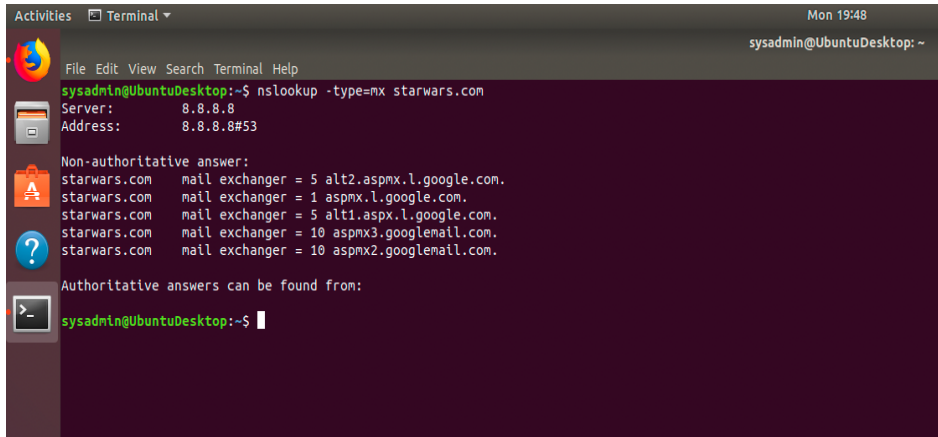


Week 9 Homework: Networks Fundamentals II Homework: *In a Network Far, Far Away!*

Mission 1:

Determine and document the mail servers for starwars.com using NSLOOKUP:



```
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 = 5 alt2.aspmx.l.google.com.
starwars.com mail exchanger = 1 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.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
```

Explain why the Resistance isn't receiving any emails:

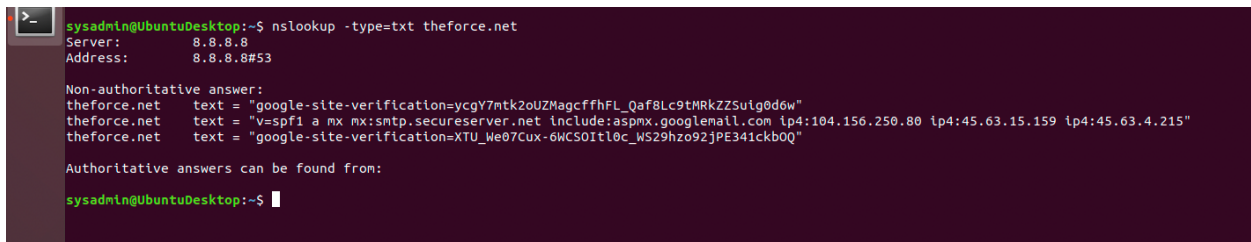
The Resistance isn't receiving any emails because the MX is not set to the new primary and secondary mail server (asltx.l.google.com and asltx.2.google.com).

Document what a corrected DNS record should be:

starwars.com mail exchanger = 5 asltx.2.google.com.
starwars.com mail exchanger = 1 asltx.l.google.com.

Mission 2:

Determine and document the SPF for theforce.net using NSLOOKUP:



```
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=ygy7mtk2oUZMagcFfhFL_Qaf8Lc9tMRkZz5uig0d6w"
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=XTU_We07Cux-6WCS0itl0c_WS29hzo92jPE341ckb0Q"

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
```

Explain why the Force's emails are going to spam:

The Force's emails are going to spam because the DNS record does not include the new sender IP address of 45.23.176.21.

Document what a corrected DNS record should be:

theforce.net text = "v=spf1 a mx mx:smtp.secureserver.net
include:aspmx.googlemail.com ip4: 45.23.176.21 ip4:104.156.250.80 ip4:45.63.15.159
ip4:45.63.4.215"

Mission 3:

Document how a CNAME should look by viewing the CNAME of www.theforce.net using NSLOOKUP:

```
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:

sysadmin@UbuntuDesktop:~$
```

Explain why the sub page of resistance.theforce.net isn't redirecting to theforce.net:

The sub page of resistance.theforce.net isn't redirecting to theforce.net because the DNS record doesn't have a line that lists resistance.theforce.net with a canonical name of theforce.net.

Document what a corrected DNS record should be:

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

Mission 4:

Confirm the DNS records for 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:

sysadmin@UbuntuDesktop:~$
```

Document how you would fix the DNS record to prevent this issue from happening again:

I would add a line with the backup DNS server that The Resistance provided:
princessleia.site nameserver = ns2.galaxybackup.com

Mission 5:

View the Galaxy Network Map and determine the OSPF shortest path from Batuu to Jedha:

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

Confirm your path doesn't include Planet N in its route:

The path does not contain Planet N in its route.

Document this shortest path so it can be used by the Resistance to develop a static route to improve the traffic:

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

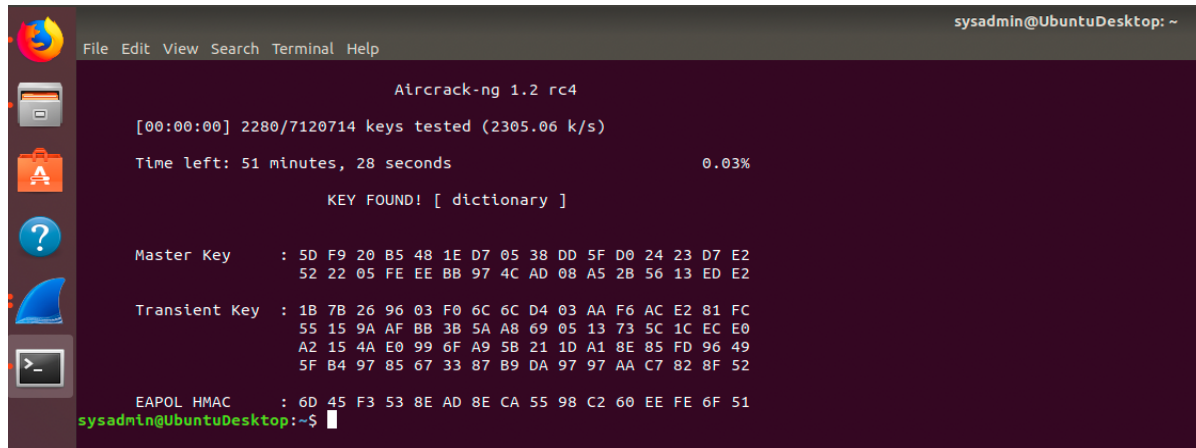
Mission 6:

Figure out the Dark Side's secret wireless key by using Aircrack-ng:

Hint: This is a more challenging encrypted wireless traffic using WPA:

In order to decrypt, you will need to use a wordlist (-w) such as rockyou.txt:

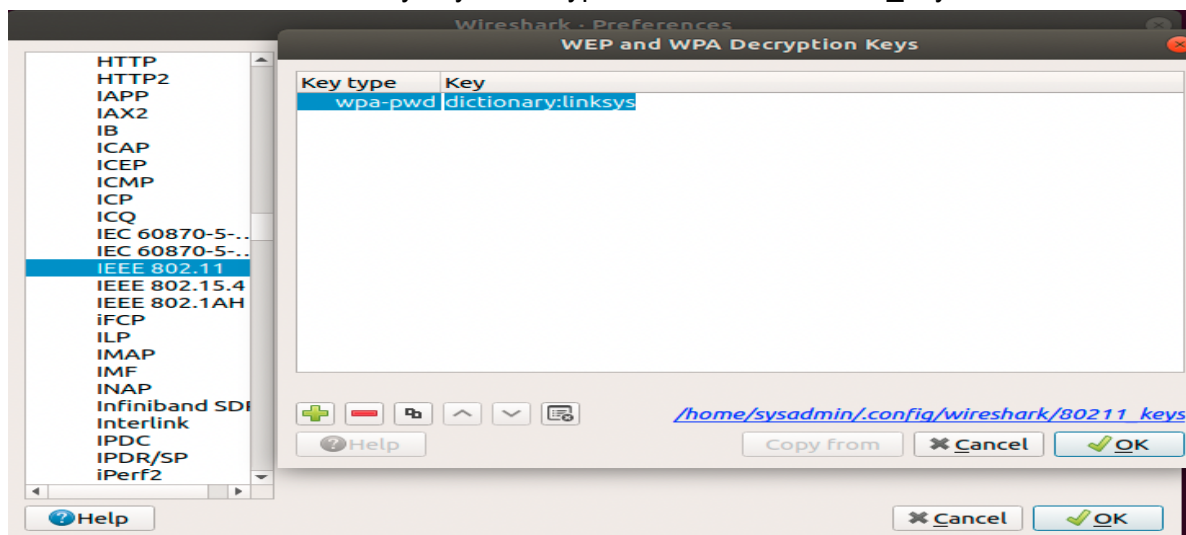
`aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt`



```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
Aircrack-ng 1.2 rc4  
[00:00:00] 2280/7120714 keys tested (2305.06 k/s)  
Time left: 51 minutes, 28 seconds 0.03%  
KEY FOUND! [ dictionary ]  
  
Master Key : 5D F9 20 B5 48 1E D7 05 38 D0 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:~$
```

Use the Dark Side's key to decrypt the wireless traffic in Wireshark:

Hint: The format for the key to decrypt wireless is <Wireless_key>:<SSID>:



Once you have decrypted the traffic, figure out the following Dark Side information:

Host IP Addresses and MAC Addresses by looking at the decrypted ARP traffic:

IP address is at MAC address

172.16.0.1 is at 00:0f:66:e3:e4:01

172.16.0.101 is at 00:13:ce:55:98:ef

Document these IP and MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory attack:

IP address is at MAC address

172.16.0.1 is at 00:0f:66:e3:e4:01

172.16.0.101 is at 00:13:ce:55:98:ef

Mission 7:

View the DNS record from Mission #4.

```
nslookup -type=txt princessleia.site
```

The Resistance provided you with a hidden message in the TXT record, with several steps to follow:

```
sysadmin@UbuntuDesktop:~$ 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:
```

Follow the steps from the TXT record:

Note: A backup option is provided in the TXT record (as a website) in case the main telnet site is unavailable

The main telnet site (telnet towel.blinkenlights.nl) was unavailable so I went to the backup option provided (www.asciimation.co.nz), which worked successfully.

Take a screen shot of the results:

