

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

```
01. 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

鼠标滚轮缩放图片

Google

intitle:后台登录

全部

图片

新闻

视频

地图

更多

搜索工具

找到约 88,100 条结果 (用时 0.33 秒)

网站管理后台登录 - 华进半导体

www.ncap-cn.com/manage/adminlogin.aspx

华进半导体封装先导技术研发中心有限公司-网站管理中心. 用户名: 密码: 版权所有 © 厦门三五互联
杭州分公司网站后台管理系统.

网站后台.登录

www.galaxyfour-usa.com/admin/index.asp

用户名: 口令:

后台登录

www.zjchihe.com/admin/Ad_Login.asp

用户名. 密码. 验证码. 看不清楚, 点击换.

企业网站后台管理登录

www.liuhaisu.org/admin/login.asp

企业网站后台管理登录. 用户名: 密码: 验证码:

后台登录- AIRSYS网站管理系统2015

www.air-sys.com/airsys/

关键环境空调解决之道. 管理员登录. 后台语言. 简体中文. 繁体中文. 用户名. 密码. 验证码. 忘记密码?

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。

01.

inurl:admin

复制代码

鼠标滚轮缩放图片

Baidu百度

inurl:admin

百度一下

网页

新闻

贴吧

知道

音乐

图片

视频

地图

文库

更多»

百度为您找到相关结果约5,760,000个

搜索工具

奥美网 后台管理

管理员账号: 管理员密码: ...

admin.choumei.cn/ - 百度快照 - 评价

后台管理员登录页面

中国网库后台管理系统用户名: 密码: 验证码: 换一张?...

admin.99114.com/ - 百度快照 - 155条评价

专家录入后台

专家录入后台忘记密码 认证专家 用户名 密码 登录...

zjadmin.zgzcw.com/ - 百度快照 - 98条评价

后台管理登录

用户名: 密码: ...

admin.ncss.org.cn/ - 百度快照 - 评价

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。

01.

intitle:index of

复制代码

🔍 您可以仅查看：[英文结果](#)

[Index of /](#)

查看此网页的中文翻译，请点击 [翻译此页](#)

[] RPM-GPG-KEY-CentOS-4 26-Feb-2005 17:51 1.8K [] RPM-GPG-KEY-CentOS-5 19-Feb-2007 17:57 1.5K [] RPM-GPG-KEY-CentOS-6 10-Jul...

[vault.centos.org/](#) - 百度快照 - 100%好评

[Index of /](#)

[Index of / \[ICO\]NameLast modifiedSizeDescription\[\] 大连理工大学图书馆校外访问申请表.doc](#)
22-Apr-2015 20:36 32K [] 大连理工大学研究生学位论文延迟发布...

[ftp.lib.dlut.edu.cn/](#) - 百度快照 - 95%好评

[Index of /](#)

查看此网页的中文翻译，请点击 [翻译此页](#)

[Index of /daily-live/ edubuntu/ include/ kubuntu-active/ kubuntu/ livecd-base/ lubuntu/ mythbuntu/ netboot/ precise/ releases/ source/ trusty/ ubuntu-...](#)

[www.cdimage.ubuntu.com/](#) - 百度快照 - 81%好评

[APOD Index](#)

NASA Technical Rep.: Jay Norris. Specific rights apply. A service of LHEA at NASA/ GSFC & Michigan Tech. U...

[apod.nasa.gov/apod/lib...](#) - 百度快照 - 评价 - 翻译此页

[Index of /](#)

[Index of /daily-live/ edubuntu/ include/ kubuntu-active/ kubuntu/ livecd-base/ lubuntu/](#)

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 /

	Name	Last modified	Size	Description
?	大连理工大学图书馆校外访问申请表.doc	22-Apr-2015 20:36	32K	
?	大连理工大学研究生学位论文延迟发布申请表.docx	10-Jun-2015 20:39	13K	
?	无线识别说明.doc	08-Apr-2010 11:23	335K	
?	学术期稿作者注意事项.ppt	08-Apr-2010 11:23	1.1M	
	身份证管理规定/	23-Apr-2015 20:00	-	
?	文电子资源库.pptx	06-Nov-2015 20:22	13M	
?	sevier期稿-2008.10.17.ppt	08-Apr-2010 11:24	1.6M	
	oteExpre训20150417/	17-Apr-2015 23:13	-	
	oteExpre讲.pptx	17-Apr-2015 23:12	2.1M	
?	rary讲.ppt	08-Apr-2010 11:23	7.7M	
?	ulty_i.ppt	08-Apr-2010 11:23	5.1M	
?	ssci讲.ppt	08-May-2015 01:01	24M	
	pport-2015-16-48.zip	09-Sep-2015 03:58	181M	

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

子域名查询

输入域名:

☐ 百度收录 ☐ 百度权重 ☐ PR ☒ 2级子域名 ☒ 3级子域名 ☒ 3级以下子域名

您输入的主域名: **ichunqiu.com**

在<ichunqiu.com>下有子域名:

1. http://bbs.ichunqiu.com

2. http://www.ichunqiu.com

3. http://ichunqiu.com

4. http://wiki.ichunqiu.com

重查所有查询失败记录

导出查询结果

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。

  [百度一下](#)

本页旨在推广信息，请注意可能的风险。

[域名whois信息查询，就到美橙互联 | 域名whois](#)
热点: [whois查询](#) 优势: 顶级域名注册 | CNNIC双认证
域名WHOIS查询，域名访问诊断，终点DNS查询来源IP查询，更多查询功能，到美橙互联。
[who.cndns.com](#) 2016-07 -  - [297条评价](#) - [商业推广](#)

[Whois查询 - 站长之家](#)
站长之家-站长工具提供[whois查询](#)工具, 汉化版的域名[whois查询](#)工具。... Whois 简单来说, 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...
[whois.chinaz.com/](#) -  - [百度快照](#) - [84%好评](#)

[whois查询-中国万网](#)
在中国最大的域名注册服务商——中国万网, 免费[查询](#)域名WHOIS信息。您可查看域名是否可以注册, 或者查看域名当前所有者的联系方式, 或者查看域名的当前状态等。
[whois.www.net.cn/](#) -  - [百度快照](#) - [95%好评](#)

[Whois域名注册信息查询](#)
ICP备案查询 | Whois域名信息查询 | ALEXA网站排名 | 域名备案查询域名sina.com.cn 的
[Whois查询](#)信息广告联系 Tell:400-6666-121 QQ:86121...
[whois.alexa.cn/](#) -  - [百度快照](#) - [69%好评](#)

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）。

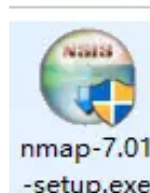
（一）nmap安装

1、软件下载

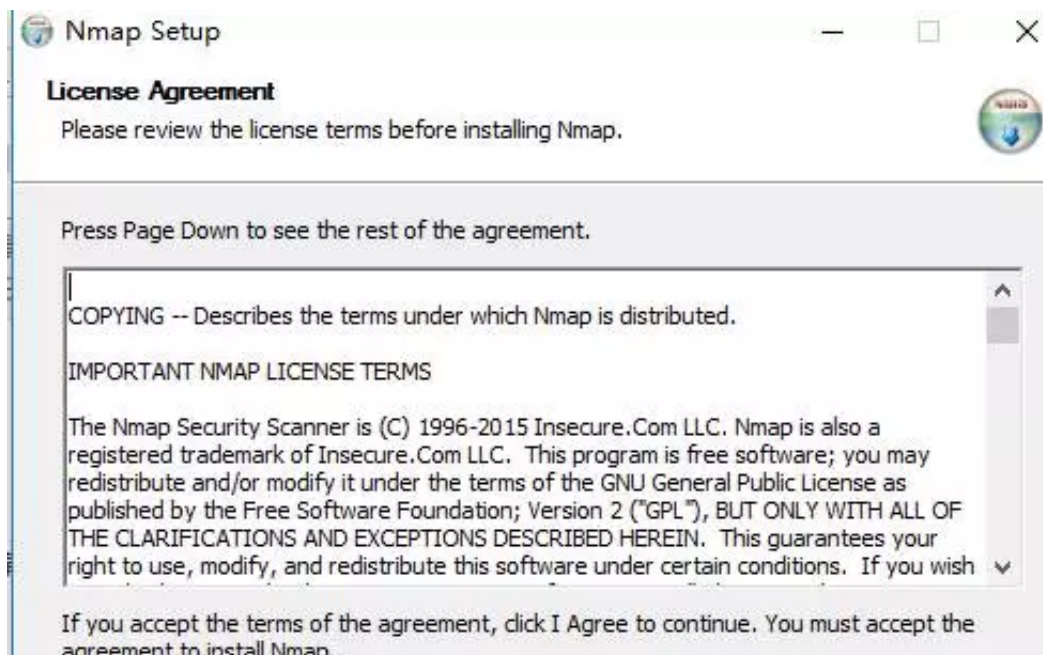
01. 百度网盘：链接：[url]<http://pan.baidu.com/s/1c2x8LcG>[url] 密码：cc4m
复制代码

01. 官网下载：<https://nmap.org>
复制代码

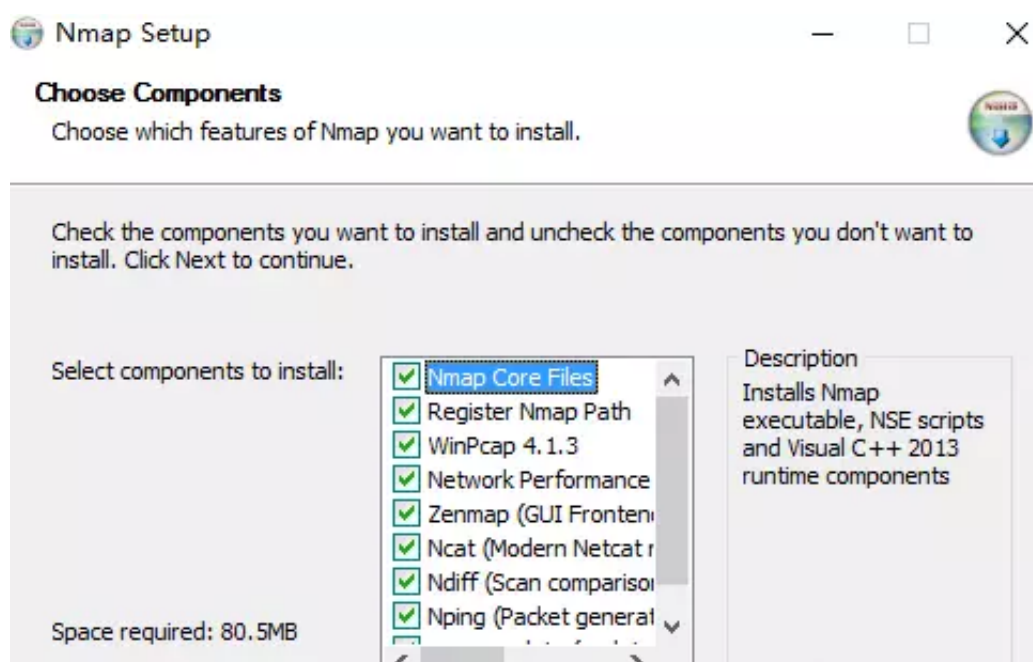
2、打开安装包



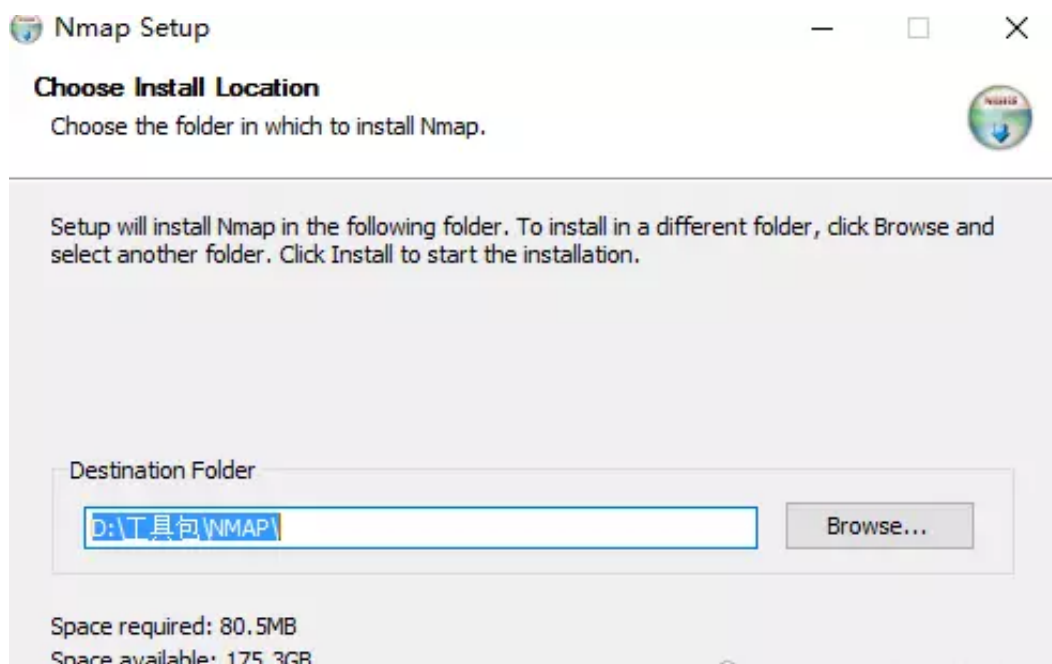
3、阅读Nmap许可协议，点击I Agree下一步。



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。

```
命令提示符
Microsoft Windows [版本 10.0.10586]
(c) 2015 Microsoft Corporation. 保留所有权利。

C:\Users\Cold>nmap
Nmap 7.01 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PW: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  --probeport <port>: Idle scan
```

(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：

命令提示符

```
C:\Users\Cold>nmap 123.60.

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-06 13:45
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sys
servers with --dns-servers
Nmap scan report for 123.60.
Host is up (0.014s latency).
Not shown: 970 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
88/tcp    filtered kerberos-sec
110/tcp   open  pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
389/tcp   filtered ldap
445/tcp   filtered microsoft-ds
464/tcp   filtered kpasswd5
593/tcp   filtered http-rpc-epmap
636/tcp   filtered ldapssl
888/tcp   open  accessbuilder
1025/tcp  filtered NFS-or-IIS
1311/tcp  open  rxmon
1433/tcp  filtered ms-sql-s
1720/tcp  filtered h323q931
2383/tcp  open  ms-olap4
3001/tcp  filtered nessus
搜狗拼音输入法 全 :cgms
```

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：

```
C:\Users\Cold>nmap -p1-100 123.60.172.195

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-06 13:58
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sy
servers with --dns-servers
Nmap scan report for 123.60.172.195
Host is up (0.012s latency).
Not shown: 99 closed ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 4.07 seconds

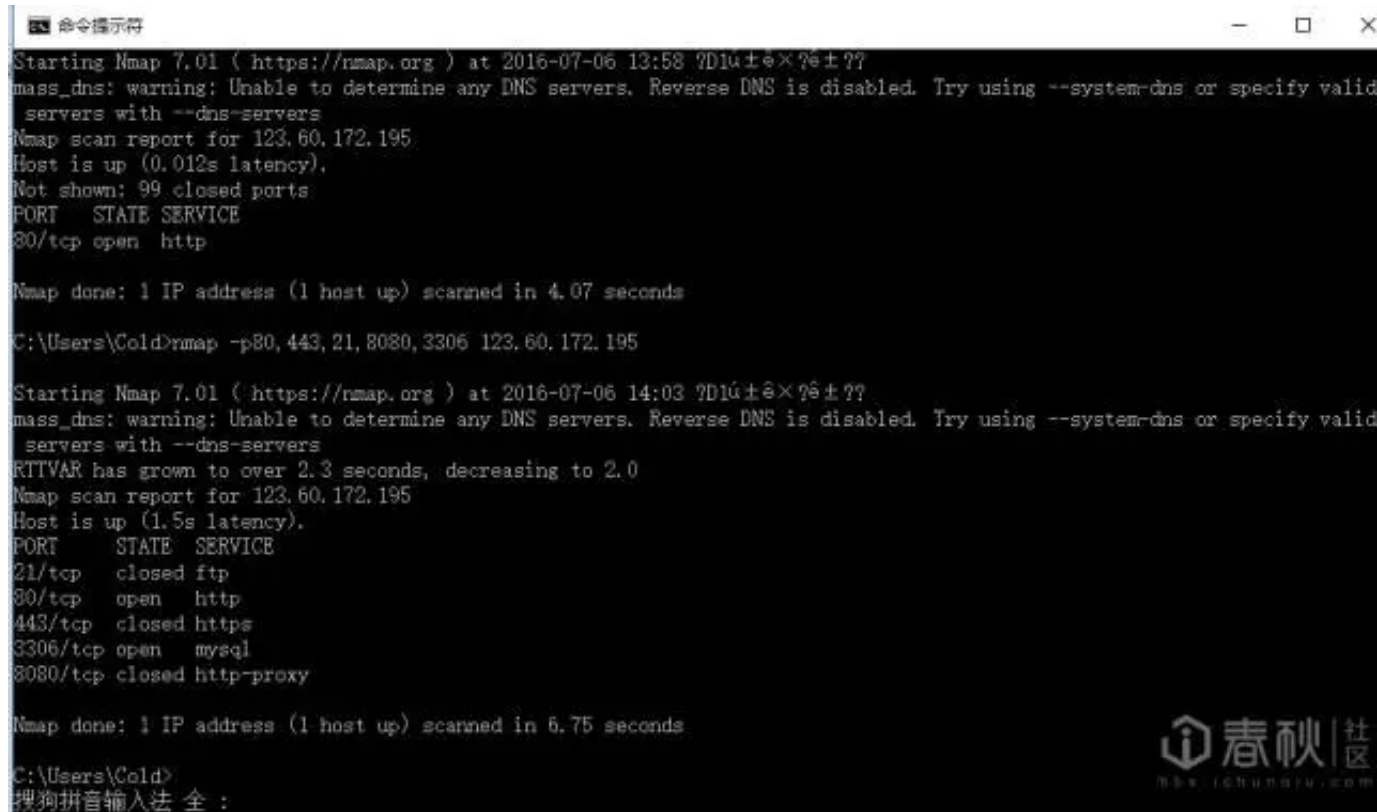
C:\Users\Cold>
搜狗拼音输入法 全 :
```

端口指定扫描

01.	<code>nmap -p80,443,21,8080,3306 192.168.1.1</code>
	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.	<code>nmap -sP 192.168.1.1/24</code>
	复制代码

后面的24是你自己设置的子网掩码

如下图：

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

本文章来源：i春秋社区，版权归属于i春秋。

未经许可，请勿转载。



微信公众号：jsrc_team

新浪官方微博：

京东安全应急响应中心

固定栏目

技术分享 | 安全意识 | 安全小课堂