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:

```
alt2.aspmx.l.google.com
aspmx3.googlemail.com
aspmx.l.google.com
aspmx2.googlemail.com
alt1.aspx.l.google.com
```

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

```
The Resistance is not receiving any emails due to the fact that their MX
record is not set to the correct primary and secondary mail servers.
```

3. Suggested DNS corrections:

```
The mail servers should be changed to reflect the correct servers:
starwars.com    mail exchanger = 1 asltx.1.google.com
Starwars.com    mail exchanger = 5 asltx.2.google.com (secondary)
```

Mission 2

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

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

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

```
It is likely due to the fact that theforce.net changed the IP address of
their mail server to 45.23.176.21 while the network was down. According to
the SPF of theforce.net, the only servers configured to send emails for the
domain are the ones with the listed Ips: 45.63.15.159 and 45.63.4.215.
It appears that the SPF has not been updated to reflect the IP change, hence
the Force's emails end up going to spam.
```

3. Suggested DNS corrections:

```
The new IP address (45.23.176.21) should be added to the SPF. Furthermore,
it should be determined if the existing two IP addresses are still relevant,
or whether they should be removed.
```

Mission 3

1. Document the CNAME records:

```
nslookup -type=cname www.theforce.net
Server:            2607:f798:18:10:0:640:7125:5204
Address:    2607:f798:18:10:0:640:7125:5204#53
Non-authoritative answer:
www.theforce.net   canonical name = theforce.net.
```

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

```
When checking for the CNAME of resistance.theforce.net, we receive the
following message:  ** server can't find resistance.theforce.net: NXDOMAIN
```

```
It is possible that the domain is offline due to server issues, or it could
be compromised in some way.
```

3. Suggested DNS corrections:

```
The CNAME record should be reconfigured to read:
resistance.theforce.net      canonical name = theforce.net
```

Mission 4

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

```
nslookup -type=ns princessleia.site
Server:           2607:f798:18:10:0:640:7125:5204
Address:    2607:f798:18:10:0:640:7125:5204#53
Non-authoritative answer:
princessleia.site nameserver = ns26.domaincontrol.com.
princessleia.site nameserver = ns25.domaincontrol.com.
```

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

```
To prevent the issue from recurring, the backup DNS server for
princessleia.site, ns2.galaxybackup.com, should be added to the backup
server reference.
```

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
```

2. Host IP addresses and MAC addresses:

    a. Sender MAC address:

```
00:13:ce:55:98:ef
```

    b. Sender IP address:

```
172.16.0.101
```

    c. Target MAC address:

```
00:0f:66:e3:e4:01
```

    d. Target IP address:

```
172.16.0.1
```

Mission 7

1. Screenshot of results: