DNS Enumeration

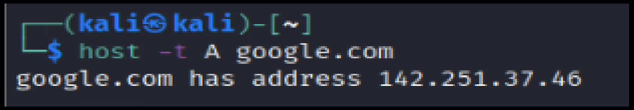
LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad

GitHub : https://github.com/0xDos

DNS Enumeration (1/3)

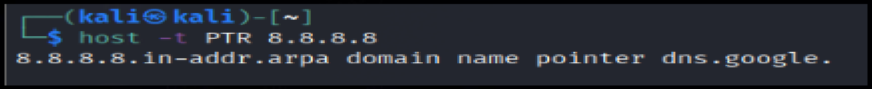
DNS شبيه جدا بأرقام التليفونات في الموبايل (بيتسجل أسماء والموبايل يتصل
بالرقم) أيضا بكتب علي Browser اسم الموقع و DNS يحوله الي IP

- What is DNS ? DNS (domain name system) is a distributed database arranged hierarchically
- Interacting with a DNS Server
  - A : • host -t A <domain name>
    - Maps a hostname to an ip , " forward " lookup / zone .



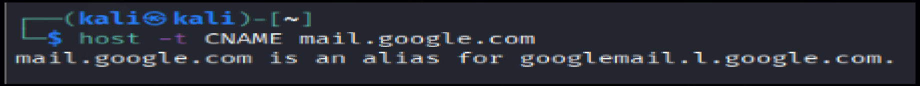
```
┌──(kali㉿kali)-[~]
└─$ host -t A google.com
google.com has address 142.251.37.46
```

  - PTR : • *Host –t PTR < IP >*
    - Maps an IP to a hostname , " reverse " lookup / zone .



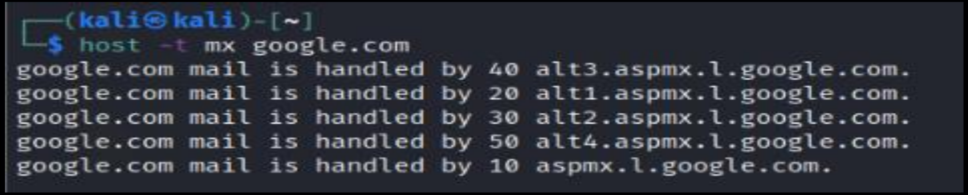
```
┌──(kali㉿kali)-[~]
└─$ host -t PTR 8.8.8.8
8.8.8.8.in-addr.arpa domain name pointer dns.google.
```

  - CNAME :
    - Maps an alias hostname to an A record hostname.



```
┌──(kali㉿kali)-[~]
└─$ host -t CNAME mail.google.com
mail.google.com is an alias for googlemail.l.google.com.
```

  - MX :
    - Contain the names of the servers responsible for handling email for the domain.
    - A domain can contain multiple MX records.



```
┌──(kali㉿kali)-[~]
└─$ host -t mx google.com
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
```

ومعناها : ان دي ال Domains بتتعامل مع رسايل mail server لجوجل

LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad GitHub : https://github.com/0xDos

- *DNS Zone Transfers*
  - Full dump of the zone files.
  - host -l <domain name> <dns server address>

Zone transfers : are usually the result of misconfiguration of the remote DNS server. they should be enabled only for trusted IP addresses .when zone transfers are available , we can enumerate all the DNS records for that zone , this includes the subdomains of our domain

فبدل ما أعمل مره ب A ومره ب MX ,...... هنا هاقوله هاتلي كل Records ال عندك الخاصه بهذا الدومين ودي ممكن admin يسيبها مفتوحه ومش
بتكون موجوده دايما ولو موجوده بتكون خطر كبير جدا لاني بشوف كل ips , network بتاعت Target
Functionality بتاعتها ايه devices , ايه services ال بيستخدمهم بالتحديد

Note : dns server = name server

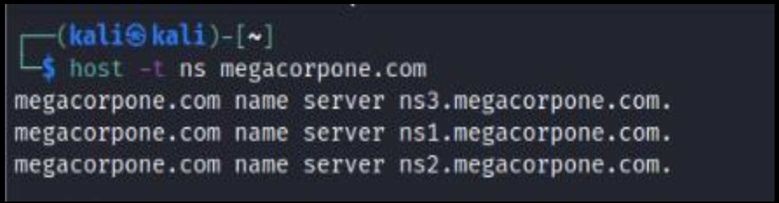
Dump zone files by host , nslookup , dig :

1. Find NS (Name Server) is the DNS server

host -t ns mydomain.com

or

nslookup -type=NS mydomain.com



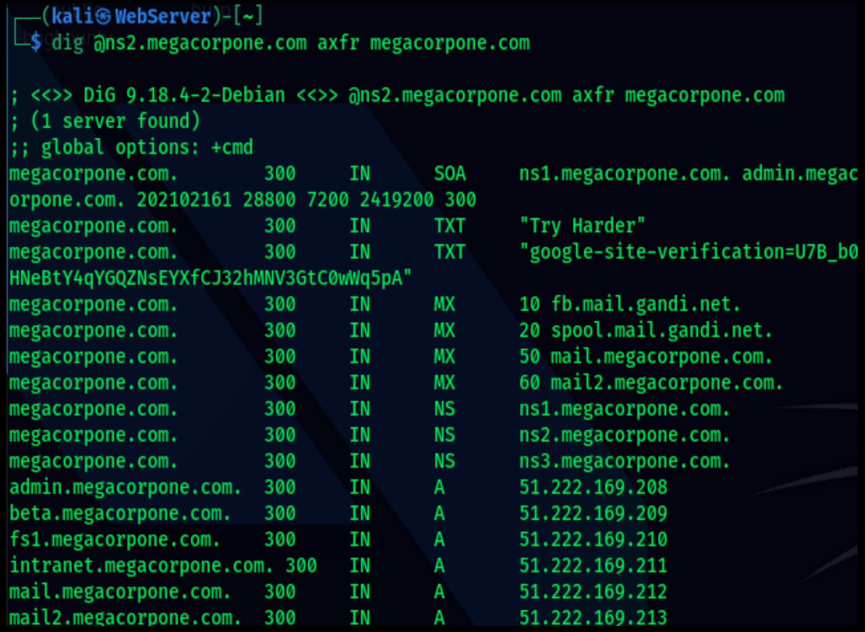
```
┌──(kali㉿kali)-[~]
└─$ host -t ns megacorpone.com
megacorpone.com name server ns3.megacorpone.com.
megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.
```

2. Dump all zone files by trying all name servers that you found

host -l mydomain.com nameserver

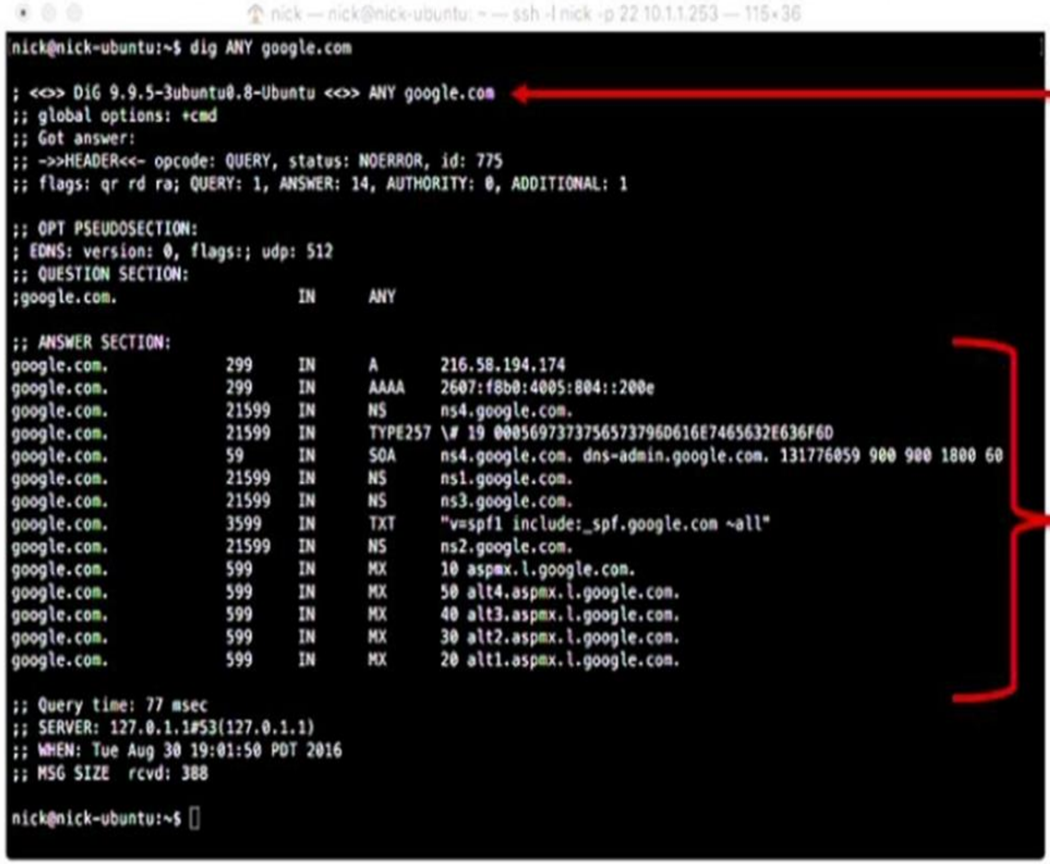
or

dig @ns2.megacorpone.com axfr megacorpone.com



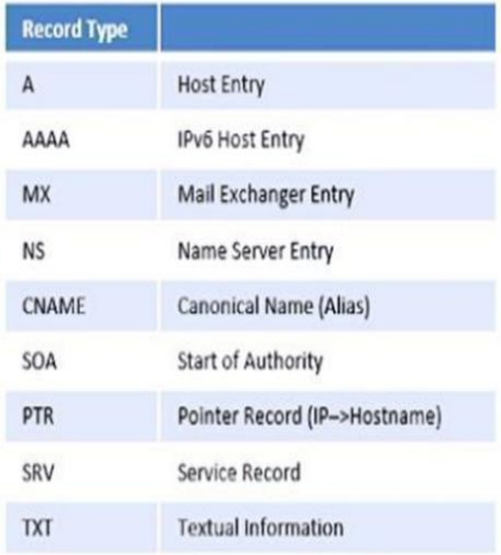
```
┌──(kali㉿WebServer)-[~]
└─$ dig @ns2.megacorpone.com axfr megacorpone.com

; <<>> DiG 9.18.4-2-Debian <<>> @ns2.megacorpone.com axfr megacorpone.com
; (1 server found)
;; global options: +cmd
megacorpone.com.        300     IN      SOA     ns1.megacorpone.com. admin.megac
orpone.com. 202102161 28800 7200 2419200 300
megacorpone.com.        300     IN      TXT     "Try Harder"
megacorpone.com.        300     IN      TXT     "google-site-verification=U7B_b0
HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0wWq5pA"
megacorpone.com.        300     IN      MX      10 fb.mail.gandi.net.
megacorpone.com.        300     IN      MX      20 spool.mail.gandi.net.
megacorpone.com.        300     IN      MX      50 mail.megacorpone.com.
megacorpone.com.        300     IN      MX      60 mail2.megacorpone.com.
megacorpone.com.        300     IN      NS      ns1.megacorpone.com.
megacorpone.com.        300     IN      NS      ns2.megacorpone.com.
megacorpone.com.        300     IN      NS      ns3.megacorpone.com.
admin.megacorpone.com.  300     IN      A       51.222.169.208
beta.megacorpone.com.   300     IN      A       51.222.169.209
fs1.megacorpone.com.    300     IN      A       51.222.169.210
intranet.megacorpone.com. 300   IN      A       51.222.169.211
mail.megacorpone.com.   300     IN      A       51.222.169.212
mail2.megacorpone.com.  300     IN      A       51.222.169.213
```

Dig (Domain Information Groper) and nslookup are the most widely used tools for gathering DNS information.


nick — nick@nick-ubuntu: ~ — ssh -l nick -p 22 10.1.1.253 — 115×36

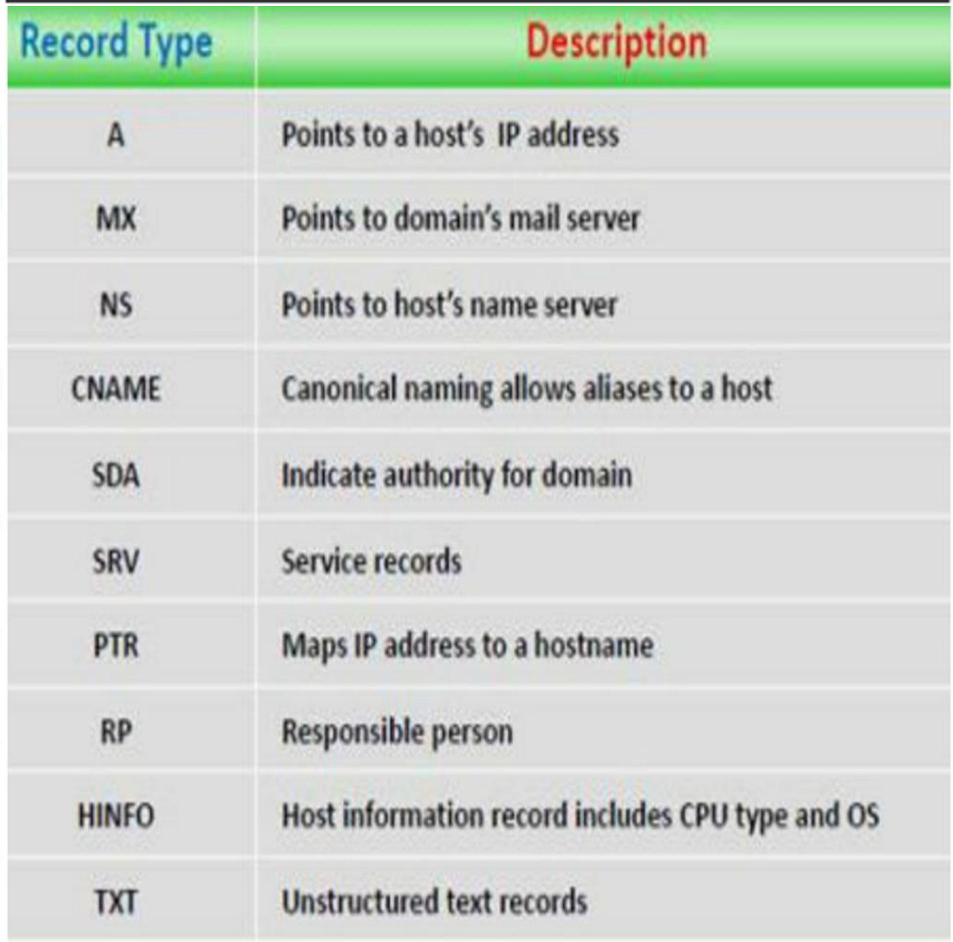
```
nick@nick-ubuntu:~$ dig ANY google.com

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> ANY google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 775
;; flags: qr rd ra; QUERY: 1, ANSWER: 14, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                    IN      ANY

;; ANSWER SECTION:
google.com.             299     IN      A       216.58.194.174
google.com.             299     IN      AAAA    2607:f8b0:4005:804::200e
google.com.             21599   IN      NS      ns4.google.com.
google.com.             21599   IN      TYPE257 \# 19 0005697373756573796D616E7465632E636F6D
google.com.             59      IN      SOA     ns4.google.com. dns-admin.google.com. 131776059 900 900 1800 60
google.com.             21599   IN      NS      ns1.google.com.
google.com.             21599   IN      NS      ns3.google.com.
google.com.             3599    IN      TXT     "v=spf1 include:_spf.google.com ~all"
google.com.             21599   IN      NS      ns2.google.com.
google.com.             599     IN      MX      10 aspmx.l.google.com.
google.com.             599     IN      MX      50 alt4.aspmx.l.google.com.
google.com.             599     IN      MX      40 alt3.aspmx.l.google.com.
google.com.             599     IN      MX      30 alt2.aspmx.l.google.com.
google.com.             599     IN      MX      20 alt1.aspmx.l.google.com.

;; Query time: 77 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Aug 30 19:01:50 PDT 2016
;; MSG SIZE  rcvd: 388

nick@nick-ubuntu:~$ 
```

The ANY keyword tells dig that you want all records it can find.



Record Type	
A	Host Entry
AAAA	IPv6 Host Entry
MX	Mail Exchanger Entry
NS	Name Server Entry
CNAME	Canonical Name (Alias)
SOA	Start of Authority
PTR	Pointer Record (IP->Hostname)
SRV	Service Record
TXT	Textual Information

Extracting DNS Information

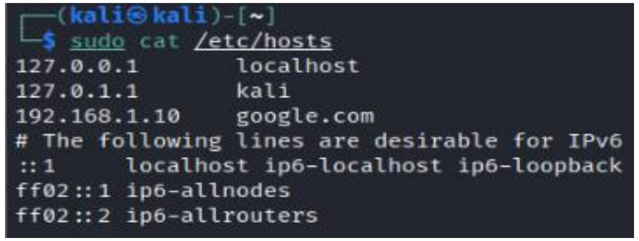


Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SDA	Indicate authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

سلسلة Records بتتم ازاي ؟

بكتب علي المتصفح google.com فالمتصفح بيبعت host name الي Client DNS علي السيستم لو لقي الإجابة عنده بيروح يزور Ip لو مش لاقاه فال OS بيعمل forward ويبعت request ال بيحاول يستعلم فيه عن Ip الخاص ب google.com ل External DNS ولما recurser يرجع بال ip يبدأ المتصفح يتصل ب ip وي loadالصفحة ال طلبها

Client DNS = local host
موجود علي /etc/hosts



```
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
192.168.1.10    google.com
# The following lines are desirable for IPv6
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```