WEB漏洞挖掘之网络信息探测

2016-11-14 中国Cold 京东安全应急响应中心

等你点蓝字关注都等出蜘蛛网了

信息探测

“而我们在进行安全渗透测试前，首先要进行的也是先去了解目标系统的信息，也就是信息探测，搜集目标系统的资料，总而言之就是搜集一切和网站有关的信息，通过信息收集后我们可以更加有效的策划对目标系统的渗透测试方案。”

我们在搜集目标系统信息的时候主要需要搜集的是：

目标服务器系统信息（IP,服务器所用系统等）；

目标网站子域名；

目标网站（服务器）的开放端口；

目标域名信息、目标网站内容管理系统（CMS）等。

一、子域名搜集

搜集子域名的方式有很多种，理论上来说，我们是没办法把所有的子域名全部找出来，我们可以找的只是被搜索引擎收录的域名。

（一）引擎命令搜集

site命令

```
site:ichunqiu.com
```

复制代码

site:域名

如，以ichunqiu.com为例，进行子域名搜索：

我们可以看到搜索出了5万多条结果，ichunqiu.com的子域名也被搜索出来。但是我们搜索一些大型网站的时候，搜索出的结果可能高达上百万、千万，由于搜索数据量太庞大，想搜集到所有的子域名是很困难的，我们一般只取前几页做信息搜集。

（二）其他的搜索引擎搜索指令

其他的搜索引擎搜索指令可以让我们更好的进行信息搜集，用最少的时间找到你要的信息。搜索指令还有很多，需要了解的同学可以去百度一下相关的信息，这里只介绍几种常用的。

intitle：

可以把搜索结果限定在网页标题的查询上。

```
01.  intitle:后台登录
```

复制代码

可以看到利用intitle:后台登录，搜索出了很多被搜索引擎收录的网站后台。

inurl：

搜索查询词出现在url中的页面。

```
inurl:admin
```
复制代码

可以看到利用inurl:admin，搜索出的url中都是带admin的。

(三) 搜索指令漏洞挖掘思路

这里给大家一个简单的漏洞挖掘思路，教大家如何用搜索指令来挖掘漏洞。

```
intitle:index of
```
复制代码

在搜索引擎输入上面的指令可以找到很多目录遍历漏洞网站。

index of是 WEB服务器的目录列表，而intitle:index of就是搜索指定网页标题为index of的内容，所以就可以搜索到那些允许目录遍历的服务器内容。

（四）子域名在线查询工具

现在有很多的子域名在线查询工具，自动化的网页结果抓取，都可以让我们更快的搜集子域

名。

http://subdomain.chaxun.la

http://tool.chinaz.com/subdomain

http://i.links.cn/subdomain

这一类工具只需要输入主域名就可以查询出子域名，相比用搜索引擎来搜集子域名更加的快、方便。但是对一些大型网站来说，包括子域名查询工具等查找到的子域名都是不完全的，搜集子域名还可以用域名枚举等方式来进行搜集。

二、域名信息查询

（一）whois查询

“whois（读作“Who is”，非缩写）是用来查询域名的IP以及所有者等信息的传输协议。简单说，whois就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、域名注册商）。通过whois来实现对域名信息的查询。早期的whois查询多以命令列接口存在，但是现在出现了一些网页接口简化的线上查询工具，可以一次向不同的数据库查询。网页接口的查询工具仍然依赖whois协议向服务器发送查询请求，命令列接口的工具仍然被系统管理员广泛使用。whois通常使用TCP协议43端口。每个域名/IP的whois信息由对应的管理机构保存。”

whois查询可以对域名的所有者信息、注册商、域名服务器等信息进行查询

如：以ichunqiu.com为例，进行whois查询。

域名 ichunqiu.com 的信息 以下信息更新时间：2016-07-04 17:19:00 立即更新

域名	ichunqiu.com [whois 反查] 其他常用域名后缀查询： cn com cc net org
注册商	HICHINA ZHICHENG TECHNOLOGY LTD.
联系人	zhang yachi [whois反查]
联系方式	huangping@integritytech.com.cn [whois反查]
更新时间	2016年01月24日
创建时间	2013年06月22日
过期时间	2020年06月22日
域名服务器	grs-whois.hichina.com
DNS	NS1.JIASULE.ORG NS2.JIASULE.ORG
状态	客户端设置禁止转移(clientTransferProhibited)

whois查询的在线工具很多，如比较大型的网站站长之家等。

站长之家whois查询：http://whois.chinaz.com

端口扫描

“端口扫描是指某些别有用心的人发送一组端口扫描消息，试图以此侵入某台计算机，并了解其提供的计算机网络服务类型（这些网络服务均与端口号[/url]相关）。端口扫描是计算机解密高手喜欢的一种方式。攻击者可以通过它了解到从哪里可探寻到攻击弱点。实质上，端口扫描包括向每个端口发送消息，一次只发送一个消息。接收到的回应类型表示是否在使用该端口并且可由此探寻弱点。”

端口扫描可以说是安全渗透测试的基础。通过端口扫描可以基本确定一个系统的一些信息，结合可能被利用的端口漏洞，对进行深入的安全测试提供信息。

一、NMAP《网络映射器》

“nmap是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端。确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统（这是亦称 fingerprinting）。它是网络管理员必用的软件之一，以及用以评估网络系统安全。”

检测活在网络上的主机（主机发现）；

检测主机上开放的端口（端口发现或枚举）；

检测到相应的端口（服务发现）的软件和版本；

检测操作系统，硬件地址，以及软件版本；

检测脆弱性的漏洞（Nmap的脚本）。

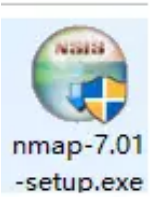
（一）nmap安装

1、软件下载

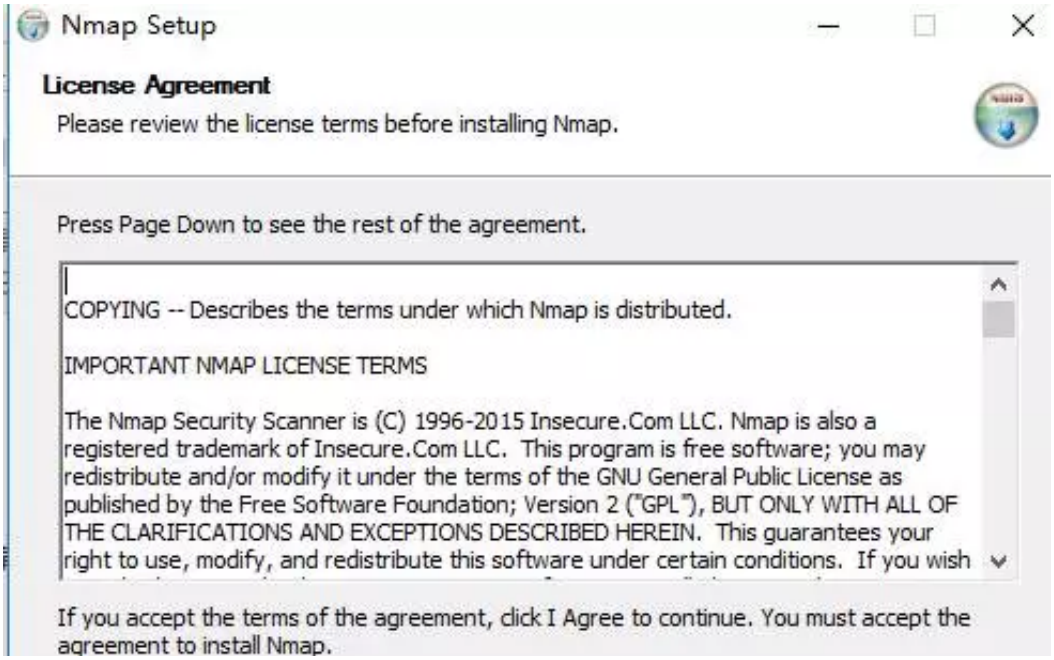
```
01.  百度网盘: 链接: [url]http://pan.baidu.com/s/1c2x8LcG[/url] 密码: cc4m
复制代码
```

```
01.  官网下载: https://nmap.org
复制代码
```

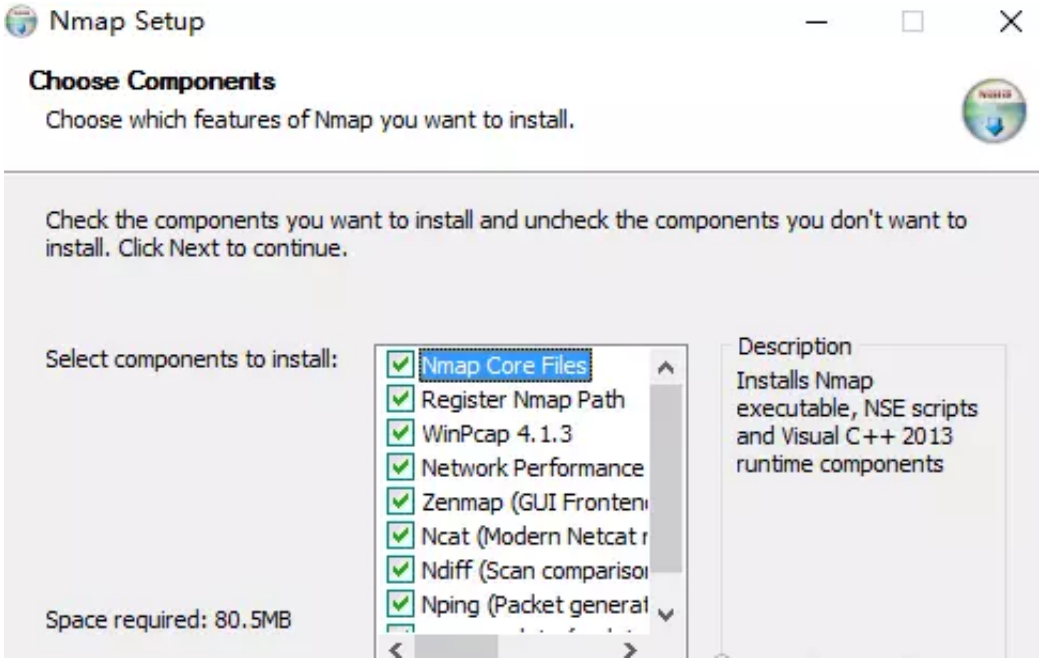
2、打开安装包



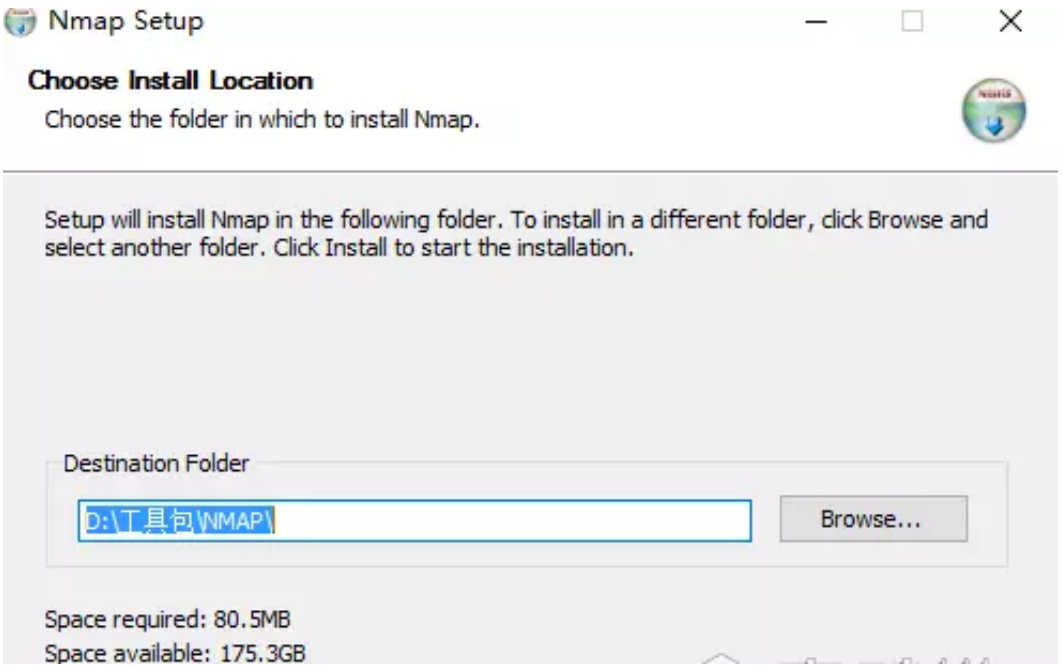
3、阅读Nmap许可协议，点击I Agree下一步。



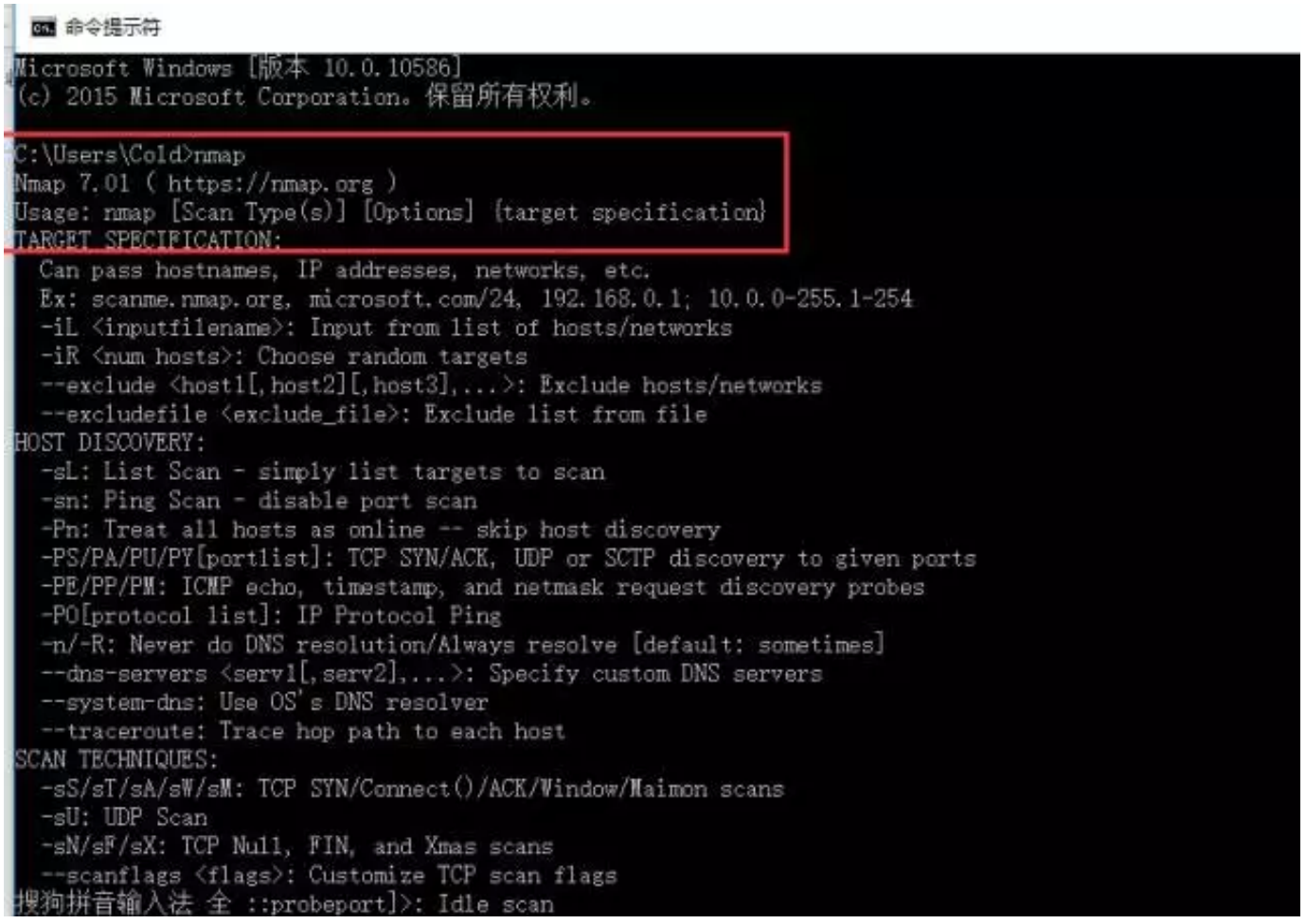
4、选择安装的组件，一般默认下一步就好，点击Next下一步。



5、选择安装路径，根据你的需要选择。接下来点击install安装即可。



6、打开CMD，输入nmap，返回nmap帮助信息，安装成功。



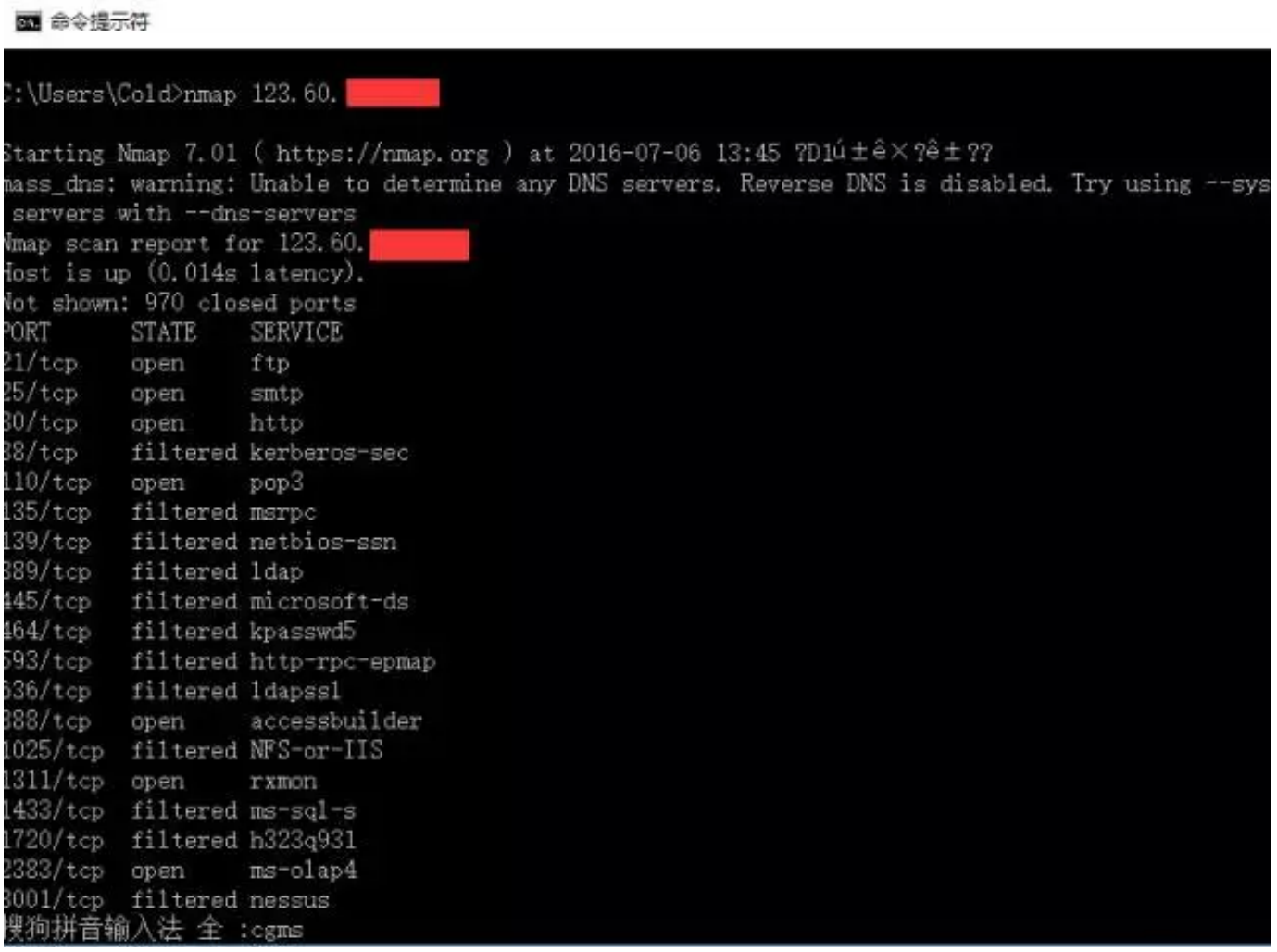
（二）nmap基础使用方法

目标系统开放端口扫描

```
01.  nmap 192.168.1.1
     复制代码
```

扫描目标系统1-10000范围内所开放的端口。

如下图：

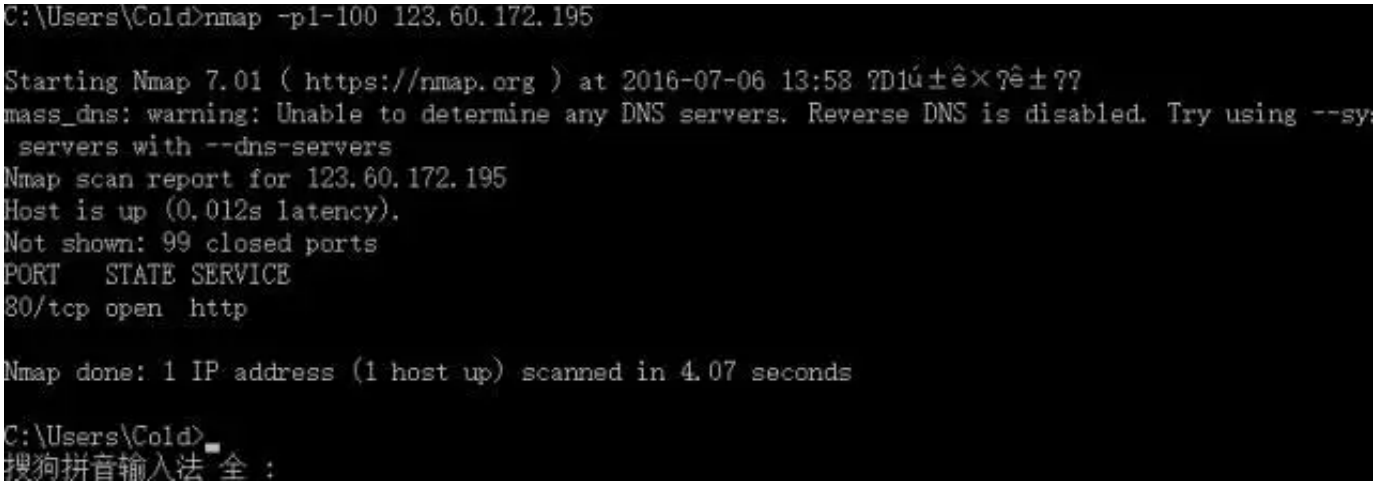


端口自定义扫描

```
01. nmap -p1-100 192.168.1.1
    复制代码
```

默认扫描目标1-10000范围内的端口号。-p 可以自定义设置我们要扫描的端口。-p1-100就是扫描1到100的端口。

如下图：

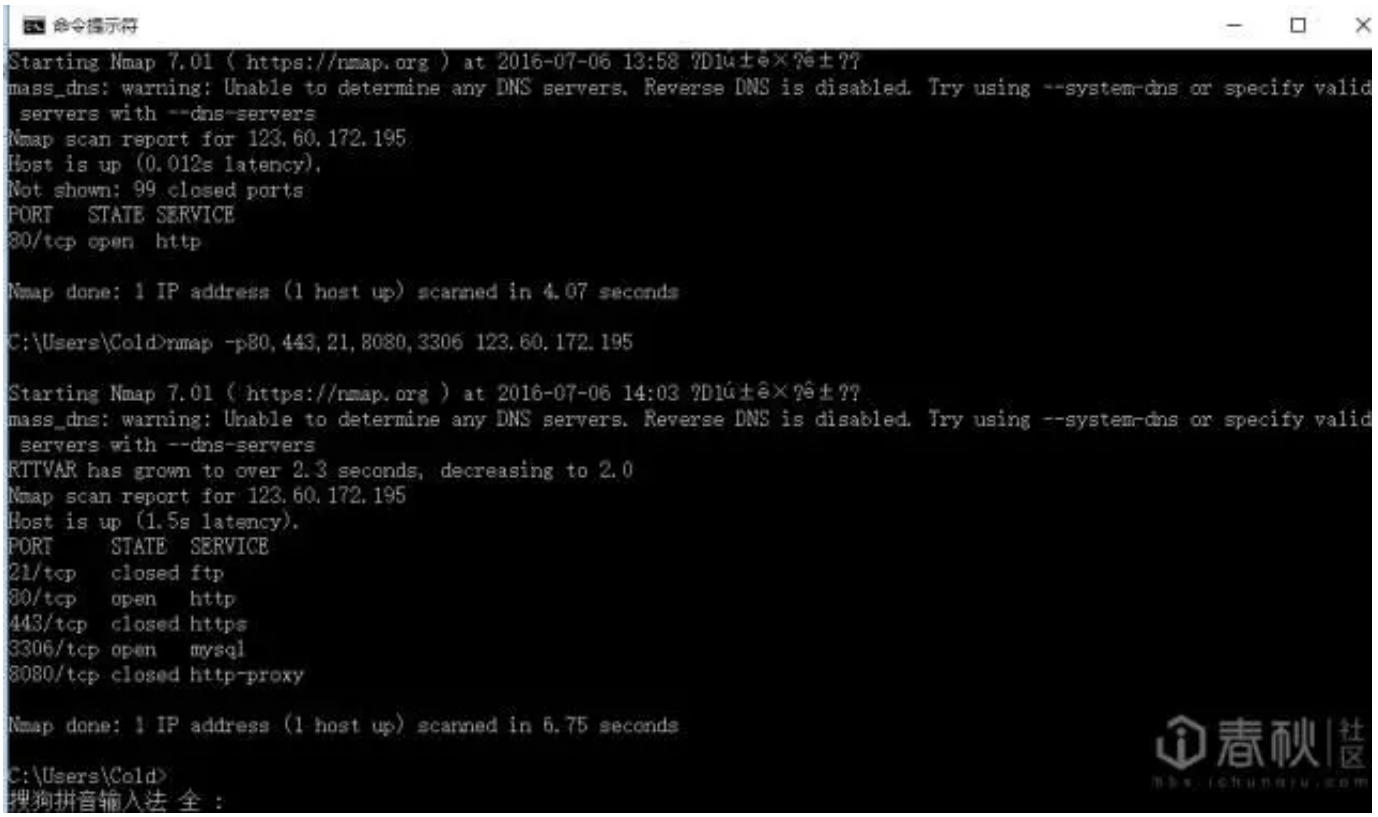


端口指定扫描

```
01.  nmap -p80,443,21,8080,3306 192.168.1.1
     复制代码
```

指定对一些你需要扫描的端口进行扫描。

如下图：

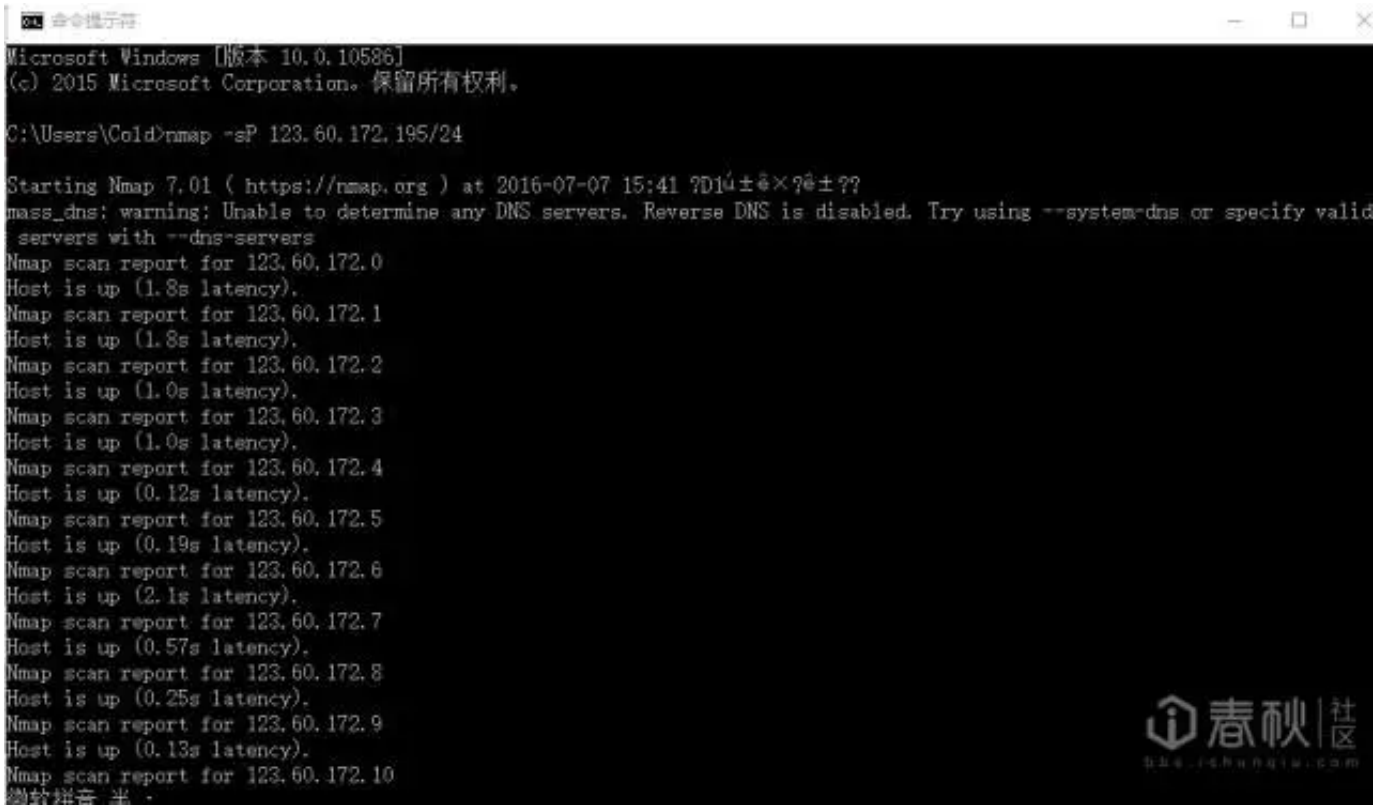


扫描整个网段

```
01.  nmap -sP 192.168.1.1/24
     复制代码
```

后面的24是你自己设置的子网掩码

如下图：

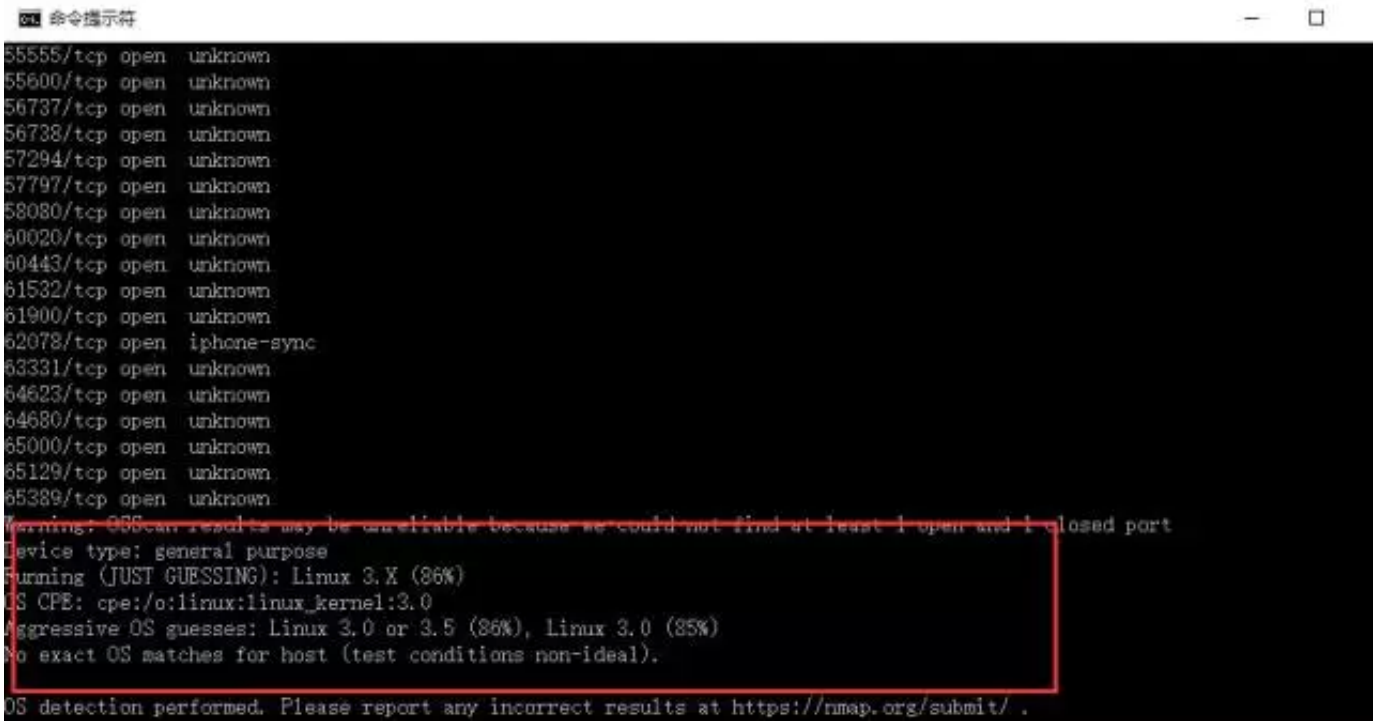


操作系统类型的探测

```
01.  nmap -O 192.168.1.1
     复制代码
```

目标系统操作系统类型的探测

如下图：



写在最后

指正：

WEB漏洞挖掘之网络信息探测这篇文章写到这基本上就结束了，本文章编写还存在很多不足之处，笔者恳请大家对本文批评指正，笔者也会尽力在下一次的文章中做的更好，感谢大家的支持。

i春秋签约作者： 中国Cold