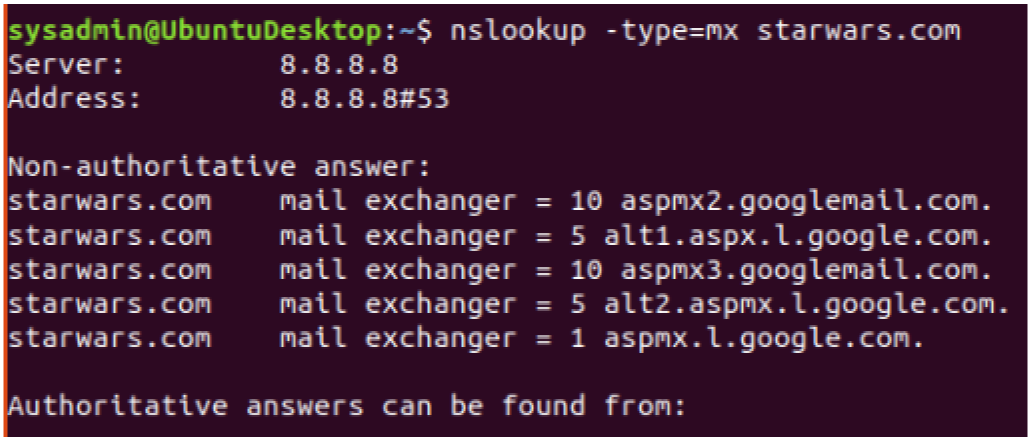
Mission 1

nslookup -type=mx starwars.com



```
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 = 10 aspmx2.googlemail.com.
starwars.com    mail exchanger = 5 alt1.aspx.l.google.com.
starwars.com    mail exchanger = 10 aspmx3.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:
```

- Why the Resistance isn't receiving any emails:

The Resistance can't receive any emails because their mx record is not set to the correct primary and secondary mail servers as provided.

asltx.l.google.com

asltx.2.google.com

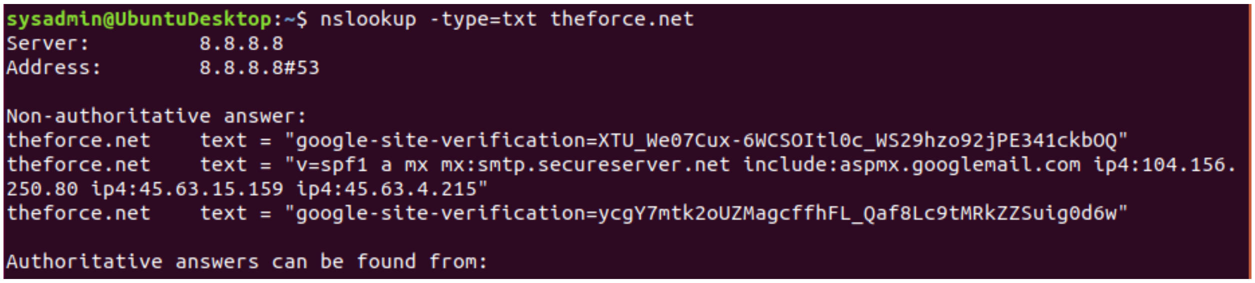
- A corrected DNS record should be**.**

starwars.com mail exchanger = 1 asltx.l.google.com.

starwars.com mail exchanger = 5 asltx.2.google.com.

Mission 2

nslookup -type=txt theforce.net



```
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=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"
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=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"

Authoritative answers can be found from:
```

- Why the Force's emails are going to spam:

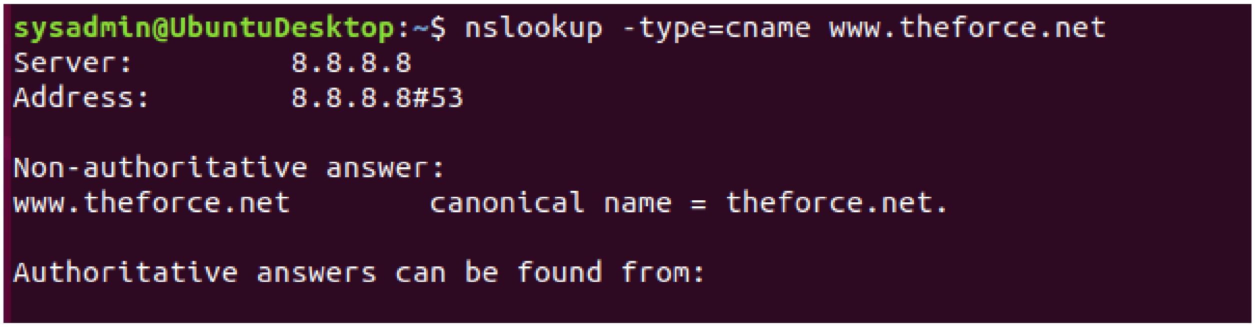
The Correct IP is not in the SPF records.

- A corrected DNS record should be:

Correct IP should be 45.23.176.21

Mission 3

nslookup -type=cname www.theforce.net



```
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:
```

- Why the sub page of `resistance.theforce.net` isn't redirecting to `www.theforce.net`.

The DNS CNAME record is missing a reference from resistance.theforce.net to www.theforce.net

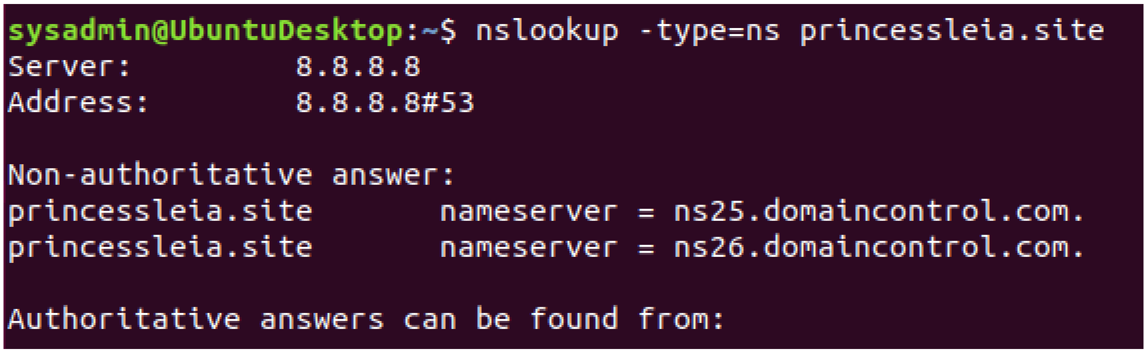
- A corrected DNS record should be.

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

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

Mission 4

nslookup -type=ns princessleia.site



```
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:
```

They should add “ns2.galaxybackup.com” to their “nameserver =”

- Confirm the DNS records for `princessleia.site`.

Current name servers:

princessleia.site nameserver = ns26.domaincontrol.com.

princessleia.site nameserver = ns25.domaincontrol.com.

- To fix the DNS record and prevent this issue from happening again.

Add a reference to the backup DNS server:

princessleia.site nameserver = ns25.domaincontrol.com.

princessleia.site nameserver = ns2.galaxybackup.com.

Mission 5

Shortest path for OSPF -N:

Batuu D C E F J I L Q T V Jedha
1 2 1 1 1 1 6 4 2 2 2 23 hops

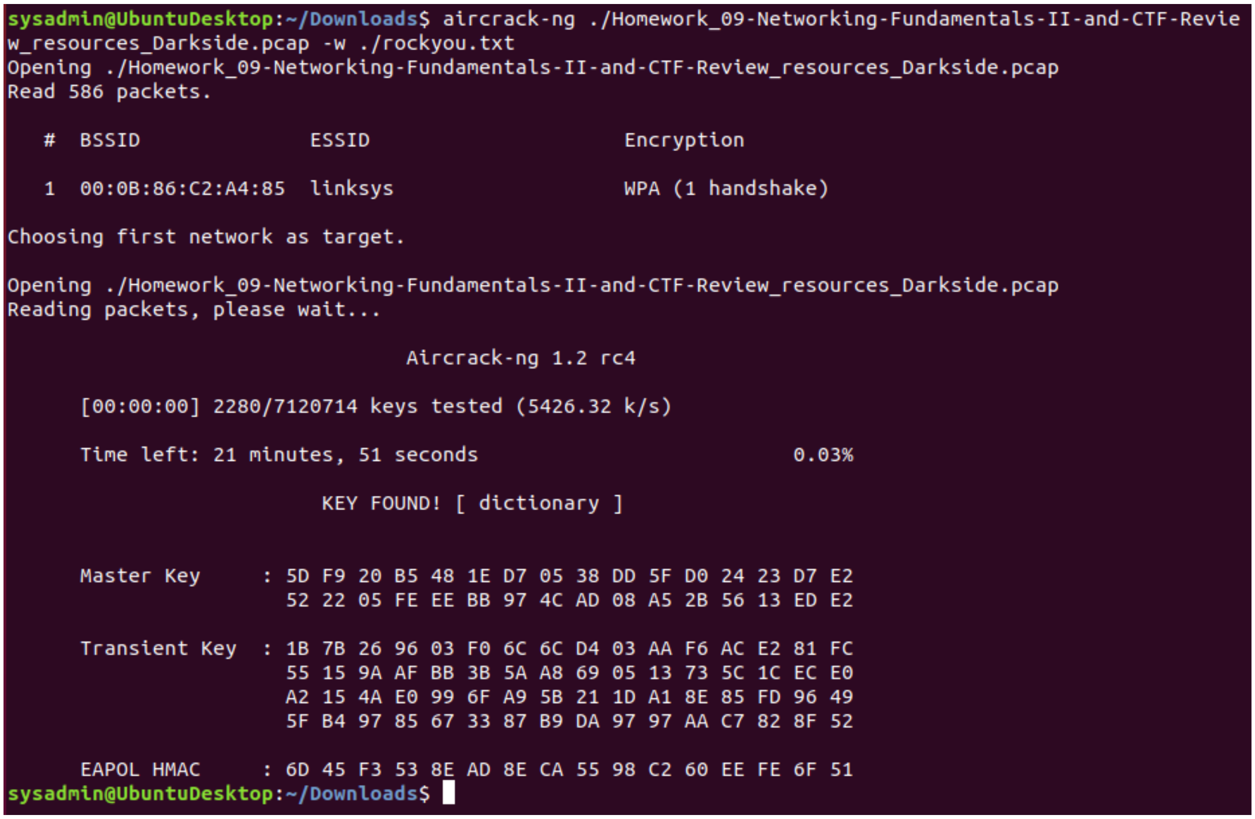
- Confirm the path doesn't include `Planet N` in its route.
D C E F J I L Q T V

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

Planet Batuu > Planet D > Planet C > Planet E > Planet F > Planet J > Planet I > Planet L > Planet Q > Planet T > Planet V > Planet Jedha

Mission 6

aircrack-ng ./Homework_09-Networking-Fundamentals-II-and-CTF-Review_resources_Darkside.pcap -w ./rockyou.txt



```
sysadmin@UbuntuDesktop:~/Downloads$ aircrack-ng ./Homework_09-Networking-Fundamentals-II-and-CTF-Revie
w_resources_Darkside.pcap -w ./rockyou.txt
Opening ./Homework_09-Networking-Fundamentals-II-and-CTF-Review_resources_Darkside.pcap
Read 586 packets.

   #  BSSID              ESSID                     Encryption

   1  00:0B:86:C2:A4:85  linksys                   WPA (1 handshake)

Choosing first network as target.

Opening ./Homework_09-Networking-Fundamentals-II-and-CTF-Review_resources_Darkside.pcap
Reading packets, please wait...

                                 Aircrack-ng 1.2 rc4

      [00:00:00] 2280/7120714 keys tested (5426.32 k/s)

      Time left: 21 minutes, 51 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:~/Downloads$ 
```

Result: Key found [dictionary]

ARP Protocol Specific Addresses:

172.16.0.101 is at 00:13:ce:55:98:ef
172.16.0.1 is at 00:0f:66:e3:e4:01

Wireshark filter: tcp.stream eq 0

There are 4 TCP sources. 1 address 172.16.0.9 sending traffic to 172.16.0.101 Then i sorted by Source and checked 172.16.0.9 traffics and 172.16.0.9 MAC address is 00:14:bf:0f:03:30

Simple Service Discovery Protocol --> HTTP/1.1 200 Ok\r\n --> --> Location: http://172.16.0.9:5431/dyndev/uuid:0014-bf0f-0330000099dc\r\n

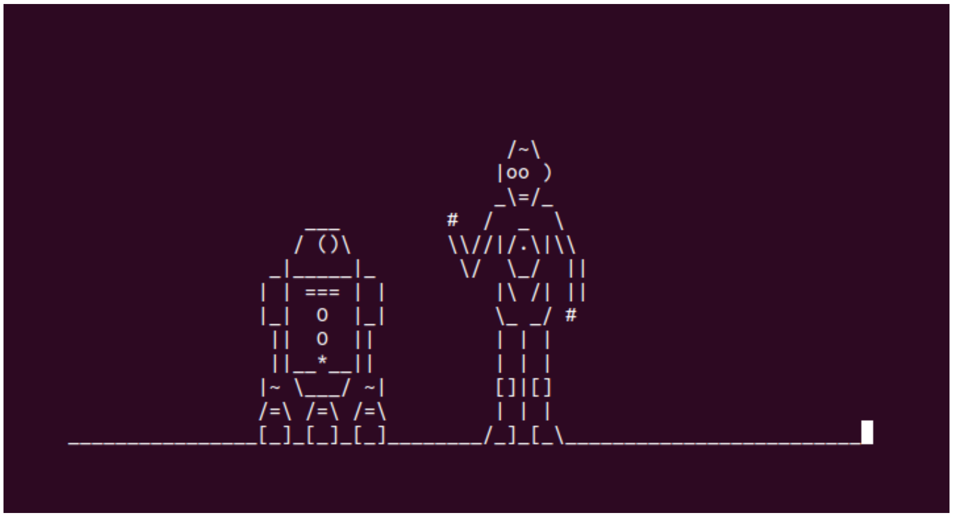
Additional IPs of interest:

172.16.0.9 is at 00:14:bf:0f:03:30
68.9.16.30 is at 00:0f:66:e3:e4:01 same mac as \
68.9.16.25 is at 00:0f:66:e3:e4:01 same mac as - 172.16.0.1
10.1.1.50 is at 00:0f:66:e3:e4:01 same mac as /

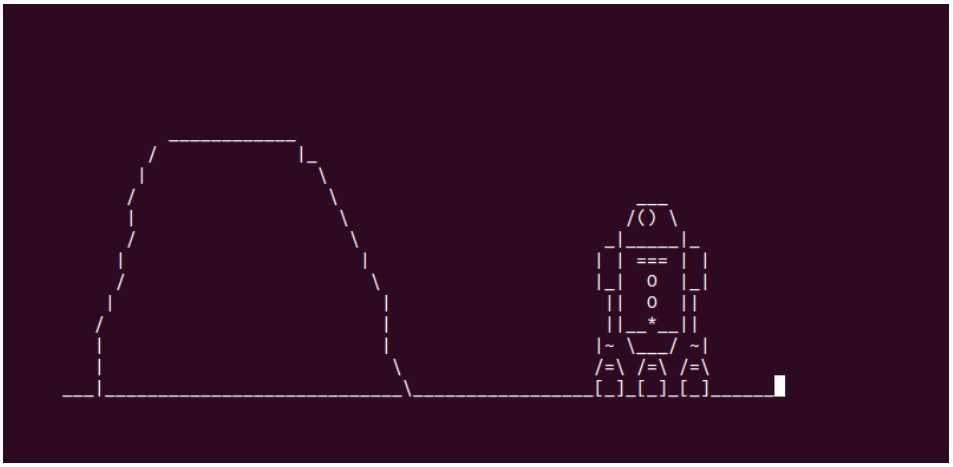
Mission 7

nslookup -type=txt princessleia.site

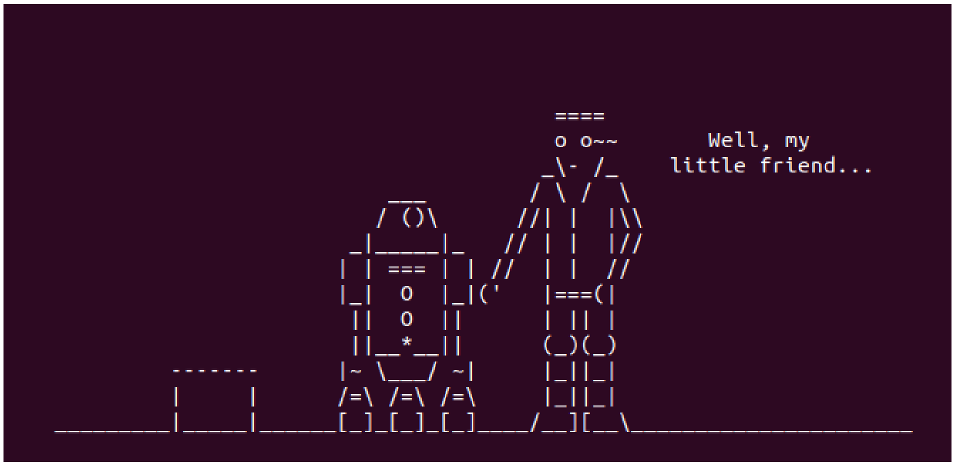
Telnet towel.blinkenlights.nl



```
                                      /~\
                                     |oo )
                                     _\=/_
                    ___          #  /  _  \
                   / ()\         \\//|/.\|\\
                 _|_____|_        \/  \_/  ||
                | | === | |          |\ /| ||
                |_|  O  |_|          \_ _/ #
                 ||  O  ||           | | |
                 ||__*__||           | | |
                |~ \___/ ~|          []|[]
                /=\ /=\ /=\          | | |
________________[_]_[_]_[_]_________/_]_[_\_________________________
```



```
          _____________
        /              |_
       |                 \
      /                   \                            ___
      |                    \                          /() \
      /                     \                       _|_____|_
     |                       |                     | | === | |
     /                        \                    |_|  O  |_|
    |                          |                    ||  O  ||
   /                           |                    ||__*__||
   |                           |                   |~ \___/ ~|
   |                            \                  /=\ /=\ /=\
___|_____________________________\_________________[_]_[_]_[_]_______
```



```
                                       ====
                                       o o~~       Well, my
                                      _\- /_    little friend...
                          ___        / \ /  \
                         / ()\      //| |  |\\
                       _|_____|_   // | |  |//
                      | | === | | //  | |  //
                      |_|  O  |_|('   |===(|
                       ||  O  ||      | || |
                       ||__*__||      (_)(_)
         -------      |~ \___/ ~|     |_||_|
         |     |      /=\ /=\ /=\     |_||_|
_________|_____|______[_]_[_]_[_]____/__][__\______________________
```

The End