Module 9 Challenge

MISSION 1.

Command: **nslookup –type=MX starwars.com**

When we look at the mail exchanger for starwars.com, we see the new primary and secondary server are not added here.

This is why they are not receiving any emails.

```
sysadmin@vm-image-ubuntu-dev-1:~$ nslookup -type=MX starwars.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
starwars.com    mail exchanger = 1 aspmx.l.google.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 = 10 aspmx2.googlemail.com.
starwars.com    mail exchanger = 10 aspmx3.googlemail.com.

Authoritative answers can be found from:
```

The correct DNS configuration should be:

starwars.com mail exchanger = 1 asltx.1.google.com

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

MISSION 2.

theforce.net with new IP of 45.23.176.21

Command: **nslookup –type=TXT theforce.net**

Shows a different IP address in the configuration of 45.63.15.159

This is why the emails are going to spam or being blocked.

```
sysadmin@vm-image-ubuntu-dev-1:~$ nslookup -type=TXT theforce.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
theforce.net    text = "v=spf1 a mx a:mail.wise-advice.com mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:45.63.15.159 ip4:45.63.4.215  ~all"
theforce.net    text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"
theforce.net    text = "google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"

Authoritative answers can be found from:
```

Need to configure the IP to 45.23.176.21

MISSION 3.

Not redirecting from resistance.theforce.net to theforce.net

Command: **nslookup –type=all www.theforce.net**

Shows the canonical name of theforce.net

This needs to be set to the alias resistance.theforce.net

And they will start redirecting again.

```
sysadmin@vm-image-ubuntu-dev-1:~$ nslookup -type=all www.theforce.net
unknown query type: all
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.theforce.net        canonical name = theforce.net.
Name:   theforce.net
Address: 45.63.4.215
```

MISSION 4.

DNS server: princessleia.site

Backup DNS server: ns2.galaxybackup.com

Command: **nslookup –type=NS princessleia.site**

Shows two servers:

princessleia.site nameserver = ns25.domaincontrol.com

princessleia.site nameserver = ns26.domaincontrol.com

```
sysadmin@vm-image-ubuntu-dev-1:~$ nslookup -type=NS princessleia.site
Server:         8.8.8.8
Address:        8.8.8.8#53

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

Authoritative answers can be found from:
```

Need to append the new backup DNS server to this list and it will be all good.

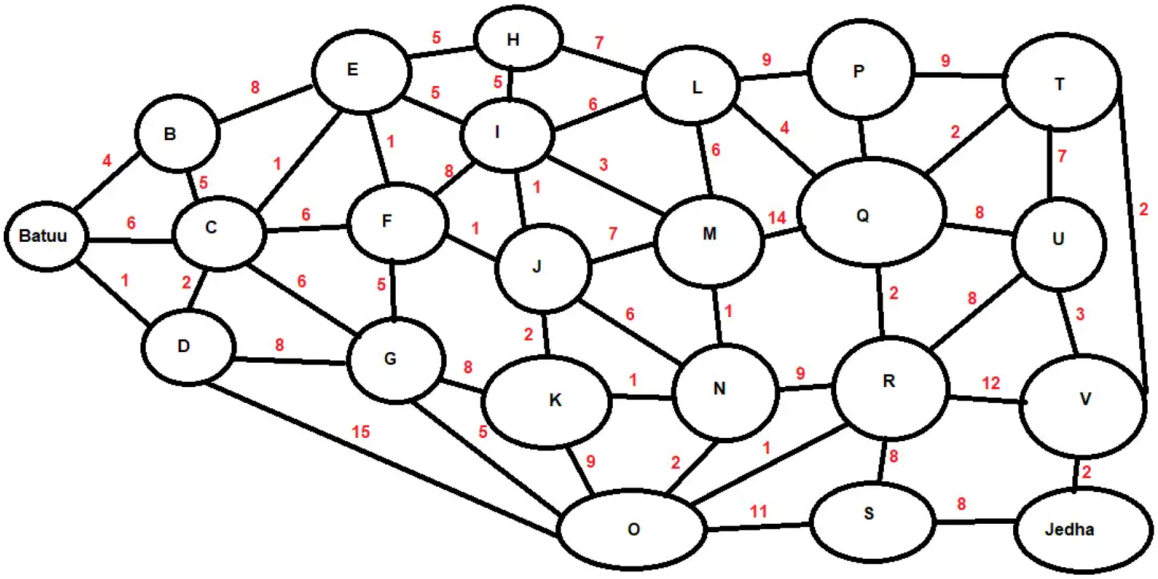
princessleia.site nameserver = ns2.galaxybackup.com

MISSION 5.

After examining multiple routes, it has been determined the shortest path is:

Batuu – D – C – E – F – J – I – L – Q – T – V – Jedha = 20 hops

---

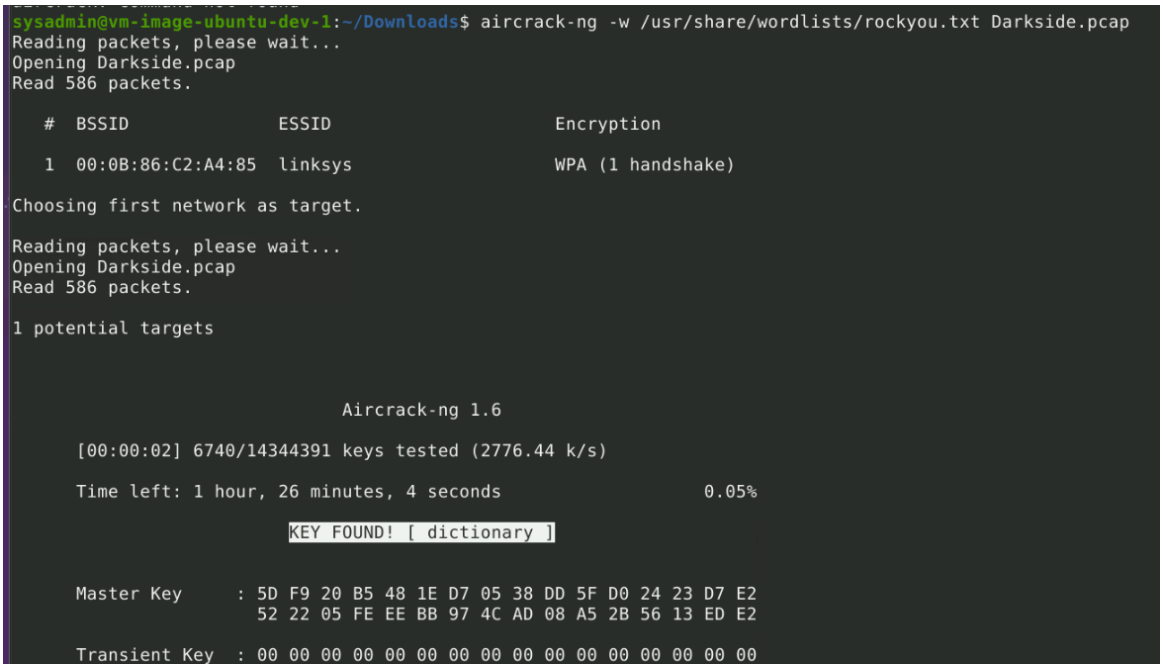


MISSION 6.

Needed to download the pcap file to VM. After doing this, I was able to navigate to the Downloads directory and run the following command.

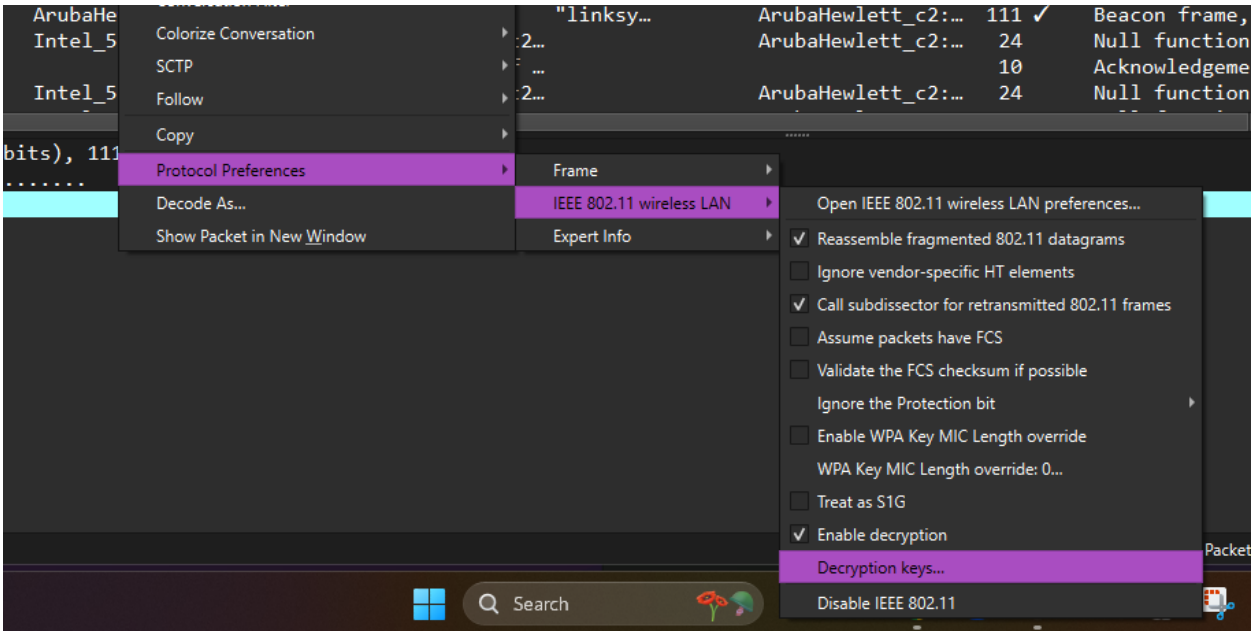
Command: **aircrack-ng -w /usr/share/wordlists/rockyou.txt Darkside.pcap**

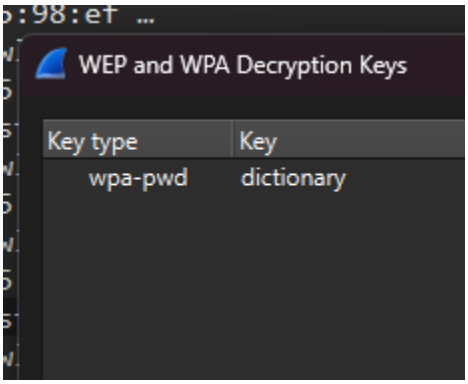
Key found: **dictionary**



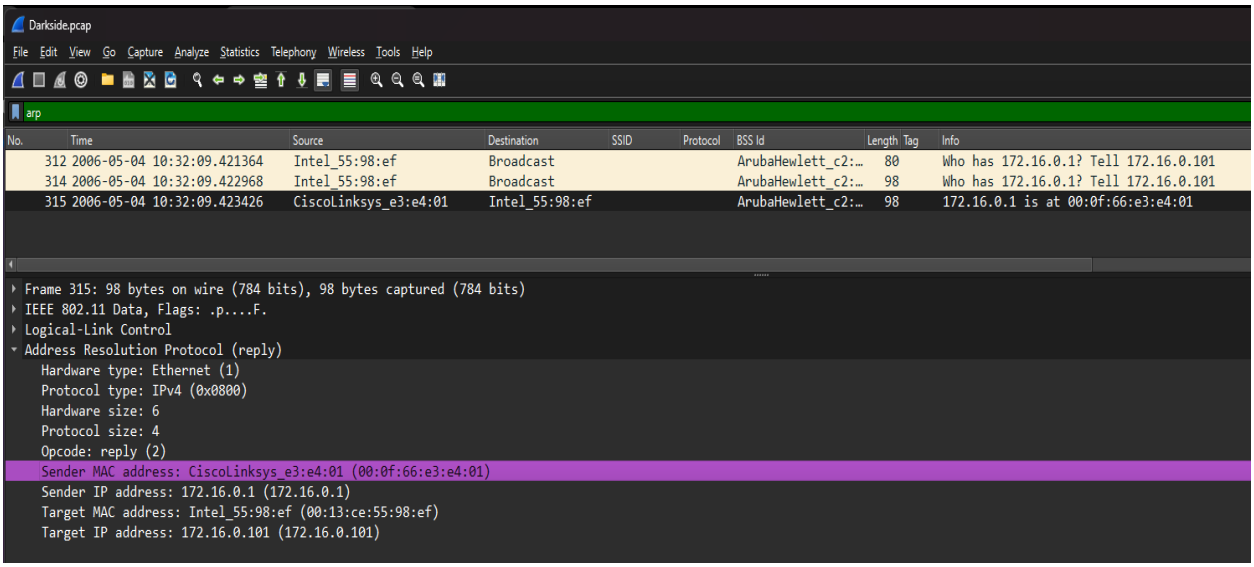
Now that I have found the key, I can go over to Wireshark and examine the decrypted ARP traffic to find the IP and MAC address of the Dark Side's host.

Navigate my way to Decryption keys. I add wpa-pwd dictionary





Then I can filter ARP, click the 3rd line because this is the reply. In the bottom pane I can see the sender IP and the sender MAC addresses.



Host IP address is: **172.16.0.1**

Host MAC address: **00:0f:66:e3:e4:01**

MISSION 7.

Hidden message in the TXT from DNS record in Mission 4.

DNS record from Mission 4 is **princessleia.site**

```
sysadmin@vm-image-ubuntu-dev-1:~$ nslookup -type=TXT princessleia.site
Server:         8.8.8.8
Address:        8.8.8.8#53

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"

Authoritative answers can be found from:
```

When I ran the command **telnet towel.blinkenlights.nl**

A short, animated film started to play about starwars episode IV. Pretty cool surprise.

(Star ASCIImotion Wars).... can also be viewed here: www.asciimation.co.nz

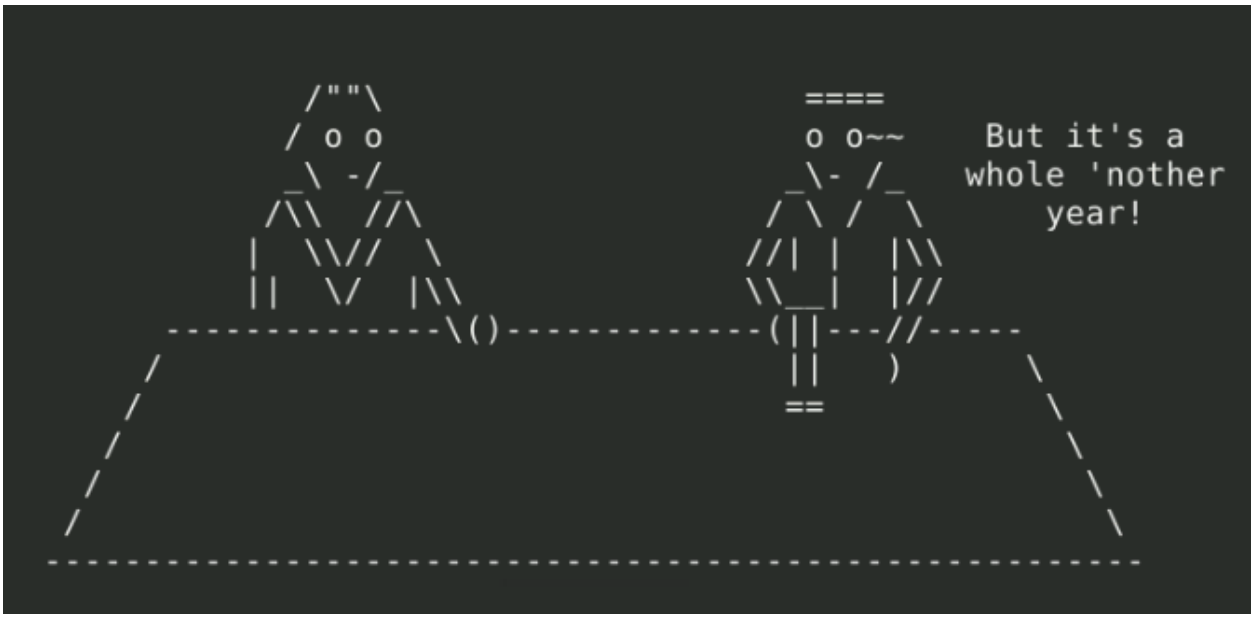
|< <<< << 1< # >1 > >> >>> >|

Last scene added:
January 2015

Frequently asked questions My other projects Original Java Asciimation The death of Jar Jar

Copyright © 1997 - 2023 Simon Jansen
jansens@asciimation.co.nz


Aircrack-ng 1.6


But it's a
whole 'nother
year!