**MISSION 1**  
sysadmin@UbuntuDesktop:~$ nslookup

> set type=mx

> starwars.com

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

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

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

The resistance isn’t receiving any emails since the new primary mail server is asltx.1.google.com and the secondary is asltx.2.google.com while ns lookup mx reveals their primary and secondary are not set to the correct servers. They need to correct their mail exchange records to reflect the following: 1 asltx.1.google.com and 5 asltx.2.google.com. This is a DNS Mail Exchange record which is a map where mail is to be delivered and at what priority. 0 being highest priority and as numbers increase indicates where mail will go for load balancing.

**Mission 2:**  
nslookup

> set type=txt

> theforce.net

Server: 8.8.8.8

Address: 8.8.8.8#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:

nslookup 45.23.176.21

21.176.23.45.in-addr.arpa name = 45-23-176-21.lightspeed.rcsntx.sbcglobal.net.

It appears that when the resistance changed the IP of their mail server, they did not include the new IP address in the spf1 which is 45.23.176.21

The correct DNS server should be the force.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 include: 45-23-176-21.lightspeed.rcsntx.sbcglobal.net -all

I have added the -all so that servers that aren’t listed in the SPF record are not able to send emails. I felt that this was important due to the resistance being in an active war with the empire and it will prevent an unautorized server sending an email on behalf of the domain. <https://www.dmarcanalyzer.com/spf/how-to-create-an-spf-txt-record/>

The DNS record is SPF which helps prevent email spoofing and limits spammers. <https://constellix.com/news/dns-record-types-cheat-sheet>

**Mission 3**  
sysadmin@UbuntuDesktop:~$ nslookup

> set 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:

A Cname is an alias that points to another domain or subdomain. Upon doing the nslookup cname of theforce.net it appears that the resistance.theforce.net is not listed. The correct cname for [www.theforce.net](http://www.theforce.net) should look like the below:  
sysadmin@UbuntuDesktop:~$ nslookup  
> set type=cname  
> [www.theforce.net](http://www.theforce.net)  
Server: 8.8.8.8  
Address: 8.8.8.8#53  
Non-authoritative answer:  
www.theforce.net canonical name = theforce.net.  
resistance.theforce.net canonical name = theforce.net

**Mission 4  
sysadmin@UbuntuDesktop:~$ nslookup**

**> set type=ns**

**> princessleia.site**

**Server: 8.8.8.8**

**Address: 8.8.8.8#53**

**Non-authoritative answer:**

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

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

Since the Empire attacked the primary server which is the first one listed (NS26), I would have the resistance remove that one which moves ns25 to primary. I would then add the backup server which would look like the below:  
> 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 = ns2.galaxybackup.com

Mission 5:  
Diagram

Description automatically generated

Shortest Path from Batuu to Jedha while avoiding N is the below:  
D - C - E - F - J - I - L - Q - T - V - Jedha  
1 - 2 - 1 - 1 - 1 - 1 - 6 - 4 - 2 - 2 - 2 = 23

OSPF means open shortest path first. This is a link state routing protocol which means routers will exchange topology information with their nearest neighbors to create a network map so that information being sent can be transmitted through the fastest path. <https://www.metaswitch.com/knowledge-center/reference/what-is-open-shortest-path-first-ospf>

Mission 6  
 aircrack-ng Darkside.pcap -w rockyou.txt

Opening Darkside.pcap

Read 586 packets.

Aircrack-ng 1.2 rc4

[00:00:00] 2280/7120714 keys tested (2434.39 k/s)

Time left: 48 minutes, 44 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

Graphical user interface, application

Description automatically generated

After the arp packets were decoded, I searched ARP in the wireshark bar which then pulled up 3 arp packets.  
A broadcast from MAC Address: 00:13:ce:55:98:ef/ IP address 172.16.0.101  
172.16.0.1 is at 00:0f:66:e3:e4:01  
Since the above IP/Mac addresses were initially encrypted, id recommend the resistance to use these to launch an attack.

Mission 7  
Text

Description automatically generated

Text

Description automatically generated