Week 9 - Networks Fundamentals II

Your Objectives:

- Review each network issue in the missions below.
- Document each DNS record type found.
- Take note of the DNS records that can explain the reasons for the existing network issue.
- Provide recommended fixes to save the Galaxy!

Mission 1

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

```
cristina@kali:~$ nslookup -type=mx starwars.com
Server:         172.16.64.2
Address:        172.16.64.2#53

Non-authoritative answer:
starwars.com    mail exchanger = 10 aspmx3.googlemail.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.
starwars.com    mail exchanger = 1 aspmx.l.google.com.

Authoritative answers can be found from:
```

Explain why the Resistance isn't receiving any emails.

- The Resistance isn't receiving any emails because the new mail servers have not been added: **asltx.l.google.com** and **asltx.2.google.com**.

Document what a corrected DNS record should be.

- A corrected DNS record will include **asltx.l.google.com** and **asltx.2.google.com** in the mail servers.

Mission 2

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

```
cristina@kali:~$ nslookup -type=txt theforce.net
Server:         172.16.64.2
Address:        172.16.64.2#53

Non-authoritative answer:
theforce.net    text = "google-site-verification=XTU_We07Cux-
6WCSOItl0c_WS29hzo92jPE341ckbOQ"
theforce.net    text = "google-site-
verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"
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"

Authoritative answers can be found from:
```

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

- The IP address **45.23.176.21** isn't showing in the authorized senders section

Document what a corrected DNS record should be.

- A corrected DNS record will include **45.23.176.21** in the SPF:

```
cristina@kali:~$ nslookup -type=txt theforce.net
Server:         172.16.64.2
Address:        172.16.64.2#53

Non-authoritative answer:
theforce.net    text = "google-site-verification=XTU_We07Cux-
6WCSOItl0c_WS29hzo92jPE341ckbOQ"
theforce.net    text = "google-site-
verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"
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"
```

```
Authoritative answers can be found from:
```

Mission 3

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

```
cristina@kali:~$ nslookup -type=cname www.theforce.net
Server:         172.16.64.2
Address:        172.16.64.2#53

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

Authoritative answers can be found from:
```

Explain why the sub page of resistance.theforce.net isn't redirecting to www.theforce.net.

- The CNAME is not configured to include **resistance.theforce.net** as a redirect.

Document what a corrected DNS record should be.

- A corrected DNS record will include **resistance.theforce.net** in the CNAME redirect:

```
cristina@kali:~$ nslookup -type=cname www.theforce.net
Server:         172.16.64.2
Address:        172.16.64.2#53

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

Authoritative answers can be found from:
```

Mission 4

Confirm the DNS records for princessleia.site.

```
cristina@kali:~/Desktop$ sudo nslookup -type=ns princessleia.site
Server:         172.16.64.2
Address:        172.16.64.2#53

Non-authoritative answer:
princessleia.site       nameserver = ns25.domaincontrol.com.
princessleia.site       nameserver = ns26.domaincontrol.com.

Authoritative answers can be found from:
```

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

- I would add **ns2.galaxybackup.com** as a name server:

```
cristina@kali:~/Desktop$ sudo nslookup -type=ns princessleia.site
Server:         172.16.64.2
Address:        172.16.64.2#53

Non-authoritative answer:
princessleia.site       nameserver = ns25.domaincontrol.com.
princessleia.site       nameserver = ns26.domaincontrol.com.
princessleia.site       nameserver = ns2.galaxybackup.com.

Authoritative answers can be found from:
```

Mission 5

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

- Batuu -> D -> C -> E -> F -> J -> I -> L -> Q -> T -> V -> Jedha (23 hops)

Confirm your path doesn't include Planet N in its route. - Does not include Planet N

Mission 6

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

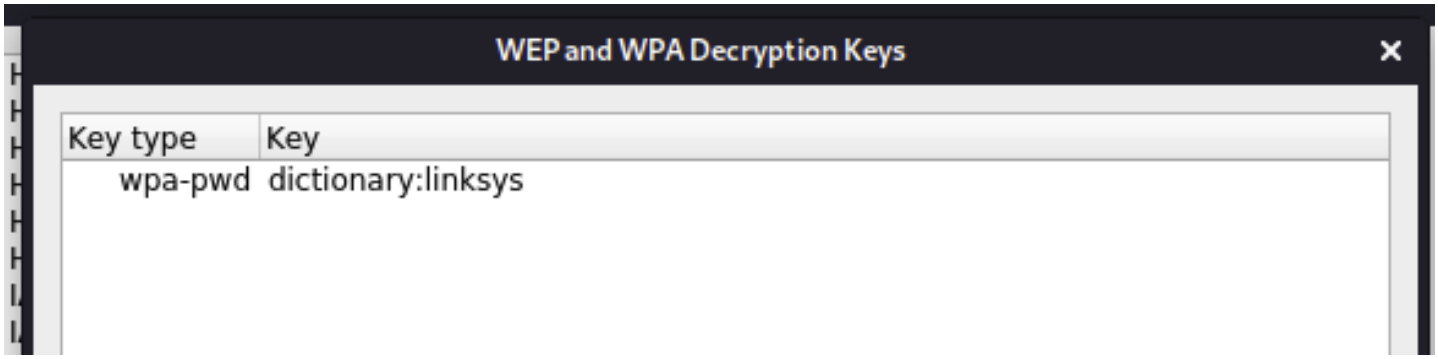
- Hint: This is a more challenging encrypted wireless traffic using WPA.
- In order to decrypt, you will need to use a wordlist (-w) such as rockyou.txt.

```
cristina@kali:~/Desktop$ sudo aircrack-ng -w rockyou.txt Darkside.pcap
[sudo] password for cristina:
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

      [00:00:05] 7245/14344392 keys tested (1451.76 k/s)

      Time left: 2 hours, 44 minutes, 40 seconds                 0.05%

                           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 00 00 00 00

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

Use the Dark Side's key to decrypt the wireless traffic in Wireshark.

- Hint: The format for the key to decrypt wireless is <Wireless_key>:<SSID>.



Once you have decrypted the traffic, figure out the following Dark Side information:

- Host IP Addresses and MAC Addresses by looking at the decrypted ARP traffic.
  - Host IP Address: **172.16.0.101**
  - Mac Address: **00:13:ce:55:98:ef**

Mission 7

View the DNS record from Mission #4.
The Resistance provided you with a hidden message in the TXT record, with several steps to follow:

```
cristina@kali:~/Desktop$ sudo nslookup -type=txt princessleia.site
Server:         172.16.64.2
Address:        172.16.64.2#53

Non-authoritative answer:
princessleia.site       text = "Run the following in a command line: telnet
towel.blinkenlights.nl or as a backup access in a browser:
www.asciimation.co.nz"
```

Follow the steps from the TXT record.

Screenshot of the results: STAR WARS!