| 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:

| To find the mail servers for starwars.com, I used:  sysadmin@vm-image-ubuntu-dev-1:~$ nslookup -type=mx starwars.com  Server: 8.8.8.8  Address: 8.8.8.8#53  Non-authoritative answer:  starwars.com mail exchanger = 5 alt1.aspx.l.google.com.  starwars.com mail exchanger = 1 aspmx.l.google.com.  starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.  starwars.com mail exchanger = 10 aspmx3.googlemail.com.  starwars.com mail exchanger = 10 aspmx2.googlemail.com. |
| --- |

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

| The resistance doesn’t receive emails because of the MX record not being set to the primary and secondary mail servers correctly. |
| --- |

1. Suggested DNS corrections:

| I would make my primary mail server: aspmx.1.google.com and I would make my secondary server: aspmx2.googlemail.com as they seem to be high on the priority list and would allow the traffic to go to the correct location. |
| --- |

### Mission 2

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

| sysadmin@vm-image-ubuntu-dev-1:~$ nslookup -type=txt theforce.net  Server: 8.8.8.8  Address: 8.8.8.8#53  Non-authoritative answer:  theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcffhFL\_Qaf8Lc9tMRkZZSuig0d6w"  theforce.net text = "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"  theforce.net text = "google-site-verification=XTU\_We07Cux-6WCSOItl0c\_WS29hzo92jPE341ckbOQ" |
| --- |

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

| The DNS hasn’t been updated to be to the email server that was changed. It is trying to connect to the wrong IP address according to the SPF record. |
| --- |

1. Suggested DNS corrections:

| The SPF record should include all IP addresses and domains used for sending emails by theforce.net. |
| --- |

### Mission 3

1. Document the CNAME records:

| sysadmin@vm-image-ubuntu-dev-1:~$ nslookup -type=cname www.theforce.net  Server: 8.8.8.8  Address: 8.8.8.8#53  Non-authoritative answer:  www.theforce.net canonical name = theforce.net. |
| --- |

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

| The CNAME is different for the destination so it isn’t redirecting correctly. It appears to be misconfigured and may lack the CNAME record for resistance.theforce.net  It is redirecting to the force.net instead of resistance.theforce.net. |
| --- |

1. Suggested DNS corrections:

| Change the CNAME record for resistance.theforce.net to point to theforce.net.The DNS record should be changed to:  resistance.theforce.net instead of theforce.net |
| --- |

### Mission 4

1. Confirm the DNS records for princessleia.site:

| sysadmin@vm-image-ubuntu-dev-1:~$ nslookup -type=ns princessleia.site  Server: 8.8.8.8  Address: 8.8.8.8#53  Non-authoritative answer:  princessleia.site nameserver = ns25.domaincontrol.com.  princessleia.site nameserver = ns26.domaincontrol.com. |
| --- |

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

| To prevent the issues from occurring again, I would suggest setting up a secondary/backup DNS server record pointing to ns2.galaxybackup.com in case the first DNS server fails to connect. |
| --- |

### Mission 5

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

| The shortest OSPF path from Batuu to Jedha would be:  Batuu D-C-E-F-J-I-L-Q-T-V-Jedha |
| --- |

* 1. OSPF path cost:

| The OSPF path cost is 23 |
| --- |

### Mission 6

1. Wireless key:

| sysadmin@vm-image-ubuntu-dev-1:~/Downloads$ aircrack-ng -w /usr/share/wordlists/rockyou.txt Darkside.pcap  Reading packets, please wait...  Opening Darkside.pcap  Read 586 packets.  # BSSID ESSID Encryption  1 00:0B:86:C2:A4:85 linksys WPA (1 handshake)  Choosing first network as target.  Reading packets, please wait...  Opening Darkside.pcap  Read 586 packets.  1 potential targets  Aircrack-ng 1.6  [00:00:02] 6636/14344391 keys tested (3124.39 k/s)  Time left: 1 hour, 16 minutes, 29 seconds 0.05%  KEY FOUND! [ dictionary ]  Master Key : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2  52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2  Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  EAPOL HMAC : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51 |
| --- |

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:

|  |
| --- |

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