# Mission 1

**Determine and document the mail servers for starwars.com using NSLOOKUP.**

$ nslookup -type=mx starwars.com

Server: cdns01.comcast.net

Address: 2001:558:feed::1

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 = 5, mail exchanger = alt2.aspmx.l.google.com

starwars.com MX preference = 10, mail exchanger = aspmx2.googlemail.com

starwars.com MX preference = 10, mail exchanger = aspmx3.googlemail.com

aspmx3.googlemail.com internet address = 173.194.209.26

aspmx.l.google.com internet address = 74.125.137.26

aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:4023:c03::1b

alt2.aspmx.l.google.com internet address = 173.194.209.26

alt2.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:4024:c02::1b

aspmx2.googlemail.com internet address = 209.85.146.26

aspmx2.googlemail.com AAAA IPv6 address = 2607:f8b0:4001:c1f::1b

5 mail servers:

alt1.aspx.l.google.com

aspmx.l.google.com

alt2.aspmx.l.google.com

aspmx2.googlemail.com

aspmx3.googlemail.com

**Explain why the Resistance isn't receiving any emails.**The resistance isn’t receiving any emails because DNS server does not have the correct entries for Mail server. Nslookup of starwars.com DNS results in above mail servers, however, the new mail servers are asltx.l.google.com and asltx.2.google.com.

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

The correct DNS record for Mail Exchange should look like below:

$ nslookup -type=mx starwars.com

Server: cdns01.comcast.net

Address: 2001:558:feed::1

Non-authoritative answer:

starwars.com MX preference = 5, mail exchanger = asltx.2.google.com

starwars.com MX preference = 1, mail exchanger = asltx.l.google.com

# Mission 2

**Determine and document the SPF for theforce.net using NSLOOKUP.**

$ nslookup -type=txt theforce.net

Server: cdns01.comcast.net

Address: 2001:558:feed::1

Non-authoritative answer:

theforce.net text =

"google-site-verification=ycgY7mtk2oUZMagcffhFL\_Qaf8Lc9tMRkZZSuig0d6w"

theforce.net text =

"google-site-verification=XTU\_We07Cux-6WCSOItl0c\_WS29hzo92jPE341ckbOQ"

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.**The SPF record for theforce.net does not authorize the new IP 45.23.176.21 to send emails on their behalf. This is why starwars mail server is unable to verify that the emails are legit and thus marking them as spam.

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

Add the new mail server IP to DNS and it should look like below:

$ nslookup -type=txt theforce.net

Server: cdns01.comcast.net

Address: 2001:558:feed::1

Non-authoritative answer:

theforce.net text =

"google-site-verification=ycgY7mtk2oUZMagcffhFL\_Qaf8Lc9tMRkZZSuig0d6w"

theforce.net text =

"google-site-verification=XTU\_We07Cux-6WCSOItl0c\_WS29hzo92jPE341ckbOQ"

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

**Document how a CNAME should look by viewing the CNAME of www.theforce.net using NSLOOKUP.**  
$ nslookup -type=CNAME www.theforce.net

Server: cdns01.comcast.net

Address: 2001:558:feed::1

Non-authoritative answer:

www.theforce.net canonical name = theforce.net

**Explain why the sub page of resistance.theforce.net isn't redirecting to theforce.net.**resistance.theforce.net is not redirecting to theforce.net because the cname entry is missing in DNS record.

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

$ nslookup -type=CNAME resistance.theforce.net

Server: cdns01.comcast.net

Address: 2001:558:feed::1

Non-authoritative answer:

resistance.theforce.net canonical name = theforce.net

### Mission 4

**Confirm the DNS records for princessleia.site.**

$ nslookup -type=ANY princessleia.site 8.8.8.8

Server: dns.google

Address: 8.8.8.8

Non-authoritative answer:

princessleia.site internet address = 34.102.136.180

princessleia.site nameserver = ns25.domaincontrol.com

princessleia.site nameserver = ns26.domaincontrol.com

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)

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"

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

Add the backup DNS server to DNS record

$ nslookup -type=ANY princessleia.site 8.8.8.8

Server: dns.google

Address: 8.8.8.8

Non-authoritative answer:

princessleia.site internet address = 34.102.136.180

princessleia.site nameserver = ns25.domaincontrol.com

princessleia.site nameserver = ns26.domaincontrol.com

princessleia.site nameserver = ns2.galaxybackup.com

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)

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"

### Mission 5

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-I-L-Q-T-V-Jedha 23

### Mission 6

**Use the Dark Side's key to decrypt the wireless traffic in Wireshark.**

sysadmin@UbuntuDesktop:~/HW$ aircrack-ng HW\_09-Networking-Fundamentals-II-and-CTF-Review\_resources\_Darkside.pcap -w /usr/share/wordlists/rockyou.txt

Aircrack-ng 1.2 rc4

[00:00:00] 2280/8053877 keys tested (2759.69 k/s)

Time left: 48 minutes, 38 seconds 0.03%

KEY FOUND! [ dictionary ]

**Once you have decrypted the traffic, figure out the following Dark Side information:**

Found 3 ARP packets but 2 unique Sender IPs:

Sender IP address: 172.16.0.101 (172.16.0.101)

Sender MAC address: IntelCor\_55:98:ef (00:13:ce:55:98:ef)

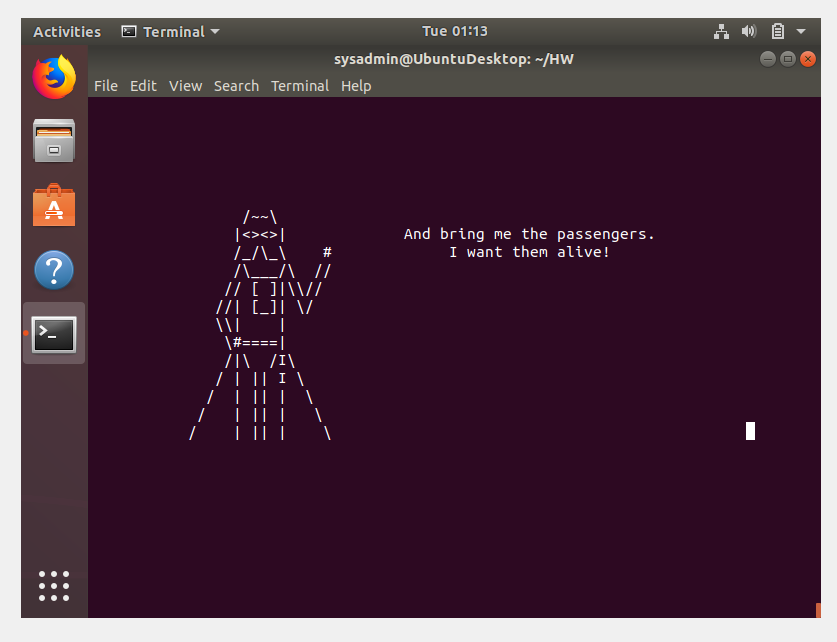
Sender IP address: 172.16.0.1 (172.16.0.1)

Sender MAC address: Cisco-Li\_e3:e4:01 (00:0f:66:e3:e4:01)

### 

### Mission 7

telnet towel.blinkenlights.nl



www.asciimation.co.nz

