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@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 = 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.
starwars.com    mail exchanger = 5 alt1.aspx.l.google.com.

Authoritative answers can be found from:
```

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

```
Per image results the new mail exchanger is not populated in the results of
the starwars.com servers, therefore resulting in no email exchanges.
```

3. Suggested DNS corrections:

```
The Corrected DNS:

Correct DNS and set it to high priority to:
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
```



```
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 ip
4:45.63.15.159 ip4:45.63.4.215  ~all"
theforce.net    text = "google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"

Authoritative answers can be found from:
```

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

```
Since they recently changed the ip address of their mail server, you are
unable to find it and it's not listed under the spf results. Only two other
ip addresses.
```

3. Suggested DNS corrections:

```
The corrected DNS record should include the new IP address:

theforce.net      text = "v=spf1 a mx a:mail.wise-advice.com
mx:smtp.secureserver.net include:aspmx.googlemail.com ip:45.23.176.21
ip4:45.63.15.159 ip4:45.63.4.215  ~all"
```

Mission 3

1. Document the CNAME records:

```
nslookup -type=CNAME www.theforce.net
```

```
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.

Authoritative answers can be found from:
```

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

```
Per results we have the wrong CNAME input above (www.theforce.net canonical
name = theforce.net. When it should include www.resistance.theforce.net.
```

3. Suggested DNS corrections:

```
Change it to:
resistance.theforce.net canonical name = theforce.net.
```

Mission 4

1. Confirm the DNS records for `princessleia.site`:

```
nslookup -type=NS 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.

Authoritative answers can be found from:
```

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

```
Add the DNS server backup to the list:

princessleia.site nameserver = ns2.galaxybackup.com
```

Mission 5

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

   a. OSPF path:
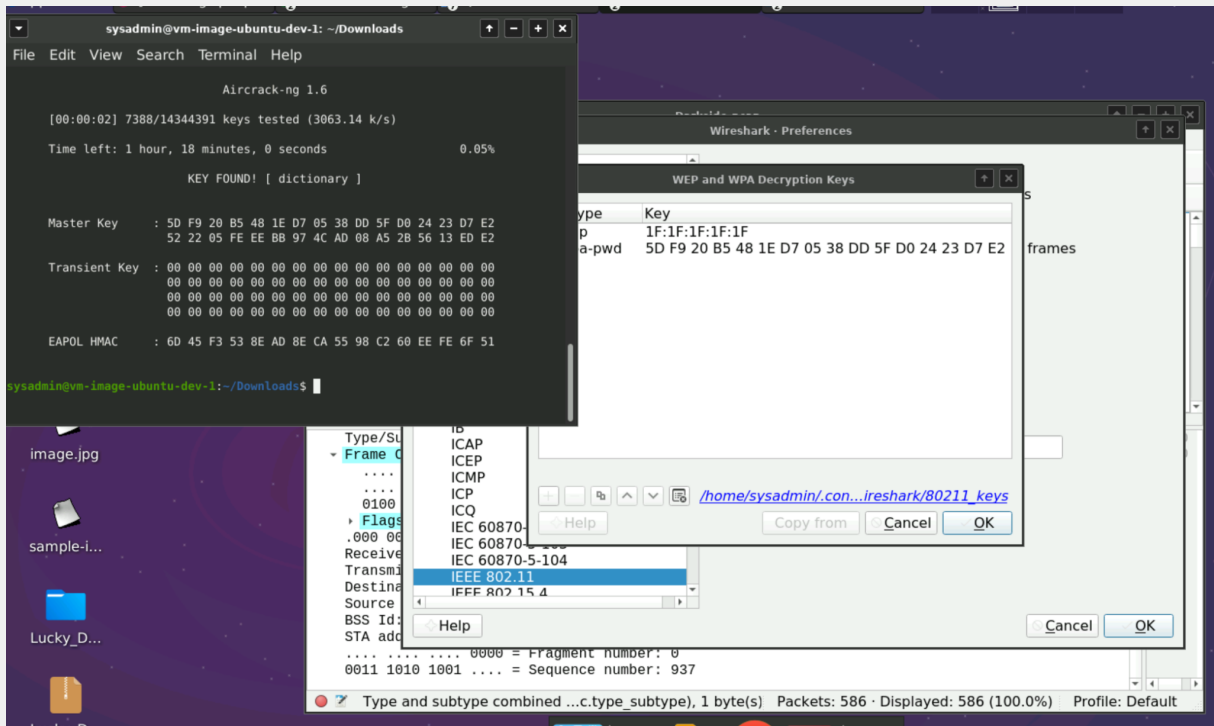
```
Batuu-D-C-E-F—J-I-L-Q-T-V-Jedha
```

   b. OSPF path cost:

```
1+2+1+1+1+1+6+4+2+2+2=23 Hops
```

Mission 6

1. Wireless key:

```
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
```

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
```
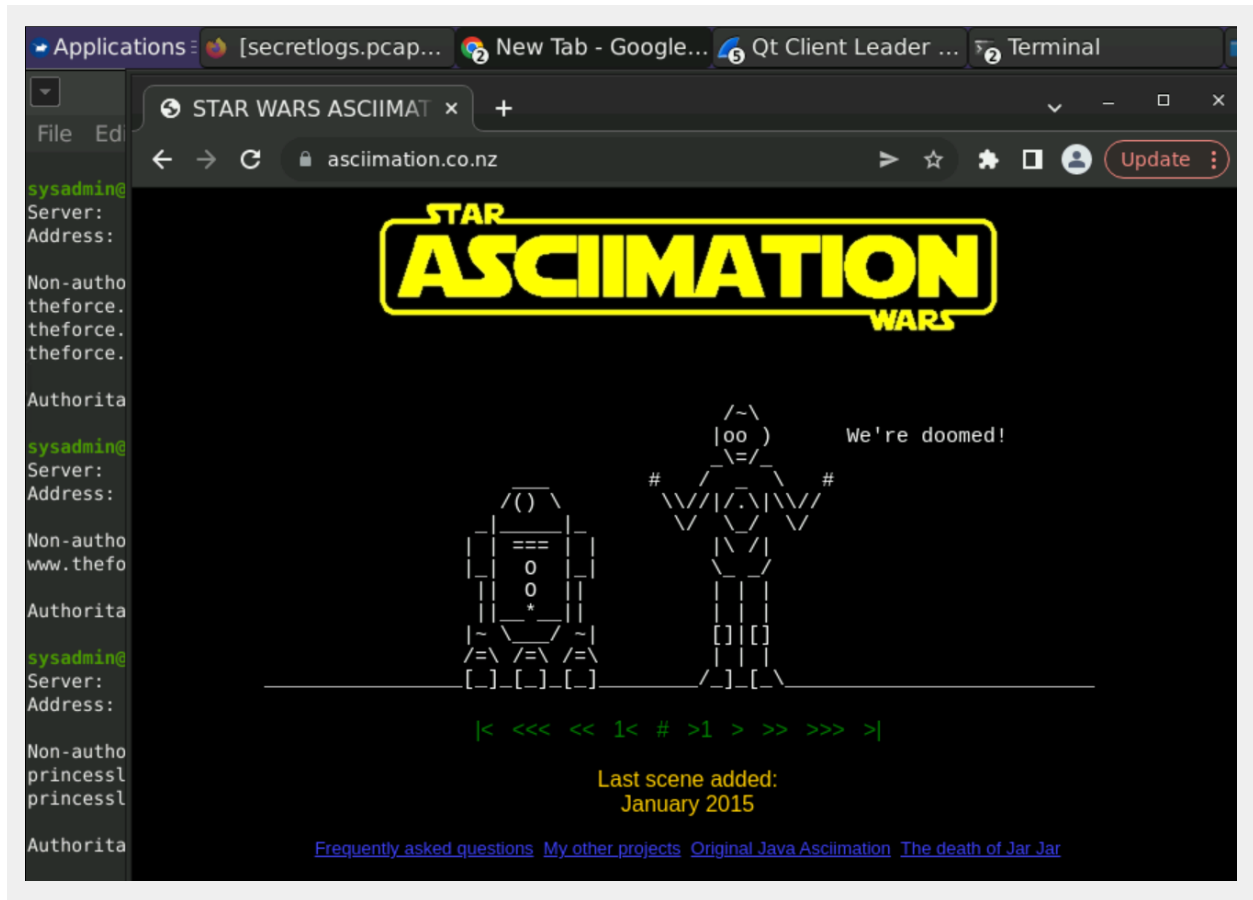
   c. Target MAC address:

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

   d. Target IP address:

```
172.16.0.1
```

Mission 7

1. Screenshot of results:

**Used Chatgpt and google for some source of help.