
ATTACK
DEFENSE
by PentesterAcademy

Name	DNS: Basic Queries
URL	https://www.attackdefense.com/challengedetails?cid=234
Type	Network Recon : 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.

Q1. What is the IP address of primary Name server of witrap.com ?

Answer: 192.168.66.4

Command: dig NS witrap.com @192.106.253.3

```
root@attackdefense:~# dig NS witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> NS witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21795
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;witrap.com.                    IN      NS

;; ANSWER SECTION:
witrap.com.             86400   IN      NS      ns2.witrap.com.
witrap.com.             86400   IN      NS      ns.witrap.com.

;; ADDITIONAL SECTION:
ns.witrap.com.          86400   IN      A       192.168.66.4
ns2.witrap.com.         86400   IN      A       192.168.68.24

;; Query time: 0 msec
;; SERVER: 192.106.253.3#53(192.106.253.3)
;; WHEN: Tue Nov 06 18:49:19 UTC 2018
;; MSG SIZE  rcvd: 106

root@attackdefense:~#
```

Q2. What is the ipv4 address of witrap.com ?

Answer: 192.168.66.2

Command: dig A witrap.com @192.106.253.3

```
root@attackdefense:~# dig A witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> A witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61952
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;witrap.com.                    IN      A

;; ANSWER SECTION:
witrap.com.             86400   IN      A       192.168.66.2
```

Q3. What is the ipv6 address of witrap.com ?

Answer: 2001:db8::1:0:0:13

Command: dig AAAA witrap.com @192.106.253.3

```
root@attackdefense:~# dig AAAA witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> AAAA witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11543
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;witrap.com.                    IN      AAAA

;; ANSWER SECTION:
witrap.com.             86400   IN      AAAA    2001:db8::1:0:0:13
```

Q4. How many mail server does witrap.com have?

Answer: 2

Command: dig MX witrap.com @192.106.253.3

```
root@attackdefense:~# dig MX witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> MX witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26721
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;witrap.com.                    IN      MX

;; ANSWER SECTION:
witrap.com.             86400   IN      MX      20 mail2.witrap.com.
witrap.com.             86400   IN      MX      10 mail.witrap.com.

;; AUTHORITY SECTION:
witrap.com.             86400   IN      NS      ns2.witrap.com.
witrap.com.             86400   IN      NS      ns.witrap.com.

;; ADDITIONAL SECTION:
mail.witrap.com.        86400   IN      A       192.168.66.10
mail2.witrap.com.       86400   IN      A       192.168.66.15
ns.witrap.com.          86400   IN      A       192.168.66.4
```

Q5. What is the IP address of Mail Server of witrap.com which has highest priority?

Answer: 192.168.66.10

Command: dig MX witrap.com @192.106.253.3

```
root@attackdefense:~# dig MX witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> MX witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26721
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;witrap.com.                    IN      MX

;; ANSWER SECTION:
witrap.com.             86400   IN      MX      20 mail2.witrap.com.
witrap.com.             86400   IN      MX      10 mail.witrap.com.

;; AUTHORITY SECTION:
witrap.com.             86400   IN      NS      ns2.witrap.com.
witrap.com.             86400   IN      NS      ns.witrap.com.

;; ADDITIONAL SECTION:
mail.witrap.com.        86400   IN      A       192.168.66.10
mail2.witrap.com.       86400   IN      A       192.168.66.15
ns.witrap.com.          86400   IN      A       192.168.66.4
```

Q6. What is the Canonical Name of www.witrap.com?

Answer: public.witrap.com

Command: dig CNAME www.witrap.com @192.106.253.3

```
root@attackdefense:~# dig CNAME www.witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> CNAME www.witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43974
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.witrap.com.                        IN      CNAME

;; ANSWER SECTION:
www.witrap.com.         86400   IN      CNAME   public.witrap.com.
```

Command: dig www.witrap.com @192.106.253.3

```
root@attackdefense:~# dig www.witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> www.witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45550
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.witrap.com.                        IN      A

;; ANSWER SECTION:
www.witrap.com.         86400   IN      CNAME   public.witrap.com.
public.witrap.com.      86400   IN      A       192.168.66.3
```

Q7. Which Certificate Authorities can Issue certificate for witrap.com?

Answer: witrapselfcert.com

Command: dig CAA witrap.com @192.106.253.3

```
root@attackdefense:~#  dig CAA witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> CAA witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36649
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;witrap.com.                    IN      CAA

;; ANSWER SECTION:
witrap.com.             86400   IN      CAA     0 issue "witrapselfcert.com"
```

Q8. What is the Geographical location of witrap.com ?

Answer: 37 46 29.744 N 122 25 9.904 W 32.00m

Command: dig LOC witrap.com @192.106.253.3

```
root@attackdefense:~# dig  LOC witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> LOC witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4179
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;witrap.com.                    IN      LOC

;; ANSWER SECTION:
witrap.com.             86400   IN      LOC     37 46 29.744 N 122 25 9.904 W 32.00m 1m 10000m 10m
```

Q9. Can you find the flag provided in the information of witrap.com?

Answer: txt_r3c0rd_0f_witr4p

Command: dig TXT witrap.com @192.106.253.3

```
root@attackdefense:~# dig  TXT witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> TXT witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7811
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;witrap.com.                    IN      TXT

;; ANSWER SECTION:
witrap.com.             86400   IN      TXT     "FLAG: txt_r3c0rd_0f_witr4p"
```

Q10. What is the IP address of machine which support sip over TCP on witrap.com?

Answer: 192.168.66.155

Commands:
nslookup -type=srv _sip._tcp.witrap.com 192.106.253.3
dig sip.witrap.com @192.106.253.3

```
root@attackdefense:~# nslookup -type=srv _sip._tcp.witrap.com 192.106.253.3
Server:         192.106.253.3
Address:        192.106.253.3#53

_sip._tcp.witrap.com    service = 10 10 5060 sip.witrap.com.

root@attackdefense:~# dig sip.witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> sip.witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50804
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sip.witrap.com.                        IN      A

;; ANSWER SECTION:
sip.witrap.com.         86400   IN      A       192.168.66.155
```

Q11. What is the administrative email of witrap.com?

Answer: root.witrap.com

Command: dig soa witrap.com @192.106.253.3

```
root@attackdefense:~# dig soa witrap.com @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> soa witrap.com @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63423
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;witrap.com.                    IN      SOA

;; ANSWER SECTION:
witrap.com.             86400   IN      SOA     ns.witrap.com. root.witrap.com. 2011071001 3600 1800 604800 86400
```

Q12. Which domain corresponds to 192.168.67.8 ?

Answer: private.witrap.com

Command: dig -x 192.168.67.8 @192.106.253.3

```
root@attackdefense:~# dig -x 192.168.67.8 @192.106.253.3

; <<>> DiG 9.11.4-4-Debian <<>> -x 192.168.67.8 @192.106.253.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7048
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;8.67.168.192.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
8.67.168.192.in-addr.arpa. 86400 IN     PTR     private.witrap.com.
```

References:

1. Bind 9 (https://www.isc.org/downloads/bind/)
2. nslookup (https://linux.die.net/man/1/nslookup)
3. dig (https://linux.die.net/man/1/dig)