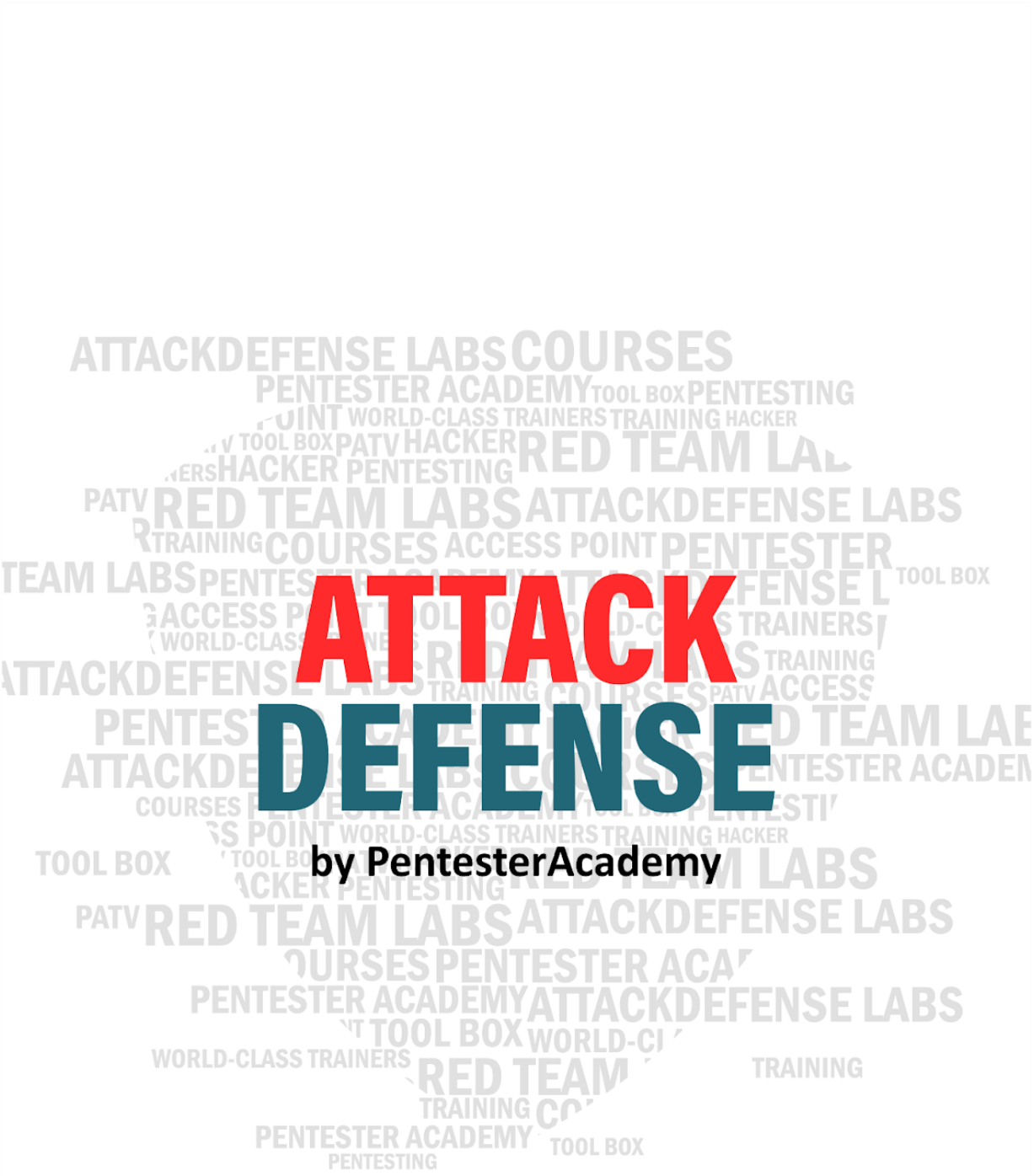
ATTACK
DEFENSE
by PentesterAcademy

Name	DNS Basics
URL	https://attackdefense.com/challengedetails?cid=2017
Type	Network Pentesting: DNS

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Check the IP address of the machine.

Command: ip a

```
root@attackdefense:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
37407: eth0@if37408: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:12:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.6/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
37409: eth1@if37410: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:d3:4f:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.211.79.2/24 brd 192.211.79.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The target DNS servers are located at the IP addresses "192.211.79.3" and "192.211.79.4" respectively.

Step 2: Using nmap to scan the target DNS servers.

Command: nmap 192.211.79.3-4

```
root@attackdefense:~# nmap 192.211.79.3-4
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-02 16:56 IST
Nmap scan report for promo.witrap.com (192.211.79.3)
Host is up (0.000016s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 02:42:C0:D3:4F:03 (Unknown)

Nmap scan report for ns1.witrap.com (192.211.79.4)
Host is up (0.000016s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 02:42:C0:D3:4F:04 (Unknown)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.32 seconds
root@attackdefense:~#
```

Port 53 is open on the target machine. By default, a DNS server listens for requests on port 53.

Step 3: Checking the default nameserver for the host machine.

Command: cat /etc/resolv.conf

```
root@attackdefense:~# cat /etc/resolv.conf
nameserver 192.211.79.3
root@attackdefense:~#
```

This is the default nameserver used to resolve a domain name.

Step 4: Using nslookup utility to perform lookup of different DNS records from the target DNS server.

Since the domain name corresponding to the target machine is not known, performing a reverse DNS lookup:

Command: nslookup 192.211.79.3

```
root@attackdefense:~# nslookup 192.211.79.3
3.79.211.192.in-addr.arpa       name = ns2.witrapper.com.
3.79.211.192.in-addr.arpa       name = witrapper.com.
3.79.211.192.in-addr.arpa       name = public.witrap.com.
3.79.211.192.in-addr.arpa       name = witrap.com.
3.79.211.192.in-addr.arpa       name = ns1.witrapper.com.
3.79.211.192.in-addr.arpa       name = promo.witrap.com.
3.79.211.192.in-addr.arpa       name = ns3.witrapper.com.

root@attackdefense:~#
```

The IP maps to various domain names:

- ns2.witrapper.com.
- witrapper.com.
- public.witrap.com.
- witrap.com.
- ns1.witrapper.com.
- promo.witrap.com.
- ns3.witrapper.com.

Using the above response, obtaining the different domains and using them to get different records:

1. Retrieving A record for witrapper.com

Command: nslookup -type=A witrapper.com

```
root@attackdefense:~# nslookup -type=A witrapper.com
Server:         192.211.79.3
Address:        192.211.79.3#53

Name:   witrapper.com
Address: 192.211.79.3

root@attackdefense:~#
```

2. Retrieving TXT records witrap.com:

Command: nslookup -type=TXT witrap.com

```
root@attackdefense:~# nslookup -type=TXT witrap.com
Server:         192.211.79.3
Address:        192.211.79.3#53

witrap.com      text = "Welcome to Witrap.com!"

root@attackdefense:~#
```

3. Retrieving all the available DNS records for witrapper.com

Command: nslookup -type=any witrapper.com

```
root@attackdefense:~# nslookup -type=any witrapper.com
Server:         192.211.79.3
Address:        192.211.79.3#53

witrapper.com
        origin = ns1.witrapper.com
        mail addr = admin.witrapper.com
        serial = 2
        refresh = 900
        retry = 900
        expire = 604800
        minimum = 900
witrapper.com   rdata_46 = SOA 7 2 900 20201106122259 20201007122259 18347 witrapper.com.
FurrDiWc4Y /xo2AidRBmge994kKBw3nsYHgpx7XlfezTSbjVePTG4Knf5SwQAk/44i lo4ak54FP9uvptyHrwudY
OzO7qtqqYdl0Wl7+UoWMEuS9MVknpXO7/cLxIOWxbXX5i YJ6NSv2hTzSAVDF8ibquWOAcMNfUcYHrj2Efstv0E0T
CHZrYDnwneN1VEGrSztaR2F 6cdW/Q==
witrapper.com   nameserver = ns1.witrapper.com.
witrapper.com   nameserver = ns3.witrapper.com.
witrapper.com   nameserver = ns2.witrapper.com.
witrapper.com   rdata_46 = NS 7 2 900 20201106122259 20201007122259 18347 witrapper.com.
DrJa6pKCA HclE4GdFUgVJHJRFREub2aWW+1gQssgRp7Ltk3rkFwlYjisX0fKHq36/ WHM6uzgKtA0BL+cP+CRy4h
YNmPI3gX71vXocV/+EbauGoXs9yp9exqkBDtwJZHKe2y F554rBSogR0R8fEyIHu16k3GtGVllovEvouKL3kbJ9lT
uVXfDhBImYw45eD1qrfNPR HzyWEg==
Name:   witrapper.com
Address: 192.211.79.3
witrapper.com   rdata_46 = A 7 2 900 20201106122259 20201007122259 18347 witrapper.com. B
qH3WyxJH vrnIwosKystOvsNjgF6Wof7eCTuUBdsprPRwf2GpRvLMousOVWE7AT5C 4q66+2JQV7e4V13caSPRYu7
Sv/9lm4xq5nnTxMpVx0KUJDDmHNjzViiW3gLQ5nspUj nFNdwG9N4qaNMR/0IpCA77SoOi3mHgIq91qf71hKtdfQF
V2f52Ey22YBWh3zLdaNOw vxXTig==
```

```
witrapper.com   mail exchanger = 50 mx5.ap.witrapper.com.
witrapper.com   mail exchanger = 70 mx7.uk.witrapper.com.
witrapper.com   mail exchanger = 40 mx4.ua.witrapper.com.
witrapper.com   mail exchanger = 10 mx1.us.witrapper.com.
witrapper.com   mail exchanger = 20 mx2.sg.witrapper.com.
witrapper.com   mail exchanger = 30 mx3.sg.witrapper.com.
witrapper.com   mail exchanger = 60 mx6.ru.witrapper.com.
witrapper.com   rdata_46 = MX 7 2 900 20201106122259 20201007122259 18347 witrapper.com.
ScWDsIWhr H++cPy5nkYsqshuzLVfVQE+avZSMzlncFDcMUCPQ+F6zA9LVR+cO6hSl 8Q2810Y7EkEot4dJ6F4Tj8
RdRWtF5jtUpY46vsvjAFrMTWZCk+y1KlZqj4QC9H+2yT m4xSM9AoGYd5UoXu47HUwJItj3LnBuWJjC5iIW1GYtzO
WAv4hmg2oBLgztwIeGwLHA BKj2mw==
witrapper.com   text = "Welcome to Witrapper.com - the parent company of witrap :)"
witrapper.com   rdata_46 = TXT 7 2 900 20201106122259 20201007122259 18347 witrapper.com.
C8Wt86EDZt kd0L6uamfecZq6GR2qDF/X5gcq3J4ZGNXTvY2RDw2YywEUSMuePXHxGe GI77K5uHLhztoaLLTEghG
ziOJvmtWRKL5t02VB1hcW27ulpMdKUFfzNqldWrjtuuZW 9CB7VsbNHUZ43qzbFB5iHh0W783tu/K6+3kOqJIQ8cm
F6tcXXYpAn+gwp5lbIrg3Cb trB0eg==
Name:   witrapper.com
Address: 2001:db8::11:0:0:17
Name:   witrapper.com
Address: 2001:db8::11:0:0:15
Name:   witrapper.com
Address: 2001:db8::11:0:0:16
Name:   witrapper.com
Address: 2001:db8::11:0:0:19
Name:   witrapper.com
Address: 2001:db8::11:0:0:20
Name:   witrapper.com
Address: 2001:db8::11:0:0:18
Name:   witrapper.com
```

```
witrapper.com   rdata_46 = DNSKEY 7 2 900 20201106122259 20201007122259 40065 witrapper.com.
0LoUwj/oaNRfU TaG5qNN5ZKOlmFy0fYTDAOKwIvf/RzKGbt44ZecVcxAhjhnHCZgMus68 Tyb3+4zINwZjnBi9OF2Ex
ZiVA/acNCZVVV2ozm6NPaNufUn9KEVHIrTlC5/uhrVPWekDz qD9brQ2gdrrK/BuIZ6tncqjW+8iRQVqZ+uzFA/ZEqgw
FqawQDh3W/SgAvUEkbu4eaaygQ kv5rz+FhacDbObKUrH2EzNelwzNh8o4yeEHABz4BU+nfNTCzWU+ynki/ /P2ZAqX0
QWnd BqNfE17uOCuLO7UOc2HyP5NEuDeT3U93E8g6tiPsrDJ8u2XXaT3okSdI xU9YgY6iRT843b6ox5swGo0KptuiRQ
rwoyE8R9aBYfx7PSBRZdfibI5E55oXoU7Zj6BX6 jMWlzlijLvHkdFc3COvs278YBFzc9Uz47v3O7Vff+AmObGuolDy0
witrapper.com   rdata_51 = 1 0 10 A3461BA5E7D5BADC
witrapper.com   rdata_46 = NSEC3PARAM 7 2 0 20201106122259 20201007122259 18347 witrapper.co
lBOIgjLSAd71coF st0Li0lNCghnKMU3GgUCNXhrZd7euV9MPyU7jaZxf3s/+iptSCyS6PCc REQuBlOegeDxNfqvqVF
7ZMzxE8ajKk/SCEqIa9GprCv+vw0WAcwoRcNb75AMZNHKjKvdr L8kHhfNCD+p9nJF/rTrPq2eFgbI/64zARkze3NYsu
VgQbRH2DHofRU9fOZocQUIqAyNLO 777Dlg==
witrapper.com   rdata_257 = 0 issue "ca.witrapper.com"
witrapper.com   rdata_46 = CAA 7 2 900 20201106122259 20201007122259 18347 witrapper.com. hZ
kjVCqFMKw6 c66/5njMEaRNocVoZ6L3TCJYV5YwEFvOTUx2IbKQ8L1n2EE5C5D1TJaR CAz2TVALvrekyN6BT+b/wGjc
rqEYCsyJqF9tXXCxA8eEKUVaBxicvH0Hyl2nz1g4Yz0th ZRT/m+vLrdO12wyJUJf+l+Oqz23+vJEW2F9AsyTaYOuAiW
E8NwWIxh3/S3z7yixKZJLkN KkqdcA==

root@attackdefense:~#
```

Notice that the records for witrapper.com are signed.

5. Retrieving DNSKEY records for witrapper.com:

Command: nslookup -type=DNSKEY witrapper.com.

```
root@attackdefense:~# nslookup -type=DNSKEY witrapper.com.
;; Truncated, retrying in TCP mode.
Server:         192.211.79.3
Address:        192.211.79.3#53

witrapper.com   rdata_48 = 256 3 7 AwEAAdVtu1J1W0DKlVj8ZXHa9bX80q7q8Ac8Tkfm37gv3OhI5VGUGtHB /HHc+e9xZNc
hk9GR0cXs3nJbggbJd0Jce29q7SIRxroA02bf4ubFZGql IBh/ADJ/Hp9kYWb4rvH9QJnyZJR+2Ogl5stB/SfvbVpIxHXnkQib/gAu
LtSII0fdI54Du19M1/kDCRVhbaOxyLU7iewAcSiiC/xLhnVXkYx7eQ3F JdloLAK1BKsj28oB7auronZ0Lnp1PSDRxcd2/eOJOCdfLo
r0UWEk/sT0 Q2hCYr4dLAuztHTQ2oVbTKA0vuhvboBd/JGKVigCD1mM7tst69Kk5/lA 3DfYGnsi+f8=
witrapper.com   rdata_48 = 257 3 7 AwEAAaSTrABLpWRwsF/p/yzC684ckLnIXp9nnOyf1d3znW3SgCvs7VBB udYLACW93fd
AjLR67Dcon930yAOmljbAqRUKfMX12hkIVT1oRR+NSnxk P26Ck7oGPmd2Jh8fcRqyFCTVB5poneaCb52pZegw98/yUrpeamCFP7BM
arWKNTZStrmELd7MdyuMT4B+QBZNSoz5RllbUC/bZeJjGkhiFJNwh1EP 5Kh9elKSVwp4JuJ7ipDiVg+BCfd/ZYj6+peZ8j42t+huSO
EqEvWsAO8H j7ek7izindVDiix25yzawVjmpN57QNzb0UaQcwwADhwg8+Ow9OFbdr07 W3VVIjKb41Qbeurp2b43Td6ONYrgW9nfFOm
4PGt0G4PCjsXL9zdLpUMZ nkmj4Fs2fJGUV2k8B26YfiVvg58DFOiJFu9P6jJSbYBPgix/CLabFii+ NmOvwT63efPCs6MZYYY1bzrK
NKaoCG7p5oKTOVLxsvmrprYKvhLvvi4G Pfl2VuaZl2rUBDmXvydKImHnVs94R38L90QbKx1UFqEnzoTEL3ks9dud r6cdVY6jHNcyn
bnhiB2T6jeHgYjmAj6YaiAKhBWldWj4feGSkTONHD1S GOdt5NQ4E6hR5P9BBtkslfZHGsZC+uvO2aDb8PH9bu9rsjFTXwqZQqsi Us
dTCzGoT57kcCCj

root@attackdefense:~#
```

The process of DNSSEC record signing works like this:

- Using a private key, the name server generates a “signature” for each “set” of records, such as all the “A” records, all the “AAAA” records or all the “TXT” records.
- That signature is stored in a “RRSIG” record for each set of records. Your domain zone file will therefore have multiple RRSIG records, one for each of the different types of DNS records stored in the file.
- The public key is then stored in a “DNSKEY” record

Reference:
https://www.internetsociety.org/resources/deploy360/2014/the-two-sides-of-dnssec-signing-and-validation/

6. Retrieving RRSIG record for witrap.com:

Command: nslookup -type=RRSIG witrapper.com.

```
root@attackdefense:~# nslookup -type=RRSIG witrapper.com.
;; Truncated, retrying in TCP mode.
Server:         192.211.79.3
Address:        192.211.79.3#53

witrapper.com   rdata_46 = SOA 7 2 900 20200906033312 20200807033312 64685 witrapper.com. XMsqYS
G1mZKwsU22fQhq9ELyG7Zd0TfVQH06vpm3+bRxSBDAIOEpTJjg HrX9QxStkYhDzlwEZZzvys9wtVDUUN9Tob6PgIfk4yOge
J7LOeqdYoSy U698pmeutxTidD5vlKbmMy530K7jcOVKBm2CbcAR71ss7GJgMVgsZg1C NgqJs6v1d5mHvcLPf0FLdgMulW2
IalEqEE6KLpyUlX4RsTqCl8uOnJv0 S0qWj9XhxkA7bfofZ5qGPXWDF/28wP+FFcjI8h5PH0wHAoCx8ay/jZkW k9r5N6JSh
yT5Ez3LK1YNpJHg/xzh5/YSyLj8UnGHGy8mzOoCrpfk5/x6 2hah4Q==
witrapper.com   rdata_46 = NS 7 2 900 20200906033312 20200807033312 64685 witrapper.com. MZUWHNj
b9XGsVGw0rTNlG2XBP5kXMK4v0idKwxuXnm1bnPFn8+JyZY+i x6MVqV0rFrflcquW1ce9cN9F1nmECcLuOV5bNQS1AA75IF
L0qP6OBPVJ jlA+FwuRvltAfy5ZRvXiakZfao/p7tkYwrI+k6+hspp9ppgd3AhxK207 JLJshHR/DP9on4u7XxVuOZfru/ac
4Ns2pCpMZ+WtgM7mWzqSyghWuBNm HICgBSyUUUm+64wB1jW3c94SwozSP+9QiQJRw2kv1WYloadkQsu+CnV8 /NFyNF5d+R
5gmkGinRG9oPTzibHh0juc4jtT6E8XUuOfGmCnYgdUI+Y3 fyBSww==
```

```
witrapper.com   rdata_46 = DNSKEY 7 2 900 20200906033312 20200807033312 64685 witrapper.com. BNG
nrIHEBlo6AMO8tlAHpZ+VUyvQme/i9u21NjElFVDUUBViJMEp6AAB FvrPcTrrFkYH40yYl9Rw+LcRWW8/3ot0Qic7TvwywH
JoP2+HvtxoxuMU fg+AnxdRMwuXTah5JgcGqKaaq4hLSthsg1aLjZX2Ph9+/lURrY+F/hbW LwQA5kvLfj6zif+rcEMbhp+a
F3Cj5iSlgdk07C9mnMFm6djB2yGVn/oa +c9LkBoH0UcuBGKY7y0vX+4x9x0p+FiWO+vClvbQL6D9AwNV9cyAhFLT lgjADL
Q68SvLqGuAIMs28BQ8qn+8vv5nD2j0BwJkay9Jt9V47/AL6flN RaNsKA==
witrapper.com   rdata_46 = NSEC3PARAM 7 2 0 20200906033312 20200807033312 64685 witrapper.com. Z
nTDzFt2ziSnL1OKQniOjeQWJHsbqpx2HEabUQFZRy+9vtdqyC65ljti yCvl2zPiMorKjRv88Oi97h/StDK3wUWIF2AOLri+
KDWewLHNUrHOsBJJ kOBlCswAl6/BXJ4+BqQYzxirJZF0H3PLeTaZOAxdO+Q0m16MsLUP+TRY tmQ9tbfa/6toAoWk0ZaiVt
q3jzMVUZqvFbAVAaBwAG6ex81NVMQETR3Z jLtMK7SgEqwCBsVM/mLAl+Kky/vV7fVh26N9hmvswXh72P7X+8hPM8Xg FhWx
bNuOhwIp4LKiwLSKBWYy+zn66v9WpFyCH/p9YMPW+9waE63cku4H 5LY6mw==
witrapper.com   rdata_46 = CAA 7 2 900 20200906033312 20200807033312 64685 witrapper.com. 04Zu6v
ZJn/zmD+CN7RQ4ZpWJYPTbomQQ5hBJLHrLnWSnNEOiW4fQJh9P v/4ASPA9u6KNrioecxfmAyRbjcLpFR31qrftx/FHMWg4d
EbW1ICuZyqW bK408iTNGfoytlRvuKaZ6GNIF8NlO8yeqqj5GmPEOeQSW71PAyJ8eEZ7 r47ccVafhM7n6w6qRaPlbLBTP6d
Y8FoeH0rwIBidJV6dtxy1isAMQvlG fyCZyc9zjPVejibBzqJ1SlH2WTOyB/FhQZHKnftsb7bw9BpTQTN3RVaH GBJbKHrpJ
fOWWBI3FFkNXklGkBELp9QbcL2w0WXJRA5yYqXjj+bv9wuP 9RhOZw==

root@attackdefense:~#
```

NSEC (next secure record): Contains a link to the next record name in the zone and lists the record types that exist for the record's name. DNS resolvers use NSEC records to verify the non-existence of a record name and type as part of DNSSEC validation. It is simpler (than NSEC3), but an attacker can use these NSEC responses to "walk the zone" and build a list of all of the records in a DNS zone.

NSEC3 (next secure record version 3): Contains links to the next record name in the zone (in hashed name sorting order) and lists the record types that exist for the name covered by the hash value in the first label of the NSEC3 record's own name. These records can be used by resolvers to verify the non-existence of a record name and type as part of DNSSEC validation. NSEC3 records are similar to NSEC records, but NSEC3 uses cryptographically hashed record names to avoid the enumeration of the record names in a zone.

NSEC3PARAM (next secure record version 3 parameters): Authoritative DNS servers use this record to calculate and determine which NSEC3 records to include in responses to DNSSEC requests for non-existing names/types.

References:

- https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- https://www.internetsociety.org/resources/deploy360/2014/dnssecnsec-vs-nsec3/

7. Retrieving SOA record for witrap.com

```
root@attackdefense:~# nslookup -type=SOA witrap.com.
Server:         192.211.79.3
Address:        192.211.79.3#53

witrap.com
        origin = ns1.witrapper.com
        mail addr = admin.witrapper.com
        serial = 1
        refresh = 900
        retry = 900
        expire = 604800
        minimum = 900

root@attackdefense:~#
```

A Start of Authority record (abbreviated as SOA record) is a type of resource record in the Domain Name System (DNS) containing administrative information about the zone, especially regarding zone transfers. The SOA record format is specified in RFC 1035.

This would return some fields like:

- **Primary master name server** for the domain (ns1.witrapper.com in this case)
- **Email address of the admin** (admin@witrapper.com in this case)
- **Serial number** for the zone. If a secondary name server slaved to this one observes an increase in this number, the slave will assume that the zone has been updated and initiate a zone transfer.

- **Refresh:** number of seconds after which the secondary name servers should query the master master for the SOA record, to detect zone changes. For small and stable zones, 86400 seconds (24 hours) is a recommended value.

- **Retry:** number of seconds after which secondary name servers should retry to request the serial number from the master if the master does not respond. It must be less than Refresh. Recommendation for small and stable zones is 7200 seconds (2 hours).

- **Expire:** number of seconds after which secondary name servers should stop answering requests for this zone if the master does not respond. This value must be bigger than the sum of Refresh and Retry. Recommendation for small and stable zones is 3600000 seconds (1000 hours).

- **Minimum:** Time to live for purposes of negative caching. Recommendation for small and stable zones is 172800 seconds (2 days).

  Note: Negative caching means to keep the resource records after they have been expired.

Reference: https://en.wikipedia.org/wiki/SOA_record

8. Retrieving all the available DNS records for witrap.com

Command: nslookup -type=any witrap.com

```
root@attackdefense:~# nslookup -type=any witrap.com
Server:         192.211.79.3
Address:        192.211.79.3#53

witrap.com      mail exchanger = 20 mx3.us.witrap.com.
witrap.com      mail exchanger = 10 mx1.us.witrap.com.
witrap.com      text = "Welcome to Witrap.com!"
witrap.com      loc = 37 46 29.744 N 122 25 9.904 W 32.00m 1m 10000m 10m
witrap.com      rdata_257 = 0 issue "ca.witrapper.com"
Name:   witrap.com
Address: 2001:db8::11:0:0:11
Name:   witrap.com
Address: 192.211.79.3
witrap.com
        origin = ns1.witrapper.com
        mail addr = admin.witrapper.com
        serial = 1
        refresh = 900
        retry = 900
        expire = 604800
        minimum = 900
witrap.com      nameserver = ns1.witrap.com.
witrap.com      nameserver = ns1.witrapper.com.
witrap.com      nameserver = ns3.witrapper.com.

root@attackdefense:~#
```

9. Performing DNS Zone Transfer (AXFR request) for witrap.com

Command: nslookup -type=axfr witrap.com.

```
root@attackdefense:~# nslookup -type=axfr witrap.com
Server:         192.211.79.3
Address:        192.211.79.3#53

witrap.com
        origin = ns1.witrapper.com
        mail addr = admin.witrapper.com
        serial = 1
        refresh = 900
        retry = 900
        expire = 604800
        minimum = 900
witrap.com      mail exchanger = 10 mx1.us.witrap.com.
witrap.com      mail exchanger = 20 mx3.us.witrap.com.
witrap.com      text = "Welcome to Witrap.com!"
witrap.com      loc = 37 46 29.744 N 122 25 9.904 W 32.00m 1m 10000m 10m
witrap.com      rdata_257 = 0 issue "ca.witrapper.com"
Name:   witrap.com
Address: 2001:db8::11:0:0:11
Name:   witrap.com
Address: 192.211.79.3
witrap.com      nameserver = ns1.witrap.com.
witrap.com      nameserver = ns1.witrapper.com.
witrap.com      nameserver = ns3.witrapper.com.
Name:   admin.witrap.com
Address: 192.211.79.41
courses.witrap.com      canonical name = witrap.com.
Name:   demo.witrap.com
Address: 192.211.79.42
dev.witrap.com  canonical name = demo.witrap.com.
Name:   info.witrap.com
Address: 192.211.79.43
labs.witrap.com canonical name = witrapper.com.
Name:   ns1.witrap.com
Address: 192.211.79.4
promo.witrap.com        canonical name = promo.witrap.com.
Name:   public.witrap.com
Address: 192.211.79.3
staging.witrap.com      canonical name = demo.witrap.com.
```

```
Name:   static.witrap.com
Address: 192.211.79.44
Name:   stats.witrap.com
Address: 192.211.79.44
Name:   training.witrap.com
Address: 192.211.79.40
Name:   mx1.us.witrap.com
Address: 192.211.79.200
Name:   mx3.us.witrap.com
Address: 192.211.79.201
witrap.com
        origin = ns1.witrapper.com
        mail addr = admin.witrapper.com
        serial = 1
        refresh = 900
        retry = 900
        expire = 604800
        minimum = 900

root@attackdefense:~#
```

Notice that all the resource records for witrap.com were retrieved.

Since zone transfer was enabled for witrap.com, a lot more info was revealed about the hosts which would normally have been hidden.

A resource record, commonly referred to as an RR, is the unit of information entry in DNS zone files. RRs are the basic building blocks of host-name and IP information and are used to resolve all DNS queries.

Reference:
https://docs.microsoft.com/en-us/windows/win32/dns/managing-dns-resource-records

Notice that the response contains CNAME (Canonical Name records as well).

A CNAME record is a type of resource record in the DNS that maps one domain name (an alias) to another (the canonical name).

Checking the canonical name for labs.witrap.com:

Command: nslookup -type=CNAME labs.witrap.com

```
root@attackdefense:~# nslookup -type=CNAME labs.witrap.com
Server:         192.211.79.3
Address:        192.211.79.3#53

labs.witrap.com canonical name = witrapper.com.

root@attackdefense:~#
```

Hence, labs.witrap.com is just an alias to witrapper.com

10. Retrieving all the available DNS records for promo.witrap.com

Command: nslookup -type=any promo.witrap.com

```
root@attackdefense:~# nslookup -type=any promo.witrap.com
Server:         192.211.79.3
Address:        192.211.79.3#53

Name:   promo.witrap.com
Address: 2001:db8::11:0:0:36
promo.witrap.com        rdata_257 = 0 issue "ca.witrapper.com"
promo.witrap.com        text = "th1s_!s_4_TXT_R3c0rd"
promo.witrap.com
        origin = ns1.witrapper.com
        mail addr = admin.witrapper.com
        serial = 1
        refresh = 900
        retry = 900
        expire = 604800
        minimum = 900
promo.witrap.com        nameserver = ns3.witrapper.com.
promo.witrap.com        nameserver = ns1.witrapper.com.
Name:   promo.witrap.com
Address: 192.211.79.3

root@attackdefense:~#
```

11. Specifying a specific DNS to retrieve the DNS records:

Command: nslookup -type=MX witrap.com ns3.witrapper.com

```
root@attackdefense:~# nslookup -type=MX witrap.com ns3.witrapper.com
Server:         ns3.witrapper.com
Address:        192.211.79.3#53

witrap.com      mail exchanger = 10 mx1.us.witrap.com.
witrap.com      mail exchanger = 20 mx3.us.witrap.com.

root@attackdefense:~#
```

The nameserver "ns3.witrapper.com" would

12. Specifying a port to be used to where the name server listens. (port 53 by default).

Command: nslookup -port=53 promo.witrap.com.

```
root@attackdefense:~#
root@attackdefense:~# nslookup -port=53 promo.witrap.com.
Server:         192.211.79.3
Address:        192.211.79.3#53

Name:   promo.witrap.com
Address: 192.211.79.3
Name:   promo.witrap.com
Address: 2001:db8::11:0:0:36

root@attackdefense:~#
```

13. Specifying a timeout interval (in seconds) for waiting for a reply.

Command: nslookup -timeout=1 port=53 promo.witrap.com.

```
root@attackdefense:~# nslookup -timeout=1 -port=53 promo.witrap.com.
Server:         192.211.79.3
Address:        192.211.79.3#53

Name:   promo.witrap.com
Address: 192.211.79.3
Name:   promo.witrap.com
Address: 2001:db8::11:0:0:36

root@attackdefense:~#
```

Specifying a wrong port (say 54) and setting timeout to 1 second:

Command: nslookup -timeout=1 port=54 promo.witrap.com.

```
root@attackdefense:~# nslookup -timeout=1 -port=54 promo.witrap.com.
;; connection timed out; no servers could be reached

root@attackdefense:~#
```

14. Using a different name server.

Syntax: nslookup <domain being queried> <nameserver IP or hostname>

Command: nslookup witrap.com 192.211.79.4

```
root@attackdefense:~# nslookup witrap.com 192.211.79.4
Server:         192.211.79.4
Address:        192.211.79.4#53

Name:   witrap.com
Address: 192.211.79.3
Name:   witrap.com
Address: 2001:db8::11:0:0:11

root@attackdefense:~#
```

14. Running nslookup in debug mode:

Command: nslookup -debug promo.witrap.com

```
root@attackdefense:~# nslookup -debug promo.witrap.com.
Server:         192.211.79.3
Address:        192.211.79.3#53

------------
    QUESTIONS:
        promo.witrap.com, type = A, class = IN
    ANSWERS:
    ->  promo.witrap.com
        internet address = 192.211.79.3
        ttl = 900
    AUTHORITY RECORDS:
    ->  promo.witrap.com
        nameserver = ns1.witrapper.com.
        ttl = 900
    ->  promo.witrap.com
        nameserver = ns3.witrapper.com.
        ttl = 900
    ADDITIONAL RECORDS:
    ->  ns1.witrapper.com
        internet address = 192.211.79.3
        ttl = 900
    ->  ns3.witrapper.com
        internet address = 192.211.79.3
        ttl = 900
------------
Name:   promo.witrap.com
Address: 192.211.79.3
------------
    QUESTIONS:
        promo.witrap.com, type = AAAA, class = IN
    ANSWERS:
    ->  promo.witrap.com
        has AAAA address 2001:db8::11:0:0:36
        ttl = 900
    AUTHORITY RECORDS:
    ->  promo.witrap.com
        nameserver = ns1.witrapper.com.
        ttl = 900
```

```
    ->  promo.witrap.com
        nameserver = ns3.witrapper.com.
        ttl = 900
    ADDITIONAL RECORDS:
    ->  ns1.witrapper.com
        internet address = 192.211.79.3
        ttl = 900
    ->  ns3.witrapper.com
        internet address = 192.211.79.3
        ttl = 900
------------
Name:   promo.witrap.com
Address: 2001:db8::11:0:0:36

root@attackdefense:~#
```

15. Running nslookup in interactive mode:

Use the following commands to retrieve the A and AAAA records for "witrap.com":

Commands:
nslookup
witrap.com

```
root@attackdefense:~# nslookup
>
> witrap.com
Server:         192.211.79.3
Address:        192.211.79.3#53

Name:   witrap.com
Address: 192.211.79.3
Name:   witrap.com
Address: 2001:db8::11:0:0:11
>
```

The above set of commands would get the A and AAAA records for witrap.com (in interactive mode).

Use the following set of commands to perform DNS Zone Transfer (AXFR request) for witrap.com

Note: type and querytype options do the same thing and are interchangeable.

Commands:
set querytype=AXFR
witrap.com

```
> set querytype=AXFR
> witrap.com
Server:         192.211.79.3
Address:        192.211.79.3#53

witrap.com
        origin = ns1.witrapper.com
        mail addr = admin.witrapper.com
        serial = 1
        refresh = 900
        retry = 900
        expire = 604800
        minimum = 900
witrap.com      mail exchanger = 10 mx1.us.witrap.com.
witrap.com      mail exchanger = 20 mx3.us.witrap.com.
witrap.com      text = "Welcome to Witrap.com!"
witrap.com      loc = 37 46 29.744 N 122 25 9.904 W 32.00m 1m 10000m 10m
witrap.com      rdata_257 = 0 issue "ca.witrapper.com"
Name:   witrap.com
Address: 2001:db8::11:0:0:11
Name:   witrap.com
Address: 192.211.79.3
witrap.com      nameserver = ns1.witrap.com.
witrap.com      nameserver = ns1.witrapper.com.
witrap.com      nameserver = ns3.witrapper.com.
Name:   admin.witrap.com
Address: 192.211.79.41
courses.witrap.com      canonical name = witrap.com.
Name:   demo.witrap.com
Address: 192.211.79.42
dev.witrap.com  canonical name = demo.witrap.com.
Name:   info.witrap.com
Address: 192.211.79.43
labs.witrap.com canonical name = witrapper.com.
Name:   ns1.witrap.com
Address: 192.211.79.4
```

```
promo.witrap.com        canonical name = promo.witrap.com.
Name:   public.witrap.com
Address: 192.211.79.3
staging.witrap.com      canonical name = demo.witrap.com.
Name:   static.witrap.com
Address: 192.211.79.44
Name:   stats.witrap.com
Address: 192.211.79.44
Name:   training.witrap.com
Address: 192.211.79.40
Name:   mx1.us.witrap.com
Address: 192.211.79.200
Name:   mx3.us.witrap.com
Address: 192.211.79.201
witrap.com
        origin = ns1.witrapper.com
        mail addr = admin.witrapper.com
        serial = 1
        refresh = 900
        retry = 900
        expire = 604800
        minimum = 900
>
```

Viewing all the options that can be set in interactive mode:

Command: set all

```
> set all
Default server: 192.211.79.3
Address: 192.211.79.3#53

Set options:
  novc                  nodebug         nod2
  search                recurse
  timeout = 10          retry = 3       port = 53       ndots = 1
  querytype = A         class = IN
  srchlist =
>
```

Step 5: Using dig (Domain Information Groper) to retrieve different DNS records from the target DNS server.

1. Obtaining A records for witrap.com:

Command: dig witrap.com

```
root@attackdefense:~# dig witrap.com

; <<>> DiG 9.11.14-3-Debian <<>> witrap.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6654
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 553b60f4a46e5713f07075fd5f2e3341a3febe7aff51fadd (good)
;; QUESTION SECTION:
;witrap.com.                    IN      A

;; ANSWER SECTION:
witrap.com.             900     IN      A       192.211.79.3

;; AUTHORITY SECTION:
witrap.com.             900     IN      NS      ns3.witrapper.com.
witrap.com.             900     IN      NS      ns1.witrapper.com.

;; ADDITIONAL SECTION:
ns1.witrapper.com.      900     IN      A       192.211.79.3
ns3.witrapper.com.      900     IN      A       192.211.79.3

;; Query time: 1 msec
;; SERVER: 192.211.79.3#53(192.211.79.3)
;; WHEN: Sat Aug 08 10:38:17 IST 2020
;; MSG SIZE  rcvd: 161

root@attackdefense:~#
```

Notice that there are different sections in the response:

i. Question Section: It contains the question that the client asks from the DNS server

In the above case the question asked is:

witrap.com. IN A

which is equivalent to:

What is the A record for witrap.com?

ii. Answer Section: This section contains the answer to the request made by the client.

For the above question, the answer contains the A records for witrap.com: 192.211.79.3

witrap.com. 900 IN A 192.211.79.3

The response means the A record for witrap.com for IN class (Internet) (it is the default class) is 192.211.79.3. The TTL (Time To Live) for the above record is 900 seconds.

iii. Authority Section: It contains the list of authoritative servers for the requested domain (witrap.com. In this case)

There are 2 nameservers listed in this section: ns3.witrapper.com. and ns1.witrapper.com.

iii. Additional Section: It contains the IP addresses of the nameservers in the above case.

Note: To obtain a less verbose output, use the following command:

Command: dig witrap.com +short

```
root@attackdefense:~# dig witrap.com +short
192.211.79.3
root@attackdefense:~#
```

The A records can also be retrieved using the following command:

Command: dig A witrap.com +short

```
root@attackdefense:~# dig A witrap.com +short
192.211.79.3
root@attackdefense:~#
```

2. Querying AAAA records for witrap.com:

Command: dig AAAA witrap.com

```
root@attackdefense:~# dig AAAA witrap.com

; <<>> DiG 9.11.14-3-Debian <<>> AAAA witrap.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58284
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: dd61797fd27896f73dd824515f7581705c206bce13e08866 (good)
;; QUESTION SECTION:
;witrap.com.                    IN      AAAA

;; ANSWER SECTION:
witrap.com.             900     IN      AAAA    2001:db8::11:0:0:11

;; AUTHORITY SECTION:
witrap.com.             900     IN      NS      ns3.witrapper.com.
witrap.com.             900     IN      NS      ns1.witrapper.com.

;; ADDITIONAL SECTION:
ns1.witrapper.com.      900     IN      A       192.211.79.3
ns3.witrapper.com.      900     IN      A       192.211.79.3

;; Query time: 0 msec
;; SERVER: 192.211.79.3#53(192.211.79.3)
;; WHEN: Thu Oct 01 12:42:48 IST 2020
;; MSG SIZE  rcvd: 173

root@attackdefense:~#
```

3. Querying MX records for witrapper.com:

Command: dig MX witrapper.com

```
root@attackdefense:~# dig MX witrapper.com

; <<>> DiG 9.11.14-3-Debian <<>> MX witrapper.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41502
;; flags: qr aa rd; QUERY: 1, ANSWER: 7, AUTHORITY: 3, ADDITIONAL: 11
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b0d94b9dfca6ae72d13954d25f2e3e8c3cf6dcf908382f2c (good)
;; QUESTION SECTION:
;witrapper.com.                 IN      MX

;; ANSWER SECTION:
witrapper.com.          900     IN      MX      40 mx4.ua.witrapper.com.
witrapper.com.          900     IN      MX      70 mx7.uk.witrapper.com.
witrapper.com.          900     IN      MX      30 mx3.sg.witrapper.com.
witrapper.com.          900     IN      MX      50 mx5.ap.witrapper.com.
witrapper.com.          900     IN      MX      60 mx6.ru.witrapper.com.
witrapper.com.          900     IN      MX      20 mx2.sg.witrapper.com.
witrapper.com.          900     IN      MX      10 mx1.us.witrapper.com.

;; AUTHORITY SECTION:
witrapper.com.          900     IN      NS      ns1.witrapper.com.
witrapper.com.          900     IN      NS      ns2.witrapper.com.
witrapper.com.          900     IN      NS      ns3.witrapper.com.

;; ADDITIONAL SECTION:
mx1.us.witrapper.com.   900     IN      A       192.211.79.45
mx2.sg.witrapper.com.   900     IN      A       192.211.79.46
mx3.sg.witrapper.com.   900     IN      A       192.211.79.47
mx4.ua.witrapper.com.   900     IN      A       192.211.79.48
mx5.ap.witrapper.com.   900     IN      A       192.211.79.49
mx6.ru.witrapper.com.   900     IN      A       192.211.79.50
mx7.uk.witrapper.com.   900     IN      A       192.211.79.51
ns1.witrapper.com.      900     IN      A       192.211.79.3
ns2.witrapper.com.      900     IN      A       192.211.79.3
ns3.witrapper.com.      900     IN      A       192.211.79.3

;; Query time: 1 msec
;; SERVER: 192.211.79.3#53(192.211.79.3)
;; WHEN: Sat Aug 08 11:26:28 IST 2020
;; MSG SIZE  rcvd: 442

root@attackdefense:~#
```

The above query will tell the MX record (or records) for the specified domain. MX record is like a pointer, or address, for a domain's email. It tells other domains what server is responsible for receiving the domain's email.

Notice that the response contains multiple mail servers configured to be used by witrapper.com

There is a number before the mail server domains. It indicates their priority. The lower the number, more would be the priority of that mail server.

If a mail server with higher priority is unreachable, then the next mail server in the list would be used.

4. Querying SOA records for promo.witrap.com:

Command: dig SOA promo.witrap.com

```
root@attackdefense:~# dig SOA promo.witrap.com

; <<>> DiG 9.11.14-3-Debian <<>> SOA promo.witrap.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28984
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 48c7125874d43d017a06aab35f2e41a3b5eab203761688c2 (good)
;; QUESTION SECTION:
;promo.witrap.com.              IN      SOA

;; ANSWER SECTION:
promo.witrap.com.       900     IN      SOA     ns1.witrapper.com. admin.witrapper.com. 1 900 900 604800 900

;; AUTHORITY SECTION:
promo.witrap.com.       900     IN      NS      ns1.witrapper.com.
promo.witrap.com.       900     IN      NS      ns3.witrapper.com.

;; ADDITIONAL SECTION:
ns1.witrapper.com.      900     IN      A       192.211.79.3
ns3.witrapper.com.      900     IN      A       192.211.79.3

;; Query time: 0 msec
;; SERVER: 192.211.79.3#53(192.211.79.3)
;; WHEN: Sat Aug 08 11:39:39 IST 2020
;; MSG SIZE  rcvd: 193

root@attackdefense:~#
```

5. Getting SOA records for witrapper.com

Command: dig SOA witrapper.com

```
root@attackdefense:~# dig SOA witrapper.com

; <<>> DiG 9.11.14-3-Debian <<>> SOA witrapper.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18993
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5c7b4db7cdb28bba2f653ec05f7581ef3e75b92146eff05e (good)
;; QUESTION SECTION:
;witrapper.com.                 IN      SOA

;; ANSWER SECTION:
witrapper.com.          900     IN      SOA     ns1.witrapper.com. admin.witrapper.com. 2 900 900 604800 900

;; AUTHORITY SECTION:
witrapper.com.          900     IN      NS      ns2.witrapper.com.
witrapper.com.          900     IN      NS      ns1.witrapper.com.
witrapper.com.          900     IN      NS      ns3.witrapper.com.

;; ADDITIONAL SECTION:
ns1.witrapper.com.      900     IN      A       192.211.79.3
ns2.witrapper.com.      900     IN      A       192.211.79.3
ns3.witrapper.com.      900     IN      A       192.211.79.3

;; Query time: 0 msec
;; SERVER: 192.211.79.3#53(192.211.79.3)
;; WHEN: Thu Oct 01 12:44:55 IST 2020
;; MSG SIZE  rcvd: 214

root@attackdefense:~#
```

6. Getting the NS records for witrap.com

Command: dig NS witrap.com

```
root@attackdefense:~# dig NS witrap.com

; <<>> DiG 9.11.14-3-Debian <<>> NS witrap.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51917
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: aa758b10af3896eed532263a5f7709f51e440dd8278c269f (good)
;; QUESTION SECTION:
;witrap.com.                    IN      NS

;; ANSWER SECTION:
witrap.com.             900     IN      NS      ns3.witrapper.com.
witrap.com.             900     IN      NS      ns1.witrap.com.
witrap.com.             900     IN      NS      ns1.witrapper.com.

;; ADDITIONAL SECTION:
ns1.witrap.com.         900     IN      A       192.211.79.4
ns1.witrapper.com.      900     IN      A       192.211.79.3
ns3.witrapper.com.      900     IN      A       192.211.79.3

;; Query time: 0 msec
;; SERVER: 192.211.79.3#53(192.211.79.3)
;; WHEN: Fri Oct 02 16:37:33 IST 2020
;; MSG SIZE  rcvd: 179

root@attackdefense:~#
```

7. Retrieving the TXT records for promo.witrap.com.

Command: dig TXT promo.witrap.com

```
root@attackdefense:~# dig TXT promo.witrap.com

; <<>> DiG 9.11.14-3-Debian <<>> TXT promo.witrap.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7227
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 657673dabd236b941ca59c625f75845c41c99afb21bc1094 (good)
;; QUESTION SECTION:
;promo.witrap.com.              IN      TXT

;; ANSWER SECTION:
promo.witrap.com.       900     IN      TXT     "th1s_!s_4_TXT_R3c0rd"

;; AUTHORITY SECTION:
promo.witrap.com.       900     IN      NS      ns3.witrapper.com.
promo.witrap.com.       900     IN      NS      ns1.witrapper.com.

;; ADDITIONAL SECTION:
ns1.witrapper.com.      900     IN      A       192.211.79.3
ns3.witrapper.com.      900     IN      A       192.211.79.3

;; Query time: 0 msec
;; SERVER: 192.211.79.3#53(192.211.79.3)
;; WHEN: Thu Oct 01 12:55:16 IST 2020
;; MSG SIZE  rcvd: 184

root@attackdefense:~#
```

8. Retrieving CAA records for witrapper.com:

Command: dig CAA witrapper.com

```
root@attackdefense:~# dig CAA witrapper.com

; <<>> DiG 9.11.14-3-Debian <<>> CAA witrapper.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38586
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4a5a74aa036fa1495c97c4245f75851d3434faf0b39754af (good)
;; QUESTION SECTION:
;witrapper.com.                 IN      CAA

;; ANSWER SECTION:
witrapper.com.          900     IN      CAA     0 issue "ca.witrapper.com"

;; AUTHORITY SECTION:
witrapper.com.          900     IN      NS      ns2.witrapper.com.
witrapper.com.          900     IN      NS      ns3.witrapper.com.
witrapper.com.          900     IN      NS      ns1.witrapper.com.

;; ADDITIONAL SECTION:
ns1.witrapper.com.      900     IN      A       192.211.79.3
ns2.witrapper.com.      900     IN      A       192.211.79.3
ns3.witrapper.com.      900     IN      A       192.211.79.3

;; Query time: 0 msec
;; SERVER: 192.211.79.3#53(192.211.79.3)
;; WHEN: Thu Oct 01 12:58:29 IST 2020
;; MSG SIZE  rcvd: 207

root@attackdefense:~#
```

9. Retrieving CNAME records for witrap.com

Command: dig CNAME labs.witrap.com +short

```
root@attackdefense:~# dig CNAME labs.witrap.com +short
witrapper.com.
root@attackdefense:~#
```

labs.witrap.com is an alias for witrapper.com

10. Getting DNSSEC records for witrapper.com

Command: dig +dnssec witrapper.com +short

```
root@attackdefense:~#
root@attackdefense:~# dig +dnssec witrapper.com +short
192.211.79.3
A 7 2 900 20201106122259 20201007122259 18347 witrapper.com. B1D9jHhMXtO+UFv
DoVf75nRecb0YyTNlo1650hlhnEEZ+bWmqH3WyxJH vrnIwosKystOvsNjgF6Wof7eCTuUBdsprP
Rwf2GpRvLMousOVWE7AT5C 4q66+2JQV7e4V13caSPRYu7Ns0xLO4LrXOSt2d5CO+kcqQS6ccKxt
64i ZO7Ik3+iVI0F+Sv/9lm4xq5nnTxMpVx0KUJDDmHNjzViiW3gLQ5nspUj nFNdwG9N4qaNMR/
0IpCA77SoOi3mHgIq91qf71hKtdfQFIUvlg8vbg5g jvDrIGvUkahf9XXyu0/FCfYatzyNGX1d8J
zV2f52Ey22YBWh3zLdaNOw vxXTig==
root@attackdefense:~#
```

11. Getting only the Question and Answer section:

Command: dig witrap.com +nocomments +noauthority +noadditional +nostats

```
root@attackdefense:~# dig witrap.com +nocomments +noauthority +noadditional +nostats

; <<>> DiG 9.11.14-3-Debian <<>> witrap.com +nocomments +noauthority +noadditional +nostats
;; global options: +cmd
;witrap.com.                    IN      A
witrap.com.             900     IN      A       192.211.79.3
root@attackdefense:~#
```

Notice that this would strip out all the other information and only provide the question section and the answer section following it.

An alternative command to get the same result would be:

Command: dig +noall +answer +question witrap.com

```
root@attackdefense:~# dig +noall +answer +question witrap.com
;witrap.com.                    IN      A
witrap.com.             900     IN      A       192.211.79.3
root@attackdefense:~#
```

12. Getting answer section for all the records:

Command: dig ANY witrap.com +noall +answer

```
root@attackdefense:~# dig ANY witrap.com +noall +answer
witrap.com.             900     IN      MX      10 mx1.us.witrap.com.
witrap.com.             900     IN      MX      20 mx3.us.witrap.com.
witrap.com.             900     IN      TXT     "Welcome to Witrap.com!"
witrap.com.             900     IN      LOC     37 46 29.744 N 122 25 9.904 W 32.00m 1m 10000m
10m
witrap.com.             900     IN      CAA     0 issue "ca.witrapper.com"
witrap.com.             900     IN      AAAA    2001:db8::11:0:0:11
witrap.com.             900     IN      A       192.211.79.3
witrap.com.             900     IN      SOA     ns1.witrapper.com. admin.witrapper.com. 1 900 9
00 604800 900
witrap.com.             900     IN      NS      ns1.witrapper.com.
witrap.com.             900     IN      NS      ns1.witrap.com.
witrap.com.             900     IN      NS      ns3.witrapper.com.
root@attackdefense:~#
```

13. Performing reverse DNS lookup on an IP address.

Command: dig -x 192.211.79.44 +short

```
root@attackdefense:~# dig -x 192.211.79.44 +short
stats.witrap.com.
static.witrap.com.
root@attackdefense:~#
```

14. Querying DNS records for multiple domains in a single command:

Command: dig promo.witrap.com TXT +noall +answer witrap.com MX +short witrapper.com AAAA +noall +answer

```
root@attackdefense:~# dig promo.witrap.com TXT +noall +answer witrap.com MX +short
 witrapper.com AAAA +noall +answer
"th1s_!s_4_TXT_R3c0rd"
20 mx3.us.witrap.com.
10 mx1.us.witrap.com.
2001:db8::11:0:0:15
2001:db8::11:0:0:14
2001:db8::11:0:0:19
2001:db8::11:0:0:20
2001:db8::11:0:0:17
2001:db8::11:0:0:18
2001:db8::11:0:0:16
root@attackdefense:~#
```

The 3 different answers are contained in the different blocks with red borders.

15. Performing a DNS zone transfer:

Command: dig axfr witrap.com +noall +answer

```
root@attackdefense:~# dig axfr witrap.com +noall +answer
witrap.com.             900     IN      SOA     ns1.witrapper.com. admin.witrapper.com. 1 900 900 604800 900
witrap.com.             900     IN      MX      10 mx1.us.witrap.com.
witrap.com.             900     IN      MX      20 mx3.us.witrap.com.
witrap.com.             900     IN      TXT     "Welcome to Witrap.com!"
witrap.com.             900     IN      LOC     37 46 29.744 N 122 25 9.904 W 32.00m 1m 10000m 10m
witrap.com.             900     IN      CAA     0 issue "ca.witrapper.com"
witrap.com.             900     IN      AAAA    2001:db8::11:0:0:11
witrap.com.             900     IN      A       192.211.79.3
witrap.com.             900     IN      NS      ns1.witrap.com.
witrap.com.             900     IN      NS      ns1.witrapper.com.
witrap.com.             900     IN      NS      ns3.witrapper.com.
admin.witrap.com.       900     IN      A       192.211.79.41
courses.witrap.com.     900     IN      CNAME   witrap.com.
demo.witrap.com.        900     IN      A       192.211.79.42
dev.witrap.com.         900     IN      CNAME   demo.witrap.com.
info.witrap.com.        900     IN      A       192.211.79.43
labs.witrap.com.        900     IN      CNAME   witrapper.com.
ns1.witrap.com.         900     IN      A       192.211.79.4
promo.witrap.com.       900     IN      CNAME   promo.witrap.com.
public.witrap.com.      900     IN      A       192.211.79.3
staging.witrap.com.     900     IN      CNAME   demo.witrap.com.
static.witrap.com.      900     IN      A       192.211.79.44
stats.witrap.com.       900     IN      A       192.211.79.44
training.witrap.com.    900     IN      A       192.211.79.40
mx1.us.witrap.com.      900     IN      A       192.211.79.200
mx3.us.witrap.com.      900     IN      A       192.211.79.201
witrap.com.             900     IN      SOA     ns1.witrapper.com. admin.witrapper.com. 1 900 900 604800 900
root@attackdefense:~#
```

Notice that all the resource records from witrap.com were retrieved!

The response contains NS, A, AAAA, CAA, LOC, TXT, MX, CNAME, and SOA records.

18. Determining the IP address of the machine that supports LDAP over TCP on witrapper.com

Command: nslookup -type=srv _ldap._tcp.witrapper.com

```
root@attackdefense:~# nslookup -type=srv _ldap._tcp.witrapper.com
Server:         192.211.79.3
Address:        192.211.79.3#53

_ldap._tcp.witrapper.com        service = 10 10 389 ldap.witrapper.com.

root@attackdefense:~#
```

Command: dig ldap.witrapper.com

```
root@attackdefense:~# dig ldap.witrapper.com

; <<>> DiG 9.11.14-3-Debian <<>> ldap.witrapper.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15045
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 17c3a17487e04f78ce79e15b5f7dd98eab878dbae30fd65f (good)
;; QUESTION SECTION:
;ldap.witrapper.com.            IN      A

;; ANSWER SECTION:
ldap.witrapper.com.     900     IN      A       192.211.79.213

;; AUTHORITY SECTION:
witrapper.com.          900     IN      NS      ns1.witrapper.com.
witrapper.com.          900     IN      NS      ns2.witrapper.com.
witrapper.com.          900     IN      NS      ns3.witrapper.com.
```

```
;; ADDITIONAL SECTION:
ns1.witrapper.com.      900     IN      A       192.211.79.3
ns2.witrapper.com.      900     IN      A       192.211.79.3
ns3.witrapper.com.      900     IN      A       192.211.79.3

;; Query time: 5 msec
;; SERVER: 192.211.79.3#53(192.211.79.3)
;; WHEN: Wed Oct 07 20:36:54 IST 2020
;; MSG SIZE  rcvd: 193

root@attackdefense:~#
```

19. Using a different nameserver.

Command: dig @192.211.79.4 witrap.com

```
root@attackdefense:~#
root@attackdefense:~# dig @192.211.79.4 witrap.com

; <<>> DiG 9.11.14-3-Debian <<>> @192.211.79.4 witrap.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5255
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0bc2707d468bcd55413e99b15f7ddb4d89c3220df8844078 (good)
;; QUESTION SECTION:
;witrap.com.                    IN      A

;; ANSWER SECTION:
witrap.com.             900     IN      A       192.211.79.3
```

```
;; AUTHORITY SECTION:
witrap.com.             900     IN      NS      ns1.witrap.com.

;; ADDITIONAL SECTION:
ns1.witrap.com.         900     IN      A       192.211.79.4

;; Query time: 1 msec
;; SERVER: 192.211.79.4#53(192.211.79.4)
;; WHEN: Wed Oct 07 20:44:21 IST 2020
;; MSG SIZE  rcvd: 117

root@attackdefense:~#
```

If the resource records for a domain does not exist on the domain server, then no Answer section is returned:

Command: dig @192.211.79.4 witrapper.com

```
root@attackdefense:~# dig @192.211.79.4 witrapper.com

; <<>> DiG 9.11.14-3-Debian <<>> @192.211.79.4 witrapper.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 38348
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d610dcb2babb33ae72b5ee255f7dc41cead91fe224eb1df7 (good)
;; QUESTION SECTION:
;witrapper.com.                 IN      A

;; Query time: 0 msec
;; SERVER: 192.211.79.4#53(192.211.79.4)
;; WHEN: Wed Oct 07 19:05:24 IST 2020
;; MSG SIZE  rcvd: 70

root@attackdefense:~#
```

References:

1. nslookup man page (https://linux.die.net/man/1/nslookup)
2. dig man page (https://linux.die.net/man/1/dig)
3. SOA Record (https://en.wikipedia.org/wiki/SOA_record)