**Networks Fundamentals II Homework: *In a Network Far, Far Away!***

Mission 1:

nslookup starwars.com

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

Name: starwars.com

Address: 172.232.19.40

Name: starwars.com

Address: 172.232.19.35

Name: starwars.com

Address: 2600:1405:c000::17dd:e1ba

Name: starwars.com

Address: 2600:1405:c000::17dd:e19a

* We need to see the mail servers
* Using nslookup type=mx starwars.com

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

starwars.com mail exchanger = 5 alt1.aspx.l.google.com.

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

starwars.com mail exchanger = 10 aspmx2.googlemail.com.

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

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

They aren’t receiving emails because asltx.l.google.com and asltx.2.google.com aren’t options from the results above.

Main server = 1 asltx.l.google.com

Secondary server = 5 asltx.2.google.com

10 aspmx2.googlemail.com

10 aspmx3.googlemail.com

Mission 2:

* we need to find information about theforce.net
* we would need to use txt to find the text info for the website
* 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 = "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"

Looking at the spf for 45.23.176.21

* 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"
* above we can see the reason why the emails are going to spam. The 45.23.176.21 is not listed in the spf

- The DNS would need to be updated with the new IP

- 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: 45.23.1766.21"

Mission 3:

First we need to run cname on [www.theforce.net](http://www.theforce.net)

* 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.

As we can see above the reason why resistance.theforce.net is not redirecting to theforce.net is because it is not listed as a redirect option.

The correct DNS would be to add

* resistance.theforce.net canonical name = theforce.net.

Mission 4:

* nslookup princessleia.site

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

Name: princessleia.site

Address: 34.102.136.180

* 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.

* 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](http://www.asciimation.co.nz)"

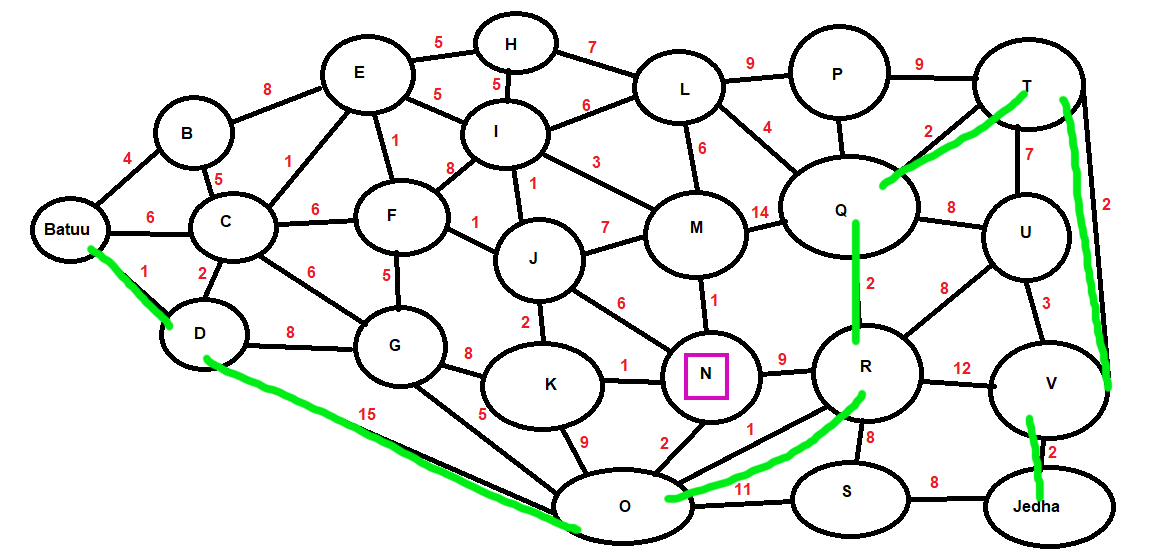
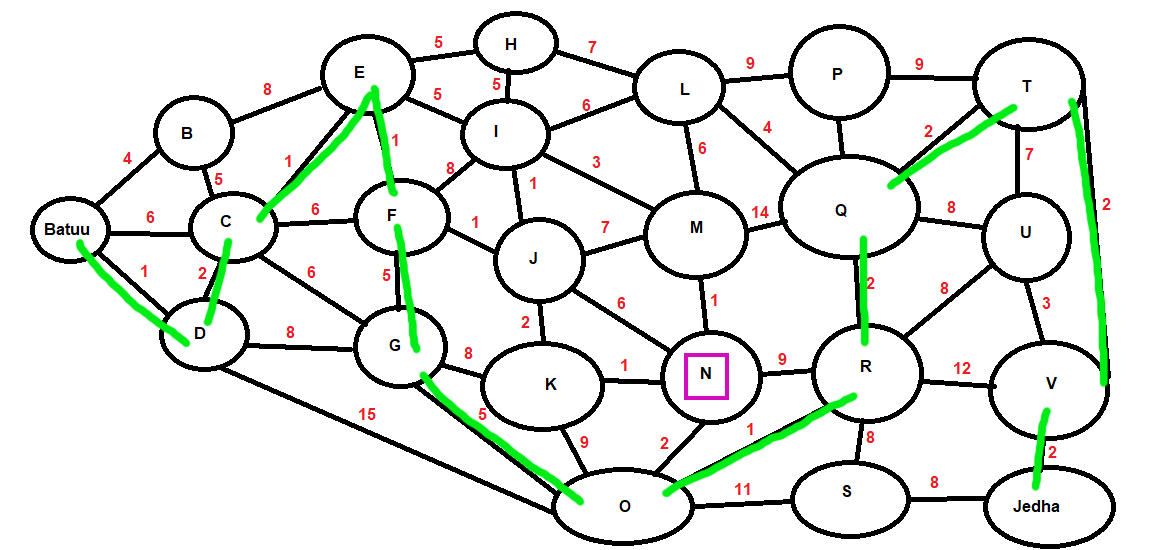
* After running the nslookup -type=ns princessleia.site
  + DNS fix would need to add

princessleia.site nameserver = ns2.galaxybackup.com

Mission 5:

* Shortest path from Batuu to Jedha

After working with the map I have decided on 2 paths -- see below



The top model shows Batuu to Jedha in 24 steps == 10 letters

The bottom model goes through less letters but is 25 steps to Jedha == 6 letters making it the shortest but not faster

Mission 6:

* I had to find my rockyou.txt file, I copied it to my downloads
  + cp rockyou.txt /home/sysadmin/Downloads

Had to run the aircrack-ng on the pcap file

* aircrack-ng -w rockyou.txt Darkside.pcap

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.

Opening Darkside.pcap

Reading packets, please wait...

Aircrack-ng 1.2 rc4

[00:00:00] 2280/8053877 keys tested (2637.86 k/s)

Time left: 50 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

After using the Key: dictionary

Running arp

The host IP is 172.16.0.101 and the MAC address is 00:13:ce:55:98:ef

Mission 7:

* 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](http://www.asciimation.co.nz)"

