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
starwars.com      mail exchanger = 5 alt1.aspx.l.google.com.
starwars.com      mail exchanger = 10 aspmx2.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 = 10 aspmx3.googlemail.com.
```

2. Explain why the Resistance isn't receiving any emails:

```
The new primary mail server is supposed to be asltx.1.google.com and the
secondary should be asltx.2.google.com but they are currently not set
correctly. Currently they should be able to send emails but are unable to
receive any.
```

3. Suggested DNS corrections:

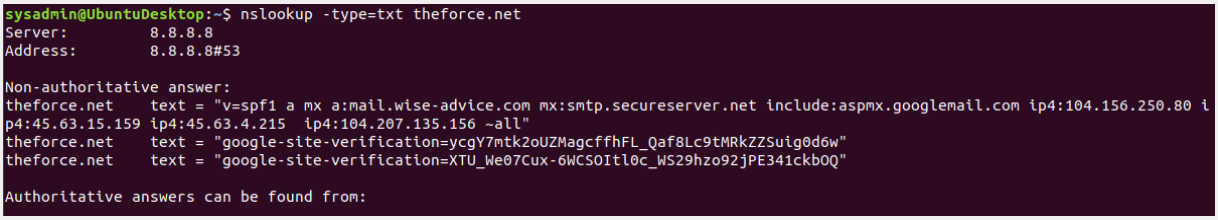
```
Correct DNS should be as follows:
starwars.com      mail exchanger = 1 asltx.1.google.com.
starwars.com      mail exchanger = 5 asltx.2.google.com.
```

Mission 2

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

```
Nslookup -type=txt theforce.net
Server:           8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
theforce.net      text = "v=spf1 a mx a:mail.wise-advice.com
mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80
ip4:45.63.15.159 ip4:45.63.4.215  ip4:104.207.135.156 ~all"
theforce.net      text =
"google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"
theforce.net      text =
"google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"
```



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

```
The emails are going to spam because they have not updated their DNS text
record the the required SPF of the newly changed mail server at 45.23.176.21
```

3. Suggested DNS corrections:

```
The DNS should report back as "v=spf1 a mx a:mail.wise-advice.com
mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80
ip4:45.63.15.159 ip4:45.63.4.215  ip4:45.23.176.21 ~all"
```

Mission 3

1. Document the CNAME records:

```
Server:     8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
www.theforce.net  canonical name = theforce.net.
```

```
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.

Authoritative answers can be found from:
```

2. Explain why the subpage `resistance.theforce.net` isn't redirecting to `theforce.net`:

```
The Cname record does not contain any reference of resistance.theforce.net
to redirect to theforce.net
```

3. Suggested DNS corrections:

```
Correct DNS record should be:
www.theforce.net canonical name = theforce.net
Resistance.theforce.net canonical name = www.theforce.net
```

Mission 4

1. Confirm the DNS records for `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.
```

```
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.

Authoritative answers can be found from:
```

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

```
Add the provided backup server to the DNS server list.
princessleia.site nameserver = ns26.domaincontrol.com.
princessleia.site nameserver = ns25.domaincontrol.com.
princessleia.site nameserver = ns2.galaxybackup.com.
```

Mission 5

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

```
Batuu -> D -> G -> O -> R -> Q -> T -> V  -> Jedha
```

    b. `OSPF` path cost:

```
Path cost = 23
```

Mission 6

1. Wireless key:

```
Wireless Key [dictionary]
```

```
                                Aircrack-ng 1.2 rc4

      [00:00:00] 2280/7120714 keys tested (3065.61 k/s)

      Time left: 38 minutes, 42 seconds                          0.03%

                          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
sysadmin@UbuntuDesktop:~$
```

2. Host IP addresses and MAC addresses:

    a. Sender MAC address:

```
IntelCor_55:98:ef (00:13:ce:55:98:ef)
```

    b. Sender IP address:

```
172.16.0.101
```

    c. Target MAC address:

```
Cisco-Li_e3:e4:01 (00:0f:66:e3:e4:01)
```

    d. Target IP address:

```
172.16.0.101
```

Mission 7

1. Screenshot of results: