实验一：扫描

扫描工具：Quickping

安装环境:windows 11

目标：对局域网进行IP地址扫描，寻找在当前局域网中存活的主机，为下

一步攻击做准备

实验步骤：

1、通过ipconfig查找本机所在ip的前缀号

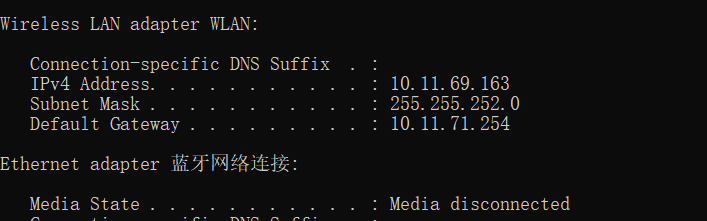


图1- 本机ip地址

2、使用quickping对本机所在ip前缀号进行查找：

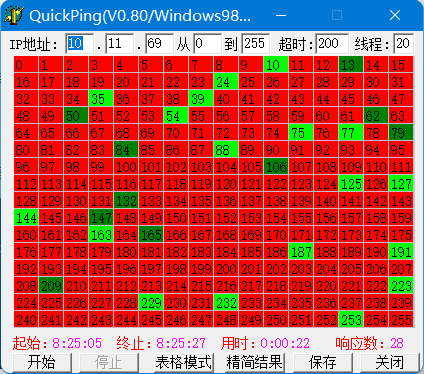


图2 – Quickping扫描精简结果



图3- QuickPing扫描详细结果

实验二：使用NAMP进行扫描

扫描工具：NAMP

安装环境：Windows11

安装版本：NMAP-7.80 Npcap-0.9993

目标：对局域网进行扫描，寻找可以攻击的目标，确认开放端口，为下一步攻击做准备：

实验步骤：

1、了解主机ip地址：

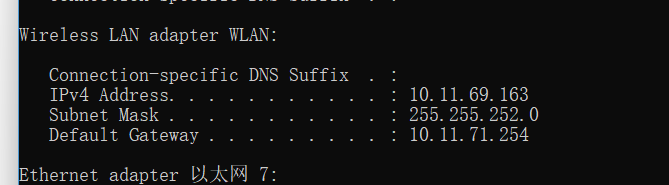


图1- 本机的内网地址

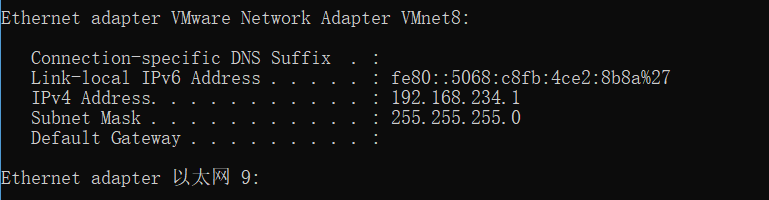


图2 本机的Vmware虚拟机内网地址

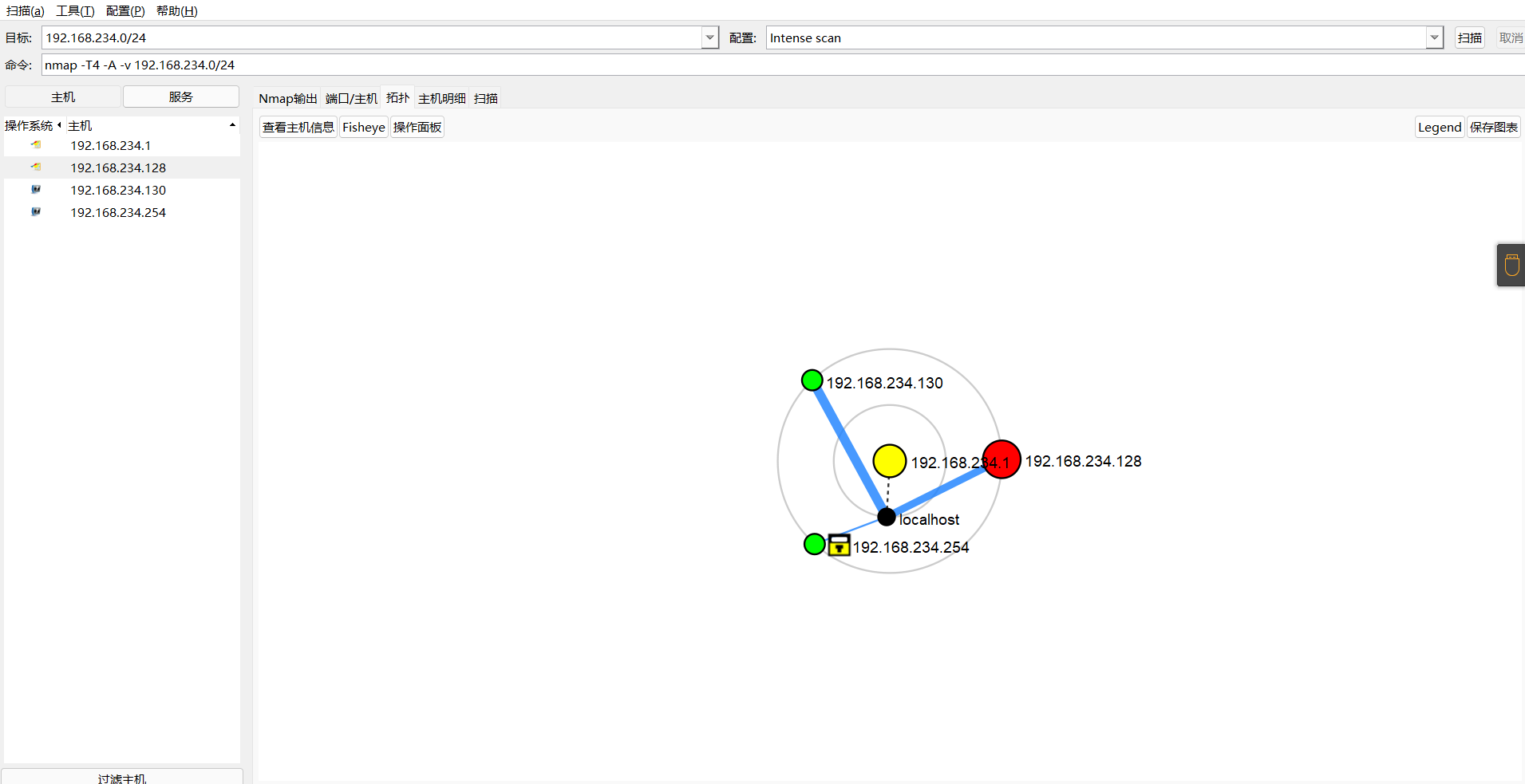


图3 扫描结果1

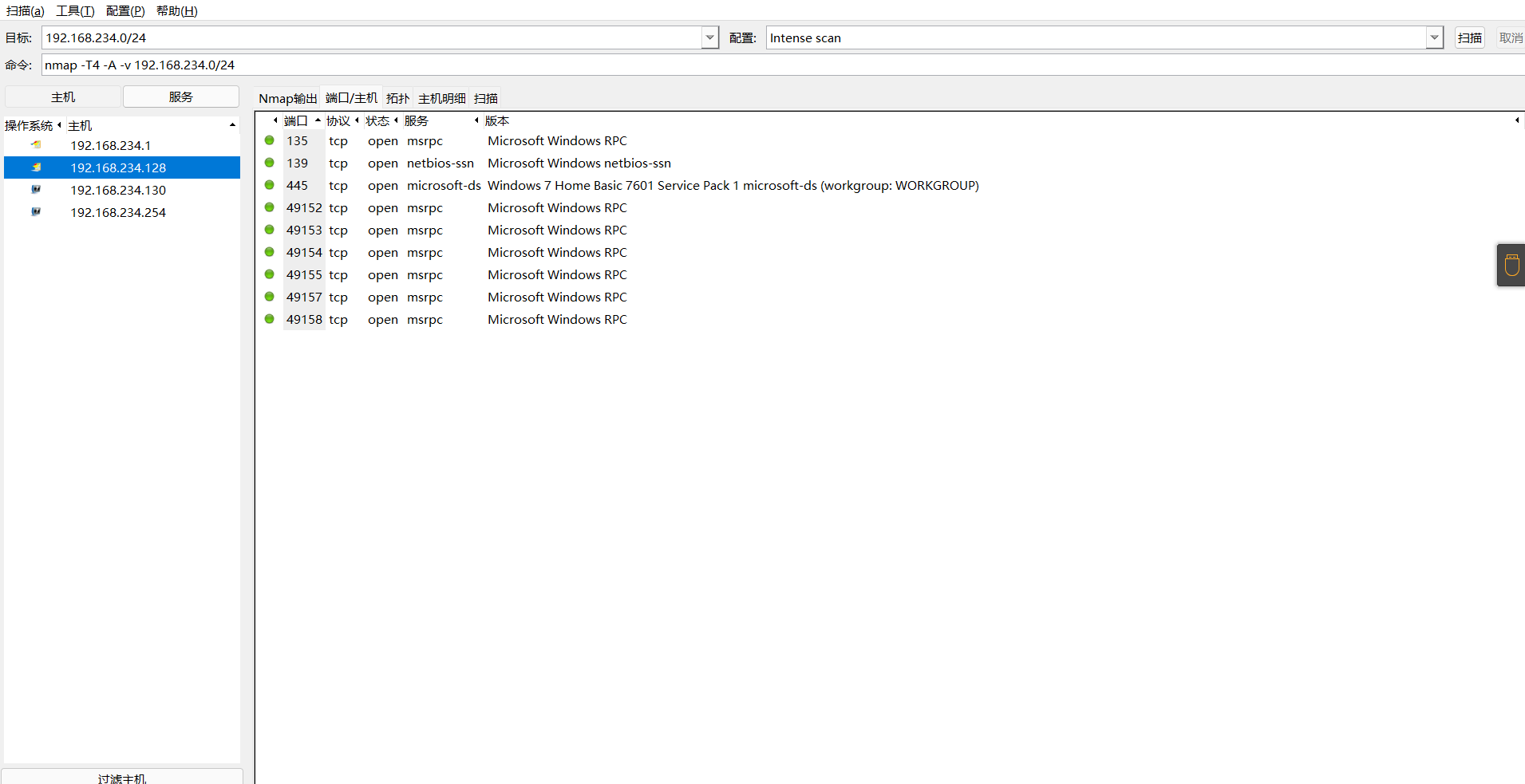


图4 扫描结果2

实验三：信息探测

使用搜索引擎（百度）

（1）site:站点域名



图1- 搜索引擎1



图2 搜索引擎2

实验4:Websitesniffer:

是一个网页嗅探器，它可以捕获浏览器访问过的数据，允许指定捕捉的文件类型， 包括html、文本、xml、css、音频视频、图片、脚本和flash(.swf)文件，允许选择 哪种类型的网站文件将被捕获的HTML文件，文本文件，XML文件，CSS文件，视频 /音频文件，图片，脚本和Flash。

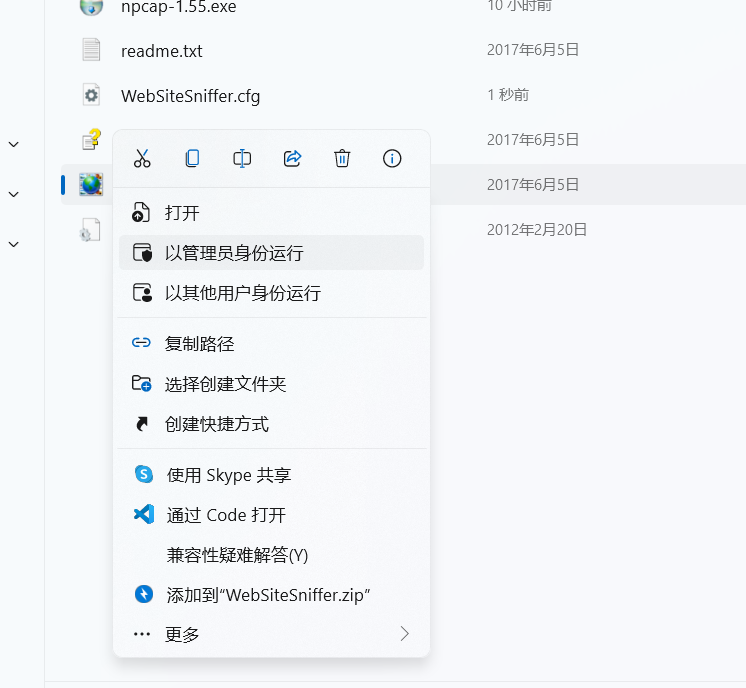


图1-运行websitesniffer



图2 配置Websitesniffer

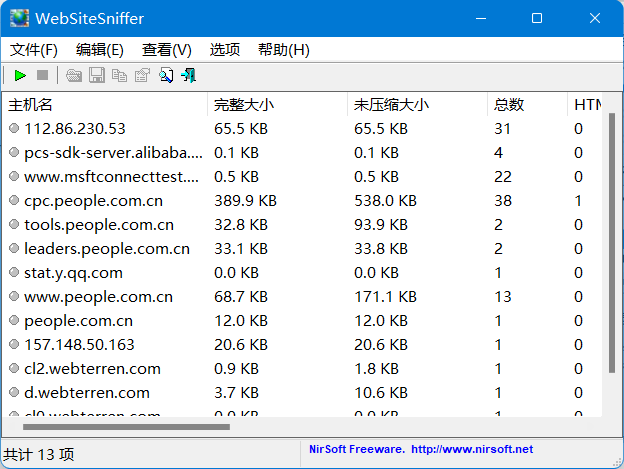


图3 抓包详情

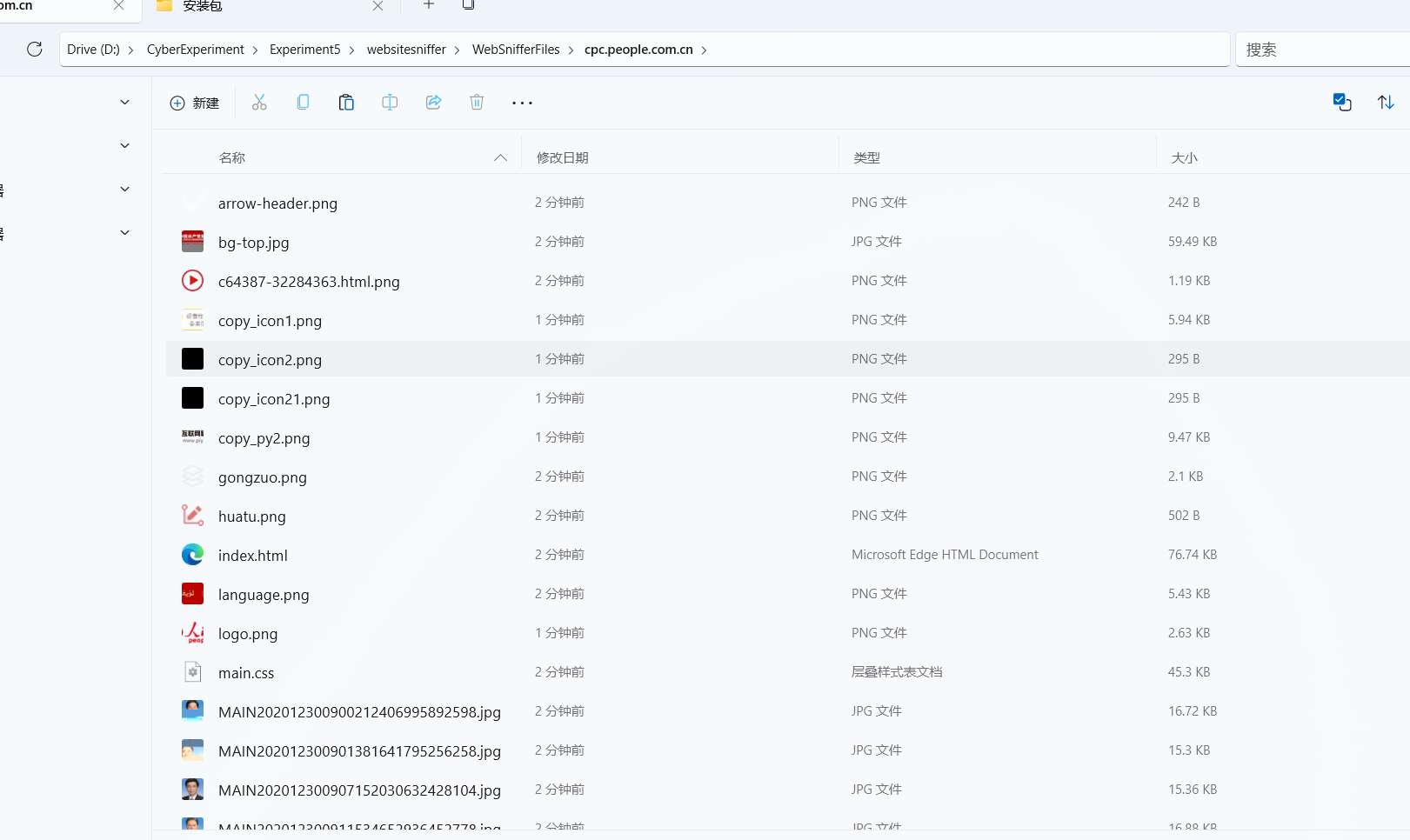


图4 捕获的文件

实验五：DirBuster

DirBuster 探测Web目录结构和隐藏的敏感文件 （1）了解网站结构 （2）获取敏感信息 ϕ后台管理界面 ②文件上传界面 ③网站源码 注：需Java运行环境（JRE）.

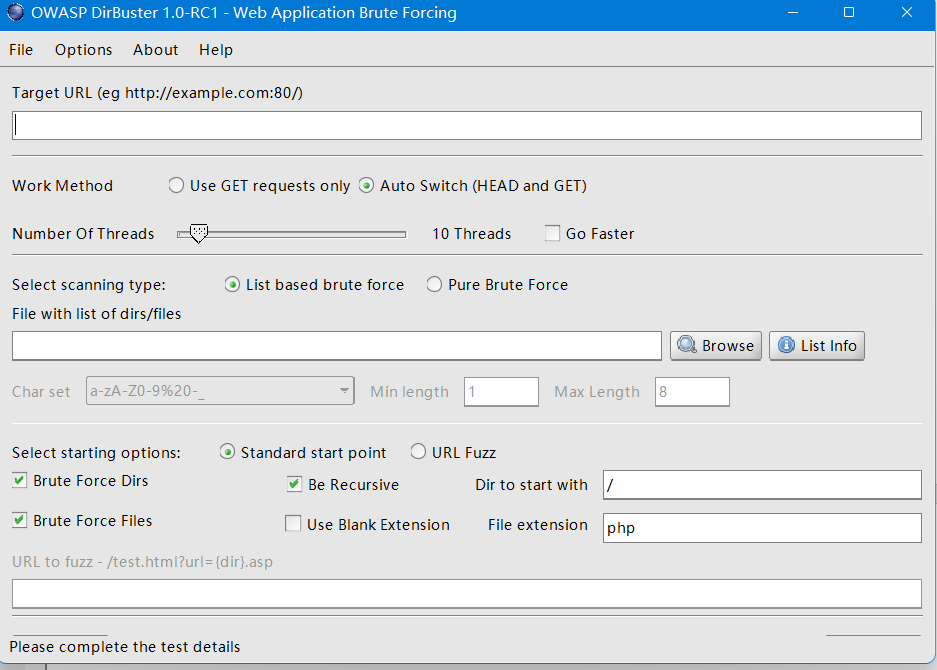


图1 DirBuster软件界面

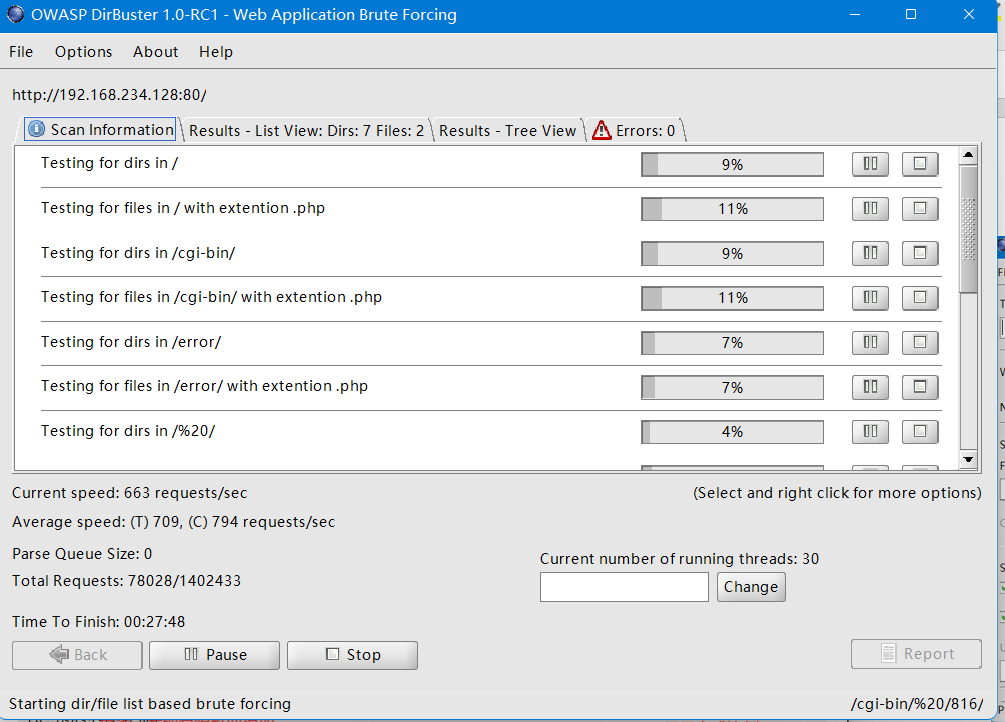


图2 工具破解中

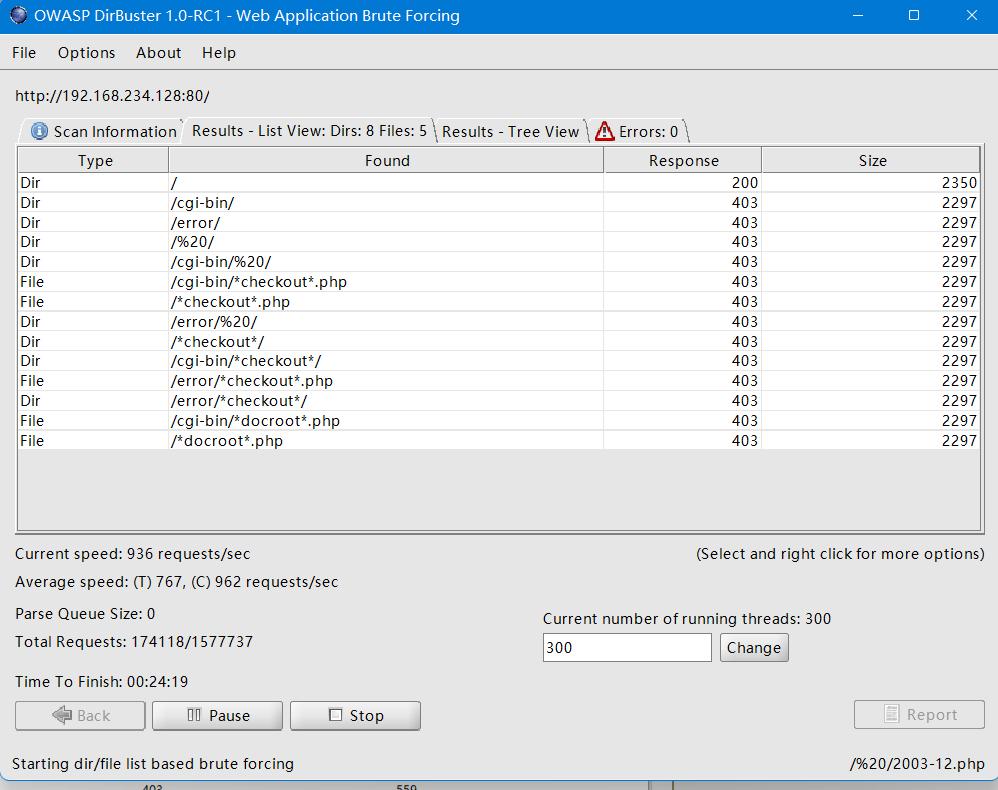


图3 猜解和爬行的结果

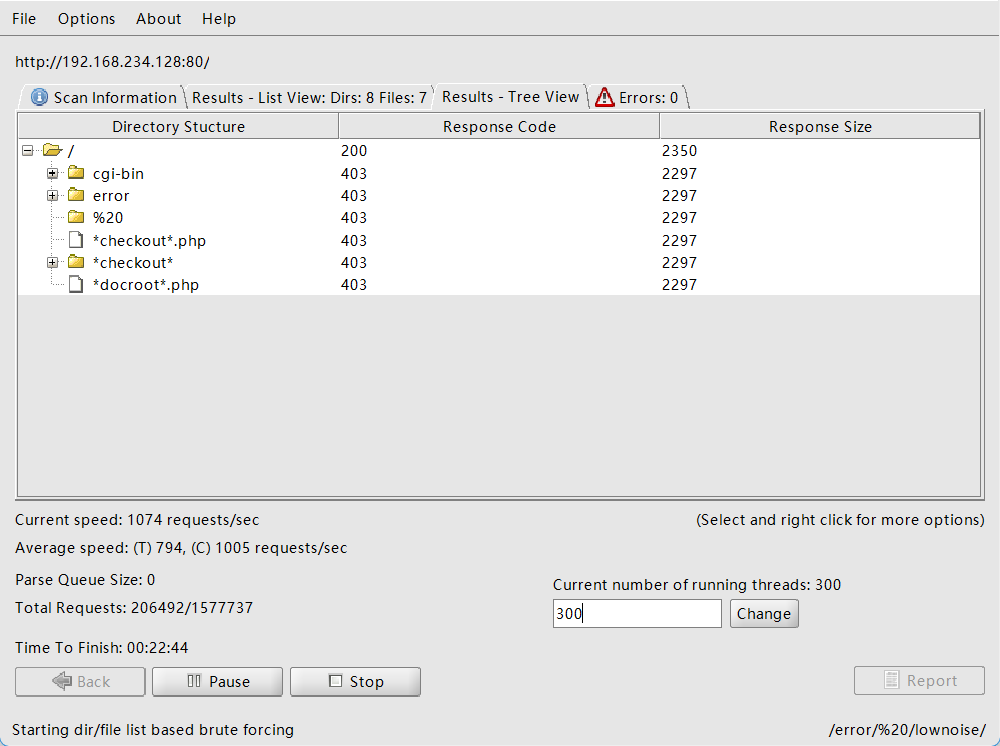


图4 树状结果展示

实验感想

通过本次实验，我学会到了一些web网络常用的信息探测工具，能够对一些简单的网络问题进行分析。