

Scenario

Task 1&2:

For this scenario, the first thing I did was, well, let's search for this URL through tools like `nslookup` or `dig`.

```
Activities Terminal Apr 28 19:54
ahammouda@localhost:~
[ahammouda@localhost ~]$ nslookup internal.example.com
Server:      163.121.128.134
Address:     163.121.128.134#53

** server can't find internal.example.com: NXDOMAIN

[ahammouda@localhost ~]$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 163.121.128.134
nameserver 163.121.128.135
nameserver 192.168.1.1
[ahammouda@localhost ~]$ nslookup internal.example.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

** server can't find internal.example.com: NXDOMAIN

[ahammouda@localhost ~]$ dig @8.8.8.8 internal.example.com

; <<>> DiG 9.16.23-RH <<>> @8.8.8.8 internal.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 24240
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
; internal.example.com. IN A
```

```
Activities Terminal Apr 28 19:54
ahammouda@localhost:~
Address:      8.8.8.8#53

** server can't find internal.example.com: NXDOMAIN

[ahammouda@localhost ~]$ dig @8.8.8.8 internal.example.com

; <<>> DiG 9.16.23-RH <<>> @8.8.8.8 internal.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 24240
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
; internal.example.com. IN A

;; AUTHORITY SECTION:
example.com. 1450 IN SOA ns.icann.org. noc.dns.icann.org. 2025011626 7200 3600 120
9600 3600

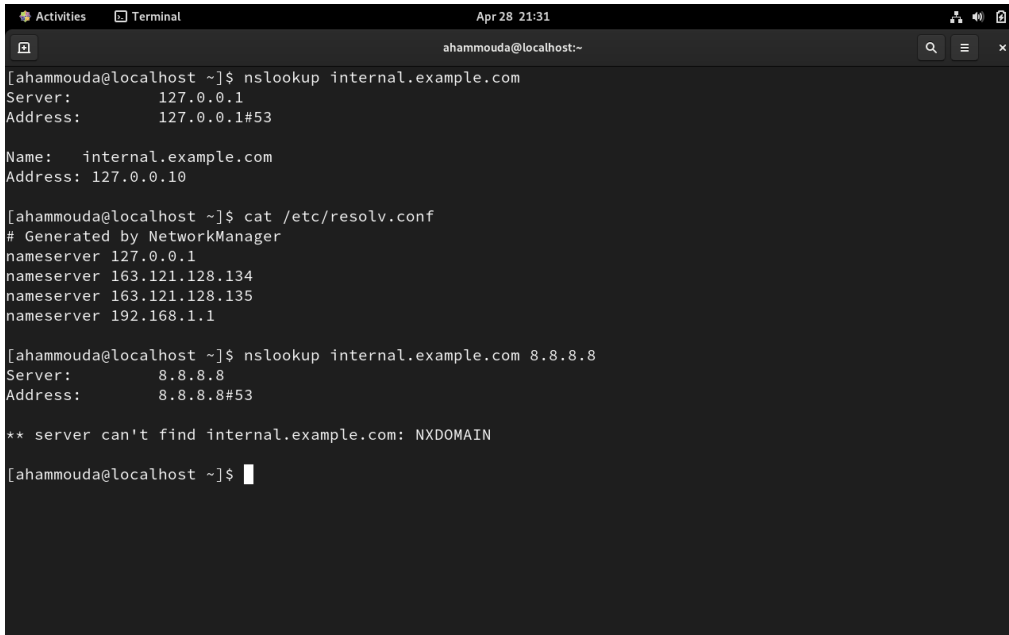
;; Query time: 69 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Apr 28 19:54:13 EEST 2025
;; MSG SIZE rcvd: 105

[ahammouda@localhost ~]$
```

There is no domain or URL with that name! Well, that is expected. As I work on my CentOS machine, I decided to add the URL and domain to `/etc/hosts`, and also, to make it appear in

commands like `nslookup` which search through DNS, I turned my machine into a small DNS server using `dnsmasq`. I added the local IP (127.0.0.10) to `internal.example.com` and added the localhost IP to `/etc/resolv.conf`.

Now I can see `internal.example.com`, although no one else can, as it is on my local machine. That is just for test purposes.

A terminal window titled 'Terminal' with a timestamp of 'Apr 28 21:31' and the user 'ahammouda@localhost'. The terminal shows the following commands and output:

```
[ahammouda@localhost ~]$ nslookup internal.example.com
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:   internal.example.com
Address: 127.0.0.10

[ahammouda@localhost ~]$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 127.0.0.1
nameserver 163.121.128.134
nameserver 163.121.128.135
nameserver 192.168.1.1

[ahammouda@localhost ~]$ nslookup internal.example.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

** server can't find internal.example.com: NXDOMAIN

[ahammouda@localhost ~]$
```

Now let's try to reach `internal.example.com`, using `ping` (it will return a response as expected as the IP is local).

If I try to see if I can reach it through ports like 80 (HTTP) or 443 (HTTPS), I couldn't, which is again normal as there is no service (web server) listening on these ports.

```
Activities Terminal Apr 28 21:37
ahammouda@localhost:~
[ahammouda@localhost ~]$ ###Task-2###
[ahammouda@localhost ~]$ ping -c 127.0.0.10
ping: invalid argument: '127.0.0.10'
[ahammouda@localhost ~]$ ping -c 5 127.0.0.10
PING 127.0.0.10 (127.0.0.10) 56(84) bytes of data.
64 bytes from 127.0.0.10: icmp_seq=1 ttl=64 time=0.058 ms
64 bytes from 127.0.0.10: icmp_seq=2 ttl=64 time=0.182 ms
64 bytes from 127.0.0.10: icmp_seq=3 ttl=64 time=0.076 ms
64 bytes from 127.0.0.10: icmp_seq=4 ttl=64 time=0.295 ms
64 bytes from 127.0.0.10: icmp_seq=5 ttl=64 time=0.124 ms

--- 127.0.0.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4129ms
rtt min/avg/max/mdev = 0.058/0.147/0.295/0.085 ms
[ahammouda@localhost ~]$ nc -vz 127.0.0.10 80
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Connection refused.
[ahammouda@localhost ~]$ curl -v http://192.168.1.5
* Trying 192.168.1.5:80...
^C
[ahammouda@localhost ~]$ curl -vk http://192.168.1.5
* Trying 192.168.1.5:80...
^C
[ahammouda@localhost ~]$
```

3. Trace the Issue – List All Possible Causes

The first thing that comes to mind is DNS-related issues, like incorrect records, misconfiguration of the DNS server, or `/etc/hosts` overrides.

The second thing is network-related issues, like the network might not be reachable either due to a wrong address or connection issues (like physical ones), or there is no service listening on the ports.

Also, it might be application-level misconfiguration.

Let's try to see how to approach each expected issue:

DNS-related Issues

- I would check the two files `/etc/hosts` and `/etc/resolv.conf` to ensure they point to the correct DNS server.
- If not, I would add the correct DNS server IP and make sure that DNS server has the correct record (depends on the server).

```
Activities Terminal Apr 28 22:46
ahammouda@localhost:~$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 127.0.0.1
nameserver 163.121.128.134
nameserver 163.121.128.135
nameserver 192.168.1.1

ahammouda@localhost ~]$ cat /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

127.0.0.10 internal.example.com
ahammouda@localhost ~]$
```

Network Reachability Issues

- I would check if the host is reachable through `ping`.
- If not, I would check for two main suspects first:
 - Physical issues through `ip addr show`.
 - If ports are the problem, I would check with `nc -zv internal.example.com 80`.
- If there is no response, I would suspect two possible causes:
 - A problem with the service not listening on the port: here I would check the service status `sudo systemctl status httpd` and enable it through `sudo systemctl enable httpd`.
 - I would also check for firewall blocking (depends on the type).
- I might also use `sudo netstat -tulnp | grep 80` to see listening ports and services.
- If there are specific app logs, I would examine them.

There is much more, but being the scenario fictional and the environment not set up correctly, there might be some inaccuracies, which we can discuss more face-to-face in the interview.

Show how to persist DNS server settings using systemd-resolved or NetworkManager

That would be from `/etc/systemd/resolved.conf`, and the exact changes required can be searched.

Abdalla Hammouda