

Dnsrecon

- DNSRecon Python是一个Ruby脚本,我写的语言和我了解DNS在2007年初。这一次我想学习Python并扩展原始工具的功能,并在此过程中重新学习DNS如何工作,以及如何在安全评估和网络故障排除过程中使用它。这个脚本提供了执行的能力:
 - 检查所有NS记录的区域转移。
 - 列举给定域的一般DNS记录(MX, SOA, NS, a, AAAA, SPF和TXT)。
 - 执行普通SRV记录枚举。
 - 顶级域(TLD)扩展。
 - 检查通配符分辨率。
 - 蛮力子域和主机A和AAAA记录给定一个域和一个单词列表。
 - 执行PTR记录查找给定的IP范围或CIDR。
 - 检查DNS服务器缓存记录的a, AAAA和CNAME记录提供了一个列表的主机记录在一个文本文件中进行检查。
 - 枚举本地网络中的公共mDNS记录
 - 使用谷歌枚举主机和子域

一, 官方帮助手册

用法: dnsrecon.py [-h] [-d 域] [-n NS_SERVER] [-r RANGE] [-D 字典] [-f] [-t 型] [-a] [-s] [-g] [-b] [-k] [-w] [-z] [-线程线程] [-生命周期] [-tcp] [-数据库] [-中央电视台] [-约翰逊] [-iw] [-禁用检查递归] [-禁用检查绑定版本] [五世]

可选参数: -h, - help显示此帮助消息并退出 -d 域, -域域 目标域。 -n NS_SERVER, - name_server NS_SERVER 要使用的域服务器。如果没有给出,则 将使用目标。可以指定多个服务器 使用逗号分隔的列表。 -r 范围, -范围范围 格式中反向查找强力的IP范围 (倒数第一)或在(范围/位掩码)内。 -D 字典, -字典字典字典 要用于的子域和主机名的字典文件 蛮力。过滤掉强力域查找, 解析为通配符定义的IP的记录 保存记录时的地址。 -f 过滤掉强力域查找, 记录 保存时解析为通配符定义的IP地址 唱片。要执行的枚举类型。 -用标准枚举执行AXFR。 -s 在SPF中执行IPv4范围的反向查找 带有标准枚举的记录。 -g 使用标准枚举执行谷歌枚举。 -b 使用标准枚举执行Bing枚举。 -k 使用标准枚举执行crt.sh枚举。 -w 执行深入的whois记录分析和反向查找 在执行标准时通过Whois找到的知识产权范围 枚举。 -z 使用标准枚举执行DNSSEC区域漫游。

- threads THREADS 反向查找中使用的线程数, 正向 查找、强力和SRV记录枚举。 -生存期等待服务器响应查询的时间。
- tcp 使用tcp协议进行查询。
- db 数据库SQLite 3文件, 用于保存找到的记录。 用于保存找到的记录的文件。
- csv, - csv CSV逗号分隔值文件。 -j JSON, - json JSON JSON文件。
- iw 继续强力强制域, 即使通配符 记录被发现了。 -禁用检查递归 禁用名称服务器上的递归检查
- disable_check_bindversion 在名称服务器上禁用BIND版本检查 -v 启用详细

usage: dnsrecon.py [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-t TYPE] [-a] [-s] [-g] [-b] [-k] [-w] [-z] [--threads THREADS] [--lifetime LIFETIME] [--tcp] [--db DB] [-x XML] [-c CSV] [-j JSON] [--iw] [--disable_check_recursion] [--disable_check_bindversion] [-v]

optional arguments: -h, --help show this help message and exit -d DOMAIN, --domain DOMAIN Target domain. -n NS_SERVER, --name_server NS_SERVER Domain server to use. If none is given, the SOA of the target will be used. Multiple servers can be specified using a comma separated list. -r RANGE, --range RANGE IP range for reverse lookup brute force in formats (first-last) or in (range/bitmask). -D DICTIONARY, --dictionary DICTIONARY Dictionary file of subdomain and hostnames to use for brute force. Filter out of brute force domain lookup, records that resolve to the wildcard defined IP address when saving records. -f Filter out of brute force domain lookup, records that resolve to the wildcard defined IP address when saving records. -t TYPE, --type TYPE Type of enumeration to perform. -a Perform AXFR with standard enumeration. -s Perform a reverse lookup of IPv4 ranges in the SPF record with standard enumeration. -g Perform Google enumeration with standard enumeration. -b Perform Bing enumeration with standard enumeration. -k Perform crt.sh enumeration with standard enumeration. -w Perform deep whois record analysis and reverse lookup of IP ranges found through Whois when doing a standard enumeration. -z Performs a DNSSEC zone walk with standard enumeration. --threads THREADS Number of threads to use in reverse lookups, forward lookups, brute force and SRV record enumeration. --lifetime LIFETIME Time to wait for a server to response to a query. --tcp Use TCP protocol to make queries. --db DB SQLite 3 file to save found records. -x XML, --xml XML XML file to save found records. -c CSV, --csv CSV Comma separated value file. -j JSON, --json JSON JSON file. --iw Continue brute forcing a domain even if a wildcard records are discovered. --disable_check_recursion Disables check for recursion on name servers --disable_check_bindversion Disables check for BIND version on name servers -v Enable verbose

二，命令实例

dnsecon -d baidu.com

检测目标域baidu.com信息

```
[+] 0 Records Found
[+] [root@parrot]~[/home/kun]
#dnsrecon -d baidu.com
[*] Performing General Enumeration of Domain: baidu.com
[-] DNSSEC is not configured for baidu.com
[*] NS ns2.baidu.com 220.181.33.31
[*] Bind Version for 220.181.33.31 b'baidu dns'
[*] NS dns.baidu.com 202.108.22.220
[*] Bind Version for 202.108.22.220 b'baidu dns'
[*] NS ns7.baidu.com 180.76.76.92
[*] Bind Version for 180.76.76.92 b'baidu dns'
[*] NS ns3.baidu.com 112.80.248.64
[*] Bind Version for 112.80.248.64 b'baidu dns'
[*] NS ns4.baidu.com 14.215.178.80
[*] Bind Version for 14.215.178.80 b'baidu dns'
[*] MX mx.n.shifen.com 220.181.3.85
[*] MX mx.n.shifen.com 220.181.50.185
[*] MX mx.maillb.baidu.com 220.181.50.185
[*] MX jpmx.baidu.com 12.0.243.41
[*] MX mx1.baidu.com 220.181.3.85
[*] MX mx1.baidu.com 111.202.115.85
[*] MX mx50.baidu.com 180.76.13.18
[*] A baidu.com 220.181.38.148
[*] A baidu.com 39.156.69.79
[*] Enumerating SRV Records
[*] SRV _sip._tcp.baidu.com vcs.wshifen.com 61.135.165.170 5060 0
[*] SRV _sips._tcp.baidu.com vcs.wshifen.com 61.135.165.170 5061 0
[*] SRV _h323cs._tcp.baidu.com vcs.wshifen.com 61.135.165.170 1720 0
[*] SRV _h323ls._udp.baidu.com vcs.wshifen.com 61.135.165.170 1719 0
[*] SRV _sip._tls.baidu.com sip.baidu.com 220.181.3.68 443 0
[*] SRV _sipfederationtls._tcp.baidu.com sip.n.shifen.com 220.181.3.68 5061 0
[*] SRV _xmpp-server._tcp.baidu.com xmpp.wshifen.com 61.135.165.169 5269 0
[*] SRV _xmpp-client._tcp.baidu.com xmpp.wshifen.com 61.135.165.169 5222 0
[*] SRV _sipinternaltls._tcp.baidu.com dirpool.internal.baidu.com no_ip 5061 0
[*] SRV _autodiscover._tcp.baidu.com email.baidu.com 220.181.50.187 443 0
[+] 10 Records Found
```

dnsrecon -r 27.254.33.19-220 -d baidu.com

制定一个扫描范围，IP范围/位掩码[^这里我制定的是27.254.33.19-220]

```
[*][root@parrot]~[/home/kun]
#dnsrecon -r 27.254.33.193-220 -d baidu.com
[-] Range provided is not valid
[-] Failed CIDR or Range is Required for type rvl
[*] Performing General Enumeration of Domain: baidu.com
[-] DNSSEC is not configured for baidu.com
[*] NS ns3.baidu.com 112.80.248.64
[*] Bind Version for 112.80.248.64 b'baidu dns'
[*] NS ns2.baidu.com 220.181.33.31
[*] Bind Version for 220.181.33.31 b'baidu dns'
[*] NS ns4.baidu.com 14.215.178.80
[*] Bind Version for 14.215.178.80 b'baidu dns'
[*] NS dns.baidu.com 202.108.22.220
[*] Bind Version for 202.108.22.220 b'baidu dns'
[*] NS ns7.baidu.com 180.76.76.92
[*] Bind Version for 180.76.76.92 b'baidu dns'
[*] MX mx1.baidu.com 111.202.115.85
[*] MX mx1.baidu.com 220.181.3.85
[*] MX mx.maillb.baidu.com 220.181.50.185
[*] MX mx.n.shifen.com 220.181.50.185
[*] MX mx.n.shifen.com 220.181.3.85
[*] MX mx50.baidu.com 180.76.13.18
[*] MX jpmx.baidu.com 12.0.243.41
[*] A baidu.com 39.156.69.79
[*] A baidu.com 220.181.38.148
[*] Enumerating SRV Records
[*] SRV _sip._tcp.baidu.com vcs.wshifen.com 61.135.165.170 5060 0
[*] SRV _sips._tcp.baidu.com vcs.wshifen.com 61.135.165.170 5061 0
[*] SRV _h323cs._tcp.baidu.com vcs.wshifen.com 61.135.165.170 1720 0
[*] SRV _h323ls._udp.baidu.com vcs.wshifen.com 61.135.165.170 1719 0
[*] SRV _sip._tls.baidu.com sip.baidu.com 220.181.3.68 443 0
[*] SRV _sipfederationtls._tcp.baidu.com sip.n.shifen.com 220.181.3.68 5061 0
[*] SRV _xmpp-server._tcp.baidu.com xmpp.wshifen.com 61.135.165.169 5269 0
[*] SRV _xmpp-client._tcp.baidu.com xmpp.wshifen.com 61.135.165.169 5222 0
[*] SRV _sipinternaltls._tcp.baidu.com dirpool.internal.baidu.com no_ip 5061 0
[*] SRV _autodiscover._tcp.baidu.com email.baidu.com 220.181.50.187 443 0
[+] 10 Records Found
[+] [root@parrot]~[/home/kun]
#
```

如果此时还不理解这个“-r”的参数，可以参考下图

```
dnsrecon -r 19-20 -d baidu.com
```

```
[root@parrot]~[/home/kun]
#dnsrecon -r 19-20 -d baidu.com
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 0.0.0.19 to 0.0.0.20
[+] 0 Records Found
[root@parrot]~[/home/kun]
#
```

```
dnsrecon -D /home/kun/test -d zsdk.org.cn
```

使用蛮力对子域和主机名的字典文件，保存时，用于过滤掉解析为通配符定义的强力域记录

```
[root@parrot]~[/home/kun]
#dnsrecon -D /home/kun/test -d zsdk.org.cn
[*] Performing General Enumeration of Domain: zsdk.org.cn
[-] DNSSEC is not configured for zsdk.org.cn
[*] NS dns15.hichina.com 140.205.81.15
[*] NS dns15.hichina.com 106.11.211.65
[*] NS dns15.hichina.com 140.205.41.15
[*] NS dns15.hichina.com 140.205.81.25
[*] NS dns15.hichina.com 106.11.141.125
[*] NS dns15.hichina.com 106.11.211.55
[*] NS dns15.hichina.com 106.11.141.115
[*] NS dns15.hichina.com 140.205.41.25
[*] NS dns15.hichina.com 2400:3200:2000:34::1
[*] NS dns16.hichina.com 140.205.41.26
[*] NS dns16.hichina.com 106.11.141.116
[*] NS dns16.hichina.com 106.11.211.66
[*] NS dns16.hichina.com 106.11.141.126
[*] NS dns16.hichina.com 140.205.81.16
[*] NS dns16.hichina.com 140.205.81.26
[*] NS dns16.hichina.com 106.11.211.56
[*] NS dns16.hichina.com 140.205.41.16
[*] NS dns16.hichina.com 2400:3200:2000:35::1
[*] MX mxbiz1.qq.com 183.57.48.34
[*] MX mxbiz2.qq.com 183.57.48.34
[*] A zsdk.org.cn 47.240.42.2
```

```
dnsrecon -f -d baidu.com
```

-f 过滤出强力域查找，记录解析为通配符定义的IP地址时记录[^可通过wireshark抓包查看两者区别]

Source	Destination	Protocol	Length	Size	Source	Destination	Protocol	Length	Size		
1.0.900090000	192.168.0.193	202.96.128.166	DNS	82	Standard query 0x34c8 1a5f68e9c1d0.	1.0.900090000	192.168.0.193	202.96.128.166	DNS	82	Standard query 0x3f08 1a5f68e9c1d0.
2.0.818181828	202.96.128.166	192.168.0.193	DNS	125	Standard query response 0x34c8 1a5f68e9c1d0.	2.0.818181828	202.96.128.166	192.168.0.193	DNS	125	Standard query response 0x3f08 1a5f68e9c1d0.
3.0.928441197	192.168.0.193	202.96.128.166	DNS	87	Standard query 0x0511 1a5f68e9c1d0.	3.0.928441197	192.168.0.193	202.96.128.166	DNS	87	Standard query 0x0516 1a5f68e9c1d0.
4.0.64529752	202.96.128.166	192.168.0.193	DNS	162	Standard query response 0x0511 1a5f68e9c1d0.	4.0.64529752	202.96.128.166	192.168.0.193	APR	42	Who has 192.168.0.100? Tell 192.168.0.100.
5.0.646222354	192.168.0.193	202.96.128.166	DNS	87	Standard query 0x2380 1a5f68e9c1d0.	5.0.646222354	192.168.0.193	202.96.128.166	DNS	162	Standard query response 0x0516 1a5f68e9c1d0.
6.2.733804173	202.96.128.166	192.168.0.193	DNS	156	Standard query response 0x2380 1a5f68e9c1d0.	6.2.733804173	192.168.0.193	202.96.128.166	DNS	87	Standard query 0x341d 1a5f68e9c1d0.
7.2.734907594	192.168.0.193	202.96.128.166	DNS	69	Standard query 0x0e02 D0N5EY balid.	7.2.734907594	192.168.0.193	202.96.128.166	DNS	69	Standard query 0x341d 1a5f68e9c1d0.
8.0.734604577	202.96.128.166	192.168.0.193	DNS	112	Standard query response 0x0e02 50a balid.	8.0.734604577	202.96.128.166	192.168.0.193	DNS	112	Standard query response 0x0e02 50a balid.
9.2.752691708	192.168.0.193	202.96.128.166	DNS	69	Standard query 0x0d55 50a balid.	9.2.752691708	192.168.0.193	202.96.128.166	DNS	69	Standard query 0x3474 D0N5EY balid.
10.2.763208801	202.96.128.166	192.168.0.193	DNS	282	Standard query response 0x0d55 50a balid.	10.2.763208801	202.96.128.166	192.168.0.193	DNS	278	Standard query response 0x4474 50a balid.
11.2.766670982	192.168.0.193	202.96.128.166	DNS	69	Standard query 0x04b0 NS balid.	11.2.766670982	192.168.0.193	202.96.128.166	DNS	69	Standard query 0x4197 NS balid.
12.2.774928701	202.96.128.166	192.168.0.193	DNS	239	Standard query response 0x04b0 NS balid.	12.2.774928701	202.96.128.166	192.168.0.193	DNS	239	Standard query response 0x4197 NS balid.
13.2.776837890	192.168.0.193	202.96.128.166	DNS	73	Standard query 0x4303 A dns balid.	13.2.776837890	192.168.0.193	202.96.128.166	DNS	73	Standard query 0x5f6e A ns3 balid.
14.2.790357382	202.96.128.166	192.168.0.193	DNS	239	Standard query response 0x4303 A dns balid.	14.2.790357382	202.96.128.166	192.168.0.193	DNS	239	Standard query response 0x5f6e A ns3 balid.

```

[~][root@parrot]-[/home/kun]
#dnsrecon -s -d baidu.com
[*] Performing General Enumeration of Domain: baidu.com
[-] DNSSEC is not configured for baidu.com
[*] NS dns.baidu.com 202.108.22.220
[*] Bind Version for 202.108.22.220 b'baidu dns'
[*] NS ns2.baidu.com 220.181.33.31
[*] Bind Version for 220.181.33.31 b'baidu dns'
[*] NS ns4.baidu.com 14.215.178.80
[*] Bind Version for 14.215.178.80 b'baidu dns'
[*] NS ns3.baidu.com 112.80.248.64
[*] Bind Version for 112.80.248.64 b'baidu dns'
[*] NS ns7.baidu.com 180.76.76.92
[*] Bind Version for 180.76.76.92 b'baidu dns'
[*] MX mx1.baidu.com 111.202.115.85
[*] MX mx1.baidu.com 220.181.3.85
[*] MX jpmx.baidu.com 12.0.243.41
[*] MX mx.n.shifen.com 220.181.3.85
[*] MX mx.n.shifen.com 220.181.50.185
[*] MX mx.maillb.baidu.com 220.181.50.185
[*] MX mx50.baidu.com 180.76.13.18
[*] A baidu.com 220.181.38.148
[*] A baidu.com 39.156.69.79
[*] Enumerating SRV Records
[*] SRV _sip._tcp.baidu.com vcs.wshifen.com 61.135.165.170 5060 0
[*] SRV _sips._tcp.baidu.com vcs.wshifen.com 61.135.165.170 5061 0
[*] SRV _h323cs._tcp.baidu.com vcs.wshifen.com 61.135.165.170 1720 0
[*] SRV _h323ls._udp.baidu.com vcs.wshifen.com 61.135.165.170 1719 0
[*] SRV _sip._tls.baidu.com sip.baidu.com 220.181.3.68 443 0
[*] SRV _xmpp-server._tcp.baidu.com xmpp.wshifen.com 61.135.165.169 5269
0
[*] SRV _xmpp-client._tcp.baidu.com xmpp.wshifen.com 61.135.165.169 5222
0
[*] SRV _sipfederationtls._tcp.baidu.com sip.n.shifen.com no_ip 5061 0
[*] SRV _autodiscover._tcp.baidu.com email.baidu.com 220.181.50.187 443
0
[*] SRV _sipinternaltls._tcp.baidu.com dirpool.internal.baidu.com no_ip
5061 0
[+] 10 Records Found

```

dnnsrecon -g -d zsdk.org.cn

使用google对域进行检索[^由于我们处于国内，所以无法访问google.com,自然而然的无法与google服务器进行握手]


```

[~][root@parrot]-[/home/kun]
#dnsrecon -g -d zsdk.org.cn
[*] Performing General Enumeration of Domain: zsdk.org.cn
[-] DNSSEC is not configured for zsdk.org.cn
[*] NS dns15.hichina.com 140.205.41.25
[*] NS dns15.hichina.com 106.11.211.65
[*] NS dns15.hichina.com 140.205.81.25
[*] NS dns15.hichina.com 140.205.81.15
[*] NS dns15.hichina.com 106.11.211.55
[*] NS dns15.hichina.com 106.11.141.125
[*] NS dns15.hichina.com 140.205.41.15
[*] NS dns15.hichina.com 106.11.141.115
[*] NS dns15.hichina.com 2400:3200:2000:34::1
[*] NS dns16.hichina.com 140.205.41.16
[*] NS dns16.hichina.com 106.11.211.56
[*] NS dns16.hichina.com 140.205.81.16
[*] NS dns16.hichina.com 106.11.141.126
[*] NS dns16.hichina.com 140.205.41.26
[*] NS dns16.hichina.com 106.11.211.66
[*] NS dns16.hichina.com 140.205.81.26
[*] NS dns16.hichina.com 106.11.141.116
[*] NS dns16.hichina.com 2400:3200:2000:35::1
[*] MX mxbiz2.qq.com 183.57.48.34
[*] MX mxbiz1.qq.com 183.57.48.34
[*] A zsdk.org.cn 47.240.42.2
[*] Enumerating SRV Records
[-] No SRV Records Found for zsdk.org.cn
[+] 0 Records Found
[*] Performing Google Search Enumeration
Traceback (most recent call last):
  File "/usr/share/dnsrecon/lib/goonenum.py", line 54, in scrape_google
    sock = urllib.urlopen(url)
AttributeError: module 'urllib' has no attribute 'urlopen'

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/lib/python3.7/urllib/request.py", line 1319, in do_open
    encode_chunked=req.has_header('Transfer-encoding'))
  File "/usr/lib/python3.7/http/client.py", line 1252, in request
    self._send_request(method, url, body, headers, encode_chunked)

```

dnsrecon -b -d baidu.com

使用Bing对baidu.com进行枚举

```

File Edit View Bookmarks Settings Help
[root@parrot]-[/home/kun]
#dnsrecon -b -d baidu.com
[*] Performing General Enumeration of Domain: baidu.com
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 47.254.33.193
[!] All queries will resolve to this address!!
[-] DNSSEC is not configured for baidu.com
[*] NS dns2.name-services.com 64.98.151.1
[-] Recursion enabled on NS Server 64.98.151.1
[*] NS dns2.name-services.com 2604:4000:4000:0:64:98:151:1
[*] NS dns1.name-services.com 98.124.243.1
[-] Recursion enabled on NS Server 98.124.243.1
[*] Bind Version for 98.124.243.1 b'Served by PowerDNS - https://www.powerdns.com/'
[*] NS dns1.name-services.com 2620:10f:5000:5002:98:124:243:1
[*] NS dns3.name-services.com 98.124.243.2
[-] Recursion enabled on NS Server 98.124.243.2
[*] NS dns3.name-services.com 2620:10f:5000:5002:98:124:243:2
[*] NS dns5.name-services.com 98.124.243.3
[-] Recursion enabled on NS Server 98.124.243.3
[*] Bind Version for 98.124.243.3 b'Served by PowerDNS - https://www.powerdns.com/'
[*] NS dns5.name-services.com 2620:10f:5000:5002:98:124:243:3
[-] Could not Resolve MX Records for baidu.com
[*] A baidu.com 47.254.33.193
[*] Enumerating SRV Records
[-] No SRV Records Found for baidu.com
[+] 0 Records Found
[*] Performing Bing Search Enumeration

```

dnsrecon -k -d baidu.com

对baidu.com举行crt.sh枚举[^crt.sh是类似与证书搜索的一个站点]

```

[root@parrot]-[/home/kun]
#dnsrecon -k -d baidu.com
[*] Performing General Enumeration of Domain: baidu.com
[-] DNSSEC is not configured for baidu.com
[*] NS ns4.baidu.com 14.215.178.80
[*] Bind Version for 14.215.178.80 b'baidu dns'
[*] NS ns2.baidu.com 220.181.33.31
[*] Bind Version for 220.181.33.31 b'baidu dns'
[*] NS ns3.baidu.com 112.80.248.64
[*] Bind Version for 112.80.248.64 b'baidu dns'
[*] NS dns.baidu.com 202.108.22.220
[*] Bind Version for 202.108.22.220 b'baidu dns'
[*] NS ns7.baidu.com 180.76.76.92
[*] Bind Version for 180.76.76.92 b'baidu dns'
[*] MX mx50.baidu.com 180.76.13.18
[*] MX mx1.baidu.com 111.202.115.85
[*] MX mx1.baidu.com 220.181.3.85
[*] MX jpmx.baidu.com 12.0.243.41
[*] MX mx.maillb.baidu.com 220.181.50.185
[*] MX mx.n.shifen.com 220.181.50.185
[*] MX mx.n.shifen.com 220.181.3.85
[*] A baidu.com 220.181.38.148
[*] A baidu.com 39.156.69.79
[*] Enumerating SRV Records
[*] SRV _sips._tcp.baidu.com vcs.wshifen.com 61.135.165.170 5061 0
[*] SRV _sip._tcp.baidu.com vcs.wshifen.com 61.135.165.170 5060 0
[*] SRV _h323ls._udp.baidu.com vcs.wshifen.com 61.135.165.170 1719 0
[*] SRV _h323cs._tcp.baidu.com vcs.wshifen.com 61.135.165.170 1720 0
[*] SRV _sip._tls.baidu.com sip.baidu.com 220.181.3.68 443 0
[*] SRV _sipfederationtls._tcp.baidu.com sip.n.shifen.com 220.181.3.68 5061 0
[*] SRV _xmpp-server._tcp.baidu.com xmpp.wshifen.com 61.135.165.169 5269 0
[*] SRV _xmpp-client._tcp.baidu.com xmpp.wshifen.com 61.135.165.169 5222 0
[*] SRV _sipinternaltls._tcp.baidu.com dirpool.internal.baidu.com no_ip 5061 0
[*] SRV _autodiscover._tcp.baidu.com email.baidu.com 220.181.50.187 443 0
[+] 10 Records Found
[*] Performing Crt.sh Search Enumeration
[*] *.baidu.com wildcard
[*] *.mai.baidu.com wildcard
[*] *.safe.baidu.com wildcard
[*] *.mai.baidu.com wildcard
[*] *.safe.baidu.com wildcard

```

dnsrecon -w -d zsdk.org.cn

执行深入的Whois记录分析和反向查找，在执行标准时通过Whois找到知识产权枚举[^温馨提示]

- 过一段时间后他会告诉你两句话你修要注意

[*]要对哪个范围执行反向查找？

[*]数字，逗号分隔列表，a表示全部，n表示无


```

#dnsrecon -w -d zsdk.org.cn
[*] Performing General Enumeration of Domain: zsdk.org.cn
[-] DNSSEC is not configured for zsdk.org.cn
[*] NS dns15.hichina.com 106.11.211.55
[*] NS dns15.hichina.com 106.11.141.125
[*] NS dns15.hichina.com 140.205.81.25
[*] NS dns15.hichina.com 106.11.211.65
[*] NS dns15.hichina.com 140.205.41.15
[*] NS dns15.hichina.com 140.205.81.15
[*] NS dns15.hichina.com 106.11.141.115
[*] NS dns15.hichina.com 140.205.41.25
[*] NS dns15.hichina.com 2400:3200:2000:34::1
[*] NS dns16.hichina.com 106.11.141.126
[*] NS dns16.hichina.com 140.205.81.26
[*] NS dns16.hichina.com 140.205.41.16
[*] NS dns16.hichina.com 106.11.211.66
[*] NS dns16.hichina.com 106.11.141.116
[*] NS dns16.hichina.com 140.205.41.26
[*] NS dns16.hichina.com 140.205.81.16
[*] NS dns16.hichina.com 106.11.211.56
[*] NS dns16.hichina.com 2400:3200:2000:35::1
[*] MX mxbiz2.qq.com 183.57.48.34
[*] MX mxbiz1.qq.com 183.57.48.34
[*] A zsdk.org.cn 47.240.42.2
[*] Enumerating SRV Records
[-] No SRV Records Found for zsdk.org.cn
[+] 0 Records Found
[*] Performing Whois lookup against records found.
[Errno 111] Connection refused
[Errno 111] Connection refused
[Errno 111] Connection refused
[Errno 110] Connection timed out
[Errno 111] Connection refused
[Errno 111] Connection refused
[Errno 111] Connection refused
[Errno 111] Connection refused
[Errno 111] Connection refused
[*] The following IP Ranges were found:
[*] 0) 106.11.0.0-106.11.255.255 Not Found
[*] 1) 183.0.0.0-183.63.255.255 Not Found
[*] What Range do you wish to do a Revers Lookup for?
[*] number, comma separated list, a for all or n for none
a
[*] Performing Reverse Lookup of range 106.11.0.0-106.11.255.255
[*] Performing Reverse Lookup from 106.11.0.0 to 106.11.255.255

```

dnsecon -z -d baidu.com

使用标准枚举执行DNSSEC区域漫游

DNSSEC全称Domain Name System Security Extensions，即DNS安全扩展，是由IETF提供的一系列DNS安全认证的机制（可参考[RFC2535](https://tools.ietf.org/html/rfc2535)）。它提供一种可以验证应答信息真实性和完整性的机制，利用密码技术，使得域名解析服务器可以验证它所收到的应答(包括域名不存在的应答)是否来自于真实的服务器，或者是否在传输过程中被篡改过。

```
[root@parrot:~]# dnsrecon -z -d baidu.com
[*] Performing General Enumeration of Domain: baidu.com
[-] DNSSEC is not configured for baidu.com
[*] NS ns2.baidu.com 220.181.33.31
[*] Bind Version for 220.181.33.31 b'bind 9.10.4'
[*] NS ns3.baidu.com 112.80.248.64
[*] Bind Version for 112.80.248.64 b'bind 9.10.4'
[*] NS ns4.baidu.com 14.215.178.80
[*] Bind Version for 14.215.178.80 b'bind 9.10.4'
[*] NS ns7.baidu.com 180.76.76.92
[*] Bind Version for 180.76.76.92 b'bind 9.10.4'
[*] NS dns.baidu.com 202.108.22.220
[*] Bind Version for 202.108.22.220 b'bind 9.10.4'
[*] MX jpmx.baidu.com 12.0.243.41
[*] MX mx.maillb.baidu.com 220.181.50.185
[*] MX mx50.baidu.com 180.76.13.18
[*] MX mx.n.shifen.com 220.181.3.85
[*] MX mx.n.shifen.com 220.181.50.185
[*] MX mx1.baidu.com 111.202.115.85
[*] MX mx1.baidu.com 220.181.3.85
[*] A baidu.com 39.156.69.79
[*] A baidu.com 220.181.38.148
[*] Enumerating SRV Records
[*] SRV _sip._tcp.baidu.com vcs.wshifen.com 61.135.165.170 5060 0
[*] SRV _sips._tcp.baidu.com vcs.wshifen.com 61.135.165.170 5061 0
[*] SRV _h323cs._tcp.baidu.com vcs.wshifen.com 61.135.165.170 1720 0
[*] SRV _sipfederationtls._tcp.baidu.com sip.n.shifen.com 220.181.3.68 5061 0
[*] SRV _sip._tls.baidu.com sip.baidu.com 220.181.3.68 443 0
[*] SRV _h323ls._udp.baidu.com vcs.wshifen.com 61.135.165.170 1719 0
[*] SRV _xmpp-server._tcp.baidu.com xmpp.wshifen.com 61.135.165.169 5269 0
[*] SRV _xmpp-client._tcp.baidu.com xmpp.wshifen.com 61.135.165.169 5222 0
[*] SRV _sipinternaltls._tcp.baidu.com dirpool.internal.baidu.com no_ip 5061 0
[*] SRV _autodiscover._tcp.baidu.com email.baidu.com 220.181.50.187 443 0
[+] 10 Records Found
[*] Performing NSEC Zone Walk for baidu.com
[*] Getting SOA record for baidu.com
[-] This zone appears to be misconfigured, no SOA record found.
[*] A baidu.com 39.156.69.79
[*] A baidu.com 220.181.38.148
[+] 2 records found
```