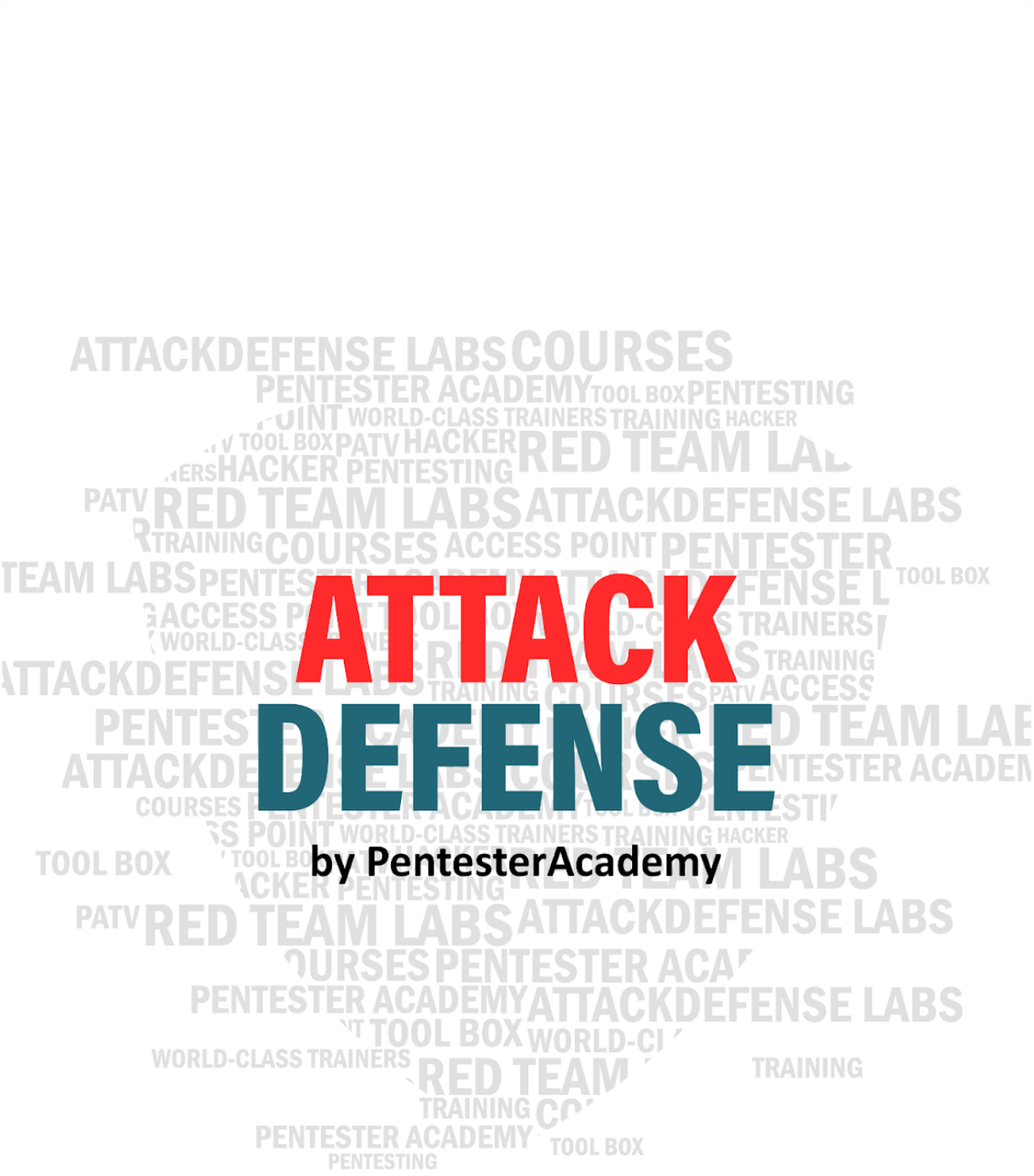
ATTACK
DEFENSE
by PentesterAcademy

Name	DNS Wildcard Entries
URL	https://attackdefense.com/challengedetails?cid=2020
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 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:~#
root@attackdefense:~# nslookup 192.211.79.3
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 = promo.witrap.com.
3.79.211.192.in-addr.arpa       name = witrap.com.

root@attackdefense:~#
```

The IP maps to various domain names:

- witrapper.com.
- public.witrap.com.
- promo.witrap.com.
- witrap.com.

As mentioned in the challenge description, the DNS records for witrap.com have to be enumerated using the dnsenum tool and the distinct IP addresses are to be determined.

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

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


Host's addresses:
__________________

witrap.com.                              900      IN    A        192.211.79.3


Wildcard detection using: zvhcsdsgzyqz
_______________________________________

zvhcsdsgzyqz.witrap.com.                 900      IN    CNAME    witrap.com.
witrap.com.                              900      IN    A        192.211.79.3


!!!!!!!!!!!!!!!!!!!!!!!!!!!!

 Wildcards detected, all subdomains will point to the same IP address
 Omitting results containing 192.211.79.3.
 Maybe you are using OpenDNS servers.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Name Servers:
_____________

ns1.witrapper.com.                      900      IN    A        192.211.79.3
ns3.witrapper.com.                      900      IN    A        192.211.79.4


Mail (MX) Servers:
__________________

mx1.us.witrap.com.                      900      IN    A        192.211.79.200
mx3.us.witrap.com.                      900      IN    A        192.211.79.201


Trying Zone Transfers and getting Bind Versions:
________________________________________________

Trying Zone Transfer for witrap.com on ns1.witrapper.com ...
AXFR record query failed: REFUSED


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

*.witrap.com.                           900      IN    CNAME    witrap.com.
1003.witrap.com.                        900      IN    CNAME    witrap.com.
1025.witrap.com.                        900      IN    CNAME    witrap.com.
1027.witrap.com.                        900      IN    CNAME    witrap.com.
1029.witrap.com.                        900      IN    CNAME    witrap.com.
1037.witrap.com.                        900      IN    CNAME    witrap.com.
1044.witrap.com.                        900      IN    CNAME    witrap.com.
1066.witrap.com.                        900      IN    CNAME    witrap.com.
1070.witrap.com.                        900      IN    CNAME    witrap.com.
1071.witrap.com.                        900      IN    CNAME    witrap.com.
1075.witrap.com.                        900      IN    CNAME    witrap.com.
1082.witrap.com.                        900      IN    CNAME    witrap.com.
1088.witrap.com.                        900      IN    CNAME    witrap.com.
11.witrap.com.                          900      IN    CNAME    witrap.com.
1106.witrap.com.                        900      IN    CNAME    witrap.com.
1107.witrap.com.                        900      IN    CNAME    witrap.com.
```

```
xmmxprod1.witrap.com.                   900     IN    CNAME    witrap.com.
zdfageh\228lter.witrap.com.             900     IN    CNAME    witrap.com.
zdfagehaelter.witrap.com.               900     IN    CNAME    witrap.com.
zdfagehalter.witrap.com.                900     IN    CNAME    witrap.com.
zdfapensionen.witrap.com.               900     IN    CNAME    witrap.com.
zensus.witrap.com.                      900     IN    CNAME    witrap.com.
zensus2011.witrap.com.                  900     IN    CNAME    witrap.com.
zfa.witrap.com.                         900     IN    CNAME    witrap.com.
zilverfonds.witrap.com.                 900     IN    CNAME    witrap.com.
zoek.witrap.com.                        900     IN    CNAME    witrap.com.


witrap.com class C netranges:
_____________________________

 192.211.79.0/24


Performing reverse lookup on 256 ip addresses:
_______________________________________________
```

Notice that there are multiple subdomain names that map to witrap.com
Most of these are random names.

This clearly indicates that there must be a wildcard DNS entry for witrap.com.

Hence, any non-existent subdomain would resolve to witrap.com

Exit the dnsenum tool by pressing CTRL + C and run it again. But this time, save the output to a file named output.txt

```
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      dmz.witrap.com.
^C
root@attackdefense:~#
```

Use the following command to save the output of dnsenum tool for witrap.com domain. The following command would send any encountered errors to /dev/null:

Command: dnsenum witrap.com 2>/dev/null 1> output.txt

```
root@attackdefense:~#
root@attackdefense:~# dnsenum witrap.com 2>/dev/null 1> output.txt
root@attackdefense:~#
```

Use the following commands to look for CNAME and A records in the output of dnsenum:

Commands:

grep 'IN CNAME' output.txt | wc -l
grep 'IN A' output.txt

```
root@attackdefense:~# grep 'IN    CNAME' output.txt | wc -l
1493
root@attackdefense:~#
root@attackdefense:~# grep 'IN    A' output.txt
witrap.com.                             900      IN    A        192.211.79.3
witrap.com.                             900      IN    A        192.211.79.3
ns1.witrapper.com.                      900      IN    A        192.211.79.3
ns3.witrapper.com.                      900      IN    A        192.211.79.4
mx1.us.witrap.com.                      900      IN    A        192.211.79.200
mx3.us.witrap.com.                      900      IN    A        192.211.79.201
admin.witrap.com.                       900      IN    A        192.211.79.41
dmz.witrap.com.                         900      IN    A        192.211.79.42
training.witrap.com.                    900      IN    A        192.211.79.40
root@attackdefense:~#
```

Use the following command to retrieve all the A records that are along with CNAME records:

Command: grep -C1 'IN CNAME' output.txt | grep 'IN A'

```
root@attackdefense:~#
root@attackdefense:~# grep -C1 'IN    CNAME' output.txt | grep 'IN    A'
witrap.com.                             900      IN    A        192.211.79.3
admin.witrap.com.                       900      IN    A        192.211.79.41
dmz.witrap.com.                         900      IN    A        192.211.79.42
training.witrap.com.                    900      IN    A        192.211.79.40
root@attackdefense:~#
```

Notice that the tool was able to uncover 4 distinct IP addresses among the wildcard CNAME records.

Hence, it could be beneficial to enumerate DNS records for servers that do have wildcard entries and don't have zone transfers enabled.

This way some internal IP addresses could still be uncovered, but that also depends on the wordlist used.

References:

1. nslookup man page (https://linux.die.net/man/1/nslookup)
2. dnsenum (https://github.com/fwaeytens/dnsenum)