

ATTACK DEFENSE LABS COURSES
PENTESTER ACADEMY TOOL BOX PENTESTING
JOINT WORLD-CLASS TRAINERS TRAINING HACKER
TOOL BOX PATV HACKER
HACKER PENTESTING
PATV RED TEAM LABS ATTACK DEFENSE LABS
TRAINING COURSES ACCESS POINT PENTESTER
TEAM LABS PENTESTER TOOL BOX PENTESTING
ACCESS POINT WORLD-CLASS TRAINERS TRAINING
WORLD-CLASS TRAINERS
ATTACK DEFENSE LABS TRAINING COURSES PATV ACCESS
PENTESTER ACADEMY TOOL BOX PENTESTING
ATTACK DEFENSE LABS TRAINING COURSES PENTESTER ACADEMY
COURSES PENTESTER ACADEMY TOOL BOX PENTESTING
TOOL BOX HACKER PENTESTING
PATV RED TEAM LABS ATTACK DEFENSE LABS
COURSES PENTESTER ACADEMY
PENTESTER ACADEMY ATTACK DEFENSE LABS
ATTACK DEFENSE LABS TRAINING COURSES
WORLD-CLASS TRAINERS
RED TEAM TRAINING COURSES
PENTESTER ACADEMY TOOL BOX PENTESTING

ATTACK DEFENSE

by PentesterAcademy

Name	DNS Enumeration
URL	https://attackdefense.com/challengedetails?cid=2019
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 IP address of the target machine is "192.211.79.3".

Step 2: Using nmap to scan the target machine.

Command: nmap 192.211.79.3

```
root@attackdefense:~# nmap 192.211.79.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-05 14:07 IST
Nmap scan report for public.witrap.com (192.211.79.3)
Host is up (0.000017s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 02:42:C0:D3:4F:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 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 DNSEnum tool to enumerate information on a domain and to discover non-contiguous IP blocks.

1. Using dnsenum tool to extract all the information for witrapper.com:

Command: dnsenum witrapper.com

```
root@attackdefense:~# dnsenum witrapper.com
dnsenum VERSION:1.2.6

-----  witrapper.com  -----

Host's addresses:

witrapp er.com.          900      IN      A      192.211.79.3

Name Servers:

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

Mail (MX) Servers:

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
```

Trying Zone Transfers and getting Bind Versions:

```
Trying Zone Transfer for witrapper.com on ns1.witrapper.com ...
witrapper.com.          900    IN   SOA      ( 
witrapper.com.          900    IN   RRSIG    ( 
witrapper.com.          900    IN   NS       ns1.witrapper.com. 
witrapper.com.          900    IN   NS       ns2.witrapper.com. 
witrapper.com.          900    IN   NS       ns3.witrapper.com. 
witrapper.com.          900    IN   RRSIG    ( 
witrapper.com.          900    IN   A        192.211.79.3 
witrapper.com.          900    IN   RRSIG    ( 
witrapper.com.          900    IN   MX      10 
witrapper.com.          900    IN   MX      20 
witrapper.com.          900    IN   MX      30 
witrapper.com.          900    IN   MX      40 
witrapper.com.          900    IN   MX      50 
witrapper.com.          900    IN   MX      60 
witrapper.com.          900    IN   MX      70 
witrapper.com.          900    IN   RRSIG    ( 
witrapper.com.          900    IN   TXT     ( 
witrapper.com.          900    IN   RRSIG    ( 
witrapper.com.          900    IN   AAAA    2001:db8::11:0:0:14 
witrapper.com.          900    IN   AAAA    2001:db8::11:0:0:15 
witrapper.com.          900    IN   AAAA    2001:db8::11:0:0:16 
witrapper.com.          900    IN   AAAA    2001:db8::11:0:0:17 
witrapper.com.          900    IN   AAAA    2001:db8::11:0:0:18 
witrapper.com.          900    IN   AAAA    2001:db8::11:0:0:19 
witrapper.com.          900    IN   AAAA    2001:db8::11:0:0:20 
witrapper.com.          900    IN   RRSIG    ( 
witrapper.com.          900    IN   DNSKEY  ( 
witrapper.com.          900    IN   DNSKEY  ( 

witrapper.com.          900    IN   RRSIG    ( 
witrapper.com.          900    IN   RRSIG    ( 
witrapper.com.          0     IN   NSEC3PARAM 1 
witrapper.com.          0     IN   RRSIG    ( 
witrapper.com.          900    IN   CAA      0 
witrapper.com.          900    IN   RRSIG    ( 
_kerberos._tcp.witrapper.com. 3600  IN   SRV     ( 
_kerberos._tcp.witrapper.com. 3600  IN   RRSIG    ( 
_kpasswd._tcp.witrapper.com. 3600  IN   SRV     ( 
_kpasswd._tcp.witrapper.com. 3600  IN   RRSIG    ( 
_ldap._tcp.witrapper.com.   3600  IN   SRV     10 
_ldap._tcp.witrapper.com.   3600  IN   RRSIG    ( 
_sip._tcp.witrapper.com.   3600  IN   SRV     10 
_sip._tcp.witrapper.com.   3600  IN   SRV     10 
_sip._tcp.witrapper.com.   3600  IN   SRV     10 
_sip._tcp.witrapper.com.   3600  IN   SRV     ( 
_sip._tcp.witrapper.com.   3600  IN   RRSIG    ( 
_smb._tcp.witrapper.com.   3600  IN   SRV     10 
_smb._tcp.witrapper.com.   3600  IN   RRSIG    ( 
_kerberos._udp.witrapper.com. 3600  IN   SRV     ( 
_kerberos._udp.witrapper.com. 3600  IN   RRSIG    ( 
_kpasswd._udp.witrapper.com. 3600  IN   SRV     ( 
```

_kpasswd._udp.witrapper.com.	3600	IN	RRSIG	(
_smb._udp.witrapper.com.	3600	IN	SRV	10
_smb._udp.witrapper.com.	3600	IN	RRSIG	(
admin.witrapper.com.	900	IN	A	192.211.79.101
admin.witrapper.com.	900	IN	RRSIG	(
mx5.ap.witrapper.com.	900	IN	A	192.211.79.49
mx5.ap.witrapper.com.	900	IN	RRSIG	(
dev.witrapper.com.	900	IN	CNAME	secondary.witrap.com.
dev.witrapper.com.	900	IN	RRSIG	(
free.witrapper.com.	900	IN	A	192.211.79.210
free.witrapper.com.	900	IN	RRSIG	(
internal.witrapper.com.	900	IN	A	192.211.79.100
internal.witrapper.com.	900	IN	RRSIG	(
ad01.krbauth.witrapper.com.	900	IN	A	192.211.79.26
ad01.krbauth.witrapper.com.	900	IN	RRSIG	(
ldap.witrapper.com.	900	IN	A	192.211.79.213
ldap.witrapper.com.	900	IN	RRSIG	(
ns1.witrapper.com.	900	IN	A	192.211.79.3
ns1.witrapper.com.	900	IN	RRSIG	(
ns2.witrapper.com.	900	IN	A	192.211.79.3
ns2.witrapper.com.	900	IN	RRSIG	(
ns3.witrapper.com.	900	IN	A	192.211.79.3
ns3.witrapper.com.	900	IN	RRSIG	(
open.witrapper.com.	900	IN	CNAME	free.witrap.com.
open.witrapper.com.	900	IN	RRSIG	(
primary.witrapper.com.	900	IN	A	192.211.79.211
primary.witrapper.com.	900	IN	RRSIG	(
prod.witrapper.com.	900	IN	CNAME	primary.witrap.com.
prod.witrapper.com.	900	IN	RRSIG	(
promo.witrapper.com.	900	IN	A	192.211.79.31
promo.witrapper.com.	900	IN	RRSIG	(
public.witrapper.com.	900	IN	A	192.211.79.30
public.witrapper.com.	900	IN	RRSIG	(
reserved.witrapper.com.	900	IN	A	192.211.79.214
reserved.witrapper.com.	900	IN	RRSIG	(
rsvd.witrapper.com.	900	IN	CNAME	reserved.witrap.com.
rsvd.witrapper.com.	900	IN	RRSIG	(
mx6.ru.witrapper.com.	900	IN	A	192.211.79.50
mx6.ru.witrapper.com.	900	IN	RRSIG	(
s3cr3tR3c0rd.witrapper.com.	900	IN	CNAME	secr3tAr3c0rd.witrap.com.
s3cr3tR3c0rd.witrapper.com.	900	IN	RRSIG	(
secondary.witrapper.com.	900	IN	A	192.211.79.212
secondary.witrapper.com.	900	IN	RRSIG	(
secr3tAr3c0rd.witrapper.com.	900	IN	A	192.211.79.225
secr3tAr3c0rd.witrapper.com.	900	IN	RRSIG	(
secr3tAr3c0rd.witrapper.com.	900	IN	TXT	Th!s_w4s_Th3_Secret_TXT_R3c0rd!
secr3tAr3c0rd.witrapper.com.	900	IN	RRSIG	(
mx2.sg.witrapper.com.	900	IN	A	192.211.79.46
mx2.sg.witrapper.com.	900	IN	RRSIG	(
mx3.sg.witrapper.com.	900	IN	A	192.211.79.47
mx3.sg.witrapper.com.	900	IN	RRSIG	(
sipserver.sg.witrapper.com.	900	IN	A	192.211.79.23
sipserver.sg.witrapper.com.	900	IN	RRSIG	(
sipserver.witrapper.com.	900	IN	A	192.211.79.22
sipserver.witrapper.com.	900	IN	RRSIG	(
smb.witrapper.com.	900	IN	A	192.211.79.21
smb.witrapper.com.	900	IN	RRSIG	(
mx4.ua.witrapper.com.	900	IN	A	192.211.79.48
mx4.ua.witrapper.com.	900	IN	RRSIG	(
mx7.uk.witrapper.com.	900	IN	A	192.211.79.51

sipserver.us.witrapper.com.	900	IN	A	192.211.79.24
sipserver.us.witrapper.com.	900	IN	RRSIG	(
09G8ANR8NVBP8RB7F4KRU6J0I2VJM8P4.witrapper.com.	900	IN	NSEC3	(
09G8ANR8NVBP8RB7F4KRU6J0I2VJM8P4.witrapper.com.	900	IN	RRSIG	(
18REFI29QTGLSGJJ4DSDHT24MC6SM4ES.witrapper.com.	900	IN	NSEC3	(
18REFI29QTGLSGJJ4DSDHT24MC6SM4ES.witrapper.com.	900	IN	RRSIG	(
1HVKUB0GPCJF0NN699FL466K4TFPJSPF.witrapper.com.	900	IN	NSEC3	(
1HVKUB0GPCJF0NN699FL466K4TFPJSPF.witrapper.com.	900	IN	RRSIG	(
1TL6PS38VES9VHPGF6GAKJR3D088ADJ9.witrapper.com.	900	IN	NSEC3	(
1TL6PS38VES9VHPGF6GAKJR3D088ADJ9.witrapper.com.	900	IN	RRSIG	(
2B0MDLCH05U3FMIE0SVEB206P88595K8.witrapper.com.	900	IN	NSEC3	(
2B0MDLCH05U3FMIE0SVEB206P88595K8.witrapper.com.	900	IN	RRSIG	(
3N12A78Q98HDAFKQ0HTUMRCPCOL25JRL.witrapper.com.	900	IN	NSEC3	(
3N12A78Q98HDAFKQ0HTUMRCPCOL25JRL.witrapper.com.	900	IN	RRSIG	(
3N71IUJ10PMKMFQ9S4RGRC6GE3SCH68F.witrapper.com.	900	IN	NSEC3	(
3N71IUJ10PMKMFQ9S4RGRC6GE3SCH68F.witrapper.com.	900	IN	RRSIG	(
438CQF00AVQ5KGQR0GA7U108ML57UVV6.witrapper.com.	900	IN	NSEC3	(
438CQF00AVQ5KGQR0GA7U108ML57UVV6.witrapper.com.	900	IN	RRSIG	(
59UA6V2A63RCP0G4H72GRHFA9F0JM7GG.witrapper.com.	900	IN	NSEC3	(
59UA6V2A63RCP0G4H72GRHFA9F0JM7GG.witrapper.com.	900	IN	RRSIG	(
6J7LEJG0ARQUR66R19RBR7RQQR64JD40.witrapper.com.	900	IN	NSEC3	(
6J7LEJG0ARQUR66R19RBR7RQQR64JD40.witrapper.com.	900	IN	RRSIG	(
71BE76LT3018E33K00G8S6GL3EL5BMJB.witrapper.com.	900	IN	NSEC3	(
71BE76LT3018E33K00G8S6GL3EL5BMJB.witrapper.com.	900	IN	RRSIG	(
8EBQR0053V10HHUBFU7SVV5DPH3F51PS.witrapper.com.	900	IN	NSEC3	(
8EBQR0053V10HHUBFU7SVV5DPH3F51PS.witrapper.com.	900	IN	RRSIG	(
8HQCI7LPALT3C98AA61QPHF70LM6571R.witrapper.com.	900	IN	NSEC3	(
8HQCI7LPALT3C98AA61QPHF70LM6571R.witrapper.com.	900	IN	RRSIG	(
PQ1A8G0H61BIETRF6CRKM2SQL2G9J10.witrapper.com.	900	IN	NSEC3	(
PQ1A8G0H61BIETRF6CRKM2SQL2G9J10.witrapper.com.	900	IN	RRSIG	(
RLP1C05S6GT7Q4LMNU2GKVJL4423QUJJ.witrapper.com.	900	IN	NSEC3	(
RLP1C05S6GT7Q4LMNU2GKVJL4423QUJJ.witrapper.com.	900	IN	RRSIG	(
RP2K9U4S2QSA8HC56VK7QDT7U4AD85J3.witrapper.com.	900	IN	NSEC3	(
RP2K9U4S2QSA8HC56VK7QDT7U4AD85J3.witrapper.com.	900	IN	RRSIG	(
S07RBLLSC160R54G0B09MTPP4RIGNENG.witrapper.com.	900	IN	NSEC3	(
S07RBLLSC160R54G0B09MTPP4RIGNENG.witrapper.com.	900	IN	RRSIG	(
T1FFV874749BEAVESNOKRGH0MV5REDTP.witrapper.com.	900	IN	NSEC3	(
T1FFV874749BEAVESNOKRGH0MV5REDTP.witrapper.com.	900	IN	RRSIG	(
V25G33Q0B7R96VBMGQADG3J9191UE1S2.witrapper.com.	900	IN	NSEC3	(
V25G33Q0B7R96VBMGQADG3J9191UE1S2.witrapper.com.	900	IN	RRSIG	(
VIK09DPV84862LT265D62AQ794JNTAOS.witrapper.com.	900	IN	NSEC3	(
VIK09DPV84862LT265D62AQ794JNTAOS.witrapper.com.	900	IN	RRSIG	(
Trying Zone Transfer for witrapper.com on ns3.witrapper.com ...				
witrapper.com.	900	IN	SOA	(
witrapper.com.	900	IN	RRSIG	(
witrapper.com.	900	IN	NS	ns1.witrapper.com.
witrapper.com.	900	IN	NS	ns2.witrapper.com.
witrapper.com.	900	IN	NS	ns3.witrapper.com.
witrapper.com.	900	IN	RRSIG	(
witrapper.com.	900	IN	A	192.211.79.3
witrapper.com.	900	IN	RRSIG	(
witrapper.com.	900	IN	MX	10
witrapper.com.	900	IN	MX	20

```

Trying Zone Transfer for witrapper.com on ns2.witrapper.com ...
witrapper.com.          900   IN  SOA      ( 
witrapper.com.          900   IN  RRSIG    ( 
witrapper.com.          900   IN  NS       ns1.witrapper.com. 
witrapper.com.          900   IN  NS       ns2.witrapper.com. 
witrapper.com.          900   IN  NS       ns3.witrapper.com. 
witrapper.com.          900   IN  RRSIG    ( 
witrapper.com.          900   IN  A        192.211.79.3 
witrapper.com.          900   IN  RRSIG    ( 
witrapper.com.          900   IN  MX      10 
witrapper.com.          900   IN  MX      20 
witrapper.com.          900   IN  MX      30 
witrapper.com.          900   IN  MX      40 
witrapper.com.          900   IN  MX      50 
witrapper.com.          900   IN  MX      60 
witrapper.com.          900   IN  MX      70 
witrapper.com.          900   IN  RRSIG    ( 
witrapper.com.          900   IN  TXT     ( 
witrapper.com.          900   IN  RRSIG    ( 
witrapper.com.          900   IN  AAAA    2001:db8::11:0:0:14 
witrapper.com.          900   IN  AAAA    2001:db8::11:0:0:15 
witrapper.com.          900   IN  AAAA    2001:db8::11:0:0:16 
witrapper.com.          900   IN  AAAA    2001:db8::11:0:0:17 
witrapper.com.          900   IN  AAAA    2001:db8::11:0:0:18 
witrapper.com.          900   IN  AAAA    2001:db8::11:0:0:19 
witrapper.com.          900   IN  AAAA    2001:db8::11:0:0:20

```

Brute forcing with /usr/share/dnsenum/dns.txt:

witrapper.com class C netranges:

192.211.79.0/24

Performing reverse lookup on 256 ip addresses:

3.79.211.192.in-addr.arpa.	900	IN	PTR	ns1.witrapper.com.
3.79.211.192.in-addr.arpa.	900	IN	PTR	ns3.witrapper.com.
3.79.211.192.in-addr.arpa.	900	IN	PTR	ns2.witrapper.com.
21.79.211.192.in-addr.arpa.	900	IN	PTR	smb.witrapper.com.
22.79.211.192.in-addr.arpa.	900	IN	PTR	sipserver.witrapper.com.
23.79.211.192.in-addr.arpa.	900	IN	PTR	sipserver.sg.witrapper.com.
24.79.211.192.in-addr.arpa.	900	IN	PTR	sipserver.us.witrapper.com.
25.79.211.192.in-addr.arpa.	900	IN	PTR	backupsipserver.us.witrapper.com.
26.79.211.192.in-addr.arpa.	900	IN	PTR	ad01.krbauth.witrapper.com.
30.79.211.192.in-addr.arpa.	900	IN	PTR	public.witrapper.com.
31.79.211.192.in-addr.arpa.	900	IN	PTR	promo.witrapper.com.
45.79.211.192.in-addr.arpa.	900	IN	PTR	mx1.us.witrapper.com.
46.79.211.192.in-addr.arpa.	900	IN	PTR	mx2.sg.witrapper.com.
47.79.211.192.in-addr.arpa.	900	IN	PTR	mx3.sg.witrapper.com.
48.79.211.192.in-addr.arpa.	900	IN	PTR	mx4.ua.witrapper.com.
49.79.211.192.in-addr.arpa.	900	IN	PTR	mx5.ap.witrapper.com.
50.79.211.192.in-addr.arpa.	900	IN	PTR	mx6.ru.witrapper.com.
51.79.211.192.in-addr.arpa.	900	IN	PTR	mx7.uk.witrapper.com.
100.79.211.192.in-addr.arpa.	900	IN	PTR	internal.witrapper.com.

```
101.79.211.192.in-addr.arpa.          900      IN      PTR      admin.witrapper.com.  
18 results out of 256 IP addresses.  
  
witrapper.com ip blocks:  
  
192.211.79.3/32  
192.211.79.21/32  
192.211.79.22/31  
192.211.79.24/31  
192.211.79.26/32  
192.211.79.30/31  
192.211.79.45/32  
192.211.79.46/31  
192.211.79.48/30  
192.211.79.100/31  
  
done.  
root@attackdefense:~#
```

The output above extracts a lot of information on the resource records from witrapper.com:

The IP blocks used by witrapper.com, the reverse lookup mapping, NSEC3, A, MX, SRV, CAA, LOC, AAAA, TXT, NS, SOA, etc records. It also performs zone transfer on the domain.

DNSEnum can also save the output into a file in XML format which could later be used by magictree.

Command: dnsenum witrap.com -o out.xml

```

root@attackdefense:~# dnsenum witrap.com -o out.xml
dnsenum VERSION:1.2.6

----- witrap.com -----

Host's addresses:

-----
witrap.com.          900      IN   A    192.211.79.3

Name Servers:

-----
ns1.witrapper.com.    900      IN   A    192.211.79.3
ns3.witrapper.com.    900      IN   A    192.211.79.3

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

Trying Zone Transfer for witrap.com on ns1.witrapper.com ...
witrap.com.          900      IN   SOA   (
witrap.com.          900      IN   MX    10
witrap.com.          900      IN   MX    20
witrap.com.          900      IN   TXT   "Welcome"
witrap.com.          900      IN   LOC   37
witrap.com.          900      IN   CAA   0
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.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.
promo.witrap.com.   900      IN   CNAME  promo.witrap.com.

```

Performing reverse lookup on 256 ip addresses:

3.79.211.192.in-addr.arpa.	900	IN	PTR	promo.witrap.com.
3.79.211.192.in-addr.arpa.	900	IN	PTR	public.witrap.com.
40.79.211.192.in-addr.arpa.	900	IN	PTR	training.witrap.com.
41.79.211.192.in-addr.arpa.	900	IN	PTR	admin.witrap.com.
42.79.211.192.in-addr.arpa.	900	IN	PTR	demo.witrap.com.
43.79.211.192.in-addr.arpa.	900	IN	PTR	info.witrap.com.
44.79.211.192.in-addr.arpa.	900	IN	PTR	stats.witrap.com.
200.79.211.192.in-addr.arpa.	900	IN	PTR	static.witrap.com.
201.79.211.192.in-addr.arpa.	900	IN	PTR	mx1.us.witrap.com.
				mx3.us.witrap.com.

8 results out of 256 IP addresses.

witrap.com ip blocks:

```
192.211.79.3/32
192.211.79.40/30
192.211.79.44/32
192.211.79.200/31
```

done.

```
root@attackdefense:~#
```

Checking the generated output:

Command: cat out.xml

```
root@attackdefense:~# cat out.xml
<?xml version="1.0" encoding="UTF-8"?>
<magictree class="MtBranchObject"><testdata class="MtBranchObject"><host>192.211.79.3<hostname>witrap.com</host><host>ns1.witrapper.com</hostname><fqdn>ns1.witrapper.com.</fqdn><host>192.211.79.3<hostname>ns3.witrapper.com</host><host>mx1.us.witrap.com</hostname><fqdn>mx1.us.witrap.com.</fqdn><host>192.211.79.201<hostname>mx1.us.witrap.com</host><fqdn>192.211.79.3<hostname>witrap.com</host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>192.211.79.3<hostname>witrap.com</host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><fqdn>admin.witrap.com.</fqdn><host>192.211.79.3<hostname>courses.witrap.com</host><fqdn>com</host><host><fqdn>demo.witrap.com.</fqdn><host>192.211.79.42<hostname>dev.witrap.com</host><fqdn>witrap.com</host><host><fqdn>info.witrap.com.</fqdn><host>192.211.79.3<hostname>labs.witrap.com</host><fqdn>promo.witrap.com</host><host><fqdn>promo.witrap.com.</fqdn><host>192.211.79.3<hostname>public.witrap.com</host><host>192.211.79.42<hostname>staging.witrap.com</host><fqdn>staging.witrap.com.</fqdn><host>192.211.79.44<host><fqdn>192.211.79.44<hostname>stats.witrap.com</host><host><fqdn>stats.witrap.com.</fqdn><host>192.211.79.44<host>aining.witrap.com.</fqdn><host>192.211.79.200<hostname>mx1.us.witrap.com</host><host><fqdn>mx1.us.witrap.com</host><host><fqdn>mx3.us.witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><host><fqdn>witrap.com.</fqdn><host>192.211.79.3<hostname>witrap.com</host><host><fqdn>admin.witrap.com.</fqdn><host>192.211.79.3<hostname>admin.witrap.com</host><host><fqdn>admin.witrap.com.</fqdn><host>192.211.79.3<hostname>courses.witrap.com</host><host>192.211.79.42<hostname>demo.witrap.com</host><host><fqdn>demo.witrap.com.</fqdn><host>192.211.79.42<host><fqdn>192.211.79.42<hostname>info.witrap.com</host><host><fqdn>info.witrap.com.</fqdn><host>192.211.79.42<host><fqdn>192.211.79.42<hostname>public.witrap.com</host><host>192.211.79.42<host><fqdn>public.witrap.com.</fqdn><host>192.211.79.42<host><fqdn>staging.witrap.com</host><host><fqdn>staging.witrap.com.</fqdn><host>192.211.79.42<host><fqdn>static.witrap.com.</fqdn><host>192.211.79.44<host><fqdn>stats.witrap.com</host><host><fqdn>witrap.com.</fqdn><host><fqdn>training.witrap.com.</fqdn><host>192.211.79.200<host>mx1.us.witrap.com
root@attackdefense:~#
```

Step 5: Using DNSRecon tool to enumerate various DNS records for a target domain.

1. Using dnsrecon tool to extract all the information for witrapper.com:

Command: dnsrecon -d witrapper.com

```

root@attackdefense:~# dnsrecon -d witrapper.com
[*] Performing General Enumeration of Domain: witrapper.com
[*] DNSSEC is configured for witrapper.com
[*] DNSKEYs:
[*] NSEC3 KSK RSASHA1NSEC3SHA1 03010001a493ac004ba56470b05fe9ff 2cc2ebce1c90b9c85e9f679cec9fd5dd f39d6dd2802beced5041b9d60b0025bd dd
f7408cb47aecd37289fdf4c803a696 36c0a9150a7cc5f5da1908553d68451f 8d4a7c643f6e8293ba063e6776261f1f 711ab21424d5079a689de6826f9da965 e830f7
cff252ba5e6a60853fb04c6ab5 8a353652b6b9842ddecc772b8c4f807e 40164d4a8cf946595b502fdb65e2631a 486214937087510fe4a87d7a5292570a 7826e27b8a
90e2560f8109f77f6588fa fa9799f23e36b7e86e48e12a12f5ac00 ef078fb7a4ee2ce29dd5438a2c76e72c dac158e6a4de7b40dcdbd14690730c00 0e1c20f3e3b0f4
e15b76bd3b5b755522 329be3541b7aeae9d9be374dde8e358a e05bd9df14e9b83c6b741b83c28ec5cb f7374ba543199e49a3e05b367c919457 693c076e987e256f83
9f0314e88916ef 4fea32526d804f822c7f08b69b1628be 3663afc13eb779f3c2b3a3196186356f 3aca34a6a8086ee9e682933952f1b2f9 aba6b60abe12efbe2e063d
f97656e699 976ad4043997bf274a2261e756cf7847 7f0bf7441b2b1d5416a127ce84c42f79 2cf5db9dfa71d558ea31cd7329db9e1 881d93ea37878188e6023e986a
200a84 15a57568f87de19291338d1c3d5218e7 6de4d43813a851e4ff4106d92c95f647 1ac642faebced9a0dbf0f1fd6eff6bb2 31535f0a9942ab2252c7530b31a84f
9e e47020a3
[*] NSEC3 ZSK RSASHA1NSEC3SHA1 03010001d56dbb52755b40ca9558fc65 71daf5b5fcfd2aeeeaf0073c4e47e6dfb8 2fdce848e551941ad1c1fc71dcf9ef71 64
d72193d191d1c5ecde725b8206c977 425c7b6f6aed2211c6ba00d366dfe2e6 c5646aa520187f00327f1e9f646166f8 aef1fd4099f264947ed8e825e6cb41fd 27ef6d
5a48c475e791089bfe002e2ed4 882347dd239e03bb5f4cd7f903091561 6da3b1c8b53b89ec007128a20bfc4b86 7557918c7b790dc525d9682c02b504ab 23dbca01ed
ababa276742e7a753d20d1 c5c776fde38938275f2e8af4516124fe c4f443684262be1d2c0bb3b474d0da85 5b4ca034bee86f6e805dfc918a562802 0f598ceedb2deb
d2a4e7f940dc37d81a 7b22f9ff
[*] NS ns2.witrapper.com 192.211.79.3
[*] Bind Version for 192.211.79.3 9.11.3-1ubuntu1.12-Ubuntu
[*] NS ns1.witrapper.com 192.211.79.3
[*] Bind Version for 192.211.79.3 9.11.3-1ubuntu1.12-Ubuntu
[*] NS ns3.witrapper.com 192.211.79.3
[*] Bind Version for 192.211.79.3 9.11.3-1ubuntu1.12-Ubuntu
[*] MX mx2.sg.witrapper.com 192.211.79.46
[*] MX mx1.us.witrapper.com 192.211.79.45
[*] MX mx7.uk.witrapper.com 192.211.79.51
[*] MX mx3.sg.witrapper.com 192.211.79.47
[*] MX mx4.ua.witrapper.com 192.211.79.48
[*] MX mx6.ru.witrapper.com 192.211.79.50
[*] MX mx5.ap.witrapper.com 192.211.79.49
[*] A witrapper.com 192.211.79.3
[*] AAAA witrapper.com 2001:db8::11:0:0:18
[*] AAAA witrapper.com 2001:db8::11:0:0:16
[*] AAAA witrapper.com 2001:db8::11:0:0:19
[*] AAAA witrapper.com 2001:db8::11:0:0:17
[*] AAAA witrapper.com 2001:db8::11:0:0:15
[*] AAAA witrapper.com 2001:db8::11:0:0:20
[*] AAAA witrapper.com 2001:db8::11:0:0:14
[*] TXT witrapper.com Welcome to Witrapper.com - the parent company of witrap :)
[*] Enumerating SRV Records
[*] SRV _kerberos._tcp.witrapper.com ad01.krbauth.witrapper.com 192.211.79.26 88 10
[*] SRV _ldap._tcp.witrapper.com ldap.witrapper.com 192.211.79.213 389 10
[*] SRV _kerberos._udp.witrapper.com ad01.krbauth.witrapper.com 192.211.79.26 88 10
[*] SRV _sip._tcp.witrapper.com backupsipserver.us.witrapper.com 192.211.79.25 5060 0
[*] SRV _sip._tcp.witrapper.com sipserver.us.witrapper.com 192.211.79.24 5060 10
[*] SRV _sip._tcp.witrapper.com sipserver.witrapper.com 192.211.79.22 5060 2
[*] SRV _sip._tcp.witrapper.com sipserver.sg.witrapper.com 192.211.79.23 5060 7
[*] SRV _kpasswd._tcp.witrapper.com ad01.krbauth.witrapper.com 192.211.79.26 464 10
[*] SRV _kpasswd._udp.witrapper.com ad01.krbauth.witrapper.com 192.211.79.26 464 10
[+] 9 Records Found
root@attackdefense:~#

```

Notice that DNSSEC is enabled for witrapper.com

2. Performing an AXFR query with standard enumeration on witrap.com:

Command: dnsrecon -d witrap.com -a

```
root@attackdefense:~# dnsrecon -d witrap.com -a
[*] Performing General Enumeration of Domain: witrap.com
[*] Checking for Zone Transfer for witrap.com name servers
[*] Resolving SOA Record
[*] Resolving NS Records
[*] NS Servers found:
[*]   NS ns1.witrapp.com 192.211.79.3
[*]   NS ns3.witrapp.com 192.211.79.3
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 192.211.79.3
[+] 192.211.79.3 Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]   SOA ns1.witrapp.com 192.211.79.3
[*]   NS ns1.witrapp.com 192.211.79.3
[*]   NS ns3.witrapp.com 192.211.79.3
[*]   TXT Welcome to Witrap.com!
[*]   AAAA @.witrap.com 2001:db8::11:0:0:11
[*]   A @.witrap.com 192.211.79.3
[*]   A admin.witrap.com 192.211.79.41
[*]   A training.witrap.com 192.211.79.40
[*]   A mx1.us.witrap.com 192.211.79.200
[*]   A public.witrap.com 192.211.79.3
[*]   A mx3.us.witrap.com 192.211.79.201
[*]   A info.witrap.com 192.211.79.43
[*]   A static.witrap.com 192.211.79.44
[*]   A demo.witrap.com 192.211.79.42
[*]   A stats.witrap.com 192.211.79.44
[*]   CNAME labs.witrap.com witrapp.com. 192.211.79.3
[*]   CNAME labs.witrap.com witrapp.com. 2001:db8::11:0:0:19
[*]   CNAME labs.witrap.com witrapp.com. 2001:db8::11:0:0:17
[*]   CNAME labs.witrap.com witrapp.com. 2001:db8::11:0:0:16
[*]   CNAME labs.witrap.com witrapp.com. 2001:db8::11:0:0:20
[*]   CNAME labs.witrap.com witrapp.com. 2001:db8::11:0:0:14
[*]   CNAME labs.witrap.com witrapp.com. 2001:db8::11:0:0:15
[*]   CNAME labs.witrap.com witrapp.com. 2001:db8::11:0:0:18
[*] LOC 37 46 29.744 N 122 25 9.904 W 32.00m
```

```

[*] A info.witrap.com 192.211.79.43
[*] A static.witrap.com 192.211.79.44
[*] A demo.witrap.com 192.211.79.42
[*] A stats.witrap.com 192.211.79.44
[*] CNAME labs.witrap.com witrapper.com. 192.211.79.3
[*] CNAME labs.witrap.com witrapper.com. 2001:db8::11:0:0:17
[*] CNAME labs.witrap.com witrapper.com. 2001:db8::11:0:0:19
[*] CNAME labs.witrap.com witrapper.com. 2001:db8::11:0:0:15
[*] CNAME labs.witrap.com witrapper.com. 2001:db8::11:0:0:18
[*] CNAME labs.witrap.com witrapper.com. 2001:db8::11:0:0:20
[*] CNAME labs.witrap.com witrapper.com. 2001:db8::11:0:0:16
[*] CNAME labs.witrap.com witrapper.com. 2001:db8::11:0:0:14
[*] LOC 37 46 29.744 N 122 25 9.904 W 32.00m
[-] DNSSEC is not configured for witrap.com
[*] NS ns3.witrapper.com 192.211.79.3
[*] Bind Version for 192.211.79.3 9.11.3-1ubuntu1.12-Ubuntu
[*] NS ns1.witrapper.com 192.211.79.3
[*] Bind Version for 192.211.79.3 9.11.3-1ubuntu1.12-Ubuntu
[*] MX mx3.us.witrap.com 192.211.79.201
[*] MX mx1.us.witrap.com 192.211.79.200
[*] A witrap.com 192.211.79.3
[*] AAAA witrap.com 2001:db8::11:0:0:11
[*] TXT witrap.com Welcome to Witrap.com!
[*] Enumerating SRV Records
[-] No SRV Records Found for witrap.com
[+] 0 Records Found
root@attackdefense:~#

```

Notice that the tool performed zone transfer for witrap.com. It had also determined the version of Bind server - 9.11.3-ubuntu1.12-Ubuntu.

Information: Berkeley Internet Name Domain (BIND) is the most popular Domain Name System (DNS) server in use today. BIND can be used to run a caching DNS server or an authoritative name server, and provides features like load balancing, notify, dynamic update, split DNS, DNSSEC, IPv6, and more.

3. Performing an AXFR query with standard enumeration on promo.witrap.com and saving the output in JSON format:

Command: dsnrecon -d promo.witrap.com -a -j ~/out.json

```
root@attackdefense:~# dnsrecon -d promo.witrap.com -a -j ~/out.json
[*] Performing General Enumeration of Domain: promo.witrap.com
[*] Checking for Zone Transfer for promo.witrap.com name servers
[*] Resolving SOA Record
[*] Resolving NS Records
[*] NS Servers found:
    NS ns1.witrapper.com 192.211.79.3
    NS ns3.witrapper.com 192.211.79.3
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 192.211.79.3
[+] 192.211.79.3 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] Zone transfer error: REFUSED
[*] Checking for Zone Transfer for promo.witrap.com name servers
[*] Resolving SOA Record
[*] Resolving NS Records
[*] NS Servers found:
    NS ns3.witrapper.com 192.211.79.3
    NS ns1.witrapper.com 192.211.79.3
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 192.211.79.3
[+] 192.211.79.3 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] Zone transfer error: REFUSED
[-] DNSSEC is not configured for promo.witrap.com
    NS ns1.witrapper.com 192.211.79.3
    Bind Version for 192.211.79.3 9.11.3-1ubuntu1.12-Ubuntu
    NS ns3.witrapper.com 192.211.79.3
    Bind Version for 192.211.79.3 9.11.3-1ubuntu1.12-Ubuntu
[-] Could not Resolve MX Records for promo.witrap.com
    A promo.witrap.com 192.211.79.3
    AAAA promo.witrap.com 2001:db8::11:0:0:36
    TXT promo.witrap.com thls_!s_4_TXT_R3c0rd
[*] Enumerating SRV Records
[-] No SRV Records Found for promo.witrap.com
[+] 0 Records Found
[*] Saving records to JSON file: /root/out.json
root@attackdefense:~#
```

Checking the generated output:

Command: cat out.json

```
root@attackdefense:~# cat out.json
[
    {
        "arguments": "./dnsrecon.py -d promo.witrap.com -a -j /root/out.json",
        "date": "2020-08-08 13:28:49.014469",
        "type": "ScanInfo"
    },
    {
        "ns_server": "192.211.79.3",
        "type": "info",
        "zone_transfer": "failed"
    },
    {
        "Version": "9.11.3-1ubuntu1.12-Ubuntu",
        "address": "192.211.79.3",
        "recursive": "True",
        "target": "ns1.witrapper.com",
        "type": "NS"
    },
    {
        "Version": "9.11.3-1ubuntu1.12-Ubuntu",
        "address": "192.211.79.3",
        "recursive": "True",
        "target": "ns3.witrapper.com",
        "type": "NS"
    },
    {
        "address": "192.211.79.3",
        "name": "promo.witrap.com",
        "type": "A"
    },
    {
        "address": "2001:db8::11:0:0:36",
        "name": "promo.witrap.com",
        "type": "AAAA"
    },
    {
        "name": "promo.witrap.com",
        "strings": "thls_!s_4_TXT_R3c0rd",
        "type": "TXT"
    }
]
root@attackdefense:~#
```

Note: If a file name was given as out.json (without ~/) the output would be saved inside the directory for dnsrecon: /usr/share/dnsrecon/

Step 6: Using the DNS Record Scanner and Enumerator auxiliary module to scan the target DNS server.

Auxiliary Module: auxiliary/gather/enum_dns

Scanning and enumeration DNS records for witrap.com:

Commands:

```
msfconsole -q
use auxiliary/gather/enum_dns
setg NS 192.211.79.3
set DOMAIN witrap.com
run
```

```
root@attackdefense:~# msfconsole -q
msf6 > use auxiliary/gather/enum_dns
msf6 auxiliary(gather/enum_dns) > setg NS 192.211.79.3
NS => 192.211.79.3
msf6 auxiliary(gather/enum_dns) > set DOMAIN witrap.com
DOMAIN => witrap.com
msf6 auxiliary(gather/enum_dns) > run

[*] Querying DNS NS records for witrap.com
[+] witrap.com NS: ns3.witrapper.com
[+] witrap.com NS: ns1.witrapper.com
[*] Attempting DNS AXFR for witrap.com from ns3.witrapper.com
W, [2020-10-08T18:27:40.358260 #1208]  WARN -- : Failed to parse RR packet from offset: 162
W, [2020-10-08T18:27:40.358363 #1208]  WARN -- : Failed to parse RR packet from offset: 190
W, [2020-10-08T18:28:10.360144 #1208]  WARN -- : Failed to parse RR packet from offset: 162
W, [2020-10-08T18:28:10.360270 #1208]  WARN -- : Failed to parse RR packet from offset: 190
[+] witrap.com Zone Transfer: [;; Answer received from 192.211.79.3:53 (627 bytes)
;;
;; HEADER SECTION
;; id = 20347
;; qr = 1      opCode: QUERY    aa = 1  tc = 0  rd = 0
;; ra = 0      ad = 0  cd = 0  rcode = NoError
;; qdCount = 1  anCount = 25    nsCount = 0     arCount = 0

;; QUESTION SECTION (1 record):
;; witrap.com.          IN      AXFR

;; ANSWER SECTION (25 records):
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
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.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.
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
]
[*] Attempting DNS AXFR for witrap.com from ns1.witrapper.com
W, [2020-10-08T18:06:11.755682 #572] WARN -- : Failed to parse RR packet from offset: 162
W, [2020-10-08T18:06:11.755782 #572] WARN -- : Failed to parse RR packet from offset: 190
W, [2020-10-08T18:06:41.757840 #572] WARN -- : Failed to parse RR packet from offset: 162
W, [2020-10-08T18:06:41.757965 #572] WARN -- : Failed to parse RR packet from offset: 190
[+] witrap.com Zone Transfer: [;; Answer received from 192.211.79.3:53 (627 bytes)
;;
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
]
[*] Querying DNS CNAME records for witrap.com
[*] Querying DNS NS records for witrap.com
[+] witrap.com NS: ns1.witrapper.com
[+] witrap.com NS: ns3.witrapper.com
[*] Querying DNS MX records for witrap.com
[+] witrap.com MX: mx3.us.witrap.com
[+] witrap.com MX: mx1.us.witrap.com
[*] Querying DNS SOA records for witrap.com
[+] witrap.com SOA: ns1.witrapper.com
[*] Querying DNS TXT records for witrap.com
[+] witrap.com TXT: Welcome to Witrap.com!
[*] Querying DNS SRV records for witrap.com
[*] Auxiliary module execution completed
msf6 auxiliary(gather/enum_dns) >

```

Various records like: NS, MX, SOA, TXT, SRV for witrap.com were retrieved from the target DNS server.

Running the same module for witrapper.com:

```
msf6 auxiliary(gather/enum_dns) > set DOMAIN witrapper.com
DOMAIN => witrapper.com
msf6 auxiliary(gather/enum_dns) > run

[*] Querying DNS NS records for witrapper.com
[+] witrapper.com NS: ns1.witrapper.com
[+] witrapper.com NS: ns2.witrapper.com
[+] witrapper.com NS: ns3.witrapper.com
[*] Attempting DNS AXFR for witrapper.com from ns1.witrapper.com
W, [2020-10-08T18:13:05.495297 #572]  WARN -- : Failed to parse RR packet from offset: 77
W, [2020-10-08T18:13:05.495777 #572]  WARN -- : Failed to parse RR packet from offset: 428
W, [2020-10-08T18:13:05.496015 #572]  WARN -- : Failed to parse RR packet from offset: 745
W, [2020-10-08T18:13:05.496863 #572]  WARN -- : Failed to parse RR packet from offset: 1204
W, [2020-10-08T18:13:05.497087 #572]  WARN -- : Failed to parse RR packet from offset: 1576
W, [2020-10-08T18:13:05.498445 #572]  WARN -- : Failed to parse RR packet from offset: 2073
W, [2020-10-08T18:13:05.498542 #572]  WARN -- : Failed to parse RR packet from offset: 2374

[*] Querying DNS CNAME records for witrapper.com
[*] Querying DNS NS records for witrapper.com
[+] witrapper.com NS: ns3.witrapper.com
[+] witrapper.com NS: ns1.witrapper.com
[+] witrapper.com NS: ns2.witrapper.com
[*] Querying DNS MX records for witrapper.com
[+] witrapper.com MX: mx2.sg.witrapper.com
[+] witrapper.com MX: mx1.us.witrapper.com
[+] witrapper.com MX: mx7.uk.witrapper.com
[+] witrapper.com MX: mx4.ua.witrapper.com
[+] witrapper.com MX: mx5.ap.witrapper.com
[+] witrapper.com MX: mx6.ru.witrapper.com
[+] witrapper.com MX: mx3.sg.witrapper.com
[*] Querying DNS SOA records for witrapper.com
[+] witrapper.com SOA: ns1.witrapper.com
[*] Querying DNS TXT records for witrapper.com
[+] witrapper.com TXT: Welcome to Witrapper.com - the parent company of witrap :)
[*] Querying DNS SRV records for witrapper.com
[+] _kerberos._tcp.witrapper.com SRV: {:host=>"_kerberos._tcp.witrapper.com", :port=>88, :priority=>10}
[+] _kerberos._udp.witrapper.com SRV: {:host=>"_kerberos._udp.witrapper.com", :port=>88, :priority=>10}
[+] _ldap._tcp.witrapper.com SRV: {:host=>"_ldap._tcp.witrapper.com", :port=>389, :priority=>10}
[+] _sip._tcp.witrapper.com SRV: {:host=>"_sip._tcp.witrapper.com", :port=>5060, :priority=>10}
[+] _sip._tcp.witrapper.com SRV: {:host=>"_sip._tcp.witrapper.com", :port=>5060, :priority=>20}
[+] _sip._tcp.witrapper.com SRV: {:host=>"_sip._tcp.witrapper.com", :port=>5060, :priority=>10}
[+] _sip._tcp.witrapper.com SRV: {:host=>"_sip._tcp.witrapper.com", :port=>5060, :priority=>10}
[*] Auxiliary module execution completed
msf6 auxiliary(gather/enum_dns) >
```

Various records like: NS, MX, SOA, TXT, SRV for witrapper.com were retrieved from the target DNS server.

In the TXT record, it is mentioned that witrapper.com is the parent company of witrap.

Note: There are some warnings shown while running the module, this is where Metasploit does not recognise some of the record types returned by the server. This is particularly noticeable on witreapper.com where it does not know about the DNSSEC records. This shows that it is good not to rely on a single tool or, if you have to, then to know its limitations.

Bruteforcing subdomains and hostnames via the supplied wordlist:

Commands:

```
show options  
set ENUM_BRT true  
set DOMAIN witrapper.com  
run
```

Module options (auxiliary/gather/enum_dns):		Required	Description
Name	Current Setting	-----	-----
DOMAIN	witrapper.com	yes	The target domain
ENUM_A	true	yes	Enumerate DNS A records
ENUM_AXFR	true	yes	Initiate a zone transfer
ENUM_BRT	false	yes	Brute force subdomains
upplied wordlist			
ENUM_CNAME	true	yes	Enumerate DNS CNAME records
ENUM_MX	true	yes	Enumerate DNS MX records
ENUM_NS	true	yes	Enumerate DNS NS records
ENUM_RVL	false	yes	Reverse lookup
ENUM_SOA	true	yes	Enumerate DNS SOA records
ENUM_SRV	true	yes	Enumerate the SRV records
ENUM_TLD	false	yes	Perform a TLD search
ith the IANA TLD list			
ENUM_TXT	true	yes	Enumerate DNS TXT records
IPRANGE		no	The target address range
NS	192.211.79.3	no	Specify the nameserver
ace separated		no	
Proxies		no	A proxy chain
ost:port][...]			
RPORT	53	yes	The target port
SEARCHLIST		no	DNS domain search list
STOP_WLDCRD	false	yes	Stops brutefor
ution is detected			
THREADS	1	no	Threads for ENUM
WORDLIST	/opt/metasploit-framework/embedded/framework/data/wordlists/namelist.txt	no	Wordlist of subdomains

Default password list file: /usr/share/metasploit-framework/data/wordlists/namelist.txt

```

msf6 auxiliary(gather/enum_dns) > set ENUM_BRT true
ENUM_BRT => true
msf6 auxiliary(gather/enum_dns) > set DOMAIN witrapper.com
DOMAIN => witrapper.com
msf6 auxiliary(gather/enum_dns) > run

[*] Querying DNS NS records for witrapper.com
[+] witrapper.com NS: ns3.witrapper.com
[+] witrapper.com NS: ns2.witrapper.com
[+] witrapper.com NS: ns1.witrapper.com
[*] Attempting DNS AXFR for witrapper.com from ns3.witrapper.com
W, [2020-10-08T18:20:27.850878 #572]  WARN -- : Failed to parse RR packet from offset: 77
W, [2020-10-08T18:20:27.851330 #572]  WARN -- : Failed to parse RR packet from offset: 428
W, [2020-10-08T18:20:27.851635 #572]  WARN -- : Failed to parse RR packet from offset: 745

[+] witrapper.com MX: mx3.sg.witrapper.com
[+] witrapper.com MX: mx7.uk.witrapper.com
[+] witrapper.com MX: mx6.ru.witrapper.com
[+] witrapper.com MX: mx1.us.witrapper.com
[*] Querying DNS SOA records for witrapper.com
[+] witrapper.com SOA: ns1.witrapper.com
[*] Querying DNS TXT records for witrapper.com
[+] witrapper.com TXT: Welcome to Witrapper.com - the parent company of witrap :)
[*] Querying DNS SRV records for witrapper.com
[+] _kerberos._tcp.witrapper.com SRV: {:host=>"_kerberos._tcp.witrapper.com", :port=>88, :priority=>10}
[+] _kerberos._udp.witrapper.com SRV: {:host=>"_kerberos._udp.witrapper.com", :port=>88, :priority=>10}
[+] _ldap._tcp.witrapper.com SRV: {:host=>"_ldap._tcp.witrapper.com", :port=>389, :priority=>10}
[+] _sip._tcp.witrapper.com SRV: {:host=>"_sip._tcp.witrapper.com", :port=>5060, :priority=>20}
[+] admin.witrapper.com A: 192.211.79.101
[+] internal.witrapper.com A: 192.211.79.100
[+] ldap.witrapper.com A: 192.211.79.213
[+] ns1.witrapper.com A: 192.211.79.3
[+] ns2.witrapper.com A: 192.211.79.3
[+] ns3.witrapper.com A: 192.211.79.3
[+] promo.witrapper.com A: 192.211.79.31
[+] public.witrapper.com A: 192.211.79.30
[+] reserved.witrapper.com A: 192.211.79.214
[*] Auxiliary module execution completed
msf6 auxiliary(gather/enum_dns) >

```

Various subdomains for witrapper.com are retrieved by this module.

References:

1. dnsenum (<https://github.com/fwaeytens/dnsenum>)
2. DNSRecon (<https://github.com/darkoperator/dnsrecon>)
3. DNS Record Scanner and Enumerator
(https://www.rapid7.com/db/modules/auxiliary/gather/enum_dns)