Isabella Candido

Mission 1:

Determine and document the mail servers for starwars.com using NSLOOKUP.

nslookup -type=MX starwars.com

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

Authoritative answers can be found from:
alt2.aspmx.l.google.com     internet address = 209.85.202.26
alt2.aspmx.l.google.com     has AAAA address 2a00:1450:400b:c00::1a
aspmx3.googlemail.com       has AAAA address 2a00:1450:400b:c00::1b
aspmx.l.google.com          internet address = 172.217.222.26
aspmx2.googlemail.com       internet address = 64.233.186.26
aspmx2.googlemail.com       has AAAA address 2800:3f0:4003:c00::1b

isabellacandido@Isabellas-MacBook-Pro ~ % nslookup -type=tx starwars.com
unknown query type: tx
Server:             2001:558:feed::1
Address: 2001:558:feed::1#53

Non-authoritative answer:
Name:    starwars.com
Address: 184.51.149.137
Name:    starwars.com
Address: 184.51.149.209
```

Explain why the Resistance isn't receiving any emails.

- “The new primary mail server is **asltx.l.google.com** and the secondary should be **asltx.2.google.com**.”
- asltx is missing from the list or is spelled incorrectly.

Document what a corrected DNS record should be.

- Add the new primary mail servers: asltx.l.google.com and asltx.2.google.com.

Mission 2:

Determine and document the SPF for theforce.net using NSLOOKUP.

nslookup -type=txt theforce.net

```
Server:             2001:558:feed::1
Address: 2001:558:feed::1#53

Non-authoritative answer:
theforce.net        text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com
ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"
theforce.net        text = "google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"
theforce.net        text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"

Authoritative answers can be found from:
```

Isabella Candido

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

- “theforce.net changed the IP address of their mail server to 45.23.176.21 while your network was down.”
- The new IP address is missing from the list.

Document what a corrected DNS record should be.

- Add the new IP address
- theforce.net text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215 ip4:45.23.176.21

Mission 3:

Document how a CNAME should look by viewing the CNAME of www.theforce.net using NSLOOKUP.

isabellacandido@Isabellas-MacBook-Pro ~ % **nslookup -type=CNAME www.theforce.net**
Server: 127.0.0.53
Address: 127.0.0.53#53

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

Authoritative answers can be found from:

isabellacandido@Isabellas-MacBook-Pro ~ % **nslookup -type=all www.theforce.net**
unknown query type: all
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
www.theforce.net canonical name = theforce.net.
Name: theforce.net
Address: 104.156.250.80

Explain why the sub page of resistance.theforce.net isn't redirecting to www.theforce.net.

- Resistance.theforce.net does not have a CNAME

Document what a corrected DNS record should be.

- Add resistance.theforce.net to the CNAME list

www.theforce.net canonical name = theforce.net.
resistance.theforce.net canonical name = theforce.net
Name: theforce.net
Address: 104.156.250.80

Isabella Candido

Mission 4:

Confirm the DNS records for princessleia.site.

nslookup -type=NS princessleia.site

```
Server:         2001:558:feed::1
Address:        2001:558:feed::1#53

Non-authoritative answer:
princessleia.site       nameserver = ns26.domaincontrol.com.
princessleia.site       nameserver = ns25.domaincontrol.com.

Authoritative answers can be found from:
ns25.domaincontrol.com          internet address = 97.74.102.13
ns25.domaincontrol.com          has AAAA address 2603:5:2161::d
ns26.domaincontrol.com          internet address = 173.201.70.13
ns26.domaincontrol.com          has AAAA address 2603:5:2261::d
```

Document how you would fix the DNS record to prevent this issue from happening again.

- add: ns2.galaxybackup.com to authoritative answers list.

Mission 5:

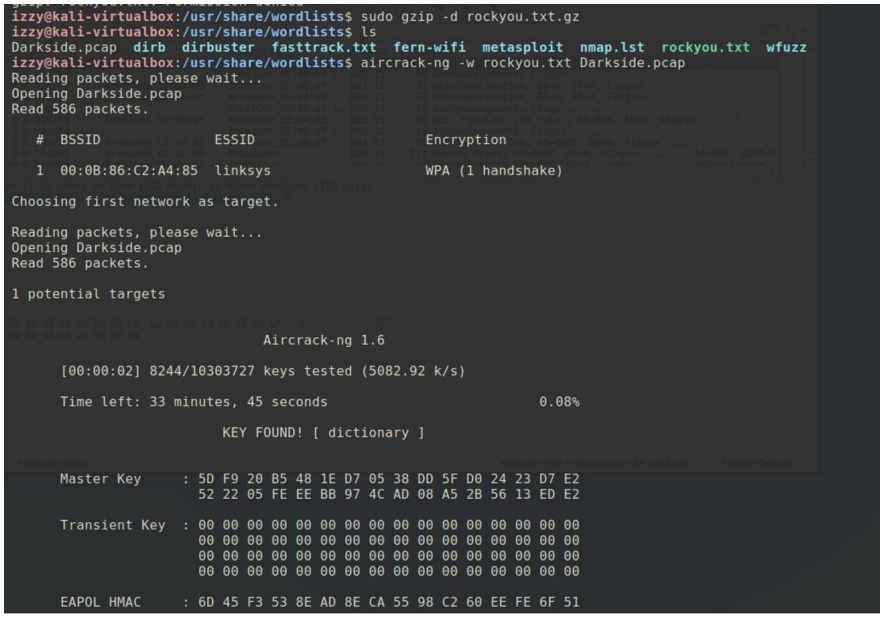
View the Galaxy Network Map and determine the OSPF shortest path from Batuu to Jedha. confirm your path doesn't include Planet N in its route.

Document this shortest path so it can be used by the Resistance to develop a static route to improve the traffic.

- **Batuu > D O R Q T V > Jedha = 22**

Mission 6:

Figure out the Dark Side's secret wireless key by using Aircrack-ng.



Isabella Candido

Document these IP and MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory attack.

- Sender MAC address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
- Sender IP address: 172.16.0.101 (172.16.0.101)

Mission 7:

The Resistance provided you with a hidden message in the TXT record, with several steps to follow.