，需要安全研究人员去发现并由相关的工作人员去修复。作为一些已经被安全研究人员发现的漏洞，它的特征十分明显，可以表现在以下几个方面：

(1) 系统内漏洞是客观存在的事物，而对于漏洞本身而言，没有人为因素的存在，它并不会直接的对系统造成任何伤害，而问题在于总是有非法用户会别有用心的去利用这些暴露出来的安全问题去搞破坏，从而导致系统出现巨大的故障，造成无法挽回的损失。

(2) 漏洞是实时出现的，随着系统不断被用户使用，系统可能存在的安全隐患也随着暴露出来，如果厂商不及时修复这些可能存在的安全隐患，就有可能随时被不法分子利用，造成巨大的损失，而即便是对软件进行更新打补丁，也依旧会随着新版本的发布而被发现新的安全隐患，这种安全隐患是长期存在的。

(3) 漏洞存在于各种智能终端设备中，而不同的智能终端设备的不同系统版本可能会存在不太相似的安全隐患，对于非授权用户而言，他们有可能通过执行一系列的操作绕过本该进行授权判断的操作，从而获取相应的管理员权限，从而攻破了所谓的坚不可摧的系统。

对漏洞而言，它的属性值很多，管理员就介绍一些常见的漏洞属性：

1) 对漏洞而言，不同的人有不同的理解方式，对普通用户而言，漏洞的出现似乎对他们影响并不是很大，只要能够正常使用终端设备即可。而对一些非授权用户而言，漏洞的出现对他们来说会产生巨大的金钱的推动效应，他们可以利用这些已获取的权限去读取用户的隐私数据进行倒卖，去换取巨大的金钱效应。

2) 漏洞的危害性因人而异，对普通用户而言，若是存在非授权用户利用这些暴露出来的漏洞去加以利用，可以使得普通用户的智能终端设备变成一台肉鸡，通过控制多台肉鸡对某些大型互联网公司或国家机关单位实行 DDOS 攻击，造成的损失是不可估计的。

3) 漏洞被非授权用户利用的方式很多，普通用户开放了一些敏感的端口比如 3306，就有可能会被非法用户给利用并实行攻击策略，普通用户在网络上随意下载一个需要管理员授权运行的程序，这个程序有可能是非法用户刻意伪造出来的病毒程序，当普通用户通过管理员权限运行这个程序的时候，有可能会被非法用户植入相关的木马，留下了对他们有利的隐藏后门，这样就可以很方便的远程读取相关主机的信息。

4) 而对漏洞而言，不同的环境下暴露出来的安全隐患的风险级别不一定是一样的，非法用户可以利用这一特点进行有针对性的攻击，从而对特定的用户或团体造成巨大的伤害，以换取高昂的报酬。

四、漏洞造成的危害

对漏洞本身而言，它是客观存在的事物，它的出现并不会影响用户正常使用程序，而这些问题被非法用户窃取并加以利用，必然会造成不可估量的经济损失，管理员可以通过以下几个方面来评估可能造成的安全风险：

(1) 系统的完整性

原本完整的系统因为漏洞的出现就有可能变得不那么完整，对于非授权用户而言，他们可以通过拼接语句去读取数据库的隐私信息，通过这些隐私数据去获取更高权限的信息，从而威胁到系统的安全性，造成数据的丢失或损坏。

(2) 系统的可用性

原本正常运行的系统可能会因为漏洞的出现变得不可以使用，对于非授权用户而言，他们可以利用漏洞去影响系统的安全运行，从而造成进程的堵塞，导致重要程序因无法及时处理而崩溃。

(3) 系统的机密性

一个完整的系统都存在许多私密的数据信息，而漏洞的产生可能会使这些原本私密的信息变成公开透明的信息。对于非授权用户而言，他们可以利用这些系统存在的安全隐患去获取相关权限，以此来读取那些私密的数据信息，从而造成用户的信息泄露。

(4) 系统的可控性

原本正常运行的系统可能会因为漏洞的出现变成无法控制，一旦漏洞被非法分子所利用，他们可以肆意破坏系统从而造成系统内进程之间失调，造成系统无法正常运行，对用户和组织来讲都是巨大的损失。

(5) 系统的可靠性

一个正常运行的系统的可靠性是值得管理员商讨的，对用户而言，系统的可靠性越高，就越能满足用户的心理预期，而在这种条件下，系统的可靠性若是受到了动摇，用户对系统的依赖程度和信任感也会随之降低，而不可靠的系统往往容易被非法分子所加以利用，从而造成无法挽回的损失。

2.1.2 漏洞分类

1970 年那会儿，很多人曾对漏洞分类有过许多研究，而许多研究成果已经被部分企业采纳并投入实际生产中，由于漏洞的分类方式很多，一一列举显然已经不太适合现在社会的发展，管理员可以考虑采用现在最主流的分类方式，根据漏洞的安全风险级别和漏洞可能造成的安全隐患等一些方面对漏洞进行相当细致的分类。

一、对系统造成的安全风险

原本正常运行的系统可能会因为漏洞的出现而变得不安全，而这种不安全的因素的直接原因就是因为存在非法用户想通过拼接某些字符串达到非授权的效果，从而获取到用户的隐私权限和数据，而这种漏洞管理员大致可以分为以下几类：

(1) 普通用户访问权限

非法用户通过利用已知的一些漏洞的定位信息，通过编写相关的 exp 去实现用户权限的获取，通过这些非法的访问权限去读取用户的隐私数据，从而导致用户相关信息泄露。

(2) 本地管理员权限

未授权用户利用已知暴露的安全问题去不断地尝试测试，编写相关的 exp 脚本，从而对未授权用户的权限进行提升，将只具有读操作的普通用户权限提升至具有写操作的管理员权限，从而极大的影响了系统的安全性，对系统和用户造成的损失更大。

(3) 远程管理员权限

对于非法用户而言，他们通常只需要以 root 身份去攻击存在安全问题的进程就可以获得远程管理员权限。而这种攻击策略并不需要用户本身的权限，只要通过构造指定的字符串序列，通过执行所构造好的字符串序列代码就可以获取用户的管理员权限。

(4) 权限提升

对于非法用户而言，通过枚举等手段可能相对容易的获取一个普通用户的用户名以及相关的登录密码，可是一般这种普通用户对相关文件的操作只有读取权限，而管理员通过利用已知存在的系统漏洞，管理员可以提升相关的用户权限，从而实现对系统的控制。

(5) 本地拒绝服务

对于非法用户而言，他们可以采取拒绝服务攻击等方式对目标主机发起攻击，从而造成系统资源的过度消耗而导致系统无法正常提供相关的服务，而对非法用户而言，可以加以利用已知的相关漏洞，对用户的进程发起攻击，去不断地消耗系统的资源，从而造成程序崩溃。

(6) 远程拒绝服务

对于非法用户而言，他们可以采取拒绝服务攻击等方式对目标主机发起攻击，从而造成系统资源的过度消耗而导致系统无法正常提供相关的服务。

(7) 读取受限文件

非法用户通过利用已知的一些漏洞的定位信息，通过编写相关的 exp 去实现用户权限的获取，通过这些非法的访问权限去读取未授权的隐私用户数据，从而

导致用户相关信息泄露。

(8) 远程非授权文件读取

非法用户通过利用已知的一些漏洞的定位信息，通过编写相关的 exp 去实现用户权限的获取，通过这些非法的访问权限去远程读取未授权的隐私用户数据。

(9) 口令恢复

非法用户可以通过市面上主流的加密方式去对加密过的用户名以及密码去逐个尝试，以此来获取到相关用户的权限信息，从而非法访问并窃取用户的隐私数据，来对用户进行致命性的打击。

(10) 欺骗

非法用户可以通过伪造相关的用户信息对系统实施欺骗，从而瞒过系统的相关安全检测，从而成功获取到系统的控制权限，达到对系统的完全控制，当然也可以通过诱导用户去主动连接并提供相关的明文信息，从而造成用户权限和隐私的泄露。

(11) 信息泄露

非法用户可以通过互联网搜索引擎去获取到目标系统的相关信息，并对这些已知的信息进行搜集和整合，通过已知系统的漏洞去编写相应的 exp 脚本进行攻击操作，从而获取到相关的权限，造成用户隐私数据的泄露。

二、安全风险级别

漏洞的安全风险级别对不同的公司而言有着不太相似的分类方式，在早期，某些公司曾经对安全风险等级有过十分细致的评估和分析，某些公司考虑将漏洞的安全风险等级分为 3 个级别，某些公司也分为四个五个级别，分的越细说明管理员对漏洞的分类研究工作做的越深入。不过即便是这样，这种分类模式还是存在许多值得注意的问题：

(1) 每个公司都有他们一套的分类标准，这些公司厂商之间没有办法把这种标准进行统一化，形成一套全球化的遵循标准，容易给人造成迷惑性。

(2) 漏洞的分类方式层次不齐，这种如此复杂的分类方式必然会增加分类的难度，漏洞库的内容也随之指数级的扩增。

(3) 不同漏洞之间事实上存在着关联关系，不同的分类方式一定程度上能够帮助管理员找出一些漏洞之间的共性，一定程度上可以帮助管理员分析和判断漏洞的类型，从而给出正确的分类方式，对症下药。

根据上述的分析，管理员大致可以对漏洞的分类得出如下结论：

1) 漏洞应该是个客观独立的个体，对漏洞的分类不能给人造成迷惑性，一个漏洞的出现只应该属于某一类中。

2) 新漏洞的发现要能够适应曾经已经确定好的分类方案，适应能力要强，这样的话漏洞分类的延展性会更好些。

3) 通过已知的漏洞分类去推测未来可能出现的新的漏洞。

2.1.3 安全漏洞库

漏洞库就是把已经被用户发现的可能存在安全隐患的漏洞进行分类，分析这些漏洞的危害性和安全风险等级，然后针对相应的漏洞采取相应的补救措施，以便未来遇到相似的漏洞能够起到更好的预防作用，防止此类相似的安全隐患再次发生。而不同的厂商建立这种安全漏洞库有不同的实施策略，这就导致厂商之间不能相互共享漏洞发现的成果，无法有效的去防止相似漏洞的发生和出现，没有一套统一管理的标准。这里管理员将介绍几种国内外常用的安全漏洞库。

一、国际 CVE 漏洞库

通用漏洞列表 CVE 是安全漏洞库中比较有名的一种，它定义了统一的安全风险评估标准，加强不同数据库之间的数据共享，为每一种存在的安全风险定义了标准化的命名规范，这种命名是唯一存在的，这将意味着这一套标准的适应化程度更高，可以应对未来风险的变化。这一套命名规则是由组委会反复商讨得出来的，一个漏洞想要被该组织收录到官方的安全库中，首先需要经过组委会的评审，确定该漏洞是否应该加入到安全漏洞库中，然后再由官方分配一个索引号，然后编辑审核好加入到官方的数据库中，再通过站点进行公开发布。

由于 CVE 通用漏洞列表的标准化，使得它在业内得到了广泛的认可，很多公司把有 CVE 编号作为公司人才招聘的门槛，以帮助他们更好地筛选人才，很多公司也会模仿 CVE 去建立自己一套的风险评估标准，通过和 CVE 共享数据库内容来完善自己安全漏洞库的缺陷，使企业更具市场竞争力。

二、其他漏洞库

国内很多公司也逐步建立了自己的安全漏洞库，而相比较而言并没有 CVE 做的这么出色，我国在漏洞分类的研究了解的还是太少了，相关方面的研究更是微乎甚微，所以作为全球第二大经济体，管理员需要快速的追赶和发展我国的互联网信息产业链，去逐步跟进和完善管理员自己的安全漏洞库，为适应全球化的发展需求去做出不懈的努力。

下面是管理员国内某些知名企业的安全漏洞库，如表 2-1 所示：

表 2-1 国内知名企业安全漏洞库

https://www.butian.net/	补天漏洞响应平台
https://security.alibaba.com/	阿里安全响应中心
https://security.tencent.com/	腾讯安全应急响应中心
https://www.nsfocus.com.cn/	绿盟科技

2.2 网络扫描技术

2.2.1 网络扫描技术工作原理

管理员站在攻击者的角度去看网络扫描器的工作原理，一切都变得清晰易

懂。作为一个攻击者，管理员会考虑首先去搜索网络上存活的主机，选择其中某一些主机作为管理员攻击的目标，管理员再通过向目标主机发送数据包，通过分析反馈的数据包，寻找可能存在的安全隐患，通过利用这些安全隐患去模拟尝试攻击，找到修复该安全隐患的解决方案，从而达到修复漏洞的目的。网络扫描器的工作原理如图 2-1 所示：

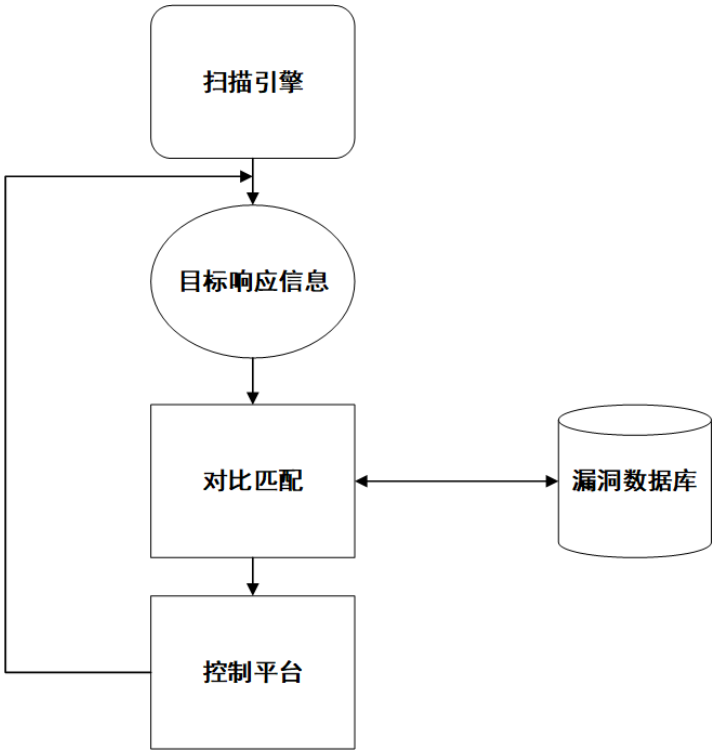


图 2-1 网络扫描器工作原理

网络扫描器应当具有如下特点：

(1) 判断主机是否存活，并读取响应存活的主机信息。

(2) 快速的扫描目标主机开放的可能会引发漏洞的端口号，并根据搜索引擎提供的相关分析做出准确的漏洞判断，然后提供可以去完善的修复方案。

2.2.2 网络扫描的主要技术

网络扫描主要是针对可能存在的安全风险进行逐一排查检测，对现阶段系统运行的状态进行实时监测，方便及时的对现阶段网络运行状况做一个准确的判断，降低安全风险等级，很多漏洞的产生源于程序员在编写相关文件配置信息的时候出现纰漏，未限制非授权用户的访问权限，没有对相关私密数据进行加密操作泄露了相关隐私数据文件的地址，给非授权用户提供了访问的可能性，从而造成用户数据的丢失。管理员可以通过模拟非授权用户的攻击策略去加固系统，从而大大降低安全风险的发生，而随着信息技术的日益复杂化，管理员很难凭借主观去应对各类安全漏洞的变种，管理员需要做的就是建立一个可预测的安全风险的模型，通过这个安全风险的模型去推测未来漏洞可能出现的变种，在漏洞暴露出来之前尽可能的修复掉，这样也给用户和企业带来一份安心和放心。

3 总体设计

3.1 运行环境

一、硬件支持：

处理器：酷睿 i5-7300 或以上。

内存：8G 或以上。

网络：100M 或以上。

二、软件支持

操作系统：Windows 7。

开发工具：Microsoft Visual C++6.0，Notepad++。

开发语言：C/C++， MFC。

3.2 模块结构

3.2.1 主机扫描模块

顾名思义，主机扫描就是扫描网络中可能存在的主机，主要是通过向特定的主机或者目的 IP 发送构造的 ICMP 协议包来确定目标网络上的主机是否可达。其流程图如图 3-1 所示。

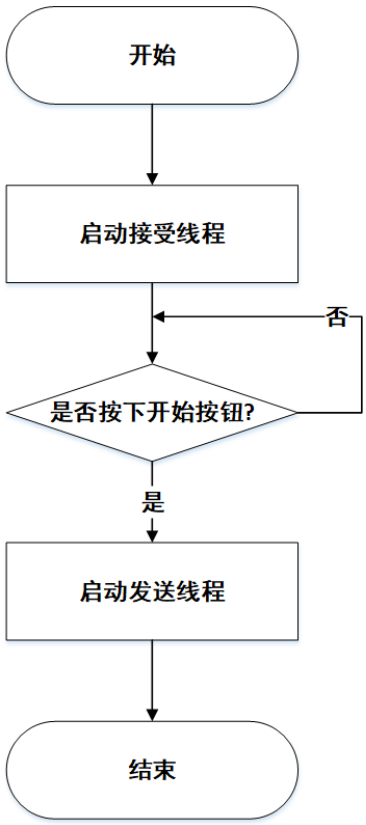


图 3-1 主机扫描模块流程图

3.2.2 端口扫描模块

对某一 IP 段目标主机 IP 的一段端口逐个连接，通过发送数据包对目标主机

进行通信，根据反馈回来的数据包信息判断该主机的开放状态，根据其开放端口所对应的主机服务去有针对性的发起相关的服务缺陷攻击。其流程图如图 3-2 所示：

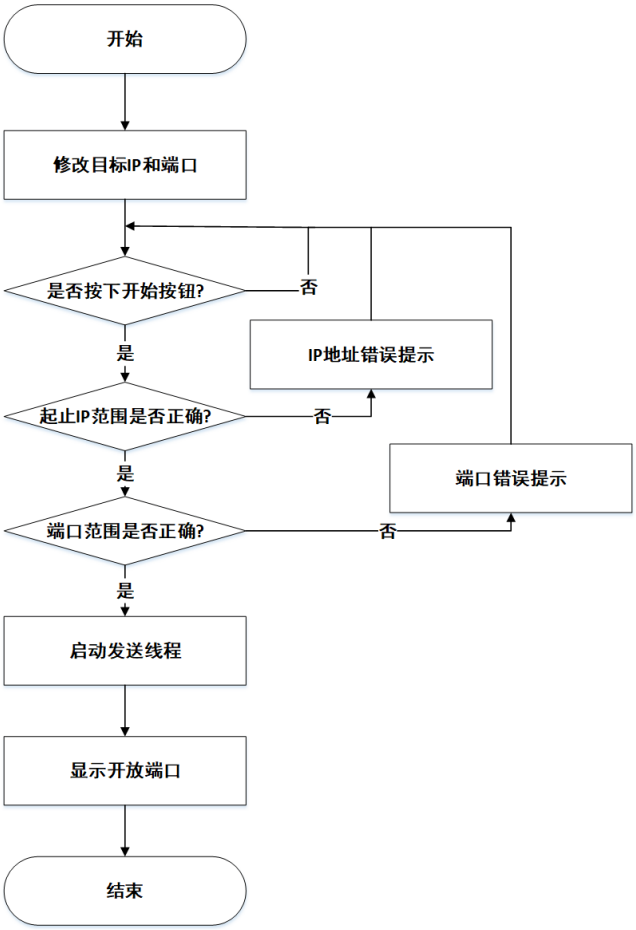


图 3-2 端口扫描模块流程图

3.2.3 NetBIOS 扫描模块

对网上基本输入输出系统 NetBIOS 协议而言，它作为应用层上的一种特殊的协议，它常常被用来管理局域网上的主机，通过该协议的相关约定，管理员可以很方便的读取到局域网上相关目标主机可拥有的相关属性的详细信息。其流程图如图 3-3 所示：

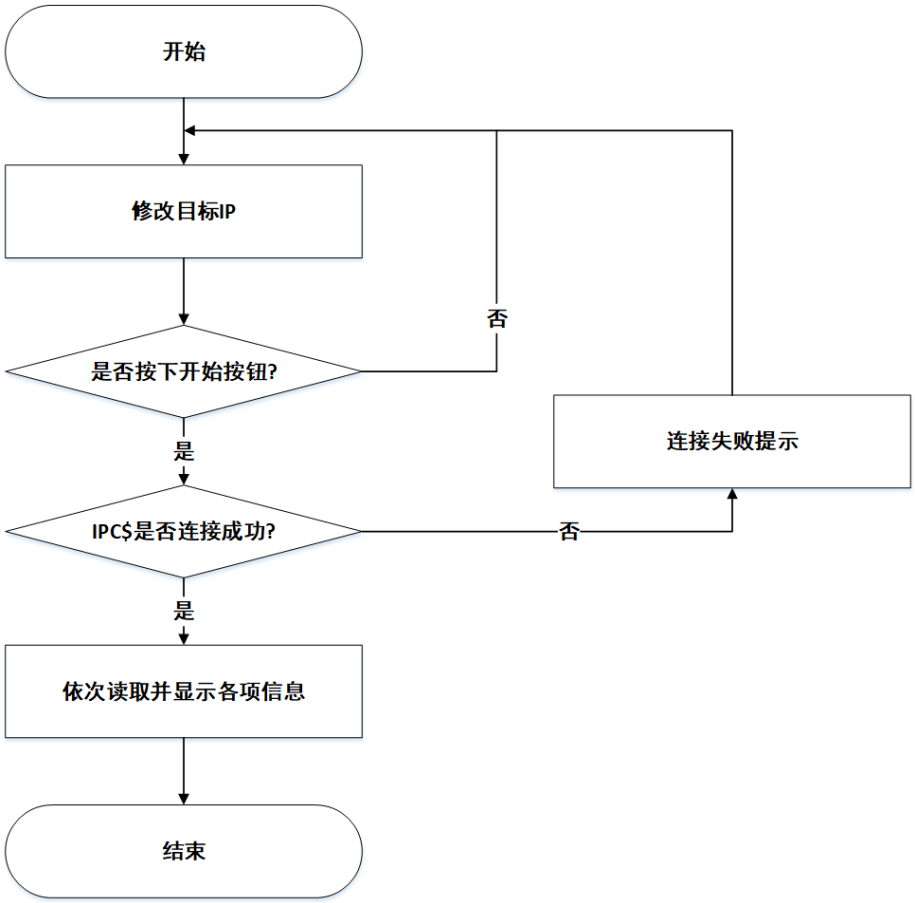


图 3-3 NetBIOS 扫描模块流程图

3.2.4 SNMP 扫描模块

简单网络管理协议 SNMP 是对智能终端设备做简单管理，管理员可以利用该协议的相关约定去获取支持该协议的各种设备的详细的信息。其流程图如图 3-4 所示：

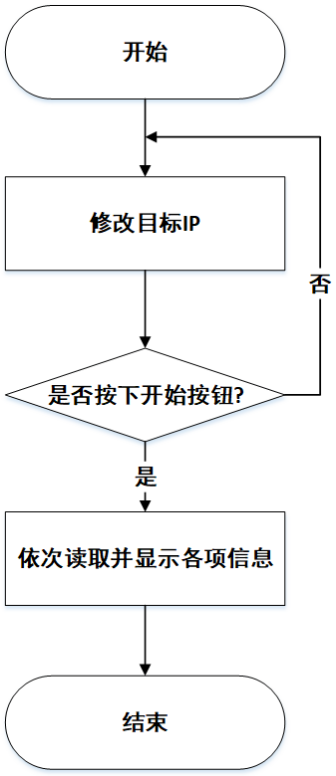


图 3-4 SNMP 扫描模块流程图

3.2.5 弱密码扫描模块

弱密码扫描是逐个对目标主机的用户名和密码进行扫描，依次穷举遍历所有的用户名和密码的组合，用遍历生成的密码去逐次尝试验证。通过密码验证系统给出的正确或错误的反馈来判断是否成功获取到了用户的信息。其流程图如图 3-5 所示：

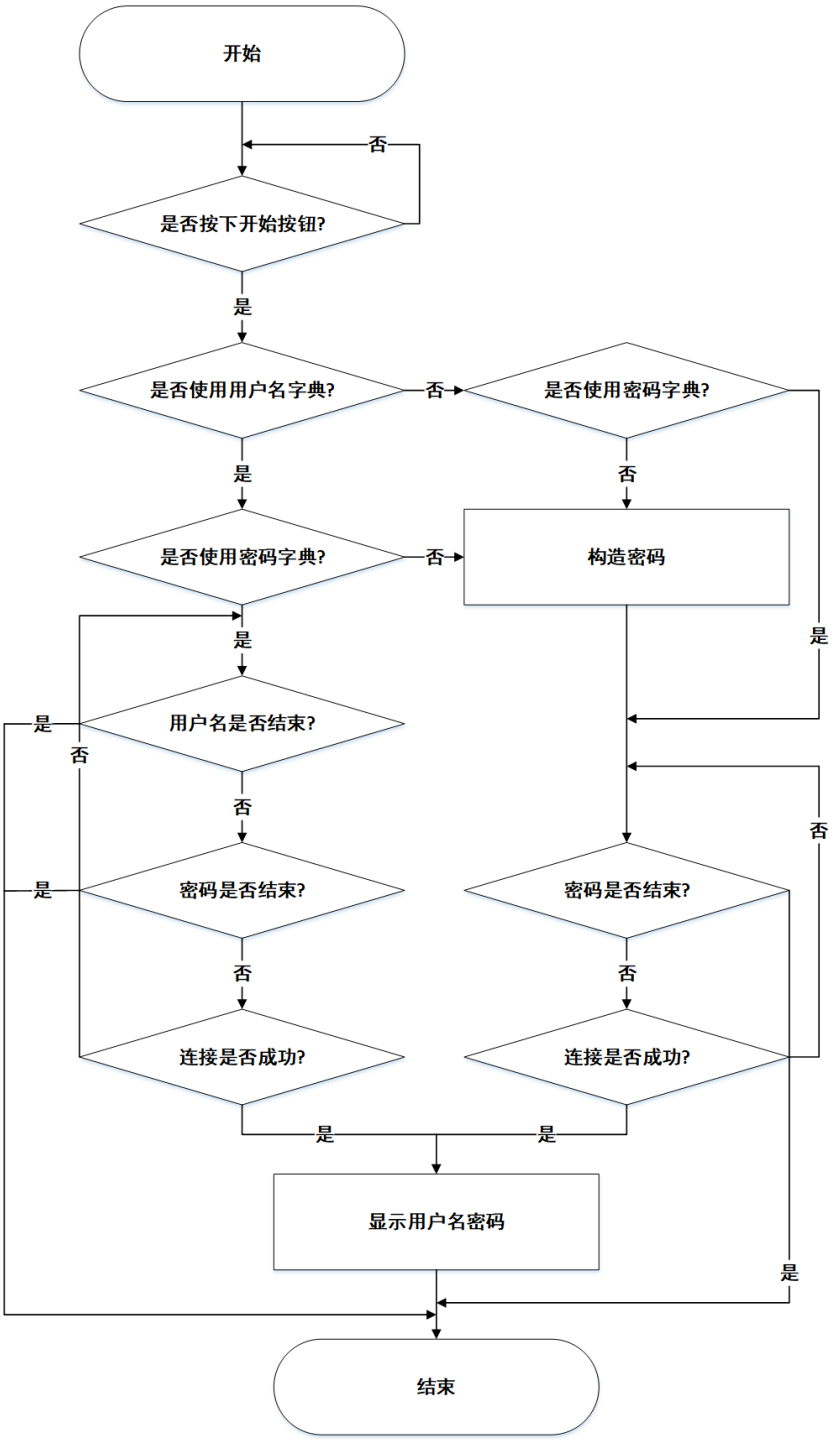


图 3-5 弱密码扫描模块流程图

3.2.6 嗅探器扫描模块

嗅探器扫描是对所接收到的所有数据包进行实时监听，然后依次与监测关键字进行匹配，筛选出那些关键信息。其流程图如图 3-6 所示：

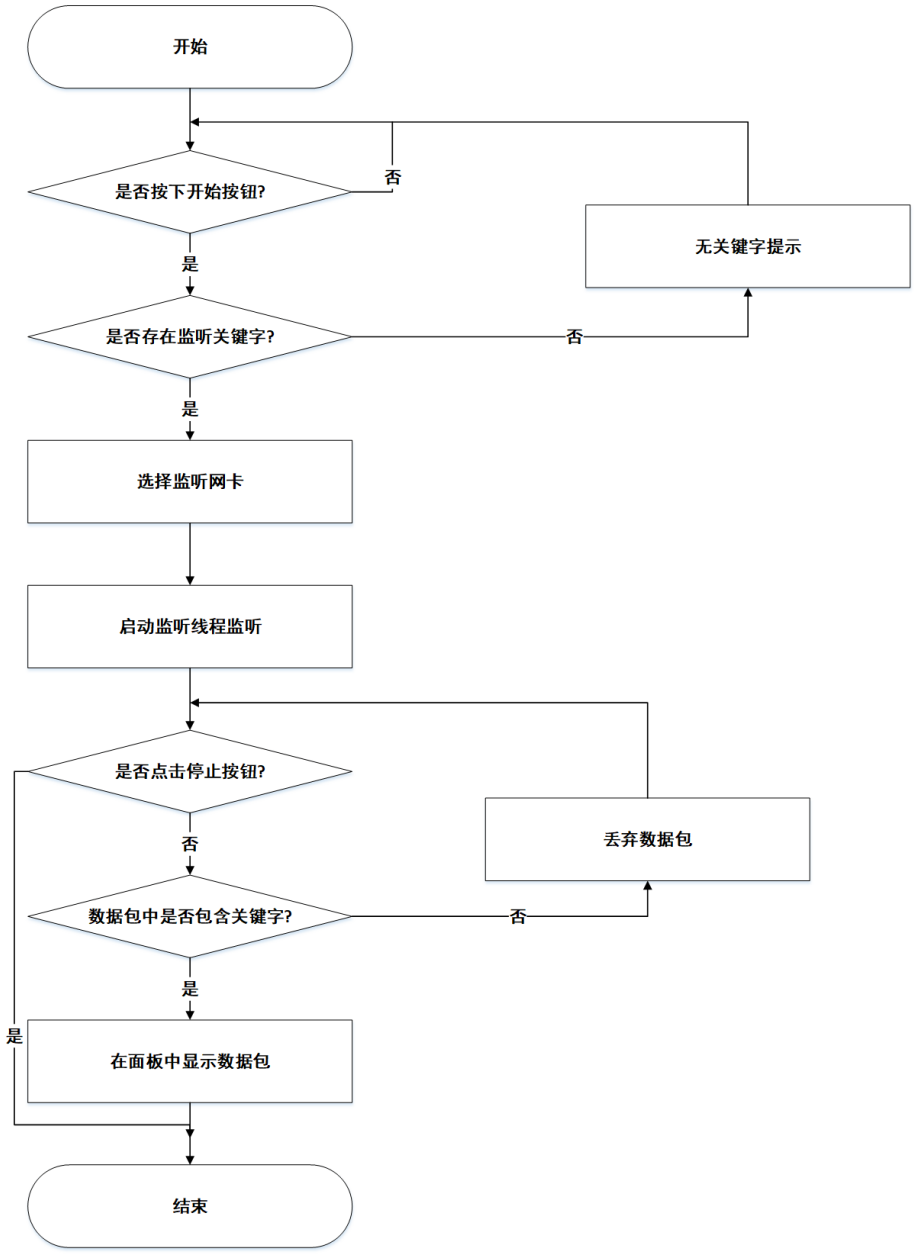


图 3-6 嗅探器扫描模块流程图

3.2.7 DOS 攻击模块

DOS 攻击是对目标 IP 的特定端口采用指定的线程数去发送大量的数据和连接请求，不断的消耗目标主机的资源，从而造成目标主机连接资源耗尽，导致其它主机无法使用这些连接资源。其流程图如图 3-7 所示：

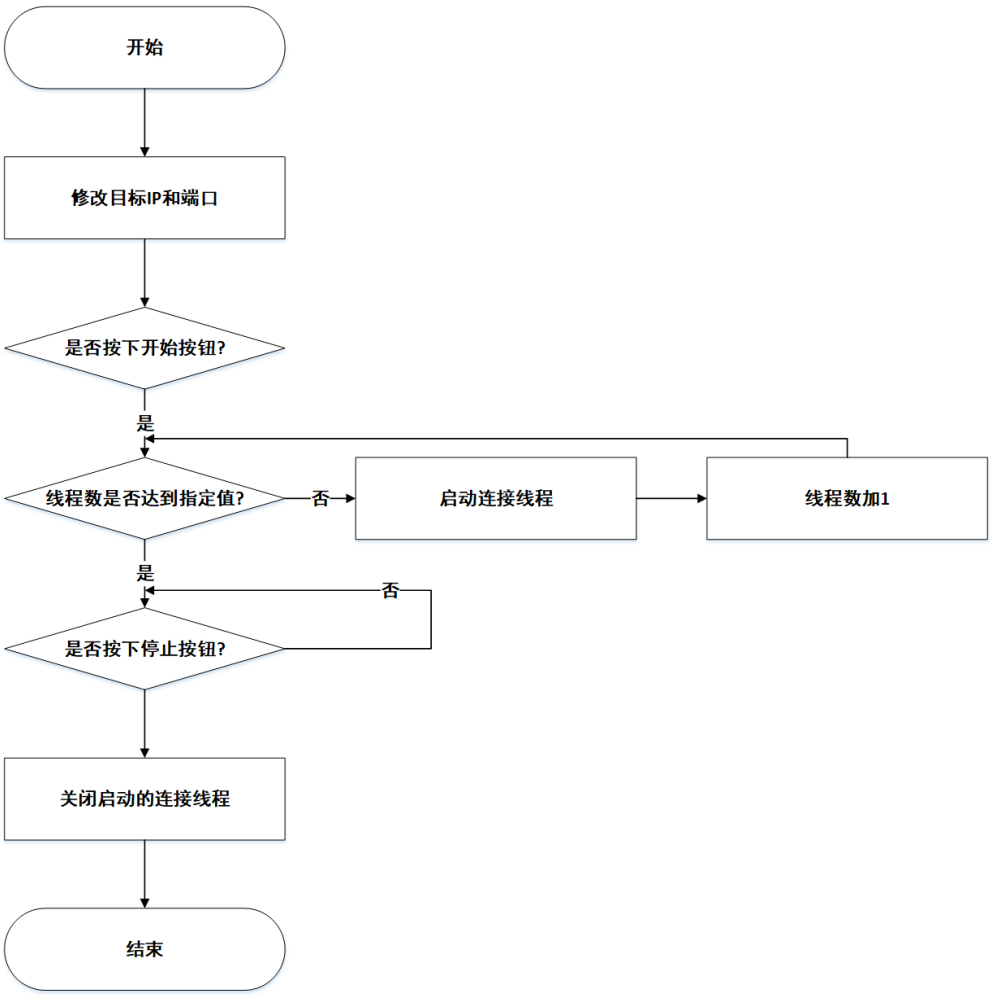


图 3-7 DOS 攻击模块流程图

3.2.8 注入检测模块

由于程序员及软件设计师在编写程序或设计相关软件模型的过程中出现了设计缺陷，导致非法用户可以通过构造一系列特殊的字符串去拼接到软件的缺陷部分，从而导致非授权用户可以绕过系统验证而读取到数据库中的隐私数据，从而造成信息的泄露，造成巨大的损失。其流程图如图 3-8 所示：

图 3-8 注入检测模块流程图

3.2.9 报告生成模块

报告生成是网络扫描器所提供的任意多种扫描功能对目标 IP 的扫描结果进行汇总，最终以报告的形式打印出来，提供了 html、txt 和 xml 三种打印格式。其流程图如图 3-9 所示：

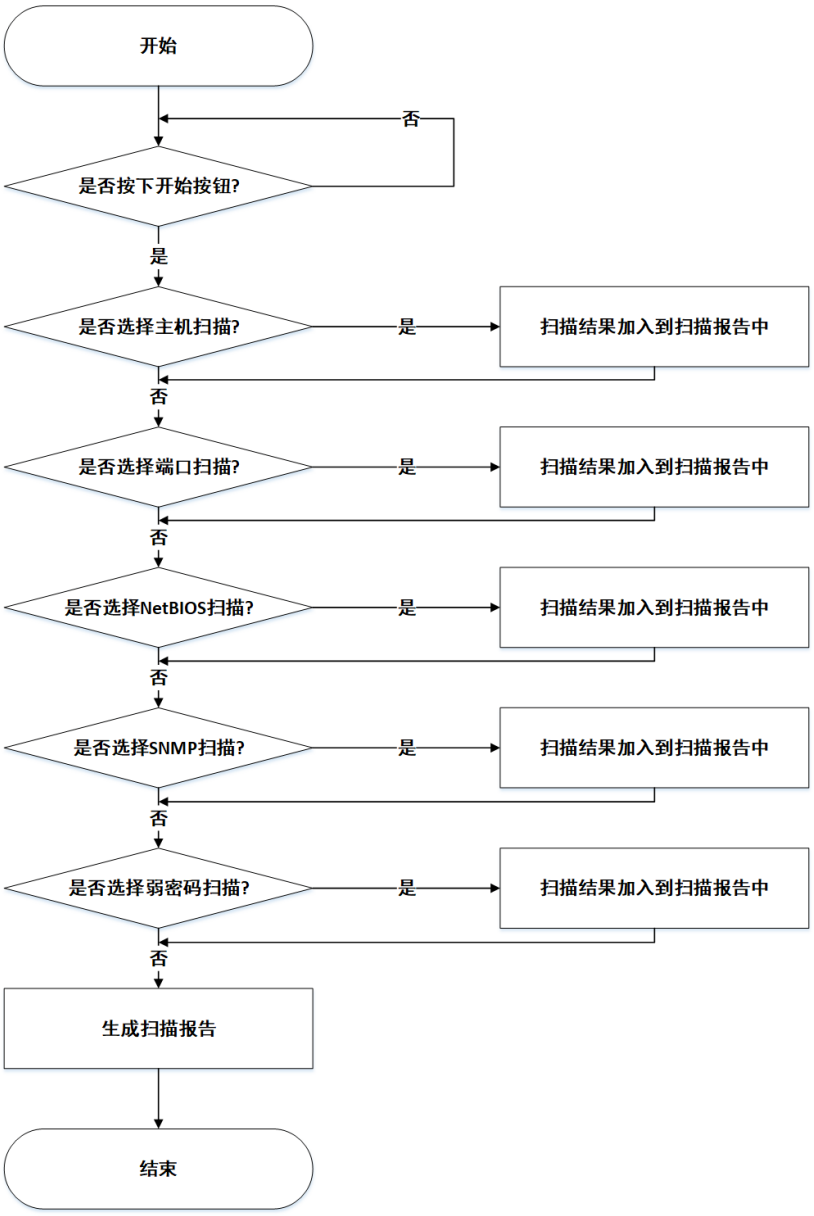


图 3-9 报告生成模块流程图

4 界面设计

4.1 界面关系图或工作流图

网络扫描器主要工作流程图如图 4-1 所示：

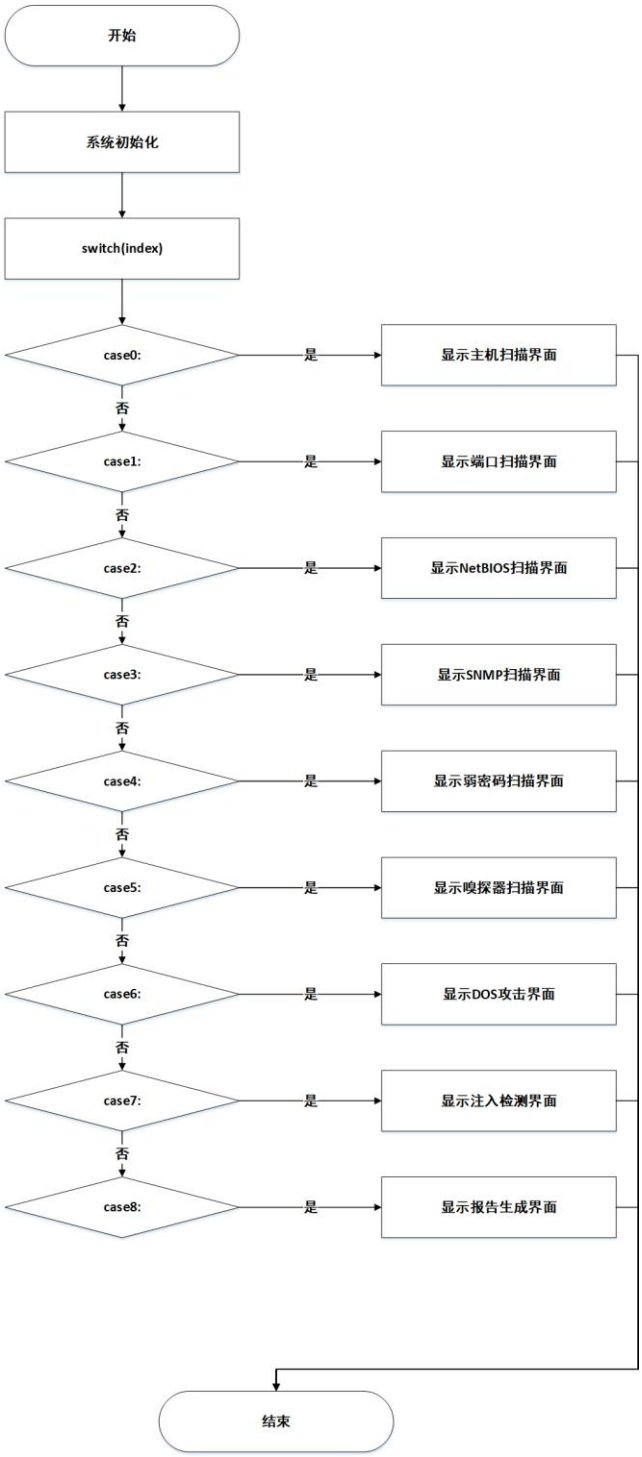


图 4-1 网络扫描器工作流程图

4.2 界面设计成果

4.2.1 主界面

网络扫描器主界面如图 4-2 所示：

图 4-2 网络扫描器主界面

4. 2. 2 子界面

网络扫描器共实现了九个功能模块，下面管理员分别看看这九个功能模块的子界面。

图 4-3 展示的是主机扫描功能模块的界面：

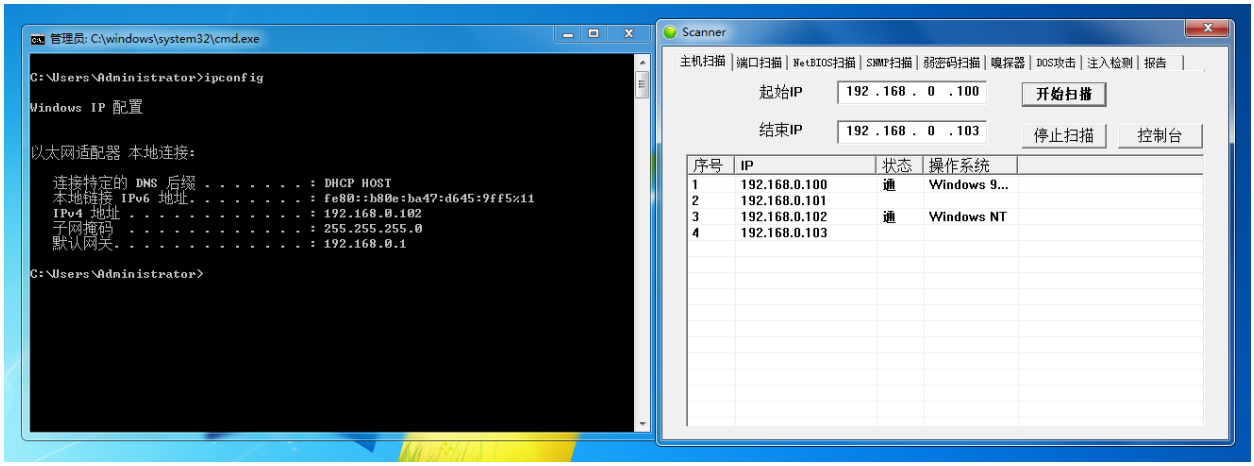


图 4-3 主机扫描功能子界面

图 4-4 展示的是端口扫描功能模块的界面：

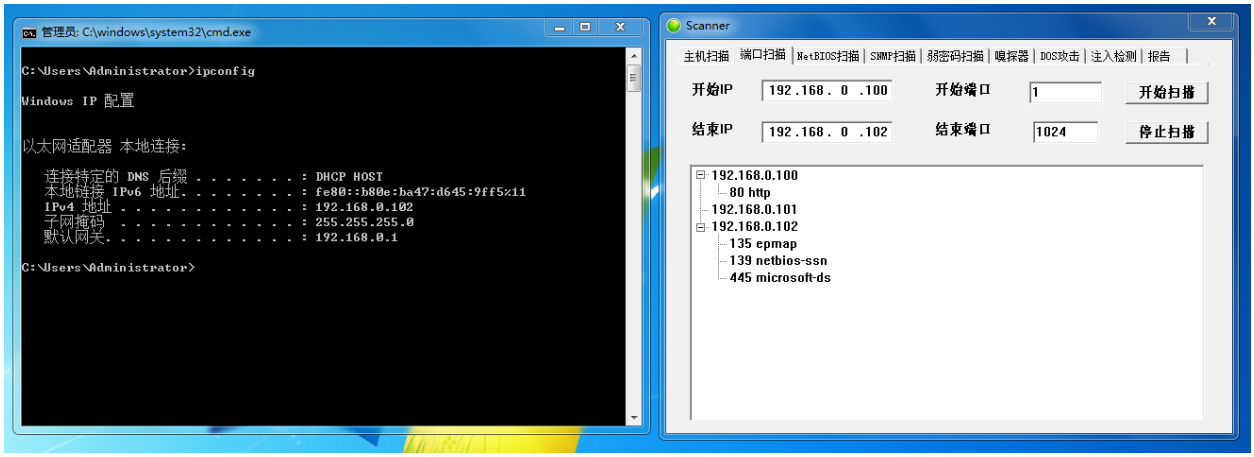


图 4-4 端口扫描功能子界面

图 4-5 展示的是 NetBIOS 扫描功能模块的界面：

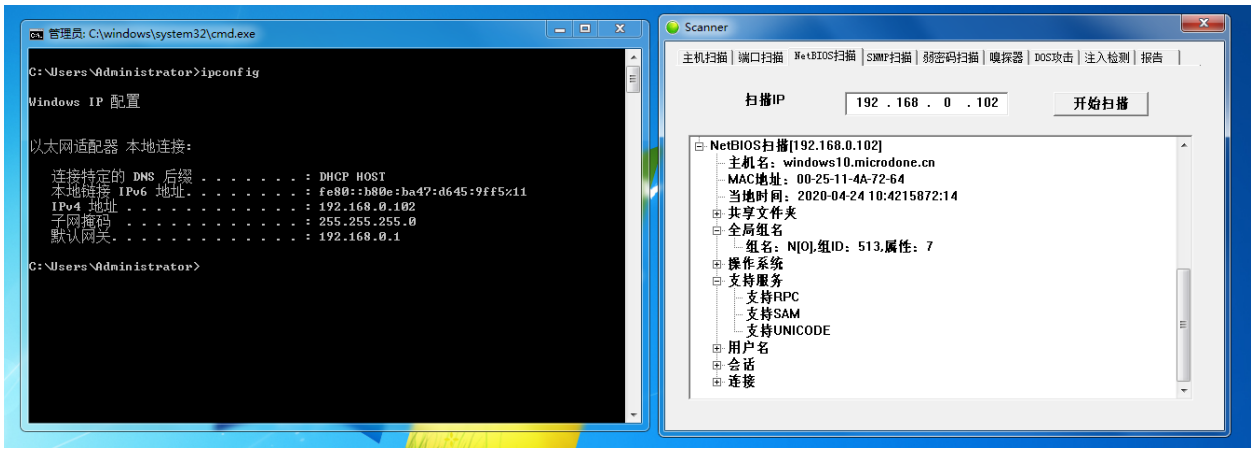


图 4-5 NetBIOS 扫描功能子界面

图 4-6 展示的是 SNMP 扫描功能模块的界面：

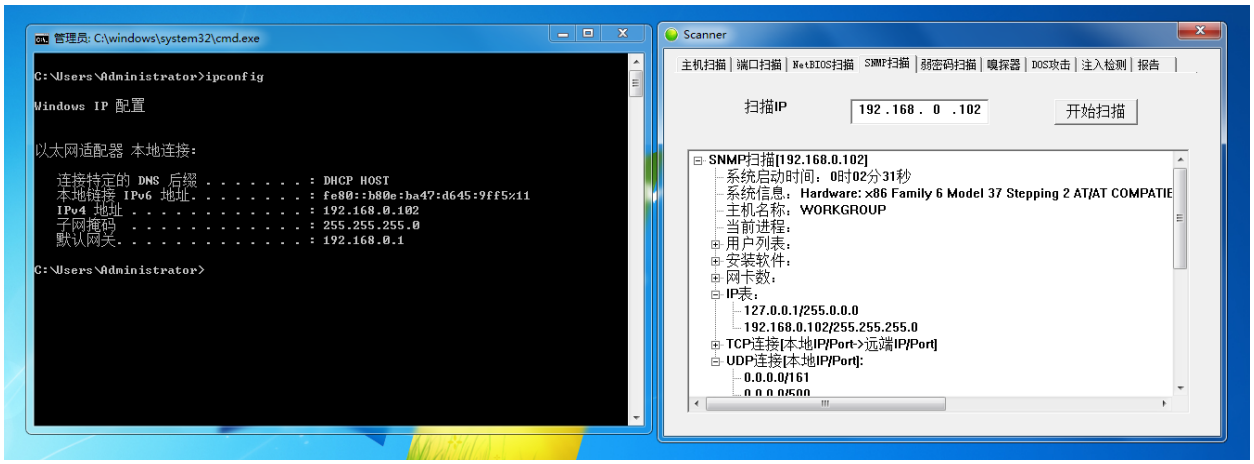


图 4-6 SNMP 功能子界面

图 4-7 展示的是弱密码扫描功能模块的界面：

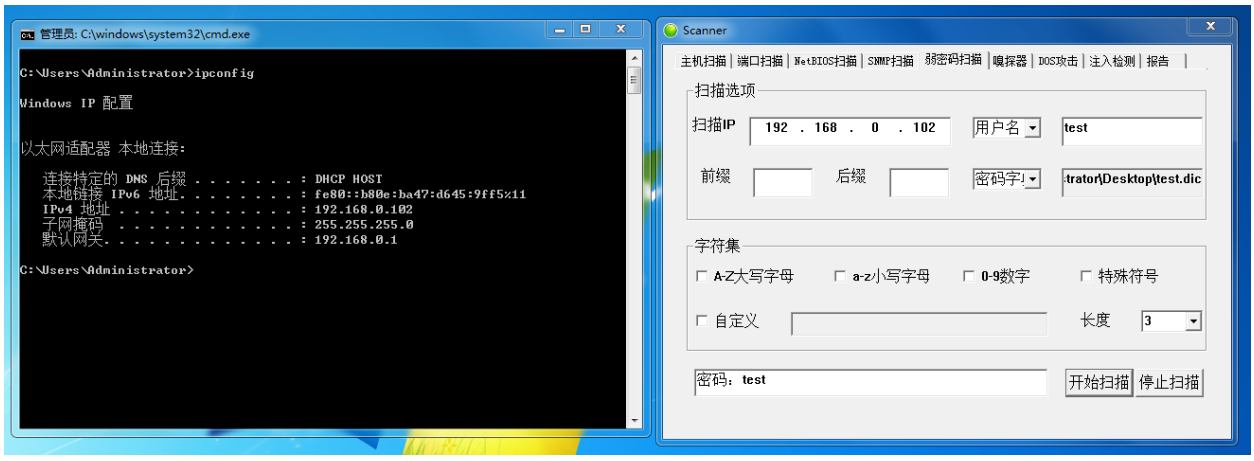


图 4-7 弱密码扫描功能子界面

图 4-8 展示的是嗅探器扫描功能模块的界面：

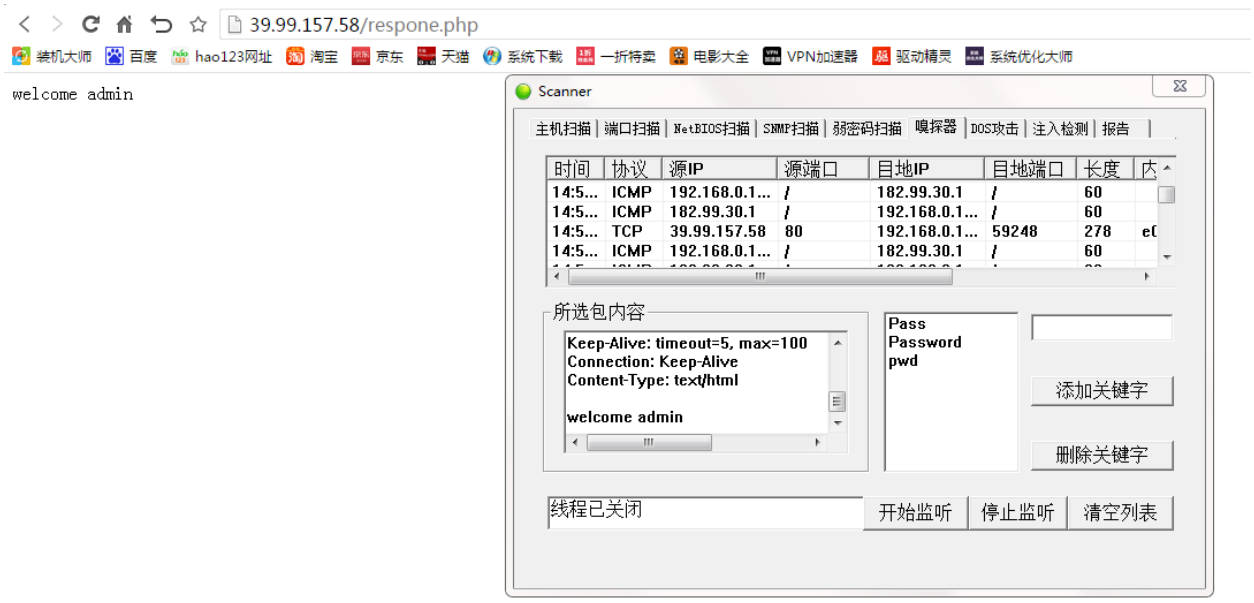


图 4-8 嗅探器扫描功能子界面

图 4-9 展示的是 DOS 攻击功能模块的界面：

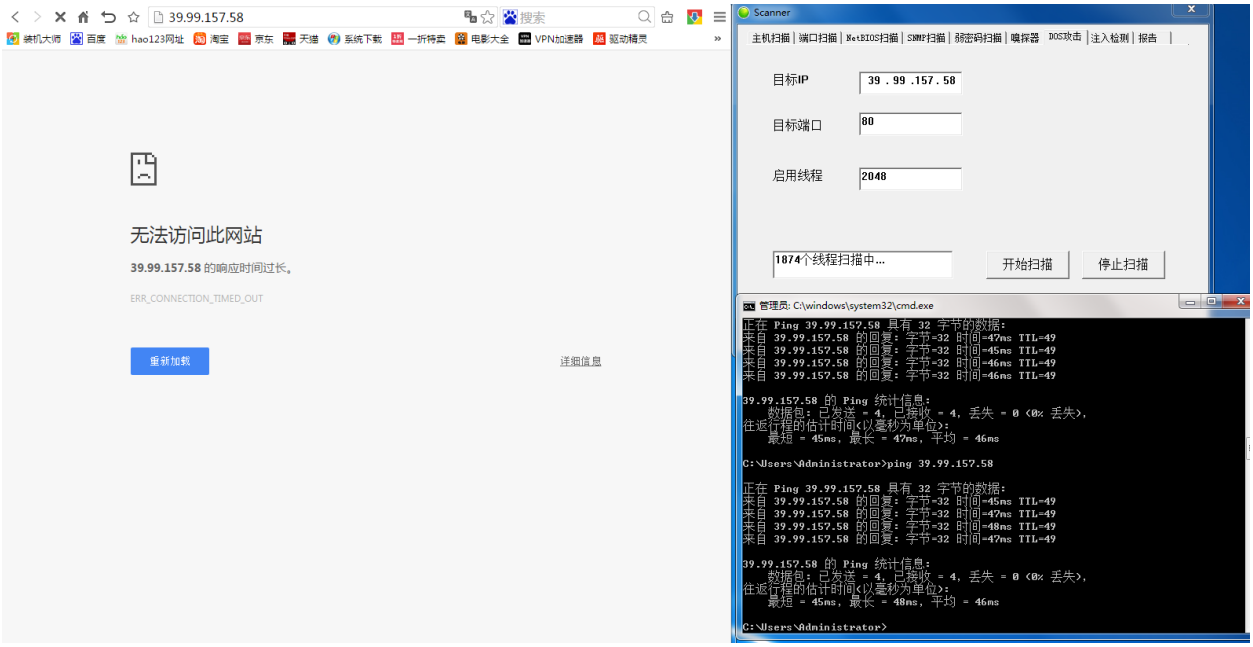


图 4-9 DOS 攻击功能子界面

图 4-10 展示的是注入检测功能模块的界面：

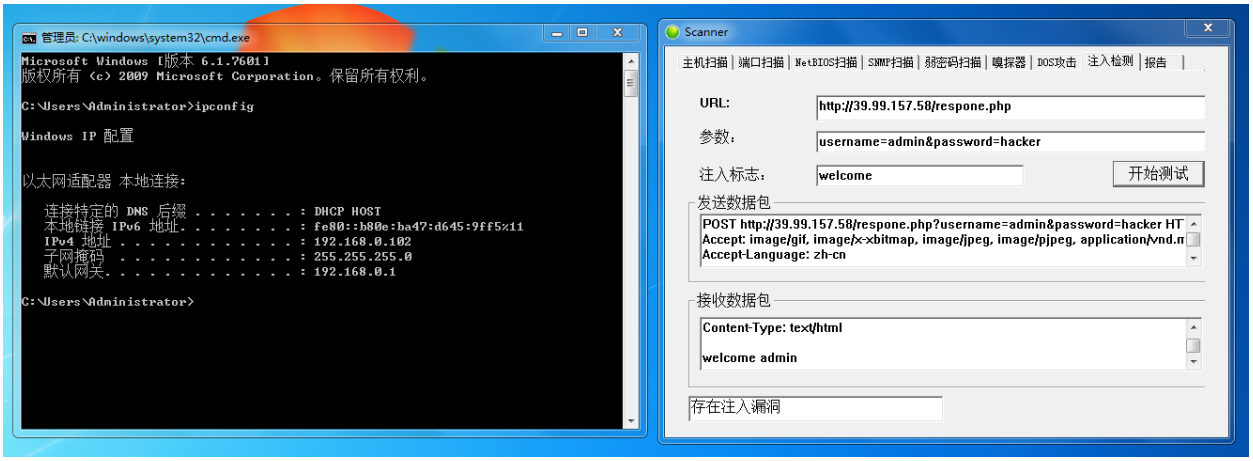


图 4-10 嗅探器扫描功能子界面

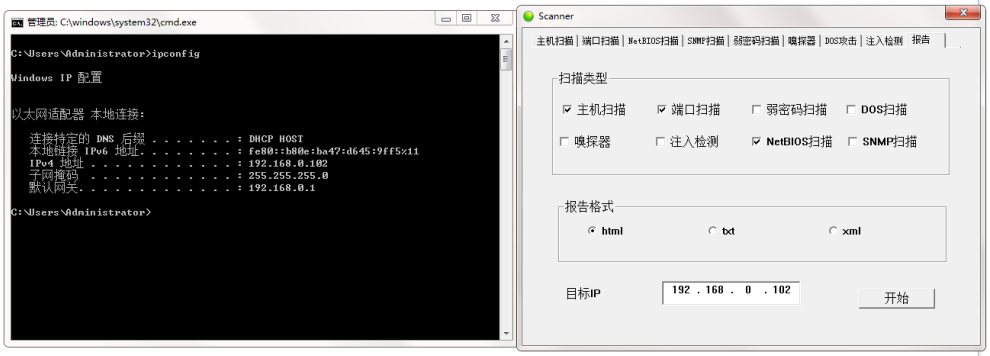
图 4-11 展示的是报告生成功能模块的界面：

1.主机扫描

IP	状态	操作系统
192.168.0.102	通	Windows NT

2.端口扫描

- 192.168.0.102
  - 135 epmap
  - 139 netbios-ssn
  - 445 microsoft-ds



3.NetBIOS扫描

- NetBIOS扫描[192.168.0.102]
- MAC地址：00-25-11-4A-72-64
- 当地时间：2020-04-24 15:4277990:05
- 共享文件夹
  - IPC$[帆ƶz]
- 全局组名
  - 组名：N[O],组ID：513,属性：7
- 操作系统
  - 平台ID：500
- 支持服务
  - 支持RPC
- 用户名
  - Administrator[]
  - 用户全名:
- 会话
  - 客户端：\\192.168.0.102;用户名：Administrator;Active:0;Idle:0
- 连接
  - 传送:\Device\NetbiosSmb;地址:USERCHI-D0AL3T4;数量:0;网址:USERCHI-D0AL3T4;域:WORKGROUP

图 4-11 报告生成功能子界面

5 详细设计

5.1 系统主要功能模块介绍

众所周知，CTabCtrl 是 MFC 的选项卡控件，目的是为了集成多个功能模块，每个功能模块都有单独的子界面，而在不同的子界面下可以插入多个控件进行操作。

管理员的目标是设计一个网络扫描器，而管理员需要设计出九个功能模块去帮助管理员完成辅助扫描的需要。而介于 GUI 界面的需要，管理员可以利用 MFC 的选项卡控件去完成这一操作，管理员需要在主对话框中使用插入条目 InsertItem 函数去创建这些选项卡控件，使管理员能够更加方便的切换各个功能模块，然后就可以对每一个功能模块进行编辑，而对不同的功能选项卡管理员要进行操作的监听，一旦有相关事件的发生，管理员能够及时作出反馈并给出正确的操作，从而大大降低了用户的使用难度，方便用户进行可视化的合理的扫描操作。

其总体设计逻辑图如图 5-1 所示：

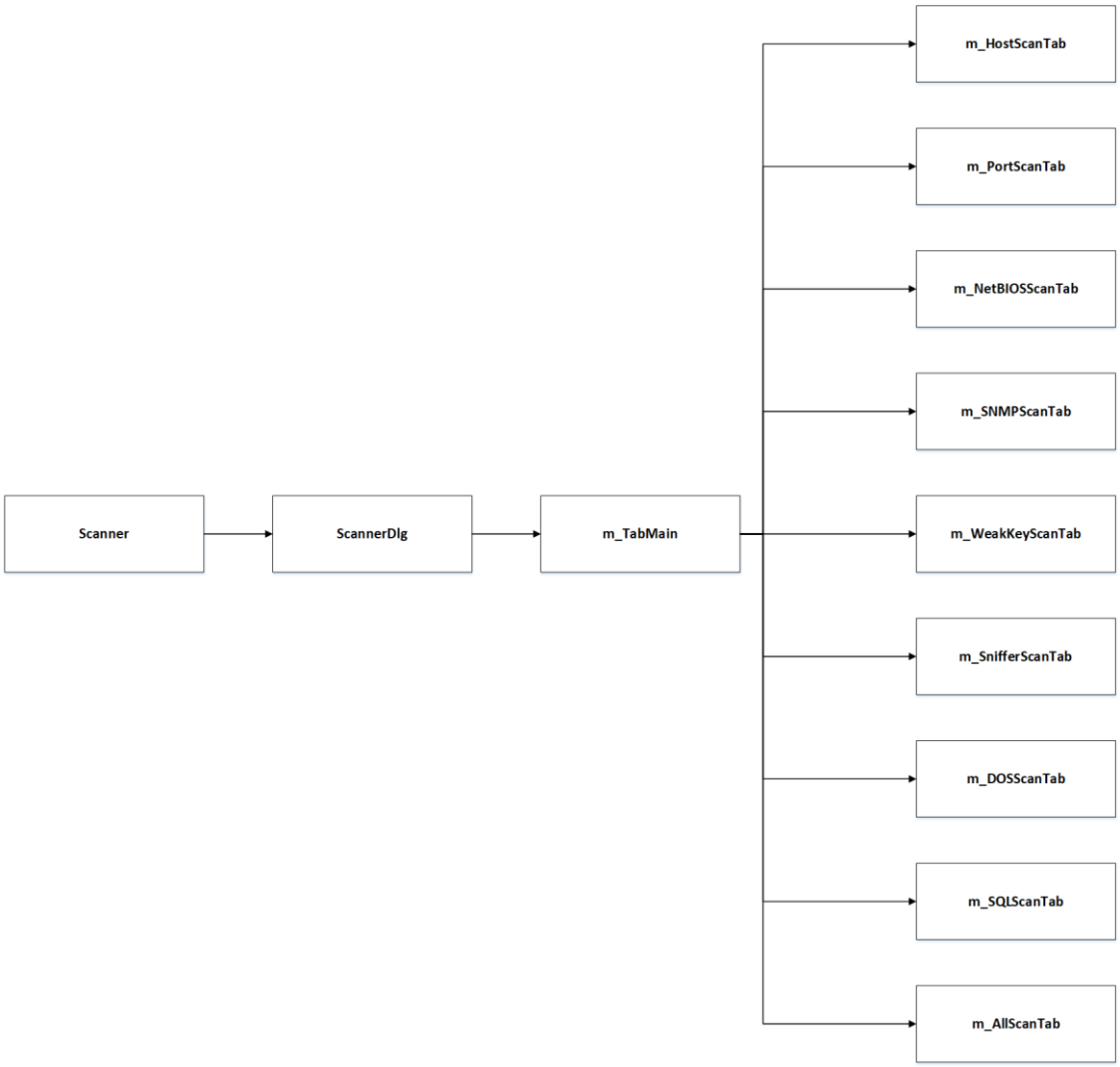


图 5-1 网络扫描器总体设计逻辑图

5.2 主机扫描模块设计

主机扫描就是扫描网络中可能存在的主机，主要是通过向特定的主机或者目的 IP 发送构造的 ICMP 协议包来确定目标网络上的主机是否可达。

网际控制报文协议 ICMP 是网络层的重要协议，它可以封装在 IP 数据包中作为数据包的数据部分，可以帮助用户了解数据异常的相关信息，以便更好的进行数据间的传输。其结构如图 5-2 所示：

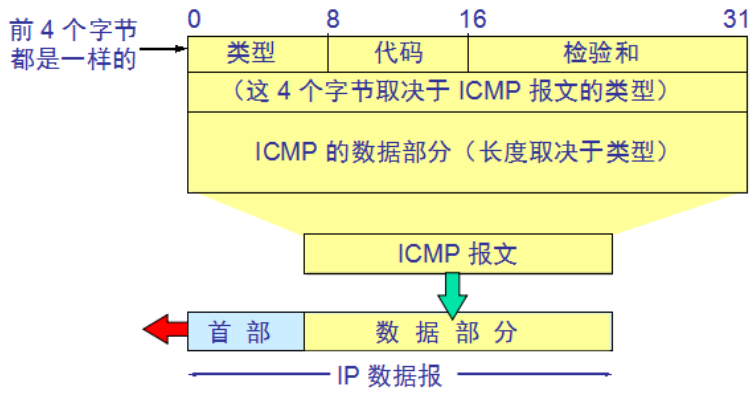


图 5-2 IP 数据报与 ICMP 数据报对比

网际控制报文 ICMP 具有统一的格式和结构，其结构如图 5-3 和图 5-4 所示：

图 5-3 ICMP 封装在 IP 内部

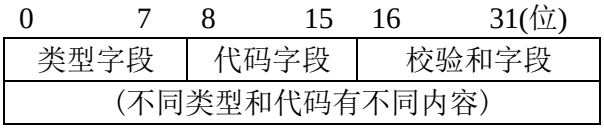


图 5-4 ICMP 报文

对套接字而言，一般管理员经常采用原始套接字去对某些协议参与直接的控制，它既能对较高层次的协议进行控制，又能对 OSI 底层的协议进行访问，能够有效的去协助网络去进行高层次的数据传输，而在某一目标主机所处的 C 段中，管理员利用管道技术对 C 段的所有主机进行多线程的 ping，而这种多线程的 ping 的间隔时间太长，往往不能满足管理员对效率的极致要求，管理员可能会另辟蹊径，寻找一条能够在几毫秒之间就能完成的操作，而这种才操作往往并不能很快的找到或发现，在这种情况下，管理员考虑通过构造网际控制报文协议 ICMP 数据包对目标主机发送连接请求，待接收到目标主机的连接请求响应后，管理员再对接收到的数据包进行分析，其程序流程图如图 5-5 所示：

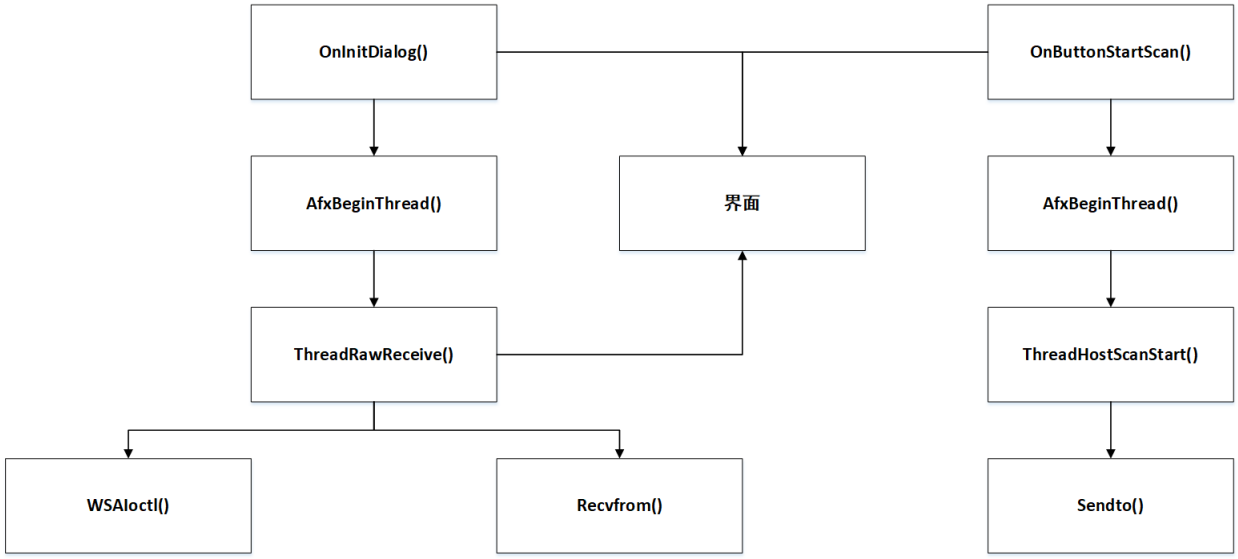


图 5-5 主机扫描模块程序流程图

5.3 端口扫描模块设计

对某一 IP 段目标主机 IP 的一段端口逐个连接，通过发送数据包对目标主机进行通信，根据反馈回来的数据包信息判断该主机的开放状态，根据其开放端口所对应的主机服务去有针对性的发起相关的服务缺陷攻击。

而对于目标端口号而言，管理员需要查找相关的端口对应表去确定相关的服务信息，而要完成如此庞大的扫描任务对计算机的计算能力来讲并不是很容易，往往在扫描过程中会出现严重的卡顿，这种多线程扫描任务对计算机来讲无疑是占用了大量的有限资源，往往很多时候这种探测都是在闲置的服务器上完成，对目标端口可能存在的安全隐患，管理员需要及时的作出相应的补救，例如关闭相关端口，其实就是关闭管理员不需要开放的通信信道，这种信道对计算机而言是有害而无一利，还有可能被非法分子利用而造成更大的损失，而对庞大的 C 段上的目标主机所开放的所有端口的探测，管理员通过原始套接字去创建出 socket 对目标 C 段上的主机的所有端口进行连接请求，将开放的端口一一的列举出来，通过查表的方式将相应端口的服务也进行展示，其程序流程图如图 5-6 所示：

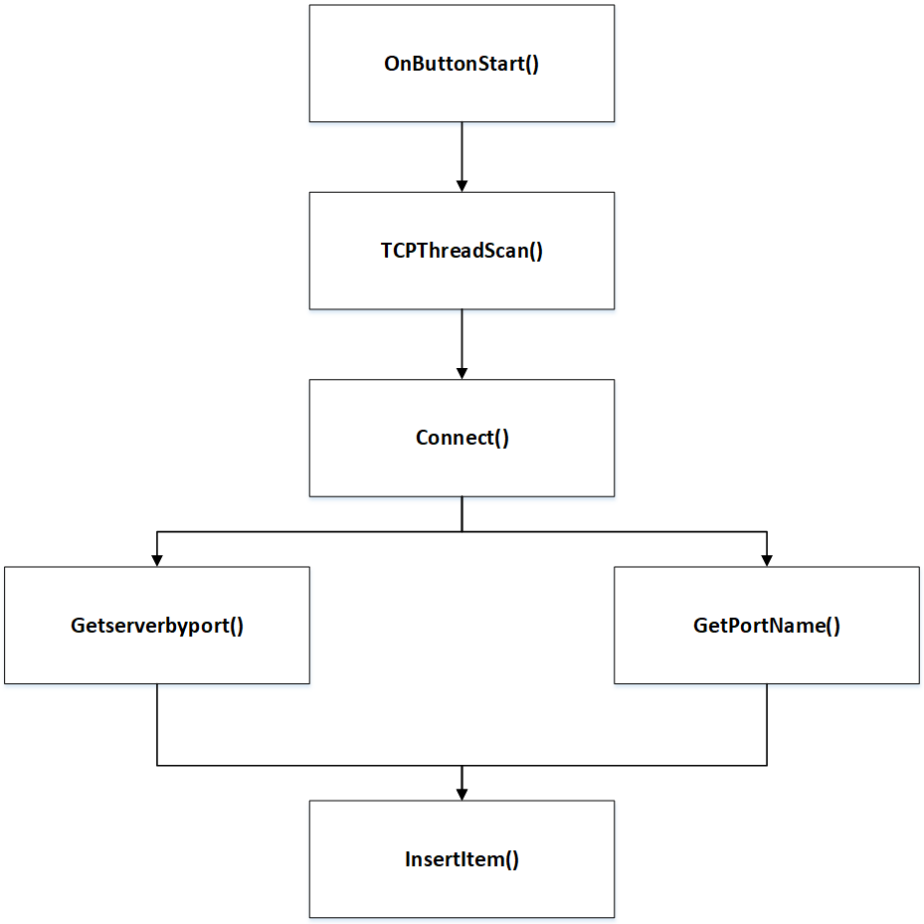


图 5-6 端口扫描模块程序流程图

5.4 NetBIOS 扫描模块设计

对网上基本输入输出系统 NetBIOS 协议而言，它作为应用层上的一种特殊的协议，它常常被用来管理局域网上的主机，通过该协议的相关约定，管理员可以很方便的读取到局域网上相关目标主机可拥有的相关属性的详细信息。

而使用网上基本输入输出系统 NetBIOS 协议，管理员可以通过读取地址信息函数 gethostbyaddr 读取到相关的主机名信息，而 SendARP 函数是被用来读取计算机唯一的 MAC 地址信息而存在的，NetRemoteTOD 和 NetShareEnum 函数是被用来读取当前的计算机时间和计算机中可能存在的共享目录，而要读取操作系统类型，管理员还是需要专门读取操作系统信息的函数 etServerGetInfo 来完成这一复杂的操作，而相关计算机所支持和存在的服务以及组列表，管理员还是需要通过 NetRemoteComputerSupports 和 NetGroupEnum 函数来完成这一操作，通过 NetShareEnum 函数，管理员可以知道 TCP 连接的相关信息，而最后管理员想要获取目标主机的用户名相关信息和会话栏，管理员需要通过 NetUserEnum 和 NetSessionEnum 来完成这些操作，其程序流程图如图 5-7 所示：

图 5-7 NetBIOS 扫描模块程序流程图

5.5 SNMP 扫描模块设计

简单网络管理协议 SNMP 是对智能终端设备做简单管理，管理员可以利用该协议的相关约定去获取支持该协议的各种设备的详细的信息。

对简单网络管理协议 SNMP 而言，管理员建立了一个专门用来查询各种智能终端设备详细的软硬件信息的 MIB 树形网络设备管理功能数据库，通过该数据库，管理员可以利用树的遍历操作去和当前设备的属性进行匹配，然后在数据库中查询到有关的信息，并显示给用户。而要完成这些纷繁复杂的操作，还是需要先发出和目标主机有关的连接请求，SnmpMgrOpen 函数可以帮助管理员完成这些连接操作，通过简单网络管理协议 SNMP 请求消息操作函数 SnmpMgrRequest 去遍历搜寻目标的智能终端设备的相关信息，并显示在屏幕上，提供给用户信息和了解这些软硬件的相关信息，其程序流程图如图 5-8 所示：

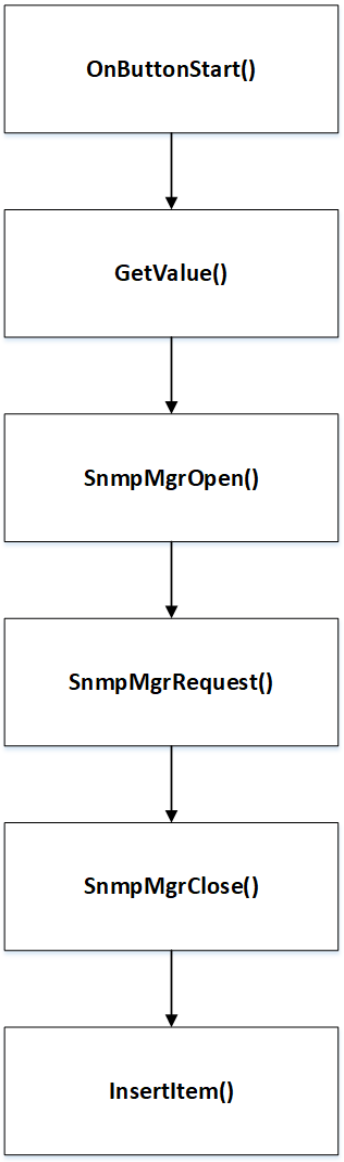


图 5-8 SNMP 扫描模块程序流程图

5.6 弱密码扫描模块设计

弱密码扫描是逐个对目标主机的用户名和密码进行扫描，依次穷举遍历所有的用户名和密码的组合，用遍历生成的密码去逐次尝试验证。通过密码验证系统给出的正确或错误的反馈来判断是否成功获取到了用户的信息。

管理员利用构造好的用户名和密码去挨个尝试，若是相应的用户名和密码信息登录成功，管理员则可以断定管理员已经成功的获取到了目标信息，相应的信息将打印到屏幕上，其程序流程图如图 5-9 所示：

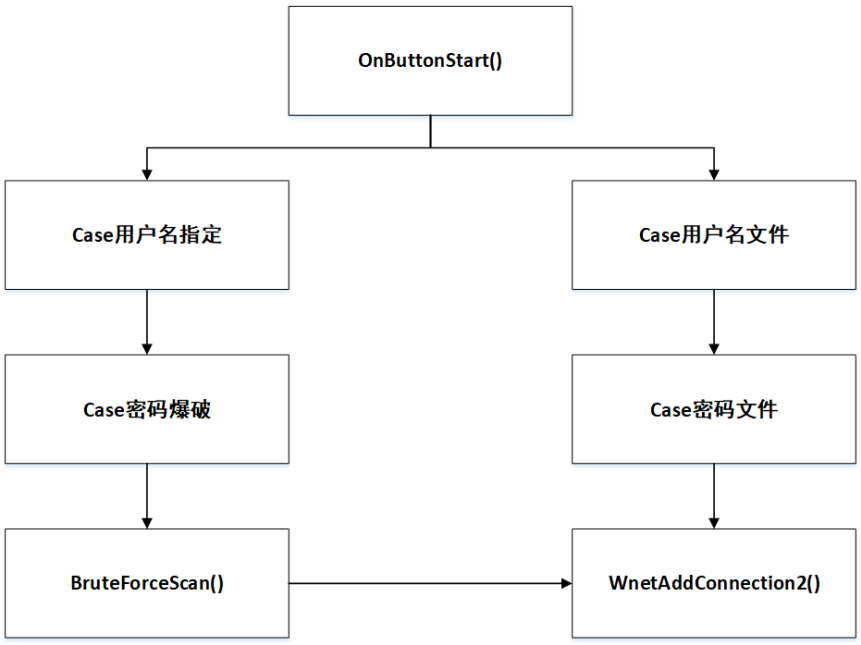


图 5-9 弱密码扫描模块程序流程图

5.7 嗅探器扫描模块设计

针对嗅探器模块的设计，管理员通过创建一个 socket 套接字去建立通信管道，然后在管道中进行数据间的通信，管理员通过绑定本地端口和响应的 IP 地址，定义好管理员筛选出的包含关键字的数据包，对本地主机采用多线程的方式通过管道的形式接收，然后等待数据包的反馈，再将接收到的数据包进行解包分析，然后去采集管理员需要获得的相关信息。

每个人对程序的理解不一样，这就造成了管理员在编写代码的时候可能会有不太一样的书写方式，密码这一词可以写成 password，也有人写 Password，甚至还有人可能写成 PassWord，这样类似的问题层次不齐，所以，如果管理员想监听“密码”这个关键字，那么有这些关键字的数据包都是管理员感兴趣的目标，当然你也可以都加入监听，这样就不用处理大小写问题，但是这样做有个问题，优先选择哪一个作为管理员监听的目标，选择最优策略往往是管理员所要考虑的问题，其程序流程图如图 5-10 所示：

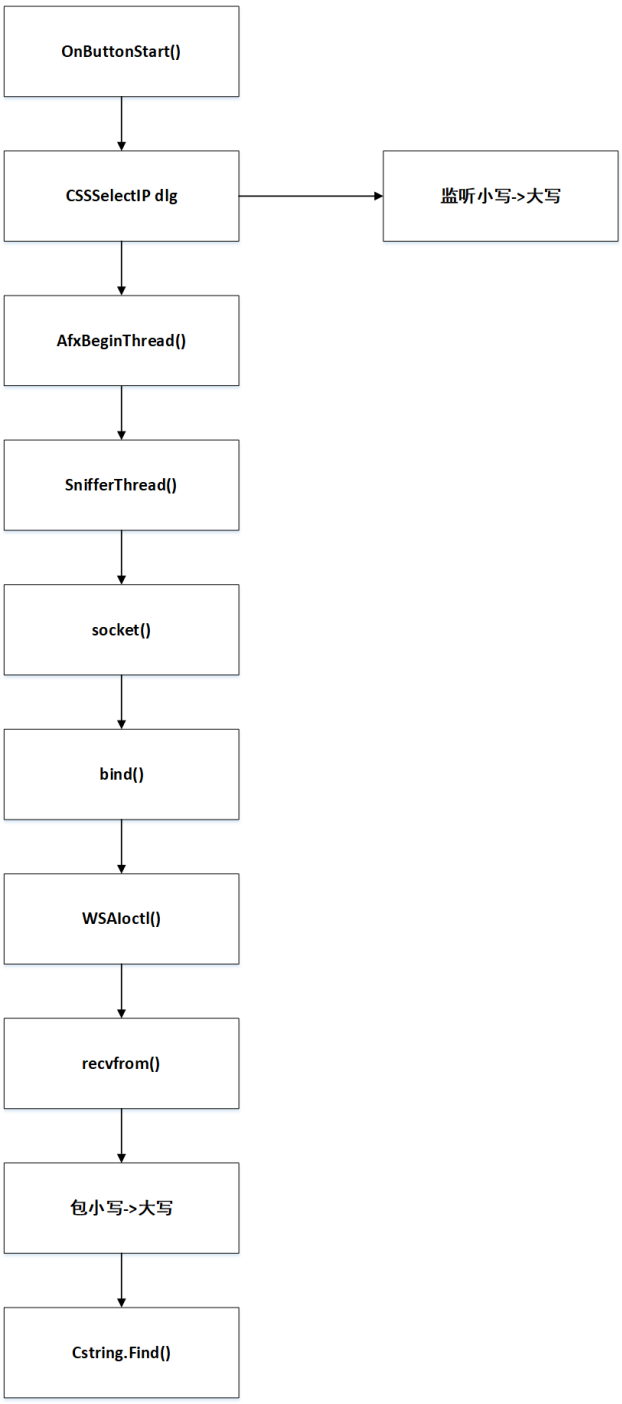


图 5-10 嗅探器扫描模块程序流程图

5.8 DOS 攻击模块设计

DOS 攻击(Denial of Service，也称为拒绝服务攻击)是对目标 IP 的特定端口采用指定的线程数去发送大量的数据和连接请求，不断的消耗目标主机的资源，从而造成目标主机连接资源耗尽，导致其它主机无法使用这些连接资源。

DOS 攻击指的是使用本地主机对目标主机机发起 DOS 攻击。此设计的网络扫描器实现的是不断地建立三次握手连接，使用本地主机对目标主机发起 DOS 攻击。

针对 DOS 攻击模块的设计，管理员通过创建一个 socket 套接字去建立通信管道，然后在管道中进行数据间的通信，管理员可以每隔一段时间对目标主机采用多线程的方式通过管道的形式发送连接请求信息，然后等待数据包的反馈，其程序流程图如图 5-11 所示：

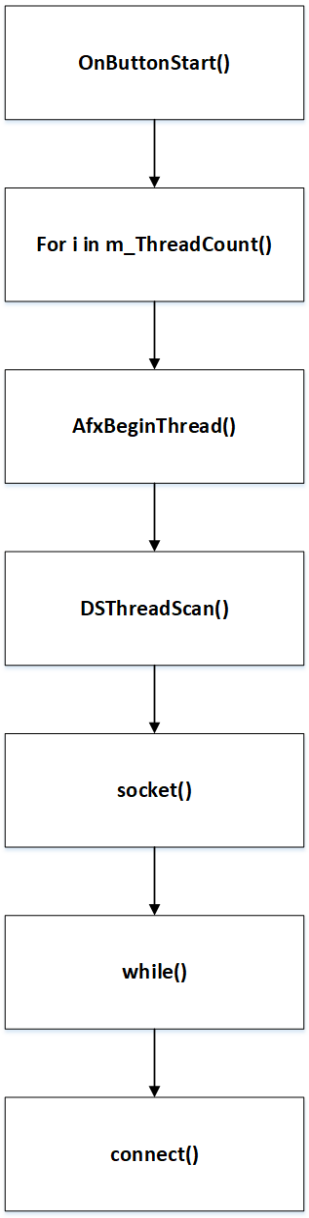


图 5-11 DOS 攻击模块程序流程图

5.9 注入检测模块设计

由于程序员及软件设计师在编写程序或设计相关软件模型的过程中出现了设计缺陷，导致非法用户可以通过构造一系列特殊的字符串去拼接到软件的缺陷部分，从而导致非授权用户可以绕过系统验证而读取到数据库中的隐私数据，从而造成信息的泄露，造成巨大的损失。

管理员可以通过创建一个 socket 套接字去建立通信管道，然后在管道中进行

数据间的通信，管理员可以利用 send 函数将构造好的数据包通过管道的形式发送出去，然后等待数据包的反馈，通过 recv 函数去接收，然后对接收到的数据包进行拆解分析，寻找是否存在管理员事先确定好的漏洞关键字，以便来确定注入漏洞的存在，来进行下一步的判断，其程序流程图如图 5-12 所示：

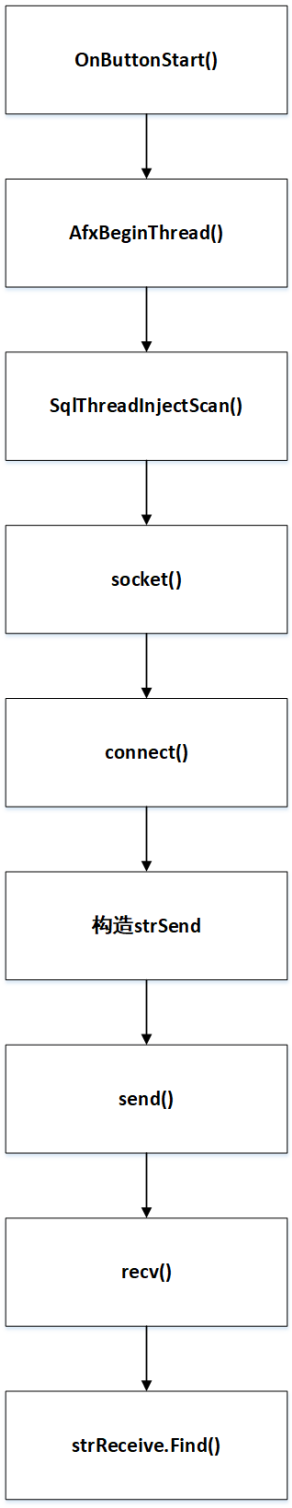


图 5-12 注入检测模块程序流程图

5.10 报告生成模块设计

报告生成是网络扫描器所提供的任意多种扫描功能对目标 IP 的扫描结果进行汇总，最终以报告的形式打印出来，提供了 html、txt 和 xml 三种打印格式。

具体操作是管理员可以通过点击开始按钮，调用相关发送消息的函数，去给每个所选中的功能模块发送打印信息，最后通过该模块去汇总，将所有的结果形成一张报告，以 HTML 的形式展现出来，其程序流程图如图 5-13 所示：

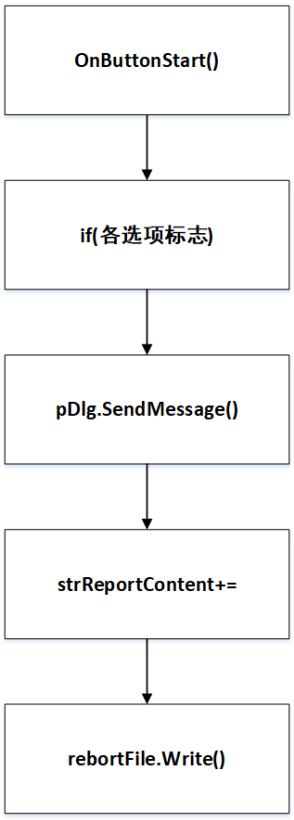


图 5-13 报告生成模块程序流程图

6 测试

6.1 测试方案设计

6.1.1 主机扫描功能模块测试

在主机扫描功能模块中，管理员输入起始 IP 为 192.168.0.100，结束 IP 为 192.168.0.103，在这个 IP 段的范围内进行测试，结果显示有两台主机处在存活状态，分别是 192.168.0.100 和 192.168.0.102，其扫描结果如图 6-1 所示：

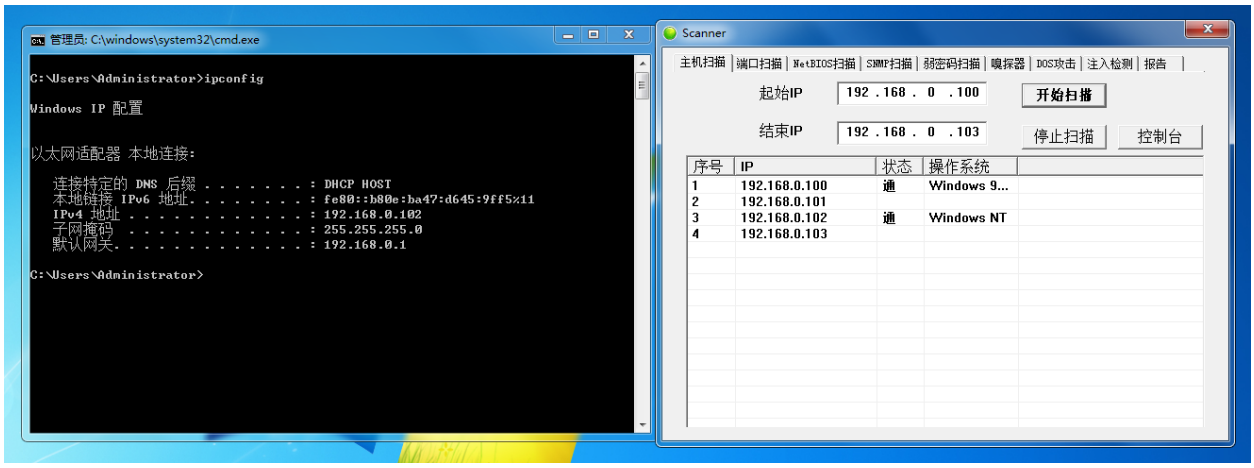


图 6-1 主机扫描测试图

6.1.2 端口扫描功能模块测试

在端口扫描功能模块中，管理员输入起始 IP 为 192.168.0.100，结束 IP 为 192.168.0.102，在这个 IP 段的范围内进行测试，端口范围设置为 1~1024，结果显示，主机 192.168.0.100 开放了 80 端口，192.168.0.102 开放了 135、139 和 445 端口，其扫描结果如图 6-2 所示：

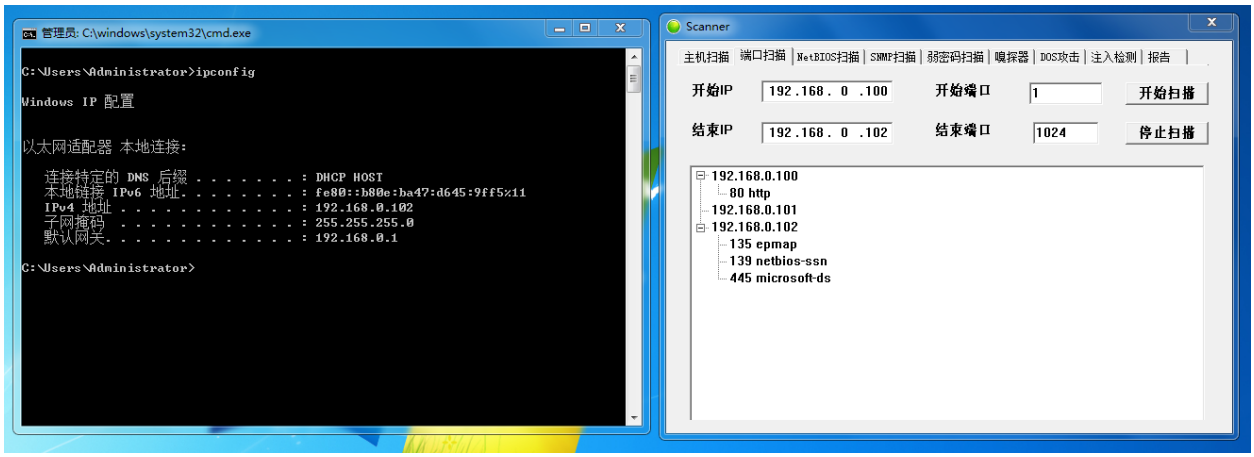


图 6-2 端口扫描测试图

6.1.3 NetBIOS 扫描功能模块测试

在网上基本输入输出系统 NetBIOS 扫描模块中，管理员选择 192.168.0.102 主机作为当前的目标主机，该主机为当前的主机 IP，显示出的结果与实际相符，其扫描结果如图 6-3 所示：

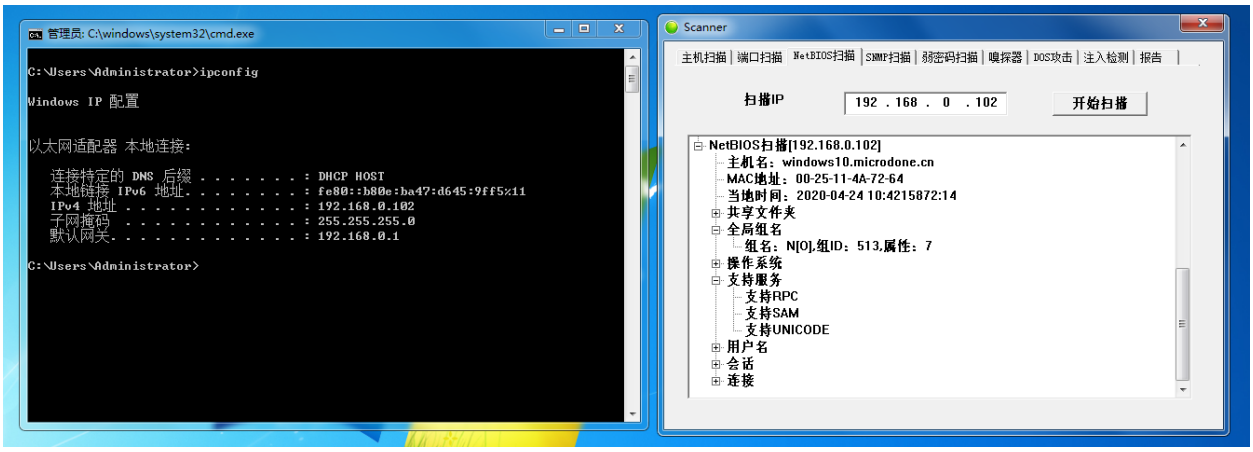


图 6-3 NetBIOS 扫描测试图

6.1.4 SNMP 扫描功能模块测试

在简单网络管理协议 SNMP 扫描功能模块中，管理员选择 192.168.0.102 主机作为当前的目标主机，该主机为当前的主机 IP，显示出的结果与实际相符，其扫描结果如图 6-4 所示：

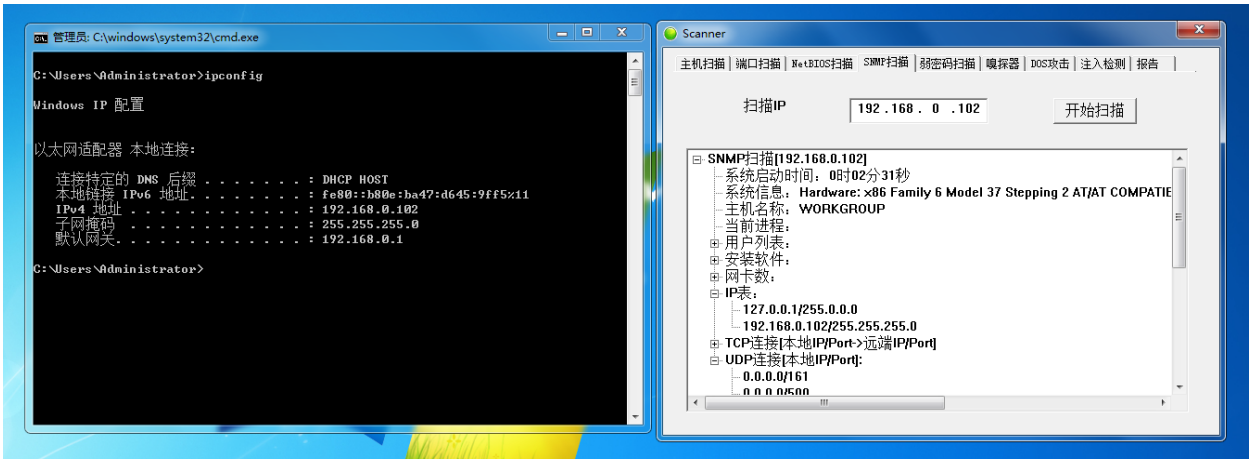


图 6-4 SNMP 扫描测试图

6.1.5 弱密码扫描功能模块测试

在弱密码扫描功能模块中，管理员选择 192.168.0.102 主机作为当前的目标主机，该主机为当前的主机 IP，用户名设置为 test，密码采用字典文件的方式去枚举，通过扫描出来的结果进行验证，可以确定该结果与实际相符，其扫描结果如图 6-5 所示：

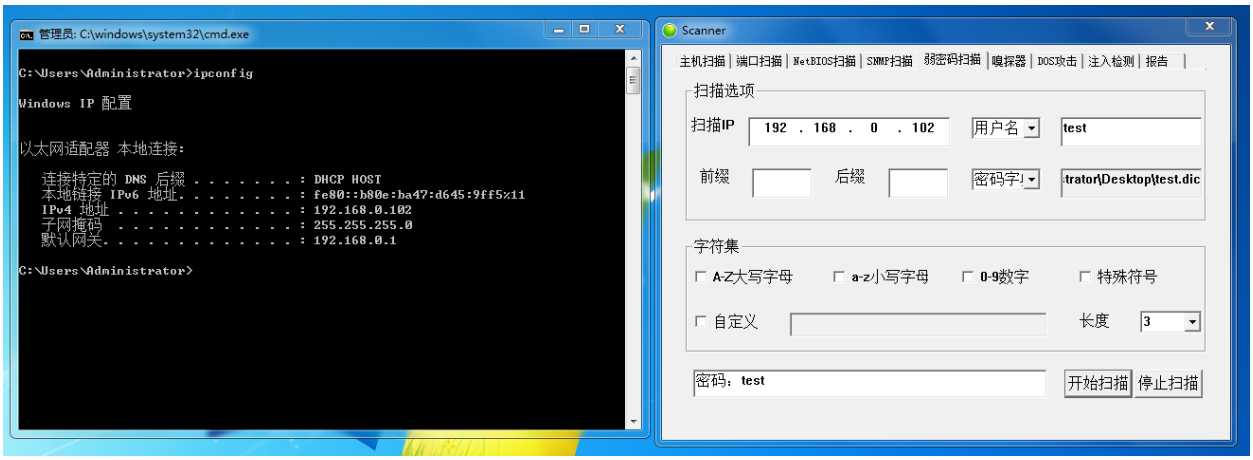


图 6-5 弱密码扫描测试图

6.1.6 嗅探器扫描功能模块测试

在嗅探器扫描功能模块中，管理员添加 Pass、Password、pwd 三个关键字对本机进行监听，然后通过由服务器搭建的一个登陆提交表单的页面去提交用户名和密码，结果成功拦截到了响应的数据包，根据数据包内容，管理员可以判断该结果与实际相符合，其扫描结果如图 6-6 所示：

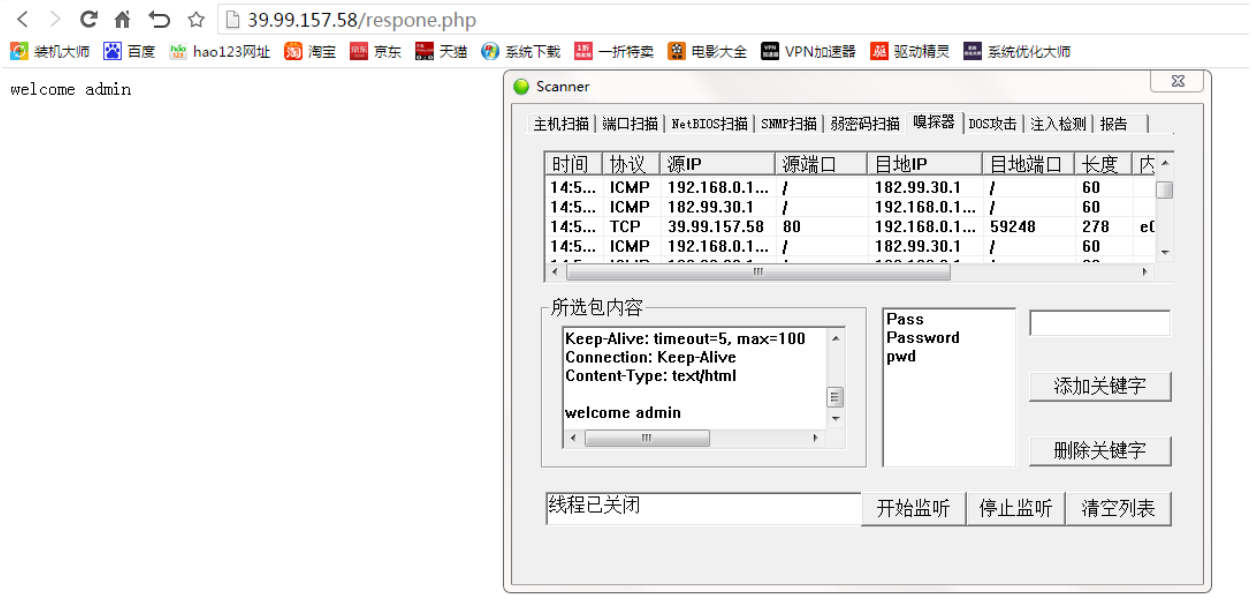


图 6-6 嗅探器扫描测试图

6.1.7 DOS 攻击功能模块测试

在 DOS 攻击功能模块中，管理员启动 2048 个线程对目标 IP 为 39.99.157.58 的 80 端口进行连接，然后再尝试访问网站，结果发现网站宕机，管理员可以判断该结果与预期相符合，其扫描结果如图 6-7 所示：

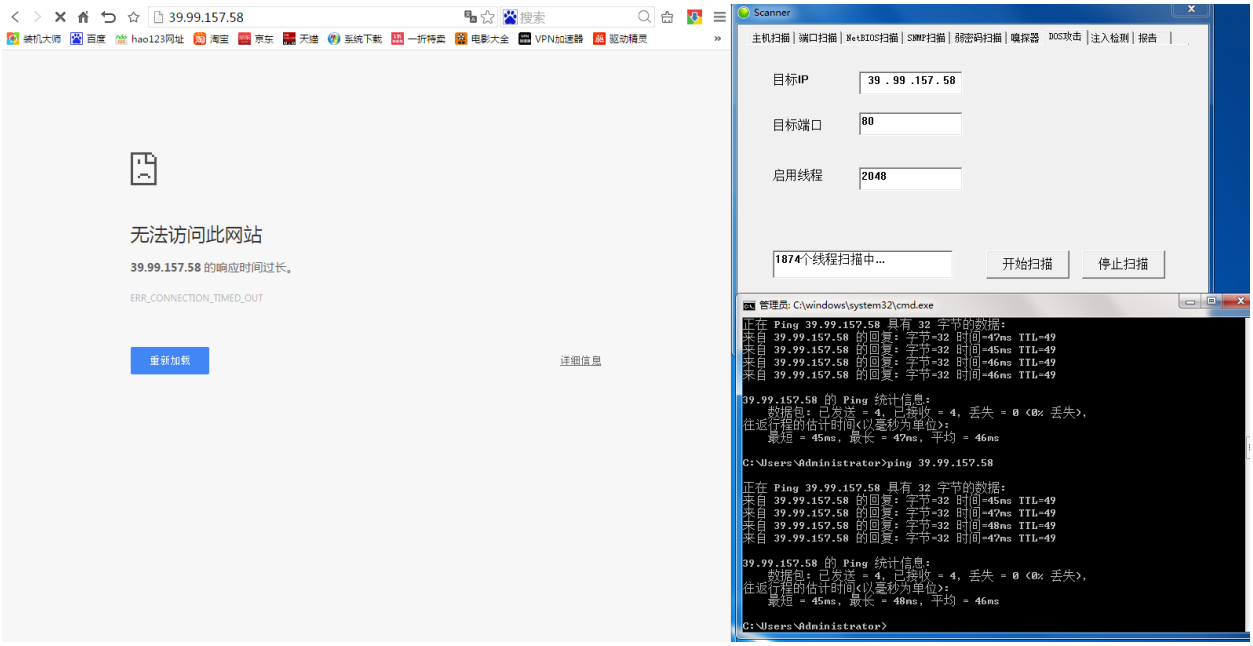


图 6-7 DOS 攻击功能模块测试结果图

6.1.8 注入检测功能模块测试

在注入检测功能模块中，为了测试结果，我尝试在服务器上搭建了一个简易的测试 Demo，网站由两部分构成，一个是登录页面 login.html，一个是验证是否登录成功的页面 respone.php，登录页面如图 6-8 所示：

图 6-8 注入检测测试登录页面

如果以 welcome+用户名的形式返回则说明登录成功，登录成功的页面如图 6-9 所示：

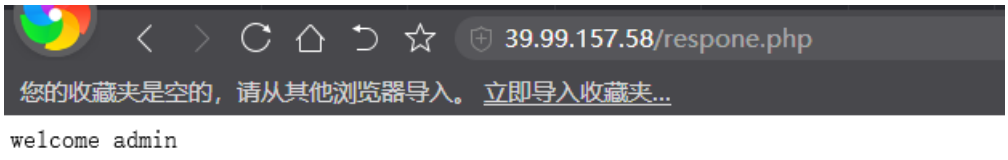


图 6-9 注入检测测试登录成功页面

如果登陆失败会返回“The username or password is wrong!”，登录失败的页面如图 6-10 所示：

图 6-10 注入检测测试登录失败页面

login.html 源代码如图 6-11 所示：

```
<!DOCTYPE html>
<html>
    <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
    </head>
    <body>
        <form action="respone.php" method="post">
            <table>
                <tr>
                    <td><span>用户名: </span></td>
                    <td><input type="text" name="username" id="username" /></td>
                </tr>
                <tr>
                    <td><span>密码: </span></td>
                    <td><input type="text" name="password" id="password" /></td>
                </tr>
                <tr>
                    <td></td>
                    <td align=right><input type="submit" value="确定" /></td>
                </tr>
            </table>
        </form>
    </body>
</html>
```

图 6-11 注入检测测试登录页面 login.html 源代码

respone.php 源代码如图 6-12 所示：

```
<?php
    if(($_POST["username"] == "admin") && ($_POST["password"] == "hacker")){
        echo "welcome ".$_POST["username"];
    }
    else{
        echo "The username or password is wrong!";
    }
?>
```

图 6-12 注入检测测试登录页面 respone.php 源代码

管理员根据以上测试分析可以得出结论，如果管理员把 welcome 一词当做注入漏洞的标志，若登录成功出现 welcome 一词，则说明网站存在注入漏洞，其结果如图 6-13 所示：

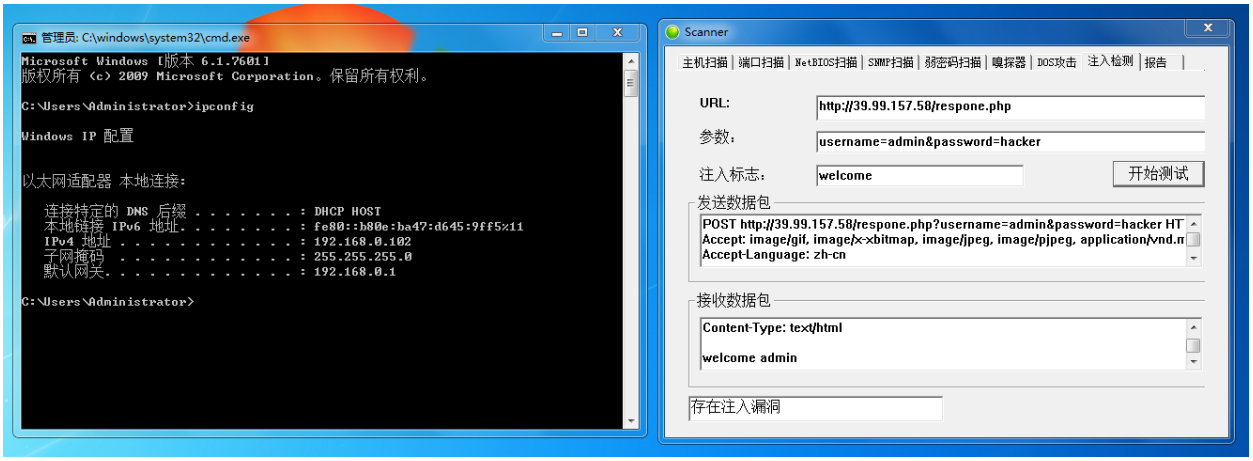


图 6-13 注入检测测试图

6.1.9 报告生成功能模块测试

在报告生成功能模块中，管理员输入目标 IP 地址，然后尝试打印部分功能扫描出来的结果，以 HTML 的形式生成，可以看出该结果与预期相符合，其结果如图 6-14 所示：

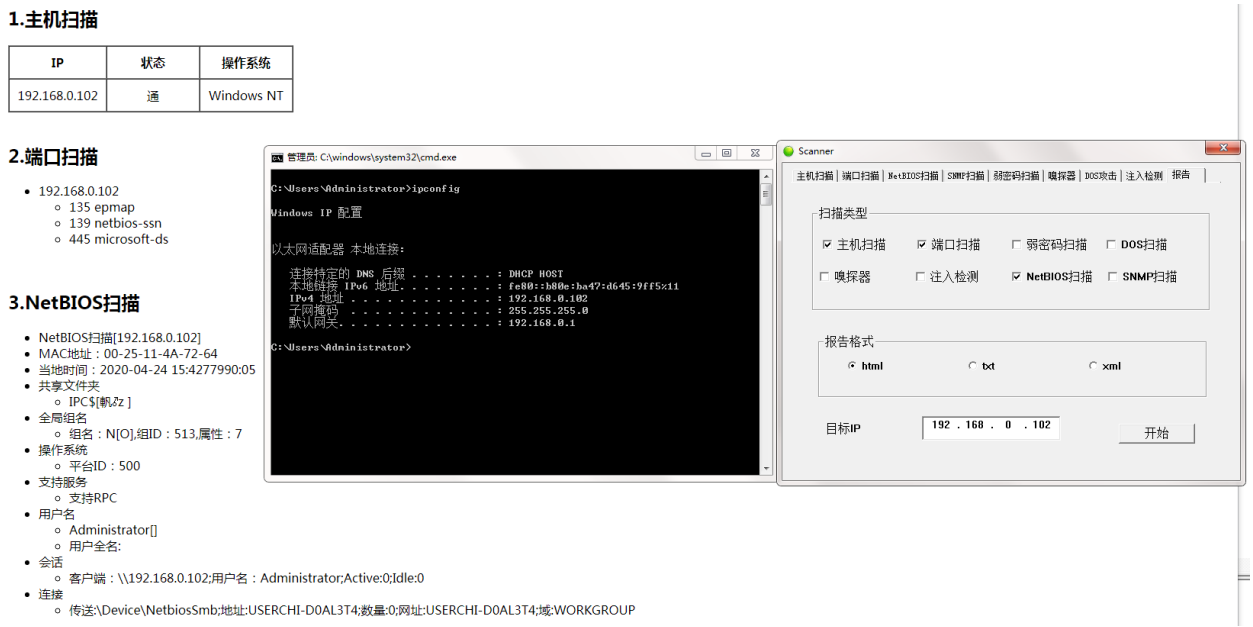


图 6-14 报告生成测试图

6.2 测试结果

通过上面的测试结果可以说明，本网络扫描器的主要功能模块可以正常运行，能够符合预期的结果，可以证明该网络扫描器设计方案是可行的。

7 总结与展望

7.1 设计工作总结

此网络扫描器基本能满足普通用户的使用需求，也存在着很多的不足，首先，该网络扫描器是在 Windows 下基于 MFC 开发的一个 EXE 程序，也就意味着这个程序只能在 Windows 下运行，不支持 macOS、Unix、Linux 等开发平台，其次是 Windows 平台向下的兼容性不好，程序在 win10 64 位的环境下会存在一些程序崩溃的问题，程序部分功能在 release 版本下正常运行，在 debug 版本下会出现运行崩溃的异常提醒。部分功能没有很好的实现，比如在做端口扫描的时候常常会出现卡顿，因为多线程的实现过于的简单，没能处理好线程之间的关系，接收到的数据包中文出现乱码，以及报告生成模块功能目前只能打印 HTML 格式的报告文件。

7.2 未来工作展望

本文所设计的网络扫描器由于时间和实验条件的限制，该网络扫描器还存在需要进一步改进的地方，主要表现在：

⑴ 该网络扫描器只能在 Windows 平台下运行，不支持 macOS、Unix、Linux 等其它主流操作系统。

⑵ 该网络扫描器的兼容性太差，在 32 位的环境下和 64 位的环境下运行结果会不太一样，需要进一步的去完善。

⑶ 网络扫描器的多线程实现过于简单，无法很好地处理线程间的关系，常常会因为卡顿而导致程序崩溃，需要进一步的去调整。

⑷ 网络扫描器接收到的数据只有英文字符不会乱码，中文字符会乱码，编码转换问题没有做好，也有待去改进和完善。

⑸ 网络扫描器目前报告只能打印 HTML 的形式，没有办法支持多种报告格式，希望能进一步的扩充其功能内容。

谢 辞

四年的本科生活即将告一段落，在这紧张而又丰富的学习生涯中，是老师和同学们的热心帮助让我受益良多。本论文的完成也正是我这四年来学习阶段的总结。

首先感谢我的导师王艳老师！王老师在我大学的最后学习阶段对我给予的帮助是无私的，她曾一遍又一遍地指出论文中的具体问题，严格把关，循循善诱。在此我向王老师表达我最衷心的感谢和最诚挚的敬意！王老师的谆谆教导，学生我铭记在心！

感谢周娟老师！周老师对我的课题和论文给予了多方面的指导和帮助，让我在学业上受益匪浅。周老师踏实严谨的学风，谦虚热情的为人对我产生了深深的影响！

感谢我的挚友们，在我遇到困难挫折的时候，是你们的关心和照顾激励着我走出低谷，在学习.工作和生活中不断前进。感谢创新创业中心的老师和同学们对我的支持和帮助，和你们在一起我感到非常愉快。

感谢学校为管理员创造的良好学习环境。

感谢朝夕相处的同学们。

最后要深深地感谢我的父母，是你们对我的深切关爱和细心照顾使我能够安心学习，做好课题；是你们对我的支持和鼓励使我能够乐观、积极地面对挫折与困难。因为有你们细心的关怀，使我能在未来的工作岗位上走的更高，看的更远，由衷的感谢你们。