

The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline of the country. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "RED TEAM", "ACCESS POINT", "TOOL BOX", "TRAINING", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "PENTESTING", and "HACKER PENTESTING". Other smaller words visible include "TEAM LABS", "PENTESTER ACADEMY", "ATTACK DEFENSE LABS", "COURSES ACCESS POINT", "PENTESTER", "ACCESS POINT", "WORLD-CLASS TRAINERS", "TRAINING COURSES", "PATV ACCESS", "PENTESTER ACADEMY", "TOOL BOX", "HACKER PENTESTING", "RED TEAM LABS", "ATTACK DEFENSE LABS", "COURSES PENTESTER ACADEMY", "PENTESTER ACADEMY", "ATTACK DEFENSE LABS", "TOOL BOX", "WORLD-CLASS TRAINERS", "TRAINING", "PENTESTER ACADEMY", "TOOL BOX", and "PENTESTING". The colors used for the text are red and dark blue. The background is white.

Name	DNS and Vhosts
URL	https://attackdefense.com/challengedetails?cid=2016
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
37679: eth0@if37680: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:12:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.5/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
37681: eth1@if37682: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:75:45:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.2.195.2/24 brd 192.2.195.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the host machine is “192.2.195.2”.

Step 2: Scanning the target machine using nmap.

Command: nmap 192.2.195.3

```
root@attackdefense:~# nmap 192.2.195.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-02 22:56 IST
Nmap scan report for witrappier.com (192.2.195.3)
Host is up (0.000017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:02:C3:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
root@attackdefense:~#
```

On the target machine port 80 and 3306 are open. Probably some website is hosted on the target machine.

Step 3: Accessing the website hosted on the target machine.

Open the target machine's IP address in firefox:

Command: firefox 192.2.195.3



Hello world!

MySQL Server version: 5.5.47-0ubuntu0.14.04.1

There is a default webpage hosted on the target machine.

Step 4: Performing a reverse lookup on the target machine's IP address.

Command: dig -x 192.2.195.3

```
root@attackdefense:~# dig -x 192.2.195.3

; <<>> DiG 9.11.14-3-Debian <<>> -x 192.2.195.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28283
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
; COOKIE: 15d1e9925aae157575928f1c5f26f83ee6c856d49cea3a6e (good)
;; QUESTION SECTION:
;3.195.2.192.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
3.195.2.192.in-addr.arpa. 900     IN      PTR      witrapper.com.
3.195.2.192.in-addr.arpa. 900     IN      PTR      public.witrap.com.
3.195.2.192.in-addr.arpa. 900     IN      PTR      witrap.com.
3.195.2.192.in-addr.arpa. 900     IN      PTR      promo.witrap.com.

;; AUTHORITY SECTION:
195.2.192.in-addr.arpa. 900     IN      NS       ns3.witrapper.com.
195.2.192.in-addr.arpa. 900     IN      NS       ns1.witrapper.com.

;; ADDITIONAL SECTION:
ns1.witrapper.com.      900     IN      A        192.2.195.5
ns3.witrapper.com.      900     IN      A        192.2.195.4

;; Query time: 0 msec
;; SERVER: 192.2.195.4#53(192.2.195.4)
;; WHEN: Sun Aug 02 23:00:38 IST 2020
;; MSG SIZE rcvd: 238

root@attackdefense:~#
```

The IP address resolves to multiple domain names:

- witrappier.com
- public.witrap.com
- witrap.com
- promo.witrap.com

To get a terse answer (less verbose), then use the following command:

Command: dig -x 192.2.195.3 +short

```
root@attackdefense:~# dig -x 192.2.195.3 +short
witrap.com.
promo.witrap.com.
witrappier.com.
public.witrap.com.
root@attackdefense:~#
```

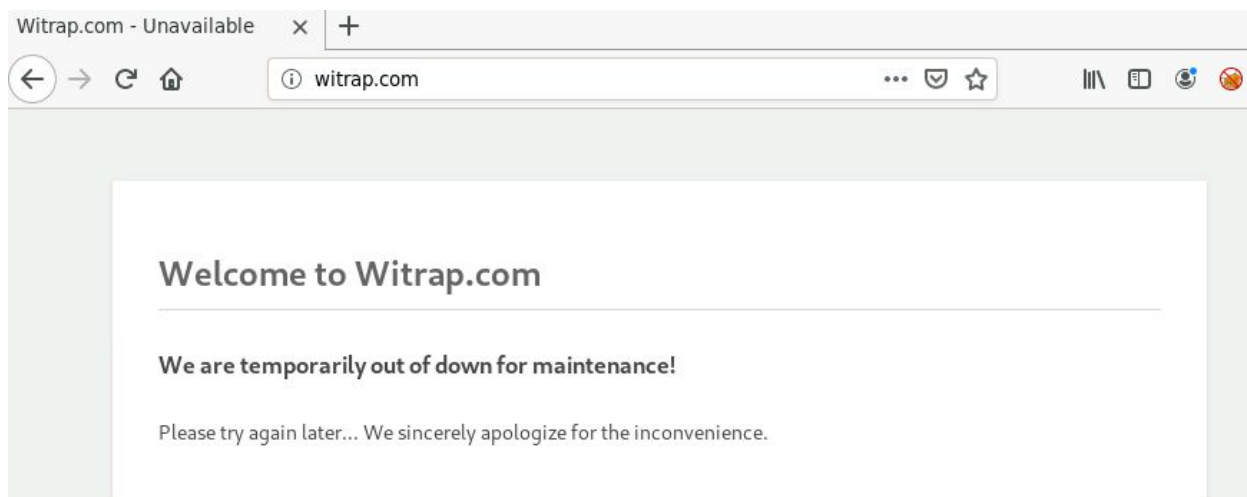
Note: A Fully Qualified Domain Name (FQDN) has a dot (.) appended at its end. But normally, while browsing, even if a dot is not appended to the URL, it still works. The reason is that the resolver when sees an unqualified domain appends a final dot to make it an FQDN.

References:

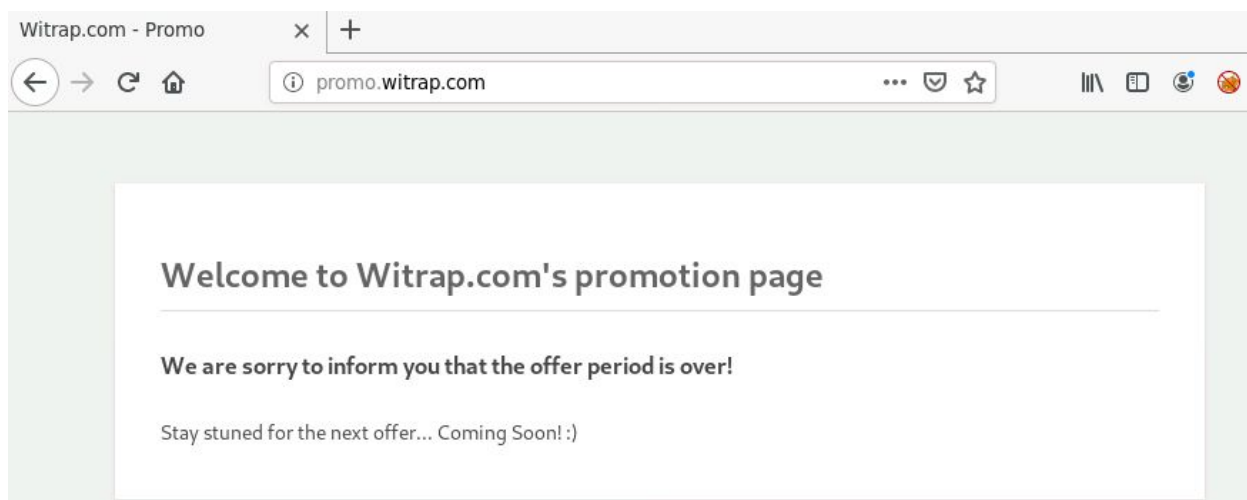
1. https://en.wikipedia.org/wiki/Fully_qualified_domain_name
2. <http://www.dns-sd.org/trailingdotsindomainnames.html>

Step 5: Accessing the web page using the domain names obtained above.

1. Accessing the web page using witrap.com:



2. Accessing the web page using promo.witrap.com:



3. Accessing the web page using witrapper.com:



Login

The following errors occurred:

ATutor was unable to access the database. If the problem persists, please report this to an Administrator with this date reference (08/02/2020 05:47:07 pm)

[Login](#) [Forgot your password?](#)

Returning User

Enter your login name or your email address, and your password.

Login Name or Email

Password

New User

If you do not have an account on this system, please create a new account by clicking on the Register Button below.

4. Accessing the web page using public.witrap.com:



Hello world!

MySQL Server version: 5.5.47-0ubuntu0.14.04.1

In 4 of the domain names, a different page was shown, even though all were mapped to the same IP address.

This was the case because the domains were served using name-based virtual hosts on a single server.

References:

1. Bind 9 (<https://www.isc.org/downloads/bind/>)
2. dig (<https://linux.die.net/man/1/dig>)
3. FQDN (https://en.wikipedia.org/wiki/Fully_qualified_domain_name)