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.

> **Non-authoritative** answer:
> **starwars.com** mail exchanger = 1 aspmx.l.google.com.
> **starwars.com** mail exchanger = 5 alt1.aspx.l.google.com.
> **starwars.com** mail exchanger = 5 alt2.aspmx.l.google.com.
> **starwars.com** mail exchanger = 10 aspmx3.googlemail.com.
> **starwars.com** mail exchanger = 10 aspmx2.googlemail.com.

MX Records are pointing to different server locations than expected for secondary server
Corrected MX records should be:
Non-authoritative answer:
starwars.com mail exchanger = 1 aspmx.l.google.com.
starwars.com mail exchanger = 5 **asltx.2.google.com**.

Mission 2

Your mission:

- 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=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:**45.23.176.21**"
```

- Explain why the Force's emails are going to spam.
- **Expected IP address for mail server is not listed in SPF string, as a result the destination mail server is being flagged as malicious**
- Document what a corrected DNS record should be.
-

```
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=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"

Mission 3

Your mission:

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

Authoritative answers can be found from:
theforce.net
origin = WebPublish_Othe
mail addr = hostmaster
serial = 2017110901
refresh = 900
retry = 600
expire = 86400
minimum = 3600

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

  There are no canonical CName records for resistance.theforce.net or

www.theforce.net

```
Authoritative answers can be found from:
> resistance.theforce.net
Server:        8.8.8.8
Address:    8.8.8.8#53

** server can't find resistance.theforce.net: NXDOMAIN
```

- Document what a corrected DNS record should be.

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

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`.

```
nslookup
> set 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.
```

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

To correct the issue, the secondary nameserver should be changed from ns26.domaincontrol.com to ns2.galaxybackup.com

Mission 5

determine the `OSPF` shortest path from `Batuu` to `Jedha`.
Batuu>
D>C>E>F>J>I>L>Q>T>V
1 2 1 1 1 6 4 2 2 : 21 hops total

- Confirm your path doesn't include `Planet N` in its route.

  Batuu>D>C>E>F>J>I>L>Q>T>V

- Document the 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

Mission 6

dictionary:linksys

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

  Sender: Cisco-Li | MAC 00:0f:66:e3:e4:01 | IP 172.16.0.1

  Target: IntelCor_55:98:ef | MAC 00:13:ce:55:98:ef | IP 172.16.0.101

Mission 7

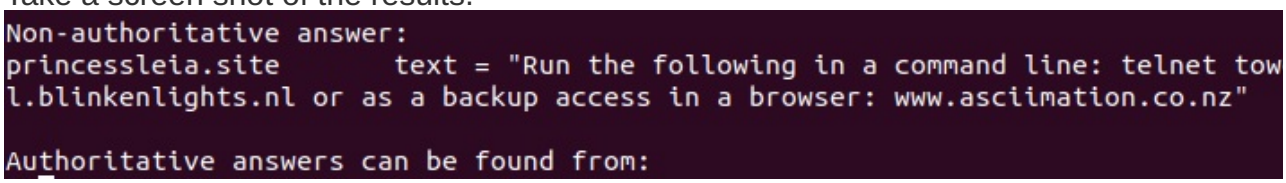
As a thank you for saving the galaxy, the Resistance wants to send you a secret message!

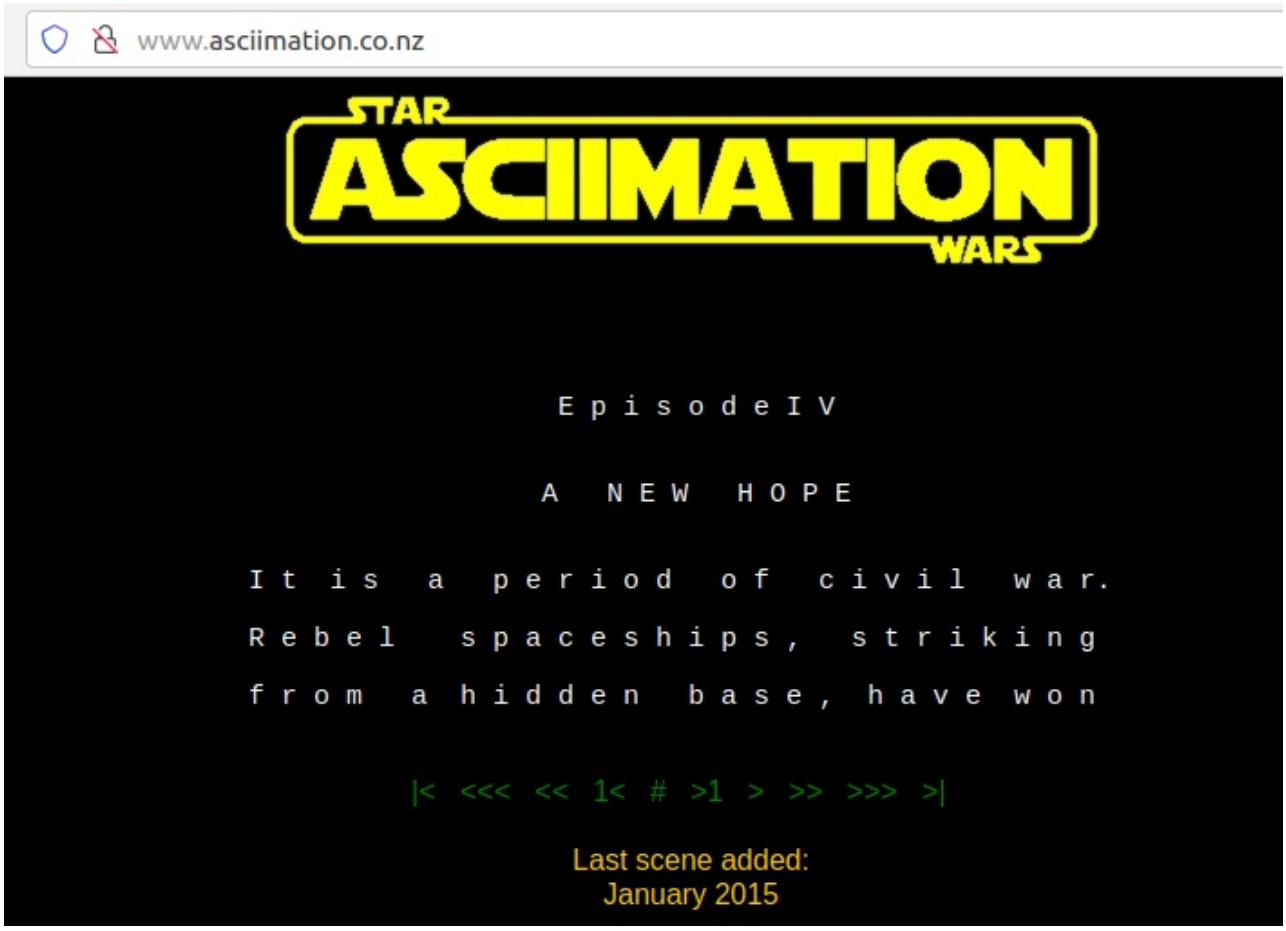
Your Mission:

- 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.

```
- nslookup
- set q = txt
- princessleia.site
```

- Take a screen shot of the results.




www.asciimation.co.nz
STAR
ASCIIMATION
WARS
EpisodeIV
A NEW HOPE
It is a period of civil war.
Rebel spaceships, striking
from a hidden base, have won
|< <<< << 1< # >1 > >> >>> >|
Last scene added:
January 2015