**<MoJarju> <Homework-9>**

**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.**

Nslookup -type=MX starwars.com

* + Server: 8.8.8.8
  + Address: 8.8.8.8#53
  + Non-authoritative answer:
  + 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.
  + starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.
  + starwars.com mail exchanger = 1 aspmx.l.google.com.
* **Explain why the Resistance isn't receiving any emails.**
  + The above servers are not the accurate asltx.1.googe.com and asltx.2.google.com servers. These servers have been changed.
* **Document what a corrected DNS record should be.**
  + The correct servers should be asltx.1.googe.com and 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.**
  + - nslookup -type=txt theforce.net

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=ycgY7mtk2oUZMagcffhFL\_Qaf8Lc9tMRkZZSuig0d6w"

theforce.net text = "google-site-verification=XTU\_We07Cux-6WCSOItl0c\_WS29hzo92jPE341ckbOQ"

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

Since the sender's IP are ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215" (**Not the allowed ip 45.23.176.21**), theforce.net mail server can identify the email as spam and potentially reject it or send it to the recipient's spam folder

* **Document what a corrected DNS record should be.**

These servers (ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215) need to be corrected to the allowed mail server ip 45.23.176.21

**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.**

Nslookup -type=CNAME [www.theforce.net](http://www.theforce.net)

* **Explain why the sub page of resistance.theforce.net isn't redirecting to theforce.net**.
  + Comes back being redirected with theforce.net not resistance.theforce.net
* **Document what a corrected DNS record should be.**
  + The above should be change to redirect resistance.theforce.net to theforce.net
  + Resistance.theforce.net comes back NXDOMAIN

**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.**
  + Non-authoritative answer: text = "Run the following in a command line: telnet towel.blinkenlights.nl or as a backup access in a browser: www.asciimation.co.nz"
* **Document how you would fix the DNS record to prevent this issue from happening again.**
  + It looks like princessleia.site is being redirected to be above url. We should fix that and add the back up ns2.galaxybackup.com dns server.

**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**](/GW-Coding-Boot-Camp/gwu-wdc-cyber-pt-10-2020-u-c/raw/master/2-Homework/09-Networking-Fundamentals-II-and-CTF-Review/resources/Galaxy_Network_map.png) **and determine the OSPF shortest path from Batuu to Jedha.** 
  + Batuu-D-C-E-F-J-K-O-R-V—JEDHA = 32
* **Confirm your path doesn't include Planet N in its route.**
  + The above bypasses ‘N’ from ‘K>O>R
* **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-K-O-R-V—JEDHA is the shortest @ 32

**Mission 6**

Your Mission:

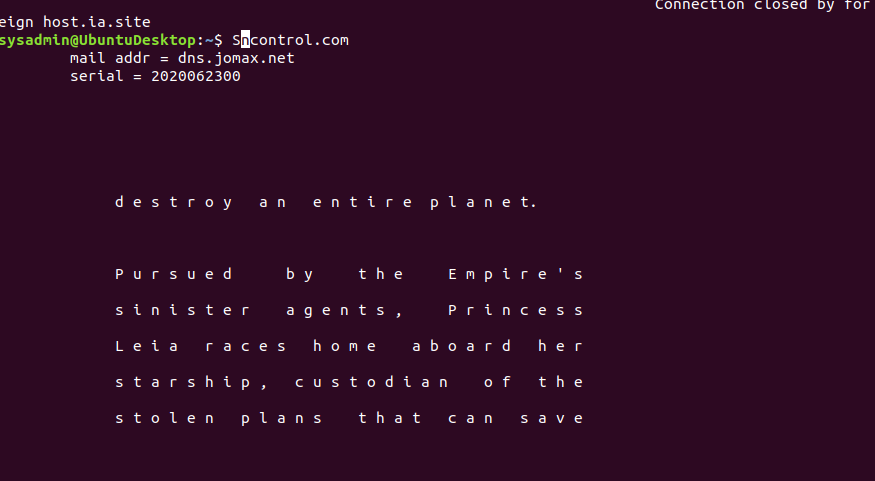
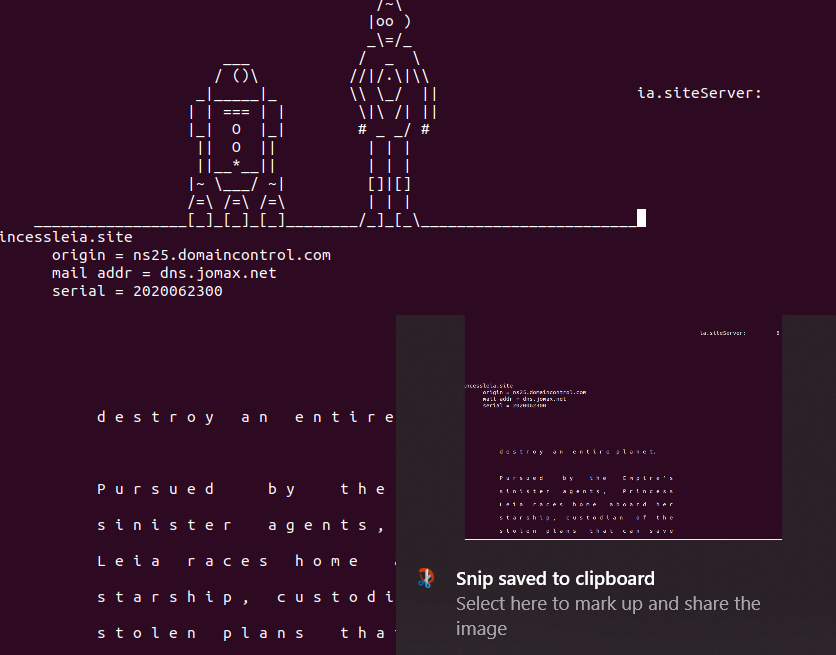
* Figure out the Dark Side's secret wireless key by using Aircrack-ng.
  + Hint: This is a more challenging encrypted wireless traffic using WPA.
  + In order to decrypt, you will need to use a wordlist (-w) such as rockyou.txt.
* Use the Dark Side's key to decrypt the wireless traffic in Wireshark.
  + 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**.
    - Wpa-pwd=dictionary:linksys Wep=00:0B:86:C2:A4:85
    - Host IP: 172.16.0.101
    - Sender 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.**
    - Host IP: 172.16.0.101
    - Sender MAC address: 00:13:ce:55:98:ef
    - Target IP: 172.16.0.1
    - Target MAC: 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.
* **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**. (Ben Kenobi, luke, Red…)

**Conclusion**

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