HW9 - Rebuilding the Jedi Network

-- Ralph Pursifull --

The Sith Empire recently carried out a DoS attack, taking out the Resistance's core network infrastructure, including its DNS servers.

This attack destroyed the Resistance's ability to communicate via email and retrieve other crucial information about each others' operations. The Empire has taken advantage of this compromised availability by ambushing numerous Resistance outposts, all vulnerable because they can no longer call for help.

Your task is a crucial one: Restore the Resistance's core DNS infrastructure and verify that traffic is routing as expected.

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:

- Current mail servers for starwars.com.

Since DNS and primary email servers were impacted, this is a good time to review Starwars.com DNS registration and authoritative DNS server configuration. These first steps will guarantee we have the right DNS data and that the hackers haven't taken over the environment even more deeply. This doesn't take long.

Start with a domain lookup at GoDaddy.com. (or another reliable major registrar) At the GoDaddy website, for instance, do a "Whois Lookup" for Starwars.com, or use this link. GoDaddy Whois for Starwars.com. Here is output from that link:

> **Domain Name: STARWARS.COM**
> Registry Domain ID: 1320421_DOMAIN_COM-VRSN
> **Registrar WHOIS Server: whois.corporatedomains.com**
> **Registrar URL: http://cscdbs.com**
> Updated Date: 2021-07-21T07:08:34Z
> Creation Date: 1996-09-04T04:00:00Z
> Registry Expiry Date: 2022-09-03T04:00:00Z
> **Registrar: CSC Corporate Domains, Inc.**

Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: A1-127.AKAM.NET
Name Server: A12-66.AKAM.NET
Name Server: A13-67.AKAM.NET
Name Server: A18-64.AKAM.NET
Name Server: A28-65.AKAM.NET
Name Server: A9-66.AKAM.NET
DNSSEC: unsigned

Need to verify the **BLUE** highlighted information above (about the registrar) is really the correct DNS registrar for Starwars.com. Need to check to see if that agrees with Resistance network documentation, financial records or any reliable personal memories that are available. For now, we have no reason to believe this registrar info is incorrect.

Choose one of the authoritative Name Server entries listed above. Here we use the first one.

```
$ nslookup -type=SOA starwars.com  a1-127.akam.net
Server:     a1-127.akam.net
Address:    193.108.91.127#53

Starwars.com
      origin = a9-66.akam.net
      mail addr = postmaster.lucasfilm.com
      serial = 2019031414
      refresh = 300
      retry = 300
      expire = 604800
      minimum = 300
```

Choose the name server on the origin line (a.k.a. primary nameserver): **a9-66.akam.net**
And ask for "ANY" Starwars.com domain records with this command. My notes in **green** and **red**.

```
$ nslookup -type=ANY starwars.com  a9-66.akam.net
Server:     a9-66.akam.net
Address:    184.85.248.66#53

starwars.com    nameserver = a18-64.akam.net.     # NS declarations match
starwars.com    nameserver = a13-67.akam.net.     # the list above.  OK
starwars.com    nameserver = a9-66.akam.net.
starwars.com    nameserver = a1-127.akam.net.
starwars.com    nameserver = a28-65.akam.net.
starwars.com    nameserver = a12-66.akam.net.
starwars.com    mail exchanger = 5 alt2.aspmx.l.google.com.  # BROKEN EMAIL
```

```
starwars.com    mail exchanger = 1 aspmx.1.google.com.       # BROKEN EMAIL
starwars.com    mail exchanger = 10 aspmx3.googlemail.com.   # BROKEN EMAIL
starwars.com    mail exchanger = 10 aspmx2.googlemail.com.   # BROKEN EMAIL
starwars.com    mail exchanger = 5 alt1.aspx.l.google.com.   # BROKEN EMAIL
Name: starwars.com                      # IPv4 for Rebel website, OK.
Address: 184.25.254.64
Name: starwars.com                      # IPv4 for Rebel website, OK.
Address: 184.25.254.91
starwars.com                            # this section looks right, OK.
      origin = a9-66.akam.net
      mail addr = postmaster.lucasfilm.com   # that's one of our people, OK.
      serial = 2019031414
      refresh = 300
      retry = 300
      expire = 604800
      minimum = 300
         # 6 lines like the following enable use of Google Workspace. All OK.
starwars.com   text =
"google-site-verification=ave4Otl9BlVJ0Zd2j4GVdJ4s4brlgM3fqPZ-_mM6EFY"
         # For outbound email. Verify SPF checks are working. OK.
starwars.com   text = "v=spf1 include:mail.zendesk.com ?all"
Name: starwars.com                   # IPv6 for Rebel website, OK.
Address: 2600:1406:40::1732:e9bd
Name: starwars.com                   # IPv6 for Rebel website, OK.
Address: 2600:1406:40::1732:e9a5
```

Since the Resistance is able to send email, TXT records involved with outbound email (like SPF and DKIM) and any other outbound DNS configuration are probably OK. Take a minute to verify the SPF checks are working. The problem is with inbound email, so the MX records must be the issue.

- Explain why the Resistance isn't receiving any emails.

Incoming email for a domain is directed to the servers listed in the domain's MX or mail exchanger DNS records. Here, email for Starwars.com, is being directed to the five members of the MX or "mail exchanger" list above (and flagged as **BROKEN EMAIL**). That doesn't match our plan. We want them to go to the new primary and secondary servers at google.com.

- Recommended DNS configuration for email servers.

Remove the five **"BROKEN EMAIL"** lines shown above. Use these two lines instead.

```
starwars.com    MX preference = 10, mail exchanger = asltx.1.google.com
starwars.com    MX preference = 20, mail exchanger = 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.

Here we used the same process as in Mission 1:

- Whois Lookup shows the following for TheForce.net.
  - Registrar is GoDaddy
  - Authoritative nameservers for TheForce.net are: NS-1.WISE-ADVICE.COM and NS-2.WISE-ADVICE.COM
- Use NSLOOKUP to get the SPF record from the authoritative name servers. Drop the “google-site-verification” lines, cuz Google Workspace licensing, is not relevant.

```
$ nslookup -type=TXT   theforce.net   ns-1.wise-advice.com
Server:    ns-1.wise-advice.com
Address:   104.207.135.156#53

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"
```

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

TheForce.Net’s new email server uses IP address: 45.23.176.21, which is not on the SPF “authorized” list. Since email from them now fails the SPF check, it is considered suspicious. The recipient’s email server will handle it like SPAM or a THREAT from an unauthorized source.

- Document what a corrected DNS record should be.

Administrators at TheForce.Net need to modify their TXT record which contains “v=spf1”. They should eventually remove any obsolete entries, but for now, just add the new email server IPv4 address, to make it look 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"
```

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.

We use these two commands to get IP and CNAME info from an authoritative name server.

```
$ nslookup www.theforce.net ns-1.wise-advice.com
Server:     ns-1.wise-advice.com
Address:    104.207.135.156#53

www.theforce.net  canonical name = theforce.net.
Name: theforce.net
Address: 104.156.250.80

$ nslookup theforce.net ns-1.wise-advice.com
Server:     ns-1.wise-advice.com
Address:    104.207.135.156#53

Name: theforce.net
Address: 104.156.250.80
```

The first nslookup tells us to get the IP address of www.theforce.com by looking for the IP address of theforce.net. The second nslookup just confirms that the IP address of theforce.net is 104.156.250.80. It doesn't go somewhere else, but is clearly defined.. That is how a CNAME configuration should appear as viewed from nslookup.

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

We check to see if resistance.theforce.net looks like that too. My note is in **red**.

```
$ nslookup resistance.theforce.net  ns-1.wise-advice.com
Server:     ns-1.wise-advice.com
Address:    104.207.135.156#53

** server can't find resistance.theforce.net: NXDOMAIN  # CAN'T FIND
```

So, that shows us: **resistance.theforce.net is not configured in DNS at all.**

- Document what a corrected DNS record should be.

To redirect resistance.theforce.net to theforce.net -- We want DNS requests for resistance.theforce.net to return the same IP as www.theforce.net. To do this, create a "CNAME" record for resistance.theforce.net and point it to theforce.net. That is how www is configured, so just replicate that. If done correctly, when you run the following command, you should get the following response. (This is from an Ubuntu VM).

```
$ nslookup resistance.theforce.net ns-1.wise-advice.com
Server:     ns-1.wise-advice.com
Address:    104.207.135.156#53

resistance.theforce.net canonical name = theforce.net.
Name: theforce.net
Address: 104.156.250.80
```

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.

Step 1: Explore ns2.galaxybackup.com. Whois Lookup for Galaxybackup.com gives this:

> Domain Name: **GALAXYBACKUP.COM**
> Registrar WHOIS Server: whois.123-reg.co.uk
> Registrar URL: http://www.meshdigital.com
> Name Server: **NS.123-REG.CO.UK**
> Name Server: NS2.123-REG.CO.UK

So the galaxybackup.com domain exists. Let's see if the backup Resistance nameserver exists.

```
$ nslookup ns2.galaxybackup.com ns.123-reg.co.uk
Server:         ns.123-reg.co.uk
Address:    212.67.202.2#53

** server can't find ns2.galaxybackup.com: NXDOMAIN  # CAN'T FIND
```

So the Resistance backup nameserver is NOT in DNS. No way that will work.

Step 2. Explore princessleia.site. Whois Lookup for PrincessLeia.site gives this:

Domain Name: **princessleia.site**
Registry Domain ID: D131344761-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-09-26T18:13:10Z
Creation Date: 2019-09-26T18:13:20Z
Registrar Registration Expiration Date: 2022-09-26T23:59:59Z
Registrar: GoDaddy.com, LLC
Name Server: **NS25.DOMAINCONTROL.COM**
Name Server: NS26.DOMAINCONTROL.COM

So princessleia.site domain exists and has authoritative nameservers. Let's explore it interactively.

```
$ nslookup
> server ns25.domaincontrol.com
Default server: ns25.domaincontrol.com
Address: 97.74.102.13#53
Default server: ns25.domaincontrol.com
Address: 2603:5:2161::d#53
> princessleia.site
Server:         ns25.domaincontrol.com
Address:   97.74.102.13#53

Name: princessleia.site
Address: 34.102.136.180
Name: princessleia.site       # website exists, but undeveloped..
Address: 20.40.202.19         # shows "parked free at GoDaddy"
> set type=ANY
> princessleia.site
Server:    ns25.domaincontrol.com
Address:   97.74.102.13#53

Name: princessleia.site
Address: 34.102.136.180
Name: princessleia.site
Address: 20.40.202.19
princessleia.site     nameserver = ns25.domaincontrol.com.
princessleia.site     nameserver = ns26.domaincontrol.com.
princessleia.site
      origin = ns25.domaincontrol.com
      mail addr = dns.jomax.net
      serial = 2021081601
```

```
        refresh = 28800
        retry = 7200
        expire = 604800
        minimum = 600
princessleia.site     text = "Run the following in a command
line: telnet towel.blinkenlights.nl or as a backup access in a
browser: www.asciimation.co.nz"   # ascii animation website
> www.princessleia.site
Server:    ns25.domaincontrol.com
Address:   97.74.102.13#53

www.princessleia.site canonical name = princessleia.site.> set
type=MX
> princessleia.site
Server:    ns25.domaincontrol.com
Address:   97.74.102.13#53
                                                  # No MX, so cannot
*** Can't find princessleia.site: No answer # receive email
```

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

The backup nameserver (NS2.galaxybackup.com) for the PricessLeia domain can not be found in DNS. Since the Resistance Network Team knows it is up and running, we need to do the following:

A. **Create a DNS "A" record for NS2.** If we trust the GalaxyBackup domain, then we can keep the name "NS2.galaxybackup.com". If we cannot, then we need to find another DNS Hosting provider and create an "A" record for NS2.newProvider.com there. We would like this newProvider to be on a very safe Resistance planet.

B. Merge the NS2.galaxybackup.com DNS configuration with any records we think might be needed from the existing ns25/ns26.domaincontrol.com.

C. At the DNS Registrar for PrincessLeia domain, list **NS2 as the primary nameserver** for the domain and if needed, as one of the nameservers. This will update the **SOA record** for PrincessLeia.

D. **Configure NS2 to replicate the DNS configuration** for PrincessLeia out to DNS servers on other planets across the rebellion. Add the names of those DNS servers to the list of Authoritative Name Servers at the DNS Registrar for PrincessLeia.

   Note: Steps C+D can be simplified by a vendor offering DNS hosting and replication across the Rebellion. Enter the NS2 DNS records into their user interface and deploy.

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.

OSPF is a link-state routing protocol so speed is a key factor, not the number of hops. The diagram gives the cost. WIthout Planet N, the path must go through one of L, M or O.

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

```
Batuu > D > C > E > F > J > I > L > Q > T > V > Jedha
```
My path does not include Planet N.

- Document this shortest path so it can be used by the Resistance to develop a static route to improve the traffic.

Based on the cost of each link, without planet N, the quickest route = lowest cost is:

```
Batuu > D > C > E > F > J > I > L > Q > T > V > Jedha
Cost: 1   2   1   1   1   1   6   4   2   2   2 = 23 total cost
```

The cost to get from Batuu to Planet Q is now 17, via Planet N it was 14.

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, will need to use a wordlist (-w) such as rockyou.txt.

Located and downloaded rockyou.txt word list with this short script:

```
#!/bin/bash
LinkPart1="https://github.com/brannondorsey/naive-hashcat"
Link="${LinkPart1}/releases/download/data/rockyou.txt"
wget ${Link}
```

Ran aircrack-ng like this:

```
$ aircrack-ng Darkside.pcap -w rockyou.txt
```

Here are the results:

```
                              Aircrack-ng 1.2 rc4

[00:00:00] 2280/7120714 keys tested (2769.44 k/s)

Time left: 42 minutes, 50 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
```

So the WPA-PWD key is dictionary

- 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>.

After examining Darkside.pcap, will decrypt SSID=linksys by entering this key into WireShark under: Edit > Preferences > Protocols > IEEE 802.11 > Description keys Edit >

Key Type = **wpa-pwd**

Key = **dictionary:linksys**

Click OK as needed to return to the data display in Wireshark.

- 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.

ARP and other protocols show 3 devices in the 172.16.0.X range,
Possible but not certain that the local subnet is 172.16.0.0/24

172.16.0.1 MAC 00:0f:66:e3:e4:01 = Cisco-Li_e3:e4:01 pckt 315 gateway, responds to PING
172.16.0.101 MAC 00:13:ce:55:98:ef = IntelCor_55:98:ef packet 215 responds to PING
172.16.0.9 MAC 00:14:bf:0f:03:30 = Cisco-Li_0f:03:30 packet 64 (TCP with 172.16.0.101)

MAC 00:0b:86:c2:a4:85 = ArubaaHe_c2:a4:85 wireless beacon SSID=linksys, sometimes MAC for off-subnet IP addresses

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

Additional IPv4 addresses not on the local subnet, could be EMPIRE wide area resources
Candidate targets for future attack. Try to access them on EMPIRE universal networks.
68.9.16.25 packet 551: this is a nameserver (responds to dns)
68.9.16.30 packet 90: this is a nameserver (responds to dns)
10.1.1.50 packet 31 access point+beacon; pckt 145: was sent dns queries, no response; packet 50: ICMP port unreachable
10.50.50.30 packet 51: was sent dns queries, did not respond
224.0.0.22 MAC IPv4mcast_16 = 01:00:5e:00:00:16 IGMPv3 Empire multicasts here?
239.255.255.250 MAC IPv4mcast_7f:ff:fa = 01:00:5e:7f:ff:fa SSDP protocol destination

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.

```
$ nslookup -type=TXT princessleia.site ns25.domaincontrol.com
Server:    ns25.domaincontrol.com
Address:   97.74.102.13#53

princessleia.site     text = "Run the following in a command line:
telnet towel.blinkenlights.nl or as a backup access in a browser:
www.asciimation.co.nz"
```

- The Resistance provided you with a hidden message in the TXT record, with several steps to follow.

You will find the TXT record highlighted during Mission 4.

- Follow the steps from the TXT record.

Telnet did not work, using my browser.

- Take a screenshot of the results.

Voila! See the next page.