



# Cybersecurity

## Networking II Challenge Submission File

### In a Network Far, Far Away!

Make a copy of this document to work in, and then for each mission, add the solution below the prompt. Save and submit this completed file as your Challenge deliverable.

#### Mission 1

1. Mail servers for starwars.com:

starwars.com	mail exchanger = 5 alt2.aspmx.l.google.com.
starwars.com	mail exchanger = 10 aspmx3.googlemail.com.
starwars.com	mail exchanger = 10 aspmx2.googlemail.com.
starwars.com	mail exchanger = 1 aspmx.l.google.com.
starwars.com	mail exchanger = 5 alt1.aspx.l.google.com.

2. Explain why the Resistance isn't receiving any emails:

The outcome from mail servers search for starwars.com indicates the above servers which appear to be outdated as the new primary and secondary servers - [asltx.1.google.com](mailto:asltx.1.google.com) and [asltx.2.google.com](mailto:asltx.2.google.com) are not appearing to be configured for the starwars.com domain.

3. Suggested DNS corrections:

Contacting the domain registrar or DNS provider the MX records for starwars.com requires to be updated to [asltx.1.google.com](mailto:asltx.1.google.com) as a primary server and [asltx.2.google.com](mailto:asltx.2.google.com) as a secondary.

```
starwars.com      mail exchanger = 5 asltx.1.google.com
starwars.com      mail exchanger = 10 asltx.2.google.com
starwars.com      mail exchanger = 10 aspmx2.googlemail.com.
starwars.com      mail exchanger = 1 aspmx.1.google.com.
starwars.com      mail exchanger = 5 alt1.aspx.1.google.com.
```

## Mission 2

1. Sender Policy Framework (SPF) of theforce.net:

```
theforce.net      text = "v=spf1 a mx a:mail.wise-advice.com
mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80
ip4:45.63.15.159 ip4:45.63.4.215 ip4:104.207.135.156 ~all"
```

2. Explain why the Force's emails are going to spam:

The new IP - 45.23.176.21 is not updated on theforce.net's SPF records as displayed above.

3. Suggested DNS corrections:

Update the SPF records of theforce.net adding the new IP 45.23.176.21.

```
theforce.net      text = "v=spf1 a mx a:mail.wise-advice.com
mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80
ip4:45.63.15.159 ip4:45.63.4.215 ip4:104.207.135.156 ip4:45.23.176.21~all"
```

## Mission 3

1. Document the CNAME records:

```
sysadmin@UbuntuDesktop:~$ nslookup -type=CNAME www.theforce.net
Server:           8.8.8.8
Address:          8.8.8.8#53
```

Non-authoritative answer:  
www.theforce.net canonical name = theforce.net.

Authoritative answers can be found from:

2. Explain why the subpage `resistance.theforce.net` isn't redirecting to `theforce.net`:

As the CNAME record indicates above the `resistance.theforce.net` appears to be not added to the `www.theforce.net` record.

To further confirm this the following command was run `nslookup -type=CNAME resistance.theforce.net` to check if there are any CNAME records for `resistance.theforce.net`, the search came up empty, unable to find any records.

3. Suggested DNS corrections:

An DNS configuration update is required for the `www.theforce.net` by adding `resistance.theforce.net www.theforce.net` which will redirect the users to theforce.net going forward.

## Mission 4

1. Confirm the DNS records for `princessleia.site`:

```
sysadmin@UbuntuDesktop:~$ nslookup princessleia.site
Server:           8.8.8.8
Address:          8.8.8.8#53
```

Non-authoritative answer:  
Name: princessleia.site  
Address: 34.102.136.180

Name: princessleia.site

Address: 20.40.202.19

```
sysadmin@UbuntuDesktop:~$ nslookup -type=NS princessleia.site
```

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

princessleia.site nameserver = ns25.domaincontrol.com.

princessleia.site nameserver = ns26.domaincontrol.com.

Authoritative answers can be found from:

## 2. Suggested DNS record corrections to prevent the issue from occurring again:

Add `ns2.galaxybackup.com` as a secondary name server in the princessleila.site's DNS configuration which will ensure to provide responses to the queries in case if primary DNS server becomes unavailable.

```
nslookup -type=NS princessleia.site
```

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

princessleia.site nameserver = ns25.domaincontrol.com.

princessleia.site nameserver = ns26.domaincontrol.com.

princessleia.site nameserver = ns2.galaxybackup.com.

Authoritative answers can be found from:

## Mission 5

### 1. Document the shortest OSPF path from Batuu to Jedha:

#### a. OSPF path:

Batuu----D----C----E----F----J----I----L----Q----T----V----Jedha

#### b. OSPF path cost:

1+2+1+1+1+1+6+4+2+2+2=23

## Mission 6

1. Wireless key:

dictionary

Key type	Key
wpa-pwd	dictionary

2. Host IP addresses and MAC addresses:

- a. Sender MAC address:

Sender MAC address: Cisco-Li\_e3:e4:01 (00:0f:66:e3:e4:01)

- b. Sender IP address:

Sender IP address: 172.16.0.1

- c. Target MAC address:

Target MAC address: IntelCor\_55:98:ef (00:13:ce:55:98:ef)

- d. Target IP address:

Target IP address: 172.16.0.101

## Mission 7

1. Screenshot of results:

