Networks Fundamentals II Homework: *In a Network Far, Far Away!*

- **You are a Network Jedi working for the Resistance.**

- **The Sith Empire recently carried out a DoS attack, taking out the Resistance's core network infrastructure, including its DNS servers.**

- **This attack destroyed the Resistance's ability to communicate via email and retrieve other crucial information about each others' operations. The Empire has taken advantage of this compromised availability by ambushing numerous Resistance outposts, all vulnerable because they can no longer call for help.**

- **Your task is a crucial one: Restore the Resistance's core DNS infrastructure and verify that traffic is routing as expected.**

Mission 1

Issue: Due to the DoS attack, the Empire took down the Resistance's DNS and primary email servers.

- The Resistance's network team was able to build and deploy a new DNS server and mail server.

- The new primary mail server is `asltx.l.google.com` and the secondary should be `asltx.2.google.com`.

- The Resistance (starwars.com) is able to send emails but unable to receive any.

Your mission:

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

Command: nslookup -type=mx starwars.com

```
Non-authoritative answer:
starwars.com mail exchanger = 10 aspmx2.googlemail.com.
starwars.com mail exchanger = 10 aspmx3.googlemail.com.
starwars.com mail exchanger = 1 aspmx.l.google.com.
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.
starwars.com mail exchanger = 5 alt1.aspx.l.google.com.
```

They are not receiving emails because primary server is aspmx.l.google.com and it should be asltx.l.google.com.

```
starwars.com mail exchanger = 1 asltx.l.google.com
starwars.com mail exchanger = 5 asltx.2.google.com
```

Mission 2

Issue: Now that you've addressed the mail servers, all emails are coming through. However, users are still reporting that they haven't received mail from the `theforce.net` alert bulletins.

- Many of the alert bulletins are being blocked or going into spam folders.

- This is probably due to the fact that `theforce.net` changed the IP address of their mail server to `45.23.176.21` while your network was down.

- These alerts are critical to identify pending attacks from the Empire.

Your mission:

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

```
nslookup -type=txt theforce.net
```

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

The SPF needs to include the new IP address of 42.23.176.21. Anything coming from this IP would be considered spam.

Mission 3

Issue: You have successfully resolved all email issues and the resistance can now receive alert bulletins. However, the Resistance is unable to easily read the details of alert bulletins online.

- They are supposed to be automatically redirected from their sub page of `resistance.theforce.net` to `theforce.net`.

Your mission:

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

```
nslookup -type=cname www.theforce.net
```

```
canonical name = theforce.net
```

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

The reason why subpage is not redirecting to theforce.net is because there is nothign specifying the redirect.

When you nslookup the www.resistance.theforce.net says the server can't find it.

- Document what a corrected DNS record should be resistance.theforce.net

Mission 4

Issue: During the attack, it was determined that the Empire also took down the primary DNS server of `princessleia.site`.

- Fortunately, the DNS server for `princessleia.site` is backed up and functioning.

- However, the Resistance was unable to access this important site during the attacks and now they need you to prevent this from happening again.
prin
- The Resistance's networking team provided you with a backup DNS server of: `ns2.galaxybackup.com`.

Your mission:

- Confirm the DNS records for `princessleia.site`.

nslookup -type=ns princessleia.site

nameserver: ns25.domaincontrol.com
nameserver: ns26.domaincontrol

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

name server: ns2.galaxybackup.com

Mission 5

Issue: The network traffic from the planet of `Batuu` to the planet of `Jedha` is very slow.

- You have been provided a network map with a list of planets connected between `Batuu` and `Jedha`.

- It has been determined that the slowness is due to the Empire attacking `Planet N`.

Your Mission:

- View the [Galaxy Network Map](resources/Galaxy_Network_map.png) 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 to D to C to E to F to J to I to L to Q to T to V to Jedha = 18 hops

Mission 6

Issue: Due to all these attacks, the Resistance is determined to seek revenge for the damage the Empire has caused.

- You are tasked with gathering secret information from the Dark Side network servers that can be used to launch network attacks against the Empire.

- You have captured some of the Dark Side's encrypted wireless internet traffic in the following pcap: [Darkside.pcap](resources/Darkside.pcap).

Your Mission:

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

  - Hint: This is a more challenging encrypted wireless traffic using WPA.

  - In order to decrypt, you will need to use a wordlist (-w) such as `rockyou.txt`.

- Use the Dark Side's key to decrypt the wireless traffic in Wireshark.

  - Hint: The format for they key to decrypt wireless is `<Wireless_key>:<SSID>`.

- Once you have decrypted the traffic, figure out the following Dark Side information:

  - Host IP Addresses and MAC Addresses by looking at the decrypted `ARP` traffic.

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

1. IP: 172.16.0.1
MAC:00:0f:66:e3:e4:01

2. IP: 172.16.0.101

MAC:00:13:ce:55:98:ef

Mission 7

As a thank you for saving the galaxy, the Resistance wants to send you a secret message!

Your Mission:

- View the DNS record from Mission #4.

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

- Follow the steps from the `TXT` record.
  - **Note**: A backup option is provided in the TXT record (as a website) in case the main telnet site is unavailable

- Take a screen shot of the results.

Conclusion

- Submit your results and findings from every mission.

- Congratulations, you have completed your mission and saved the Galaxy!
