

## Mission 1:

- To determine the Mail Servers for starwars.com, I entered the command `nslookup -type=MX starwars.com`. Results shown below:

```
sysadmin@UbuntuDesktop:~$ nslookup -type=MX starwars.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.
starwars.com mail exchanger = 5 alt1.aspx.l.google.com.
starwars.com mail exchanger = 10 aspmx3.googlemail.com.
starwars.com mail exchanger = 1 aspmx.l.google.com.
starwars.com mail exchanger = 10 aspmx2.googlemail.com.

Authoritative answers can be found from:
```

- The reason The Resistance isn't receiving any emails is due to the DNS MX record being misconfigured. A corrected DNS record should include `asltx.l.google.com` and the secondary as `astlx.2.google.com`.

## Mission 2:

- To determine the SPF for theforce.net, I used the command `nslookup -type=txt theforce.net`. Results shown below:

```
sysadmin@UbuntuDesktop:~$ 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 = "google-site-verification=XTU_We07Cux-6WCS0Itl0c_WS29hzo92jPE341ckb0Q"
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:

sysadmin@UbuntuDesktop:~$
```

- The Force's emails are being sent to spam due to the server IP address listed incorrectly in the SPF record. The correct DNS record should include the IP address 45.23.176.21.

## Mission 3:

- To determine why the Resistance isn't able to read the bulletin details, I used command **nslookup -type=cname www.theforce.net**. Results shown below:

```
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:
```

- The reason why the sub page resistance.theforce.net isn't redirecting is due to the canonical name being set to theforce.net. The correct DNS record should show the canonical name www.theforce.net for the resistance.theforce.net.

#### Mission 4:

- To confirm the DNS records for princessleia.site, I used the command **nslookup -type=ns princessleia.site**. Results shown below:

```
sysadmin@UbuntuDesktop:~$ 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:

sysadmin@UbuntuDesktop:~$
```

- To prevent the Resistance from being unable to access the site during an attack, the backup DNS server of ns2.galaxybackup.com needs to be added to the list of name servers.

#### Mission 5:

- After analyzing the Galaxy Network Map, the shortest route from Batuu to Jedha is:  
Batuu – Planet D – Planet C – Planet E – Planet F – Planet J – Planet I – Planet L – Planet Q – Planet T – Planet V – Jedha.
- The path above is the shortest path without including Planet N.

#### Mission 6:

- To determine the Dark Side's secret key, I first moved the pcap file from **Downloads** to **usr/share/wordlists/**. Then used the command **aircrack-ng Darkside.pcap -w rockyou.txt**. Results shown below:

```

                                Aircrack-ng 1.2 rc4

[00:00:01] 2280/7120714 keys tested (1722.67 k/s)

Time left: 1 hour, 8 minutes, 53 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:/usr/share/wordlists$

```

- Once I retrieved the key, I edited the decryption keys under the 802.11 Preferences and filtered for **ARP**. Results shown below:

arp							
Interface		Channel		802.11 Pr			
No.	Time	Source	Destination	Protocol	Length	Info	
312	2006-05-03 22:32:09.421364	IntelCor_55:98:ef	Broadcast	ARP	80	Wh	
314	2006-05-03 22:32:09.422968	IntelCor_55:98:ef	Broadcast	ARP	98	Wh	
315	2006-05-03 22:32:09.423426	Cisco-Li_e3:e4:01	IntelCor_55:98...	ARP	98	17	

  

Logical-Link Control Address Resolution Protocol (request) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (1) Sender MAC address: IntelCor_55:98:ef (00:13:ce:55:98:ef) Sender IP address: 172.16.0.101 (172.16.0.101) Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00) Target IP address: 172.16.0.1 (172.16.0.1)
---

arp							
Interface		Channel		802.11 Preferences			
No. Ubuntu Software		Source	Destination	Protocol	Length	Info	
312	2006-05-03 22:32:09.421364	IntelCor_55:98:ef	Broadcast	ARP	80	Who has 172.	
314	2006-05-03 22:32:09.422968	IntelCor_55:98:ef	Broadcast	ARP	98	Who has 172.	
315	2006-05-03 22:32:09.423426	Cisco-Li_e3:e4:01	IntelCor_55:98...	ARP	98	172.16.0.1 i	

  

Logical-Link Control Address Resolution Protocol (reply) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: reply (2) Sender MAC address: Cisco-Li_e3:e4:01 (00:0f:66:e3:e4:01) Sender IP address: 172.16.0.1 (172.16.0.1) Target MAC address: IntelCor_55:98:ef (00:13:ce:55:98:ef) Target IP address: 172.16.0.101 (172.16.0.101)
---

- Based from the results above, the Host IP addresses and MAC addresses are:
  - 172.16.0.101 and 172.16.0.1

## Mission 7:

- To find the secret message Resistance left, I first used the command `nslookup -type=txt princessleia.site`. Results shown below:

```
sysadmin@UbuntuDesktop:~$ nslookup -type=txt princessleia.site
Server:      8.8.8.8
Address:     8.8.8.8#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"

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
```

- The command **telnet towel.blinkenlights.nl** was followed by a note, along with some star wars animations. Results shown below:

Original Work : Simon Jansen ( <http://www.asciimation.co.nz/> )  
Telnetification : Sten Spans ( [sten@blinkenlights.nl](mailto:sten@blinkenlights.nl) )  
Terminal Tricks : Mike Edwards ( [pf-asciimation@mirkwood.net](mailto:pf-asciimation@mirkwood.net) )

The hard work was done by Simon and Mike,  
I just placed it online in a different format.

So long And Thanks for all the fish

Sten (I just need a Hug)





