| Cybersecurity |
| --- |
| Module 9 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:

| nslookup -type=MX starwars.com |
| --- |

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

| You’ll note that neither asltx.l.google.com nor asltx.2.google.com are listed in the exchange server list. This means that someone didn’t set up the MX Server correctly (or is still pointing to the downed server… go Empire!) |
| --- |

1. Suggested DNS corrections:

| Change the MX server URL’s on the server so that it would look like:  starwars.com mail exchanger = 1 asltx.1.google.com  starwars.com mail exchanger = 5 asltx.2.google.com |
| --- |

### Mission 2

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

| nslookup -type=TXT theforce.net |
| --- |

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

| The ip4 address that it should be going to (45.23.176.21) is not listed as any of the IPAddresses which are allowed |
| --- |

1. Suggested DNS corrections:

| I’d suggest that the TXT (SPF) record be updated so that it allows the new IP address (45.23.176.21) be permitted to send emails on theforce.net’s behalf. |
| --- |

### Mission 3

1. Document the CNAME records:

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

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

| I had to do some research on this, just because I don’t understand CNAME that well (yet). So, per https://www.cloudflare.com/learning/dns/dns-records/dns-cname-record/:  Oftentimes, when sites have subdomains such as blog.example.com or shop.example.com, those subdomains will have CNAME records that point to a root domain (example.com). This way if the IP address of the host changes, only the DNS A record for the root domain needs to be updated and all the CNAME records will follow along with whatever changes are made to the root.  So what I’m gathering from this is that the CNAME is set to theforce.net and should be set to resistance.theforce.net. This way, if the IP ever changes for the main domain, the cname will follow the domain rather than the IP.  However, the CNAME is an alias, so I’m not quite sure WHY you would want to redirect a subpage back to the main page. This would be basically saying (in this example) that The Resistance is futile, and they no longer have a subpage, because there is nothing there worth reading. The Empire is where it’s at, and the Resistance, by changing the CNAME to redirect back to the main domain, is cutting their own alerts off since, you know, there is no longer a Resistance subpage. |
| --- |

1. Suggested DNS corrections:

| If you really really really wanted to redirect a subpage back to the domain page, you would change the canonical name (CNAME) from:  theforce.net to resistance.theforce.net. |
| --- |

### Mission 4

1. Confirm the DNS records for princessleia.site:

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

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

| Suggest adding the backup DNS server (ns2.galaxybackup.com) to the name server, so that should the primary ever fail (or be DoS/DDoS’d), the poor Resistance won’t be lost (Great job Empire!) |
| --- |

### Mission 5

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

| There are multiple ways to get from Batuu to Jedha, all with the same path cost, IF you have to avoid Planet N (otherwise, you could get there in 20)  Battu – DCEFJILQTV – Jedha  Battu - DCGORQTV - Jedha  Battu - DGORQTV - Jedha |
| --- |

* 1. OSPF path cost:

| 23 |
| --- |

### Mission 6

1. Wireless key:

| dictionary |
| --- |

1. Host IP addresses and MAC addresses:
   1. Sender MAC address:

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

* 1. Sender IP address:

| 172.16.0.1 |
| --- |

* 1. Target MAC address:

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

* 1. Target IP address:

| 172.16.0.101 |
| --- |

### Mission 7

1. Screenshot of results:

| nslookup -type=txt princessleia.site    And.. the results of the text found.  (For future information, telnet into towel.blinkinglights.nl no longer works.)  Come to the Darkside.  We have cookies. |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.