

### Mission 1:

Determine and document the mail servers for starwars.com using NSLOOKUP.

```
nslookup -type=MX starwars.com
```

```
starwars.com      mail exchanger = 10 aspmx3.googlemail.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 aspmx2.googlemail.com.
starwars.com      mail exchanger = 5 alt2.aspmx.l.google.com.
```

Authoritative answers can be found from:

```
alt2.aspmx.l.google.com  internet address = 209.85.202.26
alt2.aspmx.l.google.com  has AAAA address 2a00:1450:400b:c00::1a
aspmx3.googlemail.com    has AAAA address 2a00:1450:400b:c00::1b
aspmx.l.google.com       internet address = 172.217.222.26
aspmx2.googlemail.com    internet address = 64.233.186.26
aspmx2.googlemail.com    has AAAA address 2800:3f0:4003:c00::1b
```

```
isabellacandido@Isabellas-MacBook-Pro ~ % nslookup -type=tx starwars.com
```

```
unknown query type: tx
```

```
Server:          2001:558:feed::1
```

```
Address: 2001:558:feed::1#53
```

Non-authoritative answer:

```
Name:   starwars.com
Address: 184.51.149.137
Name:   starwars.com
Address: 184.51.149.209
```

Explain why the Resistance isn't receiving any emails.

- “The new primary mail server is **asltx.l.google.com** and the secondary should be **asltx.2.google.com**.”
- asltx is missing from the list or is spelled incorrectly.

Document what a corrected DNS record should be.

- Add the new primary mail servers: asltx.l.google.com and asltx.2.google.com.

### Mission 2:

Determine and document the SPF for theforce.net using NSLOOKUP.

```
nslookup -type=txt theforce.net
```

```
Server:          2001:558:feed::1
```

```
Address: 2001:558:feed::1#53
```

Non-authoritative answer:

```
theforce.net      text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com
```

```
ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"
```

```
theforce.net      text = "google-site-verification=XTU_We07Cux-6WCSOI0c_WS29hzo92jPE341ckbOQ"
```

```
theforce.net      text = "google-site-verification=ycgY7mtk2oUZMagcfffL_Qaf8Lc9tMRkZZSuig0d6w"
```

Authoritative answers can be found from:

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

- “theforce.net changed the IP address of their mail server to 45.23.176.21 while your network was down.”
- The new IP address is missing from the list.

Document what a corrected DNS record should be.

- Add the new IP address
- theforce.net text = "v=spf1 a mx 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"

### Mission 3:

Document how a CNAME should look by viewing the CNAME of www.theforce.net using NSLOOKUP.

```
isabellacandido@Isabellas-MacBook-Pro ~ % nslookup -type=CNAME www.theforce.net
Server:      127.0.0.53
Address:     127.0.0.53#53
```

Non-authoritative answer:

www.theforce.net canonical name = theforce.net.

Authoritative answers can be found from:

```
isabellacandido@Isabellas-MacBook-Pro ~ % nslookup -type=all www.theforce.net
unknown query type: all
Server:      127.0.0.53
Address:     127.0.0.53#53
```

Non-authoritative answer:

www.theforce.net canonical name = theforce.net.

**Name: theforce.net**

**Address: 104.156.250.80**

Explain why the sub page of resistance.theforce.net isn't redirecting to [www.theforce.net](http://www.theforce.net).

- Resistance.theforce.net does not have a CNAME

Document what a corrected DNS record should be.

- Add resistance.theforce.net to the CNAME list  
www.theforce.net canonical name = theforce.net.  
[resistance.theforce.net](http://resistance.theforce.net) canonical name = theforce.net  
Name: theforce.net  
Address: 104.156.250.80

#### Mission 4:

Confirm the DNS records for princessleia.site.

```
nslookup -type=NS princessleia.site
```

```
Server:      2001:558:feed::1
```

```
Address:     2001:558:feed::1#53
```

Non-authoritative answer:

```
princessleia.sitenameserver = ns26.domaincontrol.com.
```

```
princessleia.sitenameserver = ns25.domaincontrol.com.
```

Authoritative answers can be found from:

```
ns25.domaincontrol.com      internet address = 97.74.102.13
```

```
ns25.domaincontrol.com      has AAAA address 2603:5:2161::d
```

```
ns26.domaincontrol.com      internet address = 173.201.70.13
```

```
ns26.domaincontrol.com      has AAAA address 2603:5:2261::d
```

Document how you would fix the DNS record to prevent this issue from happening again.

- add: ns2.galaxybackup.com to authoritative answers list.

#### Mission 5:

View the Galaxy Network Map and determine the OSPF shortest path from Batuu to Jedha.

confirm your path doesn't include Planet N in its route.

Document this shortest path so it can be used by the Resistance to develop a static route to improve the traffic.

- **Batuu > D O R Q T V > Jedha = 22**

#### Mission 6:

Figure out the Dark Side's secret wireless key by using Aircrack-ng.

```
izzy@kali-virtualbox: /usr/share/wordlists$ sudo gzip -d rockyou.txt.gz
izzy@kali-virtualbox: /usr/share/wordlists$ ls
Darkside.pcap  dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
izzy@kali-virtualbox: /usr/share/wordlists$ aircrack-ng -w 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] 8244/10303727 keys tested (5082.92 k/s)

Time left: 33 minutes, 45 seconds      0.08%

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

EAPOL HMAC   : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
```

Document these IP and MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory attack.

- Sender MAC address: IntelCor\_55:98:ef (00:13:ce:55:98:ef)
- Sender IP address: 172.16.0.101 (172.16.0.101)

### Mission 7:

The Resistance provided you with a hidden message in the TXT record, with several steps to follow.

```

Source      Destination      Protocol Length  Info
13  ArubaHe c2:a4:85 Broadcast      888  111 Beacon Frame
14  ArubaHe c2:a4:85 Broadcast      888  111 Beacon Frame
15  ArubaHe c2:a4:85 888888888888 888 888888 111 Beacon Frame
16  ArubaHe c2:a4:85 88 88 88 88 88 88 111 Beacon Frame
17  ArubaHe c2:a4:85 8888 88 88 88 888888 111 Beacon Frame
18  ArubaHe c2:a4:85 88 88 8888888888 88 88 111 Beacon Frame
19  ArubaHe c2:a4:85 8888888888 88 88 888888 111 Beacon Frame
20  ArubaHe c2:a4:85 88 88 88 88 8888888888 88 88 111 Beacon Frame
21  Cisco-L1 e3:e4:01 88 88 88 8888 888888 888888 111 Beacon Frame
22  Cisco-L1 e3:e4:01 88 88 88 88 88 88 88 88 111 Beacon Frame
23  bytes on wire (794)
24  flags: [p...f]
25  Control
26  Action Protocol (reply) 888 888 888888888888 88 88 88
27  type: Ethernet (1)
28  type: IPv4 (0x0000) 88 88 88 88 88 88888888
29
30  172: 4
31  ply (2)
32  address: Cisco-L1 e3:e4:01 (00:0f:05:e3:e4:01)
33  address: 172.16.0.1 (172.16.0.1)
34  address: IntelCor 55:98:ef (00:13:ce:55:98:ef)
35  address: 172.16.0.101 (172.16.0.101)
36
37  00 00 00 00 00 00 01 00 00 00 00 00 00 00
38  00 04 01 00 10 00 01 00 13 c2 55 98 ef 00 00
39  00 00 00 00 00 00 00 00 00 00 00 00 00 00
40  00 00 00

```