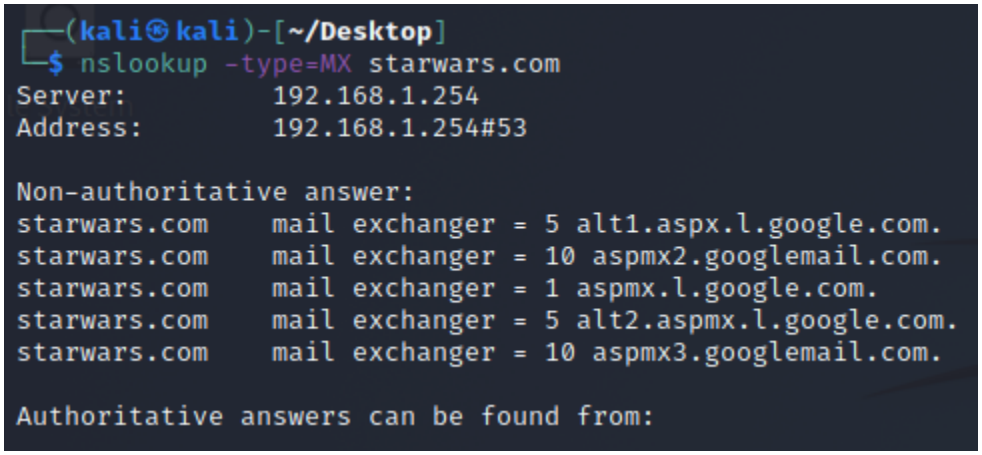
Mission 1

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.



The new primary mail server is `asltx.l.google.com` and the secondary should be `asltx.2.google.com`.

This is most suspicious.

- Explain why the Resistance isn't receiving any emails.
  According to the data given to us, the Resistance aren't receiving any emails because the MX records show that the primary and secondary mail servers are not the same as the provided ones of "asltx.l.google.com" and "asltx.2.google.com"

- Document what a corrected DNS record should be:
  starwars.com mail exchanger = 1 asltx.l.google.com
- starwars.com mail exchanger = 5 asltx.2.google.com

With 1 being the highest priority and 5 following as the next highest priority

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.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nslookup -type=TXT theforce.net
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
theforce.net    text = "google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29
hzo92jPE341ckbOQ"
theforce.net    text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8L
c9tMRkZZSuig0d6w"
theforce.net    text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.g
ooglemail.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"

Authoritative answers can be found from:
```

- Explain why the Force's emails are going to spam.
  Theforce.net had not updated their DNS text file to include the updated mail IP address of “45.23.176.21”
- Document what a corrected DNS record should be.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nslookup -type=TXT 45.23.176.21
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
21.176.23.45.in-addr.arpa       name = 45-23-176-21.lightspeed.rcsntx.sbcglobal.net.

Authoritative answers can be found from:
```

Here is the corrected DNS record

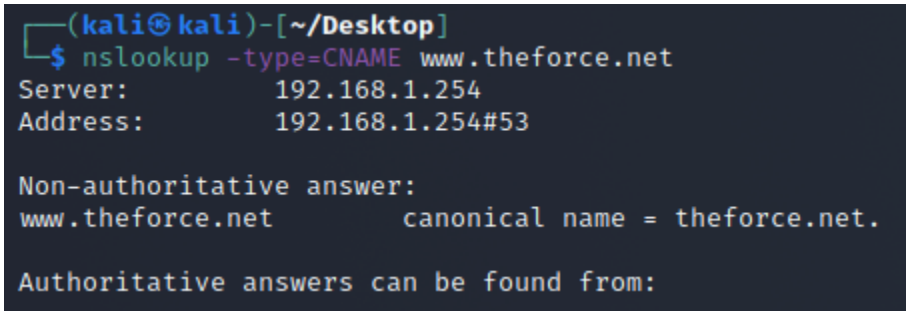
Mission 3

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.



- Explain why the sub page of resistance.theforce.net isn't redirecting to theforce.net.
  The DNS CNAME is a missing a reference for “resistance.theforce.net” associated with “theforce.net”
- Document what a corrected DNS record should be.
  The correction should be:

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

Mission 4

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

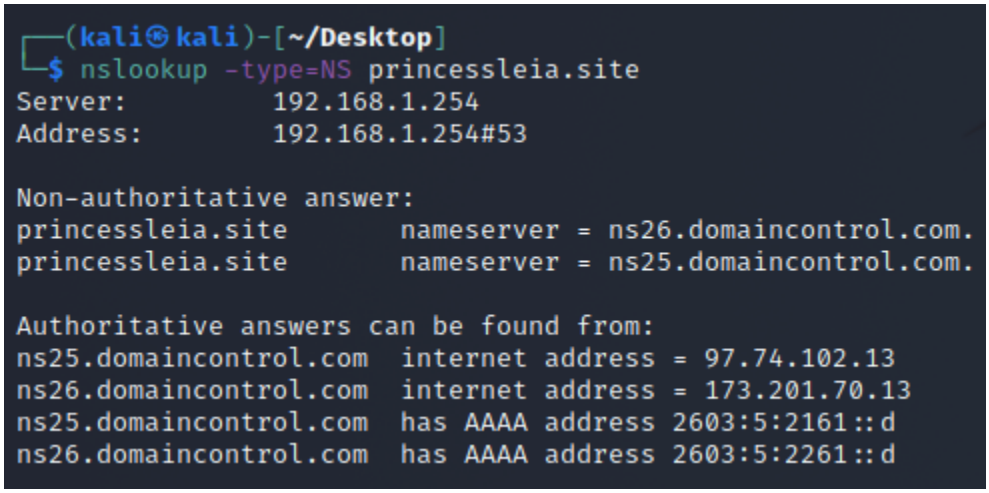
- Fortunately, the DNS server for princessleia.site is backed up and functioning.

- 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.



Our nameservers are:

princessleia.site nameserver = ns26.domaincontrol.com

princessleia.site nameserver = ns25.domaincontrol.com

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

The fix is relatively straight forward. We need to add a reference to the DNS backup server under our current list of names servers using the backup provided as “ns2.galaxybackup.com”. It would look like this:

princessleia.site nameserver = ns26.domaincontrol.com

princessleia.site nameserver = ns25.domaincontrol.com

princessleia.site nameserver = ns2.galaxybackup.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.

D C E F J I L Q T V Jedha

1 2 1 1 1 1 6 4 2 2 2 -----> 23 hops

- 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.

Planet Batuu → D → C → E → F → J → I → L → Q → T → V → Planet 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.

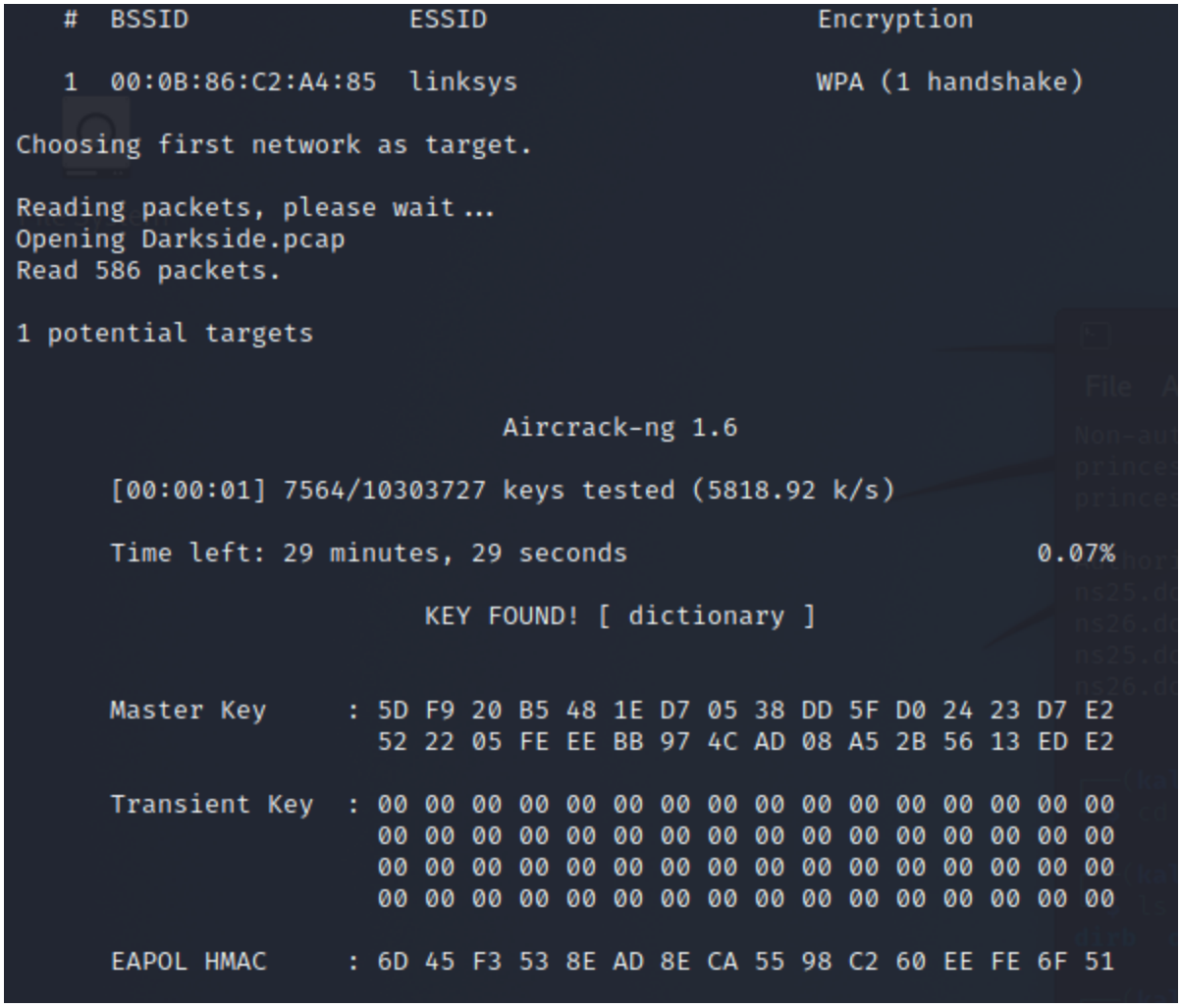
- You have captured some of the Dark Side's encrypted wireless internet traffic in the following pcap: Darkside.pcap.

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.

```
┌──(kali㉿kali)-[~/…/ucsd-sd-virt-cyber-pt-09-2021-u-c/2-Homework/09-Networking-Fundamentals-II-and-CTF-Review/resources]
└─$ aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt
```

So we're going to run this command.



Key was found to be “dictionary”

- 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>.

So now we need to go into wireshark with the key to decrypt. So We’re going to go to Edit > preferences > Protocols > IEEE 802.11 > Decryption keys “edit” > set to wpa-pwd and add “dictionary”

- 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. **We have a Broadcast sent out by IntelCor_55:98:ef with an IP of 172.16.0.101 and a MAC of 00:13:CE:55:98:ef**

The Receiving/Destination that replies is by Cisco-Li_e3:e4:01 with an IP address of 172.16.0.1 with a MAC of 00:0f:66:e3:e4:01

Other Items of Note:

68.9.16.30 is at 00:0f:66:e3:e4:01, which is the same MAC as 68.9.16.25 at 00:0f:66:e3:e4:01 which is also the same MAC as - 172.16.0.1

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

IntelCor_55:98:ef with an IP of 172.16.0.101 and a MAC of 00:13:CE:55:98:ef

Cisco-Li_e3:e4:01 with an IP address of 172.16.0.1 with a MAC of 00:0f:66:e3:e4:01

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.

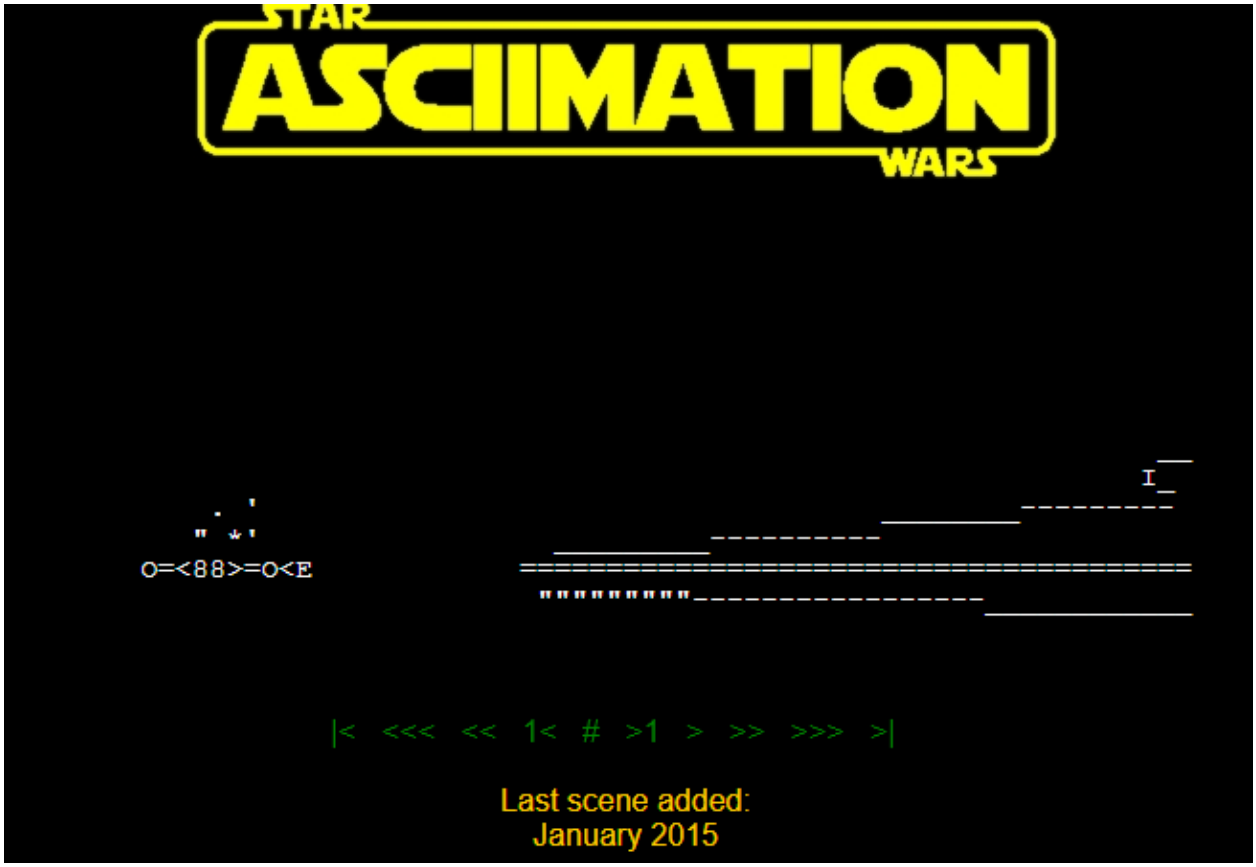
```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ nslookup -type=TXT princessleia.site
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
princessleia.site       text = "Run the following in a command line: telnet towel.blinkenlights.n
l or as a backup access in a browser: www.asciimation.co.nz"

Authoritative answers can be found from:
```

Quite interesting, let's test it out.

- 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

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ telnet towel.blinkenlights.nl
Trying 213.136.8.188 ...
Trying 2001:7b8:666:ffff::1:42 ...
telnet: Unable to connect to remote host: Network is unreachable
```

Well it did not work like intended so we will have to use the link.



Kek, it’s the opening from StarWars Episode IV: A New Hope.

- 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!