

干货 | 最全Web 渗透测试信息搜集-CheckList

zjun HACK学习呀 2022-02-19 09:13

收录于话题

#渗透测试41个

#信息收集1个

这篇文章是21年中旬记录的，平安夜p牛的直播中也谈到，对于渗透测试来说最好有一个checklist，为了避免忘记测试某一部分的内容而错过一些重要信息，同时有了checklist也容易利用自己喜欢的语言实现自动化，突然想起了这篇信息搜集相关的文章所以就分享出来。

1.获取真实IP

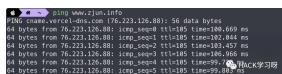
为了保证网络的稳定和快速传输，网站服务商会在网络的不同位置设置节点服务器，通过CDN（Content Delivery Network，内容分发网络）技术，将网络请求分发到最优的节点服务器上面。如果网站开启了CDN加速，就无法通过网站的域名信息获取真实的IP，要对目标的IP资源进行收集，就要绕过CDN查询到其真实的IP信息。

2.如何判断是否是CDN

在对目标IP信息收集之前，首先要判断目标网站是否开启了CDN，一般通过不同地方的主机ping域名和nslookup域名解析两种方法，通过查看返回的IP是否是多个的方式来判断网站是否开启了CDN，如果返回的IP信息是多个不同的IP，那就有可能使用了CDN技术。

使用ping域名判断是否有CDN

直接使用ping域名查看回显地址来进行判断，如下回显 `cname.vercel-dns.com`，很明显使用了cdn技术。



```
0010 www.zjun.info
ping: cname.vercel-dns.com (76.223.126.88): 56 data bytes
64 bytes from 76.223.126.88: icmp_seq=0 ttl=64 time=0.609 ms
64 bytes from 76.223.126.88: icmp_seq=1 ttl=64 time=0.884 ms
64 bytes from 76.223.126.88: icmp_seq=2 ttl=64 time=0.457 ms
64 bytes from 76.223.126.88: icmp_seq=3 ttl=64 time=0.366 ms
64 bytes from 76.223.126.88: icmp_seq=4 ttl=64 time=0.370 ms
64 bytes from 76.223.126.88: icmp_seq=5 ttl=64 time=0.370 ms
```

使用不同主机ping域名判断是否有CDN

如果自己在多地都有主机可以ping域名，就可以根据返回的IP信息进行判断。互联网有很多公开的服务可以进行多地ping来判断是否开启了CDN，比如以下几个：

CSS

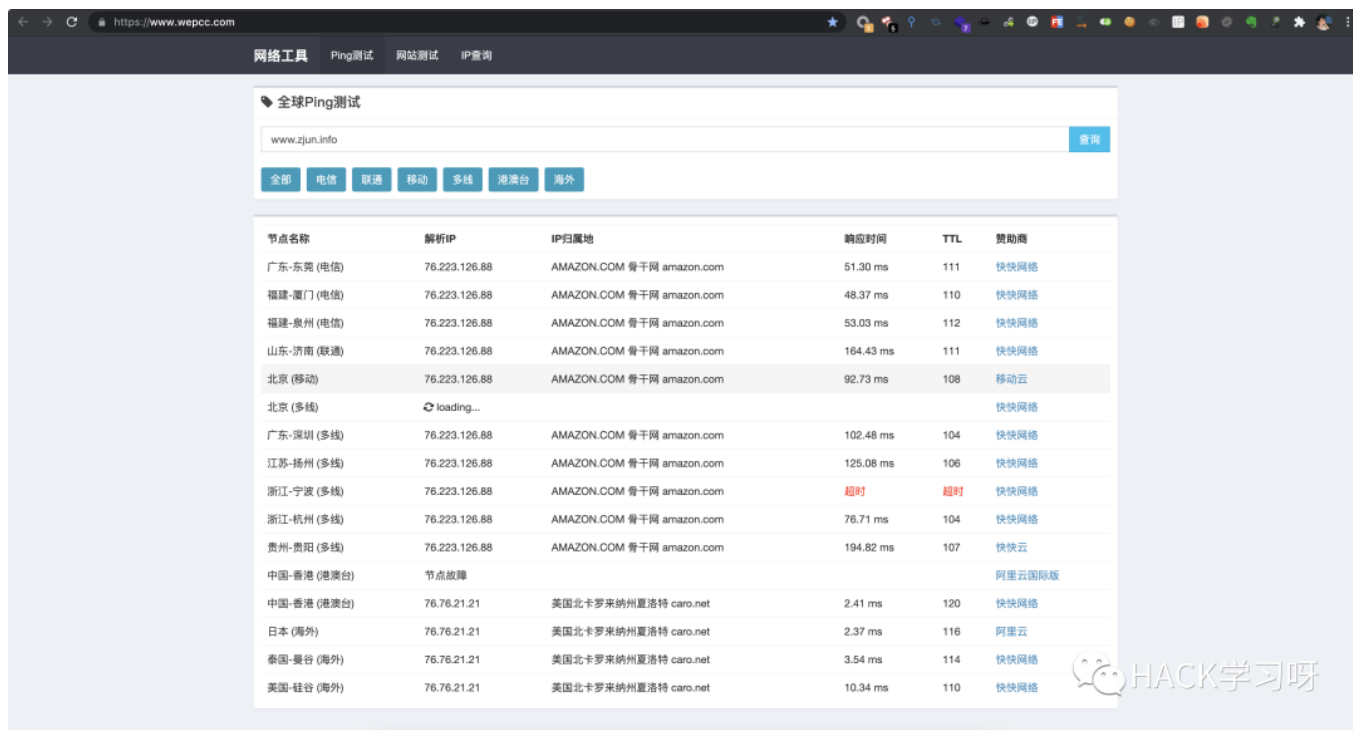
1 全球Ping测试: <https://www.wepcc.com/>

CSS

- 1 站长工具Ping检测: <http://ping.chinaz.com/>

CSS

- 1 爱站网Ping检测: <https://ping.aizhan.com/>



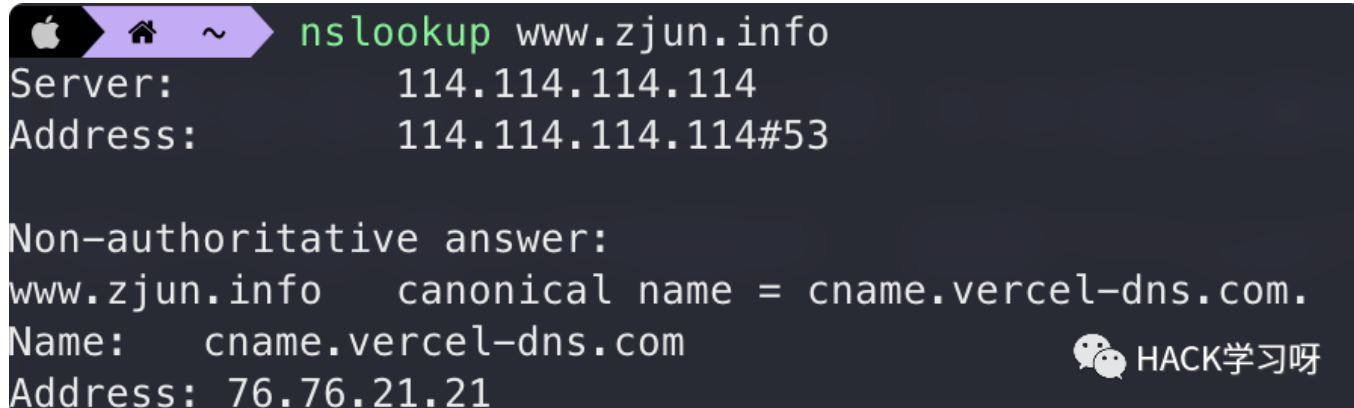
The screenshot shows the 'Global Ping Test' interface with the domain 'www.zjun.info' entered. The results table lists various nodes and their corresponding IP addresses, response times, and TTL values. The table is as follows:

节点名称	解析IP	IP归属地	响应时间	TTL	赞助商
广东-东莞 (电信)	76.223.126.88	AMAZON.COM 骨干网 amazon.com	51.30 ms	111	快快网络
福建-厦门 (电信)	76.223.126.88	AMAZON.COM 骨干网 amazon.com	48.37 ms	110	快快网络
福建-泉州 (电信)	76.223.126.88	AMAZON.COM 骨干网 amazon.com	53.03 ms	112	快快网络
山东-济南 (联通)	76.223.126.88	AMAZON.COM 骨干网 amazon.com	164.43 ms	111	快快网络
北京 (移动)	76.223.126.88	AMAZON.COM 骨干网 amazon.com	92.73 ms	108	移动云
北京 (多线)	loading...				快快网络
广东-深圳 (多线)	76.223.126.88	AMAZON.COM 骨干网 amazon.com	102.48 ms	104	快快网络
江苏-扬州 (多线)	76.223.126.88	AMAZON.COM 骨干网 amazon.com	125.08 ms	106	快快网络
浙江-宁波 (多线)	76.223.126.88	AMAZON.COM 骨干网 amazon.com	超时	超时	快快网络
浙江-杭州 (多线)	76.223.126.88	AMAZON.COM 骨干网 amazon.com	76.71 ms	104	快快网络
贵州-贵阳 (多线)	76.223.126.88	AMAZON.COM 骨干网 amazon.com	194.82 ms	107	快快云
中国-香港 (港澳台)	节点故障				阿里云国际版
中国-香港 (港澳台)	76.76.21.21	美国北卡罗来纳州夏洛特 caro.net	2.41 ms	120	快快网络
日本 (海外)	76.76.21.21	美国北卡罗来纳州夏洛特 caro.net	2.37 ms	116	阿里云
泰国-曼谷 (海外)	76.76.21.21	美国北卡罗来纳州夏洛特 caro.net	3.54 ms	114	快快网络
美国-硅谷 (海外)	76.76.21.21	美国北卡罗来纳州夏洛特 caro.net	10.34 ms	110	快快网络

可以发现对 `www.zjun.info` 的全球ping测试, 有 `76.223.126`、`76.76.21.21` 这两个不同的解析IP, 说明 `www.zjun.info` 可能使用了CDN。

使用nslookup域名解析判断是否有CDN

通过系统自带的 `nslookup` 命令对域名解析, 发现其中的 `Name` 字段直接指向 `cname.vercel-dns.com`, 毫无疑问使用了CDN技术。



```
nslookup www.zjun.info
Server:          114.114.114.114
Address:         114.114.114.114#53

Non-authoritative answer:
www.zjun.info    canonical name = cname.vercel-dns.com.
Name:   cname.vercel-dns.com
Address: 76.76.21.21
```

又比如 `www.baidu.com`, 其中 `Address` 字段也是指向两个不同IP, 即 `www.baidu.com` 可能使用了CDN。

```
nslookup www.baidu.com
Server:      114.114.114.114
Address:     114.114.114.114#53

Non-authoritative answer:
www.baidu.com canonical name = www.a.shifen.com.
Name:   www.a.shifen.com
Address: 39.156.66.14
Name:   www.a.shifen.com
Address: 39.156.66.18
```

HACK学习呀

3.如何绕过CDN获取真实IP

查询子域名

由于CDN加速需要支付一定的费用，很多网站只对主站做了CDN加速，子域名没有做CDN加速，子域名可能跟主站在同一个服务器或者同一个C段网络中，可以通过子域名探测的方式，收集目标的子域名信息，通过查询子域名的IP信息来辅助判断主站的真实IP信息。

查询历史DNS记录

通过查询DNS与IP绑定的历史记录就有可能发现之前的真实IP信息，常用的第三方服务网站有：

Groovy
1 dnsdb: https://dnsdb.io/zh-cn/
Groovy
1 viewdns: https://viewdns.info/iphistory/
CSS
1 微步在线: https://x.threatbook.cn/

使用国外主机请求域名

部分国内的CDN加速服务商只对国内的线路做了CDN加速，但是国外的线路没有做加速，这样就可以通过国外的主机来探测真实的IP信息。

探测的方式也有两种，可以利用已有的国外主机直接进行探测；如果没有国外主机，可以利用公开的多地ping服务（多地ping服务有国外的探测节点），可以利用国外的探测节点返回的信息来判断真实的IP信息。

网站信息泄露漏洞

利用网站存在的漏洞和信息泄露的敏感信息、文件（如：phpinfo文件、网站源码文件、Github泄露的信息等）获取真实的IP信息。

phpinfo页面中有一个 `SERVER_ADDR` 字段会显示该主机真实IP。

邮件信息

一般的邮件系统都在内部，没有经过CDN的解析，通过利用目标网站的邮箱注册、找回密码或者RSS订阅等功能，接收到发来的邮件后，查看邮件源码就可以获得目标的真实IP。

```
Received: from mta2[REDACTED].net (unknown [104.[REDACTED].210])
    by mail-m12[REDACTED].com (HMail) with ESMTP id 0D4179A0188
    for <i@zjun.info>; Sat, 28 Aug 2021 23:45:00 +0800 (CST)
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=pm; d=pm.mtasv.net;
    h=From:Date:Subject:To:Message-Id:MIME-Version:Content-Type;
    bh=pnjHLa9QVG0/gNdD7tnyj7nEBQQ=;
    b=QAF8dK0wiCHCYR/m1ROMkORfwGLiLFg5uwV0jKv1Y1rj0/MFuP9EXYxywZePGjroWBHxWTtMOOZ2
    TlwZn84QiDIYylFpQyDf/2WVr7dju3AfzH53LV4RYh83qoYLqPPaNH29DTVWxVl+/4crahYlKgdo
    G13k9UN8ztSWIIJWCAE=
Received: by mta210a-ord.mtasv.net id h59cvo27tk4u for <i@zjun.info>; Sat, 28 Aug 2021 11:44:57 -04
X-PM-IP: 104[REDACTED]
X-IADB-IP: 1[REDACTED]
X-IADB-IP-RE: [REDACTED].104
DKIM-Signature: v=1; a=rsa-sha256; d=opencagedata.com; s=20180530124443pm;
    c=relaxed/relaxed; i=support@opencagedata.com; t=1630165497;
    h=cc:content-transfer-encoding:content-type:date:from:in-reply-to:
    list-archive:list-help:list-id:list-owner:list-post:list-subscribe:
    list-unsubscribe:mime-version:message-id:references:reply-to:resent-cc:
    resent-date:resent-from:resent-message-id:resent-sender:resent-to:sender:
    subject:to:feedback-id;
    bh=sYHh4w4xy4NSsmKHnY9AGQG2rckxSTMriKtX42VezJc=;
```

HACK学习呀

目标网站APP应用

如果目标网站有自己的App，可以尝试利用Burp Suite等流量抓包工具抓取App的请求，从里面可能会找到目标的真实IP。

4.旁站查询（IP反查）

旁站是与攻击目标在同一服务器上的不同网站，获取到目标真实IP的情况下，在攻击目标没有可利用漏洞的情况下，可以通过查找旁站的漏洞攻击旁站，然后再通过提权拿到服务器的最高权限，拿到服务器的最高权限后攻击目标也就拿下了。

旁站信息收集也称为IP反查，主要有以下方式：

Nmap扫描获取旁站信息

使用命令

CSS

```
1 nmap -sV -p 1-65535 x.x.x.x
```

对目标IP进行全端口扫描，确保每个可能开放的端口服务都能识别到。

第三方服务获取旁站信息

旁站信息可以通过第三方服务进行收集，比如在线网站与搜索引擎等。以下是几个在线搜集网站：

CSS

```
1 站长工具同IP网站查询: http://s.tool.chinaz.com/same
```

CSS

```
1 webscan: https://www.webscan.cc/
```

CSS

```
1 云悉: https://www.yunsee.cn/
```

CSS

```
1 微步在线: https://x.threatbook.cn/
```

Gherkin

```
1 在线旁站查询|C段查询|必应接口C段查询: http://www.bug8.me/bing/bing.php
```

也可以利用搜索引擎语法来实现查询：

bing

Groovy

```
1 https://cn.bing.com/search?q=ip:x.x.x.x
```

fofa

Makefile

```
1 ip="x.x.x.x"
```

Plain Text

```
1
```

5.C段主机查询

C段主机是指与目标服务器在同一C段网络的服务器。攻击目标的C段存活主机是信息收集的重要步骤，很多企业的内部服务器可能都会在一个C段网络中。在很难找到攻击目标服务器互联网漏洞的情况下，可以通过攻击C段主机，获取对C段主机的控制权，进入企业内网，在企业的内网安全隔离及安全防护不如互联网防护健全的情况下，可以通过C段的主机进行内网渗透，这样就可以绕过互联网的防护，对目标进行攻击。但是这种攻击方式容易打偏。

Nmap扫描C段

使用命令 `nmap -sn x.x.x.x/24`，对目标IP的C段主机进行存活扫描，根据扫描的结果可以判断目标IP的C段还有哪些主机存活。

`nmap -Pn` 这个命令在实际工作中的使用很多，该命令不通过ICMP协议进行主机存活判断，会直接对端口进行扫描。这样在开启了防火墙禁Ping的情况下，也可以利用这个命令正常扫描目标是否存活及对外开启的相关服务。

搜索引擎语法收集C段信息

Google

Makefile

```
1 site:x.x.x.*
```

Fofa

Makefile

```
1 ip="x.x.x.x/24"
```

在线C段扫描工具

Gherkin

- 1 在线旁站查询|C段查询|必应接口C段查询: <http://www.bug8.me/bing/bing.php>

Groovy

- 1 查旁站: <https://chapangzhan.com/>

CSS

- 1 云悉: <https://www.yunsee.cn/>

本地C段扫描工具（其中某些工具不只是C段扫描）

Groovy

- 1 httpscan: <https://github.com/zer0h/httpscan>

Plain Text

- 1 小米范web查找器

Groovy

- 1 Goby: <https://gobies.org/>

Groovy

- 1 bufferfly: <https://github.com/dr0p/bufferfly>

Groovy

- 1 cscan: <https://github.com/z1un/cscan>

6.子域名查询

子域名是父域名的下一级，比如 blog.zjun.info 和 tools.zjun.info 这两个域名是 zjun.info 的子域名。一般企业对于主站域名的应用的防护措施比较健全，不管是应用本身的漏洞发现、漏洞修复，还是安全设备相关的防护都做得更加及时和到位，而企业可能有多个、几十个甚至更多的子域名应用，因为子域名数量多，企业子域名应用的防护可能会没有主站及时。攻击者在主站域名找

不到突破口时，就可以进行子域名的信息收集，然后通过子域名的漏洞进行迂回攻击。子域名信息收集主要包含枚举发现子域名、搜索引擎发现子域名、第三方聚合服务发现子域名、证书透明性信息发现子域名、DNS域传送发现子域名等方式。

枚举发现子域名

子域名收集可以通过枚举的方式对子域名进行收集，枚举需要一个好的字典，制作字典时会将常见子域名的名字放到字段里面，增加枚举的成功率。子域名暴力破解常用的工具以下：

Groovy
1 在线子域名查询： https://phpinfo.me/domain/
Groovy
1 OneForAll： https://github.com/shmilylty/OneForAll
Groovy
1 knock： https://github.com/guelfoweb/knock
Groovy
1 subDomainsBrute： https://github.com/lijiejie/subDomainsBrute
Groovy
1 Layer子域名挖掘机： https://github.com/euphrat1ca/LayerDomainFinder

搜索引擎发现子域名

使用搜索引擎语法，如
Google或者百度等

Makefile
1 site:xxx.com

Fofa

Makefile

```
1 domain="xxx.com"
```

Plain Text

```
1
```

第三方聚合服务发现子域名

第三方聚合平台 Netcraft、Virusotal、ThreatCrowd、DNSdumpster 和 ReverseDNS 等获取子域信息。

·
·

Apache

```
1 Sublist3r: https://github.com/aboul3la/Sublist3r
```

Groovy

```
1 OneForAll: https://github.com/shmilylty/OneForAll
```

证书透明性信息发现子域名

证书透明性（Certificate Transparency，CT）是Google的公开项目，通过让域所有者、CA和域用户对SSL证书的发行和存在进行审查，来纠正这些基于证书的威胁。具体而言，证书透明性具有三个主要目标：

·
·
·

Plain Text

```
1 使CA无法（或至少非常困难）为域颁发SSL证书，而该域的所有者看不到该证书；
```

Plain Text

```
1 提供一个开放的审核和监视系统，该系统可以让任何域所有者或CA确定证书是错误的还是恶意颁发的；
```

Plain Text

- 1 尽可能防止用户被错误或恶意颁发的证书所欺骗。

证书透明性项目有利有弊。通过证书透明性，可以检测由证书颁发机构错误颁发的SSL证书，可以识别恶意颁发证书的证书颁发机构。因为它是一个开放的公共框架，所以任何人都可以构建或访问驱动证书透明性的基本组件，CA证书中包含了域名、子域名、邮箱等敏感信息，存在一定的安全风险。

利用证书透明性进行域名信息收集，一般使用CT日志搜索引擎进行域名信息收集，如在线网站：

·
·
·

Groovy

- 1 <https://crt.sh/>

CSS

- 1 <https://transparencyreport.google.com/https/certificates>

Ruby

- 1 <https://developers.facebook.com/tools/ct/>

本地工具：

·
·

Groovy

- 1 ctfr: <https://github.com/UnaPibaGeek/ctfr>

Groovy

- 1 OneForAll: <https://github.com/shmilylty/OneForAll>

DNS域传送发现子域名

DNS服务器分为：主服务器、备份服务器和缓存服务器。在主备服务器之间同步数据库，需要使用“DNS域传送”。域传送是指备份服务器从主服务器拷贝数据，并用得到的数据更新自身数据库。

若DNS服务器配置不当，可能导致攻击者获取某个域的所有记录。造成整个网络的拓扑结构泄露给潜在的攻击者，包括一些安全性较低的内部主机，如测试服务器。同时，黑客可以快速的判定出某个特定zone的所有主机，收集域信息，选择攻击目标，找出未使用的IP地址，绕过基于网络的访问控制。目前来看"DNS域传送漏洞"已经很少了。

利用nmap漏洞检测脚本 `dns-zone-transfer` 进行检测

Fortran

```
1 nmap --script dns-zone-transfer --script-args dns-zone-transfer.domain=xxx.edu.cn -p 53 -Pn dns.xxx.edu.cn
```

Linux dig命令进行测试

Nginx

```
1 dig xxx.com ns
```

CoffeeScript

```
1 dig axfr @dns xxx.com
```

7.端口扫描

最常用的就是nmap

Erlang

```
1 -sS (TCP SYN扫描)
```

Lisp

```
1 -sT (TCP connect()扫描)
```

Erlang

```
1 -sU (UDP扫描)
```

YAML

```
1 -sN; -sF; -sX (TCP Null, FIN, and Xmas扫描)
```

Erlang

```
1 -Pn (不通过ICMP探测)
```

详细文档：

.

Ruby

```
1 https://nmap.org/man/zh/
```

其次可能还会用到masscan：

.

Groovy

```
1 https://github.com/robertdavidgraham/masscan
```

常见端口及对应服务表：

TCP/UDP Port Numbers

7 Echo	554 RTSP	2745 Bagle.H	6891-6901 Windows Live
19 Chargen	546-547 DHCPv6	2967 Symantec AV	6970 Quicktime
20-21 FTP	560 rmonitor	3050 Interbase DB	7212 GhostSurf
22 SSH/SCP	563 NNTP over SSL	3074 XBOX Live	7648-7649 CU-SeeMe
23 Telnet	587 SMTP	3124 HTTP Proxy	8000 Internet Radio
25 SMTP	591 FileMaker	3127 MyDoom	8080 HTTP Proxy
42 WINS Replication	593 Microsoft DCOM	3128 HTTP Proxy	8086-8087 Kaspersky AV
43 WHOIS	631 Internet Printing	3222 GLBP	8118 Privoxy
49 TACACS	636 LDAP over SSL	3260 iSCSI Target	8200 VMware Server
53 DNS	639 MSDP (PIM)	3306 MySQL	8500 Adobe ColdFusion
67-68 DHCP/BOOTP	646 LDP (MPLS)	3389 Terminal Server	8767 TeamSpeak
69 TFTP	691 MS Exchange	3689 iTunes	8866 Bagle.B
70 Gopher	860 iSCSI	3690 Subversion	9100 HP JetDirect
79 Finger	873 rsync	3724 World of Warcraft	9101-9103 Bacula
80 HTTP	902 VMware Server	3784-3785 Ventrilo	9119 MXit
88 Kerberos	989-990 FTP over SSL	4333 mSQL	9800 WebDAV
102 MS Exchange	993 IMAP4 over SSL	4444 Blaster	9898 Dabber
110 POP3	995 POP3 over SSL	4664 Google Desktop	9988 Rbot/Spybot
113 Ident	1025 Microsoft RPC	4672 eMule	9999 Urchin
119 NNTP (Usenet)	1026-1029 Windows Messenger	4899 Radmin	10000 Webmin
123 NTP	1080 SOCKS Proxy	5000 UPnP	10000 BackupExec
135 Microsoft RPC	1080 MyDoom	5001 Slingbox	10113-10116 NetIQ
137-139 NetBIOS	1194 OpenVPN	5001 iperf	11371 OpenPGP
143 IMAP4	1214 Kazaa	5004-5005 RTP	12035-12036 Second Life
161-162 SNMP	1241 Nessus	5050 Yahoo! Messenger	12345 NetBus
177 XDMCP	1311 Dell OpenManage	5060 SIP	13720-13721 NetBackup
179 BGP	1337 WASTE	5190 AIM/ICQ	14567 Battlefield
201 AppleTalk	1433-1434 Microsoft SQL	5222-5223 XMPP/Jabber	15118 Dipnet/Oddbob
264 BGMP	1512 WINS	5432 PostgreSQL	19226 AdminSecure
318 TSP	1589 Cisco VQP	5500 VNC Server	19638 Ensimg
381-383 HP Openview	1701 L2TP	5554 Sasser	20000 Usermin
389 LDAP	1723 MS PPTP	5631-5632 pcAnywhere	24800 Synergy
411-412 Direct Connect	1725 Steam	5800 VNC over HTTP	25999 Xfire
443 HTTP over SSL	1741 CiscoWorks 2000	5900+ VNC Server	27015 Half-Life
445 Microsoft DS	1755 MS Media Server	6000-6001 X11	27374 Sub7
464 Kerberos	1812-1813 RADIUS	6112 Battle.net	28960 Call of Duty
465 SMTP over SSL	1863 MSN	6129 DameWare	31337 Back Orifice
497 Retrospect	1985 Cisco HSRP	6257 WinMX	33434+ traceroute
500 ISAKMP	2000 Cisco SCCP	6346-6347 Gnutella	
512 rexec	2002 Cisco ACS	6500 GameSpy Arcade	
513 rlogin	2049 NFS	6566 SANE	
514 syslog	2082-2083 cPanel	6588 AnalogX	
515 LPD/LPR	2100 Oracle XDB	6665-6669 IRC	
520 RIP	2222 DirectAdmin	6679/6697 IRC over SSL	
521 RiPng (IPv6)	2302 Halo	6699 Napster	
540 UUCP	2483-2484 Oracle DB	6881-6999 BitTorrent	

Legend

- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

IANA port assignments published at <http://www.iana.org/assignments/port-numbers>

by Jeremy Stretch

HACK学习网

8.目录探测

在信息搜集中，目录扫描是一个很重要的步骤，可以帮助我们获得如网站的测试页面、后台地址、常见第三方高危组件路径等。但是目前多数网站都有云waf、主机防护等，对于频繁访问的IP会封禁处理。对于云waf，找到网站真实IP是很关键的，其余的情况基本都可以修改开源工具代码利用IP代理池或控制访问频率的方式进行探测。

常用目录扫描工具如下：

-
-
-
-

Groovy

1 dirsearch: <https://github.com/maurosoria/dirsearch>

Groovy

1 dirmap: <https://github.com/H4ckForJob/dirmap>

Groovy

1 御剑目录扫描: <https://github.com/foryujian/yjdirscan>

CSS

1 dirb: <https://tools.kali.org/web-applications/dirb>

IP代理池推荐：

-
- Groovy
- 1 ProxyPool: <https://github.com/Python3WebSpider/ProxyPool>

9.指纹识别

常见的指纹识别内容有CMS识别、框架识别、中间件识别、WAF识别。CMS识别一般利用不同的CMS特征来识别，常见的识别方式包括特定关键字识别、特定文件及路径识别、CMS网站返回的响应头信息识别等。

服务器信息搜集

服务版本识别、操作系统信息识别都可以利用nmap实现识别

CSS

1 nmap -sV -p 1-65535 x.x.x.x

CSS

1 nmap -O x.x.x.x

CMS识别

识别CMS的目的在于，方便利用已公开漏洞进行渗透测试，甚至可以到对应CMS的官网下载对应版本的CMS进行本地白盒代码审计。

特定关键字识别

CMS的首页文件、特定文件可能包含了CMS类型及版本信息，通过访问这些文件，将返回的网页信息（如 Powered by XXCMS）与扫描工具数据库存储的指纹信息进行正则匹配，判断CMS的类型。

也可能前端源码中或meta标签中的content字段存在一些CMS特征信息，下图很明显能得知是WordPress框架。

```
./script><meta name='robots' content='index, follow, max-image-preview:large, max-snippet:-1, max-video-preview:-1' />

<!-- This site is optimized with the Yoast SEO plugin v16.7 - https://yoast.com/wordpress/plugins/seo/ -->
<title>[redacted] </title>
<meta n[redacted] 19 novembre 2021" />
<link rel="canonical" href="h[redacted]v" />
<meta property="og:site_name" content="f[redacted]" />
<meta property="og:title" content="wek[redacted]" />
<meta property="og:description" content="SC[redacted]ndics" />
<meta property="og:description" content="Nice - P[redacted]1" />
<meta property="og:url" content="https[redacted]" />
<meta property="og:site_name" content="SOLUCOP" />
<meta property="article:published_time" content="https[redacted]op/" />
<meta property="article:modified_time" content="20[redacted]" />
<meta name="twitter:card" content="si[redacted]" />
<meta name="twitter:site" content="est." />
<meta name="twitter:data1" content="3 minutes" />
```

特定文件及路径识别

不同的CMS会有不同的网站结构及文件名称，可以通过特定文件及路径识别CMS。如WordPress会有特定的文件路径 /wp-admin、 /wp-includes 等，有些CMS的 robots.txt 文件也可能包含了CMS特定的文件路径，与扫描工具数据库存储的指纹信息进行正则匹配，判断CMS的类型。

CMS会有一些JS、CSS、图片等静态文件，这些文件一般不会变化，可以利用这些特定文件的MD5值作为指纹信息来判断CMS的类型。

响应头信息识别

应用程序会在响应头Server、X-Powered-By、Set-Cookie等字段中返回Banner信息或者自定义的数据字段，通过响应头返回的信息，可以对应用进行识别，有些WAF设备也可以通过响应头信息进行识别判断。当然Banner信息并不一定是完全准确的，应用程序可以自定义自己的Banner信息。

例如Shiro的响应头信息中包含 `rememberMe` 字段：



指纹识别工具

指纹识别常用的工具如下：

- Groovy

1 whatweb: <https://github.com/urbanadventurer/WhatWeb>
- Groovy

1 wappalyzer: <https://github.com/AliasIO/wappalyzer>
- Groovy

1 Glass: <https://github.com/s7ckTeam/Glass>

还有两款只支持如WordPress, Joomla, Drupal的工具

•
•
•
•

Objective-C

- 1 CMSScan: <https://github.com/ajinabraham/CMSScan>

Objective-C

- 1 CMSmap: <https://github.com/Dionach/CMSmap>

CSS

- 1 云悉: <https://www.yunsee.cn/>

CSS

- 1 bugscaner在线cms识别: <http://whatweb.bugscaner.com/look/>

10.Google hacking

Groovy

- 1 目录遍历: `site:$site intitle:index.of`

Groovy

- 1 配置文件泄露: `site:$site ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp | ext:cfg | ext:txt | ext:ora | ext:ini`

Groovy

- 1 数据库文件泄露: `site:$site ext:sql | ext:dbf | ext:mdb`

Bash

- 1 日志文件泄露: `site:$site ext:log`

Plain Text

- 1

Groovy

- 1 备份和历史文件: `site:$site ext:bkf | ext:bkp | ext:bak | ext:old | ext:backup`

Groovy

- 1 登录页面: `site:$site inurl:login`

Groovy

- 1 SQL错误: `site:$site intext:"sql syntax near" | intext:"syntax error has occurred" | intext:"incorrect syntax near" | intext:"unexpected end of SQL command" | intext:"Warning: mysql_connect()" | intext:"Warning: mysql_query()" | intext:"Warning: pg_connect()"`

Groovy

- 1 公开文件信息: `site:$site ext:doc | ext:docx | ext:odt | ext:pdf | ext:rtf | ext:sxw | ext:psw | ext:ppt | ext:pptx | ext:pps | ext:csv`

Groovy

- 1 `phpinfo()`: `site:$site ext:php intitle:phpinfo "published by the PHP Group"`

Groovy

```
1 搜索粘贴站点: site:pastebin.com | site:paste2.org | site:pastehtml.com |  
    site:slexy.org | site:snipplr.com | site:snipt.net | site:textsnip.com |  
    site:bitpaste.app | site:justpaste.it | site:heypasteit.com |  
    site:hastebin.com | site:dpaste.org | site:dpaste.com | site:codepad.org |  
    site:jsitor.com | site:codepen.io | site:jsfiddle.net | site:dotnetfiddle.net  
    | site:phpfiddle.org | site:ide.geeksforgeeks.org | site:repl.it |  
    site:ideone.com | site:paste.debian.net | site:paste.org | site:paste.org.ru  
    | site:codebeautify.org | site:codeshare.io | site:trello.com $site
```

Groovy

```
1 搜索Github、Gitlab: site:github.com | site:gitlab.com $site.
```

在线Google Hacking利用: <https://tools.zjun.info/googlehacking/>

11.社工信息收集

主要是对目标企业单位的关键员工、供应商和合作伙伴等相关信息进行收集。通过社工可以了解目标企业的人员组织结构，通过分析人员组织结构，能够判断关键人员并对其实施社会工程学鱼叉钓鱼攻击。收集到的相关信息还可以进行社工库查询或字典的制作，用于相关应用系统的暴力破解。

whois信息

whois是用来查询域名的IP及所有人等信息的传输协议。whois的本质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），可以通过whois来实现对域名信息的查询。whois查询可以通过命令行或网页在线查询工具。

whois命令

.

Nginx

```
1 whois xxx.com
```

后面的具体信息就没截出来了，可以查询域名的所有人、注册商等相关信息：

```
~/.Sectools/cms识别 ➤ whois zjun.info
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.afilias.net

domain:      INFO

organisation: Afilias Limited
address:     Level 2, Plaza 3
address:     Custom House Plaza
address:     Harbourmaster Place
address:     Dublin D01 VY76
address:     Ireland

contact:     administrative
name:        Senior Vice President
organisation: Afilias Limited
address:     C/O Afilias USA, Inc.
address:     300 Welsh Road, Building 3
address:     Suite 105
address:     Horsham Pennsylvania 19044
address:     United States
phone:       +1 215 706 5700
fax-no:      +1 215 706 5701
e-mail:      tld-admin-pec@afilias.info
```



在线工具

-
-

CSS

- 1 站长工具whois查询: <http://tool.chinaz.com/ipwhois>

CSS

- 1 爱站网whois查询: <https://whois.aizhan.com/>

12. 社会工程学

社会工程学收集的信息有很多，包含网络ID（现用和曾用）、真实姓名、手机号、电子邮箱、出生日期、身份证号、银行卡、支付宝账号、QQ号、微信号、家庭地址、注册网站（贴吧、微博、人人网

等) 等信息。

在目标相关网页中可能会存在招聘信息、客服联系等，可以利用招聘或客服聊天的方式进行钓鱼、木马植入等。

搜集到相关的人员信息后可以制作社工字典，有如下在线或本地工具：

CSS

- 1 bugku密码攻击器: <https://www.bugku.com/mima/>

Groovy

- 1 白鹿社工字典生成器: <https://github.com/z3r023/BaiLu-SED-Tool>

除了制作社工字典进行爆破外，还可以用已知信息进行社工库查询，涉及敏感信息了，所以不给出链接，在 Telegram 软件中充斥着大量免费或付费的社工查询。

最后

补充一个网址: <https://gitbook.se7ensec.cn/>

信息收集在线工具集合网站