Senko Salihbegovic - Week 9 Homework

Mission 1

First task is asking us to check the Resistance's (starwars.com) mail servers. We can get that by using the nslookup command:

nslookup -type=MX starwars.com
*-type=MX signifies that we want to look at the MX record which stands for mail exchange.

Result:
starwars.com mail exchanger = 10 aspmx2.googlemail.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 = 1 aspmx.l.google.com.
starwars.com mail exchanger = 10 aspmx3.googlemail.com.

Now, in the assignment it says that because of a DoS attack that disabled the primary mail servers, a new DNS server and a new mail server have been built and deployed. It says that "The new primary mail server is `asltx.l.google.com` and the secondary should be `asltx.2.google.com`" and that the Resistance can send but not receive emails.

The result of our nslookup query is also the answer to the riddle. While a new mail server was indeed deployed, the MX record was not updated and since Resistance can't receive any emails it means that all of the mail servers in the MX record are compromised. The MX record needs to be updated with the new mail server information mentioned above.

The updated MX record should look something like this:

starwars.com mail exchanger = 5 asltx.2.google.com
starwars.com mail exchanger = 1 asltx.l.google.com

Since this time there is a primary and only one secondary server, the MX record is a bit shorter (2 servers down from 5) but the preference numbers have been set correctly.

Mission 2

For this mission the Resistance is reporting that they're not receiving emails from theforce.net allert bulletins. Many of the alert bulletins are being blocked or going into spam folders.
Also we find out that theforce.net has changed the IP address of their mail server to 45.23.176.21 while Resistance's network was down.

This indicates that SPF (sender policy framework) record probably hasn't been updated to include the new mail server IP.

To check this, we'll be using the nslookup command again:

nslookup -type=txt theforce.net
*This time we're looking for TXT record since SPF record is a computer-readable TXT data.

Result:
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=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"
theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"

Once again the result of the nslookup gives us the answer. The IP addresses we see here are the ones allowed to send email. The reason why the emails from theforce.net are going to spam folders or are being blocked is that the new mail server IP is not on the SPF record so when the receiving mail server checks the senders mail server IP there will be a mismatch with the SPF record which will lead the receiving mail server to think that the email's are not from the genuine sender and are spam.

The updated SPF record should look something like this:

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 ip4:45.23.176.21"
theforce.net text = "google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"
theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"

The whole TXT record stays pretty much the same with the addition of the new IP address to the SPF record.

Mission 3

In this mission the Resistance is saying that they have problem reading alert bulletins online. The problem is that they should be automatically redirected from their subpage ‘resistance.theforce.net’ to ‘theforce.net’.

This looks like the problem lies in the CNAME (canonical name) record which is used to point one domain to another. The command used for this is:

nslookup -type=CNAME www.theforce.net

Result:
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:

Yet again the answer is right before us. The reason resistance.theforce.net is not pointing to theforce.net is because it is no longer in the CNAME record. To fix this, we need to add it.

Fixed CNAME record should look something like this:
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
www.theforce.net canonical name = theforce.net.
theforce.net canonical name = resistance.theforce.net

Authoritative answers can be found from:

Now when typing in the resistance.theforce.net domain, the user should be autmatically redirected to theforce.net.

Mission 4

For this mission we are asked to confirm DNS records for princessleia.site. During the attack, the Empire took the primary DNS down. Fortunately the DNS was backed up and restored. The problem was that the Resistance couldn't access the site during the attack and have asked us to prevent this from happening again.

By running the next command we can see the DNS records for princessleia.site:

nslookup -type=NS princessleia.site
*NS (name server) Record

Result:

Server: 162.252.172.57
Address: 162.252.172.57#53

Non-authoritative answer:
princessleia.site nameserver = ns26.domaincontrol.com.
princessleia.site nameserver = ns25.domaincontrol.com.

Authoritative answers can be found from:

Now we can see the DNS records for princessleia.site.

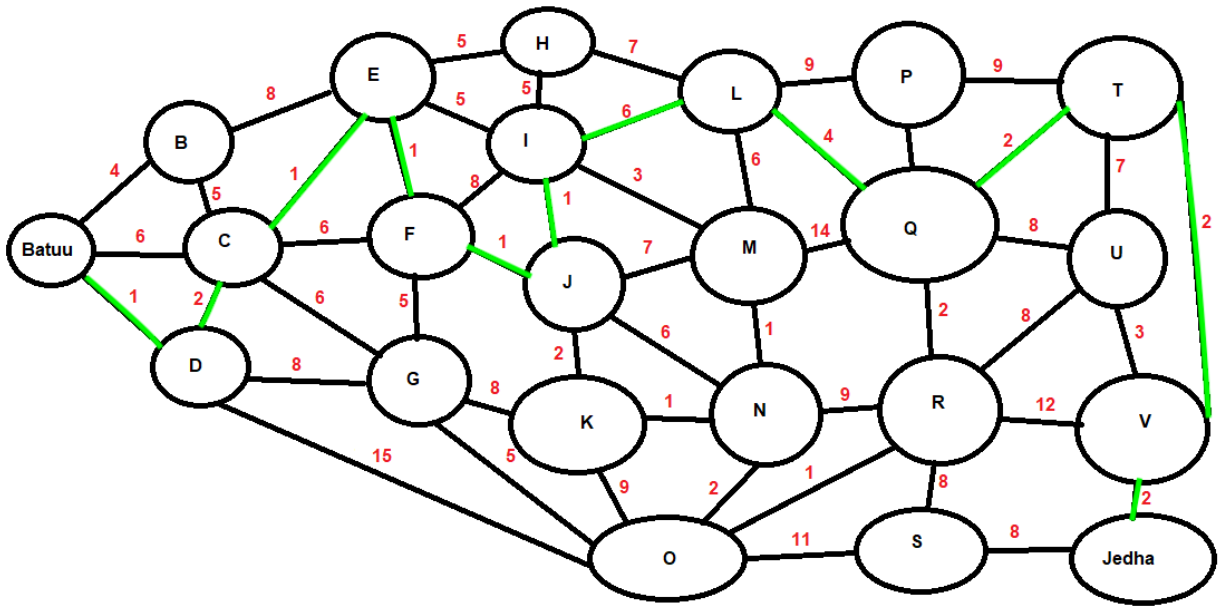
The Resistance's networking team provided us with a backup DNS server of:
`ns2.galaxybackup.com`.

What needs to be done is that ns2.galaxybackup.com needs to be added as the secondary DNS so in case of any future attack, if the primary DNS is brought down, the site will still work because we will have a secondary DNS as a backup.

Mission 5

For this mission we need to determine the `OSPF` shortest path from `Batuu` to `Jedha`. The network traffic from the planet of `Batuu` to the planet of `Jedha` is very slow. It has been determined that the slowness is due to the Empire attacking `Planet N`. Because of this we have to avoid the Planet N.

The path will look like this:



The cost of this path is 23 and it is the lowest cost path that avoids Planet N.

Mission 6

For this mission we are tasked to decrypt Dark Side's encrypted wireless internet traffic in Darkside.pcap.

The command used is:
aircrack-ng -w rockyou.txt Darkside.pcap

Result:
Opening ./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 ./Darkside.pcap
Reading packets, please wait...

                                Aircrack-ng 1.2 rc4

      [00:00:01] 2280/7120714 keys tested (2205.47 k/s)

      Time left: 53 minutes, 48 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
```

From this we got the key “dictionary”. The full key for decrypting in wireshark is “dictionary:linksys”. After decrypting and looking into ARP records I have found the following IP and MAC addresses:

Sender MAC address: Cisco-Li_e3:e4:01 (00:0f:66:e3:e4:01)
Sender IP address: 172.16.0.1 (172.16.0.1)

Target MAC address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
Target IP address: 172.16.0.101 (172.16.0.101)

Mission 7

We have saved the galaxy!!! As a thank you, we got this: