DNS Enumeration

@mmar

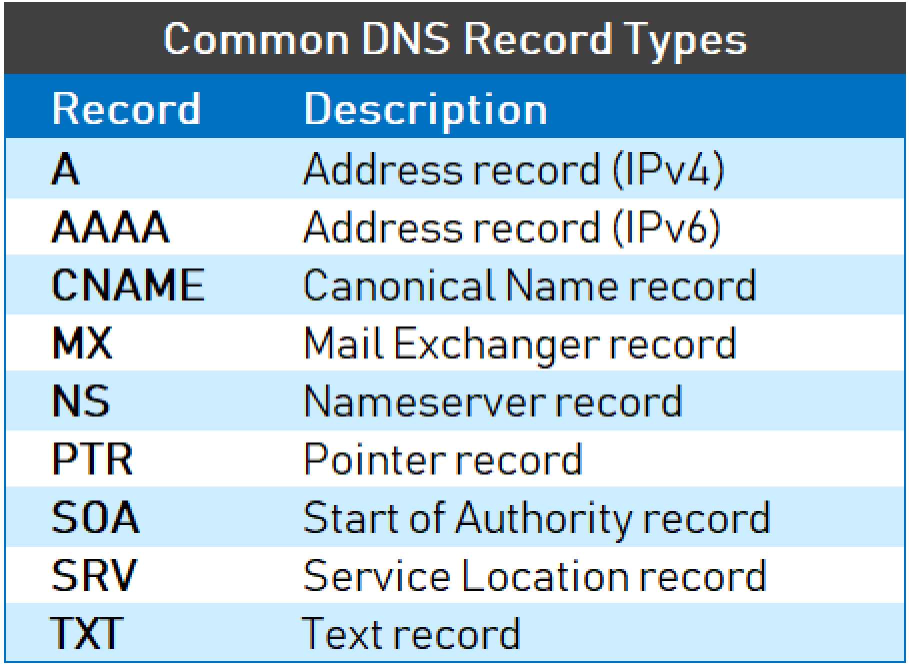
DNS Enumeration

DNS enumeration, also known as DNS recon, is the process of gathering information about a domain name system (DNS) infrastructure and its associated records. DNS is responsible for translating human-readable domain names (e.g., www.example.com) into machine-readable IP addresses (e.g., 192.168.1.1). DNS enumeration involves querying DNS servers to obtain various types of DNS records, which can reveal valuable information about the target domain including hidden or internal subdomains

DNS Enumeration

The primary purpose of DNS enumeration is to gather intelligence about a target's DNS infrastructure. It can be used by security professionals, penetration testers, or malicious actors to identify potential vulnerabilities, misconfigurations, or targets for further attacks. By gathering information about the target's DNS infrastructure, an attacker can potentially identify subdomains, mail servers, or other potential entry points for further attacks.

Record Types



Common DNS Record Types

Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record

Axfr	Zone transfer. Includes all records about a domain

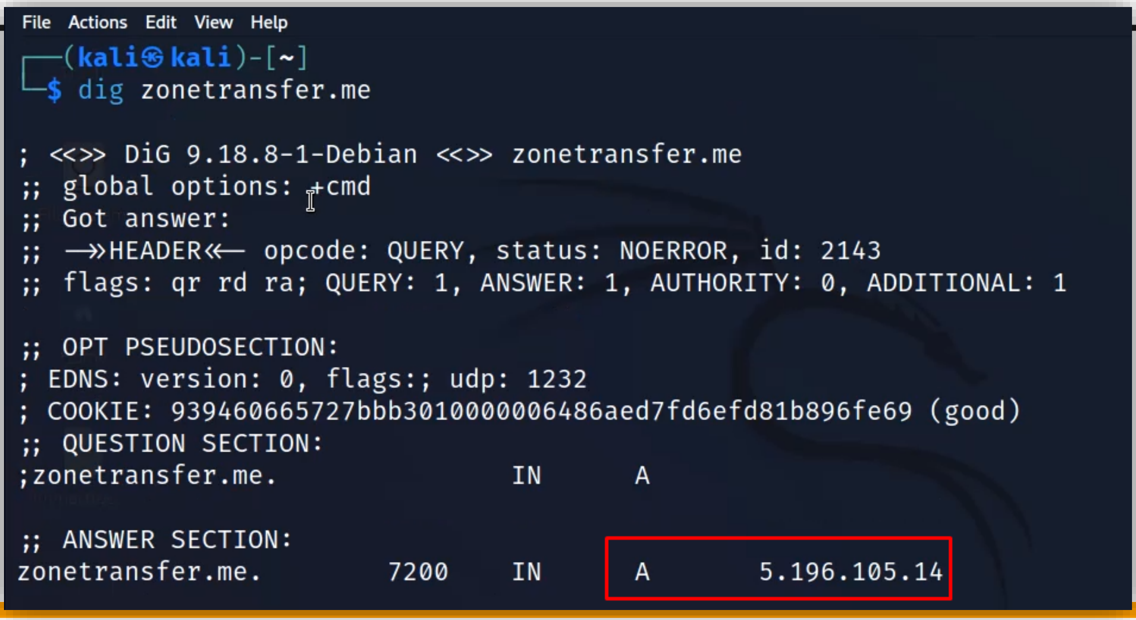
Dig

Most common DNS Enumeration tool
DNS Enumeration swiss army knife

Dig

- Dig can be used for simple domain lookup

>dig zonetransfer.me

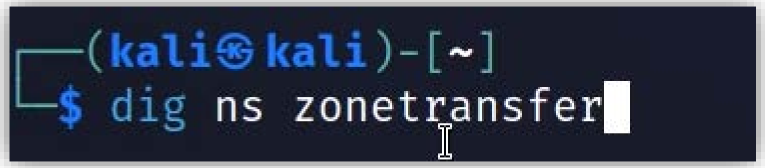


```
┌──(kali㉿kali)-[~]
└─$ dig zonetransfer.me

; <<>> DiG 9.18.8-1-Debian <<>> zonetransfer.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2143
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 939460665727bbb3010000006486aed7fd6efd81b896fe69 (good)
;; QUESTION SECTION:
;zonetransfer.me.               IN      A

;; ANSWER SECTION:
zonetransfer.me.        7200    IN      A       5.196.105.14
```

Dig

- We can also specify the type of record with dig command

>dig ns zonetransfer.me	(Name server)
>dig mx zonetransfer.me	(Mail server)
>dig cname zonetransfer.me	(cname record)



```
┌──(kali㉿kali)-[~]
└─$ dig ns zonetransfer
```

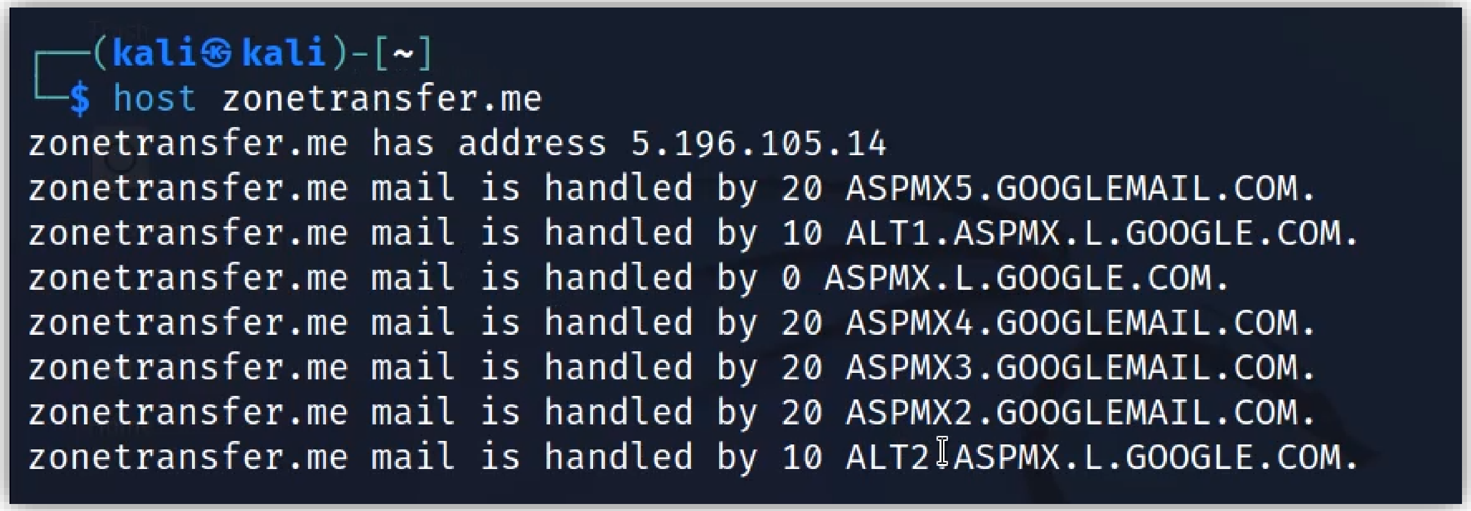
Host

Simplest DNS Enumeration tool

Host

- Host provides a simple way to perform DNS lookups and retrieve DNS records.

```
>host zonetransfer.me
```

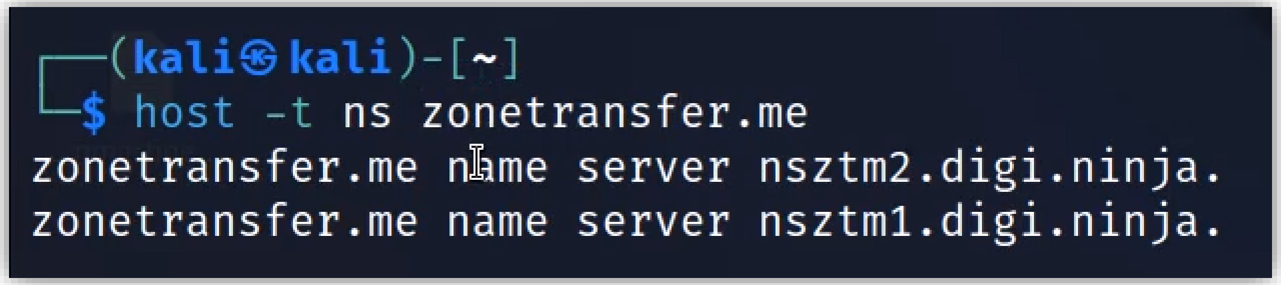


```
┌──(kali㉿kali)-[~]
└─$ host zonetransfer.me
zonetransfer.me has address 5.196.105.14
zonetransfer.me mail is handled by 20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 0 ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 10 ALT2.ASPMX.L.GOOGLE.COM.
```

Host

- We can use host tool to look up a specific record

```
>host -t ns zonetransfer.me          (Name server)
>host -t mx zonetransfer.me          (Mail server)
```

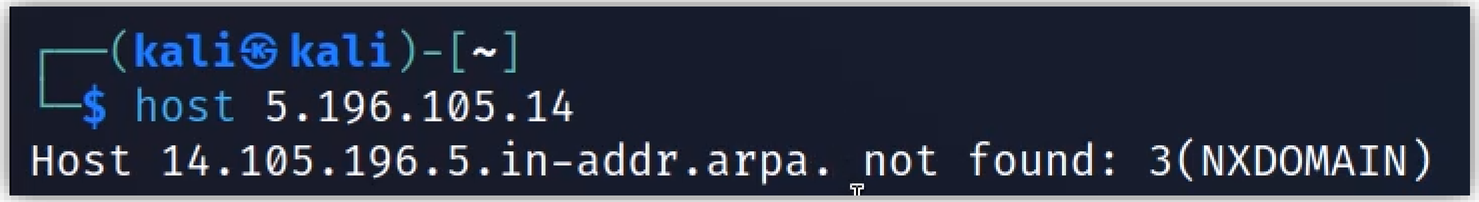


```
┌──(kali㉿kali)-[~]
└─$ host -t ns zonetransfer.me
zonetransfer.me name server nsztm2.digi.ninja.
zonetransfer.me name server nsztm1.digi.ninja.
```

Host

- Host can be used to map IP address to the website with reverse lookup

```
>host 192.168.2.2
```



```
┌──(kali㉿kali)-[~]
└─$ host 5.196.105.14
Host 14.105.196.5.in-addr.arpa. not found: 3(NXDOMAIN)
```

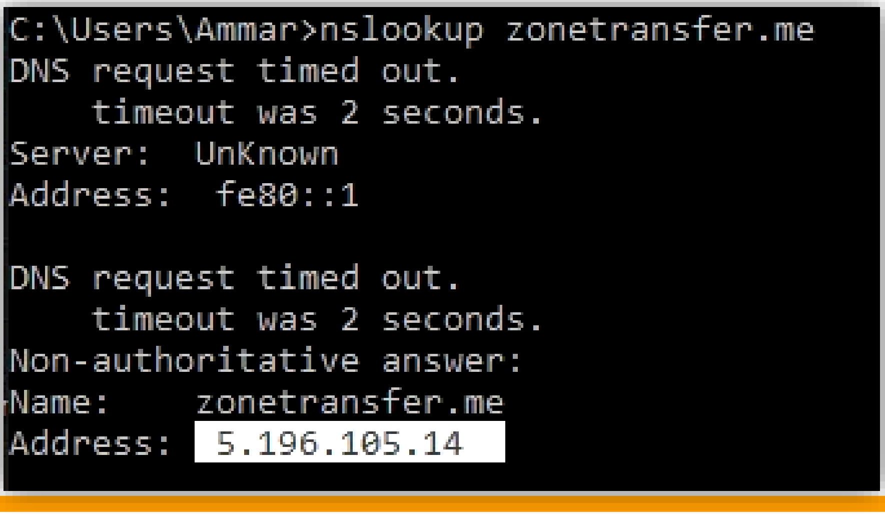
nslookup

(A cross platform tool for DNS Enumeration)

nslookup

- We can use nslookup on windows to enumerate dns records

```
>nslookup zonetransfer.me
```

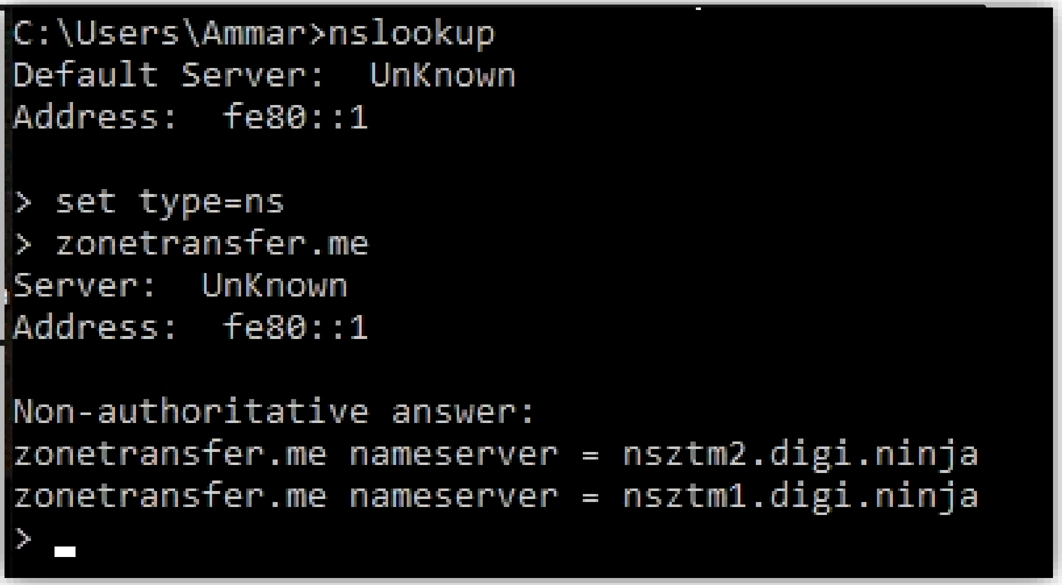


```
C:\Users\Ammar>nslookup zonetransfer.me
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  fe80::1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    zonetransfer.me
Address:  5.196.105.14
```

nslookup

- We can specify a specific record type and use the tool in an interactive manner

```
>nslookup
>Set type=ns
>zonetransfer.me
```



```
C:\Users\Ammar>nslookup
Default Server:  UnKnown
Address:  fe80::1

> set type=ns
> zonetransfer.me
Server:  UnKnown
Address:  fe80::1

Non-authoritative answer:
zonetransfer.me nameserver = nsztm2.digi.ninja
zonetransfer.me nameserver = nsztm1.digi.ninja
> 
```

Zone Transfer

Zone Transfer

Zone transfer is a mechanism in DNS for sharing and synchronizing DNS database information between servers. Pentesters and hackers can leverage zone transfer to gather intelligence about a target's DNS infrastructure. Zone transfers provide a comprehensive list of DNS records, including subdomains, IP addresses, and mail servers

CONCEPT

1

Identify the name server

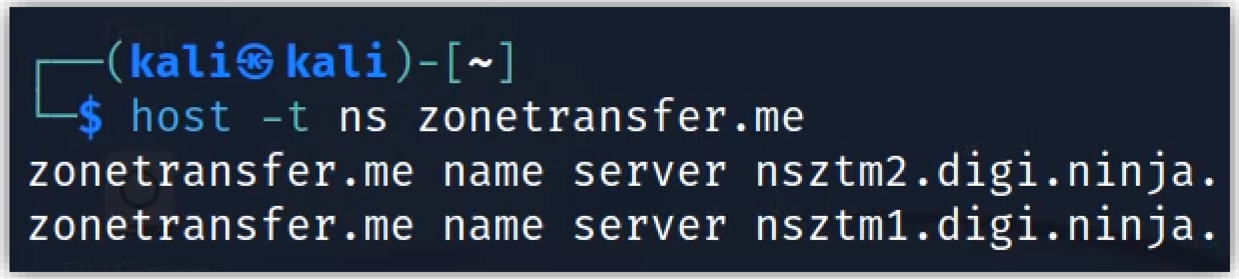
2

Initiate Zone transfer

Zone transfer

- Host tool can be used to initiate zone transfer. First look for the name server and then check if it supports zone transfer. Try all listed name servers for best results

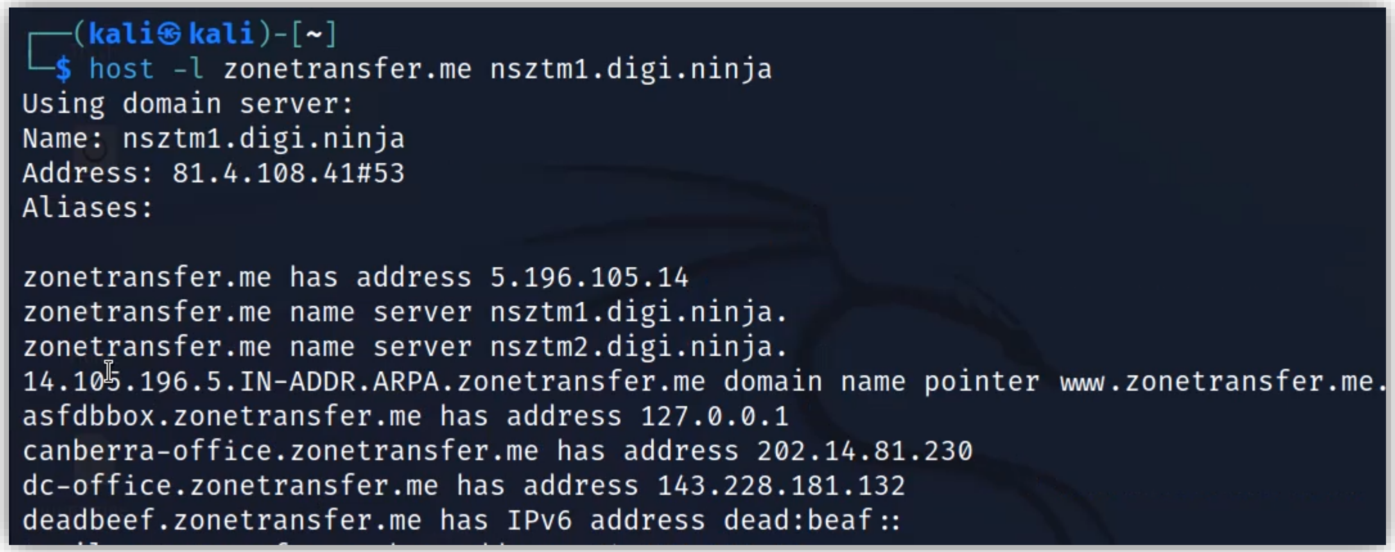
```
>host -t ns zonetransfer.me
```



```
┌──(kali㉿kali)-[~]
└─$ host -t ns zonetransfer.me
zonetransfer.me name server nsztm2.digi.ninja.
zonetransfer.me name server nsztm1.digi.ninja.
```

Zone transfer

>host –l zonetransfer.me nsztm2.digi.ninja

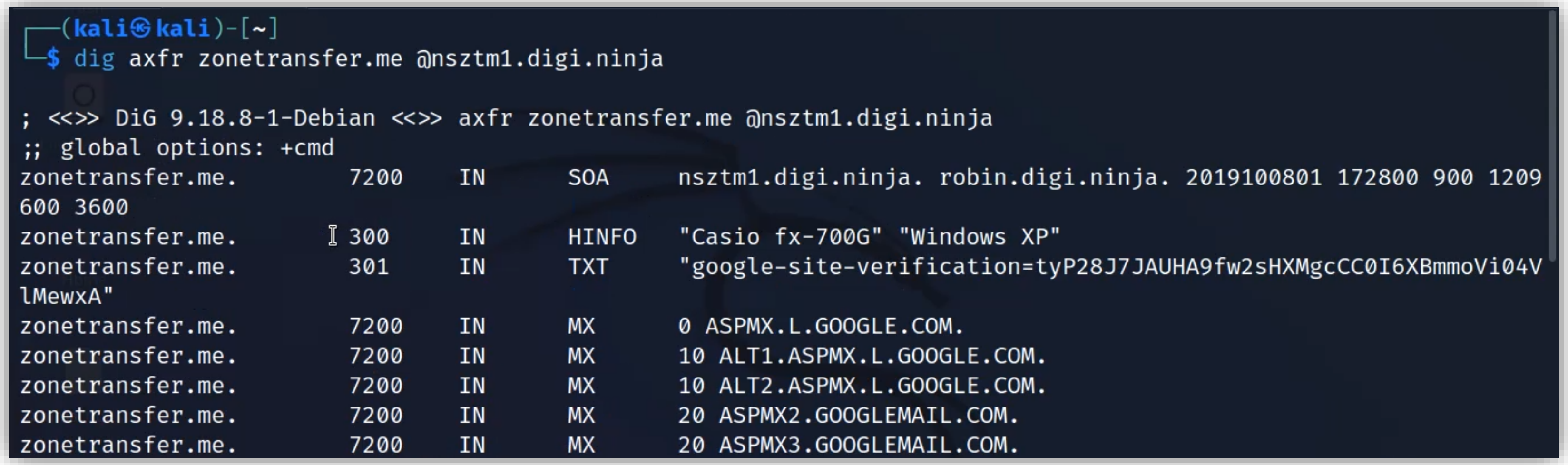


```
┌──(kali㉿kali)-[~]
└─$ host -l zonetransfer.me nsztm1.digi.ninja
Using domain server:
Name: nsztm1.digi.ninja
Address: 81.4.108.41#53
Aliases:

zonetransfer.me has address 5.196.105.14
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransfer.me.
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra-office.zonetransfer.me has address 202.14.81.230
dc-office.zonetransfer.me has address 143.228.181.132
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
```

Zone transfer

- Dig can also be used to initiate zone transfer

```
>dig ns zonetransfer.me

>dig axfr zonetransfer.me @nsztm2.digi.ninja
```

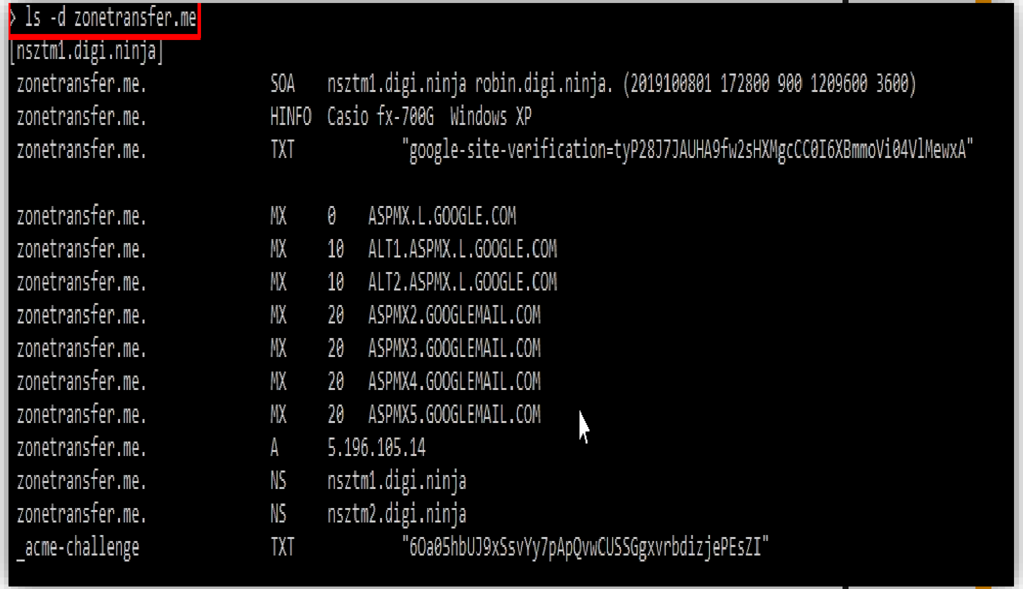


```
┌──(kali㉿kali)-[~]
└─$ dig axfr zonetransfer.me @nsztm1.digi.ninja

; <<>> DiG 9.18.8-1-Debian <<>> axfr zonetransfer.me @nsztm1.digi.ninja
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209
600 3600
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04V
lMewxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
```

Zone transfer

- Similarly, nslookup can also be used to perform zone transfer

```
>nslookup
>set type=ns
>zonetranfer.me
>server nsztm2.digi.ninja
>set type=any
>ls –d zonetransfer.me
```



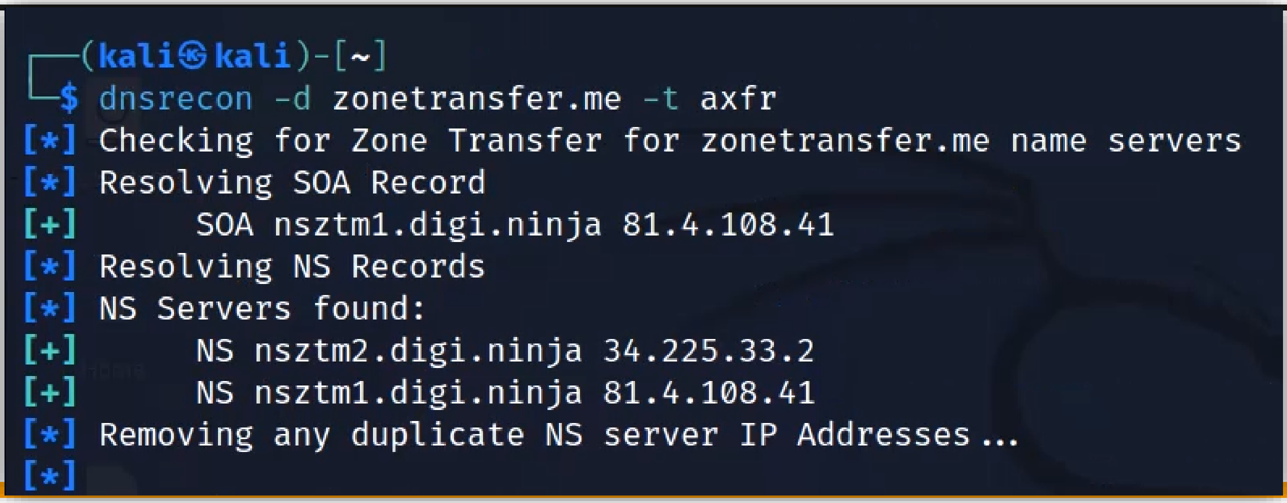
```
> ls -d zonetransfer.me
[nsztm1.digi.ninja]
 zonetransfer.me.              SOA    nsztm1.digi.ninja robin.digi.ninja. (2019100801 172800 900 1209600 3600)
 zonetransfer.me.              HINFO  Casio fx-700G  Windows XP
 zonetransfer.me.              TXT            "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"

 zonetransfer.me.              MX     0    ASPMX.L.GOOGLE.COM
 zonetransfer.me.              MX     10   ALT1.ASPMX.L.GOOGLE.COM
 zonetransfer.me.              MX     10   ALT2.ASPMX.L.GOOGLE.COM
 zonetransfer.me.              MX     20   ASPMX2.GOOGLEMAIL.COM
 zonetransfer.me.              MX     20   ASPMX3.GOOGLEMAIL.COM
 zonetransfer.me.              MX     20   ASPMX4.GOOGLEMAIL.COM
 zonetransfer.me.              MX     20   ASPMX5.GOOGLEMAIL.COM
 zonetransfer.me.              A      5.196.105.14
 zonetransfer.me.              NS     nsztm1.digi.ninja
 zonetransfer.me.              NS     nsztm2.digi.ninja
 _acme-challenge               TXT            "6Oa05hbUJ9xSsvYy7pApQvwCUSSGgxvrbdizjePEsZI"
```

Automated tools

DNS Recon

- DNSRECON is designed to automate and streamline the process of querying DNS servers, retrieving DNS records, and conducting various types of DNS-related scans

>dnsrecon –d zonetransfer.me –t axfr

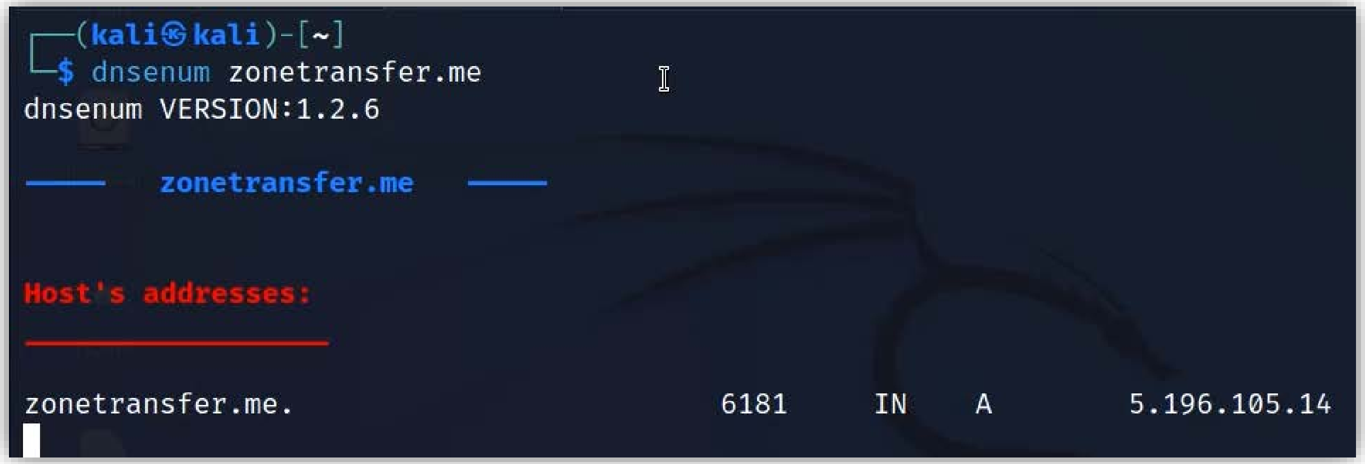


```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d zonetransfer.me -t axfr
[*] Checking for Zone Transfer for zonetransfer.me name servers
[*] Resolving SOA Record
[+]      SOA nsztm1.digi.ninja 81.4.108.41
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS nsztm2.digi.ninja 34.225.33.2
[+]      NS nsztm1.digi.ninja 81.4.108.41
[*] Removing any duplicate NS server IP Addresses...
[*]
```

DNS Enum

- DNSenum is another automated tool that collects all possible information about the target

```
>dnsenum zonetransfer.me
```

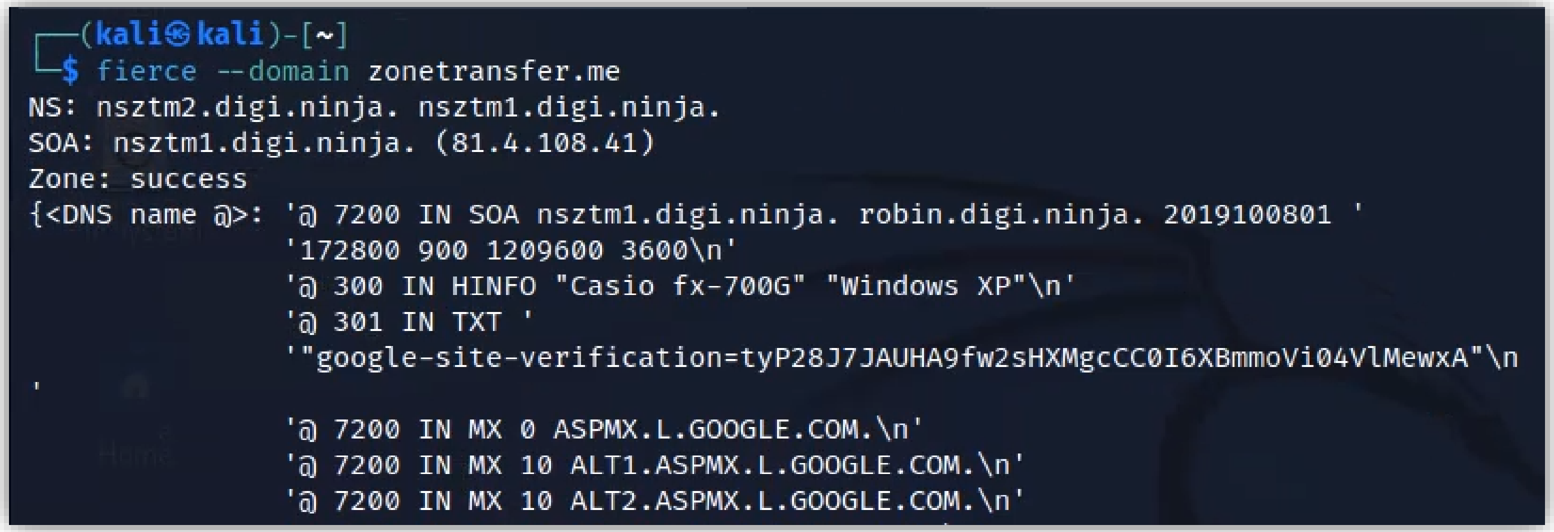


```
┌──(kali㉿kali)-[~]
└─$ dnsenum zonetransfer.me
dnsenum VERSION:1.2.6

─────   zonetransfer.me   ─────


Host's addresses:
__________________

zonetransfer.me.                         6181     IN    A        5.196.105.14
```

Fierce

- Fierce is another tool for DNS enumeration

```
>fierce --domain zonetransfer.me
```



```
┌──(kali㉿kali)-[~]
└─$ fierce --domain zonetransfer.me
NS: nsztm2.digi.ninja. nsztm1.digi.ninja.
SOA: nsztm1.digi.ninja. (81.4.108.41)
Zone: success
{<DNS name @>: '@ 7200 IN SOA nsztm1.digi.ninja. robin.digi.ninja. 2019100801 '
               '172800 900 1209600 3600\n'
               '@ 300 IN HINFO "Casio fx-700G" "Windows XP"\n'
               '@ 301 IN TXT '
               '"google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"\n
'

               '@ 7200 IN MX 0 ASPMX.L.GOOGLE.COM.\n'
               '@ 7200 IN MX 10 ALT1.ASPMX.L.GOOGLE.COM.\n'
               '@ 7200 IN MX 10 ALT2.ASPMX.L.GOOGLE.COM.\n'
```

THANKS