

Homework 09: Networks Fundamentals II Homework: *In a Network Far, Far Away!*

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.1.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`.

```
jessi@DESKTOP-G0GKD3V MINGW64 ~
$ nslookup -type=MX starwars.com
Server:  cdns1.cox.net
Address:  2001:578:3f::30

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

aspmx2.googlemail.com  internet address = 142.250.28.26
alt2.aspmx.l.google.com internet address = 142.250.125.27
alt2.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:4001:c2f::1a
aspmx3.googlemail.com  internet address = 142.250.125.27
aspmx.l.google.com      internet address = 74.125.137.26
aspmx.l.google.com      AAAA IPv6 address = 2607:f8b0:4023:c03::1b
```

```
jessi@DESKTOP-G0GKD3V MINGW64 ~
$ nslookup -type=NS starwars.com
Server:  cdns1.cox.net
Address:  2001:578:3f::30

Non-authoritative answer:
starwars.com      nameserver = a1-127.akam.net
starwars.com      nameserver = a12-66.akam.net
starwars.com      nameserver = a13-67.akam.net
starwars.com      nameserver = a9-66.akam.net
starwars.com      nameserver = a18-64.akam.net
starwars.com      nameserver = a28-65.akam.net

a12-66.akam.net  internet address = 184.26.160.66
a13-67.akam.net  internet address = 2.22.230.67
a13-67.akam.net  AAAA IPv6 address = 2600:1480:800::43
a9-66.akam.net   internet address = 184.85.248.66
a9-66.akam.net   AAAA IPv6 address = 2a02:26f0:117::42
a18-64.akam.net  internet address = 95.101.36.64
a28-65.akam.net  internet address = 95.100.173.65
a1-127.akam.net  internet address = 193.108.91.127
```

Command : `nslookup -type=mx starwars.com`

Results:

`aspmx2.googlemail.com`

alt1.aspx.1.google.com
aspmx3.googlemail.com
alt2.aspmx.1.google.com
aspmx.1.google.com

Explain why the Resistance isn't receiving any emails.

(MX) Records has an error. (MX) Records in the DNS server allow us to specify where email should be delivered. MX records specify and prioritize the incoming mail servers that receive email messages sent to your domain name. These records are just telling the sending email server, when sending an email to `asltx.1.google.com`, deliver to `asltx.1.google.com`: If that server doesn't accept the email, then send it to `asltx.2.google.com`.

Document what a corrected DNS record should be.

This can be corrected by re-configuring their mail service to use the new servers.

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.

Command: `nslookup -type=mx theforce.net`, and `nslookup -type=txt theforce.net`

```
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.

The new IP `45.23.176.21` is not in the DNS SPF/txt record that indicates IP addresses of mail servers that are allowed to send emails on its behalf and store any text-based information that can be grabbed when necessary. An SPF record's main purpose is to prevent spam, phishing, and email spoofing, by detecting emails that may have a forged sender email.

Document what a corrected DNS record should be.

The new IP should be added to the Txt Records or changed back to the original IP.

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.

```
C:\ Select MINGW64:/c/Users/jessi

jessi@DESKTOP-G0GKDJV MINGW64 ~
$ nslookup theforce.net
Server:  cdns1.cox.net
Address:  2001:578:3f::30

Non-authoritative answer:
Name:    theforce.net
Address: 104.156.250.80

jessi@DESKTOP-G0GKDJV MINGW64 ~
$ nslookup 104.156.250.80
Server:  cdns1.cox.net
Address: 2001:578:3f::30

Name:    rebelscum.com
Address: 104.156.250.80
```

Command: `nslookup www.theforce.net`

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

CNAME records are another commonly used type of DNS entry and are used to point a domain or subdomain to another hostname. Sub page is set to a page called `rebelscum.com`.

Document what a corrected DNS record should be.

CNAME record should be updated.

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.

```
MINGW64:/c/Users/jessi

jessi@DESKTOP-G0GKDJV MINGW64 ~
$ nslookup -type=NS princessleia.site
Server: cdns1.cox.net
Address: 2001:578:3f::30

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

ns25.domaincontrol.com internet address = 97.74.102.13
ns25.domaincontrol.com AAAA IPv6 address = 2603:5:2161::d
ns26.domaincontrol.com internet address = 173.201.70.13
ns26.domaincontrol.com AAAA IPv6 address = 2603:5:2261::d

jessi@DESKTOP-G0GKDJV MINGW64 ~
$
```

```
MINGW64:/c/Users/jessi

jessi@DESKTOP-G0GKDJV MINGW64 ~
$ nslookup -type=MX princessleia.site
Server: cdns1.cox.net
Address: 2001:578:3f::30

princessleia.site
    primary name server = ns25.domaincontrol.com
    responsible mail addr = dns.jomax.net
    serial = 2020062300
    refresh = 28800 (8 hours)
    retry = 7200 (2 hours)
    expire = 604800 (7 days)
    default TTL = 600 (10 mins)

jessi@DESKTOP-G0GKDJV MINGW64 ~
$ nslookup -type=txt princessleia.site
Server: cdns1.cox.net
Address: 2001:578:3f::30

Non-authoritative answer:
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"
```

This site is under domaincontrol.com

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

Looks like most of the records has been tampered with, I suggest not getting hacked. All records need updating to correct info.

How to prevent this from happening again? Audit your DNS zones, Keep your DNS servers up-to-date, Hide BIND version, Restrict Zone Transfers, Disable DNS recursion to prevent DNS poisoning attacks, Use isolated DNS servers, Use a DDOS mitigation provider, Two-Factor Authentication.

Mission 5

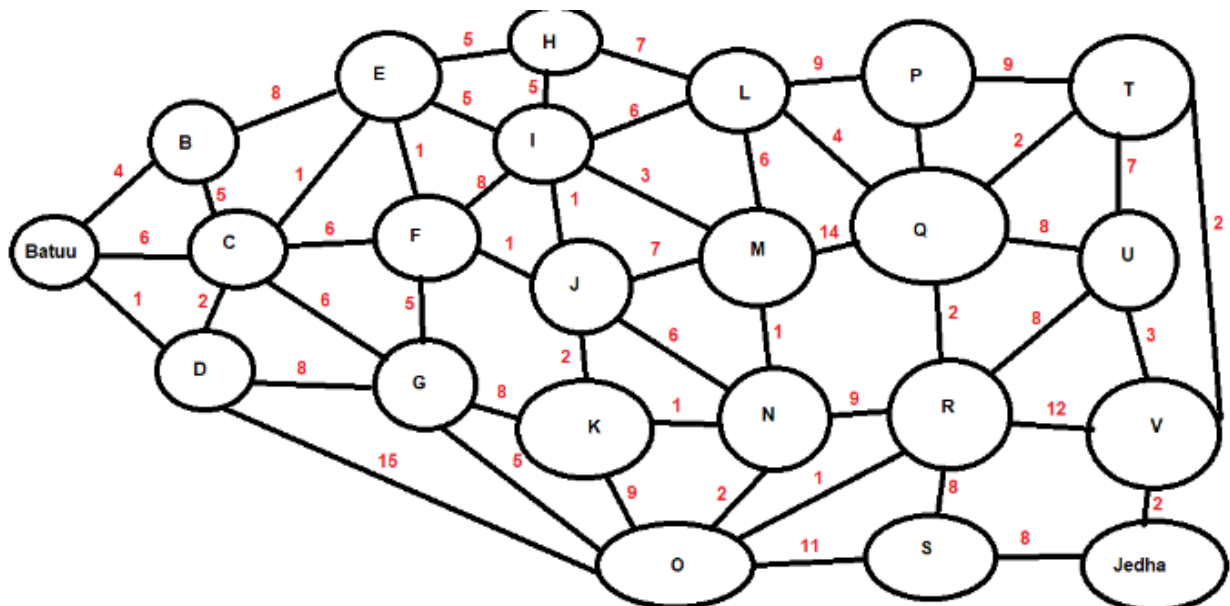
Issue: The network traffic from the planet of Batuu to the planet of Jedha is very slow.

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.



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.

OSPF : Batuu -> D -> C -> E -> F -> J -> K -> O -> R -> Q -> T -> V -> 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.

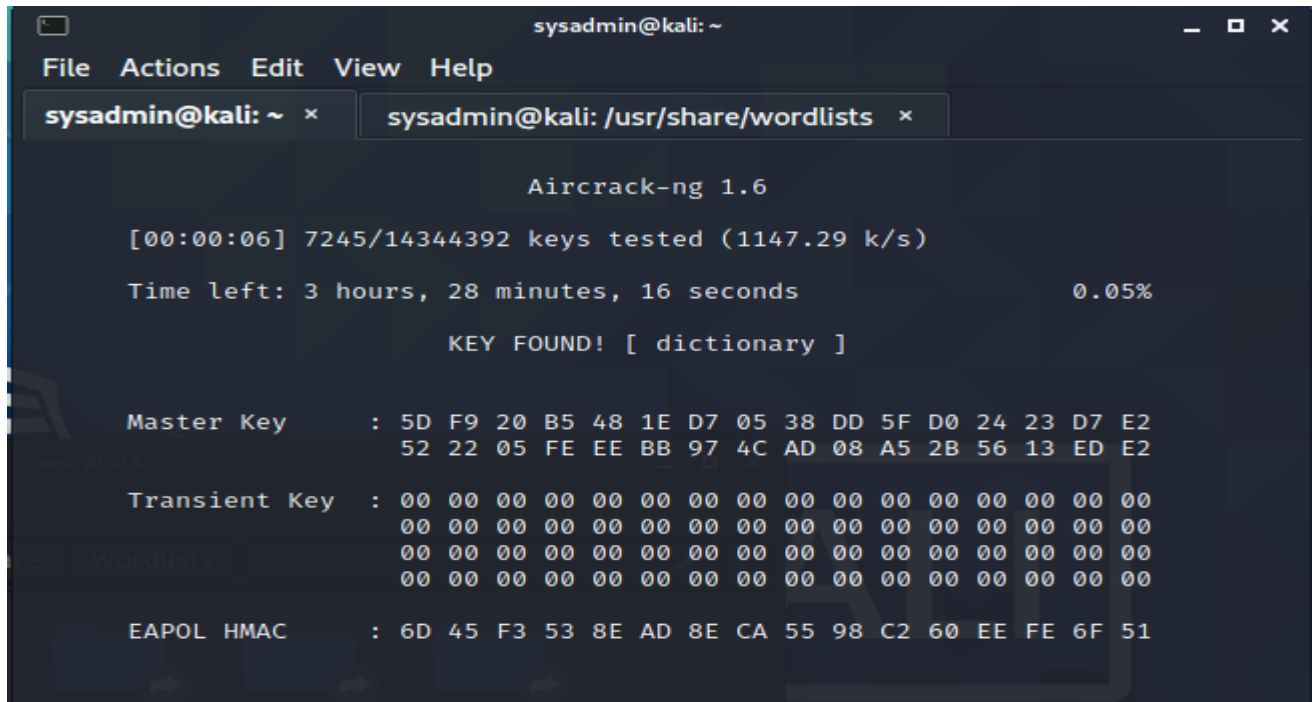
You have captured some of the Dark Side's encrypted wireless internet traffic in the following pcap: [Darkside.pcap](#).

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`.



```
sysadmin@kali: ~  
File Actions Edit View Help  
sysadmin@kali: ~ x sysadmin@kali: /usr/share/wordlists x  
  
Aircrack-ng 1.6  
[00:00:06] 7245/14344392 keys tested (1147.29 k/s)  
Time left: 3 hours, 28 minutes, 16 seconds 0.05%  
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 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
EAPOL HMAC : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
```

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>`.

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.

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

Darkside-2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
312	2006-05-04 02:32:09.421364	IntelCor_55:98:ef	Broadcast	ARP	80	Who has 172.16.0.1? Tell 172.16.0.101
314	2006-05-04 02:32:09.422968	IntelCor_55:98:ef	Broadcast	ARP	98	Who has 172.16.0.1? Tell 172.16.0.101
315	2006-05-04 02:32:09.423426	Cisco-Li_e3:e4:01	IntelCor_55:98:ef	ARP	98	172.16.0.1 is at 00:0f:66:e3:e4:01

0... = +HTC/Order flag: Not strictly ordered
.000 0000 1101 0100 = Duration: 212 microseconds
Receiver address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
Transmitter address: ArubaaHe_c2:a4:85 (00:0b:86:c2:a4:85)
Destination address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
Source address: Cisco-Li_e3:e4:01 (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.

STAR ASCIIMATION WARS

A N E W H O P E

I t i s a p e r i o d o f c i v i l w a r .
R e b e l s p a c e s h i p s , s t r i k i n g
f r o m a h i d d e n b a s e , h a v e w o n
t h e i r f i r s t v i c t o r y a g a i n s t
t h e e v i l G a l a c t i c E m p i r e .

|< <<< << 1< # >1 > >> >>> >|

Last scene added:
January 2015

[Frequently asked questions](#) [My other projects](#) [Original Java Ascimation](#) [The death of Jar Jar](#)

[Austin 7 Blog](#) [BB Blog](#)

Copyright © 1997 - 2020 Simon Jansen
jansens@ascimation.co.nz