Mission 1.

```
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 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.

Authoritative answers can be found from:
```

asltx.l.google.com has not been setup properly to be the primary mail server and asltx.2.google.com is also not on the mail exchange list for servers. The correct DNS should be aspmx.l.google.com then using SMTP(Simple Mail Transfer) on port 25, Layer 7:Application go to alt1.aspx.l.google.com in order to be properly received. The priorities of the mail servers must be set properly.

Mission 2.

```
sysadmin@UbuntuDesktop:/$ nslookup -type=txt theforce.net
Server:         8.8.8.8
Address:        8.8.8.8#53

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

Authoritative answers can be found from:
```

The SPF(Sender Policy Framework) is verified with the IP addresses of the mail servers. The IP addresses to the servers do not match the IP address 45.23.176.21. That would cause the SPF to fail and automatically send the email to the spam folder or reject the email entirely. The emails should be sent to the IP address 104.156.250.80, 45.63.15.159, or 45.63.4.215. 45.23.176.21 needs to be added to the list of acceptable IP's.

Mission 3.

```
sysadmin@UbuntuDesktop:~$ nslookup -type=all www.theforce.net
unknown query type: all
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.theforce.net        canonical name = theforce.net.
Name:   theforce.net
Address: 104.156.250.80
```

The NXDOMAIN means that the domain does not exist. It could have been hijacked by the empire or the /etc/hosts/ file is not configured correctly to redirect the canonical name. The correct DNS is www.theforce.net . resistance.theforce.net needs to be added to the Cname record for it to be sent to theforce.net

Mission 4.

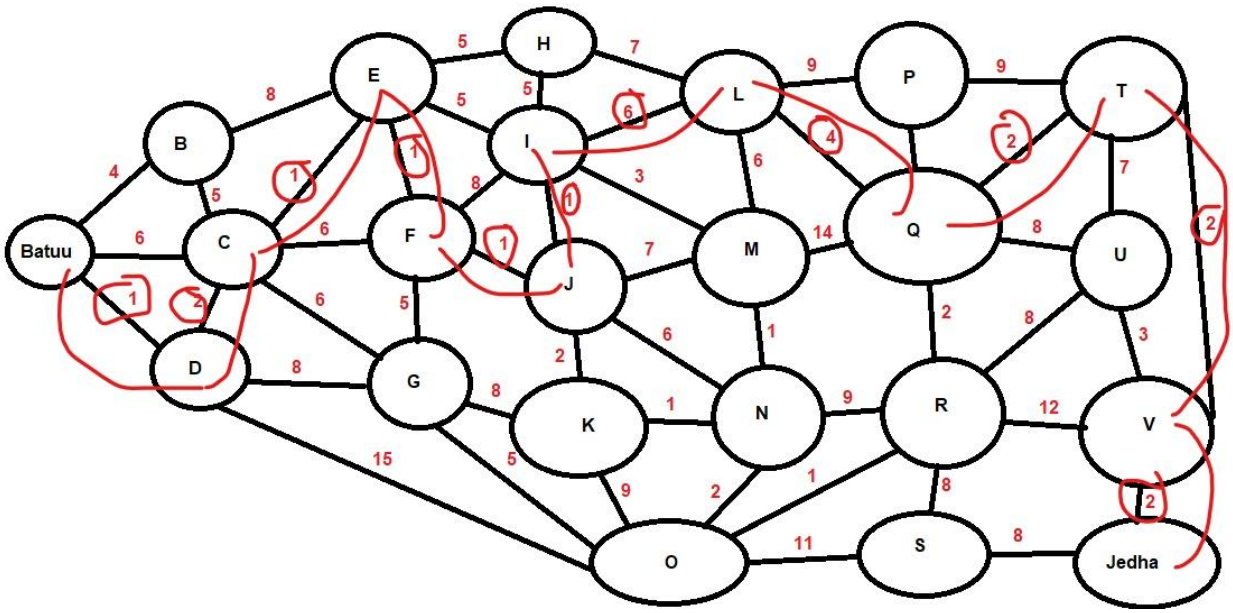
```
sysadmin@UbuntuDesktop:~$ nslookup -type=ns princessleia.site
Server:         8.8.8.8
Address:        8.8.8.8#53

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

Authoritative answers can be found from:
```

There are 2 servers for the princessleia.site, the ns2.galaxybackup.com needs to be added to the list of useable servers.

Mission 5.



Batuu, 1, D **to** D, 2, C **to** C, 1, E **to** E, 1, F **to** F, 1, J **to** J, 1, I **to** I, 6, L **to** L, 4, Q **to** Q, 2, T **to** T, 2, V **to** V, 2, Jedha

Used lowest numbers possible while avoiding planet N

Mission 6.

```
sysadmin@UbuntuDesktop:~/Desktop$ sudo aircrack-ng -w /usr/share/wordlists/rocky
ou.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

     [00:00:01] 2280/8053877 keys tested (1949.74 k/s)

     Time left: 1 hour, 8 minutes, 51 seconds                  0.03%

                             KEY FOUND! [ dictionary ]
```

Terminal

```
     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
ysadmin@UbuntuDesktop:~/Desktop$
```

arp

No.	Time	Source	Destination	Protocol	Source Port	BSS Id	INFO
3…	1146709929.421364	IntelCor_55:9…	Broadcast	ARP		00:0b:86:c2:…	Who has 172.16.0.1? Tell 172.16.0.101
3…	1146709929.422968	IntelCor_55:9…	Broadcast	ARP		00:0b:86:c2:…	Who has 172.16.0.1? Tell 172.16.0.101
3…	1146709929.423426	Cisco-Li_e3:e…	IntelCor_55:9…	ARP		00:0b:86:c2:…	172.16.0.1 is at 00:0f:66:e3:e4:01

```
> Frame 315: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> IEEE 802.11 Data, Flags: .p....F.
> Logical-Link Control
v 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)
```

MAC and IPs…^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

Mission 7.

```
sysadmin@UbuntuDesktop:~/Desktop$ 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:
```

```
                    E p i s o d e  I V

                    A   N E W   H O P E

      I t  i s   a   p e r i o d   o f   c i v i l   w a r.

      R e b e l   s p a c e s h i p s ,   s t r i k i n g

      f r o m   a  h i d d e n   b a s e ,  h a v e  w o n
```