**MISSION 1:**

**Mail Servers:**

sysadmin@UbuntuDesktop:~$ nslookup -type=MX starwars.com

Server: 127.0.0.53

Address: 127.0.0.53#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 = 10 aspmx2.googlemail.com.

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

**Why the resistance isn’t receiving emails:**

The resistance is unable to receive any email because they are using the wrong mail server. They are using asltx.l.google.com and asltx.2.google.com when they should be using the mail servers listed above.

**Corrected DNS Record:**

In order for the resistance to receive emails, their DNS record should look something like the record below.

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

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

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

**MISSION 2:**

**SPF Records:**

sysadmin@UbuntuDesktop:~$ nslookup -type=txt theforce.net

Server: 127.0.0.53

Address: 127.0.0.53#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"

**Why The Force’s emails are going to spam:**

The Force’s emails are going to spam because they didn’t add their IP after the “v=spf1”

**Corrected DNS Record:**

To fix this, the DNS Record should look something like below. Along with any other IP that would be authorized to send from theforce.net.

sysadmin@UbuntuDesktop:~$ nslookup -type=txt theforce.net

Server: 127.0.0.53

Address: 127.0.0.53#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 ip4:45.23.176.21"

**MISSION 3:**

**What CNAME looks like currently:**

Currently, the CNAME for [www.theforce.net](http://www.theforce.net) looks like what's listed below.

sysadmin@UbuntuDesktop:~$ nslookup -type=CNAME www.theforce.net

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

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

**Why the subpage isn’t redirecting:**

The subpage (resistance.theforce.net) is not redirecting to theforce.net simply because the canonical name is not set to the subpage address - resistance.theforce.net.

**What CNAME should look like:**

In order for the subpage to redirect properly, the CNAME should look something like below.

sysadmin@UbuntuDesktop:~$ nslookup -type=CNAME www.theforce.net

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

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

**MISSION 4:**

**Confirmed DNS Records of ‘princessleia.site’:**

sysadmin@UbuntuDesktop:~$ nslookup -type=any princessleia.site

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

Name: princessleia.site

Address: 34.102.136.180

Authoritative answers can be found from:

**How to fix the DNS records to prevent incident:**

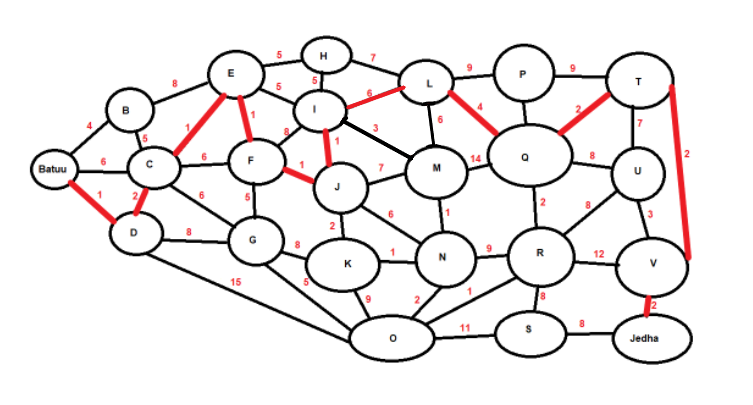
Setup a DDOS mitigation service that will do the following -

* Identify the difference between normal traffic and unwanted traffic on my network
* Regularly scrub my network for unwanted traffic to identify possible DoS attacks ASAP
* Expand the bandwidth on my network in order to resist possible attacks
* Implement load balancers in my network for redundancy

**MISSION 5:**

**Batuu-D-C-E-F-J-I-L-Q-T-V-Jedha**

**TOTAL COST = 23**



**MISSION 6:**

**Aircrack-ng command and output:**

sysadmin@UbuntuDesktop:~/Downloads$ aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt

Aircrack-ng 1.2 rc4

[00:00:00] 2280/8053877 keys tested (2605.39 k/s)

Time left: 51 minutes, 30 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

**HOST IP and MAC Addresses for The Dark Side:**

INTELCOR\_55:98:ef

IP Address - 172.16.0.101

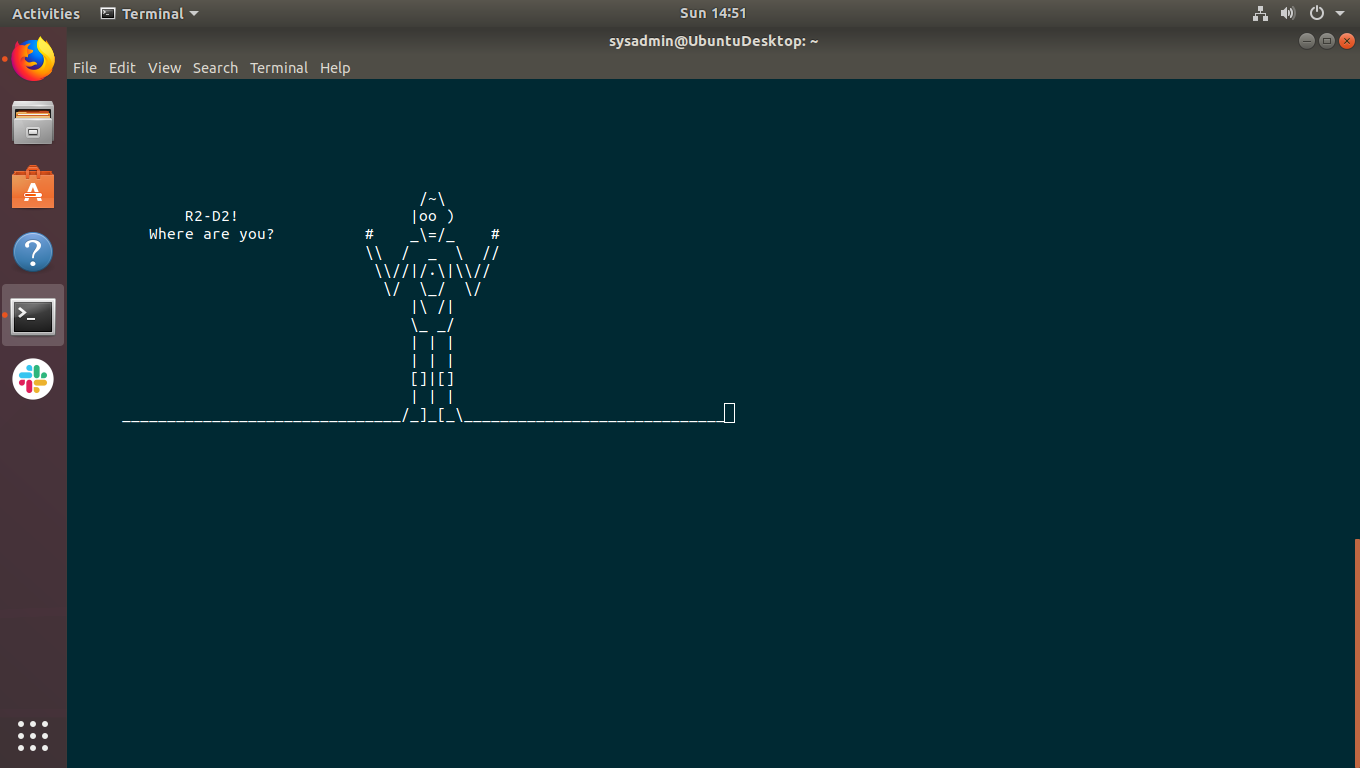
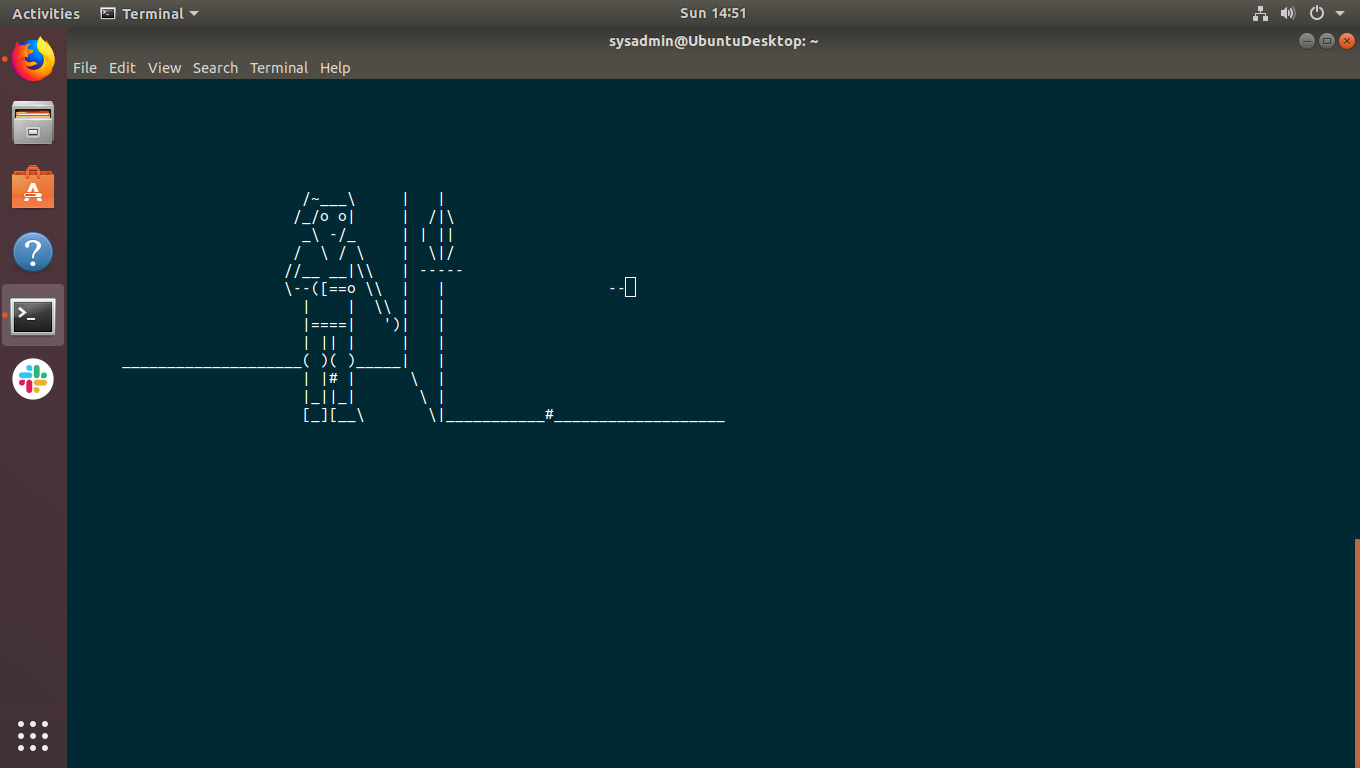
MAC Address - 00:13:ce:55:98:ef

Cisco-Li\_e3:e4:01

IP Address - 172.16.0.1

MAC Address - 00:0f:66:e3:e4:01

**MISSION 7:**

****

**Super cool! Thanks for the free movie!**