ATTACK DEFENSE

by PentesterAcademy

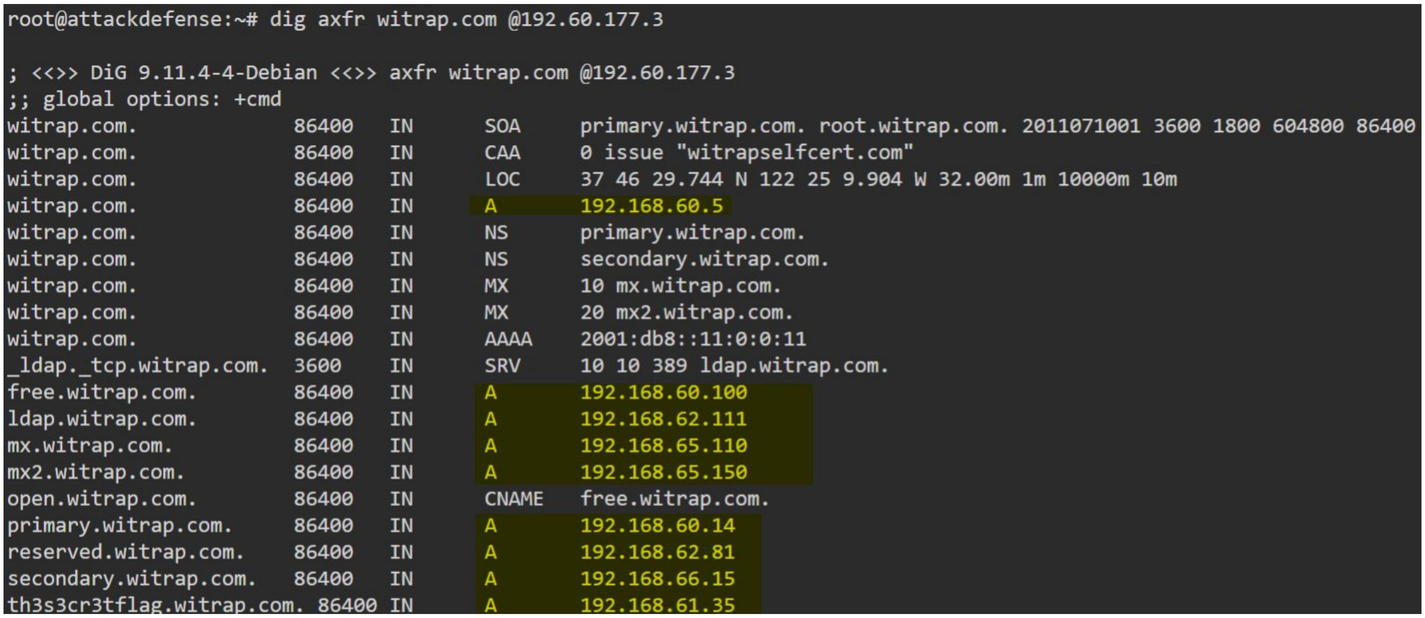
Name	DNS: Zone Transfer Enabled
URL	https://www.attackdefense.com/challengedetails?cid=235
Type	Network Recon : DNS

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



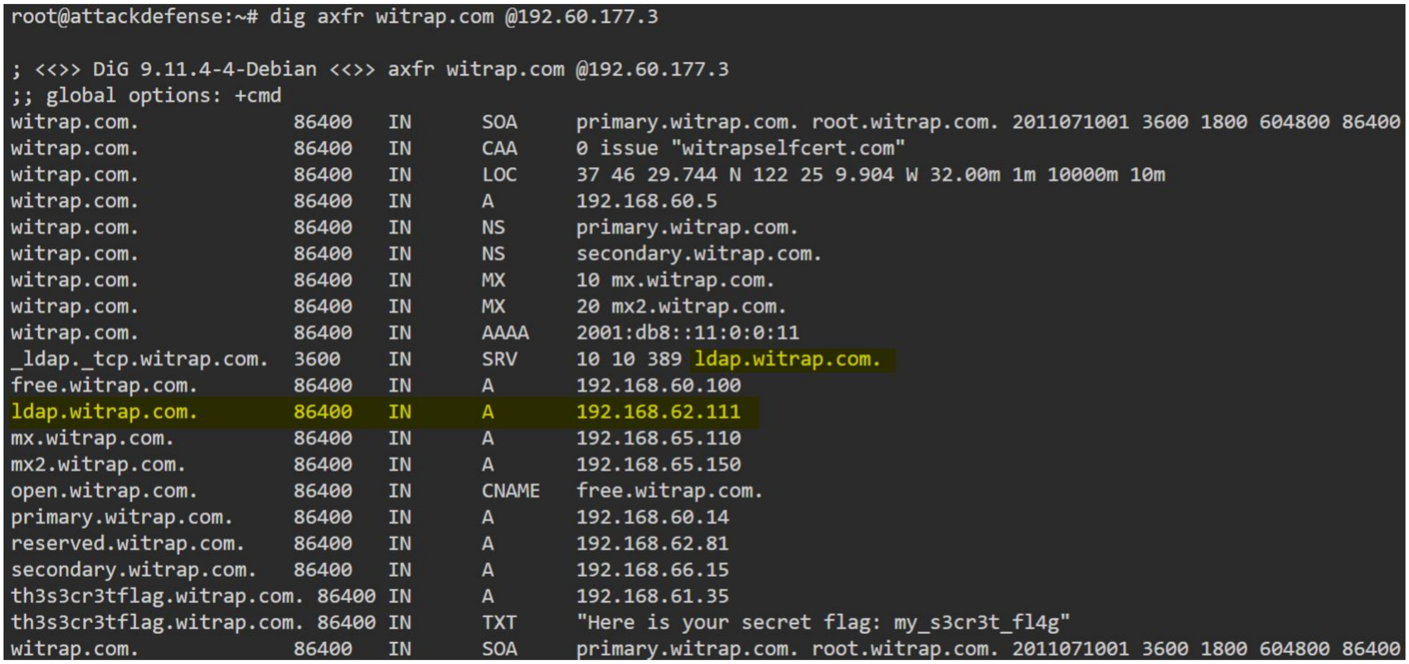
```
root@attackdefense:~# dig axfr witrap.com @192.60.177.3

; <<>> 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"
witrap.com.             86400   IN      LOC     37 46 29.744 N 122 25 9.904 W 32.00m 1m 10000m 10m
witrap.com.             86400   IN      A       192.168.60.5
witrap.com.             86400   IN      NS      primary.witrap.com.
witrap.com.             86400   IN      NS      secondary.witrap.com.
witrap.com.             86400   IN      MX      10 mx.witrap.com.
witrap.com.             86400   IN      MX      20 mx2.witrap.com.
witrap.com.             86400   IN      AAAA    2001:db8::11:0:0:11
_ldap._tcp.witrap.com.  3600    IN      SRV     10 10 389 ldap.witrap.com.
free.witrap.com.        86400   IN      A       192.168.60.100
ldap.witrap.com.        86400   IN      A       192.168.62.111
mx.witrap.com.          86400   IN      A       192.168.65.110
mx2.witrap.com.         86400   IN      A       192.168.65.150
open.witrap.com.        86400   IN      CNAME   free.witrap.com.
primary.witrap.com.     86400   IN      A       192.168.60.14
reserved.witrap.com.    86400   IN      A       192.168.62.81
secondary.witrap.com.   86400   IN      A       192.168.66.15
th3s3cr3tflag.witrap.com. 86400 IN      A       192.168.61.35
```

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

Answer: 192.168.62.111

Command: dig axfr witrap.com @192.60.177.3



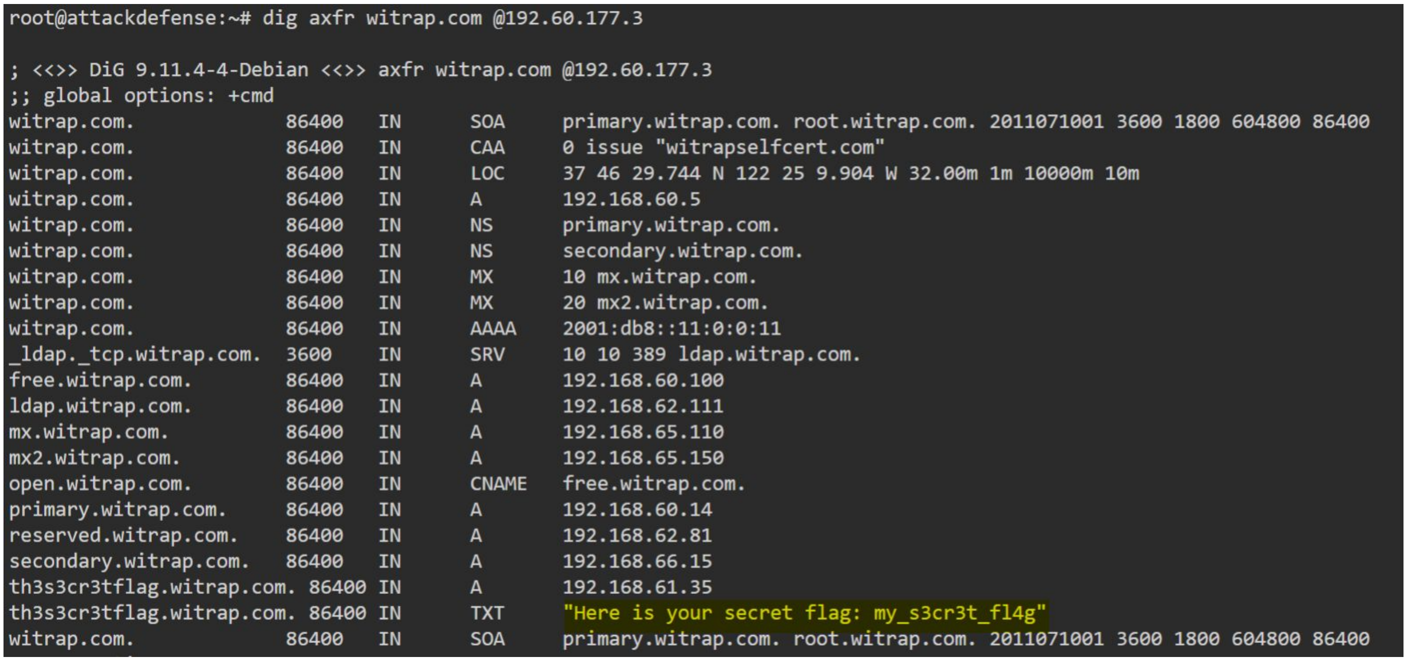
```
root@attackdefense:~# dig axfr witrap.com @192.60.177.3

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



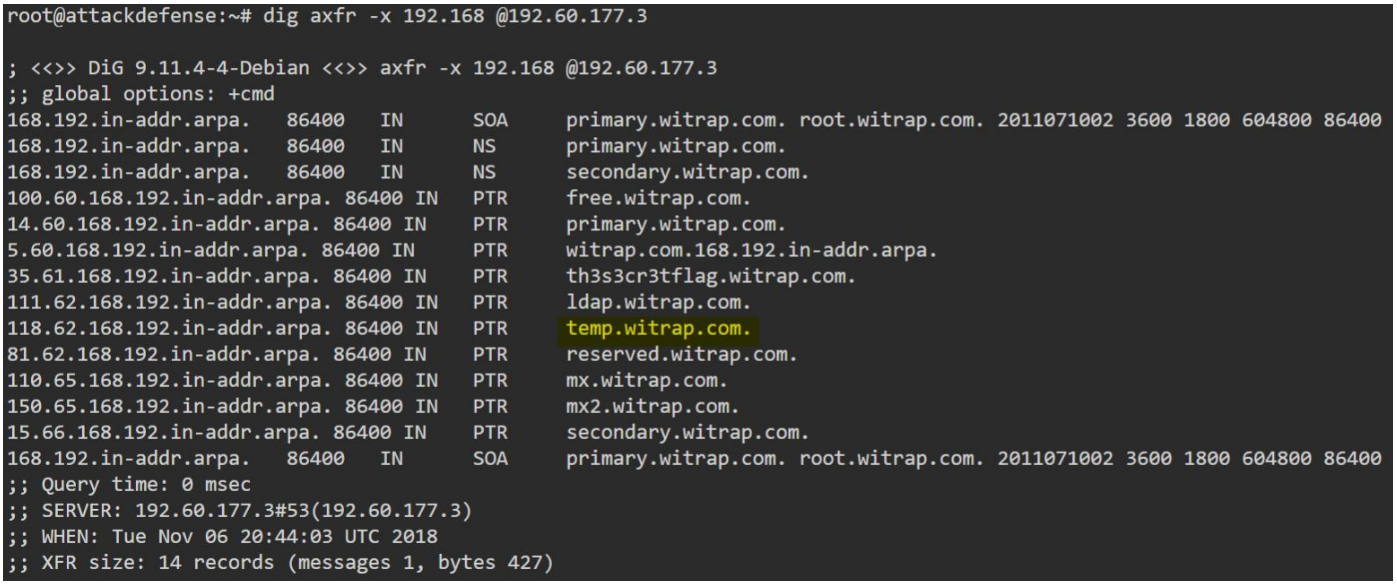
```
root@attackdefense:~# dig axfr witrap.com @192.60.177.3

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

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



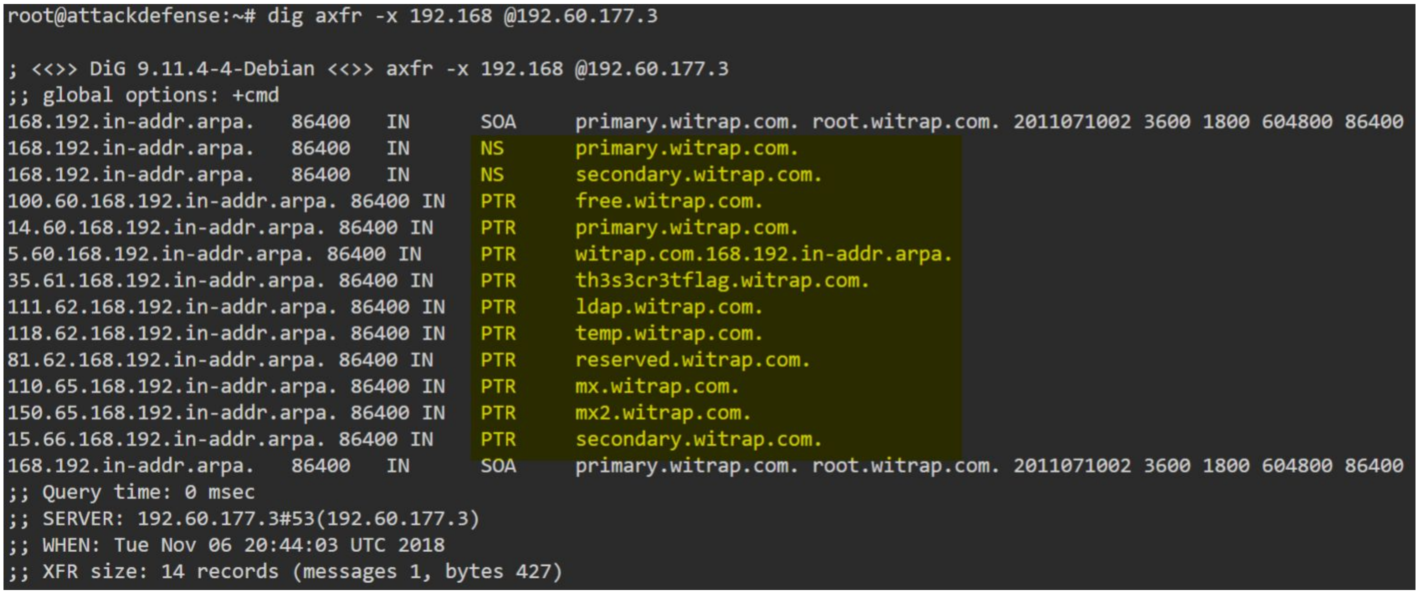
```
root@attackdefense:~# dig axfr -x 192.168 @192.60.177.3

; <<>> DiG 9.11.4-4-Debian <<>> axfr -x 192.168 @192.60.177.3
;; global options: +cmd
168.192.in-addr.arpa.   86400   IN      SOA     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.
81.62.168.192.in-addr.arpa. 86400 IN    PTR     reserved.witrap.com.
110.65.168.192.in-addr.arpa. 86400 IN   PTR     mx.witrap.com.
150.65.168.192.in-addr.arpa. 86400 IN   PTR     mx2.witrap.com.
15.66.168.192.in-addr.arpa. 86400 IN    PTR     secondary.witrap.com.
168.192.in-addr.arpa.   86400   IN      SOA     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)
```

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   IN      SOA     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.
81.62.168.192.in-addr.arpa. 86400 IN    PTR     reserved.witrap.com.
110.65.168.192.in-addr.arpa. 86400 IN   PTR     mx.witrap.com.
150.65.168.192.in-addr.arpa. 86400 IN   PTR     mx2.witrap.com.
15.66.168.192.in-addr.arpa. 86400 IN    PTR     secondary.witrap.com.
168.192.in-addr.arpa.   86400   IN      SOA     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)