此文章已于 1:02:38 2015/12/25 发布到 Net | Linux | 安全

★Kali信息收集~4.DNS系列

★.1host：DNS信息

参数：

计算机生成了可选文字:
host 
Usage: host - 
aCd1 riTwvl classl ( -N ndotsl ( - 
-R numberl ( - 
m flagl hostname (server) 
ypel 
timel 
-a 
-C 
-d 
1 
-1 
N 
-R 
T 
-v 
-4 
-6 
-m 
rootMati• - 
s 
equivalent t 
t ANY 
i fies query class for non- IN data 
spec 
compares SOA records on authoritative nameservers 
s equivalent t 
lists all hosts in a domain, using AXFR 
IP6. INT reverse lookups 
changes 
the number of dots allowed before root lookup is done 
disables recursive processing 
spec If les number of ret ries for UDP packets 
E F IL response should stop query 
if i 
the query type 
spec 
enables TCP/ IP mode 
enables verbose output 
spec If les to wait forever for a reply 
spec If les how long to wait for a reply 
use IPv4 query transport only 
use IPv6 query transport only 
set memory debugging flag (tracel recordl usage) 

**一般情况下，host查找的是A，AAAA，和MX的记录**

计算机生成了可选文字:
No 
TYPE ) 
SOA 
NS 
I'v1X 
CNAME 
IPtüt1Eä*tfi 
IPv6tüt1Eit.* 

**案例：**

* 1. **DNS服务器查询**

重要 **host -t ns 域名**

计算机生成了可选文字:
cnblogs. co 
m 
cnblogs. co 
m 
host -t ns 
name server 
name server 
cnblogs. com 
ns4. dnsv4. com. 
ns3. dnsv4. com 

* 1. **A记录和MX记录查询**

重要 **host 域名**（host -t a 域名 + host -t mx 域名）

计算机生成了可选文字:
o s. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
host cnblogs. com 
as a ress 
10 
20 
20 
30 
30 
30 
30 
aspmx. l. google. com 
altl. aspmx. l. google. com 
alt2. aspmx. 1. google. com 
aspmx5. googlemail. 
aspmx2. googlemail. 
aspmx4. googlemail. 
aspmx3. googlemail. 
mail 
mail 
mail 
mail 
mail 
mail 
mail 
handled 
handled 
handled 
handled 
handled 
handled 
handled 

**PS：A (Address) 记录**是用来指定主机名（或域名）对应的IP地址记录。用户可以将该域名下的网站服务器指向到自己的web server上。同时也可以设置您域名的子域名。通俗来说A记录就是服务器的IP,域名绑定A记录就是告诉DNS,当你输入域名的时候给你引导向设置在DNS的A记录所对应的服务器。

**PS**：**MX记录**也叫做邮件路由记录，用户可以将该域名下的邮件服务器指向到自己的mail server上，然后即可自行操控所有的邮箱设置。您只需在线填写您服务器的IP地址，即可将您域名下的邮件全部转到您自己设定相应的邮件服务器上。简单的说，通过操作MX记录，您才可以得到以您域名结尾的邮局。

4.2Dig ：DNS挖掘

* 1. 参数：

root@Kali:/home/dnt# **dig -h**

Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}

{global-d-opt} host [@local-server] {local-d-opt}

[ host [@local-server] {local-d-opt} [...]]

Where: domain         is in the Domain Name System

q-class is one of (in,hs,ch,...) [default: in]

q-type is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]

(Use ixfr=version for type ixfr)

q-opt is one of:

-x dot-notation (shortcut for reverse lookups)

-i (use IP6.INT for IPv6 reverse lookups)

-f filename (batch mode)

-b address[#port] (bind to source address/port)

-p port (specify port number)

-q name (specify query name)

-t type (specify query type)

-c class (specify query class)

-k keyfile (specify tsig key file)

-y [hmac:]name:key (specify named base64 tsig key)

-4 (use IPv4 query transport only)

-6 (use IPv6 query transport only)

-m (enable memory usage debugging)

d-opt is of the form +keyword[=value], where keyword is:

+[no]vc (TCP mode)

+[no]tcp (TCP mode, alternate syntax)

+time=### (Set query timeout) [5]

+tries=### (Set number of UDP attempts) [3]

+retry=### (Set number of UDP retries) [2]

+domain=### (Set default domainname)

+bufsize=### (Set EDNS0 Max UDP packet size)

+ndots=### (Set NDOTS value)

+[no]edns[=###] (Set EDNS version) [0]

+[no]search (Set whether to use searchlist)

+[no]showsearch (Search with intermediate results)

+[no]defname (Ditto)

+[no]recurse (Recursive mode)

+[no]ignore (Don't revert to TCP for TC responses.)

+[no]fail (Don't try next server on SERVFAIL)

+[no]besteffort (Try to parse even illegal messages)

+[no]aaonly (Set AA flag in query (+[no]aaflag))

+[no]adflag (Set AD flag in query)

+[no]cdflag (Set CD flag in query)

+[no]cl (Control display of class in records)

+[no]cmd (Control display of command line)

+[no]comments (Control display of comment lines)

+[no]rrcomments (Control display of per-record comments)

+[no]question (Control display of question)

+[no]answer (Control display of answer)

+[no]authority (Control display of authority)

+[no]additional (Control display of additional)

+[no]stats (Control display of statistics)

+[no]short (Disable everything except short

form of answer)

+[no]ttlid (Control display of ttls in records)

+[no]all (Set or clear all display flags)

+[no]qr (Print question before sending)

+[no]nssearch (Search all authoritative nameservers)

+[no]identify (ID responders in short answers)

+[no]trace (Trace delegation down from root [+dnssec])

+[no]dnssec (Request DNSSEC records)

+[no]nsid (Request Name Server ID)

+[no]sigchase (Chase DNSSEC signatures)

+trusted-key=#### (Trusted Key when chasing DNSSEC sigs)

+[no]topdown (Do DNSSEC validation top down mode)

+[no]split=## (Split hex/base64 fields into chunks)

+[no]multiline (Print records in an expanded format)

+[no]onesoa (AXFR prints only one soa record)

+[no]keepopen (Keep the TCP socket open between queries)

global d-opts and servers (before host name) affect all queries.

local d-opts and servers (after host name) affect only that lookup.

-h (print help and exit)

-v (print version and exit)

* 1. 常用：**dig 域名 any**

重要 root@Kali:/home/dnt# **dig cnblogs.com any**

; <<>> DiG 9.9.5-9+deb8u2-Debian <<>> cnblogs.com any

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18664

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:

;cnblogs.com.                        IN        ANY

;; ANSWER SECTION:

**cnblogs.com.                5        IN        NS        ns4.dnsv4.com.**

**cnblogs.com.                5        IN        NS        ns3.dnsv4.com.**

;; Query time: 2010 msec

;; SERVER: 192.168.232.2#53(192.168.232.2)

;; WHEN: Thu Dec 24 23:19:22 CST 2015

;; MSG SIZE rcvd: 71

4.3NS Lookup ：DNS裤子

**Windows+Linux都自带**

nslookup最简单的用法就是查询域名对应的IP地址，包括A记录和CNAME记录

帮助文档：**man nslookup**

计算机生成了可选文字:
NSLOOKUP( 1) 
NAME 
nsl ookup 
SYNOPSIS 
BIND9 
query Internet name servers interactively 
NSLOOKUP( 1) 
( - option) 
name I 
nstookup 
-l (server) 
DESCRIPTION 
Nstookup is a program to query Internet domain name servers. 
Nstookup has two modes: 
interactive and 
non- interactive. 
Interactive mode allows 
the user to query name servers for information about various hosts 
and domains or to print a list 
f hosts in a domain. Non- interactive mode is used to print just the name and 
requested information for a host or domain. 
ARGUMENTS 
Interactive mode IS entered in the following cases: 
2. 
when no arguments are given ( the default name server will be used) 
when the first argument is a hyphen (-) and the second argument is the host name or Internet address of a 
name server. 
Non- interactive mode is used when the name or Internet address of the host to be looked up is given as the first 
argument. The optional second argument specifi 
the host name or address of a name server. 
Options can also be spec 1 fled on the command line if they precede the arguments and are prefixed with a hyphen. For 
example, 
o change the default query type to host information, and the initial timeout to 10 seconds, 
ype: 
nslookup -query—hinf 
- timeout 
-10 
INTERACTIVE COMMANDS 
host (server-I 
00k up information 
an Internet address 
and does not have a 
server domain 
tserver domain 
for host using the current default 
server or using server, if 
1 fled. 
If host i 
spec 
and the query type IS A or P T R, the name of the host is returned. 
If host i 
s a name 
trailing period, 
the search list is used to qualif the name. 
To look up a host not in the current domain, 
Change the default 
server to domain" tserver 
while server uses 
the current default 
se rve r. 
append a period to the name. 
the initial server to look 
uses 
If an authoritative answer can 
up information about domain 
be found, 
the names o 

我们看看windows里面的帮助文档（明了一点）

计算机生成了可选文字:
: Wsers •ONT lookup 
: . dnspai.com 
ddress : 
218.3ø.118.6 
AME 
RHEI NRME2 
et OPTION 
all 
Ino Idebug 
'no Id2 
Ino Ref name 
Ino h•ecurse 
Ino Isearch 
Ino luc 
doma in —NAME 
srchlist —NI L/N2/.. 
NAME 
NAME 
root —NAME 
retry —X 
t imeout —X 
t ype —X 
queryt ype —X 
c lass —X 
Ino Imsxfr 
ixfruer—X 
eruer NAME 
Iseruer NAME 
oot 
x it 
NS, PTR, SOR SRU) 
IN (Internet)iQ ANY) 
CNRME, "X 
NS PIR 2*-) 
91 

**常用命令：nslookup**

**0.设置默认服务器**

**server 8.8.8.8**

计算机生成了可选文字:
nslookup 
server 8. 8. 8.8 
Default 
server: 8. 8. 8. 8 
Address: 8. 8. 8. 8#53 

重要 **1.简单查询域名信息**

**> set type=any**

**>** cnblogs.com

计算机生成了可选文字:
set t 
ypeeany 
30 
30 
20 
30 
10 
20 
30 
aspmx3. googlemail. 
aspmx4. googlemail. 
alt2. aspmx. 1. google. com 
aspmx5. googlemail. 
aspmx2. googlemail. 
aspmx. 1. google. com 
alt 1. aspmx. 1. 
google. com 
cnblogs. com 
Se rve r: 
Add ress: 
8. 8. 8. 8#53 
Non- authoritative answer: 
Name: 
cnblogs. com 
Add ress: 
42. 121. 252. 58 
cnblogs. com 
cnblogs. co 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
mail 
mail 
mail 
mail 
mail 
mail 
mail 
exchanger 
exchanger 
exchanger 
exchanger 
exchanger 
exchanger 
exchanger 
ns3. 
ns4. 
dnsv4. com 
dnsv4. com 
namese rver 
namese rver 
ns3. dnsv4. com 
or 1 gin 
mail addr 
enterprise2dnsadmin. dnspod. com 
se rial 
- 1450611476 
ref resh 
- 3600 
- 180 
ret ry 
found 
f rom. 
expl re 
ml nlmum 
- 1209600 
- 180 
A 
uthoritative answers can be 

重要 **2.查询域名CNAME记录(别名指向)**

**> set type=cname**

**>** cnblogs.com

计算机生成了可选文字:
set t 
ypeecname 
cnblogs. com 
Se rve r: 
Add ress: 
dnspod. co 
8. 8. 8. 8#53 
Non- authoritative answer: 
*** Can't find cnblogs. co 
m: No answer 
Authoritative answers can be found from. 
cnblogs. com 
— ns3. dnsv4. com 
or 1 gin 
mail addr 
enterprise2dnsadmin. 
se rial 
- 1450611476 
ref resh 
- 3600 
- 180 
ret ry 
expl re 
ml nlmum 
- 1209600 
- 180 

重要 **3.查询域名A记录**（**通俗来说A记录就是服务器的IP，域名绑定A记录就是告诉DNS，当你输入域名的时候给你引导向设置在DNS的A记录所对应的服务器**）

计算机生成了可选文字:
set t 
ypeea 
cnblogs. com 
Se rve r: 
Add ress: 
8. 8. 8. 8#53 
Non- authoritative answer: 
Name: 
cnblogs. com 
Address: 42. 121. 252. 58 

重要 **4.查询域名MX记录(邮件记录)**

**> set type=mx**

**>** cnblogs.com

计算机生成了可选文字:
et t 
ype—mx 
cnblogs. com 
Se rve r: 
Add ress: 
8. 8. 8. 8#53 
Non- authoritative answer: 
20 
30 
30 
20 
30 
10 
30 
alt2. aspmx. l. google. com 
aspmx5. googlemail. 
aspmx3. googlemail. 
altl. aspmx. l. google. com 
aspmx4. googlemail. 
aspmx. l. google. com 
aspmx2. googlemail 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
cnblogs. com 
A 
uthoritative 
mail 
mail 
mail 
mail 
mail 
mail 
mail 
exchanger 
exchanger 
exchanger 
exchanger 
exchanger 
exchanger 
exchanger 
answers can be found from. 

重要 **5.查询域名ns记录(域名所使用的DNS)**

计算机生成了可选文字:
set t 
ype—cname 
cnblogs. com 
Se rve r: 
Add ress: 
dnspod. co 
8. 8. 8.8 
8. 8. 8. 8#53 
Non- authoritative answer: 
*** Can' t find cnblogs. co 
m: No answer 
Authoritative answers can be found from. 
cnblogs. com 
ns3. dnsv4. com 
o r 1 gin 
mail addr 
enterprise2dnsadmin. 
se rial 
- 1450611476 
ref resh 
- 3600 
- 180 
ret ry 
— ns4. 
ns3. 
dnsv4. co 
dnsv4. co 
expl re 
ml nlmum 
set t 
ype—ns 
cnblogs. com 
Se rve r: 
Add ress: 
- 1209600 
- 180 
8. 8. 8. 8#53 
Non- authoritative answer: 
cnblogs. com 
cnblogs. com 
namese rver 
namese rver 

不懂什么意思？给你看个图：（阿里云解析）

计算机生成了可选文字:


在不懂就百度谷歌吧