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:

```
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 aspmx2.googlemail.com.
starwars.com mail exchanger = 10 aspmx3.googlemail.com.
```

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

```
We're told that asltx.l.google.com should be the primary mail server and asltx.2.google.com  should be secondary but after running nslookup -type=MX starwars.com that does not match with the info given
```

3. Suggested DNS corrections:

```
primary- starwars.com mail exchanger = 1 asltx.aspx.l.google.com
secondary- starwars.com mail exchanger = 5 asltx.2.aspmx.2.google.com
```

Mission 2

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

```
nslookup -querytype=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 ip4:104.156.250.80
ip4:45.63.15.159 ip4:45.63.4.215  ip4:104.207.135.156 ~all"
theforce.net      text =
"google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"
```

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

```
The Force has not updated their DNS record to implement their new IP
45.23.176.21; emails must come from authorized IP addresses
```

3. Suggested DNS corrections:

```
The updated DNS should include the new IP.

 "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 ip4:45.23.176.21 ~all"



theforce.net      text = "v=spf1 a mx a:mail.wise-advice.com
mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:45.23.176.21
```

Mission 3

1. Document the CNAME records:

```
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 DNS record is not specified, if done correctly, when nslookup is used
there should be a CNAME that comes up
```

3. Suggested DNS corrections:

```


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

Authoritative answers can be found from:



```

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

```
princessleia.site        nameserver = n2s.galaxybackup.com
```

Mission 5

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

```
Batuu-D-C-E-F-J-I-L-Q-T-V-Jedha
```

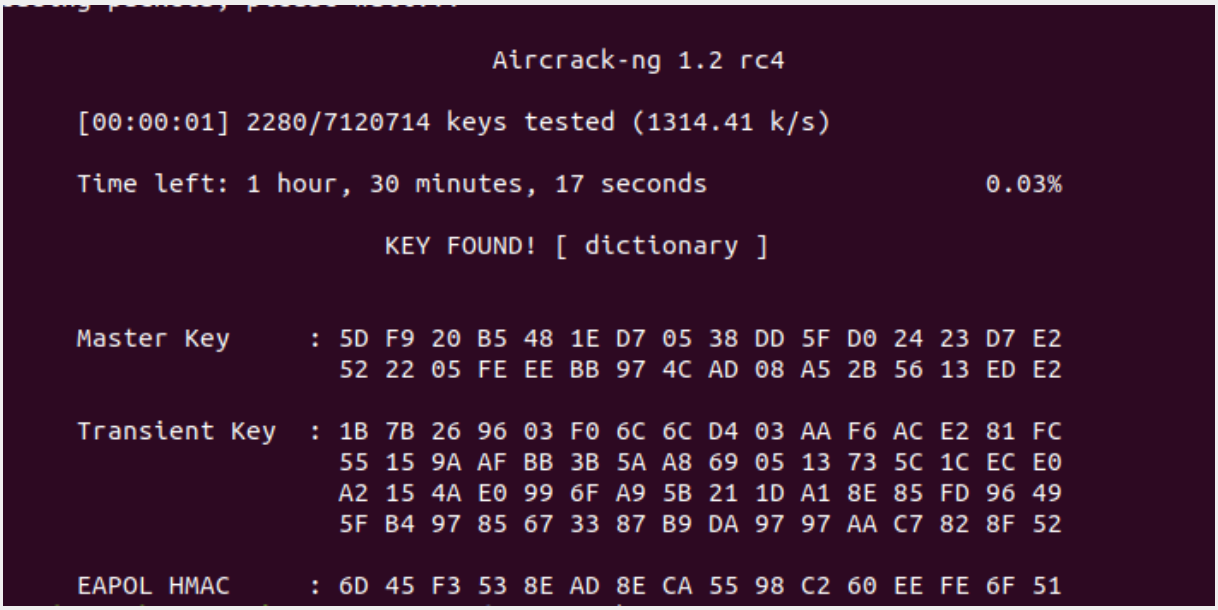
    b. `OSPF` path cost:

```
23 hops
```

Mission 6

1. Wireless key:

```
dictionary
```



2. Host IP addresses and MAC addresses:
    a. Sender MAC address:

```
00:13:ce:55:98:ef
```

    b. Sender IP address:

```
172.16.0.101
```

    c. Target MAC address:

```
00:0f:66:e3:e4:01
```

    d. Target IP address:

```
172.16.0.1
```

Mission 7

1. Screenshot of results:

```
[Insert screenshot here]
```