Homework 9

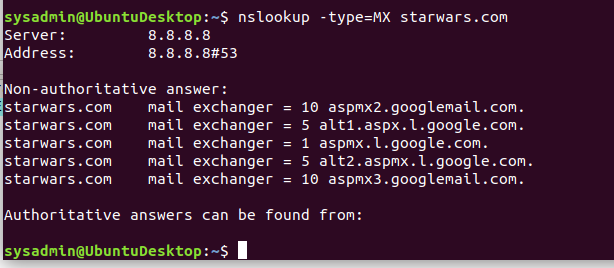
**Your Objectives:**

* Review each network issue in the missions below.
* Document each DNS record type found.
* Take note of the DNS records that can explain the reasons for the existing network issue.
* Provide recommended fixes to save the Galaxy!

**Topics Covered in Your Assignments**

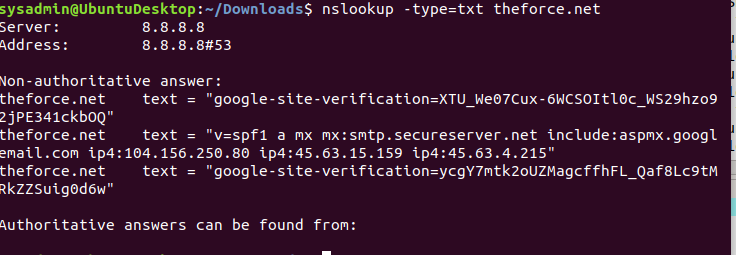
* DNS
* NSLOOKUP
* DNS record types
  + A, PTR, MX, NS, SOA, SRV, TXT
* Wireless
  + WEP, WPA
* Aircrack-ng
* Wireshark Wireless analysis and decryption

**Mission #1**



MX record places the records in numerical order so the first one would be (1) aspmx.l.google.com. The second would be (5) alt1.aspx.l.google.com (5) alt2.aspmx.l.google.com. and last would be the 10’s. The corrected record would have asltx.l.google.com first and then the secondary would be asltx.2.google.com so that it could work correctly

**Mission #2**



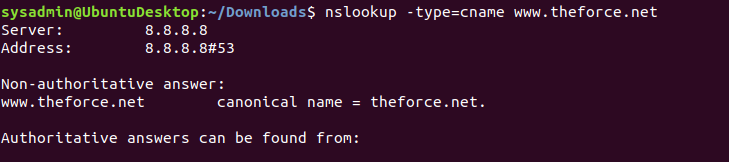
 Determine and document the SPF for theforce.net using NSLOOKUP.

 Explain why the Force's emails are going to spam.

 Document what a corrected DNS record should be.

The forces emails are going to spam because the emails are being routed to the wrong IP address. The IP address that it’s supposed to go to 45.23.176.21 is not listed in the options

**Mission #3**



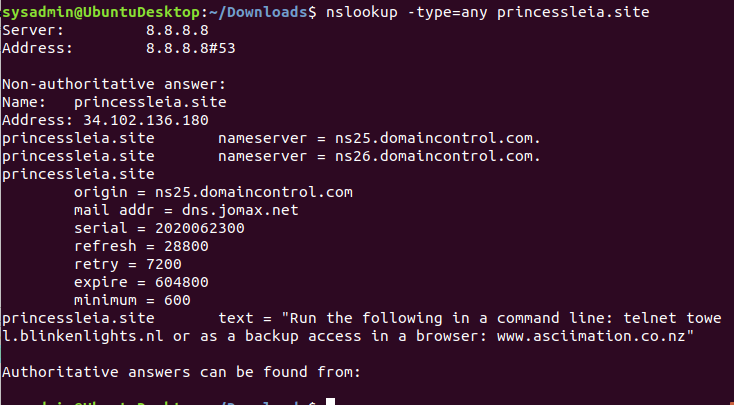
 Document how a CNAME should look by viewing the CNAME of www.theforce.net using NSLOOKUP.

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

 Document what a corrected DNS record should be.

resistance.theforce.net is not linked to to the force.net which is why it isn’t redirecting any of the traffic

**Mission #4**



 Confirm the DNS records for princessleia.site.

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

ns2.galaxybackup.com is not listed on the name server so it cannot be used as a backup since it isn’t linked to the site. The solution would be to add it to the name server so that it can be used when the other servers go down.

**Mission #5**

 Confirm your path doesn't include 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.

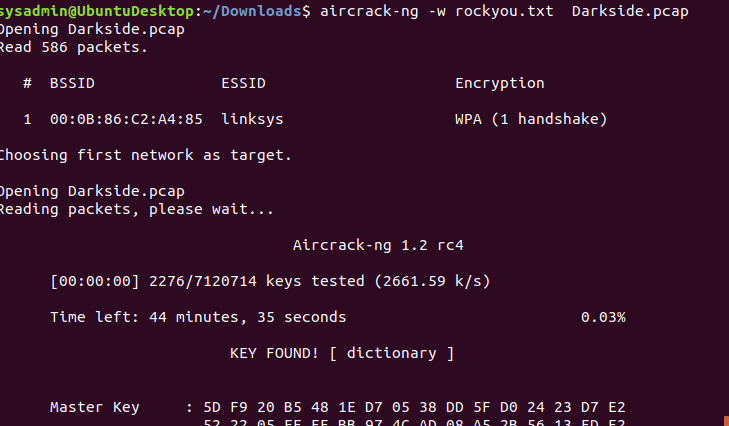
**batuu 🡪 D 🡪 O 🡪 S 🡪 Jedha**

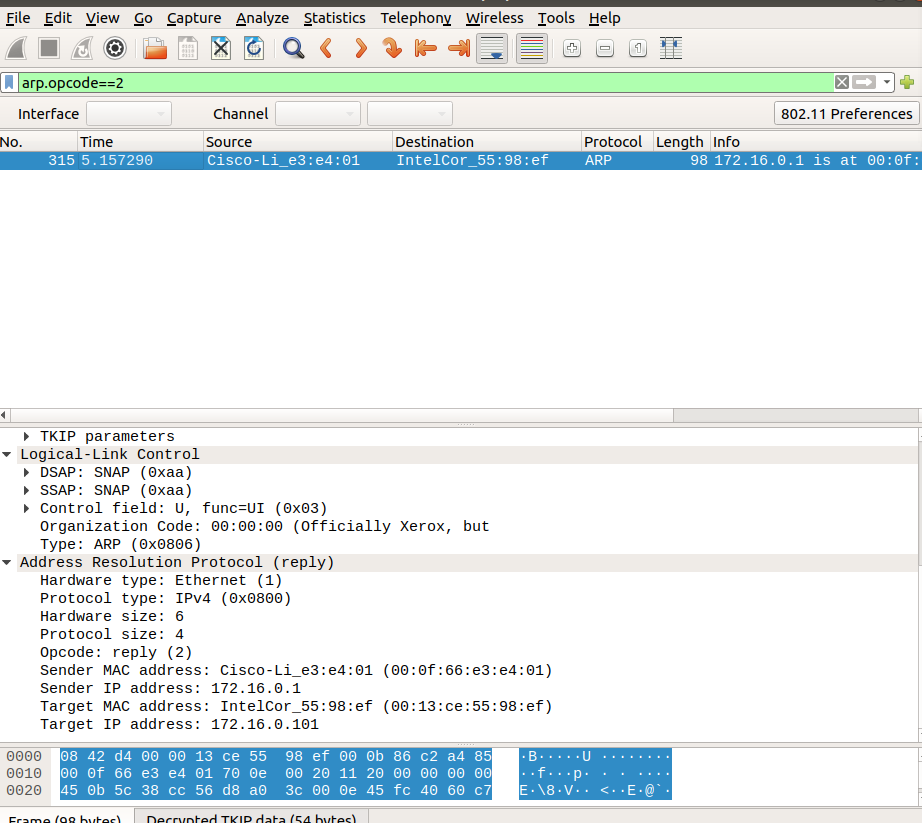
**1 + 15 + 11 + 8 = 35**

**Mission #6**

Your Mission:

* 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.
* Use the Dark Side's key to decrypt the wireless traffic in Wireshark.
  + Hint: The format for they 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.
  + Document these IP and MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory attack.

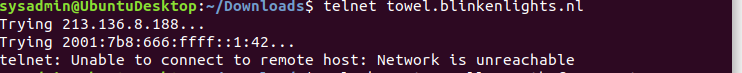


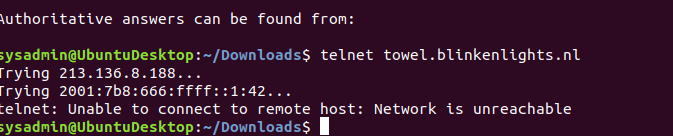


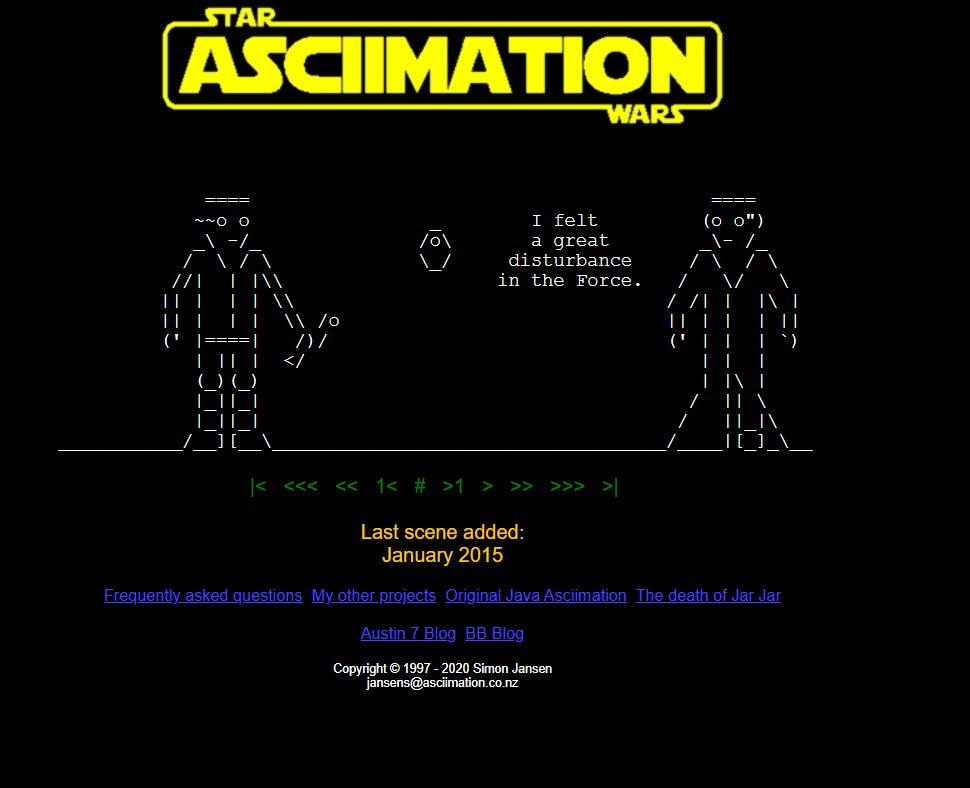
**Mission #7**

Your Mission:

* View the DNS record from Mission #4.
* The Resistance provided you with a hidden message in the TXT record, with several steps to follow.
* 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
* Take a screen shot of the results.







Running the command in command line timed out so I visited the website a took a screenshot of it.