## **In a Network Far, Far Away!**

### **Mission 1**

**Issue**: With 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.

1. Mail servers for starwars.com:

|  |
| --- |
| starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.  starwars.com mail exchanger = 10 aspmx2.googlemail.com.  starwars.com mail exchanger = 5 alt1.aspx.l.google.com.  starwars.com mail exchanger = 10 aspmx3.googlemail.com.  starwars.com mail exchanger = 1 aspmx.l.google.com.  Name: starwars.com Address: 104.77.150.175  Name: starwars.com Address: 104.77.150.136  Name: starwars.com Address: 2600:1408:ac00::17de:1010  Name: starwars.com Address: 2600:1408:ac00::17de:100b |

1. Explain why the Resistance isn’t receiving any emails:

|  |
| --- |
| The servers do not match asltx.l.google.com or 5 asltx.2.google.com. These are the servers they now use. |

1. Suggested DNS corrections:

|  |
| --- |
| Change Primary Mail to 1 asltx.l.google.com  Change Secondary Mail to 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 for identifying pending attacks from the Empire.

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

|  |
| --- |
| Server: 192.168.13.2  Address: 192.168.13.2#53  Non-authoritative answer:  theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcffhFL\_Qaf8Lc9tMRkZZSuig0d6w"  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" |

1. Explain why the Force’s emails are going to spam:

|  |
| --- |
| Since the IP address changed, the mail is going to the incorrect place. It is very similar to if a person moves houses and expects to continue to get mail without notifying anyone they moved. |

1. Suggested DNS corrections:

|  |
| --- |
| Include the new IP address:45.23.176.21 so emails do not go to 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 subpage resistance.theforce.net to theforce.net.

1. Document the CNAME records:

|  |
| --- |
| > www.theforce.net  Server: 8.8.8.8  Address: 8.8.8.8#53  Non-authoritative answer:  www.theforce.net canonical name = theforce.net.  Name: theforce.net  Address: 104.156.250.80  > |

1. Explain why the subpage resistance.theforce.net isn’t redirecting to theforce.net:

|  |
| --- |
| Address: 8.8.8.8#53  \*\* server can't find resistance.theforce.net: NXDOMAIN  >  The server does not exist |

1. Suggested DNS corrections:

|  |
| --- |
| correct the CNAME record configuration |

### **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.
* The Resistance's networking team provided you with a backup DNS server of: ns2.galaxybackup.com.

1. Confirm the DNS records for princessleia.site:

|  |
| --- |
| princessleia.site nameserver = ns25.domaincontrol.com.  princessleia.site nameserver = ns26.domaincontrol.com. |

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

|  |
| --- |
| Ns2.galaxybackup.com should be listed as a backup |

### **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 connected planets between Batuu and Jedha.
* It has been determined that the slowness is due to the Empire attacking Planet N.

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

|  |
| --- |
| Batuu: D, C, E, F, J, I, L, Q, T,V to Jedha: |

* 1. OSPF path cost:

|  |
| --- |
| 1 2 1 1 1 2 1 2 1 2 2 2 2 = 20 |

### **Mission 6**

**Issue**: The Resistance is determined to seek revenge for the damage the Empire has caused with all of its attacks.

* 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: [Dark Side PCAPLinks to an external site.](https://drive.google.com/file/d/1lleKbGhkSZA-9q2WsHuW6dxMM5KrrRyS/view?usp=sharing).

Wireless key:

|  |
| --- |
| dictionary |

Host IP addresses and MAC addresses:

* 1. Sender MAC address:

|  |
| --- |
| IntelCor\_55:98:ef (00:13:ce:55:98:ef) |

* 1. Sender IP address:

|  |
| --- |
| 172.16.0.101 (172.16.0.101) |

* 1. Target MAC address:

|  |
| --- |
| Cisco-Li\_e3:e4:01 (00:0f:66:e3:e4:01) |

* 1. Target IP address:

|  |
| --- |
| 172.16.0.1 (172.16.0.1) |

### **Mission 7**

**Issue**: As a thank you for saving the Galaxy, the Resistance wants to send you a secret message!

**Your Mission**:

1. View the DNS record from Mission 4. The Resistance provided you with a hidden message in the TXT record. Follow the steps included in the message.
2. Screenshot of results:

