| 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:

| sysadmin@UbuntuDesktop:~$ nslookup -type=MX starwars.com  Server: 8.8.8.8  Address: 8.8.8.8#53  Non-authoritative answer:  starwars.com mail exchanger = 5 alt2.aspmx.l.google.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 aspmx3.googlemail.com.  starwars.com mail exchanger = 10 aspmx2.googlemail.com. |
| --- |

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

| The Resistance is not receiving any emails because there seems to be an error in the URLs that are being shown for the email exchange servers. The URLs are not correctly displayed for both of the primary and secondary servers. |
| --- |

1. Suggested DNS corrections:

| A correction for the DNS would include the following:  starwars.com mail exchanger = 5 asltx.2.google.com. <-Secondary  starwars.com mail exchanger = 1 asltx.l.google.com. <-Primary |
| --- |

### Mission 2

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

| sysadmin@UbuntuDesktop:~$ 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=XTU\_We07Cux-6WCSOItl0c\_WS29hzo92jPE341ckbOQ"  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=ycgY7mtk2oUZMagcffhFL\_Qaf8Lc9tMRkZZSuig0d6w" |
| --- |

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

| The Force’s emails are going to spam because there the mail server’s IP Address is set to 45.23.176.21, which is not included in the SPF linked to ‘theforce.net’ to let emails come in. We need the correct server IP Address to be added. |
| --- |

1. Suggested DNS corrections:

| A correction would be to enter the correct updated IP address of 45.23.176.21 into the DNS record. |
| --- |

### Mission 3

1. Document the CNAME records:

| sysadmin@UbuntuDesktop:~$ 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 subpage ‘resistance.theforce.net’ is not redirecting to ‘theforce.net’ because the canonical name is incorrect. The canonical name needs to be changed to ‘resistance.theforce.net’ instead of ‘theforce.net’ in order for a user to be redirected properly. |
| --- |

1. Suggested DNS corrections:

| A correction for this would simply be to change the DNS record of ‘theforce.net’ to ‘resistance.theforce.net’. |
| --- |

### Mission 4

1. Confirm the DNS records for princessleia.site:

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

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

| A correction to prevent this issue from occurring again would be to add ‘ns2.galaxybackup.com’ to the nameserver for the backup DNS server, in case this attack happens again. |
| --- |

### Mission 5

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

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

* 1. OSPF path cost:

| The cost of the OSPF path is 23 hops. |
| --- |

### Mission 6

1. Wireless key:

| sysadmin@UbuntuDesktop:~/Downloads$ aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt  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.  Opening Darkside.pcap  Reading packets, please wait...  Aircrack-ng 1.2 rc4  [00:00:03] 2280/9822769 keys tested (645.15 k/s)  Time left: 4 hours, 13 minutes, 45 seconds 0.02%  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 : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC  55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0  A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49  5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52  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:

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

* 1. Sender IP address:

| Source Address: 172.16.0.1 (172.16.0.1) |
| --- |

* 1. Target MAC address:

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

* 1. Target IP address:

| Destination Address: 172.16.0.101 (172.16.0.101) |
| --- |

### Mission 7

1. Screenshot of results:

|  |
| --- |

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