PENTESTER ACADEMYTOOL BOX PENTESTING

OF THE PENTESTER ACADEMYTOOL BOX PENTESTING

OF THE PENTESTING HACKER PENTESTER

TEAM LABSPENTES TO THE PENTESTER

TEAM LABSPENTES TO THE PENTESTER

OF THE PENTESTING HACKER

THE PENTESTING HACKER

TOOL BOX

OF THE PENTESTING

Name	DNS: Zone Transfer Enabled
URL	https://www.attackdefense.com/challengedetails?cid=235
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. How many A Records are present for witrap.com and its subdomains?

Answer: 9

Command: dig axfr witrap.com @192.60.177.3

```
root@attackdefense:~# dig axfr witrap.com @192.60.177.3
; <<>> DiG 9.11.4-4-Debian <<>> axfr witrap.com @192.60.177.3
;; global options: +cmd
witrap.com.
                      86400
                              IN
                                     SOA
                                            primary.witrap.com. root.witrap.com. 2011071001 3600 1800 604800 86400
witrap.com.
                      86400 IN
                                     CAA
                                            0 issue "witrapselfcert.com"
                     86400
                                     LOC
                                            37 46 29.744 N 122 25 9.904 W 32.00m 1m 10000m 10m
witrap.com.
                             IN
                                            192.168.60.5
witrap.com.
                     86400
                             IN
                                     Α
                                     NS
witrap.com.
                      86400
                              IN
                                            primary.witrap.com.
witrap.com.
                              IN
                                     NS
                                            secondary.witrap.com.
                                          10 mx.witrap.com.
                     86400
witrap.com.
                             IN
                                     MX
                                          20 mx2.witrap.com.
                     86400 IN
witrap.com.
                                     MX
                    86400 IN
                                    AAAA 2001:db8::11:0:0:11
witrap.com.
_ldap._tcp.witrap.com. 3600
                                            10 10 389 ldap.witrap.com.
free.witrap.com.
                   86400 IN
                                            192.168.60.100
ldap.witrap.com.
                     86400 IN
                                            192.168.62.111
                     86400
mx.witrap.com.
                             IN
                                            192.168.65.110
mx2.witrap.com.
                     86400
                             IN
                                            192.168.65.150
open.witrap.com.
                      86400
                             IN
                                     CNAME
                                            free.witrap.com.
                      86400
primary.witrap.com.
reserved.witrap.com. 86400 IN
                                            192.168.62.81
secondary.witrap.com.
                                            192.168.66.15
                      86400
                             IN
th3s3cr3tflag.witrap.com. 86400 IN
                                            192.168.61.35
```

Q2. What is the IP address of machine which support Idap over TCP on witrap.com?

Answer: 192.168.62.111

Command: dig axfr witrap.com @192.60.177.3

```
root@attackdefense:~# dig axfr witrap.com @192.60.177.3
; <<>> DiG 9.11.4-4-Debian <<>> axfr witrap.com @192.60.177.3
;; global options: +cmd
                      86400
                                              primary.witrap.com. root.witrap.com. 2011071001 3600 1800 604800 86400
witrap.com.
                                       SOA
                               IN
                      86400
                               IN
                                       CAA
                                              0 issue "witrapselfcert.com"
witrap.com.
witrap.com.
                       86400
                               IN
                                      LOC
                                              37 46 29.744 N 122 25 9.904 W 32.00m 1m 10000m 10m
                      86400
witrap.com.
                               IN
                                              192.168.60.5
                      86400 IN
witrap.com.
                                              primary.witrap.com.
                      86400 IN
                                             secondary.witrap.com.
                                      NS
witrap.com.
                     86400 IN
                                             10 mx.witrap.com.
witrap.com.
                 86400 IN MX 20 mx2.witrap.com.
86400 IN AAAA 2001:db8::11:0:0:11
.com. 3600 IN SRV 10 10 389 ldap.witrap.com.
witrap.com.
witrap.com.
_ldap._tcp.witrap.com. 3600
                              IN A 192.168.60.100
IN A 192.168.62.111
free.witrap.com. 86400
ldap.witrap.com.
                      86400 IN
mx.witrap.com.
                                             192.168.65.110
                     86400 IN
                                             192.168.65.150
mx2.witrap.com.
open.witrap.com.
                    86400 IN CNAME free.witrap.com.
primary.witrap.com. 86400 IN
                                             192.168.60.14
reserved.witrap.com. 86400 IN
                                              192.168.62.81
secondary.witrap.com. 86400 IN
                                              192.168.66.15
th3s3cr3tflag.witrap.com. 86400 IN
                                              192.168.61.35
                                               "Here is your secret flag: my_s3cr3t_fl4g"
th3s3cr3tflag.witrap.com. 86400 IN
                       86400
witrap.com.
                                              primary.witrap.com. root.witrap.com. 2011071001 3600 1800 604800 86400
```

Q3. Can you find the secret flag in TXT record of a subdomain of witrap.com?

Answer: my_s3cr3t_fl4g

Command: dig axfr witrap.com @192.60.177.3

```
root@attackdefense:~# dig axfr witrap.com @192.60.177.3
; <<>> DiG 9.11.4-4-Debian <<>> axfr witrap.com @192.60.177.3
;; global options: +cmd
witrap.com.
                            86400 IN
                                                SOA
                                                          primary.witrap.com. root.witrap.com. 2011071001 3600 1800 604800 86400
                                              CAA 0 issue "witrapselfcert.com"
LOC 37 46 29.744 N 122 25 9.904 W 32.00m 1m 10000m 10m
A 192.168.60.5
witrap.com.
                            86400
witrap.com.
                            86400
                                              Α
                           86400 IN
witrap.com.
                           86400 IN
                                              NS
witrap.com.
                                                        primary.witrap.com.
                          86400 IN NS secondary.witrap.com.
86400 IN NS secondary.witrap.com.
86400 IN MX 10 mx.witrap.com.
86400 IN MX 20 mx2.witrap.com.
86400 IN AAAA 2001:db8::11:0:0:11
. 3600 IN SRV 10 10 389 ldap.witrap.com.
86400 IN A 192.168.60.100
86400 IN A 192.168.62.111
witrap.com.
witrap.com.
witrap.com.
witrap.com.
 _ldap._tcp.witrap.com. 3600
free.witrap.com. 86400 IN ldap.witrap.com. 86400 IN
ldap.witrap.com.
                                             A 192.168.65.110

A 192.168.65.150

CNAME free.witrap.com.

A 192.168.60.14

A 192.168.62.81
                           86400 IN
mx.witrap.com.
                            86400 IN
mx2.witrap.com.
                          86400 IN
86400 IN
open.witrap.com.
primary.witrap.com.
reserved.witrap.com. 86400 IN
secondary.witrap.com. 86400 IN
                                                        192.168.66.15
                                                        192.168.61.35
th3s3cr3tflag.witrap.com. 86400 IN
th3s3cr3tflag.witrap.com. 86400 IN
                                                           "Here is your secret flag: my_s3cr3t_fl4g"
                                                          primary.witrap.com. root.witrap.com. 2011071001 3600 1800 604800 86400
witrap.com.
```

Q4. What is the subdomain for which only reverse dns entry exists for witrap.com? witrap owns the ip address range: 192.168.*.*

Answer: temp.witrap.com

Command: dig axfr -x 192.168 @192.60.177.3

```
root@attackdefense:~# dig axfr -x 192.168 @192.60.177.3
; <<>> DiG 9.11.4-4-Debian <<>> axfr -x 192.168 @192.60.177.3
;; global options: +cmd
168.192.in-addr.arpa. 86400
                                        SOA
                                IN
                                                primary.witrap.com. root.witrap.com. 2011071002 3600 1800 604800 86400
168.192.in-addr.arpa.
                       86400
                                IN
                                        NS
                                                primary.witrap.com.
168.192.in-addr.arpa.
                       86400
                                IN
                                        NS
                                                secondary.witrap.com.
100.60.168.192.in-addr.arpa. 86400 IN
                                        PTR
                                                free.witrap.com.
14.60.168.192.in-addr.arpa. 86400 IN
                                        PTR
                                                primary.witrap.com.
5.60.168.192.in-addr.arpa. 86400 IN
                                        PTR
                                                witrap.com.168.192.in-addr.arpa.
35.61.168.192.in-addr.arpa. 86400 IN
                                        PTR
                                                th3s3cr3tflag.witrap.com.
111.62.168.192.in-addr.arpa. 86400 IN
                                        PTR
                                                ldap.witrap.com.
118.62.168.192.in-addr.arpa. 86400 IN
                                        PTR
                                                temp.witrap.com
                                                reserved.witrap.com.
81.62.168.192.in-addr.arpa. 86400 IN
                                        PTR
110.65.168.192.in-addr.arpa. 86400 IN
                                        PTR
                                                mx.witrap.com.
150.65.168.192.in-addr.arpa. 86400 IN
                                                mx2.witrap.com.
15.66.168.192.in-addr.arpa. 86400 IN
                                        PTR
                                                secondary.witrap.com.
                       86400 IN
                                        SOA
                                                primary.witrap.com. root.witrap.com. 2011071002 3600 1800 604800 86400
168.192.in-addr.arpa.
;; Query time: 0 msec
;; SERVER: 192.60.177.3#53(192.60.177.3)
;; WHEN: Tue Nov 06 20:44:03 UTC 2018
;; XFR size: 14 records (messages 1, bytes 427)
```

Q5. How many records are present in reverse zone for witrap.com (excluding SOA)? witrap owns the ip address range: 192.168.*.*

Answer: 12

Command: dig axfr -x 192.168 @192.60.177.3

```
root@attackdefense:~# dig axfr -x 192.168 @192.60.177.3
; <<>> DiG 9.11.4-4-Debian <<>> axfr -x 192.168 @192.60.177.3
;; global options: +cmd
168.192.in-addr.arpa. 86400
                                         SOA
                                                 primary.witrap.com. root.witrap.com. 2011071002 3600 1800 604800 86400
                                IN
                                                 primary.witrap.com.
secondary.witrap.com.
168.192.in-addr.arpa.
168.192.in-addr.arpa.
                        86400
                                IN
                                                 free.witrap.com.
100.60.168.192.in-addr.arpa. 86400 IN
14.60.168.192.in-addr.arpa. 86400 IN
                                                 primary.witrap.com.
5.60.168.192.in-addr.arpa. 86400 IN
                                                 witrap.com.168.192.in-addr.arpa.
35.61.168.192.in-addr.arpa. 86400 IN
                                        PTR
                                                 th3s3cr3tflag.witrap.com.
111.62.168.192.in-addr.arpa. 86400 IN
                                        PTR
                                                 ldap.witrap.com.
118.62.168.192.in-addr.arpa. 86400 IN
                                                 temp.witrap.com.
                                                 reserved.witrap.com.
81.62.168.192.in-addr.arpa. 86400 IN
110.65.168.192.in-addr.arpa. 86400 IN
                                                 mx2.witrap.com.
150.65.168.192.in-addr.arpa. 86400 IN
                                                 secondary.witrap.com.
15.66.168.192.in-addr.arpa. 86400 IN
168.192.in-addr.arpa.
                        86400
                                                 primary.witrap.com. root.witrap.com. 2011071002 3600 1800 604800 86400
;; Query time: 0 msec
;; SERVER: 192.60.177.3#53(192.60.177.3)
;; WHEN: Tue Nov 06 20:44:03 UTC 2018
;; XFR size: 14 records (messages 1, bytes 427)
```

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)