Web渗透技术的核心是发现Web漏洞，发现漏洞有手工和软件自动化扫描两种方式。对于用户验证漏洞、用户凭证管理问题、权限特权及访问控制漏洞、缓存漏洞、跨站脚本漏洞、加密漏洞、路径切换漏洞、代码注入漏洞、配置漏洞、数据和信息泄露、输入验证码漏洞、操作系统命令脚本注入、资源管理漏洞、SQL注入等常见Web漏洞，都可以通过Web扫描器进行扫描。

各个扫描器的功能和结果都不同，常见的包括HScan、HScan、X-Sccan、Acunetix Web Vulnerability Scanner、Jsky、Router Scan扫描工具等。本文主要讲解三个常见的Web漏洞扫描工具，分别是NMapp、ThreatScan和DirBuster。希望这篇基础性文章对你有所帮助，博主作为初学者，与你一起前行，如果有好的资源，也希望分享给我，加油!

下载地址：https://github.com/eastmountyxz/NetworkSecuritySelf-study
百度网盘：https://pan.baidu.com/s/1dsunH8EmOB_tlHYXXguOeA 提取码：izeb

文章目录

前文学习：
[网络安全自学篇] 一.入门笔记之看雪Web安全学习及异或解密示例
[网络安全自学篇] 二.Chrome浏览器保留密码功能渗透解析及登录加密入门笔记
[网络安全自学篇] 三.Burp Suite工具安装配置、Proxy基础用法及暴库示例
[网络安全自学篇] 四.实验吧CTF实战之WEB渗透和隐写术解密
[网络安全自学篇] 五.IDA Pro反汇编工具初识及逆向工程解密实战
[网络安全自学篇] 六.OllyDbg动态分析工具基础用法及Crakeme逆向破解
[网络安全自学篇] 七.快手视频下载之Chrome浏览器Network分析及Python爬虫探讨

前文欣赏：
[渗透&攻防] 一.从数据库原理学习网络攻防及防止SQL注入
[渗透&攻防] 二.SQL MAP工具从零解读数据库及基础用法
[渗透&攻防] 三.数据库之差异备份及Caidao利器
[渗透&攻防] 四.详解MySQL数据库攻防及Fiddler神器分析数据包

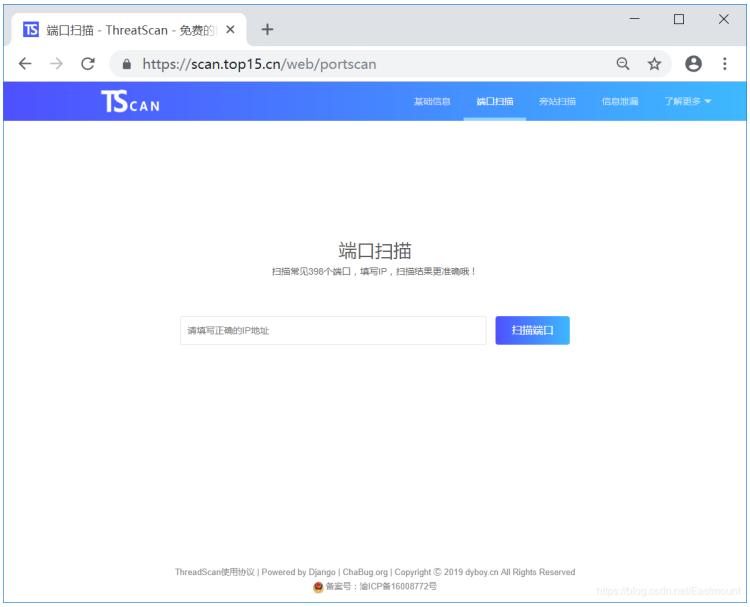
参考文献：
《安全之路Web渗透技术及实战案例解析》陈小兵老师
ThreatScan-端口扫描的实现 - DYBOY大神
https://edu.51cto.com/center/course/lesson/index?id=107002

Nmap详解 - 谢公子大神
nmap基本使用方法 - bonelee
nmap命令-----基础用法
渗透之——目录扫描神器DirBuster用法

一.ThreatScan在线扫描

ThreatScan是一款扫描器，主要用于渗透测试的第一阶段：信息搜集。这里非常推荐 DYBOY大神的博客，地址为：
https://blog.dyboy.cn/
https://github.com/dyboy2017/TScan

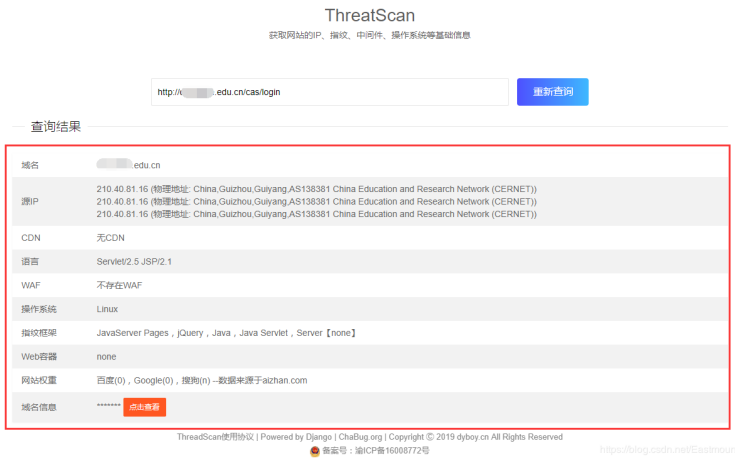
ThreatScan的网址为：https://scan.top15.cn，运行结果如下图所示。



本文以某大学的信息系统为例，进行简单的测试。

第一步：基础信息扫描
包括域名、IP地址、有无CDN、编程语言、是否存在WAF（Web应用防护系统）、操作系统、指纹框架、Web容器、网络权重等。注意，ThreatScan通过Web指纹识别，发现该网站采用Java进行开发。

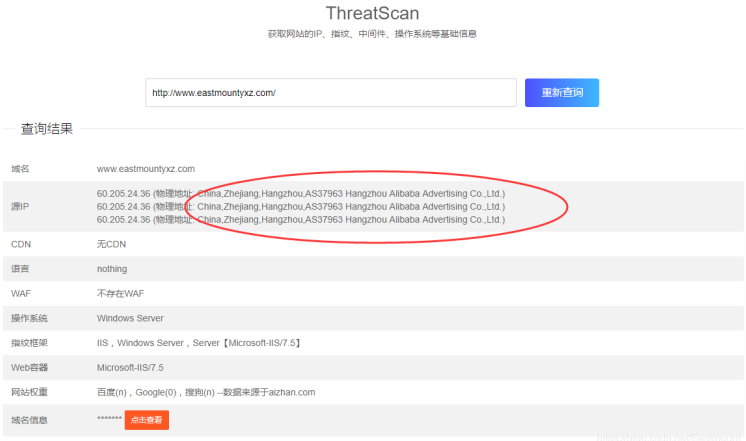
IP地址为：210.40.81.16



可以找个在线网站测试其IP物理位置。

再如，以作者在阿里云搭建的一个网站为例（http://www.eastmountyxz.com/），其运行结果如下图所示，Hangzhou Alibaba。

IP地址为：60.205.24.36



第二步：端口扫描

接着将IP地址填写到端口处，进行相关扫描。端口扫描是获取目标主机的端口信息显得十分有必要，通过一些常见端口，可以大致得出目标主机运行的服务，为后续渗透测试薄弱点提供参考。

第三步：旁站扫描

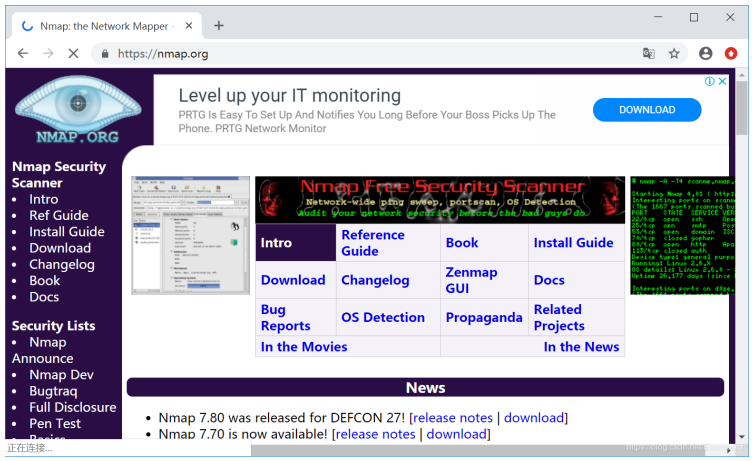
旁站扫描能扫描与该IP地址挂靠的其他网站，这有利于Web渗透，可能旁站存在漏洞。

第四步：信息泄露查询

二.Nmap工具扫描端口及服务

PS：非常推荐 大神谢公子 的网络安全文章，希望读者可以查阅。下面也参考了他的内容。

Nmap是一款开源免费的网络发现（Network Discovery）和安全审计（Security Auditing）工具。软件名字Nmap是Network Mapper的简称。Nmap最初是由Fyodor在1997年开始创建的。随后在开源社区众多的志愿者参与下，该工具逐渐成为最为流行安全必备工具之一。官网为：www.nmap.org。



一般情况下，Nmap用于列举网络主机清单、管理服务升级调度、监控主机或服务运行状况。Nmap可以检测目标机是否在线、端口开放情况、侦测运行的服务类型及版本信息、侦测操作系统与设备类型等信息。

Nmap的优点包括：

- 灵活。支持数十种不同的扫描方式，支持多种目标对象的扫描
- 强大。Nmap可以用于扫描互联网上大规模的计算机
- 可移植。支持主流操作系统：Windows/Linux/Unix/MacOS等等；源码开放，方便移植
- 简单。提供默认的操作能覆盖大部分功能，基本端口扫描nmap targetip，全面的扫描nmap –A targetip
- 自由。Nmap作为开源软件，在GPL License的范围内可以自由的使用
- 文档丰富。Nmap官网提供了详细的文档描述。Nmap作者及其他安全专家编写了多部Nmap参考书籍
- 社区支持。Nmap背后有强大的社区团队支持

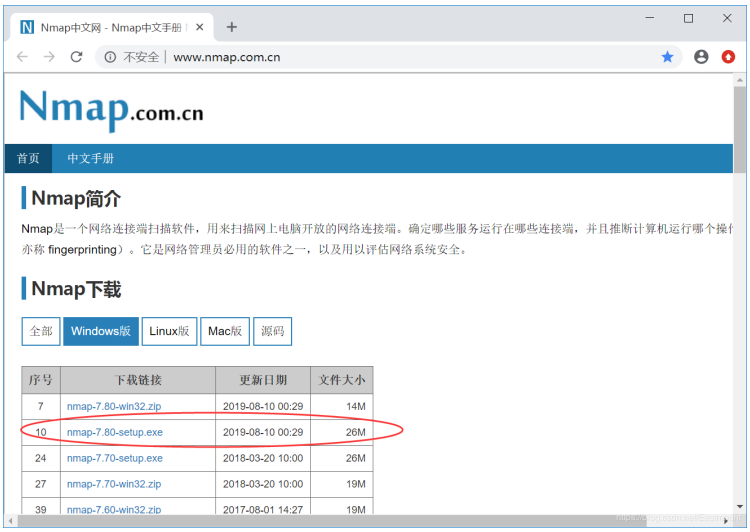
Nmap包含四项基本功能：

- 主机探测 (Host Discovery)
- 端口扫描 (Port Scanning)
- 版本侦测 (Version Detection)
- 操作系统侦测 (Operating System Detection)

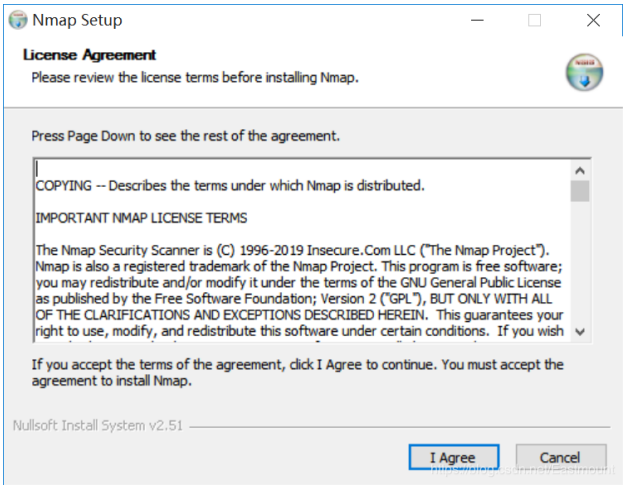
而这四项功能之间，又存在大致的依赖关系(通常情况下的顺序关系，但特殊应用另外考虑)，首先需要进行主机发现，随后确定端口状态，然后确定端口上运行的具体应用程序和版本信息，然后可以进行操作系统的侦测。而在这四项功能的基础上，nmap还提供防火墙和 IDS 的规避技巧，可以综合运用到四个基本功能的各个阶段。另外nmap还提供强大的NSE(Nmap Scripting Language)脚本引擎功能，脚本可以对基本功能进行补充和扩展。

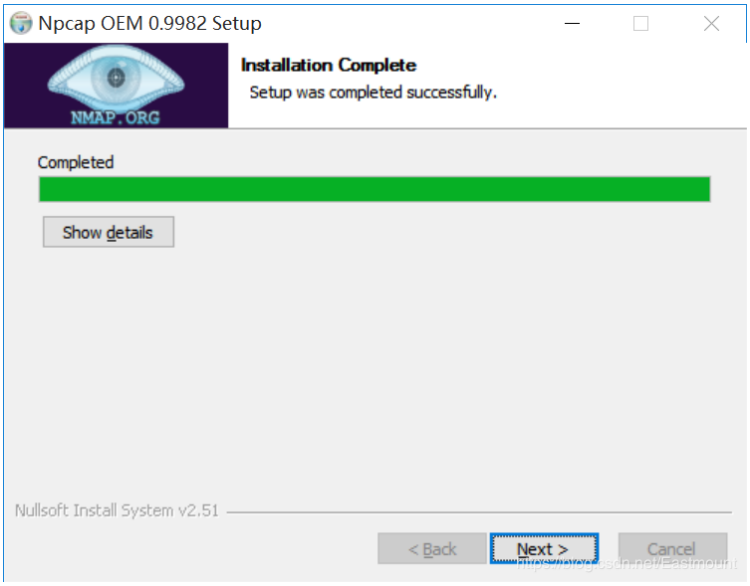
下面讲解一个可视化的Nmap工具——Zenmap。

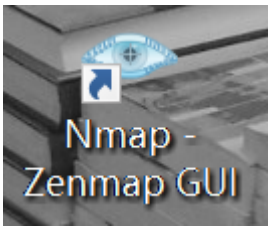
第一步：从官网下载工具（http://www.nmap.com.cn/）。



第二步：安装Nmap软件。





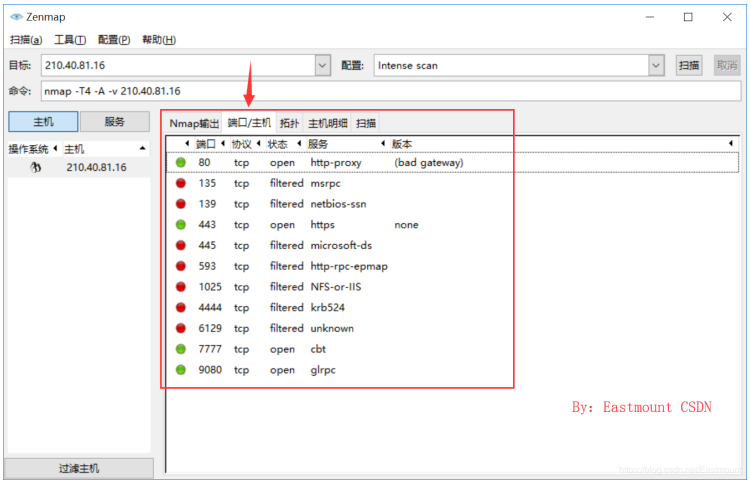


第三步：运行软件之后，如下图所示，接着输入IP地址，点击“扫描”。

命令：namp -T4 -A -v 210.40.81.16

Zenmap底层其实就是调用Nmap的命令行，运行交互式结果。

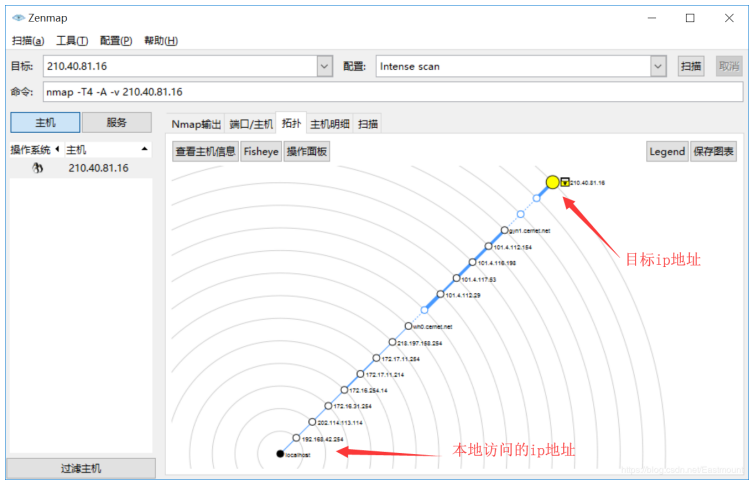
第四步：点击“端口/主机”查询开放的端口及协议，如80、443、7777、9080。



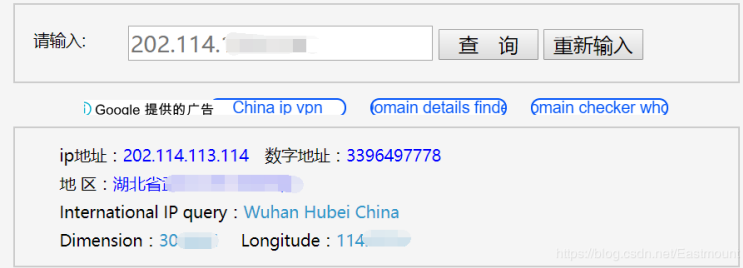
常见服务对应端口号：

服务	端口号
HTTP	80
HTTPS	443
Telnet	23
FTP	21
SSH（安全登录）、SCP（文件传输）、端口重定向	22
SMTP	25
POP3	110
WebLogic	7001
TOMCAT	8080
WIN2003远程登录	3389
Oracle数据库	1521
MS SQL* SEVER数据库sever	1433
MySQL 数据库sever	3306

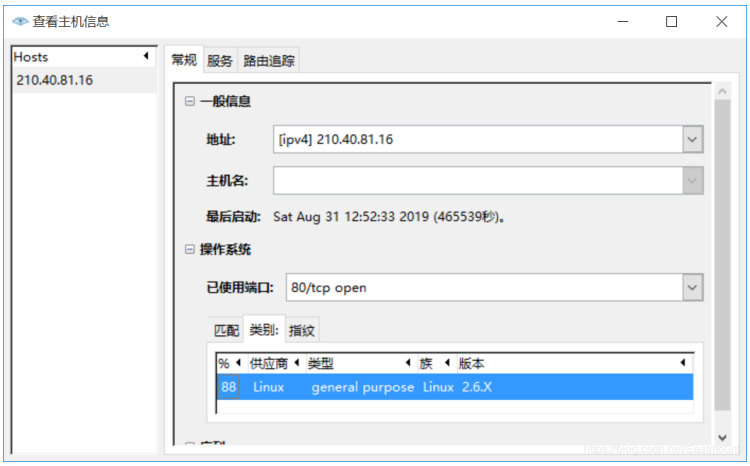
第五步：点击“拓扑”按钮可以查看UP地址拓扑图，方便观察网络跳数，尤其是大的网段。



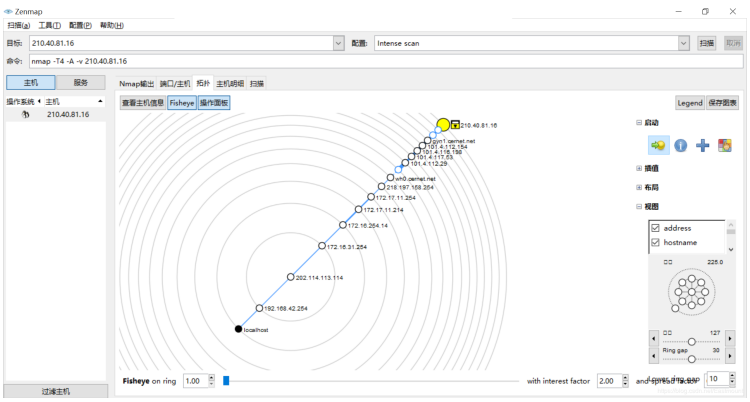
网上找个网址查询本地localhost地址，可以看到物理位置。



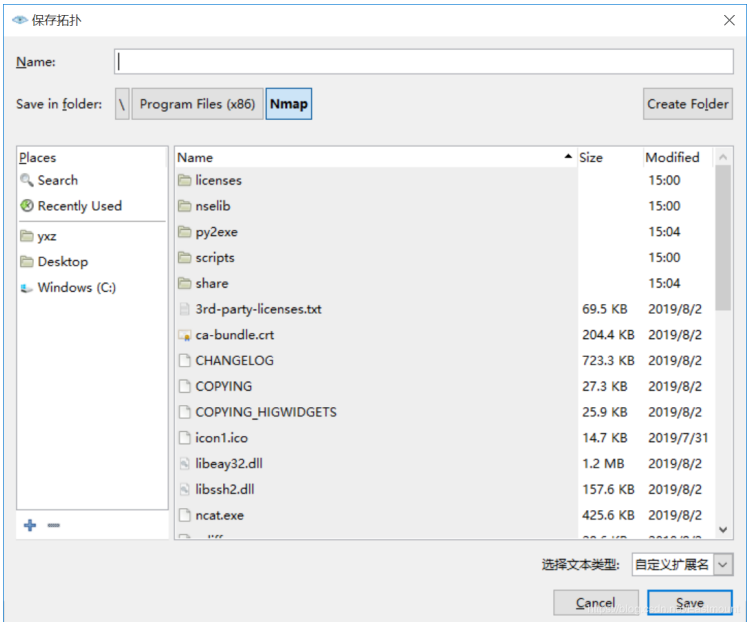
点击子按钮“查看主机信息”，如下图所示。

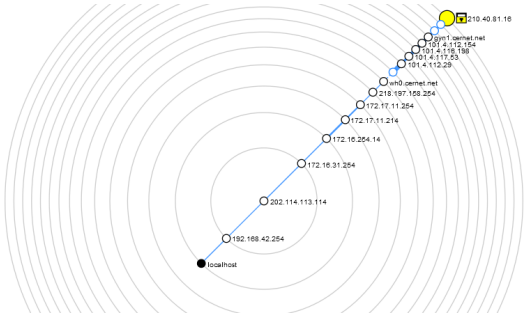


点击“操作面板”如下图所示。

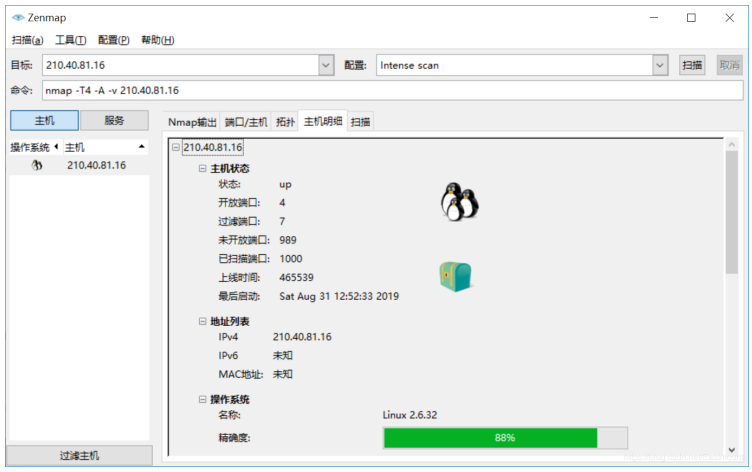


同时，可以保存拓扑图，如下图所示。

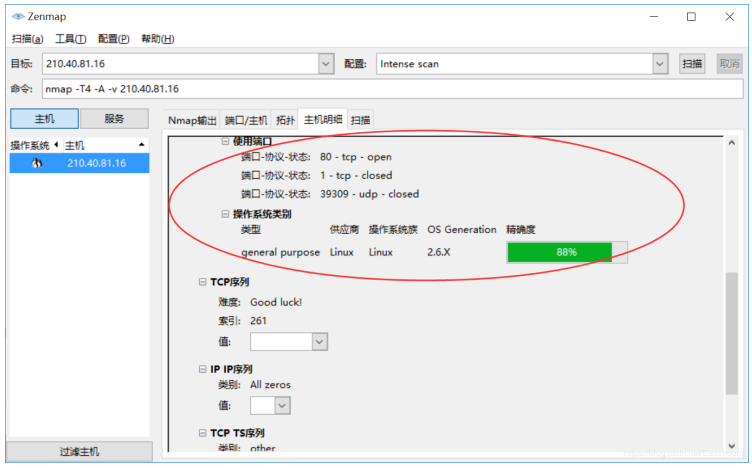




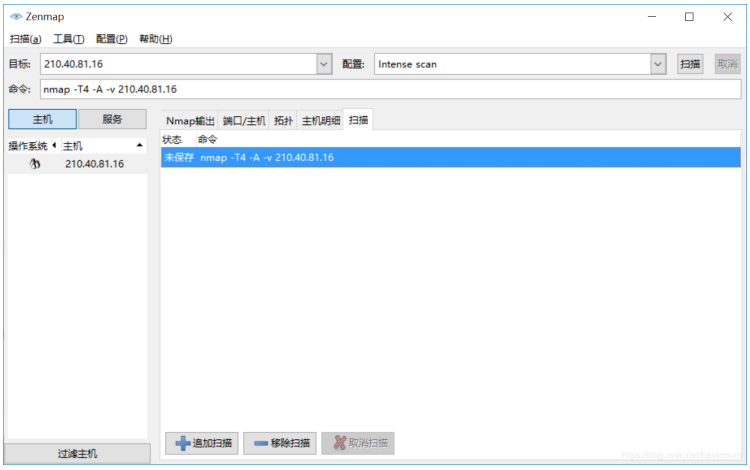
第六步：点击“主机明细”按钮，显示详情信息如下图所示。



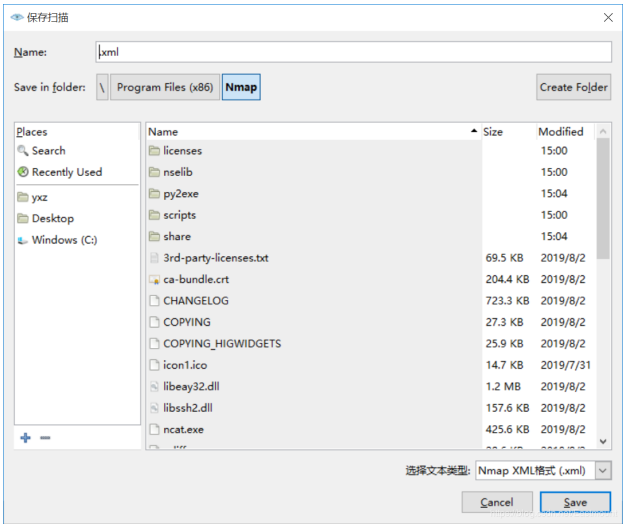
包括端口信息和操作系统类别信息。

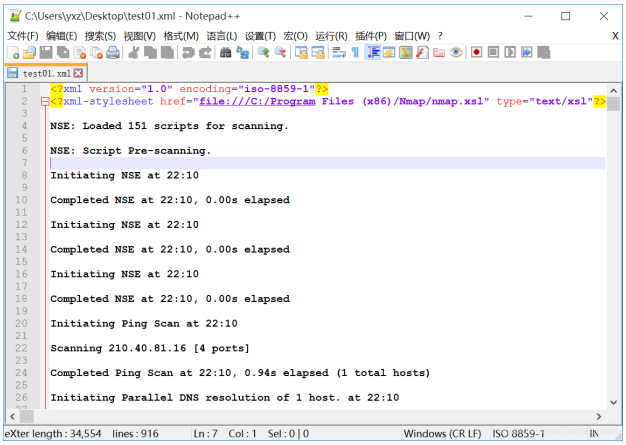


第七步：点击最后一个子按钮“扫描”，按下Ctrl+S能保存扫描信息。

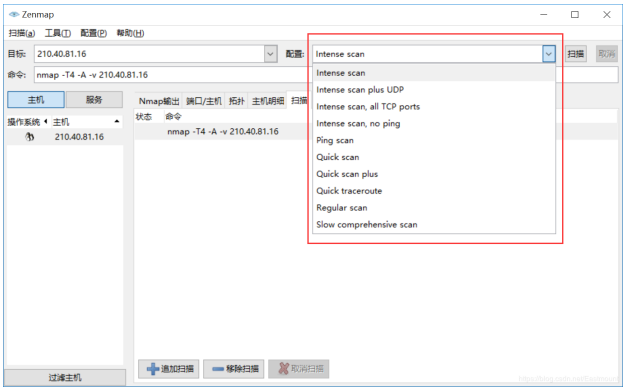


保存结果如下图所示。





同时，Zenmap还有其他功能，包括自定义模板等。

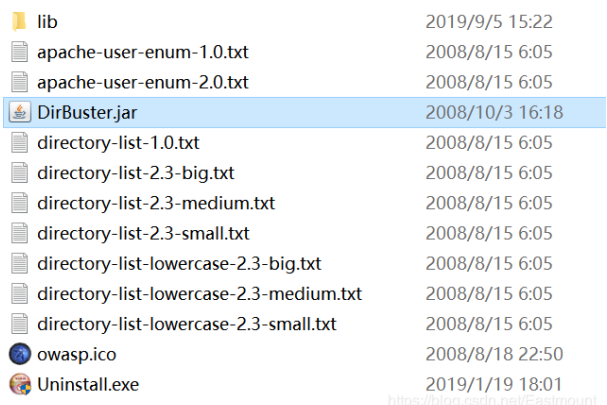


Python通过三次握手来遍历IP端口，看阅读下面这篇博客：
https://blog.csdn.net/qq_33936481/article/details/53257911

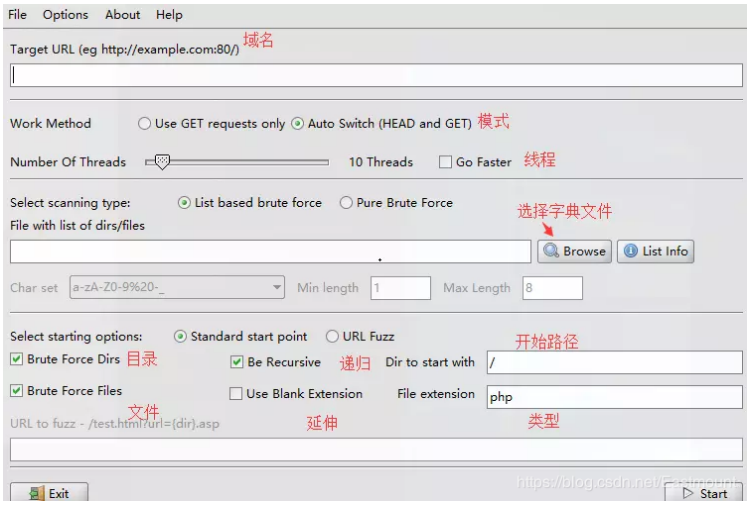
三.DirBuster工具扫描网站资源

DirBuster是Owasp(Open Web Application Security Project)开发的一款专门用于探测网站目录和文件(包括隐藏文件)的工具。由于使用Java编写，电脑中要装有JDK才能运行，它是一个多线程Java应用程序，旨在强制Web /应用程序服务器上的目录和文件名。当然，还有其他的网站目录扫描工具，如wwwscan 、御剑、椰树、北极熊等。

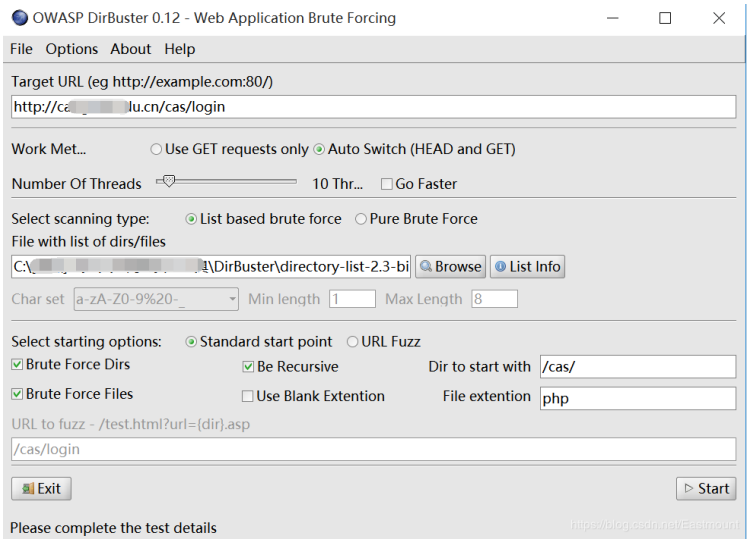
第一步：下载软件，并点击“DirBuster.jar”文件。



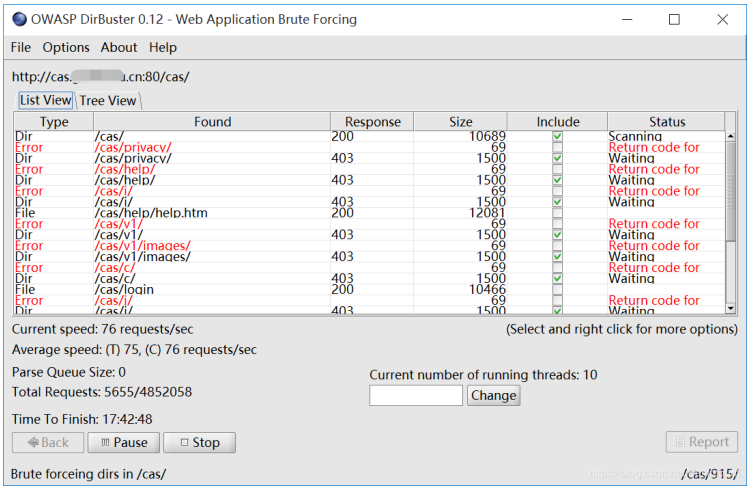
第二步：软件打开如下图所示。

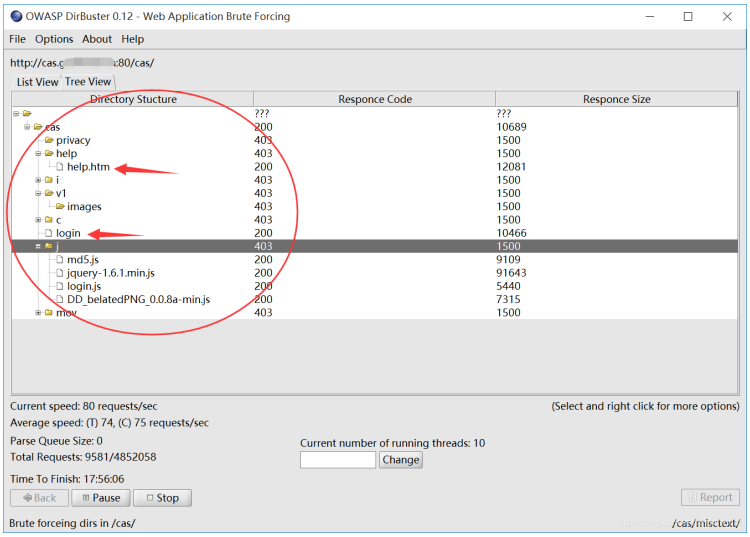


第三步：输入URL，使用List模式并点击Browse加载字典文件，点击“Start”开始扫描。



第四步：运行过程如下图所示，包括List View和Tree View两种模式。





更多操作，建议读者下来查找相关材料，后续随着作者深入学习，会尝试结合实例讲解。

四.总结

希望基础性文章对您有所帮助，作者也是这个领域的菜鸟一枚，希望与您共同进步。

(By:Eastmount 2019-09-05 深夜12点 http://blog.csdn.net/eastmount/)