

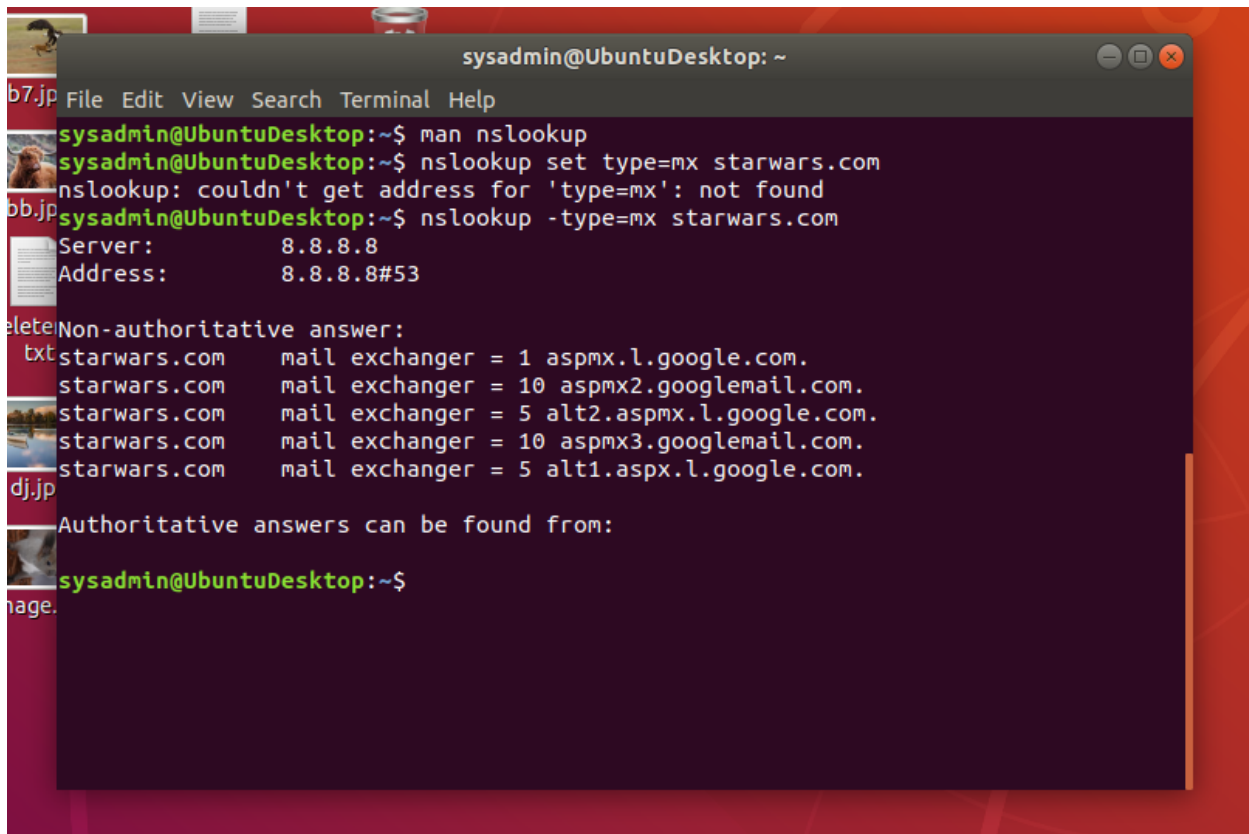
Mission 1

Issue: Due to the DoS attack, the Empire took down the Resistance's DNS and primary email servers.

- The Resistance's network team was able to build and deploy a new DNS server and mail server.
- The new primary mail server is `asltx.l.google.com` and the secondary should be `asltx.2.google.com`.
- The Resistance (`starwars.com`) is able to send emails but unable to receive any.

Your mission:

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



```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
sysadmin@UbuntuDesktop:~$ man nslookup  
sysadmin@UbuntuDesktop:~$ nslookup set type=mx starwars.com  
nslookup: couldn't get address for 'type=mx': not found  
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 = 1 aspmx.l.google.com.  
starwars.com mail exchanger = 10 aspmx2.googlemail.com.  
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.  
starwars.com mail exchanger = 10 aspmx3.googlemail.com.  
starwars.com mail exchanger = 5 alt1.aspx.l.google.com.  
  
Authoritative answers can be found from:  
  
sysadmin@UbuntuDesktop:~$
```

- Explain why the Resistance isn't receiving any emails.
 - The servers `asltx.l.google.com` & `asltx.2.google.com` are not being used.
- Document what a corrected DNS record should be.

Non-authoritative answer:

```
starwars.com mail exchanger = 5 aspmx.l.google.com.  
starwars.com mail exchanger = 10 aspmx2.googlemail.com.  
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.  
starwars.com mail exchanger = 10 aspmx3.googlemail.com.  
starwars.com mail exchanger = 5 alt1.aspx.l.google.com.  
starwars.com mail exchanger = 0 asltx.l.google.com  
starwars.com mail exchanger = 1 asltx.2.google.com
```

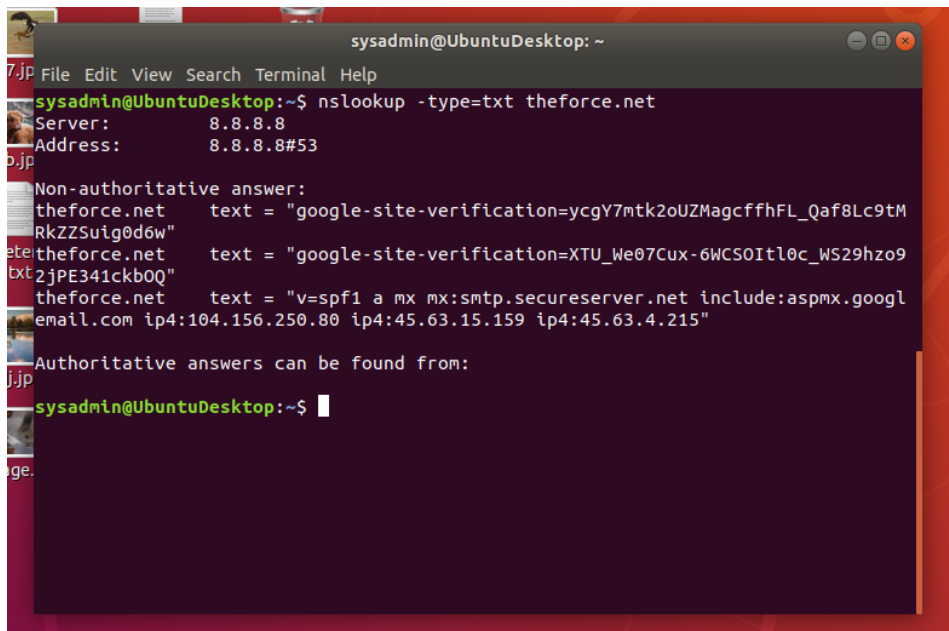
Mission 2

Issue: Now that you've addressed the mail servers, all emails are coming through. However, users are still reporting that they haven't received mail from the theforce.net alert bulletins.

- Many of the alert bulletins are being blocked or going into spam folders.
- This is probably due to the fact that theforce.net changed the IP address of their mail server to 45.23.176.21 while your network was down.
- These alerts are critical to identify pending attacks from the Empire.

Your mission:

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



```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
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=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"  
theforce.net text = "google-site-verification=XTU_We07Cux-6WCSOIItl0c_WS29hzo92jPE341ckbOQ"  
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"  
  
Authoritative answers can be found from:  
sysadmin@UbuntuDesktop:~$
```

- Explain why the Force's emails are going to spam.
 - The IP 45.23.176.21 is not listed with the others so it is not being accepted
- Document what a corrected DNS record should be.

Non-authoritative answer:

theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"

theforce.net text = "google-site-verification=XTU_We07Cux-6WCSOIItl0c_WS29hzo92jPE341ckbOQ"

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 ip445.23.176.21"

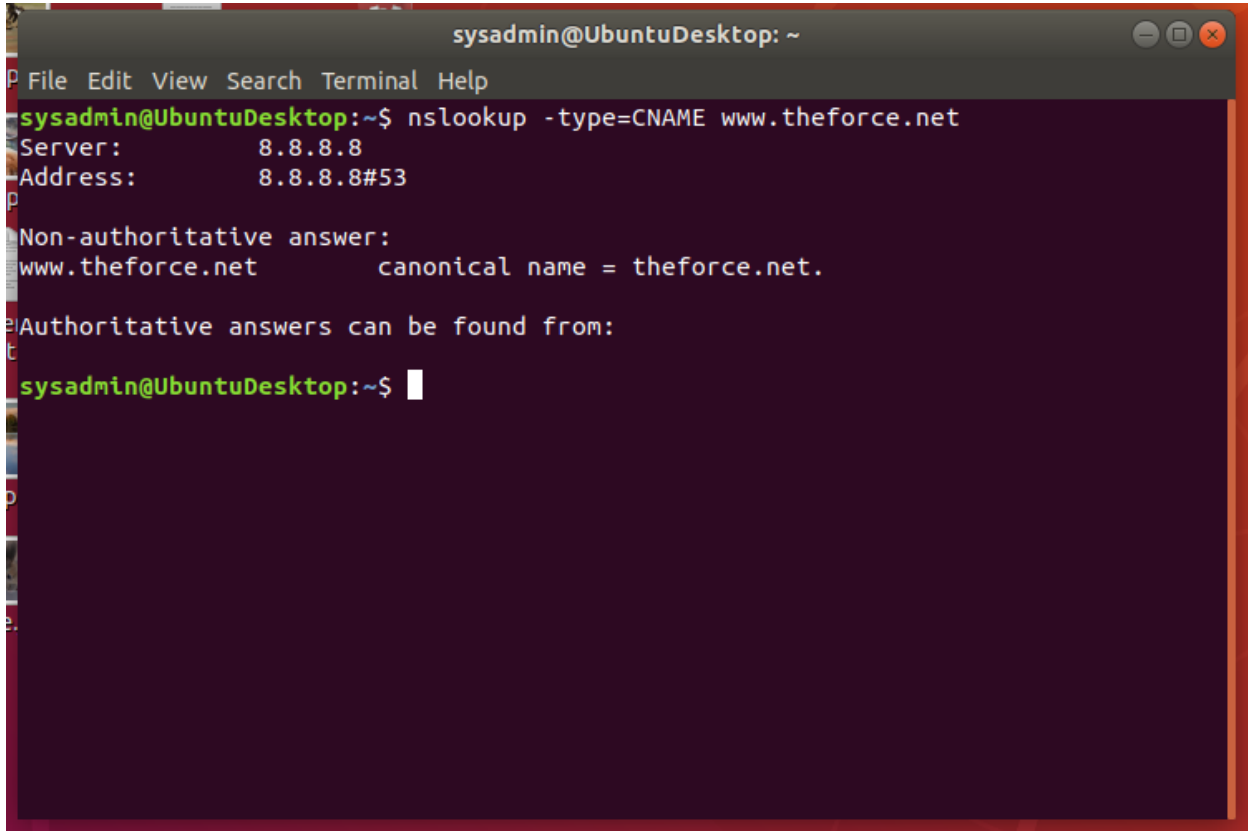
Mission 3

Issue: You have successfully resolved all email issues and the resistance can now receive alert bulletins. However, the Resistance is unable to easily read the details of alert bulletins online.

- They are supposed to be automatically redirected from their sub page of resistance.theforce.net to theforce.net.

Your mission:

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



```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
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 CNAME has not been set up correctly. It is missing the “resistance” at the beginning
- Document what a corrected DNS record should be.

Non-authoritative answer:

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

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

Authoritative answers can be found from:

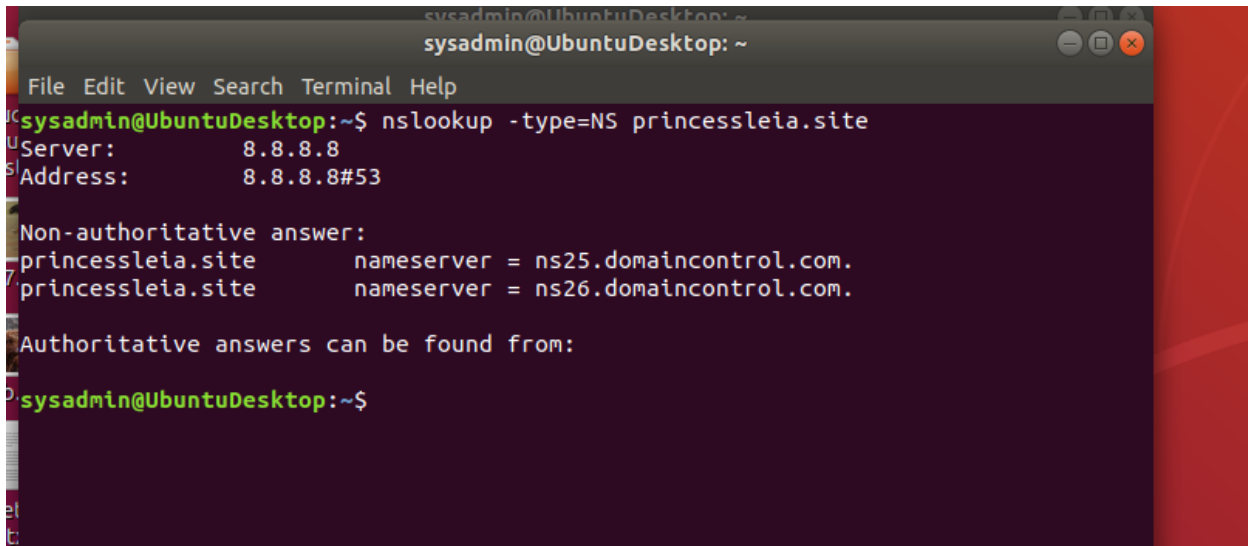
Mission 4

Issue: During the attack, it was determined that the Empire also took down the primary DNS server of princessleia.site.

- Fortunately, the DNS server for princessleia.site is backed up and functioning.
- However, the Resistance was unable to access this important site during the attacks and now they need you to prevent this from happening again.
- The Resistance's networking team provided you with a backup DNS server of: ns2.galaxybackup.com.

Your mission:

- Confirm the DNS records for princessleia.site.
- Document how you would fix the DNS record to prevent this issue from happening again.

A terminal window titled 'sysadmin@UbuntuDesktop: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'sysadmin@UbuntuDesktop:~\$'. The command 'nslookup -type=NS princessleia.site' has been entered. The output shows 'Server: 8.8.8.8' and 'Address: 8.8.8.8#53'. Below this, it says 'Non-authoritative answer:' followed by two lines: 'princessleia.site nameserver = ns25.domaincontrol.com.' and 'princessleia.site nameserver = ns26.domaincontrol.com.'. Then it says 'Authoritative answers can be found from:' and the prompt returns to 'sysadmin@UbuntuDesktop:~\$'.

```
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
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:~$
```

It needs to be changed to:

Non-authoritative answer:

princessleia.site nameserver = ns25.domaincontrol.com.

princessleia.site nameserver = ns2.galaxybackupl.com.

Mission 5

Issue: The network traffic from the planet of Batuu to the planet of Jedha is very slow.

- You have been provided a network map with a list of planets connected between Batuu and Jedha.
- It has been determined that the slowness is due to the Empire attacking Planet N.

Your Mission:

- View the Galaxy Network Map and determine the OSPF shortest path from Batuu to Jedha.
- 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,C,E,F,J,I,L,Q,T,V,JEDHA

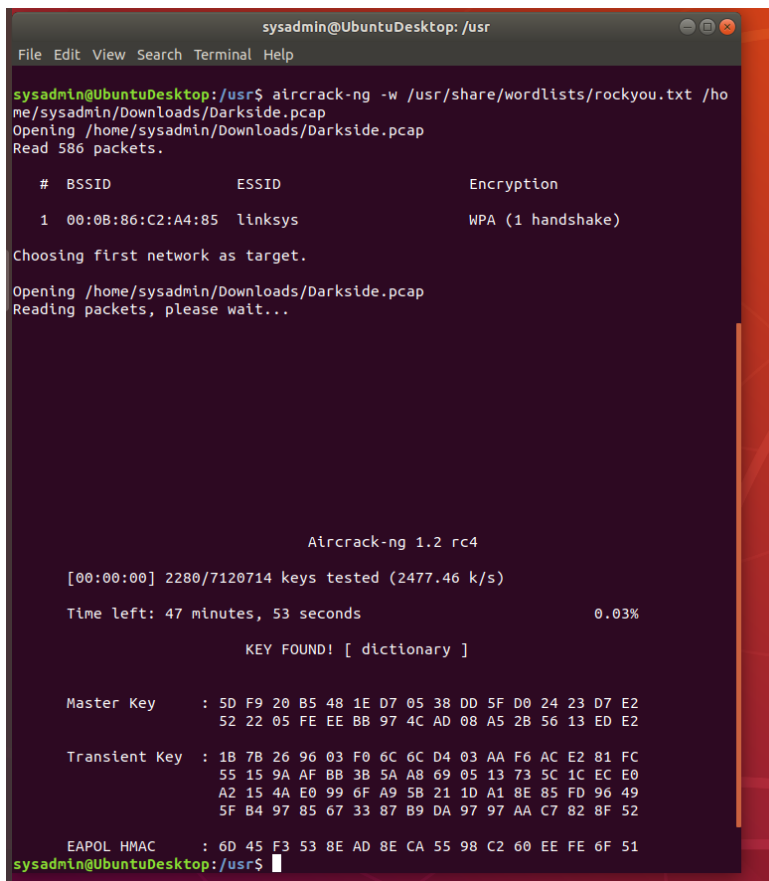
Mission 6

Issue: Due to all these attacks, the Resistance is determined to seek revenge for the damage the Empire has caused.

- You are tasked with gathering secret information from the Dark Side network servers that can be used to launch network attacks against the Empire.
- You have captured some of the Dark Side's encrypted wireless internet traffic in the following pcap: Darkside.pcap.

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.



```
sysadmin@UbuntuDesktop: /usr
File Edit View Search Terminal Help

sysadmin@UbuntuDesktop: /usr$ aircrack-ng -w /usr/share/wordlists/rockyou.txt /home/sysadmin/Downloads/Darkside.pcap
Opening /home/sysadmin/Downloads/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 /home/sysadmin/Downloads/Darkside.pcap
Reading packets, please wait...

Aircrack-ng 1.2 rc4

[00:00:00] 2280/7120714 keys tested (2477.46 k/s)

Time left: 47 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
sysadmin@UbuntuDesktop: /usr$
```

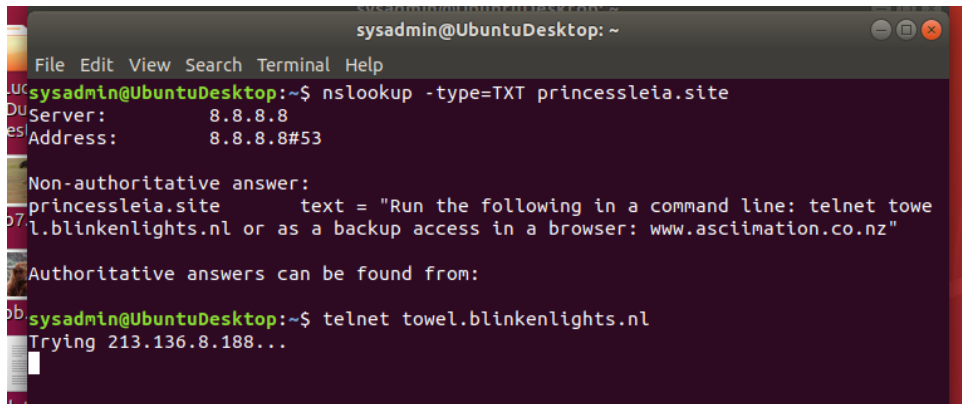
- Use the Dark Side's key to decrypt the wireless traffic in Wireshark.
 - Hint: The format for the key to decrypt wireless is <Wireless_key>:<SSID>.
- Once you have decrypted the traffic, figure out the following Dark Side information:
 - Host IP Addresses and MAC Addresses by looking at the decrypted ARP traffic.
 - Host IP - 172.16.0.101
 - Host MAC Address - 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.

Mission 7

As a thank you for saving the galaxy, the Resistance wants to send you a secret message!

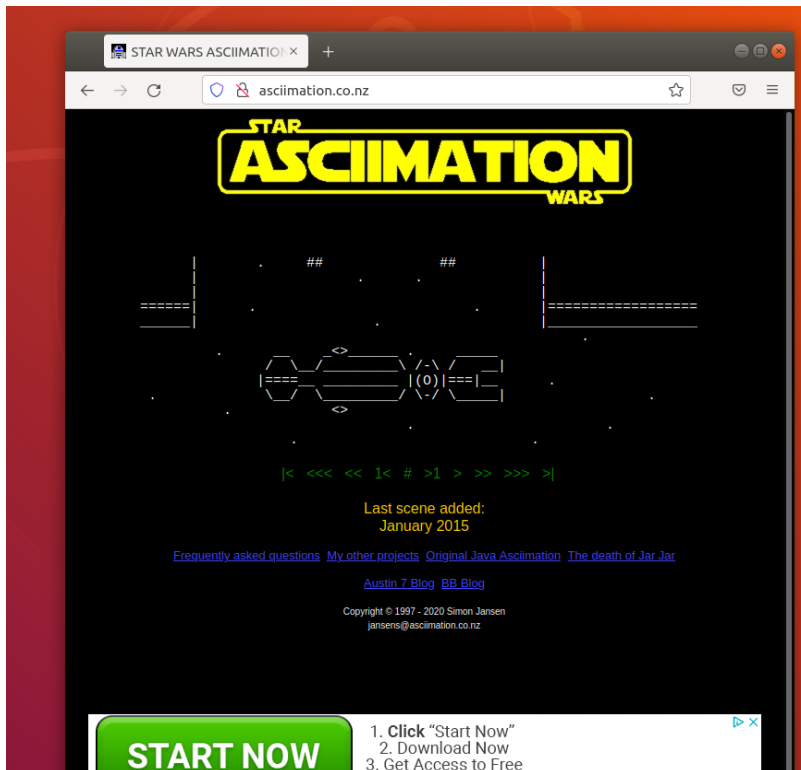
Your Mission:

- 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



```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
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.ascimation.co.nz"  
Authoritative answers can be found from:  
sysadmin@UbuntuDesktop:~$ telnet towel.blinkenlights.nl  
Trying 213.136.8.188...
```

- Take a screen shot of the results.



Conclusion

- Submit your results and findings from every mission.
- Congratulations, you have completed your mission and saved the Galaxy!